Release Notes

SonicOS

SonicOS Enhanced 5.6.5.1 Release Notes

Contents

Platform Compatibility

The SonicOS 5.6.5.1 release is supported on the following SonicWALL security appliances:

- SonicWALL NSA E8500
- SonicWALL NSA E7500
- SonicWALL NSA E6500
- SonicWALL NSA E5500
- SonicWALL NSA 5000
- SonicWALL NSA 4500
- SonicWALL NSA 3500
- SonicWALL NSA 2400
- SonicWALL NSA 240
- SonicWALL TZ 210 / 210 Wireless-N
- SonicWALL TZ 200 / 200 Wireless-N

This release supports the following Web browsers:

- Internet Explorer 8.0 and higher
- Chrome 4.0 and higher
- Mozilla 3.0 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.

Licensing

Licensing for the Active/Active Clustering (including Stateful High Availability) and BGP Advanced Routing features is included with the following SonicWALL NSA E-Class appliances, when registered:

- SonicWALL NSA E8500
- SonicWALL NSA E7500
- SonicWALL NSA E6500
- SonicWALL NSA E5500

To activate these licenses, register each appliance on MySonicWALL. Even when deployed in a High Availability pair, each unit must be individually registered to activate the licenses.

When available, a SonicOS Expanded License can be purchased for the following SonicWALL appliances to activate the BGP Advanced Routing feature:

- SonicWALL NSA 5000
- SonicWALL NSA 4500
- SonicWALL NSA 3500
- SonicWALL NSA 2400
- SonicWALL NSA 240
- SonicWALL TZ 210 / 210 Wireless-N
- SonicWALL TZ 200 / 200 Wireless-N

Note: Active/Active Clustering is supported only on SonicWALL NSA E-Class appliances.

No free trial is available for the BGP Advanced Routing feature.

Key Features

The following key features are available in SonicOS 5.6.5.1:

- **Active/Active Clustering High Availability**—Active/Active Clustering is the most recent addition to the High Availability feature set in SonicOS. A typical Active/Active Clustering deployment includes four firewalls of the same SonicWALL model configured as two Cluster Nodes, where each node consists of one Stateful High Availability pair. For larger deployments, the cluster can include eight firewalls, configured as four Cluster Nodes.

  With Active/Active Clustering, you can assign certain traffic flows to each node in the cluster, providing load sharing in addition to redundancy, and supporting a much higher throughput without a single point of failure. Earlier High Availability features, such as Stateful Synchronization and Active/Active DPI (previously called Active/Active UTM), continue to be supported and are recommended for use in conjunction with Active/Active Clustering.

  Active/Active Clustering is supported only on SonicWALL NSA E-Class appliances.

- **BGP Advanced Routing**—Border Gateway Protocol (BGP) advanced routing is a large-scale routing protocol used to communicate routing information between Autonomous Systems (AS's), which are well-defined, separately administered network domains. BGP support allows for SonicWALL security appliances to replace a traditional BGP router on the edge of a network's AS. The current SonicWALL implementation of BGP is most appropriate for "single-provider / single-homed" environments, where the network uses one ISP as their Internet provider and has a single connection to that provider. SonicWALL BGP is also capable of supporting "single-provider / multi-homed" environments, where the network uses a single ISP but has a small number of separate routes to the provider. Because BGP transmits packets in the clear, SonicWALL supports using an IPSec tunnel for secure BGP sessions. The IPSec tunnel is configured independently within the VPN configuration section of the SonicOS Web-based management interface, while BGP is enabled on the Network > Routing page and then configured on the SonicOS Command Line Interface.

  BGP Advanced Routing is available on all SonicWALL NSA and TZ appliances supported in SonicOS 5.6.5.1.

- **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. SonicOS 5.6.5.1 supports Static Link Aggregation, in which the two ends of the trunk have the same configuration. Up to 4 ports can be grouped to form a single aggregate link. If any of the ports fail, SonicOS continues to pass traffic (at a diminished throughput) while there is at least one active interface.

