Configurazione della topologia a doppio ISP con due hub e quattro spoke nella stessa area

Sommario

Introduzione

Questo documento descrive come configurare una topologia con due ISP con due hub e quattro spoke nella stessa area usando la procedura guidata SD-WAN.

Prerequisiti

Piattaforme software e hardware supportate

Responsabile	FTD	Piattaforme supportate
• FMC >= 7.6.0 e API REST	• FTD hub >= 7.6.0	Tutte le piattaforme che FMC >= 7.6.0 può gestire

FMC • cdFMC >= 7.6.0 • FDM - Non supportato	• FTD raggio >= 7.3.0	

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Management Center
- Software-Defined WAN (SD-WAN)

Componenti usati

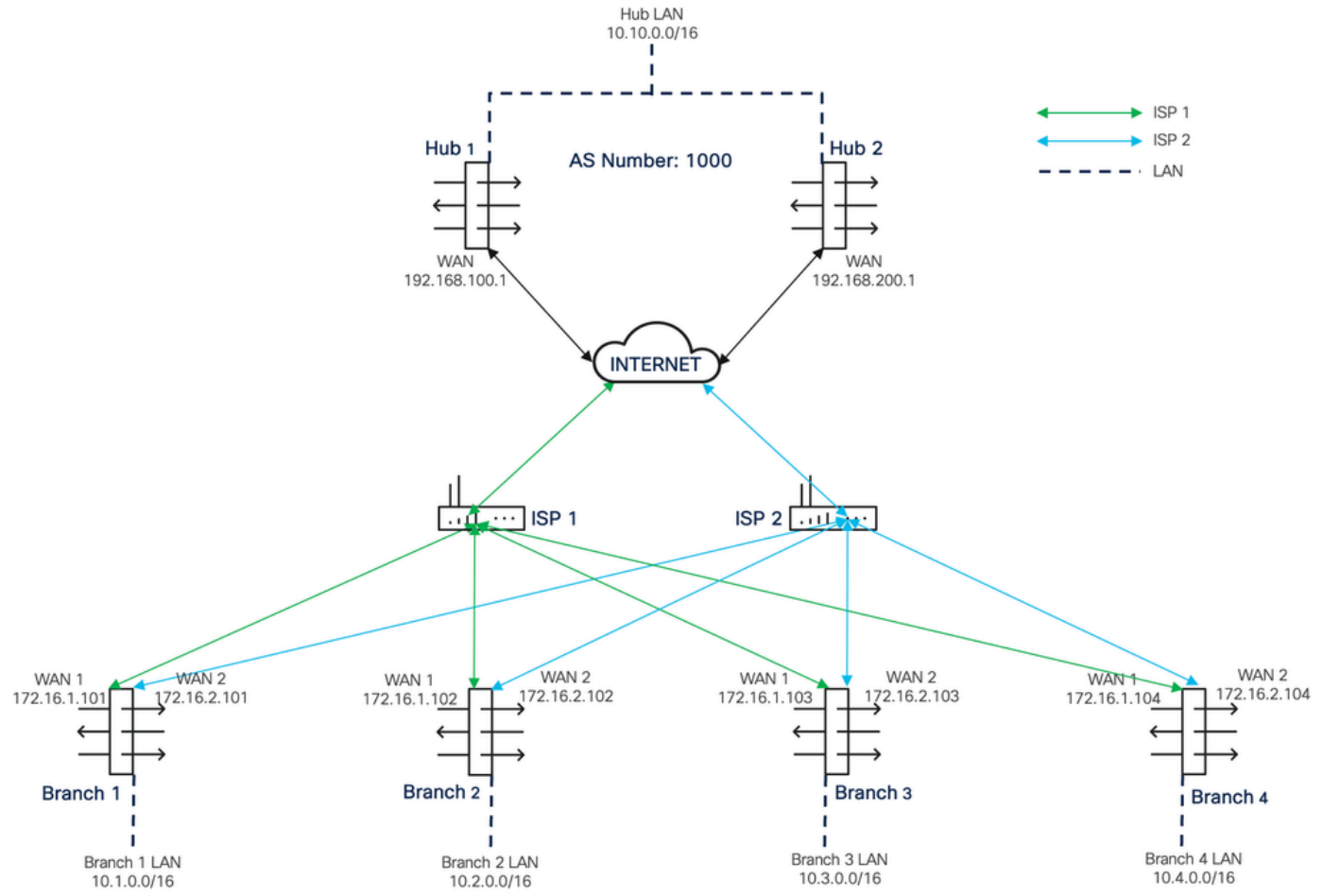
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

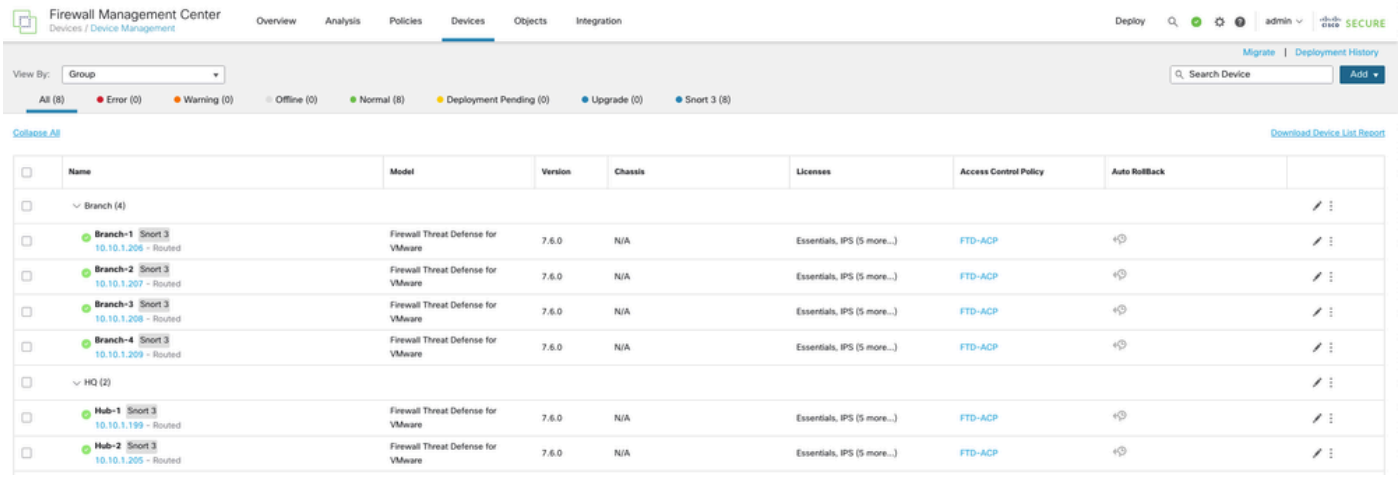
- FTD versione 7.6.0
- FMC versione 7.6.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

