NSA E5500 Getting Started Guide

SonicWALL® E-CLASS

SONICWALL®

PROTECTION AT THE SPEED OF BUSINESS™

SonicWALL NSA E5500
Getting Started Guide

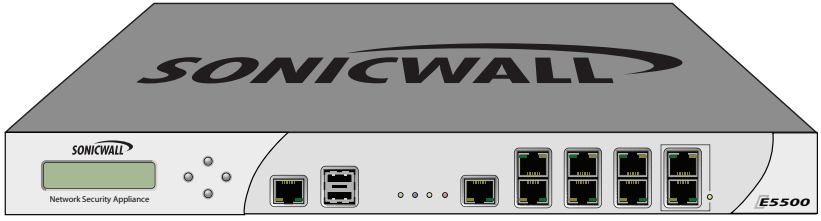
This *Getting Started Guide* provides instructions for basic installation and configuration of the SonicWALL Network Security Appliance (NSA) E5500 running SonicOS Enhanced. After you complete this guide, computers on your Local Area Network (LAN) will have secure Internet access.

Document Contents

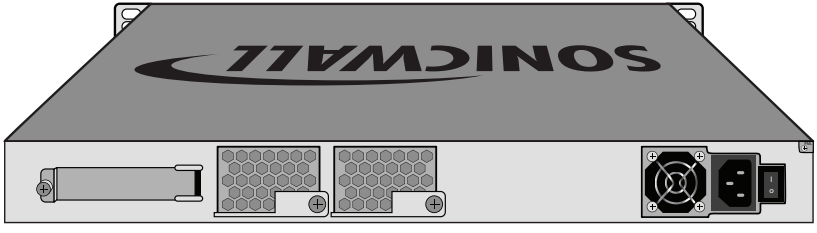
This document contains the following sections:

SonicWALL NSA E5500

Front



Back



Form Factor	1U rack-mountable
Dimensions	17 x 16.75 x 1.75 in 43.18 x 42.54 x 4.44 cm
Weight	17.30 lbs/7.9 kg
WEEE Weight	17.30 lbs/7.9 kg

Note: *Always observe proper safety and regulatory guidelines when removing administrator-serviceable parts from the SonicWALL NSA E5500. Proper guidelines can be found in the Safety and Regulatory Information section, on page 70 of this guide.*

Pre-Configuration Tasks 1

In this Section:

This section provides pre-configuration information. Review this section before setting up your SonicWALL NSA E5500.

Check Package Contents

Before setting up your SonicWALL NSA E5500, verify that your package contains the following parts:

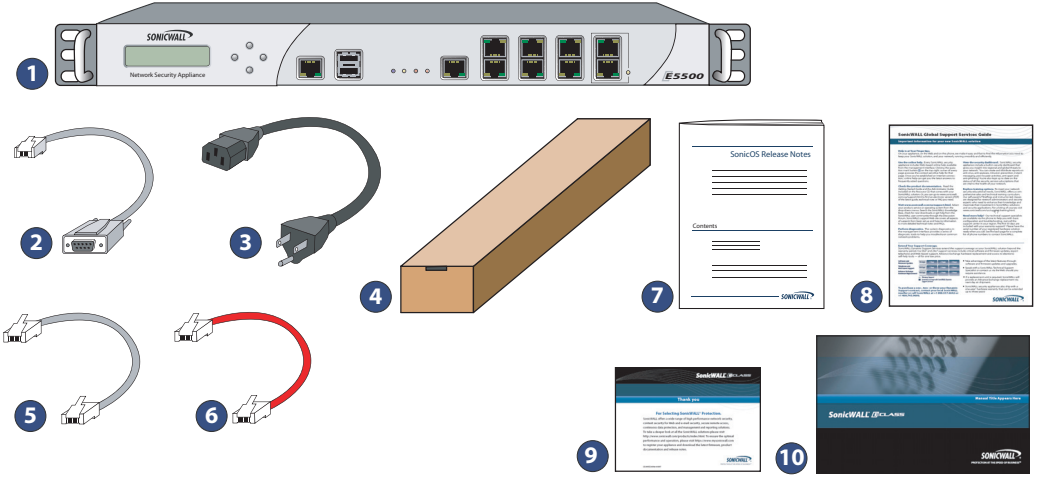
1. SonicWALL NSA E5500
2. DB9 -> RJ45 (CLI) Cable
3. Standard Power Cord*
4. Rack Kit
5. Ethernet Cable
6. Red Crossover Cable
7. Release Notes
8. Global Support Services Guide
9. Thank You Card
10. Getting Started Guide

Any Items Missing?

If any items are missing from your package, please **contact SonicWALL support**.

A listing of the most current support options is available online at: <http://www.sonicwall.com/us/support.html>

*The included power cord is intended for use in North America only. For European Union (EU) customers, a power cord is not included.



Obtain Configuration Information

Please record and keep for future reference the following setup information:

Registration Information

Serial Number:	Record the serial number found on the bottom panel of your SonicWALL appliance.
Authentication Code:	Record the authentication code found on the bottom panel of your SonicWALL appliance.

Networking Information

LAN IP Address: _____._____._____._____	Select a static IP address for your SonicWALL appliance that is within the range of your local subnet. If you are unsure, you can use the default IP address (192.168.168.168).
Subnet Mask: _____._____._____._____	Record the subnet mask for the local subnet where you are installing your SonicWALL appliance.
Ethernet WAN IP Address: _____._____._____._____	Select a static IP address for your Ethernet WAN. *This setting only applies if you are already using an ISP that assigns a static IP address.*

Administrator Information

Admin Name:	Select an administrator account name. (default is *admin)*
Admin Password:	Select an administrator password. (default is *password*)

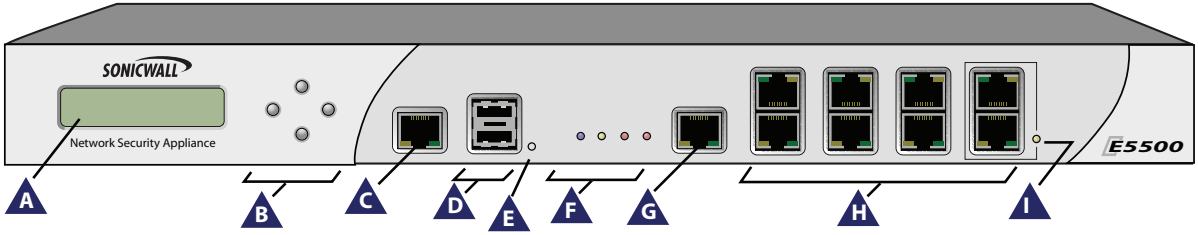
Obtain Internet Service Provider (ISP) Information

Record the following information about your current Internet service:

If You connect using	Please record
DHCP	*No information is usually required*: Some providers may require a Host name: _____
Static IP	IP Address: _____._____._____._____ Subnet Mask: _____._____._____._____ Default Gateway: _____._____._____._____ Primary DNS: _____._____._____._____ DNS 2 (optional): _____._____._____._____ DNS 3 (optional): _____._____._____._____

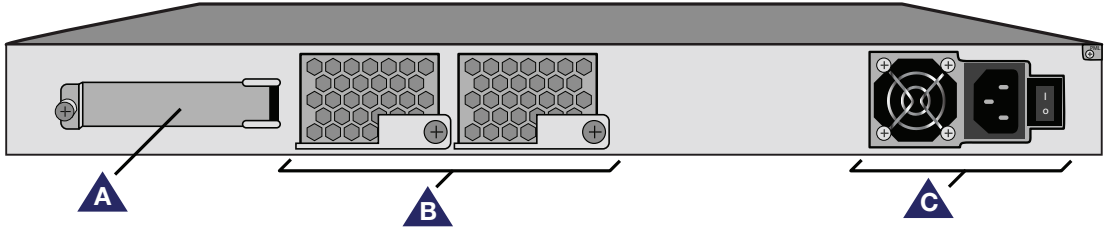
Note: *If you are not using one of the network configurations above, refer to the SonicOS Enhanced Administrator's Guide.* <http://www.sonicwall.com/us/support.html>

The Front Panel



Icon	Feature	Description
A	**LCD Screen**	Displays the front panel bezel interface which can be used to display status information, make certain configuration changes, restart the appliance or boot the appliance in SafeMode.
B	**Control Buttons**	Used to navigate the front panel bezel interface.
C	**Console Port**	Used to access the SonicOS Command Line Interface (CLI) via the DB9 -> RJ45 cable.
D	**USB Ports (2)**	Future expansion.
E	**Reset Button**	Press and hold the button for a few seconds to manually reset the appliance.
F	**LED** (from left to right)	**Power LED:** Indicates the SonicWALL NSA E5500 is powered on. **Test LED: Flickering**: Indicates the appliance is initializing. **Steady blinking**: Indicates the appliance is in SafeMode. **Solid**: Indicates that the appliance is in test mode. **Alarm LED:** Indicates an alarm condition. **HD LED:** Future extension.
G	**HA Port**	High Availability port.
H	**X0-X7 (Copper)**	Gigabit Ethernet ports.
I	**Bypass Status LED**	Future extension. Please check Release Notes for future availability.

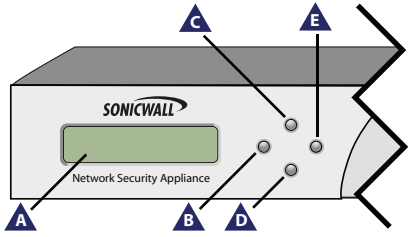
The Back Panel



Icon	Feature	Description
A	**Expansion Bay**	Future extension.
B	**Fans (2)**	The SonicWALL NSA E5500 includes two fans for system temperature control.
C	**Power Supply**	The SonicWALL NSA E5500 power supply.

Front Bezel Control Features

The SonicWALL Network Security Appliance E-Class is equipped with a front panel bezel interface that allows an administrator to customize certain aspects of the appliance or simply monitor its status without having to log into it through a separate terminal.



Icon	Feature	Description
A	**LCD Screen**	Displays the front panel bezel interface which can be used to display status information, perform basic configurations, restart the appliance or boot the appliance in SafeMode.
B C D E	**Control Buttons**	**Up**, **Down**, **Left** and **Right** buttons, used to navigate the LCD menu system.

Note: *Using the front bezel for configuration purposes prior to completing initial setup will bypass the Setup Wizard's automatic launch at startup.*

LCD Control Buttons

The LCD interface is controlled by a D-pad, consisting of four buttons: **Up**, **Down**, **Left**, **Right**. The table below describes the functions of the buttons:

Icon	Button	Navigation Features
C D	**Up/Down**	Selects options and navigates up and down lists.
B	**Left**	Cancels changes and returns to the previous menu.
E	**Right**	Confirms choices and enters menus. Also sets the appliance to screen-saver mode when used from the main menu.

Main Menu

Upon booting the LCD display will initially show the Main Menu. The menu is made up of four options:

Status >	Contains basic status values including system resources, connections and port configuration values.
Configure >	Allows configuration of basic system values including X0 (LAN) and X1 (WAN) port configuration. Requires system pin for access, default: **76642**.
Restart >	Provides the ability to restart the appliance. Requires system pin for access.
Safe Mode >	Provides the ability to restart and boot the appliance into SafeMode. Requires system pin for access.

Use the **Up** and **Down** button to select the menu you wish to enter and click the **Right** button to enter it.

Status

The Status menu allows you to view specific aspects of the appliance. Once selected, the LCD displays the Status List. This list is navigated using the **Up** and **Down** buttons. Status options available include:

- Appliance serial number
- Firmware / ROM versions
- Appliance name
- Date and Time
- Uptime
- CPU statistical readings
- Current number of connections
- Interface (X0, X1) network settings
- Interface (X0, X1) data transfer statistics

The ***X1 DNS1-3*** entries will only be displayed if they have been set from the Configure menu. If their value is still 0.0.0.0 (default value), they will not appear in the Status List.

Configure

The Configure Menu allows you to configure specific aspects of the appliance. Once selected, the LCD will display a PIN request.

Note: *The Default PIN is **76642**. This number spells SONIC on a phone keypad. The PIN number can be changed from the **System** > **Administration** page.*

All numbers are inputted using the 4 buttons. Select the individual digit field using the **Left** and **Right** button and select the desired number using the **Up** and **Down** Button. Digits increase incrementally from 0 to 9. Press the **Right** button to confirm your PIN and enter the Configuration Menu.

The appliance allows the user to navigate in and out of the Configuration Menu without having to re-enter the PIN. However, once the appliance enters Screen-Saver Mode, whether from the 6 second time out or from pressing the **Left** button from the Main Menu, the PIN number must be re-entered again to access the Configuration Menu.

After entering a new value for a setting in the configuration menu, you are asked if you want to commit changes. Using the 4-way D-pad, press the **Right** button for yes or the **Left** button for no.

If you choose yes, the screen notifies you that the settings are updated.

