Configure Dual ISP Topology with Two Hubs and Four Spokes in the Same Region

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background information

- Supported Software & Hardware Platforms

Configure

- Network Diagram
- Step 1. Create an SD-WAN Topology with WAN-1 as the VPN Interface
- Step 2. Configure the Dynamic Virtual Tunnel Interface (DVTI) on the Primary Hub
- Step 3. Configure the DVTIon the Secondary Hub
- Step 4. Configure the Spokes
- Step 5. Configure the Authentication Settings
- Step 6. Configure the SD-WAN Settings
- Step 7. Create an SD-WAN Topology with WAN-2 as the VPN Interface
- Step 8. Configure (Equal-Cost Multi-Path) ECMP Zones
- Step 9. Modify the BGP Local Preference on the Hub

Verify

- Verify Tunnel Statuses
- Verify Virtual Tunnel Interfaces (VTIs)
- Verify Load Balancing of VPN Traffic
- Verify Dual ISP Redundancy
- Verify Hub Level Redundancy

Introduction

This document describes how to configure a dual ISP topology with two hubs and four spokes in the same region using the SD-WAN wizard.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Firewall Threat Defense (FTD)
- Cisco Secure Firewall Management Center (FMC)
- Software-defined WAN (SD-WAN)

Components Used

The information in this document is based on these software and hardware versions:

- FTD version 7.6.0
- FMC version 7.6.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

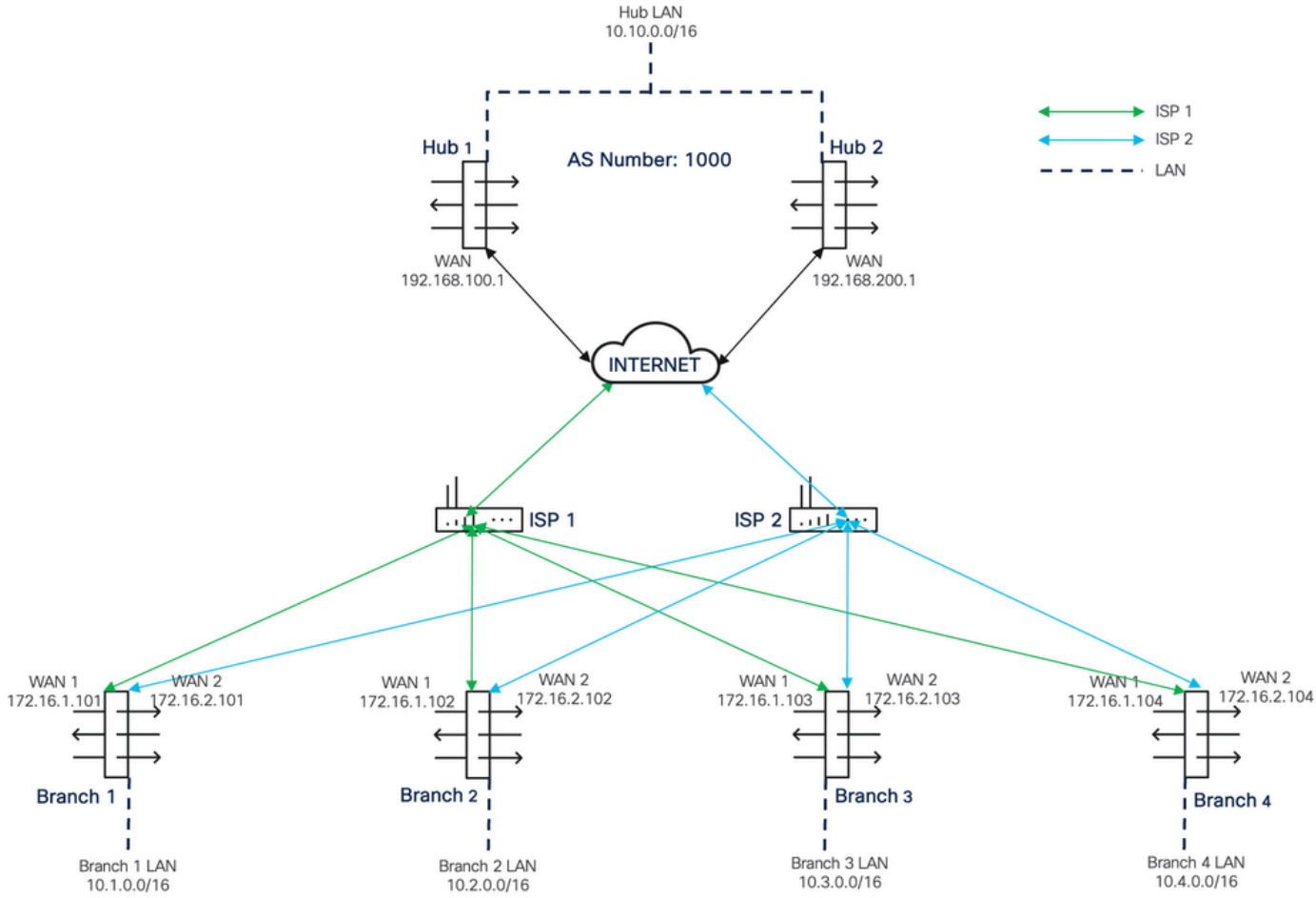
Background information

Supported Software & Hardware Platforms

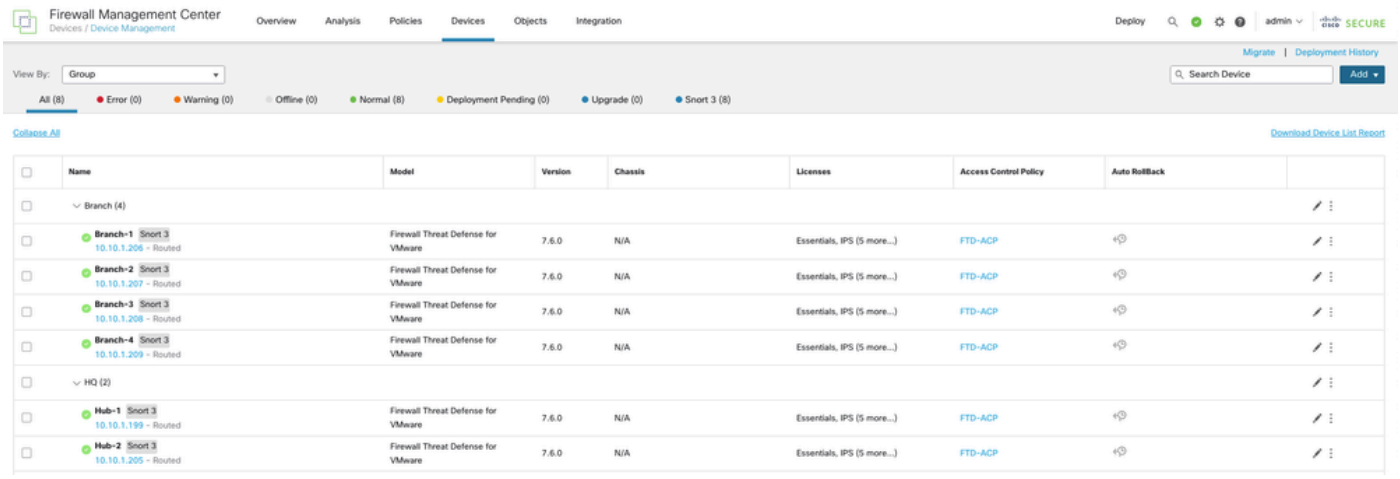
Manager	FTD	Supported Platforms
• FMC >= 7.6.0 and FMC REST API • cdFMC >= 7.6.0 • FDM - Not Supported	• Hub FTD >= 7.6.0 • Spoke FTD >= 7.3.0	All platforms that FMC >= 7.6.0 can manage

