



SonicWALL Secure Remote Access Appliances

SECURE REMOTE ACCESS

SRA 1200/4200 Getting Started Guide

Getting Started Guide



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

SonicWALL

SRA 1200/4200

Getting Started Guide

This *Getting Started Guide* contains installation procedures and configuration guidelines for deploying a SonicWALL SRA 1200/4200 appliance into an existing or new network. This document addresses the most common use-case scenarios and network topologies in which the SonicWALL SRA 1200/4200 appliance can be deployed.

Document Contents

This document contains the following sections:

- 1 [Setting Up Your Network](#) - page 3
- 2 [Connecting Your Appliance](#) - page 11
- 3 [Registering Your Appliance](#) - page 21
- 4 [Network Configuration](#) - page 27
- 5 [Upgrading Your Appliance](#) - page 41
- 6 [Safety and Regulatory Information](#) - page 53



In this Section:

This section provides pre-configuration information. Review this section before setting up your SonicWALL SRA 1200/4200 appliance.

- [SRA 1200 System Requirements](#) - page 4
- [SRA 4200 System Requirements](#) - page 5
- [Selecting a Deployment Scenario](#) - page 7
- [Applying Power to the SonicWALL SRA](#) - page 9

SRA 1200 System Requirements

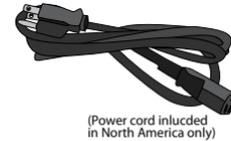
Before you begin the setup process, verify that your package contains the following parts:

- One SonicWALL SRA 1200 appliance
- One SonicWALL SRA 1200/4200 Getting Started Guide
- One straight-through Ethernet cable
- One serial CLI cable
- One rack-mount kit
- One power cord*
- A Web browser supporting Java Script and HTTP uploads.
Supported browsers include the following:

	Supported Browsers	Browser Version Number
	Internet Explorer	8.0 or higher
	Firefox	4.0 or higher
	Safari	4.0 or higher for MacOS
	Chrome	11.0 or higher

**Power cord intended for use in North America only. For other areas, please refer to your product reseller.*

Package Contents for the SonicWALL SRA 1200



(Power cord included in North America only)

Missing Items?

If any items are missing from your package, contact SonicWALL Support:

Web: <http://www.sonicwall.com/us/Support.html>

Email: customer_service@sonicwall.com

SRA 4200 System Requirements

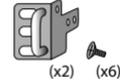
Before you begin the setup process, verify that your package contains the following parts:

- One SonicWALL SRA 4200 appliance
- One SonicWALL SRA 1200/4200 Getting Started Guide
- One straight-through Ethernet cable
- One serial CLI cable
- One rack-mount kit
- One power cord*
- A Web browser supporting Java Script and HTTP uploads. Supported browsers include the following:

	Supported Browsers	Browser Version Number
	Internet Explorer	8.0 or higher
	Firefox	4.0 or higher
	Safari	4.0 or higher for MacOS
	Chrome	11.0 or higher

*Power cord intended for use in North America only. For other areas, please refer to your product reseller.

Package Contents for the SonicWALL SRA 4200



(Power cord included in North America only)

Missing Items?

If any items are missing from your package, contact SonicWALL Support:

Web: <http://www.sonicwall.com/us/Support.html>

Email: customer_service@sonicwall.com

What You Need to Begin

- Administrative access to the network gateway device
- A Windows, Linux, or MacOS computer to use as a management station for initial configuration of the SonicWALL SRA 1200/4200
- A Web browser supporting Java Script and HTTP uploads (See previous pages for supported Web browsers)
- An Internet connection

Recording Configuration Information

Record the following setup information to use during the setup process and for future reference:

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.

Administrator Information

Admin Name:	Select an administrator account name. (default is <i>admin</i>)
Admin Password:	Select an administrator password. (default is <i>password</i>)

Network Configuration Information

Collect the following information about your current network configuration:

Primary DNS: _____

Secondary DNS (optional): _____

DNS Domain: _____

WINS server(s) (optional): _____

Selecting a Deployment Scenario

The deployment scenarios described in this section are based on actual customer deployments and are SonicWALL-recommended deployment best practices for SRA appliances .

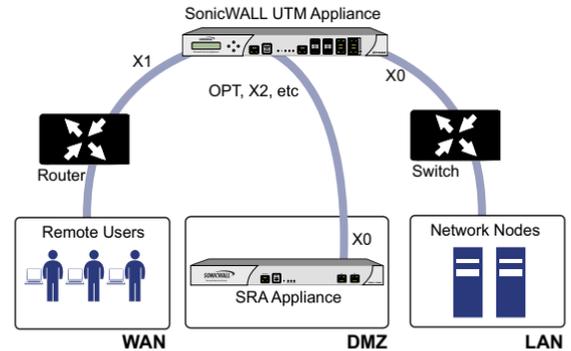
A SonicWALL SRA appliance is commonly deployed in “one-arm” mode over the DMZ or Opt interface on an accompanying gateway appliance, such as a SonicWALL NSA E7500. This method of deployment offers additional layers of security control, plus the ability to use SonicWALL’s UTM services, including Gateway Anti-Virus, Anti-Spyware, Content Filtering, Intrusion Prevention Service, and Comprehensive Anti-Spam Service, to scan all incoming and outgoing NetExtender traffic.

The primary interface (X0) on the SonicWALL SRA connects to an available segment on the gateway device. The encrypted user session is passed through the gateway to the SonicWALL SRA appliance. The SonicWALL SRA appliance decrypts the session and determines the requested resource.

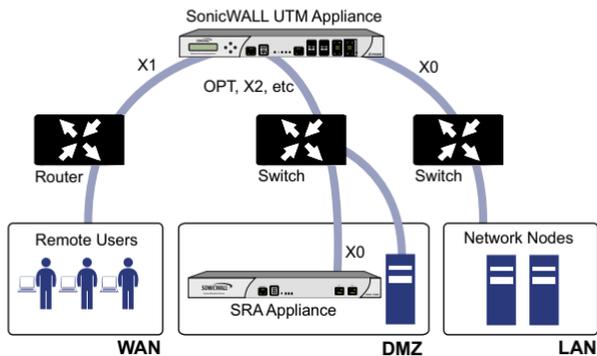
The session traffic then traverses the gateway appliance to reach the internal network resources. The gateway appliance applies security services, such as Intrusion Prevention, Gateway Anti-Virus, and Anti-Spyware inspection as data traverses the gateway. The internal network resource then returns the requested content to the SonicWALL SRA appliance through the gateway, where it is encrypted and sent to the client.

Scenario Overviews

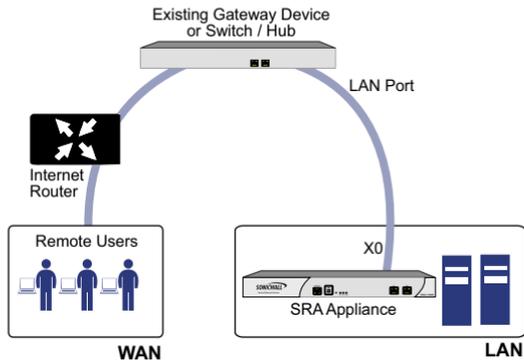
Scenario A: SRA on a New DMZ



Scenario B: SRA on an Existing DMZ



Scenario C: SRA on the LAN



SonicWALL SRA 1200/4200 Deployment Scenarios

Gateway Device	Deployment Scenario	Conditions or Requirements
SonicOS Enhanced 3.1 or higher: <ul style="list-style-type: none"> TZ Series PRO Series NSA E-Class (SonicOS 5.0+) NSA Series (SonicOS 5.0+) 	SRA on a New DMZ	<ul style="list-style-type: none"> OPT or unused interface New DMZ configured for NAT or Transparent Mode
	SRA on Existing DMZ	<ul style="list-style-type: none"> No unused interfaces One dedicated interface in use as an existing DMZ
	SRA on the LAN	<ul style="list-style-type: none"> No unused interfaces No dedicated interface for a DMZ
SonicOS Standard 3.1 or higher: <ul style="list-style-type: none"> TZ Series PRO Series 	SRA on a New DMZ	<ul style="list-style-type: none"> Open OPT or X2 interface New DMZ configured for either NAT or Transparent Mode Provide SonicWALL deep packet inspection security services (optional)
	SRA on Existing DMZ	<ul style="list-style-type: none"> OPT or X2 interface in use with an existing DMZ Provide SonicWALL deep packet inspection security services (optional)
SonicOS Standard 3.1 or higher: <ul style="list-style-type: none"> TZ Series PRO Series SonicWALLs with legacy firmware Third-Party Gateway Device	SRA on the LAN	<ul style="list-style-type: none"> Not planning to use SonicWALL deep packet inspection security services Interoperability with a third-party gateway device

Applying Power to the SonicWALL SRA

1. Plug one end of the power cord into the SonicWALL SRA 1200/4200 and the other into an appropriate power outlet.
2. Turn on the power switch located on the rear of the appliance next to the power cord.

