

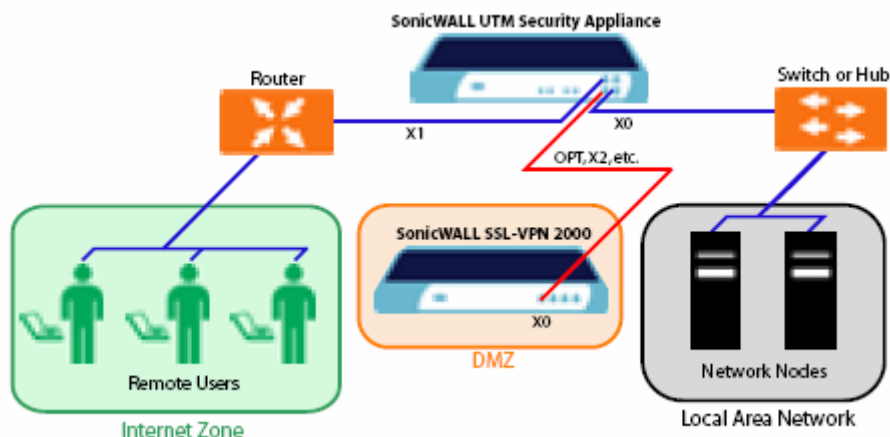
Tech Note

SSL-VPN

Using SonicWALL NetExtender to Access FTP Servers

Problem:

Using **NetExtender** to access an FTP Server on the LAN segment of a SonicWALL PRO 4060.



Solution:

Perform the following setup steps. Step 1-4 are for the administrator while Step 5 is for the remote user.

1. Configure the SonicWALL PRO 4060 (running SonicOS Enhanced firmware) so that we can connect a SonicWALL SSL-VPN appliance to it.
 - a) Create a new public zone named **SSL-VPN**.
 - b) Configure the X2 port with an appropriate IP address (192.168.200.2/24 in our case) and assign it to the X2 zone.
 - c) Change the management port numbers for HTTP/HTTPS
 - d) Configure a port forwarding policy using the Public Server Wizard (alternatively an IP mapping policy can also be configured here).
 - e) Configure the appropriate access rules.
2. Configure the SonicWALL SSL-VPN appliance in stand-alone mode (PC connected to the X0 port of the SonicWALL SSL-VPN appliance via cross-over cable) for basic network connectivity.
 - a) For the X0 port, setup the IP and mask.
 - b) Setup the default route.
3. Connect the SonicWALL SSL-VPN appliance (X0 Interface) to the SonicWALL PRO 4060 (X2 in our case), and finalize the SSL-VPN configuration.
 - a) Create a Local User in Local Domain.
 - b) Add a Range for the NetExtender.
 - c) Add Routes for NetExtender (in our case, it should know how to get to the FTP Server).
4. Setup an FTP Server on the LAN segment of the SonicWALL PRO 4060.

Tech Note

- As a Remote User, make a connection to the SonicWALL SSL-VPN appliance, and the access FTP Server using NetExtender.

IP Addressing Scheme for PRO 4060

X0: 192.168.168.168/24

X1: 200.1.1.2/29

X2: 192.168.200.2/24

Default Gateway: 200.1.1.1

PC sitting on X0 of PRO 4060

IP : 192.168.168.100/24

Default Gateway: 192.168.168.168

IP Addressing Scheme for SSL-VPN

X0: 192.168.200.1/24

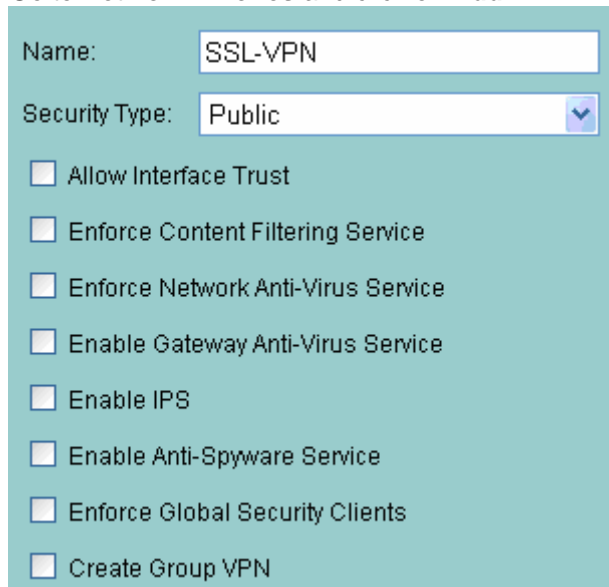
Default Gateway: 192.168.200.2

1. PRO 4060 Configuration

We are assuming the SonicWALL PRO 4060 is already connected to the Internet which means that LAN Hosts (i.e., 192.168.168.100) can go the Internet and no configuration is required for the XO and X1 ports.

a) Create a New Public Zone by the name SSL-VPN

Go to **Network > Zones** and click on **Add**.



The screenshot shows a configuration window for creating a new public zone. The 'Name' field is set to 'SSL-VPN'. The 'Security Type' is set to 'Public'. Below these fields are several checkboxes, all of which are currently unchecked:

- Allow Interface Trust
- Enforce Content Filtering Service
- Enforce Network Anti-Virus Service
- Enable Gateway Anti-Virus Service
- Enable IPS
- Enable Anti-Spyware Service
- Enforce Global Security Clients
- Create Group VPN

Click **OK**.

Tech Note

b) X2 Configuration and Zone Assignment

Navigate to the **Network > Interface** and click on **Edit** for the X2 port.

Note: In case the X2 port is already in use for some other application, for example, WAN Failover, any other available port should be considered.

Same algorithm will be applied accordingly on the SonicWALL TZ Series.

The screenshot shows the 'Interface 'X2' Settings' configuration page. At the top, there are two tabs: 'General' and 'Advanced', with 'Advanced' selected. The settings are as follows:

- Zone: SSL-VPN (dropdown menu)
- IP Assignment: Static (dropdown menu)
- IP Address: 192.168.200.2 (text input)
- Subnet Mask: 255.255.255.0 (text input)
- Comment: (empty text input)
- Management: HTTP, HTTPS, Ping, SNMP
- User Login: HTTP, HTTPS
- Add rule to enable redirect from HTTP to HTTPS

Click **OK**.

c) Changing Management Port Numbers for HTTP and HTTPS

Go to the **System > Administration** and make the following changes:

The screenshot shows the 'Web Management Settings' configuration page. The settings are as follows:

- HTTP Port: 8080 (text input)
- HTTPS Port: 444 (text input)

Click **Apply**.

Now you will be accessing the SonicWALL PRO units from the X0 port.

<http://192.168.168.168:8080>

<https://192.168.168.168:444>

Tech Note

d) Configure Port Forwarding Policy using Public Server Wizard

Go **Network > NAT Policies**, click **Public Server Wizard** and then click **Next**.

Server Type:	Web Server
Services:	<input checked="" type="checkbox"/> HTTP (TCP 80) <input checked="" type="checkbox"/> HTTPS (TCP 443)

Click **Next** once you are done with the above parameters.

Server Name:	SSL-VPN
Server Private IP Address:	192.168.200.1
Server Comment:	SSL-VPN

Click **Next** once you are done with the above parameters.

Server Public IP Address:	200.1.1.2
---------------------------	-----------

Click **Next** and then click **Apply**.

Click **Apply**. This will complete the Port Forwarding Policy for the SonicWALL SSL VPN appliance. SonicWALL PRO 4060 will create the necessary NAT Policies and Access Rules. Click on **Close** to close the Public Server Wizard.

Tech Note

e) Configure appropriate Access Rules

Go to the **Firewall > Access Rules** and click the **Matrix** radio button. Click the **Edit** button to make the modifications.

Access Rules (SSL-VPN > LAN) Items 1 to 1 (of 1)

View Style: All Rules Matrix Drop-down Boxes

#	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
1	1	Any	Any	Any	Allow	All		<input checked="" type="checkbox"/>	

Access Rules (LAN > SSL-VPN) Items 1 to 1 (of 1)

View Style: All Rules Matrix Drop-down Boxes

#	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
1	1	Any	Any	Any	Allow	All		<input checked="" type="checkbox"/>	

Access Rules (WAN > SSL-VPN) Items 1 to 1 (of 1)

View Style: All Rules Matrix Drop-down Boxes

#	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
1	1	Any	Any	Any	Allow	All		<input checked="" type="checkbox"/>	

Access Rules (SSL-VPN > WAN) Items 1 to 1 (of 1)

View Style: All Rules Matrix Drop-down Boxes

#	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
1	1	Any	Any	Any	Allow	All		<input checked="" type="checkbox"/>	

Once you are done with the changes, click **Ok** on each page.

Note: These are generic access rules. You can make them more specific depending on your network access policy.

2. SSL-VPN Basic Configuration (Stand Alone mode)

Connect the X0 Interface of the SonicWALL SSL-VPN appliance to a PC directly using a cross-over cable and configure the basic parameters, for example, IP address, subnet mask and default route. Make sure your PC is configured for the 192.168.200.x/24 network.

a) IP Assignment to X0 along with the Subnet Mask

In our case, we are using Default IP addressing scheme of the SSL-VPN appliance (X0 = 192.168.200.1/24), therefore we will not be making any changes on the Network > Interface page for the X0 port.

Interface Settings

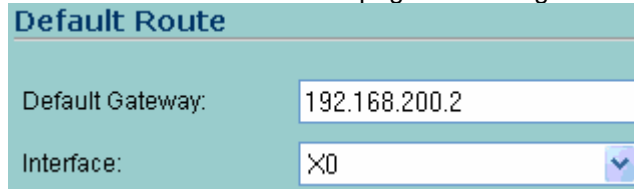
IP Address:

Subnet Mask:

Tech Note

b) Default Gateway Configuration

Go to the **Network > Routes** page and configure the following:



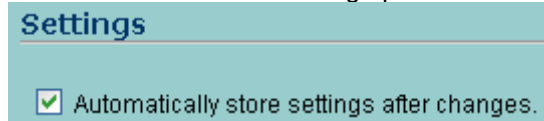
Default Route

Default Gateway:

Interface:

Click **Apply**.

Note: Make sure the following option is checked on **System > Settings**:



Settings

Automatically store settings after changes.

Otherwise, click on the following link on the same page to save the running configuration as a startup configuration.



- 3. Establishing Connectivity between PRO 4060 and SSL-VPN and finalizing the SSL-VPN Configuration**
Connect the X2 port of the SonicWALL PRO 4060 to the X0 port of the SonicWALL SSL-VPN appliance either directly or using a hub or switch, depending on your network configuration.

To access the SonicWALL PRO 4060, enter the following in a Web browser.

<http://200.1.1.2:8080>

<https://200.1.1.2:444>

Note: Assumption is that, HTTP and HTTPS is enabled for the X1 port on the SonicWALL PRO 4060.

To access the SonicWALL SSL-VPN appliance, enter the following in a Web browser.

<http://200.1.1.2>

<https://200.1.1.2>

Perform the following steps in the SonicWALL SSL-VPN appliance to finalize the configuration.

Tech Note

a) Create a Local User in Local Domain

Go to the **Users > Local Users** and click **Add User**.

Add Local User

User Name:

Group/Domain:

Password:

Confirm Password:

User Type:

Click **Add**.

b) Add a Range for the NetExtender

Go to the **NetExtender > Client Address** and configure the following accordingly:

Client IP Address Range

Client Address Range Begin:

Client Address Range End:

Click **Apply**.

c) Add Routes for NetExtender

Go to **NetExtender > Client Routes** and click **Add Client Route**.

Add Client Route

Destination Network:

Subnet Mask:

Click **Add**.

Note: Above configuration is equivalent to "Route All" where a remote client will be sending all of its traffic to the SSL-VPN appliance.

Tech Note

4. Setting up an FTP Server on the LAN segment of the SonicWALL PRO 4060.

In our case, set up the FTP Server on 192.168.168.100.

Either built-in or a third party FTP server, for example, 3COM, can be installed on this PC.

Once service is installed, do a Local FTP for verification.

5. Remote Connection to FTP Server using NetExtender

Forward the following info to a remote user:

<https://200.1.1.2>

Username : testuser

Password : abc

Domain: LocalDomain

Enter <https://200.1.1.2> in a browser window

The remote user is prompted for a username/password and once the user enters the correct credentials, he will be able to log in, in the default Portal.

Click on NetExtender. An SSL-VPN session will be established and the user will be able get into the remote network.

Upload/download files for verification.

