▷ COMPREHENSIVE INTERNET SECURITY

SonicWALL Internet Security Appliances

SonicWALL SSL VPN 4000 Getting Started Guide

SONICWALL®

SonicWALL SSL VPN 4000 Appliance Getting Started Guide

This *Getting Started Guide* contains installation procedures and configuration guidelines for deploying a SonicWALL SSL VPN 4000 appliance into an existing or new network. This document addresses the most common use-case scenarios and network topologies in which the SonicWALL SSL VPN 4000 appliance can be deployed.

The SonicWALL SSL VPN 4000 appliance provides organizations of all sizes with an affordable, simple and secure remote network and application access solution that requires no pre-installed client software. Utilizing only a standard Web browser, users can easily and securely access email, files, intranets, applications and other resources on the corporate LAN from any location.

SonicWALL SSL VPN 4000 Configuration Steps

Note: *For complete documentation, refer to the SonicWALL SSL VPN Administrator’s Guide on the SonicWALL Resource CD or at:*

http://www.sonicwall.com/us/Support.html

Before You Begin

Check Package Contents

- One SonicWALL SSL VPN 4000 appliance
- One SonicWALL SSL VPN 4000 Getting Started Guide
- One SonicWALL SSL VPN Release Notes
- One straight-through Ethernet cable
- One crossover Ethernet cable (red)
- One rack-mount kit
- One power cord*
- One SonicWALL SSL VPN Series Resource CD, which contains:
  - SonicWALL SSL VPN 4000 Product Documentation
  - Software Utilities

Any Items Missing?

If any items are missing from your package, contact:

SonicWALL Support
Web: http://www.sonicwall.com/us/Support.html
Email: customer_service@sonicwall.com

** A power cord is included only with units shipped to North America.*

What You Need to Begin

- Administrative access to your network's gateway device, such as your SonicWALL Unified Threat Management (UTM) appliance, or your perimeter firewall
- A Windows, Linux, or MacOS computer to use as a management station for initial configuration of the SonicWALL SSL VPN 4000
- A Web browser supporting Java (version 1.4 or higher), and HTTP uploads, such as Internet Explorer 6.5 or higher, Firefox 1.0 or higher, Opera 7.0 or higher, or Safari 1.2 or higher is recommended**
- An Internet connection

*** While these browsers are acceptable for use in configuring your SonicWALL SSL VPN 4000, end users will need to use IE 6.5 or higher, Firefox 1.5 or higher, Opera 9.0 or higher, or Safari 2.0 or higher for supporting JavaScript, Java, cookies, SSL and ActiveX in order to take advantage of the full suite of applications.*

Network Configuration Information

Collect the following information about your current network configuration:

Primary DNS: ____________________________

Secondary DNS (optional): ____________________________

DNS Domain: ____________________________

WINS server(s) (optional): ____________________________

Other Information

These are the default settings for accessing your SonicWALL SSL VPN management interface:

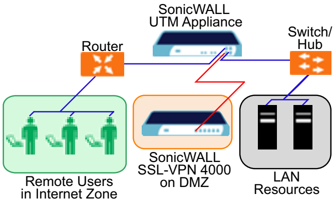
User Name: __*admin*__________________

Password: __________________________ (default: *password*)

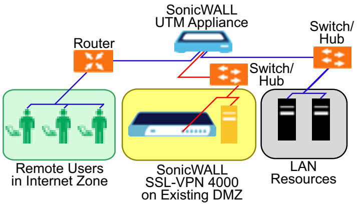
1 Selecting a SonicWALL Recommended Deployment Scenario

The deployment scenarios described in this section are based on actual customer deployments and are SonicWALL-recommended deployment best practices. This section describes three common deployments of the SonicWALL SSL VPN 4000. In Table 1, select the scenario that most closely matches your deployment.

Scenario A
SSL VPN on a New DMZ



Scenario B
SSL VPN on an Existing DMZ


SonicWALL UTM Appliance
Router
Switch/ Hub
Switch/ Hub
Remote Users in Internet Zone
SonicWALL SSL-VPN 4000 on Existing DMZ
LAN Resources

Scenario C
SSL VPN on the LAN

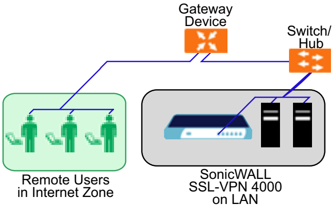
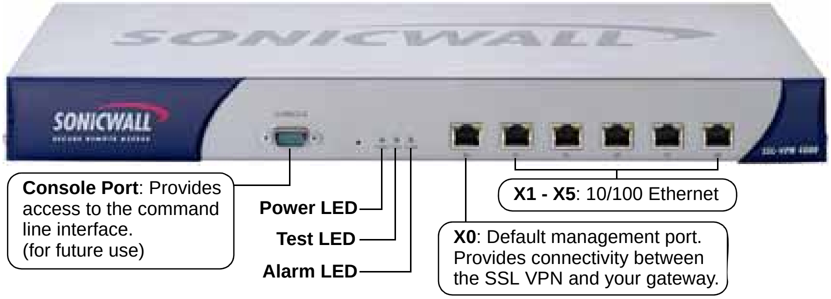


Table 1: SonicWALL SSL VPN 4000 Deployment Scenarios

Gateway Device	SonicWALL Recommended Deployment Scenarios	Conditions or Requirements
SonicOS Standard 3.1 or higher: TZ 170 TZ 180 Series PRO 1260 PRO 2040 PRO 3060	**Scenario A: SSL VPN on a New DMZ**	• OPT or X2 interface is unused • A new DMZ configured for either NAT or Transparent Mode operation. • (Optional) Plan to provide SonicWALL deep packet inspection security services such as GAV, IPS, and Anti-Spyware.
	Scenario B: SSL VPN on Existing DMZ	• OPT or X2 interface is in use with an existing DMZ • (Optional) Plan to provide SonicWALL deep packet inspection security services such as GAV, IPS, and Anti-Spyware.
SonicOS Enhanced 3.1 or higher: TZ 170 Series TZ 180 Series TZ 190 Series PRO Series NSA E-Class (SonicOS 5.0+) NSA Series (SonicOS 5.0+)	**Scenario A: SSL VPN on a New DMZ**	• OPT or unused interface • A new DMZ configured for either NAT or Transparent Mode operation.
	Scenario B: SSL VPN on Existing DMZ	• No unused interfaces • One dedicated interface in use as an existing DMZ
	Scenario C: SSL VPN on the LAN	• No unused interfaces • No dedicated interface for a DMZ
SonicOS Standard 3.1 or higher: TZ 150 Series TZ 170 Wireless TZ 170 SP SonicWALL devices running legacy firmware Third-Party Gateway Device	**Scenario C: SSL VPN on the LAN**	• Not planning to use SonicWALL deep packet inspection security services such as GAV, IPS, and Anti-Spyware. • Interoperability with a third-party gateway device

2 Applying Power to the SonicWALL SSL VPN 4000

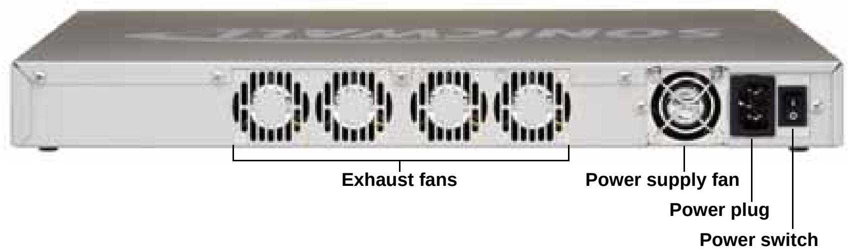
1. Plug the power cord into the SonicWALL SSL VPN 4000 and into an appropriate power outlet.
2. Turn on the power switch on the rear of the appliance next to the power cord.



Console Port: Provides access to the command line interface. (for future use)

X1 - X5: 10/100 Ethernet

X0: Default management port. Provides connectivity between the SSL VPN and your gateway.



The Power LED ● on the front panel lights up green when you turn on the SonicWALL SSL VPN 4000. 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 light is no longer lit, the SonicWALL SSL VPN 4000 is ready for configuration.

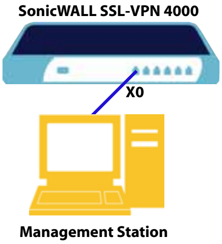
If the Test or Alarm LEDs remain lit or if the Test LED blinks red after the SonicWALL SSL VPN 4000 has booted, restart the SonicWALL SSL VPN 4000. For more troubleshooting information, refer to the *SonicWALL SSL VPN Administrator's Guide*.

Continue to Step 3

3 Accessing the Management Interface

To access the Web-based management interface of the SonicWALL SSL VPN 4000:

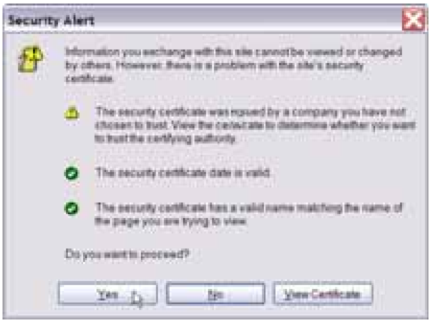
1. Connect one end of a crossover cable into the **X0** port of your SonicWALL SSL VPN 4000. Connect the other end of the cable into the computer you are using to manage the SonicWALL SSL VPN 4000.



2. Set the computer you use to manage the SonicWALL SSL VPN 4000 to have a static IP address in the **192.168.200.x/24** subnet, such as **192.168.200.20**. For help with setting up a static IP address on your computer, refer to “Configuring a Static IP Address” on page 58.

Alert: *A Web browser supporting Java and HTTP uploads, such as Internet Explorer 6.5 or higher, Firefox 1.0 or higher, Opera 7.0 or higher, or Safari 1.2 or higher is recommended.**

3. Open a Web browser and enter **http://192.168.200.1** (the default X0 management IP address) in the **Location** or **Address** field.
4. A security warning may appear. Click the **Yes** or **OK** button to continue.



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

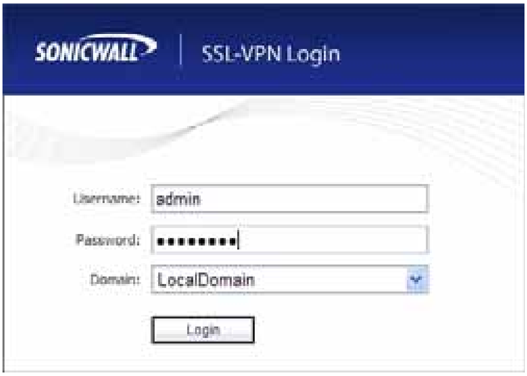
The security certificate date is valid.

The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

* *While these browsers are acceptable for use in configuring your SonicWALL SSL VPN 4000, end users will need to use IE 6.5 or higher, Firefox 1.5 or higher, Opera 9.0 or higher, or Safari 2.0 or higher in order to take advantage of the full suite of applications.*

5. The **SonicWALL SSL VPN management interface** 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.



Username: admin

Password: •••••••••

Domain: LocalDomain

Continue to Step 4

If You Cannot Login to the SSL VPN

If you cannot connect to the SonicWALL SSL VPN 4000, verify the following configurations:

- Did you plug your management workstation into the interface X0 on the SonicWALL SSL VPN appliance?
  Management can only be performed through X0.
- Is the link light lit on both the management station and the SonicWALL SSL VPN appliance?
- Did you correctly enter the SonicWALL SSL VPN 4000 management IP address in your Web browser?
- Is your computer set to a static IP address of 192.168.200.20? Refer to “Configuring a Static IP Address” on page 58 for instructions on setting your IP address.
- Is your Domain set to LocalDomain on the login screen?

4 Configuring Your SonicWALL SSL VPN 4000

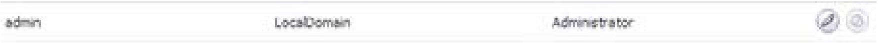
Once your SonicWALL SSL VPN 4000 is connected to a computer through the management port (X0), it can be configured through the Web-based management interface.

This section includes the following subsections:

- “Setting Your Administrator Password” on page 9
- “Adding a Local User” on page 9
- “Setting Time Zone” on page 10
- “Configuring SSL VPN Network Settings” on page 10
    - “Configuring DNS / WINS” on page 10
    - “Configuring the X0 IP address for Scenario B and Scenario C” on page 11
    - “Adding a NetExtender Client Route” on page 13

Setting Your Administrator Password

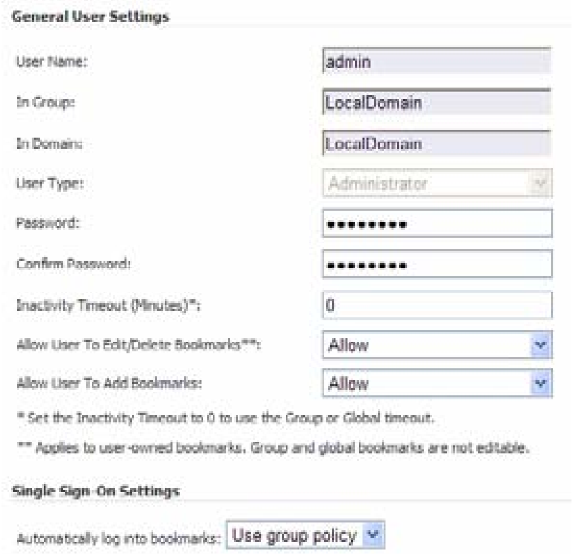
1. Select the **Users > Local Users** page
2. Click the **Configure** button ✎ corresponding to the “admin” account.



admin	LocalDomain	Administrator	✎ ⊘

Note: *Changing your password from the factory default is optional but strongly recommended. If you do change your password, be sure to keep it in a safe place. If you lose your password, you will have to reset the SonicWALL SSL VPN 4000 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
In Group:	LocalDomain
In Domain:	LocalDomain
User Type:	Administrator
Password:	•••••••••
Confirm Password:	•••••••••
Inactivity Timeout (Minutes)*:	0
Allow User To Edit/Delete Bookmarks**:	Allow
Allow User To Add Bookmarks:	Allow

* Set the Inactivity Timeout to 0 to use the Group or Global timeout.