The 'Pwr' LED on the front panel lights up blue when the appliance is turned on. The 'Test' LED lights up yellow and may blink for up to a minute while the appliance performs a series of diagnostic tests. When the 'Test' LED is no longer lit, the SonicWALL SRA 1200/4200 is ready for configuration.



If the 'Test' or 'Alarm' LEDs remain lit, or if the 'Test' LED blinks red after the SonicWALL SRA 1200/4200 has booted, restart the appliance. For more troubleshooting information, refer to the *SonicWALL SSL VPN Administrator's Guide*.

Accessing the Management Interface

To access the Web-based management interface of the SonicWALL SRA 1200/4200:

1. Connect one end of an Ethernet cable into the 'X0' port of your SonicWALL SRA 1200/4200. Connect the other end of the cable into the computer you are using to manage the SonicWALL SRA 1200/4200.
2. Set the computer you use to manage the SonicWALL SRA 1200/4200 to have a static IP address in the 192.168.200.x/24 subnet, such as **192.168.200.20**. *However, do not use 192.168.200.1, as this address will conflict with the appliance.*
3. Open a Web browser, and enter **http://192.168.200.1** (the default X0 management IP address) in the Location or Address field.



Note: *A security warning may appear. Click **Continue to this website** or **OK** to accept the certificate and continue.*

4. The 'SonicWALL SRA Management Interface Login' displays and prompts you to enter your user name and password. Enter **"admin"** in the User Name field, **"password"** in the Password field, select **"LocalDomain"** from the Domain drop-down list, and **click the Login button**.



The screenshot shows the SonicWALL SSL-VPN Login page. At the top, there is a blue header with the SonicWALL logo on the left and 'SSL-VPN Login' on the right. Below the header, there is a white form area with a decorative wavy pattern in the background. The form contains three input fields: 'Username' with the text 'admin', 'Password' with masked characters (dots), and 'Domain' with a dropdown menu showing 'LocalDomain'. Below the input fields is a 'Login' button.

You are now successfully connected to the SRA Management Interface.

Troubleshooting

If you cannot connect to the SonicWALL SRA 1200/4200, verify the following configurations:

- Did you plug your management workstation into the interface X0 on the SonicWALL SRA appliance? Management can only be performed through X0.
- Is the link light illuminated on both the management station and the SonicWALL SRA appliance?
- Did you correctly enter the SonicWALL SRA 4200 management IP address in your Web browser?
- Is your computer set to a static IP address of 192.168.200.20?
- Is your Domain set to LocalDomain on the login screen?

If you are still unable to connect to the SonicWALL SRA appliance, contact SonicWALL Support:

Web: <http://www.sonicwall.com/us/Support.html>

Email: customer_service@sonicwall.com

In this Section:

This section provides procedures for connecting your SonicWALL SRA 1200/4200 appliance.

- [Configuring Your SRA 1200/4200](#) - page 12
- [Connecting Your SRA 1200/4200](#) - page 18

Configuring Your SRA 1200/4200

Once your SonicWALL SRA 1200/4200 is connected to a computer through the management port (X0), it can be configured through the Web-based management interface.

Setting Your Administrator Password

1. From the management interface, select the **Users > Local Users** page.
2. Click the **Configure** button  corresponding to the “admin” account.

admin	LocalDomain	Administrator		
-------	-------------	---------------	---	---



Note: *Changing your password from the factory default is strongly recommended. If you change your password, be sure to keep it in a safe place. If you lose your password, you will have to reset the SonicWALL SRA to factory settings losing your configuration.*

3. **Enter a password** for the “admin” account in the Password field. **Re-enter the password** in the Confirm Password field.

General User Settings

User Name:	admin
Primary Group:	LocalDomain (see all)
In Domain:	LocalDomain
User Type:	Administrator
Password:	<input type="password"/>
Confirm Password:	<input type="password"/>
Inactivity Timeout (minutes):	<input type="text" value="0"/> 

Single Sign-On Settings

Automatically log into bookmarks:	<input type="text" value="Use group setting"/> ▼
-----------------------------------	--

4. **Click OK** to apply changes.

Adding a Local User

1. Navigate to **Users > Local Users** page.
2. Click the **Add User** button.
3. Enter a **User Name**.
4. Select **LocalDomain** from the Group/Domain drop-down menu.
5. Enter a **Password** for the user. Confirm the new password.
6. Select **User** from the User Type drop-down menu.



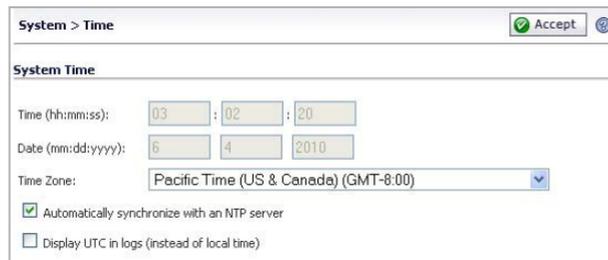
The screenshot shows the 'Users > Local Users > Add Local User' page. It contains the following fields:

- User Name: [Text input field]
- Domain: [Dropdown menu with 'LocalDomain' selected]
- Group: [Dropdown menu with 'LocalDomain' selected]
- Password: [Text input field]
- Confirm Password: [Text input field]
- User Type: [Dropdown menu with 'User' selected]

7. **Click Add** to finish adding a local user.

Setting the Time Zone

1. Navigate to the **System > Time** page.
2. Select the appropriate **Time Zone** from the drop-down menu.



The screenshot shows the 'System > Time' configuration page. It includes the following settings:

- Time (hh:mm:ss): 03 : 02 : 20
- Date (mm:dd:yyyy): 6 / 4 / 2010
- Time Zone: Pacific Time (US & Canada) (GMT-8:00)
- Automatically synchronize with an NTP server
- Display UTC in logs (instead of local time)

3. **Click Accept** to save changes to the time settings.

 **Note:** *Setting the correct time is essential to operations of the SonicWALL SRA 1200/4200. Be sure to set the time zone correctly. Automatic synchronization with an NTP server (default setting) is encouraged for accuracy.*

Configuring SRA Network Settings

You will now configure your SRA 1200/4200 network settings. Refer to the notes you took in the ["Recording Configuration Information"](#) on page 6 to complete this section.

Configuring DNS / WINS

1. Navigate to the **Network > DNS** page in the management interface.
2. **Enter a unique name for your SonicWALL SRA** in the SSL-VPN Gateway Hostname field.
3. **Enter your Primary DNS Server** information.
4. (Optional) **Enter a secondary DNS server** in the Secondary DNS Server field.

Network > DNS Accept

Hostname

SSL VPN Gateway Hostname:

DNS Settings

Primary DNS Server:

Secondary DNS Server (optional):

DNS Domain (optional):

WINS Settings

Primary WINS Server (optional):

Secondary WINS Server (optional):

5. (Optional) **Enter your DNS Domain.**
6. (Optional) **Enter your WINS servers** in the Primary WINS Server and Secondary WINS Server fields.
7. **Click Accept.**

Configuring the X0 IP Address for Scenario B and Scenario C

If you are deploying the SRA in either *Scenario B, SRA on an Existing DMZ* or *Scenario C, SRA on the LAN*, you need to reset the IP address of the X0 interface on the SRA to an address within the range of the existing DMZ or the existing LAN.

To configure the X0 IP address for either of these scenarios:

1. Navigate to the **Network > Interfaces** page.
2. Click the **Configure** icon for the X0 interface from the Interfaces table.