Configuration Options

This option allows you to configure network port settings for the appliance. Once selected, the LCD displays a list of configurable options. Status options available include:

- X0 IP and subnet
- X1 Mode
- X1 IP and subnet
- X1 Gateway
- X1 DNS settings (3 available)
- Restore defaults

The ***X1 Mode*** can be set to **Static** (default option) or to **DHCP**. If **DHCP** is selected, manual configuration options are not shown for X1 IP, subnet, gateway and DNS.

The ***Restore Defaults*** option will reset the appliance to default factory settings. If selected it will prompt for confirmation twice before restoring defaults.

If an option is selected but not modified, the appliance will display a message stating that no changes were made and will return the user to the edit value screen. If a change was made, it will prompt the user for confirmation before effecting the change.

Restart

This option allows you to safely restart without resorting to power cycling the appliance. Once selected, the LCD will display a confirmation prompt. Select **Y** for yes and press the **Right** button to confirm. The appliance will reboot.

SafeMode

This option will set the appliance to SafeMode. Once selected, the LCD will display a confirmation prompt. Select **Y** for yes and press the **Right** button to confirm. The appliance will change to SafeMode. Once SafeMode is enabled, the SonicWALL NSA E5500 must be controlled from the Web management interface.

Screen-Saver

If no button is pressed for over 60 seconds, or if the **Left** button is pressed from the Main Menu, the appliance will enter Screen-Saver mode. In this mode, the Status List will cycle, displaying every entry for a few seconds.

If the **Up** or **Down** button is pressed while in Screen-Saver mode, the appliance will display the adjacent status entry.

To exit Screen-Saver mode, press the **Right** button.

Front Bezel Configuration Example

LAN IP Configuration

The SonicWALL NSA E5500 is assigned the default LAN IP of 192.168.168.168. Complete the following steps to change it to 192.168.168.10.

1. Press **Right** to exit screen-saver mode if not at the root menu.
2. Press **Down** to select the Configuration entry.

3. Press **Right** to enter Configuration Mode.
4. Input PIN (76642 by default; SONIC on a phone keypad.)

   a. Press **Up** or **Down** until the cursor displays 7, press **Right**.
   b. Press **Up** or **Down** until the cursor displays 6, press **Right**.
   c. Press **Up** or **Down** until the cursor displays 6, press **Right**.
   d. Press **Up** or **Down** until the cursor displays 4, press **Right**.
   e. Press **Up** or **Down** until the cursor displays 2, press **Right**.

   f. Press **Right**.

5. Press **Down** until X1 IP is selected (four times).
6. Press **Right** to configure X1 IP.

7. Edit X1 IP:
   a. Press **Right** ten times to select the tenth digit.

   b. Press **UP** or **Down** until the cursor displays 0.
   c. Press **Right** once to select the next digit.
   d. Press **UP** or **Down** until the cursor displays 1.
   e. Press **Right** once to select the next digit.
   f. Press **Up** or **Down** until the cursor displays 0.

   g. Press **Right** to finish editing the X1 IP.
   h. Press **Right** again to confirm changes.

Registering Your Appliance on mysonicwall.com 2

In this Section:

This section provides instructions for registering your SonicWALL NSA E5500.

Note: *Registration is an important part of the setup process and is necessary in order to receive the benefits of SonicWALL security services, firmware updates, and technical support.*

Before You Register

You need a mysonicwall.com account to register the SonicWALL NSA E5500. You can create a new mysonicwall.com account on www.mysonicwall.com or directly from the SonicWALL management interface. This section describes how to create an account by using the Web site.

You can use mysonicwall.com to register your SonicWALL appliance and activate or purchase licenses for Security Services, ViewPoint Reporting and other services, support, or software before you even connect your device. This allows you to prepare for your deployment before making any changes to your existing network.

For a High Availability configuration, you must use mysonicwall.com to associate a backup unit that can share the Security Services licenses with your primary SonicWALL.

Note: *Your SonicWALL NSA E5500 does not need to be powered on during account creation or during the mysonicwall.com registration and licensing process.*

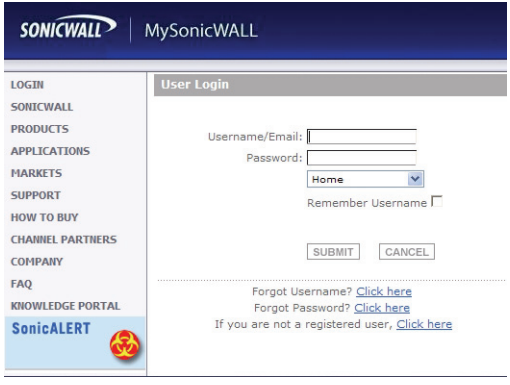
Note: *After registering a new SonicWALL appliance on mysonicwall.com, you must also register the appliance from the SonicOS management interface. This allows the unit to synchronize with the SonicWALL License Server and to share licenses with the associated appliance, if any. See* Accessing the Management Interface - *page 26*.

If you already have a mysonicwall.com account, go to Registering and Licensing Your Appliance on mysonicwall.com - page 15 to register your appliance on mysonicwall.com.

Creating a mysonicwall.com Account

To create a mysonicwall.com account, perform the following steps:

1. In your browser, navigate to www.mysonicwall.com.
2. In the login screen, click **If you are not a registered user, Click here**.



3. Complete the Registration form and then click **Register**.
4. Verify that the information is correct and then click **Submit**.
5. In the screen confirming that your account was created, click **Continue**.

Registering and Licensing Your Appliance on mysonicwall.com

This section contains the following subsections:

Product Registration

You must register your SonicWALL security appliance on mysonicwall.com to enable full functionality.

1. Login to your mysonicwall.com account.
2. On the main page, in the Register A Product field, type the appliance serial number and then click **Next**.
3. On the My Products page, under Add New Product, type the friendly name for the appliance, select the Product Group if any, type the authentication code into the appropriate text boxes, and then click **Register**.
4. On the Product Survey page, fill in the requested information and then click **Continue**.

Licensing Security Services and Software

The **Service Management - Associated Products** page in mysonicwall.com lists security services, support options, and software such as ViewPoint that you can purchase or try with a free trial. For details, click the **Info** button. Your current licenses are indicated in the **Status** column with either a license key or an expiration date. You can purchase additional services now or at a later time.

The following products and services are available for the SonicWALL NSA E5500:

- **Service Bundles:**
  - Client/Server Anti-Virus Suite
  - Comprehensive Gateway Security Suite
- **Gateway Services:**
  - Gateway AV, Anti-Spyware, Application Firewall, Intrusion Prevention Service
  - Content Filtering: Premium Edition
  - Stateful High Availability (HA) Upgrade
- **Desktop and Server Software:**
  - Enforced Client Anti-Virus and Anti-Spyware
  - Global VPN Client
  - Global VPN Client Enterprise
  - VPN Policy Upgrade (for site-to-site VPN)
  - ViewPoint
  - Global Management System
- **Support Services:**
  - Dynamic Support 24x7
  - Software and Firmware Updates
- **Consulting Services:**
  - Implementation Service
  - GMS Preventive Maintenance Service

To manage your licenses, perform the following tasks:

1. In the mysonicwall.com Service Management - Associated Products page, check the **Applicable Services** table for services that your SonicWALL appliance is already licensed for. Your initial purchase may have included security services or other software bundled with the appliance. These licenses are enabled on mysonicwall.com when the SonicWALL appliance is delivered to you.
2. If you purchased a service subscription or upgrade from a sales representative separately, you will have an **Activation Key** for the product. This key is emailed to you after online purchases, or is on the front of the certificate that was included with your purchase. Locate the product on the Services Management page and click **Enter Key** in that row.
3. In the Activate Service page, type or paste your key into the **Activation Key** field and then click **Submit**. Depending on the product, you will see an Expire date or a license key string in the **Status** column when you return to the Service Management page.
4. To license a product of service, do one of the following:
   - To try a Free Trial of a service, click **Try** in the Service Management page. A 30-day free trial is immediately activated. The Status page displays relevant information including the activation status, expiration date, number of licenses, and links to installation instructions or other documentation. The Service Management page is also updated to show the status of the free trial.
   - To purchase a product or service, click **Buy Now**.
5. In the Buy Service page, type the number of licenses you want in the **Quantity** column for either the 1 year, 2 year, or 3 year license row and then click **Add to Cart.**
6. In the **Checkout** page, follow the instructions to complete your purchase.

The mysonicwall.com server will generate a license key for the product. The key is added to the license keyset. You can use the license keyset to manually apply all active licenses to your SonicWALL appliance.

Registering a Second Appliance as a Backup

To ensure that your network stays protected if your SonicWALL appliance has an unexpected failure, you can associate a second SonicWALL with the first in a high availability (HA) pair. You can associate the two appliances as part of the registration process on mysonicwall.com. The second SonicWALL will automatically share the Security Services licenses of the primary appliance.

To register a second appliance and associate it with the primary, perform the following steps:

1. Login to your mysonicwall.com account.
2. On the main page, in the Register A Product field, type the appliance serial number and then click **Next**.
3. On the My Products page, under Add New Product, type the friendly name for the appliance, select the Product Group if any, type the authentication code into the appropriate text boxes, and then click **Register**.
4. On the Product Survey page, fill in the requested information and then click **Continue**. The Create Association Page is displayed.
5. On the Create Association Page, click the radio button to select the primary unit for this association, and then click **Continue**. The screen only displays units that are not already associated with other appliances.
6. On the Service Management - Associated Products page, scroll down to the Associated Products section to verify that your product registered successfully. You should see the HA Primary unit listed in the Parent Product section, as well as a Status value of **0** in the Associated Products / Child Product Type section.
7. Although the Stateful High Availability Upgrade and all the Security Services licenses can be shared with the HA Primary unit, you must purchase a separate ViewPoint license for the backup unit. This will ensure that you do not miss any reporting data in the event of a failover. You must also purchase a seperate support license for the backup unit. Under DESKTOP & SERVER SOFTWARE, click **Buy Now** for ViewPoint. Follow the instructions to complete the purchase.

To return to the Service Management - Associated Products page, click the serial number link for this appliance.

Registration Next Steps

Your SonicWALL NSA E5500 or E5500 HA Pair is now registered and licensed on mysonicwall.com. To complete the registration process in SonicOS and for more information, see:

- Accessing the Management Interface - page 26
- Activating Licenses in SonicOS - page 28
- Enabling Security Services in SonicOS - page 50
- Applying Security Services to Zones - page 50

Deployment Scenarios 3

In this Section:

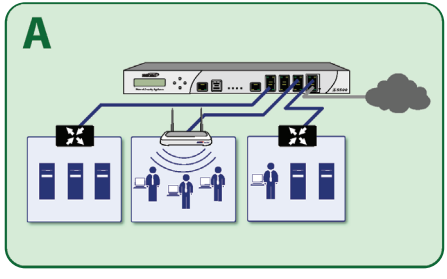
This section provides detailed overviews of advanced deployment scenarios as well as configuration instructions for connecting your SonicWALL NSA E5500.

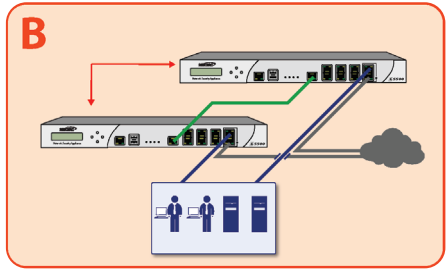
Tip: *Before completing this section, fill out the information in* Obtain Configuration Information - page 5, *and* Obtain Internet Service Provider (ISP) Information - page 5. *You will need to enter this information during the* ***Setup Wizard****.*

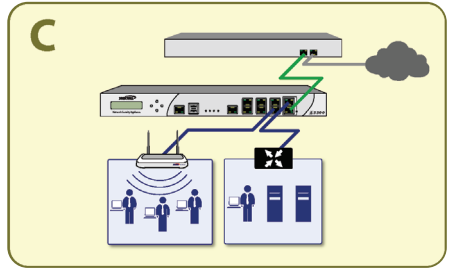
Selecting a Deployment Scenario

Before continuing, select a deployment scenario that best fits your network scheme. Reference the table below and the diagrams on the following pages for help in choosing a scenario.

Current Gateway Configuration	New Gateway Configuration	Use Scenario
No gateway appliance	Single SonicWALL NSA as a primary gateway.	**A** - NAT/Route Mode Gateway
	Pair of SonicWALL NSA appliances for high availability.	**B** - NAT with State Sync Pair
Existing Internet gateway appliance	SonicWALL NSA as replacement for an existing gateway appliance.	**A** - NAT/Route Mode Gateway
	SonicWALL NSA in addition to an existing gateway appliance.	**C** - L2 Bridge Mode
Existing SonicWALL gateway appliance	SonicWALL NSA in addition to an existing SonicWALL gateway appliance.	**B** - NAT with State Sync Pair







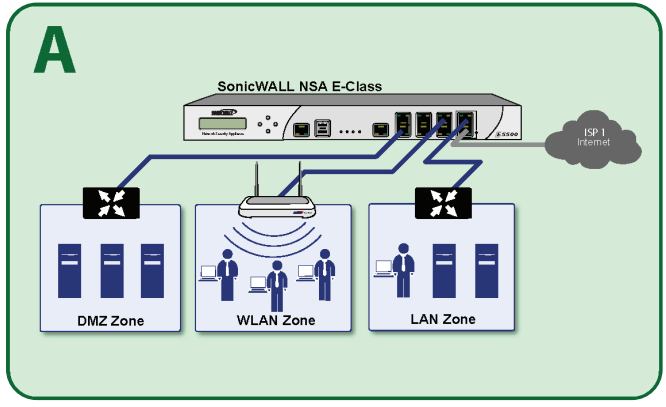
Scenario A: NAT/Route Mode Gateway - page 21
Scenario B: State Sync Pair in NAT/Route Mode - page 22
Scenario C: L2 Bridge Mode - page 23

Scenario A: NAT/Route Mode Gateway

For new network installations or installations where the SonicWALL NSA E5500 is replacing the existing network gateway.