** Applies to user-owned bookmarks. Group and global bookmarks are not editable.

Single Sign-On Settings

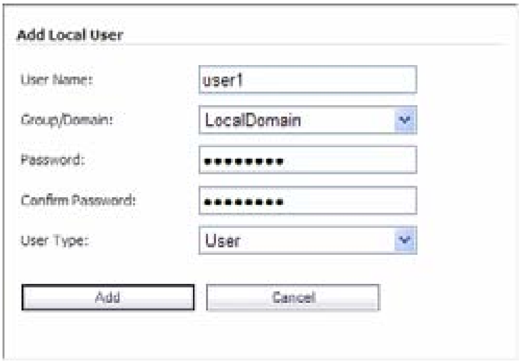
Automatically log into bookmarks: Use group policy

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

Adding a Local User

1. Select **Users > Local Users** page.
2. Click the **Add User** button.
3. Enter the desired user name in the **User Name** field.
4. Select LocalDomain from the **GroupDomain** drop-down menu.
5. Supply a password for the user in the **Password** field. Confirm the new password.

6. Select User from the **User Type** drop-down menu.



Add Local User

User Name: user1

Group/Domain: LocalDomain

Password: •••••••••

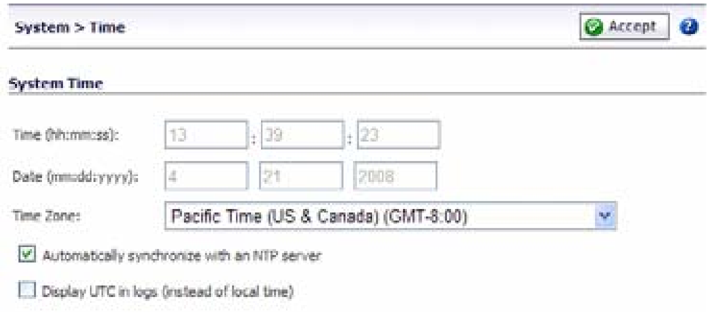
Confirm Password: •••••••••

User Type: User

7. Click the **Add** button.

Setting Time Zone

1. Select the **System > Time** page.
2. Select the appropriate time zone from the drop-down menu.



System > Time

System Time

Time (hh:mm:ss): 13 : 39 : 23

Date (mm:dd:yyyy): 4 21 2008

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 the **Accept** button.

Note: *Setting the time correctly is essential to many of the operations of the SonicWALL SSL VPN 4000. Be sure to set the time zone correctly. Automatic synchronization with an NTP server (default setting) is encouraged to ensure accuracy.*

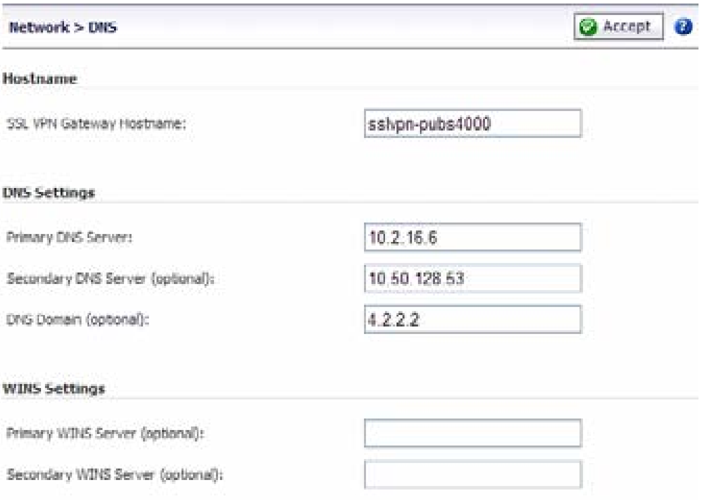
Configuring SSL VPN Network Settings

You will now configure your SSL VPN 4000 network settings. Refer to the notes you took in “Network Configuration Information” on page 3 to complete this section.

Configuring DNS / WINS

1. Select the **Network > DNS** page.
2. Enter a unique name for your SonicWALL SSL VPN 4000 in the **SSL VPN Gateway Hostname** field.

3. Enter your primary DNS server information in the **Primary DNS Server** field.
4. (Optional) Enter a secondary DNS server in the **Secondary DNS Server** field.



Hostname

SSL VPN Gateway Hostname: sslvpn-pubs4000

DNS Settings

Primary DNS Server: 10.2.16.6

Secondary DNS Server (optional): 10.50.128.53

DNS Domain (optional): 4.2.2.2

WINS Settings

Primary WINS Server (optional):

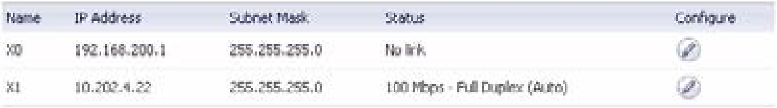
Secondary WINS Server (optional):

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

Configuring the X0 IP address for Scenario B and Scenario C

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

1. Select the **Network > Interfaces** page.
2. In the **Interfaces** table, click the **Configure** icon for the **X0** interface.



Name	IP Address	Subnet Mask	Status	Configure
X0	192.168.200.1	255.255.255.0	No link	✎
X1	10.202.4.22	255.255.255.0	100 Mbps - Full Duplex (Auto)	✎

3. In the **Interface Settings** dialog box, set the IP address and netmask to:

If you are using scenario:	Set the X0 interface to:
B - SSL VPN 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 - SSL VPN 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

When you click **OK**, you will lose your connection to the SSL VPN.

4. Reset the computer you use to manage the SonicWALL SSL VPN 4000 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**.

   For help with setting up a static IP address on your computer, refer to “Configuring a Static IP Address” on page 58.

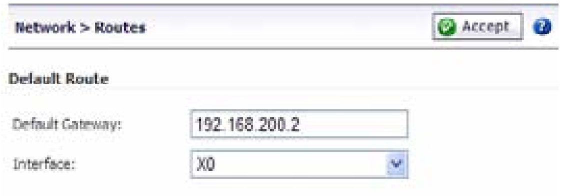
5. Log into the SSL VPN management interface again, using the IP address you just configured for the X0 interface. For example, point your browser to **http://192.168.168.200**.

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 SonicWALL Recommended Deployment Scenario” on page 4.

If you are using scenario:	**Your upstream gateway device will be:**
A - SSL VPN on a New DMZ	The DMZ you will create (for example, 192.168.200.2).
B - SSL VPN on an Existing DMZ	Your existing DMZ interface.
C - SSL VPN on the LAN	Your LAN gateway.

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



Network > Routes

Default Route

Default Gateway: 192.168.200.2

Interface: X0

4. Click the **Accept** button.

Adding a NetExtender Client Route

NetExtender allows remote clients to have seamless access to resources on your local network.

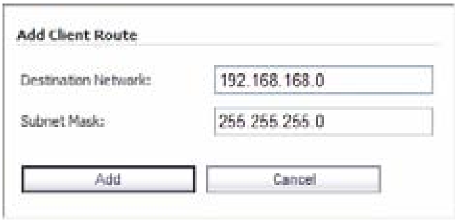
1. Select the **NetExtender > Client Routes** page.
2. Click the **Add Client Route** button.
3. Enter the IP address of the trusted network to which you would like to provide access with NetExtender in the **Destination Network** field. (For example, if you are connecting to an existing DMZ with the 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).

Note: *You can optionally tunnel-all SSL VPN client traffic through the NetExtender connection by entering 0.0.0.0 for the Destination Network and Subnet Mask.*

Some operating systems or system environments do not correctly apply the 0.0.0.0 default route. If this is the case, you may also specify tunnel-all operation by using two more specific routes as follows:

Route 1	Destination Network: **0.0.0.0** Subnet Mask: **128.0.0.0**
Route 2	Destination Network: **128.0.0.0** Subnet Mask: **128.0.0.0**

4. Enter your subnet mask in the **Subnet Mask** field.



Add Client Route

Destination Network: 192.168.168.0

Subnet Mask: 255.255.255.0

5. Click the **Add** button to add 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.

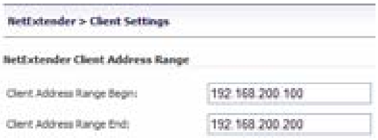
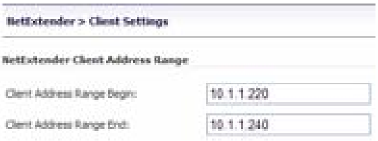
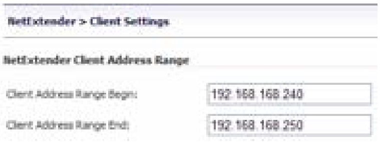
The range should fall within the same subnet as the interface to which the SonicWALL SSL VPN appliance is connected, and in cases where there are other hosts on the same segment as the SonicWALL SSL VPN appliance, it must not overlap or collide with any assigned addresses. You can determine the correct 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, perform the following steps:

1. Select 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)	 NetExtender > Client Settings NetExtender Client Address Range Client Address Range Begin: 192.168.200.100 Client Address Range End: 192.168.200.200
Scenario B	An unused range within your DMZ subnet.	 NetExtender > Client Settings NetExtender Client Address Range Client Address Range Begin: 10.1.1.220 Client Address Range End: 10.1.1.240
Scenario C	An unused range within your LAN subnet.	 NetExtender > Client Settings NetExtender Client Address Range Client Address Range Begin: 192.168.168.240 Client Address Range End: 192.168.168.250

Note: *If you have too few available addresses to support your desired number of concurrent NetExtender users you may use a new subnet for NetExtender. This condition might 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 SSL VPN 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.

Continue to Step 5

5 Connecting the SonicWALL SSL VPN 4000

Before continuing, reference the diagrams on the following pages to connect the SonicWALL SSL VPN 4000 to your network. Refer to the table in “Selecting a SonicWALL Recommended Deployment Scenario” on page 4 to determine the proper scenario for your network configuration.

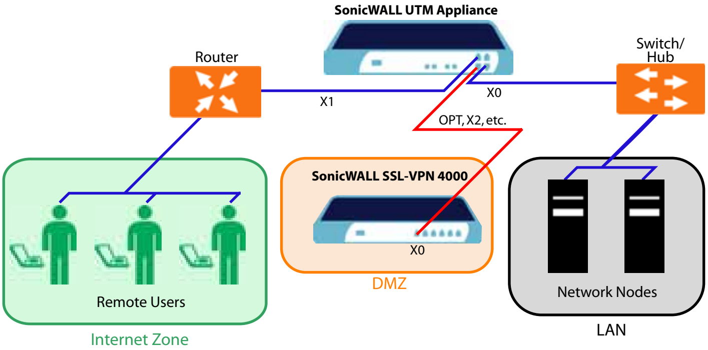
- “Scenario A: Connecting the SonicWALL SSL VPN 4000” on page 17
- “Scenario B: Configuring Your Network Interface” on page 18
- “Scenario B: Connecting the SonicWALL SSL VPN 4000” on page 19
- “Scenario C: Configuring Your Network Interface” on page 19
- “Scenario C: Connecting the SonicWALL SSL VPN 4000” on page 20

Scenario A: Connecting the SonicWALL SSL VPN 4000

To connect the SonicWALL SSL VPN 4000 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 UTM appliance.

Scenario A: SSL VPN on a New DMZ



2. Connect the other end of the Ethernet cable to the **X0** port on the front of your SonicWALL SSL VPN 4000. The **X0** Port LED lights up green indicating an active connection.

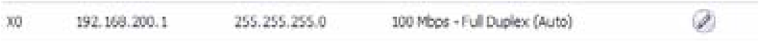
Continue to Step 6

Scenario B: Configuring Your Network Interface

Configure your SonicWALL SSL VPN 4000 to connect with your SonicWALL UTM appliance under network configurations given in Scenario B.

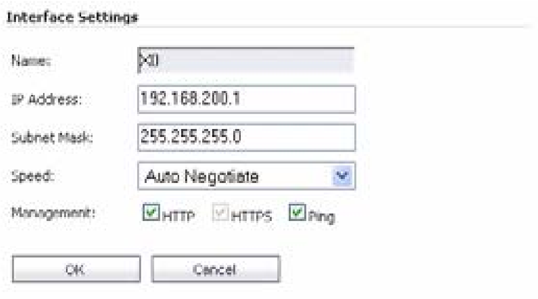
On your SonicWALL SSL VPN 4000:

1. Select the **Network > Interfaces** page.
2. Click the **Configure** button for the **X0** port.



X0	192.168.200.1	255.255.255.0	100 Mbps - Full Duplex (Auto)

3. If configuring with **Scenario B**, enter an unused IP address in your DMZ subnet in the **IP Address** field.
4. Enter your subnet mask in the **Subnet Mask** field.



Interface Settings

Name: X0

IP Address: 192.168.200.1

Subnet Mask: 255.255.255.0

Speed: Auto Negotiate

Management: ☑ HTTP ☑ HTTPS ☑ Ping

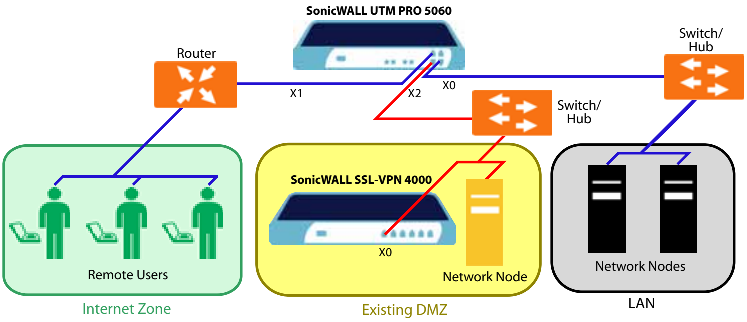
5. Click the **OK** button to apply changes.

Scenario B: Connecting the SonicWALL SSL VPN 4000

To connect the SonicWALL SSL VPN 4000 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 UTM appliance or to a hub or switch on your DMZ.

Scenario B: SSL VPN on an Existing DMZ



2. Connect the other end of the Ethernet cable to the **X0** port on the front of your SonicWALL SSL VPN 4000. The **X0** Port LED lights up green indicating an active connection.

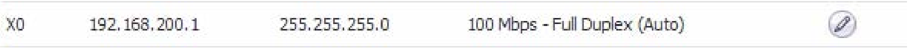
Continue to Step 6

Scenario C: Configuring Your Network Interface

Configure your SonicWALL SSL VPN 4000 to connect to your SonicWALL UTM appliance under network configurations given in Scenario C.

