



Dynamic Route Based VPN in
SonicOS 5.9.0 - Basic Config

**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 article 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 NSA220 (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.

SONICWALL® | Network Security Appliance

General Proposals Advanced

Security Policy

Policy Type: Tunnel Interface

Authentication Method: IKE using Preshared Secret

Name: To Site B

IPsec Primary Gateway Name or Address: 2.2.2.2

IKE Authentication

Shared Secret: [Masked]

Confirm Shared Secret: [Masked] Mask Shared Secret

Local IKE ID: IPv4 Address

Peer IKE ID: IPv4 Address

Ready

OK Cancel Help

SONICWALL® | Network Security Appliance

General Proposals Advanced

IKE (Phase 1) Proposal

Exchange: IKEv2 Mode

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 28800

IPsec (Phase 2) Proposal

Protocol: ESP

Encryption: 3DES

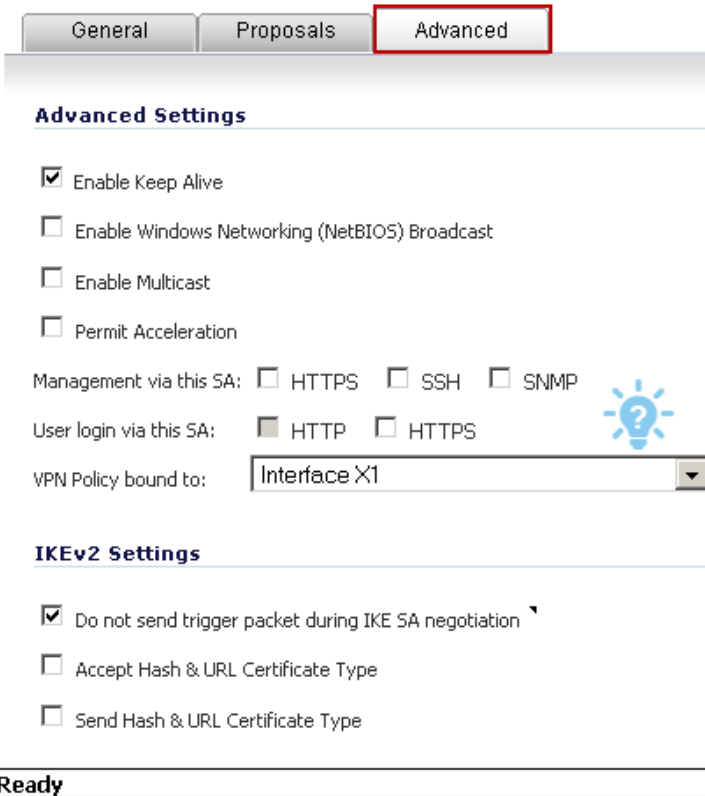
Authentication: SHA1

Enable Perfect Forward Secrecy

Life Time (seconds): 28800

Life Time (KBytes): 0

Ready



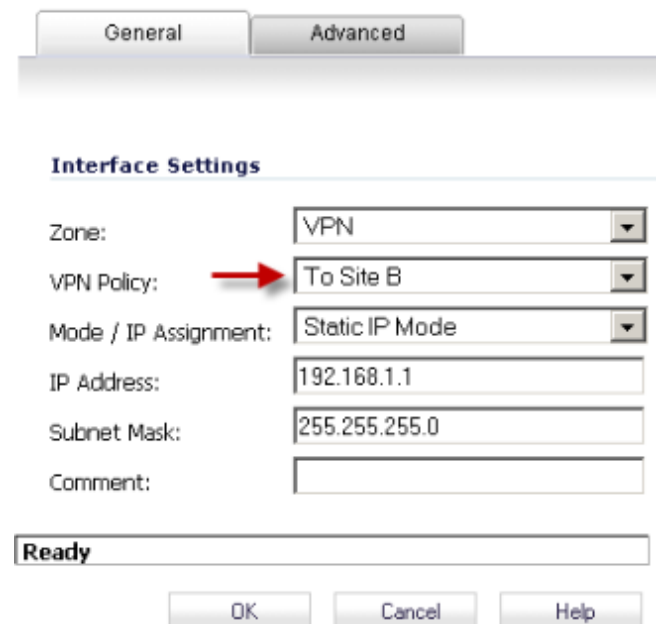
03 The **Zone** will be pre-selected with VPN.

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.

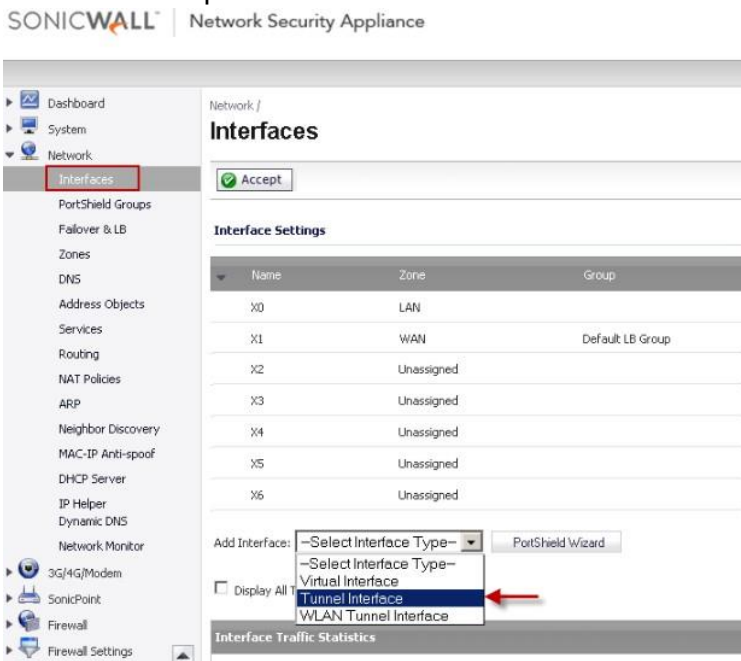
07. Click on **OK** to save.



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.



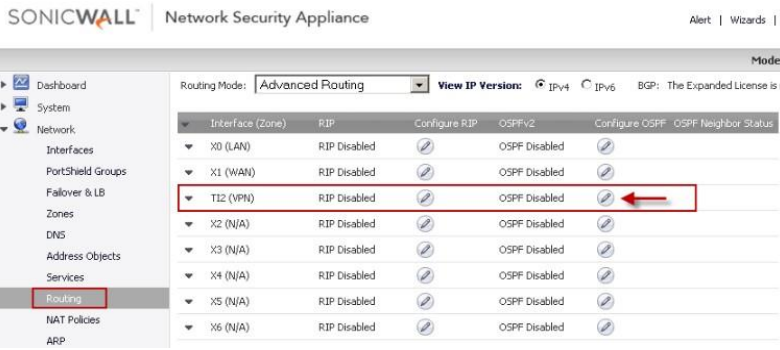
Configuring OSPF for a Tunnel Interface

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

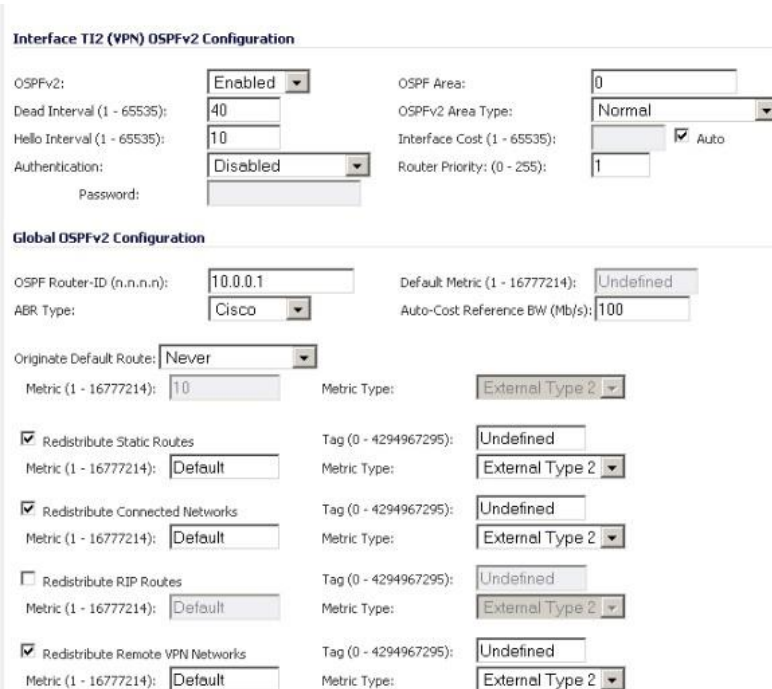
02. Click on the drop-down under **Routing Mode** and select **Advanced Routing**.

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.



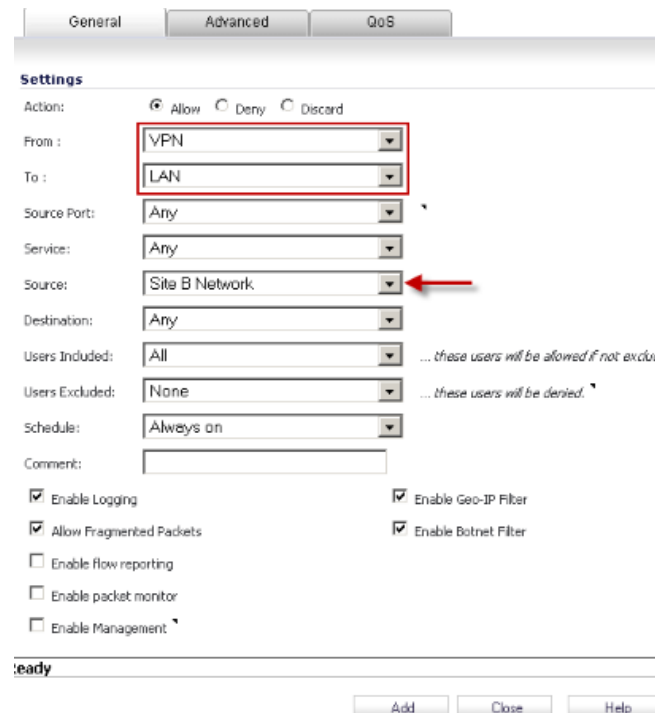
Adding rules to allow traffic over the VPN

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.



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

SONICWALL® Network Security Appliance

General Proposals **Advanced**

Security Policy

Policy Type: Tunnel Interface
 Authentication Method: IKE using Preshared Secret
 Name: To Site A
 IPsec Primary Gateway Name or Address: 1.1.1.1

IKE Authentication

Shared Secret: [Masked]
 Confirm Shared Secret: [Masked] Mask Shared Secret
 Local IKE ID: IPv4 Address
 Peer IKE ID: IPv4 Address

Ready

OK Cancel Help

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.

SONICWALL® Network Security Appliance

General Proposals **Advanced**

Security Policy

Policy Type: Tunnel Interface
 Authentication Method: IKE using Preshared Secret
 Name: To Site A
 IPsec Primary Gateway Name or Address: 1.1.1.1

IKE Authentication

Shared Secret: [Masked]
 Confirm Shared Secret: [Masked] Mask Shared Secret
 Local IKE ID: IPv4 Address
 Peer IKE ID: IPv4 Address

Ready

OK Cancel Help

SONICWALL® Network Security Appliance

General **Proposals** Advanced

IKE (Phase 1) Proposal

Exchange: IKEv2 Mode
 DH Group: Group 2
 Encryption: 3DES
 Authentication: SHA1
 Life Time (seconds): 28800

IPsec (Phase 2) Proposal

Protocol: ESP
 Encryption: 3DES
 Authentication: SHA1
 Enable Perfect Forward Secrecy
 Life Time (seconds): 28800
 Life Time (KBytes): 0

Ready

OK Cancel Help

SONICWALL® Network Security Appliance

General Proposals **Advanced**

Advanced Settings

Enable Keep Alive
 Enable Windows Networking (NetBIOS) Broadcast
 Enable Multicast
 Permit Acceleration

Management via this SA: HTTPS SSH SNMP
 User login via this SA: HTTP HTTPS
 VPN Policy bound to: Interface X1

IKEv2 Settings

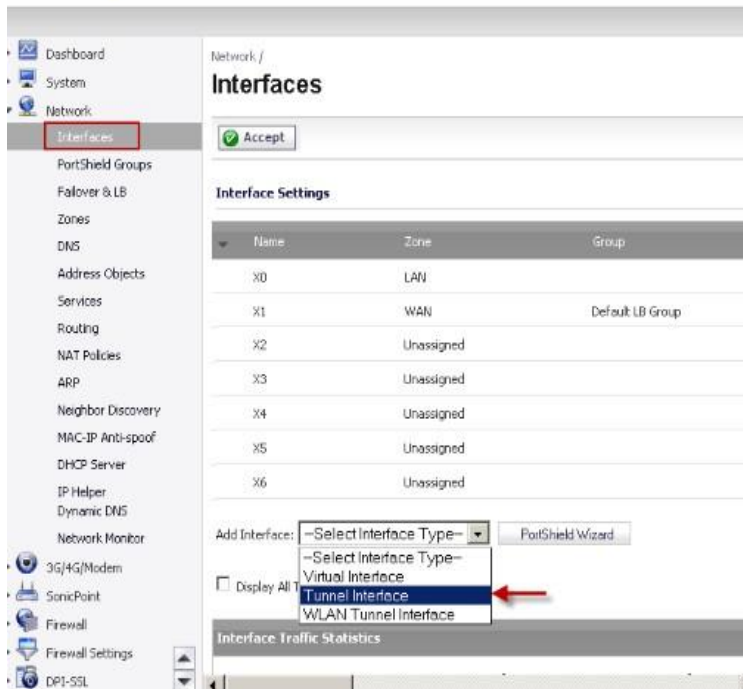
Do not send trigger packet during IKE SA negotiation
 Accept Hash & URL Certificate Type
 Send Hash & URL Certificate Type

Ready

OK Cancel Help

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.



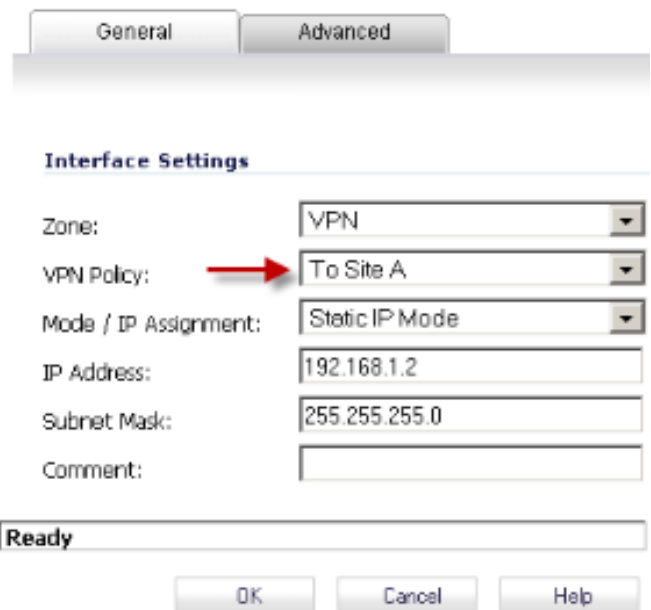
03. In the **Add Tunnel Interface** window, the Zone will be pre-selected with **VPN**.

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.

Interface T12 (VPN) OSPFv2 Configuration

OSPFv2: Enabled
 Dead Interval (1 - 65535): 40
 Hello Interval (1 - 65535): 10
 Authentication: Disabled
 Password:

OSPF Area: 0
 OSPFv2 Area Type: Normal
 Interface Cost (1 - 65535): Auto
 Router Priority (0 - 255): 1

Global OSPFv2 Configuration

OSPF Router-ID (n.n.n.n): 10.0.0.254
 ABR Type: Cisco
 Default Metric (1 - 16777214): Undefined
 Auto-Cost Reference BW (Mb/s): 100

Originate Default Route: Never
 Metric (1 - 16777214): 10
 Metric Type: External Type 2

Redistribute Static Routes
 Metric (1 - 16777214): Default
 Metric Type: External Type 2

Redistribute Connected Networks
 Metric (1 - 16777214): Default
 Metric Type: External Type 2

Redistribute RIP Routes
 Metric (1 - 16777214): Default
 Metric Type: External Type 2

Redistribute Remote VPN Networks
 Metric (1 - 16777214): Default
 Metric Type: External Type 2

Ready

OK Cancel Help

03. Navigate to **Firewall | Access Rules**

04. Go to **LAN to VPN**

05. Create an access rule as per the screenshot.

SONICWALL Network Security Appliance

General Advanced QoS

Settings

Action: Allow Deny Discard

From: LAN
 To: VPN
 Source Port: Any
 Service: Any
 Source: Any
 Destination: Site A Network
 Users Included: All
 Users Excluded: None
 Schedule: Always on

Enable Logging Enable Geo-IP Filter
 Allow Fragmented Packets Enable Botnet Filter
 Enable flow reporting
 Enable packet monitor
 Enable Management

Rule action done, please check rule table

06. Navigate to **VPN to LAN**

07. Create an access rule as per the screenshot.

General Advanced QoS

Settings

Action: Allow Deny Discard

From: VPN
 To: LAN
 Source Port: Any
 Service: Any
 Source: Site A Network
 Destination: Any
 Users Included: All
 Users Excluded: None
 Schedule: Always on

Enable Logging Enable Geo-IP Filter
 Allow Fragmented Packets Enable Botnet Filter
 Enable flow reporting
 Enable packet monitor
 Enable Management

Ready

Add Close Help

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)

Add Address Object - Mozilla Firefox

SONICWALL Network Security Appliance

Name: Site A Network
 Zone Assignment: VPN
 Type: Network
 Network: 10.10.10.0
 Netmask/Prefix Length: 255.255.255.0

Ready

Add Close

OSPF Neighborship, Dynamic Routes

The VPN tunnel status will be green as soon as the configuration of the VPN Tunnel Interface policies are completed on both sites.

The screenshots below show the OSPF neighborship status on both sites and also the dynamically learned routes from each other.

Site A

The screenshot shows the 'Routing Protocols' section for Site A. The 'OSPF Neighbor Status' for the T12 (VPN) interface is green, indicating a successful neighborship. Below, the 'Route Policies' table shows dynamically learned routes from the T12 interface.

#	Source	Destination	Service	TOS / Mask	Gateway	Interface	Metric	Priority	Probe	Comment	Configure
1	Any	255.255.255.255/32	Any	Any	0.0.0.0	X0	20	2			
2	Any	X1 Default Gateway	Any	Any	0.0.0.0	X1	20	3			
3	Any	X0 Subnet	Any	Any	0.0.0.0	X0	20	5			
4	Any	X1 Subnet	Any	Any	0.0.0.0	X1	20	6			
5	Any	T12 Subnet	Any	Any	0.0.0.0	T12	110	7			
6	Any	192.168.168.0/24	Any	Any	192.168.1.2	T12	110	8			

Site B

The screenshot shows the 'Routing Protocols' section for Site B. The 'OSPF Neighbor Status' for the T12 (VPN) interface is green. The 'Route Policies' table shows dynamically learned routes from the T12 interface.

#	Source	Destination	Service	TOS / Mask	Gateway	Interface	Metric	Priority	Probe	Comment	Configure
1	Any	255.255.255.255/32	Any	Any	0.0.0.0	X0	20	2			
2	Any	X1 Default Gateway	Any	Any	0.0.0.0	X1	20	3			
3	Any	X3 Subnet	Any	Any	0.0.0.0	X3	20	4			
4	Any	X0 Subnet	Any	Any	0.0.0.0	X0	20	6			
5	Any	X1 Subnet	Any	Any	0.0.0.0	X1	20	7			
6	Any	X4 Subnet	Any	Any	0.0.0.0	X4	20	8			
7	Any	W0 Subnet	Any	Any	0.0.0.0	W0	20	9			
8	Any	X5 Subnet	Any	Any	0.0.0.0	X5	20	10			
9	Any	X2 Subnet	Any	Any	0.0.0.0	X2	20	11			
10	Any	T12 Subnet	Any	Any	0.0.0.0	T12	110	12			
11	Any	10.10.10.0/24	Any	Any	192.168.1.1	T12	110	13			

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.

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.