NetVanta 2730

Getting Started Guide

NETWORK SECURITY APPLIANCE

ADTRAN®

ADTRAN NetVanta 2730 Getting Started Guide

This *Getting Started Guide* provides instructions for basic installation and configuration of the ADTRAN NetVanta 2730. After you complete this guide, computers on your Local Area Network (LAN) will have secure Internet access.

Document Contents

This document contains the following sections:

ADTRAN NetVanta 2730 Front Panel

LAN/WAN Port Status

Provides dedicated LAN/WAN port status as follows:

link/spd: ○ Off=10M
● Green=100M
● Amber=1,000M

activity: ● Solid=link
☼ Blinking=activity

10/100 Ethernet Port Status

Provides Ethernet port status as follows:

link/spd: ○ Off=10M
● Green=100M

activity: ● Solid=link
☼ Blinking=activity

PC Card Slot

(side of unit)
Provides an interface for the WWAN PC Card connection

Indicator LEDs

Provides power and test status
(refer to page 5)

USB Ports

For future application

10/100/1,000 Ethernet Port

Provides Ethernet port status as follows:

link/spd: ○ Off=10M
● Green=100M
● Amber=1,000M

activity: ● Solid=link
☼ Blinking=activity

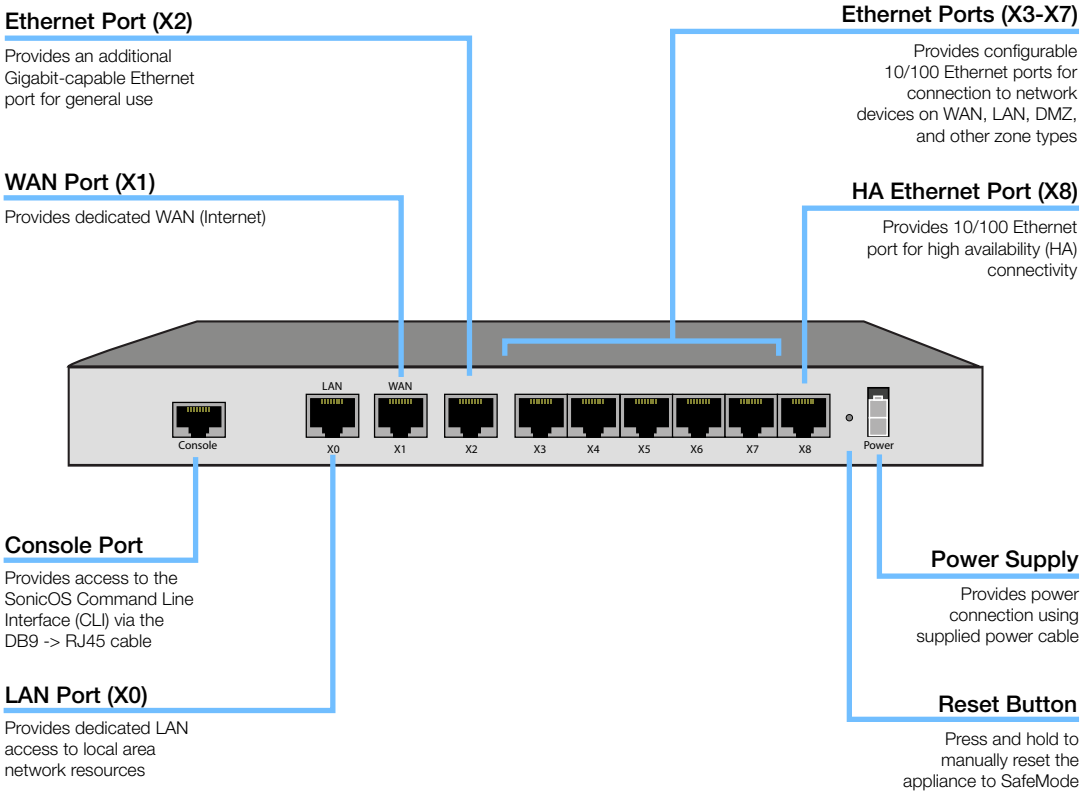
PC Card Status

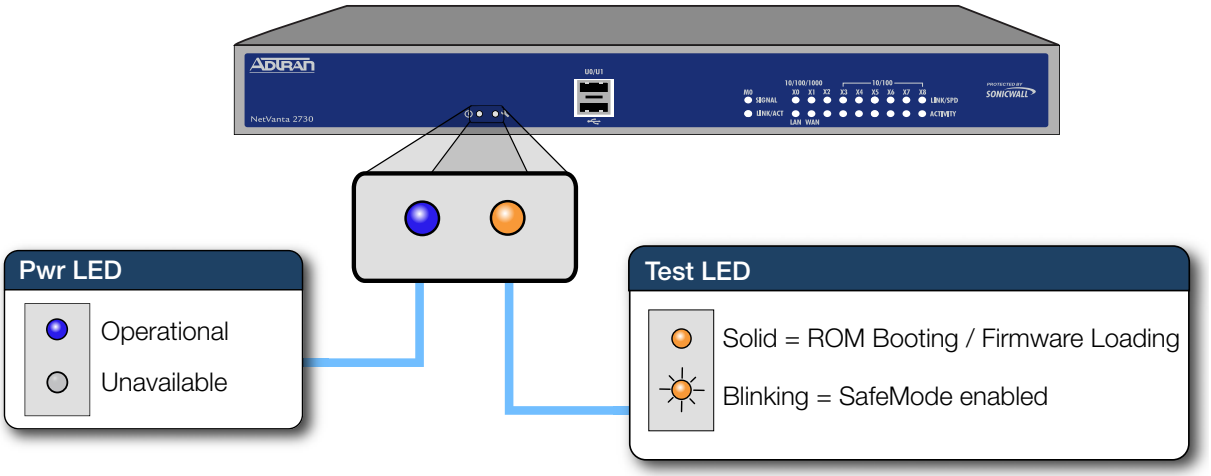
Provides WWAN PC Card status as follows:

signal: ● Green=connected
● Amber=negotiating

link/act: ● Solid=link
☼ Blinking=activity

ADTRAN NetVanta 2730 Rear Panel




NetVanta 2730
Pwr LED
Operational
Unavailable
Test LED
Solid = ROM Booting / Firmware Loading
Blinking = SafeMode enabled

Pre-Configuration Tasks 1

In this Section:

This section provides pre-configuration information. Review this section before setting up your ADTRAN NetVanta 2730 appliance.

Checking NetVanta 2730 Package Contents

Before setting up your NetVanta 2730 appliance, verify that your package contains the following parts:

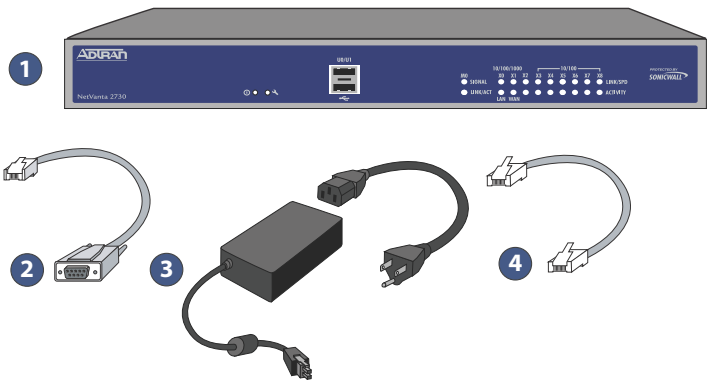
1. NetVanta 2730 Appliance
2. DB9 -> RJ45 (CLI) Cable
3. Standard Power Adaptor*
4. Ethernet Cable
5. Release Notes
6. Getting Started Guide

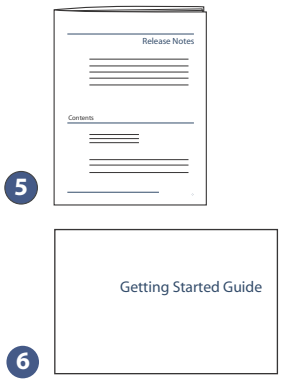
Any Items Missing?

If any items are missing from your package, please **contact ADTRAN support** at 1-888-4-ADTRAN.

A listing of the most current support documents are available online at: <http://www.adtran.com/support>

*The included power cord is intended for use in North America only. For European Union (EU) customers, a power cord is not included.





Obtaining Configuration Information

Record and keep for future reference the following setup information:

Registration Information

Serial Number:	Record the serial number found on the bottom panel of your ADTRAN appliance.
Authentication Code:	Record the authentication code found on the bottom panel of your ADTRAN appliance.

Networking Information

LAN IP Address: _____._____._____._____	Select a static IP address for your ADTRAN appliance that is within the range of your local subnet. If you are unsure, you can use the default IP address (192.168.168.168).
Subnet Mask: _____._____._____._____	Record the subnet mask for the local subnet where you are installing your ADTRAN appliance.
Ethernet WAN IP Address: _____._____._____._____	Select a static IP address for your Ethernet WAN. *This setting only applies if you are already using an ISP that assigns a static IP address.*

Administrator Information

Admin Name:	Select an administrator account name. (default is *admin)*
Admin Password:	Select an administrator password. (default is *password*)

Record the following information about your current ISP:

ISP 1

If you connect via	You likely use	Please record
Cable modem, DSL with a router	DHCP	*No Internet connection information is usually required*, although some service providers require a host name. Host Name: _____
Home DSL	PPPoE	User Name: _____ Password: _____ *Note: Your ISP may require your user name in the format: name@ISP.com*
T1/E1, Static broadband, Cable or DSL with a static IP	Static IP	IP Address: _____._____._____._____ Subnet Mask: _____._____._____._____ Default Gateway (IP Address): _____._____._____._____ Primary DNS: _____._____._____._____ Secondary DNS (optional): _____._____._____._____
Dial-in to a server	PPTP	Server Address: _____ User Name: _____ Password: _____

Record the following information about your secondary ISP:

ISP 2 (Optional for Multiple WAN Failover)

If you connect via	You likely use	Please record
Cable modem, DSL with a router	DHCP	Host Name: _____
Home DSL	PPPoE	User Name: _____ Password: _____ *Note: Your ISP may require your user name in the format: name@ISP.com*
T1/E1, Static broadband, Cable or DSL with a static IP	Static IP	IP Address: _____._____._____._____ Subnet Mask: _____._____._____._____ Default Gateway (IP Address): _____._____._____._____ Primary DNS: _____._____._____._____ Secondary DNS (optional): _____._____._____._____
Dial-in to a server	PPTP	Server Address: _____ User Name: _____ Password: _____

Obtaining WWAN Service Provider Information

Record the following information about your current WWAN service:

WWAN Service Provider

Country:	Record the country where you purchased your WWAN card.
Service Provider:	Record the service provider from whom you purchased your WWAN card. This is the brand name of the card.
Plan Type:	Record the plan type that you purchased from your provider. If you are unsure about this information, you may use **Standard** as the plan type.

WWAN Account Information

User Name/Password:	Some WWAN service providers require user specific information, such as a login and password. If your service provider requires it, you will need to provide such information during the setup process.