On the SonicWALL SSL VPN 4000:

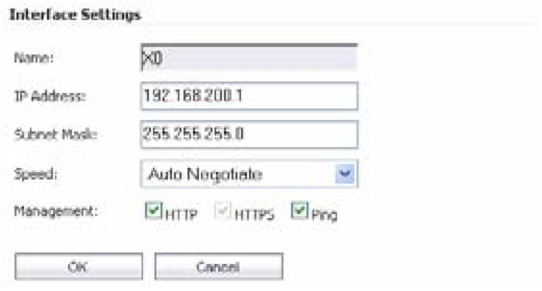
1. Select the **Network > Interfaces** page.
2. Click the **Configure** button for the **X0** port.



X0	192.168.200.1	255.255.255.0	100 Mbps - Full Duplex (Auto)

3. Enter an unused IP address in your LAN in the **IP Address** field.

4. Enter your subnet mask in the **Subnet Mask** field.



Interface Settings

Name: X0

IP Address: 192.168.200.1

Subnet Mask: 255.255.255.0

Speed: Auto Negotiate

Management: ☑ HTTP ☑ HTTPS ☑ Ping

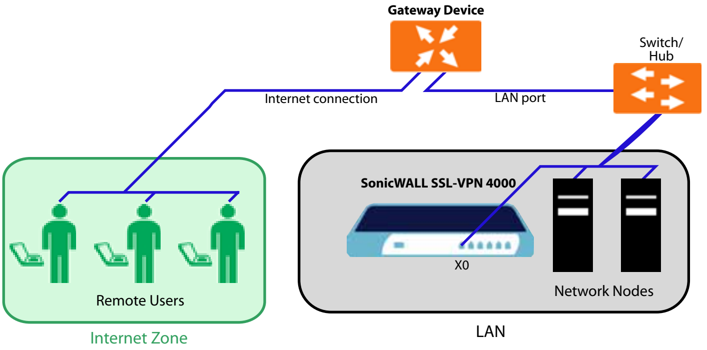
5. Click the **OK** button to apply changes.

Scenario C: Connecting the SonicWALL SSL VPN 4000

To connect the SonicWALL SSL VPN 4000 using Scenario C, perform the following steps:

1. Connect one end of a crossover cable to an **unused port** on your LAN hub or switch.

Scenario C: SSL VPN on the LAN



2. Connect the other end of the crossover cable to the **X0** port on the front of your SonicWALL SSL VPN 4000. The **X0** Port LED lights up green indicating an active connection.

Continue to Step 6

6 Configuring Your Gateway Device

Now that you have set up your SonicWALL SSL VPN 4000, you need to configure your gateway device to work with the SonicWALL SSL VPN 4000. Refer to the table in "Selecting a SonicWALL Recommended Deployment Scenario" on page 4 to determine the proper scenario for your network configuration.

This section contains the following subsections:

- "Scenario A: SSL VPN on a New DMZ" on page 21
- "Scenario B: SSL VPN on Existing DMZ" on page 35
- "Scenario C: SSL VPN on the LAN" on page 47

Scenario A: SSL VPN on a New DMZ

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

- "Scenario A: Connecting to the SonicWALL UTM Appliance" on page 21
- "Scenario A: Configuring a DMZ or OPT Port in SonicOS Standard" on page 22
- "Scenario A: Allowing WAN -> DMZ Connection in SonicOS Standard" on page 22
- "Scenario A: Allowing DMZ -> LAN Connection in SonicOS Standard" on page 24
- "Scenario A: Adding a New SSL VPN Custom Zone in SonicOS Enhanced" on page 28
- "Scenario A: Allowing WAN -> SSL VPN Connection in SonicOS Enhanced" on page 29
- "Scenario A: Allowing SSL VPN -> LAN Connection in SonicOS Enhanced" on page 32

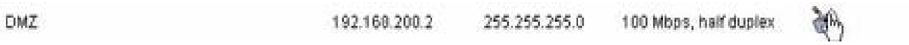
Scenario A: Connecting to the SonicWALL UTM Appliance

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

Note: *Remember that you are logging into your SonicWALL UTM appliance, not the SonicWALL SSL VPN 4000. Your user name and password combination may be different from the user name and password you recorded for your SonicWALL SSL VPN 4000.*

Scenario A: Configuring a DMZ or OPT Port in SonicOS Standard

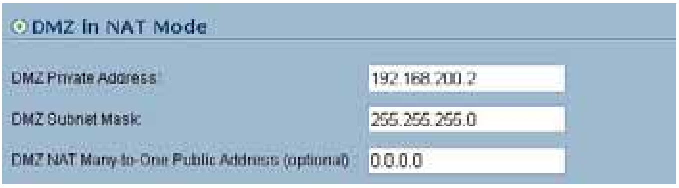
1. Select the **Network > Settings** page.
2. Click Configure button for the DMZ or OPT interface.



DMZ 192.168.200.2 255.255.255.0 100 Mbps, half duplex

Select the **DMZ in NAT Mode** radio button.

3. Enter **192.168.200.2** in the DMZ Private Address field.
4. Enter **255.255.255.0** in the DMZ Subnet Mask field.



● DMZ In NAT Mode

DMZ Private Address: 192.168.200.2

DMZ Subnet Mask: 255.255.255.0

DMZ NAT Many-to-One Public Address (optional): 0.0.0.0

5. Click the **OK** button.

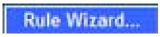
Scenario A: Allowing WAN -> DMZ Connection in SonicOS Standard

Follow this procedure if you are connecting the SonicWALL SSL VPN 4000 to a SonicWALL UTM appliance running **SonicOS Standard**. If your SonicWALL UTM appliance is running **SonicOS Enhanced**, skip to “Scenario A: Allowing WAN -> SSL VPN Connection in SonicOS Enhanced” on page 29

✓ **Tip:** *Leave the default rule to deny any access from WAN to DMZ in place, and use the Public Server Rule Wizard to create an access rule to allow HTTP and HTTPS specifically to the SonicWALL SSL VPN appliance. As you add different servers to the DMZ, you can use the wizard to create access to the new servers while still restricting all other traffic.*

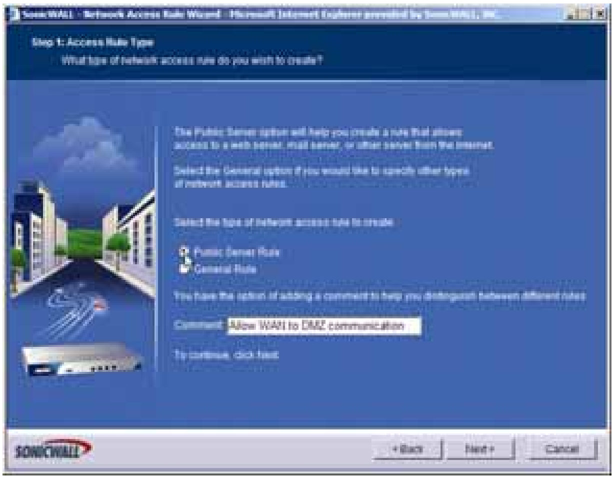
Note: *If you are allowing HTTP access to your SonicWALL SSL VPN appliance as well as HTTPS access, you need to run the wizard twice to create public server access rules for both HTTP and HTTPS.*

Create a public server access rule for HTTPS traffic:

1. Select the **Firewall > Access Rules** page.
2. Click  .

3. In the **Welcome to the SonicWALL Network Access Rules Wizard** page, click **Next.**

4. In the **Step 1: Access Rule Type** page, select **Public Server Rule** and click **Next**.



SonicWALL - Network Access Rule Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 1: Access Rule Type

What type of network access rule do you wish to create?

The Public Server option will help you create a rule that allows access to a web server, mail server, or other server from the Internet.

Select the General option if you would like to specify other types of network access rules.

Select the type of network access rule to create:

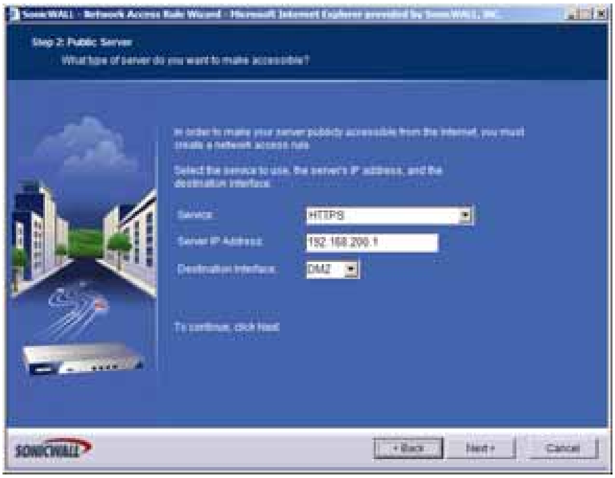
● Public Server Rule
○ General Rule

You have the option of adding a comment to help you distinguish between different rules

Comment: Allow WAN to DMZ communication

To continue, click Next.

5. In the **Step 2: Public Server** page, perform the following selections:



SonicWALL - Network Access Rule Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 2: Public Server

What type of server do you want to make accessible?

In order to make your server publicly accessible from the Internet, you must create a network access rule.

Select the service to use, the server's IP address, and the destination interface.

Service: HTTPS

Server IP Address: 192.168.200.1

Destination Interface: DMZ

To continue, click Next.

Service	**HTTPS**
Server IP Address	The X0 IP address of the SonicWALL SSL VPN appliance, **192.168.200.1** by default
Destination Interface	**DMZ**

Click **Next**.

6. In the **Congratulations** page, click **Apply** to create the rules and allow access from the WAN to the SonicWALL SSL VPN appliance on the DMZ.

If you are allowing HTTP access to the SonicWALL SSL VPN appliance, create a public server access rule for HTTP:

1. In the **Firewall > Access Rules** page, click Rule Wizard... .
2. In the **Welcome to the Network Access Rules Wizard** page, click **Next**.
3. In the **Step 1: Access Rule Type** page, select **Public Server Rule**. Click **Next.**
4. In the **Step 2: Public Server** page, perform the following selections and click **Next**:

Service	**Web (HTTP)**
Server IP Address	The X0 IP address of the SonicWALL SSL VPN appliance, **192.168.200.1** by default
Destination Interface	**DMZ**

5. In the **Congratulations** page, click **Apply** to create the rules and allow access from the WAN to the SonicWALL SSL VPN appliance on the DMZ.

Scenario A: Allowing DMZ -> LAN Connection in SonicOS Standard

When users have connected to the SSL VPN, they need to be able to connect to resources on the LAN. You need to create two rules--one to allow traffic from the SonicWALL SSL VPN appliances X0 interface to your LAN, and one to allow traffic from NetExtender to your LAN.

Note: *This procedure uses the Access Rule Wizard to create the rules. You can add the rules manually by clicking **Add** at the bottom of the **Firewall > Access Rules** page.*

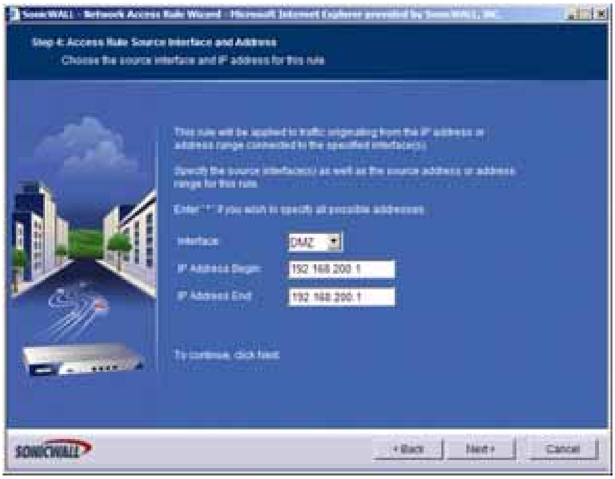
Create access to the LAN for the SSL VPN X0 interface:

1. In the **Firewall > Access Rules** page, click Rule Wizard... .
2. In the **Welcome to the SonicWALL Network Access Rules Wizard** page, click **Next**.
3. In the **Step 1: Access Rule Type** page, select **General Rule**. Click **Next**.
4. In the **Step 2: Access Rule Service** page, select **Any**. Click **Next**.
5. In the **Step 3: Access Rule Action** page configure:

Select Action for this Rule	**Allow**
TCP Connection Inactivity Timeout	**30** minutes

Click **Next.**

6. In the **Step 4: Access Rule Source Interface and Address** page, perform the following selections and click **Next**:



SonicWALL - Network Access Rule Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 4: Access Rule Source Interface and Address

Choose the source interface and IP address for this rule

This rule will be applied to traffic originating from the IP address or address range connected to the specified interface(s).

Specify the source interface(s) as well as the source address or address range for this rule.

Enter "*" if you wish to specify all possible addresses.

Interface: DMZ

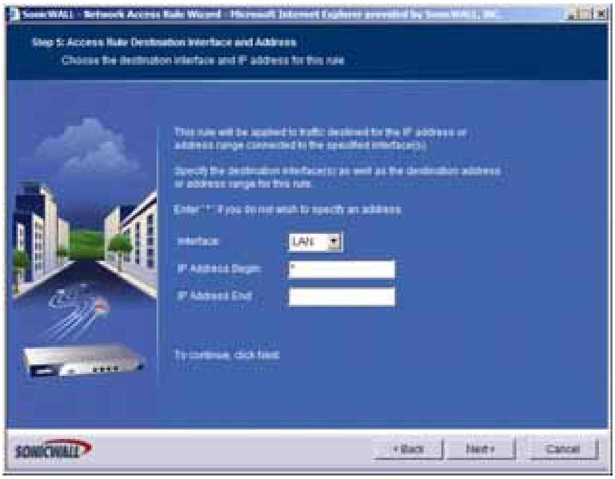
IP Address Begin: 192.168.200.1

IP Address End: 192.168.200.1

To continue, click Next.

Interface	DMZ
IP Address Begin	The X0 IP address of the SonicWALL SSL VPN appliance, **192.168.200.1** by default
IP Address End	The X0 IP address of the SonicWALL SSL VPN appliance, **192.168.200.1** by default

7. In the **Step 5: Access Rule Destination Interface and Address** page, perform the following selections and click **Next**:



SonicWALL - Network Access Rule Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 5: Access Rule Destination Interface and Address

Choose the destination interface and IP address for this rule

This rule will be applied to traffic destined for the IP address or address range connected to the specified interface(s).

Specify the destination interface(s) as well as the destination address or address range for this rule.