  Link Aggregation is useful in deployments requiring more than 1 Gbps throughput for traffic flowing between two interfaces. This feature is available on all SonicWALL NSA E-Class appliances.

  Link Aggregation is supported only on SonicWALL NSA E-Class appliances.

- **Port Redundancy**—Port Redundancy provides the ability to configure a second, redundant, physical interface for any Ethernet interface on a SonicWALL NSA E-Class appliance. When the primary interface is active, it handles all traffic to and from the interface. If the primary interface fails, the backup interface takes over and handles all incoming and outgoing traffic. When the primary interface comes up again, it takes over all the traffic handling duties from the backup interface.

  This is very useful in high end deployments to avoid a single point of failure, such as the connection to a switch. With Port Redundancy, a second interface can be connected to the same or another switch to provide an alternate path for the traffic.

  Port Redundancy is supported only on SonicWALL NSA E-Class appliances.

The following are the key features supported in all versions of SonicOS 5.6:

- **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 SonicWALL's Deep Packet Inspection technology, then re-encrypt (or optionally SSL-offload) the traffic and send it to its destination if no threats or vulnerabilities are found. This feature works for both client and server deployments. It provides additional security, application control, and data leakage prevention functionality for analyzing encrypted HTTPS and other SSL-based traffic. The following security services and features are capable of utilizing DPI-SSL: Gateway Anti-Virus, Gateway Anti-Spyware, Intrusion Prevention, Content Filtering, Application Firewall, Packet Monitor and Packet Mirror. DPI-SSL is supported on SonicWALL NSA models 240 and higher.
- **3G and Modem Support**—SonicOS 5.6 supports 3G and Modem configurations for WAN Load Balancing (WLB). (3G and Modem support is available on all NSA models except the SonicWALL NSA 2400.)
- **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 SonicOS. 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 DPI Connection Support**—Provides the ability to increase the number of simultaneous connections on which SonicWALL security appliances can apply Deep Packet Inspection (DPI) services (Intrusion Prevention Service, Application Firewall, Gateway Anti-Virus, and Gateway Anti-Spyware). This feature is intended for high-end (E-Class) customers who need to support a large number of concurrent connections. (Note: There is a slight performance decrease when this option is enabled.)
- **FairNet for SonicPoint-N**—Provides the ability to create policies that equally distribute bandwidth for all wireless users connected to a SonicPoint-N.

- **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 a SonicWALL 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 SonicWALL security appliances to download signatures even when they access the Internet through a proxy server. This feature also allows for registration of SonicWALL 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.

  NOTE*: The SonicWALL Terminal Services Agent is not supported in SonicOS 5.6.5.1 due to limitations of current SSO agent functionality that prevent its use with Active/Active Clustering.*
- **SSL VPN Enhancements**—SonicOS 5.6 provides a number of SSL VPN enhancements:
  - **Bookmarks for SSH and RDP**—Provides support for users to create bookmarks on the SSL VPN Virtual Office to access systems using SSH, RDP, VNC, and Telnet services.
  - **Granular User Controls**—Allows network administrators to configure different levels of policy access for NetExtender users based on user ID.
  - **One-Time Password**—Provides additional security by requiring users to enter a randomly generated, single-use password in addition to the standard user name and password credentials.
  - **Separate Port and Certificate Control**—Provides separate port access for SSL VPN and HTTPS management certificate control, allowing administrators to close HTTPS management while leaving SSL VPN open.
  - **Virtual Assist**—Provides a remote assistance tool to SonicWALL security appliance users. SonicWALL Virtual Assist is a thin client remote support tool provisioned via a Web browser. It enables a technician to assume control of a customer’s PC or laptop for the purpose of providing remote technical assistance.
- **Unbounded Multiple WAN Support**—Provides the ability to enable any number of WAN Ethernet interfaces for WAN Load Balancing and Failover on SonicWALL appliances.
- **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 a SonicWALL 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.

Known Issues

This section contains a list of known issues in the SonicOS 5.6.5.1 release.

