Migrating from Policy-Based VPN to Route-Based VPN with Cisco Secure Firewall Management Center

Revised: October 15, 2024

Migrating Policy-Based VPN to Route-Based VPN Using Cisco Secure Firewall Management Center

Introduction

This document guides you to migrate a policy-based VPN to a route-based VPN using the VPN wizard of the Cisco Secure Firewall Management Center.

Organizations relying on policy-based VPNs face significant challenges in managing and scaling their network infrastructure. Policy-based VPNs require complex access lists and precise ordering, making them prone to configuration errors and difficult to manage, especially as the network grows. Also, they lack support for dynamic routing protocols. Addition of new spokes requires manual VPN configuration updates on the hub. These drawbacks not only increase the administrative burden but also limit the scalability and flexibility of the network, making it less efficient and error-prone.

Migrating to route-based VPNs using Virtual Tunnel Interfaces (VTIs) simplifies configuration, management, improves network reliability, scalability, and manageability, meeting growing business needs.

About Route-Based VPN

Route-based VPN uses routable logical interfaces called Virtual Tunnel Interfaces (VTIs) to establish a VPN tunnel between peers. You can use these interfaces like other interfaces, and apply static and dynamic routing policies to them. You can create a routed security zone, add VTI interfaces to it, and define access control rules for the decrypted traffic over the VTI tunnel. The threat defense device encrypts or decrypts the traffic to or from the tunnel interface and forwards it according to the routing policy. You can configure route-based VPN with static VTI (SVTI) or dynamic VTI (DVTI) using the site-to-site VPN wizard.

Benefits of Route-Based VPN

The benefits of using a route-based VPN in a hub and spoke topology are:

- **Streamlined Setup**: VTI offers a simplified approach to VPN configuration, removing the complexity of traditional crypto maps and access lists.
- **Simplified Management**: VTI simplifies the management of peer configurations for large enterprise hub and spoke deployments. A single dynamic VTI configuration on the hub can support multiple spokes with static VTIs.
- **Adaptive Routing**: VTI accommodates dynamic routing protocols such as BGP, EIGRP, and OSPF, facilitating the automatic update of routes between VPN endpoints in response to changing network conditions.
- **Dual ISP Redundancy**: VTI enables the creation of secondary backup tunnels, enhancing connectivity reliability.
- **Load balancing**: VTI allows for the even distribution of VPN traffic through ECMP routing.

Recommendations for Migrating Policy-Based VPN to Route-Based VPN

Before you start the migration from policy-based VPN to route-based VPN using the management center, you must:

- Select a routing protocol for the route-based VPN according to your network requirements.

- Select an IP address for the spoke’s static VTI interface.

  If you have multiple spokes, we recommend that you allocate a subnet for the VTI interfaces.

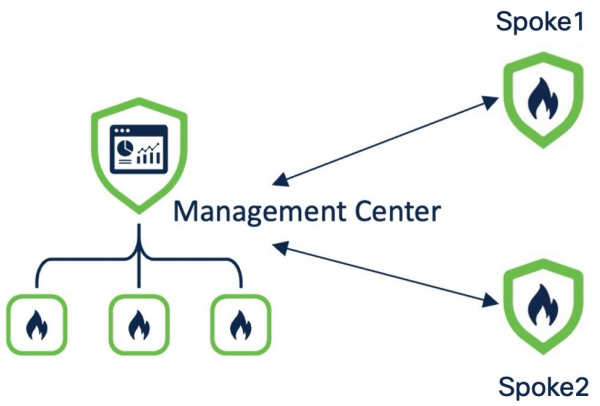
  Note the following recommendations for configuring a spoke static VTI IP address:

  - Use an IP address in the range: 169.254.x.x/16.
  - Do not use the IP address range reserved for the Threat Defense devices: 169.254.1.x/24.
  - Use an IP address with /30 as the netmask for point-to-point tunnels using static VTI, for example, use 169.254.2.1/30.

Use Case 1: Migrating Peer to Peer Policy-Based VPN to Peer to Peer Route-Based VPN

Scenario

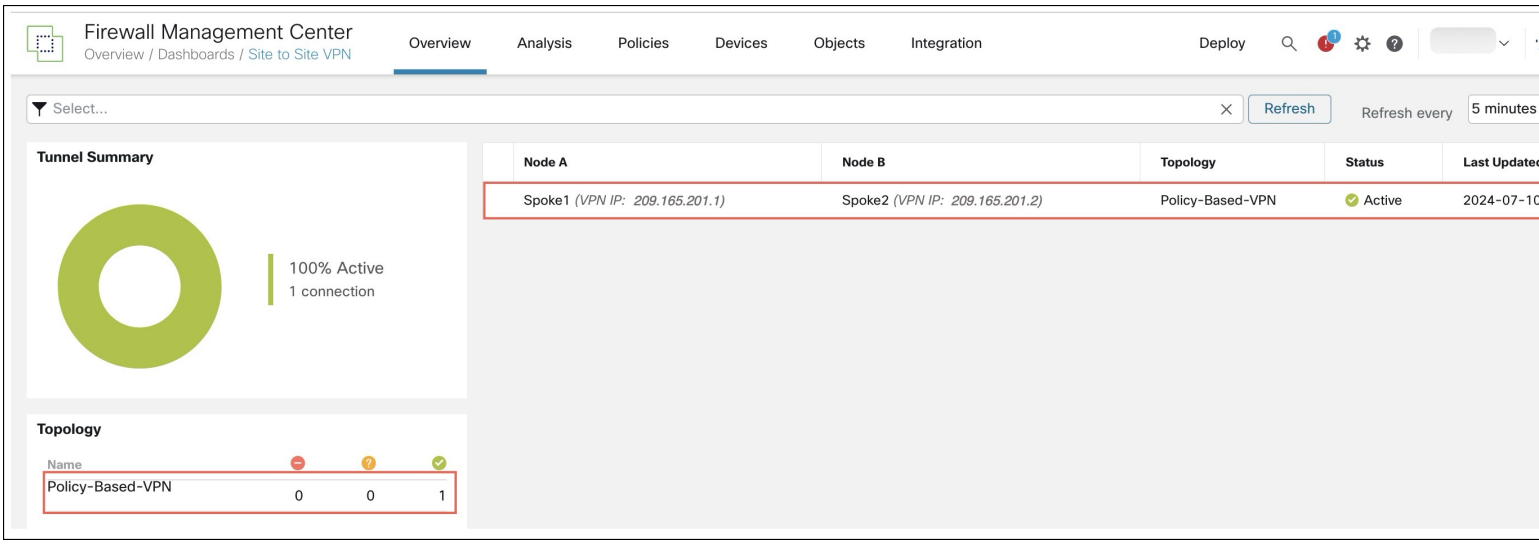
A medium-sized enterprise currently operates a network with two Threat Defense devices with a policy-based VPN. These devices are managed by a Management Center Version 7.4.1. Recognizing the advantages of route-based VPNs, such as improved scalability and simplified network management, the network administrator plans to migrate to a route-based VPN. To facilitate this transition, the administrator will utilize the Management Center's VPN wizard, which is designed to streamline the configuration process and ensure a seamless migration. This migration aims to enhance the network's robustness and flexibility, supporting the organization's growth and evolving connectivity needs.



The policy-based VPN topology has the following parameters:

Threat Defense Device	Protected Network	VPN Interface
Spoke1	198.51.100.16/28	209.165.201.1
Spoke 2	198.51.100.32/28	209.165.201.2

To view details of the VPN tunnel, choose **Overview > Dashboards > Site to Site VPN**.



