SonicWALL SSL-VPN 2000 Security Appliance
Getting Started Guide

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

The SonicWALL SSL-VPN 2000 security 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 e-mail, files, intranets, applications and other resources on the corporate LAN from any location.

SonicWALL SSL-VPN 2000 Configuration Steps

1. “Select a SonicWALL Recommended Deployment Scenario” on page 4
2. “Applying Power to the SonicWALL SSL-VPN 2000” on page 5
3. “Accessing the Management Interface” on page 6
4. “Configuring Your SonicWALL SSL-VPN 2000” on page 8
5. “Connecting the SonicWALL SSL-VPN 2000” on page 14
6. “Configuring your Gateway Device” on page 16
7. “Testing Your SSL-VPN Connection” on page 25
8. “Registering Your SonicWALL SSL-VPN 2000” on page 27
9. “Mounting Guidelines” on page 32


SonicWALL SSL-VPN 2000 Getting Started Guide
Before You Begin

Check Package Contents

- One SonicWALL SSL-VPN 2000 security appliance
- One SonicWALL SSL-VPN 2000 Getting Started Guide
- One SonicWALL SSL-VPN Release Notes
- One straight-through Ethernet cable
- One crossover Ethernet cable (red)
- One rack-mount kit
- One power cord*
- One SonicWALL SSL-VPN Series Resource CD, which contains:
  - SonicWALL SSL-VPN 2000 Product Documentation
  - Software Utilities

* 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/support/>
E-mail: 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 computer to use as a management station for initial configuration of the SonicWALL SSL-VPN 2000
- A Web browser supporting Java, and HTTP uploads, such as Internet Explorer 5.0 or higher, Netscape Navigator 4.7 or higher, Mozilla 1.7 or higher, or Firefox 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 5.0 or higher, 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)
Select a SonicWALL Recommended Deployment Scenario

The following table provides SonicWALL recommended deployment scenarios based on various network configurations.

<table>
<thead>
<tr>
<th>Gateway Device</th>
<th>SonicWALL Recommended Deployment Scenarios</th>
<th>Configuration Requirements</th>
</tr>
</thead>
</table>
| SonicOS Standard 3.1 or higher: TZ 170 PRO 1260 PRO 2040 PRO 3060 | Scenario 1: SSL-VPN on the 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. |
| SonicOS Enhanced 3.1 or higher: TZ 170 Series PRO Series | Scenario 2: 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 Wireless SonicWALL devices running legacy firmware Third-Party Gateway Device | Scenario 3: 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 |
| SonicOS Enhanced 3.1 or higher: TZ 170 Series PRO Series | Scenario 3: SSL-VPN on the LAN | • No unused interfaces  
  • No dedicated interface for a DMZ |

Table 1: SonicWALL SSL-VPN 2000 Deployment Scenarios
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 plug in the SonicWALL SSL-VPN 2000. The Test and Alarm LEDs light up 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 after the SonicWALL SSL-VPN 2000 has booted, restart the SonicWALL SSL-VPN 2000. For more troubleshooting information, refer to the SSL-VPN Administrator’s Guide.

Continue to Step 3
Accessing the Management Interface

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

1. Connect one end of a cross-over cable into the **LAN (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 “Click the OK button.” on page 29.

   **Alert:** A Web browser supporting Java, and HTTP uploads, such as Internet Explorer 5.0 or higher, Netscape Navigator 4.7 or higher, Mozilla 1.7 or higher, or Firefox is recommended*

3. Open a Web browser and enter **https://192.168.200.1** (the default LAN management IP address) in the **Location** or **Address** field.

4. A security warning may appear. Click the **Yes** button to continue.

   * While these browsers are acceptable for use in configuring your SonicWALL SSL-VPN 2000, end users will need to use IE 5.0 or higher, supporting JavaScript, Java, cookies, SSL and ActiveX 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 press the **Login** button.

![SonicWALL SSL-VPN Management Interface](image)

**If the SonicWALL SSL-VPN Login Screen Does Not Appear**

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 SSL-VPN appliance? Management can only be performed through X0.
- Is the link light lit on both the management station and the 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 “Click the OK button.” on page 29 for instructions on setting your IP address.
- Do you have the Ethernet cable connected to your computer and to the X0 port on your SonicWALL SSL-VPN 2000?
- Is your Domain set to Local Domain on the login screen?
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 8
- “Setting Time Zone” on page 9
- “Configuring SSL-VPN Network Settings” on page 9

Setting Your Administrator Password
1. Select 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.
Setting Time Zone
1. Select the System > Time page.
2. Choose the appropriate time zone from the drop-down menu.
3. Click the Apply button.

Note: Setting the time correctly is essential to many of the operation 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 3 to complete this section.

This section includes the following subsections:
- “Configuring DNS / WINS” on page 9
- “Configuring Default Route” on page 10
- “Add A Local User” on page 10
- “Adding a NetExtender Client Route” on page 11

Configuring DNS / WINS
1. Select 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 Apply button.
Configuring Default Route

Refer to the following table to correctly configure your default route. If you do not know your scenario, refer to "Select a SonicWALL Recommended Deployment Scenario" on page 4.

<table>
<thead>
<tr>
<th>If you are using scenario:</th>
<th>Your upstream gateway device will be:</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1 - SSL-VPN on the DMZ</td>
<td>The DMZ you will create (ex: 192.168.200.2)</td>
</tr>
<tr>
<td>#2 - SSL-VPN on existing DMZ</td>
<td>Your existing DMZ interface.</td>
</tr>
<tr>
<td>#3 - SSL-VPN on the LAN</td>
<td>Your LAN gateway.</td>
</tr>
</tbody>
</table>

1. Select **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 **Apply** button.

Add A Local User

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

NetExtender allows remote clients seamless access to resources on your local network.
1. Select the NetExtender > Client Routes page.
2. Click the Add Client Route button.
3. Enter the IP address of the trusted network to which you would like to provide access with NetExtender in the Destination Network field. (For example, if you are connecting to and 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).
4. Enter your subnet mask usually in the Subnet Mask field.
5. Click the Add button to add this client route.

If you are configuring your SSL-VPN using scenario 1, Continue to Step 5, “Connecting the SonicWALL SSL-VPN 2000” on page 14.

If you are configuring your SSL-VPN using scenarios 2 or 3, continue with “Extra Steps for Scenarios 2 and 3” on page 12.

If you do not know your scenario, refer to “Select a SonicWALL Recommended Deployment Scenario” on page 4.
Extra Steps for Scenarios 2 and 3

In this section, you will setup your SonicWALL SSL-VPN 2000 to operate under network configurations given in scenarios 2 and 3. If you do not know your scenario, refer to “Select a SonicWALL Recommended Deployment Scenario” on page 4.

Configuring your Network Interface
1. Select the **Network > Interfaces** page.
2. Click the **Configure** button for the **X0** port.
3. If configuring with scenario 2, enter an unused IP address in your DMZ subnet in the **IP Address** field. If configuring with scenario 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.
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 plus one (e.g. 15 users will require 16 addresses like 192.168.200.100 to 192.168.200.115). The range should fall within the same subnet as the interface to which the SSL-VPN appliance is connected, and in cases where there are other hosts on the same segment as the SSL-VPN appliance, it must not overlap or collide with any assigned addresses. You can determine the correct subnet based on your scenario:

**Scenario 1** – You may leave the NetExtender range at the default (192.168.200.100 to 192.168.200.200)

**Scenario 2** – 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 192.168.50.250, providing they are not already in use.

**Scenario 3** - 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 192.168.168.250, providing they are not already in use.

**Note:** If in scenario 2 or 3 your DMZ or LAN is configured in Transparent mode, depending on address the number of available IP addresses in your network, you might need to switch to a NAT configuration to provide an adequate number of IP addresses for NetExtender sessions.

1. Select the **NetExtender > Client Address** page.
2. Enter an address range for your clients in the **Client Address Range Begin** and **Client Address Range End** fields. If configuring with scenario 2, this must be an unused range within your DMZ subnet. If configuring with scenario 3, this must be an unused range within your LAN subnet.

3. Click the **Apply** button to apply changes.

*Continue to Step 5*
Connecting the SonicWALL SSL-VPN 2000

Before continuing, reference diagrams on the following two pages to connect the SonicWALL SSL-VPN 2000 to your network. Refer to the table in “Select a SonicWALL Recommended Deployment Scenario” on page 4 to determine the proper scenario for your network configuration.

- **Scenarios 1 and 2**, refer to the diagram below.
- **Scenario 3**, refer to the diagram on page 14.

### Scenarios 1 and 2: SSL-VPN on the DMZ or SSL-VPN on existing DMZ

1. Connect one end of a Crossover cable to the OPT, X2, or other unused port on your existing SonicWALL UTM security appliance. If you already have a DMZ set up, connect to the existing DMZ.
2. Connect the other end of the crossover cable to the X0 port on the front of your SonicWALL SSL-VPN 2000. The X0 Port LED to the above left of the port lights up in green indicating an active connection.

*Continue to Step 6*
**Scenario 3: SSL-VPN on the LAN**

1. Connect one end of a Crossover cable to an *unused port* on your LAN hub or switch.
2. Connect the other end of the crossover cable to the **X0** port on the front of your SonicWALL SSL-VPN 2000. The **X0** Port LED to the above left of the port lights up in green indicating an active connection.

*Continue to Step 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 “Select a SonicWALL Recommended Deployment Scenario” on page 4 to determine the proper scenario for your network configuration.

Configuring Web Management Port

For deployments with a single public IP address, configure the default management ports on the gateway device to allow inbound HTTP and HTTPS traffic to pass through to the SonicWALL SSL-VPN 2000 security appliance. HTTPS is required for SSL-VPN operation.

**Note:** Forwarding HTTP to the SSL-VPN is optional. HTTP allows users to access the SonicWALL SSL-VPN 2000, the session is automatically redirected to HTTPS.

After changing the management port on the gateway device, the new port will have to be used for subsequent access to the gateway device on any interface, for example: http://192.168.168.168:81 or https://67.115.118.146:444

To modify your default management ports, perform the following steps:

1. Select the **System > Administration** page.
2. Scroll to the **Web Management Settings** section.
3. Change the **HTTP** management port from 80 to an alternative, unused port, such as 81.
4. Change the **HTTPS** management port from 443 to an alternative, unused port, such as 444.
5. Click the **Apply** button at the top of the page.

Proceed to one of the following sections based on your selected deployment scenario:

- “Scenario 1: SSL-VPN on the DMZ” on page 17
- “Scenario 2: SSL-VPN on Existing DMZ” on page 21
- “Scenario 3: SSL-VPN on the LAN” on page 22
Scenario 1: SSL-VPN on the DMZ

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

Note: Remember that you are logging into your SonicWALL UTM security 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.

This section includes the following subsections:
- “Configuring a DMZ or OPT Port in SonicOS Standard” on page 17
- “” on page 18

Configuring a DMZ or OPT Port in SonicOS Standard
1. Select the Network > Settings page.
2. Click Configure button for the DMZ or OPT interface.
3. Select the DMZ in NAT Mode radio button.
4. Enter 192.168.200.1 in the DMZ Private Address field.
5. Enter 255.255.255.0 in the DMZ Subnet Mask field.
6. Click the OK button.
Allowing WAN -> DMZ Connection

1. Select the **Firewall > Access Rules** page.
2. Select **WAN -> DMZ** connection from the matrix.
3. Click the **Configure** button for the WAN -> DMZ connection. 

   ![Rule Settings Table]

4. Change the **Action** field to **Allow**.

   ![Action Field]

   **Note:** While you may use defaults (allow all) for this connection, it is recommended that you customize this rule to conform to your existing security policies for the DMZ.

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


   *Continue to Step 7*
Adding a New SSL-VPN Custom Zone in SonicOS Enhanced

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

4. Enter SSL-VPN in the **Name** field.
5. Select Public from the **Security Type** drop-down menu.
6. Un-check the **Allow Interface Trust** checkbox.
7. Check the **Gateway AV, Intrusion Prevention Service** and **Anti-Spyware** checkboxes.

   **Note:** It is suggested that you do not enable **Enforce Content Filtering Service** or **Network Anti-Virus** on the SSL-VPN zone.

8. Click the **OK** button.
9. Enter the IP address for this interface in the **IP Address** field. (For example “192.168.200.2”. This should be the same address you created in “Configuring Default Route” 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.
Allowing SSL-VPN -> LAN Connection
1. Select the Firewall > Access Rules page.
2. Select Matrix as the View Style.

<table>
<thead>
<tr>
<th>Access Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Style: All Rules Matrix Drop-down Boxes</td>
</tr>
</tbody>
</table>

3. Select SSL-VPN > LAN connection from the matrix.
4. Click the Configure button for the SSL-VPN -> LAN connection.

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>All</td>
</tr>
</tbody>
</table>

5. Change the Action field to Allow.

![Settings](image)

**Note:** While you may use defaults (allow all) for this connection, it is recommended that you customize this rule to conform to your existing security policies for the DMZ.

6. Click the OK button to apply changes.

*Continue to Step 7*
Scenario 2: SSL-VPN on Existing DMZ

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

Note: Remember that you are logging into your SonicWALL UTM security 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.

Allowing SSL-VPN -> LAN Connection
1. Select the Firewall > Access Rules page.
2. In the Matrix view, select SSL-VPN > LAN
3. Change the Action field to Allow.

Note: While you may use defaults (allow all) for this connection, it is recommended that you customize this rule to conform to your existing security policies for the DMZ.

4. Click the OK button to apply changes.

Setting Public Server Access
- Users of SonicOS Standard, continue to “Setting Public Server Access in SonicOS Standard” on page 23
- Users of SonicOS Enhanced, continue to “Setting Public Server Access in SonicOS Enhanced” on page 24

Continue to Step 7
Scenario 3: SSL-VPN on the LAN

Connecting to the SonicWALL UTM Security Appliance
1. Using a computer connected to your LAN, launch your Web browser and log in to your current gateway interface.

Configuring your Gateway to Recognize the SonicWALL SSL-VPN 2000

Complete the following steps to configure your gateway to recognize and allow the SonicWALL SSL-VPN 2000 connection.
1. Set your gateway’s web management port to 444
2. Configure your gateway device to allow an outside connection through the SSL-VPN into your Local Area Network.

Continue to Step 7
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 the IP address of your SSL-VPN device in the **Server IP Address** 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.

For more information on configuring your SonicWALL security appliance with SonicWALL GAV, IPS and Anti-Spyware, refer to the SonicWALL SSL-VPN Administrator’s Guide.

*Continue to Step 7*
Setting Public Server Access in SonicOS Enhanced

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

5. Click the Next button to continue the Wizard.
6. Enter SSL-VPN in the Server Name 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. (This should be the same IP address you recorded in Step 1, “Applying Power to the SonicWALL SSL-VPN 2000” on page 5.)
11. Click the Next Button.
12. Click the Apply Button.

For more information on configuring your SonicWALL security appliance with SonicWALL GAV, IPS, and Anti-Spyware, refer to the SonicWALL SSL-VPN Administrator’s Guide.
Testing Your SSL-VPN Connection

Now you have configured your SonicWALL UTM security 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:
   \[https://<WAN_IP_address_of_gateway_device>\]

2. When prompted, enter the User Name and Password created in “Add A Local User” on page 10 of this guide.

3. Select LocalDomain from the drop-down menu and click the Login button.

4. The SonicWALL Virtual Office screen appears in your Web browser.

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

6. Click the NetExtender Button and complete the client installation. The following message is displayed:
   
   **Status:** Connected

7. 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.
Still Having Trouble Connecting? Did You…

**Restarting your Management Station**

Your management station may need to restart to accept new network settings from the DHCP server in the SonicWALL security appliance.

**Restarting your DSL Modem**

Your DSL Modem may need to restart to communicate with the DHCP Client in the SonicWALL security appliance.

*For more troubleshooting information, refer to the SonicWALL SSL-VPN Administrator's Guide.*
Registering Your SonicWALL SSL-VPN 2000

Before You Register

Make sure the DNS and Time settings on your SonicWALL SSL-VPN 2000 are correct when you register the device. Configure Time settings in the System > Time page. Configure DNS settings in the Edit Interface window from the Network > Interfaces page.

You need a mySonicWALL.com account to register the SonicWALL SSL-VPN 2000. You can create a new mySonicWALL.com account directly from the SonicWALL management interface.

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

Registering with MySonicWALL

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. If the System > Status page is not displaying in the management interface, click System in the left-navigation menu, and then click Status.
3. On the System > Status page, in the Security Services section, click the Register link. The mySonicWALL.com Login page is displayed.

4. Enter your mySonicWALL.com account username and password in the User Name field.
5. At the top of the Product Survey page, Enter a “friendly name” for your SonicWALL content security appliance in the Friendly Name field.
6. Please complete the Product Survey. SonicWALL uses this information to further tailor services to fit your needs.
7. Click Submit.
8. When the mySonicWALL.com server has finished processing your registration, you will see a page informing you that your SonicWALL SSL-VPN 2000 is registered. Click Continue.

Congratulations

Your SonicWALL SSL-VPN 2000 is now fully operational.
Configuring Dynamic DNS

Using any Dynamic DNS service begins with setting up an account with the DDNS service provider (or providers) of your choice. It is possible to use multiple providers simultaneously. Refer to the links for the various providers listed above. The registration process normally involves a confirmation e-mail from the provider, with a final acknowledgment performed by visiting a unique URL embedded in the confirmation e-mail.

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 security appliance to use your DDNS service.

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

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

2. If Enable this DDNS Profile is checked, the profile is administratively enabled, and the SonicWALL security appliance takes the actions defined in the Online Settings section on the Advanced tab.

3. If Use Online Settings is checked, 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. Check **Backup MX** if you

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 Providers 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 security 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 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 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.
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.
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 PRO device 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. Choose a mounting location where all four mounting holes line up with those of the mounting bars of the 19-inch rack mount cabinet.
- Mount in a location away from direct sunlight and sources of heat. A maximum ambient temperature of 104º F (40º C) is recommended.
- Route cables away from power lines, fluorescent lighting fixtures, and sources of noise such as radios, transmitters, and broadband amplifiers.
- 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

**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.

**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.

**Packet** - A unit of information transmitted over the internet or within any TCP/IP network. Packets have a header, which contains information about the source, destination, and protocol to be used for the data, and a body, which contains the data being transmitted.

**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 subnetnumber.

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

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

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

**WAN** - A Wide Area Network is a geographically distributed network composed of multiple networks joined into a single large network. The Internet is a global WAN.
SonicWALL SSL-VPN 2000 Security Appliance Regulatory Statement and Safety Instructions

<table>
<thead>
<tr>
<th>Regulatory Model/Type</th>
<th>Product Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1RK0A-02A</td>
<td>SSL-VPN 2000</td>
</tr>
</tbody>
</table>

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

**Lithium Battery Warning**

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

**Cable Connections**

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

© 2005 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.


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.