Symptom	Condition / Workaround	Issue
In Active/Active clustering, a node cannot access MySonicWALL for license synchronization, and diagnostic tests to the Default Gateway and DNS server fail.	Occurs when the node does not own a Virtual Group, which can occur when it is configured with factory defaults and not aware of its A/A Clustering license, or when the license is activated, but the unit is not yet configured to own a Virtual Group. **Workaround**: Before connecting the node to the A/A Cluster, register the units and synchronize with MySonicWALL.	97905
The redundant port for the X1 WAN interface does not pass traffic after X1 is disconnected.	Occurs when High Availability is enabled for Active/Passive mode, and X4 or another interface is configured as a redundant port for X1, and then the X1 interface is physically disconnected. **Workaround**: Disable High Availability and then traffic is passed on the redundant port.	97883
The gateway IP address is wrong for default routes received from OSPF.	Occurs when a remote router or firewall is connected to a SonicWALL appliance (X1 on router is connected to a DMZ zone port (X2) on the appliance). OSPF is enabled on both devices, the router advertises a default route to the appliance, and the appliance adds the default route to its routing table. However, the gateway IP address for the default route is set to the IP address of the router's X1 interface, rather than to the router's gateway IP address.	97409
In Active/Active clustering, the IP address for interface X1, Virtual Group 2 reverts to the IP address for X1, Virtual Group 1.	Occurs when verifying NAT policies after running the Public Server Wizard. The IP address for X1-Virtual Group 2 incorrectly displays the address for X1-Virtual Group 1 instead.	95327
In a two-node Active/Active cluster, an active Manual Key VPN policy tunnel does not appear in the VPN settings of a backup unit in Node 2, although traffic continues to pass and the active unit shows the tunnel.	Occurs when the policy is bound to Virtual Group 1 and a node-level failover occurs while the tunnel is in active use on Node 1.	93392
When Active/Active clustering is enabled, settings for the Packet Monitor filter are copied to the Display filter. The Display filter settings cannot be removed.	Occurs when the Packet Monitor filter settings are added before enabling Active/Active clustering. The Display filter contains these settings even after manually clearing them and then restarting the SonicWALL appliance.	93188
When using Active/Active Clustering with four nodes where each node is part of HA pair, traffic from the HA idle units cannot go out and they cannot connect to the License manager.	Occurs on Active/Active clusters with four nodes configured as HA pairs. Multiple WAN interfaces are configured and probing/probe target is enabled. When one of the WAN interfaces is down, the default route of the idle units remain pointed to the down WAN interface.	90256

Symptom	Condition / Workaround	Issue
Traffic over static VPN routes is dropped after a node level link failover.	Occurs after the X1 link on the Master node is disconnected. Traffic will drop over the VPN tunnel, but after flushing the connection, traffic will recommence flowing through the tunnel.	90215
Active/Active clustering IP Helper support does not yet exist.	Occurs when trying to use IP Helper in an Active/Active clustering deployment.	89265
On the Policy-Based Routing screen, BGP routes are shown as "OSPF or RIP route."	Occurs when viewing the comment settings for a BGP route in the Network > Routing page. The comment should show as "BGP route."	89112
When a node is deleted from the Active/Active Nodes table on the High Availability page, the interface is not deleted from the Network > Interfaces page.	Occurs when deleting a node from the Active/Active Nodes table and then viewing the Network > Interfaces page. **Workaround**: Click the edit icon for the deleted interface and then click OK. The interface will be deleted.	89017
OSPF continues to advertise the Default Route even after a WAN link failure due to WAN Load Balancing logical probing.	Occurs when the option is enabled to advertise the default route when the WAN is up, and WLB Probing is enabled on the WAN. Upon a WAN link failure, OSPF will still display the default route.	88371
Incorrectly configured routes prevent the user from connecting to or pinging the directly connected network.	Occurs when a preferences file is uploaded containing custom routes in which the Destination network is pointing to a LAN subnet and the Default Gateway is in the same subnet, or the Destination firewall interface IP address is routed to the Default Gateway IP address.	68413

Resolved Issues

This section contains a list of resolved issues in the SonicOS 5.6.5.1 release.

