Secure Remote Access Solutions

APPLIANCES | **SonicWALL SSL-VPN Series**

SSL-VPN 2000
Getting Started Guide

SONICWALL®

SonicWALL SSL-VPN 2000 Appliance Getting Started Guide

Thank you for your purchase of the SonicWALL SSL-VPN 2000, the solution for secure remote access to mission-critical resources from virtually any end point—including desktops, laptops, PDAs and smartphones.

The SonicWALL SSL-VPN 2000 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.

> **Note:** *To ensure optimal performance, please visit <https://www.mysonicwall.com> to register your new appliance, download the latest version of SonicOS SSL-VPN firmware, and view complete product documentation.*

This *Getting Started Guide* contains installation procedures and configuration guidelines for deploying a SonicWALL SSL-VPN 2000 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 2000 appliance can be deployed.

For complete documentation, refer to the *SonicWALL SSL-VPN Administrator's Guide* at: <http://www.sonicwall.com/us/Support.html>.

SonicWALL SSL-VPN 2000 Configuration Steps

1. "Selecting a SonicWALL Recommended Deployment Scenario" on page 3
2. "Applying Power to the SonicWALL SSL-VPN 2000" on page 4
3. "Accessing the Management Interface" on page 5
4. "Configuring Your SonicWALL SSL-VPN 2000" on page 7
5. "Connecting the SonicWALL SSL-VPN 2000" on page 15
6. "Configuring Your Gateway Device" on page 20
7. "Testing Your SSL-VPN Connection" on page 54
8. "Registering Your SonicWALL SSL-VPN 2000" on page 56
9. "Mounting Guidelines" on page 64

Before You Begin

Check Package Contents

- One SonicWALL SSL-VPN 2000 appliance
- One SonicWALL SSL-VPN 2000 Getting Started Guide
- One SonicWALL SSL-VPN Release Notes
- One straight-through Ethernet cable
- One rack-mount kit
- One power cord*

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

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

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 2000
- 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 2000, 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:

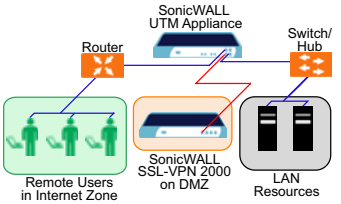
User Name: *admin*

Password: _____ (default: *password*)

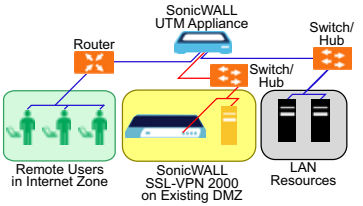
1 Selecting a SonicWALL Recommended Deployment Scenario

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 2000.
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



Scenario C
SSL-VPN on the LAN

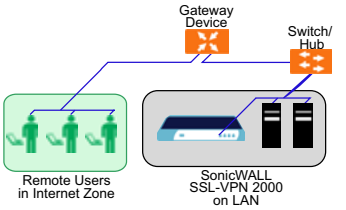
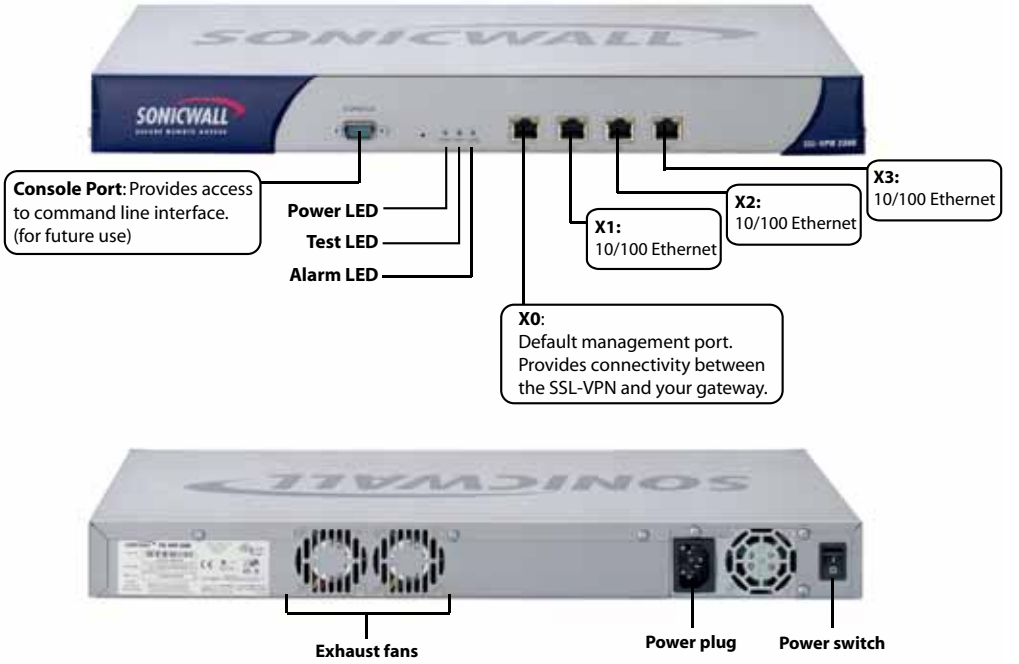


Table 1: SonicWALL SSL-VPN 2000 Deployment Scenarios

Gateway Device	SonicWALL Recommended Deployment Scenarios	Conditions or Requirements
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 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 Standard 3.1 or higher: TZ 150 Series TZ 170 Wireless TZ 170 SP TZ 180 Series PRO 1260 / 2040 / 3060 SonicWALLs with 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 2000

1. Plug the power cord into the SonicWALL SSL-VPN 2000 and into an appropriate power outlet.
2. Turn on the power switch on the rear of the appliance next to the power cord.



The Power LED on the front panel lights up green when you turn on the SonicWALL SSL-VPN 2000. 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 2000 is ready for configuration.

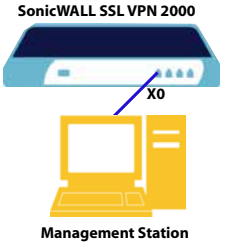
If the Test or Alarm LEDs remain lit or if the Test LED blinks red after the SonicWALL SSL-VPN 2000 has booted, restart the SonicWALL SSL-VPN 2000. For more troubleshooting information, refer to the *SonicWALL SSL-VPN Administrator's Guide*.

Continue to Step 3

3 Accessing the Management Interface

To access the Web-based management interface of the SonicWALL SSL-VPN 2000:

1. Connect one end of an Ethernet cable into the **X0** port of your SonicWALL SSL-VPN 2000. Connect the other end of the cable into the computer you are using to manage the SonicWALL SSL-VPN 2000.



2. Set the computer you use to manage the SonicWALL SSL-VPN 2000 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 62.

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 **Continue to this website** or the **OK** button to accept the certificate and continue.

* *While these browsers are acceptable for use in configuring your SonicWALL SSL-VPN 2000, 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.

Continue to Step 4

If You Cannot Login to the SSL-VPN

If you cannot connect to the SonicWALL SSL-VPN 2000, 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 2000 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 62 for instructions on setting your IP address.
- Is your Domain set to LocalDomain on the login screen?

4 Configuring Your SonicWALL SSL-VPN 2000

Once your SonicWALL SSL-VPN 2000 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 7
- "Adding a Local User" on page 8
- "Setting Time Zone" on page 9
- "Configuring SSL-VPN Network Settings" on page 9
  - "Configuring DNS / WINS" on page 9
  - "Configuring the X0 IP address for Scenario B and Scenario C" on page 10
  - "Configuring a Default Route" on page 11
  - "Adding a NetExtender Client Route" on page 12

Setting Your Administrator Password

1. Navigate to the **Users > Local Users** page
2. Click the **Configure** button corresponding to the "admin" account.

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 2000 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.

