Release Notes

SonicOS

SonicOS Enhanced 5.5.6.0 Release Notes

Contents

Platform Compatibility

This version of SonicOS 5.5.6.0 supports Internet Protocol Version 6 (IPv6) and provides gateway Deep Packet Inspection for IPv6 networks.

SonicOS 5.5.6.0 is supported on the following SonicWALL network security appliances:

- SonicWALL NSA E7500
- SonicWALL NSA E6500
- SonicWALL NSA E5500
- SonicWALL NSA 5000
- SonicWALL NSA 4500
- SonicWALL NSA 3500
- SonicWALL NSA 2400
- SonicWALL NSA 240

NOTE: SonicOS 5.5.6 cannot be booted with current Preferences on an appliance that is running a SonicOS release that does not support IPv6. Administrators must first export the Preferences file, load the SonicOS 5.5.6 firmware with factory default settings, and then import the Preferences file. For more information, see Importing Preferences to SonicOS Enhanced 5.5.6 on page 13.

This release supports the following Web browsers:

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

Strong SSL and TLS Encryption Required in Your Browser

The internal SonicWALL 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 2.0 and Microsoft Internet Explorer 7.0 enable SSL 3.0 and TLS, and disable SSL 2.0. SonicWALL 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. In Internet Explorer, go to Tools > Internet Options on the Advanced tab and scroll to the bottom of the Settings menu. In Firefox, go to Tools > Options on the Advanced tab, and then select the Encryption tab.

IPv6 in SonicOS

SonicOS 5.5.6.0 supports Internet Protocol Version 6 (IPv6) and provides gateway Deep Packet Inspection for IPv6 networks.

IPv6 is the successor to IPv4. On February 3rd, 2011, the Internet Assigned Numbers Authority (IANA) distributed the last-remaining blocks of IPv4 addresses to the Regional Internet Registries (RIRs). After the RIRs distribute these addresses to ISPs later this year, the world's supply of new IPv4 addresses will be exhausted. By increasing the address length from 32 bits to 128 bits, IPv6 dramatically increases the number of available addresses compared to IPv4:

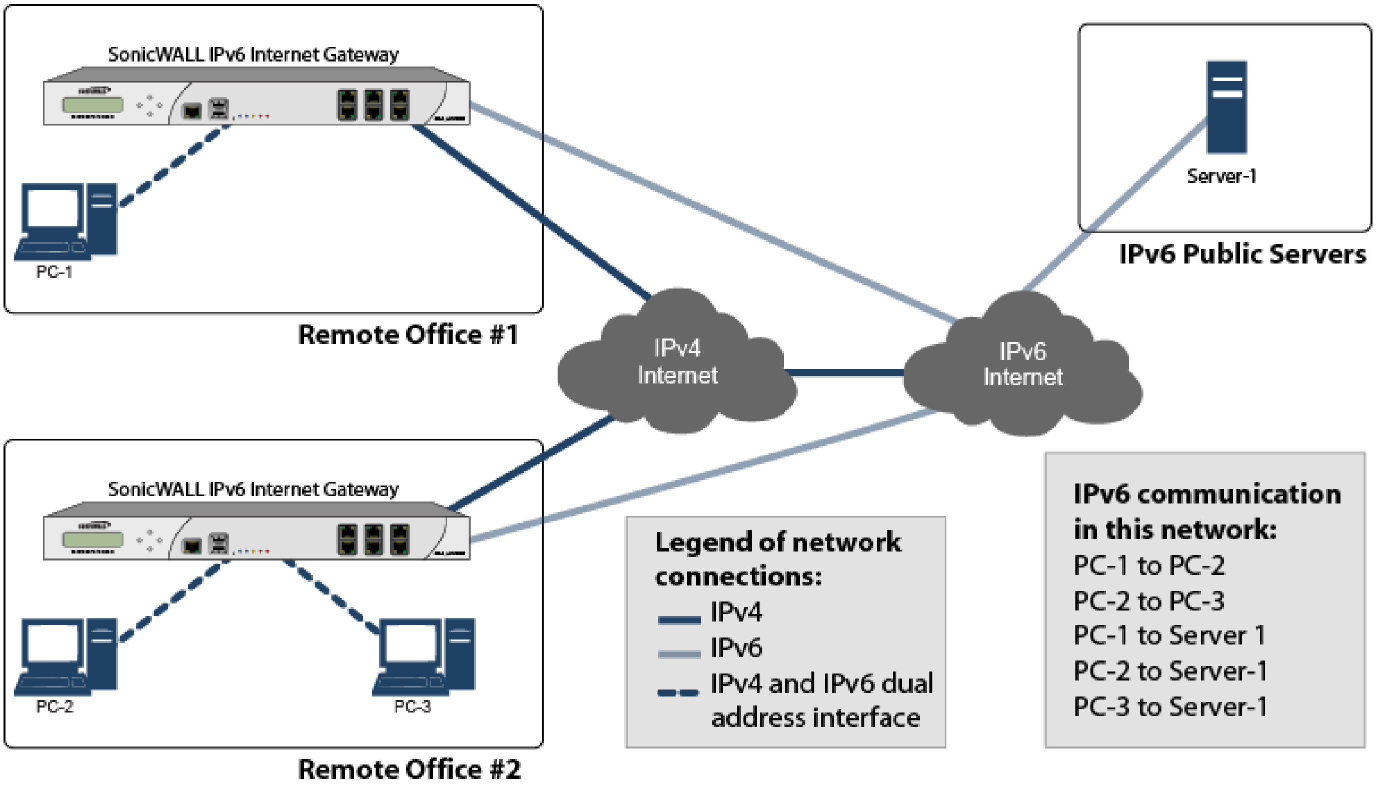
- IPv4: 4,294,967,296 addresses
- IPv6: 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses

IPv6 addresses are written in eight groups of four hexadecimal digits separated by colons, for example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334. IPv6 addresses are logically divided into two parts: a 64-bit (sub-)network prefix, and a 64-bit interface identifier. Here is an example of an IPv6 address:

- 2001:0db8:85a3:0000:0000:8a2e:0370:7334

IPv6 will first impact large networks and ISPs. End users are unlikely to be impacted by IPv6 for several years. But it will become increasing important for network administrators to be able to configure networks to interoperate with both IPv4 and IPv6.

The following diagram shows a basic dual-stack topology with two remote offices, where clients have both IPv4 and IPv6 addresses:



IPv6 Ready Certification

SonicWALL has met the requirements for “IPv6 Ready” Phase-1 and Phase-2, as specified by the IPv6 Forum, a world-wide consortium providing technical guidance for the deployment of IPv6. The IPv6 Ready Logo Program is a conformance and interoperability testing program intended to increase user confidence by demonstrating that IPv6 is available now and ready to be used.

The IPv6 Ready series of tests extends from a basic level of minimum coverage in Phase-1 to a more complete coverage with Phase-2:

- **Phase-1 (Silver) Logo:** In a first stage, the Logo indicate that the product includes IPv6 mandatory core protocols and can interoperate with other IPv6 implementations.
- **Phase-2 (Gold) Logo:** The "IPv6 ready" step implies a proper care, technical consensus and clear technical references. The IPv6 Ready Logo will indicate that a product has successfully satisfied strong requirements stated by the IPv6 Logo Committee (v6LC).

SonicWALL has been certified for Phase 2 (Gold) IPv6 Ready status. A future Phase-3 level of IPv6 Ready coverage is currently being developed. For more information, see http://www.ipv6ready.org/

IPv6 Feature Support

The following table lists the IPv6 features that are supported in SonicOS Enhanced 5.5.6.0, and the features that are not currently supported in this release.

NOTE: SonicOS Enhanced 5.5.6.0 is a dual IP stack firmware. Features that are not supported for IPv6 are still supported for IPv4.

IPv6 Features Supported	IPv6 Features Not Currently Supported
• 6to4 tunnel (allows IPv6 nodes to connect to outside IPv6 services over an IPv4 network) • Access Rules • Address Objects • Anti-Spyware • Application Firewall • Attack prevention: o Land Attack o Ping of Death o Smurf o SYN Flood • Connection Cache • Connection Monitor • Content Filtering Service • DHCP • DNS client • DNS lookup and reverse name lookup • EPRT • EPSV • FTP • Gateway Anti-Virus	• Anti-Spam • Command Line Interface • Connection Limiting for IPv6 connections • DHCP over VPN • DHCP Relay • Dynamic Address Objects for IPv6 addresses • Dynamic DNS • Dynamic Routing (RIP and OSPF) • FQDN • Global VPN Client (GVC) • GMS • H.323 • High Availability support for the following features: o Dynamic Address Objects o IPv6 management IP address o Multicast o SonicPoints o VoIP • IKEv1 • IPv6 Syslog messages • L2TP

IPv6 Features Supported	IPv6 Features Not Currently Supported
• High Availability: o Connection Cache o FTP o NDP • HTTP/HTTPS management over IPv6 • ICMP • IKEv2 • Intrusion Prevention Service • IP Spoof Protection • IPv4 Syslog messages, including messages with IPv6 addresses • Layer 2 Bridge Mode • Logging IPv6 events • Login uniqueness • Multicast Routing with Multicast Listener Discovery • NAT • Neighbor Discovery Protocol • NetExtender connections for users with IPv6 addresses • Packet Capture • Ping • Policy Based Routing • Remote management • Site-to-site IPv6 tunnel with IPSec for security • SonicPoint IPv6 support • Security services for IPv6 traffic with DPI • SSL VPN • Stateful inspection of IPv6 traffic • User status • VPN policies • Wireless	• LDAP • MAC-IP Anti-Spoof • NAT load balancing • NAT between IPv6 and IPv4 addresses • NetBIOS over VPN • NTP • Oracle SQL/Net • QoS Mapping • PPPoE • RADIUS • RAS Multicast Forwarding • RTSP • Route-based VPNs • Single Sign On • SIP • SMTP Real-Time Black List (RBL) Filtering • SNMP • SSH • Transparent Mode • ViewPoint • Virtual Assistant • Virtualization • VLAN interfaces with IPv6 addresses • Web proxy

Supported IPv6 RFCs

This section lists the IPv6 RFCs that are supported in the SonicOS Enhanced 5.5.6.0 release.