Configure

Network Diagram



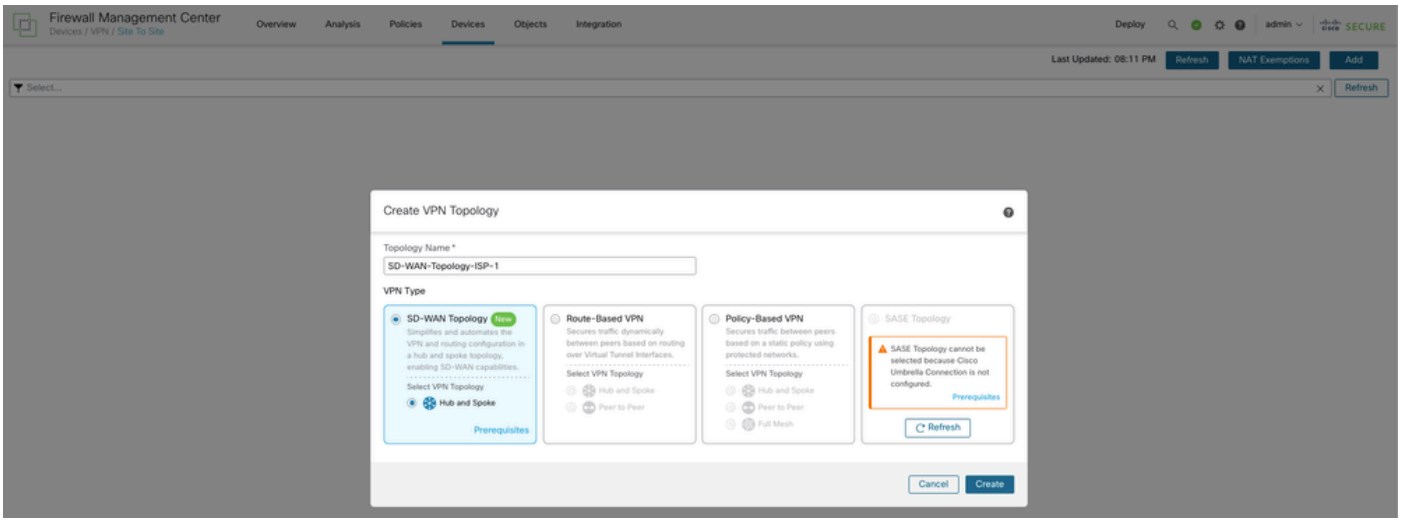
Network topology diagram



List of devices

Step 1. Create an SD-WAN Topology with WAN-1 as the VPN Interface

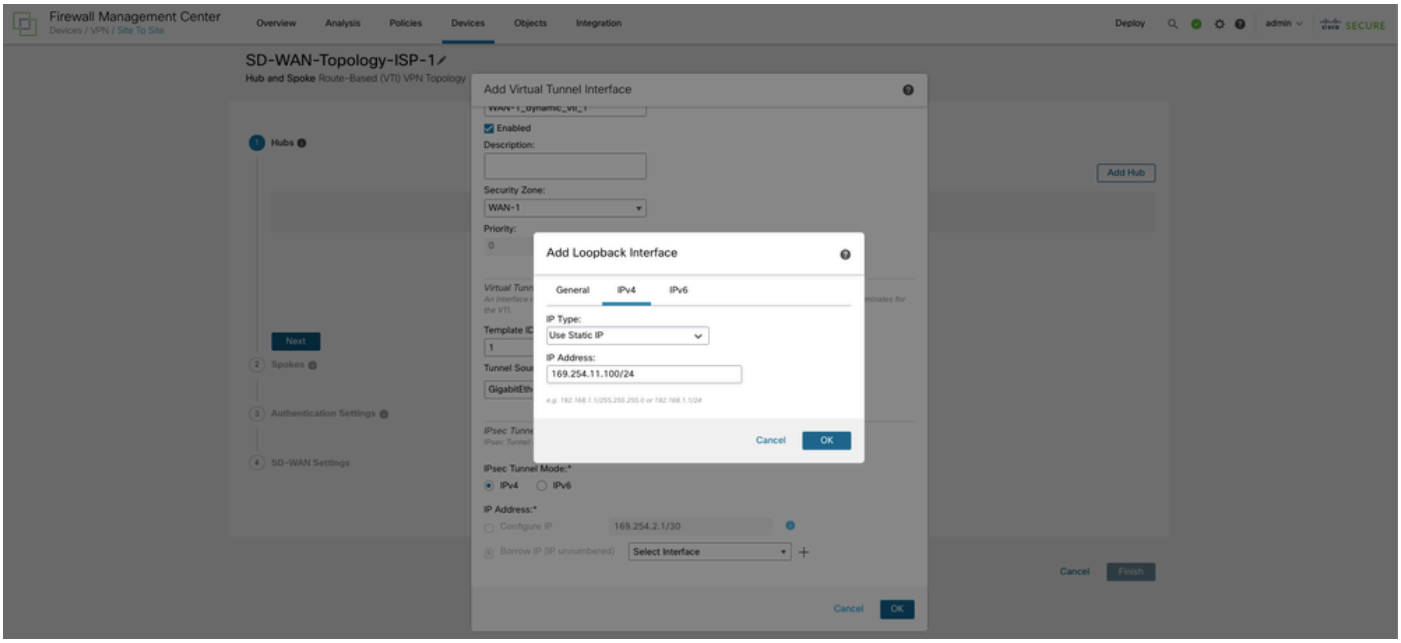
Navigate to **Devices > VPN > Site To Site**. Choose **Add**, and enter a suitable name in the **Topology Name** field for the first topology with WAN-1 as the VPN interface. Click **SD-WAN Topology>Create**.



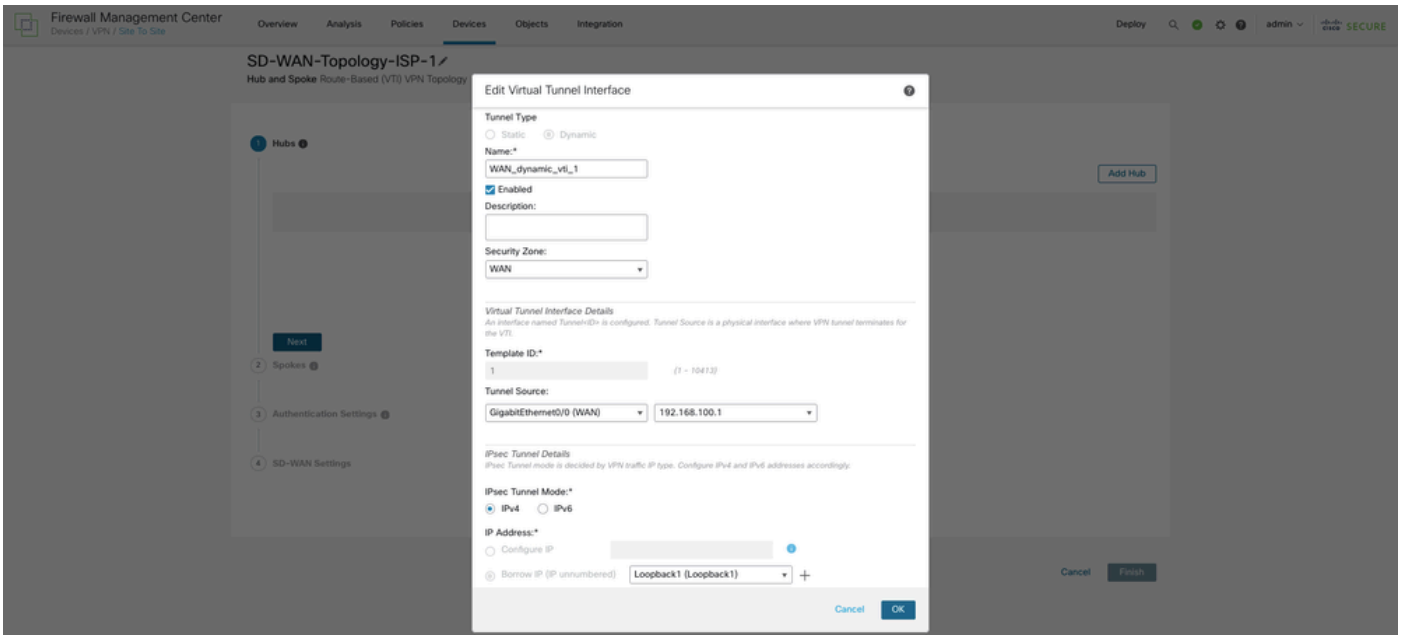
Create an SD-WAN Topology with WAN-1 as the VPN Interface

Step 2. Configure the Dynamic Virtual Tunnel Interface (DVTI) on the Primary Hub

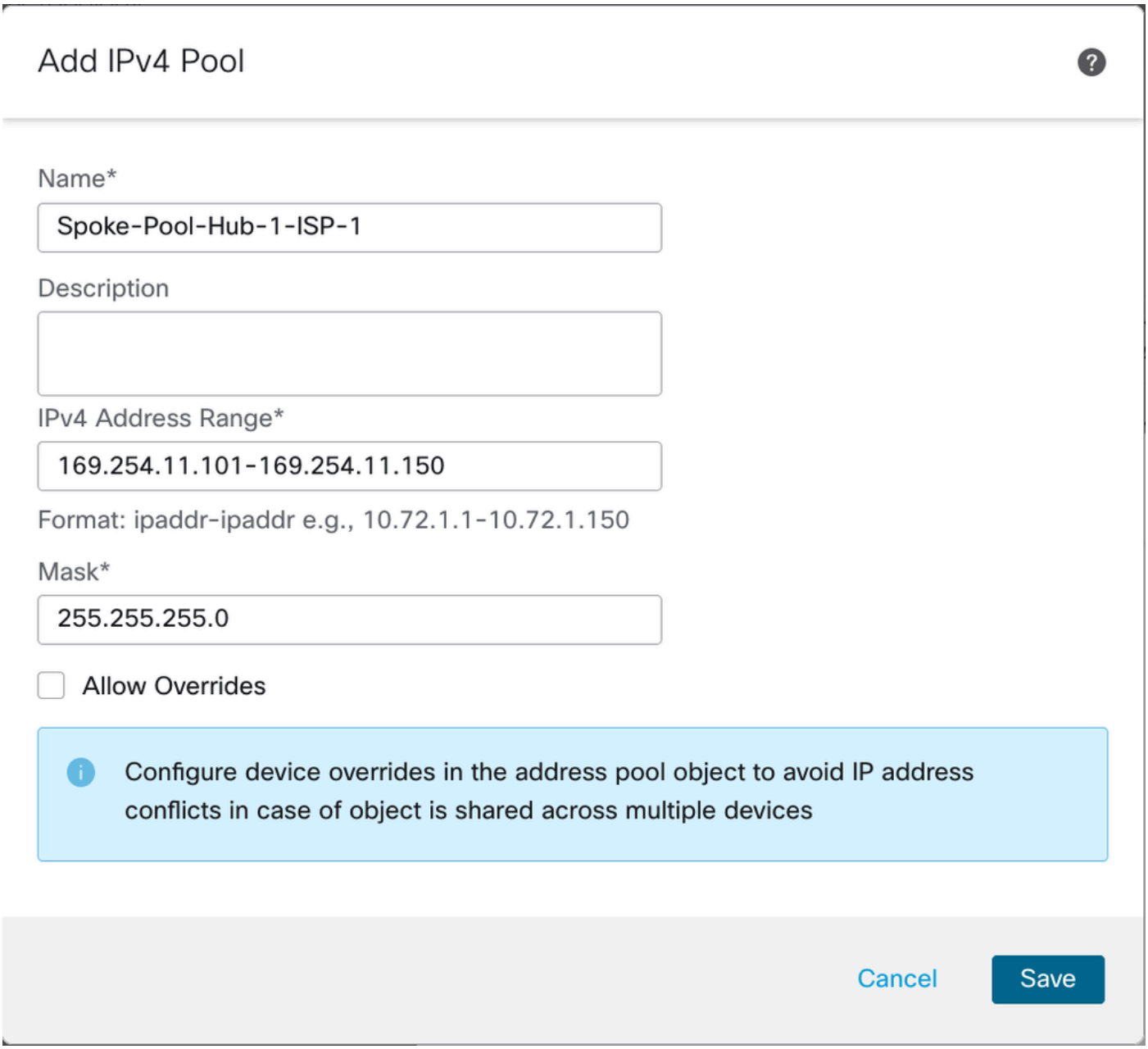
Click **Add Hub** and choose the primary hub from the **Device** drop-down list. Click the + icon next to **Dynamic Virtual Tunnel Interface (DVTI)**. Configure a name, security zone, and template ID and assign WAN-1 as the **Tunnel Source** interface for the DVTI.