Note: ***WWAN Account Information*** *is automatically populated based on the chosen service provider and plan type. In most cases, if you selected the correct service provider and plan type the WWAN account information does not have to be altered.*

Verifying System Requirements

Before you begin the setup process, verify that you have:

- An Internet connection
- A Web browser supporting Java Script and HTTP uploads. Supported browsers include the following:

	Supported Browsers	**Browser Version Number**
	Internet Explorer	6.0 or higher
	Firefox	2.0 or higher
	Netscape	9.0 or higher
	Opera	9.10 or higher for Windows
	Safari	2.0 or higher for MacOS

Preparing Your WWAN PC Card

2

In this Section:

This section provides instructions to set up your WWAN PC card for use in the ADTRAN NetVanta 2730 appliance.

Alert: *DO NOT insert your PC card into the ADTRAN NetVanta 2730 appliance until you have completed the setup process for your card as described in this section.*

If your WWAN PC card is already registered and activated with your service provider and you are able to access the Internet through your PC using this card, you may skip this section and continue to *Registering Your Appliance - page 11*.

WWAN PC Card Setup

Complete the following steps to set up and provision your WWAN PC card. Verify at the www.adtran.com Website that your WWAN PC card and service provider are supported by the ADTRAN NetVanta 2730 appliance.

Alert: *DO NOT insert your PC card into the ADTRAN NetVanta 2730 appliance until you have completed the setup process for your card as described in this section and successfully accessed the Internet through your computer using the PC card.*

If you are using a GSM-based WWAN service provider, you may be required to remove the PIN protection from your SIM chip before using it with the appliance. Please contact your WWAN service provider for more information on setup and PIN removal procedures.

Activating Your PC Card Software

This section covers prerequisites necessary to set up most WWAN PC cards to work with the ADTRAN NetVanta 2730. Using an available desktop or laptop PC with Type II PC card slot, complete the following steps:

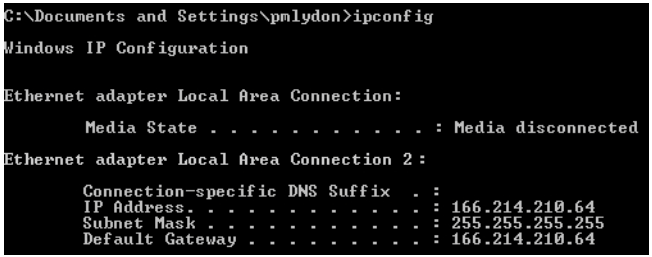
1. Install the software that came bundled with your WWAN PC card before activating the card.
2. When prompted, insert the WWAN PC card into an available Type II PC card slot on the Laptop or Desktop PC you are using for card configuration.
3. Install updates to your WWAN PC card, if available.
4. Activate your PC card, if required.

Verifying Your Connection

After activating the card on your PC, you can view your connection type and verify that the WWAN PC card is transferring data. For valid connection testing, it is important that you first disable all other network connections, such as a WiFi or LAN connection, before continuing. Leave only your PC card connection enabled.

1. Use the software that came with your WWAN PC card to initialize a connection with your service provider.
2. In the Windows interface, select **Start > Run**.
3. Enter **cmd** in the Open field and click the **OK** button.
4. At the prompt, type the command **ipconfig** and press **Enter** on the keyboard.
5. Your network device status will display. Verify that you have obtained an IP Address for your Ethernet adaptor, and that all other Local Area Network Connections display “Media disconnected” as their status.

Note: *The name of your **Ethernet adaptor** may differ from the screenshot below. Common names for newly acquired cards are “Local Area Connection 2” or “Local Area Connection 3.”*



6. Open a Web browser and navigate to a Website, such as <*http://www.adtran.com*>, to verify that your connection can transfer data.

Congratulations! You have set up and provisioned your WWAN PC card.

Registering Your Appliance

3

In this Section:

This section provides instructions for registering your ADTRAN NetVanta 2730 appliance.

Note: *Registration is an important part of the setup process and is necessary to receive the benefits of ADTRAN security services, firmware updates, and technical support.*

Before You Register

You need a NetVanta Security Portal account to register the ADTRAN NetVanta 2730 appliance. You can create a new NetVanta Security Portal account on www.adtran.com/NetVantaSecurityPortal or directly from the ADTRAN management interface. This section describes how to create an account by using the Website.

If you already have a NetVanta Security Portal account, go to *Registering and Licensing Your Appliance on NetVanta Security Portal - page 13* to register your appliance on NetVanta Security Portal. You can also postpone registration until after you set up the appliance. Skip ahead to *Deployment Scenarios - page 17* and register your appliance directly from the management interface once you reach *Activating Licenses* - page 40.

For a High Availability (HA) configuration, you must use NetVanta Security Portal to associate a backup unit that can share the Security Services licenses with your primary appliance.

If you do not yet have a NetVanta Security Portal account, you can use NetVanta Security Portal to register your ADTRAN appliance and activate or purchase licenses for Security Services, ViewPoint Reporting and other services, support, or software before you even connect your device. This method allows you to prepare for your deployment before making any changes to your existing network.

Note that your ADTRAN NetVanta 2730 appliance does not need to be powered on during account creation or during the registration and licensing process on www.adtran.com/NetVantaSecurityPortal.

Creating a NetVanta Security Portal Account

To create a NetVanta Security Portal account, perform the following steps:

1. In your browser, navigate to www.adtran.com/NetVantaSecurityPortal.
2. In the login screen, click the **Not a registered user?** link.

3. Complete the Registration form and click **Register**.
4. Verify the information is correct and click **Submit**.
5. In the screen confirming that your account was created, click **Continue**.

Registering and Licensing Your Appliance on NetVanta Security Portal

This section contains the following subsections:

Product Registration

You must register your ADTRAN security appliance on NetVanta Security Portal to enable full functionality.

1. Login to your NetVanta Security Portal account. If you do not have an account, you can create one at www.adtran.com/NetVantaSecurityPortal.
2. On the main page, type the appliance serial number in the **Register A Product** field. Then click **Next**.
3. On the My Products page, under **Add New Product**, type the friendly name for the appliance, select the **Product Group** if any, type the authentication code into the appropriate text boxes, and then click **Register**.
4. On the Product Survey page, fill in the requested information and then click **Continue**.

Licensing Security Services and Software

The Service Management - Associated Products page in NetVanta Security Portal lists security services, support options, and software that you can purchase or try with a free trial. For details, click the **Info** button. Your current licenses are indicated in the **Status** column with either a license key or an expiration date. You can purchase additional services now or at a later time.

The following products and services are available for the ADTRAN NetVanta 2730:

- **Service Bundles:**
  - Client/Server Anti-Virus Suite
  - Comprehensive Gateway Security Suite
- **Gateway Services:**
  - Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Firewall
  - Global Management System
  - Content Filtering: Premium Edition
  - Stateful High Availability Upgrade
- **Desktop and Server Software:**
  - Enforced Client Anti-Virus and Anti-Spyware
  - Global VPN Client
  - Global VPN Client Enterprise
- **Support Services:**
  - Dynamic Support 8x5
  - Dynamic Support 24x7
  - Software and Firmware Updates

Managing Licenses

To manage your licenses, perform the following tasks:

1. In the NetVanta Security Portal Service Management - Associated Products page, check the **Applicable Services** table for services that your ADTRAN appliance is already licensed for. Your initial purchase may have included security services or other software bundled with the appliance. These licenses are enabled on NetVanta Security Portal when the ADTRAN appliance is delivered to you.
2. If you purchased a service subscription or upgrade from a sales representative separately, you will have an **Activation Key** for the product. This key is emailed to you after online purchases, or is on the front of the certificate that was included with your purchase. Locate the product on the Service Management page and click **Enter Key** in that row.
3. In the Activate Service page, type or paste your key into the **Activation Key** field and then click **Submit**. Depending on the product, you will see an expiration date or a license key string in the **Status** column when you return to the Service Management page.

4. To license a product of service, do one of the following:
   - To try a Free Trial of a service, click **Try** in the Service Management page. A 30-day free trial is immediately activated. The Status page displays relevant information including the activation status, expiration date, number of licenses, and links to installation instructions or other documentation. The Service Management page is also updated to show the status of the free trial.
   - To purchase a product or service, click **Buy Now**.
5. In the Buy Service page, type the number of licenses you want in the **Quantity** column for either the 1 year, 2 year, or 3 year license row and then click **Add to Cart.**
6. In the Checkout page, follow the instructions to complete your purchase.

The NetVanta Security Portal server will generate a license key for the product. The key is added to the license keyset. You can use the license keyset to manually apply all active licenses to your ADTRAN appliance.

Registering a Second Appliance as a Backup

To ensure that your network stays protected if your ADTRAN appliance has an unexpected failure, you can purchase a license to associate a second appliance of the same model as the first in a High Availability (HA) pair. After registering and associating the second appliance, this appliance will automatically share the Security Services licenses of the primary appliance.

To register a second appliance and associate it with the primary, perform the following steps:

1. Login to your NetVanta Security Portal account.
2. On the main page, in the Register A Product field, type the appliance serial number and then click **Next**.
3. On the My Products page, under Add New Product, type the friendly name for the appliance, select the Product Group if any, type the authentication code into the appropriate text boxes, and then click **Register**.
4. On the Product Survey page, fill in the requested information and then click **Continue**. The Create Association Page is displayed.
5. On the Create Association Page, click the radio button to select the primary unit for this association, and then click **Continue**. The screen only displays units that are not already associated with other appliances.

6. On the Service Management - Associated Products page, scroll down to the Associated Products section to verify that your product registered successfully. You should see the HA Primary unit listed in the Parent Product section, as well as a Status value of **0** in the Associated Products / Child Product Type section.
7. Although the Stateful High Availability Upgrade and all the Security Services licenses can be shared with the HA Primary unit, you must purchase a separate ViewPoint license for the backup unit. This will ensure that you do not miss any reporting data in the event of a failover. Under Desktop & Server Software, click **Buy Now** for ViewPoint. Follow the instructions to complete the purchase.

To return to the Service Management - Associated Products page, click the serial number link for this appliance.

For information on configuring an HA pair, see *Scenario B: HA Pair in NAT/Route Mode* section, on page 24.

Registration Next Steps

Your ADTRAN NetVanta 2730 HA Pair is now registered and licensed on NetVanta Security Portal. To complete the registration process and for more information, see:

- *Accessing the Management Interface* - page 21
- *Activating Licenses* - page 40
- *Enabling Security Services* - page 40

Deployment Scenarios

4

In this Section:

This section provides detailed overviews of advanced deployment scenarios as well as configuration instructions for connecting your ADTRAN NetVanta 2730.

Tip: *Before completing this section, fill out the information in Obtaining Configuration Information - page 3. You will need to enter this information during the* ***Setup Wizard****.*

Initializing the NetVanta 2730

To begin deployment of your ADTRAN NetVanta 2730 appliance, first insert the WWAN PC card and then apply power to the appliance.

Inserting the WWAN PC Card

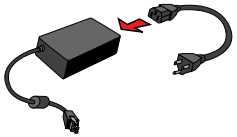
Before inserting the WWAN PC card into your ADTRAN NetVanta 2730 appliance, be sure your WWAN PC card is activated and unlocked. If you are not sure whether your card is unlocked or not, contact the PC card vendor to verify.