TCP/IP stack and Network Protocols

- RFC 1886 DNS Extensions to support IP version 6 [IPAPPL dns client]
- RFC 1981 Path MTU Discovery for IPv6
- RFC 2113 IP Router Alert Option
- RFC 2373 IPv6 Addressing Architecture
- RFC 2374 An IPv6 Aggregatable Global Unicast Address Format (obsoleted by 3587)
- RFC 2375 IPv6 Multicast Address Assignments
- RFC 2460 IPv6 specification
- RFC 2461 Neighbour discovery for IPv6
- RFC 2462 IPv6 Stateless Address Autoconfiguration
- RFC 2463 ICMPv6 for IPv6 specification
- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 2473 Generic Packet Tunneling in IPv6 Specification
- RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
- RFC 2553 Basic Socket Interface Extensions for IPv6
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
- RFC 2711 IPv6 Router Alert Option
- RFC 2784 Generic Routing Encapsulation
- RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers
- RFC 2991 Multipath Issues in Unicast and Multicast Next-Hop Selection
- RFC 3056 Connection of IPv6 Domains via IPv4 Clouds
- RFC 3484 Default Address Selection for Internet Protocol version 6 (IPv6) (no policy hooks)
- RFC 3493 Basic Socket Interface Extensions for IPv6
- RFC 3513 Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3542 Advanced Sockets Application Program Interface (API) for IPv6
- RFC 3587 IPv6 Global Unicast Address Format (obsoletes 2374)

IPsec Conformance

- RFC 1826 IP Authentication Header [old AH]
- RFC 1827 IP Encapsulating Security Payload (ESP) [old ESP]

NAT Conformance

- RFC 2663 IP Network Address Translator (NAT) Terminology and Considerations.
- RFC 3022 Traditional IP Network Address Translator (Traditional NAT).

DNS Conformance

- RFC 1886 DNS Extensions to support IP version 6

Non-Supported IPv6 RFCs

This section lists the IPv6 RFCs that are currently not supported in the SonicOS Enhanced 5.5.6.0 release.

- RFC 2002 IP Mobility Support
- RFC 2766 Network Address Translation - Protocol Translation (NAT-PT)
- RFC 2472 IP Version 6 over PPP
- RFC 2452 IP Version 6 Management Information Base for the Transmission Control Protocol.
- RFC 2454 IP Version 6 Management Information Base for the User Datagram Protocol.
- RFC 2465 Management Information Base for IP Version 6: Textual Conventions and General Group.

Known Issues

This section contains a list of known issues in the SonicOS Enhanced 5.5.6.0 release.

IPv6

Symptom	Condition / Workaround	Issue
The local IPv6 routing policy entry for an interface is deleted from the configuration if the physical cable for that interface is disconnected and reconnected.	Occurs when the physical cable for a IPv6 interface is disconnected and reconnected.	93673
A firewall with separate VPN tunnels configured for both IPv4 and IPv6 crashes, and the HA backup fails to takeover.	Occurs on a SonicWALL NSA 4500 with three VPN tunnels configured for IPv4 and three VPN tunnels configured for IPv6. The crash occurs when IPv4 traffic is being passed through two of the IPv4 VPN tunnels.	94328

Networking

Symptom	Condition / Workaround	Issue
A firewall in PPTP client cannot connect to the PPTP server after the firewall is rebooted.	Observed on a firewall that had successfully configured a WAN interface for PPTP client mode. to allow remote PPTP client access. After the firewall is rebooted, the WAN interface can no longer connect to the PPTP server. **Workaround**: Change the WAN interface configuration from PPTP client mode to Static mode and then back to PPTP client mode.	93198

Resolved Issues

This section contains a list of resolved issues in the SonicOS Enhanced 5.5.6.0 release.

Anti-Spam

Symptom	Condition / Workaround	Issue
The Anti-Spam service cannot perform IP reputation DNS lookups, or log events are created when it does so.	Occurs when DNS Rebinding attack prevention is enabled for either blocking or logging.	83648

High Availability

Symptom	Condition / Workaround	Issue
High Availability fails to synchronize the deletion of a static route to the idle unit.	Occurs after a static route is configured on the active appliance of any HA pair and synchronized to the secondary unit. If the route is then deleted on the active unit, it is not deleted on the idle unit. **Workaround**: The administrator must restart the active unit to force a failover to the idle unit, and then log into the unit's Web management interface and delete the static route.	79355

Modem

Symptom	Condition / Workaround	Issue
A modem connected to the USB port fails to connect after the SonicWALL security appliance is rebooted.	Occurs if there is an active VPN tunnel when the appliance is rebooted.	81720

Multiple WAN Interfaces

Symptom	Condition / Workaround	Issue
In an active-passive load balancing configuration with probe monitoring, the secondary WAN interface is unable to maintain a steady connection after failover from the primary WAN interface occurs.	Occurs when DNS resolution is being used. If a static IP address is set, this issue does not occur.	82779