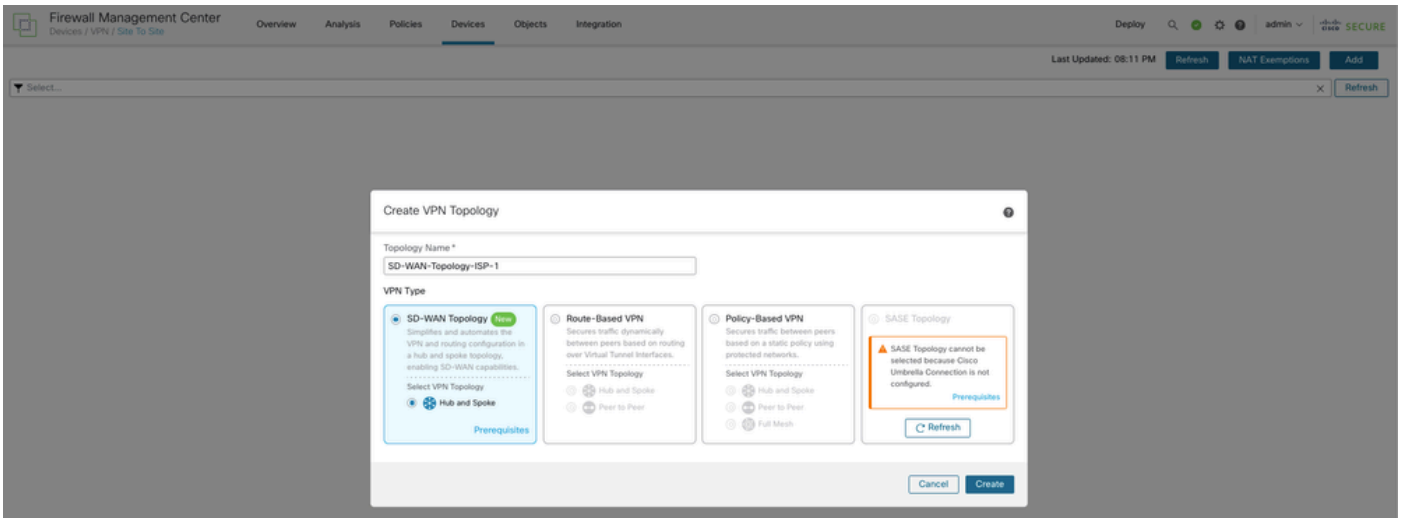
Esempio di rete





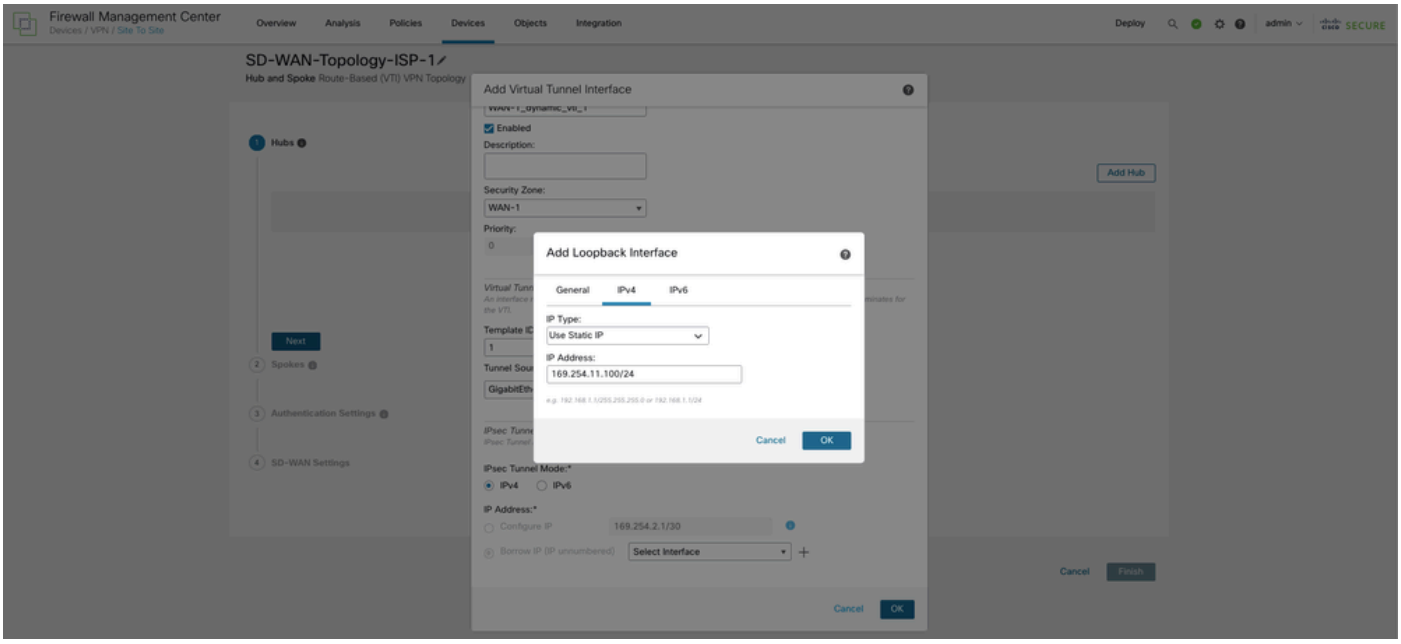
Passaggio 1. Creare una topologia SD-WAN con WAN-1 come interfaccia VPN

Selezionare Dispositivi > VPN > Sito - Sito. Selezionare Add, quindi immettere un nome appropriato nel campo Topology Name (Nome topologia) per la prima topologia con WAN-1 come interfaccia VPN. Selezionare SD-WAN Topology (Topologia SD-WAN) e selezionare Create (Crea).

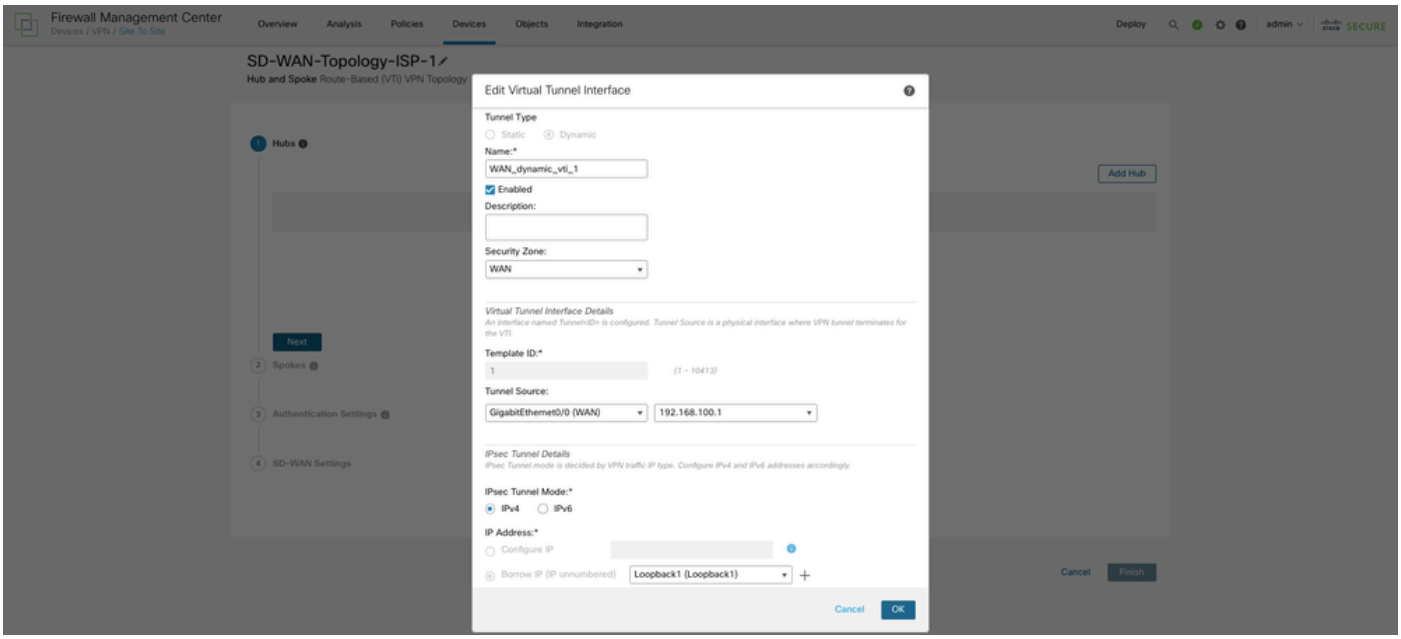


Passaggio 2. Configurare l'interfaccia DVTI (Dynamic Virtual Tunnel Interface) sull'hub primario

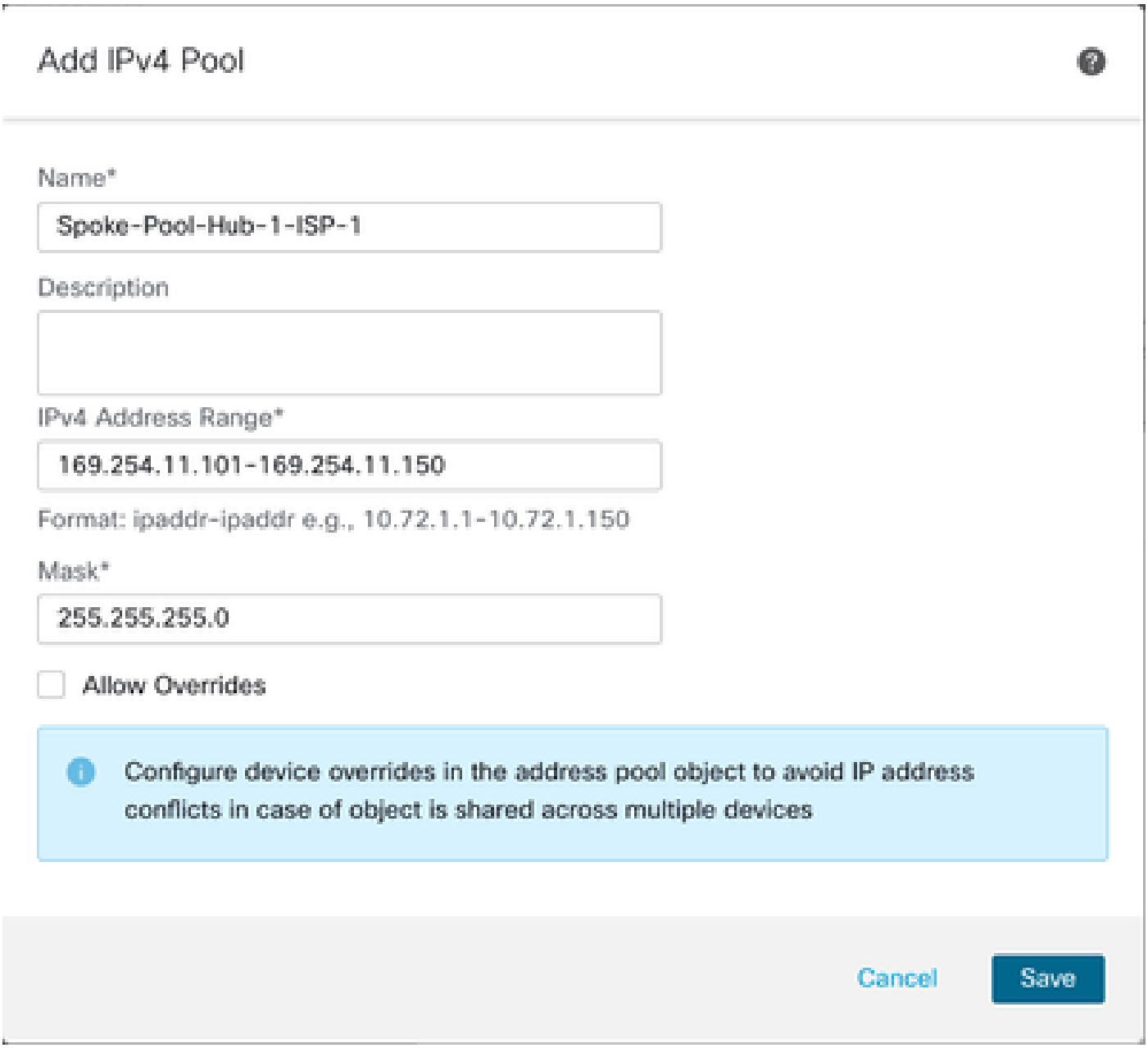
Selezionare Add Hub e scegliere l'hub principale dall'elenco a discesa Device (Dispositivo). Selezionare l'icona + accanto a Dynamic Virtual Tunnel Interface (DVTI). Configurare un nome, un'area di sicurezza e un ID modello e assegnare WAN-1 come interfaccia origine tunnel per DVTI.