Alert: *Do not insert or remove the WWAN PC card while the ADTRAN NetVanta 2730 is powered on.*

1. Ensure that the ADTRAN NetVanta 2730 is **not** connected to a power source.
2. Insert your WWAN PC card “face up” into the PC CARD slot on the left side of the ADTRAN NetVanta 2730 appliance. The card should sit firmly in place.

Applying Power

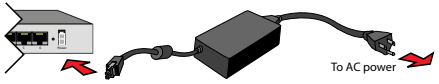
1. Connect the AC plug to the power supply.



2. Plug one end of the power supply to the back of the ADTRAN NetVanta 2730.

Warning: *ADTRAN power supplies are platform specific. Do not use power supplies from other ADTRAN platforms.*

3. *Connect the AC plug to an appropriate power outlet.*



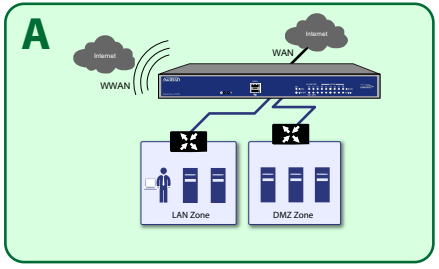
The Power LED on the front panel lights up blue when you plug in the ADTRAN NSA. The Test LED will light up and may blink while the appliance performs a series of diagnostic tests.
When the Power LED is lit and the Test LED is no longer lit, the ADTRAN NetVanta 2730 is ready for configuration. This typically occurs within a few minutes of applying power to the appliance. If the Test LED remains lit after the ADTRAN NetVanta 2730 appliance has been booted, restart the appliance by cycling power.

Selecting a Deployment Scenario

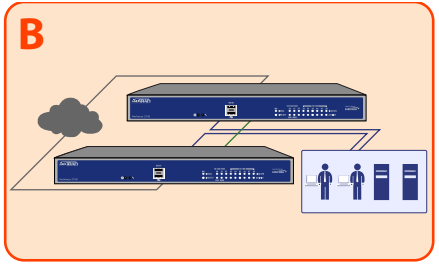
Before continuing, select a deployment scenario that best fits your network scheme. Reference the table below and the diagrams on the following pages for help in choosing a scenario.

Current Gateway Configuration	New Gateway Configuration	Use Scenario
No gateway appliance	Single ADTRAN NetVanta 2730 as a primary gateway.	**A** - NAT/Route Mode Gateway
	Pair of ADTRAN NetVanta 2730 appliances for high availability.	**B** - NAT with HA Pair
Existing Internet gateway appliance	ADTRAN NetVanta 2730 as replacement for an existing gateway appliance.	**A** - NAT/Route Mode Gateway
	ADTRAN NetVanta 2730 in addition to an existing gateway appliance.	**C** - Layer 2 Bridge Mode
Existing ADTRAN NetVanta 2730 gateway appliance	ADTRAN NetVanta 2730 in addition to an existing ADTRAN NetVanta 2730 gateway appliance.	**B** - NAT with HA Pair

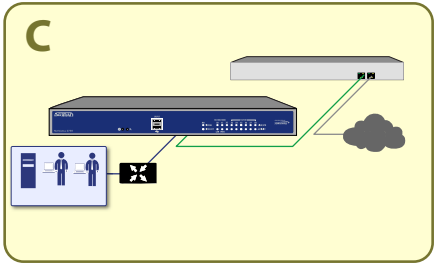
NAT/Route Mode Gateway



NAT with HA Pair

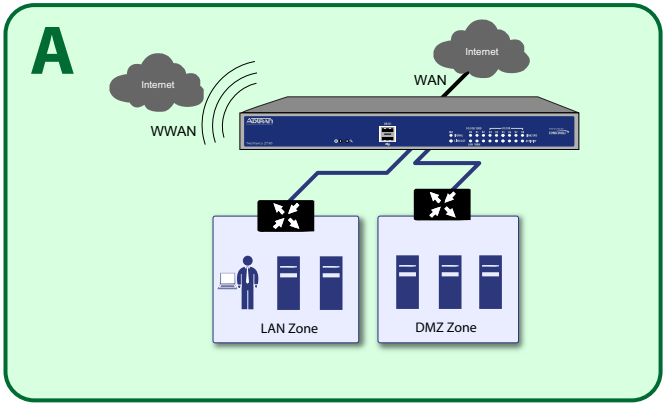


Layer 2 Bridge Mode



Scenario A: NAT/Route Mode Gateway

In this scenario, the ADTRAN NetVanta 2730 is configured in NAT/Route mode to operate as a single network gateway. Two Internet sources may be routed through the ADTRAN appliance for load balancing and failover purposes. Because only a single ADTRAN appliance is deployed, the added benefits of high availability with a stateful synchronized pair are not available.

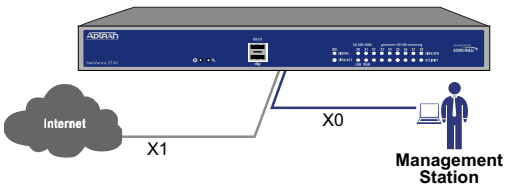


This section provides initial configuration instructions for connecting your ADTRAN NetVanta 2730. Follow these steps if you are setting up **Scenario A**.

This section contains the following subsections:

Connecting the WAN Port

1. Connect one end of an Ethernet cable to your Internet connection.
2. Connect the other end of the cable to the **X1** (**WAN**) port on your ADTRAN NetVanta appliance.



Connecting the LAN Port

1. Connect one end of the provided Ethernet cable to the computer you are using to manage the ADTRAN NetVanta 2730 appliance.
2. Connect the other end of the cable to the **X0** port on your ADTRAN NetVanta appliance.

   The Link LED above the **X0** (**LAN**) port will light up in green or amber depending on the link throughput speed, indicating an active connection:

   - Amber indicates 1 Gbps
   - Green indicates 100 Mbps
   - Unlit while the right (activity) LED is illuminated indicates 10 Mbps

Accessing the Management Interface

The computer you use to manage the ADTRAN NetVanta appliance must be set up to have an unused IP address on the 192.168.168.x/24 subnet, such as 192.168.168.20.

To access the Web-based management interface:

1. Start your Web browser. Remember to disable pop-up blocking software or add the management IP address http://192.168.168.168 to your pop-up blocker's allow list.
2. Enter **http://192.168.168.168** (the default LAN management IP address) in the **Location** or **Address** field.
3. The **ADTRAN Setup Wizard** launches and guides you through the configuration and setup of your ADTRAN NetVanta 2730 appliance.

The **Setup Wizard** launches only upon initial loading of the ADTRAN NetVanta 2730 management interface. You may also access the wizard by clicking on the **Wizards** icon in the toolbar.

4. Follow the on-screen prompts to complete the Setup Wizard. Depending on the changes made during your setup configuration, the appliance may restart.

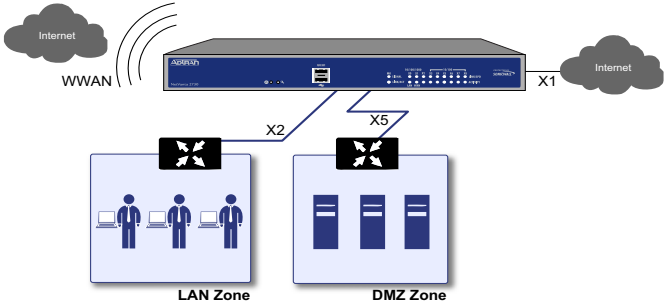
Troubleshooting Initial Setup

If you cannot connect to the ADTRAN NetVanta 2730 appliance or the **Setup Wizard** does not display, verify the following configurations:

- Did you correctly enter the management IP address in your Web browser?
- Are the Local Area Connection settings on your computer set to use DHCP or set to a static IP address on the 192.168.168.x/24 subnet?
- Do you have the Ethernet cable connected to your computer and to the **X0** (**LAN**) port on your appliance?
- Is the connector clip on your network cable properly seated in the port of the security appliance?

Note: *Some pop-up blockers may prevent the launch of the Setup Wizard. You can temporarily disable your pop-up blocker, or add the management IP address of your appliance (192.168.168.168 by default) to your pop-up blocker's allow list.*

Connecting to Your Network



The ADTRAN NetVanta 2730 ships with the internal DHCP server active on the LAN port. However, if a DHCP server is already active on your LAN, the appliance will disable its own DHCP server to prevent conflicts.

Ports X1 and X0 are preconfigured as WAN and LAN. The remaining ports (X2-X8) can be configured to meet the needs of your network. As an example, zones in the example above are configured as: X1: WAN, X2: LAN, and X5: DMZ.

Testing Your Connection

1. After you exit the Setup Wizard, the login page reappears. Log back into the management interface and verify your IP and WAN connection.
2. Ping a host on the Internet.
3. Open another Web browser and navigate to: <http://www.adtran.com>

   If you can view the ADTRAN home page, you have configured your ADTRAN NetVanta 2730 appliance correctly.

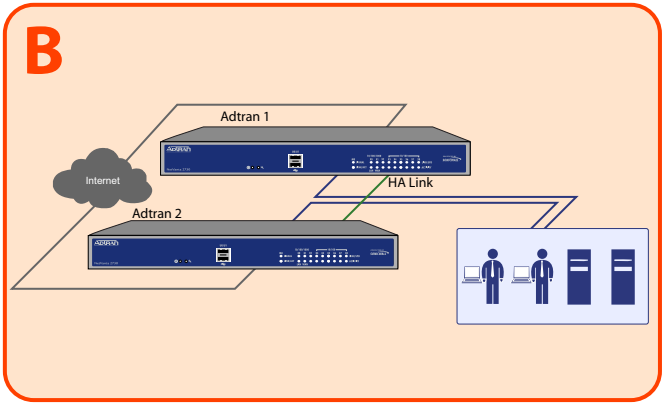
   If you cannot view the ADTRAN home page, renew your management station DHCP address.
4. If you still cannot view a Web page, try one of these solutions:
   - **Restart your Management Station** to accept new network settings from the DHCP server in the ADTRAN security appliance.
   - **Restart your Internet Router** to communicate with the DHCP Client in the ADTRAN security appliance.

Continue to Verifying Your Connection section, on page 35 to verify your WWAN connection.

Scenario B: HA Pair in NAT/Route Mode

For network installations with two ADTRAN NetVanta 2730 appliances configured as a stateful synchronized pair for redundant high availability networking.

In this scenario, one ADTRAN NetVanta 2730 operates as the primary gateway device and the other ADTRAN NetVanta 2730 is in passive mode. All network connection information is synchronized between the two devices so that the backup appliance can seamlessly switch to active mode without dropping any connections if the primary device loses connectivity.



This section provides instructions for configuring a pair of ADTRAN NetVanta 2730 appliances for High Availability (HA). This section is relevant to administrators following deployment **Scenario B**.

Note: *High Availability is supported for two ADTRAN NetVanta 2730 appliances of the same model.*

This section contains the following subsections:

Initial HA Setup

Before you begin the configuration of HA on the Primary ADTRAN security appliance, perform the following setup:

1. On the back panel of the Backup ADTRAN security appliance, locate the serial number and write the number down. You need to enter this number in the **High Availability** > **Settings** page.
2. Verify that the Primary appliance and Backup ADTRAN security appliances are registered and running the same ADTRAN Security services.
3. Make sure the Primary appliance and Backup ADTRAN security appliances' LAN, WAN and other interfaces are properly configured for failover.
4. Connect the X8 ports on the Primary appliance and Backup ADTRAN appliances with a CAT 5 Ethernet cable. The Primary and Backup security appliances must have a dedicated connection.
5. Power up the Primary ADTRAN security appliance, and then power up the Backup ADTRAN security appliance.
6. Do not make any configuration changes to the Primary's X8; the High Availability configuration in an upcoming step takes care of this issue.