Symptom	Condition / Workaround	Issue
Changes made on the primary unit of a High Availability pair are not automatically synchronize to the backup unit.	Occurs when the HA pair is fully configured and then the backup unit is powered down while changes are made on the primary unit, and then the backup is powered up again.	97875
A firewall access rule using an FQDN destination object does not work normally after restarting the appliance.	Occurs when a deny rule is configured for traffic from the LAN to the WAN zone. After configuring the rule, pings do not go through from LAN to a destination on the WAN. After restarting the appliance, pings succeed.	97001
With BGP disabled and Stealth mode enabled, the firewall resets the connection for TCP port 179 when a port scan occurs.	Occurs when performing a TCP port scan on the WAN after disabling BGP and enabling Stealth mode on the Firewall > Advanced screen.	96949
A Virtual Group IP address is not accessible in an Active/Active cluster.	Occurs when attempting to access the LAN Virtual Group IP address of Node 2 in the cluster. All the other Virtual IP addresses are accessible.	96891
On a SonicWALL TZ 210 Wireless-N appliance, some buttons/links are missing from the Network > Interfaces page, preventing the administrator from adding a subnet to the WLAN zone.	Occurs because the **Add WLAN Subnets** button and the **3G/4G/Dial-up use can be set at Network > Failover & LB** link are missing from the Network > Interfaces page.	96836
When Virtual MAC is enabled, modifying the Virtual MAC interface value causes the logical IP address of the interface to become inaccessible.	Occurs when the option to override Virtual Mac is enabled and the Virtual Mac interface value is modified, in a Stateful High Availability environment with Virtual Mac enabled. After disabling Virtual Mac and then re-enabling it, the logical IP is accessible again.	93123

Upgrading SonicOS Image Procedures

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

Obtaining the Latest SonicOS Image Version

To obtain a new SonicOS 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 image file to a directory on your management station.

You can update the SonicOS 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.

Upgrading a SonicOS Image with Current Preferences

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

1. Download the SonicOS 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 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 image version information is listed on the **System** > **Settings** page.

Importing Preferences to SonicOS 5.6

Preferences importing to SonicWALL security appliances is generally supported from the following SonicWALL appliances running SonicOS:

- NSA Series
- NSA E-Class Series
- TZ 210/200/100/190/180/170 Series
- PRO Series

There are certain exceptions to preferences importing on these appliances running the SonicOS 5.6 release. Preferences cannot be imported in the following cases:

- Settings files containing Portshield interfaces created prior to SonicOS 5.x
- Settings files containing VLAN interfaces are not accepted by the TZ 100/200 Series firewalls
- Settings files from a PRO 5060 with optical fiber interfaces where VLAN interfaces have been created

Full support for preferences importing from these appliances is targeted for a future release. At that time, you will need to upgrade your firmware to the latest SonicOS maintenance release available on MySonicWALL.

Importing Preferences from SonicOS Standard to SonicOS 5.6 Enhanced

The SonicOS Standard to Enhanced Settings Converter is designed to convert a source Standard Network Settings file to be compatible with a target SonicOS Enhanced appliance. Due to the more advanced nature of SonicOS Enhanced, its Network Settings file is more complex than the one SonicOS Standard uses. They are not compatible. The Settings Converter creates an entirely new target Enhanced Network Settings file based on the network settings found in the source Standard file. This allows for a rapid upgrade from a Standard deployment to an Enhanced one with no time wasted in re-creating network policies. **Note**: SonicWALL recommends deploying the converted target Network Settings file in a testing environment first and always keeping a backup copy of the original source Network Settings file.

The SonicOS Standard to Enhanced Settings Converter is available at:
https://convert.global.sonicwall.com/

If the preferences conversion fails, email your SonicOS Standard configuration file to settings_converter@sonicwall.com with a short description of the problem. In this case, you may also consider manually configuring your SonicWALL appliance.