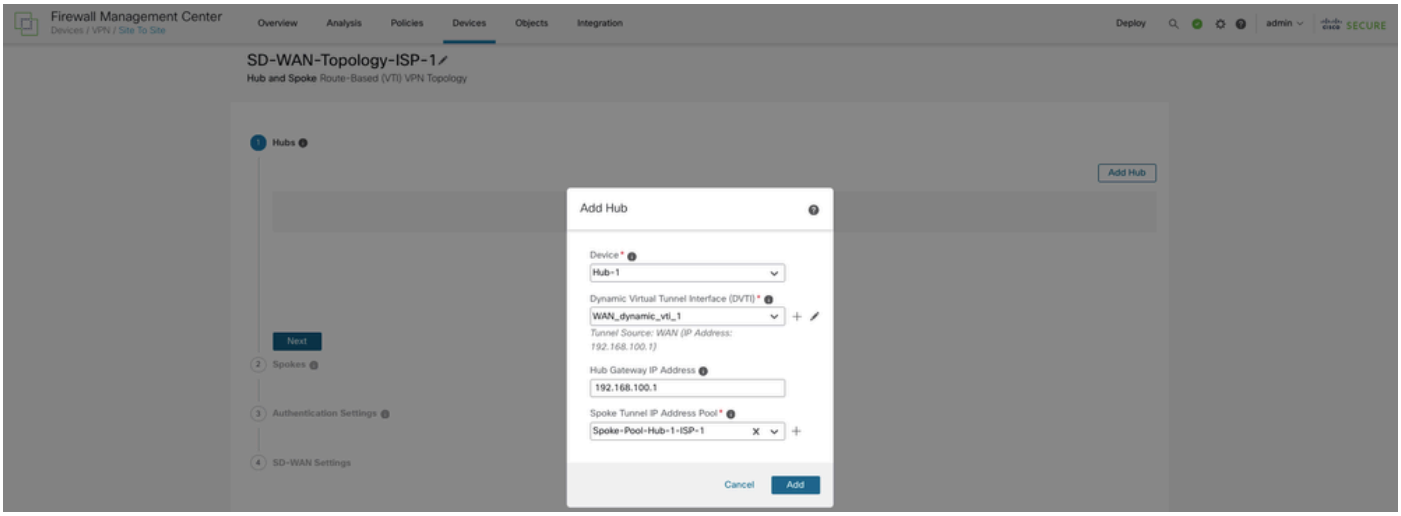
Scegliere un'interfaccia fisica o di loopback dall'elenco a discesa Indirizzo IP prestito. Nella topologia corrente, la tecnologia DVTI eredita un indirizzo IP dell'interfaccia di loopback. Selezionare OK.



Scegliere un pool di indirizzi o selezionare l'icona + accanto a Pool di indirizzi IP tunnel spoke per creare un nuovo pool di indirizzi. Quando si aggiungono spoke, la procedura guidata genera automaticamente interfacce tunnel spoke e assegna indirizzi IP a tali interfacce spoke da questo pool di indirizzi IP.

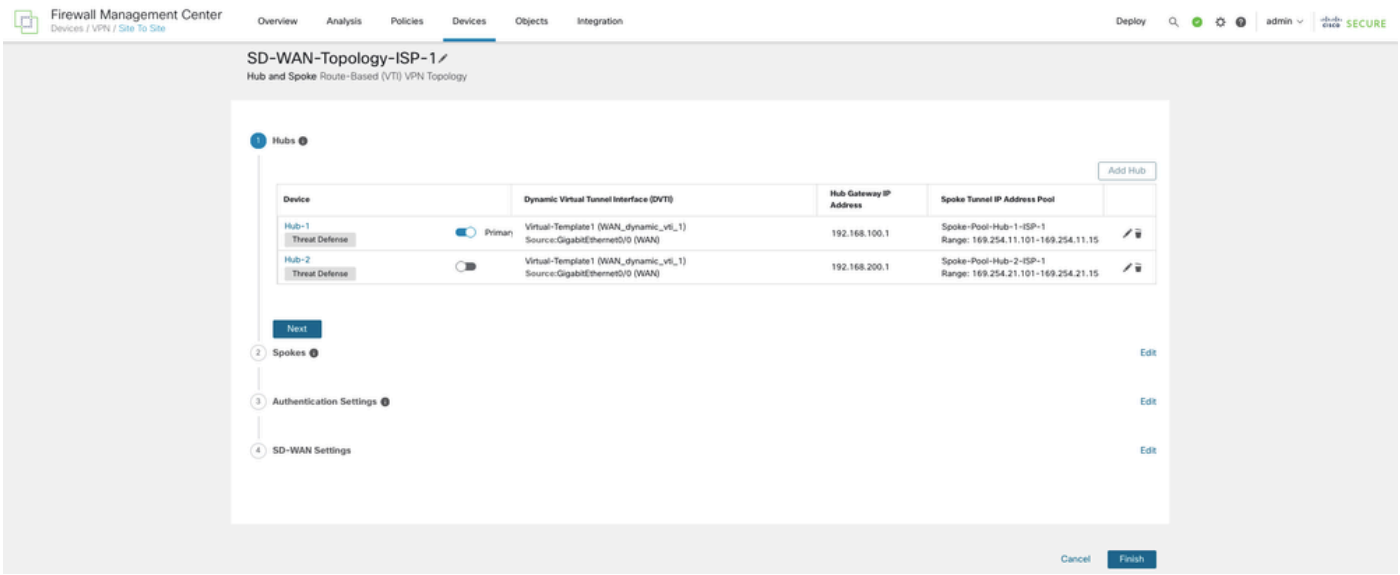


Una volta completata la configurazione dell'hub primario, selezionare Aggiungi per salvare l'hub primario nella topologia.



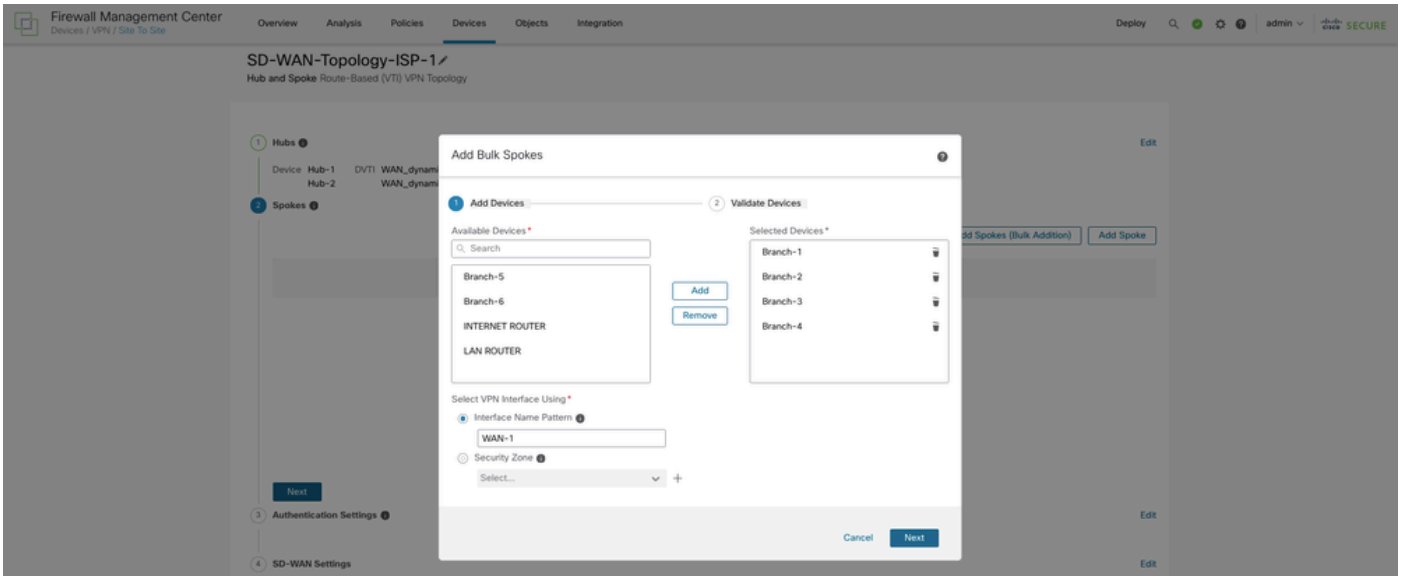
Passaggio 3. Configurare l'interfaccia DVTI (Dynamic Virtual Tunnel Interface) sull'hub secondario

Selezionare Add Hub di nuovo per configurare l'hub secondario nella topologia con WAN-1 come interfaccia VPN ripetendo i passaggi 1 e 2. Selezionare Next.

