SonicWall™ SonicOS 5.9

Upgrade Guide

April 2017

This *Upgrade Guide* provides instructions for upgrading your SonicWall™ network security appliance to SonicOS 5.9 from a previous release.

ⓘ **NOTE:** On SonicWall TZ series and some smaller NSA series platforms such as the NSA 220, performance may be affected after upgrading to SonicOS 5.9.1.8. This is due to the large number of features, enhancements, and vulnerability fixes provided in SonicOS 5.9, as compared to the SonicOS 5.8 releases. These features and updates are essential to better secure your network.

This guide also provides information about importing the configuration settings from an appliance running SonicOS 5.8 or 5.9 to a different appliance. See Importing Configuration Settings for details about the platforms and firmware versions supported.

Topics:

- Obtaining the Latest SonicOS Firmware
- Creating a System Backup and Exporting Your Settings
- Upgrading Firmware with Current Settings
- Upgrading Firmware with Factory Default Settings
- Upgrading Caveats for VPN Tunnel Interfaces
- Using SafeMode to Upgrade Firmware
- Importing Configuration Settings
- SonicWall Support

Obtaining the Latest SonicOS Firmware

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

1. In a browser on your management computer, log into your MySonicWALL account at https://www.mysonicwall.com/.
2. In MySonicWALL, click **Downloads** in the left navigation pane to display the Download Center screen.
3. Select your product in the **Software Type** drop-down list to display available firmware versions.
4. To download the firmware to your computer, click the link for the firmware version you want. You can also download the *Release Notes* and other associated files in the same way.

Creating a System Backup and Exporting Your Settings

Topics:

- Creating a System Backup
- Creating Backup Settings
- Exporting Settings

Creating a System Backup

Before beginning the update process, you can use the **Create Backup** button to make a system backup on your SonicWall appliance.

On SonicWall NSA 2400 and above, and on E-Class NSA appliances, the backup feature saves a copy of the current system state, firmware, and configuration settings on your appliance, protecting all your existing settings if you need to return to a previous configuration.

ⓘ **NOTE:** The TZ series, SOHO, NSA 220 series, NSA 240, and NSA 250M series do not support a full firmware image backup.

Creating Backup Settings

On SonicWall TZ series (except TZ 100 and TZ 200 series), SOHO, NSA 220 series, NSA 240, and NSA 250M series, you can use the **Create Backup Settings** button to save a copy of the configuration settings locally on the firewall. The saved settings can be used with the current firmware version or with a newly uploaded firmware version.

ⓘ **NOTE:** The TZ 100 series and TZ 200 series do not support saving a copy of the settings directly on the unit.

Exporting Settings

On all appliance platforms, you can export the appliance configuration settings to a file on your local management station. This file serves as an external backup of the configuration settings, and can be imported into another appliance or into the same appliance if it is necessary to reboot the firmware with factory default settings.

To save a system backup on your appliance and export configuration settings to a file on your local management station:

1. To save a system backup or backup settings in the **System > Settings** page, do one of the following:
   - On an NSA 2400 or above, click **Create Backup**. SonicOS takes a snapshot of your current system state, firmware, and configuration preferences, and makes it the new System Backup firmware image. Clicking **Create Backup** overwrites the existing System Backup image, if any. The **System Backup** entry is displayed in the Firmware Management table.
   - On a TZ series, SOHO, NSA 220 series, NSA 240, or NSA 250M series, click **Create Backup Settings**. SonicOS saves a small file on the appliance with all your configuration settings. Any previous backup settings file is overwritten. The Firmware Management table displays the Current Firmware with Backup Settings entry.

ⓘ **NOTE:** A **Download** button is displayed in the Firmware Management table for System Backup. However, the downloaded file cannot be imported into an appliance, nor can it be uploaded like firmware. Use **Export Settings** to save your configuration settings for import into another appliance.

2. To export your settings to a local file, click **Export Settings.**
3. Click **Export** in the popup window that displays the name of the saved file.

Upgrading Firmware with Current Settings

You can update the SonicOS image on a SonicWall security appliance by connecting your computer to the LAN (X0) port or you can update it remotely if the LAN or WAN interface is configured for remote management access.

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 and save it to a location on your local computer.
2. Point your browser to the appliance IP address, and log in as an administrator.
3. On the **System > Settings** page, click **Upload New Firmware**.
4. Navigate to the location where you saved the SonicOS firmware image file, select the file, and click **Upload**. After the firmware finishes uploading, it is displayed in the Firmware Management table.
5. On the **System > Settings** page, click the Boot icon in the row for **Uploaded Firmware – New!**
6. In the confirmation dialog box, click **OK**. The appliance restarts and displays the login page.
7. Enter your user name and password. Your new SonicOS image version information is displayed on the **System > Status** page.

