Configurazione di SD-WAN per la VPN da sito a sito su firewall protetto

Sommario

Introduzione

Questo documento descrive gli scenari di distribuzione di VPN basate su route con routing di overlay BGP utilizzando la funzione SD-WAN su Secure Firewall.

Prerequisiti

Tutti gli hub e gli spoke eseguono software FTD 7.6 o versioni successive e sono gestiti tramite lo stesso FMC, che esegue anche software 7.6 o versioni successive.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- IKEv2
- VPN basata sul percorso
- VTI (Virtual Tunnel Interfaces)
- IPSec
- BGP

Componenti usati

Le informazioni fornite in questo documento si basano su:

- Cisco Secure Firewall Threat Defense 7.7.10

- Cisco Secure Firewall Management Center 7.7.10

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.

Informazioni sulle funzionalità

Il Management Center semplifica la configurazione dei tunnel VPN e il routing tra le sedi centrali (hub) e le sedi remote (spoke) utilizzando la nuova procedura guidata SD-WAN.

· Automazione della configurazione VPN sfruttando la tecnologia DVTI (Dynamic Virtual Tunnel Interface) sugli hub e la tecnologia SVTI (Static Virtual Tunnel Interface) sugli spoke, con overlay routing abilitato tramite BGP.

· Assegna automaticamente gli indirizzi IP SVTI per gli spoke e attiva la configurazione VTI completa, inclusi i parametri crittografici.

· Fornisce una semplice configurazione del routing in un unico passaggio all'interno della stessa procedura guidata per abilitare BGP per il routing sovrapposto.

· Abilita il routing scalabile e ottimale sfruttando l'attributo route-reflector per BGP.

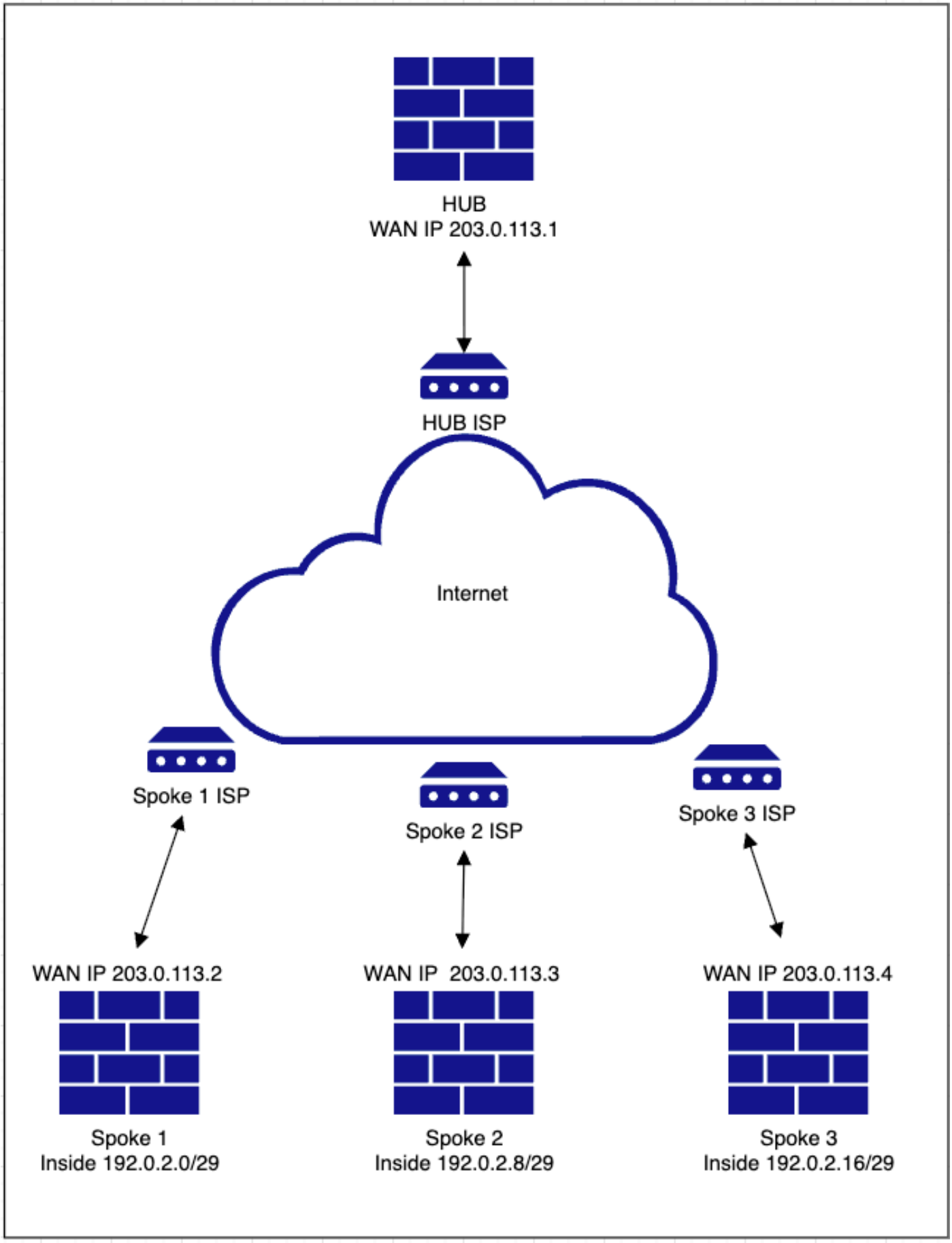
· Consente l'aggiunta simultanea di più raggi con il minimo intervento da parte dell'utente.

Topologie trattate

In questo articolo vengono illustrate più topologie per garantire che gli utenti siano a conoscenza dei diversi scenari di distribuzione.

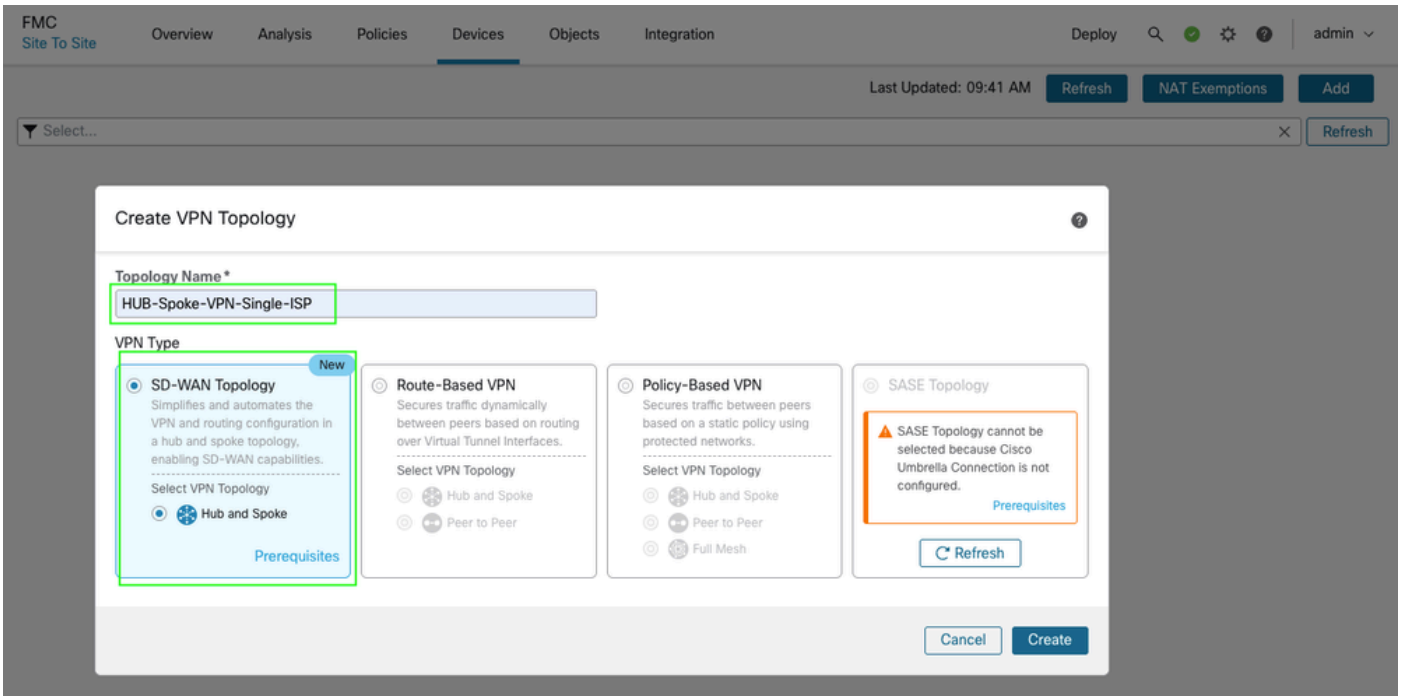
HUB e spoke (ISP singolo)

Esempio di rete

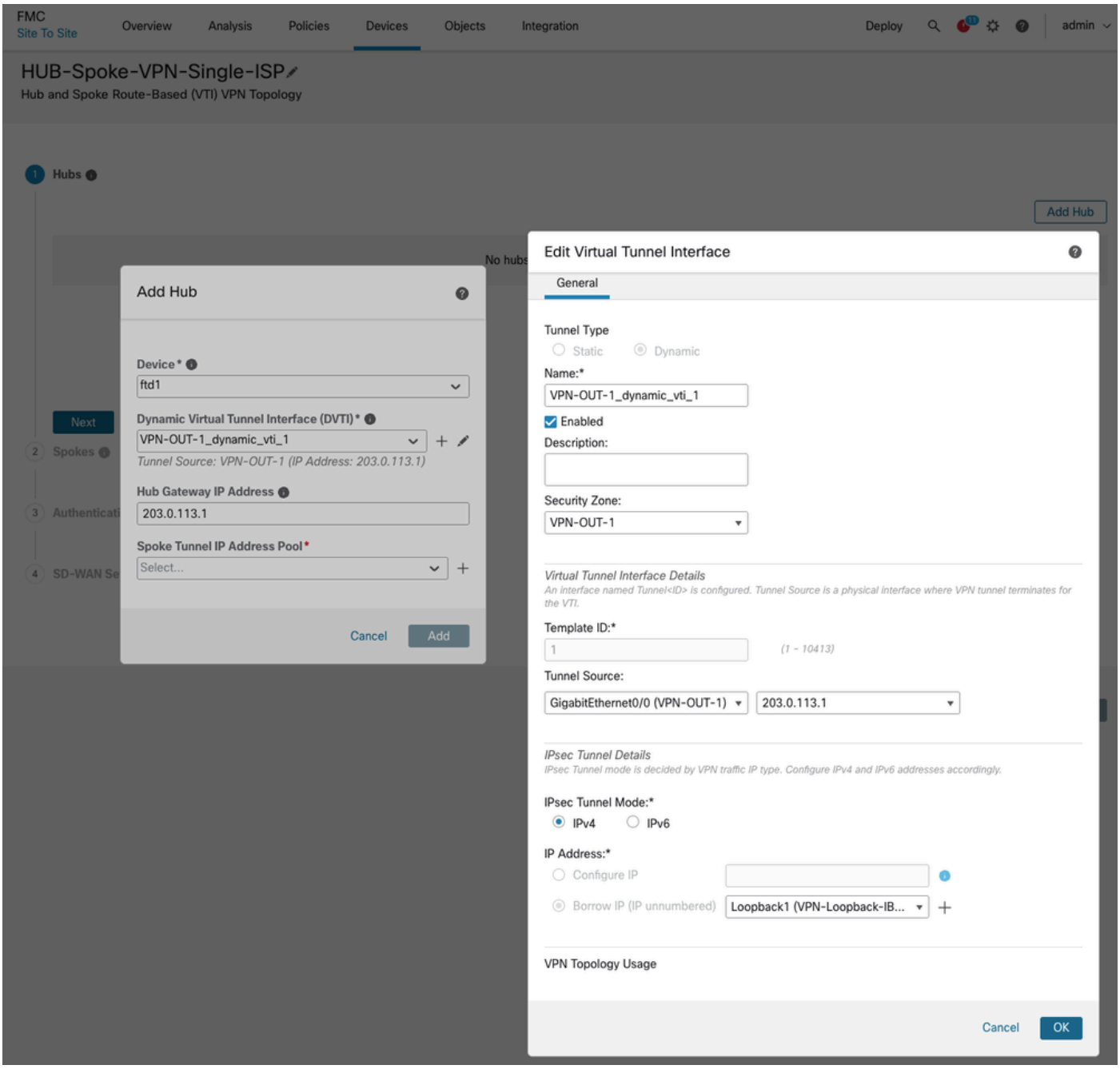


Configurazioni

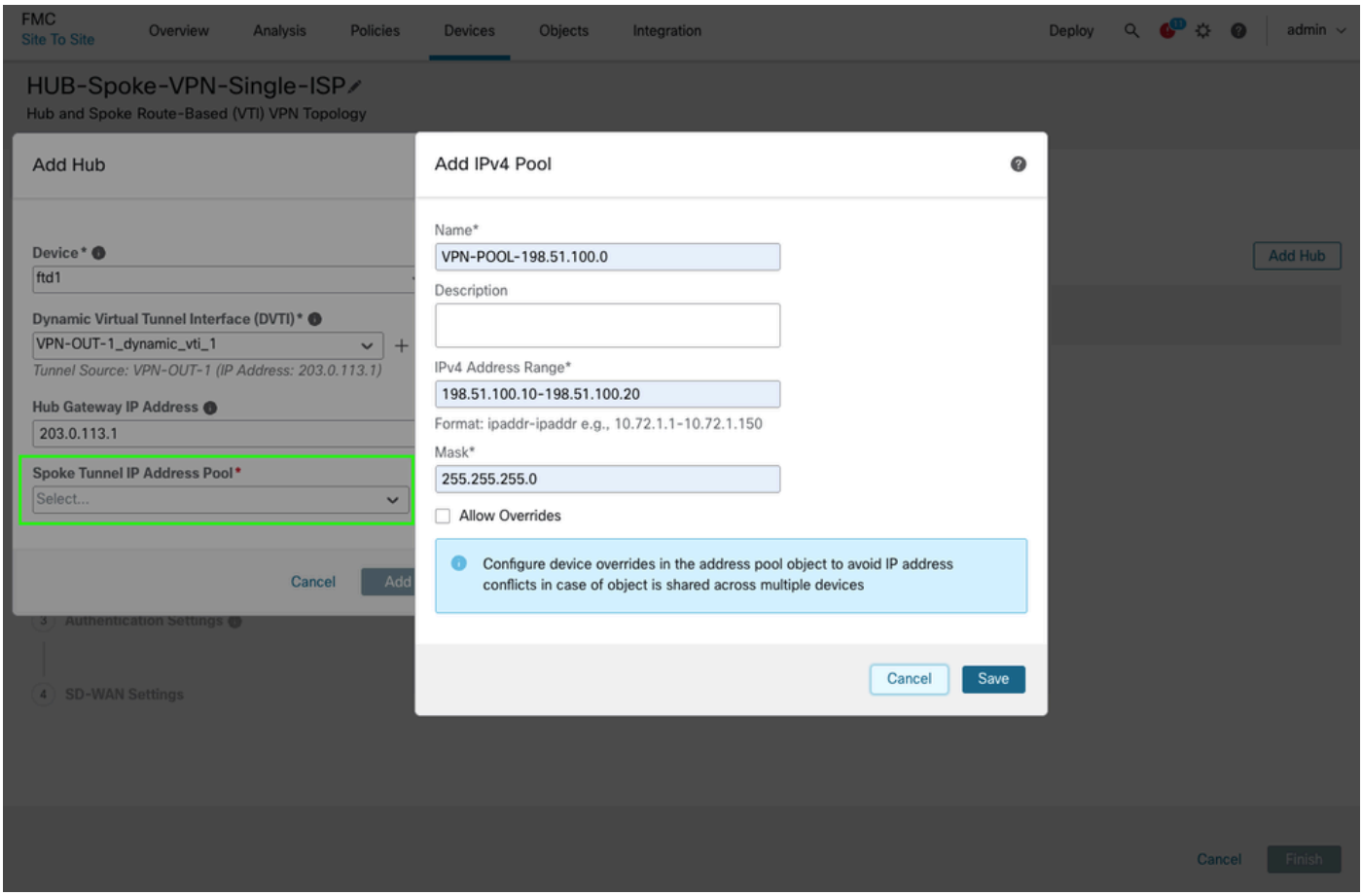
- Selezionare Dispositivi > VPN > Sito in sito > Aggiungi > Topologia SD-WAN > > Crea.