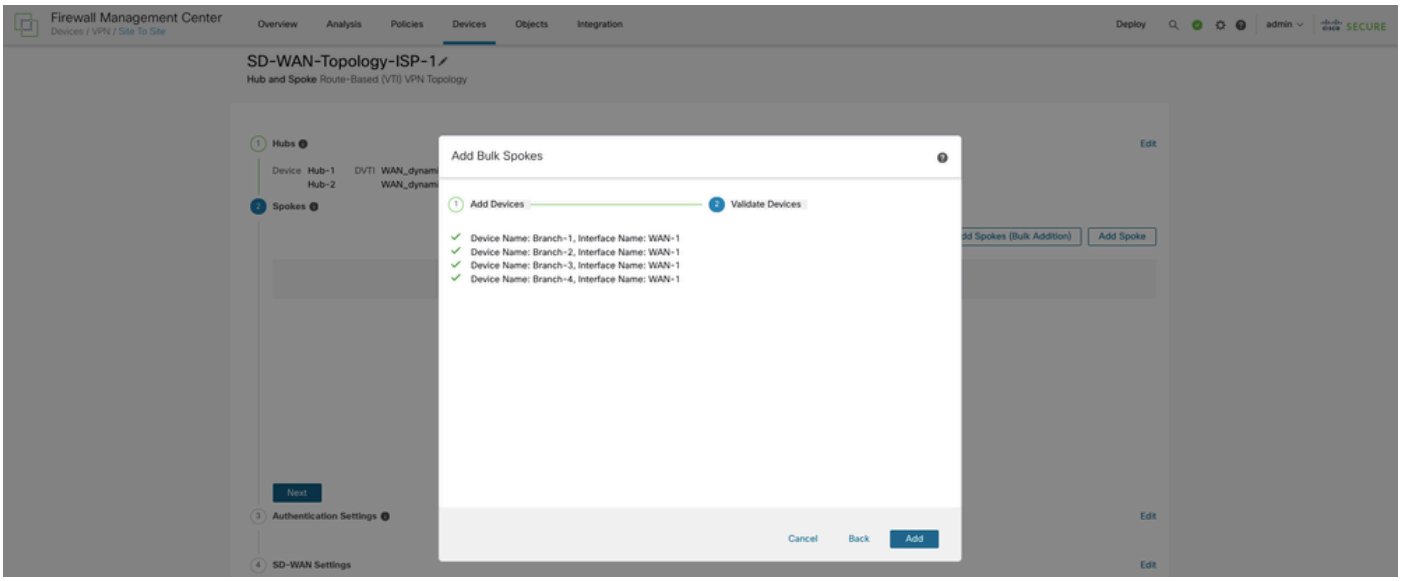


Passaggio 4. Configurazione dei raggi

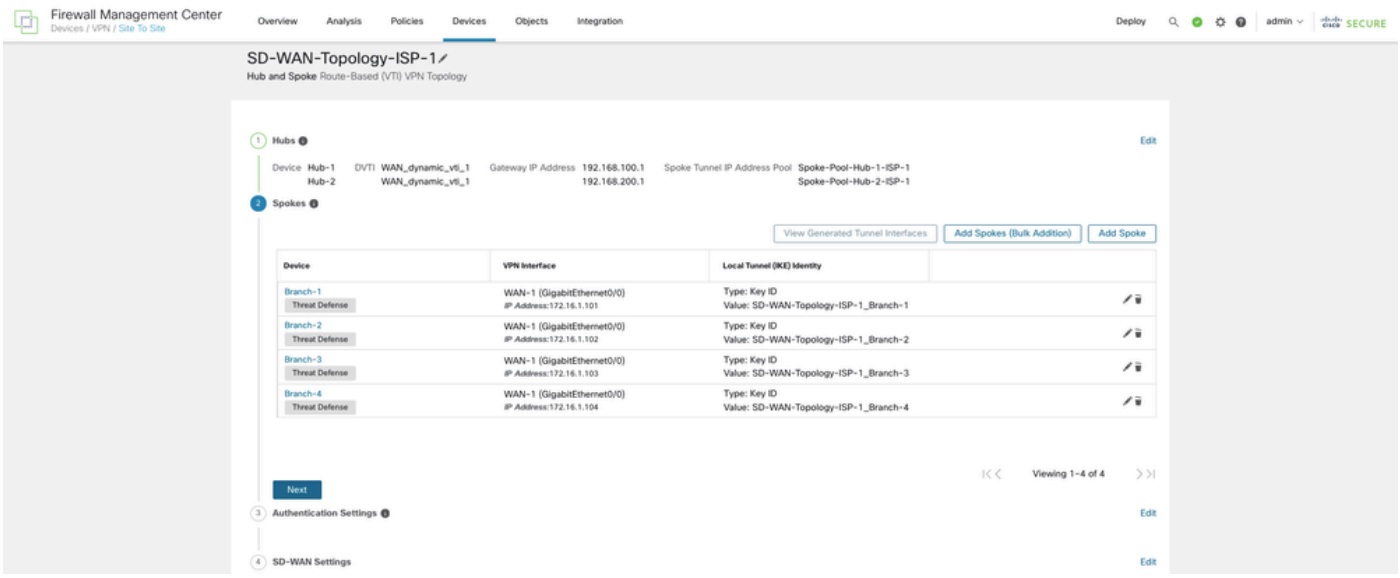
Selezionare Aggiungi spoke per aggiungere un dispositivo a spoke singolo oppure fare clic su Aggiungi spoke (aggiunta di massa) per aggiungere più spoke alla topologia. La topologia corrente utilizza quest'ultima opzione per aggiungere più FTD di diramazione alla topologia. Nella finestra di dialogo Aggiungi raggi ausiliari, selezionate gli FTD da aggiungere come raggi. Selezionare un modello di nome interfaccia comune che corrisponda al nome logico della WAN-1 su tutti i spoke o all'area di sicurezza associata alla WAN-1.



Selezionare Avanti in modo che la procedura guidata verifichi se gli spoke dispongono di interfacce con il pattern o l'area di sicurezza specificati.

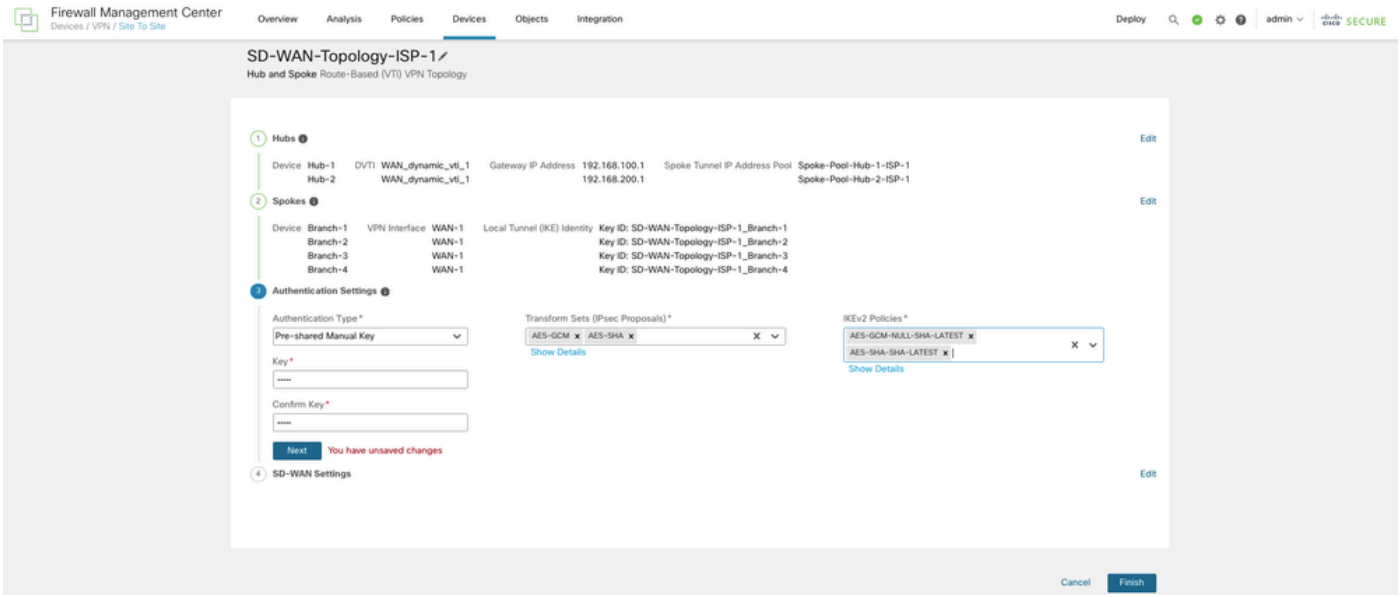


Selezionare Add (Aggiungi). La procedura guidata seleziona automaticamente il DVTI dell'hub come indirizzo IP di origine del tunnel per ogni spoke.



