Release Notes

NetVanta

ADTRAN NetVanta 5.6.0.9 Release Notes

Contents

Platform Compatibility and Enhancements

The ADTRAN NetVanta 5.6.0.9 release is supported on the following ADTRAN security appliances:

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

This release supports the following Web browsers:

- Microsoft Internet Explorer 7.0 and higher
- Mozilla Firefox 3.0 and higher
- Chrome 4.0 and higher

Strong SSL and TLS Encryption Required in Your Browser

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

TIP: By default, Mozilla Firefox 3.0, Microsoft Internet Explorer 8.0, and Google Chrome enable SSL 3.0 and TLS, and disable SSL 2.0. ADTRAN recommends using the most recent Web browser releases. If you are using a previous release of these browsers, you should enable SSL 3.0 and TLS and disable SSL 2.0.

Key Features

The following key features are supported in all versions of ADTRAN NetVanta 5.6 firmware:

- **3G and Modem Support** – ADTRAN NetVanta 5.6 firmware supports 3G and Modem configurations for WAN Load Balancing (WLB) on all supported platforms except the ADTRAN NetVanta 2830.

- **Command Line Interface Enhancements** – Provides increased support through the command line interface to configure and modify Network Address Translation (NAT) Policies, Access Rules, Service Objects, and Service Groups.

- **Diagnostic Improvements** – Includes a diagnostic tool which automatically checks the network connectivity and service availability of several pre-defined functional areas of the firmware. The tool also returns results and attempts to describe causes, if any exceptions are detected.

- **Dynamic DNS per Interface** – Provides the ability to assign a Dynamic DNS (DDNS) profile to a specific WAN interface. This allows administrators who are configuring WAN Load Balancing to advertise a predictable IP address to the DDNS service.

- **Increased UTM Connection Support** – Provides the ability to increase the number of simultaneous connections on which ADTRAN NetVanta security appliances can apply Unified Threat Management (UTM) services (Application Firewall, Anti-Spyware, Gateway Anti-Virus, and Intrusion Prevention Service). This feature is intended for customers who need to support a large number of concurrent connections. (Note: There is a slight performance decrease when this option is enabled.)

- **MAC-IP Spoof Detection and Prevention –** Provides additional protection against MAC address and IP address based spoofing attacks (such as Man-in-the-Middle attacks) through configurable Layer 2 and Layer 3 admission control.

- **Packet Mirroring –** Provides the ability to capture copies of specified network packets from other ports. This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion detection system. Customers can now gather data from one of the other ports on an ADTRAN NetVanta to look for threats and vulnerabilities and help aid with diagnostics and troubleshooting.

- **Route-based VPN with Dynamic Routing Support –** Extends support for advanced routing (either OSPF or RIP) to VPN networks. This simplifies complex VPN deployments by enabling dynamic routing to determine the best path that traffic should take over a VPN tunnel.

- **Signature Download through a Proxy Server –** Provides the ability for ADTRAN NetVanta security appliances to download signatures even when they access the Internet through a proxy server. This feature also allows for registration of ADTRAN NetVanta security appliances through a proxy server without compromising privacy.

- **Single Sign-on for Terminal Services and Citrix –** Provides support for transparent authentication of users logged in from a Terminal Services or Citrix server. This transparent authentication enables Application Firewall and CFS policy enforcement in Terminal Services and Citrix environments.

- **Unbounded Multiple WAN Support –** Provides the ability to enable any number of WAN Ethernet interfaces for WAN Load Balancing and Failover on ADTRAN NetVanta security appliances.

- **Virtual Access Points for ADTRAN NetVanta 2630 Wireless –** Enables the use of Virtual Access Points (VAPs) to segment different wireless groups by creating logical segmentation on a single wireless radio.

- **VPN Policy Bound to VLAN Interface** – Allows users to bind a VPN policy to a VLAN interface when configuring a site-to-site VPN.

- **WebCFS Server Failover** – Provides the ability to enable WebCFS server failover, allowing an ADTRAN NetVanta security appliance to contact another server for URL rating information if the local server is unavailable. This ensures performance continuity for Web navigation and Web content filtering functionality.

- **Wireless Bridging for ADTRAN NetVanta Wireless Platforms –** The ADTRAN NetVanta 2630 Wireless now supports Wireless Bridging, which provides the ability to extend a single wireless network across multiple ADTRAN NetVanta wireless security appliances.

Known Issues

This section contains a list of known issues in the ADTRAN NetVanta 5.6 firmware:

Wireless

Symptom	Condition / Workaround	Issue
A performance drop is seen for PC-card 3G interface throughput on the NetVanta 2730.	Occurs when using a wireless 3G PC card on a NetVanta 2730 to download an FTP file or to load Web pages in a browser.	95135

VPN

Symptom	Condition / Workaround	Issue
Transport Mode does not allow traffic to pass through a VPN tunnel.	Occurs when transport mode is enabled after the tunnel interface VPN is configured in Aggressive/Main Mode.	94175

Networking

Symptom	Condition / Workaround	Issue
Modifying the interface IP address may result in issues for the corresponding static DHCP scope entry.	Occurs after changing a dynamic DHCP interface to static, and then back again to dynamic in a different subnet. For the X0 interface, the static DHCP IP range is removed. For another LAN interface, the static DHCP IP range remains unchanged.	94053

High Availability

Symptom	Condition / Workaround	Issue
The wrong interface can be unassigned when removing interfaces from a Load Balancing group.	Occurs when X1 and X3 are configured as WAN interfaces and assigned to the default LB group with X3 having a higher rank. After setting X3 back to unassigned, it remains in the LB group and X1 is removed from the LB group.	94598

CFS

Symptom	Condition / Workaround	Issue
A new custom schedule used by a CFS policy can be deleted.	Occurs after creating and applying a new custom schedule to the CFS policy. A user is then able to delete the new custom schedule.	94007

Bandwidth Management

Symptom	Condition / Workaround	Issue
Fragmented, non-VPN outbound packets are not accounted for in Bandwidth Management (BWM).	Occurs when the user enables fragmented, non-VPN outbound packets after enabling BWM. Fragmented outbound packets are not being accounted for by BWM.	93951
Bandwidth Management uses the wrong active WAN and BWM settings after WAN Load Balancing (WLB) is disabled.	Occurs when WLB and BWM are enabled for two interfaces (X3, X5) with BWM ingress and egress set to 1 Gbps. BWM is disabled on X1 with the default values unchanged. While WLB is enabled, the active WAN interface is X3. After disabling WLB, the BWM module uses X1 as the default WAN, while the WLB module still uses X3.	93919

Last updated: 11/29/2010
PN 232-001868-00 Rev A