ITCorporation

SONICWALL®

• SecureFirst •

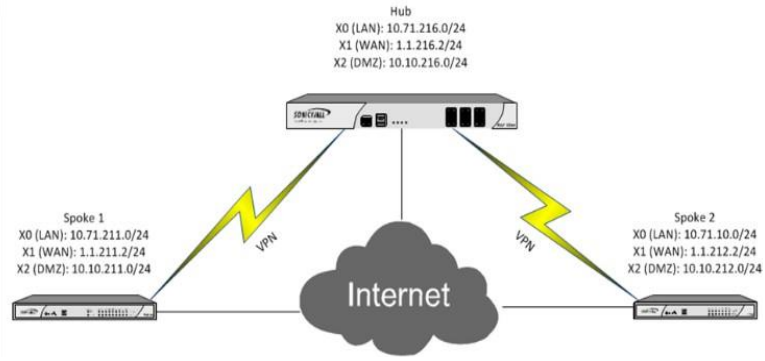
How to create a Hub and Spoke Tunnel Interface VPN network with OSPF

KNOWLEDGE DATABASE

How to create a Hub and Spoke Tunnel Interface VPN network with OSPF

DESCRIPTION:

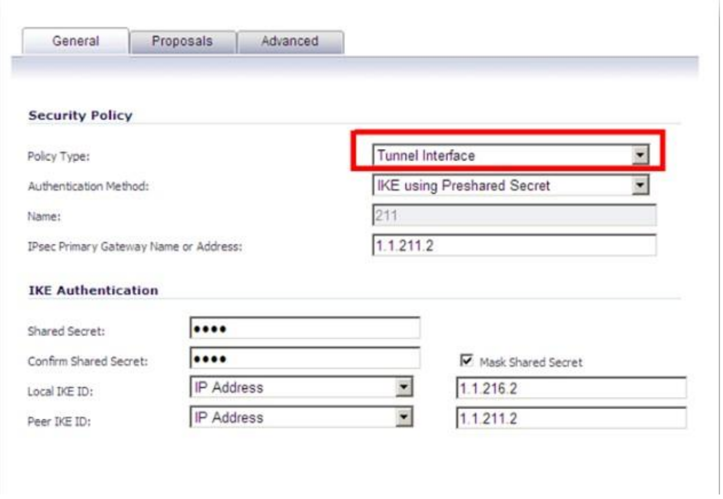
This document explains how to create a Hub and Spoke VPN network architecture using Tunnel Interface and OSPF instead of policy-based Site to Site VPN tunnels.
Dynamic Route-based VPN using Tunnel Interface and OSPF offers a greater flexibility as there is little to do if the network architecture changes. Adding a new Spoke will also be greatly simplified as all the existing spokes will automatically get the new network architecture using OSPF.



CREATION OF THE HUB AND SPOKE VPN ENVIRONMENT

A- <u>HUB</u>

Create VPN tunnel from the hub to both spokes under **VPN | Settings.**
We will first create the tunnel from the Hub to Spoke-1 with gateway IP address 1.1.211.2 in our example.
Under **VPN | Settings**, add a new policy.


General | Proposals | Advanced

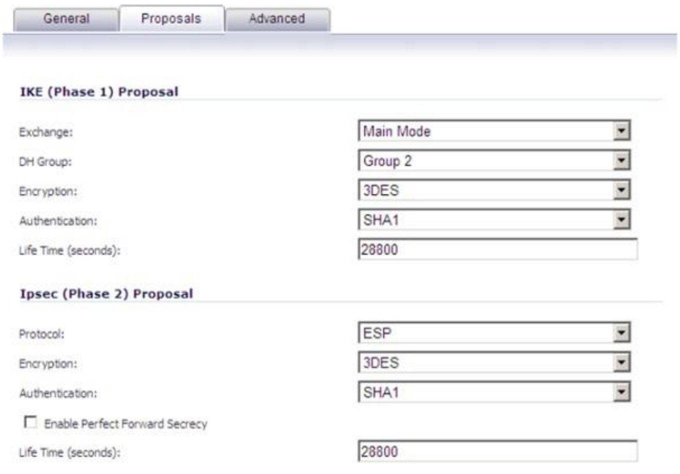
Security Policy

Policy Type: Tunnel Interface
Authentication Method: IKE using Preshared Secret
Name: 211
IPsec Primary Gateway Name or Address: 1.1.211.2

IKE Authentication

Shared Secret: ••••
Confirm Shared Secret: ••••
☑ Mask Shared Secret
Local IKE ID: IP Address 1.1.216.2
Peer IKE ID: IP Address 1.1.211.2

Use a Police Type of Tunnel Interface instead of Site to Site, Enter the remote IP address, the shared secret and IKE Ids


General | Proposals | Advanced

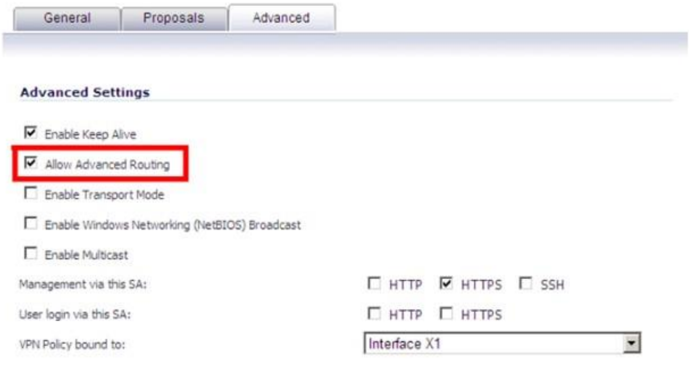
IKE (Phase 1) Proposal

Exchange: Main 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

Proposal options can left as default

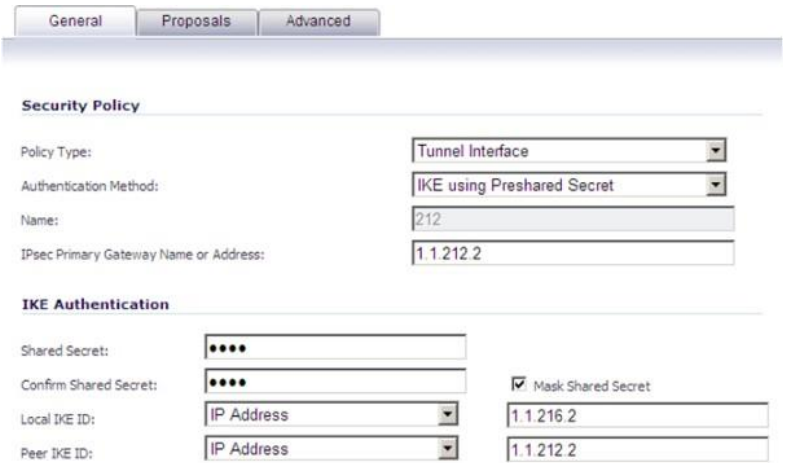

General | Proposals | Advanced

Advanced Settings

☑ Enable Keep Alive
☑ Allow Advanced Routing
□ Enable Transport Mode
□ Enable Windows Networking (NetBIOS) Broadcast
□ Enable Multicast
Management via this SA: □ HTTP ☑ HTTPS □ SSH
User login via this SA: □ HTTP □ HTTPS
VPN Policy bound to: Interface X1

In the Advanced Options), it is important to enable "**Allow Advanced Routing**" as it will allow use of RIP or OSPF

Make similar configuration for the second VPN tunnel to Spoke 2



Security Policy

Policy Type: Tunnel Interface

Authentication Method: IKE using Preshared Secret

Name: 212

IPsec Primary Gateway Name or Address: 1.1.212.2

IKE Authentication

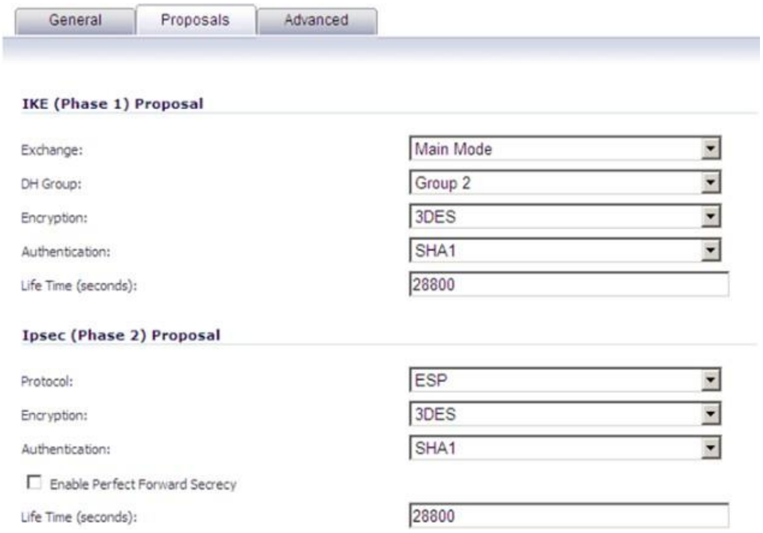
Shared Secret: ••••

Confirm Shared Secret: •••• ☑ Mask Shared Secret

Local IKE ID: IP Address 1.1.216.2

Peer IKE ID: IP Address 1.1.212.2

figure 4



IKE (Phase 1) Proposal

Exchange: Main Mode

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

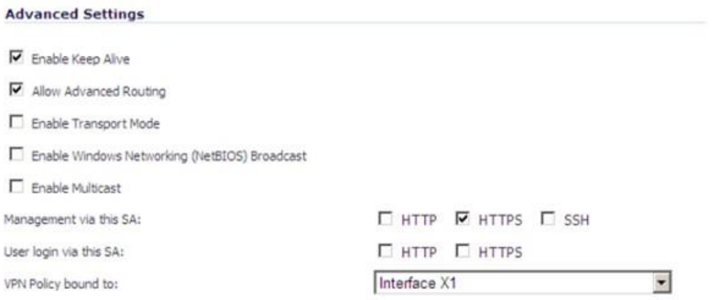
Encryption: 3DES

Authentication: SHA1

☐ Enable Perfect Forward Secrecy

Life Time (seconds): 28800

figure 5



Advanced Settings

☑ Enable Keep Alive

☑ Allow Advanced Routing

☐ Enable Transport Mode

☐ Enable Windows Networking (NetBIOS) Broadcast

☐ Enable Multicast

Management via this SA: ☐ HTTP ☑ HTTPS ☐ SSH

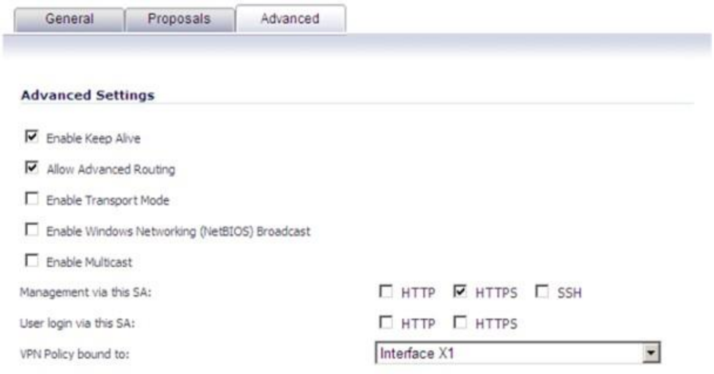
User login via this SA: ☐ HTTP ☐ HTTPS

VPN Policy bound to: Interface X1

Figure 6

B- SPOKE 1

The Figure 7, 8 and 9 show the configuration made on Spoke 1



Advanced Settings

☑ Enable Keep Alive

☑ Allow Advanced Routing

☐ Enable Transport Mode

☐ Enable Windows Networking (NetBIOS) Broadcast

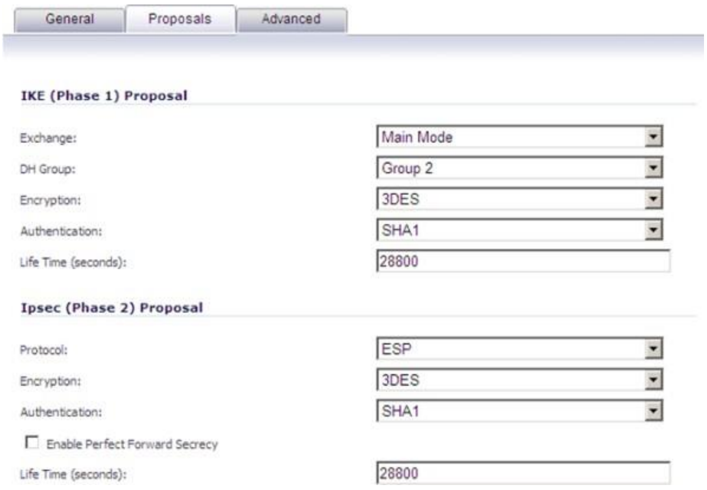
☐ Enable Multicast

Management via this SA: ☐ HTTP ☑ HTTPS ☐ SSH

User login via this SA: ☐ HTTP ☐ HTTPS

VPN Policy bound to: Interface X1

Figure 7



IKE (Phase 1) Proposal

Exchange: Main Mode

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

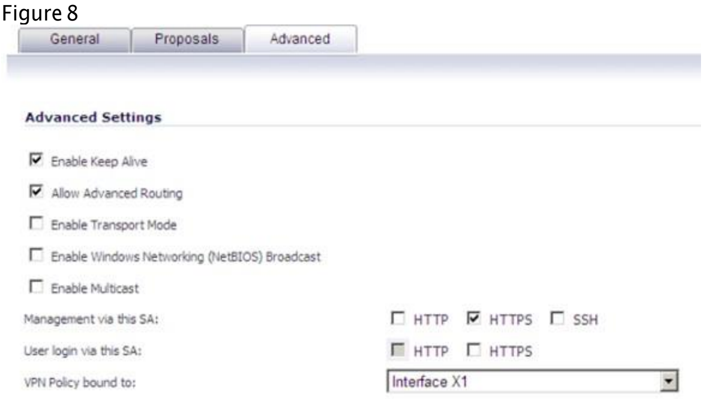
Encryption: 3DES

Authentication: SHA1

☐ Enable Perfect Forward Secrecy

Life Time (seconds): 28800

Figure 8



Advanced Settings

☑ Enable Keep Alive

☑ Allow Advanced Routing

☐ Enable Transport Mode

☐ Enable Windows Networking (NetBIOS) Broadcast

☐ Enable Multicast

Management via this SA: ☐ HTTP ☑ HTTPS ☐ SSH

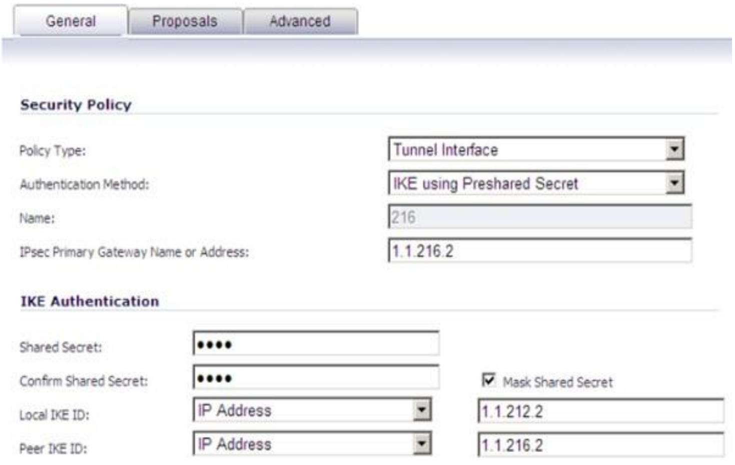
User login via this SA: ☐ HTTP ☐ HTTPS

VPN Policy bound to: Interface X1

Figure 9

C- SPOKE 2

Finally, figures 10, 11 and 12 show the configuration on Spoke 2



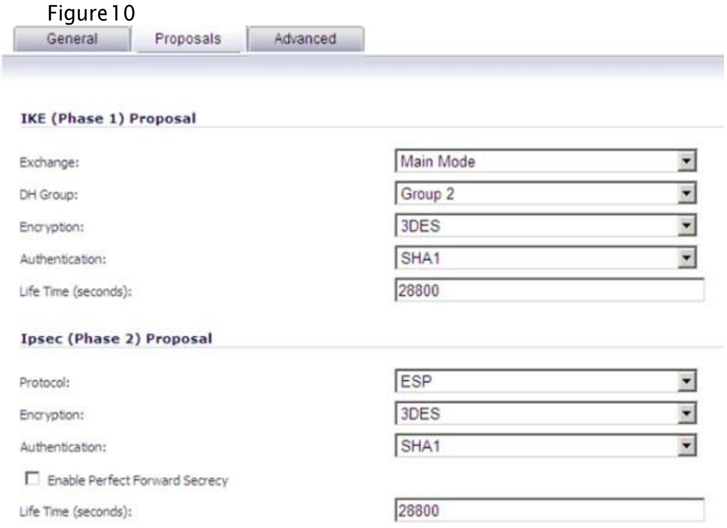
Security Policy

Policy Type: Tunnel Interface
Authentication Method: IKE using Preshared Secret
Name: 216
IPsec Primary Gateway Name or Address: 1.1.216.2

IKE Authentication

Shared Secret: ••••
Confirm Shared Secret: •••• ☑ Mask Shared Secret
Local IKE ID: IP Address 1.1.212.2
Peer IKE ID: IP Address 1.1.216.2

Figure 10



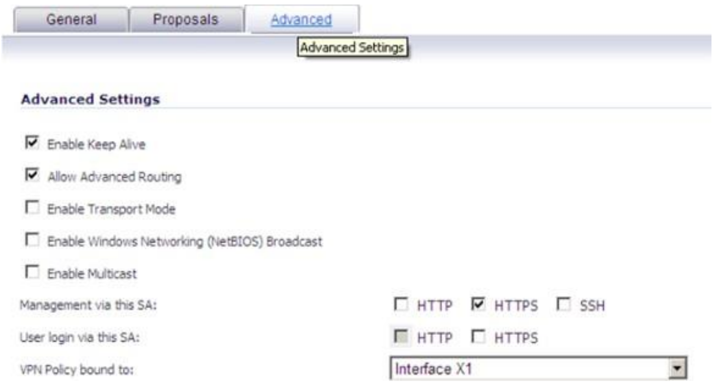
IKE (Phase 1) Proposal

Exchange: Main 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

Figure 11

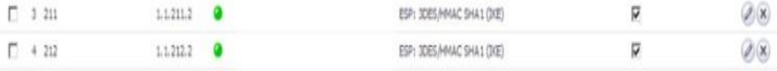


Advanced Settings

☑ Enable Keep Alive
☑ Allow Advanced Routing
☐ Enable Transport Mode
☐ Enable Windows Networking (NetBIOS) Broadcast
☐ Enable Multicast
Management via this SA: ☐ HTTP ☑ HTTPS ☐ SSH
User login via this SA: ☐ HTTP ☐ HTTPS
VPN Policy bound to: Interface X1

Figure 12

Once done, the tunnel should quickly be up and a Green LED will appear as show below (Figure 13) for the Hub



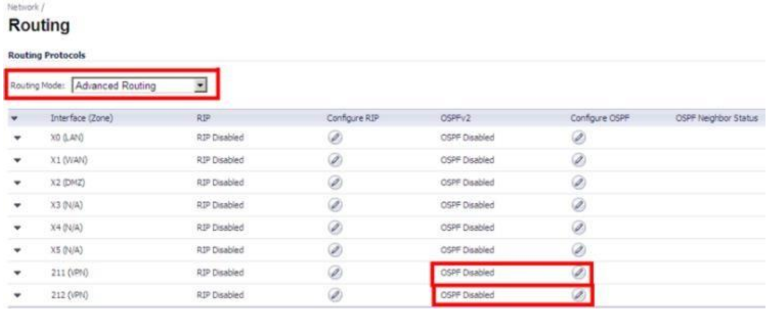
☐	3 211	1.1.211.2	●	ESP: 3DES/HMAC SHA1 (IKE)	☑	
☐	4 212	1.1.212.2	●	ESP: 3DES/HMAC SHA1 (IKE)	☑	

Figure 13

Creation of the OSPF network

A- HUB

Under **Network | Routing**, ensure you have activated the **Advanced Routing Mode** (Figure 14) and then configure OSPF for both VPN Tunnel Interface (Figure 15)



Network /
Routing

Routing Protocols

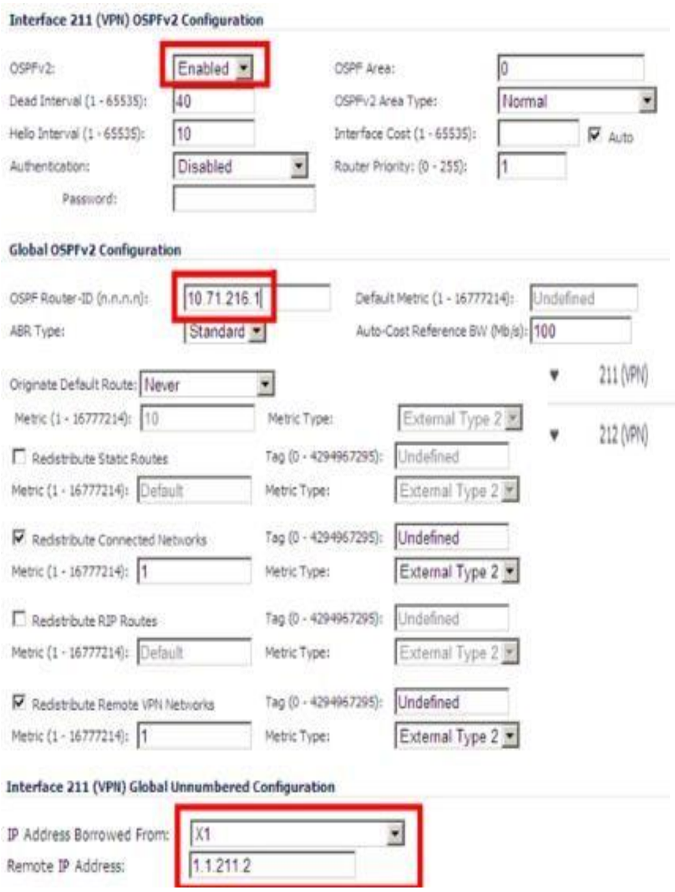
Routing Mode: Advanced Routing

Interface (Zone)	RIP	Configure RIP	OSPFv2	Configure OSPF	OSPF Neighbor Status
X0 (LAN)	RIP Disabled		OSPF Disabled		
X1 (WAN)	RIP Disabled		OSPF Disabled		
X2 (DMZ)	RIP Disabled		OSPF Disabled		
X3 (N/A)	RIP Disabled		OSPF Disabled		
X4 (N/A)	RIP Disabled		OSPF Disabled		
X5 (N/A)	RIP Disabled		OSPF Disabled		
211 (VPN)	RIP Disabled		OSPF Disabled		
212 (VPN)	RIP Disabled		OSPF Disabled		

Figure 14

- Set OSPF mode to “Enabled”.
- Set "OSPF Router ID" to the X0 IP address. This value will need to be different on every router of your OSPF network otherwise OSPF neighborship may not be established.
- Enable Redistribute Connected Networks.
- Enable Redistribute Remote VPN Networks.
- Set "IP Borrowed From" under “**Global Unnumbered Configuration**” as X1 IP.
- Set Remote IP Address as Spoke-1 X1 Interface IP address.

The Figure 15 show all this configuration



Interface 211 (VPN) OSPFv2 Configuration

OSPFv2: Enabled
OSPF Area: 0
Dead Interval (1 - 65535): 40
OSPFv2 Area Type: Normal
Hello Interval (1 - 65535): 10
Interface Cost (1 - 65535): ☑ Auto
Authentication: Disabled
Router Priority: (0 - 255): 1
Password:

Global OSPFv2 Configuration

OSPF Router-ID (n.n.n.n): 10.71.216.1
Default Metric (1 - 16777214): Undefined
ABR Type: Standard
Auto-Cost Reference BW (Mb/s): 100

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

□ Redistribute Static Routes
Tag (0 - 4294967295): Undefined
Metric (1 - 16777214): Default
Metric Type: External Type 2

☑ Redistribute Connected Networks
Tag (0 - 4294967295): Undefined
Metric (1 - 16777214): 1
Metric Type: External Type 2

□ Redistribute RIP Routes
Tag (0 - 4294967295): Undefined
Metric (1 - 16777214): Default
Metric Type: External Type 2

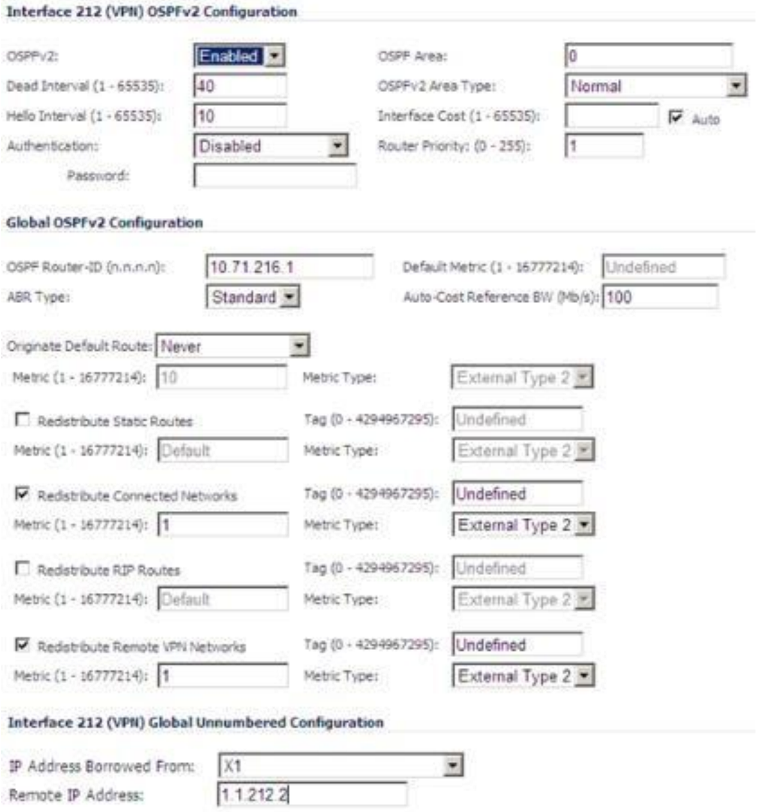
☑ Redistribute Remote VPN Networks
Tag (0 - 4294967295): Undefined
Metric (1 - 16777214): 1
Metric Type: External Type 2

Interface 211 (VPN) Global Unnumbered Configuration

IP Address Borrowed From: X1
Remote IP Address: 1.1.211.2

Figure 15

Make the same kind of configuration for the second Spoke VPN Tunnel Interface, as per Figure 16



Interface 212 (VPN) OSPFv2 Configuration

OSPFv2: Enabled
OSPF Area: 0
Dead Interval (1 - 65535): 40
OSPFv2 Area Type: Normal
Hello Interval (1 - 65535): 10
Interface Cost (1 - 65535): ☑ Auto
Authentication: Disabled
Router Priority: (0 - 255): 1
Password:

Global OSPFv2 Configuration

OSPF Router-ID (n.n.n.n): 10.71.216.1
Default Metric (1 - 16777214): Undefined
ABR Type: Standard
Auto-Cost Reference BW (Mb/s): 100

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

□ Redistribute Static Routes
Tag (0 - 4294967295): Undefined
Metric (1 - 16777214): Default
Metric Type: External Type 2

☑ Redistribute Connected Networks
Tag (0 - 4294967295): Undefined
Metric (1 - 16777214): 1
Metric Type: External Type 2

□ Redistribute RIP Routes
Tag (0 - 4294967295): Undefined
Metric (1 - 16777214): Default
Metric Type: External Type 2

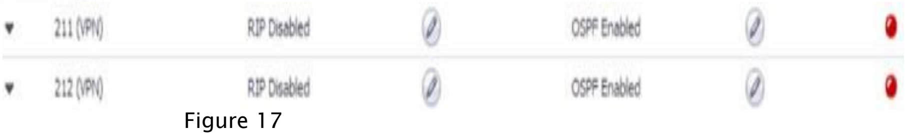
☑ Redistribute Remote VPN Networks
Tag (0 - 4294967295): Undefined
Metric (1 - 16777214): 1
Metric Type: External Type 2

Interface 212 (VPN) Global Unnumbered Configuration

IP Address Borrowed From: X1
Remote IP Address: 1.1.212.2

Figure 16

The OSPF is now ready on the Hub but is still not synchronized, the red LED show that no neighbour have been detected as show on Figure 17

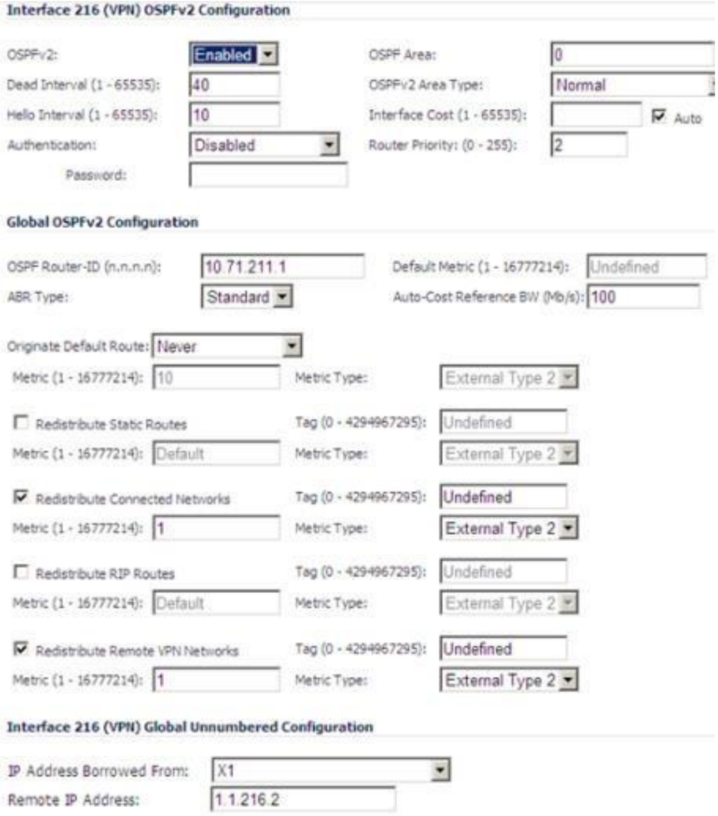


▼	211 (VPN)	RIP Disabled	OSPF Enabled	●
▼	212 (VPN)	RIP Disabled	OSPF Enabled	●

Figure 17

B- Spoke 1

Figure 18 show the configuration made on Spoke1



Interface 216 (VPN) OSPFv2 Configuration

OSPFv2: Enabled
OSPF Area: 0
Dead Interval (1 - 65535): 40
OSPFv2 Area Type: Normal
Hello Interval (1 - 65535): 10
Interface Cost (1 - 65535): ☑ Auto
Authentication: Disabled
Router Priority: (0 - 255): 2
Password:

Global OSPFv2 Configuration

OSPF Router-ID (n.n.n.n): 10.71.211.1
Default Metric (1 - 16777214): Undefined
ABR Type: Standard
Auto-Cost Reference BW (Mb/s): 100

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

□ Redistribute Static Routes
Tag (0 - 4294967295): Undefined
Metric (1 - 16777214): Default
Metric Type: External Type 2

☑ Redistribute Connected Networks
Tag (0 - 4294967295): Undefined
Metric (1 - 16777214): 1
Metric Type: External Type 2

□ Redistribute RIP Routes
Tag (0 - 4294967295): Undefined
Metric (1 - 16777214): Default
Metric Type: External Type 2

☑ Redistribute Remote VPN Networks
Tag (0 - 4294967295): Undefined
Metric (1 - 16777214): 1
Metric Type: External Type 2

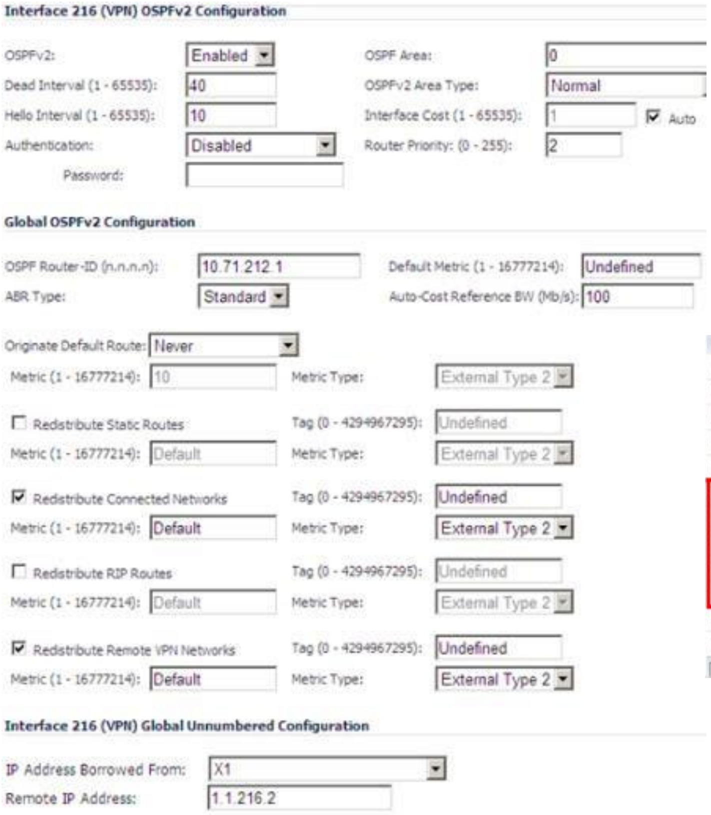
Interface 216 (VPN) Global Unnumbered Configuration

IP Address Borrowed From: X1
Remote IP Address: 1.1.216.2

Figure 18

C- SPOKE 2

The configuration for Spoke 2 is shown in Figure 19



Interface 216 (VPN) OSPFv2 Configuration

OSPFv2:	Enabled	OSPF Area:	0
Dead Interval (1 - 65535):	40	OSPFv2 Area Type:	Normal
Hello Interval (1 - 65535):	10	Interface Cost (1 - 65535):	1 ☑ Auto
Authentication:	Disabled	Router Priority: (0 - 255):	2
Password:			

Global OSPFv2 Configuration

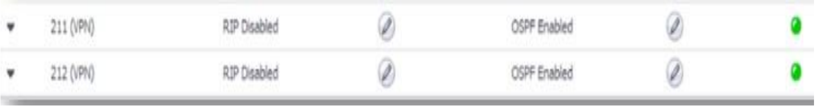
OSPF Router-ID (n.n.n.n):	10.71.212.1	Default Metric (1 - 16777214):	Undefined
ABR Type:	Standard	Auto-Cost Reference BW (Mb/s):	100
Originate Default Route:	Never		
Metric (1 - 16777214):	10	Metric Type:	External Type 2
□ Redistribute Static Routes		Tag (0 - 4294967295):	Undefined
Metric (1 - 16777214):	Default	Metric Type:	External Type 2
☑ Redistribute Connected Networks		Tag (0 - 4294967295):	Undefined
Metric (1 - 16777214):	Default	Metric Type:	External Type 2
□ Redistribute RIP Routes		Tag (0 - 4294967295):	Undefined
Metric (1 - 16777214):	Default	Metric Type:	External Type 2
☑ Redistribute Remote VPN Networks		Tag (0 - 4294967295):	Undefined
Metric (1 - 16777214):	Default	Metric Type:	External Type 2

Interface 216 (VPN) Global Unnumbered Configuration

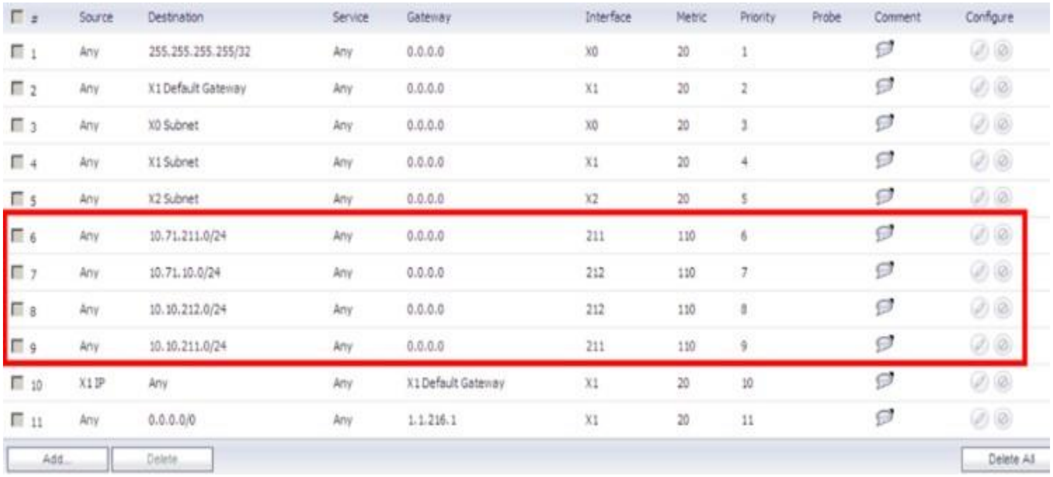
IP Address Borrowed From:	X1
Remote IP Address:	1.1.216.2

Figure 19

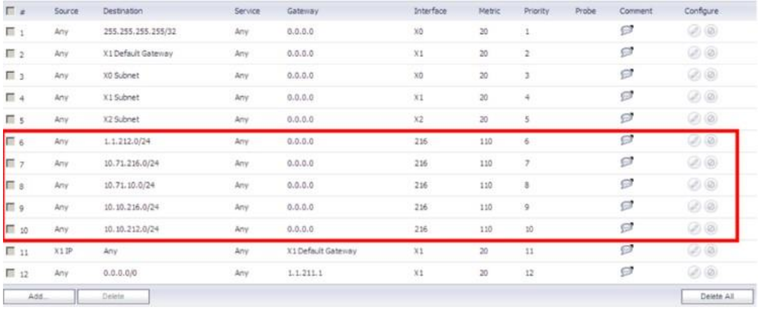
Once the entire OSPF configuration is finished, the OSPF neighborship will be established within few seconds and gren LED will appear on Network, Routing page as in Figure 20 for the Hub.



▾	211 (VPN)	RIP Disabled	OSPF Enabled		●
▾	212 (VPN)	RIP Disabled	OSPF Enabled		●

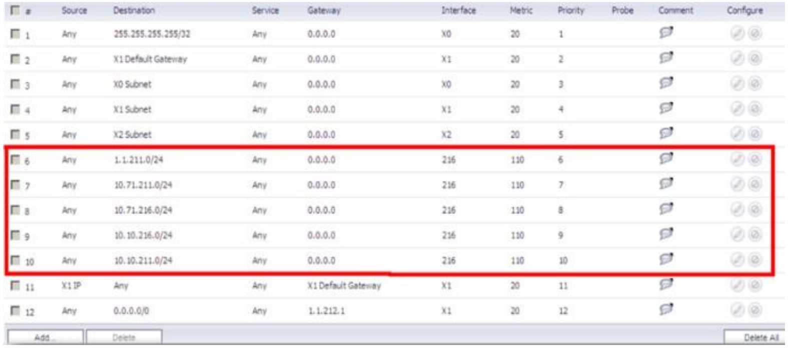


□ #	Source	Destination	Service	Gateway	Interface	Metric	Priority	Probe	Comment	Configure
□ 1	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	1			
□ 2	Any	X1 Default Gateway	Any	0.0.0.0	X1	20	2			
□ 3	Any	X0 Subnet	Any	0.0.0.0	X0	20	3			
□ 4	Any	X1 Subnet	Any	0.0.0.0	X1	20	4			
□ 5	Any	X2 Subnet	Any	0.0.0.0	X2	20	5			
□ 6	Any	10.71.211.0/24	Any	0.0.0.0	211	110	6			
□ 7	Any	10.71.10.0/24	Any	0.0.0.0	212	110	7			
□ 8	Any	10.10.212.0/24	Any	0.0.0.0	212	110	8			
□ 9	Any	10.10.211.0/24	Any	0.0.0.0	211	110	9			
□ 10	X1 IP	Any	Any	X1 Default Gateway	X1	20	10			
□ 11	Any	0.0.0.0/0	Any	1.1.216.1	X1	20	11			



□ #	Source	Destination	Service	Gateway	Interface	Metric	Priority	Probe	Comment	Configure
□ 1	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	1			
□ 2	Any	X1 Default Gateway	Any	0.0.0.0	X1	20	2			
□ 3	Any	X0 Subnet	Any	0.0.0.0	X0	20	3			
□ 4	Any	X1 Subnet	Any	0.0.0.0	X1	20	4			
□ 5	Any	X2 Subnet	Any	0.0.0.0	X2	20	5			
□ 6	Any	1.1.212.0/24	Any	0.0.0.0	216	110	6			
□ 7	Any	10.71.216.0/24	Any	0.0.0.0	216	110	7			
□ 8	Any	10.71.10.0/24	Any	0.0.0.0	216	110	8			
□ 9	Any	10.10.216.0/24	Any	0.0.0.0	216	110	9			
□ 10	Any	10.10.212.0/24	Any	0.0.0.0	216	110	10			
□ 11	X1 IP	Any	Any	X1 Default Gateway	X1	20	11			
□ 12	Any	0.0.0.0/0	Any	1.1.211.1	X1	20	12			

Figure 22



□ #	Source	Destination	Service	Gateway	Interface	Metric	Priority	Probe	Comment	Configure
□ 1	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	1			
□ 2	Any	X1 Default Gateway	Any	0.0.0.0	X1	20	2			
□ 3	Any	X0 Subnet	Any	0.0.0.0	X0	20	3			
□ 4	Any	X1 Subnet	Any	0.0.0.0	X1	20	4			
□ 5	Any	X2 Subnet	Any	0.0.0.0	X2	20	5			
□ 6	Any	1.1.211.0/24	Any	0.0.0.0	216	110	6			
□ 7	Any	10.71.211.0/24	Any	0.0.0.0	216	110	7			
□ 8	Any	10.71.216.0/24	Any	0.0.0.0	216	110	8			
□ 9	Any	10.10.216.0/24	Any	0.0.0.0	216	110	9			
□ 10	Any	10.10.211.0/24	Any	0.0.0.0	216	110	10			
□ 11	X1 IP	Any	Any	X1 Default Gateway	X1	20	11			
□ 12	Any	0.0.0.0/0	Any	1.1.212.1	X1	20	12			

Figure 23

Creating Rules

Once neighborship is established and dynamic routes have been obtained, you need to create access rules in each site to allow traffic from one site to the other.

For example to allow traffic from the LAN zone to the remote sites, create the following access rules in the Hub and the Spokes.

Create the following access rules in the **Hub**:

- **Zone: LAN to VPN**
- Service: Any
- Source: **LAN Subnets**
- Destination: **Spoke-1 Network.**

- **Zone: LAN to VPN**
- Service: Any
- Source: **LAN Subnets**
- Destination: **Spoke-2 Network.**

To allow traffic from the remote sites to the LAN zone, create the following access rules:

- **Zone: VPN to LAN**
- Service: Any

- Source: **Spoke-1 Network + Spoke-2 Network** (Address Objects Group)
- Destination: LAN Subnets

To allow traffic from one Spoke to the other Spoke over the VPN, create the following access rules:

- **Zone: VPN to VPN**
- Service: Any
- Source: **Spoke-1 Network**
- Destination: **Spoke-2 Network**
- **Zone: VPN to VPN**
- Service: Any
- Source: **Spoke-2 Network**
- Destination: **Spoke-1 Network**

Likewise, in **Spoke-1** create the following access rules

- **Zone: LAN to VPN**
- Service: Any
- Source: LAN Subnets
- Destination: **Hub Network.**
- **Zone: LAN to VPN**
- Service: Any
- Source: LAN Subnets
- Destination: **Spoke-2 Network.**

To allow traffic from the remote sites to the LAN zone, create the following access rules:

- **Zone: VPN to LAN**
- Service: Any
- Source: **Spoke-2 Network + Hub Network** (Address Objects Group)
- Destination: LAN Subnets

In **Spoke-2** create the following access rules

- **Zone: LAN to VPN**
- Service: Any
- Source: LAN Subnets
- Destination: **Hub Network.**
- **Zone: LAN to VPN**
- Service: Any
- Source: LAN Subnets
- Destination: **Spoke-1 Network.**

To allow traffic from the remote sites to the LAN zone, create the following access rules:

- **Zone: VPN to LAN**
- Service: Any
- Source: **Spoke-1 Network + Hub Network** (Address Objects Group)
- Destination: LAN Subnets

Troubleshooting:

If the Tunnel Interface does not comes up:
Check the VPN Pre-shared Key, needs to be the same both sides of the tunnel
Check the IKE IDs, needs to be symmetrical (Local ID on site A is Remote ID on site B)
Check Proposal tab, needs to be the same on both side of the tunnel
If the OSPF neighborship cannot be established :
- Check the OSPF Router ID is different on every firewall
- Check the Unnumbered Global Configuration is correctly configured (Use the WAN or Public Interfaces)