Release Notes

SonicOS

SonicOS 5.5.1.2 FIPS / Common Criteria Release Notes

Contents

Platform Compatibility

The SonicOS 5.5.1.2 FIPS release is supported on the following SonicWALL UTM appliances:

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

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.

New Features

The SonicOS 5.5.1.2 FIPS release complies with Federal Information Processing Standards (FIPS). These standards are created by the United States federal government for use by government contractors and agencies, and include security related standards for encryption and data encoding, and other standards.

The SonicOS 5.5.1.2 FIPS release is certified for Level 3 Cryptographic Module Specification and Level 3 Design Assurance, both in support of the new Common Criteria 3.1 requirements.

The Common Criteria (Common Criteria for Information Technology Security) is an international standard (ISO 15408) that defines a rigorous process for specifying, implementing and evaluating information security products. Common Criteria defines a set of components, including Protection Profiles to identify security requirements, Security Targets to specify the security capabilities of a particular product, and Evaluation Assurance Levels (EALs) that define how thoroughly the product is tested to determine that it meets its Security Target. EALs are rated from 1 to 7, where level one represents the least amount of testing and seven represents the most thorough testing.

The SonicWALL NSA appliances listed under Supported Platforms above are certified for Common Criteria EAL-4+ when running SonicOS 5.5.1.2.

The Common Criteria SonicOS 5.5.1 listing is available on the Communication Security Establishment's Web site:

http://www.cse-cst.gc.ca/its-sti/services/cc/sonicos-v551-apr-eng.html

Report and product listings are available at the following location, certificate numbers pending:

http://www.cse-cst.gc.ca/its-sti/services/cc/sonicos-v551-apr-maint-eng.html

Known Issues

This section contains a list of known issues in the SonicOS 5.5.1.2 FIPS release.

FIPS

Symptom	Condition / Workaround	Issue
The firewall should check Phase 2 Encryption and Authentication settings when enabling FIPS mode, and should print an error message if a conflict is found.	Occurs when an S2S VPN policy is added, with DES and MD5 selected for Phase 2 Encryption and Authentication, and then an attempt is made to enable FIPS mode.	91475
With FIPS mode enabled, "None" can be selected as authentication mode for an S2S VPN policy, which prevents the tunnel from being established. The "None" option should not be available.	Occurs when FIPS mode is enabled and an S2S VPN policy is added with SHA1 selected for Phase 2 and a matching policy is added on the remote firewall. If EAP is used, a "None" option becomes available for authentication. After the tunnel is up, SHA1 is changed to "None" for Phase 2. The system shows that the change is saved, but when this VPN policy is edited again, SHA1 is still selected as the authentication method for Phase 2. At this point, the tunnel cannot be established.	91465

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.

Upgrading a SonicOS Enhanced 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 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.

Importing Preferences to SonicOS Enhanced 5.5

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

- 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 a SonicOS Enhanced 5.5.1.x release. Preferences cannot be imported in the following cases:

- Settings files containing Portshield interfaces created prior to SonicOS 5.x
- 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 Enhanced 5.5

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.