In this scenario, the SonicWALL NSA E5500 is configured in NAT/Route mode to operate as a single network gateway. Two Internet sources may be routed through the SonicWALL appliance for load balancing and failover purposes. Because only a single SonicWALL appliance is deployed, the added benefits of high availability with a stateful synchronized pair are not available.

To set up this scenario, follow the steps covered in the *Initial Setup* section. If you have completed setup procedures in that section, continue to the *Additional Deployment Configuration* section, on page 43 to complete configuration.

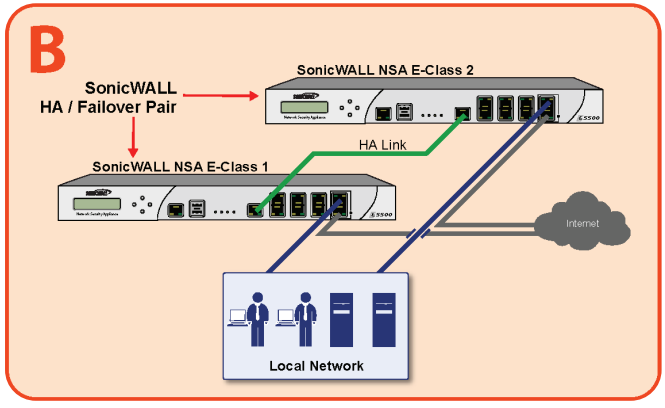


Scenario B: State Sync Pair in NAT/Route Mode

For network installations with two SonicWALL NSA E-Series appliances configured as a stateful synchronized pair for redundant high-availability networking.

In this scenario, one SonicWALL NSA E5500 operates as the primary gateway device and the other SonicWALL NSA E5500 is in passive mode. All network connection information is synchronized between the two devices so that the backup appliance can seamlessly switch to active mode without dropping any connections if the primary device loses connectivity.

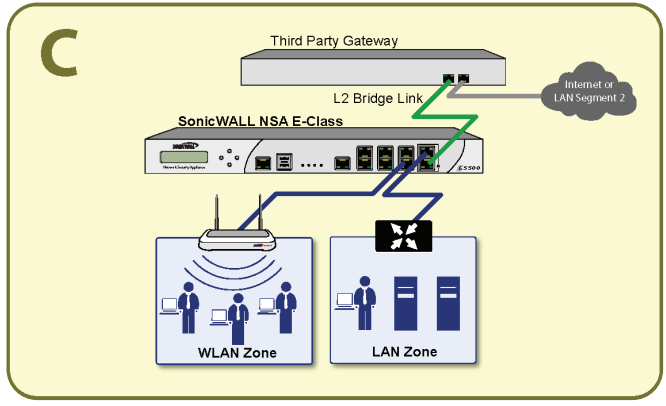
To set up this scenario, follow the steps covered in the *Initial Setup* and the Configuring a State Sync Pair in NAT/Route Mode - page 32 sections. If you have completed setup procedures in those sections, continue to the *Additional Deployment Configuration* section, on page 43 to complete configuration.



Scenario C: L2 Bridge Mode

For network installations where the SonicWALL NSA E5500 is running in tandem with an existing network gateway.

In this scenario, the original gateway is maintained. The SonicWALL NSA E5500 is integrated seamlessly into the existing network, providing the benefits of deep packet inspection and comprehensive security services on all network traffic.



L2 Bridge Mode employs a secure learning bridge architecture, enabling it to pass and inspect traffic types that cannot be handled by many other methods of transparent security appliance integration. Using L2 Bridge Mode, a SonicWALL security appliance can be non-disruptively added to any Ethernet network to provide in-line deep-packet inspection for all traversing IPv4 TCP and UDP traffic. L2 Bridge Mode can pass all traffic types, including IEEE 802.1q VLANs, Spanning Tree Protocol, multicast, broadcast and IPv6.

To set up this scenario, follow the steps covered in the *Initial Setup* and the *Configuring L2 Bridge Mode* sections. If you have completed setup procedures in those sections, continue to the *Additional Deployment Configuration* section, on page 43 to complete configuration.

Initial Setup

This section provides initial configuration instructions for connecting your SonicWALL NSA E5500. Follow these steps if you are setting up **scenario A**, **B**, or **C**.

This section contains the following sub-sections:

System Requirements

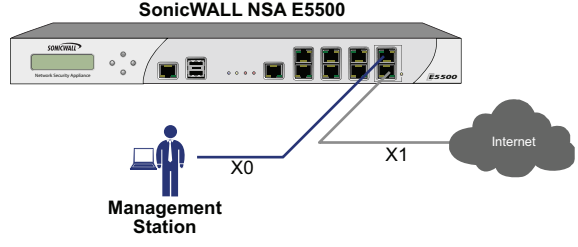
Before you begin the setup process, check to verify that you have:

- An Internet connection
- A Web browser supporting Java Script and HTTP uploads

	Accepted Browser	Browser Version Number
	Internet Explorer	6.0 or higher
	Firefox	2.0 or higher
	Netscape	9.0 or higher
	Opera	9.10 or higher for Windows
	Safari	2.0 or higher for MacOS

Connecting the WAN Port

1. Connect one end of an Ethernet cable to your Internet connection.
2. Connect the other end of the cable to the **X1** (**WAN**) port on your SonicWALL NSA E5500.



Connecting the LAN Port

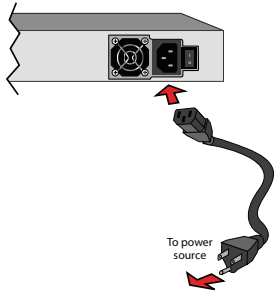
1. Connect one end of the provided ethernet cable to the computer you are using to manage the SonicWALL NSA E5500.
2. Connect the other end of the cable to the **X0** port on your SonicWALL NSA E5500.

   The Link LED above the **X0** (**LAN**) port will light up in green or amber depending on the link throughput speed, indicating an active connection:

   - Amber indicates 1 Gbps
   - Green indicates 100 Mbps
   - Unlit while the right (activity) LED is illuminated indicates 10 Mbps

Applying Power

1. Plug the power cord into an appropriate power outlet.
2. Turn on the power switch on the rear of the appliance next to the power cords.



The Power LEDs on the front panel light up blue when you plug in the SonicWALL NSA E5500. The Alarm LED may light up and the Test LED will light up and may blink while the appliance performs a series of diagnostic tests.

When the Power LEDs are lit and the Test LED is no longer lit, the SonicWALL NSA E5500 is ready for configuration. This typically occurs within a few minutes of applying power to the appliance.

Alert: *When disconnecting power, be sure to remove both power cords from the unit.*

Note: *If the Test or Alarm LEDs remain lit after the SonicWALL NSA E5500 has booted, restart the appliance by cycling power.*

Accessing the Management Interface

The computer you use to manage the SonicWALL NSA E5500 must be set up to accept a dynamic IP address, or have an unused IP address on the 192.168.168.x/24 subnet, such as 192.168.168.20.

To access the SonicOS Enhanced Web-based management interface:

1. Start your Web browser.

Note: *Disable pop-up blocking software or add the management IP address http://192.168.168.168 to your pop-up blocker's allow list.*

2. Enter **http://192.168.168.168** (the default LAN management IP address) in the **Location** or **Address** field.
3. The **SonicWALL Setup Wizard** launches and guides you through the configuration and setup of your SonicWALL NSA E5500.

   The **Setup Wizard** launches upon initial loading of the SonicWALL NSA E5500 management interface.
4. Follow the on-screen prompts to complete the Setup Wizard.

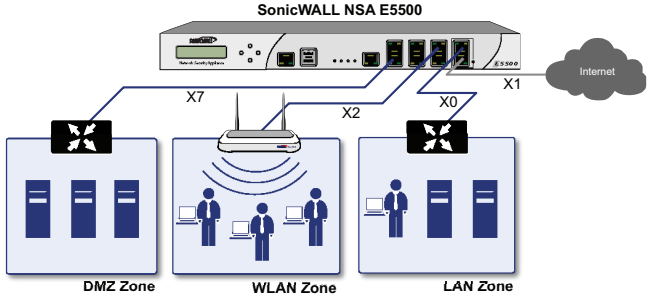
Depending on the changes made during your setup configuration, the SonicWALL may restart.

Using the Setup Wizard

If you cannot connect to the SonicWALL NSA E5500 or the **Setup Wizard** does not display, verify the following configurations:

- Did you correctly enter the SonicWALL NSA E5500 management IP address in your Web browser?
- Are the Local Area Connection settings on your computer set to use DHCP or set to a static IP address on the 192.168.168.x/24 subnet?
- Do you have the Ethernet cable connected to your computer and to the **X0** (**LAN**) port on your SonicWALL?
- Is the connector clip on your network cable properly seated in the port of the security appliance?
- Some browsers may not launch the **Setup Wizard** automatically. In this case:
  - Log into SonicWALL NSA E5500 using "**admin**" as the user name and "**password**" as the password.
  - Click the **Wizards** button on the **System** > **Status** page.
  - Select **Setup Wizard** and click **Next** to launch the Setup Wizard.
  - Some pop-up blockers may prevent the launch of the Setup Wizard. You can temporarily disable your pop-up blocker, or add the management IP address of your SonicWALL (192.168.168.168 by default) to your pop-up blocker's allow list.

Connecting to Your Network



The SonicWALL NSA E5500 ships with the internal DHCP server active on the LAN port. However, if a DHCP server is already active on your LAN, the SonicWALL will disable its own DHCP server to prevent conflicts.

As shown in the illustration on this page, ports X1 and X0 are preconfigured as WAN and LAN respectively. The remaining ports (X2-X7) can be configured to meet the needs of your network. In the graphical example on this page, the zones are: X1: WAN, X0: LAN, X2: WLAN, X7: DMZ.

Refer to the *SonicOS Enhanced Administrator's Guide* for advanced configuration deployments.

Testing Your Connection

1. After you exit the Setup Wizard, the login page reappears. Log back into the Management Interface and verify your IP and WAN connection.
2. Ping a site outside of your local network, such as <http://www.sonicwall.com>.
3. Open another Web browser and navigate to: <http://www.sonicwall.com>.

   If you can view the SonicWALL home page, you have configured your SonicWALL NSA E5500 correctly.

   If you cannot view the SonicWALL home page, renew your management station DHCP address.
4. If you still cannot view a Web page, try one of these solutions:
   - **Restart your Management Station** to accept new network settings from the DHCP server in the SonicWALL security appliance.
   - **Restart your Internet Router** to communicate with the DHCP Client in the SonicWALL security appliance.

Activating Licenses in SonicOS

After completing the registration process in SonicOS, you must perform the following tasks to activate your licenses and enable your licensed services from within the SonicOS user interface:

- Activate licenses
- Enable security services
- Apply services to network zones

This section describes how to activate your licenses. For instructions on how to enable security services and apply services to network zones, see the following sections:

- Enabling Security Services in SonicOS - page 50
- Applying Security Services to Zones - page 50

To activate licensed services in SonicOS, you can enter the license keyset manually, or you can synchronize all licenses at once with mysonicwall.com.

The Setup Wizard automatically synchronizes all licenses with mysonicwall.com if the appliance has Internet access during initial setup. If initial setup is already complete, you can synchronize licenses from the **System** > **Licenses** page.

Manual upgrade using the license keyset is useful when your appliance is not connected to the Internet. The license keyset includes all license keys for services or software enabled on mysonicwall.com. It is available on mysonicwall.com at the top of the Service Management page for your SonicWALL appliance.

To activate licenses in SonicOS:

1. Navigate to the **System** > **Licenses** page.
2. Under Manage Security Services Online do one of the following:
   - Enter your mysonicwall.com credentials, then click the **Synchronize** button to synchronize licenses with mysonicwall.com.
   - Paste the license keyset into the **Manual Upgrade Keyset** field.
3. Click **Submit**.

Upgrading Firmware on Your SonicWALL

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

Obtaining the Latest Firmware

1. To obtain a new SonicOS Enhanced firmware image file for your SonicWALL security appliance, connect to your mysonicwall.com account at <http://www.mysonicwall.com>.
2. Copy the new SonicOS Enhanced image file to a convenient location on your management station.