Configuring HA

The first task in setting up HA after initial setup is configuring the **High Availability** > **Settings** page on the Primary ADTRAN security appliance. Once you configure HA on the Primary ADTRAN security appliance, it communicates the settings to the Backup ADTRAN security appliance.

To configure HA on the Primary appliance, perform the following steps:

7. Navigate to the **High Availability** > **Settings** page. Select the **Enable High Availability** checkbox.
8. 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 ADTRAN security appliance, or in the **System** > **Status** screen of the backup unit. The serial number for the Primary ADTRAN appliance is automatically populated.
9. Click **Apply** to retain these settings.

Configuring Advanced High Availability Settings

10. Navigate to the **High Availability** > **Advanced** page. To configure Stateful HA, select **Enable Stateful Synchronization**. A dialog box is displayed with recommended settings for the **Heartbeat Interval** and **Probe Interval** fields. The settings it shows are minimum recommended values. Lower values may cause unnecessary failovers, especially when the appliance is under a heavy load. You can use higher values if your appliance handles a lot of network traffic. Click **OK**.

Tip: *Preempt mode is recommended to be disabled after enabling Stateful Synchronization. This is because preempt mode can be over-aggressive about failing over to the backup appliance.*

11. To backup the firmware and settings when you upgrade the firmware version, select **Generate/Overwrite Backup Firmware and Settings When Upgrading Firmware**.
12. 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 WAN switch to which the two appliances are connected to needs to be notified. All outside devices will continue to route to the single shared MAC address.

13. The **Heartbeat Interval** controls how often the two units communicate. The default is 5000 milliseconds; the minimum recommended value is 1000 milliseconds. Less than this may cause unnecessary failovers, especially when the appliance is under a heavy load.
14. Typically, ADTRAN recommends leaving the **Heartbeat Interval**, **Election Delay Time (seconds)**, and **Dynamic Route Hold-Down Time** fields to their default settings. These fields can be tuned later as necessary for your specific network environment:
    - The **Failover Trigger Level** sets the number of heartbeats that can be missed before failing over. By default, this is set to 5 missed heartbeats.
    - The **Election Delay Time** is the number of seconds allowed for internal processing between the two units in the HA pair before one of them takes the primary role.
    - The **Probe Level** sets the interval in seconds between communication with upstream or downstream systems. 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.
    - The **Dynamic Route Hold-Down Time** setting is used when a failover occurs on a HA pair that is using either RIP or OSPF dynamic routing, and it is only displayed when the **Advanced Routing** option is selected on the **Network** > **Routing** page. 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.
15. Select the **Include Certificates/Keys** checkbox to have the appliances synchronize all certificates and keys.
16. Click **Synchronize Settings** to synchronize the settings between the Primary and Backup appliances.
17. Click **Synchronize Firmware** if you previously uploaded new firmware to your Primary unit while the Secondary unit was offline, and it is now online and ready to upgrade to the new firmware. **Synchronize Firmware** is typically used after taking your Secondary appliance offline while you test a new firmware version on the Primary unit before upgrading both units to it.
18. Click **Apply** to retain the settings on this screen.

Synchronizing Settings

Once you have configured the HA settings on the Primary ADTRAN security appliance, it will automatically synchronize the settings to the Backup unit, causing the Backup to reboot. You do not need to click the **Synchronize Settings** button. However, if you later choose to do a manual synchronization of settings, click the **Synchronize Settings** button. You will see a **HA Peer Firewall has been updated** notification at the bottom of the management interface page. Also note that the management interface displays **Logged Into: Primary ADTRAN Status: (green ball) Active** in the upper-right-hand corner.

By default, the **Include Certificate/Keys** setting is enabled. This specifies that certificates, certificate revocation lists (CRL), and associated 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 ADTRAN security appliances are functioning correctly, wait a few minutes, then trigger a test failover by logging into the Primary unit and doing a restart. The Backup ADTRAN security appliance should quickly take over.

From your management workstation, test connectivity through the Backup appliance by accessing a site on the public Internet – note that the Backup appliance, when active, assumes the complete identity of the Primary, including its IP addresses and Ethernet MAC addresses.

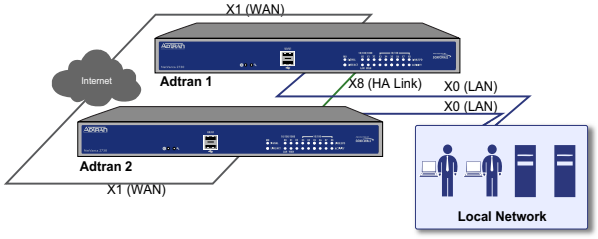
Log into the Backup appliance's unique LAN IP address. The management interface should now display **Logged Into: Backup ADTRAN Status: (green ball) Active** in the upper-right-hand corner.

Now, power the Primary appliance back on, wait a few minutes, then log back into the management interface. If stateful synchronization is enabled (automatically disabling preempt mode), the management GUI should still display **Logged Into: Backup ADTRAN Status: (green ball) Active** in the upper-right-hand corner.

If you are using the Monitor Interfaces feature, experiment with disconnecting each monitored link to ensure correct configuration.

Configuring HA License Overview

You can configure HA license synchronization by associating two ADTRAN security appliances as HA Primary and HA Secondary on NetVanta Security Portal. Note that the Backup appliance of your HA pair is referred to as the HA Secondary unit on NetVanta Security Portal.



You must purchase a single set of security services licenses for the HA Primary appliance. To use Stateful HA, you must first activate the Stateful High Availability Upgrade license for the primary unit on the interface. This is automatic if your appliance is connected to the Internet. See *Registering and Licensing Your Appliance on NetVanta Security Portal - page 13*.

License synchronization is used during HA so that the Backup appliance can maintain the same level of network protection provided before the failover. To enable HA, you can use the interface to configure your two appliances as a HA pair in Active/Idle mode.

NetVanta Security Portal 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. You can associate two units that are both already registered. Or you can select a registered unit and then add a new appliance with which to associate it.

Note: *After registering new ADTRAN appliances, you must also register each appliance from the management interface by clicking the registration link on the **System** > **Status** page. This allows each unit to synchronize with the ADTRAN license server and share licenses with the associated appliance.*

Associating Pre-Registered Appliances

To associate two already-registered ADTRAN security appliances so that they can use HA license synchronization, perform the following steps:

1. Login to NetVanta Security Portal and click **My Products**.
2. 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**.
3. On the Service Management - Associated Products page, scroll down to the Associated Products section.
4. Under Associated Products, click **HA Secondary**.
5. 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.
6. Select the group from the **Product Group** drop-down list. The product group setting specifies the NetVanta Security Portal users who can upgrade or modify the appliance.
7. Click **Register**.
8. Continue to *Additional Deployment Configuration - page 47*.

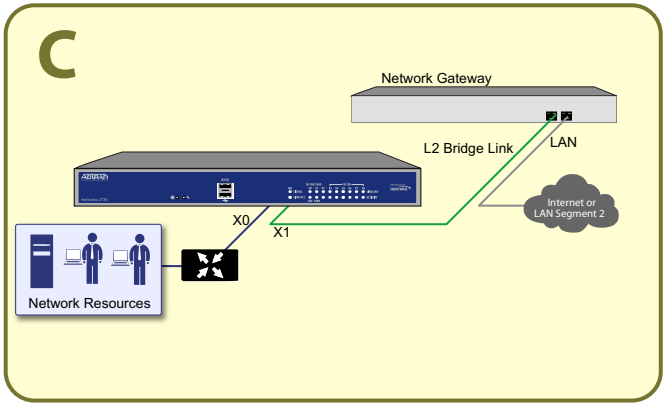
Continue to the Verifying Your Connection section, on page 35 to verify your WWAN connection.

Scenario C: L2 Bridge Mode

For network installations where the ADTRAN NetVanta 2730 is running in tandem with an existing network gateway.

In this scenario, the original gateway is maintained. The ADTRAN NetVanta 2730 is integrated seamlessly into the existing network, providing the benefits of deep packet inspection and comprehensive security services on all network traffic.

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 ADTRAN security appliance can be non-disruptively added to any Ethernet network to provide in-line deep packet inspection for all traversing IPv4 TCP and UDP traffic. L2 Bridge Mode can pass all traffic types, including IEEE 802.1Q VLANs, Spanning Tree Protocol, multicast, broadcast, and IPv6.

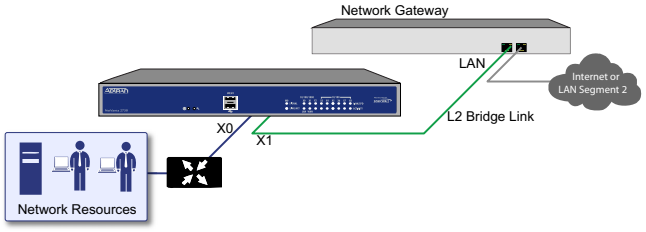


This section provides instructions to configure the ADTRAN NetVanta 2730 appliance in tandem with an existing Internet gateway device. This section is relevant to users following deployment **Scenario C**.

This section contains the following subsections:

Connection Overview

Connect the X1 port on your ADTRAN NetVanta 2730 to the LAN port on your existing Internet gateway device. Then connect the X0 port on your ADTRAN to your LAN.



Configuring the Primary Bridge Interface

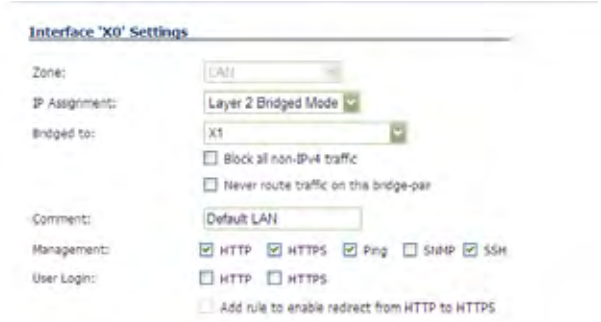
The primary bridge interface is your existing Internet gateway device. The only step involved in setting up your primary bridge interface is to ensure that the WAN interface is configured for a static IP address. You will need this static IP address when configuring the secondary bridge.

Note: *The primary bridge interface must have a static IP assignment.*

Configuring the Secondary Bridge Interface

Complete the following steps to configure the ADTRAN appliance:

1. Navigate to **Network** > **Interfaces**.
2. Click the Configure icon in the right column of the X0 (LAN) interface.



3. In the **IP Assignment** drop-down list, select **Layer 2 Bridge Mode**.
4. In the **Bridged to** drop-down list, select the **X1** interface.
5. Configure management options (HTTP, HTTPS, Ping, SNMP, SSH, User logins, or HTTP redirects).
6. Click **OK**.