Network > Interfaces Configure

Interfaces

Name	IP Address	Subnet Mask	IPv6 Address	Status	Configure
X0	192.168.200.1	255.255.255.0	fe80::217:c5ff:fe66:1514/64	1000 Mbps - Full Duplex (Auto)	
X1	192.168.201.1	255.255.255.0	fe80::217:c5ff:fe66:1515/64	No link	

- In the Interface Settings dialog box, **set the IP address and subnet mask** to:

If you are using scenario:	Set the X0 interface to:
B - SRA on an Existing DMZ	IP Address: An unused address within your DMZ subnet, for example: 10.1.1.240 Subnet Mask: Must match your DMZ subnet mask
C - SRA on the LAN	IP Address: An unused address within your LAN subnet, for example: 192.168.168.200 Subnet Mask: Must match your LAN subnet mask

- Click OK.** Note that you will lose connection to the SRA.
- Reset the management computer to have a static IP address in the range you just set for the X0 interface, for example, **10.1.1.20** or **192.168.200.20**.
- Log into the SRA management interface again, using the IP address you just configured for the X0 interface. For example, point your browser to **http://192.168.168.200**.

Configuring a Default Route

Refer to the following table to correctly configure your default route. If you do not know your scenario, refer to [“Selecting a Deployment Scenario” on page 7](#).

If you are using scenario:	Your upstream gateway device will be:
A - SRA on a New DMZ	The DMZ interface you will create
B - SRA on an Existing DMZ	The existing DMZ interface
C - SRA on the LAN	The LAN gateway

To configure a default route:

- Navigate to the **Network > Routes** page.
- Enter the IP address of your upstream gateway device** in the Default Gateway field.
- Select **X0** in the Interfaces drop-down list.

The screenshot shows the 'Network > Routes' configuration window. Under the 'Default Route' section, there are four input fields: 'Default IPv4 Gateway' (containing '192.168.200.2'), 'Interface' (a dropdown menu with 'X0' selected), 'Default IPv6 Gateway' (empty), and another 'Interface' dropdown menu (with 'X0' selected). An 'Accept' button is visible in the top right corner of the window.

- Click Accept.**

Adding a NetExtender Client Route

NetExtender allows remote clients to have seamless access to resources on your local network. You can also enable Tunnel All Mode so that, when NetExtender clients connect, all the traffic will be tunneled through the NetExtender connection.

To configure a NetExtender client route:

1. Navigate to the **NetExtender > Client Routes** page.



NetExtender > Client Routes Accept

Tunnel All Mode: Disabled

Destination IPv4 Network	Subnet Mask	Delete
192.168.200.0	255.255.255.0	×

Destination IPv6 Network: Prefix: Delete

No Entries

Add Client Route...

Note: The NetExtender Client Routes are passed to all NetExtender clients and determine which private networks the remote user can access via the SSL-VPN connection.

2. To force all SRA client traffic to pass through the NetExtender tunnel, select **Enabled** from the Tunnel All Mode drop-down list.
3. **Click Add Client Route.**

4. **Enter the IP address of the trusted network to which you would like to provide access with NetExtender** in the Destination Network field. For example, if you are connecting to an existing DMZ with the network 192.168.50.0/24 and you want to provide access to your LAN network 192.168.168.0/24, you would enter 192.168.168.0.
5. **Enter your subnet mask** in the Subnet Mask field.



NetExtender > Client Routes > Add Client Route

Destination Network:

Subnet Mask/Prefix:

6. **Click Add** to finish adding this client route.

Setting Your NetExtender Address Range

The NetExtender IP range defines the IP address pool from which addresses will be assigned to remote users during NetExtender sessions. The range needs to be large enough to accommodate the maximum number of concurrent NetExtender users you wish to support.

The range should fall within the same subnet as the interface to which the SonicWALL SRA appliance is connected, and in cases where there are other hosts on the same segment as the SonicWALL SRA appliance, it must not overlap or collide with any assigned addresses. You can determine the correct subnet based on your network scenario selection:

Scenario A	Use the default NetExtender range: 192.168.200.100 to 192.168.200.200
Scenario B	Select a range that falls within your existing DMZ subnet. For example, if your DMZ uses the 192.168.50.0/24 subnet, and you want to support up to 30 concurrent NetExtender sessions, you could use 192.168.50.220 to 192.168.50.249 , providing they are not already in use.
Scenario C	Select a range that falls within your existing LAN subnet. For example, if your LAN uses the 192.168.168.0/24 subnet, and you want to support up to 10 concurrent NetExtender sessions, you could use 192.168.168.240 to 192.168.168.249 , providing they are not already in use.

To set your NetExtender address range in the management interface:

1. Navigate to the **NetExtender > Client Settings** page.
2. **Enter an address range for your clients** in the Client Address Range Begin and Client Address Range End fields.

Scenario A	192.168.200.100 to 192.168.200.200 (default range)
Scenario B	An unused range within your DMZ subnet
Scenario C	An unused range within your LAN subnet

If you do not have enough available addresses to support your desired number of concurrent NetExtender users, you may use a new subnet for NetExtender. This condition may occur if your existing DMZ or LAN is configured in NAT mode with a small subnet space, such as 255.255.255.224, or more commonly if your DMZ or LAN is configured in Transparent mode and you have a limited number of public addresses from your ISP. In either case, you may assign a new, unallocated IP range to NetExtender (such as 192.168.10.100 to 192.168.10.200) and configure a route to this range on your gateway appliance.

For example, if your current Transparent range is 67.115.118.75 through 67.115.118.80, and you wish to support 50 concurrent NetExtender clients, configure your SRA X0 interface with an available IP address in the Transparent range, such as 67.115.118.80, and configure your NetExtender range as 192.168.10.100 to 192.168.10.200. Then, on your gateway device, configure a static route to 192.168.10.0/255.255.255.0 using 67.115.118.80.

Connecting Your SRA 1200/4200

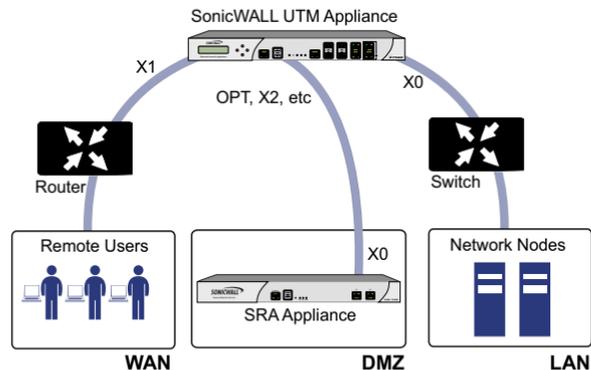
Before continuing, reference the diagrams on the following pages to connect the SonicWALL SRA 1200/4200 to your network.

Refer to the options in [“Selecting a Deployment Scenario”](#) on [page 7](#) to determine the proper scenario for your network configuration:

- [Scenario A: Connecting Your Network Interfaces](#) - page 18
- [Scenario B: Connecting Your Network Interfaces](#) - page 19
- [Scenario C: Connecting Your Network Interfaces](#) - page 19

Scenario A: Connecting Your Network Interfaces

Scenario A: SRA on a New DMZ



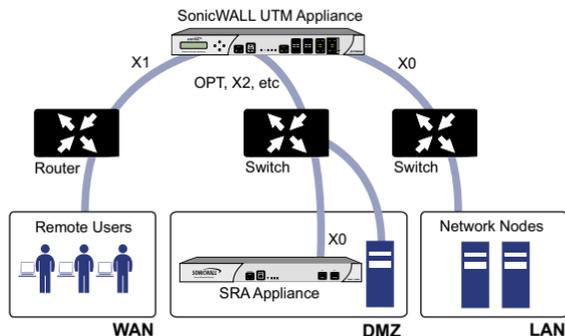
To connect the SonicWALL SRA 1200/4200 using Scenario A, perform the following steps:

1. **Connect one end of an Ethernet cable to the OPT, X2, or other unused port on your existing SonicWALL security appliance.**
2. **Connect the other end of the Ethernet cable to the X0 port on the front of your SonicWALL SRA 1200/4200.** The X0 Port LED lights up green indicating an active connection.

Continue to Chapter **3**

Scenario B: Connecting Your Network Interfaces

Scenario B: SRA on an Existing DMZ



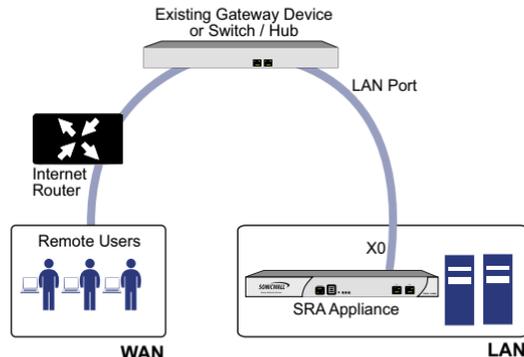
To connect the SonicWALL SRA 1200/4200 using Scenario B, perform the following steps:

1. **Connect one end of an Ethernet cable to an unused port on your DMZ**, either directly to the OPT or X2 on your existing SonicWALL security appliance, or to a hub or switch on your DMZ.
2. **Connect the other end of the Ethernet cable to the X0 port** on your SonicWALL SRA 1200/4200. The X0 Port LED lights up green indicating an active connection.