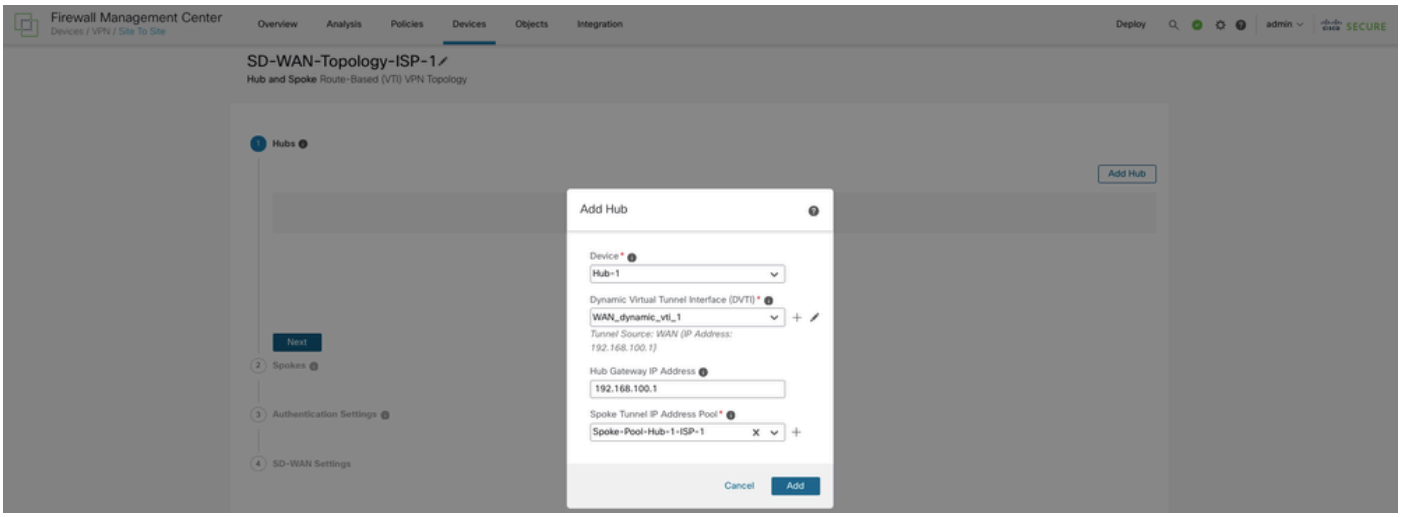
Choose a physical or loopback interface from the **Borrow IP** drop-down list. In the current topology, the DVTI inherits a loopback interface IP address. Click **OK**.



Choose an address pool or click the **+** icon next to **Spoke Tunnel IP Address Pool** in order to create a new address pool. When you add spokes, the wizard auto generates spoke tunnel interfaces, and assigns IP addresses to these spoke interfaces from this IP address pool.

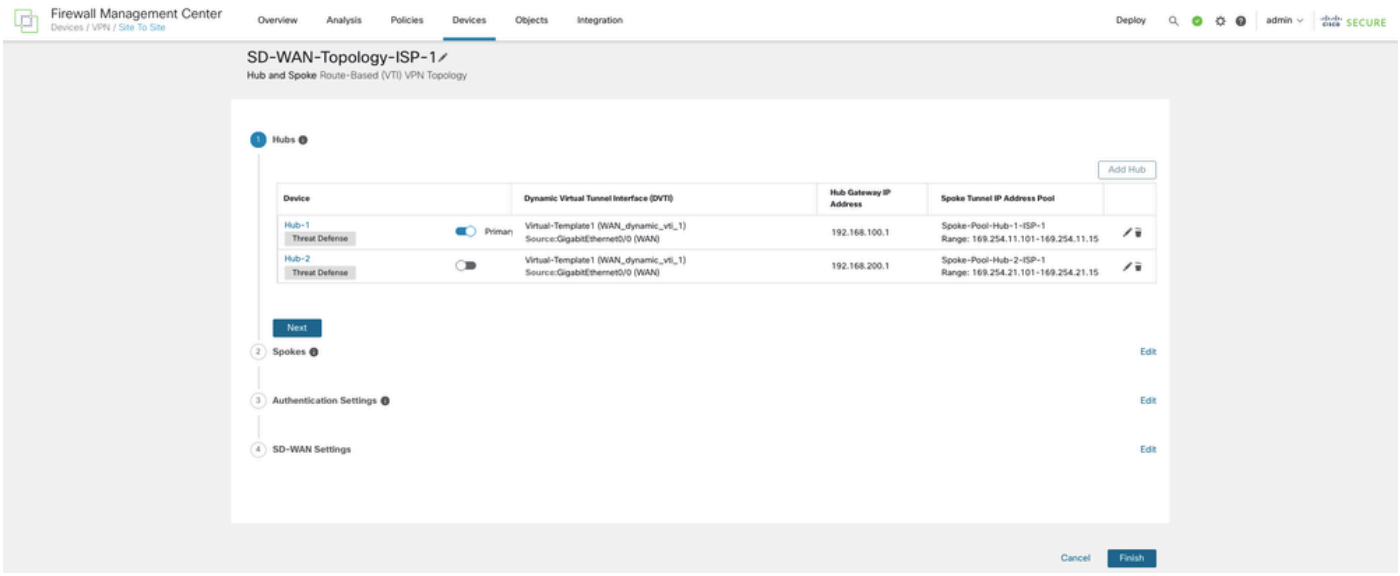


Once the primary hub configuration is complete, choose **Add** in order to save the primary hub in the topology.



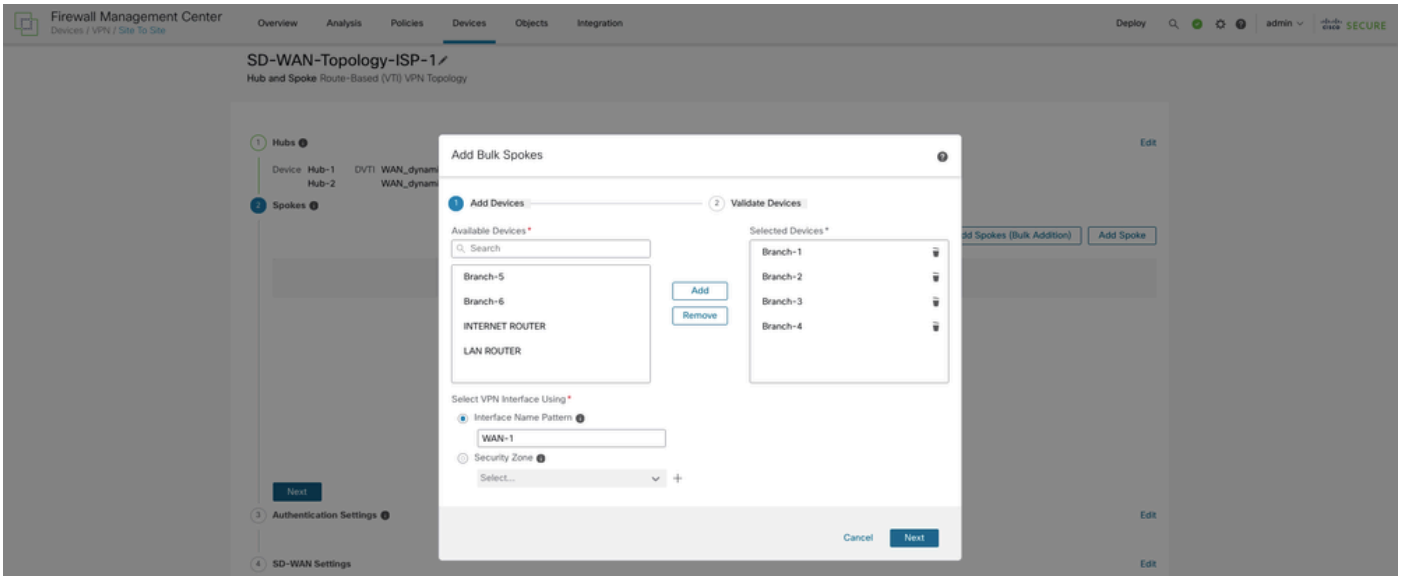
Step 3. Configure the DVTI on the Secondary Hub

Now choose **Add Hub** again in order to configure the secondary hub in the topology with WAN-1 as the VPN interface by repeating steps 1 and 2. Click **Next**.