Networking

Symptom	Condition / Workaround	Issue
RIP is disabled on an interface, and the published network is not updated on the router.	Occurs when RIPv2 is enabled on a LAN interface and then the interface IP address is changed to a different subnet.	83512
Changing the zone assignment of an interface leads to the user being unable to edit the DHCP relay policy for that interface.	Occurs when an interface is assigned to a customized zone and then a DHCP relay policy is configured with the customized zone as the source. If the interface is then assigned to a different interface, the DHCP relay policy can no longer be edited.	79363
The Default Gateway and Secondary Gateway address objects are always shown as 0.0.0.0. They can still be selected, but do not work. These objects are to be removed as part of the Multiple WAN feature.	Occurs when attempting to use the Default Gateway or Secondary Gateway address object in SonicOS Enhanced release 5.5. Note that the address objects are shown as 0.0.0.0 when booted to factory default settings, or if the gateways are not configured upon upgrade.	79059

Single Sign On

Symptom	Condition / Workaround	Issue
The Single Sign-On (SSO) configuration is not synchronized from the primary appliance to the backup appliance in a Stateful High Availability (HA) pair.	Occurs when failover occurs in a HA pair where the primary appliance has SSO configured.	82791
SSO fails to work after new firmware is uploaded to the appliance.	Occurs when uploading new firmware to an appliance with SSO enabled. **Workaround:** Disable SSO before booting the new firmware and then re-enable it afterwards.	82781

VPN

Symptom	Condition / Workaround	Issue
H.323 endpoint calls made through Route-Based VPN with Tunnel Interface configured cannot be established.	Occurs when attempting to make H.323 calls from a NetMeeting client on the LAN of firewall A to the Polycom client or to the NetMeeting client on the LAN of firewall B.	81549

This section contains a list of resolved issues in the SonicOS Enhanced 5.5.1.0 release.

Anti-Spam

Symptom	Condition / Workaround	Issue
The SonicWALL anti-spam service does not check for GRID return codes 127.0.0.10 and 127.0.0.11.	Occurs when the SonicWALL security appliance receives spam that is marked for GRID return codes 127.0.0.10 or 127.0.0.11.	81656
HTTP rules are deleted on startup when Anti-Spam is disabled or unlicensed.	Occurs after creating a **LAN>WAN LAN>WAN Any:Any:HTTP** rule and then restarting the firewall. **Workaround:** Manually re-add the rule or enable Anti-Spam. Also, you can navigate to **Firewall>Services**, create a custom group and add only the HTTP service. Then, create your firewall rule using the custom group with HTTP.	81502

GVC

Symptom	Condition / Workaround	Issue
GVC clients cannot access the LAN and wireless networks.	Occurs when the WLAN and LAN interfaces are bridged on the SonicWALL security appliance. **Workaround**: Configure the Virtual Adapter settings for **None on the group VPN**.	82044

High Availability

Symptom	Condition / Workaround	Issue
The Multicore Utilization page does not show any statistics for the idle unit in an active-active High Availability (HA) pair.	Occurs in an active-active HA pair.	81657
The HA > Monitoring **Allow Management on Primary/Backup IP address of Primary WAN** option is disabled during an upgrade to SonicOS 5.5.	Occurs when the option is enabled before upgrading from SonicOS Enhanced 5.2.0.1 or 5.4.0.0 to SonicOS 5.5.0.0.	81591
The WAN monitoring IP on the backup unit is inaccessible if WLB probing is enabled.	Occurs when WLB probing is enabled on a HA pair. ARPs are seen coming from the Backup for the probing address, but no probes are sent. The backup unit puts the primary WAN interface in failover, making it inaccessible using the HA monitoring IP.	73580

Modem

Symptom	Condition / Workaround	Issue
After failover to the 3G WWAN, it repeatedly reconnects at 30 second intervals.	Occurs when logical monitoring is enabled on the Ethernet WAN and then a logical failover to the WWAN occurs.	83431
A USB modem fails to autodial the WWAN service after the connection is lost.	Occurs when an active WWAN connection is lost. This was observed when using a Sprint Novatel U760 WWAN card.	82240

Networking

Symptom	Condition / Workaround	Issue
A policy based static route (PBR) is not reinstated after the network monitor checking its state fails and then recovers.	Occurs when an IPSec VPN is used for a backup route and takes over as the active route after the network monitor fails.	82339
The TZ 210W appliance causes a switch on the X0 interface to stop passing traffic.	Occurs when a TZ 210W connects to a switch such as an HP Procurve, Cisco Catalyst 2950, or Dell PowerConnect 2848 or 2748 through the X0 port when X0 is a member of a port shield group with one of the other ports. After attempting to connect, any devices on the switch will lose Layer 2 connectivity to each other.	80732
The SonicWALL becomes part of a broadcast storm, and can lock up in some situations.	Occurs when the SonicWALL forwards unicast traffic broadcast from a hub or port mirror back to the source host, instead of dropping traffic whose destination MAC address is not one of the SonicWALL's interfaces.	80604
After a period of time, the TZ 200W loses awareness of its USB 3G wireless card.	Occurs possibly when plugging in the X1 Ethernet cable.	79435
When an interface is assigned to any non-WAN zone, SonicOS automatically adds a NAT policy that translates the interface IP address to the IP address of the primary LAN interface.	Occurs when attempting to assign X2 to a non-WAN zone; the NAT policy will be auto-added from X2 to X0.	73166

