Release Notes

SonicOS

SonicOS 5.6.0.5 Release Notes

Contents

Platform Compatibility

The SonicOS Enhanced 5.6.0.5 release is supported on the following SonicWALL UTM appliances:

- SonicWALL TZ 100
- SonicWALL TZ 100 Wireless-N
- SonicWALL TZ 200
- SonicWALL TZ 200 Wireless-N
- SonicWALL TZ 210
- SonicWALL TZ 210 Wireless-N
- SonicWALL NSA 240
- SonicWALL NSA 2400
- SonicWALL NSA 3500
- SonicWALL NSA 4500
- SonicWALL NSA 5000
- SonicWALL NSA E5500
- SonicWALL NSA E6500
- SonicWALL NSA E7500

NOTE: SonicOS 5.6.0.5 supports the following wireless access points:

- SonicPoint-Ne
- SonicPoint-Ni

This release supports the following Web browsers:

- Microsoft Internet Explorer 8.0 and higher
- Mozilla Firefox 3.0 and higher
- Chrome 4.0 and higher

Strong SSL and TLS Encryption Required in Your Browser

The internal 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 3.0 and Microsoft Internet Explorer 8.0 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.

SonicPoint-Ne / SonicPoint-Ni Support

SonicOS 5.6.0.5 supports two new wireless access point products from SonicWALL, the **SonicPoint-Ne** and **SonicPoint-Ni**.

These new devices provide the following features and capabilities:

- 802.11 a/b/g/n (2.4 GHz and 5 GHz) 3x3 MIMO single radio subsystems on board
- One 10/100/1000 Base-T RJ-45 interface and one RJ-45 console port
- 16 MB Flash, 64 MB DDR2 RAM
- 802.3af compliant Power Over Ethernet (PoE)
- Ceiling or wall mountable
- SonicPoint-Ne has 3 SMA connectors (coaxial RF connectors) for external antennas, and can use a power adaptor or PoE injector
- SonicPoint-Ni has 3 internal antennas, and is powered by PoE injector only

For more information about the SonicPoint-Ne and SonicPoint-Ni, see the *SonicPoint-Ne / SonicPoint-Ni Getting Started Guide*, available on http://www.sonicwall.com/us/Support.html.

Key Features in SonicOS 5.6

The following are the key features supported in 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 Capture and Packet Mirror. DPI-SSL is initially available on SonicWALL NSA models 3500 and above.

- **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 UTM Connection Support** – Provides the ability to increase the number of simultaneous connections on which SonicWALL 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 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.
- **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 TZ and NSA appliances.
- **Virtual Access Points for SonicWALL TZ Wireless Platforms –** The SonicWALL TZ 100W, TZ 200W and TZ 210W platforms now support Virtual Access Points (VAPs). VAPs enable users to segment different wireless groups by creating logical segmentation on a single wireless radio. Note that VAPs are not supported on SonicPoint or SonicPoint-N devices.
- **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.
- **Wireless Bridging for SonicWALL TZ Wireless Platforms –** The SonicWALL TZ 100W, TZ 200W and TZ 210W platforms now support Wireless Bridging, which provides the ability to extend a single wireless network across multiple SonicWALL wireless security appliances.

Known Issues

This section contains a list of known issues in the SonicOS 5.6.0.5 release.