Note: *Do not enable **Never route traffic on the bridge-pair** unless your network topology requires that all packets entering the L2 Bridge remain on the L2 Bridge segments.*

*You may optionally enable the **Block all non-IPv4 traffic** setting to prevent the L2 bridge from passing non-IPv4 traffic.*

Continue to Verifying Your Connection section, on page 35 to verify your WWAN connection.

Verifying Your Connection

5

In this Section:

This section provides instructions to ensure proper connectivity of your ADTRAN NetVanta 2730 appliance.

Verifying Management Interface Connectivity

1. If your appliance did not require a restart, skip to the *Verifying WAN (Internet) Connectivity* section, on page 36. Otherwise, continue with step 2.
2. Wait for the ADTRAN NetVanta 2730 to reboot. When the Test LED is no longer lit, the ADTRAN NetVanta 2730 is ready for login.
3. If the login page does not display after reboot, open a Web browser on the computer and manually navigate to the LAN IP address of your ADTRAN NetVanta 2730.
4. Using your new **username** and **password**, login to the appliance.

If the **System > Security Dashboard** page displays, then you have correctly configured the ADTRAN NetVanta 2730 to work with the computer on your LAN. Complete the next section to verify WAN (Internet) connectivity.

Verifying WAN (Internet) Connectivity

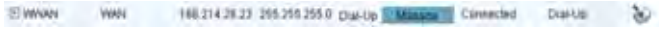
Complete the following steps to confirm your Internet connectivity.

1. In the Windows interface of a computer connected to the LAN port, select **Start > Run**.
2. Enter “cmd” in the **Open** field and click the **OK** button.
3. At the prompt, type the command “ping www.adtran.com” and press **Enter** on the keyboard.
   If the ping times out, you may have to renew your computer’s IP address.
4. If the ping is successful, use your Web browser to navigate to a Website, such as:
   <http://www.adtran.com/>
   If the Website displays, your ADTRAN NetVanta 2730 is configured correctly as your gateway device.

Viewing the WWAN Connection Status

The **Network > Interfaces** page allows you to view the current WWAN connection status.

1. Log into the ADTRAN NetVanta 2730 appliance management interface.
2. Navigate to **Network > Interfaces**.
3. In the Interface Settings section, the WWAN interface line displays the current status as follows:



The following messages describe the status of the WWAN interface:

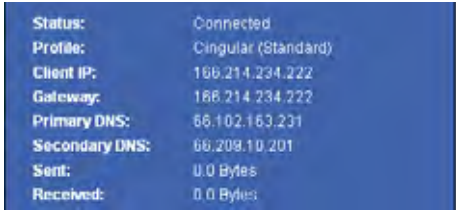
On hook	Indicates that the WWAN card is present but not yet connected.
Connected and starting PPP authentication	Indicates that the WWAN card is associated and currently attempting a connection to the WWAN network.
Connected	Indicates an active connection.

Managing the WWAN Connection Status

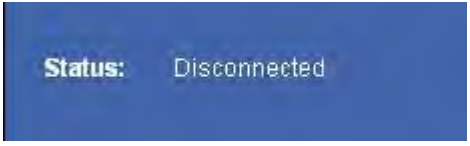
The Connection Manager window allows you to connect, disconnect, and view current WWAN connection status.

1. In the ADTRAN NetVanta 2730 appliance management interface, navigate to **Network > Interfaces**.
2. In the Interface Settings section, under WWAN, click the **Manage** button.

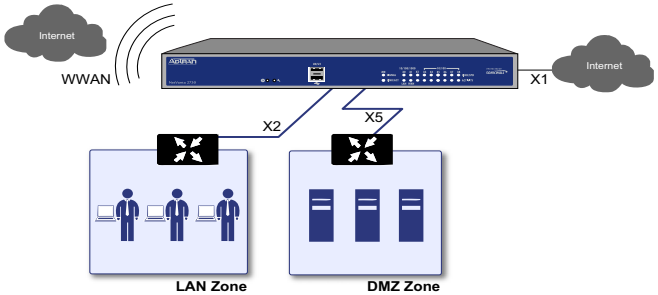
3. The Connection Manager windows displays your connection status.



4. If the Connection Manager shows “disconnected,” click the **Connect** button. You will connect to a network if one is available.



Verifying WWAN Failover Functionality



Complete the following steps to confirm your WWAN Internet connectivity.

1. Unplug your appliance's WAN port (if you plugged it in during the initial setup).
2. Wait a few moments for the NetVanta 2730 to failover to the WWAN for Internet connectivity. Refer to the front panel of the appliance to see when the WWAN PC card shows activity.
3. Launch a Website, such as <*http://www.adtran.com*> in a browser, using a computer that is connected to the ADTRAN NetVanta 2730 appliance and using the appliance as its sole Internet connection.

If the Website displays, your ADTRAN NetVanta 2730 is operational and connected to a valid WWAN service provider account. Remember to plug the WAN back in if you wish to use WWAN as a failover.

Enabling Essential Security Services

6

In this Section:

Security services are an essential component of a secure network deployment. This section provides instructions for registering and enabling security services on your ADTRAN NetVanta 2730 appliance.

Activating Licenses

After completing the registration process, you must perform the following tasks to activate your licenses and enable your licensed services from within the user interface:

- Activate licenses
- Enable security services
- Apply services to network zones

To activate licensed services, you can enter the license keyset manually, or you can synchronize all licenses at once with NetVanta Security Portal.

The Setup Wizard automatically synchronizes all licenses with NetVanta Security Portal if the appliance has Internet access during initial setup. If initial setup is already complete, you can synchronize licenses from the **System** > **Licenses** page.

Manual upgrade using the license keyset is useful when your appliance is not connected to the Internet. The license keyset includes all license keys for services or software enabled on NetVanta Security Portal. It is available on <http://www.adtran.com/NetVantaSecurityPortal>.

To activate licenses:

1. Navigate to the **System** > **Licenses** page.
2. Under Manage Security Services Online do one of the following:
   - Enter your NetVanta Security Portal credentials, then click the **Synchronize** button to synchronize licenses with NetVanta Security Portal.
   - Paste the license keyset into the **Manual Upgrade Keyset** field.
3. Click **Submit**.

Enabling Security Services

ADTRAN security services are key components of threat management. The core security services are Gateway Anti-Virus, Intrusion Prevention Services, and Anti-Spyware.

You must enable each security service individually in the user interface. See the following procedures to enable and configure the three security services that must be enabled:

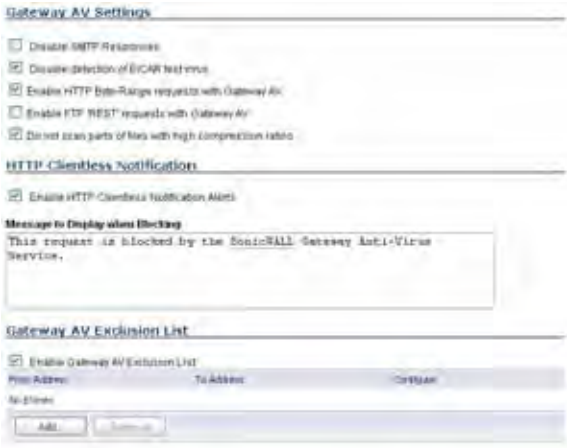
- *Enabling Gateway Anti-Virus - page 41*
- *Enabling Intrusion Prevention Services - page 42*
- *Enabling Anti-Spyware - page 43*
- *Enabling Content Filtering Service - page 44*

Enabling Gateway Anti-Virus

To enable Gateway Anti-Virus:

1. Navigate to the **Security Services** > **Gateway Anti-Virus** page. Select the **Enable Gateway Anti-Virus** checkbox.

2. Select the **Enable Inbound Inspection** checkboxes for the protocols to inspect. By default, ADTRAN GAV inspects all inbound **HTTP**, **FTP**, **IMAP**, **SMTP** and **POP3** traffic. **CIFS/ NetBIOS** can optionally be enabled to allow access to shared files. 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.
3. Enabling **Outbound Inspection** for SMTP scans mail for viruses before it is delivered to an internally hosted SMTP server.
4. For each protocol you can restrict the transfer of files with specific attributes by clicking on the **Settings** button under the protocol. In the Settings dialog box, you can configure the following:
   - **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 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 files that contain VBA macros.
   - **Restrict Transfer of packed executable files (UPX, FSG, etc.)** - Disables the transfer of packed executable files. Packers are utilities that compress and encrypt executables. Although there are legitimate applications for these, they can be used with the intent of obfuscation, and can 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,
5. Click **Configure Gateway AV Settings**. The **Gateway AV Settings** window allows you to configure clientless notification alerts and create a ADTRAN GAV exclusion list.



6. Select the **Disable SMTP Responses** box to suppress the sending of email messages to clients from ADTRAN GAV when a virus is detected in an email or attachment.
7. Select **Enable HTTP Clientless Notification Alerts** and customize the message to be displayed when GAV detects a threat from the HTTP server.
8. Select **Enable Gateway AV Exclusion List** and then click **Add** to define a range of IP addresses whose traffic will be excluded from ADTRAN GAV scanning.
9. When finished in the Add GAV Range dialog box, click **OK**.
10. In the Gateway AV Config View window, click **OK**.
11. In the **Security Services** > **Gateway Anti-Virus** page, click **Accept**.

Enabling Intrusion Prevention Services

To enable Intrusion Prevention Services:

1. Navigate to the **Security Services** > **Intrusion Prevention** page. Select the **Enable Intrusion Prevention** checkbox.

2. In the Signature Groups table, select the **Prevent All** and **Detect All** checkboxes for each attack priority that you want to prevent. Selecting the **Prevent All** and **Detect All** check boxes for **High Priority Attacks** and **Medium Priority Attacks** protects your network against the most dangerous and disruptive attacks.

3. To log all detected attacks, leave the **Log Redundancy Filter** field set to zero. To enforce a delay between log entries for detections of the same attack, enter the number of seconds to delay.
4. Click **Configure IPS Settings** to enable IP packet reassembly before inspection and create an ADTRAN IPS exclusion list.
5. In the IPS Config View window, select **Enable IPS Exclusion List** and then click **Add** to define a range of IP addresses whose traffic will be excluded from ADTRAN IPS scanning.
6. When finished in the Add IPS Range dialog box, click **OK**.
7. In the IPS Config View window, click **OK**.
8. In the **Security Services** > **Intrusion Prevention** page, click **Accept**.

Enabling Anti-Spyware

To enable Anti-Spyware:

1. Navigate to the **Security Services** > **Anti-Spyware** page. Select the **Enable Anti-Spyware** checkbox.

2. In the Signature Groups table, select the **Prevent All** and **Detect All** checkboxes for each spyware danger level that you want to prevent.

3. To log all spyware attacks, leave the **Log Redundancy Filter** field set to zero. To enforce a delay between log entries for detections of the same attack, enter the number of seconds to delay.
4. Click **Configure Anti-Spyware Settings** to configure clientless notification alerts and create an ADTRAN Anti-Spyware exclusion list.
5. Select the **Disable SMTP Responses** box to suppress the sending of email messages to clients from ADTRAN Anti-Spyware when spyware is detected in an email or attachment.
6. Select **Enable HTTP Clientless Notification Alerts** and customize the message to be displayed in the browser when ADTRAN Anti-Spyware detects a threat from the HTTP server.
7. Select **Enable Anti-Spyware Exclusion List** and then click **Add** to define a range of IP addresses whose traffic will be excluded from ADTRAN Anti-Spyware scanning.
8. When finished in the Add Anti-Spyware Range dialog box, click **OK**.
9. In the Anti-Spyware Config View window, click **OK**.
10. Select the **Enable Inbound Inspection** checkboxes for the protocols to inspect. By default, ADTRAN GAV inspects all inbound **HTTP**, **FTP**, **IMAP**, **SMTP**, and **POP3** traffic.
11. Select the **Enable Inspection of Outbound Communication** checkbox to enable scanning of traffic that originates internally.
12. On the **Security Services** > **Anti-Spyware** page, click **Accept**.