Passaggio 5. Configurare le impostazioni di autenticazione

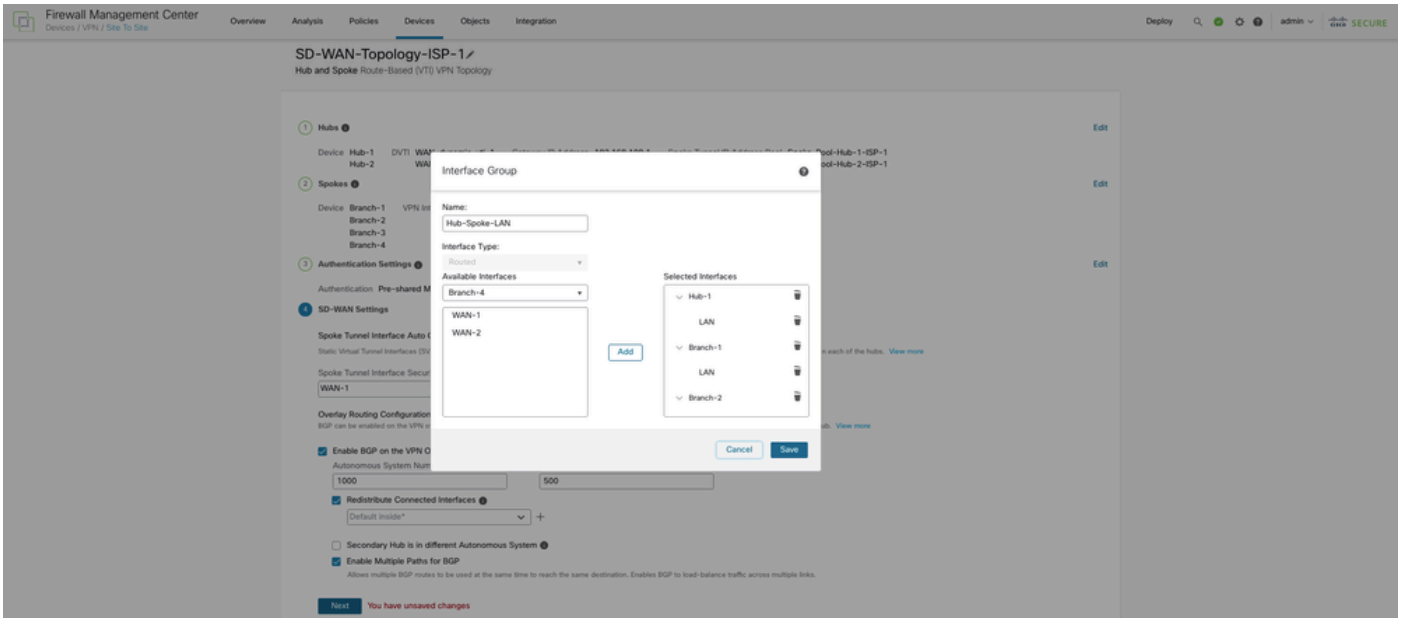
Selezionare Avanti per configurare le impostazioni di autenticazione. Per l'autenticazione dei dispositivi, è possibile selezionare una chiave precondivisa manuale, una chiave precondivisa generata automaticamente o un certificato nell'elenco a discesa Tipo di autenticazione. Selezionare uno o più algoritmi dagli elenchi a discesa Set di trasformazioni e Criteri IKEv2.



Passaggio 6. Configurare le impostazioni SD-WAN

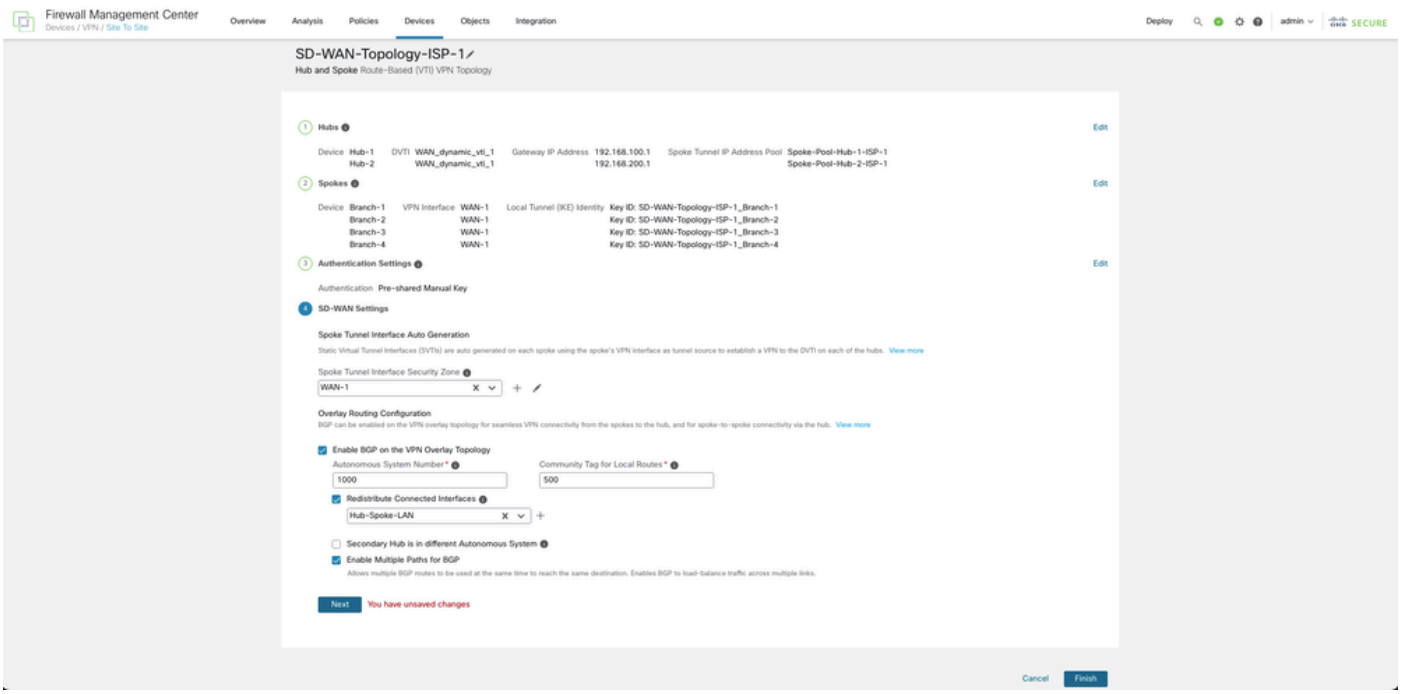
Selezionare Next (Avanti) per configurare le impostazioni SD-WAN. Questo passaggio include la generazione automatica di interfacce tunnel spoke e la configurazione BGP della rete overlay. Dall'elenco a discesa Area di sicurezza interfaccia tunnel spoke, scegliere un'area di sicurezza o selezionare + per creare un'area di sicurezza alla quale la procedura guidata aggiunga automaticamente le SVTI (Static Virtual Tunnel Interfaces) generate automaticamente dallo spoke.

Selezionare la casella di controllo Abilita BGP sulla topologia di overlay VPN per automatizzare le configurazioni BGP tra l'interfaccia del tunnel di overlay. Nel campo Numero sistema autonomo, immettere un numero AS (Autonomous System). Selezionare la casella di controllo Ridistribuisci interfacce connesse e scegliere un gruppo di interfacce dall'elenco a discesa oppure selezionare + per creare un gruppo di interfacce con interfacce LAN connesse degli hub e degli spoke per la ridistribuzione della route BGP nella topologia di overlay.

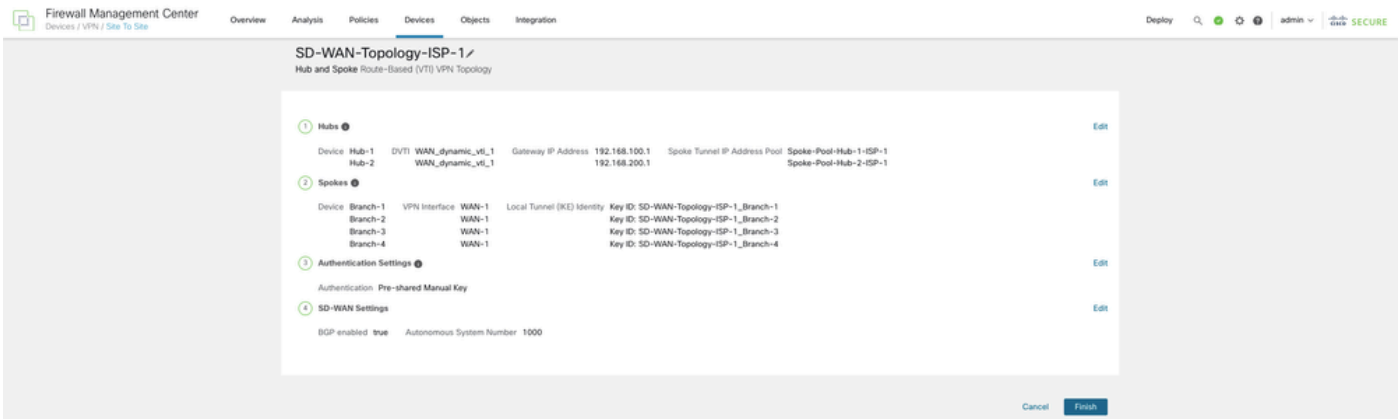


Nel campo Tag community per route locali, immettere l'attributo della community BGP per