Symptom	Condition / Workaround	Issue
Static routes and connected networks with “non-classful” prefix lengths are in specific cases not redistributed by OSPF.	Occurs when OSPF is enabled for networks that have a prefix longer—more restrictive network mask—than other connected networks, and the other networks do not use /8, /16, /24, or /32 subnets. In this scenario, when the connected networks are redistributed, those which do not have /8, /16, /24, or /32 prefixes (subnet mask length) may not be advertised by OSPF.	89382
A user may not be able to login to the firewall if DPI-SSL is enabled.	Occurs when a user is unable to login to a firewall from a LAN-side PC, even when the user or user group is specifically selected on the exclusion list for DPI-SSL.	89324
Packets can be dropped when WAN to LAN inbound rules and NATs are created to allow services on additional WAN public IPs.	Occurs when the WAN interface is L2-bridged with another interface, and port-forwarding to a NAT-enabled network does not work from WAN to LAN when any additional public IPs are used from the WAN subnet.	89307
Some connections are not made between a SonicPoint and a firewall that has a stateful failover setup.	Occurs when wireless guest services are configured on the WLAN zone, and the firewall has Active-Active UTM and Force UTM offload enabled.	88842
The appliance may restart if certain static routes are configured and Terminal Services Agents are used.	Occurs when one or more LAN-side routes are using a group address object as their destination. **Workaround:** Configure these routes individually, each with a single address object as the destination.	87697
The “Enable SSID Suppress” checkbox will be unchecked after subsequently making changes on the Wireless > Settings management interface page.	Occurs when a user selects the “Enable SSID Suppress” checkbox of the default Virtual Access Point (VAP) object, and then selects the Internal AP Group for internal wireless on the Wireless > Settings management interface page. **Workaround**: Select the “Enable SSID Suppress” checkbox again.	87440
A user is unable to open the SSL VPN portal page.	Occurs when a user selects a custom certificate on the SSL VPN server settings page, then deletes the imported certificate, and then attempts to access the SSL VPN portal page from a LAN client.	87361
The 802.11n high throughput of a wireless client is reduced after modifying the wireless security method.	Occurs when a user changes the security method from WEP-Shared or WEP-Both to an Open, WPA or WPA2 method. **Workaround:** Reboot the UTM appliance to return throughput to the correct level.	87156
A DPI-SSL SSL server is removed after modifying an Address Object name.	Occurs when the Address Object name being used by this SSL server is modified.	87074

Gateway Anti-Virus (GAV) and Anti-Spyware do not log or block virus or spyware infected downloads when FTP over SSL is enabled.	Occurs when SonicOS has client DPI-SSL, GAV, and Anti-Spyware enabled on the LAN zone, and SSL is enabled on an FTP server in the WAN zone, and a LAN client downloads files from the FTP server.	86620
The Wireless Wizard does not configure the authentication mode for “W0” radio.	Occurs when “Internal AP Group” is selected for Virtual Access Point Group under Wireless > Settings, but the Wireless Wizard does not configure the authentication mode. **Workaround:** Wireless Wizard will work, if “Internal AP Group” is not selected.	86578
Static routes are not redistributed over RIPv2.	Occurs when static routes over a tunnel interface are created using Address Groups rather than Address Objects.	86575
Exchanging members in a default load balancing group is not allowed and errors are issued.	Occurs when a user attempts to reconfigure and exchange interfaces on a default load balancing group consisting of interface X1 as a member, and interface X2 as a final backup. **Workaround**: Remove the interfaces from their respective assignments, click OK, and then set the interfaces to their new assignments.	86088
An FTP client cannot connect to an FTP server in passive mode.	Occurs when a user configures a WAN interface as a Layer 2 Tunneling Protocol client, then tries connecting to a WAN-side FTP server using passive mode, from a LAN-side PC.	85765
On No-ip.com, status remains “offline” when the profile within the device shows as “online.”	Occurs when the Dynamic DNS profile is enabled on the firewall, but the firewall cannot sync with the provider, No-ip.com, to update status.	85391
Network Monitor ICMP probes fail when the probe target is on other side of normal S2S VPN tunnel.	Occurs when Network Monitor sends the probes out using the WAN interface, rather than using the S2S VPN tunnel.	82272

Resolved Issues

This section contains a description of a resolved issue in the SonicOS 5.6.0.5 release.