Enabling Content Filtering Service

The default Content Filtering Service (CFS) policy is available with or without a CFS subscription. The **Security Services > Content Filter** page provides links to purchase a license or get a free trial, and displays subscription status and basic configuration settings.

You can enforce or disable content filtering on each zone from the **Network > Zones** page, as described in the *Applying Security Services to Network Zones* section, on page 46.

With a valid CFS subscription, you can create custom CFS policies and apply them to network zones or to groups of users. For example, a school could create one policy for teachers and another for students.

Content Filtering Service (CFS) Bypass for Administrators

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 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, perform the following steps:

1. Select the **Do not bypass CFS blocking for the Administrator checkbox**.
2. Click **Accept**.

Enabling and Adding to the CFS Exclusion List

To enable the CFS Exclusion List and add a range of IP addresses to it, perform the following steps:

1. Select the **Enable CFS Exclusion List** checkbox.
2. Click **Add**. The **Add CFS Range Entry** window is displayed.
3. Enter the first IP address in the excluded range into the **IP Address From:** field and the last address into the **IP Address To:** field.
4. Click **OK**. The IP address range is added to the CFS Exclusion List.
5. On the **Security Services > Content Filter** page, click **Accept**.

Disabling, Editing, or Deleting Addresses from the CFS Exclusion List

You can temporarily disable CFS exclusions without removing all entries from the list. You can also delete some or all IP address ranges from the CFS Exclusion List.

1. To keep the CFS Exclusion List entries, but temporarily allow content filtering policies to be applied to these IP addresses, uncheck the **Enable CFS Exclusion List** checkbox. This disables CFS exclusions.
2. To edit a trusted domain entry, click the pencil icon in the Configure column.
3. To delete an individual trusted domain from the CFS Exclusion List, click the **Delete** icon for the entry in the Configure column.

4. To delete all trusted domains from the CFS Exclusion List, click **Delete All**.
5. On the **Security Services > Content Filter** page, click **Accept**.

Applying Security Services to Network Zones

A network zone is a logical group of one or more interfaces to which you can apply security rules to regulate traffic passing from one zone to another zone.

Security services such as Gateway Anti-Virus are automatically applied to the LAN and WAN network zones. To protect other zones such as the DMZ, you must apply the security services to the network zones.

To apply services to network zones:

1. Navigate to the **Network** > **Zones** page.
2. In the Zone Settings table, click the **Configure** icon for the zone where you want to apply security services.
3. In the Edit Zone dialog box on the General tab, select the checkboxes for the security services to enable on this zone.
4. On the Edit Zone page, select the checkboxes for the security services that you want to enable. Then, Click **OK**.
5. To enable security services on other zones, repeat steps 2 through step 4 for each zone.

Additional Deployment Configuration 7

In this Section:

This section provides basic configuration information to begin building network security policies for your deployment. This section also contains several diagnostic tools and a deployment configuration reference checklist.

Manually Configuring WWAN Failover

To manually configure WWAN Failover:

1. Navigate to the **WWAN** > **Connection Profiles** page. Under **Connection Profiles**, click **Add**.
2. On the **General** tab, specify **Country**, **Service Provider**, and **Plan Type**. Click **OK**.

Note: *If you are unsure about your Plan Type, select Standard.*

3. Next, navigate to the **Network** > **Interfaces** page.
4. Verify the **WAN Connection Model** is set to **Ethernet with WWAN Failover**.

Note: *If you WWAN service plan is bandwidth/time limited, enable **Configure Data Usage Limiting** to stay within your plan's limitations.*

Configuring Additional Interfaces

The Web-based management interface allows you to configure two ports as WAN interfaces. Port X1 is preconfigured as the WAN. You have the option of choosing another port (X2-X8) to configure as a second WAN interface.

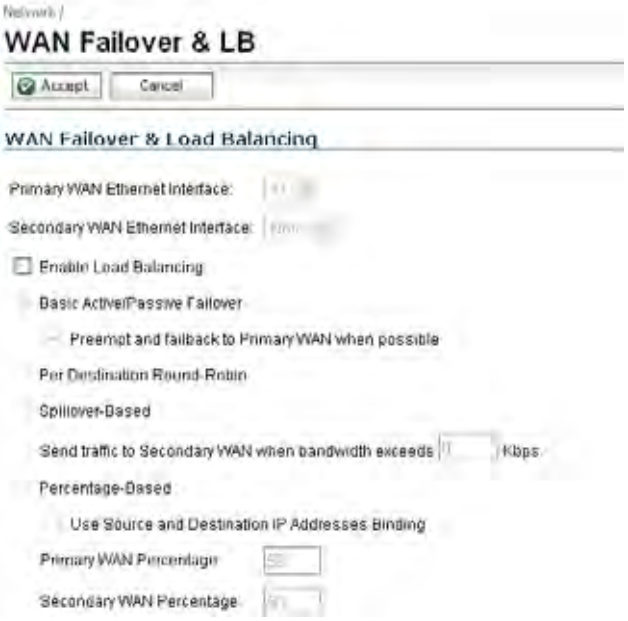
To configure a second WAN interface:

1. Click the Configure icon of the port you wish to configure as the second WAN interface.
2. In the **Zone** list, select **WAN**. Specify the settings for this interface. Click **OK** when you are finished.

Activating WAN Failover and Selecting the Load Balancing Method

To configure the appliance for WAN failover and load balancing, follow the steps below:

1. On the **Network > WAN Failover & LB** page, select Enable Load Balancing.



2. If there are multiple possible secondary WAN interfaces, select an interface from the **Secondary WAN Ethernet Interface**.
3. Select a load balancing method. By default, the appliance will select **Basic Active/Passive Failover** as a method, but there are four load balancing methods available:

- **Basic Active/Passive Failover**—Sends traffic through the Secondary WAN interface if the Primary WAN interface has been marked inactive. This item has an associated **Preempt and fail back to Primary WAN when possible** checkbox. When selected, the ADTRAN security appliance switches back to sending its traffic across the Primary WAN interface when it resumes responding to the ADTRAN security appliance's checks.
- **Per Destination Round-Robin**—Load balances outgoing traffic on a per-destination basis. This is a simple load balancing method that allows you to utilize both links in a basic fashion.
- **Spillover-Based**—When this setting is selected, the user can specify when the ADTRAN security appliance starts sending traffic through the Secondary WAN interface. Specify the maximum allowed bandwidth on the primary WAN interface in the **Send traffic to Secondary WAN interface when bandwidth exceeds _ Kbps** field.
- **Percentage-Based**—When this setting is selected, you can specify the percentages of traffic sent through the Primary WAN and Secondary WAN interfaces, utilizing both interfaces.
    - **Use Source and Destination IP Address Binding**—This checkbox enables you to maintain a consistent mapping of traffic flows with a single outbound WAN interface, regardless of the percentage of traffic through that interface.

4. Click **Accept**.

WAN Probe Monitoring

Enabling probe monitoring on the Network > WAN Failover & Load Balancing page instructs the ADTRAN security appliance to perform logical checks of upstream targets to ensure that the line is indeed usable, eliminating this potential problem, as well as continue to do physical monitoring. Under the default probe monitoring configuration, the appliance performs an ICMP ping probe of both WAN ports' default gateways. Unfortunately, this is also not an assured means of link monitoring because service interruption may be occurring further upstream.

To perform reliable link monitoring, you can choose ICMP or TCP as monitoring method, and can specify up to two targets for each WAN port. TCP is preferred because many devices on the public Internet now actively drop or block ICMP requests. If you specify two targets for each WAN interface, you can logically link the two probe targets such that if either one fails the line will go down, or that both must fail for the line to be considered down. Using the latter method, you can configure a sort of 'deep check' to see if the line is truly usable – for instance, you could set first probe target of your ISP's router interface using ICMP (assuming they allow this), and then do a secondary probe target of a DNS server on the public Internet using TCP Port 53. With this method, if the ICMP probe of the ISP's router fails but the farther upstream continues to respond, the ADTRAN security appliance assumes the link is usable and continues to send traffic across it.

Configuring PortShield Interfaces

The PortShield feature enables you to configure some or all of the switch ports on the ADTRAN NetVanta 2730 appliance into separate contexts, or PortShield interfaces, providing protection from traffic on the LAN, WAN, and DMZ, as well as the devices inside your network. Each context has its own wire-speed switch ports that have protection of a dedicated, deep-packet inspection firewall.

To Configure Switch Ports Using PortShield:

1. On the **Network** > **Interfaces** page, click the **PortShield Wizard** button. This will run the PortShield Setup Wizard. Read the Introduction and click **Next**.
2. Select the appropriate groupings of SwitchPort interfaces for the ADTRAN NetVanta 2730 appliance. Click **Next** to continue.This will prompt a configuration summary to appear. Verify the ports assigned are correct.
3. Click **Apply** to change port assignments.

Note: *If you select* WAN/DMZ/LAN Switch*, the X3-X8 ports will all be in a single PortShield group. Navigate to* ***Network*** > ***Interfaces*** *to enable or disable PortShield on each port.*

Creating Network Access Rules

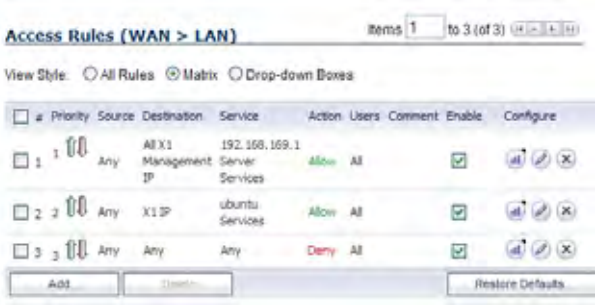
A Zone is a logical grouping of one or more interfaces designed to make management, such as the definition and application of access rules, a simpler and more intuitive process than following a strict physical interface scheme.

By default, the ADTRAN security appliance's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic from the Internet to the LAN. The following behaviors are defined by the "Default" stateful inspection packet access rule enabled in the ADTRAN security appliance:

Originating Zone	Destination Zone	Action
LAN	WAN, DMZ	Allow
DMZ	WAN	Allow
WAN	DMZ	Deny
WAN and DMZ	LAN	Deny

To create an access rule:

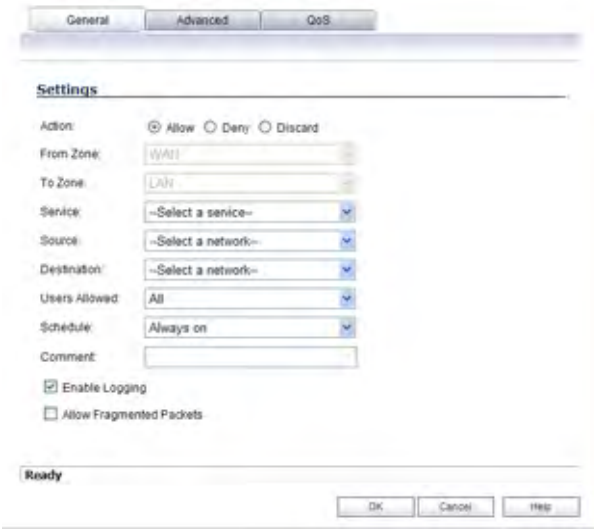
1. On the **Firewall** > **Access Rules** page in the matrix view, select two zones that will be bridged by this new rule.
   - On the Access Rules page, click **Add**.



