Configureer de topologie van dubbele ISP met twee hubs en vier spraakpunten in dezelfde regio

Inhoud

Inleiding

Dit document beschrijft hoe u een dubbele ISP-topologie met twee hubs en vier spaken in hetzelfde gebied kunt configureren met behulp van de SD-WAN-wizard.

Voorwaarden

Ondersteunde software- en hardwareplatforms

bedrijfsleider	FTD	Ondersteunde platforms
• FMC >= 7.6.0 en FMC REST API	• Hub FTD >= 7.6.0 • Gesproken FTD >= 7.3.0	Alle platforms die FMC >= 7.6.0 kan beheren

• cdFMC >= 7,6,0 • FDM - niet-ondersteunde producten		

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Firewall-bescherming tegen bedreigingen
- Cisco Secure Firewall Management Center
- Softwaregedefinieerde WAN (SD-WAN)

Gebruikte componenten

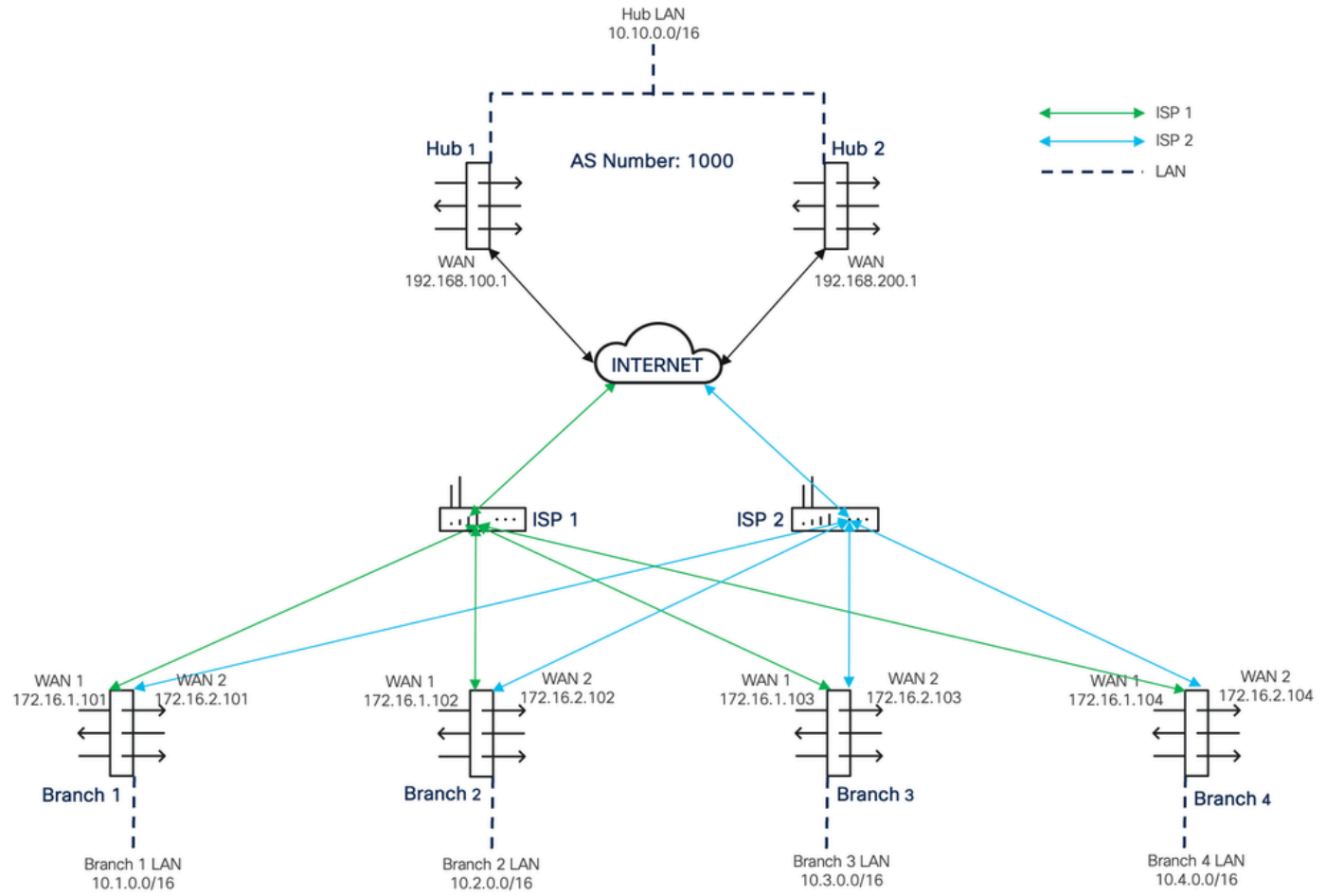
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

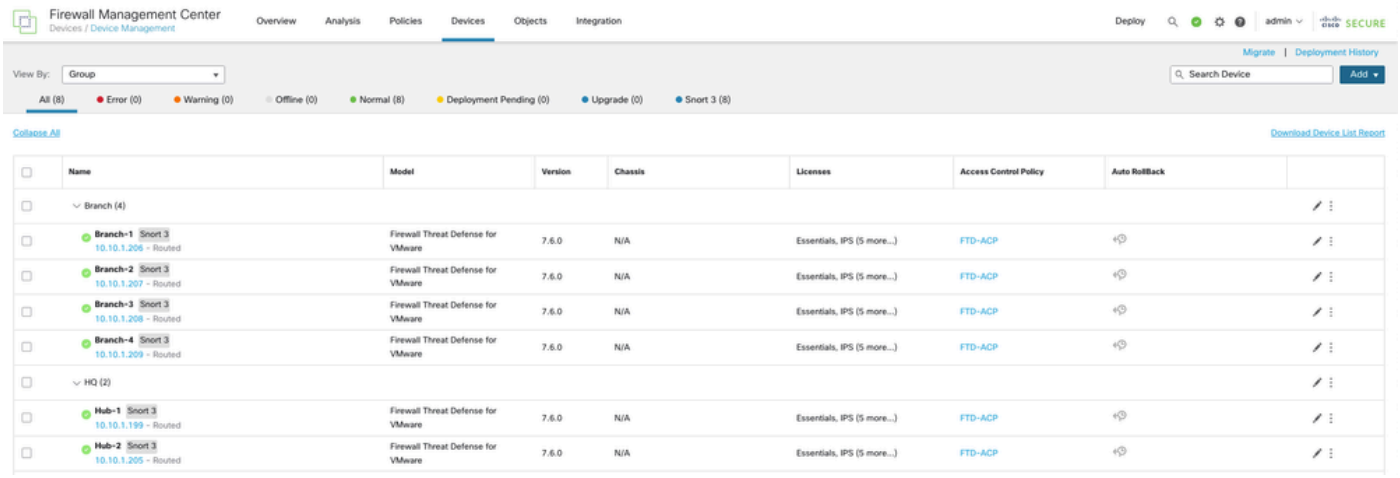
- FTD versie 7.6.0
- FMC versie 7.6.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

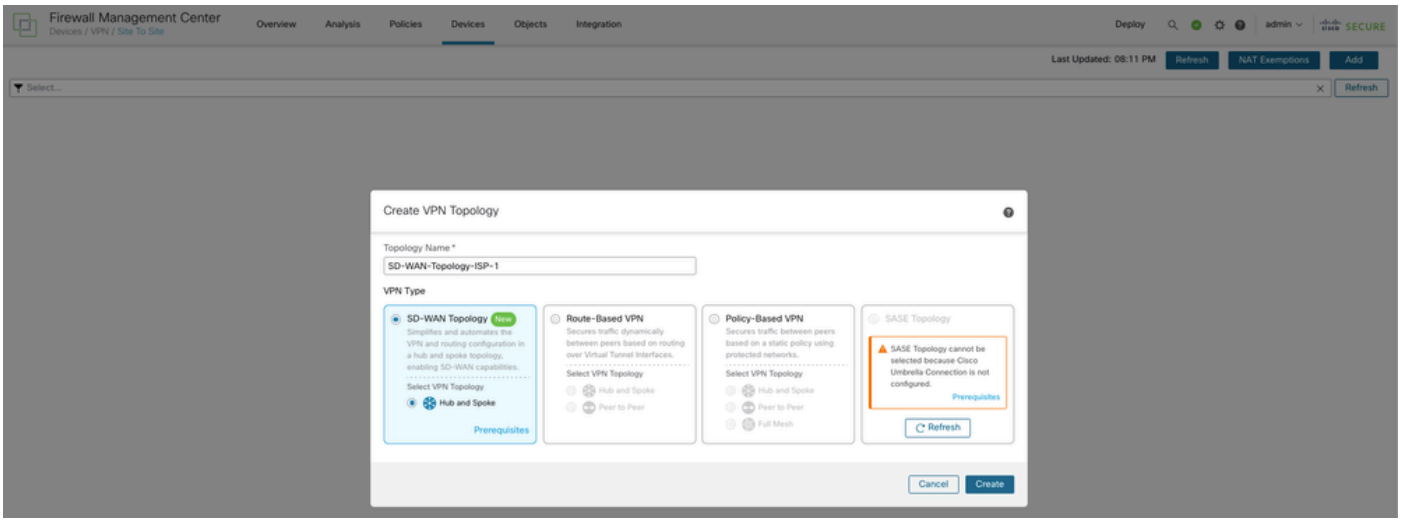
Netwerkdiagram





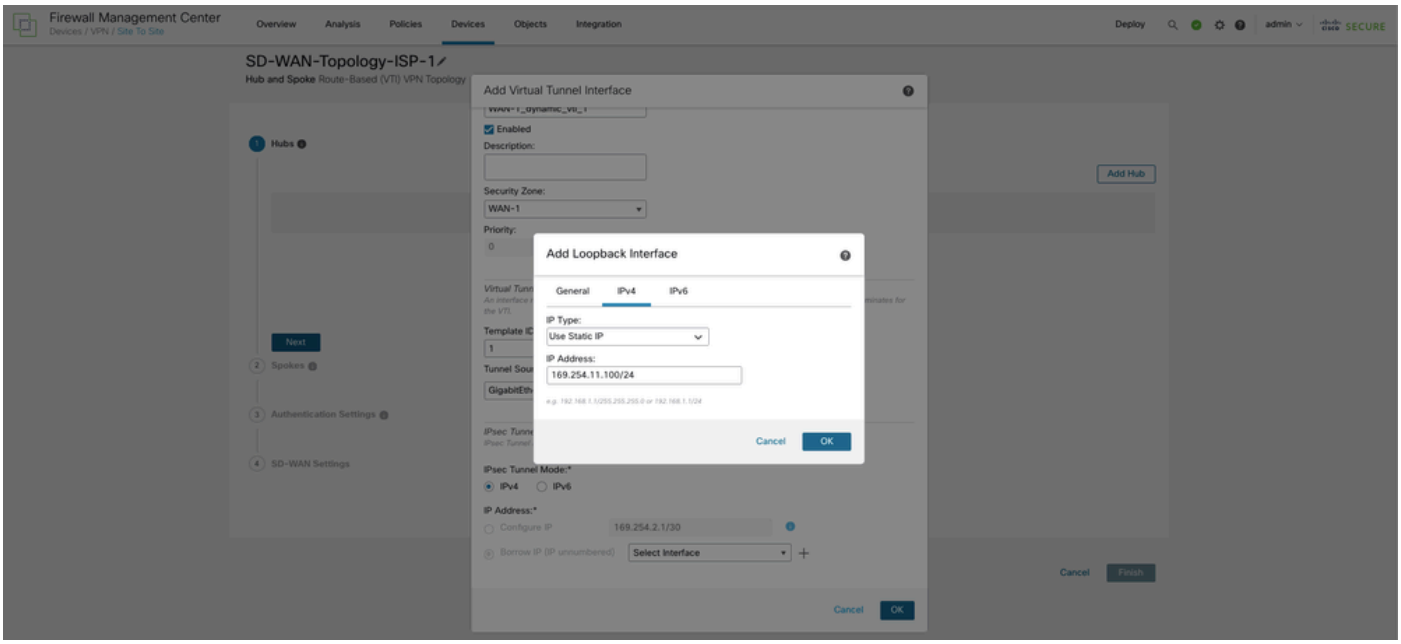
Stap 1. Maak een SD-WAN topologie met WAN-1 als VPN-interface

Ga naar Apparaten > VPN > Site to Site. Selecteer Add, en ga een geschikte naam op het gebied van de Naam van de Topologie voor de eerste topologie met WAN-1 als interface van VPN in. Kies SD-WAN Topologie en selecteer Maken.

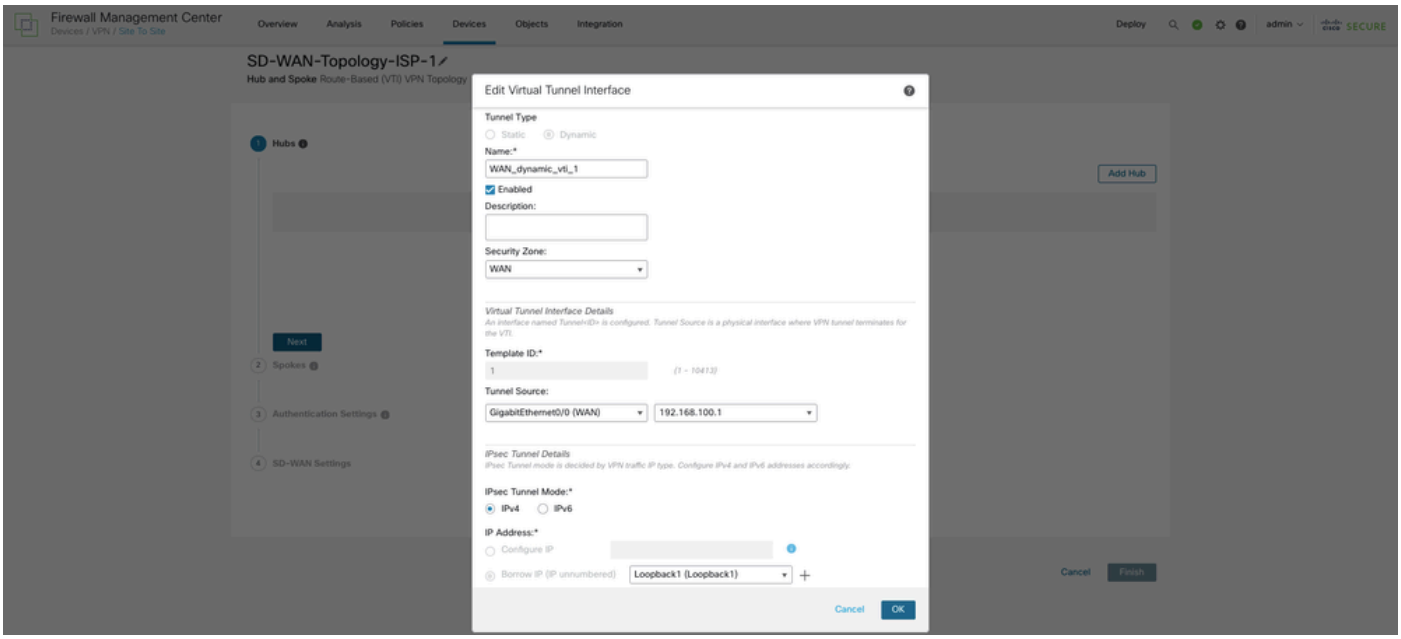


Stap 2. Configureer de Dynamic Virtual Tunnel Interface (DVTI) op de primaire hub

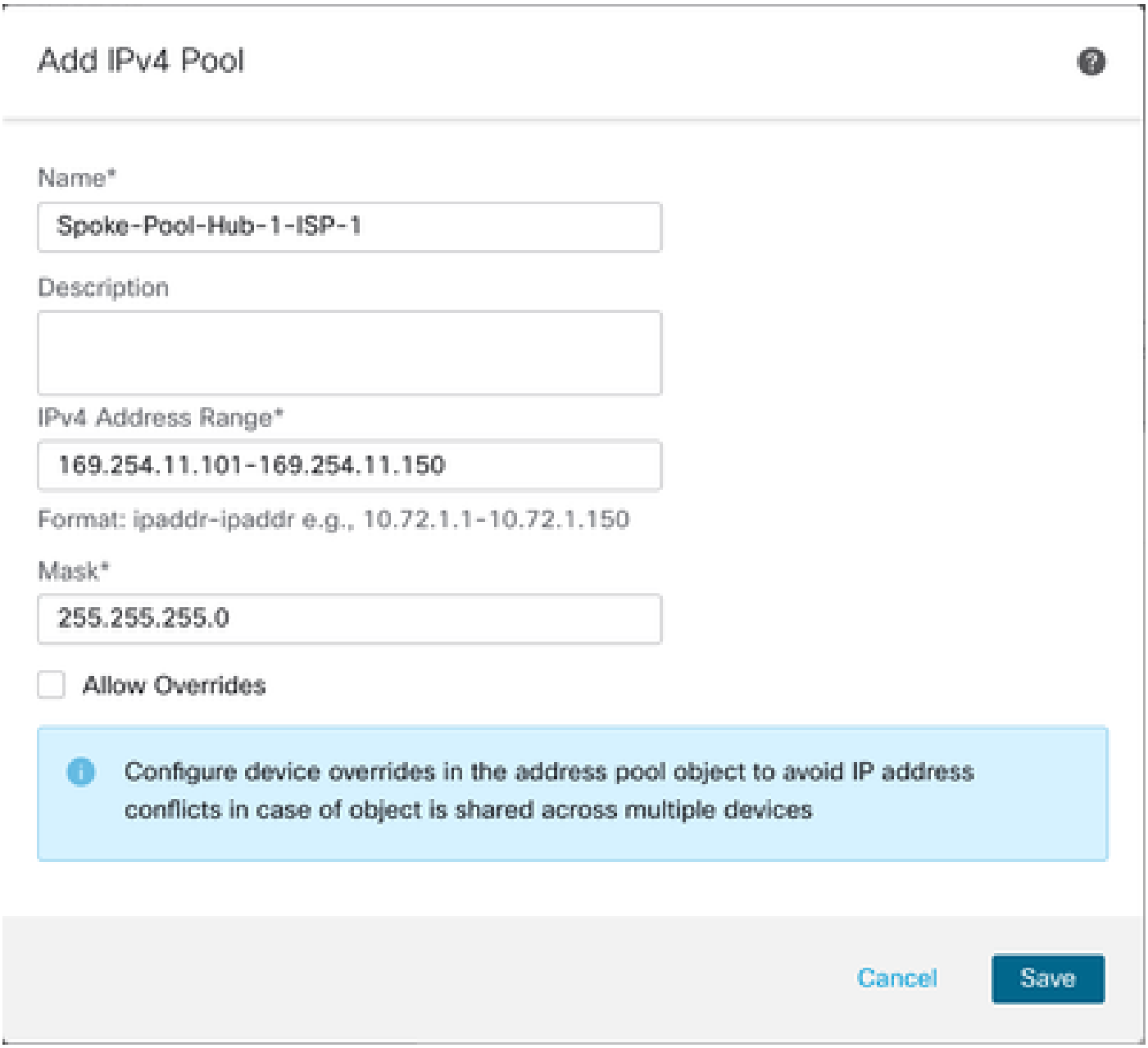
Selecteer Hub toevoegen en kies de primaire hub uit de vervolgkeuzelijst Apparaat. Selecteer het +-pictogram naast Dynamic Virtual Tunnel Interface (DVTI). Configureer een naam, beveiligingszone en sjabloon-ID en wijs WAN-1 toe als de Tunnel Source interface voor de DVTI.



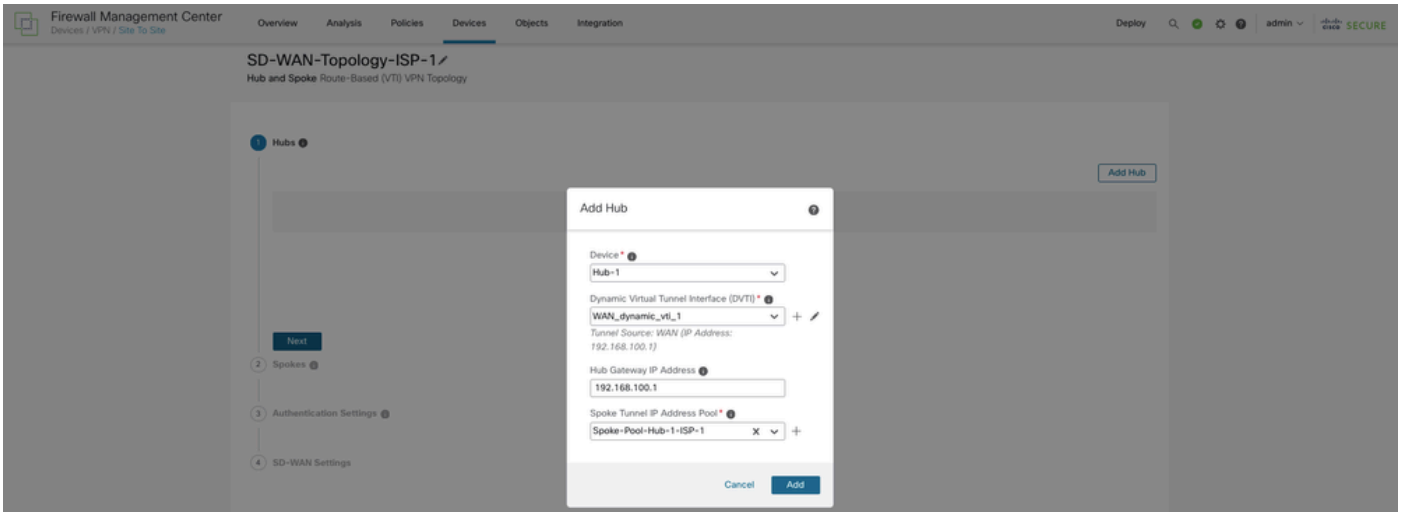
Kies een fysieke of loopback-interface uit de vervolgkeuzelijst Borrow IP. In de huidige topologie, erft DVTI een loopback interface IP adres. Selecteer OK.



Kies een adrespool of selecteer het + pictogram naast Spoke Tunnel IP Address Pool om een nieuwe adrespool te maken. Wanneer u spaken toevoegt, genereert de wizard automatisch spraaktunnelinterfaces en wijst IP-adressen toe aan deze spraakinterfaces vanuit deze IP-adrespool.

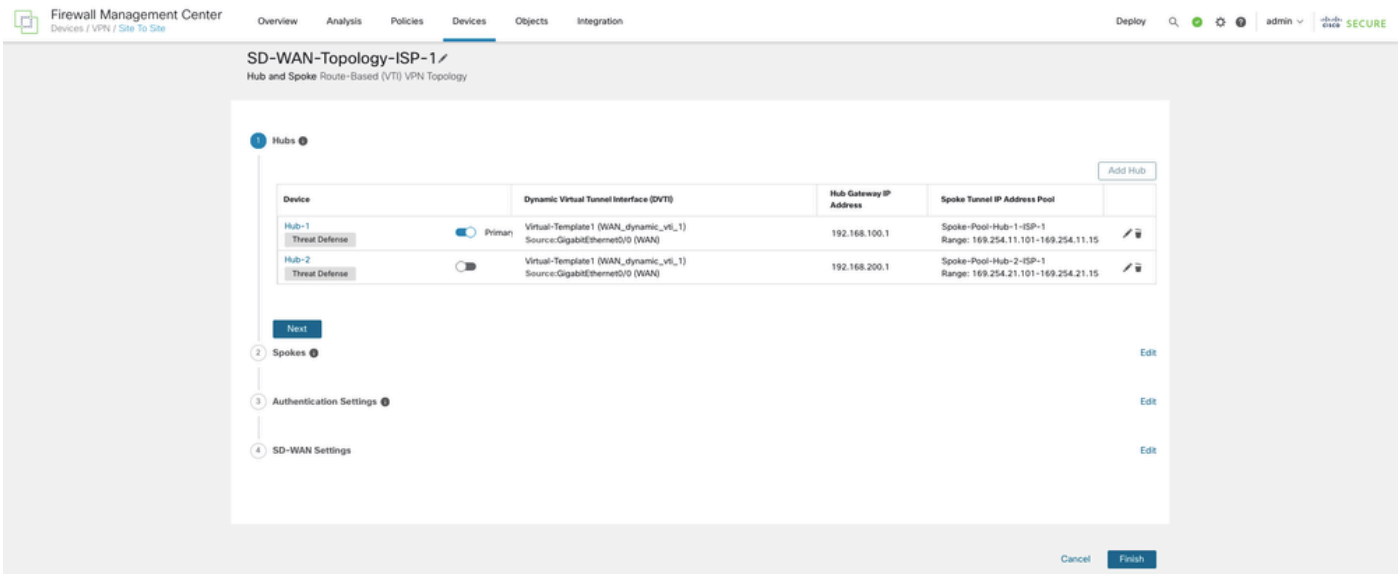


Zodra de primaire hubconfiguratie is voltooid, selecteert u Toevoegen om de primaire hub in de topologie op te slaan.



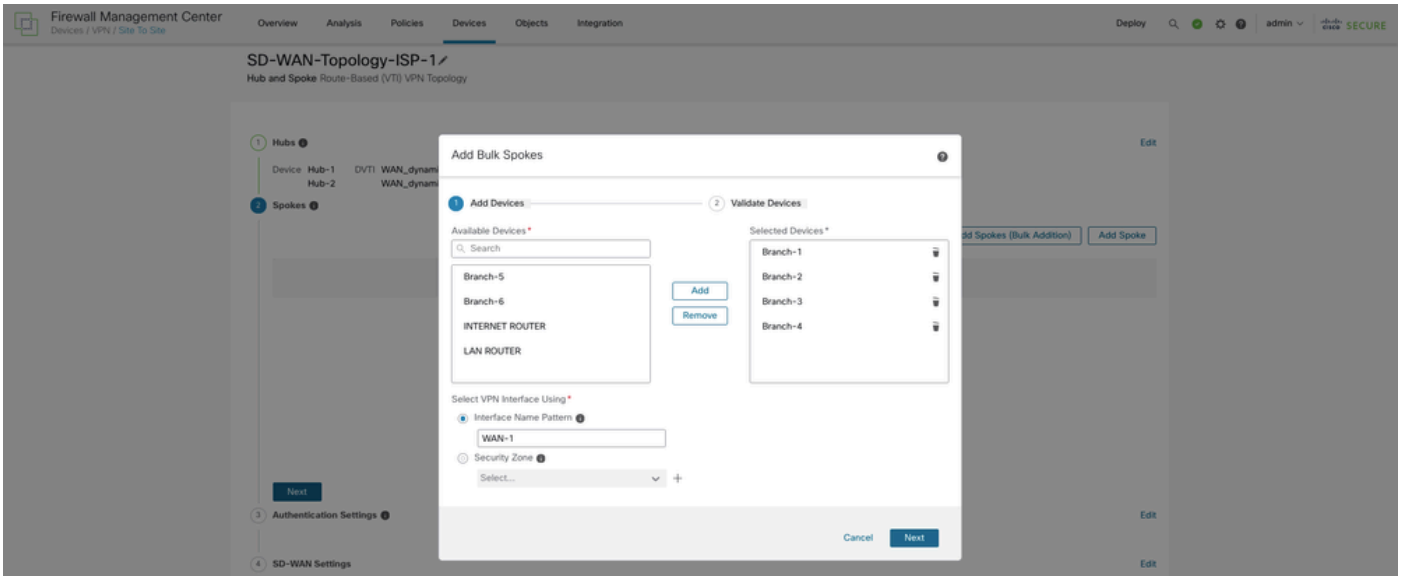
Stap 3. Configureer de Dynamic Virtual Tunnel Interface (DVTI) op de secundaire hub

Selecteer nu Add Hub opnieuw om de secundaire hub in de topologie met WAN-1 als VPN-interface te configureren door stap 1 en 2 te herhalen. Selecteer Volgende.

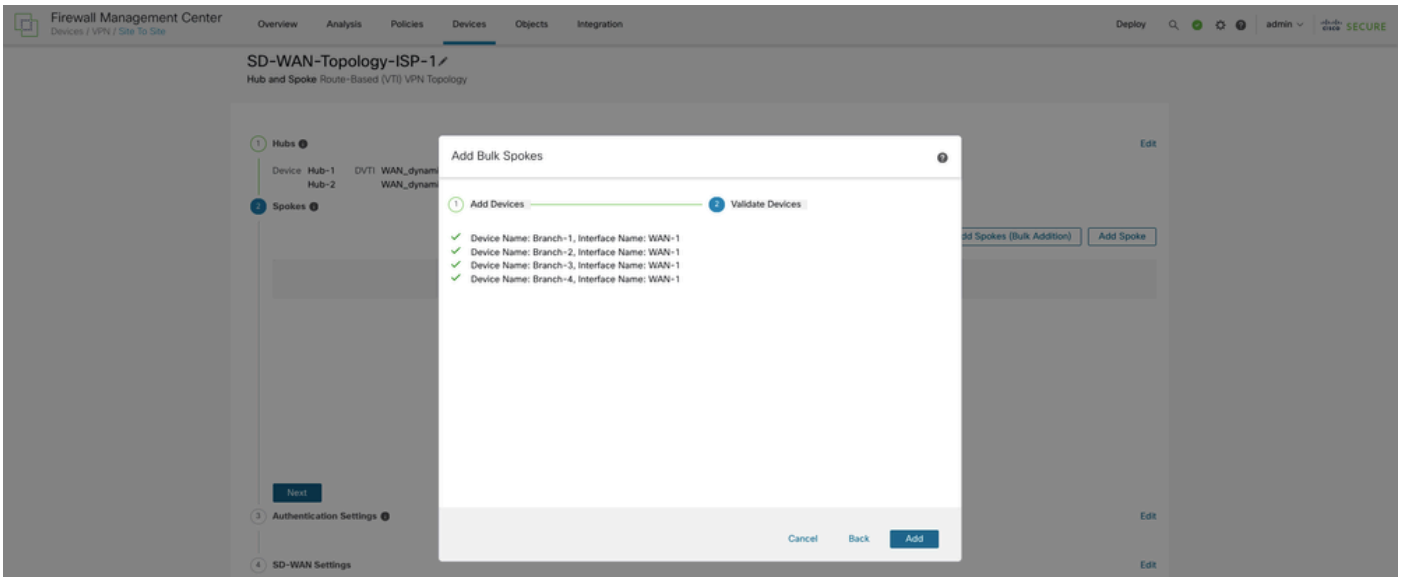


Stap 4. Configureer de Spokes

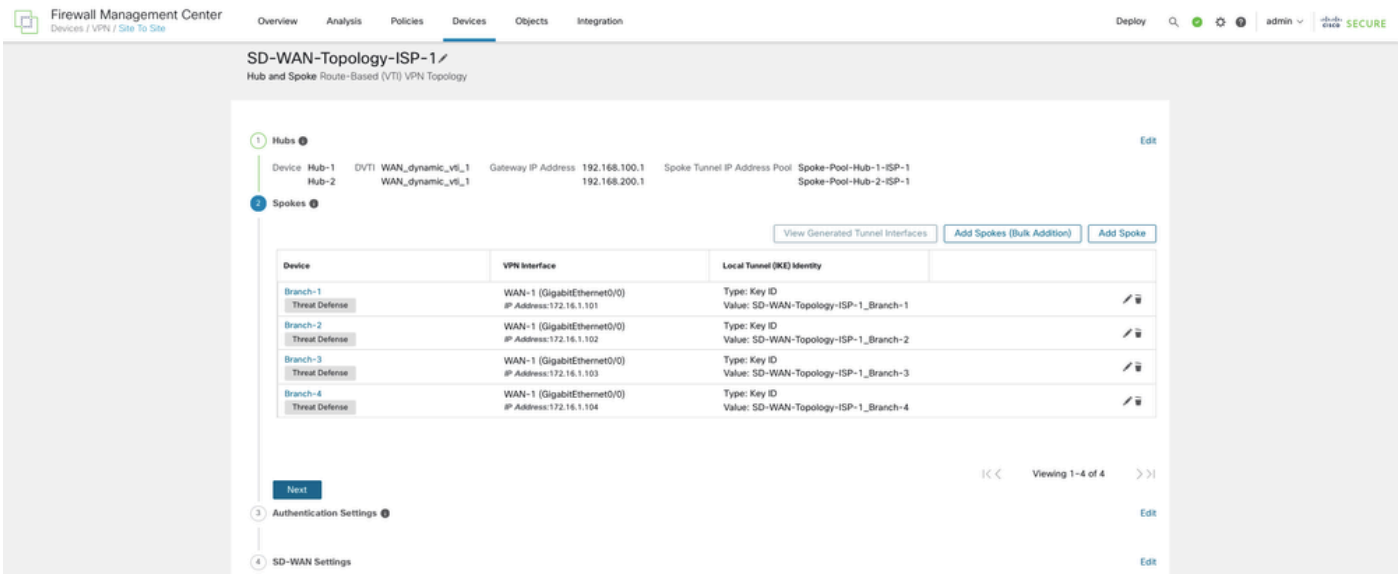
Selecteer Add Spoke om een enkel spaak apparaat toe te voegen, of klik op Add Spokes (Bulk Addition) om meerdere spaken toe te voegen aan uw topologie. De huidige topologie gebruikt de laatstgenoemde optie om meerdere tak FTDs aan de topologie toe te voegen. Selecteer in het dialoogvenster Bulkspaken toevoegen de gewenste FTD's die u als spaken wilt toevoegen. Selecteer of een gemeenschappelijk Patroon van de interfacenaam dat de logische naam van WAN-1 op alle spaken of de Veiligheidszone aanpast die met WAN-1 wordt geassocieerd.



Selecteer Volgende zodat de wizard valideert of de spaken interfaces hebben met het opgegeven patroon of de beveiligingszone.

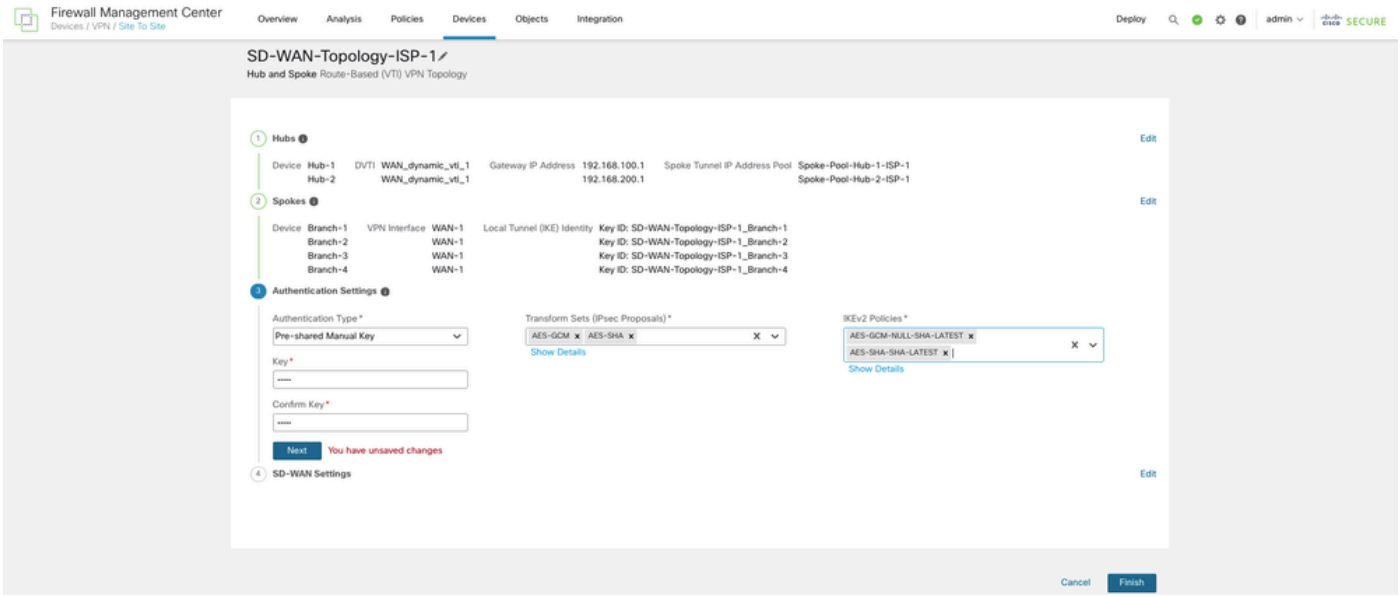


Selecteer Add en de wizard selecteert automatisch de hub DVTI als het IP-adres van de tunnelbron voor elke spaak.



Stap 5. De verificatie-instellingen configureren

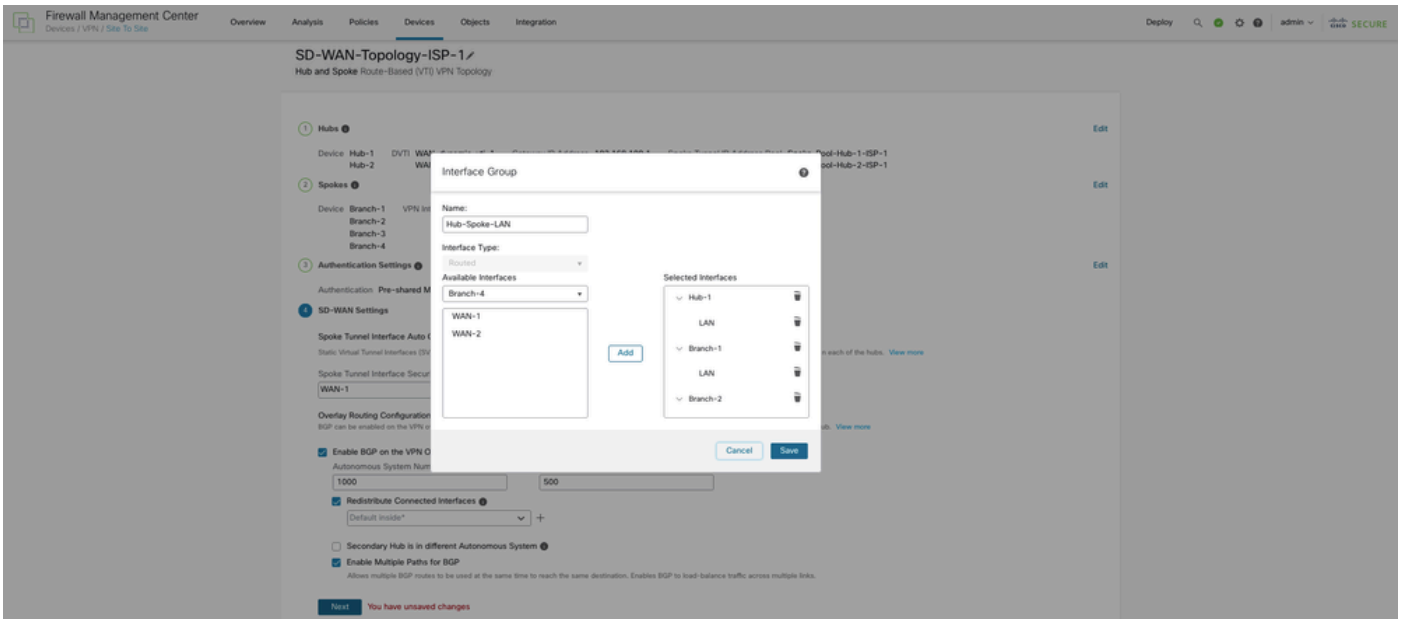
Selecteer Volgende om de verificatie-instellingen te configureren. Voor apparaatverificatie kunt u een handmatige vooraf gedeelde sleutel, een automatisch gegenereerde vooraf gedeelde sleutel of een certificaat in de vervolgkeuzelijst Verificatietype selecteren. Kies een of meer algoritmen uit de vervolgkeuzelijsten Transformatiesets en IKEv2-beleid.