Saving a Backup Copy of Your Preferences

Before beginning the update process, make a system backup of your SonicWALL security appliance configuration settings. The backup feature saves a copy of the 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 state 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 procedures 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 the Firmware with Current Settings

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

Tip: *The appliance must be properly registered before it can be upgraded. Refer to* Registering and Licensing Your Appliance on mysonicwall.com - page 15 *for more information.*

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 the **Upload** button.
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.

Upgrading the Firmware 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 the **Upload** button.
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 recover quickly 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. To configure the appliance in SafeMode, perform one of the following:
   - 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 one second. 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 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.

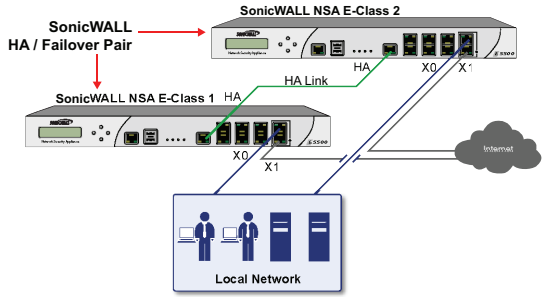
   The Test light starts blinking when the SonicWALL security appliance has rebooted into SafeMode.
3. Point the Web browser on your computer to **192.168.168.168**. The SafeMode management interface displays.
4. If you have made any configuration changes to the security appliance, select the **Create Backup 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 the **Upload** button.
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.

If You Are Following Scenario...	Proceed to Section:
A - NAT/Route Mode Gateway	Additional Deployment Configuration - page 43
B - NAT with State Sync Pair	Configuring a State Sync Pair in NAT/Route Mode - page 32
C - L2 Bridge Mode	Configuring L2 Bridge Mode - page 40

Configuring a State Sync Pair in NAT/Route Mode

This section provides instructions for configuring a pair of SonicWALL NSA E5500 appliances for high availability (HA). This section is relevant to administrators following deployment **scenario B**.

This section contains the following sub-sections:



Initial High Availability Setup

Before you begin the configuration of HA on the Primary SonicWALL security appliance, perform the following setup:

- On the bottom panel of the Backup SonicWALL security appliance, locate the serial number and write the number down. You need to enter this number in the **High Availability** > **Settings** page.
- Verify that the Primary SonicWALL and Backup SonicWALL security appliances are registered, running the same SonicOS Enhanced versions.
- Make sure the Primary SonicWALL and Backup SonicWALL security appliances' LAN, WAN and other interfaces are properly configured for failover.

- Connect the HA ports on the Primary SonicWALL and Backup SonicWALL appliances with a CAT6-rated crossover cable (red crossover cable). The Primary and Backup SonicWALL security appliances must have a dedicated connection using the HA interface. SonicWALL recommends cross-connecting the two together using a CAT 6 crossover Ethernet cable, but a connection using a dedicated 100Mbps hub/switch is also valid.
- Power up the Primary SonicWALL security appliance, and then power up the Backup SonicWALL security appliance.
- Do not make any configuration changes to the Primary's HA interface; the High Availability configuration in an upcoming step takes care of this issue. When done, disconnect the workstation.

Configuring High Availability

The first task in setting up HA after initial setup is configuring the **High Availability** > **Settings** page on the Primary SonicWALL security appliance. Once you configure HA on the Primary SonicWALL security appliance, it communicates the settings to the Backup SonicWALL security appliance.

To configure HA on the Primary SonicWALL, perform the following steps:

1. Navigate to the **High Availability** > **Settings** page.
2. Select the **Enable High Availability** checkbox.
3. Under **SonicWALL Address Settings**, type in the serial number for the Backup SonicWALL appliance.

You can find the serial number on the back of the SonicWALL security appliance, or in the **System** > **Status** screen of the backup unit. The serial number for the Primary SonicWALL is automatically populated.

4. Click **Apply** to retain these settings.

Configuring Advanced HA Settings

1. Navigate to the **High Availability** > **Advanced** page.
2. To configure Stateful HA, select **Enable Stateful Synchronization**. A dialog box is displayed with recommended settings for the **Heartbeat Interval** and **Probe Interval** fields. The settings it shows are minimum recommended values. Lower values may cause unnecessary failovers, especially when the SonicWALL is under a heavy load. You can use higher values if your SonicWALL handles a lot of network traffic. Click **OK**.
3. To backup the firmware and settings when you upgrade the firmware version, select **Generate/Overwrite Backup Firmware and Settings When Upgrading Firmware**.
4. Select the **Enable Virtual MAC** checkbox. Virtual MAC allows the Primary and Backup appliances to share a single MAC address. This greatly simplifies the process of updating network ARP tables and caches when a failover occurs. Only the WAN switch that the two appliances are connected to needs to be notified. All outside devices will continue to route to the single shared MAC address.
5. Optionally adjust the **Heartbeat Interval** to control how often the two units communicate. The default is 5000 milliseconds; the minimum recommended value is 1000 milliseconds. Less than this may cause unnecessary failovers, especially when the SonicWALL is under a heavy load.

6. Set the **Probe Level** for the interval in seconds between communication with upstream or downstream systems. SonicWALL recommends that you set the interval for at least 5 seconds. You can set the Probe IP Address(es) on the **High Availability** > **Monitoring** screen.
7. Typically, SonicWALL recommends leaving the **Failover Trigger Level (missed heart beats)**, **Election Delay Time (seconds)**, and **Dynamic Route Hold-Down Time** fields to their default settings. These fields can be tuned later as necessary for your specific network environment.
   - The **Failover Trigger Level** sets the number of heartbeats that can be missed before failing over.
   - The **Election Delay Time** is the number of seconds allowed for internal processing between the two units in the HA pair before one of them takes the primary role.
   - The **Dynamic Route Hold-Down Time** setting is used when a failover occurs on a HA pair that is using either RIP or OSPF dynamic routing. When a failover occurs, **Dynamic Route Hold-Down Time** is the number of seconds the newly-active appliance keeps the dynamic routes it had previously learned in its route table. During this time, the newly-active appliance relearns the dynamic routes in the network. When the **Dynamic Route Hold-Down Time** duration expires, it deletes the old routes and implements the new routes it has learned from RIP or OSPF. The default value is 45 seconds. In large or complex networks, a larger value may improve network stability during a failover.
8. Click the **Include Certificates/Keys** checkbox to have the appliances synchronize all certificates and keys.
9. Click **Synchronize Settings** to synchronize the settings between the Primary and Backup appliances.
10. Click **Synchronize Firmware** if you previously uploaded new firmware to your Primary unit while the Secondary unit was offline, and it is now online and ready to upgrade to the new firmware. **Synchronize Firmware** is typically used after taking your Secondary appliance offline while you test a new firmware version on the Primary unit before upgrading both units to it.
11. Click **Apply** to retain the settings on this screen.

Synchronize Settings

Once you have configured the HA setting on the Primary SonicWALL security appliance, click the **Synchronize Settings** button. You should see a **HA Peer Firewall has been updated** message at the bottom of the management interface page. Also note that the management interface displays **Logged Into: Primary SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

By default, the **Include Certificate/Keys** setting is enabled. This specifies that Certificates, CRLs and associated settings (such as CRL auto-import URLs and OCSP settings) are synchronized between the Primary and Backup units. When Local Certificates are copied to the Backup unit, the associated Private Keys are also copied. Because the connection between the Primary and Backup units is typically protected, this is generally not a security concern.

Tip: *A compromise between the convenience of synchronizing Certificates and the added security of not synchronizing Certificates is to temporarily enable the **Include Certificate/Keys** setting and manually synchronize the settings, and then disable **Include Certificate/Keys**.*

To verify that Primary and Backup SonicWALL security appliances are functioning correctly, wait a few minutes, then power off the Primary SonicWALL device. The Backup SonicWALL security appliance should quickly take over.

From your management workstation, test connectivity through the Backup SonicWALL by accessing a site on the public Internet – note that the Backup SonicWALL, when active, assumes the complete identity of the Primary, including its IP addresses and Ethernet MAC addresses.

Log into the Backup SonicWALL's unique LAN IP address. The management interface should now display **Logged Into: Backup SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

Now, power the Primary SonicWALL back on, wait a few minutes, then log back into the management interface. If stateful synchronization is enabled (automatically disabling preempt mode), the management GUI should still display **Logged Into: Backup SonicWALL Status: (green ball) Active** in the upper-right-hand corner.

If you are using the Monitor Interfaces feature, experiment with disconnecting each monitored link to ensure correct configuration.

Adjusting High Availability Settings

On the **High Availability** > **Settings** page, there are four user-configurable timers that can be adjusted to suit your network's needs:

- **Heartbeat Interval (seconds)** – This timer is the length of time between status checks. By default this timer is set to 5 seconds; using a longer interval will result in the SonicWALL taking more time to detect when/if failures have occurred.
- **Failover Trigger Level (missed heart beats)** – This timer is the number of heartbeats the SonicWALL will miss before failing over. By default, this time is set to 5 missed heart beats.This timer is linked to the Heartbeat Interval timer – for example, if you set the Heartbeat Interval to 10 seconds, and the Failover Trigger Level timer to 5, it will be 50 seconds before the SonicWALL fails over.
- **Probe Interval** – This timer controls the path monitoring speed. Path monitoring sends pings to specified IP addresses to monitor that the network critical path is still reachable. The default is 20 seconds, and the allowed range is from 5 to 255 seconds.
- **Election Delay Time** – This timer can be used to specify an amount of time the SonicWALL will wait to consider an interface up and stable, and is useful when dealing with switch ports that have a spanning-tree delay set.

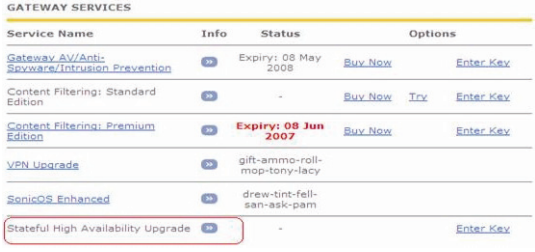
Synchronizing Firmware

Checking the **Synchronize Firmware Upload and Reboot** checkbox allows the Primary and Backup SonicWALL security appliances in HA mode to have firmware uploaded on both devices at once, in staggered sequence to ensure security is always maintained. During the firmware upload and reboot, you are notified via a message dialog box that the firmware is loaded on the Backup SonicWALL security appliance, and then the Primary SonicWALL security appliance. You initiate this process by clicking on the **Synchronize Firmware** button.

HA License Configuration Overview

You can configure HA license synchronization by associating two SonicWALL security appliances as HA Primary and HA Secondary on mysonicwall.com. Note that the Backup appliance of your HA pair is referred to as the HA Secondary unit on mysonicwall.com. Also note that the backup appliance must be an identical model to the primary applicancy (such as two NSA E5500 appliances).

You must purchase a single set of security services licenses for the HA Primary appliance. To use Stateful HA, you must first activate the Stateful High Availability Upgrade license for the primary unit in SonicOS. This is automatic if your appliance is connected to the Internet. See Registering and Licensing Your Appliance on mysonicwall.com - page 15.


GATEWAY SERVICES

Service Name	Info	Status	Options		
Gateway AV/Anti-Spyware/Intrusion Prevention		Expiry: 08 May 2008	Buy Now		Enter Key
Content Filtering: Standard Edition		-	Buy Now	Try	Enter Key
Content Filtering: Premium Edition		**Expiry: 08 Jun 2007**	Buy Now		Enter Key
VPN Upgrade		gift-ammo-roll-mop-tony-lacy			
SonicOS Enhanced		drew-tint-fell-san-ask-pam			
Stateful High Availability Upgrade		-			Enter Key

License synchronization is used during HA so that the Backup appliance can maintain the same level of network protection provided before the failover. To enable HA, you can use the SonicOS UI to configure your two appliances as a HA pair in Active/Idle mode.

mysonicwall.com provides several methods of associating the two appliances. You can start by registering a new appliance, and then choosing an already-registered unit to associate it with. You can associate two units that are both already registered. Or, you can select a registered unit and then add a new appliance with which to associate it.

Note: *After registering new SonicWALL appliances on mysonicwall.com, you must also register each appliance from the SonicOS management interface by clicking the registration link on the **System** > **Status** page. This allows each unit to synchronize with the SonicWALL license server and share licenses with the associated appliance.*

Associating Pre-Registered Appliances

To associate two already-registered SonicWALL security appliances so that they can use HA license synchronization, perform the following steps:

1. Login to mysonicwall.com.
2. In the left navigation bar, click **My Products**.
3. On the My Products page, under Registered Products, scroll down to find the appliance that you want to use as the parent, or primary, unit. Click the product **name** or **serial number**.
4. On the Service Management - Associated Products page, scroll down to the Associated Products section.
5. Under Associated Products, click **HA Secondary**.
6. On the My Product - Associated Products page, in the text boxes under Associate New Products, type the **serial number** and the friendly **name** of the appliance that you want to associate as the child/secondary/backup unit.
7. Select the group from the **Product Group** drop-down list. The product group setting specifies the mysonicwall users who can upgrade or modify the appliance.
8. Click **Register**.