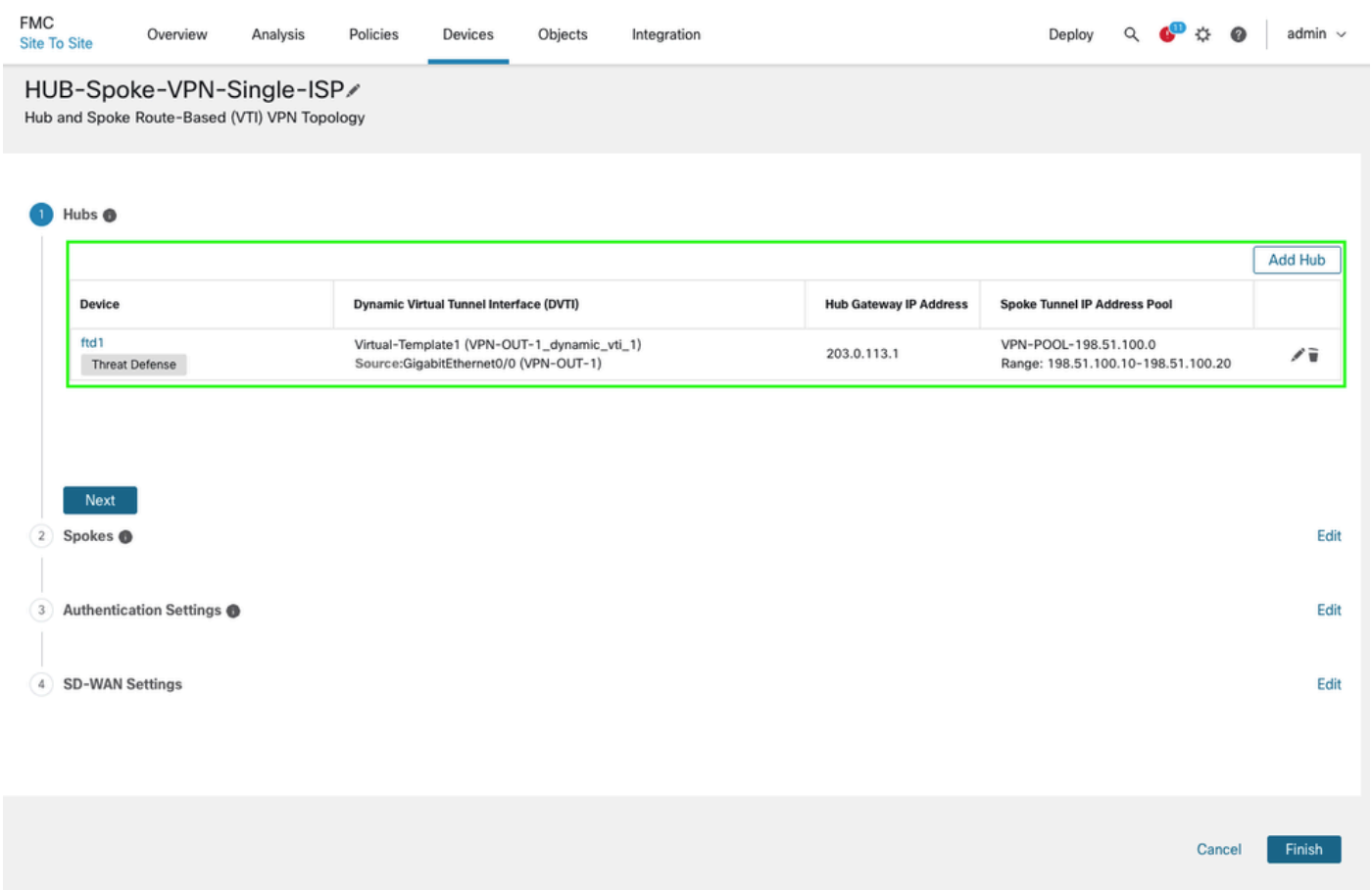


· Aggiungere un hub e creare un DVTI all'estremità dell'hub. Come parte della configurazione DVTI, assicurarsi di selezionare l'interfaccia di origine del tunnel corretta in base alla topologia.



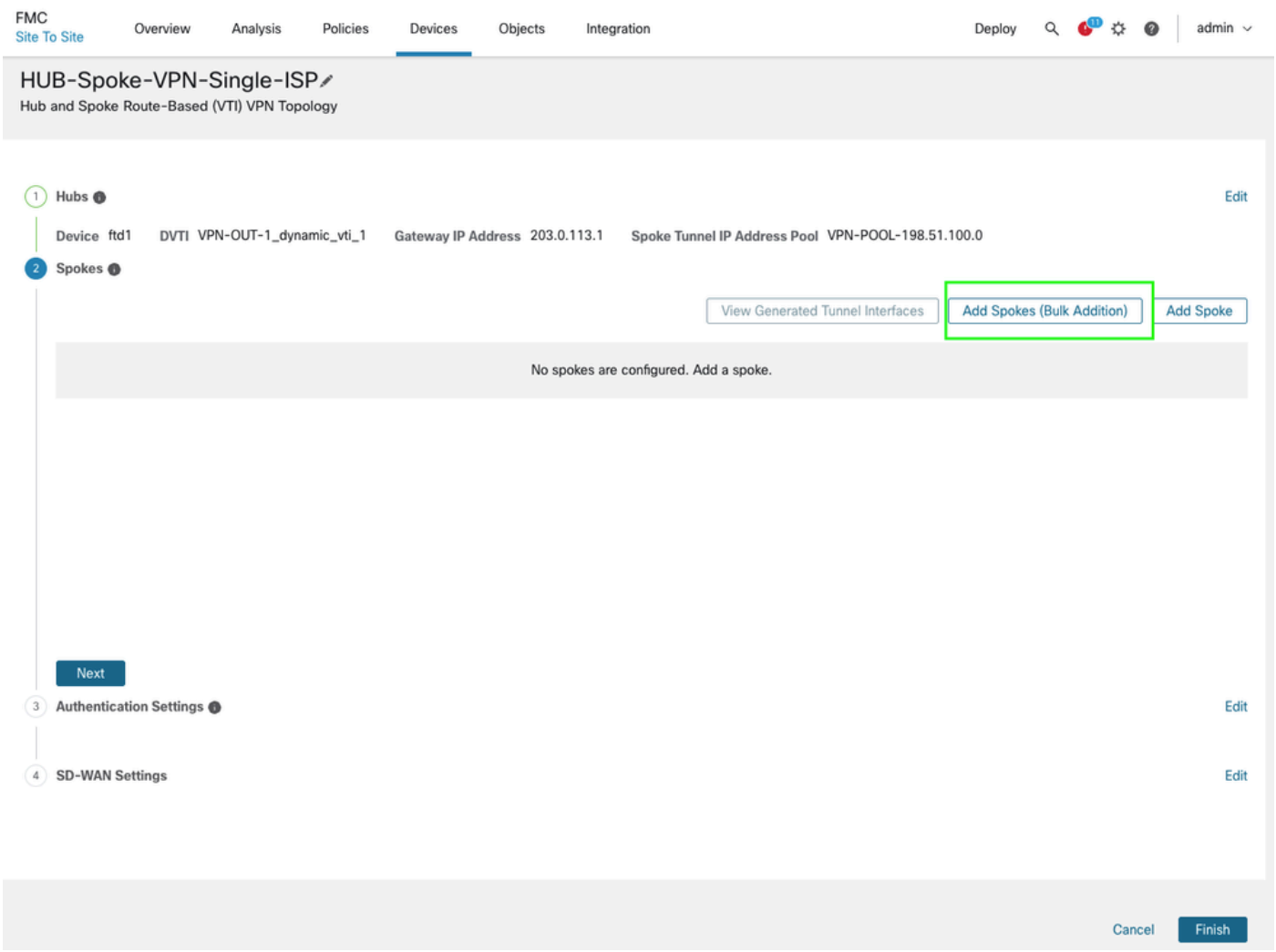
- Creare un pool di indirizzi IP del tunnel spoke, fare clic su Salva, quindi su Aggiungi. Il pool di indirizzi IP viene utilizzato per assegnare gli indirizzi IP del tunnel VTI agli spoke.



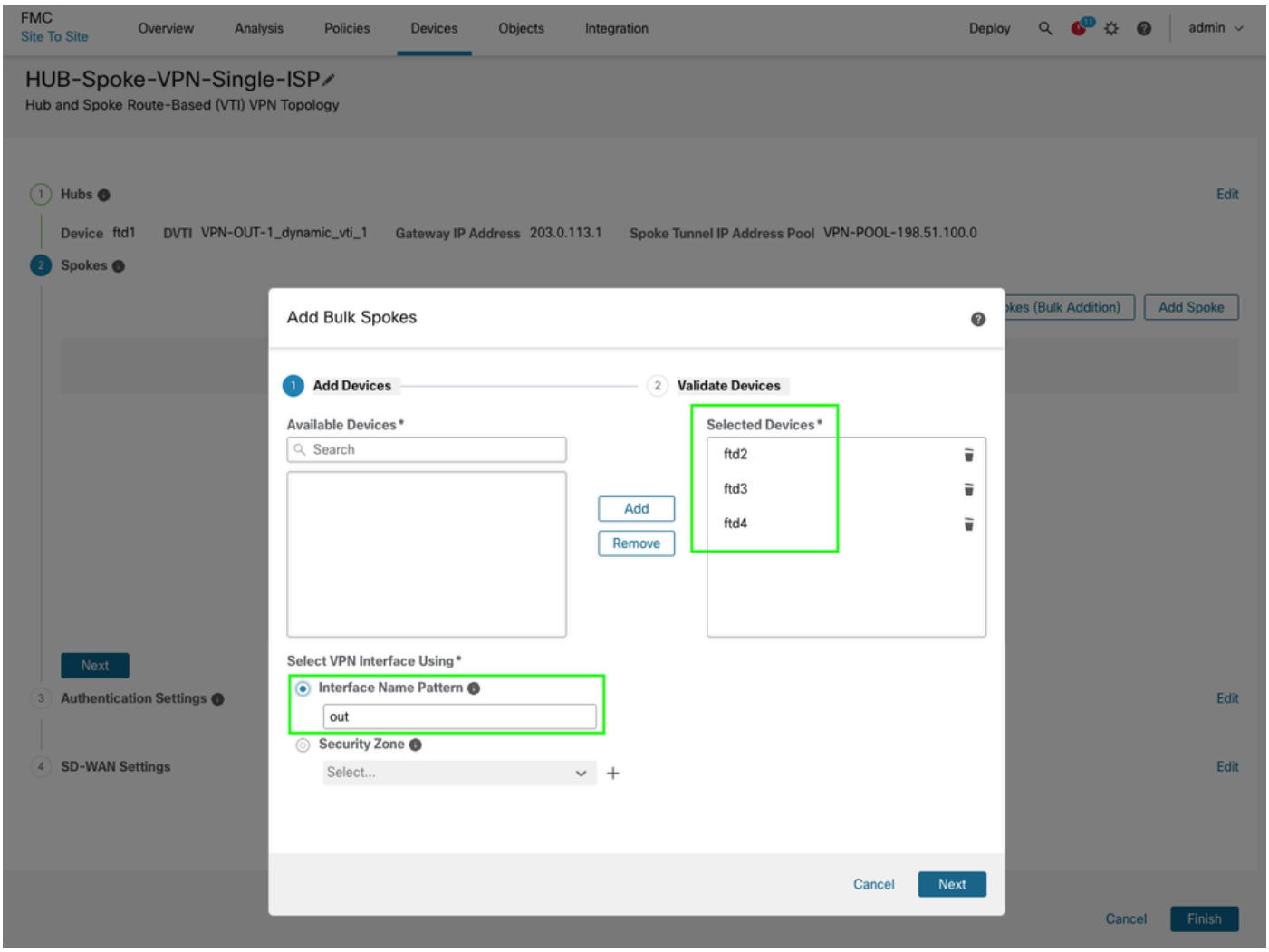


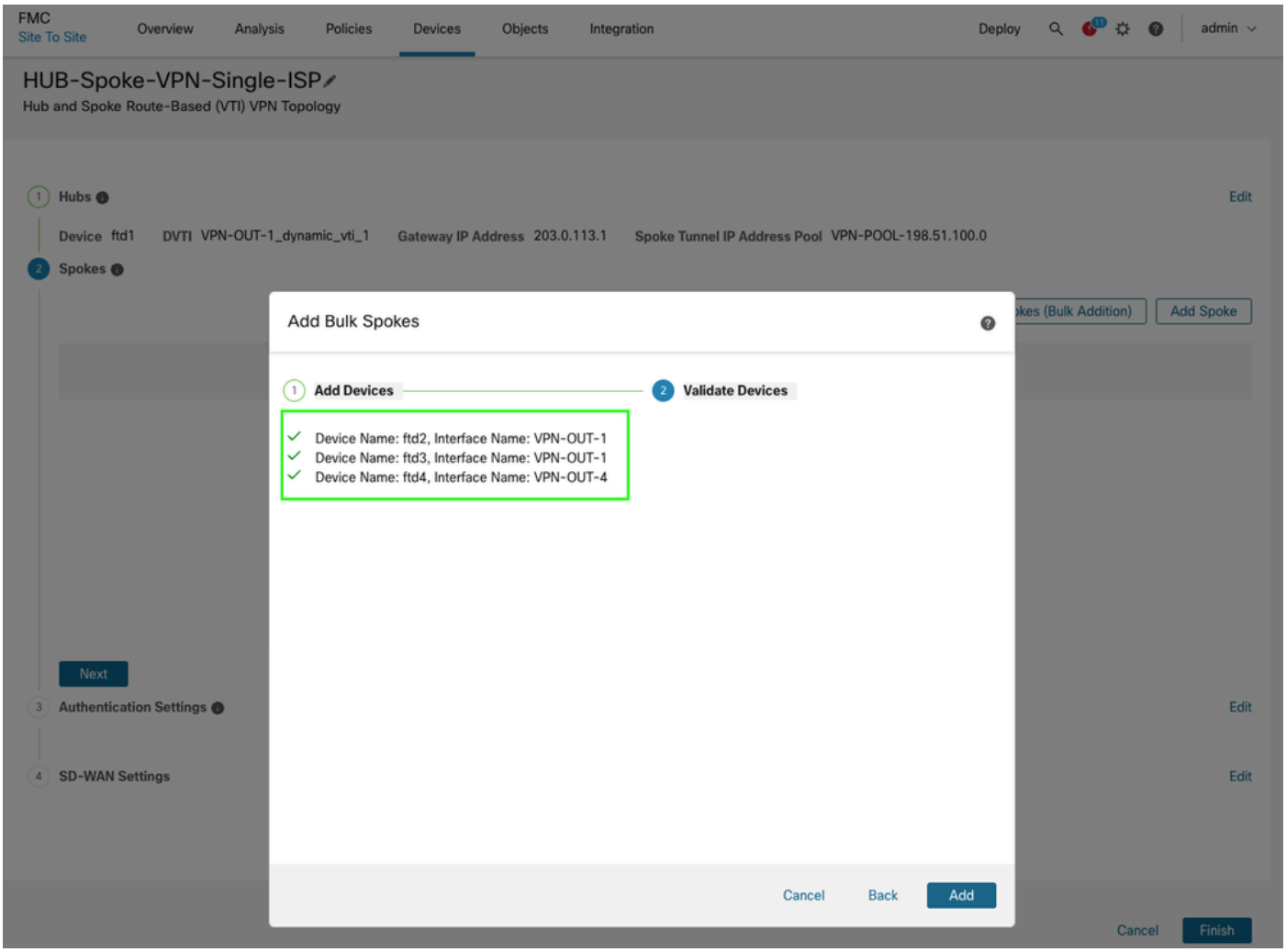
- Fare clic su Next (Avanti) per continuare e aggiungere i raggi. È possibile utilizzare entrambe le opzioni di aggiunta di massa se si dispone di nomi di interfaccia/zona comuni o se si

aggiungono i singoli raggi.

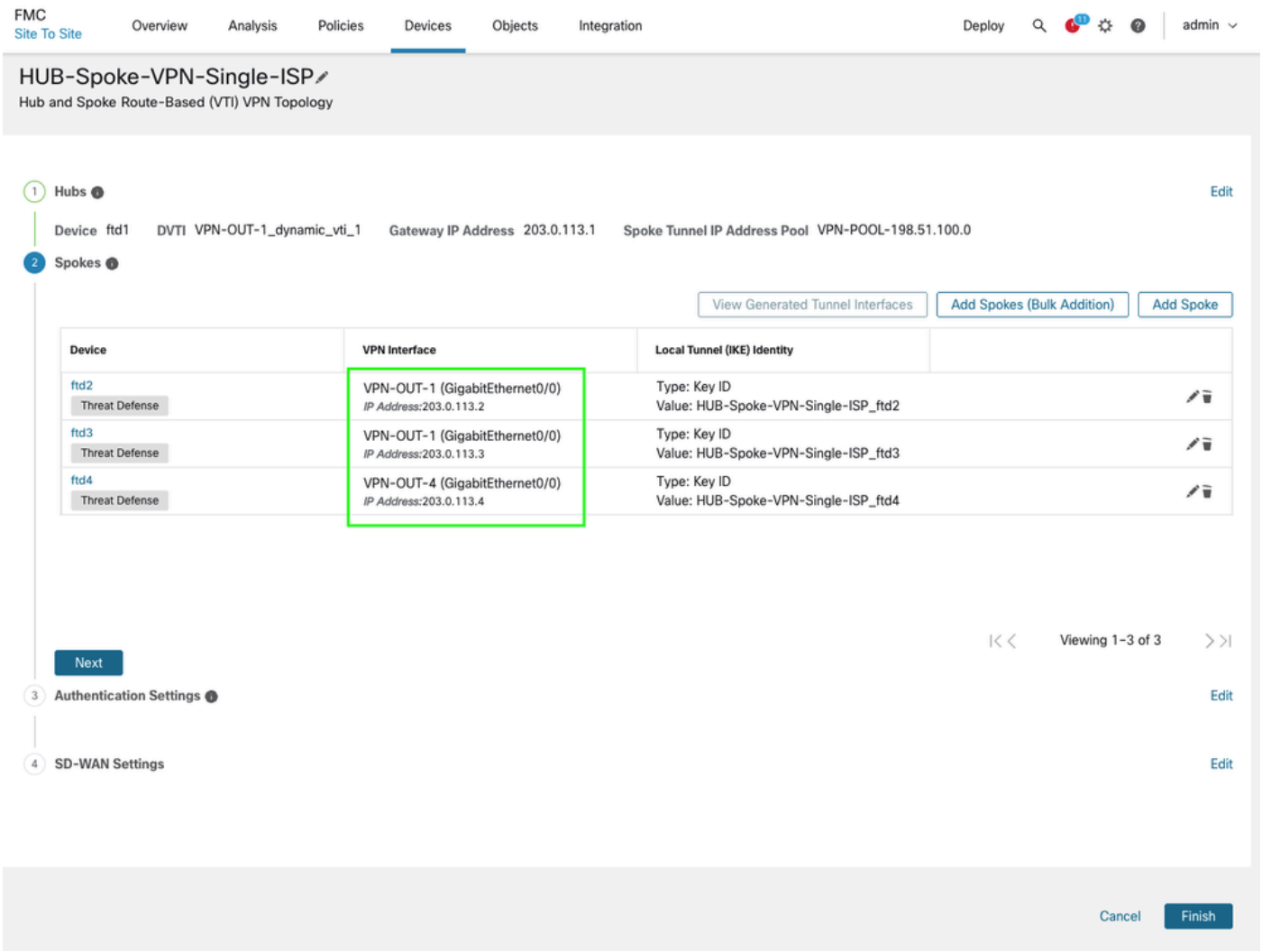


- Selezionare i dispositivi e specificare un modello di denominazione per l'interfaccia WAN/esterna. Se i dispositivi condividono lo stesso nome di interfaccia, è sufficiente utilizzare le iniziali. Fare clic su Avanti e, se la convalida ha esito positivo, fare clic su Aggiungi. Per le aggiunte di massa, potete utilizzare anche il nome della zona nello stesso modo.