Continue to Chapter **3**

Scenario C: Connecting Your Network Interfaces

Scenario C: SRA on the LAN



To connect the SonicWALL SRA 1200/4200 using Scenario C, perform the following steps:

1. **Connect one end of an Ethernet cable to an unused port on your LAN hub or switch.**
2. **Connect the other end of the Ethernet cable to the X0 port** on the front of your SonicWALL SRA 1200/4200. The X0 Port LED lights up green indicating an active connection.

Continue to Chapter **3**

In this Section:

This section provides instructions for registering your SonicWALL SRA 1200/4200 appliance.

- [Creating a MySonicWALL Account](#) - page 22
- [Registering Your SonicWALL SRA](#) - page 22
- [Services and Licensing](#) - page 23



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

Creating a MySonicWALL Account

A MySonicWALL account is required for product registration. If you already have an account, continue to the following section.

Perform the following steps to create a MySonicWALL account:

1. In your browser, **navigate to www.mysonicwall.com**.
2. In the login screen, **click the [Not a registered user?](#) link**.



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

Registering Your SonicWALL SRA

This section contains the following subsections:

- [Before You Register](#) - page 22
- [Product Registration](#) - page 22

Before You Register

Verify that the time, DNS, and default route settings on your SonicWALL SRA 1200/4200 are correct before you register your appliance. To verify or configure these settings, navigate to the 'System > Time', 'Network > DNS', or 'Network > Routes' pages, respectively.

Product Registration

Register your SonicWALL SRA on MySonicWALL to enable full functionality.

1. **Login to your MySonicWALL account.** If you do not have an account, you can create one at www.mysonicwall.com.
2. On the main page, **enter the appliance serial number** in the Register A Product field. **Click Next.**
3. On the My Products page, under Add New Product, **enter the friendly name for the appliance**, select the **Product Group** if any, **enter the authentication code** into the appropriate text boxes, and then **click Register.**
4. On the Product Survey page, **fill in the requested information and click Continue.**

Services and Licensing

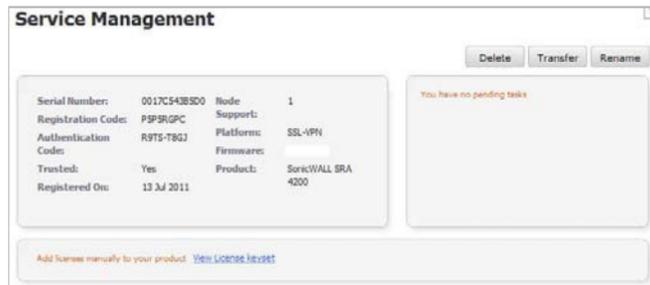
This section contains the following subsections:

- [Service Management](#) - page 23
- [Flexible Per-User Licensing](#) - page 24
- [Activating Services and Software](#) - page 24
- [Trying or Purchasing Services](#) - page 25

Service Management

The Service Management page in MySonicWALL lists services, support options, and software, such as Web Application Firewall and ViewPoint, that you can purchase or try with a free trial. For details on a product or service, **click the Info arrow icon** next to the desired item.

If you purchased an appliance that is pre-licensed, you may be required to **enter your activation key** here unless current licenses are already indicated in the Status column with either a license key or an expiration date.



The following products and services are available for the SonicWALL SRA 1200/4200 appliance:

- Gateway Service Bundles:
 - Per-user license upgrades in flexible block increments
- Desktop and Server Software:
 - Virtual Assist
 - Web Application Firewall
 - ViewPoint
- Support Services:
 - Dynamic Support 8x5
 - Dynamic Support 24x7
 - Software and Firmware Updates

Flexible Per-User Licensing

Your SonicWALL SRA comes standard with a set number of user licenses. However, as the needs of your organization change, SonicWALL offers flexible options when it comes to adding additional licenses. The ability to purchase a convenient number of additional licenses allows you to plan sensibly for the future, or provide immediate scalability when you need it most.

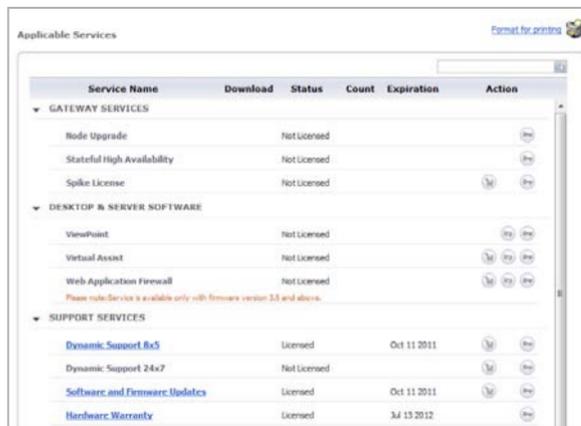
Appliance	SRA 1200	SRA 4200
Initial User Licenses	5	25
Additional Per-User License Packages	1 - 5 - 10	10 - 25 - 100
Maximum Concurrent User Sessions Allowed	50	500

Activating Services and Software

If you purchase a service subscription or upgrade from a sales representative, you will receive an activation key. This key is emailed to you after online purchases, or is on the front of the certificate that was included with your purchase.

To activate existing licenses, perform the following tasks:

1. Navigate to the 'My Products' page and **select the registered product** you want to manage.
2. Locate the product on the 'Service Management' page and **click Enter Key** in that row.



- In the 'Activate Service' page, **type or paste your key** into the Activation Key field and then **click Submit**.

Once the service is activated, you will see an expiration date or a license key string in the Status column on the Service Management page.

Activate Service: Virtual Assist

Please enter the Activation Key(s).
Multiple activations can be performed by adding keys for the same service separated by a comma, space or enter key.

Activation Key(s):

Submit Cancel

Trying or Purchasing Services

To try a free trial of a service, **click Try** in the 'Service Management' page.

To purchase a product or service, **click Buy Now** in the 'Service Management' page to complete your purchase.

Buy Service

Product Name: Techpubs_SRA4200
Serial Number: 0017C543B608

Price List

The following services can be purchased for your unit: Techpubs_SRA4200 0017C543B608

Part No.	Description	Unit Price	Quantity
01-SSC-8967	SSL-VPN Virtual Assist Up to 1 Tech	USD 495.00	1
01-SSC-8974	SSL-VPN Virtual Assist Up to 5 Techs	USD 1995.00	0

Service Status

If you have changed the "Quantity" value above and would like to see the status of this service, upon order completion, click "CALCULATE".
Techpubs_SRA4200 0017C543B608

Virtual Assist

Current Status	Status Upon Order Completion
	VPN Clients on Order Completion: 6

CALCULATE

When activation is complete, MySonicWALL displays an activation screen with service status and expiration information. The service management screen also displays the product you licensed.

You have successfully registered your SonicWALL appliance.

In this Section:

This section provides detailed overviews of deployment scenarios, as well as configuration instructions for connecting your SonicWALL SRA to various network devices, including gateway appliances.

- [Scenario A: SRA on a New DMZ](#) - page 27
- [Scenario B: SRA on an Existing DMZ](#) - page 32
- [Scenario C: SRA on the LAN](#) - page 36
- [Testing Your Remote Connection](#) - page 39



Tip: *Before completing this section, fill out the information on "[Recording Configuration Information](#)" on page 6.*

Scenario A: SRA on a New DMZ

This section provides procedures to configure your gateway appliance based on Scenario A. This section contains the following subsections:

- [Connecting to a SonicWALL Security Appliance](#) - page 28
- [Adding a New SRA Custom Zone](#) - page 28
- [Allowing a WAN -> SRA Connection](#) - page 29
- [Allowing an SRA -> LAN Connection](#) - page 30

Connecting to a SonicWALL Security Appliance

1. Using a computer connected to your LAN, launch your Web browser and **enter the IP address of your existing SonicWALL security appliance** in the Location or Address field.
2. When the management interface displays, **enter your user name and password** in the appropriate fields and **click Login**.