Single Sign-On

Symptom	Condition / Workaround	Issue
Users may see timeouts in browsers or other traffic and/or redirections to the SonicWALL login page or to a page saying that access is barred. The Application section in the Windows event log on the server PC where the SSO agent is running may contain many errors with source "SonicWALL SSO Agent".	Occurs when using Single Sign-On and users are located on a different interface to the domain server and SonicWALL CFS is enforced for traffic from the zone where those users are located. **Workaround**: Add all IP addresses of all domain servers to the CFS Exclusion List on the Security Services > Content Filter page.	79988

User Interface

Symptom	Condition / Workaround	Issue
The **Drop all packets while IPS, GAV, and Anti-Spyware database is reloading** check box cannot be selected.	Occurs when attempting to configure the **Security Services > Summary** page. If the page is refreshed, no changes will have been made, and the checkbox remains unselected.	80069

VPN

Symptom	Condition / Workaround	Issue
When editing a route policy that remains from a deleted VPN tunnel interface, the firewall crashes, leaving the tWebmain task suspended.	Occurs when attempting to edit a route policy or modify its interface to a newly created VPN tunnel interface.	81498
The L2TP SonicWALL shows it is establishing a connection, but the connection never finishes.	Occurs when attempting to setup L2TP on an appliance while connecting to 15 or more users.	78349

Wireless

Symptom	Condition / Workaround	Issue
Wireless Clients in Wireless Bridge mode cannot obtain an IP address from an external DHCP server.	Occurs when attempting to connect to the SonicPoint after configuring it as a Wireless Bridge.	81503
Bypass WGS authentication does not work with custom wireless station Address Objects.	Occurs when WGS is enabled with the custom AO as the bypass WGS authentication list, but works fine with an automatically generated AO that has the same MAC address, created when adding 'Allow station'.	81111

Upgrading SonicOS Enhanced Image Procedures

The following procedures are for upgrading an existing SonicOS Enhanced image to a newer version:

Obtaining the Latest SonicOS Enhanced Image Version

To obtain a new SonicOS Enhanced firmware image file for your SonicWALL security appliance:

1. Connect to your mysonicwall.com account at http://www.mysonicwall.com.
2. Copy the new SonicOS Enhanced image file to a directory on your management station.

You can update the SonicOS Enhanced image on a SonicWALL security appliance remotely if the LAN interface or the WAN interface is configured for management access.

Saving a Backup Copy of Your Configuration Preferences

Before beginning the update process, make a system backup of your SonicWALL security appliance configuration settings. The backup feature saves a copy of your current configuration settings on your SonicWALL security appliance, protecting all your existing settings in the event that it becomes necessary to return to a previous configuration state.

In addition to using the backup feature to save your current configuration settings to the SonicWALL 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 SonicWALL security appliance.

Perform the following steps 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.

Importing Preferences to SonicOS Enhanced 5.5.6

NOTE: SonicOS 5.5.6 cannot be booted with current Preferences on an appliance that is running a SonicOS release that does not support IPv6. Administrators must first export the Preferences file, load the SonicOS 5.5.6 firmware with factory default settings, and then import the Preferences file.

To load SonicOS Enhanced 5.5.6 on an appliance, perform the following steps:

1. On the **System > Settings** page, click the **Export Settings** button and save the current configuration file.
2. Click the **Upload New Firmware** button to upload the SonicOS 5.5.6 firmware.
3. Once the firmware has loaded, click the **Boot** button on the **Uploaded Firmware with Factory Default Settings** line.
4. After the appliance has rebooted with the SonicOS 5.5.6 firmware, click the **Import Settings** and import the Preferences file you saved in step 1.

Downgrading from Higher SonicOS Versions to SonicOS Enhanced 5.5.6

SonicOS does not support importing preference files from higher versions of SonicOS (such as SonicOS 5.6 or 5.8) when installing SonicOS 5.5.6. There are two options for installing SonicOS 5.5.6 on an appliance running SonicOS 5.6 or higher:

1. Upload a SonicOS 5.5.1 preference file and then add any new configuration changes.
2. Restore the appliance to factory default settings and then reconfigure the appliance.

Updating an Appliance Running SonicOS 5.5.6 to a Non-IPv6 Firmware Version

Special consideration should be taken when updating the firmware on an appliance running SonicOS 5.5.6 to a version of SonicOS that does not support IPv6. If the firmware has the 6to4 Tunnel Interface configured, the appliance cannot load new non-IPv6 firmware with the current settings. Similarly, the saved Preferences file for a SonicOS 5.5.6 release (with the 6to4 Tunnel Interface configured) should not be imported to an appliance running a non-IPv6 version of SonicOS. There are two options for migrating from SonicOS 5.5.6 (when the 6to4 Tunnel Interface is configured) to a non-IPv6 SonicOS version:

1. Delete the 6to4 Tunnel Interface, load the non-IPv6 firmware, and boot it with current settings.
2. Load the non-IPv6 firmware, boot it with factory default settings, and then reconfigure the appliance.

