

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- HUB

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 | | | |
|-----------------------|-----------------|----------|-----------|--------------------|---|
| ecurity Policy | | | | | |
| olicy Type: | | | Tunnel In | terface | ٠ |
| uthentication Method | | | IKE using | Preshared Secret | |
| lame: | | 211 | | | |
| Psec Primary Gateway | Name or Address | | 1.1.211.2 | | |
| KE Authenticatio | n | | | | |
| hared Secret: | | | | | |
| Confirm Shared Secret | | | | Mask Shared Secret | |
| | IP Add | ress | - | 1.1.216.2 | |
| ocal IKE ID: | | | | | |

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

| Exchange: | Main Mode | • |
|---|---------------------|---|
| DH Group: | Group 2 | • |
| Encryption: | 3DES | • |
| Authentication: | SHA1 | • |
| Life Time (seconds): | 28800 | |
| | | |
| Ipsec (Phase 2) Proposal Protocol: | ESP | |
| Ipsec (Phase 2) Proposal Protocol: Encryption: | ESP 3DES | × |
| Ipsec (Phase 2) Proposal Protocol: Encryption: Authentication: | ESP 3DES SHA1 | • |
| Ipsec (Phase 2) Proposal Protocol: Encryption: Authentication: Enable Perfect Forward Secrecy | ESP 3DES SHA1 | • |

Proposal options can left as default

| General | Proposals | Advanced | | | | |
|-----------------------|----------------------|---------------|-------------|---------|-------|---|
| Advanced Set | tings | | | | | |
| Enable Keep A | live | | | | | |
| Allow Advance | ed Routing | | | | | |
| Enable Transp | ort Mode | | | | | |
| Enable Window | ws Networking (NetBI | OS) Broadcast | | | | |
| Enable Multica | ist | | | | | |
| Management via th | is SA: | | П НТТР | HTTPS | C SSH | |
| User login via this S | SA: | | П нттр | П нттря | | |
| VPN Policy bound to | 0: | | Interface) | (1 | | * |

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

General Proposals Advanced

| Policy Type: | Tunnel Interface | |
|---------------------------------------|----------------------------|---|
| Authentication Method: | IKE using Preshared Secret | - |
| Vame: | 212 | |
| Psec Primary Gateway Name or Address: | 1.1.212.2 | |

| Snareu seureu | | | |
|------------------------|------------|--------------------|---|
| 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

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 | |

figure 5

Advanced Settings

| VPN Policy bound to: | Interface X1 |
|---|----------------------|
| User login via this SA: | 🗆 НТТР 🗖 НТТРS |
| Management via this SA: | 🗆 НТТР 💌 НТТРЅ 🗖 SSH |
| Enable Multicast | |
| Enable Windows Networking (NetBIOS) Broadcast | |
| Enable Transport Mode | |
| Allow Advanced Routing | |
| Enable Keep Alive | |
| | |

Figure 6

B- SPOKE 1

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

| General | Proposals | Advanced | | | | |
|------------------------|----------------------|---------------|-------------|---------|-------|---|
| Advanced Sett | ings | | | | | |
| Enable Keep Al | ive | | | | | |
| Allow Advance | d Routing | | | | | |
| Enable Transpo | ort Mode | | | | | |
| Enable Window | is Networking (NetBI | OS) Broadcast | | | | |
| Enable Multicas | st | | | | | |
| danagement via thi | s SA: | | 🗆 НТТР | HTTPS | 🗖 SSH | |
| Jser login via this Si | A: | | 🗆 нттр | П нттря | | |
| /PN Policy bound to | | | Interface) | (1 | | * |

Figure 7

General Proposals Advanced

| • |
|---|
| • |
| • |
| - |
| |
| |
| |
| ٠ |
| * |
| • |
| |
| |
| |
| |
| |

Figure 9

User login via this SA:

VPN Policy bound to:



Calle 140 #11-45. Bogotá D.C. Colombia +57 1 3680290 / +57318 4914652 sales@itclatam.com / tss@itclatam.com REV1.01

■ HTTP □ HTTPS

Interface X1

•



C- SPOKE 2

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

General Proposals Advanced

| olicy Type: | | Tunnal In | terface | |
|---|--|-----------|--------------------|---|
| oncy i ype: | | IVE using | Dracharad Sacrat | |
| umentication Method: | | INE USIN | y mesnared Secret | - |
| ame: | 216 | | | |
| rsec Primary Gateway Nar | me or Address: | 1.1.216.2 | | |
| KE Authentication | | | | |
| hared Secret: | •••• | | | |
| onfirm Shared Secret: | •••• | | Mask Shared Secret | |
| ocal IKE ID: | IP Address | • | 1.1.212.2 | |
| eer IKE ID: | IP Address | | 1.1.216.2 | |
| IKE (Phase 1) Prop | osal | | | |
| Exchange: | | Main N | lode | |
| OH Group: | | Group | 2 | |
| Encryption: | | 3DES | | 1 |
| Authentication: | | SHA1 | | |
| Life Time (seconds): | | 28800 | | |
| Ipsec (Phase 2) Pr | oposal | | | |
| Protocol: | | ESP | | |
| Encryption: | | 3DES | • | |
| Authentication: | | SHA1 | | |
| Enable Perfect Forw | ard Secrecy | | | |
| | | | | |
| Life Time (seconds): | | 28800 | | |
| Life Time (seconds): Figure 11 | | 28800 | | |
| life Time (seconds): Figure 1 1 General F | Proposals Advanced | 28800 | | |
| Life Time (seconds): Figure 1 1 General F | Proposals Advanced | 28800 | | |
| Life Time (seconds): Figure 11 General F Advanced Settings | Proposals Advanced Advar | 28800 | | |
| Life Time (seconds): Figure 11 General F Advanced Settings F Enable Keep Alive | Proposals Advanced Advar | 28800 | | |
| Advanced Settings | Proposals <u>Advanced</u> Advar s | 28800 | | |
| Advanced Settings Advanced Settings Advanced Reup Alive Aliow Advanced Rou Enable Transport Mo | Proposals Advanced Advantes | 28800 | | |
| Advanced Settings Enable Keep Alive Allow Advanced Rou Enable Transport Mc Enable Windows Net | Proposals Advanced Advanced | 28800 | | |
| Advanced Settings | Proposals Advanced Advar : : : : : : : : : : : : : : : : : : : | 28800 | | |
| Life Time (seconds): Figure 11 General F Advanced Settings F Enable Keep Alive Allow Advanced Rou Enable Transport Mo Enable Transport Mo Enable Windows Net Enable Multicast Management via this SA: | Proposals Advanced Advar s s s s s de tworking (NetBIOS) Broadcast | 28800 | р 🗹 нттрз 🗖 SSH | |

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

| | Figure 13 | | | | |
|---|-----------|-----------|---------------------------|---|----|
| Π | 4 212 | 1.1.212.2 | ESP: 3DES/HMAC SHA1 (IKE) | R | Ø× |
| 0 | 3 211 | 1.1.211.2 | ESP1 3DE5/HMAC SHA1 (XE) | R | Ø× |

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)

| Routing | |
|---------|--|
| | |

| Routi | uting Protocols | | | | | | | | | | |
|--------|------------------------|--------------|---------------|---------------|----------------|----------------------|--|--|--|--|--|
| Routin | Mode: Advanced Routing | | | | | | | | | | |
| v | Interface (Zone) | RIP | Configure RIP | OSPFv2 | Configure OSPF | OSPF Neighbor Status | | | | | |
| * | X0 0.440 | RJP Disabled | Ø | OSP# Disabled | 0 | | | | | | |
| * | X1 (MAN) | RJP Disabled | Ø | OSPF Disabled | Ø | | | | | | |
| • | X2 (DMZ) | RJP Disabled | Ø | OSPF Disabled | Ø | | | | | | |
| * | X3 (N/A) | RJP Disabled | Ø | OSPF Disabled | 0 | | | | | | |
| * | X4 (N(A) | RJP Disabled | Ø | OSPF Disabled | Ø | | | | | | |
| * | X5 (N/A) | RJP Disabled | Ø | OSPF Disabled | ۲ | | | | | | |
| * | 211 (VPN) | RJP Disabled | Ø | OSPF Disabled | Ø | | | | | | |
| * | 212 (VPN) | RIP Disabled | Ø | OSP# Disabled | Ø | | | | | | |



- 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 "IPBorrowed 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





Enabled · OSPFv2: OSPF Area: Normal Dead Interval (1 - 65535): 40 OSPEV2 Area Type: ٠ Helio Interval (1 - 65535): 10 Interface Cost (1 - 65535): Auto Authentication: Disabled Router Priority: (0 - 255): . Password: Global OSPEv2 Configuration 10.71.216.1 Default Metric (1 - 16777214): Undefined OSPF Router-ID (n.n.n.n): Auto-Cost Reference BW (Mb/s): 100 ABR Type: Standard . 211 (VPN) ٧ Originate Default Route: Never ٠ Metric (1 - 16777214): 10 Metric Type: External Type 2 212 (VPN) Tag (0 · 4294967295): C Redistribute Static Routes 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 💌 Undefined C Redistribute RJP Routes Tag (0 - 4294957295): Metric (1 - 16777214): Default Metric Type: External Type 2 💌 Redistribute Remote VPN Networks Tag (0 - 4294967295): Undefined External Type 2 • Metric (1 - 16777214): 1 Metric Type: Interface 211 (VPN) Global Unnumbered Configuration IP Address Borrowed From ٠ 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

Interface 211 (VPN) OSPFv2 Configuration

| OSPPV2: | Enabled | OSPF Area | ĸ | 0 | 1 |
|-----------------------------|---------------|-----------------------|----------------------|--------------|------|
| Dead Interval (1 + 65535): | 40 | OSPFV2 Ar | ea Type: | Normal | * |
| Hello Interval (1 - 65535): | 10 | Interface | Cost (1 - 65535): | [| Auto |
| Authentications | Disabled | Router Pri | ority: (0 - 255): | 1 | |
| Password: | | | | | |
| Global OSPFv2 Configural | ion | | | | |
| OSPF Router-ID (n.n.n.n): | 10.71.216 | 1 Defau | it Metric (1 + 16777 | 214): Unde | Sned |
| ABR Type: | Standard | Auto- | Cost Reference BW | (Mb/s): 100 | |
| Originate Default Route: Ne | ver | * | | | |
| Metric (1 - 16777214): 10 | | Metric Type: | External Type | 2 - | |
| C Redistribute Static Rout | es | Tag (0 + 4294967295): | Undefined | | |
| Metric (1 - 16777214): Do | fault | Metric Type: | External Type | 02 | |
| Redistribute Connected | Networks | Tag (0 + 4294967295): | Undefined | | |
| Metric (1 - 16777214): 1 | | Metric Type: | External Type | 2 💌 | |
| C Redistribute RIP Routes | | Tag (0 - 4294967295): | Undefined | | |
| Metric (1 - 16777214): De | fault. | Metric Type: | External Type | ≥ 2 <u>×</u> | |
| Redstribute Remote VP | N Networks | Tag (0 + 4294967295): | Undefined | | |
| Metric (1 - 16777214): 1 | , N | Metric Type: | External Type | 2 - | |
| Interface 212 (VPN) Glob | al Unnumbered | Configuration | | | |
| IP Address Borrowed Fro | m: X1 | | | | |
| Remote IP Address: | 1 1 212 2 | 2 | _ | | |

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

| RIP Disabled | 0 | OSPEI | Enabled | Ø | 0 |
|-----------------------------------|----------------|---------------------|----------------------|---------------|-------|
| RIP Disabled | 0 | OSPE | Enabled | 0 | 0 |
| Figure 17 | 0 | | | | |
| B- Spoke 1 Figure 18 sl | now the | e configura | tion mad | de on Si | ooke1 |
| Interface 216 (VPN) 05 | PFv2 Configura | tion | | 1 | |
| OSPFv2: | Enabled | OSPF An | ea: | 0 | |
| Dead Interval (1 - 65535): | 40 | OSPFv2 | Area Type: | Normal | |
| Hello Interval (1 - 65535): | 10 | Interfac | e Cost (1 - 65535): | | Auto |
| Authentication: | Disabled | Router P | riority: (0 - 255): | 2 | |
| Password: | 2 | | | | |
| Global OSPFv2 Configur | ation | | | | |
| OSPF Router-ID (n.n.n.n): | 10 71 21 | 1.1 Defa | ult Metric (1 - 1677 | 7214): Undefi | ned |
| ABR Type: | Standard | Auto | -Cost Reference BV | V (Mb/s): 100 | |
| Originate Default Route: | lavor | - | | | |
| Matrix (1 - 16777214): | ő. | Matrix Turner | External Tur | 0.2 - | |
| ocosti anniti li | v | Chevie Type- | LEAteniai Typ | C 4 | |
| Redistribute Static Ros | utes | Tag (0 - 4294967295 |): Undefined | | |
| Metric (1 - 16777214): | lefault | Metric Type: | External Typ | e 2 🔻 | |
| Redistribute Connecte | d Networks | Tag (0 - 4294967295 | : Undefined | | |
| Metric (1 - 16777214): 1 | | Metric Type: | External Typ | e 2 💌 | |
| Redistribute RIP Route | 5 | Tag (0 - 4294967295 | : Undefined | | |
| Metric (1 - 16777214): | lefault | Metric Type: | External Typ | e 2 💌 | |
| Redistribute Remote V | PN Networks | Tag (0 - 4294967295 | Undefined | _ | |
| Metric (1 - 16777214): 1 | 1 | Metric Type: | External Typ | e 2 🔻 | |
| Interface 216 (VPN) Glo | bal Unnumber | ed Configuration | | | |
| IP Address Borrowed Fr | om: X1 | | | | |
| Remote IP Address: | 1.1.216 | 2 | _ | | |

Figure 18

Figure 16

Corporation® Visit our Website: www.itclatam.com

6 SONICWA Knowledge Database

C- SPOKE 2

The configuration for Spoke 2 is shown in Figure

19 Interface 216 (VPN) OSPFv2 Configuration 255.255.255.255/32 0.0.0.0 Π1 12. . OSPFv2: Enabled · OSPF Area: 40 Normal OSPFv2 Area Type: Dead Interval (1 - 65535): 10 6 Auto Hello Interval (1 - 65535): Interface Cost (1 - 65535): Disabled 5 Authentication: Router Priority: (0 - 255): Password: Global OSPFv2 Configuratio 10.71.212.1 Default Metric (1 - 16777214): Undefined OSPF Router-ID (n.n.n.n): ABR Type: Standard · Auto-Cost Reference BW (Mb/s): 100 Originate Default Route: Never -Metric (1 - 16777214): 10 Metric Type: External Type 2 👻 C Redistribute Static Routes Tag (0 - 4294967295): Undefined Metric (1 - 16777214): Default Metric Type: External Type 2 Tag (0 - 4294967295): Undefined Redstribute Connected Networks Metric (1 - 16777214): Default Metric Type: External Type 2 ø 10.71.216.0/24 0.0.0.0 216 Tag (0 - 4294967295): Undefined 10.10.216.0/24 0.0.0.0 216 ø Redistribute RIP Routes ø 10.10.211.0/24 0.0.0.0 216 Metric (1 - 16777214): Default Metric Type: External Type 2 (1 Defa 0.0.0.0/0 d E 12 1.1.212.1 Redstribute Remote VPN Networks Tao (0 - 4294967295): Undefined External Type 2 💌 Metric (1 - 16777214): Default Metric Type: Figure 23

Interface 216 (VPN) Global Unnumbered Configuration

X1

1.1.216.2

IP Address Borrowed From: Remote IP Address:

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.

.

| ٠ | 211 (VPN) | RIP Disabled | Ø | OSPF Enabled | Ø | 0 |
|---|-----------|--------------|---|--------------|---|---|
| ٠ | 212 (VPN) | RIP Disabled | 0 | OSPF Enabled | 0 | |

| L 44 | | Datata | | | | | | | | Dalate 5.5 |
|-------------|--------|--------------------|---------|--------------------|-----------|--------|----------|-------|---------|------------|
| E 11 | Any | 0.0.0.0/0 | Any | 1.1.216.1 | ×1 | 20 | 11 | | ø | 00 |
| ■ 10 | X1IP | Any | Any | X1 Default Gateway | ×1 | 20 | 10 | | ø | Ø® |
| 9 | Any | 10.10.211.0/24 | Any | 0.0.0.0 | 211 | 110 | 9 | | ø | 00 |
| П в | Any | 10.10.212.0/24 | Any | 0.0.0.0 | 212 | 110 | | | ø | 00 |
| F 7 | Any | 10.71.10.0/24 | Any | 0.0.0.0 | 212 | 110 | 7 | | ø | Ø® |
| E 6 | Any | 10.71.211.0/24 | Any | 0.0.0.0 | 211 | 110 | 6 | | ø | 00 |
| E 5 | Any | x2 Subnet | Any | 0.0.0.0 | X2 | 20 | 5 | | ø | Ø |
| F 4 | Any | X1 Subnet | Any | 0.0.0.0 | ×1 | 20 | 4 | | ø | 00 |
| П з | Any | X0 Subnet | Any | 0.0.0.0 | x0 | 20 | 3 | | ø | 00 |
| E 2 | Any | X1 Default Gateway | Any | 0.0.0.0 | ×1 | 20 | 2 | | ø | 00 |
| Π1 | Any | 255,255,255,255/32 | Any | 0.0.0.0 | xo | 20 | 1 | | ø | 00 |
| Π = | Source | Destnation | Service | Gateway | Interface | Metric | Priority | Probe | Comment | Configure |

| | П з | Any | X0 Subnet | Any | 0.0.0.0 | xo | 20 | 3 | | ø | 00 |
|------------|--------------|--------|------------------|---------|--------------------|-----------|--------|----------|-------|---------|-----------|
| | FE 4 | Any | X1 Subnet | Any | 0.0.0.0 | 81 | 20 | 4 | | ø | 00 |
| | ∏ s | Any | X2 Subnet | Any | 0.0.0.0 | X2 | 20 | 5 | | ø | 00 |
| | FT 6 | Any | 1.1.212.0/24 | Απγ | 0.0.0.0 | 216 | 110 | 6 | | ø | ØØ |
| | III 7 | Any | 10.71.216.0/24 | Any | 0.0.0.0 | 216 | 110 | 7 | | ø | 00 |
| | III 8 | Απγ | 10.71.10.0/24 | Any | 0.0.0.0 | 216 | 110 | 8 | | ø | 00 |
| | 9 11 | Any | 10.10.216.0/24 | Any | 0.0.0.0 | 216 | 110 | 9 | | ø | 00 |
| | MT 10 | Any | 10.10.212.0/24 | Any | 0.0.0.0 | 216 | 110 | 20 | | ø | 00 |
| | E 11 | X1IP | Any | Any | X1 Default Gateway | ×1 | 20 | 11 | | ø | Ø ® |
| | FT 12 | Any | 0.0.0.0/0 | Any | 1.1.211.1 | ×1 | 20 | 12 | | ø | 00 |
| | Add | 1 | Delete | | | | | | | | Delete A |
| | | Fig | jure 22 | | | | | | | | |
| | Source | ce Des | stination | Service | Gateviay | Interface | Metric | Priority | Probe | Comment | Configure |
| 1 | Any | 255 | 5.255.255.255/32 | Any | 0.0.0.0 | xo | 20 | 1 | | ø | 00 |
| 2 | Any | X1 | Default Gateway | Any | 0.0.0.0 | X1 | 20 | 2 | | ø | 00 |
| П з | Any | ж0 | Subnet | Any | 0.0.0.0 | xo | 20 | 3 | | ø | 00 |
| 1 4 | Any | X1 | Subnet | Any | 0.0.0.0 | XI | 20 | 4 | | ø | 00 |
| T s | Any | X2 | Subret | Any | 0.0.0.0 | X2 | 20 | 5 | | ø | 00 |
| Π 6 | Απγ | 1.1 | | Any | 0.0.0.0 | 216 | 110 | 6 | | ø | 00 |
| | Anv | 10 | 71.211.0/24 | Anu. | 0.0.0.0 | 216 | 110 | | | C1 | 00 |

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 theother.

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

Calle 140 #11-45. Bogotá D.C. Colombia +57 1 3680290 / +57318 4914652 sales@itclatam.com/tss@itclatam.com REV1.01

orporation /isitourWebsite:www.itclatam.com



- 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)