Note: *Remember that you are logging into your SonicWALL security appliance, not the SonicWALL SRA.*

Adding a New SRA Custom Zone

1. Navigate to the **Network > Interfaces** page, **click Configure** for the X2 interface (or any other available interface).
2. **Select Create New Zone** in Zone field. The 'Add Zone' window opens.

General Guest Services

General Settings

Name: SRA

Security Type: Public

Allow Interface Trust

Enforce Content Filtering Service

CFS Policy: Default

Enable Client AV Enforcement Service

Enable Gateway Anti-Virus Service

Enable IPS

Enable Anti-Spyware Service

Enforce Global Security Clients

Create Group VPN

Enable SSL Control

Enable SSL VPN Access

Ready

OK Cancel

3. **Enter SRA** in the Name field.
4. **Select Public** from the Security Type drop-down menu.
5. **Un-select the Allow Interface Trust checkbox.**

6. **Select the Gateway AV, Intrusion Prevention Service and Anti-Spyware checkboxes. Click OK.**
7. On the 'Edit Interface' window, **enter the IP address for this interface** in the IP Address field. (For example, "192.168.200.2". This should be the same address you created in "[Configuring the X0 IP Address for Scenario B and Scenario C](#)" on page 14).
8. **Enter your Subnet Mask.**
9. On the 'Management' area, **enable the desired management options.**
10. **Click OK** to apply changes.

Allowing a WAN -> SRA Connection

To create a public server access rule for HTTP and HTTPS traffic:

1. **Click the Wizards icon** in the top right corner of the management interface.
2. On the 'Welcome' page, **select the Public Server Wizard, and then click Next.**
3. On the 'Public Server Type' page, select:

Server Type	Other
Services	Create new group

The 'Add Service Group' dialog box appears.

4. In the 'Add Service Group' dialog box, **create a service group** for HTTP and HTTPS:
 - **Enter a name for the service.**
 - Select both **HTTP** and **HTTPS** and click .
 - **Click OK** when both the HTTP and HTTPS are in the right column.

5. On the 'Server Private Network Configuration' page, **enter the following**, and **click Next**:

Server Name	Name for the SonicWALL SRA
Server Private IP Address	SonicWALL SRA's 'X0' IP address, 192.168.200.1 by default
Server Comment	Brief description of the server

6. On the 'Server Public Information' page, **accept the default IP address**, or **enter an IP address** in your allowed public IP range. **Click Next**.



Note: *The default IP address is the WAN IP address of your SonicWALL security appliance. If you accept this default, all HTTP and HTTPS traffic to this IP address will be routed to your SonicWALL SRA.*

7. The 'Public Server Configuration Summary' page displays all the configuration actions that will be performed to create the public server. **Click Apply** to create the configuration and allow access from the WAN to the SRA on the DMZ.

Allowing an SRA -> LAN Connection

When users have connected to the SRA, they need to be able to connect to resources on the LAN. To allow an SRA to LAN connection, perform the following steps:

1. Navigate to the **Network > Address Objects** page.
2. In the 'Address Objects' section, **click** .
3. In the 'Add Address Object' dialog box, **create an address object** for the X0 interface IP address of your SonicWALL SRA:

Name	Name for the SonicWALL SRA
Zone Assignment	SRA
Type	Host
IP Address	SonicWALL SRA's 'X0' IP address, 192.168.200.1 by default

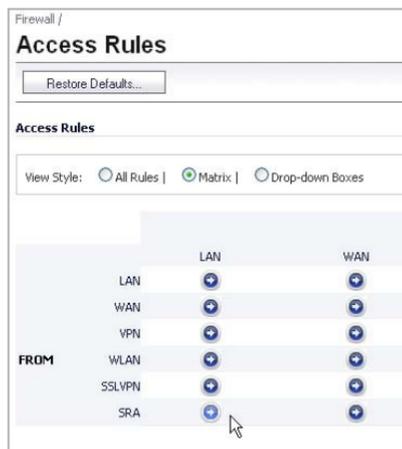
4. **Click Add** to create the object. Once done, **click Close**.
5. **Click** again to create an address object for the NetExtender range.

6. In the 'Add Address Object' dialog box, **create an address object** for the X0 interface IP address of the SonicWALL SRA:

Name	Name for NetExtender
Zone Assignment	SRA
Type	Range
Starting IP Address	Start of the NetExtender IP address range, 192.168.200.100 by default
Ending IP Address	End of the NetExtender IP address range, 192.168.200.200 by default

7. **Click Add** to create the object. Once done, **click Close**.
8. On the 'Network > Address Objects' page, in the 'Address Groups' section, **click** .
9. In the 'Add Address Object Group' dialog box, **create a group** for the X0 interface IP address of your SonicWALL SRA and the NetExtender IP range:
- **Enter a name for the group.**
 - In the left column, **select the two groups you created** and **click the right arrow button** .
 - **Click OK** to create the group when both objects are in the right column.
10. In the administrative interface, navigate to the **Firewall > Access Rules** page.

11. On the 'Firewall > Access Rules' page, in the matrix view, **click the SRA > LAN icon**.



12. On the resulting 'Firewall > Access Rules' page, **click**



13. In the 'Add Rule' window, **create a rule** to allow access to the LAN for the address group you just created:

Action	Allow
From Zone	SRA
To Zone	LAN
Service	Any
Source	The address group you just created, such as SonicWALL_SRA_Group
Destination	Any
Users Allowed	All
Schedule	Always on
Enable Logging	Selected
Allow Fragmented Packets	Selected

14. **Click OK** to create the rule.

Continue to ["Testing Your Remote Connection" on page 39](#)

Scenario B: SRA on an Existing DMZ

This section provides procedures to configure your gateway appliance based on Scenario B. This section contains the following subsections:

Prerequisites

- [Connecting to a SonicWALL Security Appliance](#) - page 32
- [Allowing WAN -> DMZ Connection](#) - page 33
- [Allowing DMZ -> LAN Connection](#) - page 34

Connecting to a SonicWALL Security Appliance

1. Using a computer connected to your LAN, launch your Web browser, and **enter the IP address** of your existing SonicWALL security appliance in the Location or Address field.
2. When the management interface displays, **enter your User Name** and **Password** in the appropriate fields and **click Login**.



Note: *Remember that you are logging into your SonicWALL firewall, not the SonicWALL SRA.*

Allowing WAN -> DMZ Connection

If you are already forwarding HTTP or HTTPS to an internal server, and you only have a single public IP address, you will need to select different (unique) ports of operation for either the existing servers or for the SonicWALL SRA appliance, because both cannot concurrently use the same IP address and port combinations.

To create a public server access rule for HTTPS traffic:

1. **Click the Wizards icon** at the top right of the interface.
2. On the 'Welcome' page, select the **Public Server Wizard** and then **click Next**.
3. On the 'Public Server Type' page, select:

Server Type	Other
Services	Create new group

The 'Add Service Group' dialog box is displays.

4. In the 'Add Service Group' dialog box, **create a service group for HTTP and HTTPS**:
 - **Enter a name for the service.**
 - Select both **HTTP** and **HTTPS** and click .
 - **Click OK** when HTTP and HTTPS are in the right column.
5. On the 'Public Server Type' page, **click Next**.

6. On the 'Server Private Network Configuration' page, **enter the following** and **click Next**:

Server Name	Name for the SonicWALL SRA
Server Private IP Address	'X0' IP address of the SRA appliance within your DMZ range, such as 10.1.1.200
Server Comment	Brief description of the server

7. On the 'Server Public Information' page, **accept the default IP address** or **enter an IP address** in your allowed public IP range. **Click Next**.



Note: *The default IP address is the WAN IP address of your SonicWALL firewall. If you accept this default, all HTTP and HTTPS traffic to this IP address will be routed to your SonicWALL SRA.*

8. The 'Public Server Configuration Summary' page displays all configuration actions that will be performed to create the public server. **Click Apply** to create the configuration and allow access from the WAN to the SonicWALL SRA on the DMZ.

Allowing DMZ -> LAN Connection

When users have connected to the SRA, they need to be able to connect to resources on the LAN.

1. Navigate to the **Network > Address Objects** page.
2. In the 'Address Objects' section, click .
3. In the 'Add Object' dialog box, **create an address object** for the X0 interface IP address of your SonicWALL SRA, then **click OK**.

Name	Name for the SonicWALL SRA
Zone Assignment	DMZ
Type	Host
IP Address	'X0' IP address of the SRA appliance within your DMZ range, such as 10.1.1.200

4. **Click** again to create an address object for the NetExtender range.