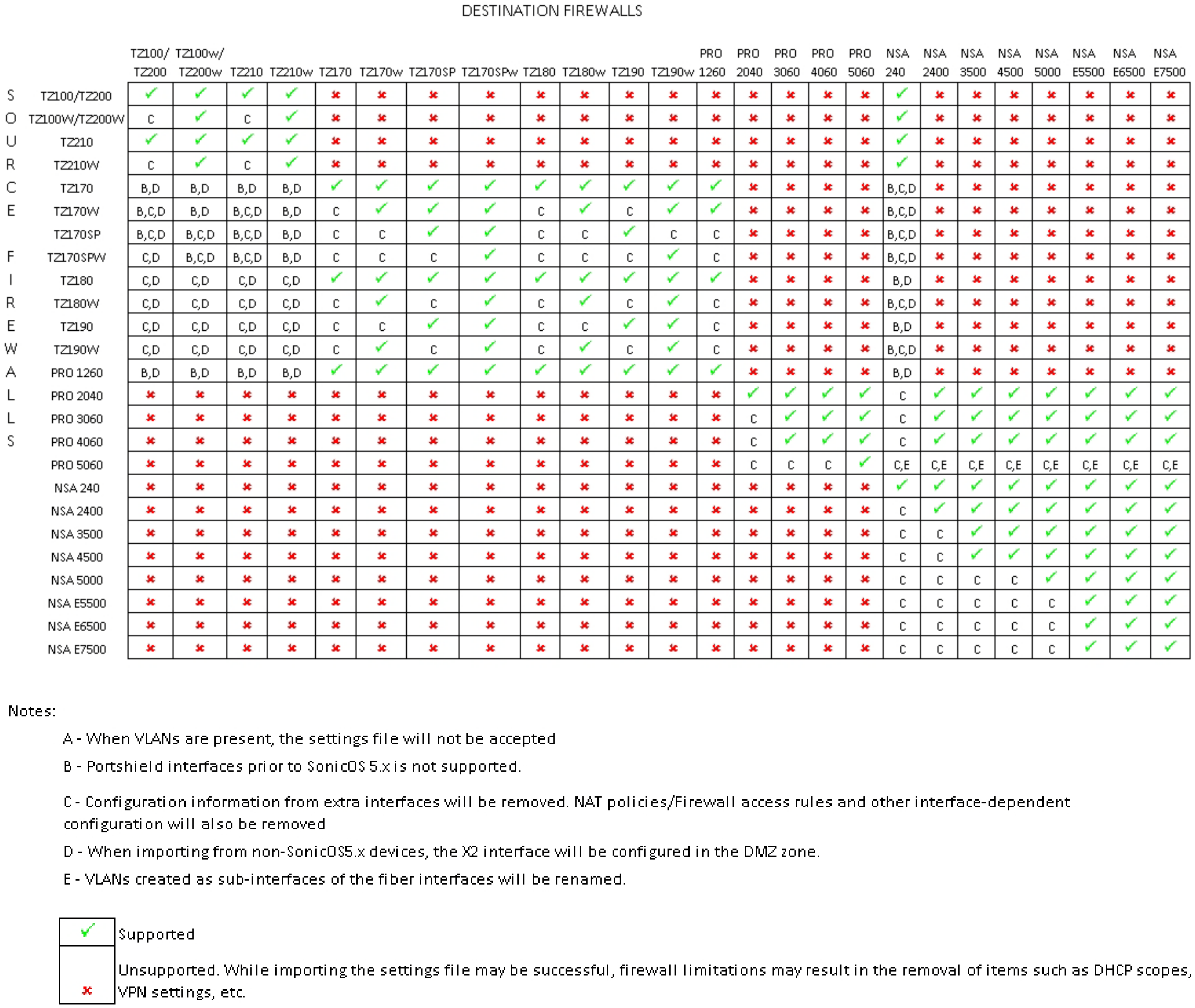
Upgrading a SonicOS Enhanced Image with Current Preferences

Note: *This procedure applies only when loading SonicOS 5.5.6 to an appliance that is already running a version of SonicOS that supports IPv6.*

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

1. Download the SonicOS Enhanced firmware image file from mysonicwall.com 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 SonicOS Enhanced firmware image file, select the file, and click **Upload**.
4. On the **System > Settings** page, click the **Boot** icon in the row for **Uploaded Firmware**.
5. In the confirmation dialog box, click **OK**. The SonicWALL restarts and then displays the login page.
6. Enter your user name and password. Your new SonicOS Enhanced image version information is listed on the **System > Settings** page.