To convert a Standard Network Settings file to an Enhanced one:

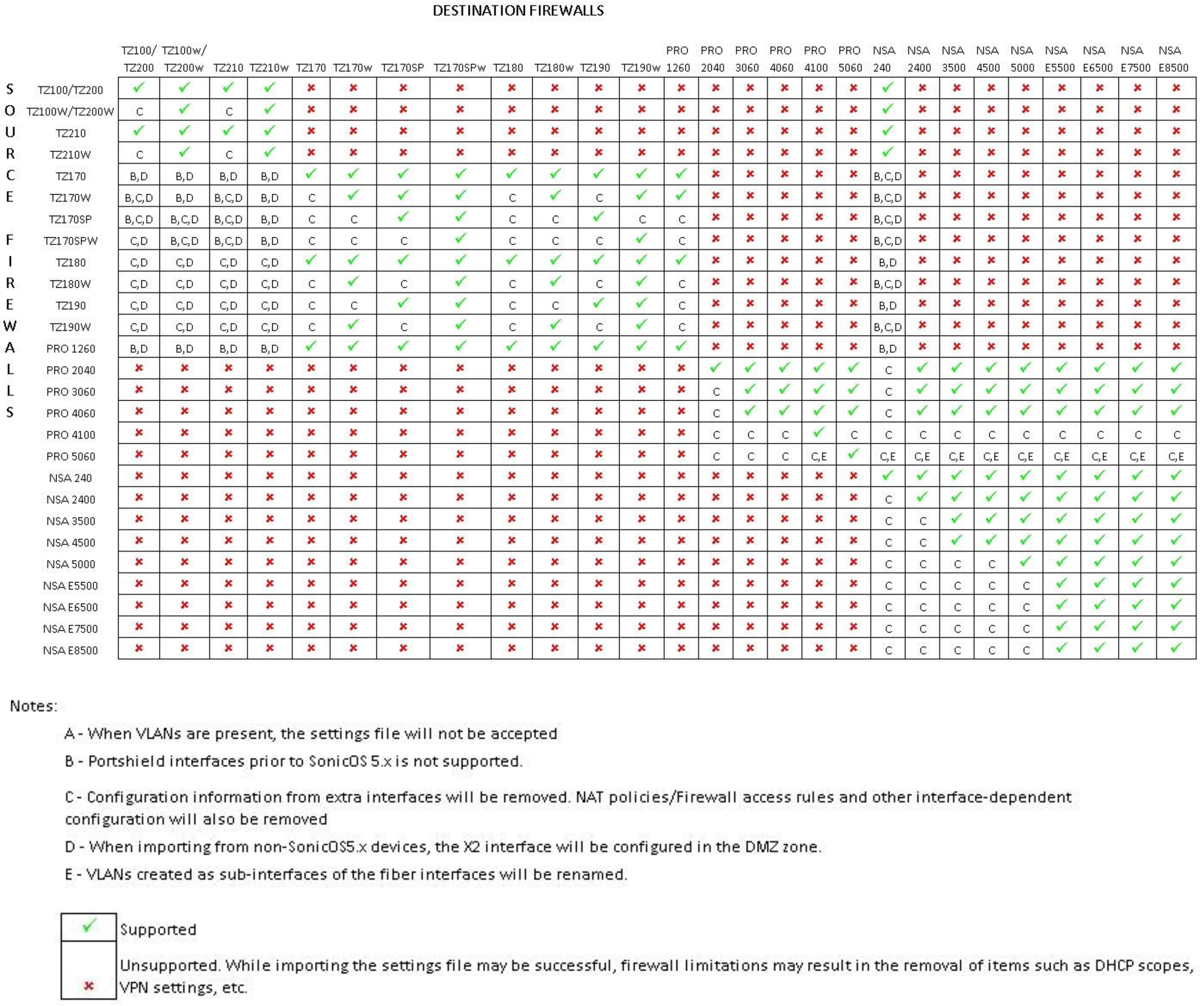
1. Log in to the management interface of your SonicOS Standard appliance, navigate to **System > Settings**, and save your network settings to a file on your management computer.
2. On the management computer, point your browser to https://convert.global.sonicwall.com/.
3. Click the **Settings Converter** button.
4. Log in using your MySonicWALL credentials and agree to the security statement.