To view the tunnel details, use the **show crypto ikev2 sa** and **show crypto ipsec sa** commands on the Threat Defense devices:

```
> show crypto ipsec sa
interface: outside
    Crypto map tag: CSM_outside_map, seq num: 1, local addr: 209.165.201.1

      access-list CSM_IPSEC_ACL_1 extended permit ip 198.51.100.16 255.255.255.240 198.51.100.32 255.255.255.240
      Protected vrf (ivrf):
      local ident (addr/mask/prot/port): (198.51.100.16/255.255.255.240/0/0)
      remote ident (addr/mask/prot/port): (198.51.100.32/255.255.255.240/0/0)
      current_peer: 209.165.201.2


      #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
      #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 209.165.201.1/500    remote crypto endpt.: 209.165.201.2/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 460FEE39
      current inbound spi : A258BF8E

    inbound esp sas:
      spi: 0xA258BF8E (2723725198)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
         slot: 0, conn_id: 14, crypto-map: CSM_outside_map
         sa timing: remaining key lifetime (kB/sec): (4055040/27945)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0x460FEE39 (1175449145)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
         slot: 0, conn_id: 14, crypto-map: CSM_outside_map
         sa timing: remaining key lifetime (kB/sec): (3916799/27945)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

```
> show crypto ikev2 sa

IKEv2 SAs:

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                   Remote                                  fvrf/ivrf     Status
30504265  209.165.201.1/500                       209.165.201.2/500                       Global/Global      READY
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/876 sec
Child sa: local selector  198.51.100.16/0 - 198.51.100.31/65535
          remote selector 198.51.100.32/0 - 198.51.100.47/65535
          ESP spi in/out: 0xa258bf8e/0x460fee39
```

Migrating a Peer-to-Peer Policy-Based VPN to a Route-Based VPN

To migrate the peer-to-peer policy-based VPN to a route-based VPN:

Step	Task	More Information
1	Configure a peer-to-peer route-based VPN using the VPN wizard.	Configuring Peer to Peer Route-Based VPN, on page 6
2	Configure a routing protocol.	Configure a Routing Protocol, on page 7
3	Delete the policy-based VPN.	-
4	Deploy the configurations on the devices.	-
5	Verify VPN tunnel statuses and configurations.	Verify VPN Tunnel Statuses and Configurations, on page 8

Configuring Peer to Peer Route-Based VPN

Procedure

Step 1 Choose **Devices > Site To Site**.

Step 2 Click **+ Site To Site VPN**.

Step 3 In the **Topology Name** field, enter a name for the VPN topology.

Step 4 Click the **Route Based (VTI)** radio button.

Step 5 Select **Point to Point** as the network topology.

Step 6 Check the **IKEv1** or **IKEv2** check box to choose the IKE version to use during IKE negotiations.

Step 7 Click the **Endpoints** tab.

Step 8 For **Node A**, configure the following parameters:

a) Choose **Spoke1** from the **Device** drop-down list.

b) Click **+** to create a static VTI.

The **Add Virtual Tunnel Interface** dialog box is prepopulated with default configurations. However, you must configure the following parameters:

1. From the **Tunnel Source** drop-down list, choose the physical interface that is the source of the static VTI. Choose the IP address of this interface from the adjacent drop-down list.
2. In the **Configure IP** field, enter an IP address for the static VTI.

   In this example, the static VTI IP address is 169.254.2.1/30.
3. Click **OK**.

Step 9 For **Node B**, configure the following parameters:

a) Choose **Spoke2** from the **Device** drop-down list.

b) Click **+** to create a static VTI.

To configure the static VTI parameters, repeat Step 8bi to Step 8biii. In this example, the static VTI IP address is 169.254.2.2/30.

Step 10 Click **Save**.

Configure a Routing Protocol

For a route-based VPN, you must configure a routing protocol such as BGP, OSPF, or EIGRP. Dynamic VTI does not support static routes. In this example, we use BGP as the routing protocol.

Procedure

Step 1 Choose **Devices > Device Management**.

Step 2 Click the edit icon adjacent to Spoke1.

Step 3 Click the **Routing** tab.

Step 4 In the left pane, choose **General Settings > BGP**.

Step 5 Check the **Enable BGP** check box.

Step 6 In the **AS Number** field, enter the AS number of the device.

Step 7 Other fields are optional, and you can configure them according to your requirements.

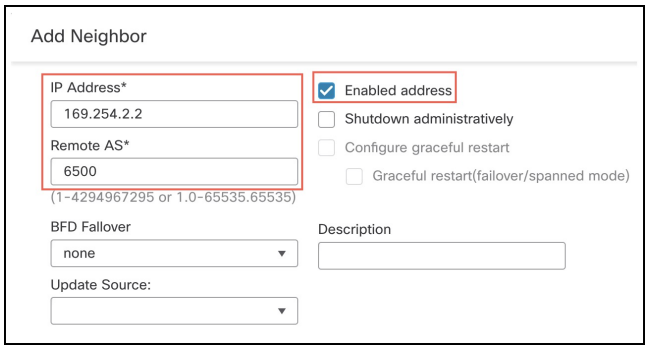
Step 8 Click **Save**.

Step 9 In the left pane, choose **BGP > IPv4**.

Step 10 Check the **Enable IPv4** check box.

Step 11 Click the **Neighbor** tab and click **+ Add**.

In the **Add Neighbor** dialog box, configure the following parameters:



a) In the **IP Address** field, enter the IP address of the peer.

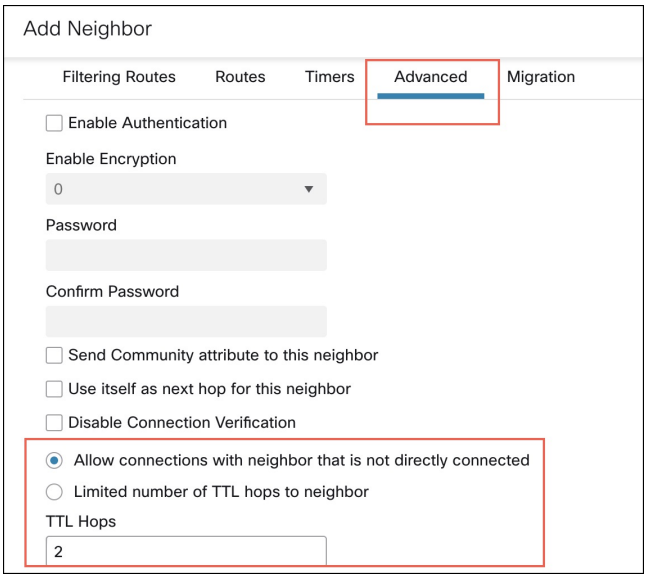
In this example, it is the VTI IP address of Spoke 2 (169.254.2.2).

b) In the **Remote AS** field, enter the peer's AS number.

c) Check the **Enabled address** check box.

d) Other fields are optional, and you can configure them according to your requirements.

e) (Optional) If the devices are in different regions, they use External Border Gateway Protocol (eBGP) to exchange routing information, and you must configure the multi-hop parameter.



1. Click the **Advanced** tab.
2. Select the **Allow connections with neighbor that is not directly connected** radio button.
3. In the **TTL Hops** field, enter the value as 2.
4. Other fields are optional, and you can configure them according to your requirements.

f) Click **OK**.

Step 12 Click the **Networks** tab and click **+ Add** to advertise the networks to the peers.

In the **Add Networks** dialog box, configure the following parameters:

a) From the **Network** drop-down list, choose the protected network of the device.

In this example, for Spoke1, it is the protected network 198.51.100.16/28.

b) (Optional) From the **Route Map** drop-down list, choose the route map that should be examined to filter the advertised networks. By default, all networks are redistributed.

c) Click **OK**.

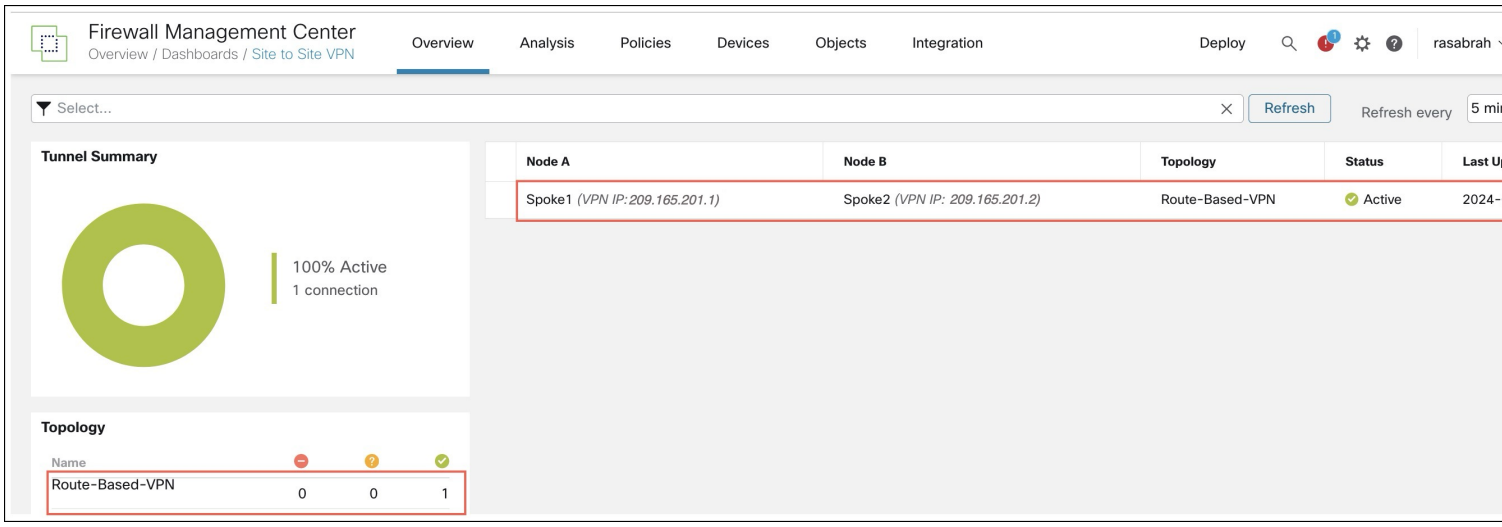
Step 13 Click **Save**.

Step 14 To configure BGP on the peer (Spoke2), repeat Step 1 to Step 13.

Step 15 Deploy the configurations to both the devices.

Verify VPN Tunnel Statuses and Configurations

To view the VPN tunnel details, choose **Overview > Dashboards > Site To Site VPN**:



To view the tunnel details, use the **show crypto ipsec sa** and **show crypto ikev2 sa** commands on the devices.