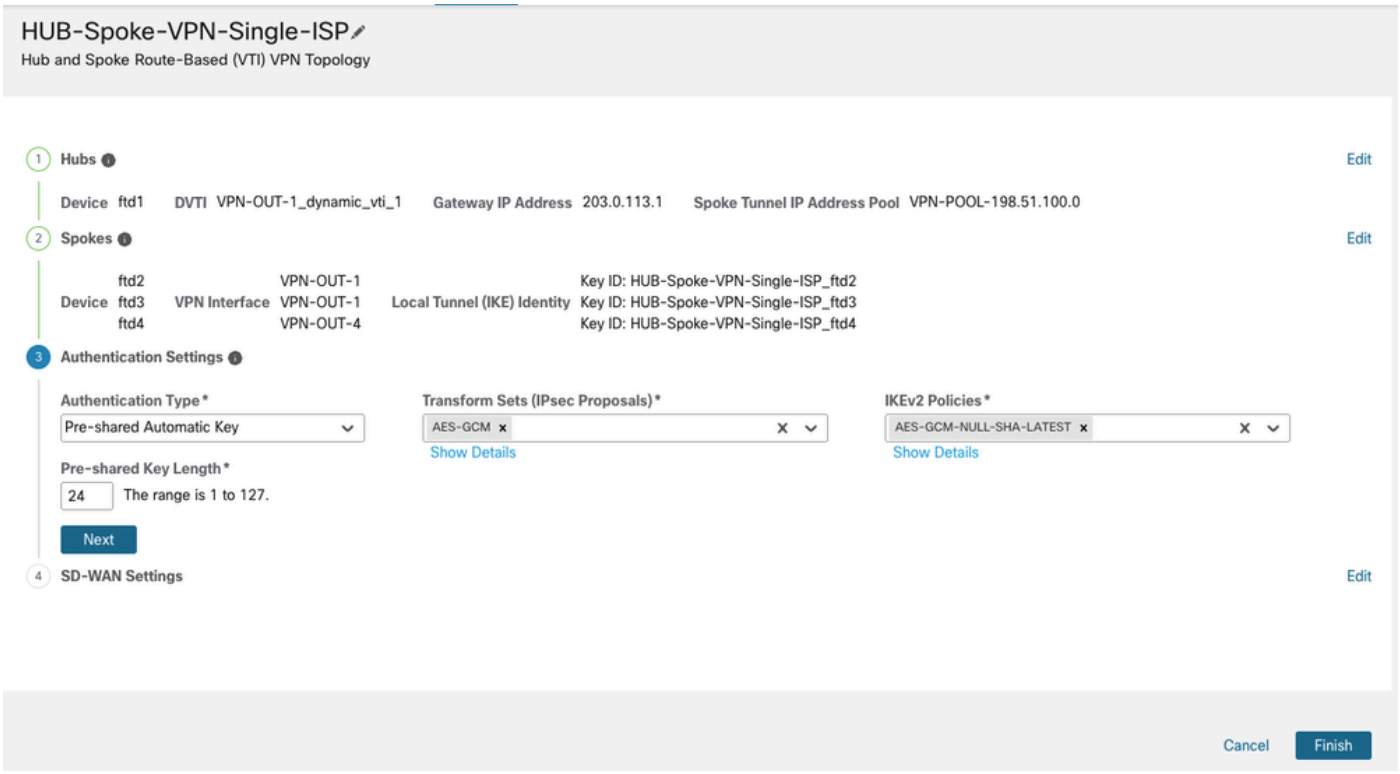

FMC
Site To Site
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
HUB-Spoke-VPN-Single-ISP
Hub and Spoke Route-Based (VTI) VPN Topology
1 Hubs
Edit
Device ftd1
DVTI VPN-OUT-1_dynamic_vti_1
Gateway IP Address 203.0.113.1
Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.0
2 Spokes
Add Spoke
Add Bulk Spokes
1 Add Devices
2 Validate Devices
Available Devices*
Search
Add
Remove
Selected Devices*
ftd2
ftd3
ftd4
Select VPN Interface Using*
Interface Name Pattern
out
Security Zone
Select...
Next
3 Authentication Settings
Edit
4 SD-WAN Settings
Edit
Cancel
Next
Cancel
Finish



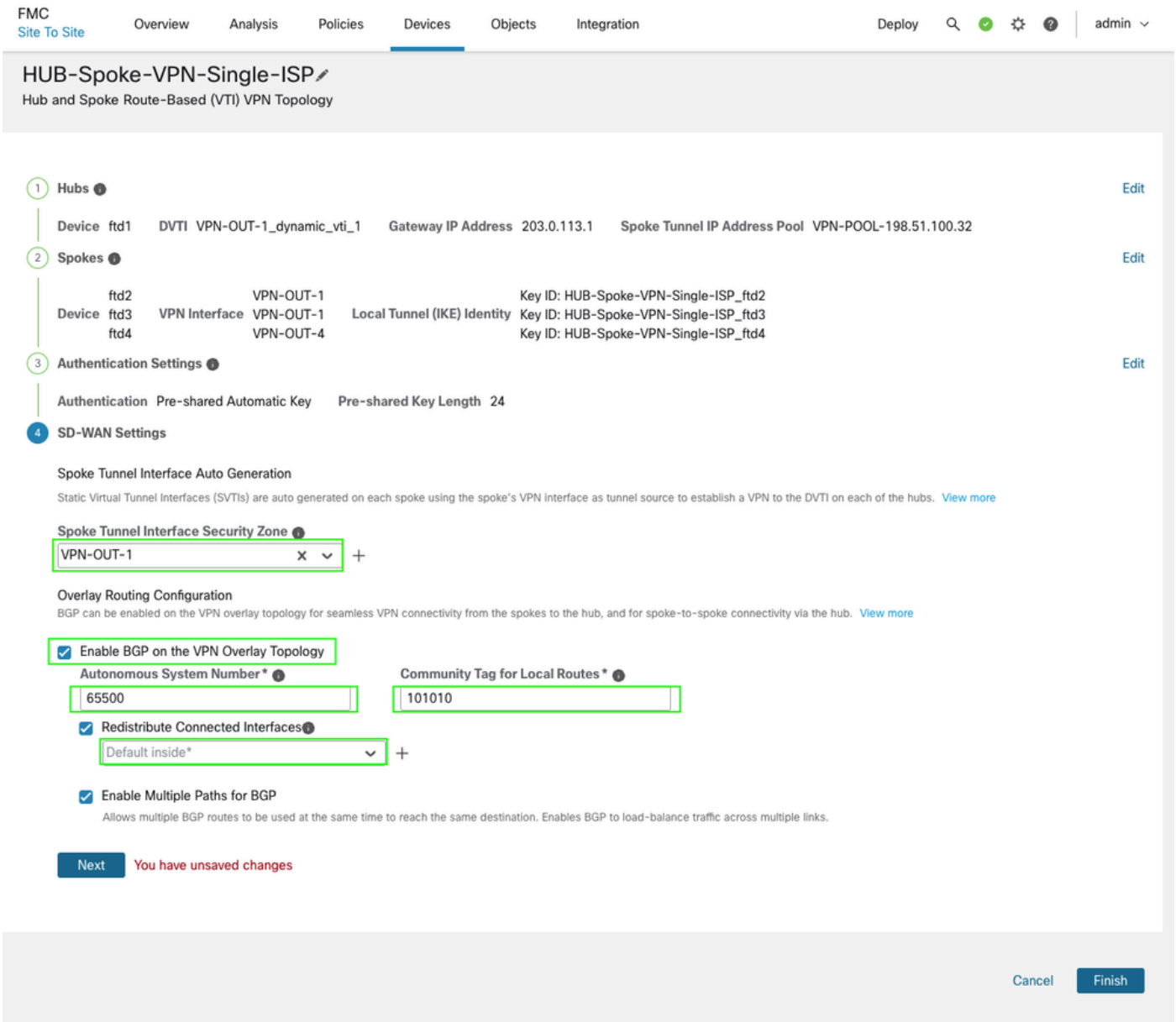
- Verificare i dettagli dell'interfaccia spoke e overlay per assicurarsi che siano selezionate le interfacce corrette, quindi fare clic su Next (Avanti).



- È possibile mantenere i parametri predefiniti per la configurazione IPSec o specificare cifrature personalizzate in base alle esigenze. Fare clic su Next (Avanti) per continuare. In questo documento vengono utilizzati i parametri predefiniti.



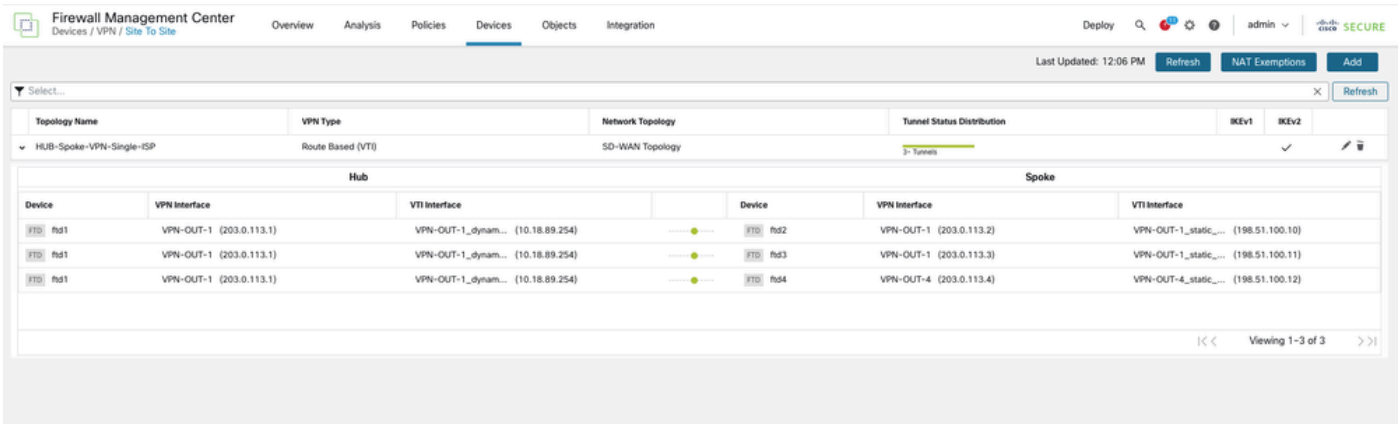
- Infine, è possibile configurare il routing di overlay all'interno della stessa procedura guidata per questa topologia specificando i parametri BGP appropriati, ad esempio il numero AS, l'annuncio dell'interfaccia interna e i tag della community per il filtro dei prefissi. L'area di sicurezza può essere utile per il filtro del traffico tramite i criteri di controllo di accesso, mentre è possibile creare un oggetto per le interfacce e utilizzarlo nella ridistribuzione delle interfacce connesse se il nome è diverso da quello interno o non è simmetrico tra i dispositivi nella topologia.



- Per completare il processo, fare clic su Avanti, quindi su Fine e infine su Distribuisci.

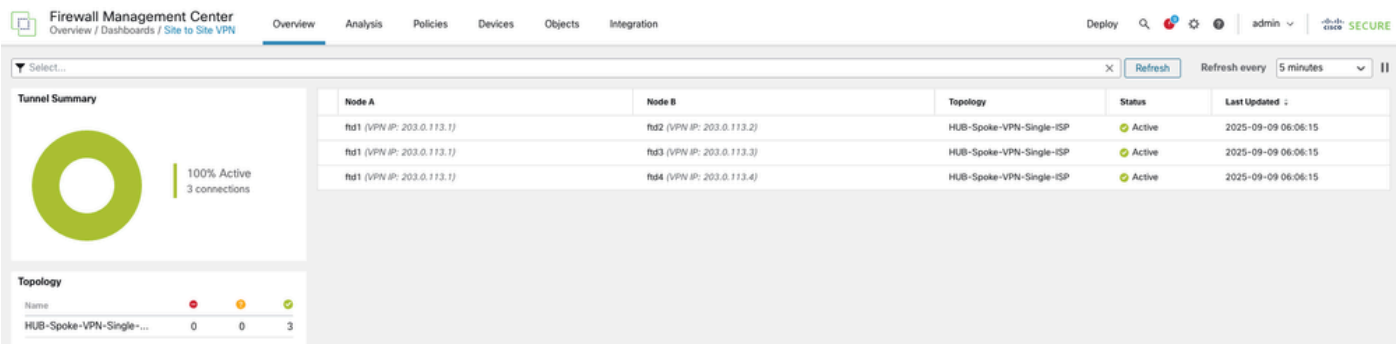
Verifica

- Per verificare lo stato del tunnel, selezionare Dispositivi > VPN > Sito in sito.

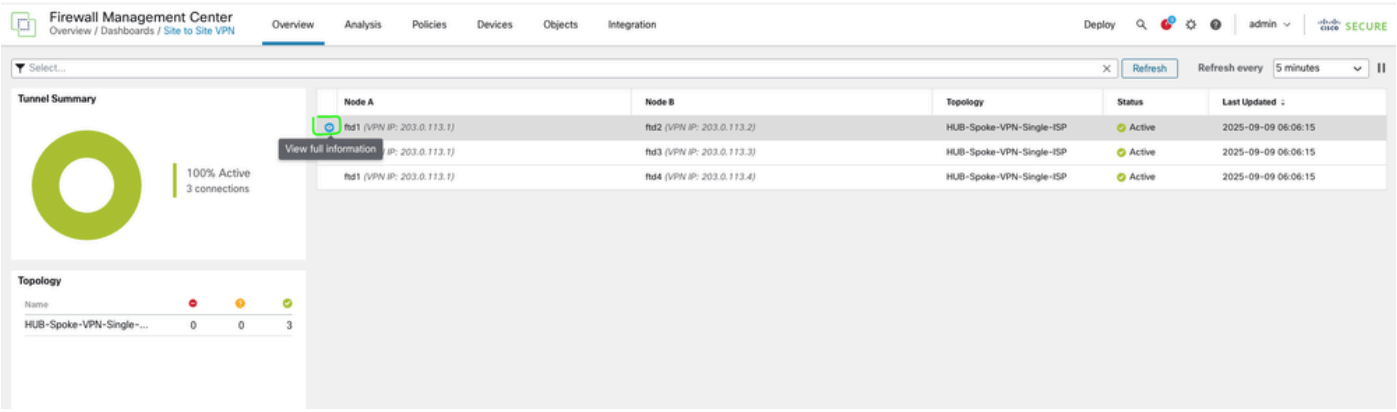


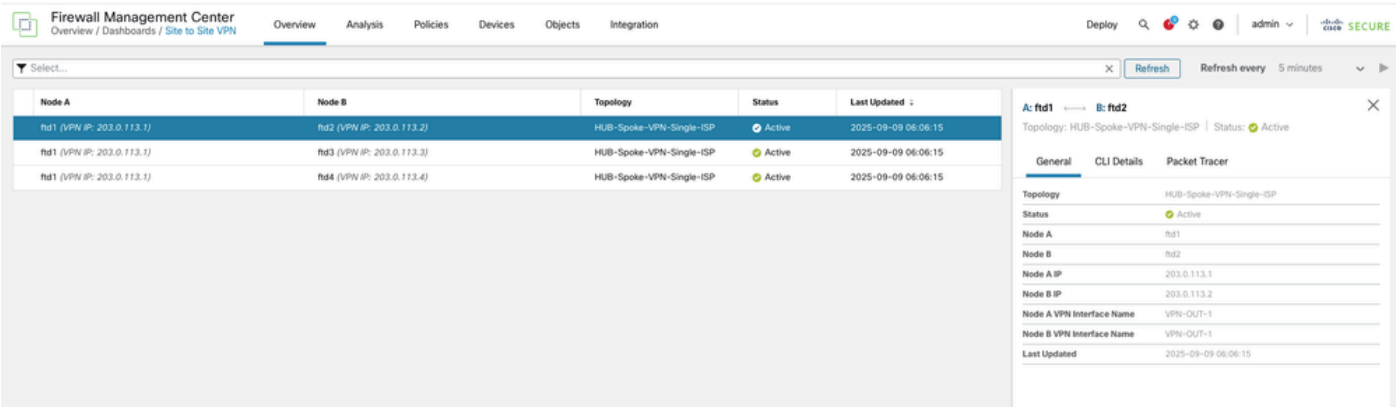
- È possibile verificare ulteriori dettagli selezionando Panoramica > Dashboard > VPN da sito