Stap 6. Configureer de SD-WAN instellingen

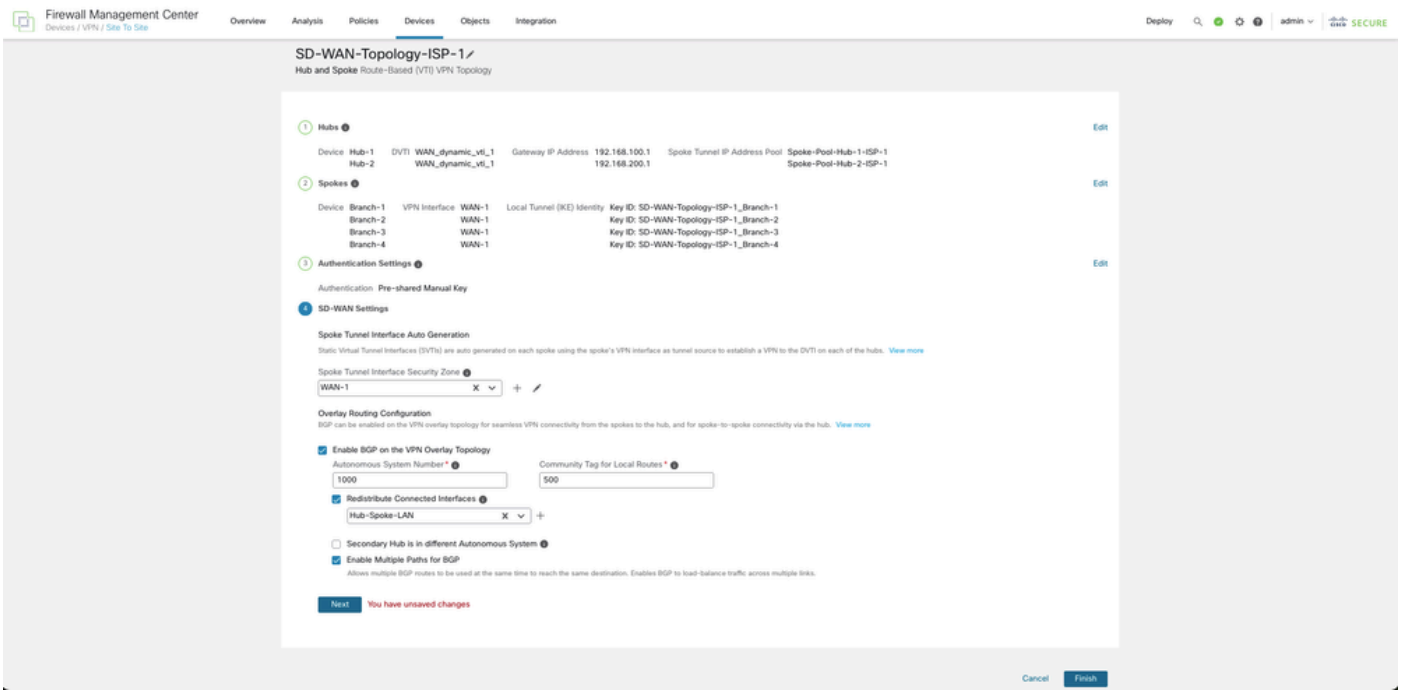
Selecteer Volgende om de SD-WAN instellingen te configureren. Deze stap omvat de auto-generatie van spraaktunnelinterfaces en de BGP-configuratie van het overlay-netwerk. Kies in de vervolgkeuzelijst Spoke Tunnel Interface Security Zone een beveiligingszone of selecteer + om een beveiligingszone te maken waarin de wizard automatisch de automatisch gegenereerde Statische virtuele tunnelinterfaces (SVTI's) van de spaken toevoegt.

Schakel het aanvinkvakje BGP inschakelen in op het aanvinkvakje VPN Overlay Topology om BGP-configuraties tussen de interface van de overlay-tunnel te automatiseren. Voer in het veld Autonomous System Number een Autonomous System (AS) in. Controleer het aanvinkvakje Redistribute Connected Interfaces en kies een interfacegroep uit de vervolgkeuzelijst of selecteer + om een interfacegroep met aangesloten LAN-interfaces van de hubs en spaken voor BGP-routeherverdeling in de overlay-topologie te maken.

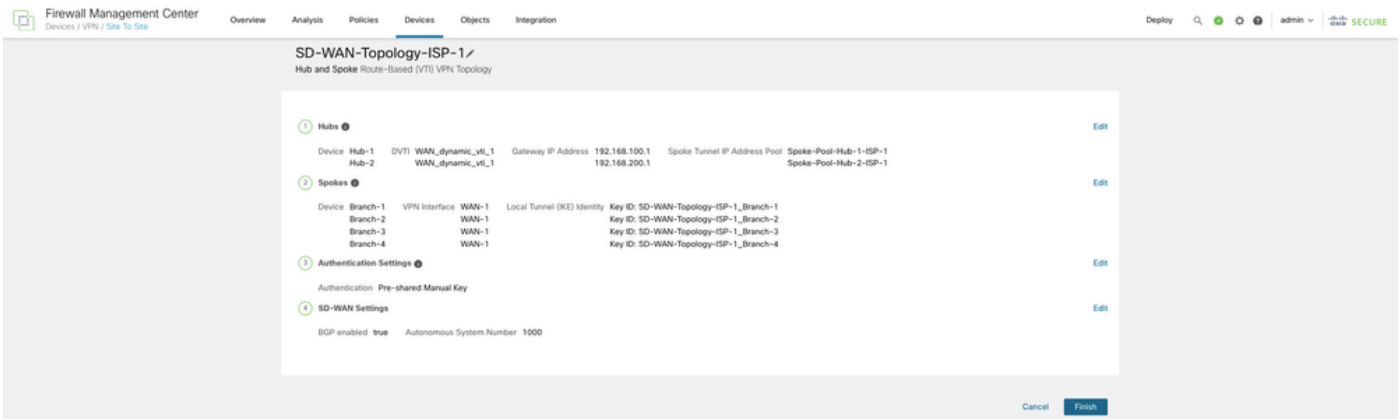


Voer in het veld Community Tag for Local Routes het BGP-communitykenmerk in om verbonden

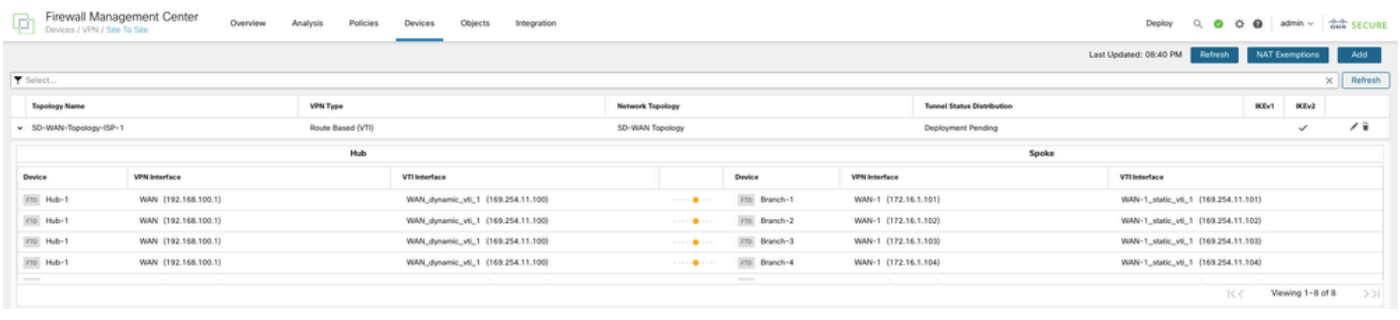
en herverdeelde lokale routes te taggen. Deze eigenschap laat gemakkelijke route het filtreren toe. Controleer of de secundaire hub in het aanvinkvakje Verschillende Autonomous System staat als u een secundaire hub in een andere AS hebt. Tenslotte schakelt u het aanvinkvakje Meervoudige paden inschakelen voor BGP in om BGP in staat te stellen het taakbalansverkeer over meerdere koppelingen te spreiden.



Klik op Voltooien om de SD-WAN topologie op te slaan en te valideren.