```
> show crypto ipsec sa
interface: outside_static_vti_1
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 209.165.201.1

      Protected vrf (ivrf): Global
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer: 209.165.201.2


      #pkts encaps: 24, #pkts encrypt: 24, #pkts digest: 24
      #pkts decaps: 31, #pkts decrypt: 31, #pkts verify: 31
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 24, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 209.165.201.1/500    , remote crypto endpt.: 209.165.201.2/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: EDA26B0F
      current inbound spi : BBAE8073

    inbound esp sas:
      spi: 0xBBAE8073 (3148775539)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 6, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4055037/24765)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0xFFFFFFFF
    outbound esp sas:
      spi: 0xEDA26B0F (3986844431)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 6, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (3916798/24765)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

```
> show crypto ikev2 sa

IKEv2 SAs:

Session-id:6, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                                 R
  13394065  209.165.201.1/500                                   2
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth s
      Life/Active Time: 86400/2485 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xbbae8073/0xeda26b0f
```

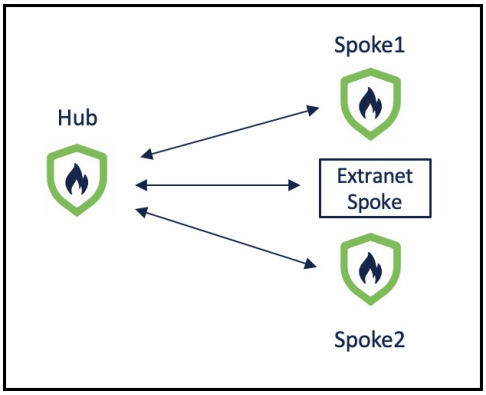
Verify Routing Configuration on the Threat Defense Devices

To verify the BGP, OSPF, or EIGRP routes on the hub and the spokes, use the **show route** command on the device. You can also use the **show bgp**, **show eigrp**, or **show ospf** commands.

Use Case 2: Migrating a Hub and Spoke Policy-Based VPN to Hub and Spoke Route-Based VPN

Scenario

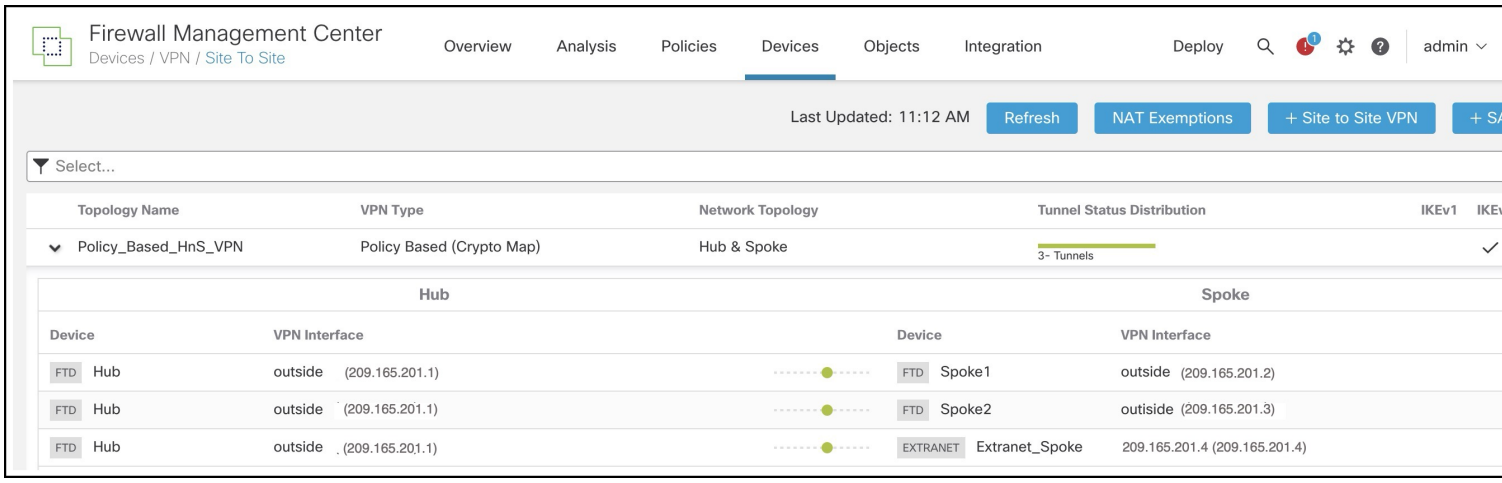
A medium-sized enterprise currently has a hub and spoke network with three Threat Defense devices (one hub and two spokes) and an extranet device. These devices are connected using a policy-based VPN, managed by a Management Center Version 7.4.1. Considering the advantages of a route-based VPN and the ability to scale the network easily, a network administrator plans to migrate this network to a route-based VPN using the management center VPN wizard.



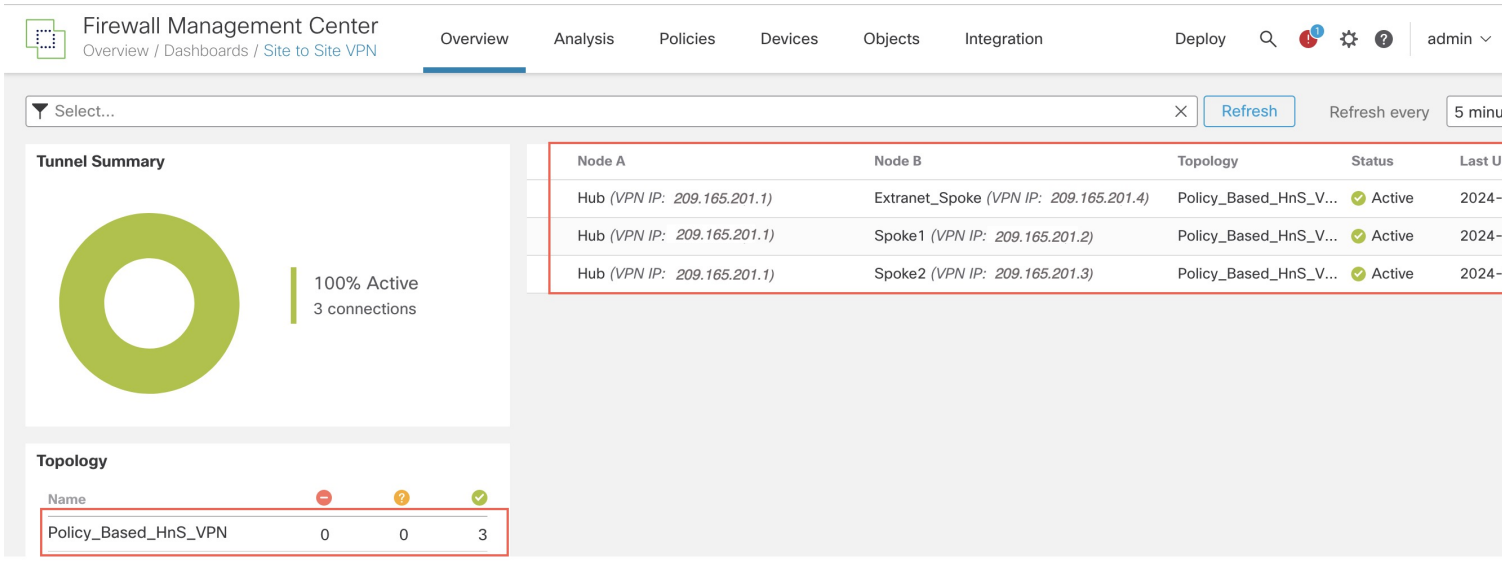
The policy-based VPN has the following parameters:

Device	Protected Network	VPN Interface
Hub	198.51.100.16/28	209.165.201.1
Spoke1	198.51.100.32/28	209.165.201.2
Spoke2	198.51.100.64/28	209.165.201.3
Extranet Spoke	209.165.200.225/27	209.165.201.4

You can view the policy-based VPN in the **Site-to-Site VPN Summary** page:



You can view details of the policy-based VPN in the **Site-to-Site VPN Dashboard**:



To view more details of the VPN tunnels, use the **show crypto ikev2 sa** and **show crypto ipsec sa** commands on the devices.

```
> show crypto ipsec sa
interface: outside
    Crypto map tag: CSM_outside_map, seq num: 5, local addr: 209.165.201.1

      access-list CSM_IPSEC_ACL_1 extended permit ip 198.51.100.16 255.255.255.224 198.51.100.32 255.255.255.224
      Protected vrf (ivrf):
      local ident (addr/mask/prot/port): (198.51.100.16/255.255.255.224/0/0)
      remote ident (addr/mask/prot/port): (198.51.100.32/255.255.255.224/0/0)
      current_peer: 209.165.201.2


      #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 2, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 209.165.201.1/500  remote crypto endpt.: 209.165.201.2/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: C470054C
      current inbound spi : 307C5CE9

    inbound esp sas:
      spi: 0x307C5CE9 (813456617)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
         slot: 0, conn_id: 74, crypto-map: CSM_outside_map
         sa timing: remaining key lifetime (kB/sec): (4285440/28168)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0xC470054C (3295675724)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
         slot: 0, conn_id: 74, crypto-map: CSM_outside_map
         sa timing: remaining key lifetime (kB/sec): (4147199/28168)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001

    Crypto map tag: CSM_outside_map, seq num: 4, local addr: 209.165.201.1

      access-list CSM_IPSEC_ACL_2 extended permit ip  198.51.100.16 255.255.255.224 198.51.100.64 255.255.255.224
      Protected vrf (ivrf):
      local ident (addr/mask/prot/port): (198.51.100.16/255.255.255.224/0/0)
      remote ident (addr/mask/prot/port): (198.51.100.64/255.255.255.224/0/0)
      current_peer: 209.165.201.3


      #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 209.165.201.1      remote crypto endpt.: 209.165.201.3
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 29E5932E
      current inbound spi : FE2CD7DC
```

```
> show crypto ikev2 sa

IKEv2 SAs:

Session-id:17, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                   Remote                                  fvrf/ivrf     Status
 169182659  209.165.201.1                         209.165.201.2/500                                       READY
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/131 sec
Child sa: local selector    198.51.100.16 - 198.51.100.31
          remote selector   198.51.100.32 - 198.51.100.47
          ESP spi in/out: 0x307c5ce9/0xc470054c

IKEv2 SAs:

Session-id:18, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                   Remote                                  fvrf/ivrf     Status
 171392979  209.165.201.1/500                     209.165.201.3/500                                       READY
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/115 sec
Child sa: local selector     198.51.100.16 - 198.51.100.31
          remote selector    198.51.100.64 - 198.51.100.79
          ESP spi in/out: 0xfe2cd7dc/0x29e5932e
```

Migrating Hub and Spoke Policy-Based VPN to Route-Based VPN

Prerequisites

For the extranet device:

- You must make the required configurations in the third-party deployment with the extranet device.
- If you plan to use route-based VPN on the extranet, the extranet device must support the following:
  - Static VTI
  - BGP, OSPF or EIGRP as the routing protocol. Dynamic VTI does not support static routes.
- If you plan to use policy-based VPN on the extranet, the Dynamic VTI hub supports policy-based VPN and can form tunnels with the extranet.

Procedure

To migrate the hub and spoke policy-based VPN to a hub and spoke route-based VPN:

Step	Task	More Information
1	Configure a loopback interface on the hub and the spokes. This loopback interface emulates the VPN tunnel network on both the devices.	Configure Loopback Interfaces on the Hub and Spokes, on page 14
2	Configure a hub and spoke route-based VPN using the VPN wizard.	Configure Hub and Spoke Route-Based VPN, on page 15
3	Configure a routing protocol. You can use BGP, EIGRP, or OSPF as the routing protocol.	• Configure BGP on Hub and Spokes, on page 17 • Configure EIGRP on Hub and Spokes, on page 16 • Configure OSPF on Hub and Spokes, on page 19

Step	Task	More Information
3	Delete the policy-based VPN.	-
4	Deploy the configurations on the devices.	-
5	Verify VPN tunnel statuses and configurations.	Verify Tunnel Statuses and Configurations of Route-Based VPN, on page 21

Configure Loopback Interfaces on the Hub and Spokes

Procedure

Step 1 Choose **Devices > Device Management**.

Step 2 Click the edit icon adjacent to the device.

Step 3 Click the **Interfaces** tab.

Step 4 From the **Add Interfaces** drop-down list, choose **Loopback Interface**.

In the **Add Loopback Interface** dialog box, configure the following parameters:

a) In the **Name** field, enter the name for the loopback interface.
b) Check the **Enabled** check box.
c) In the **Loopback ID** field, enter an ID between 1 to 1024.
d) Click the **IPv4** or **IPv6** tab.
e) In the **IP Address** field, enter the IP address for the loopback interface.
f) Click **OK**.

Step 5 Repeat Step 1 to Step 4 to configure a loopback interface on the other two Threat Defense devices.

In this example, the loopback interfaces emulating the VPN tunnel network of the devices is called Tunnel_Loopback.

The table below lists the loopback interfaces of the devices used in this example:

Device	Protected Network	Tunnel_Loopback Interface	VPN Interface
Hub	198.51.100.16/28	192.0.2.1/24	209.165.201.1
Spoke1	198.51.100.32/28	192.0.2.2/24	209.165.201.2
Spoke2	198.51.100.64/28	192.0.2.3/24	209.165.201.3
Extranet Spoke	209.165.200.225/27	192.0.2.4/24	209.165.201.4

For loopback interfaces, note the following:

- If you use BGP as the routing protocol: You can use /32 mask to conserve IP addresses as you manually define the peer IP address.
- If you use OSPF or EIGRP or as the routing protocol: The peer device must be in the same subnet for OSPF or EIGRP neighborship to come up by default. If you prefer to use the /32 mask, then you can manually define the peer IP address.

Configure Hub and Spoke Route-Based VPN

Procedure

Step 1 Choose **Devices** > **Site To Site**.

Step 2 Click **+ Site To Site VPN**.

Step 3 In the **Topology Name** field, enter a name for the VPN topology.

Step 4 Click the **Route Based (VTI)** radio button.

Step 5 Select **Hub and Spoke** as the network topology.

Step 6 Check the **IKEv1** or **IKEv2** check box to choose the IKE version to use during IKE negotiations.

Step 7 Click the **Endpoints** tab.

Step 8 For **Hub Nodes**, configure the following parameters:

In the **Add Endpoint** dialog box, configure the following parameters:

a) Choose **Hub** from the **Device** drop-down list.

b) Click **+** next to the **Dynamic Virtual Tunnel Interface** drop-down.

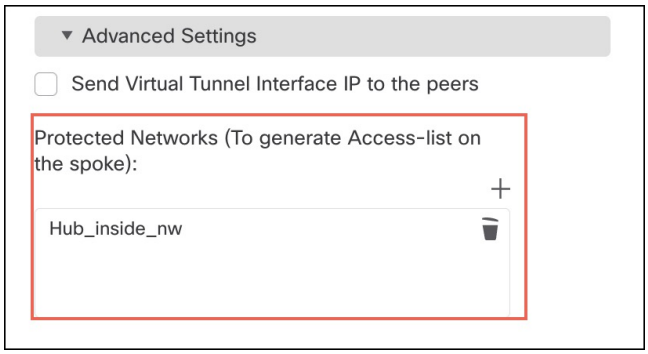
The **Add Virtual Tunnel Interface** dialog box is prepopulated with default configurations. However, you must configure the following parameters:

1. From the **Tunnel Source** drop-down list, choose the physical interface that is the source of the dynamic VTI. Choose the IP address of this interface from the adjacent drop-down list.
2. From the **Borrow IP** drop-down list, choose a loopback interface from the drop-down list. The dynamic VTI inherits this IP address.