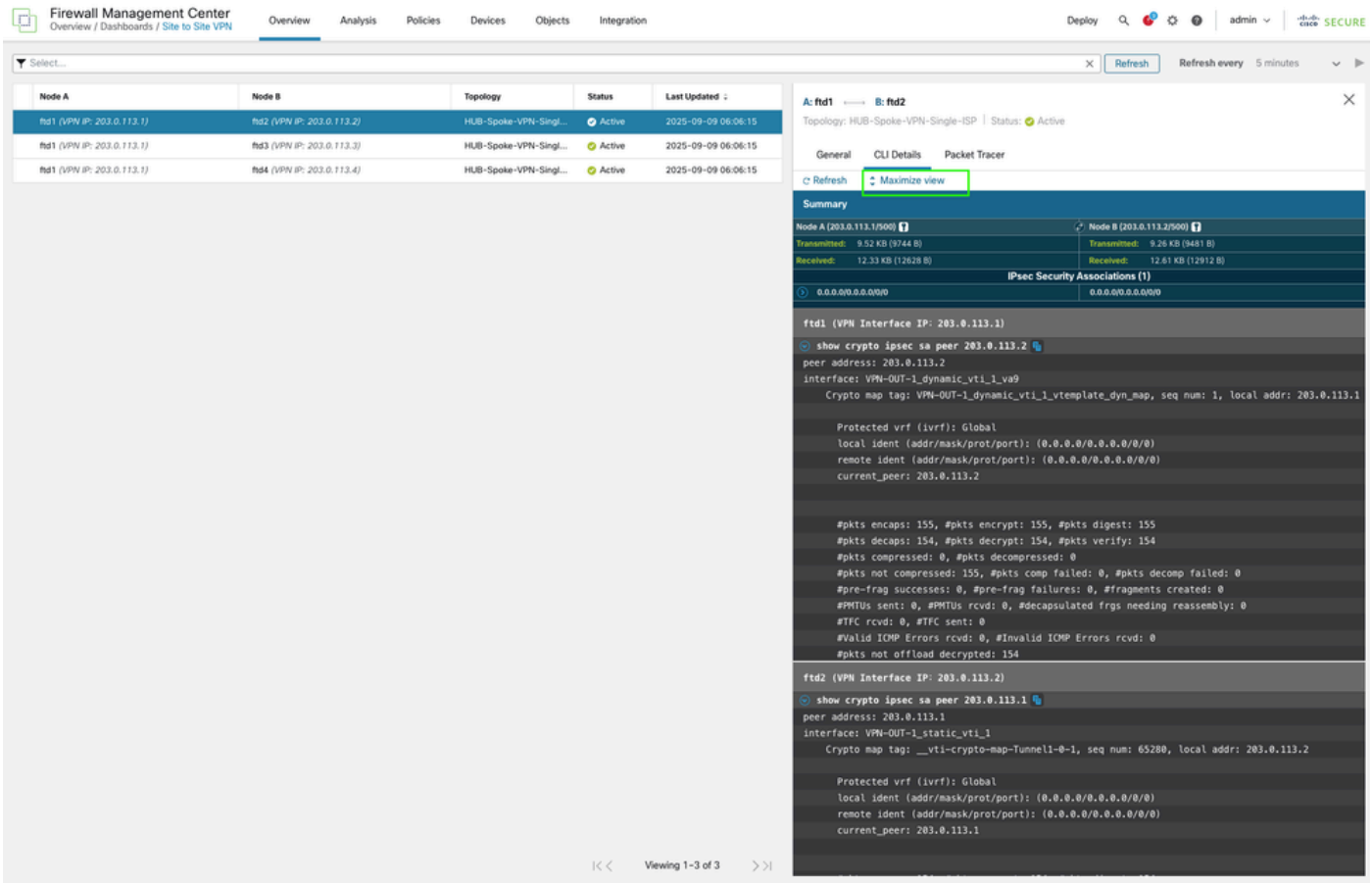
a sito.



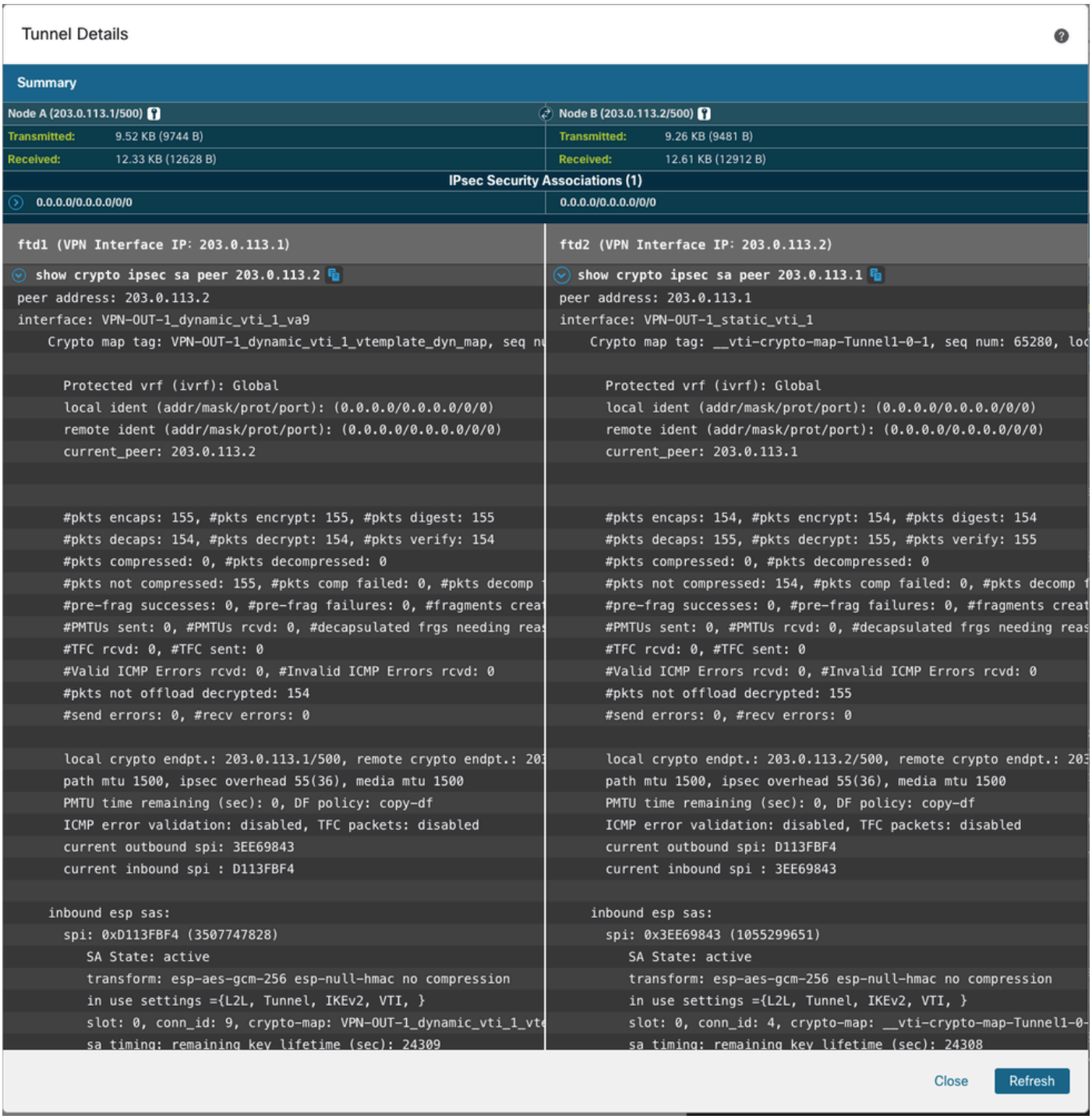
- Per ulteriori informazioni, selezionare il tunnel e fare clic su Visualizza informazioni complete.







- L'output viene visualizzato direttamente dalla CLI FTD e può essere aggiornato per visualizzare contatori aggiornati e informazioni importanti, quali i dettagli SPI (Security Parameter Index).



- La CLI di FTD può essere utilizzata anche per controllare le informazioni di routing e lo stato del peering BGP.

Sul lato dell'hub

<#root>

HUB1# show bgp summary

```
BGP router identifier 198.51.100.3, local AS number 65500
BGP table version is 7, main routing table version 7
2 network entries using 400 bytes of memory
2 path entries using 160 bytes of memory
```

```
1/1 BGP path/bestpath attribute entries using 208 bytes of memory
1 BGP community entries using 24 bytes of memory
1 BGP route-map cache entries using 64 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 856 total bytes of memory
BGP activity 2/0 prefixes, 4/2 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
198.51.100.10   4        65500 4       6              7    0    0 00:00:45  0
```

<<<<< spoke 1 bgp peering

```
198.51.100.11   4        65500 5       5              7    0    0 00:00:44  1
```

<<<<< spoke 2 bgp peering

```
198.51.100.12   4        65500 5       5              7    0    0 00:00:52  1
```

<<<<< spoke 3 bgp peering

<#root>

HUB1# show route bgp

```
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

B        192.0.2.0 255.255.255.248 [200/1] via 198.51.100.10, 00:00:18
```

<<<<<<<< spoke 1 inside network

```
B        192.0.2.8 255.255.255.248 [200/1] via 198.51.100.11, 00:08:08
```

<<<<<<<< spoke 2 inside network

```
B        192.0.2.16 255.255.255.248 [200/1] via 198.51.100.12, 00:08:16
```

<<<<<<<< spoke 3 inside network

<#root>

HUB1#show bgp ipv4 unicast neighbors 198.51.100.10 routes

<<<<< to check only prefix receieved from specific peer

```
BGP table version is 14, local router ID is 198.51.100.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop        Metric LocPrf Weight  Path
*>i192.0.2.0/29     198.51.100.10        1    100      0  ?
```

<<<<<<<<<< routes received from spoke 1

```
Total number of prefixes 1
```

<#root>

HUB1#show bgp ipv4 unicast neighbors 198.51.100.11 routes

<<<<< to check only prefix receieved from specific peer

```
BGP table version is 14, local router ID is 198.51.100.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop        Metric LocPrf Weight  Path
*>i192.0.2.8/29     198.51.100.11        1    100      0  ?
```

<<<<<<<<<< routes received from spoke 2

```
Total number of prefixes 1
```

<#root>

HUB1#show bgp ipv4 unicast neighbors 198.51.100.12 routes

<<<<< to check only prefix receieved from specific peer

```
BGP table version is 14, local router ID is 198.51.100.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop        Metric LocPrf Weight  Path
*>i192.0.2.16/29    198.51.100.12        1    100      0  ?
```

<<<<<<<<<< routes received from spoke 3

```
Total number of prefixes 1
```

Su lato raggio

La stessa verifica può essere eseguita anche sui dispositivi spoke. Ecco un esempio da uno dei raggi.

<#root>

Spoke1# show bgp summary

```
BGP router identifier 198.51.100.4, local AS number 65500
BGP table version is 12, main routing table version 12
3 network entries using 600 bytes of memory
3 path entries using 240 bytes of memory
2/2 BGP path/bestpath attribute entries using 416 bytes of memory
2 BGP rrinfo entries using 80 bytes of memory
1 BGP community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1360 total bytes of memory
BGP activity 5/2 prefixes, 7/4 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
198.51.100.1    4        65500 12      11            12    0    0 00:07:11  2
```

<<<<<<<<< BGP peering with HUB

<#root>

Spoke1# show bgp ipv4 unicast neighbors 198.51.100.1 routes

```
BGP table version is 12, local router ID is 198.51.100.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop        Metric LocPrf Weight  Path
*>i192.0.2.8/29     198.51.100.1         1    100      0  ?
```

<<<<<<< route received from HUB for spoke 2

```
*>i192.0.2.16/29    198.51.100.1         1    100      0  ?
```

<<<<<<< route received from HUB for spoke 3

```
Total number of prefixes 2
```

<#root>

Spoke1# show bgp ipv4 unicast neighbors 198.51.100.1 advertised-routes

```
BGP table version is 12, local router ID is 198.51.100.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop        Metric LocPrf Weight  Path
*> 192.0.2.0/29     0.0.0.0              0         32768  ?
```

<<<<<<<< route advertised by this spoke into BGP

```
Total number of prefixes 1
```

<#root>

Spoke1# show route bgp

```
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

B        192.0.2.8 255.255.255.248 [200/1] via 198.51.100.1, 00:13:42
```

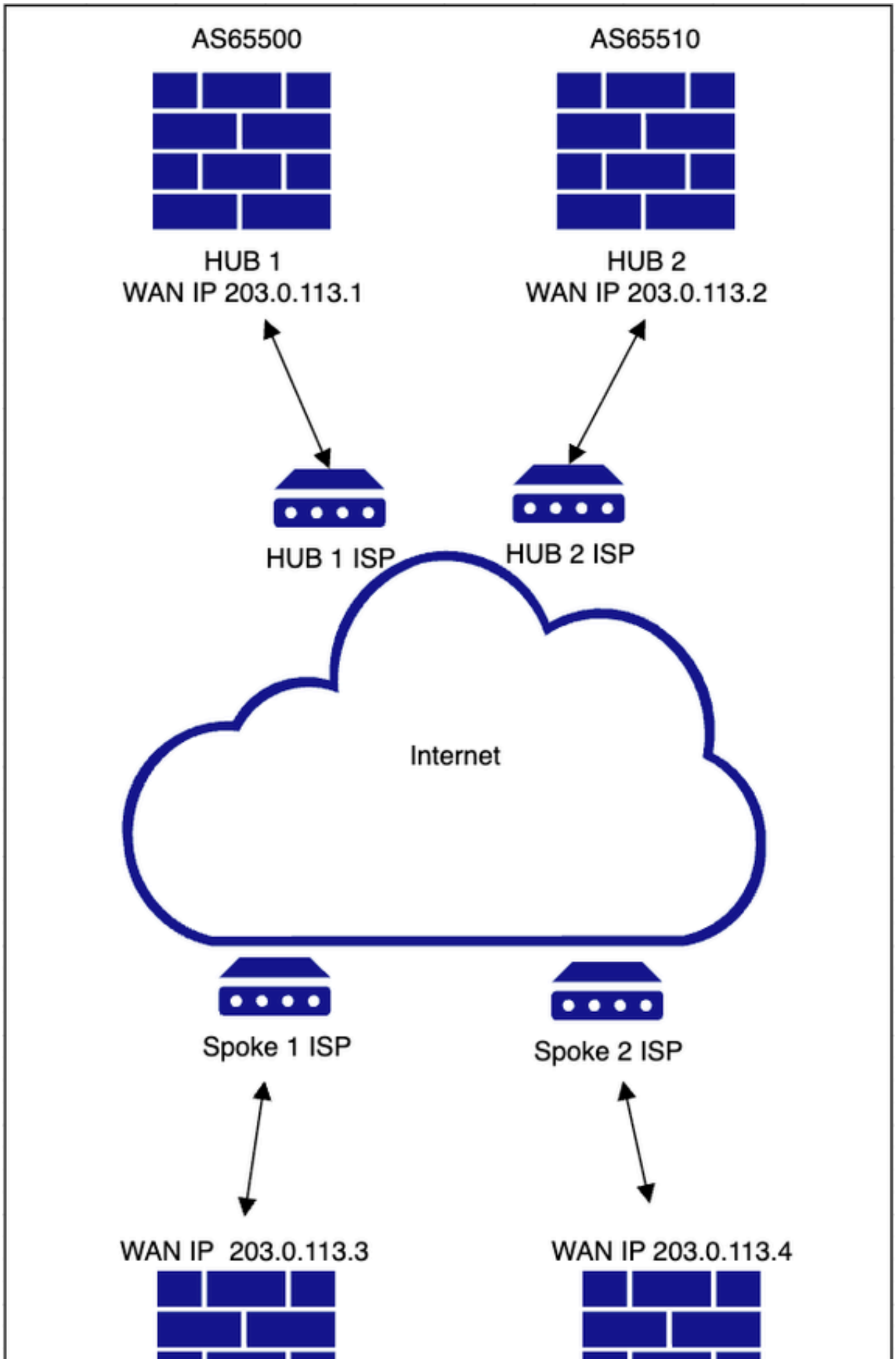
<<<<<< spoke 2 inside network

```
B        192.0.2.16 255.255.255.248 [200/1] via 198.51.100.1, 00:13:42
```

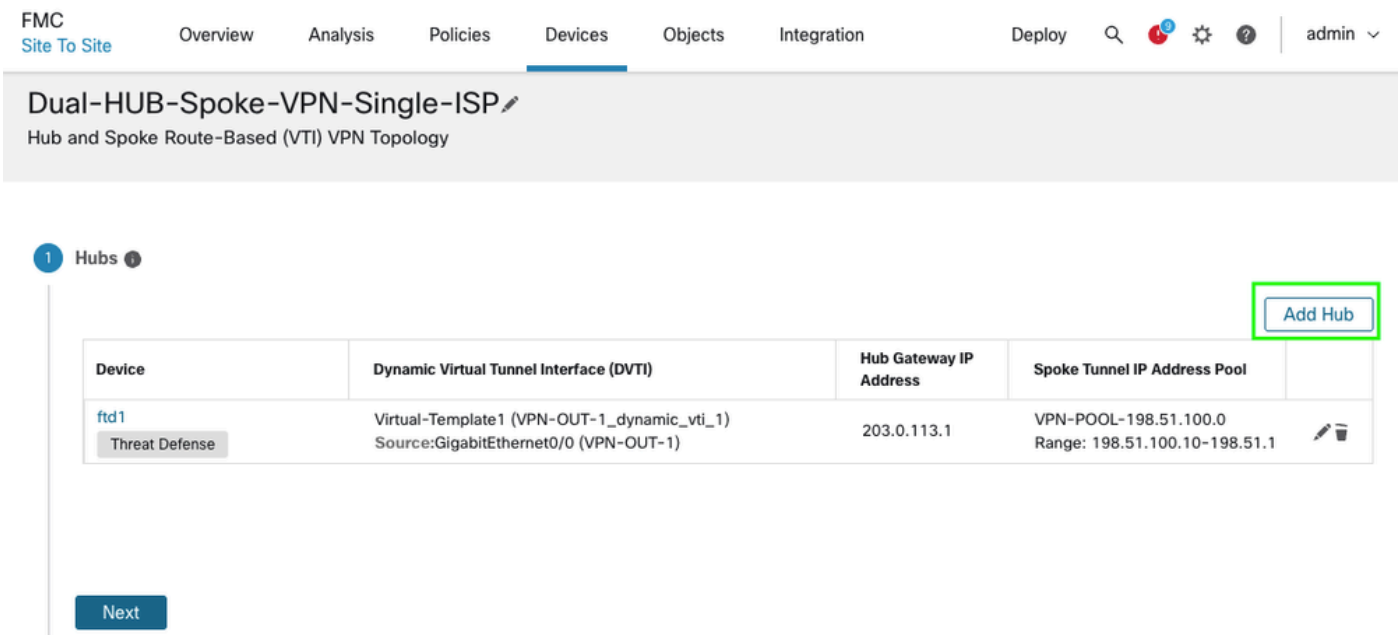
<<<<<< spoke 3 inside network

Due hub e spoke (ISP singolo per hub ridondante tramite EBGP tra hub secondario e spoke)