   The source Standard Network Setting file must be uploaded to MySonicWALL as part of the conversion process. The Setting Conversion tool uses MySonicWALL authentication to secure private network settings. Users should be aware that SonicWALL will retain a copy of their network settings after the conversion process is complete.
5. Upload the source Standard Network Settings file:
   - Click **Browse**.
   - Navigate to and select the source SonicOS Standard Settings file.
   - Click **Upload**.
   - Click the right arrow to proceed.
6. Review the source SonicOS Standard Settings Summary page.

   This page displays useful network settings information contained in the uploaded source Network Settings file. For testing purposes, the LAN IP and subnet mask of the appliance can be changed on this page in order to deploy it in a testing environment.
   - (Optional) Change the LAN IP address and subnet mask of the source appliance to that of the target appliance.
   - Click the right arrow to proceed.
7. Select the target SonicWALL appliance for the Enhanced deployment from the available list.

   SonicOS Enhanced is configured differently on various SonicWALL appliances, mostly to support different interface numbers. As such, the converted Enhanced Network Settings file must be customized to the appliance targeted for deployment.
8. Complete the conversion by clicking the right arrow to proceed.
9. Optionally click the **Warnings** link to view any differences in the settings created for the target appliance.
10. Click the **Download** button, select Save to Disk, and click OK to save the new target SonicOS Enhanced Network Settings file to your management computer.
11. Log in to the management interface for your SonicWALL appliance.
12. Navigate to **System > Settings**, and click the **Import Settings** button to import the converted settings to your appliance.

Support Matrix for Importing Preferences



DESTINATION FIREWALLS

		TZ100/	TZ100w/											PRO	PRO	PRO	PRO	PRO	PRO	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA
		TZ200	TZ200w	TZ210	TZ210w	TZ170	TZ170w	TZ170SP	TZ170SPw	TZ180	TZ180w	TZ190	TZ190w	1260	2040	3060	4060	4100	5060	240	2400	3500	4500	5000	E5500	E6500	E7500	E8500
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 4100	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	C	✓	C	C	C	C	C	C	C	C	C	C
	PRO 5060	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	C	C,E	✓	C,E	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	✓	✓	✓	✓
	NSA E8500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	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 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 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 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 firmware image, select the file, and click **Upload**.
6. Select the boot icon in the row for one of the following:
   - **Uploaded Firmware – New!** ☞

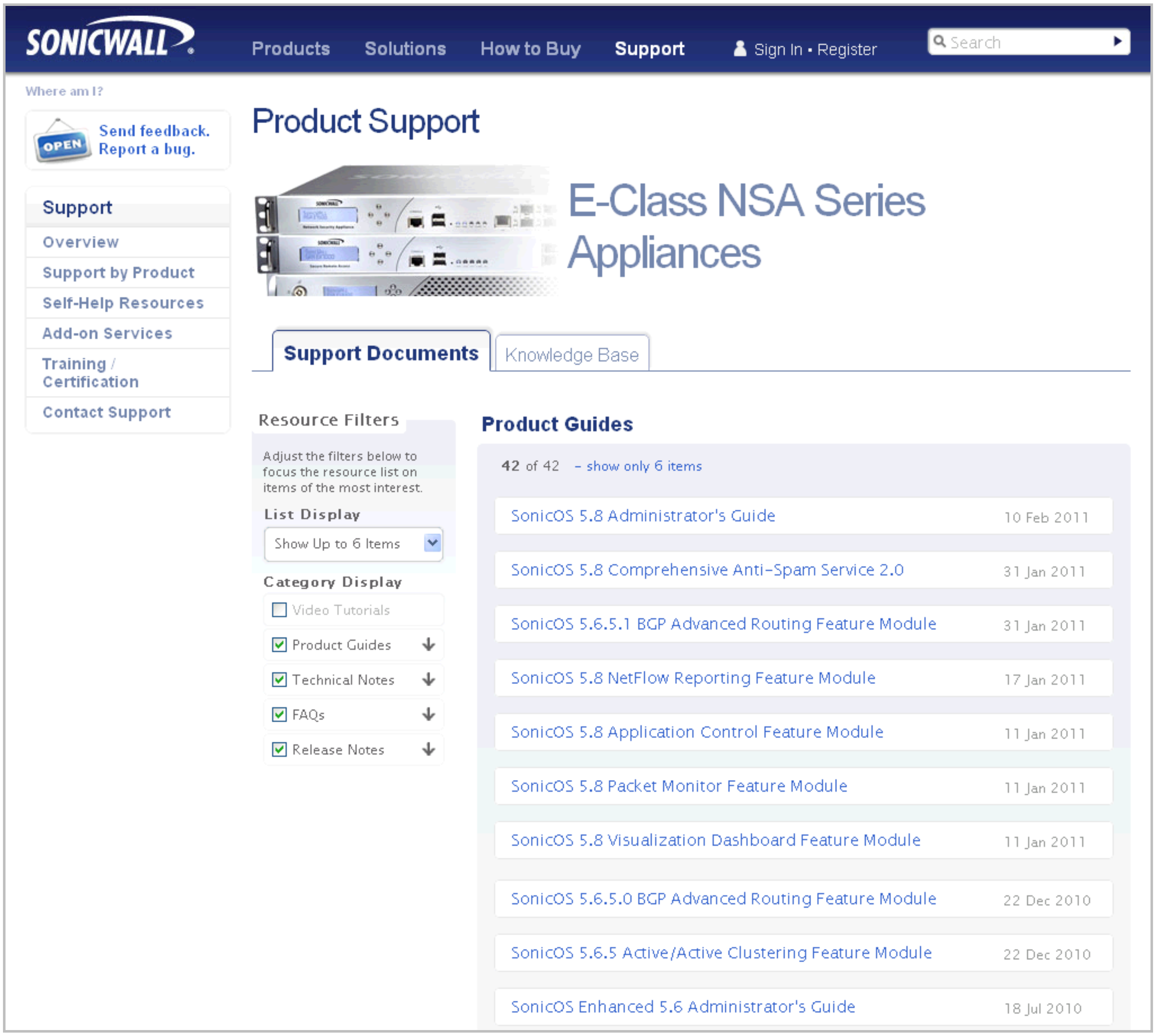
     Use this option to restart the appliance with your current configuration settings.
   - **Uploaded Firmware with Factory Defaults – New!** ☞

     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.



Resource Filters

Adjust the filters below to focus the resource list on items of the most interest.

List Display

Show Up to 6 Items

Category Display

□ Video Tutorials
☑ Product Guides
☑ Technical Notes
☑ FAQs
☑ Release Notes

Product Guides

42 of 42 – show only 6 items

SonicOS 5.8 Administrator's Guide	10 Feb 2011
SonicOS 5.8 Comprehensive Anti-Spam Service 2.0	31 Jan 2011
SonicOS 5.6.5.1 BGP Advanced Routing Feature Module	31 Jan 2011
SonicOS 5.8 NetFlow Reporting Feature Module	17 Jan 2011
SonicOS 5.8 Application Control Feature Module	11 Jan 2011
SonicOS 5.8 Packet Monitor Feature Module	11 Jan 2011
SonicOS 5.8 Visualization Dashboard Feature Module	11 Jan 2011
SonicOS 5.6.5.0 BGP Advanced Routing Feature Module	22 Dec 2010
SonicOS 5.6.5 Active/Active Clustering Feature Module	22 Dec 2010
SonicOS Enhanced 5.6 Administrator's Guide	18 Jul 2010

Last updated: 4/7/2011