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

Adding a Local User

1. Navigate to the **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.

7. Click the **Add** button.

Setting Time Zone

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

3. Click the **Accept** button.

Note: *Setting the time correctly is essential to many of the operations of the SonicWALL SSL-VPN 2000. Be sure to set the time-zone correctly. Automatic synchronization with an NTP server (default setting) is encouraged to ensure accuracy.*

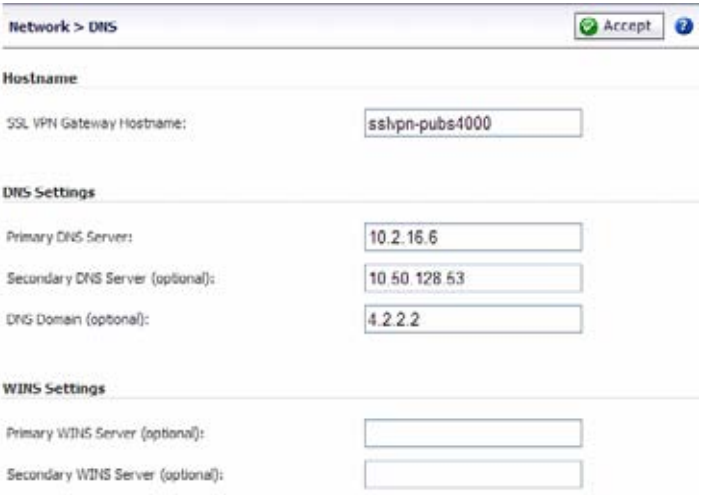
Configuring SSL-VPN Network Settings

You will now configure your SSL-VPN 2000 network settings. Refer to the notes you took in “Network Configuration Information” on page 2 to complete this section.

Configuring DNS / WINS

1. Navigate to the **Network > DNS** page.
2. Enter a unique name for your SonicWALL SSL-VPN 2000 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.

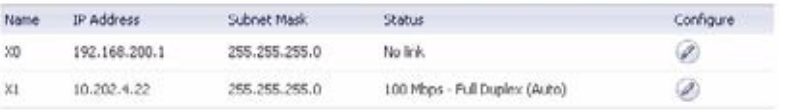


5. (Optional) Enter your DNS Domain in the **DNS Domain** Field.
6. (Optional) Enter your WINS servers in the **Primary WINS Server** and **Secondary WINS Server** fields.
7. Click the **Accept** button.

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



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.

4. Click **OK**. When you click **OK**, you will lose your connection to the SSL-VPN.
5. Reset the computer you use to manage the SonicWALL SSL-VPN 2000 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 62.

6. 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**.

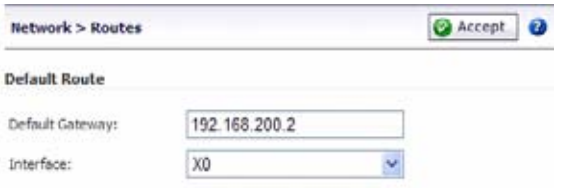
Configuring a Default Route

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 3.

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. Navigate to 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.



4. Click the **Accept** button.

Adding a NetExtender Client Route

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

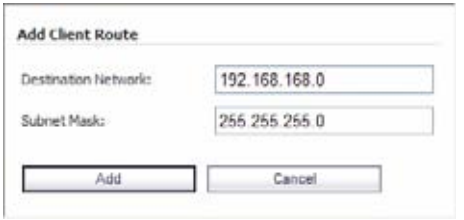
1. Navigate to the **NetExtender > Client Routes** page.
2. Click the **Add Client Route** button.
3. Enter the IP address of the trusted network to which you would like to provide access with NetExtender in the **Destination Network** field. (For example, if you are connecting to an existing DMZ with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



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

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

If you 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 2000

Before continuing, reference the diagrams on the following pages to connect the SonicWALL SSL-VPN 2000 to your network. Refer to the table in “Selecting a SonicWALL Recommended Deployment Scenario” on page 3 to determine the proper scenario for your network configuration.

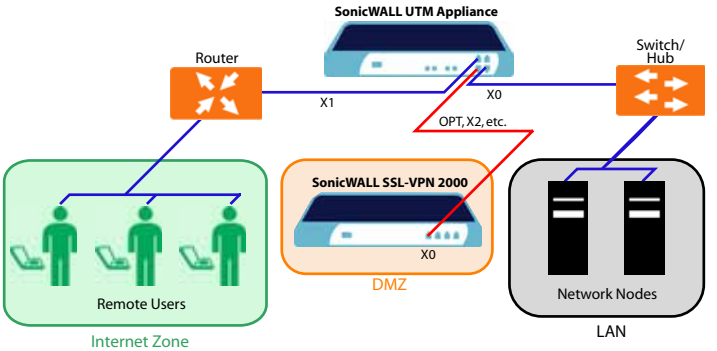
- “Scenario A: Connecting the SonicWALL SSL-VPN 2000” on page 15
- “Scenario B: Configuring Your Network Interface” on page 16
- “Scenario B: Connecting the SonicWALL SSL-VPN 2000” on page 17
- “Scenario C: Configuring Your Network Interface” on page 18
- “Scenario C: Connecting the SonicWALL SSL-VPN 2000” on page 19

Scenario A: Connecting the SonicWALL SSL-VPN 2000

To connect the SonicWALL SSL-VPN 2000 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 2000. 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 2000 to connect with your SonicWALL UTM appliance under network configurations given in Scenario B.

On your SonicWALL SSL-VPN 2000:

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

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.

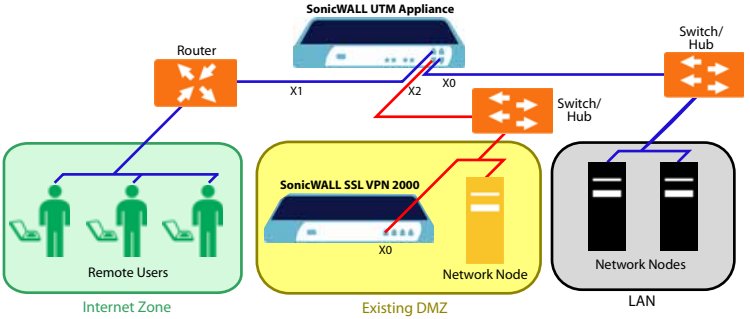
5. Click the **OK** button to apply changes.

Scenario B: Connecting the SonicWALL SSL-VPN 2000

To connect the SonicWALL SSL-VPN 2000 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 2000. 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 2000 to connect to your SonicWALL UTM appliance under network configurations given in Scenario C.

On the SonicWALL SSL-VPN 2000:

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

3. Enter an unused IP address in your LAN in the **IP Address** field.
4. Enter your subnet mask in the **Subnet Mask** field.

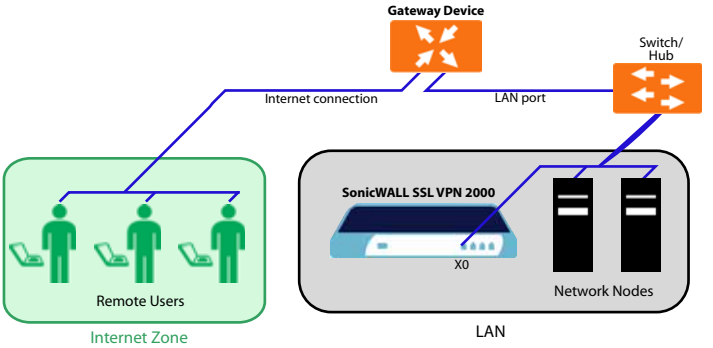
5. Click the **OK** button to apply changes.

Scenario C: Connecting the SonicWALL SSL-VPN 2000

To connect the SonicWALL SSL-VPN 2000 using Scenario C, perform the following steps:

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

Scenario C: SSL-VPN on the LAN



2. Connect the other end of the Ethernet cable to the **X0** port on the front of your SonicWALL SSL-VPN 2000. 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 2000, you need to configure your gateway device to work with the SonicWALL SSL-VPN 2000. Refer to the table in "Selecting a SonicWALL Recommended Deployment Scenario" on page 3 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 20
- "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 20
- "Scenario A: Configuring a DMZ or OPT Port in SonicOS Standard" on page 21
- "Scenario A: Allowing WAN -> DMZ Connection in SonicOS Standard" on page 21
- "Scenario A: Allowing DMZ -> LAN Connection in SonicOS Standard" on page 23
- "Scenario A: Adding a New SSL-VPN Custom Zone in SonicOS Enhanced" on page 27
- "Scenario A: Allowing WAN -> SSL-VPN Connection in SonicOS Enhanced" on page 28
- "Scenario A: Allowing SSL-VPN -> LAN Connection in SonicOS Enhanced" on page 31

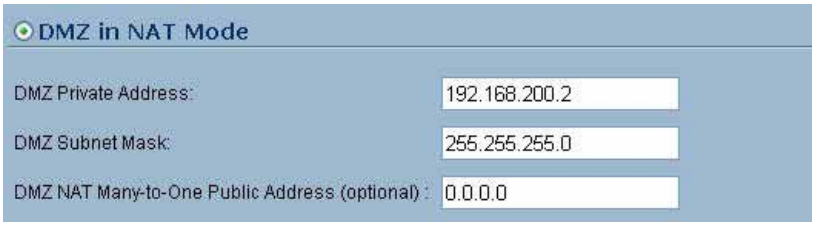
Scenario A: Connecting to the SonicWALL UTM Appliance

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 2000. Your user name and password combination may be different from the user name and password you recorded for your SonicWALL SSL-VPN 2000.*

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

1. Navigate to the **Network > Settings** page.
2. Click the **Configure** button for the DMZ or OPT interface.
3. Select the **DMZ in NAT Mode** radio button.
4. Enter **192.168.200.2** in the DMZ Private Address field.
5. Enter **255.255.255.0** in the DMZ Subnet Mask field.