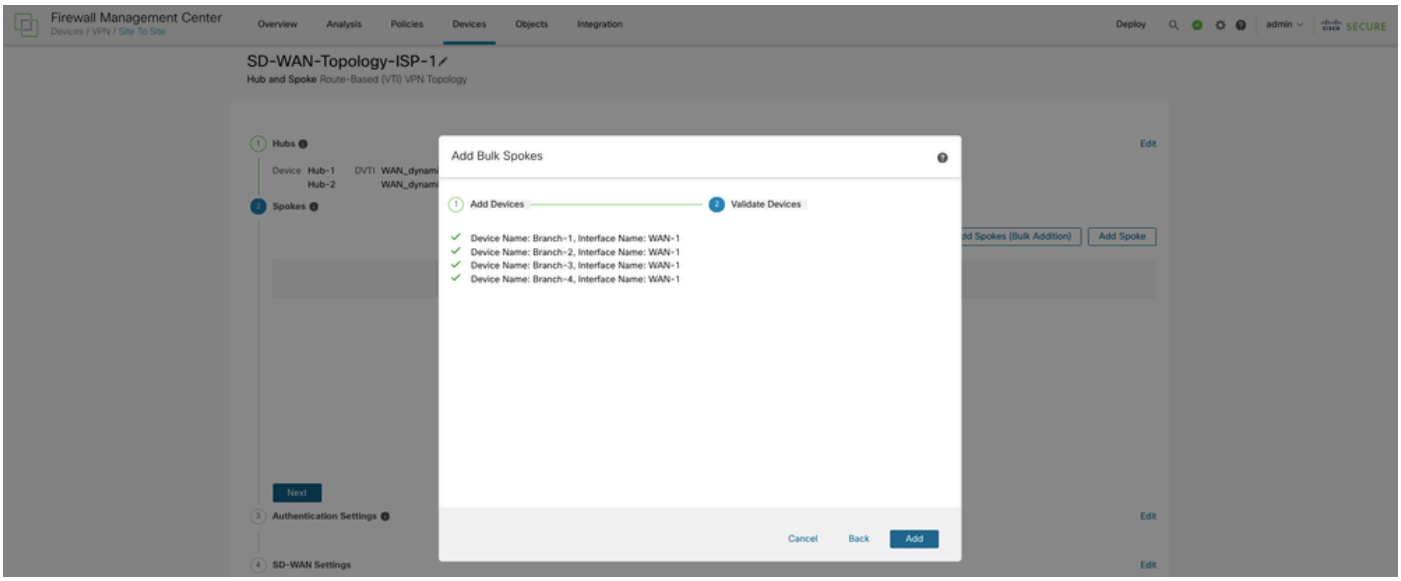


Step 4. Configure the Spokes

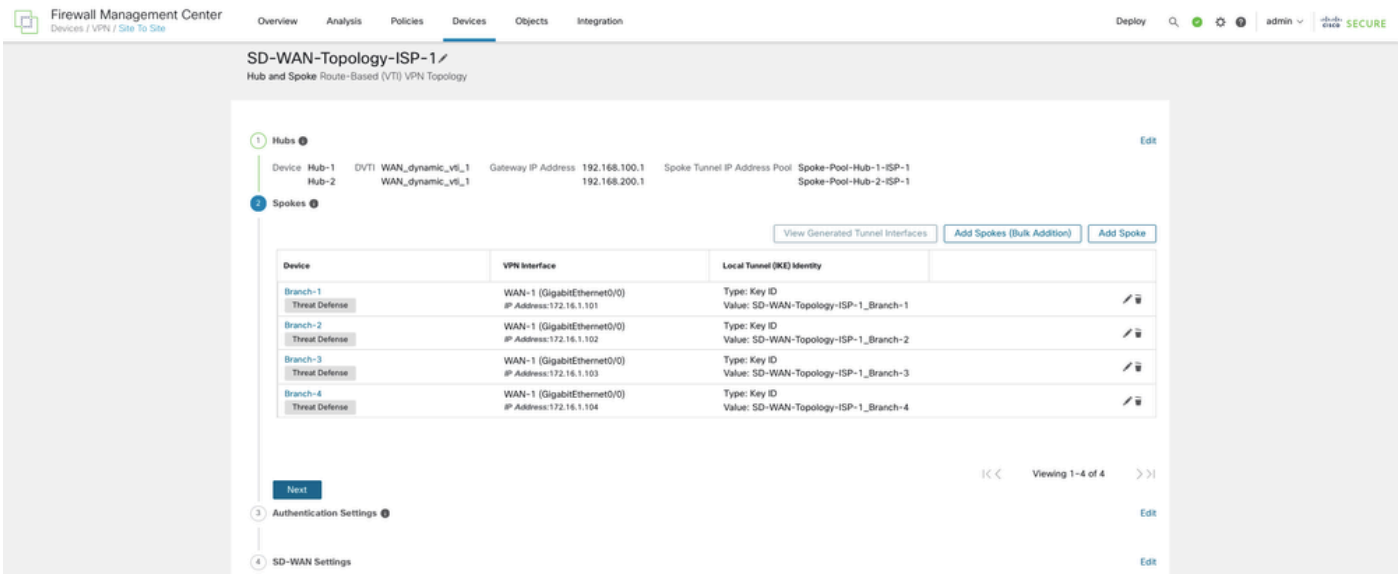
Choose **Add Spoke** in order to add a single spoke device, or click **Add Spokes (Bulk Addition)** in order to add multiple spokes to your topology. The current topology uses the latter option in order to add multiple branch FTDs to the topology. In the **Add Bulk Spokes** dialog box, choose the required FTDs in order to add them as spokes. Choose either a common **Interface Name Pattern** that matches the logical name of WAN-1 on all spokes or the **Security Zone** that is associated with WAN-1.



Click **Next** so that the wizard validates if the spokes have interfaces with the specified pattern or security zone.

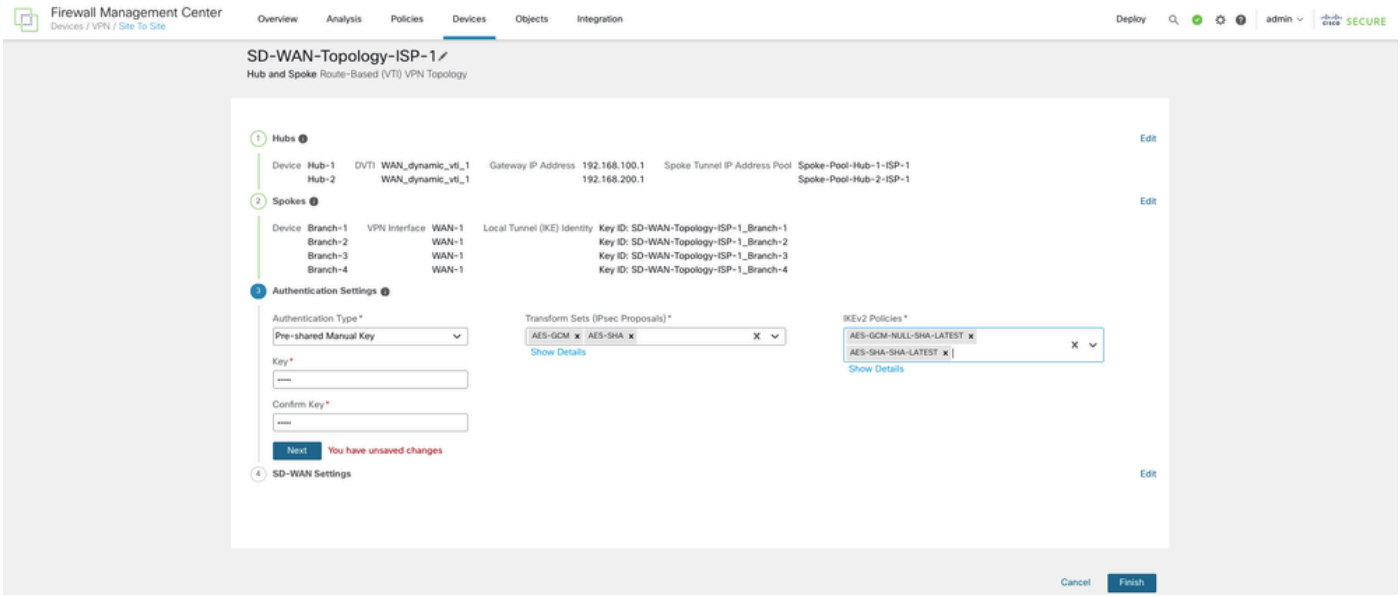


Choose **Add** and the wizard automatically chooses the hub DVTI as the tunnel source IP address for each spoke.



Step 5. Configure the Authentication Settings

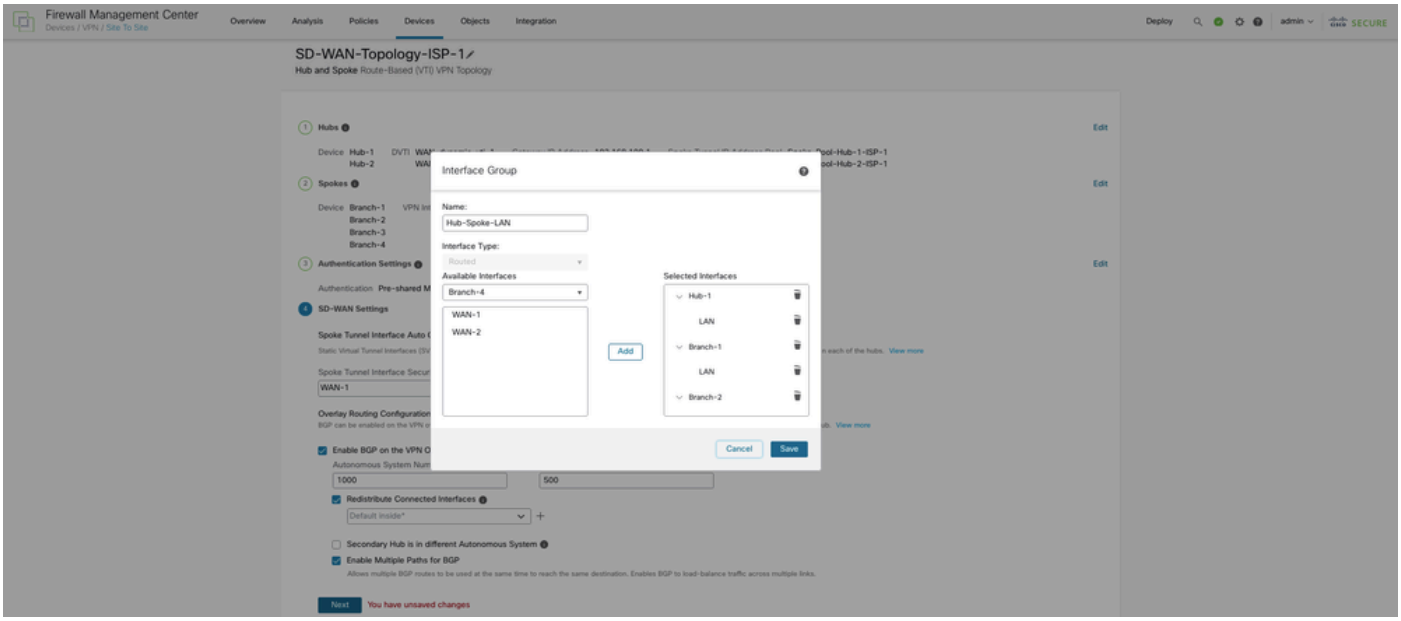
Click **Next** in order to configure the **Authentication Settings**. For device authentication, you can choose a manual pre-shared key, an auto-generated pre-shared key, or a certificate in the **Authentication Type** drop-down list. Choose one or more algorithms from the **Transform Sets** and **IKEv2 Policies** drop-down lists.