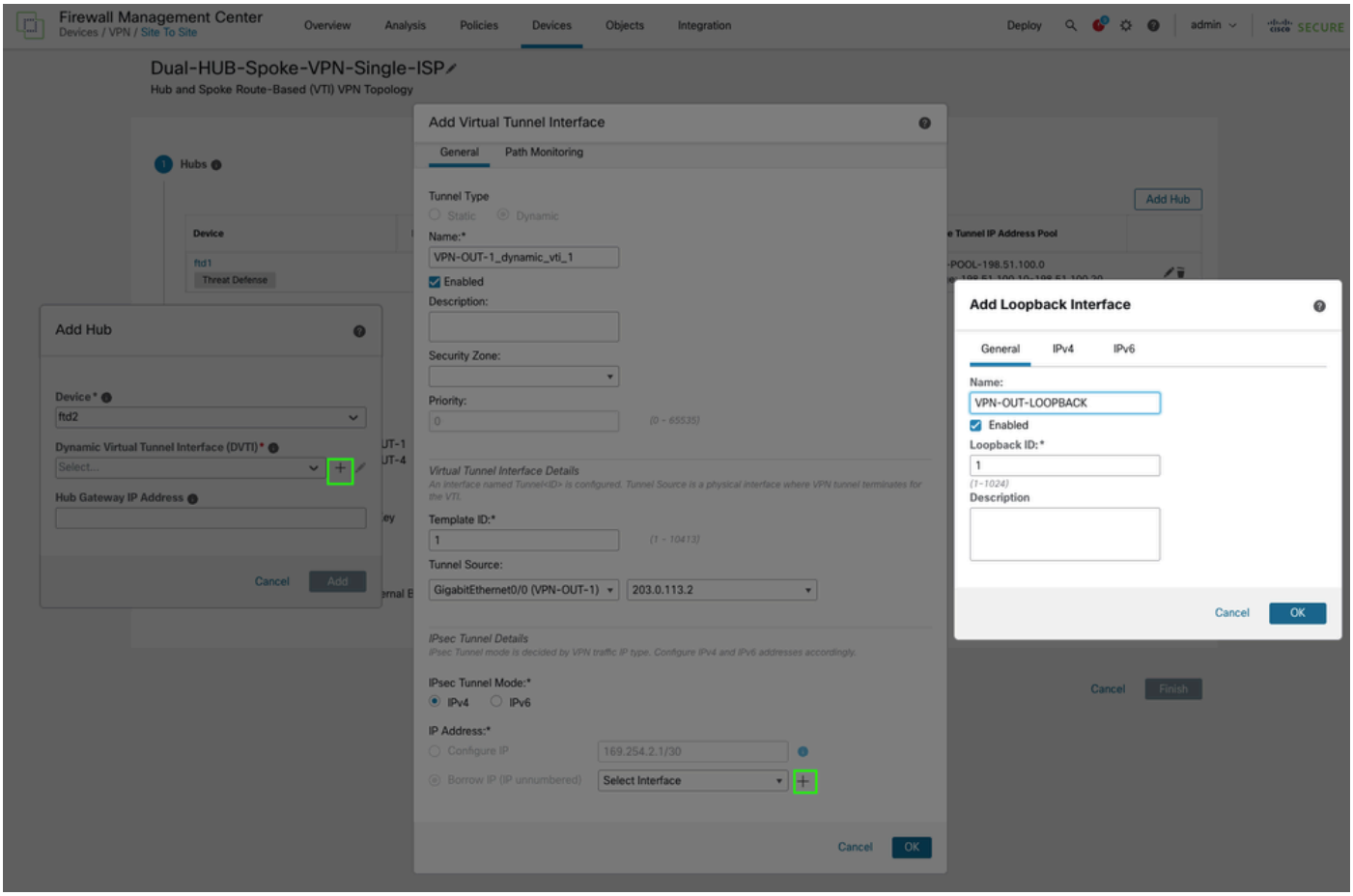
Esempio di rete


AS65500
AS65510
HUB 1
WAN IP 203.0.113.1
HUB 2
WAN IP 203.0.113.2
HUB 1 ISP
HUB 2 ISP
Internet
Spoke 1 ISP
Spoke 2 ISP
WAN IP 203.0.113.3
WAN IP 203.0.113.4

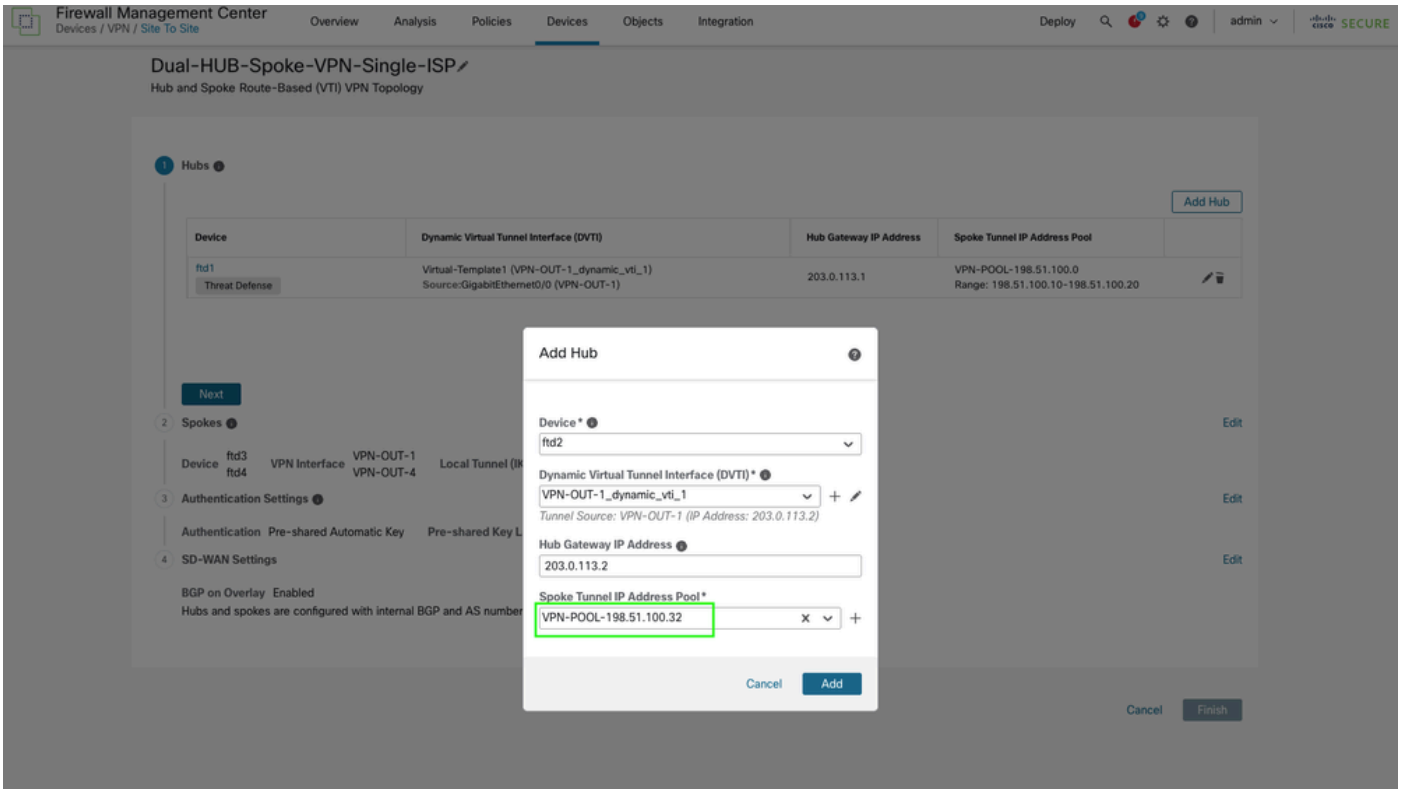
Dopo aver aggiunto il primo HUB, procedere con l'aggiunta del secondo HUB seguendo la stessa procedura utilizzata in precedenza per HUB1.

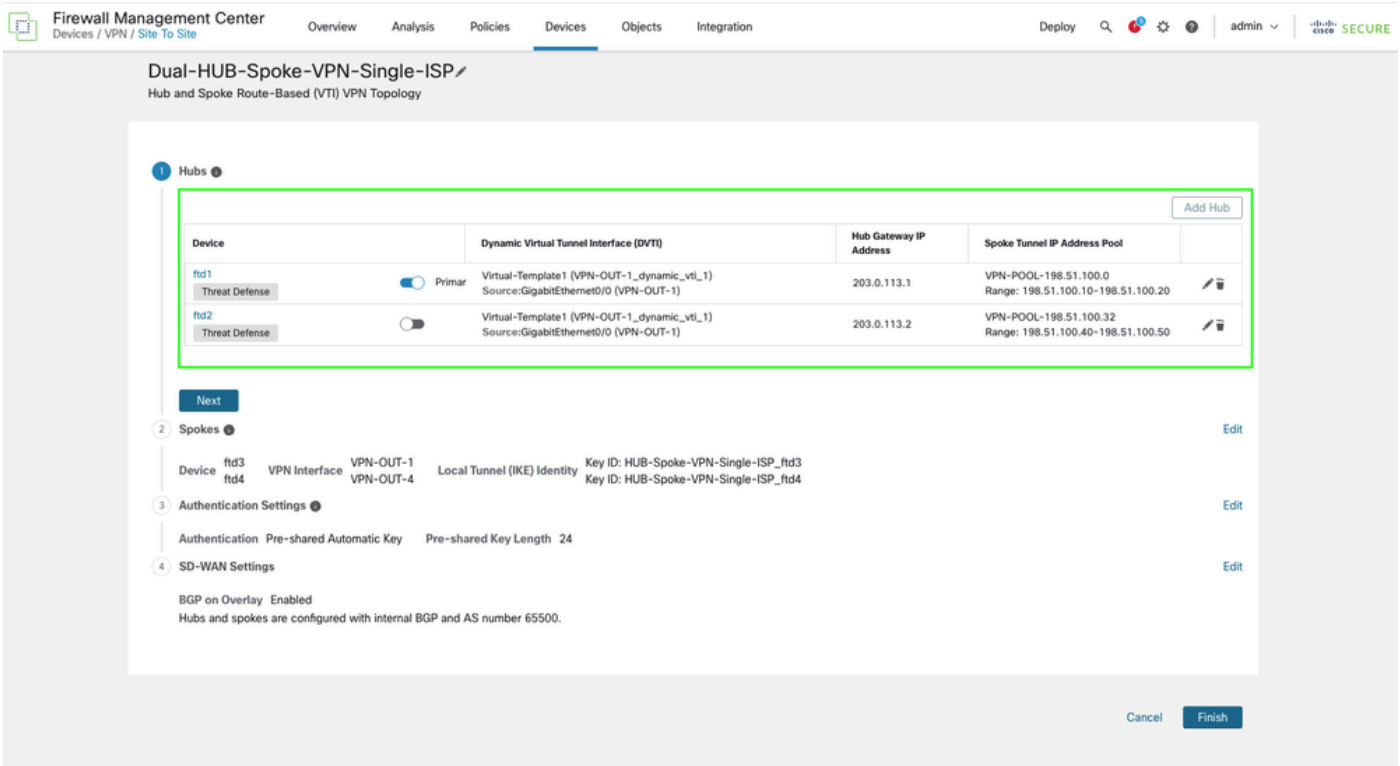


- Continuare con la creazione della DVTI (Dynamic Virtual Tunnel Interface).

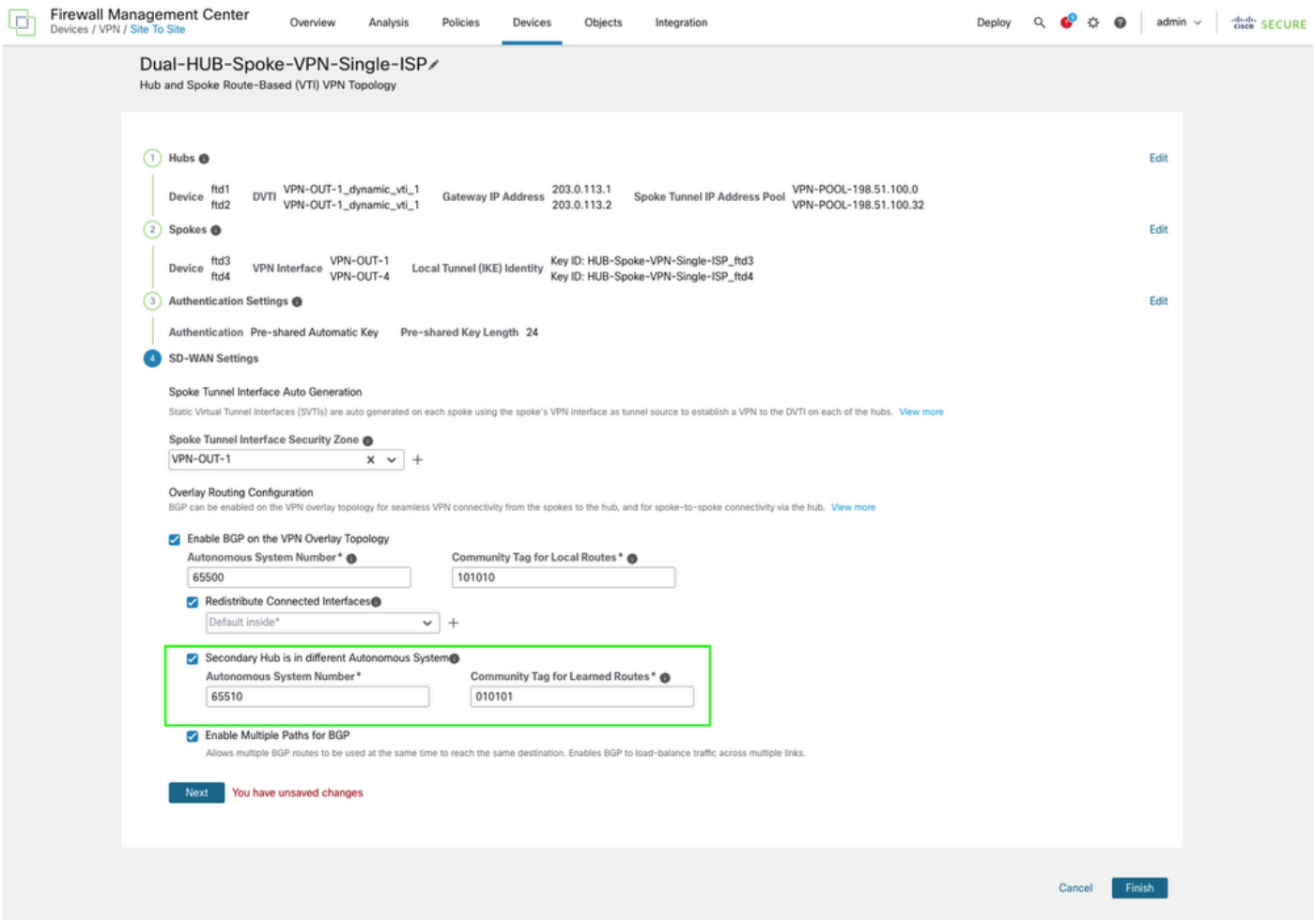


- È necessario un nuovo pool di indirizzi IP per i tunnel VTI HUB 2 sul lato spoke. Creare e configurare il nuovo pool, quindi salvare le modifiche.