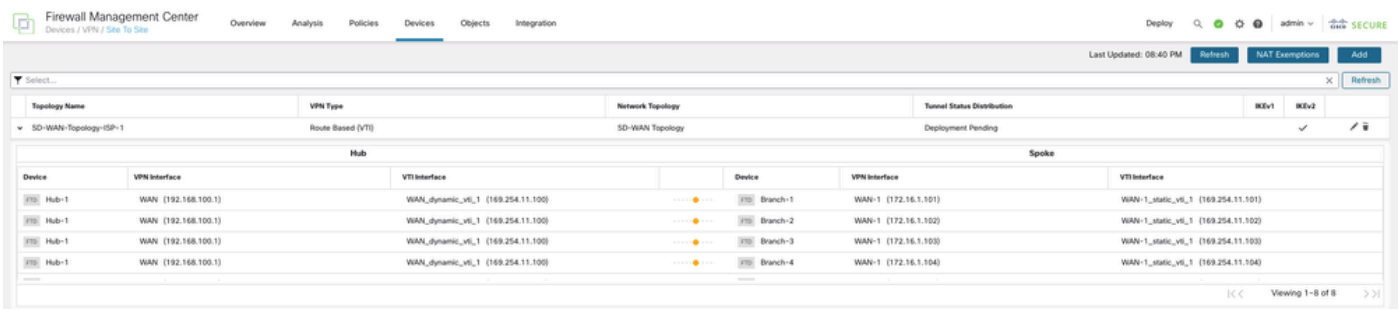
contrassegnare le route locali connesse e ridistribuite. Questo attributo consente di applicare facilmente filtri di route. Selezionare la casella di controllo Hub secondario in sistema autonomo diverso se si dispone di un hub secondario in un SA diverso. Infine, selezionare la casella di controllo Enable Multiple Paths for BGP per abilitare BGP per il bilanciamento del carico del traffico su più collegamenti.



Fare clic su Finish (Fine) per salvare e convalidare la topologia SD-WAN.

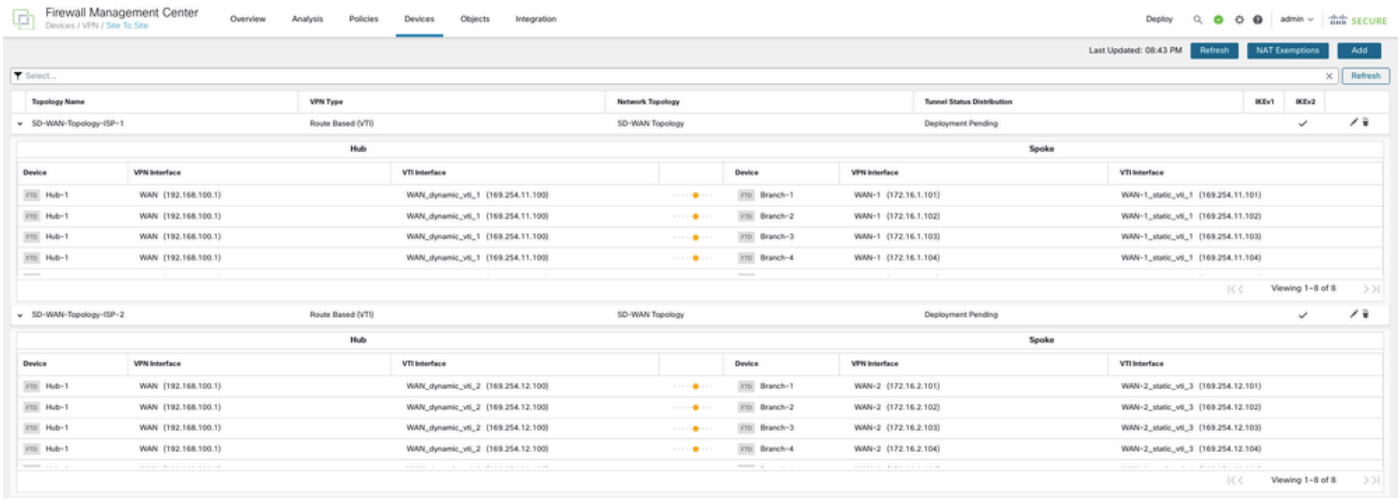


È possibile visualizzare la topologia in Dispositivi > VPN da sito a sito. Il numero totale di tunnel nella prima topologia SD-WAN è 8.



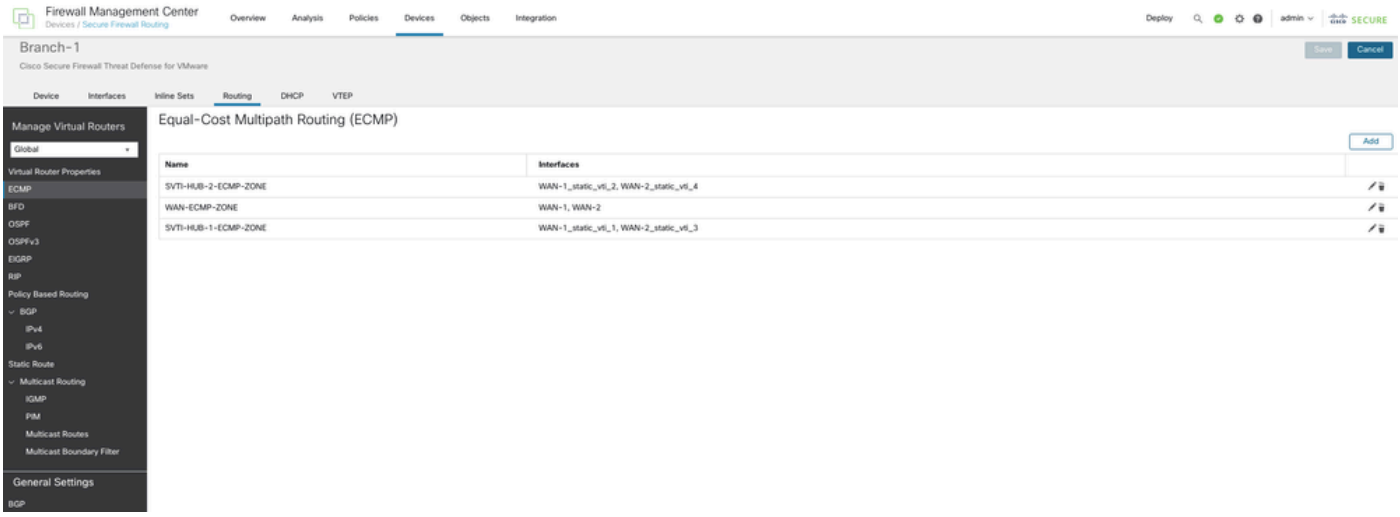
Passaggio 7. Creare una topologia SD-WAN con WAN-2 come interfaccia VPN

Ripetere i passaggi da 1 a 6 per configurare una topologia SD-WAN con WAN-2 come interfaccia VPN. Il numero totale di tunnel nella seconda topologia SD-WAN è 8. Le topologie finali devono essere simili all'immagine mostrata di seguito.



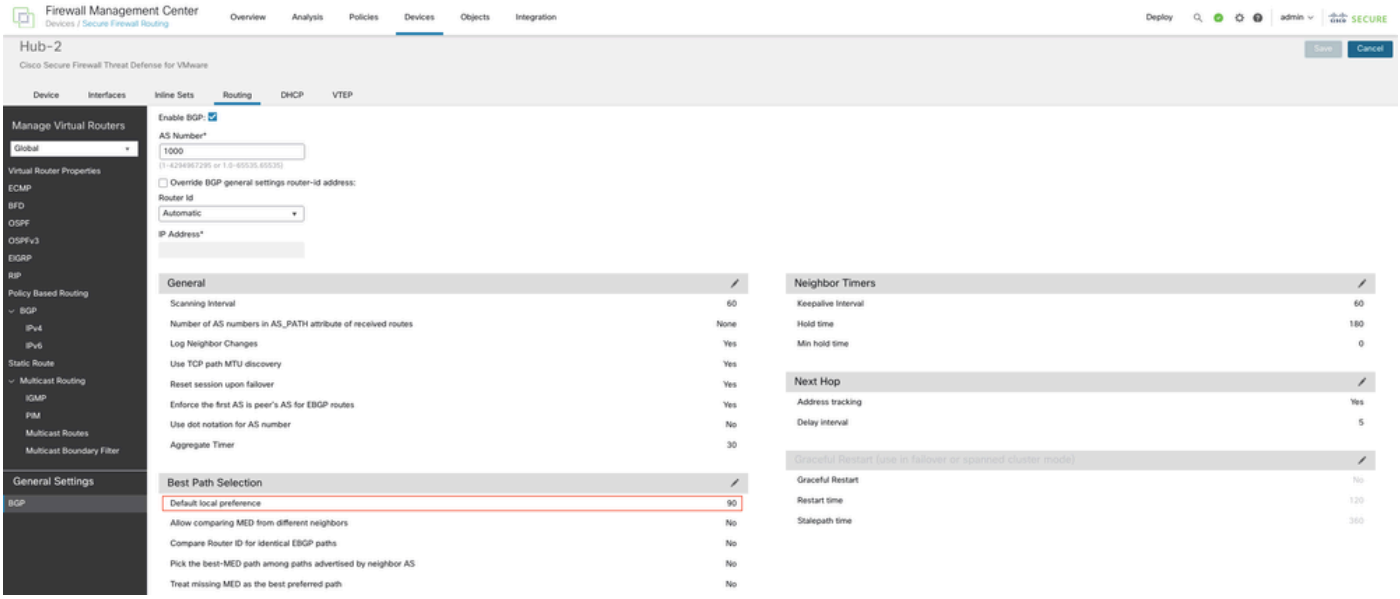
Passaggio 8. Configurazione delle zone ECMP

Su ciascuna filiale, selezionare Routing > ECMP e configurare le zone ECMP (Equal-Cost Multi-Path) per le interfacce WAN e gli SVTI che si connettono all'hub principale e a quello secondario, come mostrato di seguito. In questo modo è possibile fornire ridondanza dei collegamenti e abilitare il bilanciamento del carico del traffico VPN.



