Dynamic Route Based VPN in SonicOS 5.9.0 - Basic Config

KNOWLEDGE DATABASE

SONICWALL Knowledge Database

Dynamic Route Based VPN in SonicOS 5.9.0 - Basic Config

Beginning with SonicOS 5.9.0, configuring dynamic route based VPN has changed from previous versions. In the new configuration method, a Tunnel Interface must be configured under **Network | Interfaces** page and OSPF configured on the Tunnel Interface under **Network | Routing | Advanced Routing** page.

This articles describes the basic method to perform this task.

- The first step involves creating a Tunnel Interface VPN policy . The crypto suites used to secure the traffic between two end-points are defined in the policy.
- The second step is to create a new Tunnel Interface under **Network | Interfaces**.
- The third step involves configuring OSPF for the Tunnel Interface under **Network |Routing**.
- The fourth step involves creating access rules from LAN/DMZ to VPN and from VPN to LAN/DMZ to allow traffic over the VPN.

In this scenario a Dynamic Route-based VPN is configured between an NSA 2400 (Site A) and an NSA 220 (Site B). For this article, we'll be using the following IP addresses as examples to demonstrate the VPN configuration. You can use these examples to create VPN policies for your network, substituting your IP addresses for the examples shown here:

Site A - NSA 2400

WAN (X1): 1.1.1.1
LAN (X0) Subnet: 10.10.10.0/24
Tunnel Interface IP: 192.168.1.1/24

Site B - NSA 220

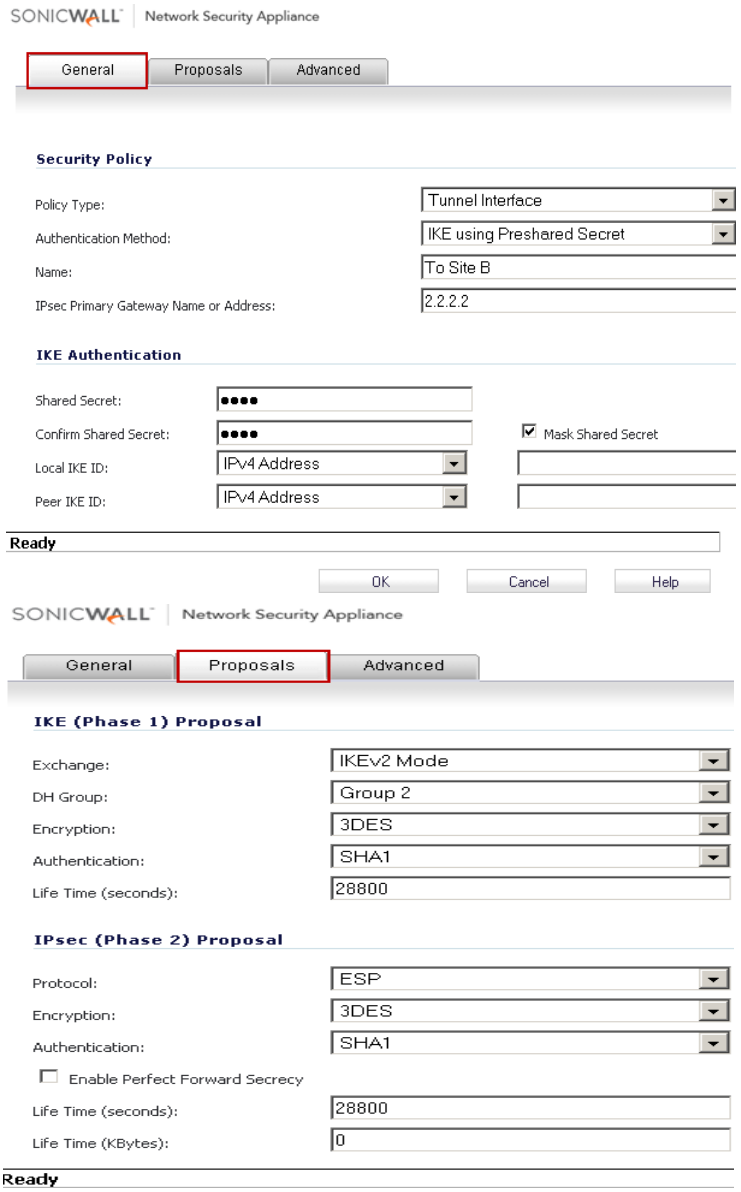
WAN (X1): 2.2.2.2
LAN (X0) Subnet: 192.168.168.0/24
Tunnel Interface IP: 192.168.1.2/24