The access rules are sorted from the most specific at the top to the least specific at the bottom of the table. At the bottom of the table is the **Any** rule.

Note: *The default firewall rules are set in this way for ease of initial configuration, but do not reflect best practice installations. Firewall rules should only allow the required traffic and deny all other traffic.*

2. In the Add Rule page in the **General** tab, select **Allow** or **Deny** or **Discard** from the **Action** list to permit or block IP traffic.



- Select the service or group of services affected by the access rule from the **Service** drop-down list. 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.
- Select the source of the traffic affected by the access rule from the **Source** drop-down list. Selecting **Create New Network** displays the **Add Address Object** window.
- Select the destination of the traffic affected by the access rule from the **Destination** drop-down list. Selecting **Create New Network** displays the **Add Address Object** window.
- Select a user or user group from the **Users Allowed** drop-down list.
- Select a schedule from the **Schedule** drop-down list. The default schedule is **Always on**.
- Enter any comments to help identify the access rule in the **Comments** field.

3. Click on the **Advanced** tab.

   - In the **TCP Connection Inactivity Timeout (minutes)** field, set the length of TCP inactivity after which the access rule will time out. The default value is **15** minutes.
   - In the **UDP Connection Inactivity Timeout (minutes)** field, set the length of UDP inactivity after which the access rule will time out. The default value is **30** minutes.
   - In the **Number of connections allowed (% of maximum connections)** field, specify the percentage of maximum connections that is allowed by this access rule. The default is 100%.
   - Select **Create a reflexive rule** to create a matching access rule for the opposite direction, that is, from your destination back to your source.
4. Click on the **QoS** tab to apply DSCP or 802.1p Quality of Service coloring/marking to traffic governed by this rule.
5. Click **OK** to add the rule.

Creating a NAT Policy

The Network Address Translation (NAT) engine allows users to define granular NAT policies for their incoming and outgoing traffic. By default, the ADTRAN security appliance has a preconfigured NAT policy to perform Many-to-One NAT between the systems on the LAN and the IP address of the WAN interface. The appliance does not perform NAT by default when traffic crosses between the other interfaces.

You can create multiple NAT policies on an appliance for the same object – for instance, you can specify that an internal server uses one IP address when accessing Telnet servers, and uses a different IP address for all other protocols. Because the NAT engine supports inbound port forwarding, it is possible to access multiple internal servers from the WAN IP address of the ADTRAN security appliance. The more granular the NAT Policy, the more precedence it takes.

Before configuring NAT Policies, you must create all Address Objects that will be referenced by the policy. For instance, if you are creating a One-to-One NAT policy, first create Address Objects for your public and private IP addresses.

Address Objects are one of four object classes: Address, User, Service, and Schedule. Once you define an Address Object, it becomes available for use wherever applicable throughout the management interface. For example, consider 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, you can create an Address Object to store the Web server's IP address. This Address Object, "My Web Server," can then be used in any configuration screen that employs Address Objects as a defining criterion.

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.
- **Range –** Range Address Objects define a range of contiguous IP addresses.
- **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.
- **MAC Address –** MAC Address Objects allow for the identification of a host by its hardware address or MAC (Media Access Control) address.
- **FQDN Address –** FQDN Address Objects allow for the identification of a host by its Fully Qualified Domain Names (FQDN), such as www.adtran.com.

The number of default Address Objects that cannot be modified or deleted are displayed. You can use the default Address Objects when creating a NAT policy, or you can create custom Address Objects to use. All Address Objects are available in the drop-down lists when creating a NAT policy.

Creating 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 ADTRANsecurity appliance.

To add an Address Object:

1. Navigate to the **Network** > **Address Objects** page.
2. Below the **Address Objects** table, click **Add**.
3. In the **Add Address Object** dialog box, enter a name for the Address Object in the **Name** field.

4. Select the zone to assign to the Address Object from the **Zone Assignment** drop-down list.
5. Select **Host**, **Range**, **Network**, **MAC**, or **FQDN** from the **Type** menu.
   - For **Host**, enter the IP address in the **IP Address** field.
   - For **Range**, enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.
   - For **Network**, enter the network IP address and netmask in the **Network** and **Netmask** fields.
   - For **MAC**, enter the MAC address in the **MAC Address** field.
   - For **FQDN**, enter the domain name for the individual site or range of sites (with a wildcard) in the **FQDN** field.
6. Click **OK**.

Configuring NAT Policies

NAT policies allow you 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. The following NAT configurations are available:

- Many-to-One NAT Policy
- Many-to-Many NAT Policy
- One-to-One NAT Policy for Outbound Traffic
- One-to-One NAT Policy for Inbound Traffic (Reflexive)
- One-to-Many NAT Load Balancing

- Inbound Port Address Translation via One-to-One NAT Policy
- Inbound Port Address Translation via WAN IP Address

This section describes how to configure a One-to-One NAT policy. One-to-One is the most common NAT policy used to route traffic to an internal server, such as a Web server. Most of the time, this means that incoming requests from external IPs are translated from the IP address of the ADTRAN security appliance WAN port to the IP address of the internal Web server. An example configuration illustrates the use of the fields in the Add NAT Policy procedure. To add a One-to-One NAT policy that allows all Internet traffic to be routed through a public IP address, two policies are needed: one for the outbound traffic, and one for the inbound traffic.

To add the components of a One-to-One NAT policy, perform the following steps:

1. Navigate to the **Network** > **NAT Policies** page. Click **Add**. The **Add NAT Policy** dialog box displays.
2. For **Original Source**, select **Any**.
3. For **Translated Source**, select **Original**.
4. For **Original Destination**, select **X0 IP**.
5. For **Translated Destination**, select **Create new address object** and create a new address object using **WAN** for Zone Assignment and **Host** for Type.
6. For **Original Service**, select **HTTP**.
7. For **Translated Service,** select **Original**.
8. For **Inbound Interface**, select **X0**.
9. For **Outbound Interface**, select **Any**.
10. For **Comment**, enter a short description.
11. Select the **Enable NAT Policy** checkbox.
12. Select the **Create a reflexive policy** checkbox if you want a matching NAT Policy to be automatically created in the opposite direction. This will create the outbound as well as the inbound policies.
13. Click **Add**.

Policies for subnets behind the other interfaces of the ADTRAN security appliance can be created by emulating these steps. Create a new NAT policy in which you adjust the source interface and specify the **Original Source**: the subnet behind that interface.

Upgrading Firmware on Your ADTRAN

Obtaining the Latest Firmware

1. To obtain a new firmware image file for your ADTRAN security appliance, connect to your NetVanta Security Portal account at: <http://www.adtran.com/NetVantaSecurityPortal>
2. Copy the new image file to a convenient location on your management station.

Saving a Backup Copy of Your Preferences

Before beginning the update process, make a system backup of your ADTRAN security appliance configuration settings. The backup feature saves a copy of the current configuration settings on your ADTRAN security appliance, protecting all your existing settings in the event that it becomes necessary to return to a previous configuration state. The System Backup shows you the current configuration and firmware in a single, clickable restore image.

In addition to using the backup feature to save your current configuration state to the ADTRAN security appliance, you can export the configuration preferences file to a directory on your local management station. This file serves as an external backup of the configuration preferences, and can be imported back into the ADTRAN security appliance.

Perform the following procedures to save a backup of your configuration settings and export them to a file on your local management station:

1. On the **System** > **Settings** page, click **Create Backup**. Your configuration preferences are saved. The System Backup entry is displayed in the **Firmware Management** table.
2. To export your settings to a local file, click **Export Settings**. A popup window displays the name of the saved file.

Upgrading the Firmware with Current Settings

Perform the following steps to upload new firmware to your ADTRAN appliance and use your current configuration settings upon startup.

The appliance must be properly registered before it can be upgraded. Refer to *Registering and Licensing Your Appliance on NetVanta Security Portal - page 13* for more information.

1. Download the firmware image file from NetVanta security Portal and save it to a location on your local computer.
2. On the **System** > **Settings** page, click **Upload New Firmware**.
3. Browse to the location where you saved the firmware image file, select the file and click the **Upload** button.
4. On the **System** > **Settings** page, click the **Boot** icon in the row for **Uploaded Firmware**.

Note: On the **System** > **Settings** page, click the **Boot** icon in the row for **Uploaded Firmware with Factory Default Settings**.

5. In the confirmation dialog box, click **OK**. The appliance restarts and then displays the login page.
6. Enter your user name and password. Your new image version information is listed on the **System** > **Settings** page.

Using SafeMode to Upgrade Firmware

If you are unable to connect to the ADTRAN security appliance's management interface, you can restart the ADTRAN security appliance in SafeMode. The SafeMode feature allows you to recover quickly from uncertain configuration states with a simplified management interface that includes the same settings available on the **System** > **Settings** page.

To use SafeMode to upgrade firmware on the ADTRAN security appliance, perform the following steps:

1. Connect your computer to the X0 port on the ADTRAN appliance and configure your IP address with an address on the 192.168.168.0/24 subnet, such as 192.168.168.20.
2. To configure the appliance in SafeMode, perform one of the following:
   - Use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the reset button on the back of the security appliance for one second. The reset button is in a small hole next to the power supply.
   - The Test light starts blinking when the ADTRAN security appliance has rebooted into SafeMode.
3. Point the Web browser on your computer to **192.168.168.168**. The SafeMode management interface displays.
4. If you have made any configuration changes to the security appliance, select the **Create Backup On Next Boot** checkbox to make a backup copy of your current settings. Your settings will be saved when the appliance restarts.
5. Click **Upload New Firmware**, and then browse to the location where you saved the firmware image, select the file and click the **Upload** button.
6. Select the boot icon in the row for one of the following:
   - **Uploaded Firmware - New!**
     Use this option to restart the appliance with your current configuration settings.
   - **Uploaded Firmware with Factory Defaults - New!**
     Use this option to restart the appliance with default configuration settings.
7. In the confirmation dialog box, click **OK** to proceed.
8. After successfully booting the firmware, the login screen is displayed. If you booted with factory default settings, enter the default user name and password (admin / password) to access the ADTRAN management interface.

