



**Adding a subnet to an existing  
Site to Site VPN Tunnel  
(SonicOS Enhanced)(KB Article  
and**

**KNOWLEDGE  
DATABASE**

## Adding a subnet to an existing Site to Site VPN Tunnel (SonicOS Enhanced)(KB Article and Video Tutorial)

### DESCRIPTION:

VPN: Adding a subnet to an existing Site to Site VPN Tunnel (SonicOS Enhanced)(KB Article and Video Tutorial)

### RESOLUTION:

### Feature/Application:

Adding a subnet or subnets to an existing Site to Site VPN Tunnel (SonicOS Enhanced). This scenario based article illustrates how additional subnet/s can be added to an active Site to Site VPN tunnel between two Sonicwall appliances.

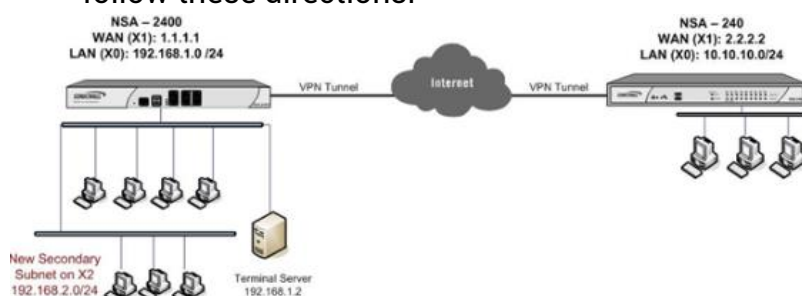
In this scenario we have an active VPN tunnel between a NSA 2400 (Site A) at the central site and a NSA 240 (Site B) at the remote site with the following configuration:

**Site A : NSA 2400: X1: WAN - 1.1.1.1**  
**X0: LAN - 192.168.1.0/24**

**Site B: NSA 240: X1: WAN - 2.2.2.2**  
**X0: LAN - 10.10.10.0/24**

The Tunnel is up and both sites are able to access the other site's LAN segment.

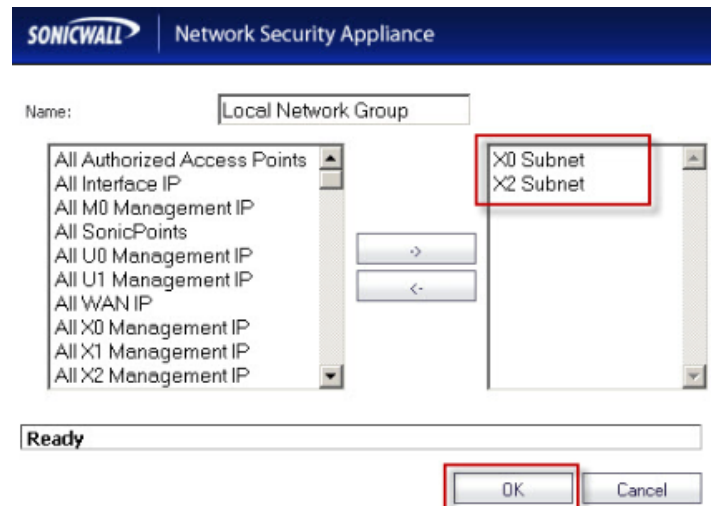
Site A has expanded their network to include a DMZ segment to their local network: **X2: DMZ - 192.168.2.0/24**. In order to add the new subnets to the site to site VPN tunnel follow these directions:



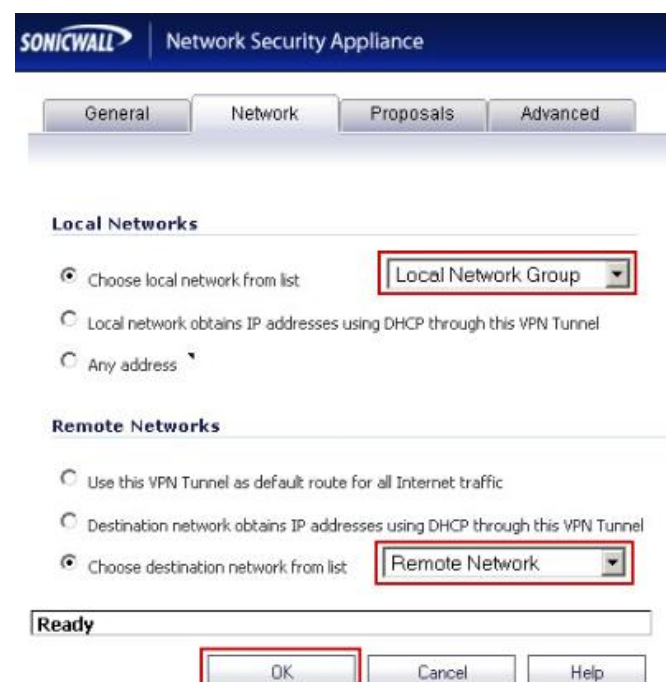
### Procedure:

#### Central Site Configuration (Site A)

Step 1. Create a group called Central Site Network and add the default Address Objects X0 Subnets and X2 Subnets to it.



Step 2. Edit the VPN Policy and select the group Central Site Network from the "Choose local network from list" drop-down list under Local Networks in the Network tab.



Step 3. Click on OK to save the settings.

## Remote Site Configuration (Site B)

Step 1. Create an Address Object called Central Site DMZ with the following settings:

**Name:** Central Site DMZ

**Zone:** VPN

**Type:** Network

**Network:** 192.168.2.0

**Net Mask:** 255.255.255.0

**SONICWALL Network Security Appliance**

Name:

Zone Assignment:

Type:

Network:

Netmask:

Ready

Step 2. Create a group called Central Site Network and add Address Objects Central Site LAN and Central Site DMZ to it. Here it is assumed that an address object Central Site LAN was created when configuring the Site to Site VPN.

Step 3. Edit the VPN Policy and select the group Central Site Network from the "Choose destination network from list" drop-down list under Destination Networks in the Network tab.

**SONICWALL Network Security Appliance**

General | **Network** | Proposals | Advanced

**Local Networks**

Choose local network from list

Local network obtains IP addresses using DHCP through this VPN Tunnel

Any address

**Remote Networks**

Use this VPN Tunnel as default route for all Internet traffic

Destination network obtains IP addresses using DHCP through this VPN Tunnel

Choose destination network from list

Ready

## How to Test:

Ping from a workstation on the Remote Site to a workstation in the X2 subnet on the Central Site, for eg. 192.168.2.2. Refresh the VPN > Settings page on both side and you should see a green icon on both LAN and DMZ segments.

**VPN Policies**

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
1	WAN Group/VPN			ESP: 3DES/MAC SHA1 (IKE)	<input checked="" type="checkbox"/>	
2	WLAN Group/VPN			ESP: 3DES/MAC SHA1 (IKE)	<input type="checkbox"/>	
3	To Central Site	1.1.1.1		192.168.1.1 - 192.168.1.255 192.168.2.1 - 192.168.2.255	<input checked="" type="checkbox"/>	

Site To Site Policies: 1 Policies Defined, 1 Policies Enabled, 10 Maximum Policies Allowed  
 Group/VPN Policies: 2 Policies Defined, 1 Policies Enabled, 6 Maximum Policies Allowed

**Currently Active VPN Tunnels**

#	Created	Name	Local	Remote	Gateway	Renegotiate
1	02/25/2010 23:34:33	To Central Site	10.10.10.1 - 10.10.10.255	192.168.1.1 - 192.168.1.255	1.1.1.1	<input type="button" value="Renegotiate"/>
2	02/25/2010 23:34:32	To Central Site	10.10.10.1 - 10.10.10.255	192.168.2.1 - 192.168.2.255	1.1.1.1	<input type="button" value="Renegotiate"/>