6. Click the **OK** button.

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

Follow this procedure if you are connecting the SonicWALL SSL-VPN 2000 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 28

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.*

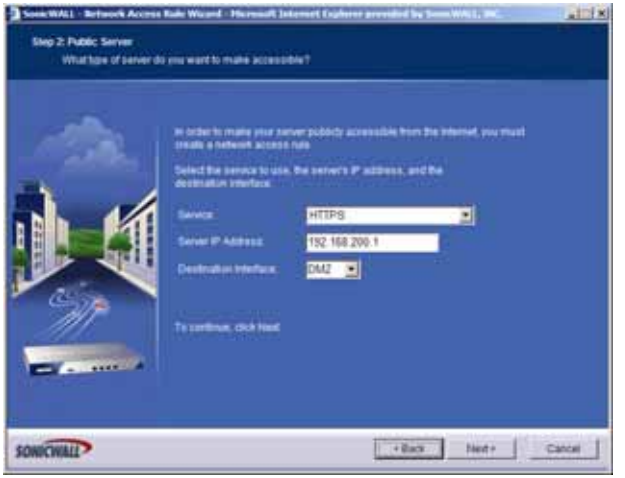
Note: *If you are allowing HTTP access to your SonicWALL SSL-VPN appliance as well as HTTPS access, you need to run the wizard twice to create public server access rules for both HTTP and HTTPS.*

Create a public server access rule for HTTPS traffic:

1. Navigate to the **Firewall > Access Rules** page.
2. Click Rule Wizard....
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 then click **Next**.

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

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.*

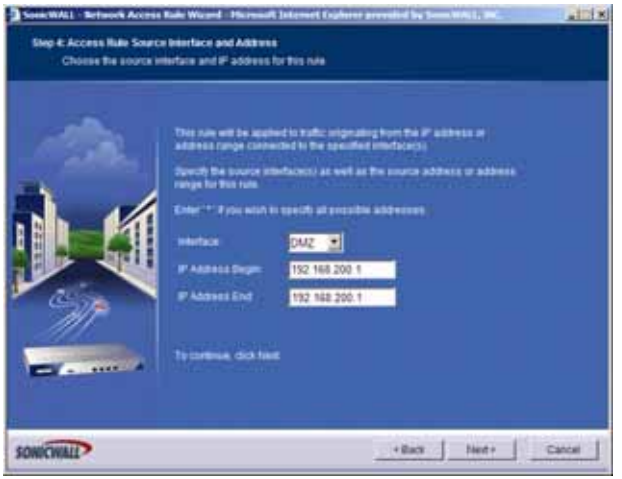
Create access to the LAN for the SSL-VPN X0 interface:

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 the following:

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

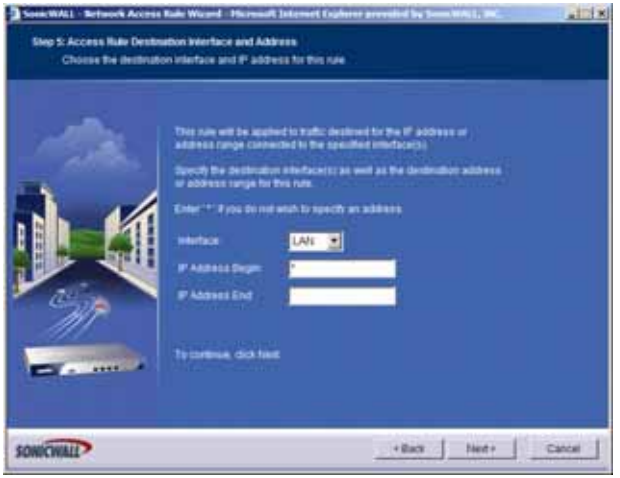
6. Click **Next**.

7. In the **Step 4: Access Rule Source Interface and Address** page, perform the following selections and then 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

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



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

9. 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.
10. 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 then 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**

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

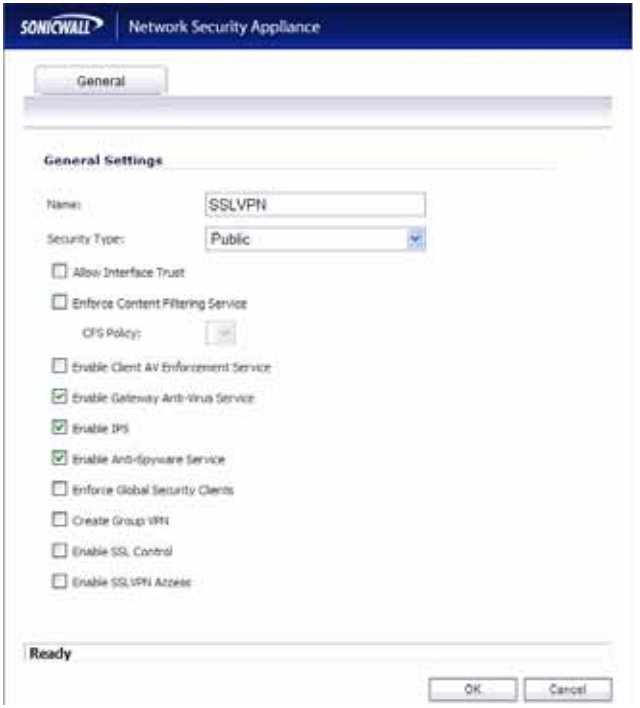
Interface	**LAN**
IP Address Begin	*****
IP Address End	Leave blank

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. Navigate to 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.



4. Type **SSLVPN** in the **Name** field.
5. Select **Public** from the **Security Type** drop-down menu.
6. Un-check the **Allow Interface Trust** checkbox.
7. Select the **Gateway AV**, **Intrusion Prevention Service** and **Anti-Spyware** checkboxes.
8. Click **OK**.
9. In the **Edit Interface** window, enter the IP address for this interface in the **IP Address** field. (For example "**192.168.200.2**". This should be the same address you created in "Configuring the X0 IP address for Scenario B and Scenario C" on page 10).
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 2000 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 21.

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

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

Server Type	Other
Services	Create new group

The **Add Service Group** dialog box appears.

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

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

5. In the **Server Private Network Configuration** page, enter:

Server Name	A name for your SonicWALL SSL-VPN 2000
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

6. Click **Next**.

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

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 2000.*

8. Click **Next**.
9. The **Public Server Configuration Summary** page displays all the configuration actions that will be performed to create the public server.

Click **Apply** to create the configuration and allow access from the WAN to the SonicWALL SSL-VPN 2000 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. In the **Address Objects** section, click Add....
3. In the **Add Object** dialog box, create an address object for the X0 interface IP address of your SonicWALL SSL-VPN 2000:

Name	Enter a name for the SonicWALL SSL-VPN 2000
Zone Assignment	**SSLVPN**
Type	**Host**
IP Address	The SonicWALL SSL-VPN 2000's X0 IP address, **192.168.200.1** by default

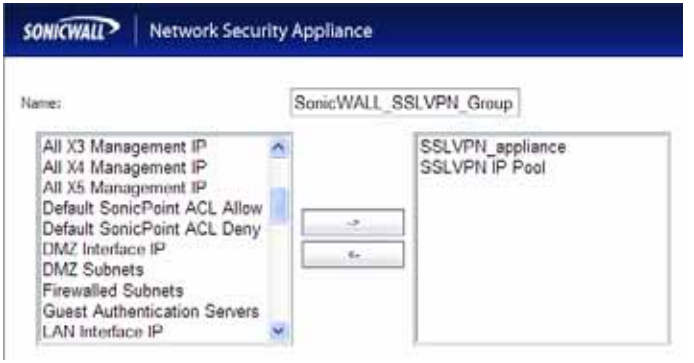
Click **OK** to create the object.