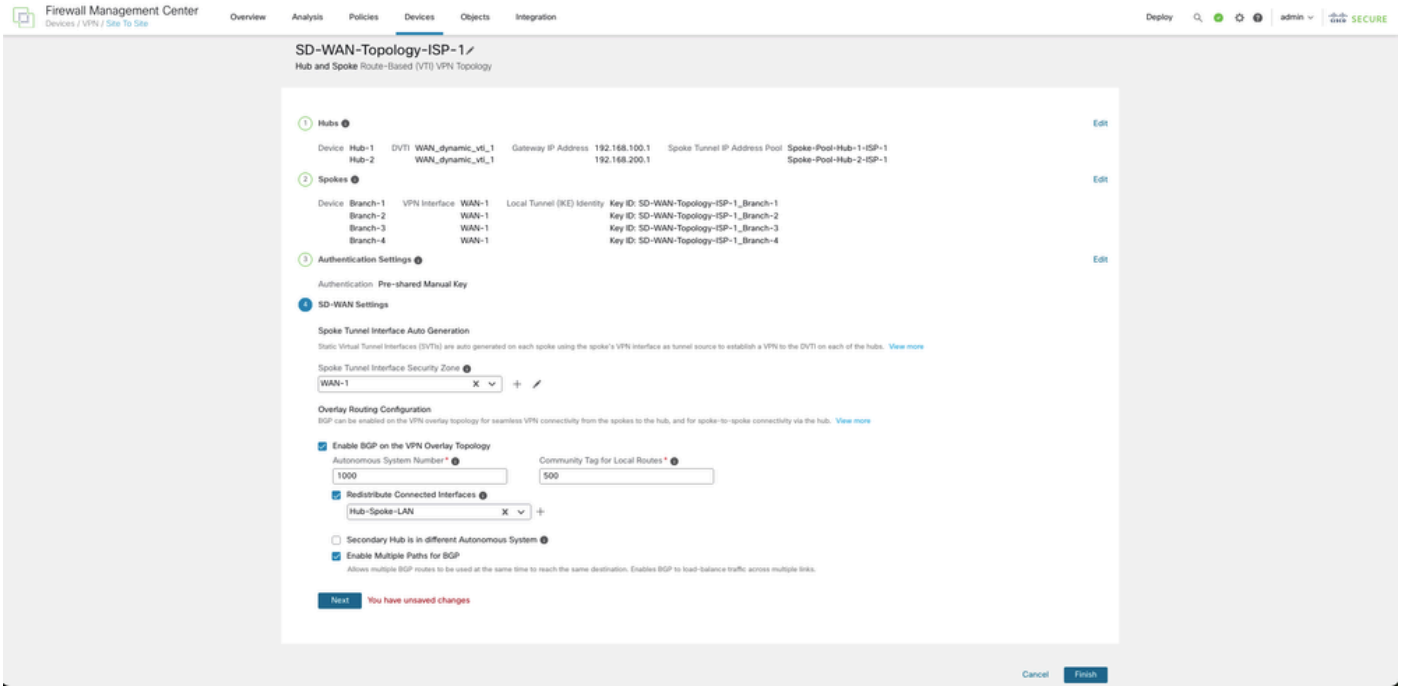
Step 6. Configure the SD-WAN Settings

Click **Next** in order to configure the **SD-WAN Settings**. This step involves the auto-generation of spoke tunnel interfaces, and Border Gateway Protocol (BGP) configuration of the overlay network. From the **Spoke Tunnel Interface Security Zone** drop-down list, choose a security zone or click **+** in order to create a security zone to which the wizard automatically adds the spokes' auto-generated Static Virtual Tunnel Interfaces (SVTIs).

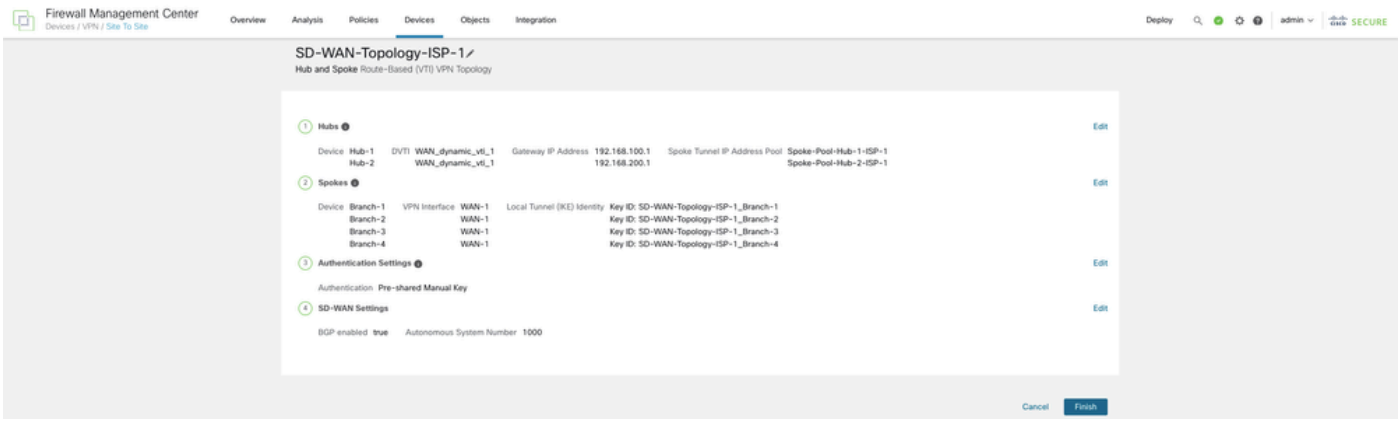
Check the **Enable BGP on the VPN Overlay Topology** check box in order to automate BGP configurations between the overlay tunnel interface. In the **Autonomous System Number** field, enter an Autonomous System (AS) number. Check the **Redistribute Connected Interfaces** check box and choose an interface group from the drop-down list or choose **+** in order to create an interface group with connected LAN interfaces of the hubs and spokes for BGP route redistribution in the overlay topology.



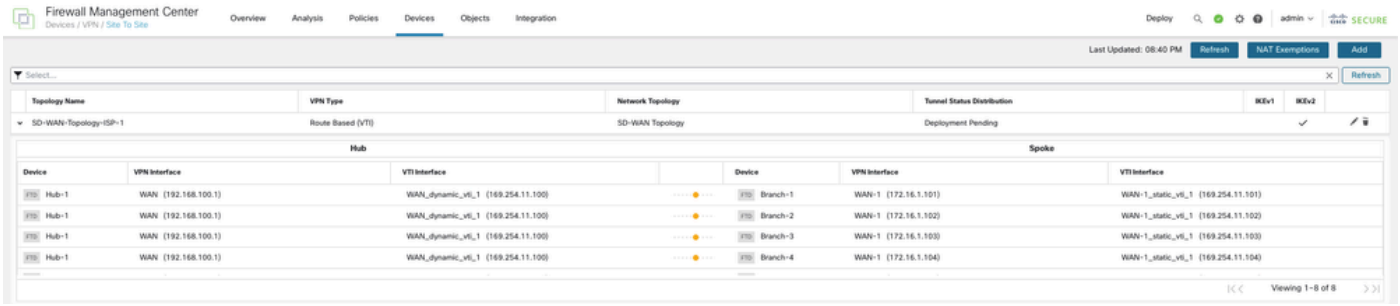
In the **Community Tag for Local Routes** field, enter the BGP community attribute in order to tag connected and redistributed local routes. This attribute enables easy route filtering. Check the **Secondary Hub is in the Different Autonomous System** check box if you have a secondary hub in a different AS. Finally, check the **Enable Multiple Paths for BGP** check box in order to enable BGP to load-balance traffic across multiple links.



Click **Finish** in order to save and validate the SD-WAN topology.

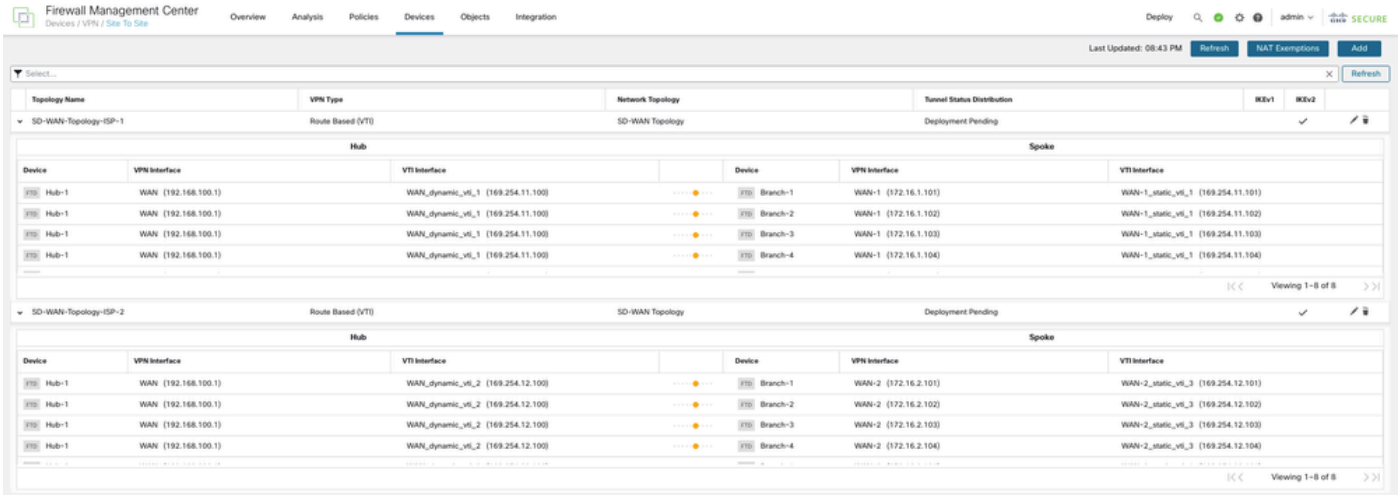


You can view the topology under **Devices > Site-to-site VPN**. The total number of tunnels in the first SD-WAN topology is 8.