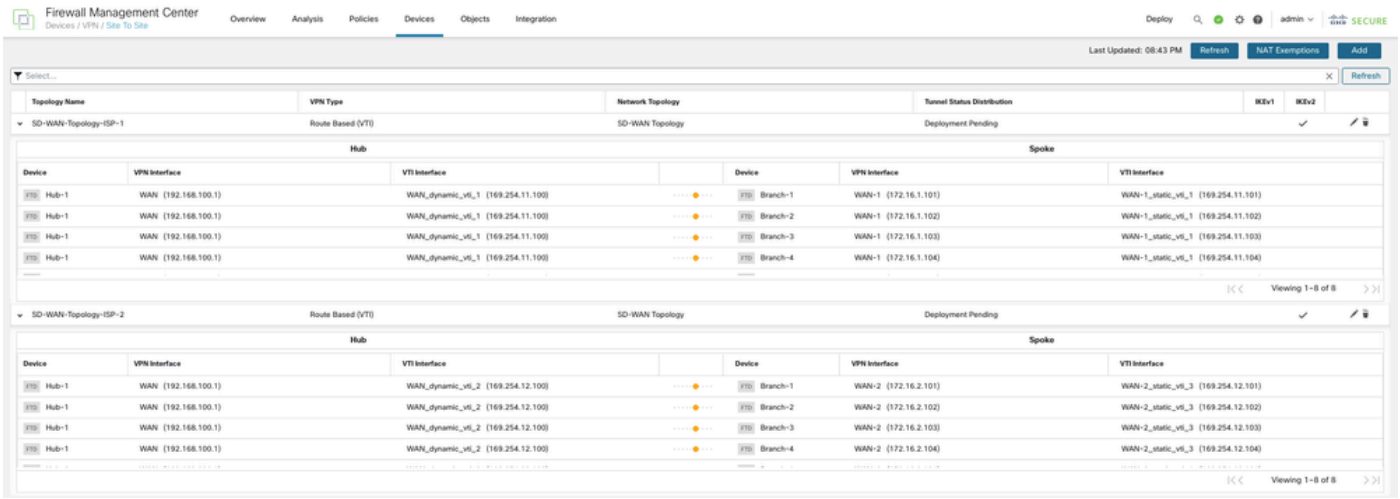


U kunt de topologie bekijken onder Apparaten > Site-to-site VPN. Het totale aantal tunnels in de eerste SD-WAN topologie is 8.



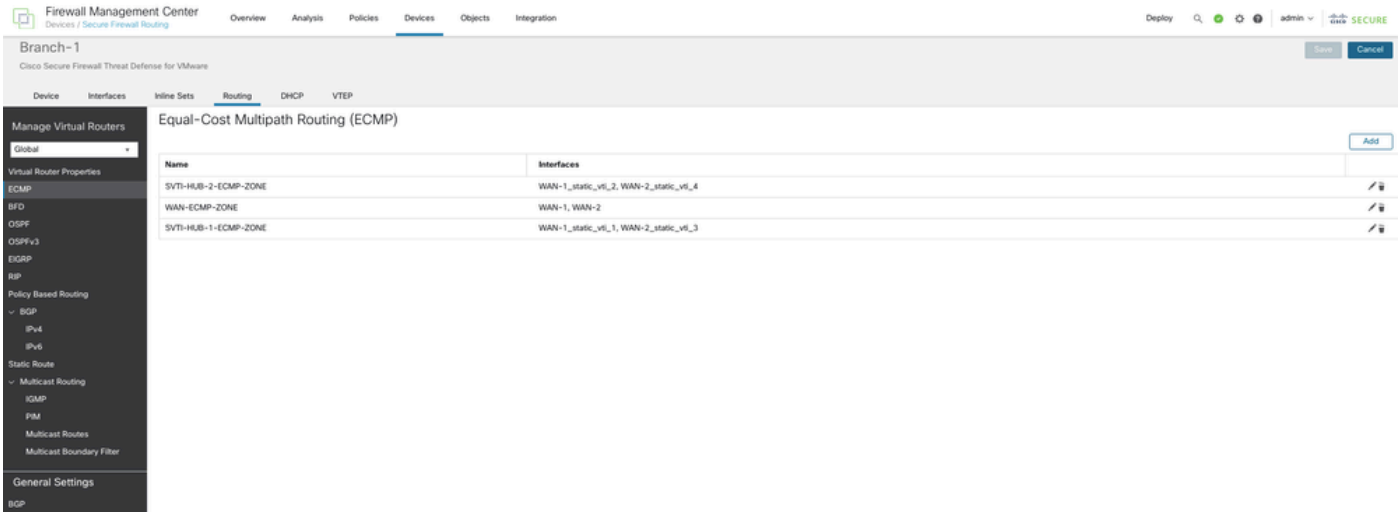
Stap 7. Maak een SD-WAN topologie met WAN-2 als VPN-interface

Herhaal stap 1 tot en met 6 om een SD-WAN topologie met WAN-2 als VPN-interface te configureren. Het totale aantal tunnels in de tweede SD-WAN topologie is 8. De definitieve topologieën moeten op het hieronder getoonde beeld kijken.



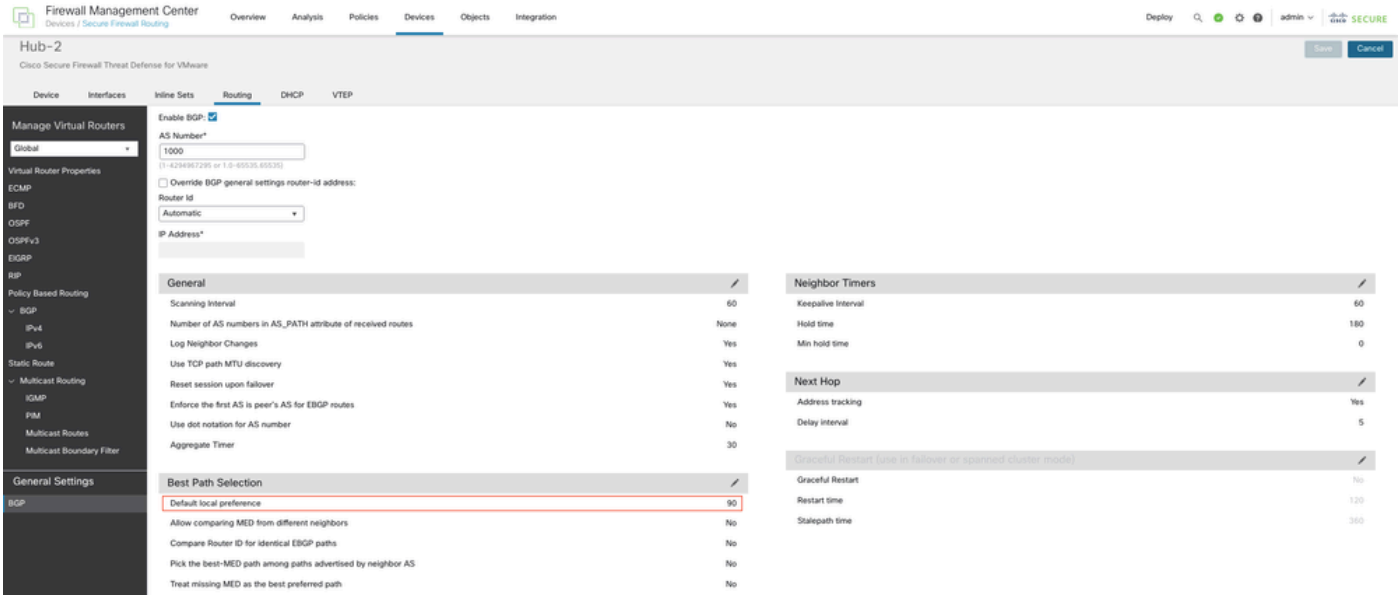
Stap 8. ECMP-zones instellen

Navigeer in elke vestiging naar Routing > ECMP en configureer de ECMP-zones (Equal-Cost Multi-Path) voor de WAN-interfaces en SVTI's die verbinding maken met zowel de primaire als de secundaire hub, zoals hieronder wordt getoond. Dit kan linkredundantie bieden en taakverdeling van het VPN-verkeer inschakelen.



Stap 9. Wijzig de BGP lokale voorkeur op de hub

Navigeer naar Routing > Algemene instellingen > BGP op de secundaire hub. Selecteer BGP inschakelen, het AS-nummer configureren en de standaard lokale voorkeurswaarde onder Best Path Selection instellen op een lagere waarde dan die welke op de primaire hub is geconfigureerd. Selecteer Opslaan. Dit zorgt ervoor dat routes naar de primaire hub de voorkeur krijgen boven routes naar de secundaire hub. Wanneer de primaire hub naar beneden gaat, nemen de routes naar de secundaire hub over.