Upgrading Firmware with Factory Default Settings

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 and save it to a location on your local computer.
2. Point your browser to the appliance IP address, and log in as an administrator.
3. Navigate to the **System > Settings** page and click **Upload New Firmware**.
4. Navigate 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 – New!**
6. In the confirmation dialog box, click **OK**. The appliance restarts and then displays the options to launch the Setup Wizard or go to the login page of the SonicOS management interface.

> ⓘ **NOTE:** The IP address for the X0 (LAN) interface reverts to the default, 192.168.168.168. You can log into SonicOS by connecting to X0 and pointing your browser to https://192.168.168.168/.

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

Upgrading Caveats for VPN Tunnel Interfaces

VPN tunnel interfaces created in SonicOS 5.8 are missing on some platforms after upgrading to SonicOS 5.9. This includes tunnel interfaces with or without advanced routing (OSPF and RIP) enabled.

An unnumbered tunnel interface does not have an IP address and can be used as an egress interface when defining a static route. If enabled for advanced routing, it must *borrow* an IP address from either a physical or logical (VLAN) interface. A numbered tunnel interface has an IP address specifically assigned to it.

On platforms supporting unnumbered tunnel interfaces in SonicOS 5.9, all VPN tunnel interfaces continue to function normally after upgrading.

However, the upgrading process does not automatically convert unnumbered tunnel interfaces in SonicOS 5.8 to numbered tunnel interface configurations in SonicOS 5.9.

ⓘ **NOTE:** To work around this issue, manually reconfigure VPN tunnel interfaces and routing settings after upgrading to SonicOS 5.9.

When using advanced routing in SonicOS 5.8, borrowed interfaces do not have to be in the same subnet on both ends of the VPN tunnel. However, it is a best practice to do so. When using numbered tunnel interfaces for advanced routing in SonicOS 5.9, the subnet must be the same on both ends of the VPN tunnel. Be sure to consider this when reconfiguring tunnel interfaces after upgrading to SonicOS 5.9.

Numbered and unnumbered tunnel interface implementations are mutually exclusive in SonicOS 5.9, so if numbered tunnel interfaces are supported on a device, unnumbered tunnel interfaces are *not* supported on that device and vice versa.

Tunnel Interface Support per Platform in SonicOS 5.9

Numbered Tunnel Interface supported, No Conversion from Unnumbered Tunnel Interfaces	Unnumbered Tunnel Interfaces Supported, Advanced Routing Supported	Unnumbered Tunnel Interfaces Supported, Advanced Routing Not Supported
NSA E8510	NSA 2400MX	TZ 100/100W
NSA E8500	TZ 210/210W	
NSA E7500	TZ 205/205W	
NSA E6500	TZ 200/200W	
NSA E5500	TZ 105/105W	
NSA 5000	SOHO	
NSA 4500		
NSA 3500		
NSA 2400		
NSA 250M/250MW		
NSA 240		
NSA 220/220W		
TZ 215/215W		

ⓘ **NOTE:** When advanced routing is configured and OSPF is enabled on an unnumbered tunnel interface, the tunnel interface maximum transmission unit (MTU) in SonicOS 5.8 is different from the MTU in SonicOS 5.9:

- SonicOS 5.8 – MTU is 1500
- SonicOS 5.9 – MTU is 1446

If you have this type of tunnel between one appliance running 5.8 and another running 5.9, the OSPF tunnel interface MTU must be adjusted or set to be ignored.

Using SafeMode to Upgrade Firmware

If you are unable to connect to the SonicOS 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.

The SafeMode procedure uses a recessed reset button in a small pinhole:

- 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 connection on the back.

To use SafeMode to upgrade firmware on a SonicWall security appliance:

1. Connect your computer to the X0 port on the appliance and configure your computer with an IP 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 security appliance for more than 20 seconds.
   - On platforms with an LCD screen and control buttons on the front bezel, you can use the LCD control buttons to set the appliance to SafeMode. 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 appliance has rebooted into SafeMode.

ⓘ **NOTE:** Holding the reset button for two seconds sends a diagnostic snapshot to the console. Holding the reset button for six to eight seconds reboots the appliance in regular mode.