   In this example, the Borrow IP is the Tunnel_Loopback interface (192.0.2.1/24).
3. Click **OK**.

c) (Optional) If you want to add the hub's protected network to the VTI configuration:

1. Expand **Advance Settings**.
2. Click **+** adjacent to **Protected Networks**.
3. In the **Network Objects** dialog box, choose the hub's protected network from the **Available Networks** list.
4. Click **Add** to move it to **Selected Networks**.
5. Click **OK**.



d) Click **OK**.

Step 9 For **Spoke Nodes**, click + to configure a spoke:

In the **Add Endpoint** dialog box, configure the following parameters:

a) From the **Device** drop-down list, choose **Spoke1**.
b) Click + adjacent to the **Static Virtual Tunnel Interface** drop-down list.

The **Add Virtual Tunnel Interface** dialog box is prepopulated with default configurations. However, you must configure the following parameters:

1. From the **Tunnel Source** drop-down list, choose the physical interface that is the source of the static VTI. Choose the IP address of this interface from the adjacent drop-down list.
2. From the **Borrow IP** drop-down list, choose a loopback interface from the drop-down list. The static VTI inherits this IP address.

   In this example, the Borrow IP for Spoke1 is the Tunnel_Loopback interface (192.0.2.2/24).
3. Click **OK**.

c) (Optional) If you want to add the spoke's protected network to the VTI configuration, repeat Step 8c.
d) Click **OK**.

Step 10 Repeat Step 9 to configure Spoke2.

Step 11 To configure the extranet device, click + adjacent to **Spoke Nodes**.

In the **Add Endpoint** dialog box, configure the following parameters:

a) From the **Device** drop-down list, choose **Extranet**.
b) In the **Device Name** field, enter the name of the device.
c) For **Endpoint IP Address**, click the **Static** or **Dynamic** radio button.
d) Enter the IP address of the device.
e) Click **OK**.

Configure EIGRP on Hub and Spokes

If you choose EIGRP as the routing protocol, use the following procedure:

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Click the edit icon adjacent to Hub.

Step 3 Click the **Routing** tab.

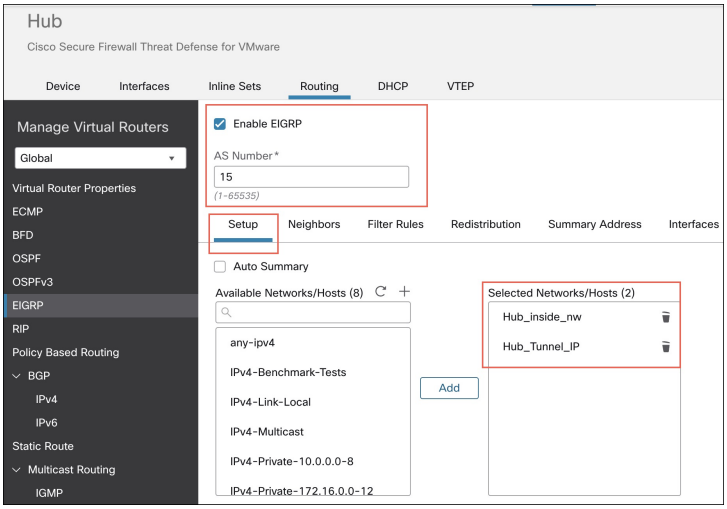
Step 4 In the left pane, choose **EIGRP**.

Step 5 Check the **Enable EIGRP** check box.

Step 6 In the **AS Number** field, enter the AS number of the device.

Step 7 Click the **Setup** tab.

Step 8 From the **Available Networks/Hosts** list, choose the protected network and the VPN tunnel network of the device. If you do not have network objects for these networks, click **+ Add** to create them.



Step 9 Other fields are optional, configure them according to your requirements.

Step 10 Click **Save**.

Step 11 To configure EIGRP on Spoke1 and Spoke2, repeat Step 1 to Step 10.

Step 12 Deploy the configurations to all the devices.

Configure BGP on Hub and Spokes

If you choose BGP as the routing protocol, use the following procedure:

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Click the edit icon adjacent to Hub.

Step 3 Click the **Routing** tab.

Step 4 In the left pane, choose **General Settings** > **BGP**.

Step 5 Check the **Enable BGP** check box.

Step 6 In the **AS Number** field, enter the AS number of the device.

Step 7 Other fields are optional, and you can configure them according to your requirements.

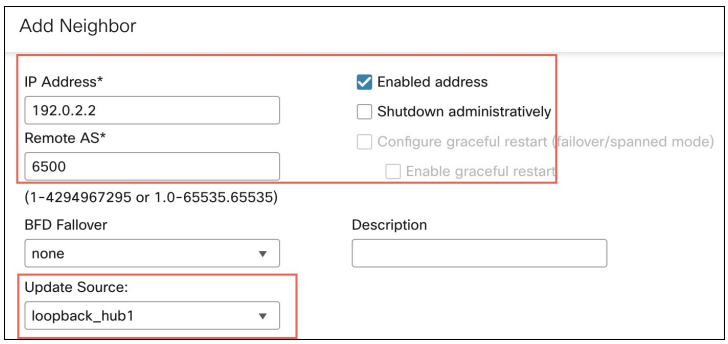
Step 8 Click **Save**.

Step 9 In the left pane, choose **BGP** > **IPv4**.

Step 10 Check the **Enable IPv4** check box.

Step 11 Click the **Neighbor** tab and click **+ Add**.

In the **Add Neighbor** dialog box, configure the following parameters:



a) In the **IP Address** field, enter the IP address of the peer.

In this example, it is the VTI IP address of Spoke1 (192.0.2.2/24).

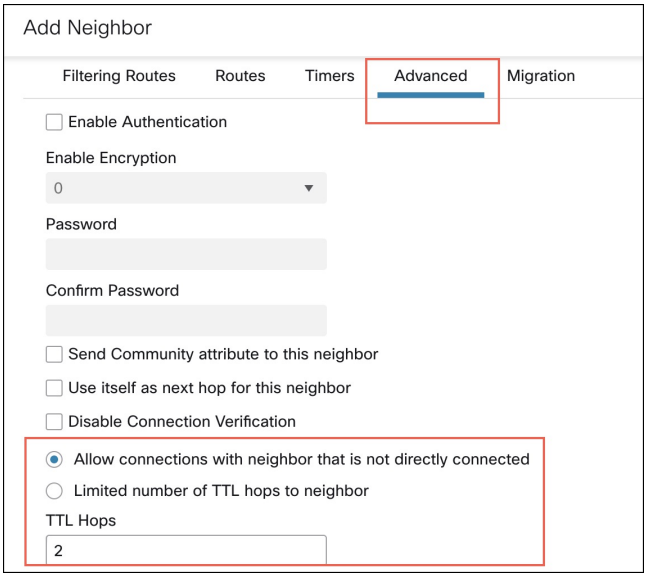
b) In the **Remote AS** field, enter the peer's AS number.

c) Check the **Enabled address** check box.

d) From the **Update Source** drop-down list, choose the loopback interface of the device.

e) Other fields are optional, and you can configure them according to your requirements.

f) (Optional) If the devices are in different regions, they use External Border Gateway Protocol (eBGP) to exchange routing information, and you must configure the multi-hop parameter.



1. Click the **Advanced** tab.

2. Select the **Allow connections with neighbor that is not directly connected** radio button.
3. In the **TTL Hops** field, enter the value as 2.
4. Other fields are optional, and you can configure them according to your requirements.

g) Click **OK**.

Step 12 To add Spoke2 as the neighbor, repeat Step 11.

Step 13 Click the **Networks** tab.

Step 14 Click **+ Add** to advertise the networks to the peers.

In the **Add Networks** dialog box, configure the following parameters:

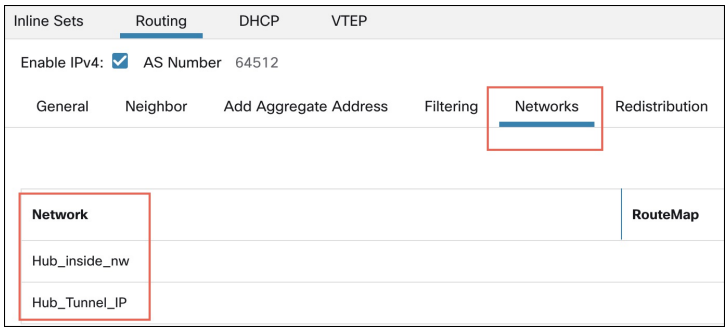
a) From the **Network** drop-down list, choose the protected network of the device.