Vulnerability

Symptom	Condition / Workaround	Issue
A cross site request forgery (CSRF) vulnerability exists which can allow a specifically constructed string to be executed in the context of a Web browser.	This can occur when certain input is entered into the Web or SSH interface of the device. This vulnerability was identified and submitted through the SecuriTeam Secure Disclosure program working with Nikolas Sotiriu.	91804

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 the SonicWALL UTM 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:

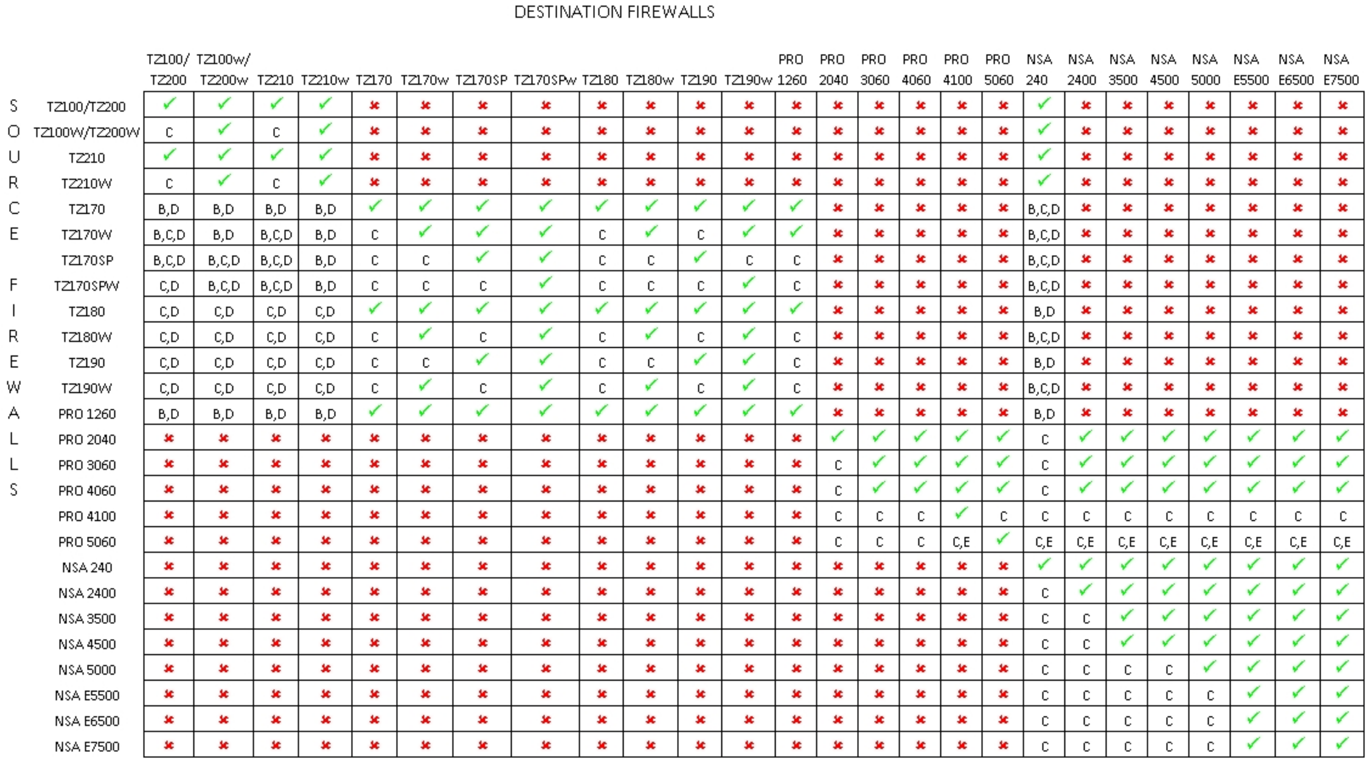
1. Log in to the management interface of your SonicOS Standard appliance, navigate to **System > Settings**, and save your network settings to a file on your management computer.
2. On the management computer, point your browser to https://convert.global.sonicwall.com/.
3. Click the **Settings Converter** 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
		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
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
	PRO 5060	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	C	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	✓	✓	✓

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 login page.
7. Enter the default user name and password (admin / password) to access the SonicWALL management interface.

Using SafeMode to Upgrade Firmware

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. The reset button is in a small hole next to the USB ports.
   - 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.