If You Are Following Scenario...	Proceed to Section:
B - NAT with State Sync Pair	Additional Deployment Configuration - page 43

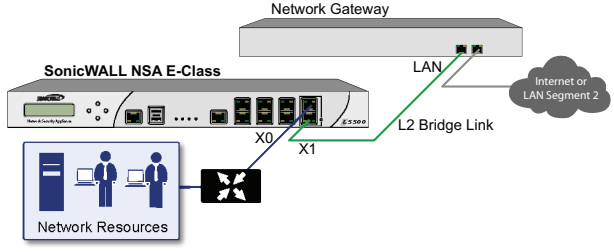
Configuring L2 Bridge Mode

This section provides instructions to configure the SonicWALL NSA E5500 appliance in tandem with an existing Internet gateway device. This section is relevant to users following deployment **scenario C**.

This section contains the following sub-sections:

Connection Overview

Connect the X1 port on your SonicWALL NSA E5500 to the LAN port on your existing Internet gateway device. Then connect the X0 port on your SonicWALL to your LAN.



Configuring the Primary Bridge Interface

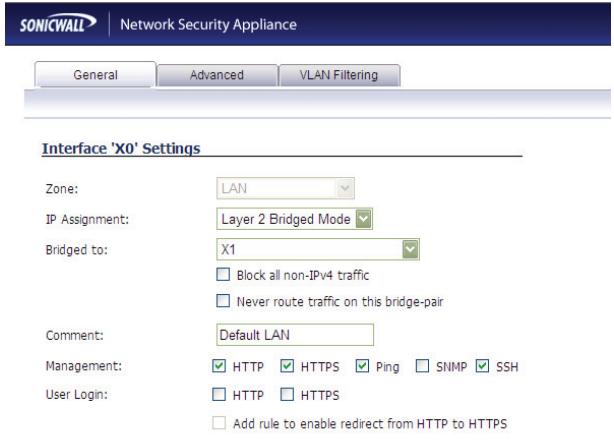
The primary bridge interface is your existing Internet gateway device. The only step involved in setting up your primary bridge interface is to ensure that the WAN interface is configured for a static IP address. You will need this static IP address when configuring the secondary bridge.

Note: *The primary bridge interface must have a static IP assignment.*

Configuring the Secondary Bridge Interface

Complete the following steps to configure the SonicWALL appliance:

1. Navigate to the **Network** > **Interfaces** page from the navigation panel.
2. Click the Configure icon in the right column of the X0 (LAN) interface.



3. In the **IP Assignment** drop-down, select **Layer 2 Bridged Mode**.
4. In the **Bridged to** drop-down, select the **X1** interface.
5. Configure management options (HTTP, HTTPS, Ping, SNMP, SSH, User logins, or HTTP redirects).

Note: *Do not enable **Never route traffic on the bridge-pair** unless your network topology requires that all packets entering the L2 Bridge remain on the L2 Bridge segments.*

*You may optionally enable the **Block all non-IPv4 traffic** setting to prevent the L2 bridge from passing non-IPv4 traffic.*

If You Are Following Scenario...	Proceed to Section:
C - L2 Bridge Mode	Additional Deployment Configuration - page 43

Additional Deployment Configuration 4

In this Section:

This section provides basic configuration information to begin building network security policies for your deployment. This section also contains several SonicOS diagnostic tools and a deployment configuration reference checklist.

An Introduction to Zones and Interfaces

Zones split a network infrastructure into logical areas, each with its own set of usage rules, security services, and policies. Most networks include multiple definitions for zones, including those for trusted, untrusted, public, encrypted, and wireless traffic.

Some basic (default) zone types include:

WAN - Untrusted resources outside your local network

LAN - Trusted local network resources

WLAN - Local wireless network resources originating from SonicWALL wireless enabled appliances such as SonicPoints.

DMZ - Local network assets that must be accessible from the WAN zone (such as Web and FTP servers)

VPN - Trusted endpoints in an otherwise untrusted zone, such as the WAN

The security features and settings configured for the zones are enforced by binding a zone to one or more physical interfaces (such as, X0, X1, or X2) on the SonicWALL UTM appliance.

The X1 and X0 interfaces are preconfigured as WAN and LAN respectively. The remaining ports can be configured to meet the needs of your network, either by using basic zone types (WAN, LAN, WLAN, DMZ, VPN) or configuring a custom zone type to fit your network requirements (for example: Gaming Console Zone, Wireless Printer Zone, Wireless Ticket Scanner Zone).

Creating Network Access Rules

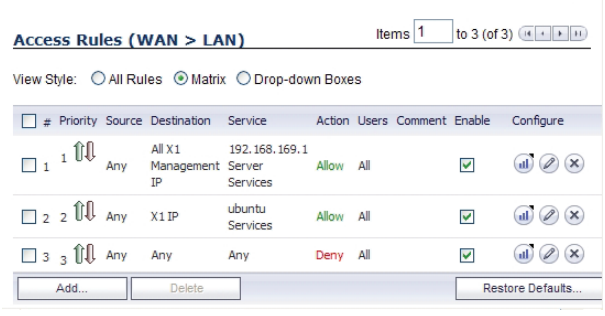
A zone is a logical grouping of one or more interfaces designed to make management, such as the definition and application of access rules, a simpler and more intuitive process than following a strict physical interface scheme.

By default, the SonicWALL security appliance's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic from the Internet to the LAN. The following behaviors are defined by the "Default" stateful inspection packet access rule enabled in the SonicWALL security appliance:

Originating Zone	Destination Zone	Action
LAN, WLAN	WAN, DMZ	Allow
DMZ	WAN	Allow
WAN	DMZ	Deny
WAN and DMZ	LAN or WLAN	Deny

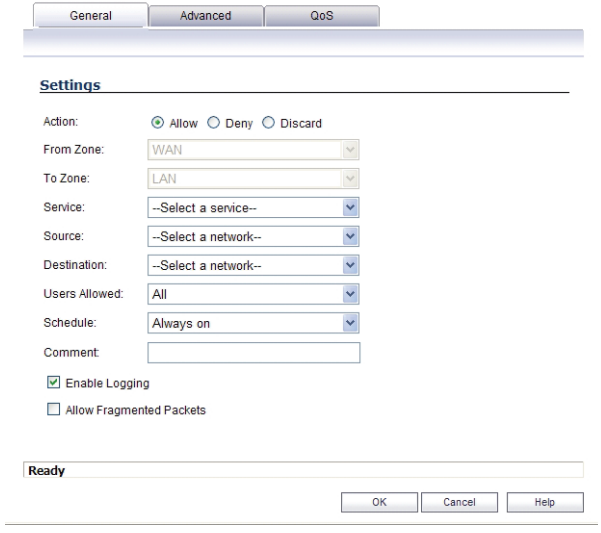
To create an access rule:

1. On the **Firewall** > **Access Rules** page in the matrix view, click the arrow connecting the two zones that need a rule.
2. On the Access Rules page, click **Add**.



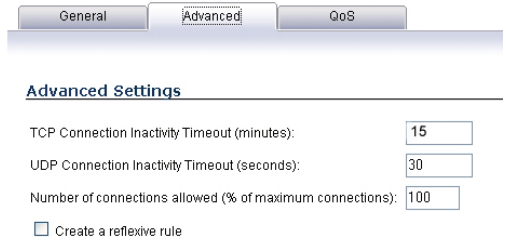
The access rules are sorted from the most specific at the top to the least specific at the bottom of the table. At the bottom of the table is the **Any** rule.

3. In the Add Rule page in the **General** tab, select **Allow** | **Deny | Discard** from the **Action** list to permit or block IP traffic.



- Select the from and to zones from the **From Zone** and **To Zone** menus.
- Select the service or group of services affected by the access rule from the **Service** list. If the service is not listed, you must define the service in the **Add Service** window. Select **Create New Service** or **Create New Group** to display the **Add Service** window or **Add Service Group** window.
- Select the source of the traffic affected by the access rule from the **Source** list. Selecting **Create New Network** displays the **Add Address Object** window.
- Select the destination of the traffic affected by the access rule from the **Destination** list. Selecting **Create New Network** displays the **Add Address Object** window.
- From the **Users Allowed** menu, add the user or user group affected by the access rule.
- Select a schedule from the **Schedule** menu. The default schedule is **Always on**.
- Enter any comments to help identify the access rule in the **Comments** field.

4. Click on the **Advanced** tab.



- If you would like for the access rule to timeout after a different period of TCP inactivity, set the amount of time, in minutes, in the **TCP Connection Inactivity Timeout (minutes)** field. The default value is **15** minutes.
- If you would like for the access rule to timeout after a different period of UDP inactivity, set the amount of time, in minutes, in the **UDP Connection Inactivity Timeout (minutes)** field. The default value is **30** minutes.
- Specify the number of connections allowed as a percent of maximum number of connections allowed by the SonicWALL security appliance in the **Number of connections allowed (% of maximum connections)** field.
- Select **Create a reflexive rule** if you want to create a matching access rule to this one in the opposite direction--from your destination zone or address object to your source zone or address object.

5. Click on the **QoS** tab if you want to apply DSCP or 802.1p Quality of Service coloring/marking to traffic governed by this rule. See the *SonicOS Enhanced Administrator's Guide* for more information on managing QoS marking in access rules.
6. Click **OK** to add the rule.

Creating a NAT Policy

The Network Address Translation (NAT) engine in SonicOS Enhanced allows users to define granular NAT policies for their incoming and outgoing traffic. By default, the SonicWALL security appliance has a preconfigured NAT policy to allow all systems connected to the **LAN** interface to perform Many-to-One NAT using the IP address of the **WAN** interface, and a policy to not perform NAT when traffic crosses between the other interfaces.

You can create multiple NAT policies on a SonicWALL running SonicOS Enhanced for the same object – for instance, you can specify that an internal server use one IP address when accessing Telnet servers, and to use a totally different IP address for all other protocols. Because the NAT engine in SonicOS Enhanced supports inbound port forwarding, it is possible to hide multiple internal servers off the WAN IP address of the SonicWALL security appliance. The more granular the NAT Policy, the more precedence it takes.

Before configuring NAT Policies, you must create all Address Objects associated with the policy. For instance, if you are creating a One-to-One NAT policy, first create Address Objects for your public and private IP addresses.

Address Objects are one of four object classes (Address, User, Service and Schedule) in SonicOS Enhanced. These Address Objects allow for entities to be defined one time, and to be re-used in multiple referential instances throughout the SonicOS interface. For example, take an internal Web server with an IP address of 67.115.118.80. Rather than repeatedly typing in the IP address when constructing Access Rules or NAT Policies, Address Objects allow you to create a single entity called "My Web Server" as a Host Address Object with an IP address of 67.115.118.80. This Address Object, "My Web Server", can then be easily and efficiently selected from a drop-down menu in any configuration screen that employs Address Objects as a defining criterion.

Since there are multiple types of network address expressions, there are currently the following Address Objects types:

- **Host –** Host Address Objects define a single host by its IP address.
- **Range –** Range Address Objects define a range of contiguous IP addresses.
- **Network –** Network Address Objects are like Range objects in that they comprise multiple hosts, but rather than being bound by specified upper and lower range delimiters, the boundaries are defined by a valid netmask.

- **MAC Address –** MAC Address Objects allow for the identification of a host by its hardware address or MAC (Media Access Control) address.
- **FQDN Address –** FQDN Address Objects allow for the identification of a host by its Fully Qualified Domain Names (FQDN), such as www.sonicwall.com.

SonicOS Enhanced provides a number of Default Address Objects that cannot be modified or deleted. You can use the Default Address Objects when creating a NAT policy, or you can create custom Address Objects to use. All Address Objects are available in the drop-down lists when creating a NAT policy.

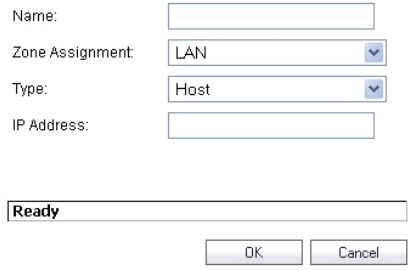
Configuring Address Objects

The **Network** > **Address Objects** page allows you to create and manage your Address Objects. You can view Address Objects in the following ways using the **View Style** menu:

- **All Address Objects** - displays all configured Address Objects.
- **Custom Address Objects** - displays Address Objects with custom properties.
- **Default Address Objects** - displays Address Objects configured by default on the SonicWALL security appliance.

To add an Address Object:

1. Navigate to the **Network** > **Address** Objects page.
2. Below the Address Objects table, click **Add**.
3. In the Add Address Object dialog box, enter a name for the Address Object in the **Name** field.