Support Matrix for Importing Preferences



DESTINATION FIREWALLS

		TZ100/	TZ100w/											PRO	PRO	PRO	PRO	PRO	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA
		TZ200	TZ200w	TZ210	TZ210w	TZ170	TZ170w	TZ170SP	TZ170SPw	TZ180	TZ180w	TZ190	TZ190w	1260	2040	3060	4060	5060	240	2400	3500	4500	5000	E5500	E6500	E7500
S	TZ100/TZ200	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
O	TZ100W/TZ200W	C	✓	C	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
U	TZ210	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
R	TZ210W	C	✓	C	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
C	TZ170	B,D	B,D	B,D	B,D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗
E	TZ170W	B,C,D	B,D	B,C,D	B,D	C	✓	✓	✓	C	✓	C	✓	✓	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗
	TZ170SP	B,C,D	B,C,D	B,C,D	B,D	C	C	✓	✓	C	C	✓	C	C	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗
F	TZ170SPW	C,D	B,C,D	B,C,D	B,D	C	C	C	✓	C	C	C	✓	C	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗
I	TZ180	C,D	C,D	C,D	C,D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	B,D	✗	✗	✗	✗	✗	✗	✗
R	TZ180W	C,D	C,D	C,D	C,D	C	✓	C	✓	C	✓	C	✓	C	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗
E	TZ190	C,D	C,D	C,D	C,D	C	C	✓	✓	C	C	✓	✓	C	✗	✗	✗	✗	B,D	✗	✗	✗	✗	✗	✗	✗
W	TZ190W	C,D	C,D	C,D	C,D	C	✓	C	✓	C	✓	C	✓	C	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗
A	PRO 1260	B,D	B,D	B,D	B,D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	B,D	✗	✗	✗	✗	✗	✗	✗
L	PRO 2040	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	C	✓	✓	✓	✓	✓	✓	✓
L	PRO 3060	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	✓	✓	✓	C	✓	✓	✓	✓	✓	✓	✓
S	PRO 4060	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	✓	✓	✓	C	✓	✓	✓	✓	✓	✓	✓
	PRO 5060	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	C	✓	C,E	C,E	C,E	C,E	C,E	C,E	C,E	C,E
	NSA 240	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓
	NSA 2400	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	✓	✓	✓	✓	✓	✓	✓
	NSA 3500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	✓	✓	✓	✓	✓	✓
	NSA 4500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	✓	✓	✓	✓	✓	✓
	NSA 5000	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	C	C	✓	✓	✓	✓
	NSA E5500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	C	C	C	✓	✓	✓
	NSA E6500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	C	C	C	✓	✓	✓
	NSA E7500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	C	C	C	✓	✓	✓

Notes:

A - When VLANs are present, the settings file will not be accepted

B - Portshield interfaces prior to SonicOS 5.x is not supported.

C - Configuration information from extra interfaces will be removed. NAT policies/Firewall access rules and other interface-dependent configuration will also be removed

D - When importing from non-SonicOS5.x devices, the X2 interface will be configured in the DMZ zone.

E - VLANs created as sub-interfaces of the fiber interfaces will be renamed.

✓	Supported
✗	Unsupported. While importing the settings file may be successful, firewall limitations may result in the removal of items such as DHCP scopes, VPN settings, etc.

Upgrading a SonicOS Enhanced Image with Factory Defaults

Perform the following steps to upload new firmware to your SonicWALL appliance and start it up using the default configuration:

1. Download the SonicOS Enhanced firmware image file from mysonicwall.com and save it to a location on your local computer.
2. On the System > Settings page, click **Create Backup**.
3. Click **Upload New Firmware**.
4. Browse to the location where you saved the SonicOS Enhanced firmware image file, select the file, and click **Upload**.
5. On the System > Settings page, click the **Boot** icon in the row for **Uploaded Firmware with Factory Default Settings**.
6. In the confirmation dialog box, click **OK**. The SonicWALL restarts and then displays the Setup Wizard, with a link to the login page.
7. Enter the default user name and password (admin / password) to access the SonicWALL management interface.

Using SafeMode to Upgrade Firmware

The SafeMode procedure uses a reset button in a small pinhole, whose location varies: on the NSA models, the button is near the USB ports on the front; on the TZ models, the button is next to the power cord on the back. If you are unable to connect to the SonicWALL security appliance's management interface, you can restart the SonicWALL security appliance in SafeMode. The SafeMode feature allows you to quickly recover 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 SonicWALL security appliance, perform the following steps:

1. Connect your computer to the X0 port on the SonicWALL appliance and configure your IP address with an address on the 192.168.168.0/24 subnet, such as 192.168.168.20.
2. Do one of the following to restart the appliance in SafeMode:
   - Use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the reset button on the front of the security appliance for more than 20 seconds.
   - Use the LCD control buttons on the front bezel to set the appliance to Safe Mode. Once selected, the LCD displays a confirmation prompt. Select **Y** and press the **Right** button to confirm. The SonicWALL security appliance changes to SafeMode.

   The **Test** light starts blinking when the SonicWALL security appliance has rebooted into SafeMode.