3. Point the browser on your computer to 192.168.168.168. The SafeMode management interface displays.
4. Click **Upload New Firmware**.
5. Navigate to where you saved the SonicOS firmware image, select the file, and click **Upload**.
6. Click 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 Default Settings – New!**

     Use this option to restart the appliance with factory default configuration settings.
7. In the confirmation dialog box, click **OK** to proceed.
8. If you booted with current configuration settings, reconfigure your computer as needed to automatically obtain an IP address and DNS server address, or reset it to its normal static values.
9. Connect the computer to your network or leave it connected to the X0 (LAN) interface of the appliance, and point your browser to the WAN or LAN (depending on how you are connected) IP address of the SonicWall appliance.
10. If you booted with factory default settings, enter the default user name and password (admin / password) to access the SonicOS management interface. The default IP address of the X0 interface is 192.168.168.168.

Importing Configuration Settings

You can import configuration settings from one appliance to another, which can save time when replacing an older appliance with a newer model. This feature is also useful when you need multiple appliances with similar configuration settings.

Importing configuration settings, or preferences (also called *prefs*), to SonicWall network security appliances running SonicOS 5.9 is generally supported from the following SonicWall appliances:

- NSA E-Class Series
- NSA Series
- TZ 215/210/205/105 Series
- TZ 200/100/190/180/170 Series
- PRO Series

Preferences cannot be imported in the following situations:

- Settings files containing Portshield interfaces created prior to SonicOS 5.0
- 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

To export the configuration settings from an appliance:

1. Navigate to the **System > Settings** page in SonicOS.
2. Click the **Export Settings** button.
3. Import the settings file to another appliance by clicking the **Import Settings** button on that page.

Refer to the related topics and import matrices in the following sections:

- Importing Settings from SonicOS Standard to SonicOS 5.9 Enhanced
- SonicOS Versions Supporting Configuration Import
- SOHO, NSA, and TZ Legend
- SOHO Configuration Import Support
- NSA / E-Class NSA Configuration Import Support
- TZ / NSA Configuration Import Support

Importing Settings from SonicOS Standard to SonicOS 5.9 Enhanced

The SonicOS Standard to Enhanced Settings Converter is designed to convert a source Standard Network Settings file to be compatible with a target appliance running SonicOS Enhanced, such as SonicOS 5.9. 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.
2. Navigate to **System > Settings**.
3. Export your network settings to a file on your management computer.
4. On the management computer, point your browser to https://convert.global.sonicwall.com/.
5. Click the **Settings Converter** button.
6. Log in using your MySonicWall credentials and agree to the security statement.
7. Upload the source Standard Network Setting file 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.

8 Upload the source Standard Network Settings file:

   a Click **Browse**.

   b Navigate to and select the source SonicOS Standard Settings file.

   c Click **Upload**.

   d Click the right arrow to proceed.

9 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 to deploy it in a testing environment.

   a (Optional) Change the LAN IP address and subnet mask of the source appliance to that of the target appliance.

   b Click the right arrow to proceed.

10 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.

11 Complete the conversion by clicking the right arrow to proceed.

12 Optionally click the **Warnings** link to view any differences in the settings created for the target appliance.

13 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.

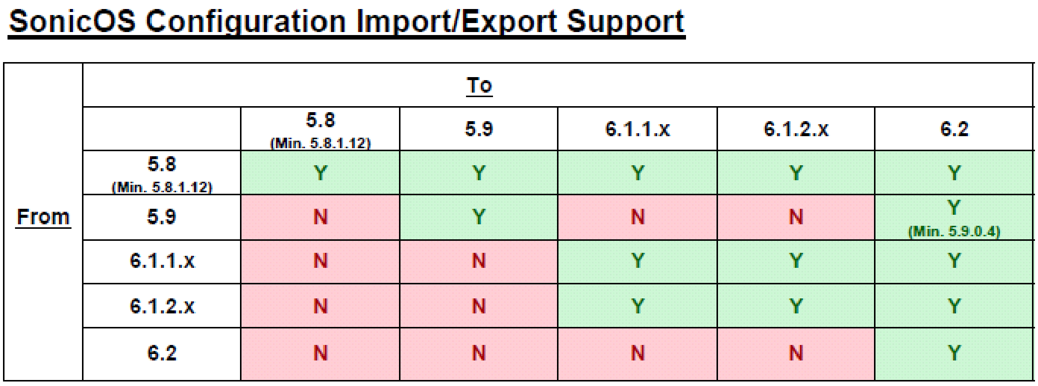
14 Log in to the management interface for your SonicWall appliance.