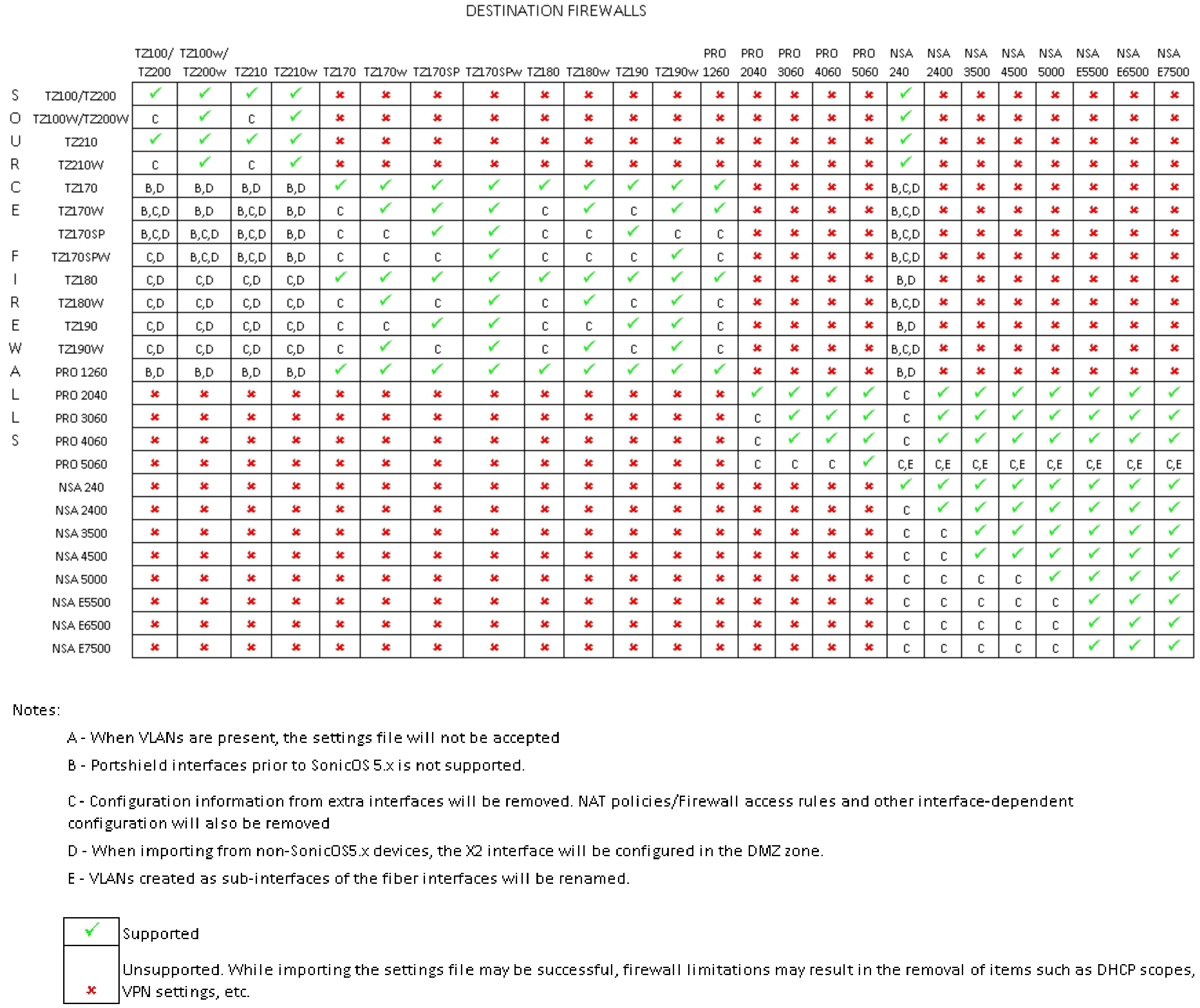
6. Review the source SonicOS Standard Settings Summary page.

   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	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 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.