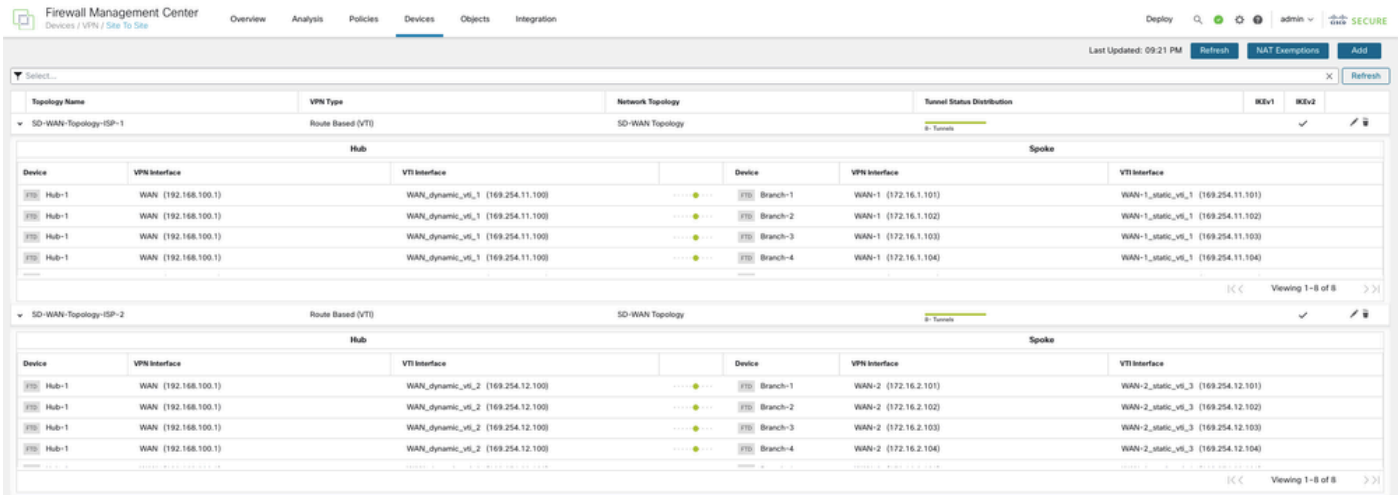


Stel de configuraties aan alle apparaten op.

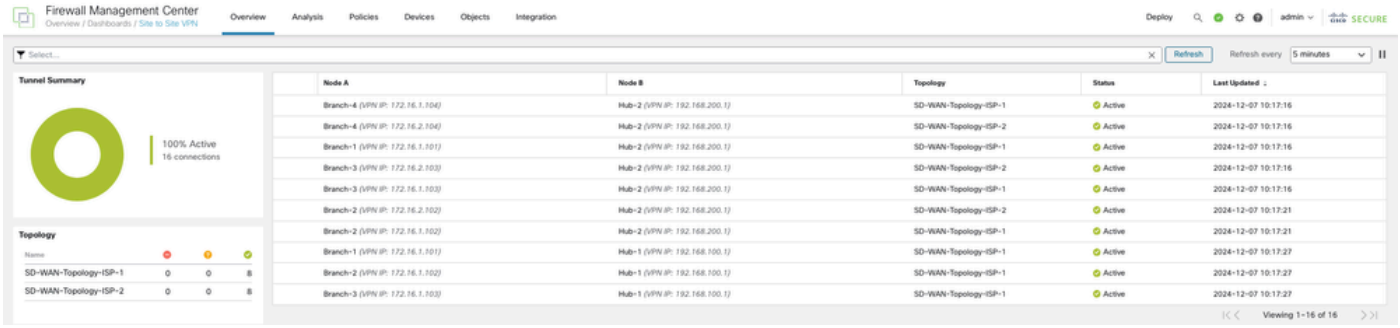
Verifiëren

Controleer de tunnelstatus

Om te verifiëren of de VPN-tunnels van de SD-WAN topologieën zijn geopend, selecteert u Apparaat > VPN > Site-to-Site.

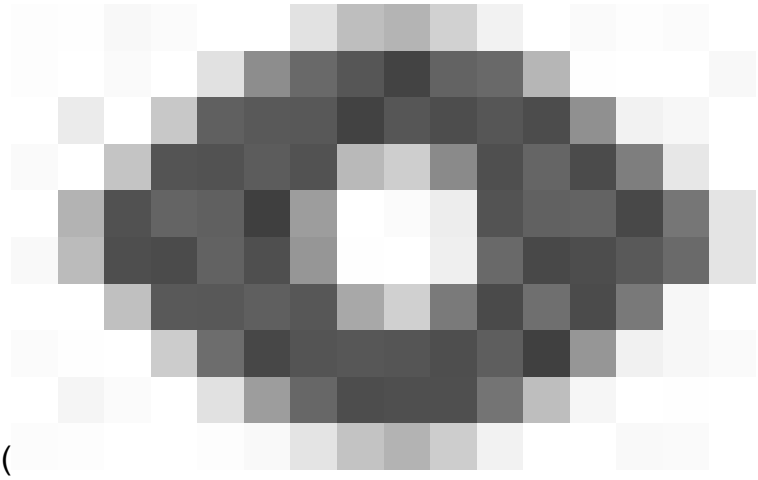


Om de details van de SD-WAN VPN-tunnels te bekijken, kiest u Overzicht > Dashboards > Site-to-site VPN.



U kunt als volgt meer details over elke VPN-tunnel weergeven:

1. Hang over een tunnel.



2. Selecteer Volledige informatie bekijken ( ) pictogram. Er verschijnt een venster met tunneldetails en meer acties.

3. Selecteer het tabblad CLI-details in het zijdeelvenster om de opdrachten voor de show en de details van de beveiligingskoppelingen voor IPsec te bekijken.

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

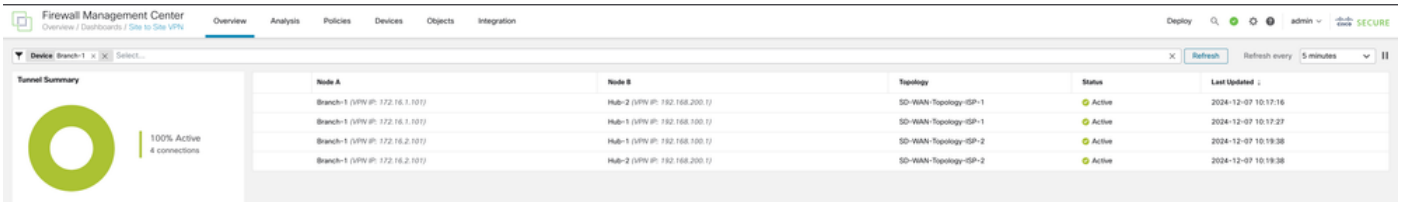
Branch-1 (VPN Interface IP: 172.16.2.101)

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

WAN-2_statistical_vti_3 - SVTI naar Hub 1 via ISP 2
WAN-1_statische_vti_2 - SVTI naar Hub 2 via ISP 1
WAN-2_statische_vti_4 - SVTI naar Hub 2 via ISP 2

Controleer taakverdeling bij VPN-verkeer

De tunnelstatus is te zien in het dashboard Site to Site VPN. Idealiter moeten alle tunnels actief zijn:



Routes naar de primaire hub hebben de voorkeur. De opdracht route voor show op Tak 1 geeft aan dat het VPN-verkeer is gebalanceerd tussen de twee SVTI's op ISP 1 en ISP 2 naar de primaire hub:

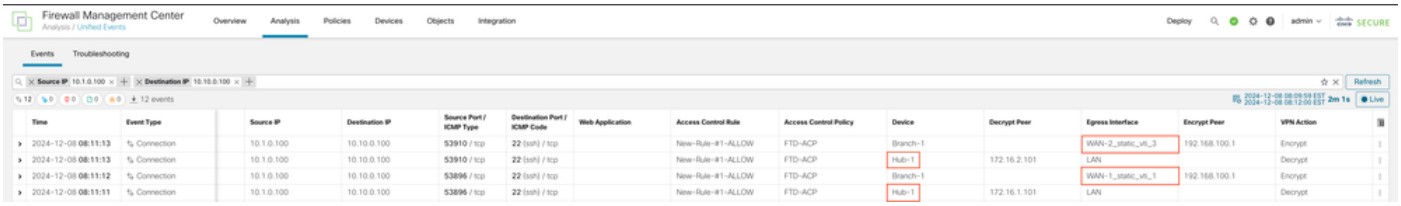
CLI Troubleshoot

>_ 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 169.254.12.100, 01:41:02
                               [200/1] via 169.254.11.100, 01:41:02
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        169.254.12.0 255.255.255.0 is directly connected, WAN-2_static_vti_3
V        169.254.12.100 255.255.255.255
           connected by VPN (advertised), WAN-2_static_vti_3
L        169.254.12.101 255.255.255.255
           is directly connected, WAN-2_static_vti_3
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        169.254.22.0 255.255.255.0 is directly connected, WAN-2_static_vti_4
V        169.254.22.100 255.255.255.255
           connected by VPN (advertised), WAN-2_static_vti_4
L        169.254.22.101 255.255.255.255
           is directly connected, WAN-2_static_vti_4
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
C        172.16.2.0 255.255.255.0 is directly connected, WAN-2
L        172.16.2.101 255.255.255.255 is directly connected, WAN-2
D        192.168.1.0 255.255.255.0 [90/768] via 172.16.1.1, 02:03:26, WAN-1
D        192.168.2.0 255.255.255.0 [90/768] via 172.16.2.1, 02:03:26, WAN-2
D        192.168.100.0 255.255.255.0 [90/1024] via 172.16.2.1, 02:03:26, WAN-2
                                     [90/1024] via 172.16.1.1, 02:03:26, WAN-1
D        192.168.200.0 255.255.255.0 [90/1024] via 172.16.2.1, 02:03:26, WAN-2
                                     [90/1024] via 172.16.1.1, 02:03:26, WAN-1
```

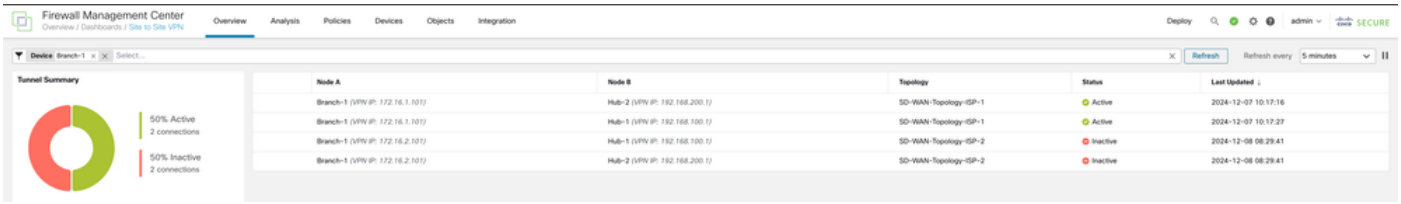
Close

De uitgaande interface die voor het huidige VPN-verkeer wordt gebruikt, kan in Unified Events worden weergegeven:



Controleer redundantie van dubbele ISP

Wanneer ISP-2 beneden is, wijst de tunnelstatus erop dat de tunnels via ISP-1 actief zijn:



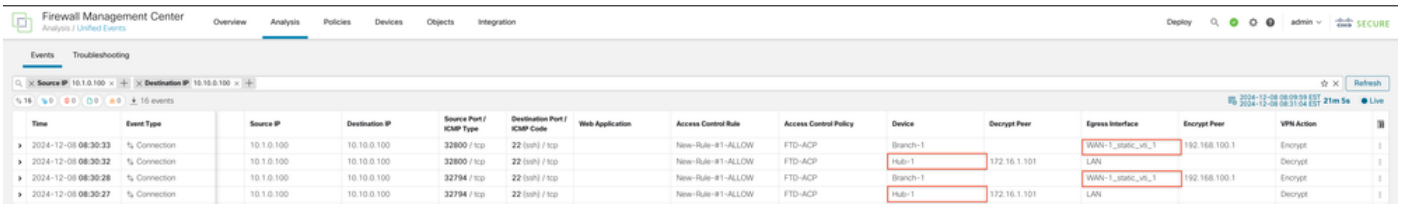
Routes naar de primaire hub hebben de voorkeur. De opdracht route in show op Branch 1 geeft aan dat het VPN-verkeer via de SVTI's op ISP-1 naar de primaire hub wordt geleid:

CLI Troubleshoot

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

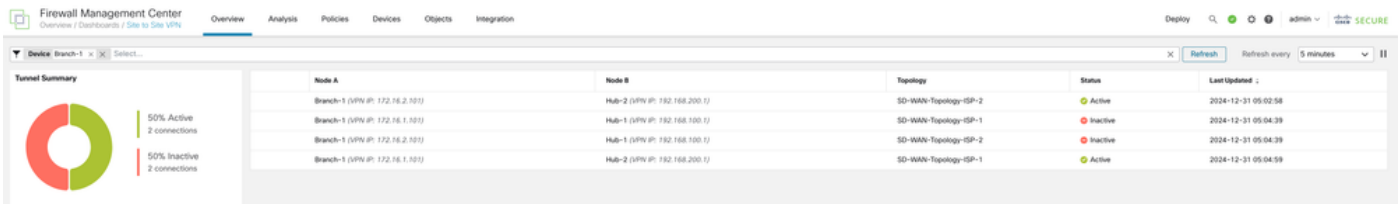
```
> show route

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
```

De uitgaande interface die voor het huidige VPN-verkeer wordt gebruikt, kan in Unified Events worden weergegeven:

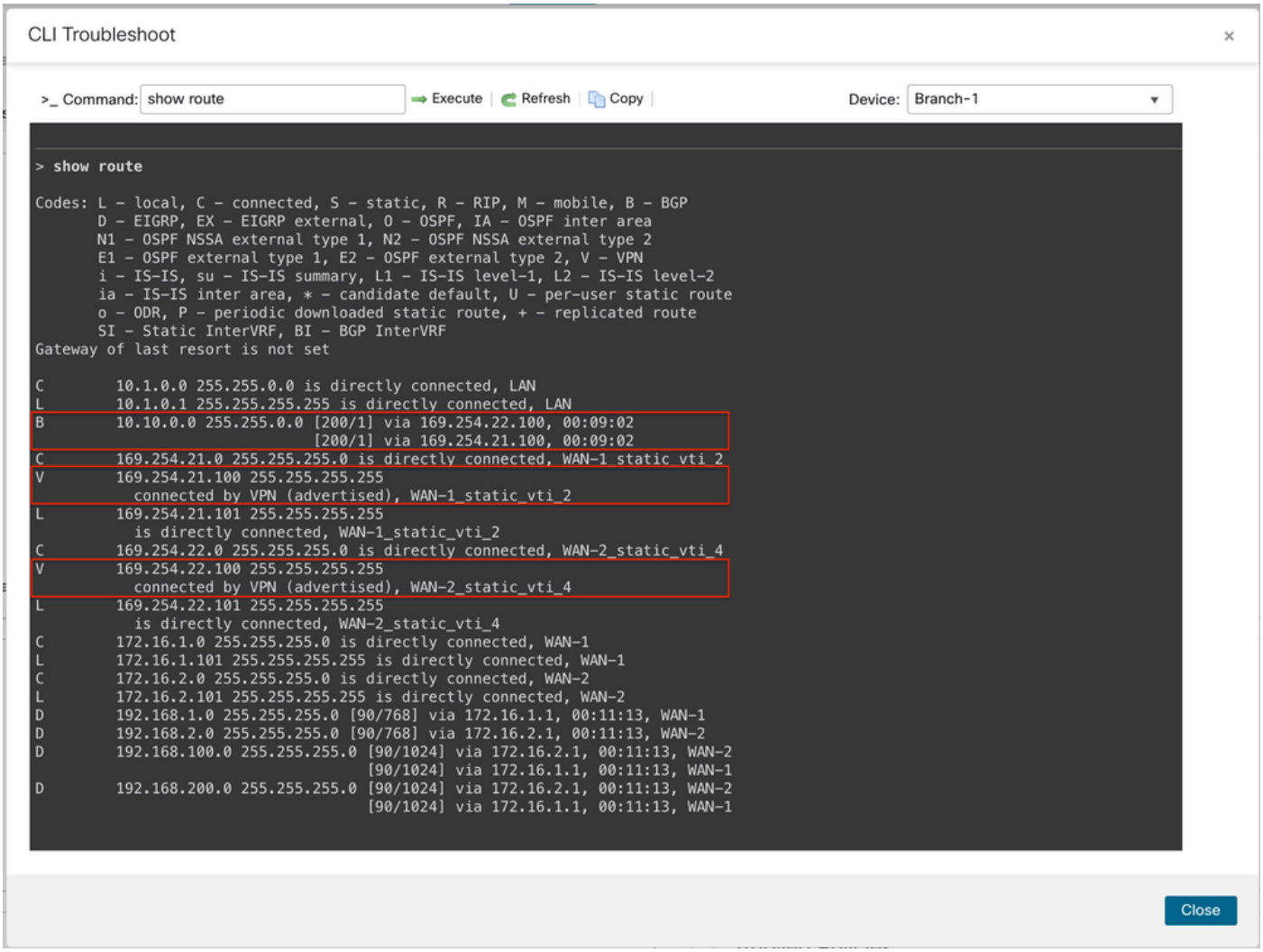


Controleer de redundantie van hubniveau

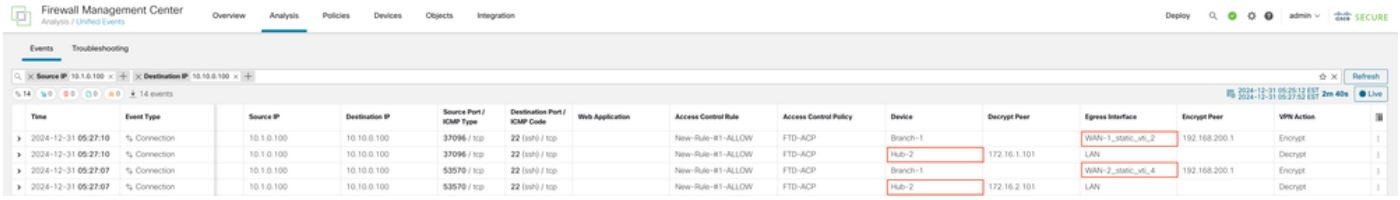
Wanneer de primaire hub is ingestort, geeft de tunnelstatus aan dat de tunnels naar de secundaire hub actief zijn:



Aangezien de primaire hub is ingestort, hebben de routes naar de secundaire hub de voorkeur. De opdracht route voor show op Tak 1 geeft aan dat het VPN-verkeer is gebalanceerd tussen de twee SVTI's op ISP 1 en ISP 2 naar de secundaire hub:



De uitgaande interface die voor het huidige VPN-verkeer wordt gebruikt, kan in Unified Events worden weergegeven:


Firewall Management Center
Analysis / Unified Events
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
SECURE
Events
Troubleshooting
Source IP 10.1.0.100
Destination IP 10.10.0.100
Refresh
14 events
2024-12-31 05:25:12 EST
2024-12-31 05:27:52 EST 2m 40s
Live
Time
Event Type
Source IP
Destination IP
Source Port / ICMP Type
Destination Port / ICMP Code
Web Application
Access Control Rule
Access Control Policy
Device
Decrypt Peer
Egress Interface
Encrypt Peer
VPN Action
2024-12-31 05:27:10 Connection 10.1.0.100 10.10.0.100 37096 / tcp 22 (ssh) / tcp New-Rule-#1-ALLOW FTD-ACP Branch-1 WAN-1_static_vti_2 192.168.200.1 Encrypt
2024-12-31 05:27:10 Connection 10.1.0.100 10.10.0.100 37096 / tcp 22 (ssh) / tcp New-Rule-#1-ALLOW FTD-ACP Hub-2 172.16.1.101 LAN Decrypt
2024-12-31 05:27:07 Connection 10.1.0.100 10.10.0.100 53570 / tcp 22 (ssh) / tcp New-Rule-#1-ALLOW FTD-ACP Branch-1 WAN-2_static_vti_4 192.168.200.1 Encrypt
2024-12-31 05:27:07 Connection 10.1.0.100 10.10.0.100 53570 / tcp 22 (ssh) / tcp New-Rule-#1-ALLOW FTD-ACP Hub-2 172.16.2.101 LAN Decrypt

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.