Note: *Remember to change your IP address settings back to DHCP. Otherwise, you may not be able to connect to the Internet.*

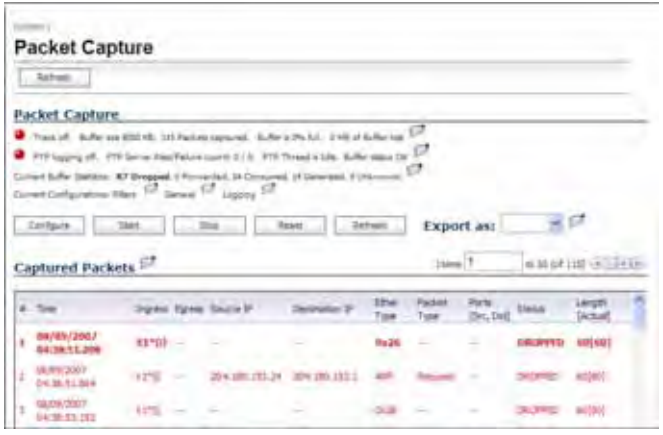
Troubleshooting Diagnostic Tools

Several diagnostic tools are provided to help you maintain your network and troubleshoot problems. Several tools can be accessed on the **System** > **Diagnostics** page, and others are available on other screens.

This section contains the following subsections:

Using Packet Capture

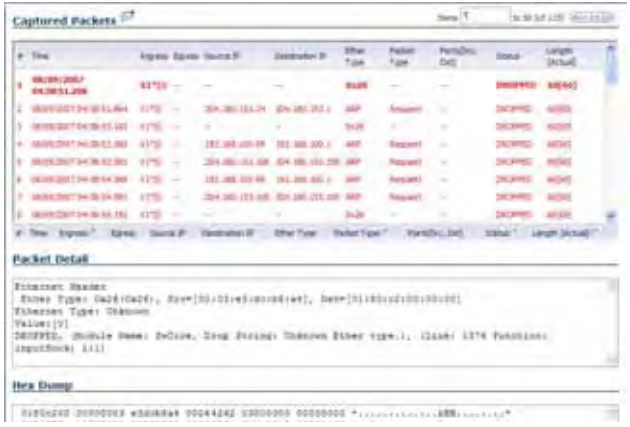
Packet Capture allows you to capture and examine the contents of individual data packets that traverse your ADTRAN firewall appliance. The captured packets contain both data and addressing information. The **System** > **Packet Capture** page provides a way to configure the capture criteria, display settings and file export settings, and displays the captured packets.



The Packet Capture screen has buttons for starting and stopping a packet capture. If you simply click **Start** without any configuration, 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**.

The user interface provides three windows to display different views of the captured packets:

- Captured Packets
- Packet Detail
- Hex Dump

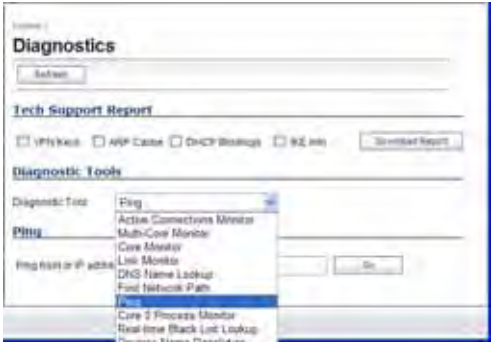


Click the **Configure** button to customize the settings for the capture. Once the configuration is complete, click **Start** to begin capturing packets. The settings available in the five main areas of configuration are summarized below:

- **General** – number of bytes to capture, wrap capture buffer
- **Capture Filter** – interfaces, packet types, source/ destination
- **Display Filter** – interfaces, packet types, source/ destination
- **Logging** – automatic transfer of buffer to FTP server
- **Advanced** – generated packets, syslog, management

Using Ping

Ping is available on the **System** > **Diagnostics** page.



The Ping test bounces a packet off a machine on the Internet and returns it to the sender. This test shows if the ADTRAN security appliance 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.

Using the Active Connections Monitor

The **Active Connections Monitor** displays real-time, exportable (plain text or CSV), filterable views of all connections to and through the ADTRAN security appliance. This tool is available on the **Systems** > **Diagnostics** page.

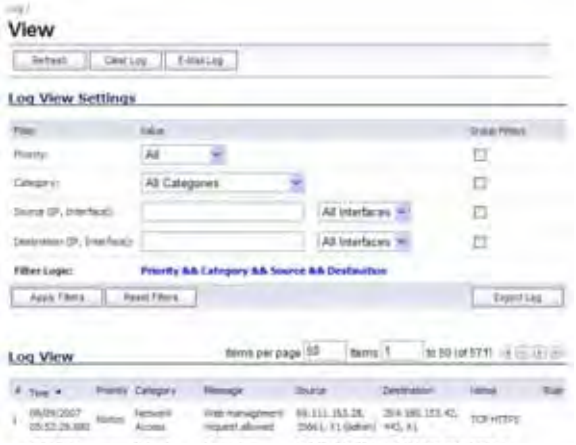
You can filter the results to display only connections matching certain criteria. You can filter by **Source IP**, **Destination IP**, **Destination Port**, **Protocol**, **Src Interface**, and **DST Interface**. Enter your filter criteria in the **Active Connections Monitor Settings** table. The fields you enter values into are combined into a search string with a logical **AND**. Select the **Group Filters** box next to any two or more criteria to combine them with a logical **OR**.

Using the Log > View Page

The ADTRAN security appliance maintains an Event log for tracking potential security threats. You can view the log in the **Log** > **View** page, or it can be automatically sent to an email address for convenience and archiving. The log is displayed in a table and can be sorted by column.

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**).

The fields you enter values into are combined into a search string with a logical **AND**. Select the **Group Filters** box next to any two or more criteria to combine them with a logical **OR**.



In this Section:

This section provides regulatory, trademark, and copyright information.

Note: *Safety and Regulatory compliance in this section is based on SonicWALL, Inc. regulatory model / type as shown.*

Regulatory Model/Type	Product Name
APL19-05C	NetVanta 2730

Mounting the appliance

- Mount in a location away from direct sunlight and sources of heat. A maximum ambient temperature of 104º F (40º C) is recommended.
- Route cables away from power lines, fluorescent lighting fixtures, and sources of noise such as radios, transmitters, and broadband amplifiers
- The included power cord is intended for use in North America only. For European Union (EU) customers, a power cord is not included.
- Ensure that no water or excessive moisture can enter the unit.
- Allow unrestricted airflow around the unit and through the vents on the side of the unit. A minimum of 1 inch (25.44mm) clearance is recommended.
- Consideration must be given to the connection of the equipment to the supply circuit and the effect of overloading the circuits has minimal impact on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings must be used when addressing this concern.

Lithium Battery Warning

The Lithium Battery used in the ecurity appliance may not be replaced by the user. Return the security appliance to an authorized service center for replacement with the same or equivalent type recommended by the manufacturer. If, for any reason, the battery or security appliance must be disposed of, do so following the battery manufacturer's instructions.

Cable Connections

All Ethernet and RS232 (Console) cables are designed for intra-building connection to other equipment. Do not connect these ports directly to communication wiring or other wiring that exits the building where the product is located.

Power Supply Information

If the power supply is missing from your ADTRAN product package, please contact ADTRAN Customer Support Services (1-888-4-ADTRAN) for a replacement. This product should only be used with a UL listed power supply marked I.T.E. LPS, with an output rated 12 VDC, minimum 3.0 A.

Weitere Hinweise zur Montage

- Wählen Sie für die Montage einen Ort, der keinem direkten Sonnenlicht ausgesetzt ist und sich nicht in der Nähe von Wärmequellen befindet. Die Umgebungstemperatur darf nicht mehr als 40 °C betragen.
- Führen Sie die Kabel nicht entlang von Stromleitungen, Leuchtstoffröhren und Störquellen wie Funksendern oder Breitbandverstärkern.
- Das beigefügte Netzkabel ist nur für den Betrieb in Nordamerika vergesehen. Für Kunden in der Europäischen Union ist kein Kabel beigefügt.
- Stellen Sie sicher, dass das Gerät vor Wasser und hoher Luftfeuchtigkeit geschützt ist.
- Stellen Sie sicher, dass die Luft um das Gerät herum zirkulieren kann und die Lüftungsschlitze an der Seite des Gehäuses frei sind. Hier ist ein Belüftungsabstand von mindestens 26 mm einzuhalten.
- Vergewissern Sie sich, dass das Gerät sicher im Rack befestigt ist.

Hinweis zur Lithiumbatterie

Die in der Internet Security Appliance von verwendete Lithiumbatterie darf nicht vom Benutzer ausgetauscht werden. Zum Austauschen der Batterie muss die in ein von autorisiertes Service-Center gebracht werden. Dort wird die Batterie durch denselben oder entsprechenden, vom Hersteller empfohlenen Batterietyp ersetzt. Beachten Sie bei einer Entsorgung der Batterie oder der Internet Security Appliance die diesbezüglichen Anweisungen des Herstellers.

Kabelverbindungen

Alle Ethernet- und RS232-C-Kabel eignen sich für die Verbindung von Geräten in Innenräumen. Schließen Sie an die Anschlüsse der Produkt keine Kabel an, die aus dem Gebäude herausgeführt werden, in dem sich das Gerät befindet.

Informationen zur Stromversorgung

Sollte das Netzteil nicht im Lieferumfang der ADTRAN enthalten sein, wenden Sie sich diesbezüglich an den technischen Support von ADTRAN. Dieses Produkt darf nur in Verbindung mit einem nach den Normen der Underwriter Laboratories, USA als „UL-gelistet“ zugelassenen Netzteil der Kategorie „I.T.E. LPS“ verwendet werden. Ausgang: 12 VDC Gleichsspannung, mind. 3.0 A.

FCC Part 15 Class B Notice

NOTE: This equipment was tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. And, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from the receiver connection.
- Consult ADTRAN (1-888-4-ADTRAN) for assistance.

Complies with EN55022 Class B and CISPR22 Class B.
*Refer to the label on the bottom of the unit for device information including Class A or Class B FCC information.

Canadian Radio Frequency Emissions Statement

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Declaration of Conformity

Application of council Directive	2004/108/EC (EMC) and 2006/95/EC (LVD)
Standards to which conformity is declared	EN 5502 (2006) +A (2007) Class A EN 55024 (1998) +A1 (2001), +A2 (2003) EN 61000-3-2 (2006) EN 61000-3-3 (2008) EN 60950-1 +A11 (2006) National Deviations: AT, AU, BE, CH, CN, CZ, DE, DK, FI, FR, GB, GR, HU, IE, IL, IN, IT, JP, KR, NL, NO, PL, SE, SG, SI

VCCI Statement

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

Caution: Modifying this equipment or using this equipment for purposes not shown in this manual without the written consent of SonicWALL could void the user's authority to operate this equipment.

Regulatory Information for Korea

방송통신위원회	Ministry of Information and Telecommunication Certification Number “SWL-APL-19-05C”

All products with country code “” (blank) and “A” are made in the USA.
All products with country code “B” are made in China.
All products with country code “C” or “D” are made in Taiwan R.O.C.
All certificates held by Secuwide, Corp.

A급 기기 (업무용 정보통신기기)

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 만약 잘못판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Copyright Notice

Trademarks

ADTRAN is a registered trademark of ADTRAN.

Microsoft Windows 98, Windows Vista, Windows 2000, Windows XP, Windows Server 2003, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

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.

Firefox is a trademark of the Mozilla Foundation.

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.

Notes

P/N: 232-001867-50
10/10/2010

ADTRAN, Inc.
901 Explorer Boulevard
Huntsville, AL 35806

WWW.ADTRAN.COM