4. Select the zone to assign to the Address Object from the **Zone Assignment** drop-down list.
5. Select **Host**, **Range**, **Network**, **MAC**, or **FQDN** from the **Type** menu.
   - If you selected **Host**, enter the IP address in the **IP Address** field.
   - If you selected **Range**, enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.
   - If you selected **Network**, enter the network IP address and netmask in the **Network** and **Netmask** fields.
   - If you selected **MAC**, enter the MAC address and netmask in the **Network** and **MAC Address** field.
   - If you selected **FQDN**, enter the domain name for the individual site or range of sites (with a wildcard) in the **FQDN** field.

6. Click **OK**.

Configuring NAT Policies

NAT policies allow you the flexibility to control Network Address Translation based on matching combinations of Source IP address, Destination IP address and Destination Services. Policy-based NAT allows you to deploy different types of NAT simultaneously. The following NAT configurations are available in SonicOS Enhanced:

- Many-to-One NAT Policy
- Many-to-Many NAT Policy
- One-to-One NAT Policy for Outbound Traffic
- One-to-One NAT Policy for Inbound Traffic (Reflexive)
- One-to-Many NAT Load Balancing
- Inbound Port Address Translation via One-to-One NAT Policy
- Inbound Port Address Translation via WAN IP Address

This section describes how to configure a Many-to-One NAT policy. Many-to-One is the most common NAT policy on a SonicWALL security appliance, and allows you to translate a group of addresses into a single address. Most of the time, this means that you are taking an internal “private” IP subnet and translating all outgoing requests into the IP address of the SonicWALL security appliance WAN port, such that the destination sees the request as coming from the IP address of the SonicWALL security appliance WAN port, and not from the internal private IP address.

For other NAT configurations, see the *SonicOS Enhanced Administrator’s Guide*.

An example configuration illustrates the use of the fields in the Add NAT Policy procedure. To add a Many-to-One NAT policy that allows all systems on the **X1** interface to initiate traffic using the SonicWALL security appliance’s WAN IP address, perform the following steps:

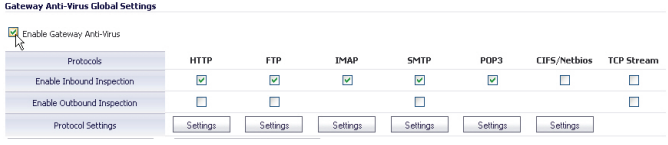
1. Navigate to the **Network** > **NAT** Policies page. Click **Add**. The **Add NAT Policy** dialog box displays.
2. For **Original Source**, select **Any**.
3. For **Translated Source**, select **WAN Interface IP**.
4. For **Original Destination**, select **Any**.
5. For **Translated Destination**, select **Original**.
6. For **Original Service**, select **Any**.
7. For **Translated Service**, select **Original**.
8. For **Inbound Interface**, select **X1**.
9. For **Outbound Interface**, select **X1**.
10. For **Comment**, enter a short description.
11. Select the **Enable NAT Policy** checkbox.
12. Leave **Create a reflexive policy** unchecked.
13. Click **Add**.

This policy can be duplicated for subnets behind the other interfaces of the SonicWALL security appliance – just replace the **Original Source** with the subnet behind that interface, adjust the source interface, and add another NAT policy.

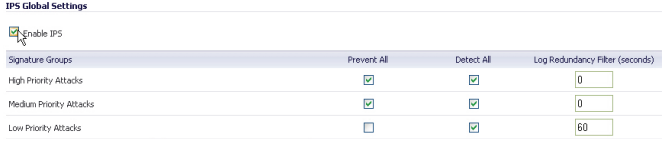
Enabling Security Services in SonicOS

You must enable each security service individually in the SonicOS user interface. See the following procedures to enable and configure the following three basic security services:

Gateway Anti-Virus



Intrusion Prevention



Anti-Spyware

For more information on configuring your security services, refer to the *SonicOS Administrator's Guide*.

Applying Security Services to Zones

A network zone is a logical group of one or more interfaces to which you can apply security rules to regulate traffic passing from one zone to another zone.

Security services such as Gateway Anti-Virus are automatically applied to the LAN and WAN network zones when you activate the license and enable the service. To protect other zones such as the DMZ or Wireless LAN (WLAN), you must apply the security services to the network zones. For example, you can configure SonicWALL Intrusion Prevention Service for incoming and outgoing traffic on the WLAN zone to add more security for internal network traffic.

To apply services to network zones:

1. Navigate to the **Network** > **Zones** page.
2. In the Zone Settings table, click the **Configure** icon for the zone where you want to apply security services.
3. In the Edit Zone dialog box on the **General** tab, select the checkboxes for the security services to enable on this zone.
4. On the Edit Zone page, select the checkboxes for the security services that you want to enable.
5. Click **OK**.
6. To enable security services on other zones, repeat steps 2 through 4 for each zone.

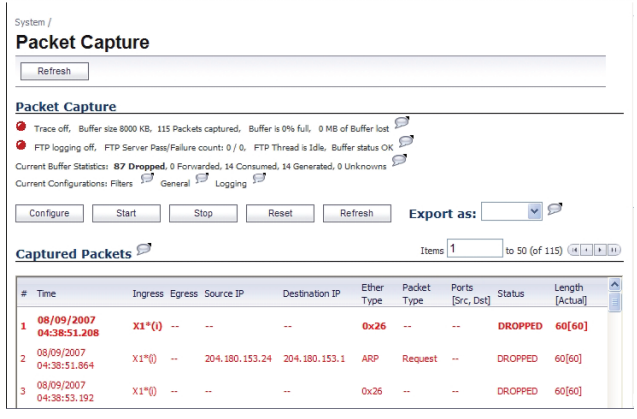
Troubleshooting Diagnostic Tools

SonicOS provides a number of diagnostic tools to help you maintain your network and troubleshoot problems. Several tools can be accessed on the **System** > **Diagnostics** page, and others are available on other screens.

This section contains the following subsections:

Using Packet Capture

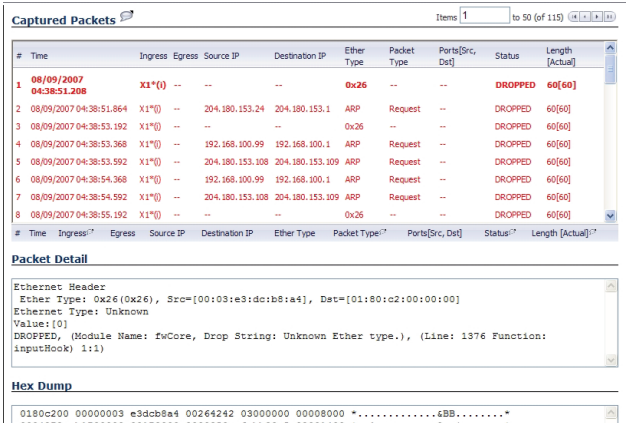
Packet Capture allows you to capture and examine the contents of individual data packets that traverse your SonicWALL firewall appliance. The captured packets contain both data and addressing information. The **System** > **Packet Capture** page provides a way to configure the capture criteria, display settings and file export settings, and displays the captured packets.



The Packet Capture screen has buttons for starting and stopping a packet capture. If you simply click **Start** without any configuration, the SonicWALL appliance will capture all packets except those for internal communication, and will stop when the buffer is full or when you click **Stop**.

The SonicOS user interface provides three windows to display different views of the captured packets:

- Captured Packets
- Packet Detail
- Hex Dump

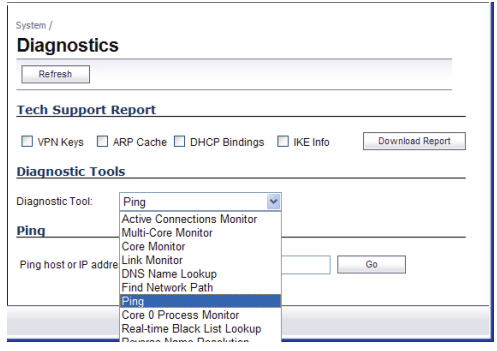


Click the **Configure** button to customize the settings for the capture. Once the configuration is complete, click **Start** to begin capturing packets. The settings available in the five main areas of configuration are summarized below:

- **General** - number of bytes to capture, wrap capture buffer
- **Capture Filter** - interfaces, packet types, source/ destination
- **Display Filter** - interfaces, packet types, source/ destination
- **Logging** - automatic transfer of buffer to FTP server
- **Advanced** - generated packets, GMS, syslog, management

Using Ping

Ping is available on the **System** > **Diagnostics** page.



The Ping test bounces a packet off a machine on the Internet and returns it to the sender. This test shows if the SonicWALL security appliance is able to contact the remote host. If users on the LAN are having problems accessing services on the Internet, try pinging the DNS server, or another machine at the ISP location. If the test is unsuccessful, try pinging devices outside the ISP. If you can ping devices outside of the ISP, then the problem lies with the ISP connection.

Using the Active Connections Monitor

The **Active Connections Monitor** displays real-time, exportable (plain text or CSV), filterable views of all connections to and through the SonicWALL security appliance. This tool is available on the **Systems** > **Diagnostics** page.

You can filter the results to display only connections matching certain criteria. You can filter by **Source IP**, **Destination IP**, **Destination Port**, **Protocol**, **Src Interface** and **Dst Interface**. Enter your filter criteria in the **Active Connections Monitor Settings** table.

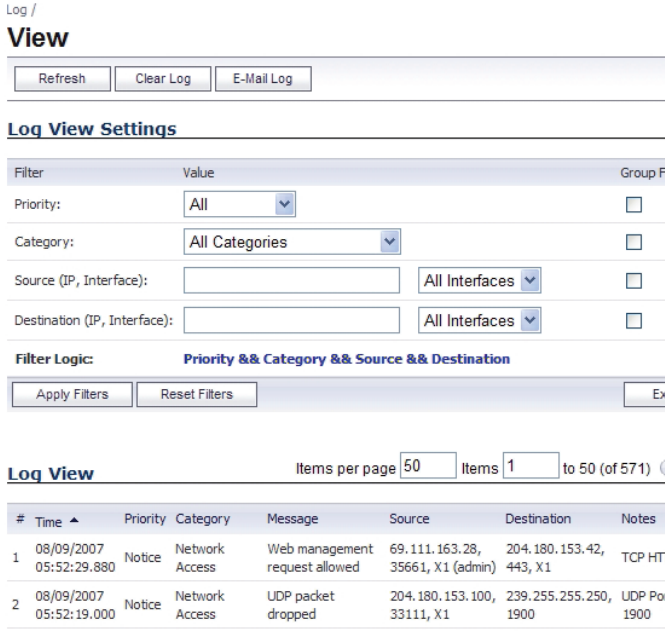
The fields you enter values into are combined into a search string with a logical **AND**. Select the **Group Filters** box next to any two or more criteria to combine them with a logical **OR**.

Using Log > View

The SonicWALL security appliance maintains an Event log for tracking potential security threats. You can view the log in the **Log** > **View** page, or it can be automatically sent to an email address for convenience and archiving. The log is displayed in a table and can be sorted by column.

You can filter the results to display only event logs matching certain criteria. You can filter by **Priority**, **Category**, **Source** (**IP** or **Interface**), and **Destination** (**IP** or **Interface**).

The fields you enter values into are combined into a search string with a logical **AND**. Select the **Group Filters** box next to any two or more criteria to combine them with a logical **OR**.



Deployment Configuration Reference Checklist

Use this checklist to find more information about various deployment tasks within the *SonicOS Enhanced Administrator's Guide*.

For this Task...	See this Chapter...
Inspecting the rule base for inbound and outbound rules	Configuring Access Rules
Setting logging levels	Configuring Log Categories (“Logging Level” section)
Configuring threat prevention on all used zones	Configuring Zones (“Enabling SonicWALL Security Services on Zones” section)
Configuring Web filtering protection	Configuring SonicWALL Content Filtering Service
Changing administrator login	Configuring Administration Settings ("Administrator Name & Password“ section)
Setting administrator email	Configuring Log Automation (“Email Log Automation“ section)
Disabling HTTP and ping access	Configuring Interfaces (“Configuring Advanced Settings for the Interfaces“ section)
Disabling or enabling DHCP	Setting Up the DHCP Server
Configuring user management	Managing Users and Authentication Settings
Configuring VPN policies	Configuring VPN Policies
Securing wireless access	Managing SonicPoints

Support and Training Options

5

In this Section:

This section provides overviews of customer support and training options for the SonicWALL NSA E5500.

Customer Support

SonicWALL offers Web-based and telephone support to customers who have a valid Warranty or who purchased a Support Contract. Please review our Warranty Support Policy for product coverage. SonicWALL also offers a full range of consulting services to meet your needs, from our innovative implementation services to traditional statement of work-based services.