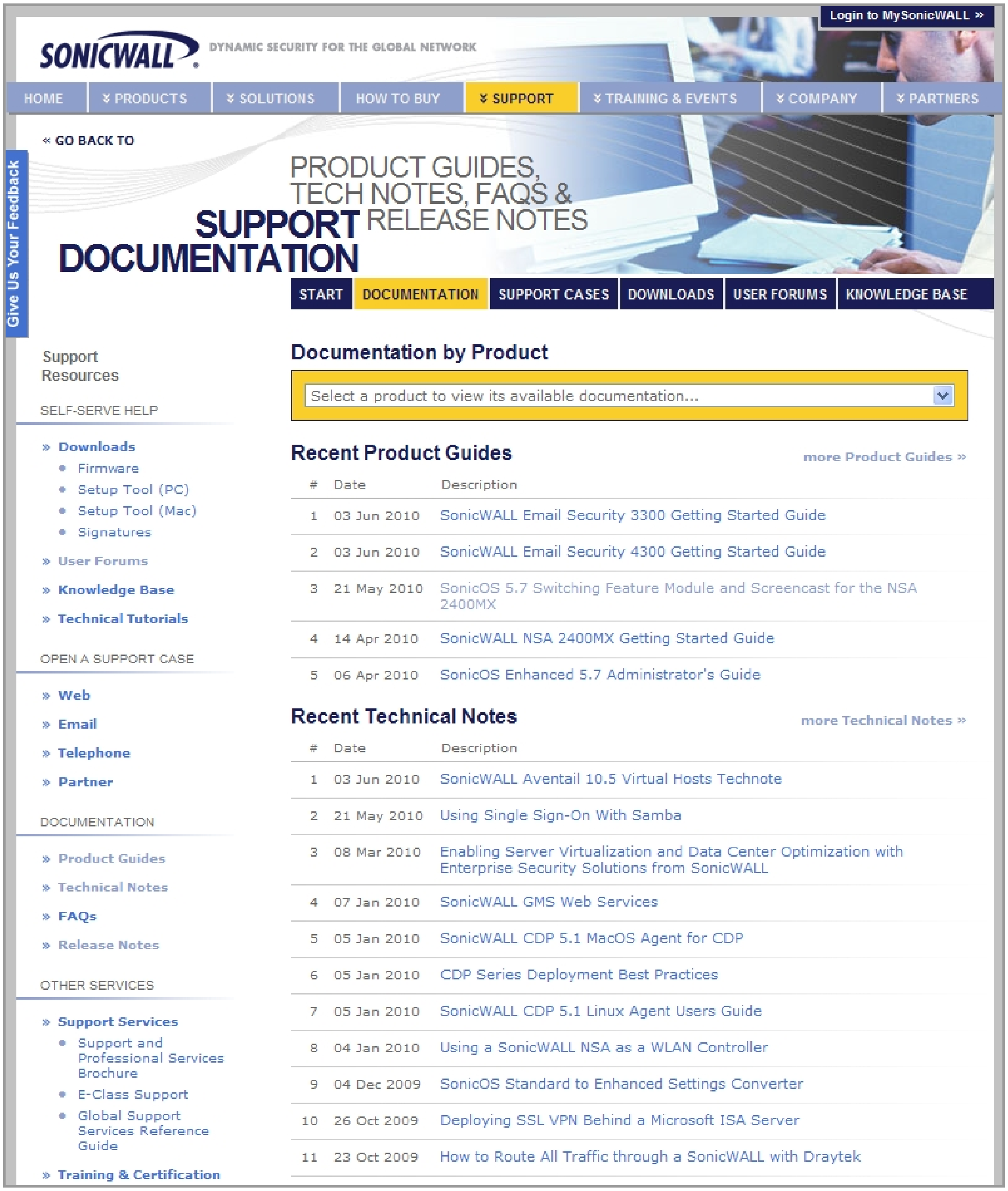
   The **Test** light starts blinking when the SonicWALL security appliance has rebooted into SafeMode.

   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 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.



Documentation by Product

Select a product to view its available documentation...

Recent Product Guides

more Product Guides »

#	Date	Description
1	03 Jun 2010	SonicWALL Email Security 3300 Getting Started Guide
2	03 Jun 2010	SonicWALL Email Security 4300 Getting Started Guide
3	21 May 2010	SonicOS 5.7 Switching Feature Module and Screencast for the NSA 2400MX
4	14 Apr 2010	SonicWALL NSA 2400MX Getting Started Guide
5	06 Apr 2010	SonicOS Enhanced 5.7 Administrator's Guide

Recent Technical Notes

more Technical Notes »

#	Date	Description
1	03 Jun 2010	SonicWALL Aventail 10.5 Virtual Hosts Technote
2	21 May 2010	Using Single Sign-On With Samba
3	08 Mar 2010	Enabling Server Virtualization and Data Center Optimization with Enterprise Security Solutions from SonicWALL
4	07 Jan 2010	SonicWALL GMS Web Services
5	05 Jan 2010	SonicWALL CDP 5.1 MacOS Agent for CDP
6	05 Jan 2010	CDP Series Deployment Best Practices
7	05 Jan 2010	SonicWALL CDP 5.1 Linux Agent Users Guide
8	04 Jan 2010	Using a SonicWALL NSA as a WLAN Controller
9	04 Dec 2009	SonicOS Standard to Enhanced Settings Converter
10	26 Oct 2009	Deploying SSL VPN Behind a Microsoft ISA Server
11	23 Oct 2009	How to Route All Traffic through a SonicWALL with Draytek

Last updated: 7/16/2010