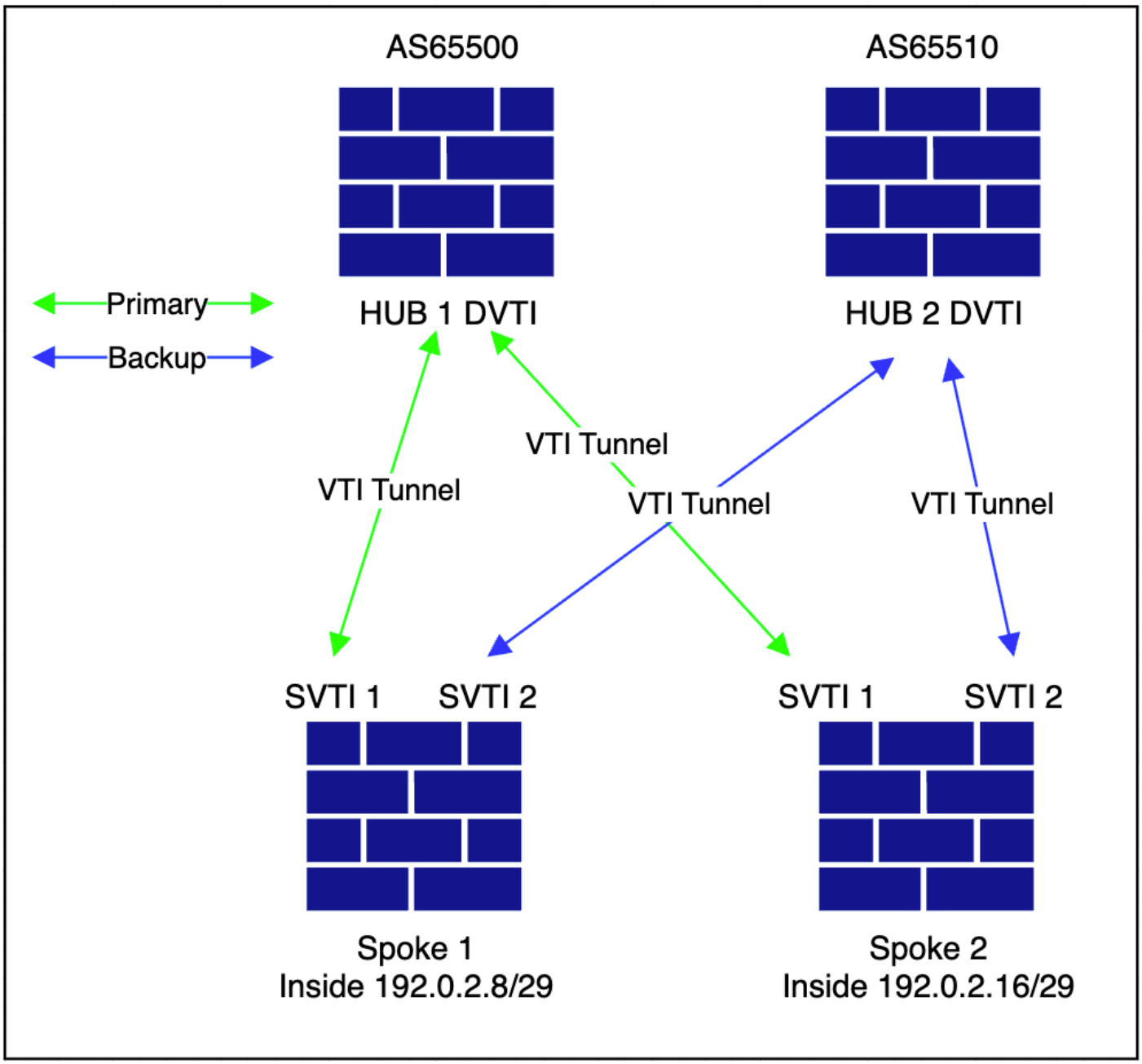
- Per configurare il peering eBGP tra il secondo HUB e gli spoke, modificare le impostazioni SD-WAN nel passaggio finale. Abilitare l'opzione L'hub secondario si trova in un sistema autonomo diverso e specificare il numero del sistema autonomo (AS) per l'hub secondario. È inoltre possibile utilizzare IBGP se non vi sono limitazioni all'uso di un numero AS diverso nell'ambiente, lasciando deselezionata l'opzione Hub secondario in un sistema autonomo diverso. In questo modo, viene inviato lo stesso tag community e lo stesso numero AS anche per l'hub secondario. L'articolo è incentrato su eBGP per la configurazione corrente.



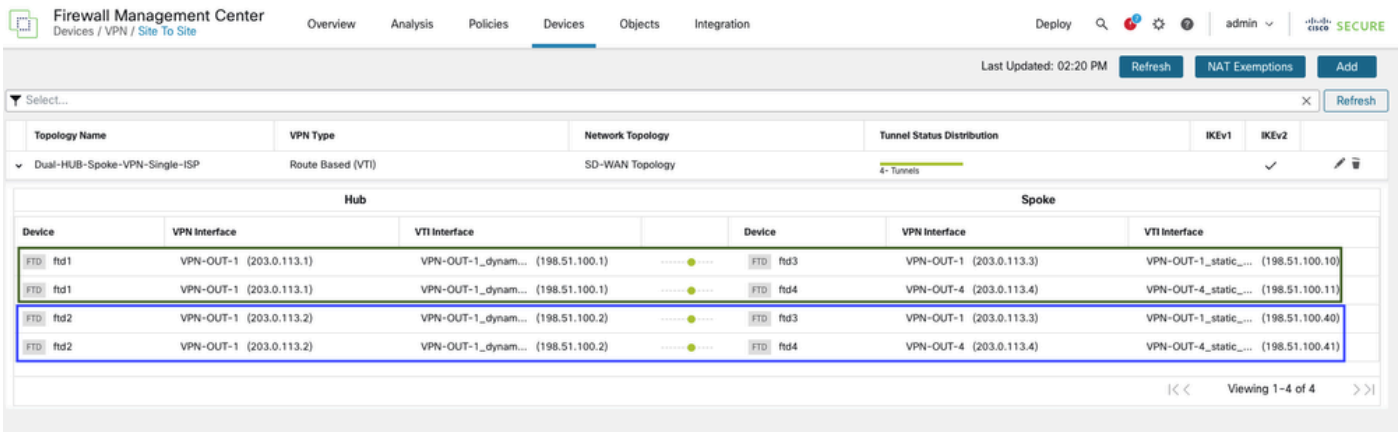
Verificare che il numero Autonomous System (AS) e il tag community siano univoci in questa configurazione.

Verifica

Il diagramma mostra la topologia di sovrapposizione.



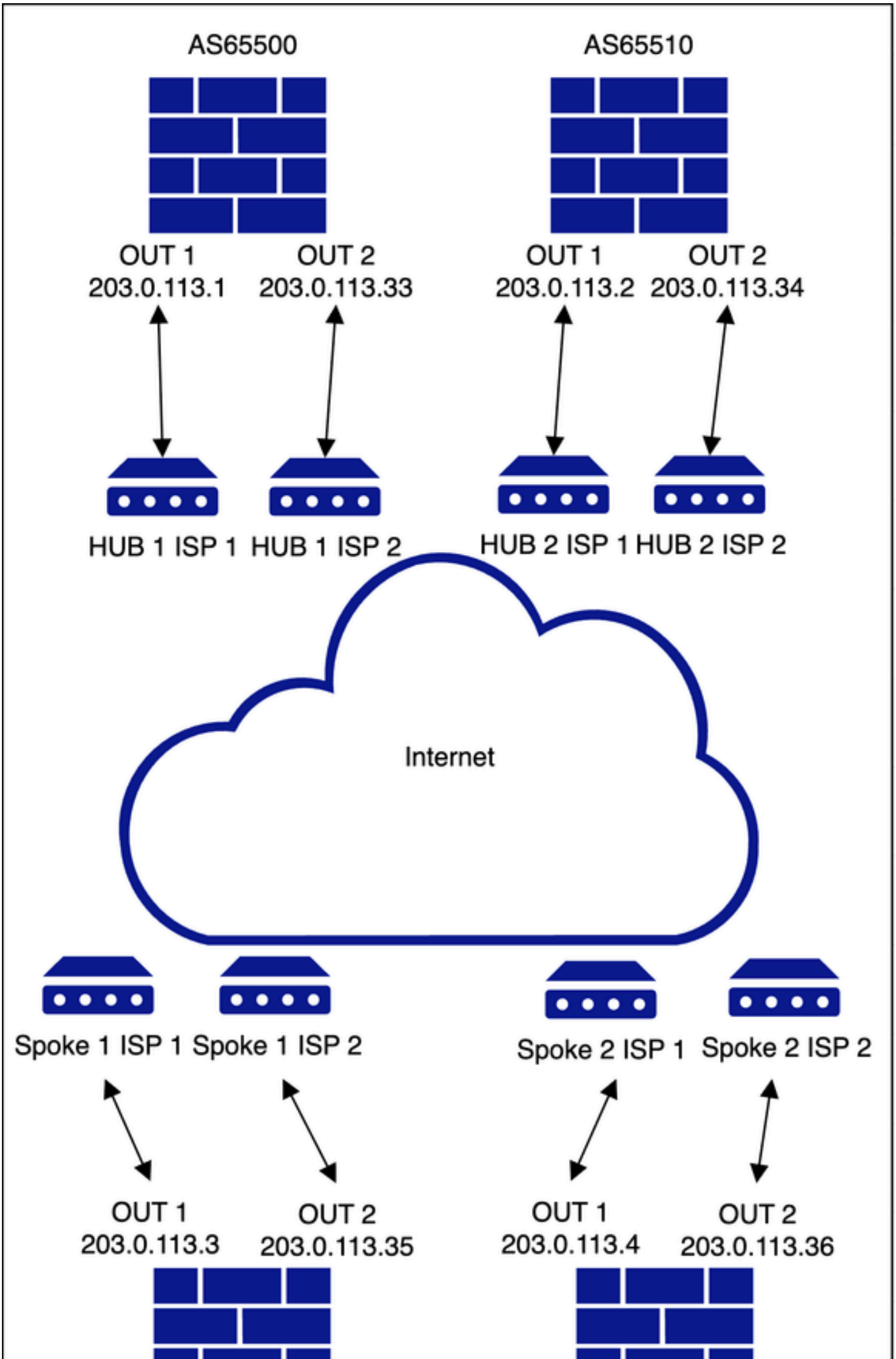
- Nel FMC, selezionare Devices > VPN > Site to Site (Dispositivi > VPN > Da sito a sito).



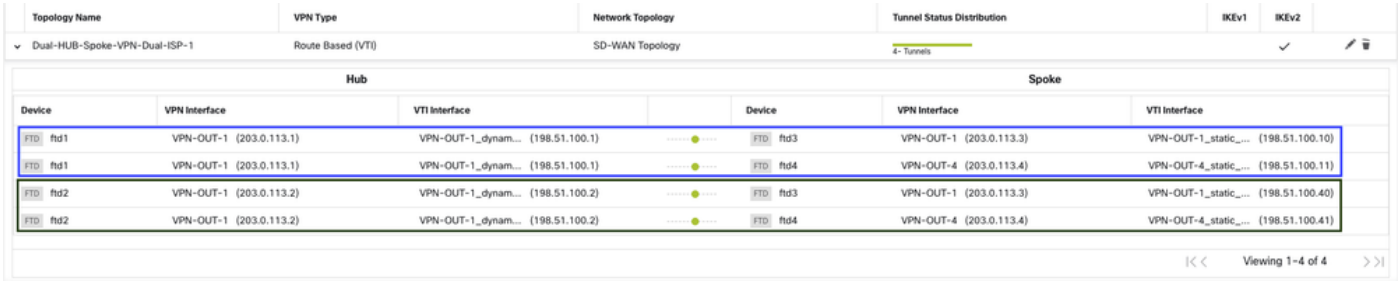
- Tutti gli altri passaggi rimangono invariati.

Hub e spoke doppi (ISP doppio per hub e ISP ridondanti tramite EBGP tra hub e spoke secondari)

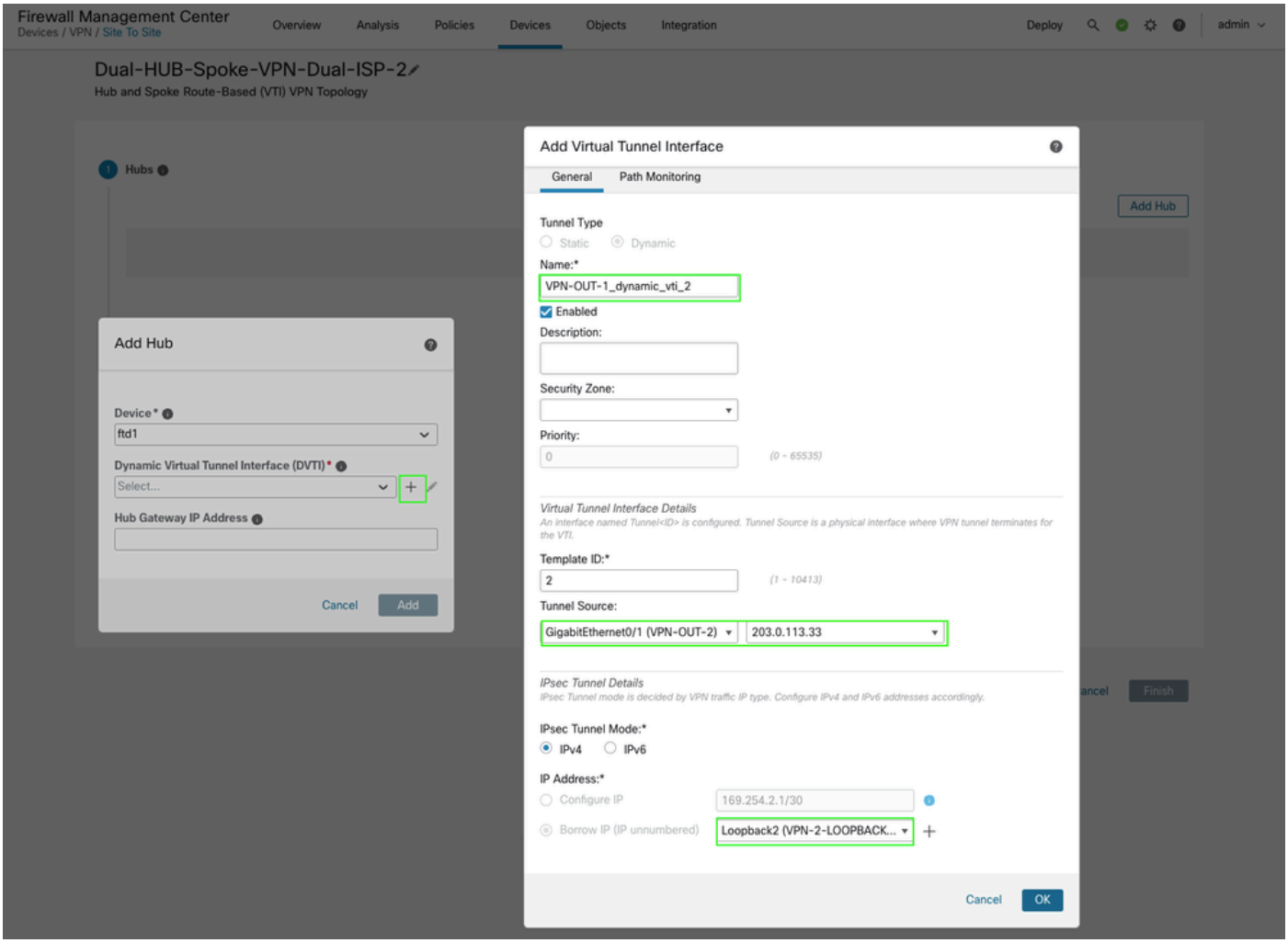
Esempio di rete


AS65500
AS65510
OUT 1
203.0.113.1
OUT 2
203.0.113.33
OUT 1
203.0.113.2
OUT 2
203.0.113.34
HUB 1 ISP 1
HUB 1 ISP 2
HUB 2 ISP 1
HUB 2 ISP 2
Internet
Spoke 1 ISP 1
Spoke 1 ISP 2
Spoke 2 ISP 1
Spoke 2 ISP 2
OUT 1
203.0.113.3
OUT 2
203.0.113.35
OUT 1
203.0.113.4
OUT 2
203.0.113.36

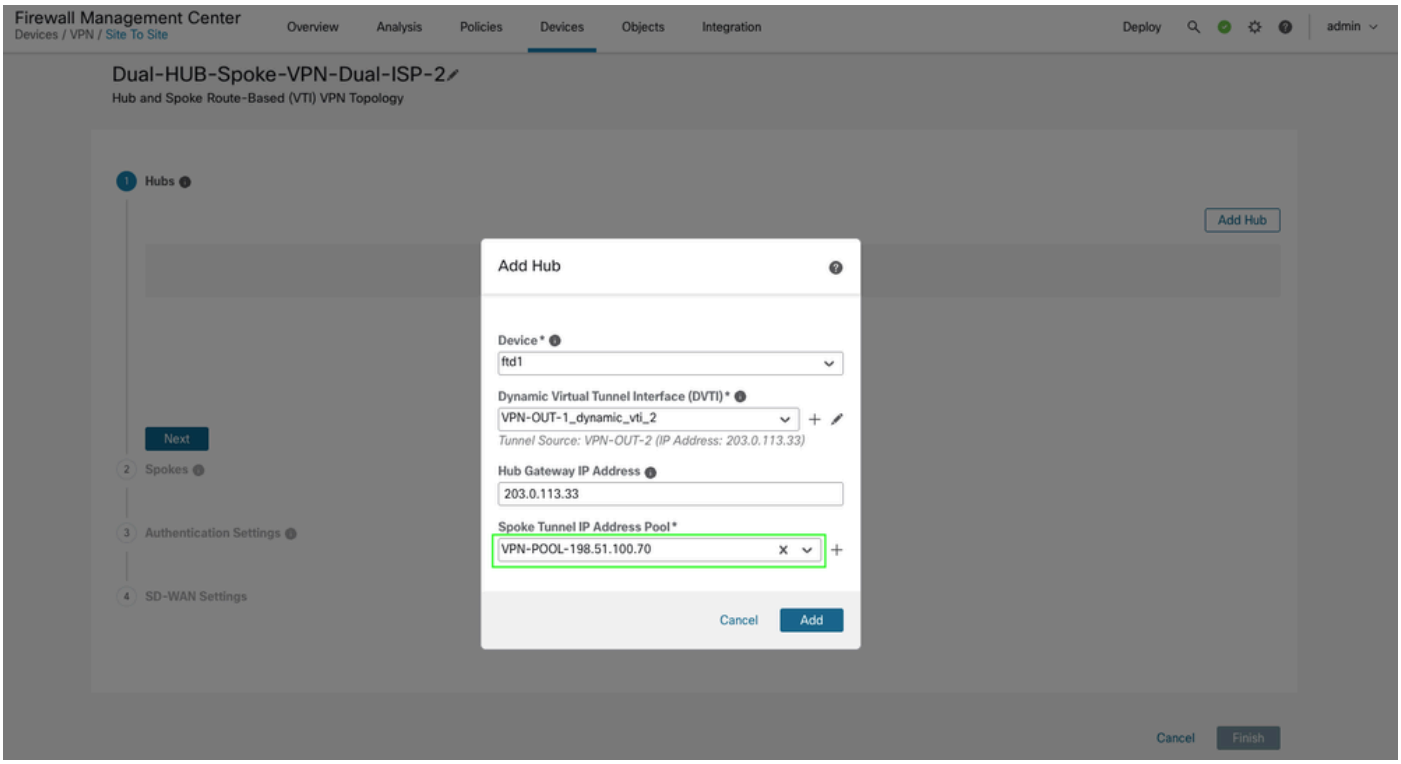
La distribuzione per questa topologia viene ignorata utilizzando il primo ISP, poiché tale argomento è trattato nella topologia precedente.