Enter "*" if you do not wish to specify an address.

Interface: LAN

IP Address Begin: *

IP Address End:

To continue, click Next.

Interface	LAN
IP Address Begin	*
IP Address End	Leave blank

8. In the **Step 6: Access Rule Time** page, leave **Time Active** set to **Always Active** unless you want to limit when you want SSL VPN clients to have access to the LAN.
9. In the **Congratulations** page, click **Apply** to create the access rule.

Create access to the LAN for NetExtender:

1. In the **Firewall > Access Rules** page, click Rule Wizard... .
2. In the **Welcome to the SonicWALL Network Access Rules** page, click **Next**.
3. In the **Step 1: Access Rule Type** page, select **General Rule**. Click **Next**.
4. In the **Step 2: Access Rule Service** page, select **Any**. Click **Next**.
5. In the **Step 3: Access Rule Action** page, configure:

Select Action for this Rule	**Allow**
TCP Connection Inactivity TImeout	**30** minutes

   Click **Next**.

6. In the **Step 4: Access Rule Source Interface and Address** page, perform the following selections and click **Next**:

Interface	**DMZ**
IP Address Begin	The beginning of the NetExtender range, default, **192.168.200.100**
IP Address End	The end of the NetExtender range, default, **192.168.200.200**

   Click **Next**.

7. In the **Step 5: Access Rule Destination Interface and Address** page, perform the following selections and click **Next**:

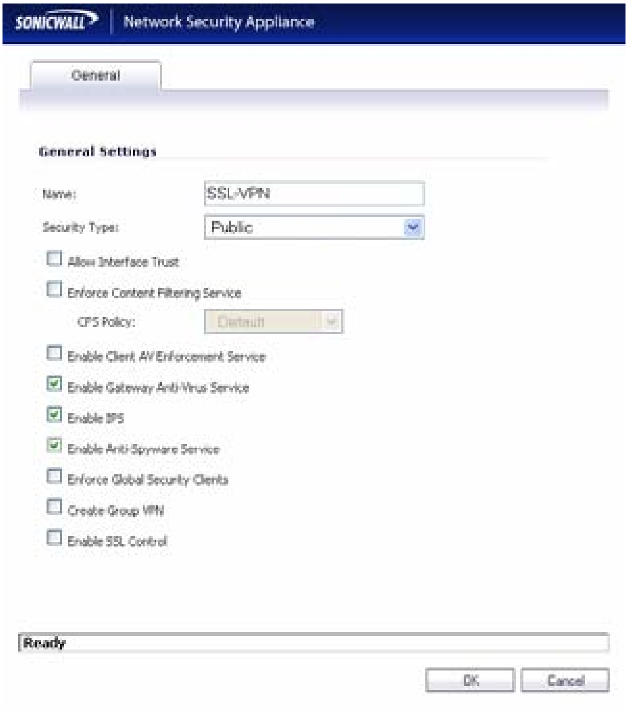
Interface	**LAN**
IP Address Begin	*****
IP Address End	Leave blank

8. In the **Step 6: Access Rule Time** page, leave **Time Active** set to **Always Active** unless you want to limit when you want SSL VPN clients to have access to the LAN.
9. In the **Congratulations** page, click **Apply** to create the access rule.

Continue to Step 7

Scenario A: Adding a New SSL VPN Custom Zone in SonicOS Enhanced

1. Select the **Network > Interfaces** page.
2. Click **Configure** button for the X2 interface (or any other available interface).
3. Select Create New Zone in **Zone** field. The **Add Zone** window opens.



General Settings

Name: SSL-VPN

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

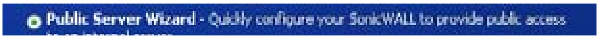
Ready

4. Enter SSL VPN in the **Name** field.
5. Select Public from the **Security Type** drop-down menu.
6. Un-check the **Allow Interface Trust** checkbox.
7. Check the **Gateway AV**, **Intrusion Prevention Service** and **Anti-Spyware** checkboxes.
8. Click the **OK** button.
9. 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 11).
10. Enter your subnet mask in the **Subnet Mask** field.
11. In the **Management** area, enable the desired management options.
12. Click the **OK** button to apply changes.

Scenario A: Allowing WAN -> SSL VPN Connection in SonicOS Enhanced

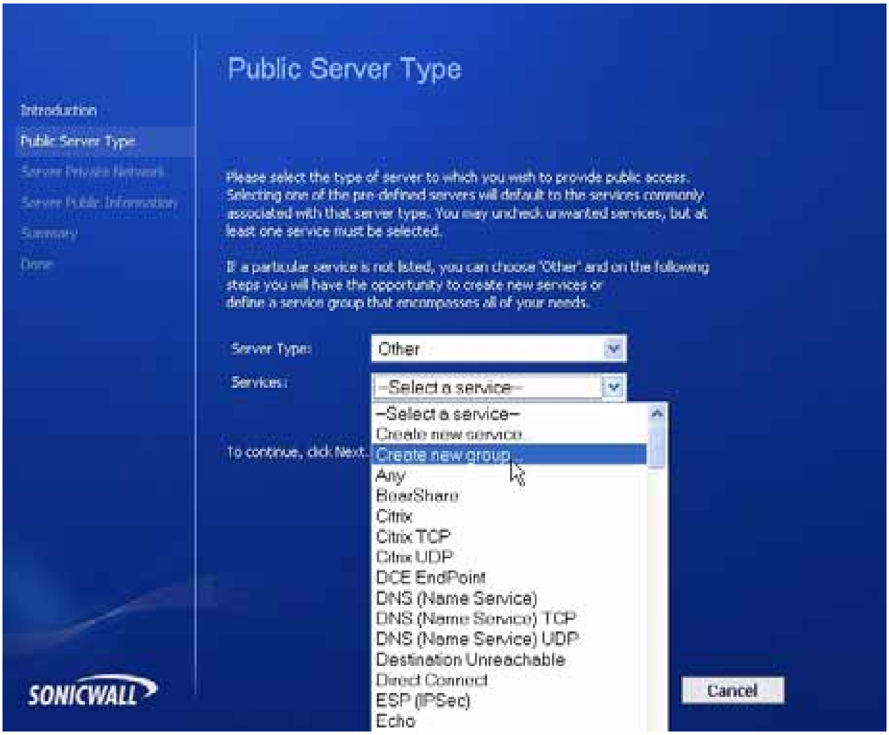
Follow this procedure if you are connecting your SonicWALL SSL VPN 4000 to a SonicWALL UTM appliance running **SonicOS Enhanced**. If your SonicWALL UTM appliance is running **SonicOS Standard**, refer to “Scenario A: Allowing WAN -> DMZ Connection in SonicOS Standard” on page 22.

Create a public server access rule for HTTP and HTTPS traffic:

1. Select the **Firewall > Access Rules** page.
2. Click 

Public Server Wizard - Quickly configure your SonicWALL to provide public access

 .
3. In the **Welcome to the SonicWALL Public Server Wizard** page, click **Next**.
4. In the **Step 1: Public Server Type** page, select:.



Public Server Type

Please select the type of server to which you wish to provide public access. Selecting one of the pre-defined servers will default to the services commonly associated with that server type. You may uncheck unwanted services, but at least one service must be selected.

If a particular service is not listed, you can choose 'Other' and on the following steps you will have the opportunity to create new services or define a service group that encompasses all of your needs.

Server Type: Other

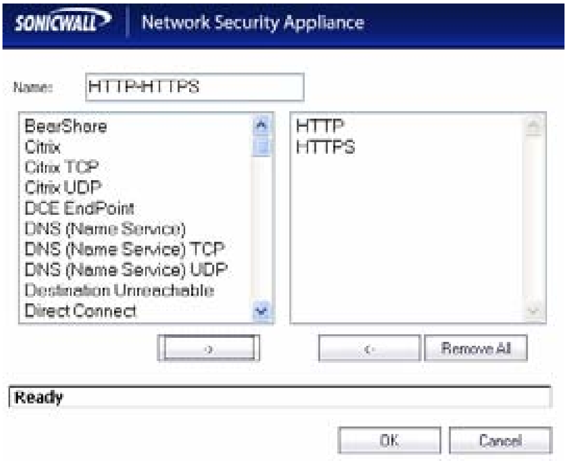
Services: --Select a service--

To continue, click Next.

Server Type	Other
Services	Create new group

The **Add Service Group** dialog box should display.

5. In the **Add Service Group** dialog box, create a service group for HTTP and HTTPS:



Name: HTTP-HTTPS

BearShare
Citrix
Citrix TCP
Citrix UDP
DCE EndPoint
DNS (Name Service)
DNS (Name Service) TCP
DNS (Name Service) UDP
Destination Unreachable
Direct Connect

HTTP
HTTPS

Ready

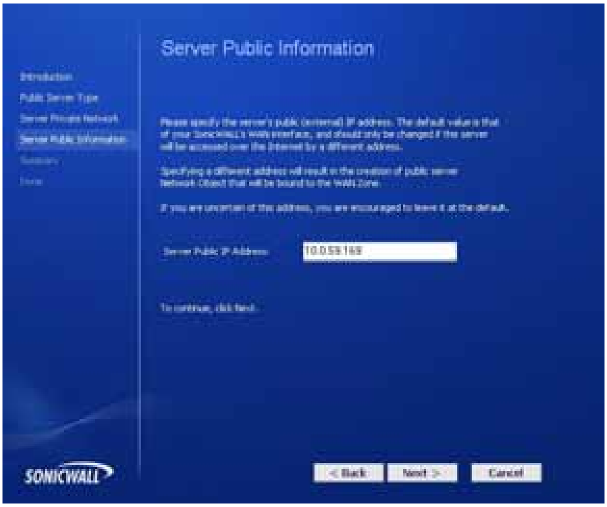
- Enter a name for the service.
- Select both HTTP and HTTPS and click -> .
- Click OK when both HTTP and HTTPS are in the right column.

6. In the **Step 2: Server Private Network Configuration** page, enter:

Server Name	A name for your SonicWALL SSL VPN 4000
Server Private IP Address	The X0 IP address of the SonicWALL SSL VPN appliance, **192.168.200.1** by default
Server Comment	A brief description of the server

Click **Next**.

7. In the **Step 3: Server Public Information** page, either accept the default IP address or enter an IP address in your allowed public IP range.



Server Public Information

Please specify the server's public (external) IP address. The default value is that of your SonicWALL's WAN interface, and should only be changed if the server will be accessed over the Internet by a different address.

Specifying a different address will result in the creation of public server Network Object that will be bound to the WAN Zone.

If you are uncertain of the address, you are encouraged to leave it at the default.

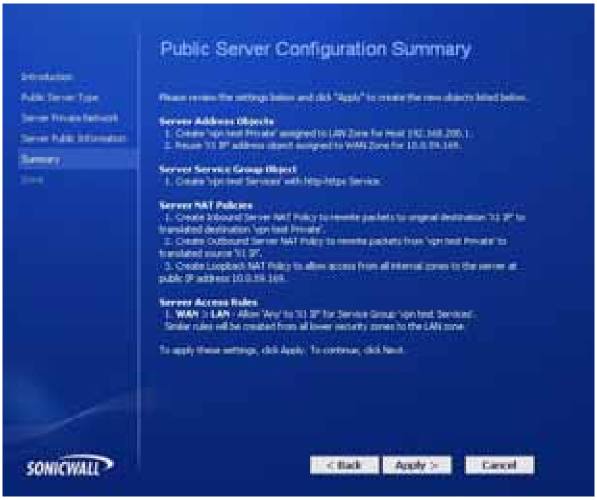
Server Public IP Address: 10.0.59.169

To continue, click Next.

Note: *The default IP address is the WAN IP address of your SonicWALL UTM appliance. If you accept this default, all HTTP and HTTPS traffic to this IP address will be routed to your SonicWALL SSL VPN 4000.*

Click **Next**.

8. The **Step 4: Public Server Configuration Summary** page displays all the configuration actions that will be performed to create the public server.



Public Server Configuration Summary

Please review the settings below and click "Apply" to create the new objects listed below.

Server Address Objects
1. Create 'vpn test Private' assigned to LAN Zone for Host 192.168.200.1.
2. Reuse 'X1 IP' address object assigned to WAN Zone for 10.0.59.169.

Server Service Group Object
1. Create 'vpn test Services' with http-https Service.

Server NAT Policies
1. Create Inbound Server NAT Policy to rewrite packets to original destination 'X1 IP' to translated destination 'vpn test Private'.
2. Create Outbound Server NAT Policy to rewrite packets from 'vpn test Private' to translated source 'X1 IP'.
3. Create Loopback NAT Policy to allow access from all internal zones to the server at public IP address 10.0.59.169.

Server Access Rules
1. **WAN > LAN** - Allow 'Any' to 'X1 IP' for Service Group 'vpn test Services'.
Similar rules will be created from all lower security zones to the LAN zone.

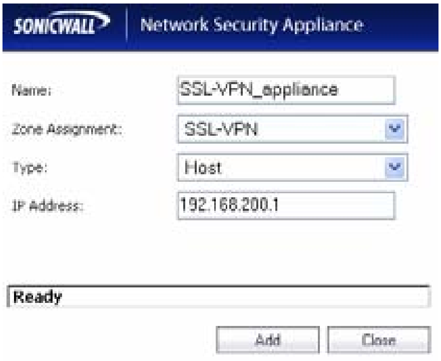
To apply these settings, click Apply. To continue, click Next.

Click **Apply** to create the configuration and allow access from the WAN to the SonicWALL SSL VPN 4000 on the DMZ.