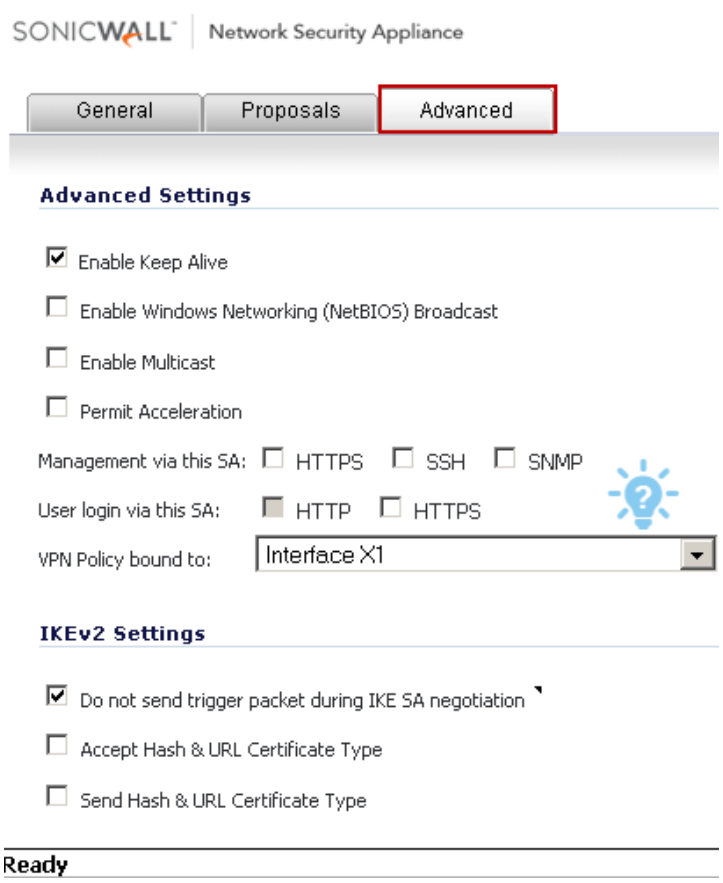
Site A (NSA 2400) Configuration

1. Adding a Tunnel Interface VPN policy
2. Create and configure a tunnel interface
3. Configuring OSPF for a Tunnel Interface
4. Adding rules to allow traffic over the VPN

Adding a Tunnel Interface VPN policy

01. Login to the SonicWall management interface.
02. Navigate to the **VPN** | **Settings** page.
03. Click on the **Add** button to create a tunnel interface VPN as per the screen shots.