In this example, for Hub, it is the protected network 198.51.100.16/28.

b) (Optional) From the **Route Map** drop-down list, choose the route map that should be examined to filter the advertised networks. By default, all networks are redistributed.

c) Click **OK**.

Step 15 To add the VPN tunnel network to be advertised over the tunnel, repeat Step 14.



Step 16 Click **Save**.

Step 17 To configure BGP on the peers (Spoke1 and Spoke2), repeat Step 1 to Step 16.

Step 18 Deploy the configurations to both the devices.

Configure OSPF on Hub and Spokes

If you choose OSPF as the routing protocol, use the following procedure:

Procedure

Step 1 Choose **Devices > Device Management**.

Step 2 Click the edit icon adjacent to Hub.

Step 3 Click the **Routing** tab.

Step 4 In the left pane, choose **OSPF**.

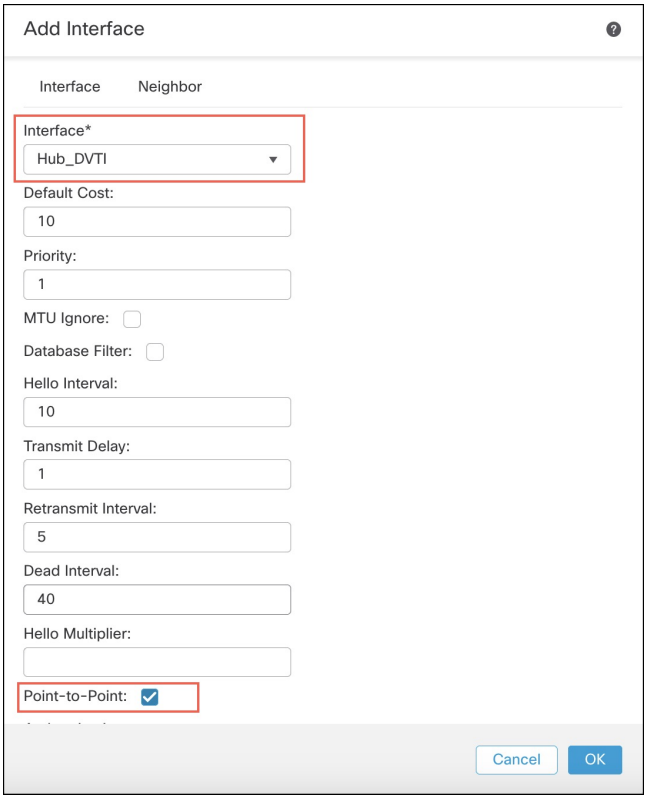
Step 5 Check the **Process 1** check box to enable an OSPF instance.

Step 6 Click the **Interface** tab.

Step 7 Click **+Add**.

In the **Add Interface** dialog box, configure the following parameters:

a) From the **Interface** drop-down list, choose the Dynamic VTI interface of the device.
b) Check the **Point-to-point** check box to transmit OSPF routes over VPN tunnels.
c) Use default values for the rest of the fields.



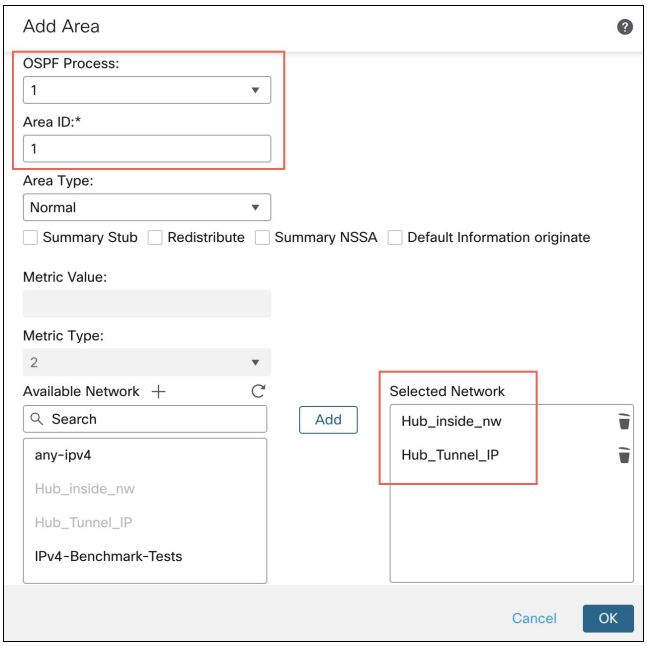
d) Click **OK**.

Step 8 Click the **Area** tab.

Step 9 Click **+Add**.

In the **Add Area** dialog box, configure the following parameters:

a) From the **OSPF Process** drop-down list, choose 1.
b) In the **Area ID** field, enter 1.
c) Use default values for the rest of the fields.
d) From the **Available Network** list, choose the protected network and the VPN tunnel network of the device. If you do not have network objects for these networks, click + to create them.



e) Click **OK**.

Step 10 Click **Save**.

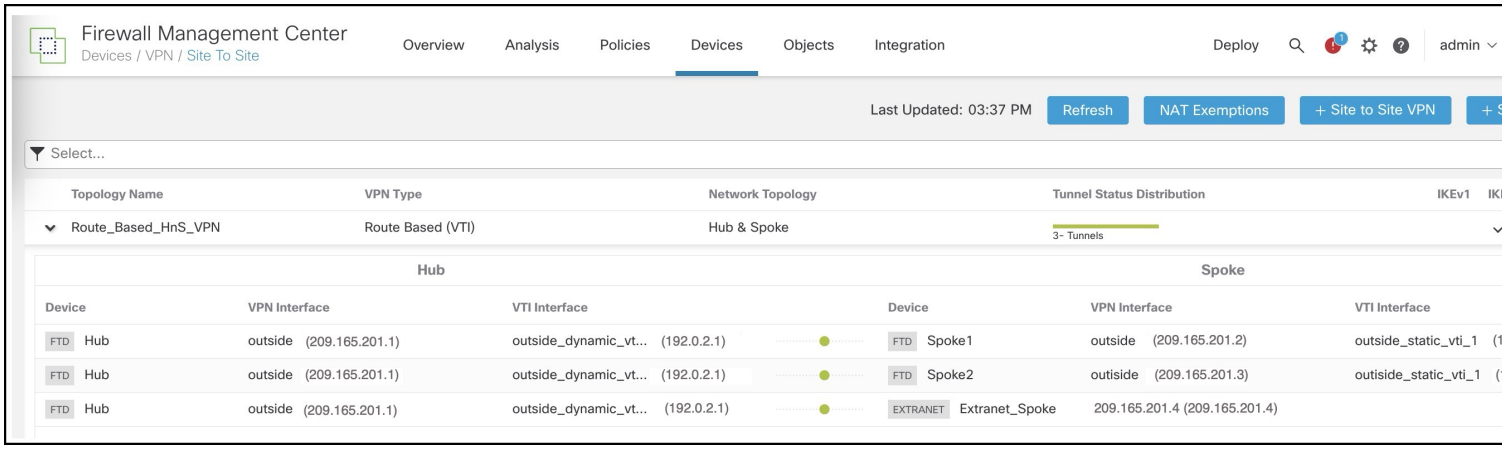
Step 11 To configure OSPF on Spoke1 and Spoke2, repeat Step 1 to Step 10.

Step 12 Deploy the configurations to all the devices.