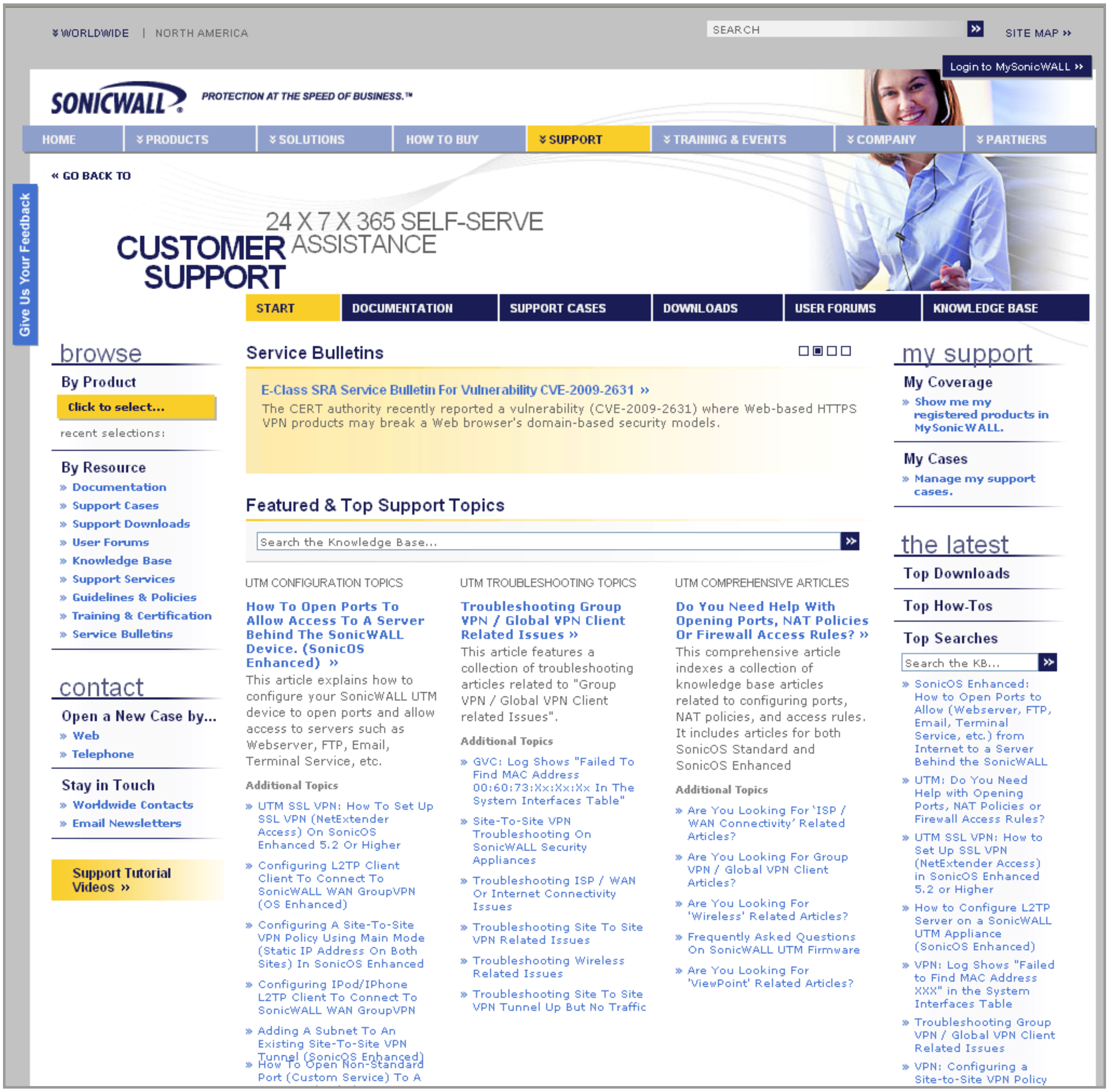
   The **Test** light starts blinking when the SonicWALL security appliance has rebooted into SafeMode.