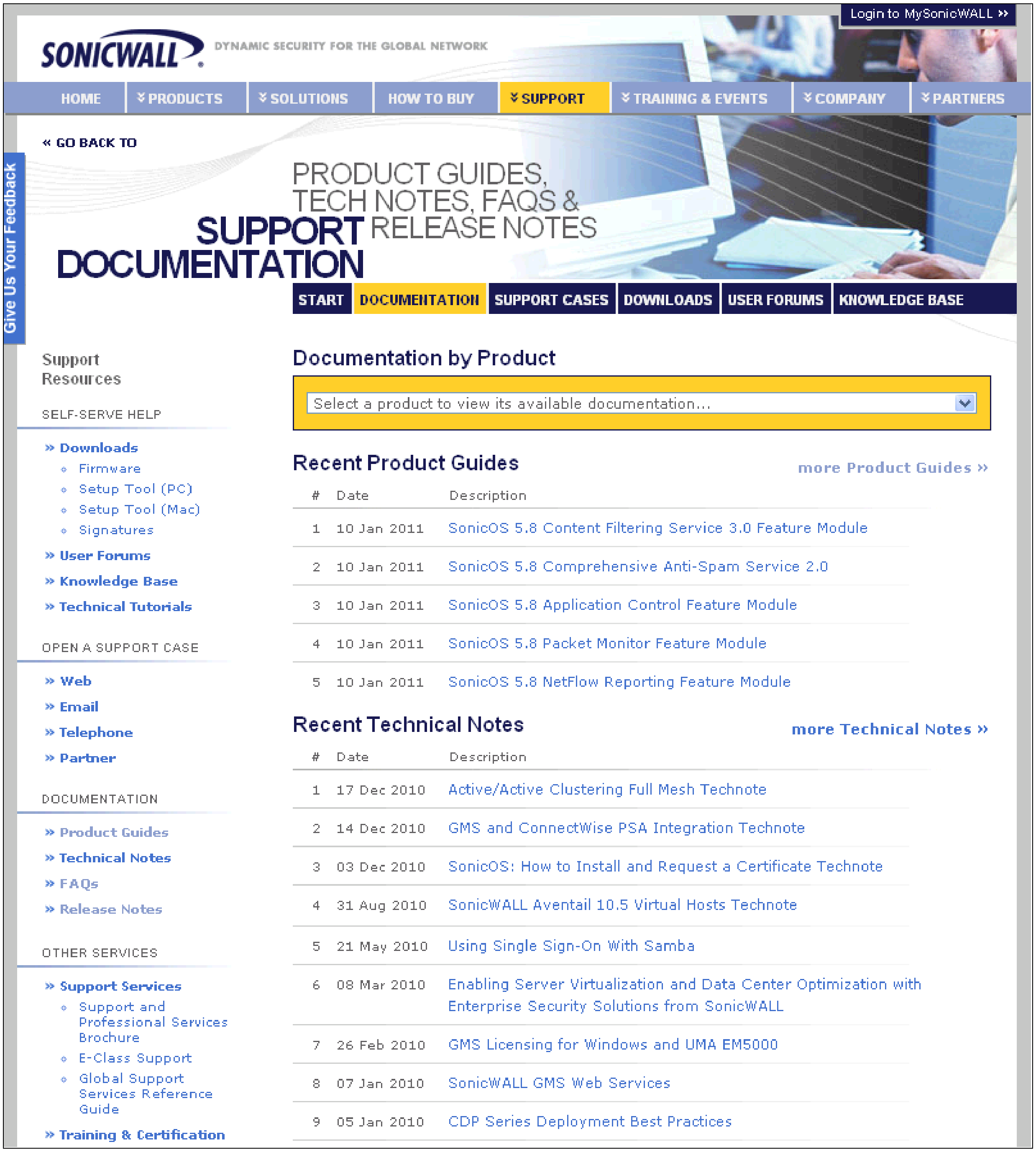
   Note: *Holding the reset button for two seconds will send a diagnostic snapshot to the console. Holding the reset button for six to eight seconds will reboot the appliance in regular mode.*
3. Point the Web browser on your computer to **192.168.168.168**. The SafeMode management interface displays.
4. 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 SonicOS Enhanced firmware image, select the file, and click **Upload**.

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 SonicWALL management interface.

Related Technical Documentation

SonicWALL user guides and reference documentation is available at the SonicWALL Technical Documentation Online Library: http://www.sonicwall.com/us/Support.html

For basic and advanced deployment examples, refer to SonicOS Guides and SonicOS TechNotes available on the Web site, including the ***IPv6 in SonicOS*** feature guide.



Documentation by Product

Recent Product Guides

#	Date	Description
1	10 Jan 2011	SonicOS 5.8 Content Filtering Service 3.0 Feature Module
2	10 Jan 2011	SonicOS 5.8 Comprehensive Anti-Spam Service 2.0
3	10 Jan 2011	SonicOS 5.8 Application Control Feature Module
4	10 Jan 2011	SonicOS 5.8 Packet Monitor Feature Module
5	10 Jan 2011	SonicOS 5.8 NetFlow Reporting Feature Module

Recent Technical Notes

#	Date	Description
1	17 Dec 2010	Active/Active Clustering Full Mesh Technote
2	14 Dec 2010	GMS and ConnectWise PSA Integration Technote
3	03 Dec 2010	SonicOS: How to Install and Request a Certificate Technote
4	31 Aug 2010	SonicWALL Aventail 10.5 Virtual Hosts Technote
5	21 May 2010	Using Single Sign-On With Samba
6	08 Mar 2010	Enabling Server Virtualization and Data Center Optimization with Enterprise Security Solutions from SonicWALL
7	26 Feb 2010	GMS Licensing for Windows and UMA EM5000
8	07 Jan 2010	SonicWALL GMS Web Services
9	05 Jan 2010	CDP Series Deployment Best Practices

Last updated: 4/21/2011