Verify Tunnel Statuses and Configurations of Route-Based VPN

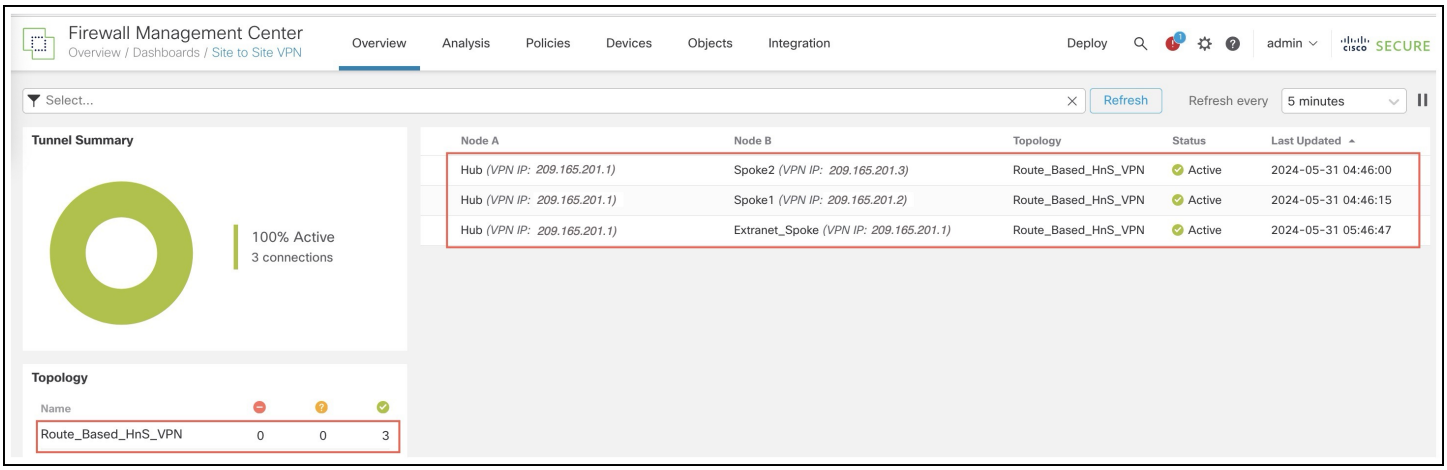
Verify Tunnel Statuses in the Site-to-Site VPN Summary Page

To verify the statuses of the VPN tunnels, choose **Device > VPN > Site To Site**.

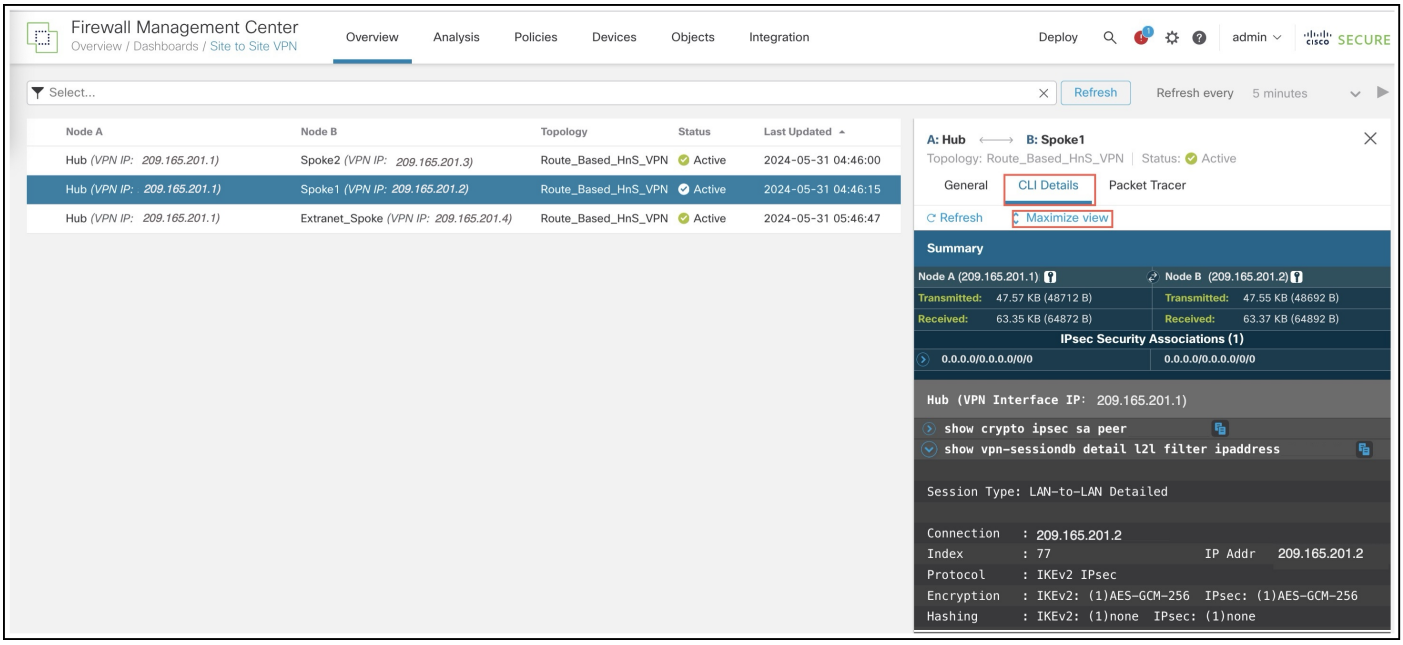


Verify Tunnel Statuses in the Site-to-Site VPN Dashboard

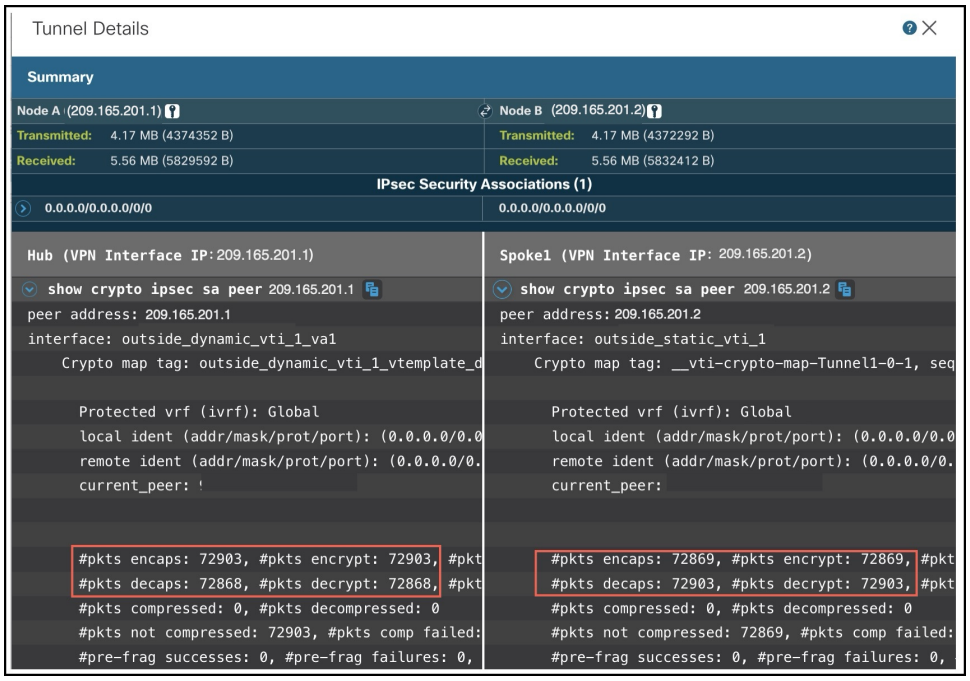
1. To view details of the VPN tunnel, choose **Overview > Dashboards > Site to Site VPN**.



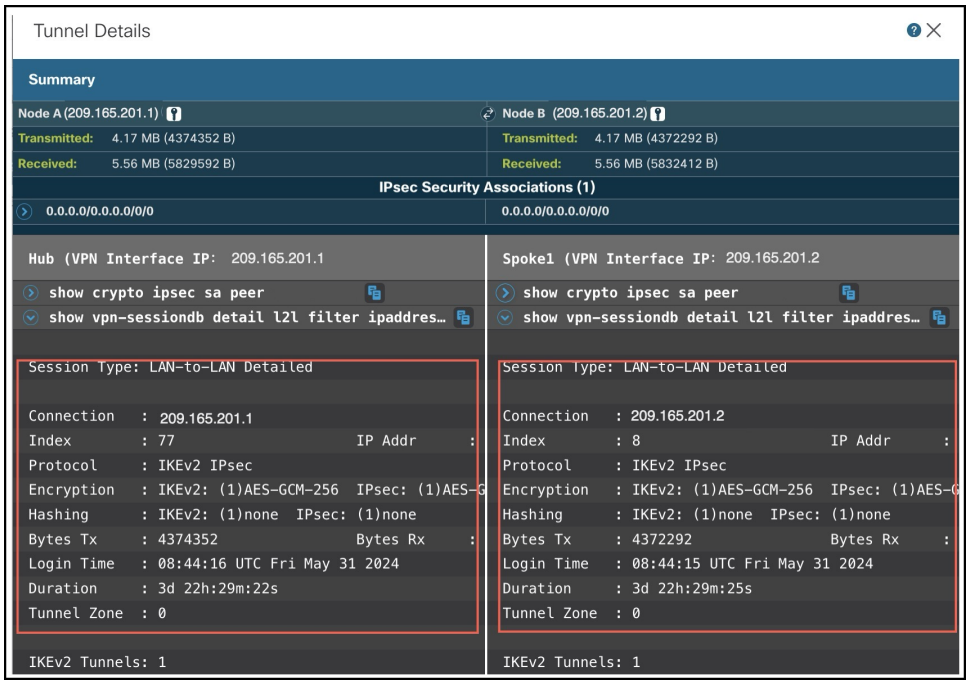
2. For each tunnel, hover your cursor over a topology and click the **View** icon to view more information about the tunnels.
3. Click the **CLI Details** tab.



4. Click **Maximize View**. You can view the output of the following commands:
   - **show crypto sa peer**: Shows the number of packets that are transmitted through the tunnel.



- **show vpn-sessiondb detail l2lfilter ipaddress**: Shows more detailed data for the VPN connection.



Verify Routing Configuration on Threat Defense Devices

To verify the BGP, OSPF, or EIGRP routes on the hub and the spokes, use the **show route** command on the device using the Management Center or the device CLI. You can also use the **show bgp**, **show ospf**, or **show eigrp** commands.

1. In the Management Center, choose **Devices > Device Management**.
2. Click the edit icon adjacent to the device.
3. Click the **Device** tab.
4. Click **CLI** in the **General** card.

   In the **CLI Troubleshoot** window, enter **show route** in the **Command** field and click **Execute**.

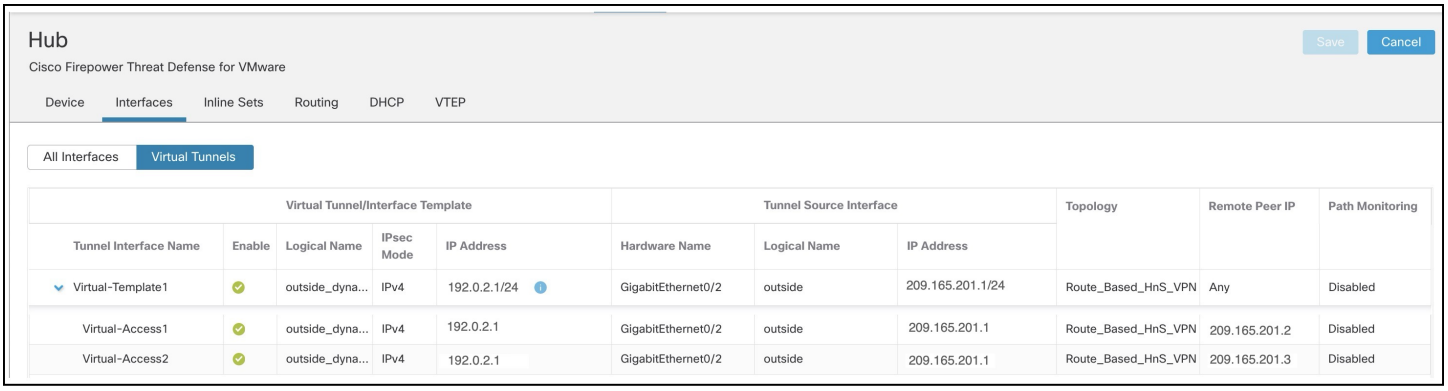
View Virtual Tunnel Interfaces of the Threat Defense Devices

To view the dynamic VTIs of hubs and static VTIs of spokes:

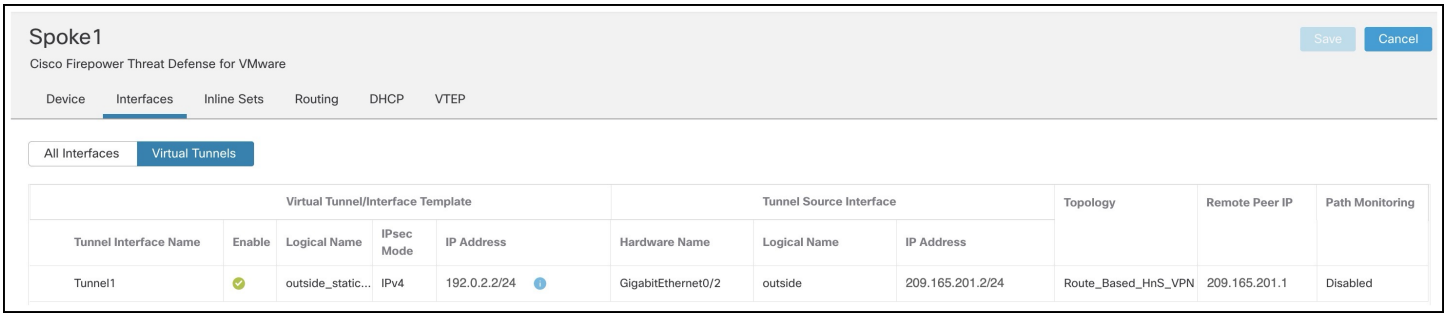
1. Choose **Devices > Device Management**.
2. Click the edit icon adjacent to the device.
3. Click the **Interfaces** tab.
4. Click the **Virtual Tunnels** tab.

For each VTI, you can view details such as name, IP address, IPsec mode, tunnel source interface details, topology, and remote peer IP.

The dynamic VTI and the dynamically created virtual access interfaces of the Hub are shown in the figure below:



The static VTI created on Spoke1 is shown in the figure below:



Troubleshoot Route-Based VPN Tunnels

After the deployment, use the following CLI commands and tools to debug issues related to route-based VPN tunnels on Threat Defense devices.

CLI and Debug Commands

Command	Description
ping	Ping the outside IP address of the peer to the check the connectivity between the devices.
show vpnsession db	Displays summary information about current VPN sessions.
debug crypto condition peer <peer-IP>	Enable conditional debugging for a particular peer
debug vti 255	Debug the Virtual Tunnel Interface information.

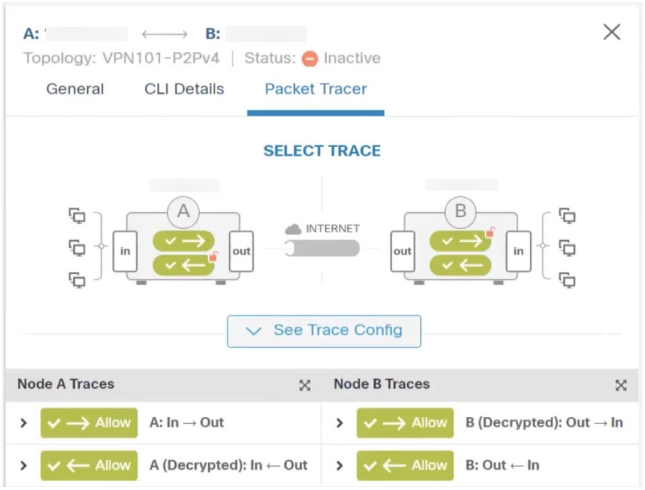
Packet Tracer

The Packet Tracer tool allows you to test policy configurations by modeling a packet with source and destination addresses, and protocol characteristics. Besides verifying your configuration, you can use this tool to debug unexpected behaviour, such as packets being denied access.

To use a packet tracer on Threat Defense devices, choose **Devices > Packet Tracer**. You must be an Admin or Maintenance user to use this tool.

You can also use the Packet Tracer in the **Site to Site VPN Dashboard** to troubleshoot VPN tunnels between two Threat Defense devices.

1. Choose **Overview > Dashboards**.
2. For each tunnel, hover your cursor over a topology and click the View icon to view more information about the tunnels.
3. Click the **Packet Tracer** tab.
4. Configure the parameters.
5. Click **Trace Now**.
6. After the trace completes, you can view the output of the trace with the results of each module.


A: ⟷ B:
Topology: VPN101-P2Pv4 | Status: Inactive
General
CLI Details
Packet Tracer
SELECT TRACE
A
in
out
INTERNET
B
out
in
See Trace Config
Node A Traces
Allow
A: In → Out
Allow
A (Decrypted): In ← Out
Node B Traces
Allow
B (Decrypted): Out → In
Allow
B: Out ← In

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.