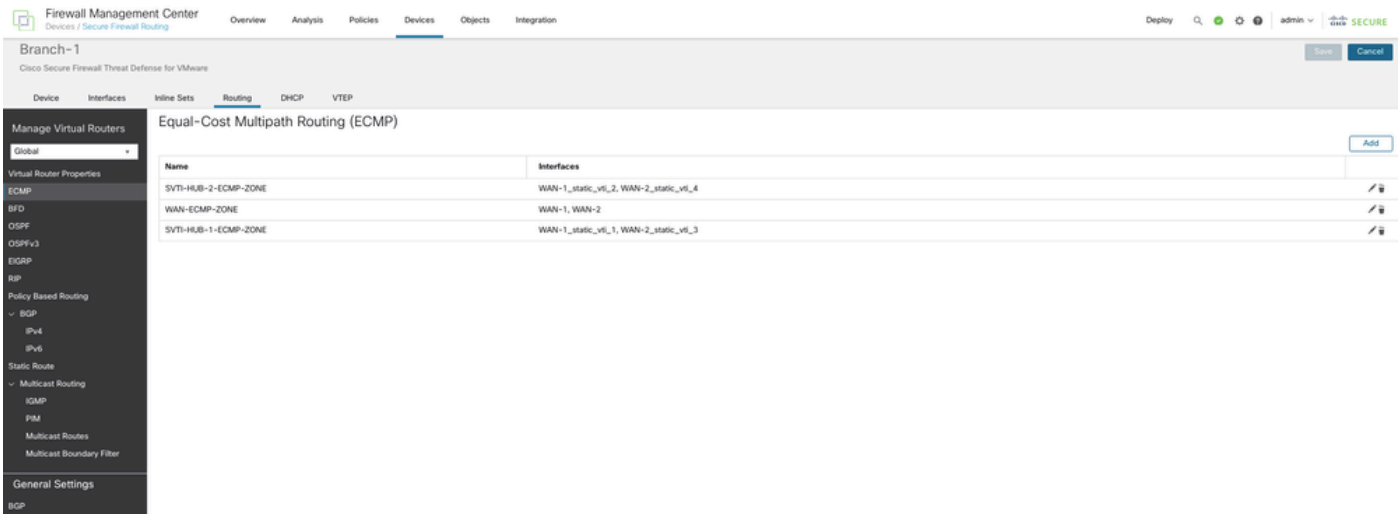
Step 7. Create an SD-WAN Topology with WAN-2 as the VPN Interface

Repeat steps 1 through 6 in order to configure an SD-WAN Topology with WAN-2 as the VPN interface. The total number of tunnels in the second SD-WAN topology is 8. The final topologies must look like the image shown:



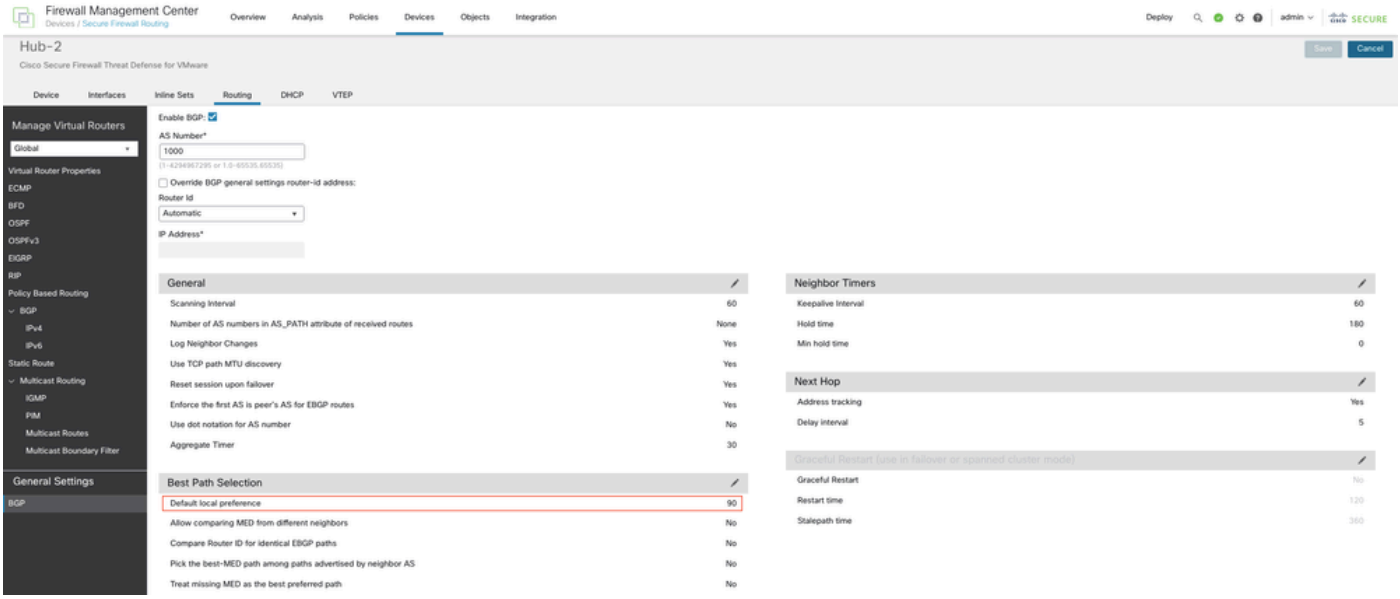
Step 8. Configure (Equal-Cost Multi-Path) ECMP Zones

On each branch, navigate to **Routing > ECMP** and configure ECMP Zones for the WAN interfaces and SVTIs connecting to both the primary and secondary Hub, as shown. This can provide link redundancy and enable load balancing of the VPN traffic.



Step 9. Modify the BGP Local Preference on the Hub

Navigate to **Routing > General Settings > BGP** on the secondary hub. Click **Enable BGP**, configure the **AS Number**, and set the **default local preference** value under **Best Path Selection** to a value lower than the one configured on the primary hub. Click **Save**. This ensures that routes to the primary hub are preferred over routes to the secondary hub. When the primary hub goes down, the routes to the secondary hub take over.

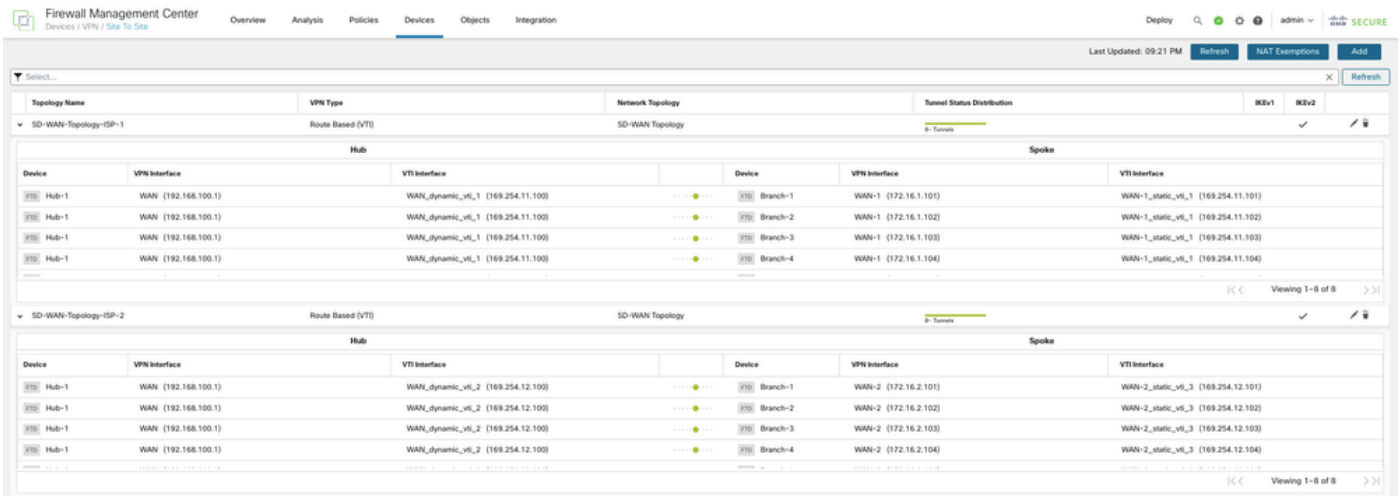


Deploy the configurations to all the devices.