Passaggio 9. Modificare la preferenza locale BGP sull'hub

Selezionare Routing > General Settings > BGP sull'hub secondario. Selezionare Abilita BGP, configurare il numero AS e impostare il valore della preferenza locale predefinita in Selezione del miglior percorso su un valore inferiore a quello configurato sull'hub primario. Selezionare Salva. In questo modo le route verso l'hub principale vengono preferite rispetto alle route verso l'hub secondario. Quando l'hub primario diventa inattivo, subentrano i percorsi verso l'hub secondario.

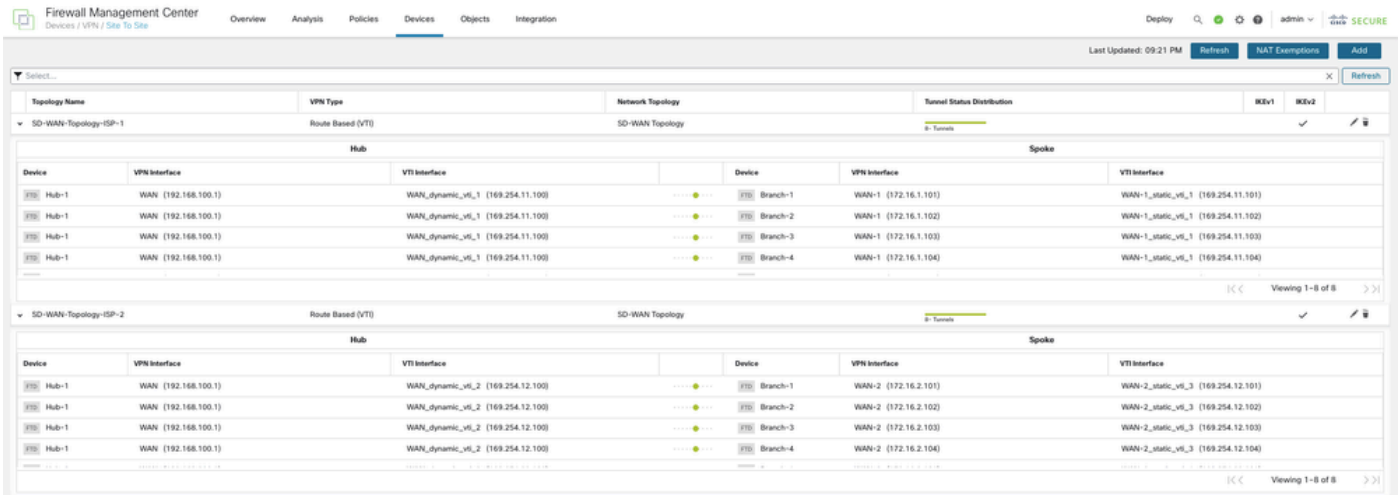


Distribuire le configurazioni su tutti i dispositivi.

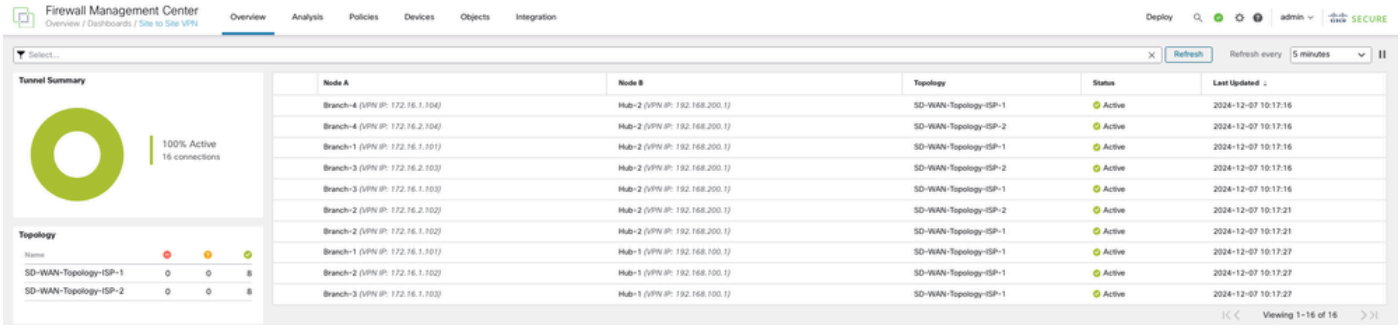
Verifica

Verifica degli stati del tunnel

Per verificare se i tunnel VPN delle topologie SD-WAN sono attivi, selezionare Dispositivo > VPN > Da sito a sito.

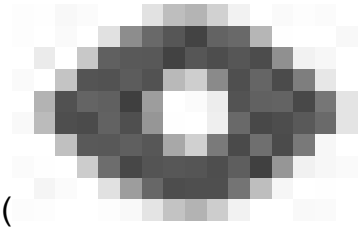


Per visualizzare i dettagli dei tunnel VPN da sito a sito, scegliere Panoramica > Dashboard > VPN da sito a sito.



Per visualizzare ulteriori dettagli su ciascun tunnel VPN:

1. Passare il mouse su un tunnel.



2. Selezionare il pulsante di opzione Visualizza informazioni complete ( ). Verrà visualizzato un riquadro con i dettagli del tunnel e altre azioni.

3. Selezionare la scheda Dettagli CLI nel riquadro laterale per visualizzare i comandi show e i dettagli delle associazioni di sicurezza IPsec.

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

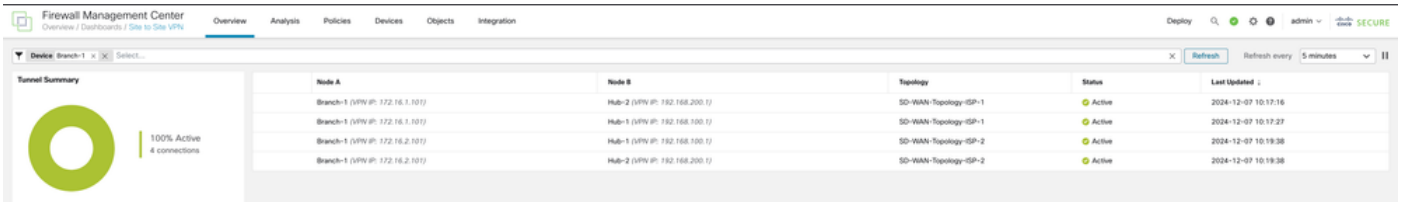
Branch-1 (VPN Interface IP: 172.16.2.101)

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

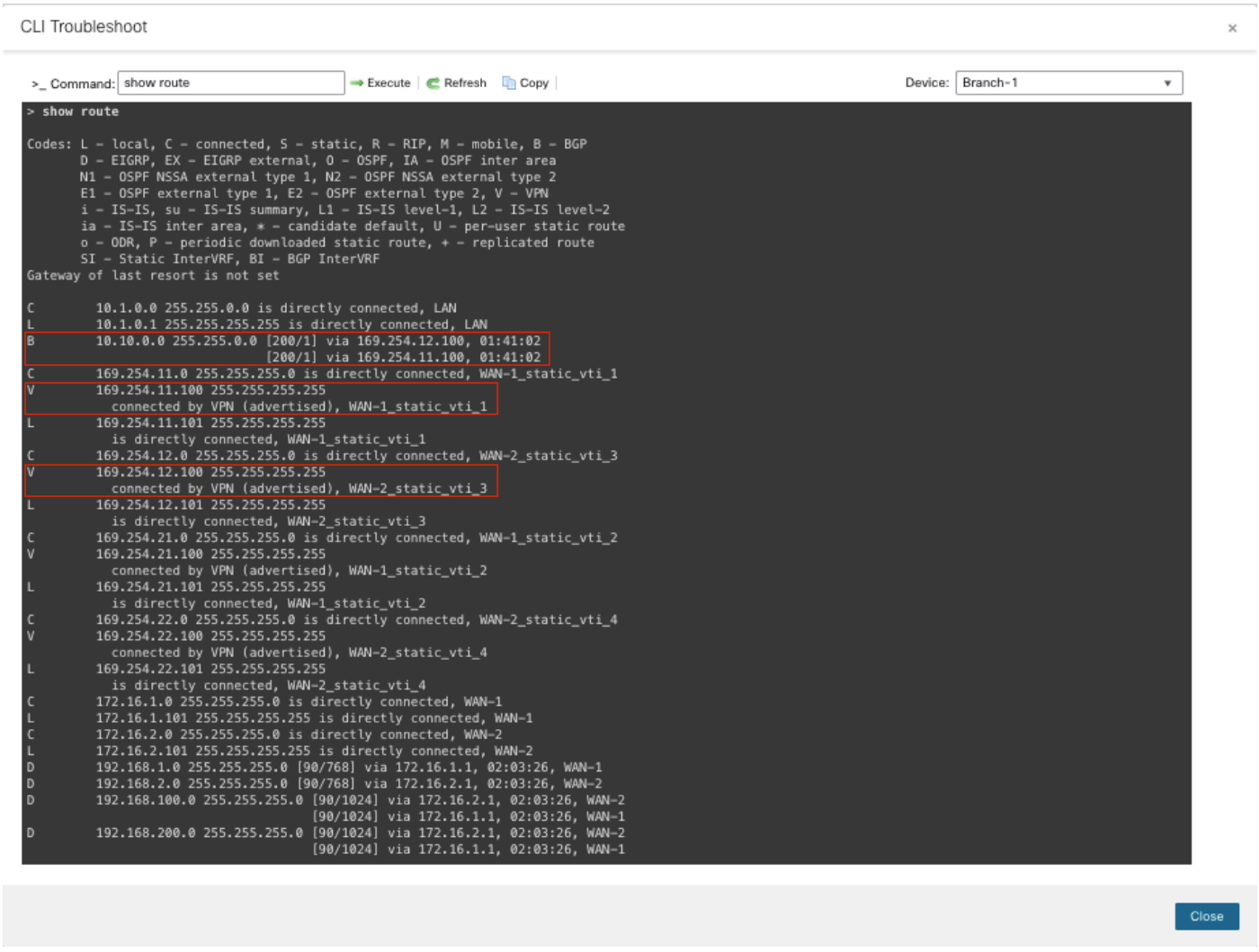
WAN-2_static_vti_3 - Da SVTI a Hub 1 tramite ISP 2
WAN-1_static_vti_2 - Da SVTI a Hub 2 tramite ISP 1
WAN-2_static_vti_4 - Da SVTI a Hub 2 tramite ISP 2

Verifica del bilanciamento del carico del traffico VPN

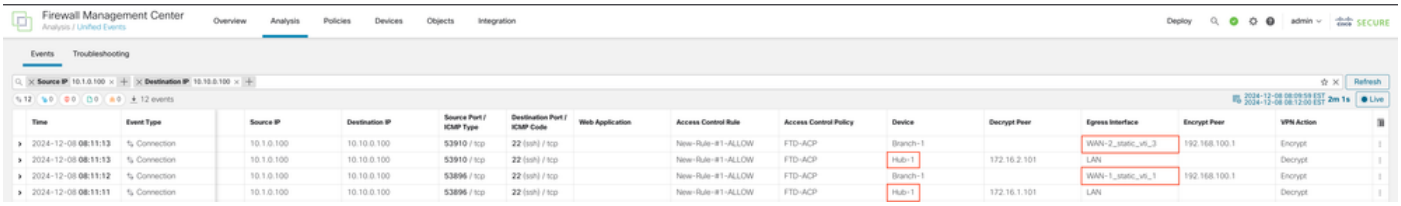
Lo stato del tunnel può essere visualizzato nel dashboard della VPN da sito a sito. Idealmente, tutti i tunnel devono essere attivi:



Le route all'hub principale sono preferibili. Il comando show route sulla filiale 1 indica che il traffico VPN è con carico bilanciato tra i due SVTI sull'ISP 1 e sull'ISP 2 e diretti all'hub principale:

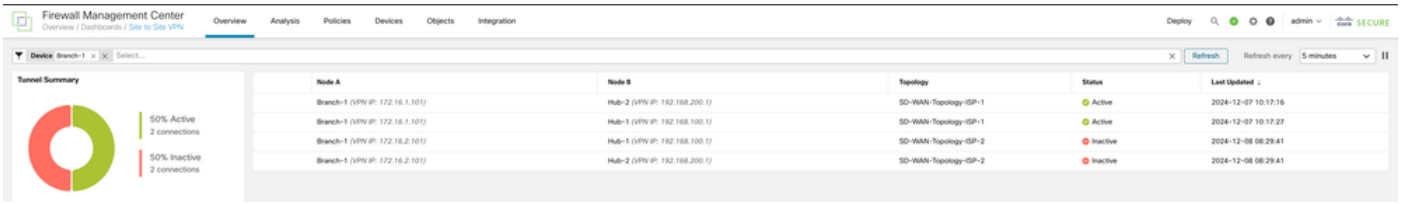


L'interfaccia in uscita utilizzata per il traffico VPN effettivo può essere rilevata in Eventi unificati:



Verifica della ridondanza di due ISP

Quando l'ISP-2 non è attivo, lo stato del tunnel indica che i tunnel tramite ISP-1 sono attivi:



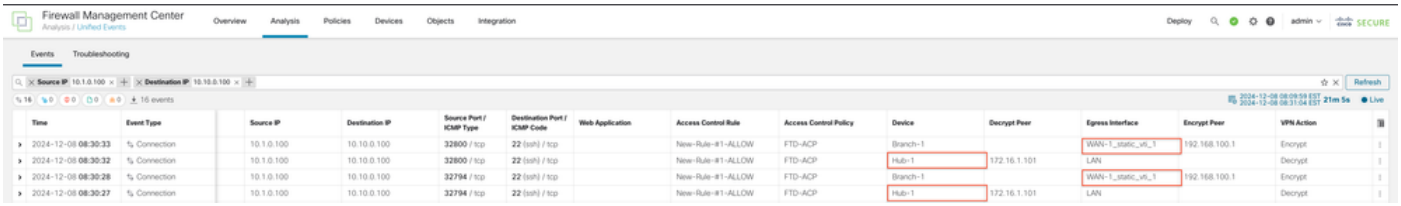
Le route all'hub principale sono preferibili. Il comando show route sulla filiale 1 indica che il traffico VPN viene instradato tramite SVTI sull'ISP-1 all'hub principale:

CLI Troubleshoot

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

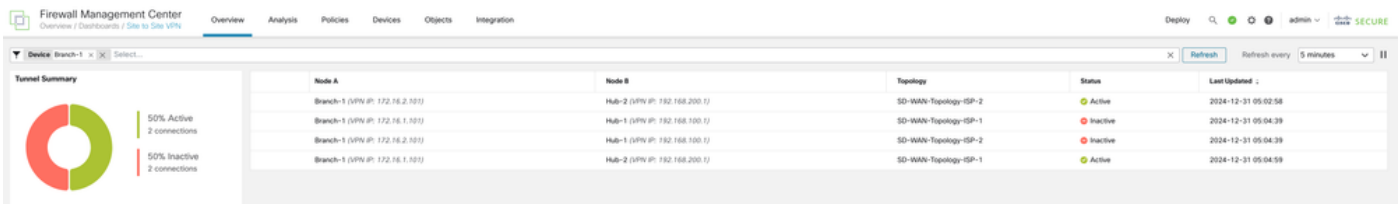
```
> show route

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
```

L'interfaccia in uscita utilizzata per il traffico VPN effettivo può essere rilevata in Eventi unificati:



Verifica ridondanza a livello di hub

Quando l'hub primario è inattivo, lo stato del tunnel indica che i tunnel verso l'hub secondario sono attivi:



Poiché l'hub primario non è attivo, vengono preferiti i percorsi all'hub secondario. Il comando show route sulla filiale 1 indica che il traffico VPN è con carico bilanciato tra i due SVTI sull'ISP 1 e sull'ISP 2 e diretti all'hub secondario:

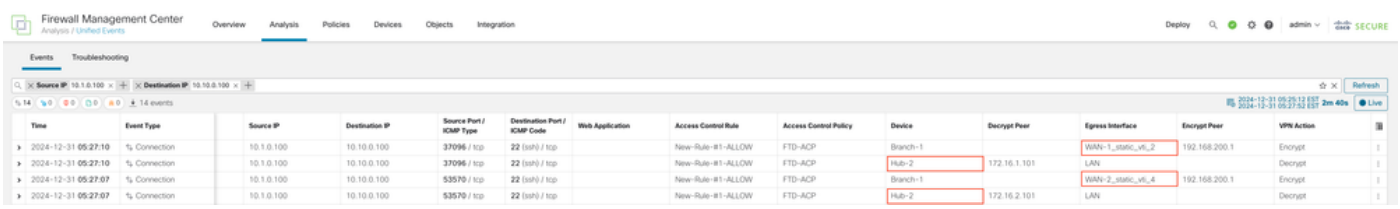
CLI Troubleshoot

>_ 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 169.254.22.100, 00:09:02
                               [200/1] via 169.254.21.100, 00:09:02
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, 00:11:13, WAN-1
D        192.168.2.0 255.255.255.0 [90/768] via 172.16.2.1, 00:11:13, WAN-2
D        192.168.100.0 255.255.255.0 [90/1024] via 172.16.2.1, 00:11:13, WAN-2
                                     [90/1024] via 172.16.1.1, 00:11:13, WAN-1
D        192.168.200.0 255.255.255.0 [90/1024] via 172.16.2.1, 00:11:13, WAN-2
                                     [90/1024] via 172.16.1.1, 00:11:13, WAN-1
```

Close

L'interfaccia in uscita utilizzata per il traffico VPN effettivo può essere rilevata in Eventi unificati:



Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).