15 Navigate to **System > Settings**, and click the **Import Settings** button to import the converted settings to your appliance.

SonicOS Versions Supporting Configuration Import

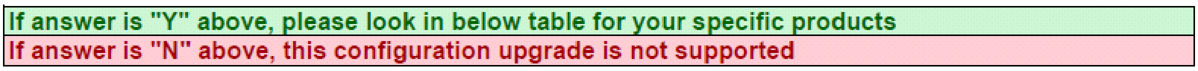
The following matrix illustrates the supported source and destination versions of SonicOS when importing configuration settings from one appliance to another. As the matrix shows, it is not supported to import configuration settings from an appliance running SonicOS 6.x to one running SonicOS 5.9.

ⓘ **NOTE:** For information about importing settings from SonicOS 5.9 to SonicOS 6.2, see the *SonicOS 6.2 Upgrade Guide*, available at https://support.sonicwall.com/technical-documents.



SonicOS Configuration Import/Export Support

		To				
		5.8 (Min. 5.8.1.12)	5.9	6.1.1.x	6.1.2.x	6.2
From	5.8 (Min. 5.8.1.12)	Y	Y	Y	Y	Y
	5.9	N	Y	N	N	Y (Min. 5.9.0.4)
	6.1.1.x	N	N	Y	Y	Y
	6.1.2.x	N	N	Y	Y	Y
	6.2	N	N	N	N	Y

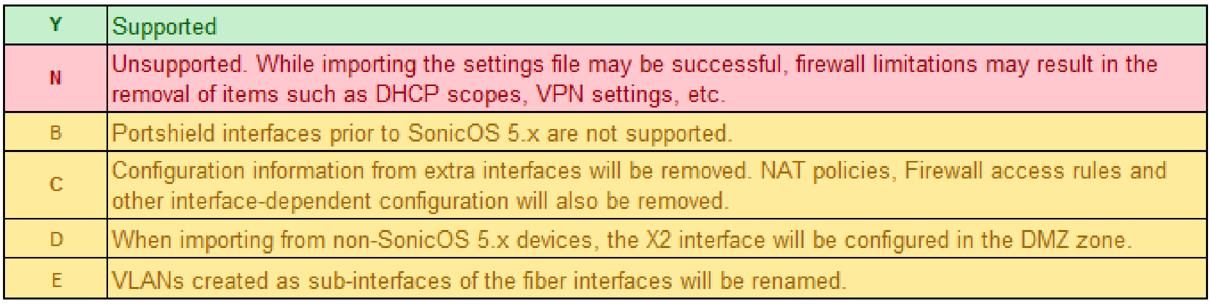


If answer is "Y" above, please look in below table for your specific products

If answer is "N" above, this configuration upgrade is not supported

SOHO, NSA, and TZ Legend

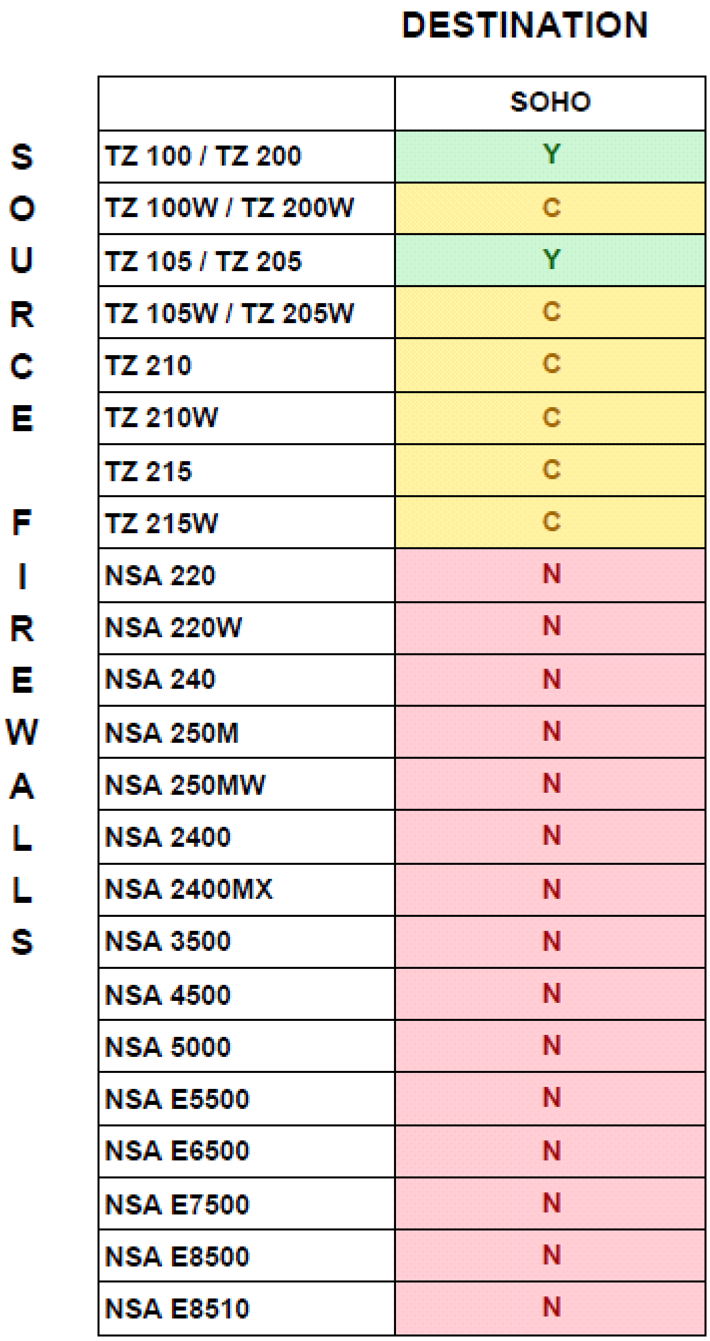
This legend defines the letter-codes used in the SOHO, NSA, and TZ configuration import tables in the following sections.