Scenario A: Allowing SSL VPN -> LAN Connection in SonicOS Enhanced

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

1. In the administration interface, navigate to the **Network > Address Objects** page.
2. At the bottom of the page, below the **Address Objects** table, click Add .
3. In the **Add Object** dialog box, create an address object for the X0 interface IP address of your SonicWALL SSL VPN 4000:



Name: SSL-VPN_appliance
Zone Assignment: SSL-VPN
Type: Host
IP Address: 192.168.200.1

Ready

Name	Enter a name for the SonicWALL SSL VPN 4000
Zone Assignment	**SSL VPN**
Type	**Host**
IP Address	The SonicWALL SSL VPN 4000's X0 IP address, **192.168.200.1** by default

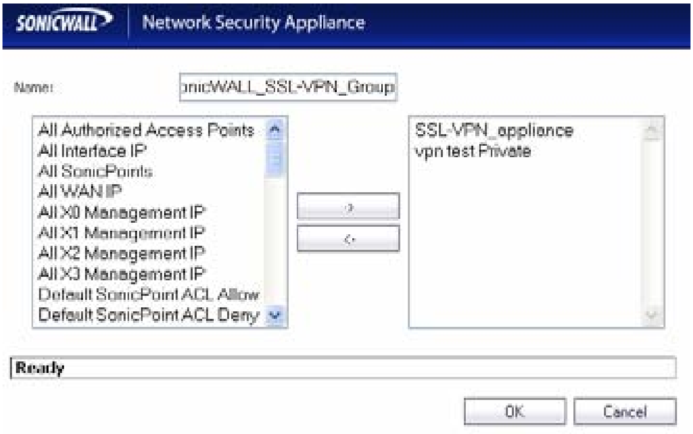
Click **OK** to create the object.

4. Click Add 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 SSL VPN 4000:

Name	Enter a name for NetExtender
Zone Assignment	**SSL VPN**
Type	**Range**
Starting IP Address	The start of the NetExtender IP address range, **192.168.200.100** by default
Ending IP Address	The end of the NetExtender IP address range, **192.168.200.200** by default

Click **OK** to create the object.

6. In the middle of the **Network > Address Objects** page, below the **Address Groups** table, click Add Group... .
7. In the **Add Address Object Group** dialog box, create a group for the X0 interface IP address of your SonicWALL SSL VPN 4000 and the NetExtender IP range:

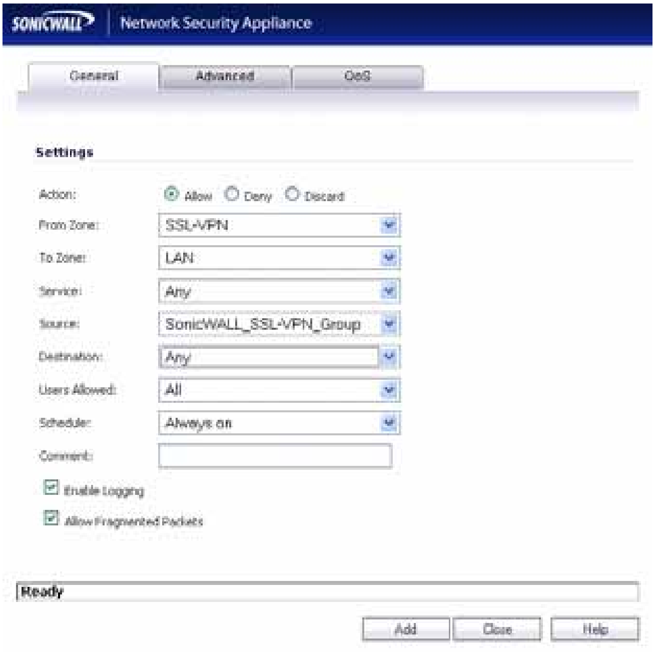


Name: onicWALL_SSL-VPN_Group

- Enter a name for the group.
- In the left column, select the two groups you created in steps 1 through 5, and click the arrow button -> .
- Click **OK** when both objects are in the right column to create the group.

8. In the administrative interface, navigate to the **Firewall > Access Rules** page.
9. At the bottom of the **Firewall > Access Rules** page, click Add... .

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



Settings

Action: ● Allow ○ Deny ○ Discard

From Zone: SSL-VPN

To Zone: LAN

Service: Any

Source: SonicWALL_SSL-VPN_Group

Destination: Any

Users Allowed: All

Schedule: Always on

Comment:

☑ Enable Logging

☑ Allow Fragmented Packets

Ready

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

Click **Add** to create the rule.

Continue to Step 7

Scenario B: SSL VPN on Existing DMZ

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

- "Scenario B: Connecting to the SonicWALL UTM Appliance" on page 35
- "Scenario B: Allowing WAN -> DMZ Connection in SonicOS Standard" on page 35
- "Scenario B: Allowing DMZ -> LAN Connection in SonicOS Standard" on page 37
- "Scenario B: Allowing WAN -> DMZ Connection in SonicOS Enhanced" on page 41
- "Scenario B: Allowing DMZ -> LAN Connection in SonicOS Enhanced" on page 44

Scenario B: Connecting to the SonicWALL UTM Appliance

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

Note: *Remember that you are logging into your SonicWALL UTM appliance, not the SSL VPN. Your user name and password combination may be different from the user name and password you recorded for your SSL VPN 4000.*

Scenario B: Allowing WAN -> DMZ Connection in SonicOS Standard

Follow this procedure if you are connecting the SonicWALL SSL VPN 4000 to a SonicWALL UTM appliance running **SonicOS Standard**. If your SonicWALL UTM appliance is running **SonicOS Enhanced**, skip to "Scenario A: Allowing WAN -> SSL VPN Connection in SonicOS Enhanced" on page 29.

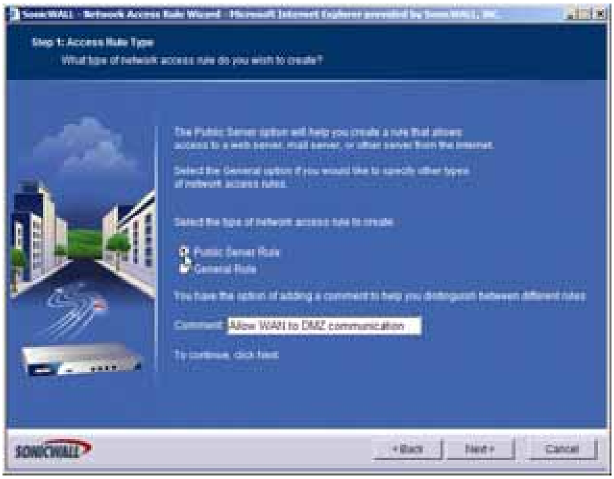
Note: *If you are allowing HTTP access to your SonicWALL SSL VPN appliance as well as HTTPS access, you need to run the wizard twice to create public server access rules for both HTTP and HTTPS.*

Create a public server access rule for HTTPS traffic:

1. Select the **Firewall > Access Rules** page.
2. Click

.
3. In the **Welcome to the SonicWALL Network Access Rules Wizard** page, click **Next**.

4. In the **Step 1: Access Rule Type** page, select **Public Server Rule** and click **Next**.



SonicWALL - Network Access Rule Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 1: Access Rule Type

What type of network access rule do you wish to create?

The Public Server option will help you create a rule that allows access to a web server, mail server, or other server from the Internet.

Select the General option if you would like to specify other types of network access rules.

Select the type of network access rule to create:

● Public Server Rule

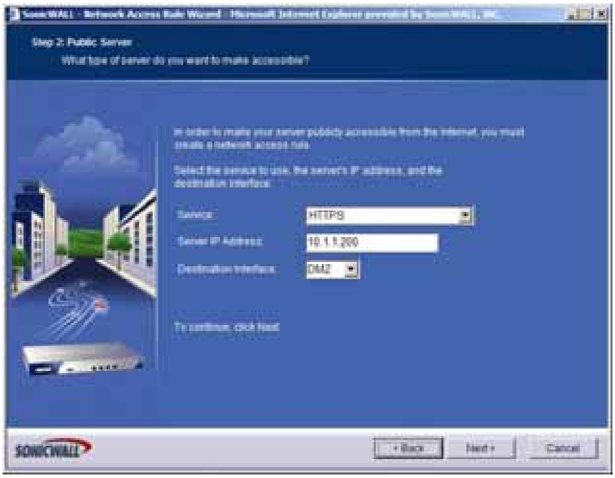
○ General Rule

You have the option of adding a comment to help you distinguish between different rules

Comment: Allow WAN to DMZ communication

To continue, click Next.

5. In the **Step 2: Public Server** page, perform the following selections:



SonicWALL - Network Access Rule Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 2: Public Server

What type of server do you want to make accessible?

In order to make your server publicly accessible from the Internet, you must create a network access rule.

Select the service to use, the server's IP address, and the destination interface.

Service: HTTPS

Server IP Address: 10.1.1.200

Destination Interface: DMZ

To continue, click Next.

Service	**HTTPS**
Server IP Address	The X0 IP address of the SonicWALL SSL VPN appliance within your DMZ range, for example **10.1.1.200**.
Destination Interface	**DMZ**

Click **Next**.

6. In the **Congratulations** page, click **Apply** to create the rules and allow access from the WAN to the SonicWALL SSL VPN appliance on the DMZ.

If you are allowing HTTP access to the SonicWALL SSL VPN appliance, create a public server access rule for HTTP:

1. In the **Firewall > Access Rules** page, click Rule Wizard... .
2. In the **Welcome to the Network Access Rules Wizard** page, click **Next**.
3. In the **Step 1: Access Rule Type** page, select **Public Server Rule**. Click **Next.**
4. In the **Step 2: Public Server** page, perform the following selections and click **Next**:

Service	**Web (HTTP)**
Server IP Address	The X0 IP address of the SonicWALL SSL VPN appliance within your DMZ range, for example **10.1.1.200**.
Destination Interface	**DMZ**

5. In the **Congratulations** page, click **Apply** to create the rules and allow access from the WAN to the SonicWALL SSL VPN appliance on the DMZ.

Scenario B: Allowing DMZ -> LAN Connection in SonicOS Standard

When users have connected to the SSL VPN, they need to be able to connect to resources on the LAN. You need to create two rules--one to allow traffic from the SonicWALL SSL VPN appliance's X0 interface to your LAN, and one to allow traffic from NetExtender to your LAN.

Note: *This procedure uses the Access Rule Wizard to create the rules. You can add the rules manually by clicking **Add** at the bottom of the **Firewall > Access Rules** page.*

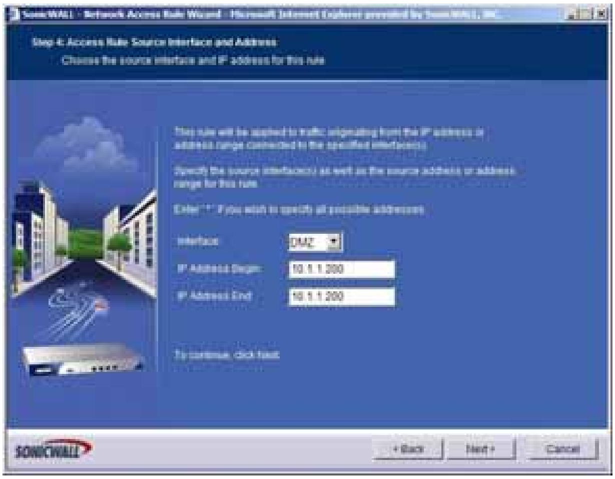
Create access to the LAN for the SSL VPN X0 interface:

1. In the **Firewall > Access Rules** page, click Rule Wizard... .
2. In the **Welcome to the SonicWALL Network Access Rules Wizard** page, click **Next**.
3. In the **Step 1: Access Rule Type** page, select **General Rule**. Click **Next**.
4. In the **Step 2: Access Rule Service** page, select **Any**. Click **Next**.
5. In the **Step 3: Access Rule Action** page, configure:

Select Action for this Rule	**Allow**
TCP Connection Inactivity Timeout	**30** minutes

Click **Next**.

6. In the **Step 4: Access Rule Source Interface and Address** page, perform the following selections and click **Next**:



SonicWALL - Network Access Rule Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 4: Access Rule Source Interface and Address

Choose the source interface and IP address for this rule

This rule will be applied to traffic originating from the IP address or address range connected to the specified interface(s).

Specify the source interface(s) as well as the source address or address range for this rule.

Enter "*" if you wish to specify all possible addresses.

Interface: DMZ

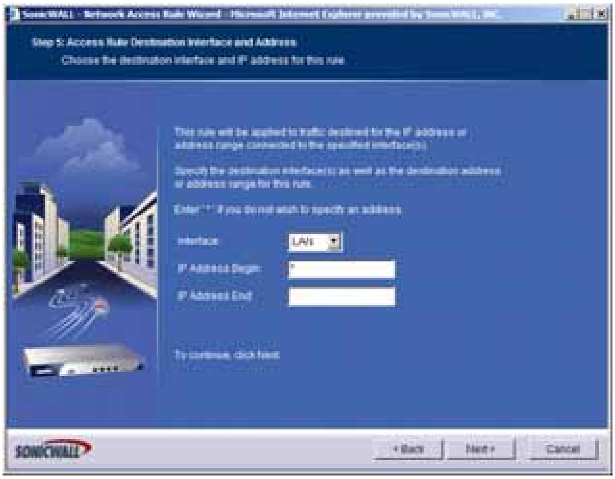
IP Address Begin: 10.1.1.200

IP Address End: 10.1.1.200

To continue, click Next.

Interface	DMZ
IP Address Begin	The X0 IP address of the SonicWALL SSL VPN appliance within your DMZ range, for example **10.1.1.200**.
IP Address End	The X0 IP address of the SonicWALL SSL VPN appliance, the same as above, for example **10.1.1.200**.

7. In the **Step 5: Access Rule Destination Interface and Address** page, perform the following selections and click **Next**:



SonicWALL - Network Access Rule Wizard - Microsoft Internet Explorer provided by SonicWALL, INC.

Step 5: Access Rule Destination Interface and Address

Choose the destination interface and IP address for this rule

This rule will be applied to traffic destined for the IP address or address range connected to the specified interface(s).

Specify the destination interface(s) as well as the destination address or address range for this rule.

Enter "*" if you do not wish to specify an address

Interface: LAN

IP Address Begin: *

IP Address End:

To continue, click Next.

Interface	LAN
IP Address Begin	*
IP Address End	Leave blank

8. In the **Step 6: Access Rule Time** page, leave **Time Active** set to **Always Active** unless you want to limit when you want SSL VPN clients to have access to the LAN.
9. In the **Congratulations** page, click **Apply** to create the access rule.