For further information, visit:

http://www.sonicwall.com/us/support/contact.html

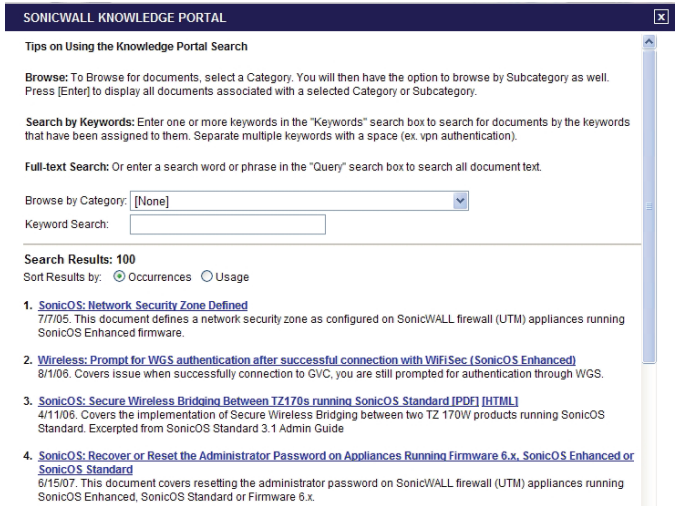
Knowledge Portal

The Knowledge Portal is a resource which allows users to search for SonicWALL documents based on the following types of search tools:

- Browse
- Search for keywords
- Full-text search

For further information, visit:

<http://www.sonicwall.com/us/support.html>



User Forums

The SonicWALL User Forums is a resource that provides users the ability to communicate and discuss a variety of security and appliance subject matters. In this forum, the following categories are available for users:

- Content Security Manager topics
- Continuous Data Protection topics
- Email Security related topics
- Firewall related topics
- Network Anti-Virus related topics
- Security Services and Content Filtering topics
- GMS and Viewpoint related topics
- SonicPoint and Wireless related topics
- SSL VPN related topics
- TZ 190 / Wireless WAN - 3G Capability
- VPN Client related topics
- VPN site-to-site and interoperability topics

For further information, visit:

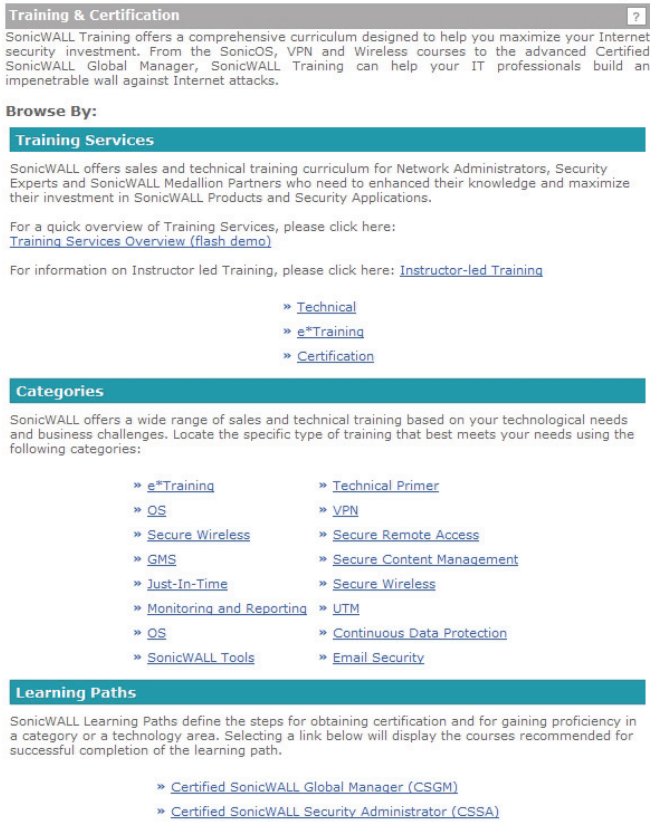
<https://forum.sonicwall.com/>

Training

SonicWALL offers an extensive sales and technical training curriculum for Network Administrators, Security Experts and SonicWALL Medallion Partners who need to enhance their knowledge and maximize their investment in SonicWALL Products and Security Applications. SonicWALL Training provides the following resources for its customers:

- E-Training
- Instructor-Led Training
- Custom Training
- Technical Certification
- Authorized Training Partners

For further information, visit:
<http://www.sonicwall.com/us/support/training.html>



Related Documentation

See the following related documents for more information:

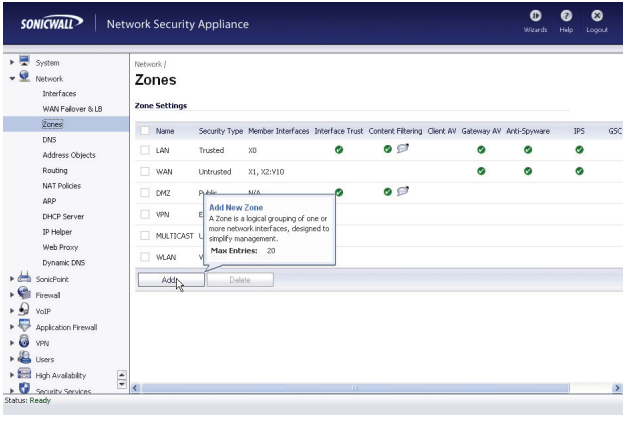
- *SonicOS Enhanced 5.0 Administrator's Guide*
- *SonicOS Enhanced 5.0 Release Notes*
- *SonicOS Enhanced 5.0 Feature Modules*
  - Application Firewall
  - Dashboard
  - HA License Sync
  - Multiple Admin
  - NAT Load Balancing
  - Packet Capture
  - RF Management
  - Single Sign On
  - SSL Control
  - Virtual Access Points
- *SonicWALL GVC 4.0 Administrator's Guide*
- *SonicWALL ViewPoint 4.1 Administrator's Guide*
- *SonicWALL GAV 2.1 Administrator's Guide*
- *SonicWALL IPS 2.0 Administrator's Guide*
- *SonicWALL Anti-Spyware Administrator's Guide*
- *SonicWALL CFS Administrator's Guide*

For further information, visit:

<http://www.sonicwall.com/us/support/289.html>

Dynamic Tooltips

SonicOS features a dynamic tooltips that appear over various elements of the GUI when the mouse hovers over them. Elements that display these tooltips include text fields, radio buttons, and checkboxes.

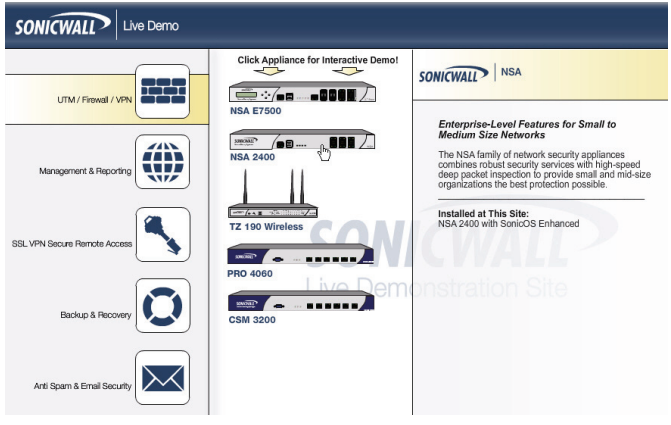


SonicWALL Live Product Demos

The SonicWALL Live Demo Site provides free test drives of SonicWALL security products and services through interactive live product installations:

- Unified Threat Management Platform
- Secure Cellular Wireless
- Continuous Data Protection
- SSL VPN Secure Remote Access
- Content Filtering
- Secure Wireless Solutions
- Email Security
- SonicWALL GMS and ViewPoint

For further information, visit:
<*http://livedemo.sonicwall.com/*>



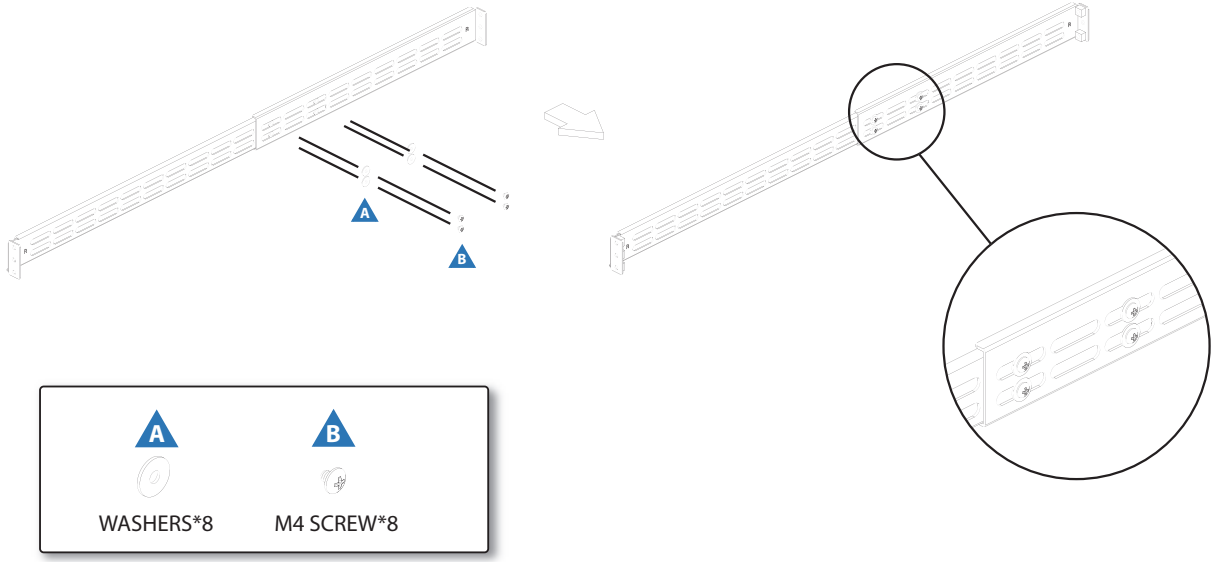
Rack Mounting Instructions 6

In this Section:

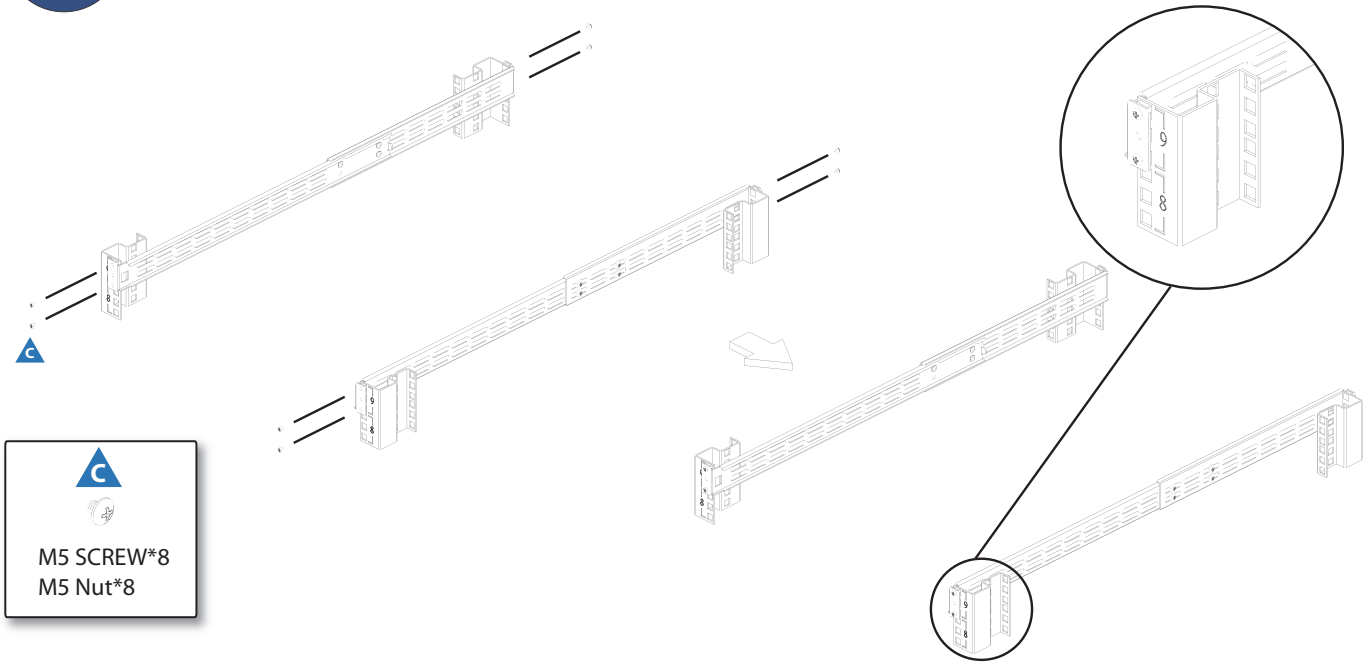
This section provides illustrated rack mounting instructions for the SonicWALL NSA E5500.