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 2000:

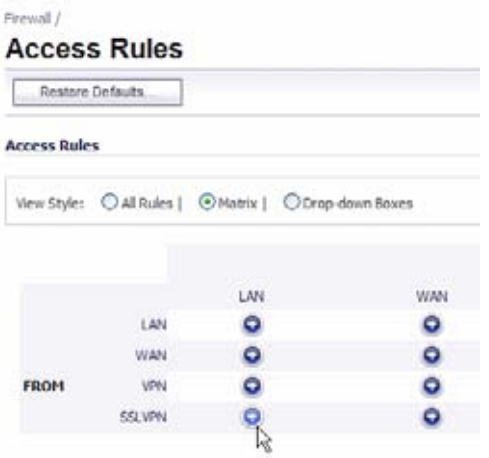
Name	Enter a name for NetExtender
Zone Assignment	**SSLVPN**
Type	**Range**
Starting IP Address	The start of the NetExtender IP address range, **192.168.200.100** by default
Ending IP Address	The end of the NetExtender IP address range, **192.168.200.200** by default

   Click **OK** to create the object.
6. On the **Network > Address Objects** page, in the **Address Groups** section, 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 2000 and the NetExtender IP range:



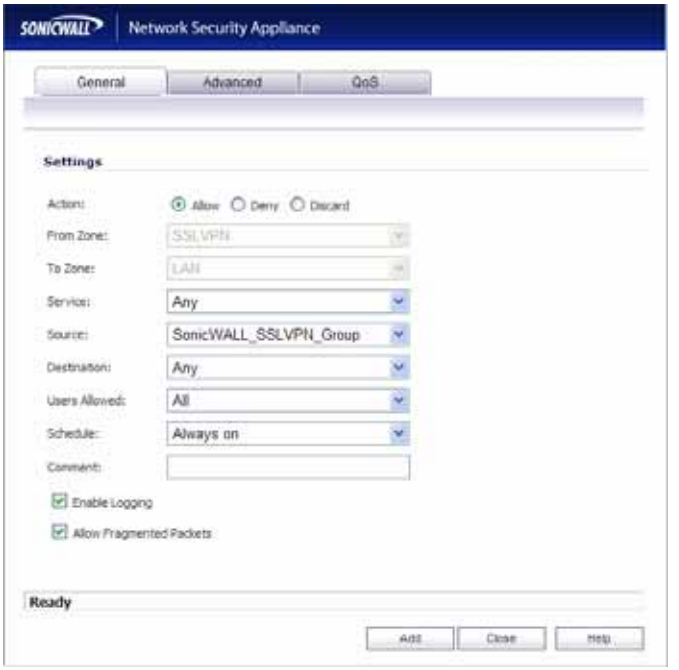
   - Enter a name for the group.
   - In the left column, select the two groups you created and click the arrow button .
   - Click **OK** to create the group when both objects are in the right column.
8. In the administrative interface, navigate to the **Firewall > Access Rules** page.

9. On the **Firewall > Access Rules** page in the matrix view, click the **SSLVPN > LAN** icon.



10. On the resulting **Firewall > Access Rules** page, click Add....

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



Action	**Allow**
From Zone	**SSLVPN**
To Zone	**LAN**
Service	**Any**
Source	The address group you just created, such as **SonicWALL_SSLVPN_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 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 43

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 2000.*

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

Follow this procedure if you are connecting the SonicWALL SSL-VPN 2000 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 28.

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.*

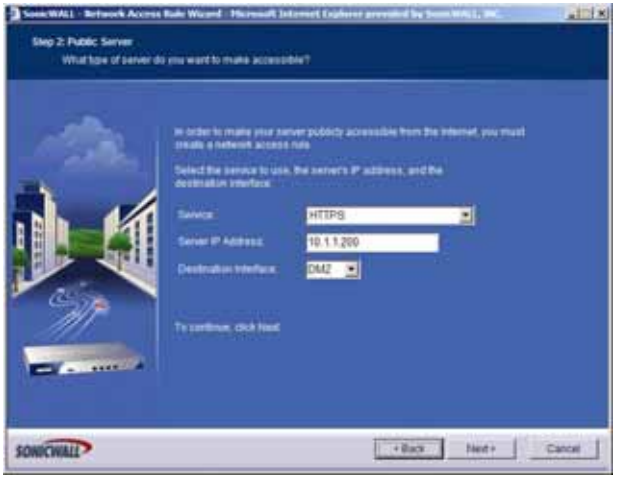
Create a public server access rule for HTTPS traffic:

1. Navigate to 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 then click **Next**.

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

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:

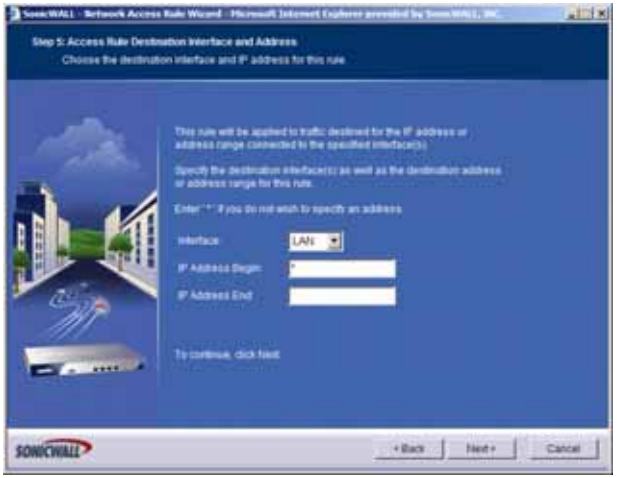
1. In the **Firewall > Access Rules** page, click Rule Wizard....
2. In the **Welcome to the SonicWALL Network Access Rules Wizard** page, click **Next**.
3. In the **Step 1: Access Rule Type** page, select **General Rule**. Click **Next**.
4. In the **Step 2: Access Rule Service** page, select **Any**.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

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

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

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

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

7. In the **Step 5: Access Rule Destination Interface and Address** page, perform the following selections and then 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 2000 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 21.

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. In the SonicOS Enhanced management interface, click the **Wizards** icon at the top right of the window.
2. On the **Welcome** page, select the **Public Server Wizard** and then click **Next**.
3. In the **Public Server Type** page, select:.

Server Type	Other
Services	Create new group

The **Add Service Group** dialog box is displayed.

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

   - Enter a name for the service.
   - Select both **HTTP** and **HTTPS** and click .
   - Click **OK** when both **HTTP** and **HTTPS** are in the right column.
5. In the **Public Server Type** page, click **Next**.
6. In the **Server Private Network Configuration** page, enter the following and then click **Next**:

Server Name	A name for your SonicWALL SSL-VPN 2000
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

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

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 2000.*

8. Click **Next**.
9. The **Public Server Configuration Summary** page displays all the configuration actions that will be performed to create the public server.

   Click **Apply** to create the configuration and allow access from the WAN to the SonicWALL SSL-VPN 2000 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 SonicOS Enhanced management interface, navigate to the **Network > Address Objects** page.
2. In the **Address Objects** section, click Add....

3. In the **Add Object** dialog box, create an address object for the X0 interface IP address of your SonicWALL SSL-VPN 2000:

Name	Enter a name for the SonicWALL SSL-VPN 2000
Zone Assignment	**DMZ**
Type	**Host**
IP Address	The SonicWALL SSL-VPN 2000's X0 interface IP address within your DMZ range, for example, **10.1.1.200**

Click **OK** to create the object.

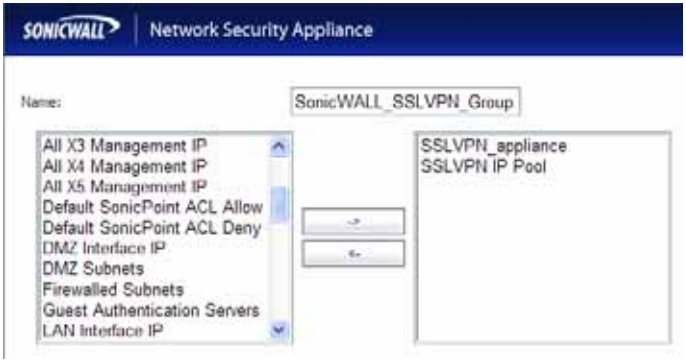
4. Click Add... again to create an address object for the NetExtender range.
5. In the **Add Object** dialog box, create an address object for the X0 interface IP address of your SonicWALL SSL-VPN 2000:

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 **Address Groups** section, 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 2000 and the NetExtender IP range:



   - Enter a name for the group.
   - In the left column, select the two groups you created 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. On the **Firewall > Access Rules** page in the matrix view, click the **DMZ > LAN** icon.
10. On the resulting **Firewall > Access Rules** page, click [Add...].