5. In the 'Add Object' dialog box, **create an address object** for the X0 interface IP address of your SonicWALL SRA, then **click OK**.

Name	Name for NetExtender
Zone Assignment	DMZ
Type	Range
Starting IP Address	Start of the NetExtender IP address range within your DMZ range, e.g., 10.1.1.220
Ending IP Address	End of the NetExtender IP address range within your DMZ range, e.g., 10.1.1.250

6. In the 'Address Groups' section, click .

7. In the 'Add Address Object Group' dialog box, **create a group** for the X0 interface IP address of your SonicWALL SRA and the NetExtender IP range, then **click OK**.
 - **Enter a name for the group.**
 - In the left column, **select the two groups you created** and **click the arrow button**  .



8. Navigate to the **Firewall > Access Rules** page.
9. On the 'Firewall > Access Rules' page in the matrix view, **click the DMZ > LAN icon**.
10. On the resulting 'Firewall > Access Rules' page, **click**



11. In the 'Add Rule' window, **create a rule** to allow access to the LAN for the address group you just created:

Action	Allow
From Zone	DMZ
To Zone	LAN
Service	Any
Source	Address group you just created, such as SonicWALL_SRA_Group
Destination	Any
Users Allowed	All
Schedule	Always on
Enable Logging	Selected
Allow Fragmented Packets	Selected

12. Click **OK** to create the rule.

Continue to ["Testing Your Remote Connection" on page 39](#)

Scenario C: SRA on the LAN

This section provides procedures to configure your gateway appliance based on Scenario C. This section contains the following subsections:

- [Connecting to a SonicWALL Security Appliance](#) - page 36
- [Configuring SRA -> LAN Connectivity](#) - page 36
- [Setting Public Server Access](#) - page 38

Connecting to a SonicWALL Security Appliance

1. Using a computer connected to your LAN, launch your Web browser and **enter the IP address** of your existing SonicWALL security appliance in the Location or Address field.
2. When the management interface displays, **enter your User Name** and **Password** in the appropriate fields and click **Login**.



Note: *Remember that you are logging into your SonicWALL security appliance, not the SonicWALL SRA.*

Configuring SRA -> LAN Connectivity

In order for users to access local resources through the SonicWALL SRA, you must configure your gateway device to allow an outside connection through the SRA into your LAN.

1. Navigate to the **Network > Address Objects** page.
2. In the 'Address Objects' section, click .
3. In the 'Add Object' dialog box, **create an address object** for the X0 interface IP address of your SonicWALL SRA, then **click OK**.

Name	Name for the SonicWALL SRA
Zone Assignment	SRA
Type	Host
IP Address	SonicWALL SRA's X0 IP address, 192.168.200.1 by default

4. **Click OK** to create the object.
5. **Click** again to create an address object for the NetExtender range.

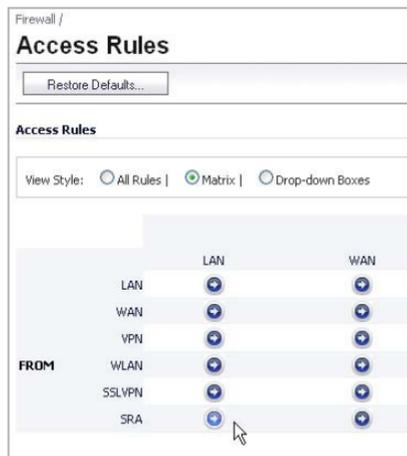
- In the 'Add Object' dialog box, **create an address object** for the X0 interface IP address of your SonicWALL SRA, then **click OK**.

Name	Name for NetExtender
Zone Assignment	SRA
Type	Range
Starting IP Address	Start of the NetExtender IP address range, 192.168.200.100 by default
Ending IP Address	End of the NetExtender IP address range, 192.168.200.200 by default

- On the 'Network > Address Objects' page, in the 'Address Groups' section, **click** .
- In the 'Add Address Object Group' dialog box, **create a group** for the X0 interface IP address of your SRA and the NetExtender IP range, then **click OK**.



- Navigate to the **Firewall > Access Rules** page, set the page to matrix view, and **click the SRA > LAN icon**.



- On the resulting 'Firewall > Access Rules' page, **click**



11. In the 'Add Rule' window, **create a rule** to allow access to the LAN for the address group you just created:

Action	Allow
From Zone	SRA
To Zone	LAN
Service	Any
Source	Address group just created , such as SonicWALL_SRA_Group
Destination	Any
Users Allowed	All
Schedule	Always on
Enable Logging	Selected
Allow Fragmented Packets	Selected

12. **Click OK** to finish creating the rule.

Setting Public Server Access

1. **Click the Wizards icon** in the top right corner of the SonicOS management interface.
2. Select the **Public Server Wizard** option and **click Next**.
3. Select **Web Server** from the Server Type drop-down menu.
4. **Select HTTP and HTTPS checkboxes**, and **click Next**.
5. **Enter SRA** in the Server Name field.
6. **Enter 192.168.168.200** (or the address you have configured to the SRA's X0 interface) in the Private IP field.
7. **Enter a comment**, such as "WAN to SRA" to describe your connection, and **click Next**.
8. Verify the Public Server field contains the correct IP address and **click Next**.
9. **Click Apply** to finish setting public server access.

Testing Your Remote Connection

You have now configured your SonicWALL security appliance and SonicWALL SRA for secure SSL-VPN remote access. This section provides instructions to verify your connection using a remote client on the WAN.

Verifying a User Connection from the Internet

1. From a WAN connection outside of your corporate network, launch a Web browser and **enter the following**:
https://<WAN_IP_address_of_gateway_device>
2. When prompted, **enter the User Name** and **Password** created in "[Adding a Local User](#)" on page 13 of this guide.
3. Select **LocalDomain** from the drop-down menu and **click Login**. The SonicWALL Virtual Office screen appears in your Web browser.



4. **Click NetExtender** to start the NetExtender client installation.
5. If prompted, **click Install** to complete the client installation.
6. **Ping a host on your corporate LAN** to verify your remote connection.

You have now successfully set up your SonicWALL SRA.



Tip: *It is easier for remote users to access the SonicWALL SRA appliance using an a fully qualified domain name (FQDN) rather than an IP address. It is recommended that you create a DNS record to allow for FQDN access to your SonicWALL SRA. If you do not manage your own public DNS servers, contact your ISP for assistance.*

In this Section:

This section provides procedures for upgrading an existing SRA SSL VPN image on a SonicWALL SRA 4200, 1200 to a newer version.

- [Obtaining the Latest SRA SSL VPN Image](#) - page 42
- [Exporting a Copy of Your Configuration Settings](#) - page 42
- [Uploading a New SRA SSL VPN Image](#) - page 43
- [Resetting the Appliance Using SafeMode](#) - page 44

Obtaining the Latest SRA SSL VPN Image

To obtain a new SRA SSL VPN image file for your SonicWALL security appliance, connect to your mysonicwall.com account at <<http://www.mysonicwall.com>>.



Note: *If you have already registered your SonicWALL SSL VPN appliance, and you selected **Notify me when new firmware is available** on the **System > Settings** page, you are automatically notified of any updates available for your model.*

Copy the new SRA SSL VPN image file to a directory on your management station. For the appliances, this is a file ending in “.sig” (a signed image).

Exporting a Copy of Your Configuration Settings

Before beginning the update process, export a copy of your SonicWALL SRA appliance configuration settings to your local machine. The Export Settings feature saves a copy of your current configuration settings on your SonicWALL SRA appliance, protecting all your existing settings in the event that it becomes necessary to return to a previous configuration state.



Note: *Exporting and Importing system configuration settings is supported when upgrading from a SonicWALL SSL-VPN 200/2000/4000 appliance to a SonicWALL SRA 1200/4200 appliance*

Perform the following procedures to save a copy of your configuration settings and export them to a file on your local management station:

1. Click the **Export Settings . . .** button on the **System > Settings** page and save the settings file to your local machine. The default settings file is named sslvpnSettings.zip.