Create access to the LAN for NetExtender:

1. In the **Firewall > Access Rules** page, click Rule Wizard... .
2. In the **Welcome to the SonicWALL Network Access Rules** page, click **Next.**
3. In the **Step 1: Access Rule Type** page, select **General Rule**. Click **Next**.
4. In the **Step 2: Access Rule Service** page, select **Any**. Click **Next.**
5. In the **Step 3: Access Rule Action** page, configure:

Select Action for this Rule	**Allow**
TCP Connection Inactivity Timeout	**30** minutes

   Click **Next.**

6. In the **Step 4: Access Rule Source Interface and Address** page, perform the following selections and click **Next**:

Interface	**DMZ**
IP Address Begin	The beginning of the NetExtender range within your DMZ range, for example, **10.1.1.220**
IP Address End	The end of the NetExtender range within your DMZ range, for example, **10.1.1.250**

   Click **Next.**

7. In the **Step 5: Access Rule Destination Interface and Address** page, perform the following selections and click **Next**:

Interface	**LAN**
IP Address Begin	*
IP Address End	Leave blank

8. In the **Step 6: Access Rule Time** page, leave **Time Active** set to **Always Active** unless you want to limit when you want SSL VPN clients to have access to the LAN.
9. In the **Congratulations** page, click **Apply** to create the access rule.

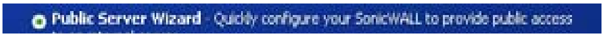
Continue to Step 7

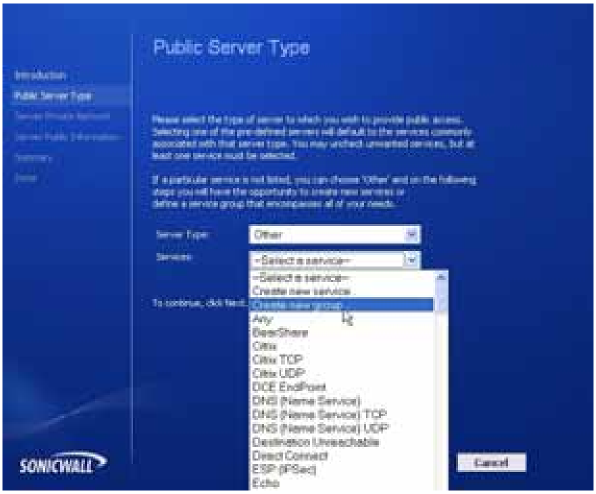
Scenario B: Allowing WAN -> DMZ Connection in SonicOS Enhanced

Follow this procedure if you are connecting your SonicWALL SSL VPN 4000 to a SonicWALL UTM appliance running **SonicOS Enhanced**. If your SonicWALL UTM appliance is running **SonicOS Standard**, refer to “Scenario A: Allowing WAN -> DMZ Connection in SonicOS Standard” on page 22.

Create a public server access rule for HTTP and HTTPS traffic:

Note: *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 SSL VPN appliance, because both cannot concurrently use the same IP address and port combinations.*

1. Select the **Firewall > Access Rules** page.
2. Click  .
Public Server Wizard - Quickly configure your SonicWALL to provide public access
3. In the **Welcome to the SonicWALL Public Server Wizard** page, click **Next.**
4. In the **Step 1: Public Server Type** page, select:.



Public Server Type

Please select the type of server to which you wish to provide public access. Selecting one of the pre-defined servers will default to the services commonly associated with that server type. You may uncheck unwanted services, but at least one service must be selected.

If a particular service is not listed, you can choose 'Other' and on the following steps you will have the opportunity to create new services or define a service group that encompasses all of your needs.

Server Type: Other

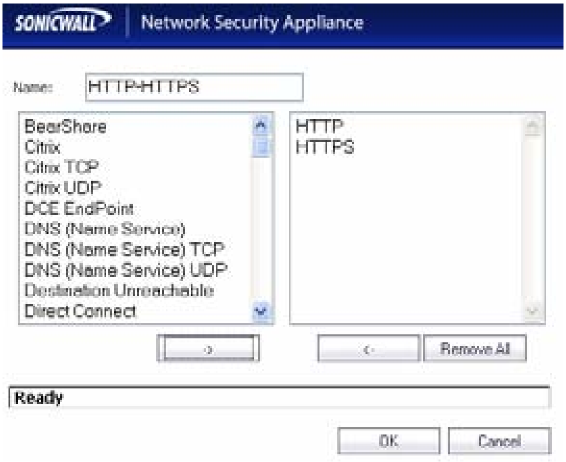
Services: --Select a service--

To continue, click Next.

Server Type	Other
Services	Create new group

The **Add Service Group** dialog box should display.

5. In the **Add Service Group** dialog box, create a service group for HTTP and HTTPS:



Name: HTTP-HTTPS

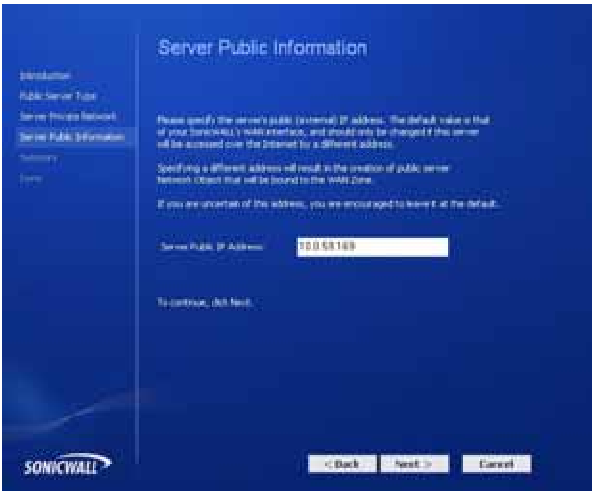
- Enter a name for the service.
- Select both **HTTP** and **HTTPS** and click →.
- Click **OK** when both **HTTP** and **HTTPS** are in the right column.

6. In the **Step 2: Server Private Network Configuration** page, enter:

Server Name	A name for your SonicWALL SSL VPN 4000
Server Private IP Address	The X0 IP address of the SonicWALL SSL VPN appliance within your DMZ range, for example, **10.1.1.200**
Server Comment	A brief description of the server

Click **Next**.

7. In the **Step 3: Server Public Information** page, either accept the default IP address or enter an IP address in your allowed public IP range.



Server Public Information

Please specify the server's public (external) IP address. The default value is that of your SonicWALL's WAN interface, and should only be changed if the server will be accessed over the Internet by a different address.

Specifying a different address will result in the creation of public server Network Object that will be bound to the WAN Zone.

If you are uncertain of this address, you are encouraged to leave it at the default.

Server Public IP Address: 10.0.58.169

To continue, click Next.

Note: *The default IP address is the WAN IP address of your SonicWALL UTM appliance. If you accept this default, all HTTP and HTTPS traffic to this IP address will be routed to your SonicWALL SSL VPN 4000.*

Click **Next**.

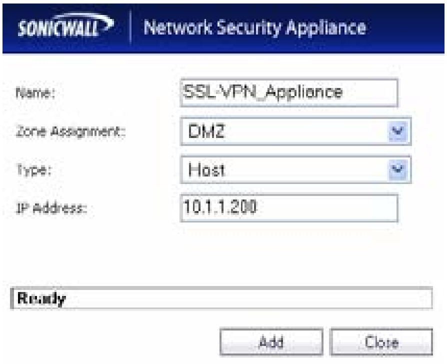
8. The Step 4: Public Server Configuration Summary page displays all the configuration actions that will be performed to create the public server.

   Click **Apply** to create the configuration and allow access from the WAN to the SonicWALL SSL VPN 4000 on the DMZ.

Scenario B: Allowing DMZ -> LAN Connection in SonicOS Enhanced

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

1. In the administration interface, navigate to the **Network > Address Objects** page.
2. At the bottom of the page, below the **Address Objects** table, click Add .
3. In the **Add Object** dialog box, create an address object for the X0 interface IP address of your SonicWALL SSL VPN 4000:



Name: SSL-VPN_Appliance
Zone Assignment: DMZ
Type: Host
IP Address: 10.1.1.200

Ready

Name	Enter a name for the SonicWALL SSL VPN 4000
Zone Assignment	**DMZ**
Type	**Host**
IP Address	The SonicWALL SSL VPN 4000’s X0 interface IP address within your DMZ range, for example, **10.1.1.200**

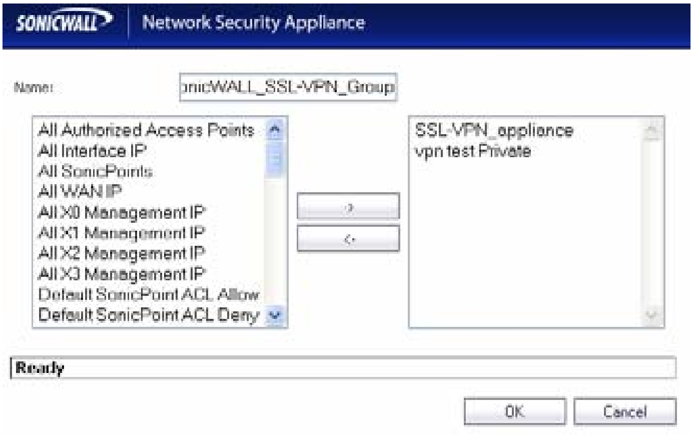
Click **OK** to create the object.

4. Click Add 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 SSL VPN 4000:

Name	Enter a name for NetExtender
Zone Assignment	**DMZ**
Type	**Range**
Starting IP Address	The start of the NetExtender IP address range within your existing DMZ range, for example, **10.1.1.220**
Ending IP Address	The end of the NetExtender IP address range within your existing DMZ range, for example, **10.1.1.250**

Click **OK** to create the object.

6. In the middle of the **Network > Address Objects** page, below the **Address Groups** table, click Add Group... .
7. In the **Add Address Object Group** dialog box, create a group for the X0 interface IP address of your SonicWALL SSL VPN 4000 and the NetExtender IP range:



Name: onicWALL_SSL-VPN_Group

All Authorized Access Points
All Interface IP
All SonicPoints
All WAN IP
All X0 Management IP
All X1 Management IP
All X2 Management IP
All X3 Management IP
Default SonicPoint ACL Allow
Default SonicPoint ACL Deny

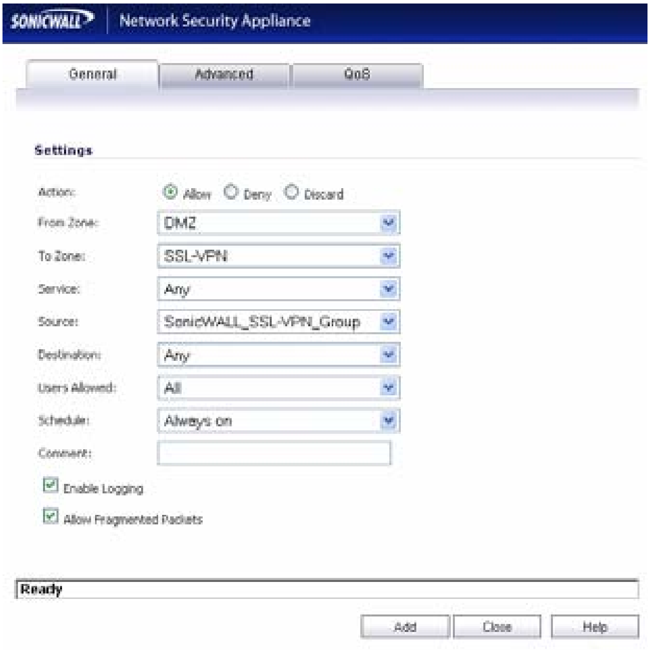
SSL-VPN_appliance
vpn test Private

Ready

- Enter a name for the group.
- In the left column, select the two groups you created in steps 1 through 5, and click the arrow button -> .
- Click **OK** when both objects are in the right column to create the group.

8. In the administrative interface, navigate to the **Firewall > Access Rules** page.
9. At the bottom of the **Firewall > Access Rules** page, click Add... .

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



Settings

Action: ● Allow ○ Deny ○ Discard

From Zone: DMZ

To Zone: SSL-VPN

Service: Any

Source: SonicWALL_SSL-VPN_Group

Destination: Any

Users Allowed: All

Schedule: Always on

Comment:

☑ Enable Logging

☑ Allow Fragmented Packets

Ready

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

Click **OK** to create the rule.

Continue to Step 7

Scenario C: SSL VPN on the LAN

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

- “Scenario C: Connecting to the SonicWALL UTM Appliance” on page 47
- “Scenario C: Configuring Your Gateway to Recognize the SonicWALL SSL VPN 4000” on page 47
- “Scenario C: Configuring SSL VPN -> LAN Connectivity” on page 47
- “Scenario C: Setting Public Server Access in SonicOS Standard” on page 48
- “Scenario C: Setting Public Server Access in SonicOS Enhanced” on page 49

Scenario C: Connecting to the SonicWALL UTM Appliance

Using a computer connected to your LAN, launch your Web browser and log in to your current gateway interface.

Scenario C: Configuring Your Gateway to Recognize the SonicWALL SSL VPN 4000

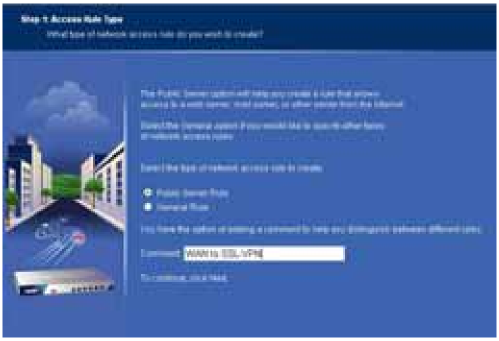
Complete the following steps to configure your gateway to recognize and allow the SonicWALL SSL VPN 4000 connection.

Scenario C: Configuring SSL VPN -> LAN Connectivity

In order for users to access local resources through the SonicWALL SSL VPN 4000, you must configure your gateway device to allow an outside connection through the SSL VPN into your LAN.

Scenario C: Setting Public Server Access in SonicOS Standard

1. Select **Wizards** in the left navigation bar.
2. Click the **Network Access Rules Wizard** option and press the **Next** button.
3. Select **Public Server Rule**.
4. Enter a comment, such as “WAN to SSL VPN” to describe your connection.



Step 1: Access Rule Type

What type of network access rule do you wish to create?

The Public Server option will help you create a rule that allows access to a web server, mail server, or other server from the Internet.

Select the General option if you would like to specify other types of network access rules.

Select the type of network access rule to create.

● Public Server Rule

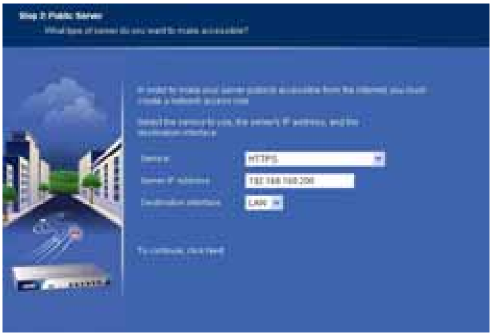
○ General Rule

You have the option of adding a comment to help you distinguish between different rules.