Assemble the Slide Rail

1 Fasten 4 screws to the rail.

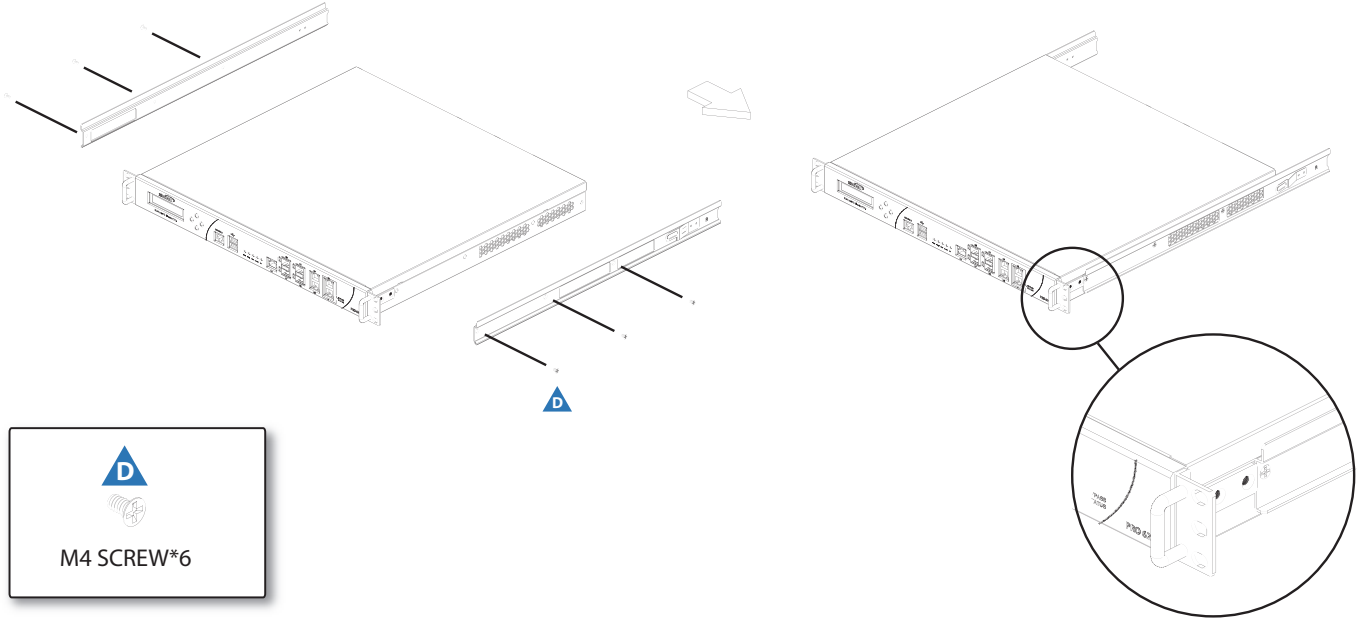


2 Fasten two-sided screws to the rail.

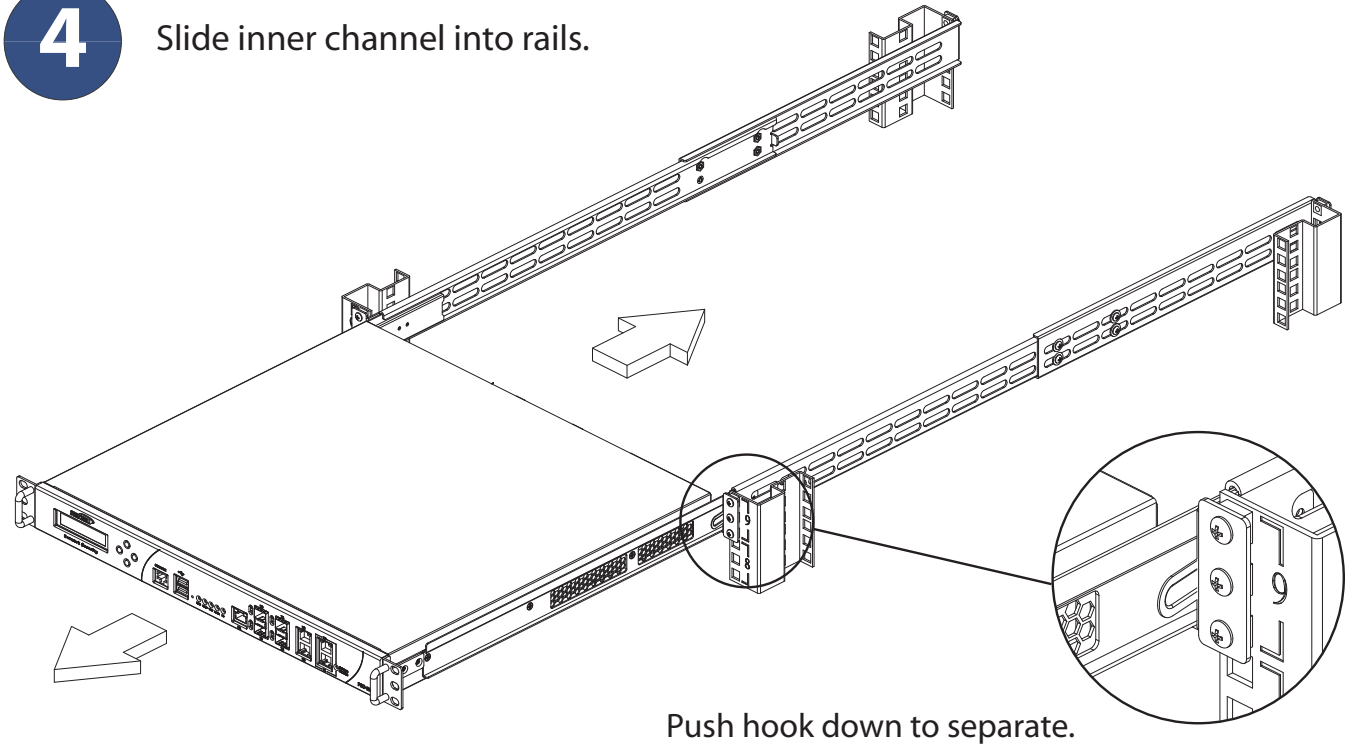


Assemble Inner Rail to Chassis

3 Fasten 6 screws to attach the inner channel onto the chassis.



4 Slide inner channel into rails.



Push hook down to separate.

Product Safety and Regulatory Information 7

In this Section:

This section provides regulatory along with trademark and copyright information.

Safety and Regulatory Information

Regulatory Model/Type	Product Name
1RK12-050 1RK22-073	E5500

Rack Mounting the SonicWALL

The above SonicWALL appliances are designed to be mounted in a standard 19-inch rack mount cabinet. The following conditions are required for proper installation:

- Use the mounting hardware recommended by the rack manufacturer and ensure that the rack is adequate for the application.
- Four mounting screws, compatible with the rack design, must be used and hand tightened to ensure secure installation. Choose a mounting location where all four mounting holes line up with those of the mounting bars of the 19-inch rack mount cabinet.
- Mount in a location away from direct sunlight and sources of heat. A maximum ambient temperature of 104º F (40º C) is recommended.
- Route cables away from power lines, fluorescent lighting fixtures, and sources of noise such as radios, transmitters and broadband amplifiers.
- The included power cord is intended for use in North America only. For European Union (EU) customers, a power cord is not included.
- Ensure that no water or excessive moisture can enter the unit.
- Allow unrestricted airflow around the unit and through the vents on the side of the unit. A minimum of 1 inch (25.44mm) clearance is recommended.
- Mount the SonicWALL appliances evenly in the rack in order to prevent a hazardous condition caused by uneven mechanical loading.
- Consideration must be given to the connection of the equipment to the supply circuit. The effect of overloading the circuits has minimal impact on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings must be used when addressing this concern.
- Reliable grounding of rack-mounted equipment must be maintained. Particular attention must be given to power supply connections other than direct connections to the branch circuits such as power strips.

Lithium Battery Warning

The Lithium Battery used in the SonicWALL Internet security appliance may not be replaced by the user. The SonicWALL must be returned to a SonicWALL authorized service center for replacement with the same or equivalent type recommended by the manufacturer. If, for any reason, the battery or SonicWALL Internet security appliance must be disposed of, do so following the battery manufacturer's instructions.

Cable Connections

All Ethernet and RS232 (Console) cables are designed for intra-building connection to other equipment. Do not connect these ports directly to communication wiring or other wiring that exits the building where the SonicWALL is located.

Weitere Hinweise zur Montage

Die oben genannten SonicWALL-Modelle sind für eine Montage in einem standardmäßigen 19-Zoll-Rack konzipiert. Für eine ordnungsgemäße Montage sollten die folgenden Hinweise beachtet werden:

- Vergewissern Sie sich, dass das Rack für dieses Gerät geeignet ist und verwenden Sie das vom Rack-Hersteller empfohlene Montagezubehör.
- Verwenden Sie für eine sichere Montage vier passende Befestigungsschrauben, und ziehen Sie diese mit der Hand an.
- Wählen Sie für die Montage einen Ort, der keinem direkten Sonnenlicht ausgesetzt ist und sich nicht in der Nähe von Wärmequellen befindet. Die Umgebungstemperatur darf nicht mehr als 40 °C betragen.
- Achten Sie darauf, das sich die Netzwerkkabel nicht in der unmittelbaren Nähe von Stromleitungen, Leuchtstoffröhren und Störquellen wie Funksendern oder Breitbandverstärkern befinden.
- Das beigefügte Netzkabel ist nur für den Gebrauch in Nordamerikas Vorgesehen. Für Kunden in der Europaïschen Union (EU) ist ein Netzkabel nicht im Lieferumfang enthalten.
- Stellen Sie sicher, dass das Gerät vor Wasser und hoher Luftfeuchtigkeit geschützt ist.
- Stellen Sie sicher, dass die Luft um das Gerät herum zirkulieren kann und die Lüftungsschlitze an der Seite des Gehäuses frei sind. Hier ist ein Belüftungsabstand von mindestens 26 mm einzuhalten.
- Bringen Sie die SonicWALL waagerecht im Rack an, um mögliche Gefahren durch ungleiche mechanische Belastung zu vermeiden.
- Prüfen Sie den Anschluss des Geräts an die Stromversorgung, damit der Überstromschutz sowie die elektrische Leitung nicht von einer eventuellen Überlastung der Stromversorgung beeinflusst werden. Prüfen Sie dabei sorgfältig die Angaben auf dem Aufkleber des Geräts.
- Vergewissern Sie sich, dass das Gerät sicher im Rack befestigt ist. Insbesondere muss auf nicht direkte Anschlüsse an Stromquellen geachtet werden wie z. B. bei Verwendung von Mehrfachsteckdosen.

Hinweis zur Lithiumbatterie

Die in der Internet Security Appliance von SonicWALL verwendete Lithiumbatterie darf nicht vom Benutzer ausgetauscht werden. Zum Austauschen der Batterie muss die SonicWALL in ein von SonicWALL autorisiertes Service-Center gebracht werden. Dort wird die Batterie durch denselben oder entsprechenden, vom Hersteller empfohlenen Batterietyp ersetzt. Beachten Sie bei einer Entsorgung der Batterie oder der SonicWALL Internet Security Appliance die diesbezüglichen Anweisungen des Herstellers.

Kabelverbindungen

Alle Ethernet- und RS232-C-Kabel eignen sich für die Verbindung von Geräten in Innenräumen. Schließen Sie an die Anschlüsse der SonicWALL keine Kabel an, die aus dem Gebäude in dem sich das Gerät befindet ,herausgeführt werden.

FCC Part 15 Class A Notice

NOTE: This equipment was tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. And if not installed and used in accordance with the instruction manual, the device may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the interference at his own expense.

Complies with EN 55022 Class A and CISPR22 Class A.

Caution: *Modifying this equipment or using this equipment for purposes not shown in this manual without the written consent of SonicWALL, Inc. could void the user's authority to operate this equipment.*

BMSI Statement

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

VCCI Statement

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－ A

Canadian Radio Frequency Emissions Statement

This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à toutes la norme NMB-003 du Canada.

CISPR 22 (EN 55022) Class A

Warning: This is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Declaration of Conformity
Application of council Directive 2004/108/EC (EMC) and 2006/95/EC (LVD)
Standards to which conformity is declared
EN 55022 (2006) +A1 (2007) Class A
EN 55024 (1998) +A1 (2001), +A2 (2003)
EN 61000-3-2 (2006)
EN 61000-3-3 (1995) +A1 (2001), +A2 (2005)
EN 60950-1 (2001) +A11

National Deviations: AR, AT, AU, BE, BR, CA, CH, CN, CZ, DE, DK, FI, FR, GB, GR, HU, IL, IN, IT, JP, KE, KR, MY, NL, NO, PL, SE, SG, SI, SK, US

Regulatory Information for Korea

MIC	Ministry of Information and Telecommunication Certification Number

All products with country code “A” and “J” are made in the USA.
All products with country code “B” are made in China.
All products with country code "C" or "D" are made in Taiwan R.O.C.
All certificates held by NetSonic, Inc.

A급 기기 (업무용 정보통신기기)

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 만약 잘못판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Copyright Notice

Trademarks

Notes

Notes

Notes

SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

PN: 232-001052-52
Rev A 06/09

PROTECTION AT THE SPEED OF BUSINESS™