Tip: *To more easily restore settings in the future, rename the .zip file to include the version of the SonicWALL SSL VPN image from which you are exporting the settings.*

Uploading a New SRA SSL VPN Image



Note: *SonicWALL SRA 4200/1200 appliances do not support downgrading an image and using the configuration settings file from a higher version. If you are downgrading to a previous version of a SRA SSL VPN image, you must select **Uploaded Firmware with Factory Defaults – New!** You can then import a settings file saved from the previous version or reconfigure manually.*

To upload new firmware on the appliance:

1. Download the SRA SSL VPN image file from www.mysonicwall.com and save it to a location on your local computer.
2. Select **Upload New Firmware** from the **System > Settings** page. Browse to the location where you saved the SRA SSL VPN image file, select the file, and click the **Upload** button. The upload process can take up to one minute.

On a SonicWALL SRA 4200/1200, you are ready to reboot your appliance with the new SRA SSL VPN image.

Do one of the following:

1. To reboot the image with current preferences, click the boot icon for the following entry:

Uploaded Firmware – New!

2. To reboot the image with factory default settings, click the boot icon for the following entry:

Uploaded Firmware with Factory Defaults – New!



Note: *Be sure to save a backup of your current configuration settings to your local machine before rebooting the SonicWALL SSL VPN appliance with factory default settings, as described in the previous “Saving a Backup Copy of Your Configuration Settings” section.*

3. A warning message dialog is displayed saying **Are you sure you wish to boot this firmware?** Click **OK** to proceed. After clicking OK, do not power off the device while the image is being uploaded to the flash memory.
4. After successfully uploading the image to your SonicWALL SSL VPN appliance, the login screen is displayed. The updated image information is displayed on the **System > Settings** page.

Resetting the Appliance Using SafeMode

If you are unable to connect to the SonicWALL security appliance's management interface, you can restart the SonicWALL security appliance in SafeMode. The SafeMode feature allows you to quickly recover from uncertain configuration states with a simplified management interface that includes the same settings available on the **System > Settings** page.

To reset the SonicWALL security appliance, perform the following steps:

1. Connect your management station to a LAN port on the SonicWALL security appliance and configure your management station IP address with an address on the 192.168.200.0/24 subnet, such as 192.168.200.20.



Note: *The SonicWALL security appliance can also respond to the last configured LAN IP address in SafeMode. This is useful for remote management recovery or hands off recovery in a datacenter.*

2. Use a narrow, straight object, like a straightened paper clip or a pen tip, to press and hold the reset button on the security appliance for five to ten seconds. The reset button is on the front panel in a small hole to the right of the USB connectors.



Tip: *If this procedure does not work while the power is on, turn the unit off and on while holding the reset button until the Test light starts blinking.*

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

3. Connect to the management interface by pointing the Web browser on your management station to **http://192.168.200.1**. The SafeMode management interface displays.
4. Try rebooting the SonicWALL security appliance with your current settings. Click the **boot** icon in the same line with Current Firmware.
5. After the SonicWALL security appliance has rebooted, try to open the management interface again. If you still cannot open the management interface, use the **reset** button to restart the appliance in SafeMode again. In SafeMode, restart the SRA SSL VPN image with the factory default settings. Click the **boot** icon in the same line with Current Firmware with Factory Default Settings.

In this Section:

This section provides overviews of customer support and training options for SonicWALL SRA appliances.

- [Customer Support](#) - page 46
- [Knowledge Base](#) - page 46
- [User Forums](#) - page 47
- [Training](#) - page 48
- [Related Documentation](#) - page 49
- [SonicWALL Live Product Demos](#) - page 50
- [SonicWALL Secure Wireless Network Integrated Solutions Guide](#) - page 51

Customer Support

SonicWALL's customer support Web site is where you will find featured support topics, tutorials, and more. If you need further assistance, SonicWALL offers telephone, email, and Web-based support to customers with valid Warranty Support or a purchased support contract. Please review our Warranty Support Policy for product coverage.

For answers to support questions, visit:
<<http://www.sonicwall.com/us/Support.html>>

The screenshot shows the SonicWALL Support website homepage. The navigation bar includes links for Products, Solutions, How to Buy, Support, and a sign-in/register option. The main content area is titled "Support for SonicWALL® Products and Services" and features a "Service Bulletins" section with a highlighted article about a vulnerability in E-Class SSL-VPN. Below this is a "Search the Knowledge Base" search bar. A sidebar on the left lists various support resources like "Support by Product", "Self-Help Resources", and "Support Services". At the bottom, there are sections for "Top Support Topics" and "Recent Video Tutorials", with a video thumbnail titled "How to Configure Standard Ports on a SonicWALL Firewall".

Knowledge Base

The Knowledge Base 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/kb.asp>>

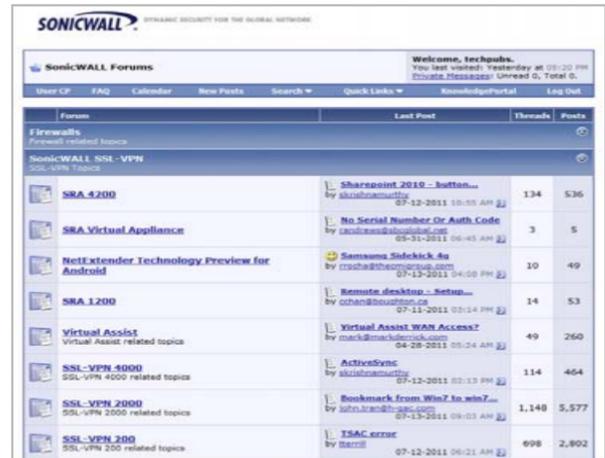
The screenshot shows the SonicWALL Knowledge Base search interface. The navigation bar is identical to the homepage. The main content area is titled "Support Knowledge Base" and features a search bar with a "Go" button. Below the search bar are several filters and options, including "Search Using Text", "Refine search by product", "Sort Search Results", and "Knowledge Base" filters. A sidebar on the left lists various support resources. At the bottom, there is a section for "Most Relevant Info For All Categories" with a list of search results.

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. Categories include:

- SSL-VPN topics
- VPN Client topics
- Continuous Data Protection topics
- Email Security topics
- Network Anti-Virus topics
- SonicPoint and Wireless topics

For further information, visit:
<<https://forum.sonicwall.com/>>



The screenshot shows the SonicWALL User Forums interface. At the top, there is a navigation bar with links for User CP, FAQ, Calendar, New Posts, Search, Quick Links, KnowledgePortal, and Log Out. A user greeting for 'teehubs' is visible in the top right corner. The main content area displays a list of forum topics under the 'SonicWALL SSL-VPN' category. Each row includes a topic title, a thumbnail icon, the author's name, the last post date and time, and the number of threads and posts.

Forum	Last Post	Threads	Posts
SonicWALL SSL-VPN SSL-VPN Topics			
SRA 4200	Sharepoint 2010 - button... by skishnamuthy 07-12-2011 10:05 AM	134	536
SRA Virtual Appliance	No Serial Number Or Auth Code by teehubs@sonicwall.com 05-31-2011 09:43 AM	3	5
NetExtender Technology Preview for Android	Samsung Sidekick 4g by rrs08@sonicwall.com 07-13-2011 04:50 PM	10	49
SRA 1200	Remote desktop - Setup... by cshan@sonicwall.com 07-11-2011 03:14 PM	14	53
Virtual Assist Virtual Assist related topics	Virtual Assist WAN Access? by mark@markderrick.com 04-28-2011 05:24 AM	49	260
SSL-VPN 4000 SSL-VPN 4000 related topics	ActiveSync by skishnamuthy 07-12-2011 02:13 PM	114	464
SSL-VPN 2000 SSL-VPN 2000 related topics	Bookmark from Win7 to win7... by jduhman@sonicwall.com 07-13-2011 09:03 AM	1,148	5,577
SSL-VPN 200 SSL-VPN 200 related topics	TSSAC error by Barm 07-12-2011 06:21 AM	698	2,902

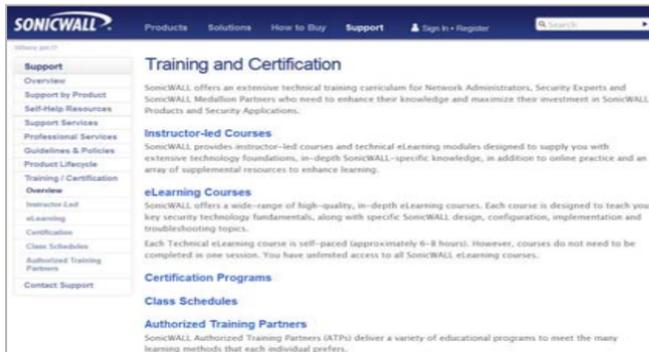
Training

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/training.html>>



The screenshot shows the SonicWALL website's 'Training and Certification' page. The page has a dark blue header with the SonicWALL logo and navigation links for Products, Solutions, How to Buy, Support, Sign In, and Register. A search bar is located in the top right corner. On the left side, there is a 'Support' menu with options: Overview, Support by Product, Self-Help Resources, Support Services, Professional Services, Guidelines & Policies, Product Lifecycle, and Training / Certification. The main content area is titled 'Training and Certification' and includes sections for 'Instructor-led Courses', 'eLearning Courses', 'Certification Programs', and 'Class Schedules'. The 'eLearning Courses' section mentions that each technical eLearning course is self-paced (approximately 6-8 hours) and that users have unlimited access to all SonicWALL eLearning courses. The 'Authorized Training Partners' section states that these partners deliver a variety of educational programs to meet the many learning methods that each individual prefers.