Y	Supported
N	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.
B	Portshield interfaces prior to SonicOS 5.x are 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-SonicOS 5.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.

SOHO Configuration Import Support

The following matrix shows the SonicWall firewalls whose configuration settings can be imported to SonicWall SOHO platform. The source firewalls are in the left column, and the destination firewalls are listed across the top.



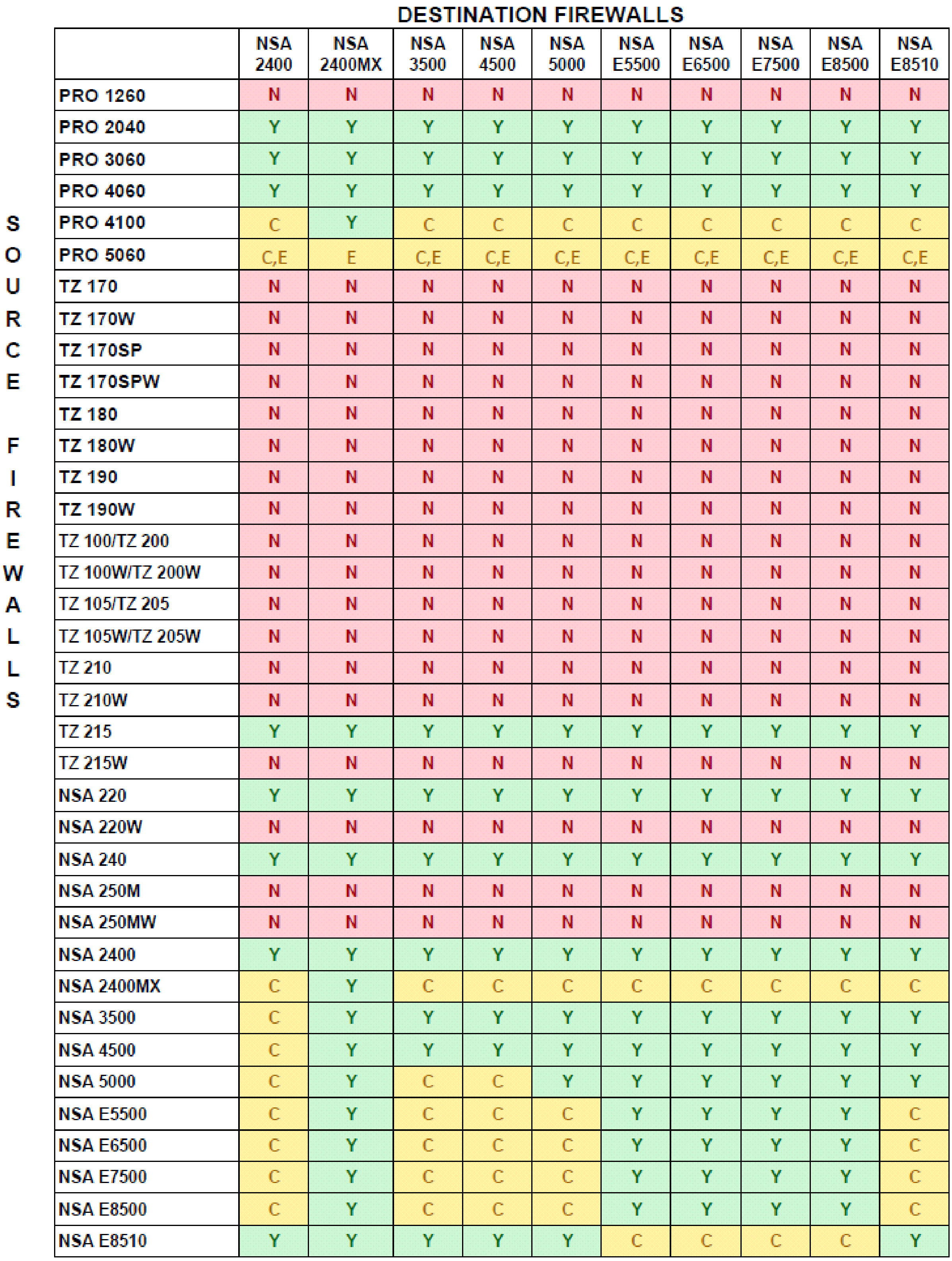
DESTINATION

SOURCE FIREWALLS

	SOHO
TZ 100 / TZ 200	Y
TZ 100W / TZ 200W	C
TZ 105 / TZ 205	Y
TZ 105W / TZ 205W	C
TZ 210	C
TZ 210W	C
TZ 215	C
TZ 215W	C
NSA 220	N
NSA 220W	N
NSA 240	N
NSA 250M	N
NSA 250MW	N
NSA 2400	N
NSA 2400MX	N
NSA 3500	N
NSA 4500	N
NSA 5000	N
NSA E5500	N
NSA E6500	N
NSA E7500	N
NSA E8500	N
NSA E8510	N

NSA / E-Class NSA Configuration Import Support

The following matrix shows the SonicWall firewalls whose configuration settings can be imported to SonicWall NSA and E-Class NSA platforms. The source firewalls are in the left column, and the destination firewalls are listed across the top.