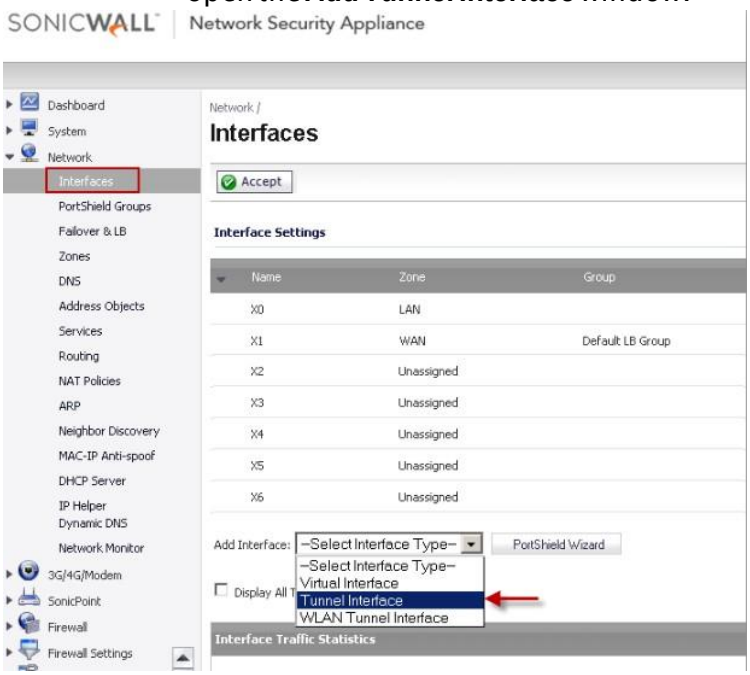




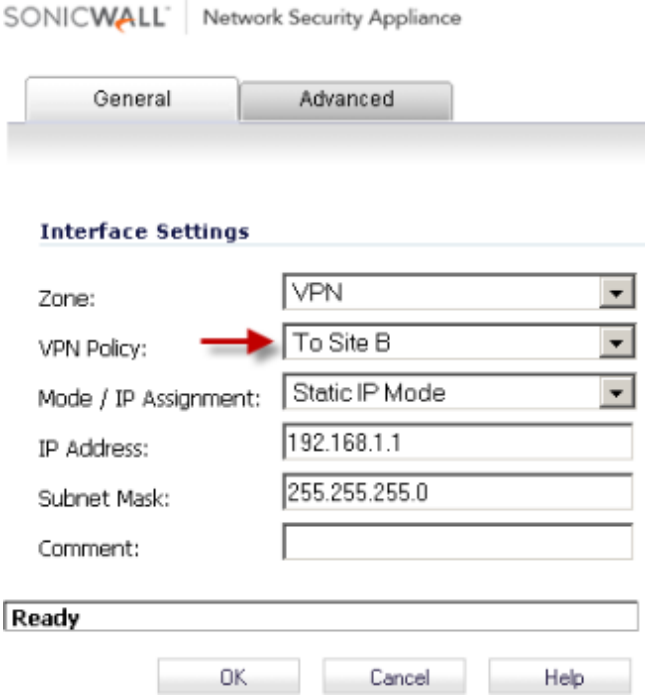
Create and configure a Tunnel Interface

01. Navigate to the **Network** | **Interfaces** page.

02. Select **Tunnel Interface** from the **Add** Interface drop-down menu to open the **Add Tunnel Interface** window.

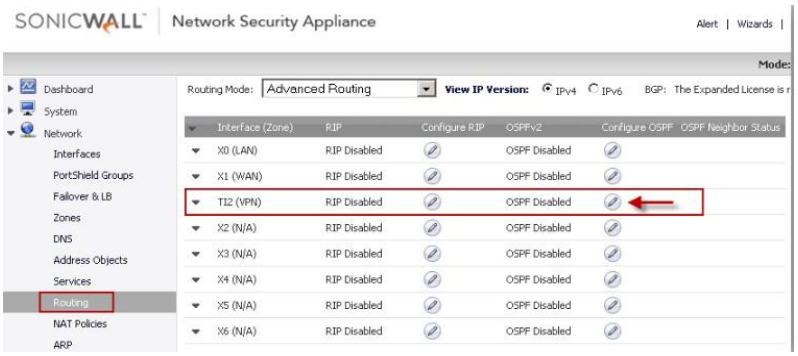


03The **Zone** will be pre-selected with VPN.
04. Under **VPN Policy**, select the VPN policy created earlier.
05. **Mode / IP Assignment** will be pre-selected with **Static IP Mode**.
06. Under **IP Address** and **Subnet Mask**, enter an IP address and subnet mask. The remote site must be in the same subnet as this IP address.
07. Click on **OK** to save.

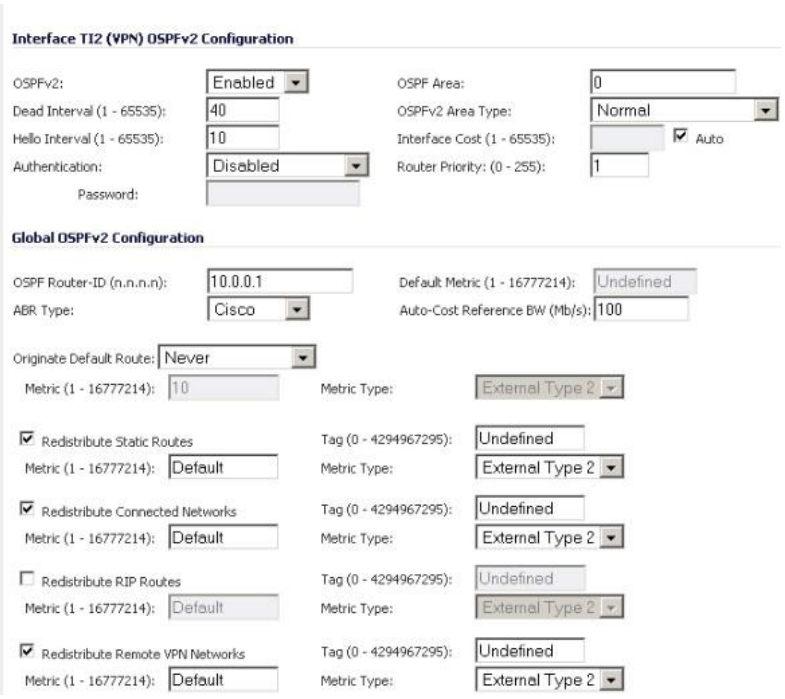


Configuring OSPF for a Tunnel Interface

01. Navigate to the **Network** | **Routing** Page.
02. Click on the drop-down under **Routing Mode** and select **Advanced Routing**.
03. Click on **OK** on the warning window.
04. The tunnel interface created earlier will be visible now.



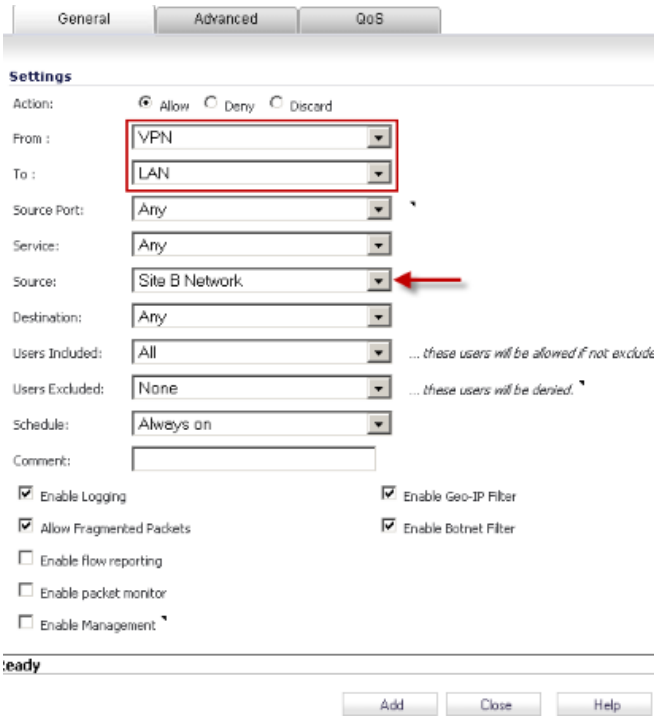
05. Click on the **Configure OSPF** button on the **Tunnel Interface** to open the OSPF configuration window.
06. Enter information as per the screenshot in the **OSPFv2 Configuration** window
07. The **OSPF Router ID** must be a unique IP address in your network.
08. Click on **OK** to save the settings.



Adding rules to allow traffic over the VPN

Although the tunnel will be up and OSPF will be able to detect neighbors, traffic will be blocked to the other side of the tunnel until access rules are created from the local zones to the VPN zone.
01. Navigate to **Network| Address Objects**
02. Click on **Add** to create an address object for the destination network (see screenshot below)

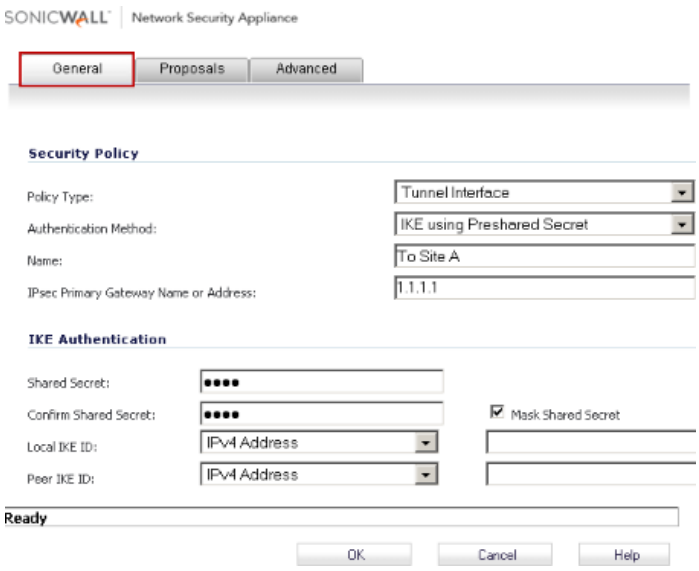
03. Navigate to **Firewall | Access Rules**
04. Go to **LAN** to **VPN**
05. Create an access rule as per the screenshot.

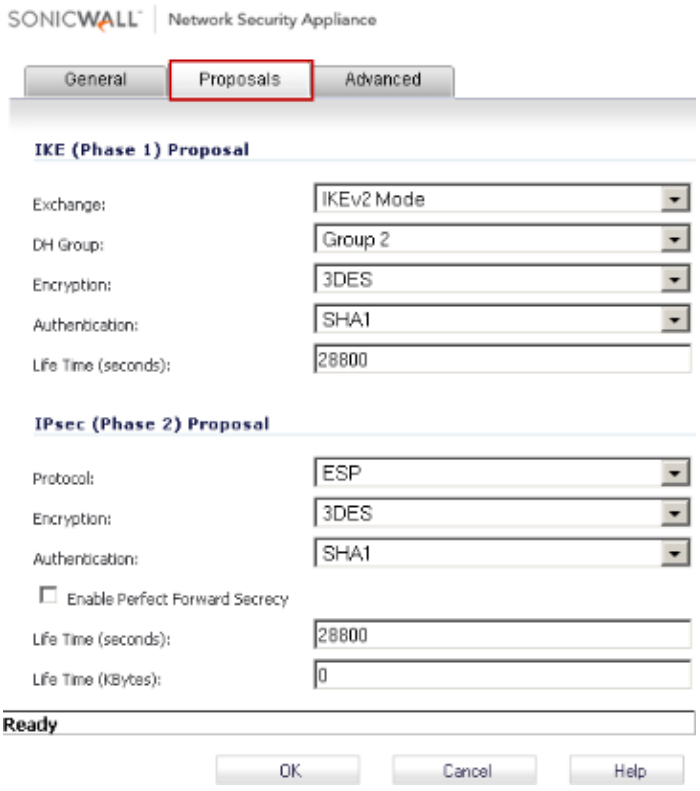


Calle 140 #11-45. Bogotá D.C. Colombia
+57 1 3680290 / +57 318 4914652
sales@itclatam.com / tss@itclatam.com

06. Navigate to **VPN** to **LAN**

07. Create an access rule as per the screenshot.



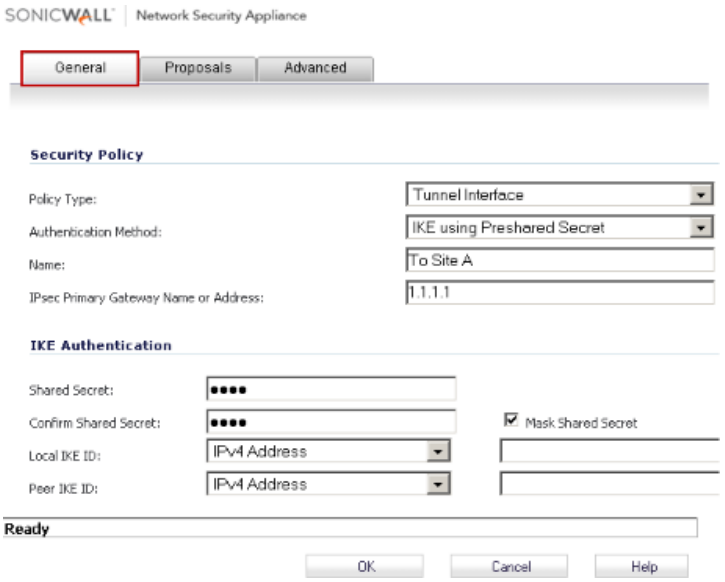


Site B (NSA 220) Configuration

1. Adding a Tunnel Interface
2. Create and configure a Tunnel Interface
3. Configuring OSPF for a Tunnel Interface
4. Adding rules to allow traffic over the VPN

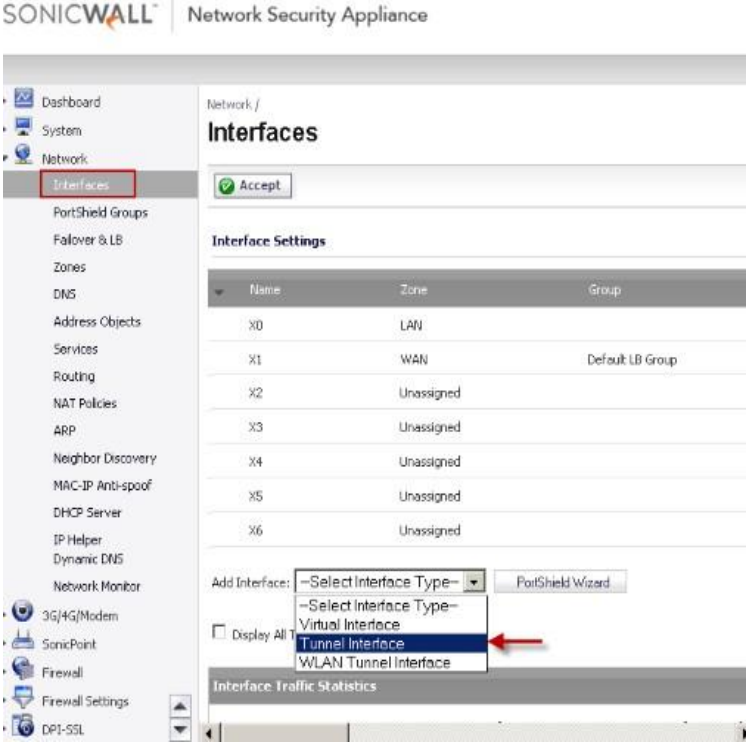
Adding a Tunnel Interface VPN policy

01. Login to the SonicWall management interface.
02. Navigate to the **VPN** | **Settings** page.
03. Click on the **Add** button to create a tunnel interface VPN as per the screen shots.



Create and configure a Tunnel Interface

01. Navigate to the **Network** | **Interfaces** page.
02. Select **Tunnel Interface** from the **Add Interface** drop-down menu to open the **Add Tunnel Interface** window.



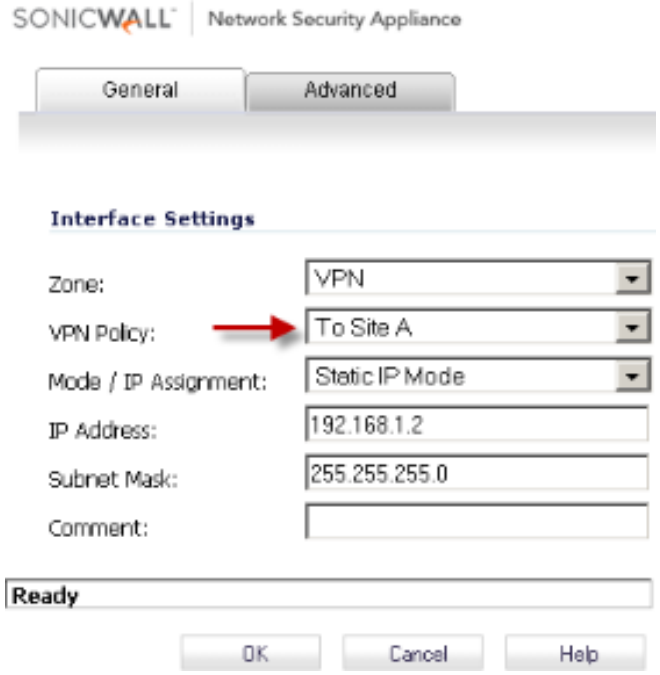
03. In the **Add Tunnel Interface** window, the Zone will be pre-selected with VPN.

04. Under **VPN Policy**, select the VPN policy created earlier.

05. **Mode / IP Assignment** will be pre-selected with **Static IP Mode**.

06. Under **IP Address** and **Subnet Mask**, enter an IP address and subnet mask. The remote site must be in the same subnet as this IP address.

07. Click on **OK** to save.



Configuring OSPF for a Tunnel Interface

01. Navigate to the **Network** | **Routing** Page.

02. Click on the drop-down under **Routing Mode** and select **Advanced Routing**.

03. Click on **OK** on the warning window.

04. The Tunnel Interface created earlier will be visible now.

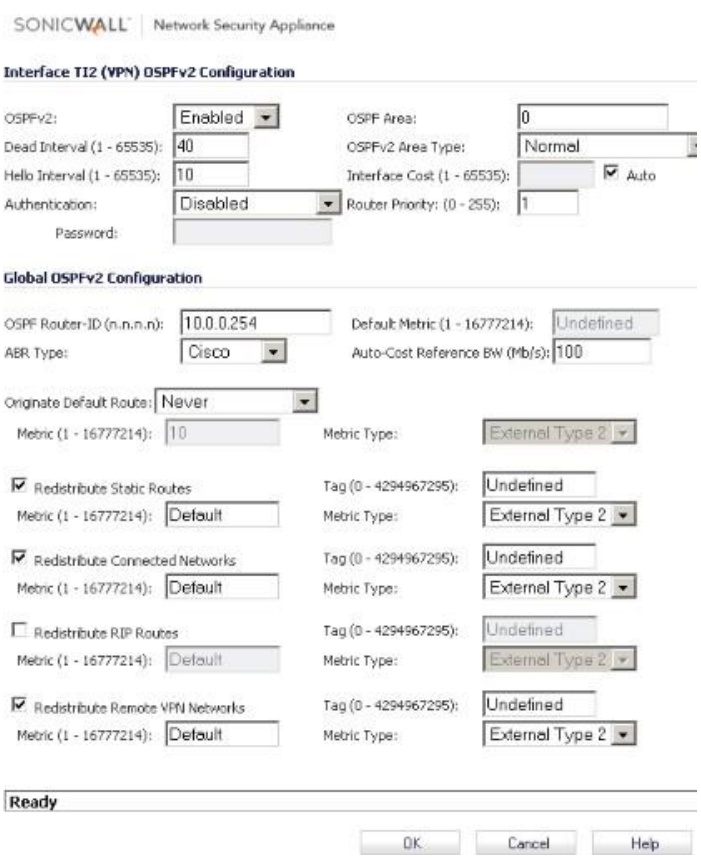
05. Click on the **Configure OSPF** button on the **Tunnel Interface** to open the OSPF configuration window.

06. Enter information as per the screenshot in the **OSPFv2 Configuration** window

07. The **OSPF Router ID** must be a unique IP address in your network.

08. Click on **OK** to save the settings.

Calle 140 #11-45. Bogotá D.C. Colombia
+57 1 3680290 / +57 318 4914652
sales@itclatam.com / tss@itclatam.com

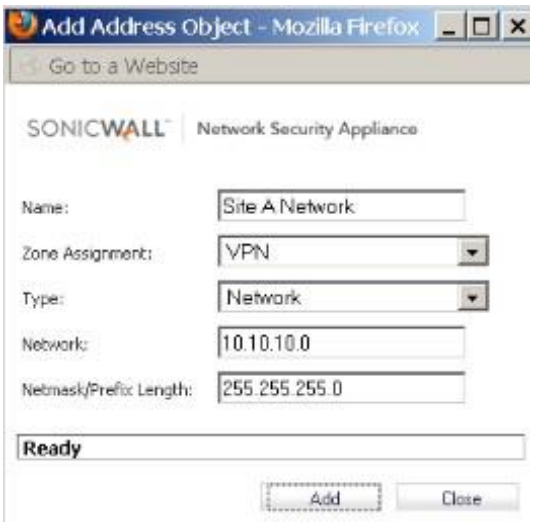


Adding rules to allow traffic over the VPN

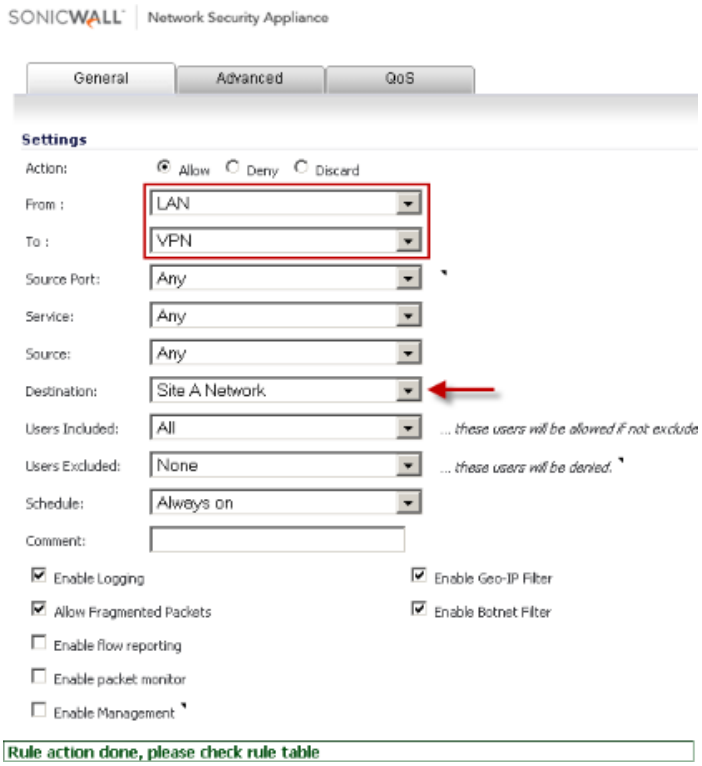
Although the tunnel will be up and OSPF will be able to detect neighbors, traffic will be blocked to the other side of the tunnel until access rules are created from the local zones to the VPN zone.

01. Navigate to **Network** | **Address Objects**

02. Click on **Add** to create an address object for the destination networks and group them (see screenshot below)



03. Navigate to **Firewall** | **Access Rules**
04. Go to **LAN** to **VPN**
05. Create an access rule as per the screenshot.



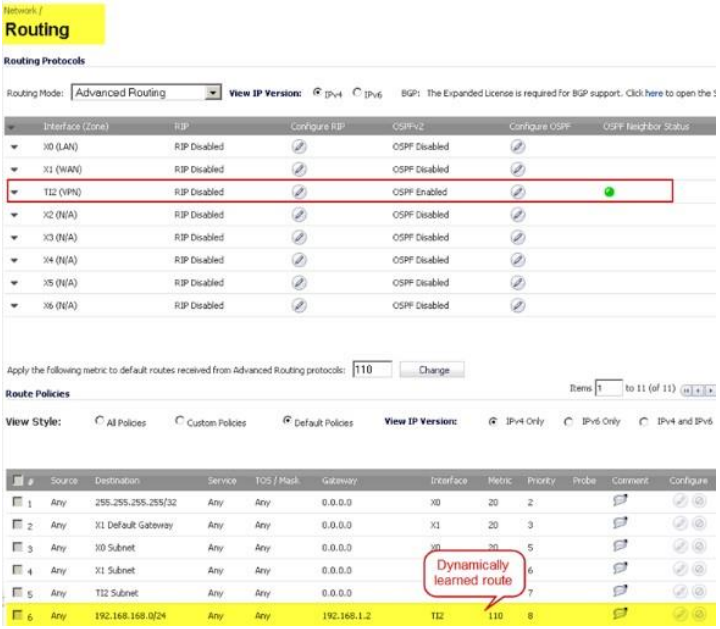
06. Navigate to **VPN** to **LAN**
07. Create an access rule as per the screenshot.

Calle 146 #7-64. Bogotá D.C. Colombia
+57 1 466 0599 / +57 315 786 8258
sales@itclatam.com / tss@itclatam.com

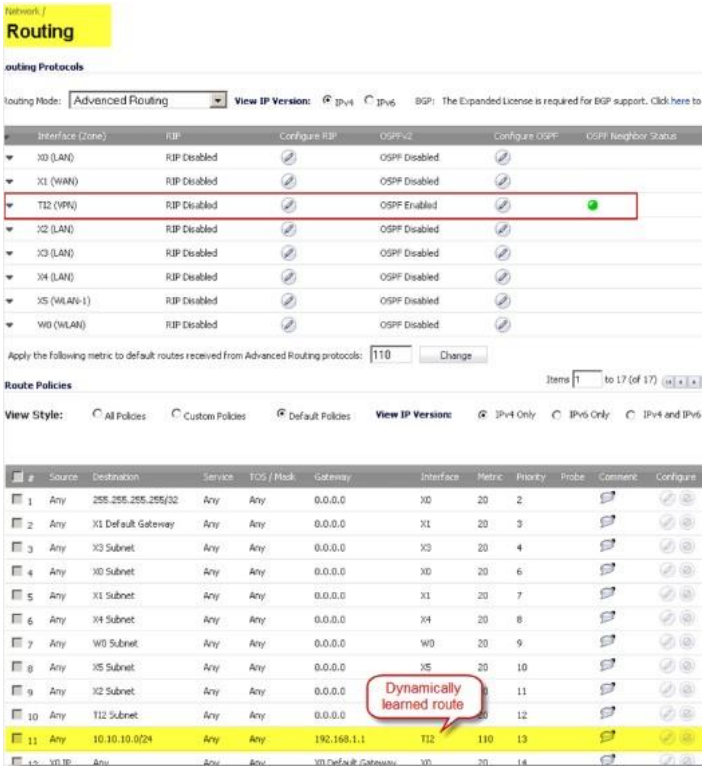
OSPF Neighborship, Dynamic Routes

The VPN tunnel status will be green as soon as the the configuration of the VPN Tunnel Interface policies are completed on both sites.
The screenshots below shows the OSPF neighborship status on both sites and also the dynamically learned routes from each other.

Site A



Site B



Testing

Test by pinging an IP address from one site to another. Only the subnets defined in the access rules will be accessible.

Troubleshooting

Check the following when the VPN tunnel is not up:

1. Gateway IP address.
2. Pre-shared secret
3. Proposal mismatch

Check the following when the VPN tunnel is up but the VPN Tunnel Interface is unable to form neighborship:

1. Make sure the interface the VPN is bound to is not configured in L2 Bridged Mode.
2. Make sure the VPN Tunnel Interfaces are in the same **OSPF Area**
3. **OSPFv2 Areas Type** must have the same area type on both sites. (Normal, Stub Area, Totally Stubby Area, Not-So-Stubby Area, Totally Stubby NSSA)
4. **OSPF Router-ID** should not be duplicate.
5. The Tunnel Interfaces created should be configured with an IP addresses in the same subnet.
6.

Check the following when the VPN Tunnel Interface has formed neighborship but dynamic routes are not present:

1. Make sure the local and destination networks are not overlapping.
2. Make sure **Redistribute Connected Networks** is checked in the OSPFv2 Configuration.

Check the following when unable to pass traffic across the tunnel even after neighborship is formed

1. Make sure OSPF has dynamically learnt the routes to the remote networks. Look under **Route Policies** on the **Network** | **Routing** page.

Calle 146 #7-64. Bogotá D.C. Colombia
+57 1 466 0599 / +57 315 786 8258
sales@itclatam.com / tss@itclatam.com

2. Make sure access rules have been created from local network zones to the VPN zone.
3. Make sure access rules have been created from the VPN zone to local network zones.
4. The zone of local network address objects should match the zone to which that network belongs to. For eg. LAN, DMZ etc
5. The destination network should be assigned zone VPN.
6. Make sure no conflicting rules with higher priority are present.
7. Make sure no conflicting static routes are present in the routing table. Check under **Route Policies** on the **Network** | **Routing** page.

Calle 146 #7-64. Bogotá D.C. Colombia
+57 1 466 0599 / +57 315 786 8258
sales@itclatam.com / tss@itclatam.com