   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.



browse

By Product

Click to select...

recent selections:

By Resource

- » Documentation
- » Support Cases
- » Support Downloads
- » User Forums
- » Knowledge Base
- » Support Services
- » Guidelines & Policies
- » Training & Certification
- » Service Bulletins

contact

Open a New Case by...

- » Web
- » Telephone

Stay in Touch

- » Worldwide Contacts
- » Email Newsletters

Support Tutorial Videos »

Service Bulletins

□▣□□

E-Class SRA Service Bulletin For Vulnerability CVE-2009-2631 »

The CERT authority recently reported a vulnerability (CVE-2009-2631) where Web-based HTTPS VPN products may break a Web browser's domain-based security models.

Featured & Top Support Topics

Search the Knowledge Base...

UTM CONFIGURATION TOPICS

How To Open Ports To Allow Access To A Server Behind The SonicWALL Device. (SonicOS Enhanced) »

This article explains how to configure your SonicWALL UTM device to open ports and allow access to servers such as Webserver, FTP, Email, Terminal Service, etc.

Additional Topics

- » UTM SSL VPN: How To Set Up SSL VPN (NetExtender Access) On SonicOS Enhanced 5.2 Or Higher
- » Configuring L2TP Client Client To Connect To SonicWALL WAN GroupVPN (OS Enhanced)
- » Configuring A Site-To-Site VPN Policy Using Main Mode (Static IP Address On Both Sites) In SonicOS Enhanced
- » Configuring IPod/IPhone L2TP Client To Connect To SonicWALL WAN GroupVPN
- » Adding A Subnet To An Existing Site-To-Site VPN Tunnel (SonicOS Enhanced)
- » How To Open Non-Standard Port (Custom Service) To A

UTM TROUBLESHOOTING TOPICS

Troubleshooting Group VPN / Global VPN Client Related Issues »

This article features a collection of troubleshooting articles related to "Group VPN / Global VPN Client related Issues".

Additional Topics

- » GVC: Log Shows "Failed To Find MAC Address 00:60:73:Xx:Xx:Xx In The System Interfaces Table"
- » Site-To-Site VPN Troubleshooting On SonicWALL Security Appliances
- » Troubleshooting ISP / WAN Or Internet Connectivity Issues
- » Troubleshooting Site To Site VPN Related Issues
- » Troubleshooting Wireless Related Issues
- » Troubleshooting Site To Site VPN Tunnel Up But No Traffic

UTM COMPREHENSIVE ARTICLES

Do You Need Help With Opening Ports, NAT Policies Or Firewall Access Rules? »

This comprehensive article indexes a collection of knowledge base articles related to configuring ports, NAT policies, and access rules. It includes articles for both SonicOS Standard and SonicOS Enhanced

Additional Topics

- » Are You Looking For 'ISP / WAN Connectivity' Related Articles?
- » Are You Looking For Group VPN / Global VPN Client Articles?
- » Are You Looking For 'Wireless' Related Articles?
- » Frequently Asked Questions On SonicWALL UTM Firmware
- » Are You Looking For 'ViewPoint' Related Articles?

my support

My Coverage

- » Show me my registered products in MySonicWALL.

My Cases

- » Manage my support cases.

the latest

Top Downloads

Top How-Tos

Top Searches

Search the KB...

- » SonicOS Enhanced: How to Open Ports to Allow (Webserver, FTP, Email, Terminal Service, etc.) from Internet to a Server Behind the SonicWALL
- » UTM: Do You Need Help with Opening Ports, NAT Policies or Firewall Access Rules?
- » UTM SSL VPN: How to Set Up SSL VPN (NetExtender Access) in SonicOS Enhanced 5.2 or Higher
- » How to Configure L2TP Server on a SonicWALL UTM Appliance (SonicOS Enhanced)
- » VPN: Log Shows "Failed to Find MAC Address XXX" in the System Interfaces Table
- » Troubleshooting Group VPN / Global VPN Client Related Issues
- » VPN: Configuring a Site-to-Site VPN Policy

Last updated: 7/20/2010