Comment: WAN to SSL VPN

To continue, click Next.

5. Click the **Next** button to continue the Wizard.
6. Select **HTTPS** from the **Service** drop-down list.
7. Enter **192.168.168.200** (or the IP address to which you have configured your X0 interface on your SonicWALL SSL VPN appliance) in the **Private IP** field.
8. Select **LAN** or **DMZ** in the Destination Interface drop-down list. The destination interface will depend on your deployment configuration.



Step 2: Public Server

What type of server do you want to make accessible?

In order to make your server publicly accessible from the Internet, you must create a network access rule.

Select the service you use, the server's IP address, and the destination interface.

Service: HTTPS

Server IP Address: 192.168.168.200

Destination Interface: LAN

To continue, click Next.

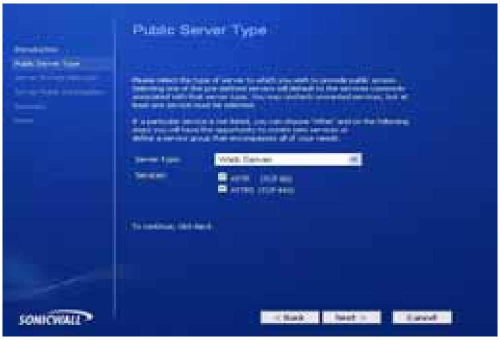
9. Click the **Next** button.
10. Click the **Apply** button to save changes.

✓ **Tip:** *If you wish to support automatic redirection of your SSL VPN users from HTTP to HTTPS, you should repeat the Public Server Rule Wizard process for the HTTP service.*

Continue to Step 7

Scenario C: Setting Public Server Access in SonicOS Enhanced

1. Select **Wizards** in the left navigation bar.
2. Click the **Public Server Wizard** option and press the **Next** button.
3. Select **Web Server** from the **Server Type** drop-down menu.
4. Select **HTTP** and **HTTPS** checkboxes.



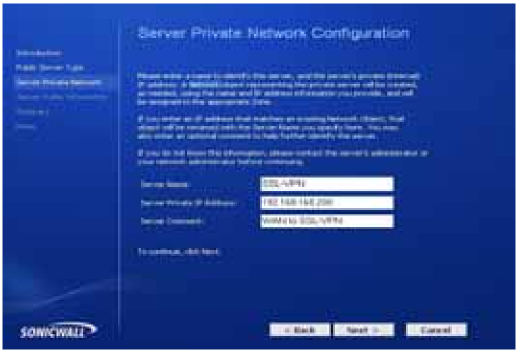
Public Server Type

Server Type: Web Server

Services: ☑ HTTP (TCP 80) ☑ HTTPS (TCP 443)

To continue, click Next.

5. Click the **Next** button to continue the Wizard.
6. Enter **SSL VPN** in the **Server Name** field.
7. Enter **192.168.168.200** (or the address to which you have configured your X0 interface on your SonicWALL SSL VPN appliance) in the **Private IP** field.
8. Enter a comment, such as “WAN to SSL VPN” to describe your connection.



Server Private Network Configuration

Server Name: SSL-VPN

Server Private IP Address: 192.168.168.200

Server Comment: WAN to SSL-VPN

To continue, click Next.

9. Click the **Next** button to continue the Wizard.
10. Verify that the **Public Server** field contains the correct IP address (You can generally leave this at the default setting).
11. Click the **Next** button.
12. Click the **Apply** button.

Continue to Step 7

7 Testing Your SSL VPN Connection

Now you have configured your SonicWALL UTM appliance and SonicWALL SSL VPN 4000 for secure SSL VPN remote access.This section provides instructions to verify your SSL VPN connection using a remote client on the WAN.

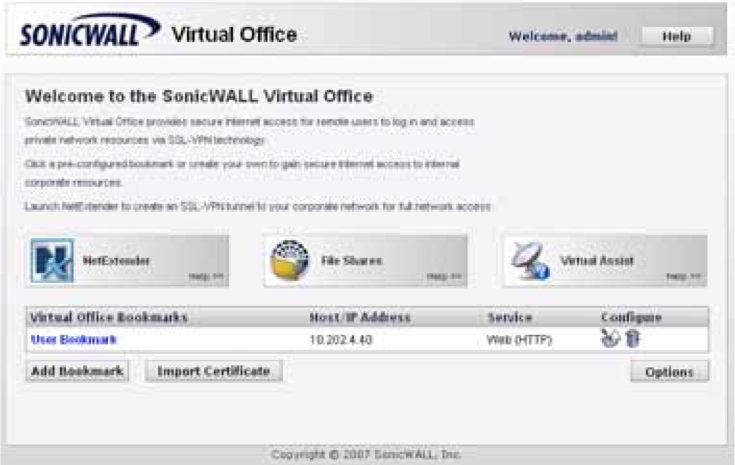
Verifying a User Connection from the Internet

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>*____________________

Note: *It will be easier for your remote users to access the SonicWALL SSL VPN appliance using an FQDN (fully qualified domain name) rather than an IP address. For example, browsing to “http://www.sonicwall.com” is simpler than browsing to “http://64.41.140.167”. It is therefore recommended, if you have not already done so, that you create a DNS record to allow for FQDN access to your SonicWALL SSL VPN appliance. If you do not manage your own public DNS servers, contact your Internet Service Provider for assistance.*

For configurations where your ISP provides dynamic IP addressing rather than a static IP address, refer to the steps in “Configuring Dynamic DNS” on page 51 to set up DDNS for your remote users.

2. When prompted, enter the **User Name** and **Password** created in “Adding a Local User” on page 9 of this guide.
3. Select **LocalDomain** from the drop-down menu and click the **Login** button. The SonicWALL Virtual Office screen appears in your Web browser.



Welcome to the SonicWALL Virtual Office

SonicWALL Virtual Office provides secure Internet access for remote users to log in and access private network resources via SSL-VPN technology.

Click a pre-configured bookmark or create your own to gain secure Internet access to internal corporate resources.

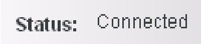
Launch NetExtender to create an SSL-VPN tunnel to your corporate network for full network access.

Virtual Office Bookmarks	Host/IP Address	Service	Configure
User Bookmark	10.202.4.40	Web (HTTP)	

Copyright © 2007 SonicWALL, Inc.

4. Select **NetExtender** from the left navigation bar. This will start the NetExtender client installation.

5. Click the **NetExtender** button and complete the client installation. When complete, the following message is displayed:


Status: Connected

6. Ping a host on your corporate LAN to verify your SSL VPN remote connection.

Congratulations! You have successfully set up your SonicWALL SSL VPN 4000.

Continue to Step 8

8 Registering Your SonicWALL SSL VPN 4000

Before You Register

Verify that the time, DNS, and default route settings on your SonicWALL SSL VPN are correct before you register your appliance. To verify or configure the time settings, navigate to the **System > Time** page. To verify or configure the DNS setting, navigate to the **Network > DNS** page. To verify or configure the default route, navigate to the **Network > Routes** page.

You need a mySonicWALL.com account to register the SonicWALL SSL VPN 4000. You can create a new mySonicWALL.com account directly from the SonicWALL management interface.

Note: *mySonicWALL.com registration information is not sold or shared with any other company.*

Creating a MySonicWALL Account from System > Licenses

1. On the System > Licenses page, click **Activate, Upgrade, or Renew services**. The License Management page is displayed.
2. If you do not have a MySonicWALL account or if you forgot your user name or password, click the **https://www.mysonicwall.com** link at the bottom of the page. The **MySonicWALL User Login** page is displayed.

   Do one of the following:

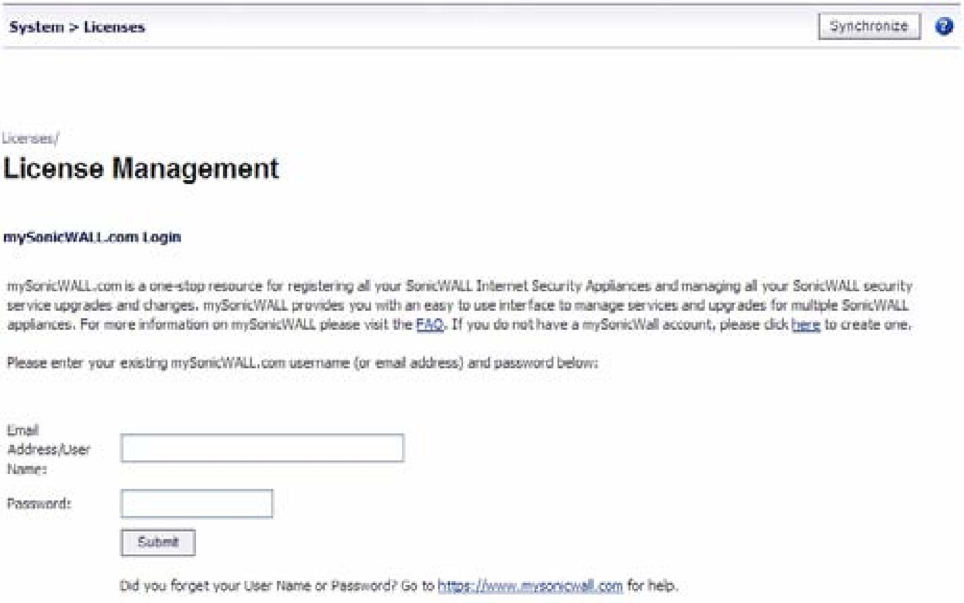
   - If you forgot your user name, click the **Forgot Username?** link.
   - If you forgot your password, click the **Forgot Password?** link.
   - If you do not have a MySonicWALL account, click the **Not a registered user?** link.
3. Follow the instructions to activate your MySonicWALL account.

Registering with MySonicWALL

On a new SonicWALL SSL VPN appliance or after upgrading to SonicWALL SSL VPN 3.0 firmware from an earlier release, you can register your appliance from the **System > Licenses** page.

1. If you are not logged into the SonicWALL SSL VPN 4000 management interface, log in with the username ***admin*** and the administrative password you set in the Setup Wizard.
2. To navigate to the **System > Licenses** page, click **System** in the left-navigation menu, and then click **Licenses**.

3. On the System > Licenses page, click **Activate, Upgrade, or Renew services**. The **License Management** page is displayed.



Licenses/

License Management

mySonicWALL.com Login

mySonicWALL.com is a one-stop resource for registering all your SonicWALL Internet Security Appliances and managing all your SonicWALL security service upgrades and changes. mySonicWALL provides you with an easy to use interface to manage services and upgrades for multiple SonicWALL appliances. For more information on mySonicWALL please visit the FAQ. If you do not have a mySonicWall account, please click here to create one.

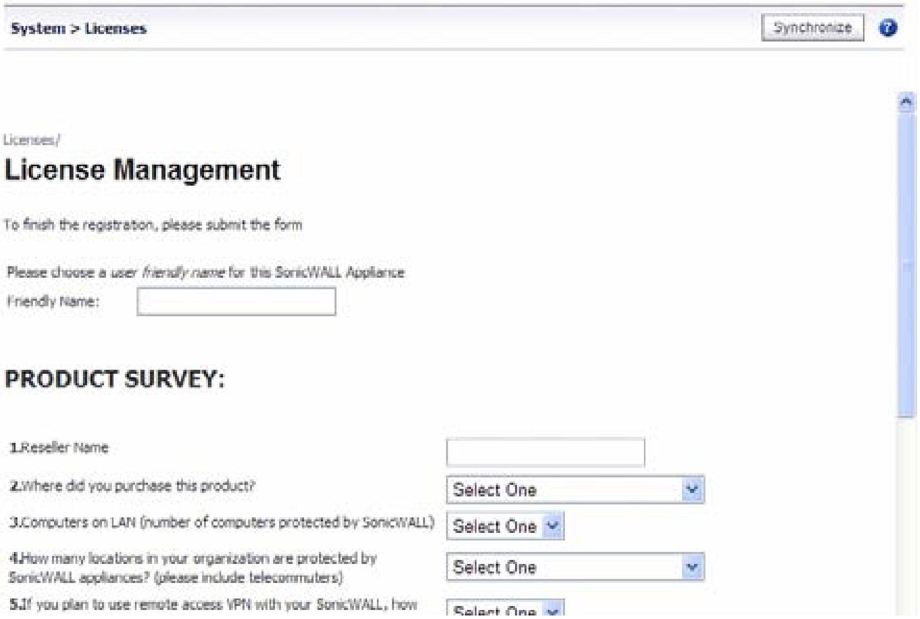
Please enter your existing mySonicWALL.com username (or email address) and password below:

Email Address/User Name:

Password:

Did you forget your User Name or Password? Go to https://www.mysonicwall.com for help.

4. If you have a mySonicWALL.com account, enter your mySonicWALL.com user name and password into the fields and then click **Submit**. The display changes.



Licenses/

License Management

To finish the registration, please submit the form

Please choose a *user friendly name* for this SonicWALL Appliance

Friendly Name:

PRODUCT SURVEY:

1.Reseller Name

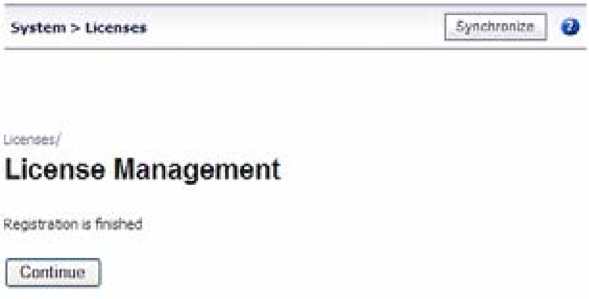
2.Where did you purchase this product? Select One

3.Computers on LAN (number of computers protected by SonicWALL) Select One

4.How many locations in your organization are protected by SonicWALL appliances? (please include telecommuters) Select One

5.If you plan to use remote access VPN with your SonicWALL, how Select One

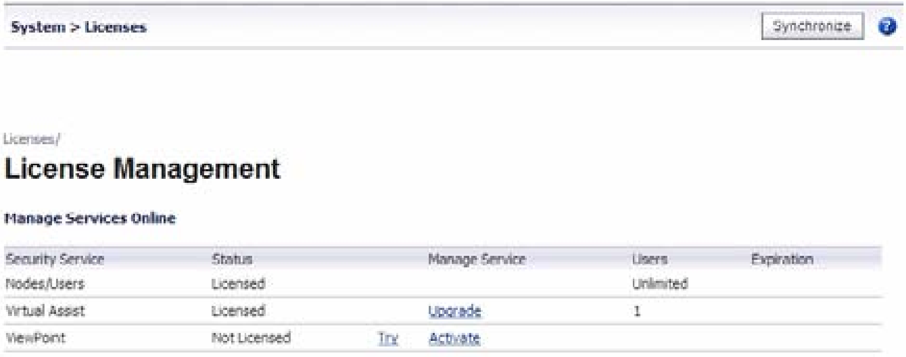
5. Enter a descriptive name for your SonicWALL SSL VPN in the **Friendly Name** field.
6. Under **Product Survey**, fill in the requested information and then click **Submit**. The display changes to inform you that your SonicWALL SSL VPN 4000 is registered.



License Management

Registration is finished

7. Click **Continue**.
8. In the License Management page, your latest license information is displayed.



License Management

Manage Services Online

Security Service	Status		Manage Service	Users	Expiration
Nodes/Users	Licensed			Unlimited	
Virtual Assist	Licensed		Upgrade	1	
ViewPoint	Not Licensed	Try	Activate		

Congratulations

Your SonicWALL SSL VPN 4000 is now fully operational.

After registration, some network environments require the SSL VPN appliance to be offline so that it is unable to connect to the SonicWALL licensing server. In this mode, the appliance will still honor the valid licenses; however, timed-based licenses may not be valid.

Configuring Dynamic DNS

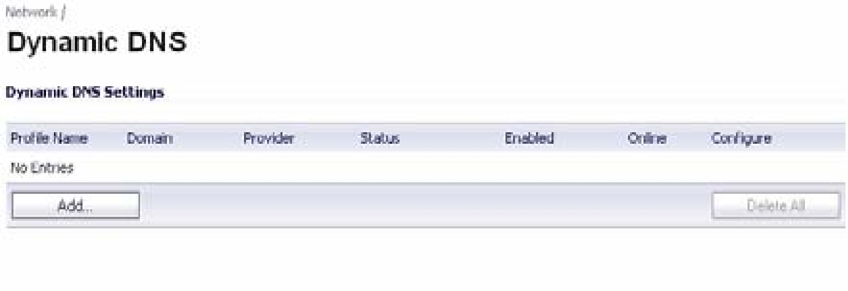
To begin using Dynamic DNS, you must first set up an account with one of the 4 free service providers listed below:

- DynDNS.org
- changeip.com
- No-IP.com
- yi.org

It is possible to use multiple providers simultaneously. The registration process normally involves a confirmation email from the provider, with a final acknowledgment performed by visiting a unique URL embedded in the confirmation email.

After logging in to the selected provider's page, you should visit the administrative link (typically 'add' or 'manage'), and create your host entries. This must be performed prior to attempting to use the dynamic DNS client on SonicOS.

The **Network > Dynamic DNS** page provides the settings for configuring the SonicWALL UTM appliance to use your DDNS service.



Network /

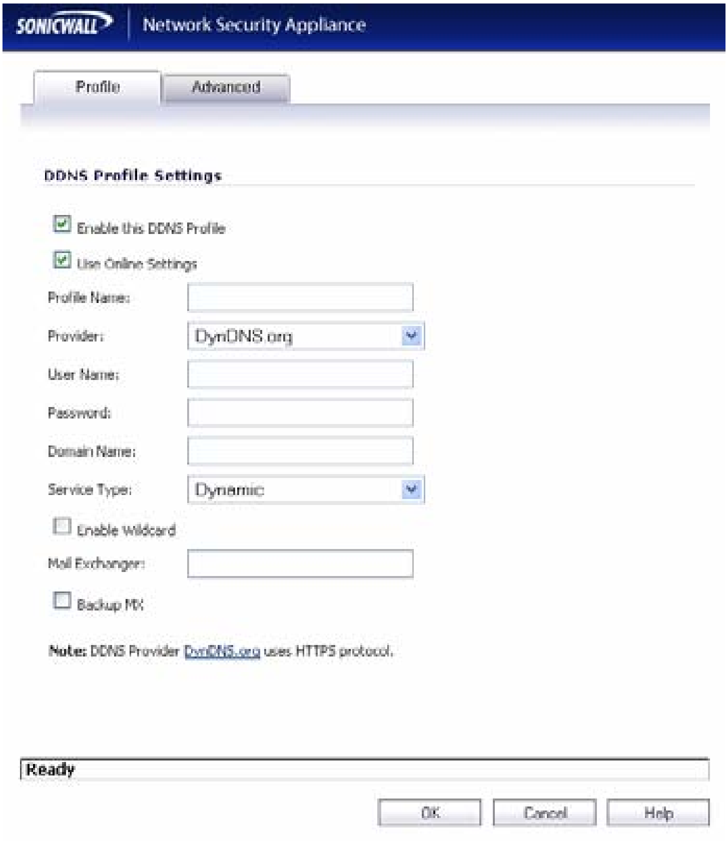
Dynamic DNS

Dynamic DNS Settings

Profile Name	Domain	Provider	Status	Enabled	Online	Configure
No Entries						

To configure Dynamic DNS on the SonicWALL UTM appliance, perform these steps:

1. On the **Network > Dynamic DNS** page, click the **Add** button. The **Add DDNS Profile** window is displayed.



DDNS Profile Settings

☑ Enable this DDNS Profile

☑ Use Online Settings

Profile Name:

Provider: DynDNS.org

User Name:

Password:

Domain Name:

Service Type: Dynamic

□ Enable Wildcard

Mail Exchanger:

□ Backup MX

Note: DDNS Provider DynDNS.org uses HTTPS protocol.

Ready

2. If **Enable this DDNS Profile** is selected, the profile is administratively enabled, and the SonicWALL UTM appliance takes the actions defined in the **Online Settings** section on the **Advanced** tab.
3. If **Use Online Settings** is selected, the profile is administratively online.
4. Enter a name to assign to the DDNS entry in the **Profile Name** field. This can be any value used to identify the entry in the **Dynamic DNS Settings** table.
5. In the **Profile** page, select the **Provider** from the drop-down list at the top of the page. This example uses *DynDNS.org*. Dyndns.org requires the selection of a service. This example assumes you have created a dynamic service record with dyndns.org.
6. Enter your dyndns.org username and password in the **User Name** and **Password** fields.

7. Enter the fully qualified domain name (FQDN) of the hostname you registered with dyndns.org. Make sure you provide the same hostname and domain as you configured.
8. You may optionally select **Enable Wildcard** and/or configure an MX entry in the **Mail Exchanger** field.
9. Click the **Advanced** tab. You can typically leave the default settings on this page.
10. The **On-line Settings** section provides control over what address is registered with the dynamic DNS provider. The options are:

    Let the server detect IP Address - The dynamic DNS provider determines the IP address based upon the source address of the connection. This is the most common setting.

    Automatically set IP Address to the Primary WAN Interface IP Address - This will cause the SonicWALL device to assert its WAN IP address as the registered IP address, overriding auto-detection by the dynamic DNS server. Useful if detection is not working correctly.

    Specify IP Address manually - Allows for the IP address to be registered to be manually specified and asserted.
11. The **Off-line Settings** section controls what IP Address is registered with the dynamic DNS service provider if the dynamic DNS entry is taken off-line locally (disabled) on the SonicWALL. The options are:

    Do nothing - the default setting. This allows the previously registered address to remain current with the dynamic DNS provider.

    Use the Off-Line IP Address previously configured at Provider’s site - If your provider supports manual configuration of Off-Line Settings, you can select this option to use those settings when this profile is taken administratively offline.
12. Click the **OK** button.

Configuring a Static IP Address

If you did not enable the SonicWALL UTM appliance DHCP server, you must configure each computer with a static IP address from your LAN or WLAN IP address range. After the SonicWALL SSL VPN 4000 has restarted, follow the steps below for configuring your network clients running any of the following Microsoft Windows operating systems on your LAN/WLAN:

Windows XP

1. Open the **Local Area Connection Properties** window.
2. Double-click **Internet Protocol (TCP/IP)** to open the **Internet Protocol (TCP/IP) Properties** window.
3. Select **Use the following IP address** and type an IP address from your LAN IP range in the **IP address** field.
4. Type the appropriate subnet mask (for example, **255.255.255.0**) in the **Subnet Mask** field.
5. Type the SonicWALL SSL VPN 4000 LAN IP Address into the **Default Gateway** field.
6. Type the DNS IP address in the **Preferred DNS Server** field. If you have more than one address, type the second one in the **Alternate DNS server** field.
7. Click **OK** for the settings to take effect.

Windows 2000

1. From your Windows **Start** menu, select **Settings**.
2. Open **Network and Dial-up Connections**.
3. Click **Properties**.
4. Highlight **Internet Protocol (TCP/IP)** and click **Properties**.
5. Select **Use the following IP address**.
6. Type an IP address from your LAN IP range **IP address** field.
7. Type the appropriate subnet mask (for example, **255.255.255.0**) in the **Subnet Mask** field.
8. Type the SonicWALL SSL VPN 4000 LAN IP Address into the **Default Gateway** field.
9. If you have a DNS Server IP address from your ISP, enter it in the **Preferred DNS Server** field.
10. Click **OK** for the settings to take effect.

Windows NT

1. From the **Start** menu, highlight **Settings** and then select **Control Panel**.
2. Open **Network**.
3. Double-click **TCP/IP** in the **TCP/IP Properties** window.
4. Select **Specify an IP Address**.
5. Type an IP address from your LAN IP range in the **IP Address** field.
6. Type the appropriate subnet mask (for example, **255.255.255.0**) in the **Subnet Mask** field.
7. Type the SonicWALL SSL VPN 4000 LAN IP Address in the **Default Gateway** field.
8. Click **DNS** at the top of the window.
9. Type the DNS IP address in the **Preferred DNS Server** field. If you have more than one address, enter the second one in the **Alternate DNS server** field.
10. Click **OK**, and then click **OK** again.
11. Restart the computer for changes to take effect.

9 Mounting Guidelines

The SonicWALL SSL VPN 4000 is 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. SonicWALL includes a rack mounting kit with the SonicWALL SSL VPN appliance that is compatible with most computer equipment racks.
- Four mounting screws, compatible with the rack design, must be used and hand tightened to ensure secure installation. Select 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
- 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 and 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 using power strips.

Glossary of Networking Terms

ActiveX - A technology that allows the sharing of applications and data across the Web. For example, Active X allows you to view Microsoft Word and Adobe Acrobat documents within the Internet Explorer Web browser without downloading the files and launching the appropriate application. The SonicWALL SSL VPN network client, NetExtender, uses an ActiveX control when launched or installed from Internet Explorer on Windows. With Firefox, XPCOM is used, which is similar to ActiveX. On Linux or MacOS systems, Java is used with NetExtender.

Default Gateway - A device on an internetwork that forwards packets to another network.

DHCP - Dynamic Host Configuration Protocol allocates IP addresses to computers on the network automatically without assigning a computer a static (fixed) IP address.

DMZ - A network zone segregated from the LAN, typically used for servers accessible from the Internet. Traffic between the Internet and the DMZ and between the DMZ and the LAN can be carefully monitored and controlled. DMZ comes from “Demilitarized Zone”.

DNS - Domain Name System, a hierarchical naming system that resolves a domain name with its associated IP address. A DNS server looks up the name of a computer and finds the corresponding IP address. This allows users to access hosts using friendly text-based names instead of IP addresses. These names are called fully qualified domain names (FQDN).

IP Address - Internet Protocol Address, a thirty-two bit number that identifies a computer or other resource on the Internet or on any TCP/IP network. The number is usually expressed as four numbers from 0 to 255 separated by periods, for example, 172.16.31.254.

LAN - A Local Area Network is typically a group of computers located at a single location, and is commonly based on the Ethernet architecture.

NetExtender - A network client that allows Windows users to connect to a network through the SonicWALL SSL VPN 4000. When using NetExtender, users have access to files and network resources as if they were physically within the network.

Portal - A gateway, usually through the Internet to network resources or services. The SonicWALL SSL VPN 4000 provides a Portal as the user interface for remote access to protected LAN resources such as Web and FTP servers, files shares, and remote desktops.

PPPoE - The Point to Point Protocol over Ethernet supports the transmission of network packets over an analog phone line.

Private IP Address - An IP address for a resource in your network that is not known or published outside the zone (for example LAN) where it is located.

Public IP Address - An IP address for a resource in your network that is published outside your network to the WAN.

Router - A device that routes data between networks through IP address information in the header of the IP packet. A router forwards packets to other routers until the packets reach their destination. The Internet is the largest example of a routed network.

SSL VPN - Secure Socket Layer Virtual Private Networking. A secured private communications network usually used within a company, or by several different companies or organizations, communicating over a public network. SSL technology is used either for tunneling the entire network stack, or for securing what is essentially a Web proxy.

Subnet - A portion of a network. Each subnet within a network shares a common network address and is uniquely identified by a subnetwork number.

Subnet Mask - A 32-bit number used to separate the network and host sections of an IP address. A subnet mask subdivides an IP network into smaller pieces. An example of a subnet mask might be 255.255.255.248 for subnet with only eight IP addresses.

TCP/IP - Transmission Control Protocol/Internet Protocol is the basic communication protocol of the Internet. It supports sending information in packets, and identifies each device with a unique numeric IP address.

VPN - A Virtual Private Network is a virtual network that encrypts data and sends it privately over the Internet to protect sensitive information.

WAN - A Wide Area Network is a geographically distributed network composed of multiple networks joined into a single large network. The Internet is a global WAN.

SonicWALL SSL VPN 4000 Appliance Regulatory Statement and Safety Instructions

Regulatory Model/Type	Product Name
1RK09-032	SonicWALL SSL VPN 4000

Detailed regulatory information can be found in the electronic file, "**SonicWALL_SSL-VPN_Regulatory_Statement.pdf**," located on the SonicWALL Resource CD provided with the unit or on the SonicWALL Web site: <http://www.sonicwall.com>.

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.

Copyright Notice

Specifications and descriptions subject to change without notice.

Trademarks

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: 232-001459-00
Rev A 5/08