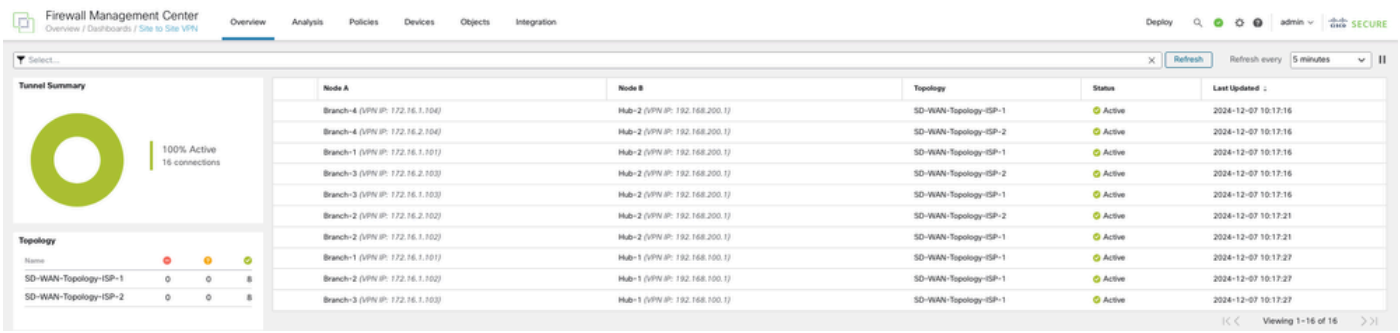
Verify

Verify Tunnel Statuses

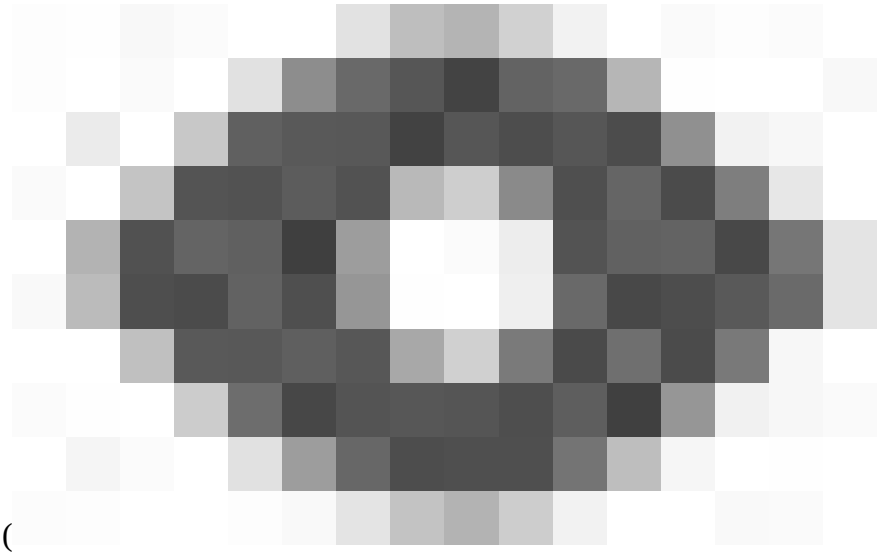
In order to verify if the VPN tunnels of the SD-WAN topologies are up, navigate to **Device > VPN > Site-to-Site**.



In order to view details of the SD-WAN VPN tunnels, choose **Overview > Dashboards > Site-to-site VPN**.



In order to view more details of each VPN tunnel:

1. Hover over a tunnel.
2. Click the **View Full Information** () icon. A pane with tunnel details and more actions appears.
3. Click the **CLI Details** tab in the side pane in order to view the show commands and details of the IPsec security associations.

A: Branch-1 ⟷ B: Hub-1

Topology: SD-WAN-Topology-ISP-2 | Status: Active

General | CLI Details | Packet Tracer

Refresh | Maximize view

Summary

Node A (172.16.2.101/500)		Node B (192.168.100.1/500)	
Transmitted:	8.46 KB (8664 B)	Transmitted:	5.98 KB (6123 B)
Received:	27.73 KB (28400 B)	Received:	7.68 KB (7868 B)

IPsec Security Associations (2)

0.0.0.0/0.0.0.0/0/0		0.0.0.0/0.0.0.0/0/0	
Settings:	L2L,Tunnel,IKEv2,...	Settings:	L2L,Tunnel,IKEv2,VTI
Encaps/Encrypt:	140 / 140 pkts	Encaps/Encrypt:	92 / 92 pkts
Dcaps/Decrypt:	232 / 232 pkts	Dcaps/Decrypt:	96 / 96 pkts

Remaining Lifetime for SPI ID: 0x5B2983A9

Outbound:	3.69 GB (3962871000 B) 12:47:26 (26246 sec)	Inbound:	3.65 GB (3916794000 B) 12:50:26 (26426 sec)

Remaining Lifetime for SPI ID: 0x0F4EA9C0

Inbound:	3.99 GB (4285416000 B) 12:47:26 (26246 sec)	Outbound:	3.69 GB (3962874000 B) 12:50:26 (26426 sec)

0.0.0.0/0.0.0.0/0/0		
Settings:	L2L,Tunnel,IKEv2,...	
Encaps/Encrypt:	96 / 96 pkts	Info is not available for Extranet device
Dcaps/Decrypt:	92 / 92 pkts	

Remaining Lifetime for SPI ID: 0x1DEFCB21

Outbound:	4.03 GB (4331514000 B) 12:50:25 (26425 sec)	Inbound:	No data

Remaining Lifetime for SPI ID: 0x53B1AE47

Inbound:	3.65 GB (3916794000 B) 12:50:25 (26425 sec)	Outbound:	No data

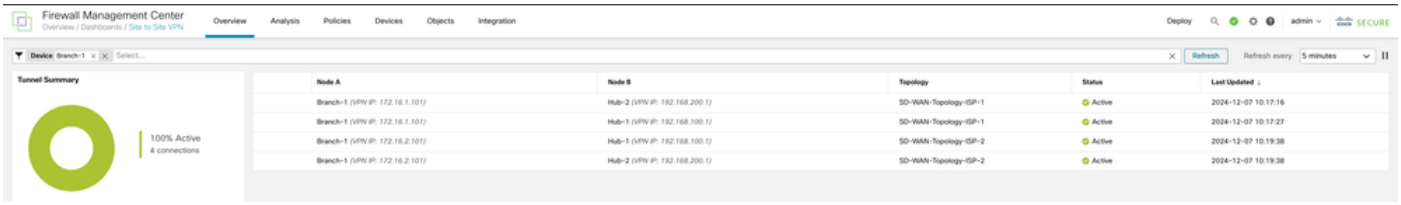
Branch-1 (VPN Interface IP: 172.16.2.101)

```
show crypto ipsec sa peer 192.168.100.1
```

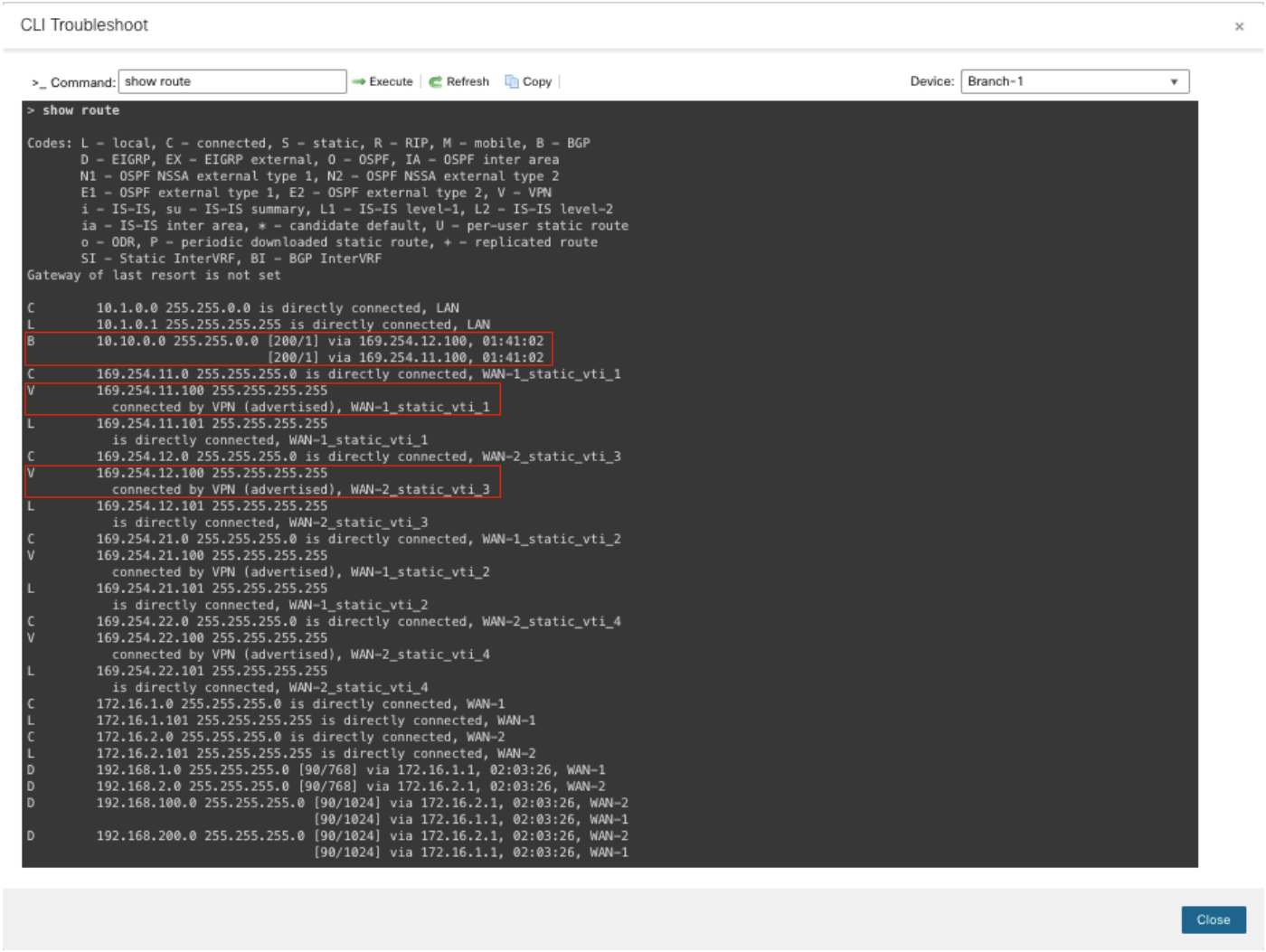
WAN-2_static_vti_3 - SVTI to Hub 1 via ISP 2
WAN-1_static_vti_2 - SVTI to Hub 2 via ISP 1
WAN-2_static_vti_4 - SVTI to Hub 2 via ISP 2