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

Action	**Allow**
From Zone	**DMZ**
To Zone	**LAN**
Service	**Any**
Source	The address group you just created, such as **SonicWALL_SSLVPN_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 SSL-VPN -> LAN Connectivity in SonicOS Enhanced" on page 47
- "Scenario C: Setting Public Server Access in SonicOS Standard" on page 51
- "Scenario C: Setting Public Server Access in SonicOS Enhanced" on page 52

Scenario C: 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 2000. Your user name and password combination may be different from the user name and password you recorded for your SonicWALL SSL-VPN 2000.*

Scenario C: Configuring SSL-VPN -> LAN Connectivity in SonicOS Enhanced

In order for users to access local resources through the SonicWALL SSL-VPN 2000, you must configure your gateway device to allow an outside connection through the SSL-VPN into your LAN.

1. In the administration interface, navigate to the **Network > Address Objects** page.
2. In the **Address Objects** section, click

.

3. In the **Add Object** dialog box, create an address object for the X0 interface IP address of your SonicWALL SSL-VPN 2000:

Name	Enter a name for the SonicWALL SSL-VPN 2000
Zone Assignment	**SSLVPN**
Type	**Host**
IP Address	The SonicWALL SSL-VPN 2000's X0 IP address, **192.168.200.1** by default

Click **OK** to create the object.

4. Click

again to create an address object for the NetExtender range.
5. In the **Add Object** dialog box, create an address object for the X0 interface IP address of your SonicWALL SSL-VPN 2000:

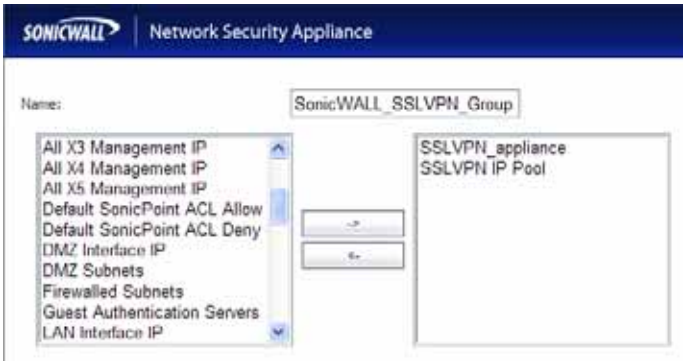
Name	Enter a name for NetExtender
Zone Assignment	**SSLVPN**
Type	**Range**
Starting IP Address	The start of the NetExtender IP address range, **192.168.200.100** by default
Ending IP Address	The end of the NetExtender IP address range, **192.168.200.200** by default

Click **OK** to create the object.

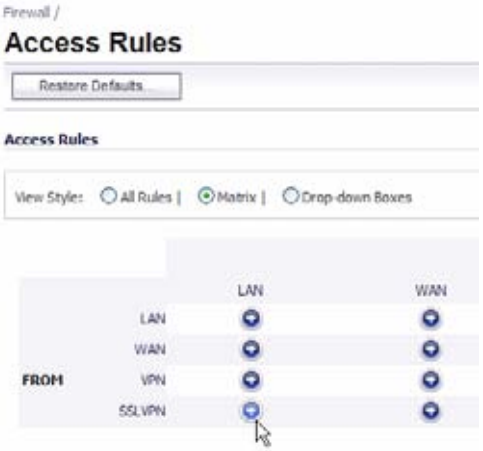
6. On the **Network > Address Objects** page, in the **Address Groups** section, click

.

7. In the **Add Address Object Group** dialog box, create a group for the X0 interface IP address of your SonicWALL SSL-VPN 2000 and the NetExtender IP range:

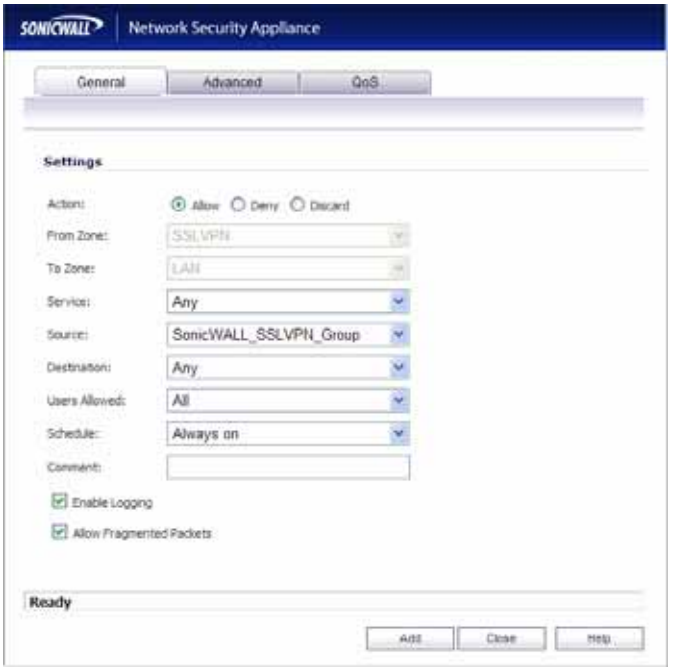


   - Enter a name for the group.
   - In the left column, select the two groups you created and click the arrow button .
   - Click **OK** to create the group when both objects are in the right column.
8. In the administrative interface, navigate to the **Firewall > Access Rules** page.
9. On the **Firewall > Access Rules** page in the matrix view, click the **SSLVPN > LAN** icon.



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

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



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

Click **OK** to create the rule.

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.

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.

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. Click the **Wizards** icon in the top right corner of the SonicOS Enhanced management interface.
2. Select the **Public Server Wizard** option and then click **Next**.
3. Select **Web Server** from the **Server Type** drop-down menu.
4. Select the **HTTP** and **HTTPS** checkboxes.

5. Click the **Next** button to continue the Wizard.
6. Enter **SSLVPN** 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.

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 2000 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 8 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.

4. Click **NetExtender** to start the NetExtender client installation.

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

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 2000.

Continue to Step 8

8 Registering Your SonicWALL SSL-VPN 2000

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 account to register the SonicWALL SSL-VPN 2000. You can create a new MySonicWALL 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:

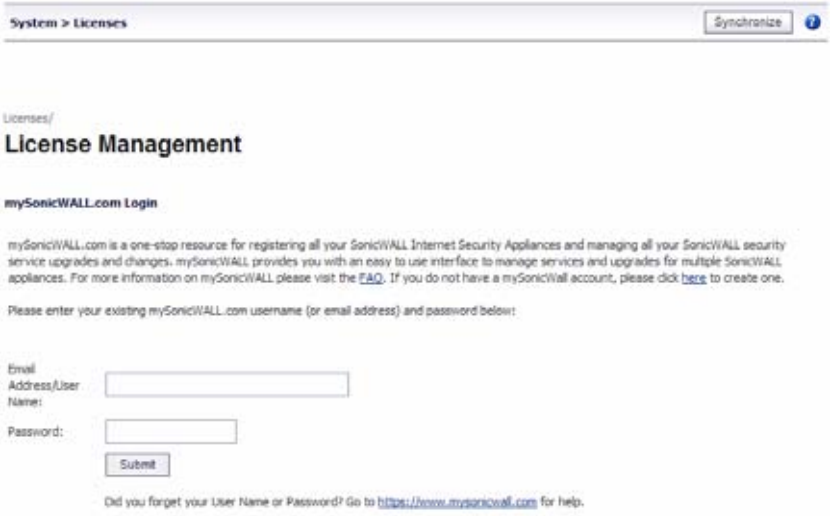
   - If you forgot your user name, click the **Forgot Username?** link.
   - If you forgot your password, click the **Forgot Password?** link.
   - If you do not have a MySonicWALL account, click the **Not a registered user?** link.
3. Follow the instructions to activate your MySonicWALL account.

Registering with MySonicWALL

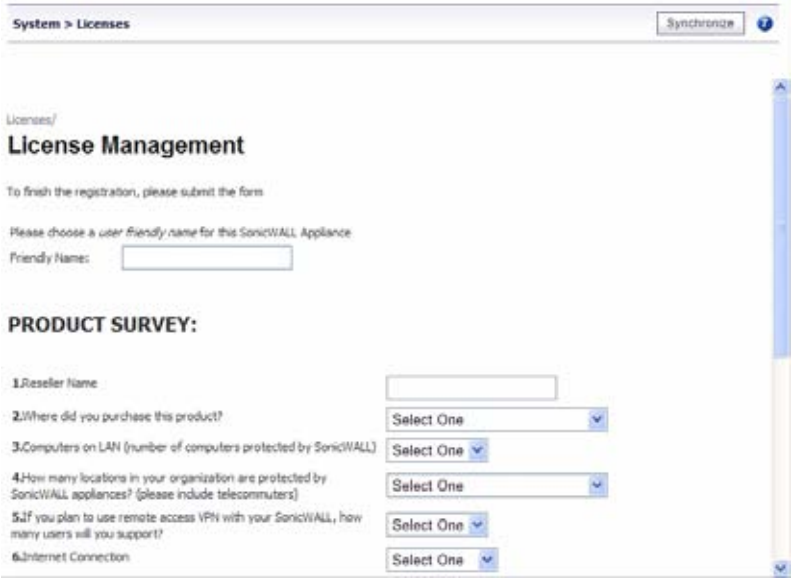
On a new SonicWALL SSL-VPN appliance or after upgrading to SonicWALL SSL-VPN 3.0 firmware from an earlier release, you can register your appliance from the **System > Licenses** page.

1. If you are not logged into the SonicWALL SSL-VPN 2000 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.



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.



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 2000 is registered.

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

Congratulations

Your SonicWALL SSL-VPN 2000 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

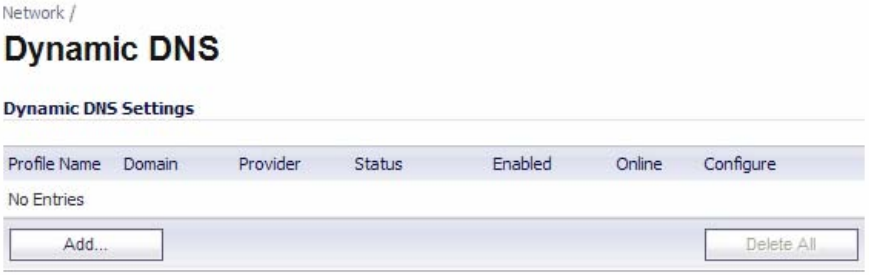
To begin using Dynamic DNS, you must first set up an account with one of the four free service providers listed below:

- 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.

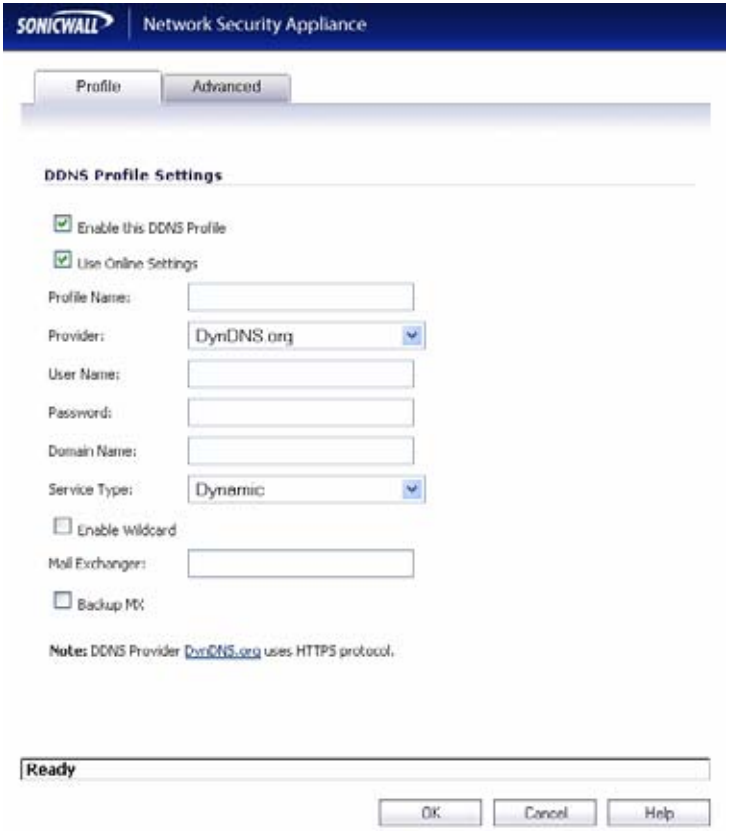
After logging in to the selected provider's page, you should visit the administrative link (typically 'add' or 'manage'), and create your host entries. This must be performed prior to attempting to use the dynamic DNS client on SonicOS.

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



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.



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 2000 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 Vista

1. From the **Start** menu, right-click **Network** and select **Properties**.
2. In the **Tasks** menu, click **Manage network connections**. The **Network Connections** window displays.
3. Right-click on **Local Area Connection** and select **Properties**.
4. In the list, double-click **Internet Protocol Version 4 (TCP/IP)**.
5. Select **Use the following IP address** and 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 2000 LAN IP Address into the **Default Gateway** field.
8. 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.
9. Click **OK**, and then click **OK** again for the settings to take effect.

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 2000 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**, and then click **OK** again 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 2000 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 2000 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 2000 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 2000. 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 2000 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 Global Support Services

On your appliance, on the Web, and on the phone, we make it easy and fast to find the information you need to keep your SonicWALL solution, and your network, running smoothly and efficiently.

Use the Online Help. Every SonicWALL security appliance includes Web-based online help available from the management interface. Clicking the question mark button on the top-right corner of every page accesses the context-sensitive help for that page. Once you've established an Internet connection, online help can get you the latest answers to frequently asked questions. Access to online help requires an Internet connection; fees may apply.

Visit SonicWALL online. Select your product, service, or operating system from the drop-down menus. Read the Getting Started Guide and the Administrator Guide available on the website. Search the SonicWALL Knowledge Base, check for new downloads, or get help from the SonicWALL user community through the Discussion Forum. SonicWALL's support website covers all aspects of support, from basic set-up and how-to information to more detailed technical notes and FAQs.

Explore training options. To meet your network security educational needs, SonicWALL offers a comprehensive sales and technical training curriculum. Our self-paced e*Briefings and instructor-led classes are designed for network administrators and security experts who need to enhance their knowledge and maximize their investment in SonicWALL solutions and security applications.

Need more help? Our technical support specialists are available by phone to help you with basic configuration and troubleshooting. Just call the support center in your region. The first 90 days of support are included with your warranty![1]

See the following sections for more information:

- "Customer Support" on page 68
- "Extend Your Support Coverage." on page 69
- "Knowledge Portal" on page 70
- "User Forums" on page 71
- "Training" on page 72
- "Related Documentation" on page 73
- "SonicWALL Live Product Demos" on page 74
- "SonicWALL Secure Wireless Network Integrated Solutions Guide" on page 75
- "SonicWALL Global Technical Assistance Center Contact Information" on page 76

1. *Warranty support and hardware warranty begin on the date of product registration. Telephone fees may apply for phone assistance. Telephone numbers and hours of operation vary by geographic region and are subject to change.*

Customer Support

SonicWALL offers Web-based and telephone support to customers who have a valid Warranty or who purchased a Support Contract. Please review our Warranty Support Policy for product coverage. SonicWALL also offers a full range of consulting services to meet your needs, from our innovative implementation services to traditional statement of work-based services. For telephone support, please have the serial number of your registered hardware solution ready when you call.

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

Extend Your Support Coverage.

SonicWALL Dynamic Support Services extend the support coverage on your SonicWALL solution beyond the warranty period. Our 8x5[1] and 24x7 support services include critical software and firmware updates, expert telephone and Web-based support, Advance Exchange hardware replacement, and access to electronic self-help tools — all for one low price.

- Take advantage of the latest features through software and firmware updates and upgrades.
- Speak with a SonicWALL Technical Support Specialist or contact us via the Web should you require assistance.
- If a replacement unit is required, SonicWALL will provide an Advance Exchange replacement via next-day air shipment.
- SonicWALL security appliances also ship with a one-year hardware warranty that can be extended up to three years!

To purchase a one-, two-, or three-year Dynamic Support contract, contact your local SonicWALL reseller or call SonicWALL at
+1 888.557.6642 or +1 408.745.9600.

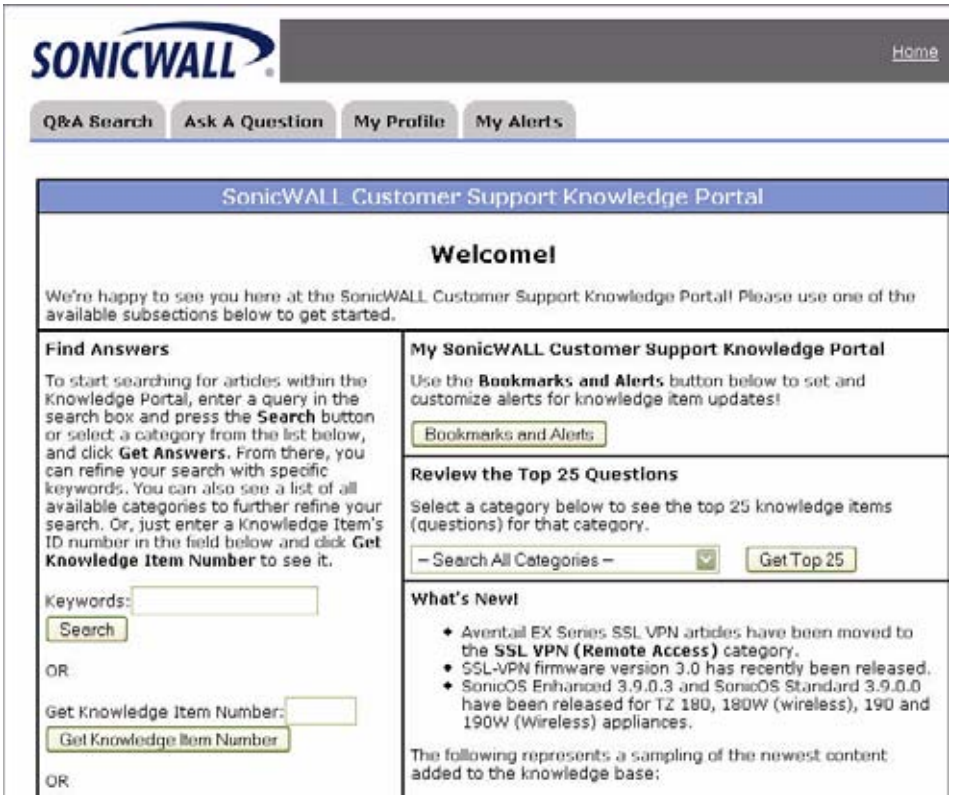
1. *8:00 am-5:00 pm local time is defined as follows: In North America: 8:00 am-5:00 pm Mountain Standard Time (MST); In Latin America: 8:00 am-5:00 pm Local Standard Time in the country where the product is deployed; In Europe, the Middle East and Africa: 9:00 am-6:00 pm GMT +1; In Asia Pacific: 8:00 am-5:00 pm Local Standard Time in the country where the product is deployed; In Japan: 5:00 pm-2:00 am UTC/GMT. Support for SonicWALL security services is limited to the subscription and does not include issues related to the operation of the appliance, firmware or software updates/upgrades, or hardware replacement.*

Knowledge Portal

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

- Browse
- Search for keywords
- Full-text search

For further information, navigate to the **Support** > **Knowledge Portal** page at: <http://www.mysonicwall.com/>



User Forums

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

- Content Security Manager topics
- Continuous Data Protection topics
- Email Security topics
- Firewall topics
- Network Anti-Virus topics
- Security Services and Content Filtering topics
- SonicWALL GMS and Viewpoint topics
- SonicPoint and Wireless topics
- SSL VPN topics
- NSA 240 / Wireless WAN - 3G Capability topics
- VPN Client topics
- VPN site-to-site and interoperability topics

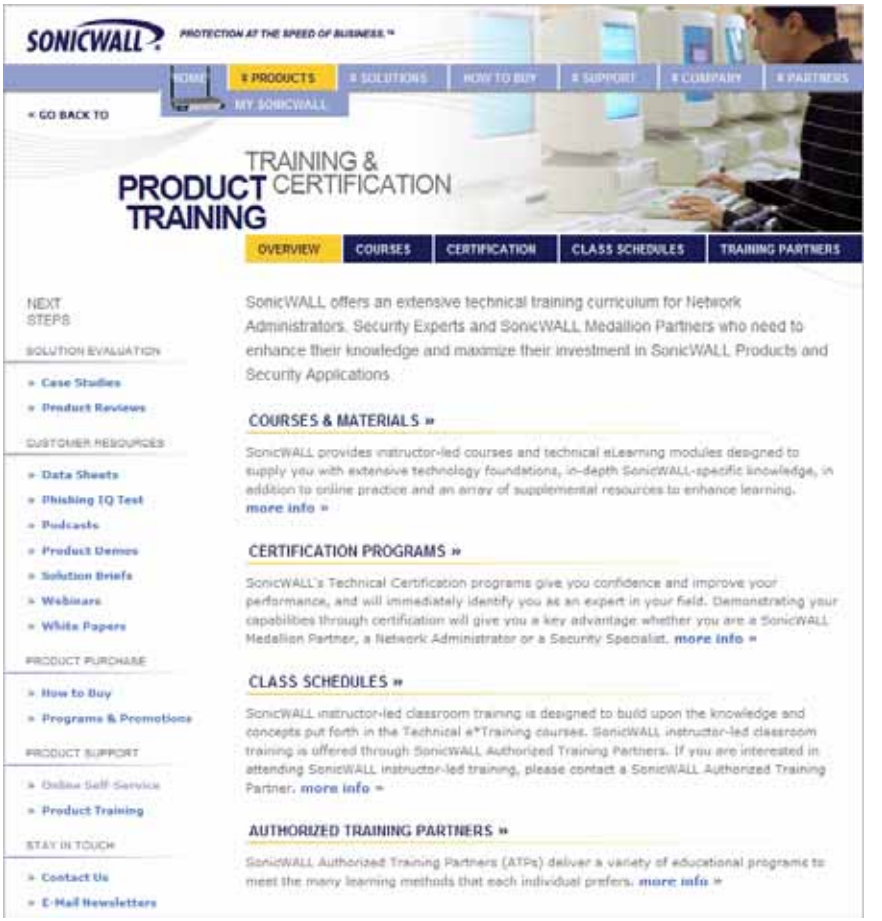
For further information, visit:
<https://forum.sonicwall.com/>

Training

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

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

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



Related Documentation

See the following related documents for more information:

- SonicWALL SSL-VPN Administrator's Guide
- SonicWALL SSL-VPN Release Notes
- SonicWALL SSL-VPN Feature Modules
  - SonicWALL SSL-VPN 3.0 Virtual Assist Feature Module
  - SonicWALL SSL-VPN 3.0 NetExtender Feature Module
  - SonicWALL SSL-VPN 3.0 File Shares Applet Feature Module
  - SonicWALL SSL-VPN 3.0 HTTP(S) Reverse Proxy Feature Module
  - SonicWALL SSL-VPN 3.0 One Time Password Feature Module
- SonicOS Enhanced Administrator's Guide
- SonicOS Enhanced Feature Modules
- SonicWALL GMS Administrator's Guide
- SonicWALL ViewPoint Administrator's Guide
- SonicWALL GAV Administrator's Guide
- SonicWALL IPS Administrator's Guide
- SonicWALL Anti-Spyware Administrator's Guide
- SonicWALL CFS Administrator's Guide
- SonicWALL GVC Administrator's Guide

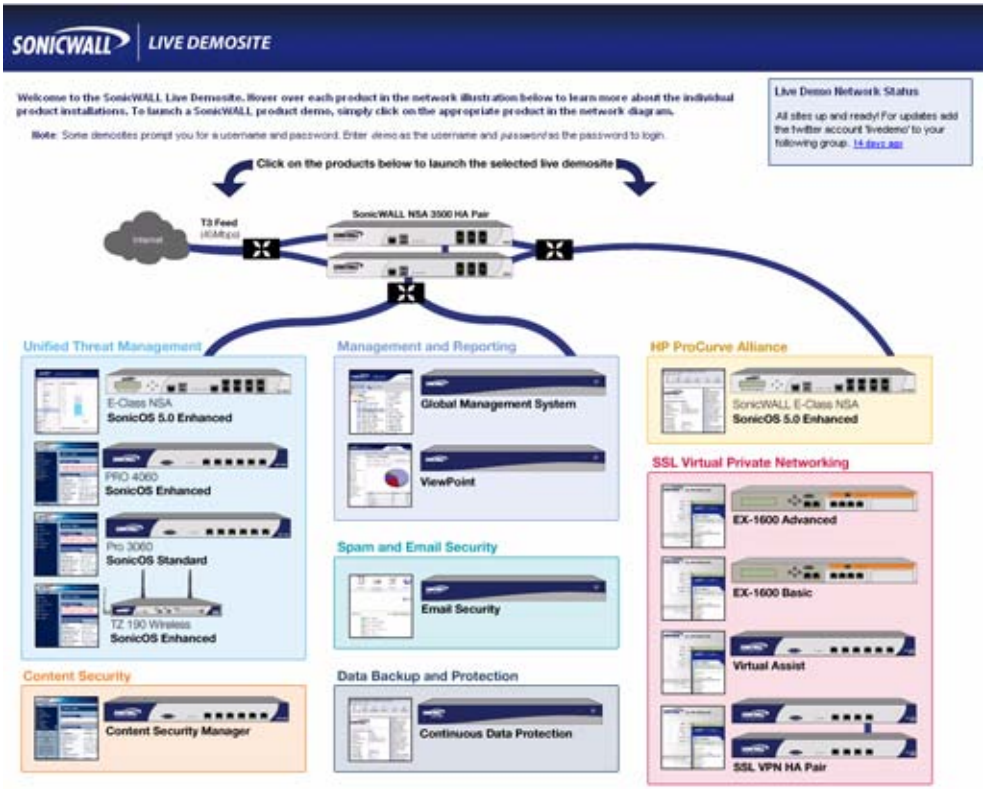
For further information, visit:
<http://www.sonicwall.com/us/support/289.html>

SonicWALL Live Product Demos

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

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

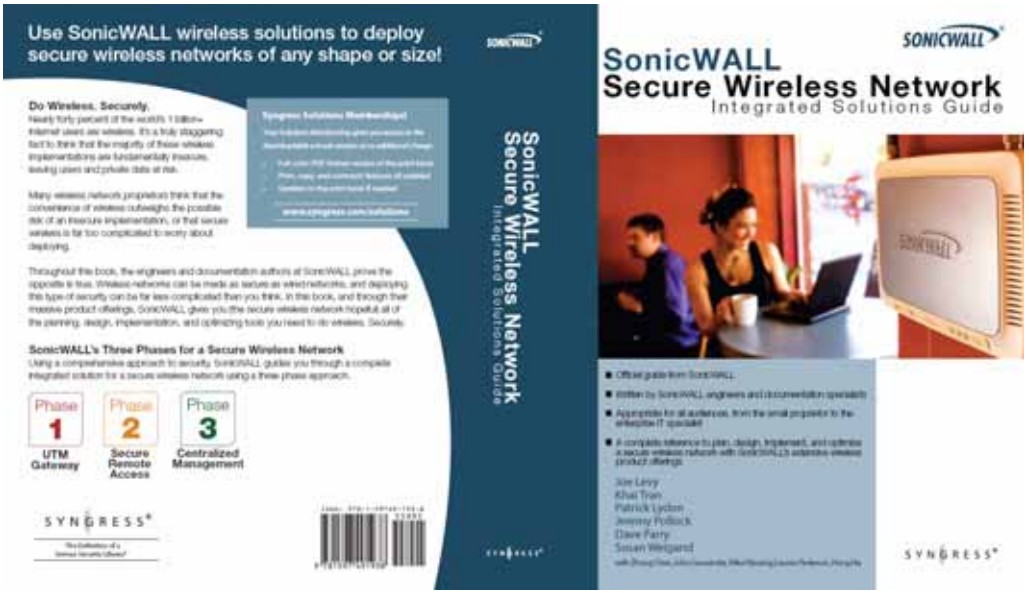
For further information, visit:
<http://livedemo.sonicwall.com/>



SonicWALL Secure Wireless Network Integrated Solutions Guide

The Official Guide to SonicWALL's market-leading wireless networking and security devices. This 512-page book is available in hardcopy. Order the book directly from Elsevier Publishing at:

<http://www.elsevier.com>



SonicWALL Global Technical Assistance Center Contact Information

Table 2: Global Technical Assistance Contact List

Country	Toll Free Phone Number	Toll Phone Number
Calling from North America (Support available in English)		
United States	+1 888.777.1476	
Canada	+1 888.777.1476	
Calling from Europe, the Middle East and Africa (Support available in English, French, German, Italian, and Spanish)		
Austria		+43 (0) 820.400.105
Belgium		+31 (0) 411.617.810
Czech Republic		+31 (0) 411.617.810
Denmark	807.02.652	
Egypt		+31 (0) 411.617.810
Finland	800.77.0265	
France	0800.970.019	+31 (0) 411.617.812
Germany	0800.0003.668	+31 (0) 411.617.813
Ireland		+31 (0) 411.617.811
Italy	800.909.106	+31 (0) 411.617.814
Jordan		+31 (0) 411.617.810
Luxembourg		+31 (0) 411.617.810
Netherlands		0.411.617.810
Nigeria		+31 (0) 411.617.810
Norway	800.57.477	
Poland		+31 (0) 411.617.810
Russia		+31 (0) 411.617.810
Saudi Arabia		+31 (0) 411.617.810
South Africa		+31 (0) 411.617.810
Spain	900.811.056	+31 (0) 411.617.815
Switzerland	0800.562.221	+31 (0) 411.617.810
Sweden	+020.140.14.25	
Turkey		+31 (0) 411.617.810
United Arab Emirates	8000.4411.869	
United Kingdom	0800.0280.488	+31 (0) 411.617.811
All Other Countries		+31 (0) 411.617.810

Calling from Asia Pacific (Support available in English except for Japan where support is offered in Japanese only)		
Australia		+1 800.35.1642
Hong Kong		+1 800.93.0997
India		000.800.100.3395
Japan		+81 (0)3.3457.8971
New Zealand		800.446489
Singapore		+ 800.110.1441
Calling from Latin America (Support available in English)		
Brazil	0800.891.4306	
Mexico		+1 888.777.1476

SonicWALL SSL-VPN 2000 Regulatory Statement and Safety Instructions

Regulatory Model/Type	Product Name
1RK0A-02A	SSL-VPN 2000

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

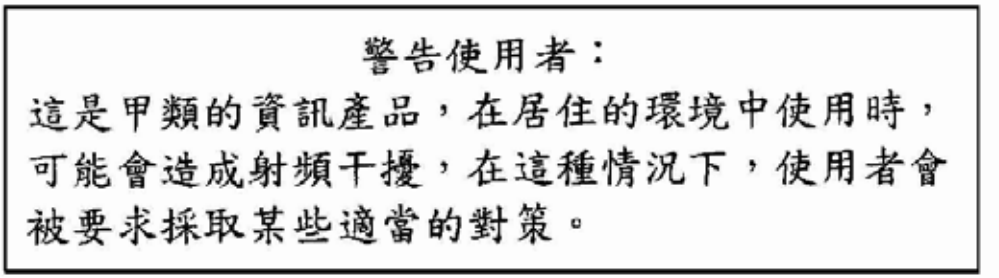
FCC Part 15 Class A Notice

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

Complies with EN 55022 Class A and CISPR22 Class A.

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

BMSI Statement



VCCI Statement

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

Canadian Radio Frequency Emissions Statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à toutes la norme NMB-003 du Canada.

CISPR 22 (En 55022) Class A

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

Declaration of Conformity

Application of council Directive	Directive 89/336/EEC (EMC) and 72/23/EEC (LVD)
Standards to which conformity is declared	EN 55022 (1998) Class A EN 55024 (1998) EN 61000-3-2 (1995) + A1, A2, A14 EN 61000-3-3 (1994) EN 60950 (1992) + A1, A2, A4, A11 National Deviations: AT, AU, BE, CH, CN, CZ, DE, DK, FI, FR, GB, GR, HU, IE, IL, IN, IT, JP, KR, NL, NO, PL, SE, SG, SI

Regulatory Information for Korea

All products with country code “” (blank) and “A” are made in the USA.

All products with country code “B” are made in China.

All products with country code “C” or “D” are made in Taiwan R.O.C.

A급 기기 (업무용 정보통신기기)

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

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.

Mounting the SonicWALL SSL-VPN 2000

See “Mounting Guidelines” on page 64.

Copyright Notice

© 2008 SonicWALL, Inc.

All rights reserved.

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

Specifications and descriptions subject to change without notice.

Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.

Microsoft Windows Vista, Windows XP, Windows 2000, Windows NT, Windows Server 2003, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

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

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

Firefox is a trademark of the Mozilla Foundation.

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

Notes

Notes

Notes

SonicWALL, Inc.
1143 Borregas Avenue
Sunnyvale CA 94089-1306
T +1 408.745.9600
F +1 408.745.9300
www.sonicwall.com

PN: 232-001458-50 Rev A

©2008 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice.