

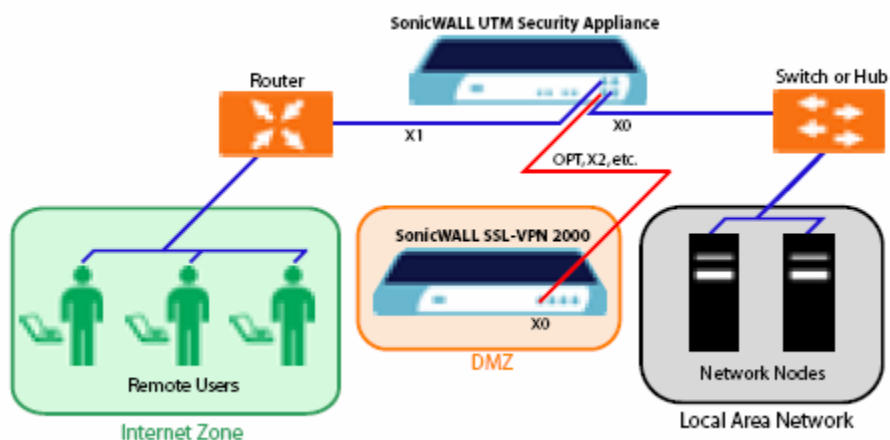
Tech Note

SSL-VPN

Configuring Virtual Office Bookmarks to Access FTP Servers

Problem:

Using **Virtual Office BookMarks**, how a Remote User can access an FTP Server sitting on 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 SSL-VPN device to it.
 - a) Create a new Public zone name **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 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. Now connect 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) Create a Bookmark for FTP Server.
4. Setup an FTP Server on the LAN segment of the SonicWALL PRO 4060.

Tech Note

5. As a Remote User, make a connection to SonicWALL SSL-VPN appliance and then access FTP Server using Virtual Office Bookmark Option.

IP Addressing Scheme for SonicWALL 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 SonicWALL PRO 4060

IP : 192.168.168.100/24

Default Gateway: 192.168.168.168

IP Addressing Scheme for SonicWALL SSL-VPN

X0: 192.168.200.1/24

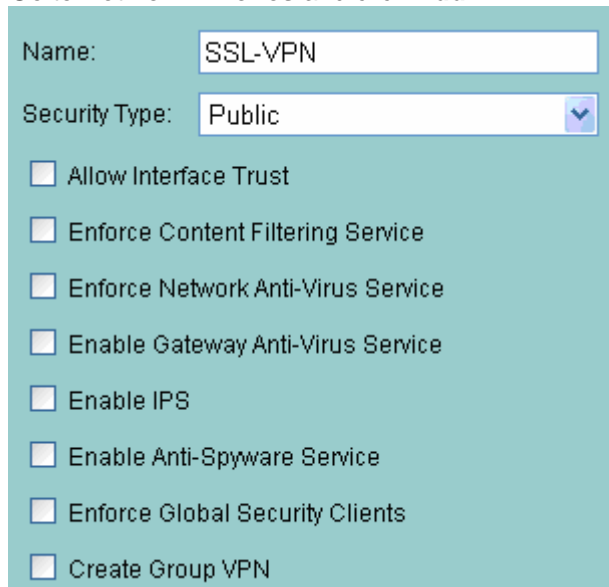
Default Gateway: 192.168.200.2

1. SonicWALL PRO 4060 Configuration

We are assuming the SonicWALL PRO 4060 is already connected to the Internet which means that LAN Hosts (for example, 192.168.168.100) can go the Internet and no configuration is required for the X0 and X1 ports.

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

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



The screenshot shows the configuration form for a new 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

And finally click **Ok**.

Tech Note

b) X2 Configuration and Zone Assignment

Go to the **Network > Interface** and click Edit for X2.

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 'Advanced' tab of the 'Interface 'X2' Settings' configuration page. The 'Zone' is set to 'SSL-VPN' and 'IP Assignment' is set to 'Static'. The 'IP Address' is 192.168.200.2 and the 'Subnet Mask' is 255.255.255.0. The 'Management' section has checkboxes for HTTP, HTTPS, Ping, and SNMP, with HTTP, HTTPS, and Ping checked. The 'User Login' section has checkboxes for HTTP and HTTPS, both unchecked. There is an unchecked checkbox for 'Add rule to enable redirect from HTTP to HTTPS'.

And finally click on **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 'HTTP Port' is set to 8080 and the 'HTTPS Port' is set to 444.

And finally 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 the Public Server Wizard**
Go **Network > NAT Policies**, click on **Public Server Wizard** and 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** to complete the Port Forwarding Policy for this SonicWALL SSL-VPN Device and SonicWALL PRO 4060 and create the necessary NAT Policies and Access Rules.
Click **Close** to close the Public Server Wizard.

Tech Note

e) Configure the appropriate access rules.

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

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

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

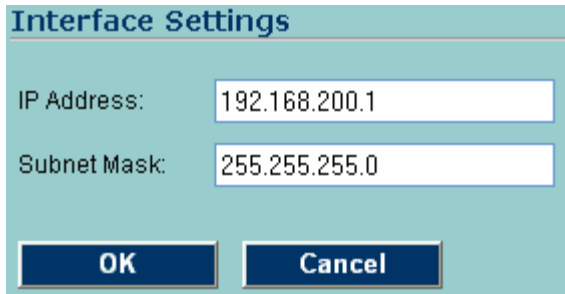
Connect the X0 Interface of the SonicWALL SSL-VPN device to a PC directly via cross-over cable and configure the basic parameters, for example., IP address, subnet mask, and default route. Make sure the PC is configured for 192.168.200.x/24.



Tech Note

a) IP Assignment to X0 along with the Subnet Mask

In this case, use the default IP addressing scheme of SSL-VPN appliance (X0 = 192.168.200.1/24). No custom changes on the **Network > Interface** page for X0 are required.



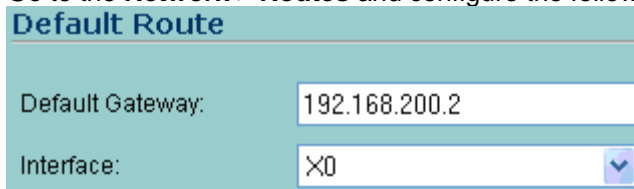
Interface Settings

IP Address:

Subnet Mask:

b) Default Gateway Configuration

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



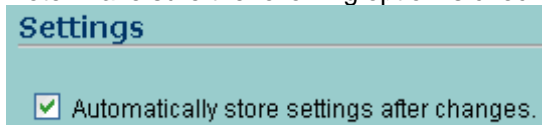
Default Route

Default Gateway:

Interface:

Click on **Apply** once you are done.

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



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.



Tech Note

3. Establishing Connectivity Between PRO4060 and SSL-VPN and Finalizing SSL-VPN Configuration

Connect X2 of PRO4060 to X0 of SSL-VPN either directly or via Hub/Switch, depending on your network configuration.

For accessing PRO4060, enter the following in IE.

<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.

For accessing the SonicWALL SSL-VPN, enter the following in IE.

<http://200.1.1.2>

<https://200.1.1.2>

Perform the following 3 steps in the SonicWALL SSL-VPN device to finalize the configuration.

a) Create a Local User in Local Domain

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

Add Local User

User Name:

Group/Domain: ▼

Password:

Confirm Password:

User Type: ▼

Click on **Add** once you are done with it.

b) Create a Book Mark for FTP Server

Go to Virtual Office, and click on **Add Bookmark**.

Add Bookmark

Bookmark Name:

Name or IP Address:

Service: ▼

Click on **Add**, once you are done.

Virtual Office Bookmarks	Host/IP Address	Service	Configure
FTP Server	192.168.168.100	File Transter Protocol	 

Tech Note

4. Setting up on an FTP Server on 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 3rd Party FTP Server, for example, 3COM, can be installed on this PC.

Once service is installed, try to do a local FTP, for verification.

5. Remote Connection to FTP Server using Virtual Office Bookmarks

Forward the following 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 correct credentials are entered the user will be able to login, in the default Portal.

Click on FTP Server under Virtual Office Bookmarks, the user will be prompted for the FTP Server's Username/Password, and once the correct credentials are entered, the user be able to upload/download the files.

Upload/download files to verify.

