Contents

Contents 1
Platform Compatibility and Enhancements 1
Key Features 2
Known Issues 5
Resolved Issues 7

Platform Compatibility and Enhancements

The ADTRAN NetVanta 5.8.1.3 release is supported on the following ADTRAN security appliances:

- ADTRAN NetVanta 2630
- ADTRAN NetVanta 2630 Wireless
- ADTRAN NetVanta 2730
- ADTRAN NetVanta 2830

Browser Support

ADTRAN NetVanta with Visualization uses advanced browser technologies such as HTML5, which are supported in most recent browsers. ADTRAN recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of NetVanta appliances.

This release supports the following Web browsers:

- Chrome 11.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 4.0 and higher
- Internet Explorer 8.0 and higher (do not use compatibility mode)
- Safari 5.0 and higher

Mobile device browsers are not recommended for NetVanta appliance system administration.

Key Features

The following key features are supported in all versions of ADTRAN NetVanta 5.8 firmware:

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

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

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

  - Report to App Flow Collector
  - Report to EXTERNAL Flow Collector

- **Application Intelligence + Control**—This feature has two components for more network security:

  (a) **Identification**: Identify applications and track user network behaviors in real-time.
  (b) **Control**: Allow/deny application and user traffic based on bandwidth limiting policies.

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

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

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

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

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

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

- **Gateway Anti-Virus Enhancements (Cloud GAV)**—The Cloud Gateway Anti-Virus feature introduces an advanced malware scanning solution that compliments and extends the existing Gateway AV scanning mechanisms to counter the continued growth in the number of malware samples in the wild. Cloud Gateway Anti-Virus expands the Reassembly Free Deep Packet Inspection engine capabilities by consulting with the data center based malware analysis servers. This approach keeps the foundation of RFDPI-based malware detection by providing a low-latency, real-time solution that is capable of scanning unlimited numbers of files of unlimited size on all protocols that are presently supported without adding any significant incremental

processing overhead to the appliances themselves. This additional layer of security extends the current protection to cover multiple millions of pieces of malware.

- **NTP Authentication**—When adding a Network Time Protocol server, the Add NTP Server dialog box provides a field to specify the NTP authentication type, such as MD5. Fields are also available to specify the trust key ID, the key number and the password.
- **Link Aggregation**—Link Aggregation provides the ability to group multiple Ethernet interfaces to form a trunk which looks and acts like a single physical interface. This feature is useful for high end deployments requiring more than 1 Gbps throughput for traffic flowing between two interfaces. This functionality is available on all NSA E-Class platforms.
- **Port Redundancy**—Port Redundancy provides the ability to configure a redundant physical interface for any Ethernet interface in order to provide a failover path in case a link goes down. Port Redundancy is available on all NSA E-Class platforms.

  When the primary interface is active, it handles all traffic from/to the interface. When the primary interface goes down, the backup interface takes over and handles all outgoing/incoming traffic. When the primary interface comes up again, it takes over all the traffic handling duties from the backup interface.

  When Port Redundancy, High Availability and WAN Load Balancing are used together, Port Redundancy takes precedence followed by High Availability, then followed by WAN Load Balancing.
- **Content Filtering Enhancements**—The CFS enhancements provide policy management of network traffic based on Application usage, User activity, and Content type. Administrators are now able to create multiple CFS policies per user group and set restrictive 'Bandwidth Management Policies' based on CFS categories.
- **IPFIX and NetFlow Reporting**—This feature enables administrators to gain visibility into traffic flows and volume through their networks, helping them with tracking, auditing and billing operations. This feature provides standards-based support for NetFlow Reporting and IPFIX. The data exported through IPFIX contains information about network flows such as applications, users, and URLs extracted through Application Intelligence, along with standard attributes such as source/destination IP address (includes support for IPv6 networks), source/destination port, IP protocol, ingress/egress interface, sequence number, timestamp, number of bytes/packets, and more.
- **Enhanced Connection Limiting**—Connection Limiting enhancements expand the original Connection Limiting feature which provided global control of the number of connections for each IP address. This enhancement is designed to increase the granularity of this kind of control so that the administrator can configure connection limitation more flexibly. Connection Limiting uses Firewall Access Rules and Policies to allow the administrator to choose which IP address, which service, and which traffic direction when configuring connection limiting.
- **Dynamic WAN Schedule**—ADTRAN NetVanta release 5.8 supports scheduling to control when Dynamic WAN clients can connect. A Dynamic WAN client connects to the WAN interface and obtains an IP address with the PPPoE, L2TP, or PPTP. This enhancement allows the administrator to bind a schedule object to Dynamic WAN clients so that they can connect when the schedule allows it and they are disconnected at the end of the configured schedule. In the ADTRAN NetVanta management interface, a Schedule option is available on the WAN interface configuration screen when one of the above protocols is selected for IP Assignment. Once a schedule is applied, a log event is recorded upon start and stop of the schedule.
- **NTLM Authentication with Mozilla Browsers**—As an enhancement to Single Sign-On, ADTRAN NetVanta firmware can now use NTLM authentication to identify users who are browsing using Mozilla-based browsers (including Internet Explorer, Firefox, Chrome and Safari). NTLM is part of a browser authentication suite known as "Integrated Windows Security" and should be supported by all Mozilla-based browsers. It allows a direct authentication request from the appliance to the browser with no SSO agent involvement. NTLM authentication works with browsers on Windows, Linux and Mac PCs, and provides a mechanism to achieve Single Sign-On with Linux and Mac PCs that are not able to interoperate with the SSO agent.
- **SSL VPN NetExtender Update**—This enhancement supports password change capability for SSL VPN users, along with various fixes. When the password expires, the user is prompted to change it when logging in via the NetExtender client or SSL VPN portal. It is supported for both local users and remote users (RADIUS and LDAP).

- **DHCP Scalability Enhancements**—The DHCP server in ADTRAN appliances has been enhanced to provide between 2 to 4 times the number of leases previously supported. To enhance the security of the DHCP infrastructure, the ADTRAN NetVanta DHCP server now provides server side conflict detection to ensure that no other device on the network is using the assigned IP address. Conflict detection is performed asynchronously to avoid delays when obtaining an address.
- **SIP Application Layer Gateway Enhancements**—ADTRAN NetVanta release 5.8 provides SIP operational and scalability enhancements. The SIP feature-set remains equivalent to previous ADTRAN NetVanta releases, but provides drastically improved reliability and performance. The **SIP Settings** section under the **VoIP > Settings** page is unchanged.

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

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

  - **SIP Endpoint Information Database** – The algorithm for maintaining the state information for known endpoints is redesigned to use a database for improved performance and scalability. Endpoint information is no longer tied to the user ID, allowing multiple user IDs to be associated with a single endpoint. Endpoint database access is flexible and efficient, with indexing by NAT policy as well as by endpoint IP address and port.
  - **Automatically Added SIP Endpoints** – User-configured endpoints are automatically added to the database based on user-configured NAT policies, providing improved performance and ensuring correct mappings, as these endpoints are pre-populated rather than “learnt.”
  - **SIP Call Database** – A call database for maintaining information about calls in progress is implemented, providing improved performance and scalability to allow ADTRAN NetVanta to handle a much greater number of simultaneous calls. Call database entries can be associated with multiple calls.
  - **B2BUA Support Enhancements** – SIP Back-to-Back User Agent support is more efficient with various algorithm improvements.
  - **Connection Cache Improvements** – Much of the data previously held in the connection cache is offloaded to either the endpoint database or the call database, resulting in more efficient data access and corollary performance increase.
  - **Graceful Shutdown** – Allows SIP Transformations to be disabled without requiring the firewall to be restarted or waiting for existing SIP endpoint and call state information to time out.
- **Geo-IP & Botnet Filter** – Geo-IP and Botnet Filter features are now licensed services, although these features are currently available on a free trial license basis. You simply need to click on the link to activate the trial license with your NetVanta Security Portal account.

  Note: App Visualization must also be both licensed and enabled to enable Geo-IP and Botnet Filter.

  To use the Geo-IP and Botnet Filter features, first active the Application CGSS license bundle, which is part of the CGSS license bundle. If Application Visualization is licensed but not enabled, the Status icon appears orange.

  After Application Visualization is licensed, go to the **Log > Flow Reporting** page and enable Flow Reporting and Visualization. You must then restart the appliance. The appliance will then download the country database (which may take up to five minutes). Geo-IP and Botnet Filter will then be ready to use.

Known Issues

This section contains a list of known issues in the ADTRAN NetVanta 5.8.1.3 firmware:

Application Control

Symptom	Condition / Workaround	Issue
App Control advanced signatures are applied to traffic from and to the VPN zone, rather than the WAN zone only.	Occurs when enabling the App Control service on the WAN zone, and then enabling the logging or blocking action for any signature. After traffic is generated from the LAN to the VPN, the App control signatures are applied to VPN traffic.	107296
App rules remain in effect even when disabled globally.	Occurs when the Enable App Rules checkbox is cleared to disable these policies globally, then an app rule is created. When traffic on the WAN interface matches the rule, the configured policy action is applied. **Workaround**: Uncheck Enable App Rules and the reboot the appliance.	101194
Related traffic configured in an application rule is blocked even though the **Enable App Rules** checkbox is not selected.	Occurs when an application rule is created using Create Rule on the App Flow Monitor page and the Enable App Rules checkbox is not selected, which is the factory default setting. The app rule is created and functions properly, even though the **Enable App Rules** checkbox is disabled. **Workaround**: Uncheck Enable App Rules and the reboot the appliance.	100120

Bandwidth Management

Symptom	Condition / Workaround	Issue
Traffic is dropped when the ingress or egress values for an interface are modified and traffic is passing through that interface.	Occurs when modifying the ingress or egress interface values while the interface is passing traffic. **Workaround**: Stop traffic on the interface, and then modify the values.	101286
Bandwidth management application rules are sometimes mapped to the wrong global BWM priority queue.	Occurs when creating a bandwidth management rule on the **App Flow Monitor** page and setting the priority to **High**. The **App Flow Monitor** page displays the created rule with a **Medium** priority setting, even though **High** was selected.	100116

High Availability

Symptom	Condition / Workaround	Issue
With Active/Passive High Availability enabled with probing, and the primary WAN interface configured with a redundant port, the primary WAN interface and all routes to this subnet are marked as down when the primary port stops working.	Occurs when HA is enabled with probing and the primary WAN interface is configured with a redundant port. If the link for the active port goes down, Load Balancing (enabled by default) will change the status of the primary WAN interface to “Failover”. All routes to the primary WAN subnet will be marked as down and traffic destined to the subnet will fail. However, traffic will still succeed to any destination that is on the far side of the default	97883

	gateway of the primary WAN interface, by using the redundant port. **Workaround**: Disable Load Balancing or HA probing.	

Networking

Symptom	Condition / Workaround	Issue
Configuring more than one remote appliance with a tunnel interface and OSPF could result in dropped routes.	Occurs when an additional remote appliance is configured with a tunnel interface and OSPF is enabled.	102961

Visualization

Symptom	Condition / Workaround	Issue
The NetFlow EndTime timestamp results in 0.00000 for valid and allowed TCP packets.	Occurs when the NetFlow collector's logging is enabled on Applicable Interfaces and Rules, and TCP traffic is sent to the allowed destination. Upon checking the packet capture details, the EndTime timestamp displays as 0.00000.	102961

VPN

Symptom	Condition / Workaround	Issue
Sometimes, the secondary IPSec gateway is unable to establish a tunnel with a peer if the primary gateway is unreachable.	Occurs when there are two ADTRAN NetVanta devices with VPN configured and the cable from the secondary gateway is unplugged.	103935
Having multiple tunnel interface policies with the same IPSec gateway but different ports configured on the firewall can cause only one tunnel to be active.	Occurs when there are two or more tunnel interface policies using the same IPSec gateway and those interfaces are bound to different ports.	103398

Resolved Issues

This section contains a list of resolved issues in the ADTRAN NetVanta 5.8.1.3 firmware:

Symptom	Condition / Workaround	Issue
The Botnet Service is incorrectly listed on the Security Services > Summary page and the System > Status page of the ADTRAN NetVanta wireless appliance, even though the service is not supported on this platform.	Botnet Command & Control Filtering is not supported on the ADTRAN NetVanta wireless appliances (as also reflected in the Supported Features by Appliance Model table of the Release Notes). The Botnet service listing indicating 'Not Licensed' on the System > Status page should be ignored.	108038
An iPad client fails to connect to the L2TP server if MSCHAPv2 authentication is set as the first order authentication method.	Occurs when GroupVPN is enabled and configured for an L2TP. The iPad can successfully connect if PAP authentication is set as the first order authentication method, but fails if MSCHAPv2 is prefered. A Windows XP client can succesfully connect using MSCHAPv2. **Workaround**: Move MSCHAPv2 to the bottom of the authentication protocol list (by clicking on the Down Arrow button).	106801

Last updated: 12/19/2011
PN 232-00xxxx-00 Rev A