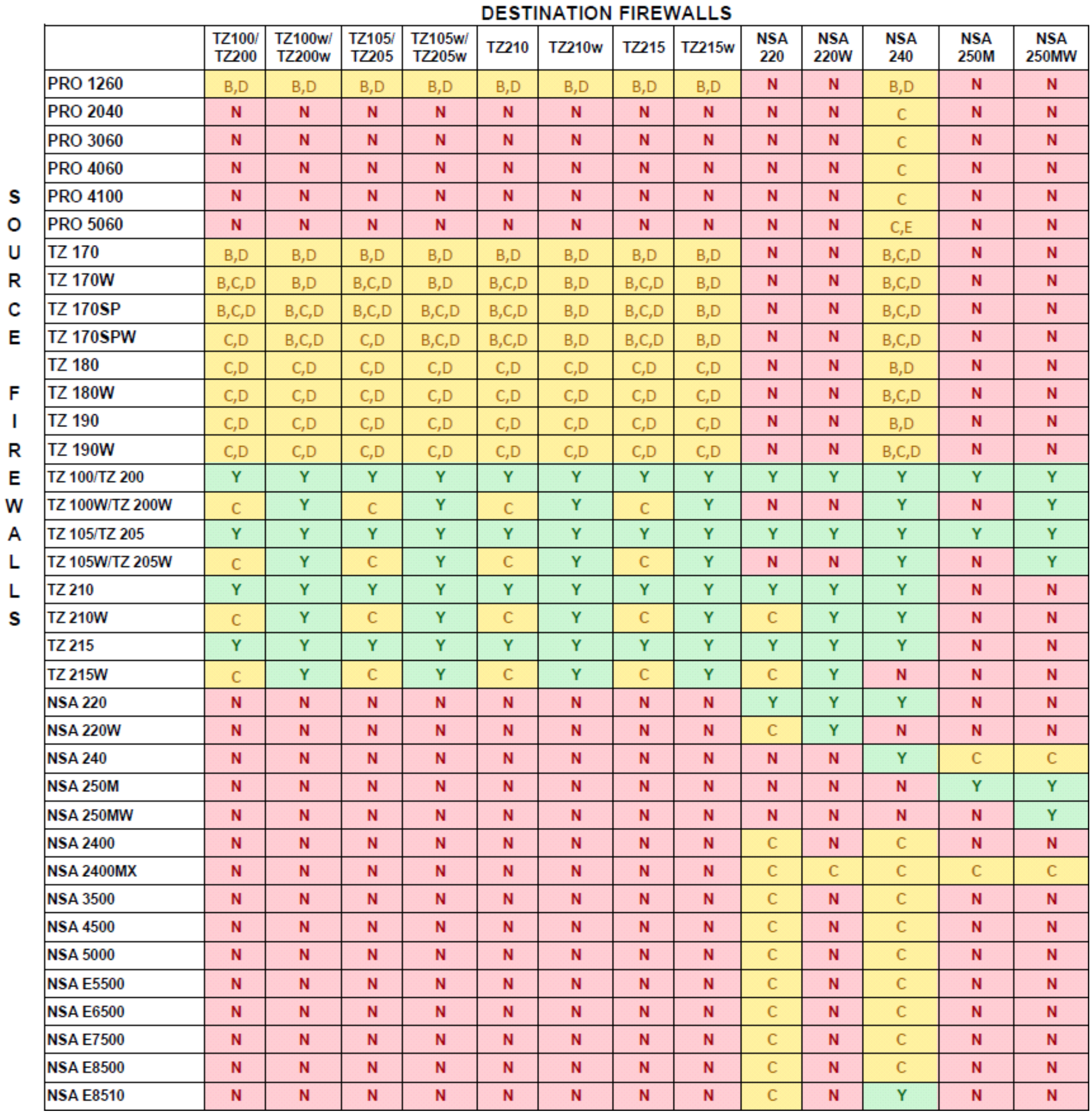


DESTINATION FIREWALLS

		NSA 2400	NSA 2400MX	NSA 3500	NSA 4500	NSA 5000	NSA E5500	NSA E6500	NSA E7500	NSA E8500	NSA E8510
SOURCE FIREWALLS	PRO 1260	N	N	N	N	N	N	N	N	N	N
	PRO 2040	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	PRO 3060	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	PRO 4060	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	PRO 4100	C	Y	C	C	C	C	C	C	C	C
	PRO 5060	C,E	E	C,E	C,E	C,E	C,E	C,E	C,E	C,E	C,E
	TZ 170	N	N	N	N	N	N	N	N	N	N
	TZ 170W	N	N	N	N	N	N	N	N	N	N
	TZ 170SP	N	N	N	N	N	N	N	N	N	N
	TZ 170SPW	N	N	N	N	N	N	N	N	N	N
	TZ 180	N	N	N	N	N	N	N	N	N	N
	TZ 180W	N	N	N	N	N	N	N	N	N	N
	TZ 190	N	N	N	N	N	N	N	N	N	N
	TZ 190W	N	N	N	N	N	N	N	N	N	N
	TZ 100/TZ 200	N	N	N	N	N	N	N	N	N	N
	TZ 100W/TZ 200W	N	N	N	N	N	N	N	N	N	N
	TZ 105/TZ 205	N	N	N	N	N	N	N	N	N	N
	TZ 105W/TZ 205W	N	N	N	N	N	N	N	N	N	N
	TZ 210	N	N	N	N	N	N	N	N	N	N
	TZ 210W	N	N	N	N	N	N	N	N	N	N
	TZ 215	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	TZ 215W	N	N	N	N	N	N	N	N	N	N
	NSA 220	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	NSA 220W	N	N	N	N	N	N	N	N	N	N
	NSA 240	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	NSA 250M	N	N	N	N	N	N	N	N	N	N
	NSA 250MW	N	N	N	N	N	N	N	N	N	N
	NSA 2400	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	NSA 2400MX	C	Y	C	C	C	C	C	C	C	C
	NSA 3500	C	Y	Y	Y	Y	Y	Y	Y	Y	Y
	NSA 4500	C	Y	Y	Y	Y	Y	Y	Y	Y	Y
	NSA 5000	C	Y	C	C	Y	Y	Y	Y	Y	Y
	NSA E5500	C	Y	C	C	C	Y	Y	Y	Y	C
	NSA E6500	C	Y	C	C	C	Y	Y	Y	Y	C
	NSA E7500	C	Y	C	C	C	Y	Y	Y	Y	C
	NSA E8500	C	Y	C	C	C	Y	Y	Y	Y	C
	NSA E8510	Y	Y	Y	Y	Y	C	C	C	C	Y

TZ / NSA Configuration Import Support

The following matrix shows the SonicWall firewalls whose configuration settings can be imported to SonicWall TZ 100/200/105/205/210/215 series and NSA 220/240/250M series platforms. The source firewalls are in the left column, and the destination firewalls are listed across the top.



DESTINATION FIREWALLS

SOURCE FIREWALLS

	TZ100/ TZ200	TZ100w/ TZ200w	TZ105/ TZ205	TZ105w/ TZ205w	TZ210	TZ210w	TZ215	TZ215w	NSA 220	NSA 220W	NSA 240	NSA 250M	NSA 250MW
PRO 1260	B,D	B,D	B,D	B,D	B,D	B,D	B,D	B,D	N	N	B,D	N	N
PRO 2040	N	N	N	N	N	N	N	N	N	N	C	N	N
PRO 3060	N	N	N	N	N	N	N	N	N	N	C	N	N
PRO 4060	N	N	N	N	N	N	N	N	N	N	C	N	N
PRO 4100	N	N	N	N	N	N	N	N	N	N	C	N	N
PRO 5060	N	N	N	N	N	N	N	N	N	N	C,E	N	N
TZ 170	B,D	B,D	B,D	B,D	B,D	B,D	B,D	B,D	N	N	B,C,D	N	N
TZ 170W	B,C,D	B,D	B,C,D	B,D	B,C,D	B,D	B,C,D	B,D	N	N	B,C,D	N	N
TZ 170SP	B,C,D	B,C,D	B,C,D	B,C,D	B,C,D	B,D	B,C,D	B,D	N	N	B,C,D	N	N
TZ 170SPW	C,D	B,C,D	C,D	B,C,D	B,C,D	B,D	B,C,D	B,D	N	N	B,C,D	N	N
TZ 180	C,D	C,D	C,D	C,D	C,D	C,D	C,D	C,D	N	N	B,D	N	N
TZ 180W	C,D	C,D	C,D	C,D	C,D	C,D	C,D	C,D	N	N	B,C,D	N	N
TZ 190	C,D	C,D	C,D	C,D	C,D	C,D	C,D	C,D	N	N	B,D	N	N
TZ 190W	C,D	C,D	C,D	C,D	C,D	C,D	C,D	C,D	N	N	B,C,D	N	N
TZ 100/TZ 200	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
TZ 100W/TZ 200W	C	Y	C	Y	C	Y	C	Y	N	N	Y	N	Y
TZ 105/TZ 205	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
TZ 105W/TZ 205W	C	Y	C	Y	C	Y	C	Y	N	N	Y	N	Y
TZ 210	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N
TZ 210W	C	Y	C	Y	C	Y	C	Y	C	Y	Y	N	N
TZ 215	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N
TZ 215W	C	Y	C	Y	C	Y	C	Y	C	Y	N	N	N
NSA 220	N	N	N	N	N	N	N	N	Y	Y	Y	N	N
NSA 220W	N	N	N	N	N	N	N	N	C	Y	N	N	N
NSA 240	N	N	N	N	N	N	N	N	N	N	Y	C	C
NSA 250M	N	N	N	N	N	N	N	N	N	N	N	Y	Y
NSA 250MW	N	N	N	N	N	N	N	N	N	N	N	N	Y
NSA 2400	N	N	N	N	N	N	N	N	C	N	C	N	N
NSA 2400MX	N	N	N	N	N	N	N	N	C	C	C	C	C
NSA 3500	N	N	N	N	N	N	N	N	C	N	C	N	N
NSA 4500	N	N	N	N	N	N	N	N	C	N	C	N	N
NSA 5000	N	N	N	N	N	N	N	N	C	N	C	N	N
NSA E5500	N	N	N	N	N	N	N	N	C	N	C	N	N
NSA E6500	N	N	N	N	N	N	N	N	C	N	C	N	N
NSA E7500	N	N	N	N	N	N	N	N	C	N	C	N	N
NSA E8500	N	N	N	N	N	N	N	N	C	N	C	N	N
NSA E8510	N	N	N	N	N	N	N	N	C	N	Y	N	N

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid support maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://support.sonicwall.com.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- Download software
- View video tutorials
- Collaborate with peers and experts in user forums
- Get licensing assistance
- Access MySonicWall
- Learn about SonicWall professional services
- Register for training and certification

To contact SonicWall Support, visit https://support.sonicwall.com/contact-support.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal/.

Legend

⚠ **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

△ **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

ⓘ **IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Last updated: 4/21/17

232-000926-01 Rev A