Related Documentation

See the following related documents for more information:

- *SonicOS SSL-VPN Administrator's Guide*
- *SonicOS SSL-VPN User's Guide*
- *SonicOS SSL-VPN Release Notes*
- *SonicOS SSL-VPN Feature Modules*
- *SonicOS Administrator's Guide*
- *SonicOS Feature Modules*
- *SonicWALL GMS Administrator's Guide*
- *SonicWALL ViewPoint Administrator's Guide*
- *SonicWALL GAV Administrator's Guide*
- *SonicWALL IPS Administrator's Guide*
- *SonicWALL Anti-Spyware Administrator's Guide*
- *SonicWALL Comprehensive Anti-Spam Services Guide*
- *SonicWALL CFS Administrator's Guide*
- *SonicWALL GVC Administrator's Guide*

For further information, visit:

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

The screenshot shows the SonicWall support website. The header includes the SonicWall logo and navigation links for Products, Solutions, How to Buy, Support, and Sign In/Register. A search bar is located in the top right. The main content area is titled "Support for SonicWALL® Products and Services" and features a "Service Bulletins" section with a highlighted vulnerability notice for E-Class SSL-VPN ActiveX Control format. Below this is a "Search the Knowledge Base" section with a search input field and a "Search" button. A navigation bar contains icons for Network Security, SSL VPN Secure Remote Access, Email Security, Backup & Recovery, Endpoint Security, and Management & Reporting. The "Top Support Topics" section lists several articles, including "How To Open Ports To Allow Access To A Server Behind The SonicWALL Device" and "UTM SSL VPN: How To Set Up SSL VPN (NetExtender Access On SonicOS Enhanced 5.2 Or Higher)". The "Recent Video Tutorials" section features a video thumbnail titled "How to Configure Standard Ports on a SonicWALL Firewall".

SonicWALL Live Product Demos

Get the most out of your appliance with the complete line of SonicWALL products. The SonicWALL Live Demo Site provides free test drives of SonicWALL security products and services through interactive live product installations:

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

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

SONICWALL Live Demo

Click an Appliance to Launch Demo

UTM / Firewall / VPN / GSM

Management & Reporting

SSL VPN Secure Remote Access

Backup & Recovery

Anti Spam & Email Security

SRA EX1600 Basic

SRA EX1600 Advanced

SSL VPN 2000

SSL VPN 4000 / Virtual Assist

SONICWALL SSL VPN Virtual Assist

Provide Live Desktop Support to Clients from Virtually Anywhere

Virtual Assist allows a technician to provide on-demand technical assistance for laptop or desktop issues to a customer using a Web browser's SSL connection.

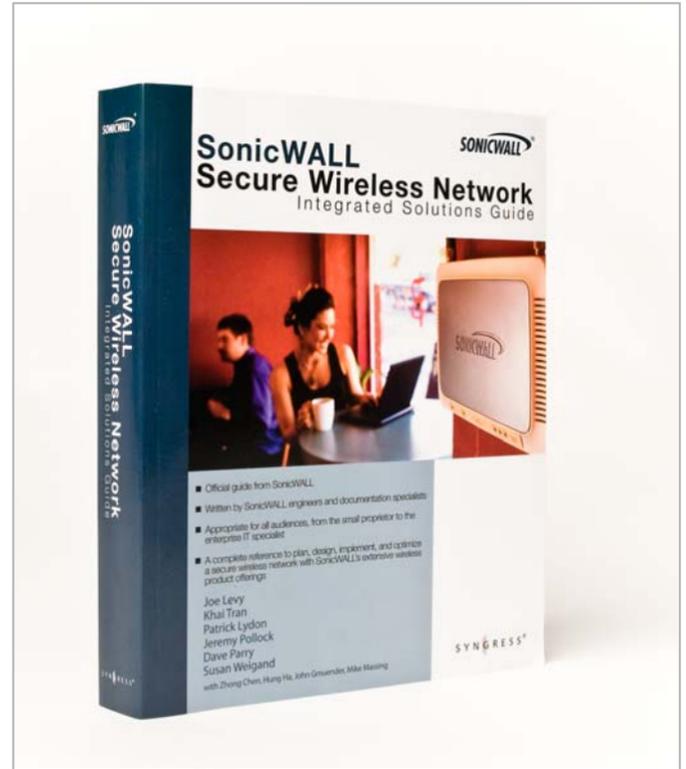
Installed at This Site:
SonicWALL SSL VPN 4000 with 4.0.0.3 firmware
Virtual Assist License

SONICWALL
Live Demonstration Site

SonicWALL Secure Wireless Network Integrated Solutions Guide

Looking to go wireless? Have questions about what it takes to build a truly “secure” wireless network? Check out the SonicWALL Secure Wireless Network Integrated Solutions Guide. This book is the official guide to SonicWALL’s market-leading wireless networking and security devices.

This title is available in hardcopy at fine book retailers everywhere, or by ordering directly from Elsevier Publishing at: <<http://www.elsevier.com>>



In this Section:

This section provides safety and regulatory information for the SonicWALL SRA 1200/4200 appliances.

- [SonicWALL SRA 1200/4200 Appliance Regulatory Statement and Safety Instructions](#) - page 54
- [Copyright Notice](#) - page 58
- [Trademarks](#) - page 58

SonicWALL SRA 1200/4200 Appliance Regulatory Statement and Safety Instructions

Regulatory Model/Type	Product Name
1RK23-088 1RK23-07C	SonicWALL SRA 1200 SonicWALL SRA 4200

This regulatory information can also be found in the electronic file, "**SonicWALL_SRA_Regulatory_Statement.pdf**," located on the SonicWALL Web site: <<http://www.sonicwall.com>>.

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 104° F (40° C).
- 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.
- If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient temperature. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum recommended ambient temperature shown above.
- 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

Das SonicWALL Modell ist 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 einen Ort im 19-Zoll-Rack, wo alle vier Befestigungen der Montageschienen verwendet werden.
- 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, dass sich die Netzkabel 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 Europäischen Union (EU) ist ein Netzkabel nicht im Lieferumfang enthalten.
- Stellen Sie sicher, dass das Gerät vor Wasser und höher 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.

- Wenn das Gerät in einem geschlossenen 19"-Gehäuse oder mit mehreren anderen Geräten eingesetzt ist, wird die Temperatur in der Gehäuse höher sein als die Umgebungstemperatur. Achten Sie darauf, daß die Umgebungstemperatur nicht mehr als 40 °C beträgt.
- Bringen Sie die SonicWALL waagrecht 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.
- Eine sichere Erdung der Geräte im Rack muss gewährleistet sein. 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.

Canadian Radio Frequency Emissions Statement

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

Complies with EN 55022 Class A and CISPR22 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.

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.

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) +A (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 (2006)

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

BMSI Statement (Class A)

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。

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

Regulatory Information for Korea



방송통신위원회

Ministry of Information and Telecommunication
Certification Numbers SWL-1RK23-07C and
SWL-1RK23-088

All products with country code "" (blank) and "A" 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 Secuwide, Corp.

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

© 2010 SonicWALL, Inc.

All rights reserved.

Under the copyright laws, this manual or the software described within, can not be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

Specifications and descriptions subject to change without notice.

Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.

Microsoft Windows Vista, Windows XP, Windows 2000, Windows NT, Windows Server 200, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Firefox is a trademark of the Mozilla Foundation.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Notes

Notes

SonicWALL, Inc.

2001 Logic Drive
San Jose, CA 95124-3452
www.sonicwall.com

P/N 232-000745-00
Rev A 7/2011

T +1 408.745.9600
F +1 408.745.9300



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™