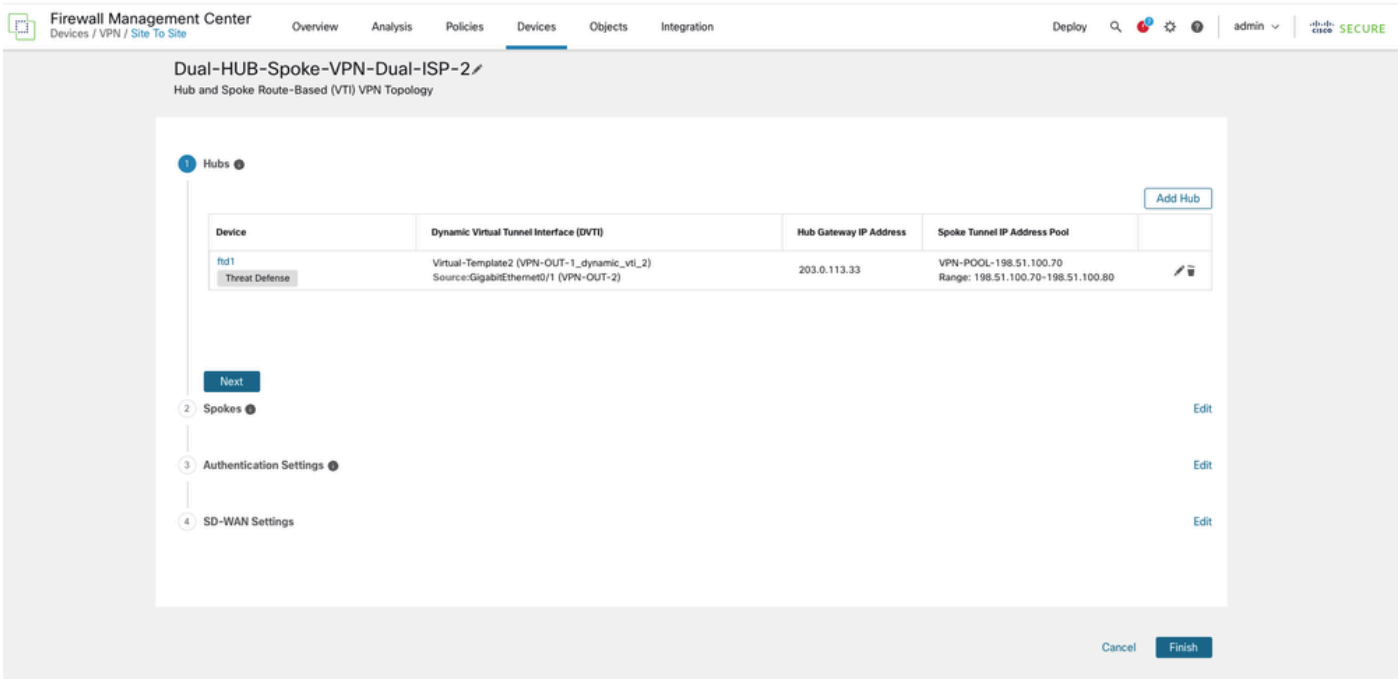


- Quindi, procedere all'aggiunta della seconda topologia creando due interfacce DVTI aggiuntive per HUB, ciascuna utilizzando l'interfaccia sottostante per ISP 2 (VPN-OUT-2).

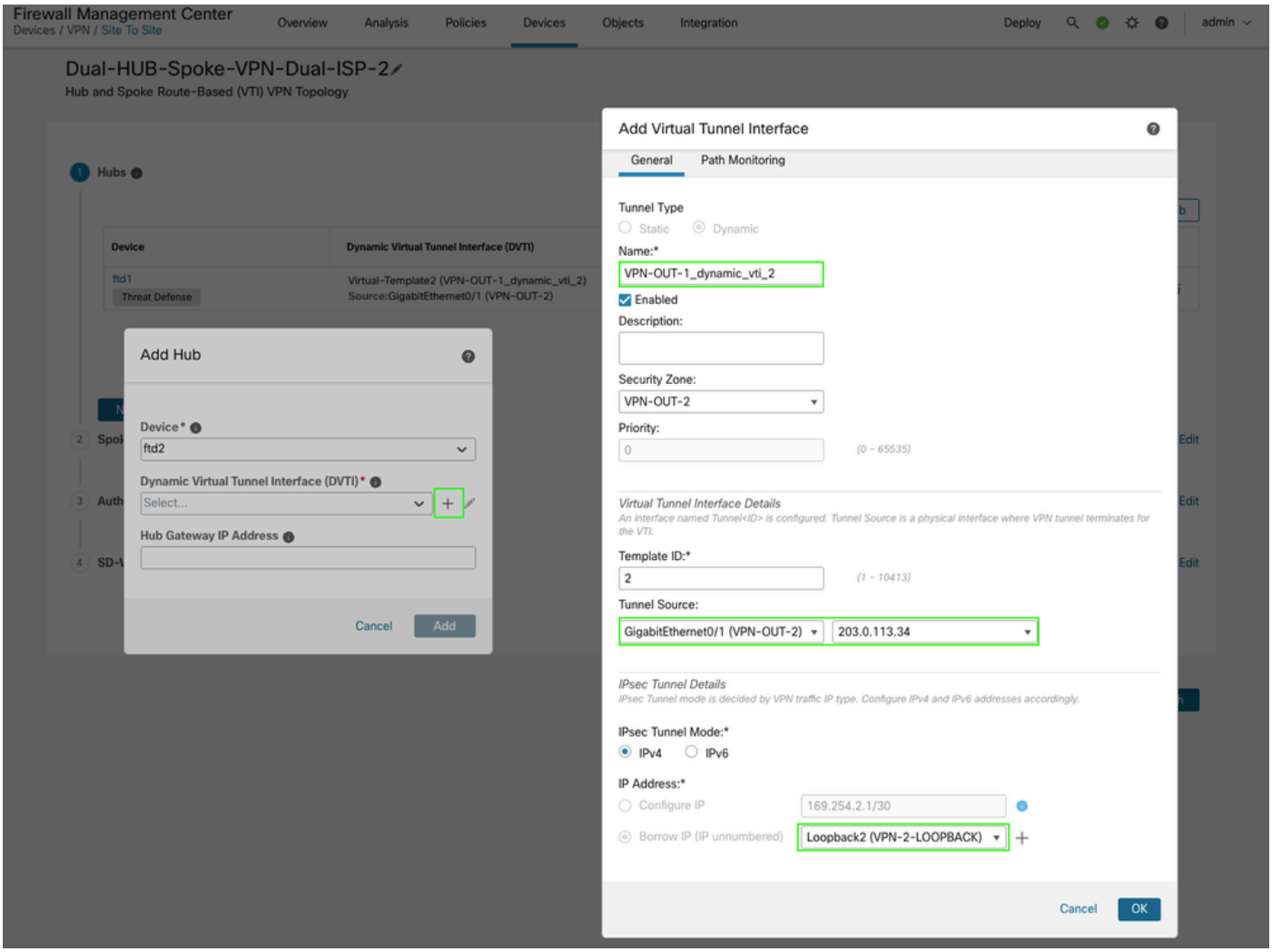


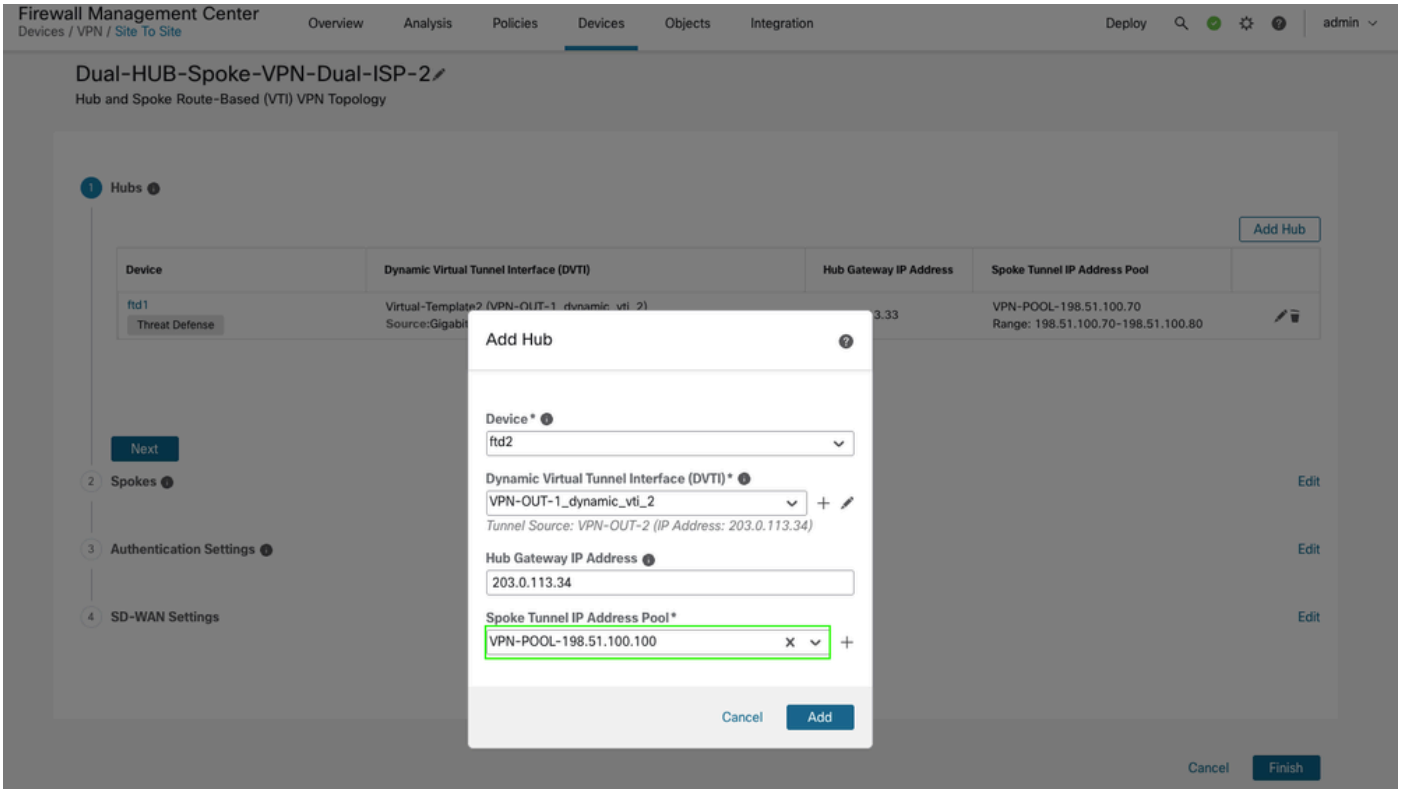
- È stato effettuato il provisioning di un pool di indirizzi IP VPN aggiuntivo specifico per gli indirizzi VTI (Virtual Tunnel Interface) spoke.



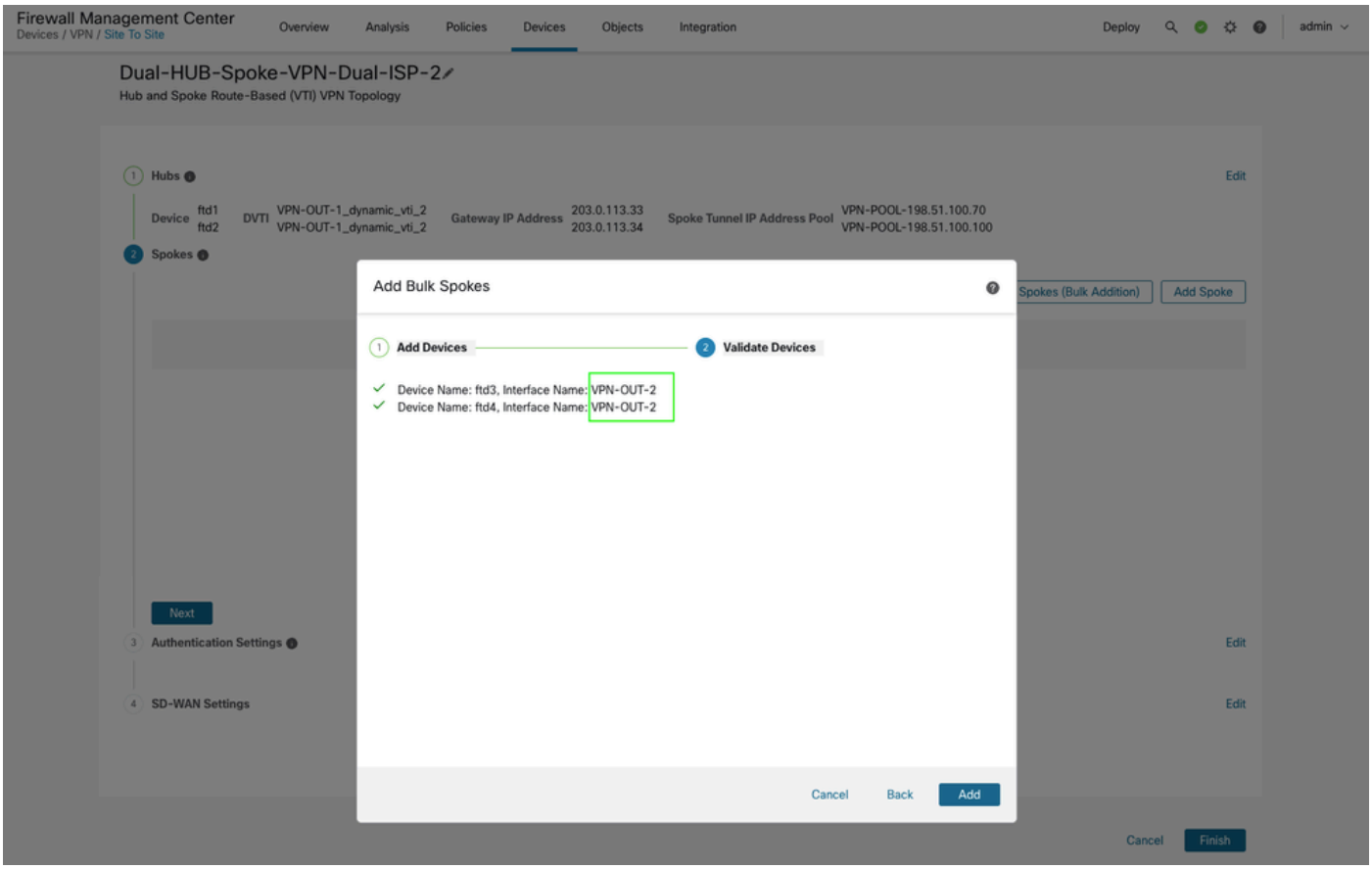


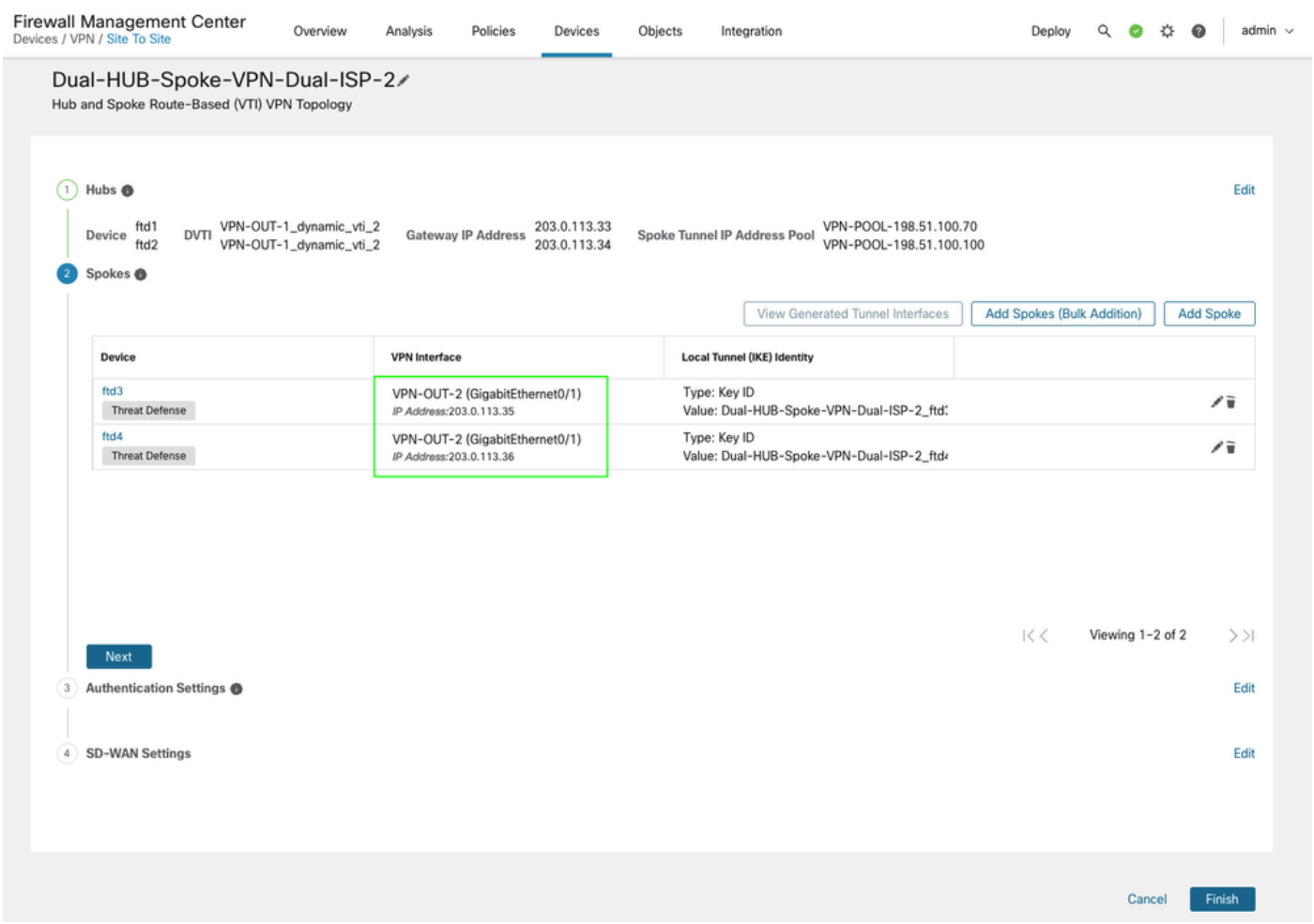
- Per aggiungere un hub secondario, ripetere il processo creando DVTI 2 utilizzando l'interfaccia ISP secondaria (VPN-OUT-2) e configurare un pool IP aggiuntivo per gli indirizzi VTI spoke-end.





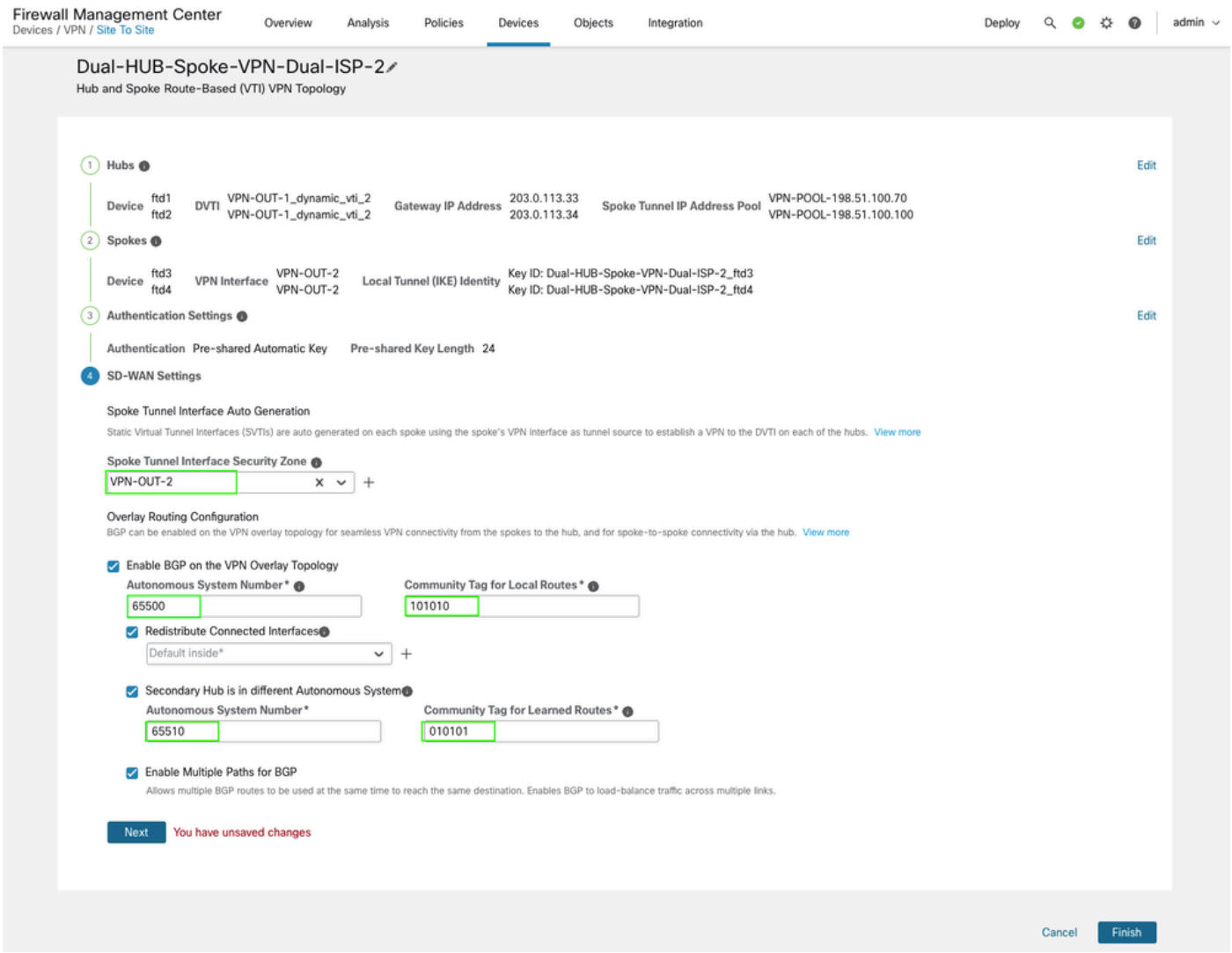
- Quando si aggiunge uno spoke, accertarsi che sia specificata l'interfaccia WAN/underlay corretta per i tunnel VTI. Questa topologia utilizza l'interfaccia ISP secondaria VPN-OUT-2.





- Quando si configura il routing, verificare che i tag della community e i numeri AS per

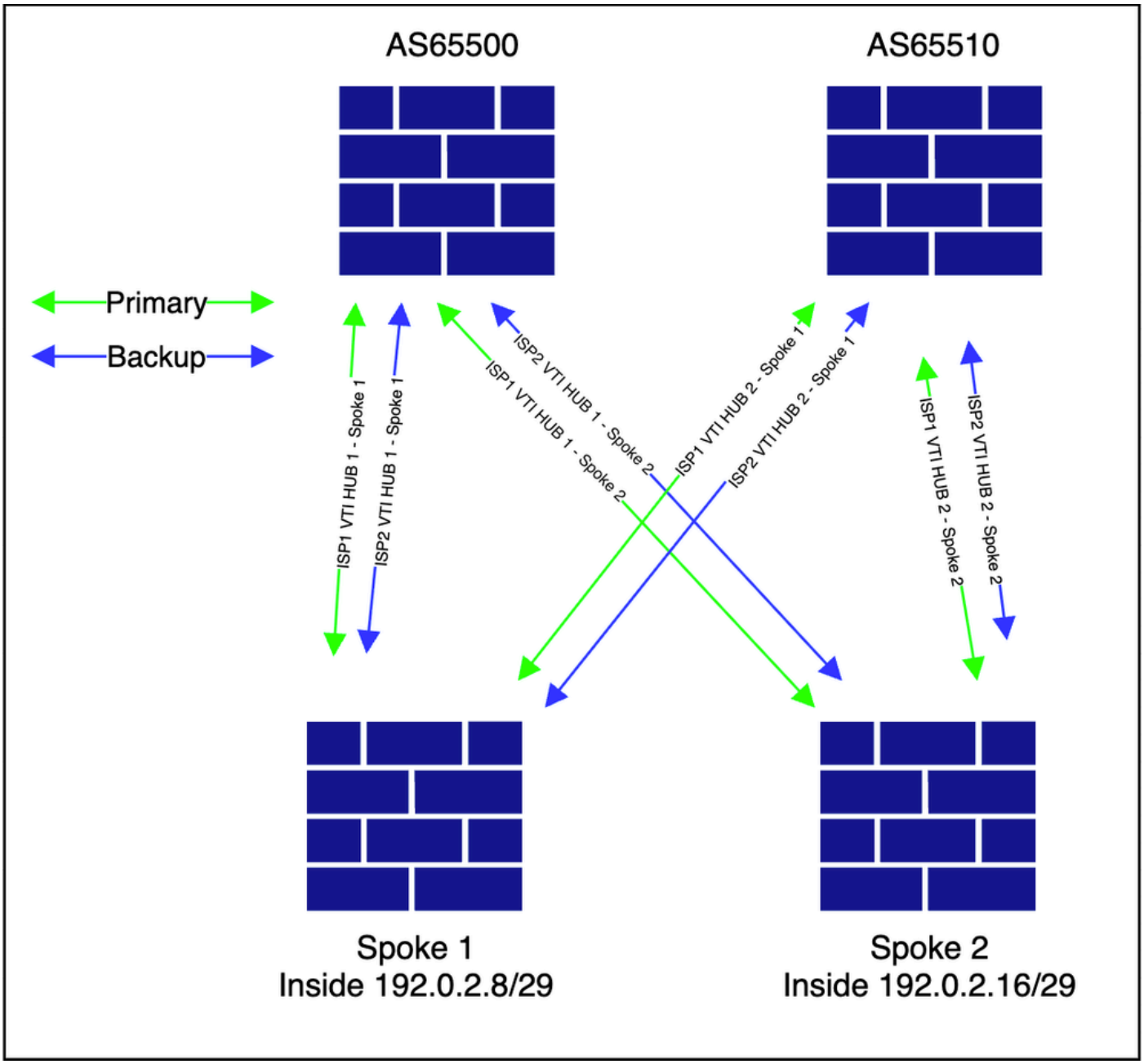
entrambi gli HUB in questa topologia siano coerenti con quelli utilizzati nella topologia ISP1 precedente. La topologia utilizza aree di sicurezza diverse, ma le configurazioni rimanenti, come i numeri AS per gli HUB primario e secondario, insieme ai tag della community sono le stesse. Questa operazione è obbligatoria per il completamento della convalida della topologia da parte dell'interfaccia utente.



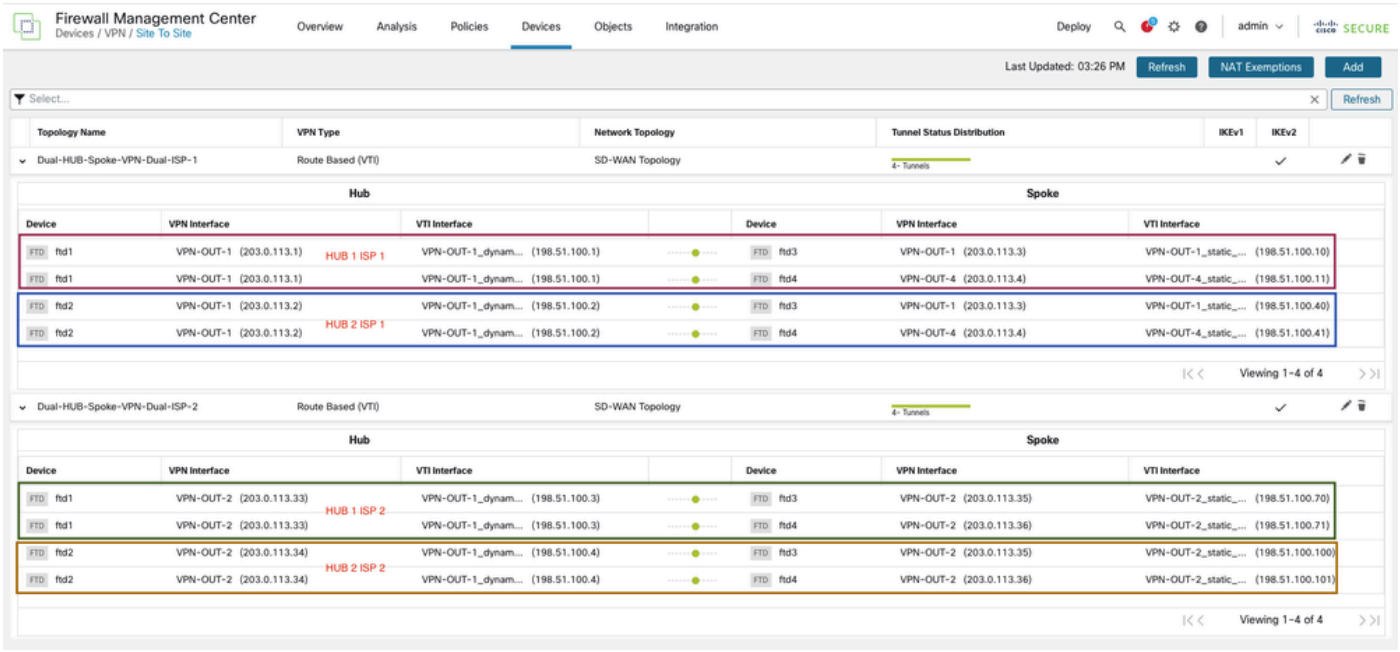
- Tutte le altre impostazioni rimangono invariate. Completare la procedura guidata e procedere con la distribuzione.

Verifica

- La topologia viene visualizzata come illustrato.



- Passare a Dispositivi > VPN > Da sito a sito per visualizzare la topologia.



Questa configurazione comporta quattro peer BGP per dispositivo e ogni spoke ha le route appropriate per raggiungere altri spoke. Ad esempio, potete recuperare l'output da uno dei raggi.

Per raggio 1

<#root>

Spoke1#show bgp summary

```
BGP router identifier 203.0.113.35, local AS number 65500
BGP table version is 4, main routing table version 4
2 network entries using 400 bytes of memory
7 path entries using 560 bytes of memory
1 multipath network entries and 2 multipath paths
3/2 BGP path/bestpath attribute entries using 624 bytes of memory
1 BGP rrinfo entries using 40 bytes of memory
1 BGP AS-PATH entries using 40 bytes of memory
2 BGP community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1712 total bytes of memory
BGP activity 2/0 prefixes, 7/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
198.51.100.1    4        65500 229     226             4    0    0 04:07:22  1
```

<<<<<<<<<< HUB 1 ISP 1 VTI

```
198.51.100.2    4        65510 226     230             4    0    0 04:06:36  2
```

<<<<<<<<<< HUB 2 ISP 1 VTI

```
198.51.100.3    4        65500 182     183             4    0    0 03:16:45  1
```

<<<<<<<<<< HUB 1 ISP 2 VTI

```
198.51.100.4    4        65510 183     183             4    0    0 03:16:30  2
```

<<<<<<<<<< HUB 2 ISP 2 VTI

<#root>

Spoke1#show bgp ipv4 unicast neighbors 198.51.100.1 routes <<<< check for specific prefixes received via

```
BGP table version is 4, local router ID is 203.0.113.35
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop        Metric LocPrf Weight  Path
*>i192.0.2.16/29    198.51.100.1         1    100      0  ?
```

<<<<<<<< spoke 2 network received via HUB 1 ISP 1 tunnel

```
Total number of prefixes 1
```

<#root>

Spoke1#show bgp ipv4 unicast neighbors 198.51.100.3 routes <<<< check for specific prefixes received via

```
BGP table version is 4, local router ID is 203.0.113.35
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop        Metric LocPrf Weight  Path
*mi192.0.2.16/29    198.51.100.3         1    100      0  ?
```

<<<<<<<< spoke 2 network received via HUB 1 ISP 2 tunnel

```
Total number of prefixes 1
```

<#root>

Spoke1# show bgp ipv4 unicast neighbors 198.51.100.2 routes <<<< check for specific prefixes received vi

```
BGP table version is 4, local router ID is 203.0.113.35
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop        Metric LocPrf Weight  Path
*  192.0.2.8/29     198.51.100.2       100             0  65510 65510 ?
```

<<<<<<< inside network receieved cause we advertised it to HUB 1 from ISP 2 topology

```
*  192.0.2.16/29    198.51.100.2       100             0  65510 65510 ?
```

<<<<<<<< spoke 2 network received via HUB 2 ISP 1 tunnel but not preferred

```
Total number of prefixes 2
```

<#root>

Spoke1# show bgp ipv4 unicast neighbors 198.51.100.4 routes <<<< check for specific prefixes received vi

```
BGP table version is 4, local router ID is 203.0.113.35
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop        Metric LocPrf Weight  Path
*  192.0.2.8/29     198.51.100.4       100             0  65510 65510 ?
```

<<<<<<< inside network receieved cause we advertised it to HUB 2 from ISP 1 topology

```
*  192.0.2.16/29    198.51.100.4       100             0  65510 65510 ?
```

<<<<<<<< spoke 2 network received via HUB 2 ISP 2 tunnel but not preferred

```
Total number of prefixes 2
```

La tabella di routing viene visualizzata come mostrato per confermare che il traffico è con carico bilanciato tra entrambi i collegamenti sul lato spoke.

<#root>

Spoke1#show route bgp

```
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

B        192.0.2.16 255.255.255.248 [200/1] via 198.51.100.3, 03:23:53
```

<<<<< multipath for spoke 2 inside network

```
                                    [200/1] via 198.51.100.1, 03:23:53
```

<<<<< multipath for spoke 2 inside network

<#root>

Spoke1#show bgp 192.0.2.16

```
BGP routing table entry for 192.0.2.16/29, version 4
Paths: (4 available, best #4, table default)
Multipath: eBGP iBGP
  Advertised to update-groups:
             2          4
  65510 65510
    198.51.100.4 from 198.51.100.4 (198.51.100.4)
```

<<<< HUB2 ISP2 next-hop

```
      Origin incomplete, metric 100, localpref 100, valid, external
      Community: 10101
  Local
    198.51.100.3 from 198.51.100.3 (198.51.100.3)
```

<<<< HUB1 ISP2 next-hop

```
      Origin incomplete, metric 1, localpref 100, valid, internal, multipath
      Community: 10101
      Originator: 203.0.113.36, Cluster list: 198.51.100.3
  65510 65510
    198.51.100.2 from 198.51.100.2 (198.51.100.4)
```

<<<< HUB2 ISP1 next-hop

```
      Origin incomplete, metric 100, localpref 100, valid, external
      Community: 10101
  Local
    198.51.100.1 from 198.51.100.1 (198.51.100.3)
```

<<<< HUB1 ISP1 next-hop

```
      Origin incomplete, metric 1, localpref 100, valid, internal, multipath, best
      Community: 10101
      Originator: 203.0.113.36, Cluster list: 198.51.100.3
```

Conclusioni

Lo scopo di questo articolo è quello di spiegare vari scenari di distribuzione che possono essere facilmente implementati utilizzando una singola procedura guidata di installazione.

Informazioni correlate

- Per ulteriore assistenza, contattare TAC. È necessario un contratto di supporto valido:Contatti del supporto Cisco internazionali.
- Qui è possibile anche visitare la Cisco VPN Community.

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).