Verify Load Balancing of VPN Traffic

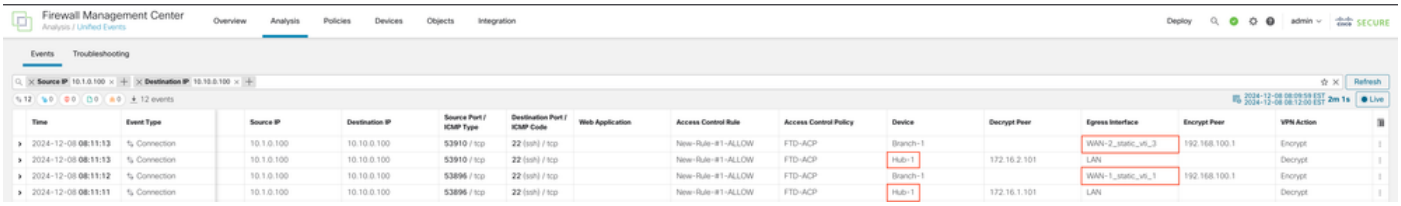
The tunnel status can be seen in the **Site to Site VPN** dashboard. Ideally, all tunnels must be active:



Routes to the primary hub are preferred. The **show route** command on Branch 1 indicates that the VPN traffic is load-balanced between the two SVTIs on ISP 1 and ISP 2 to the primary hub:

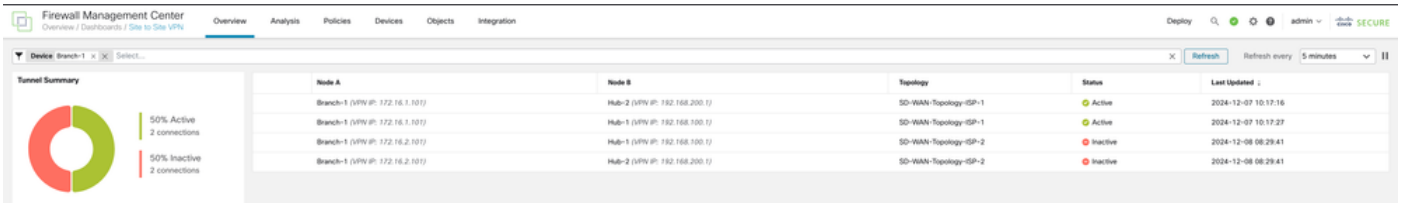


The **Egress Interface** taken for the actual VPN traffic can be seen in **Unified Events**:



Verify Dual ISP Redundancy

When ISP-2 is down, the tunnel status indicates that the tunnels via ISP-1 are active:



Routes to the primary hub are preferred. The **show route** command on Branch 1 indicates that the VPN traffic is routed via the SVTIs on ISP-1 to the primary hub:

CLI Troubleshoot

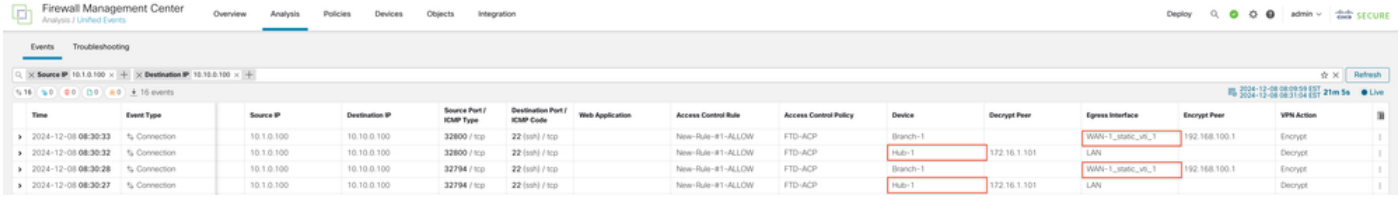
>_ Command: show route | Execute | Refresh | Copy | Device: Branch-1

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set

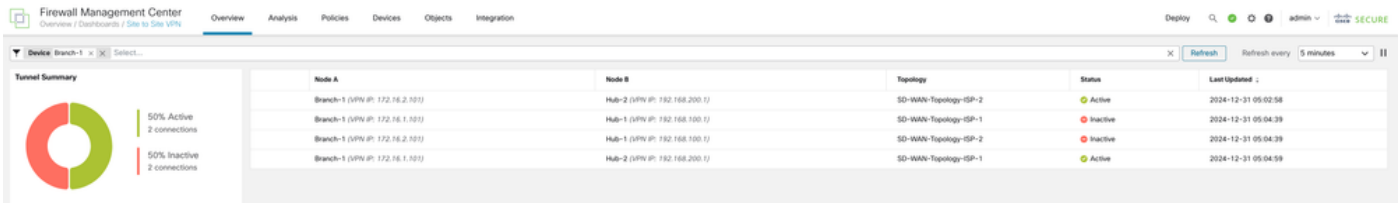
C        10.1.0.0 255.255.0.0 is directly connected, LAN
L        10.1.0.1 255.255.255.255 is directly connected, LAN
B        10.10.0.0 255.255.0.0 [200/1] via 169.254.11.100, 00:04:02
C        169.254.11.0 255.255.255.0 is directly connected, WAN-1_static_vti_1
V        169.254.11.100 255.255.255.255
           connected by VPN (advertised), WAN-1_static_vti_1
L        169.254.11.101 255.255.255.255
           is directly connected, WAN-1_static_vti_1
C        169.254.21.0 255.255.255.0 is directly connected, WAN-1_static_vti_2
V        169.254.21.100 255.255.255.255
           connected by VPN (advertised), WAN-1_static_vti_2
L        169.254.21.101 255.255.255.255
           is directly connected, WAN-1_static_vti_2
C        172.16.1.0 255.255.255.0 is directly connected, WAN-1
L        172.16.1.101 255.255.255.255 is directly connected, WAN-1
D        172.16.2.0 255.255.255.0 [90/1280] via 172.16.1.1, 00:04:03, WAN-1
D        192.168.1.0 255.255.255.0 [90/768] via 172.16.1.1, 22:12:57, WAN-1
D        192.168.2.0 255.255.255.0 [90/1024] via 172.16.1.1, 00:04:03, WAN-1
D        192.168.100.0 255.255.255.0 [90/1024] via 172.16.1.1, 00:04:03, WAN-1
D        192.168.200.0 255.255.255.0 [90/1024] via 172.16.1.1, 00:04:03, WAN-1
```

The **Egress Interface** taken for the actual VPN traffic can be seen in **Unified Events**:

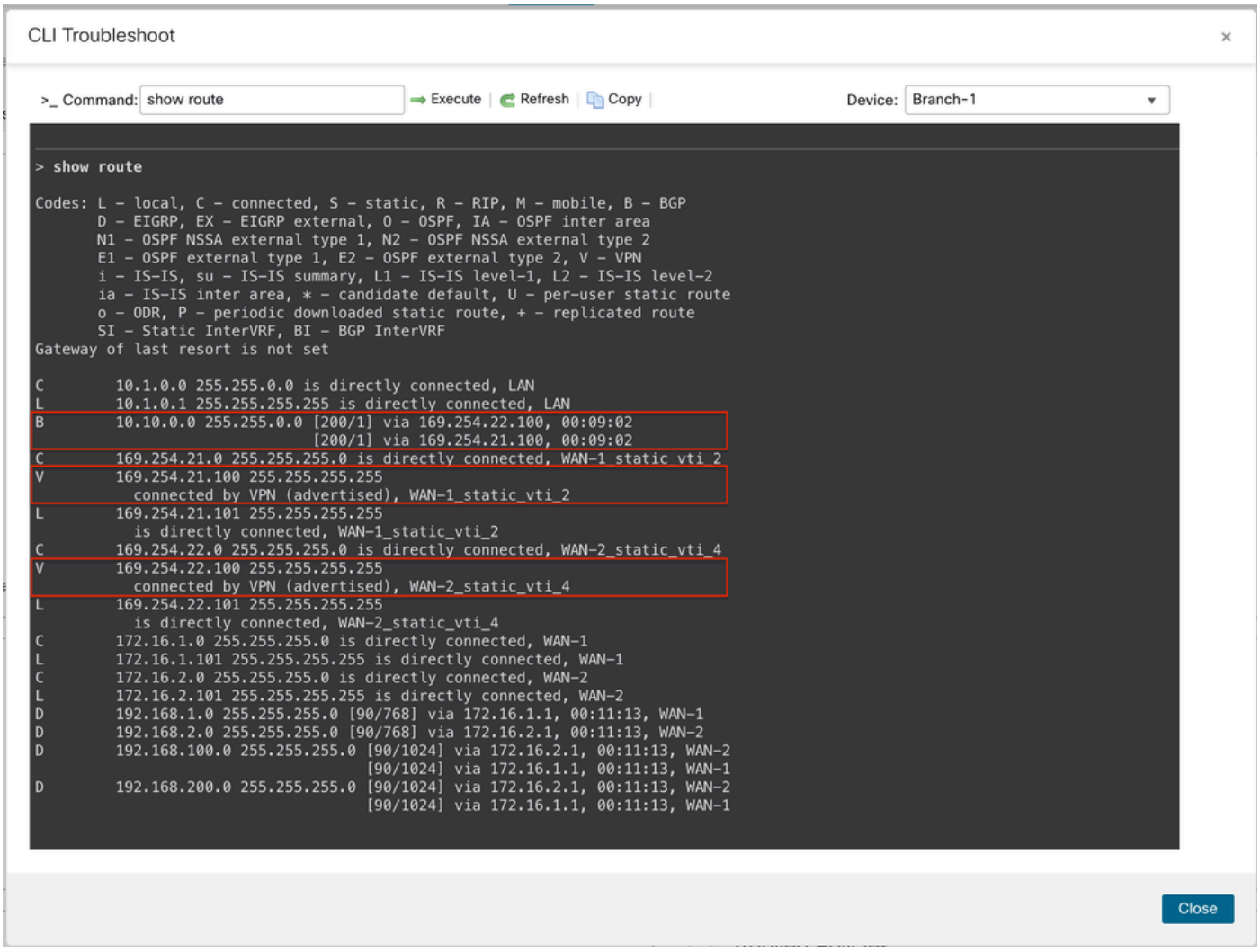


Verify Hub Level Redundancy

When the primary hub is down, the tunnel status indicates that the tunnels to the secondary hub are active:



Since the primary hub is down, the routes to the secondary hub are preferred. The **show route** command on Branch 1 indicates that the VPN traffic is load-balanced between the two SVTIs on ISP 1 and ISP 2 to the secondary hub:



The **Egress Interface** taken for the actual VPN traffic can be seen in **Unified Events**:

