Configuration de SD-WAN pour VPN site à site sur pare-feu sécurisé

Table des matières

Introduction

Ce document décrit les scénarios de déploiement VPN basés sur la route avec le routage de superposition BGP utilisant la fonctionnalité SD-WAN sur Secure Firewall.

Conditions préalables

Tous les concentrateurs et les rayons exécutent le logiciel FTD 7.6 ou version ultérieure et sont gérés via le même FMC, qui exécute également le logiciel 7.6 ou version ultérieure.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- IKEv2
- VPN reposant sur des routes
- Interfaces de tunnel virtuel (VTI)
- IPsec
- BGP

Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Cisco Secure Firewall Threat Defense 7.7.10
- Cisco Secure Firewall Management Center 7.7.10

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations sur les fonctionnalités

Management Center simplifie la configuration des tunnels VPN et le routage entre le siège central (concentrateurs) et les sites distants (satellites) à l'aide du nouvel assistant SD-WAN.

· Automatise la configuration VPN en exploitant DVTI (Dynamic Virtual Tunnel Interface) sur les concentrateurs et SVTI (Static Virtual Tunnel Interface) sur les rayons, avec routage de superposition activé via BGP.

· Attribue automatiquement des adresses IP SVTI pour les rayons et applique la configuration VTI complète, y compris les paramètres de chiffrement.

· Configuration simple et en une étape du routage dans le même assistant pour activer le routage de superposition BGP.

· Permet un routage évolutif et optimal en exploitant l'attribut route-reflector pour BGP.

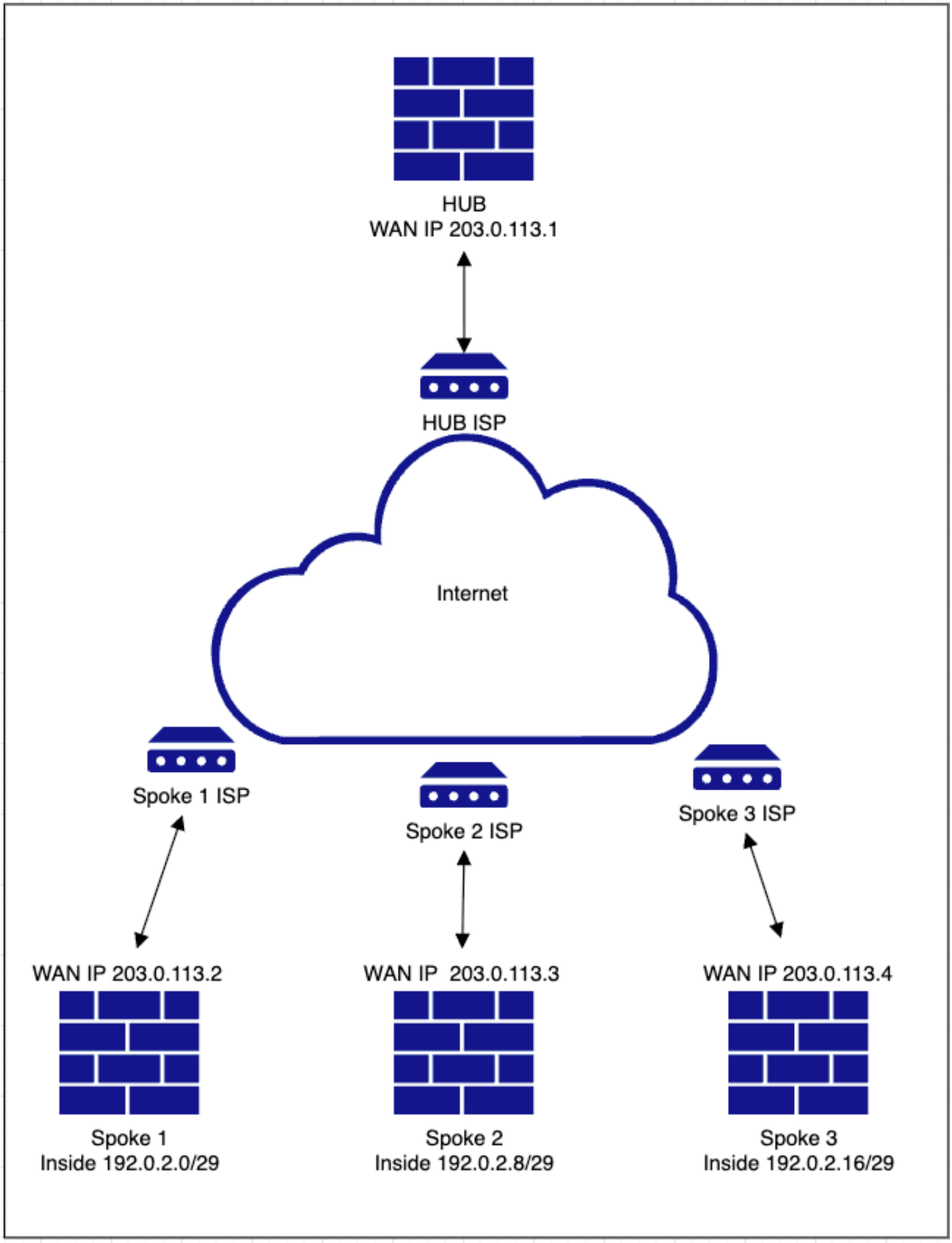
· Permet l'ajout simultané de plusieurs rayons avec une intervention minimale de l'utilisateur.

Topologies couvertes

Dans cet article, plusieurs topologies sont abordées pour garantir que les utilisateurs connaissent les différents scénarios de déploiement.

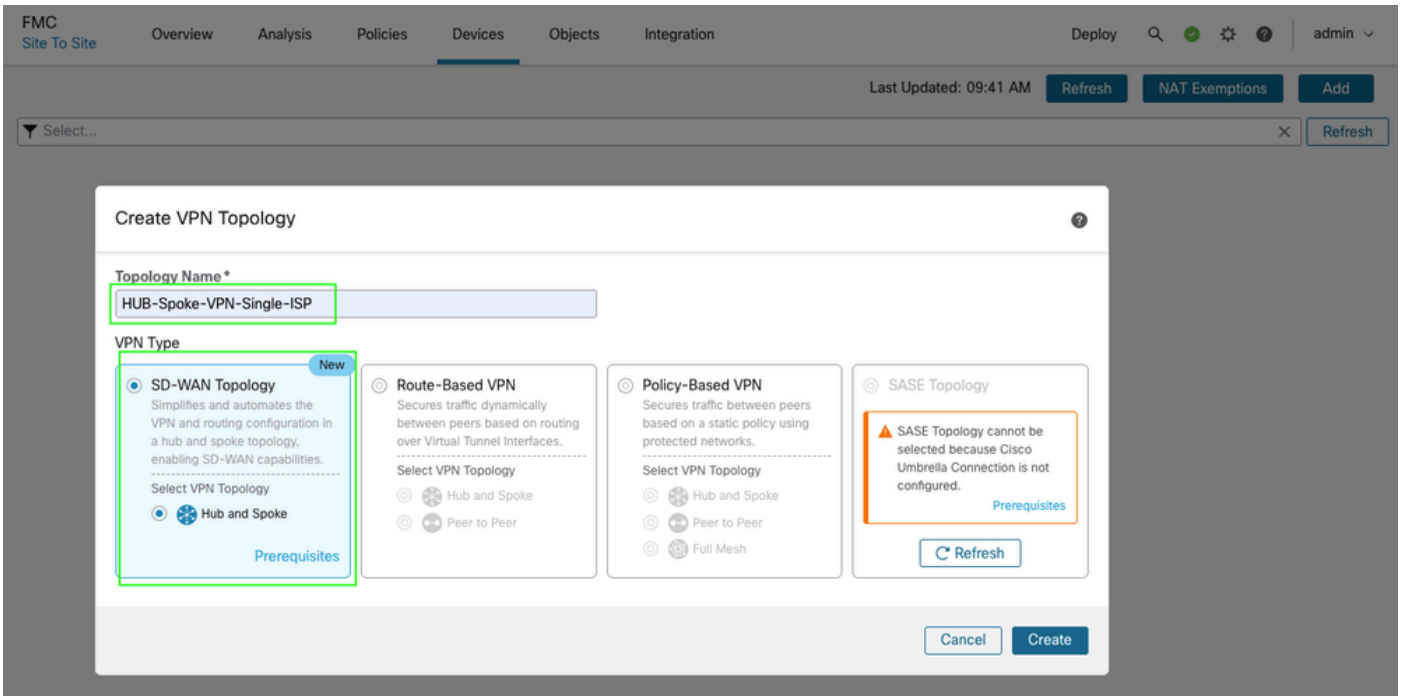
HUB & Spoke (FAI unique)

Diagramme du réseau

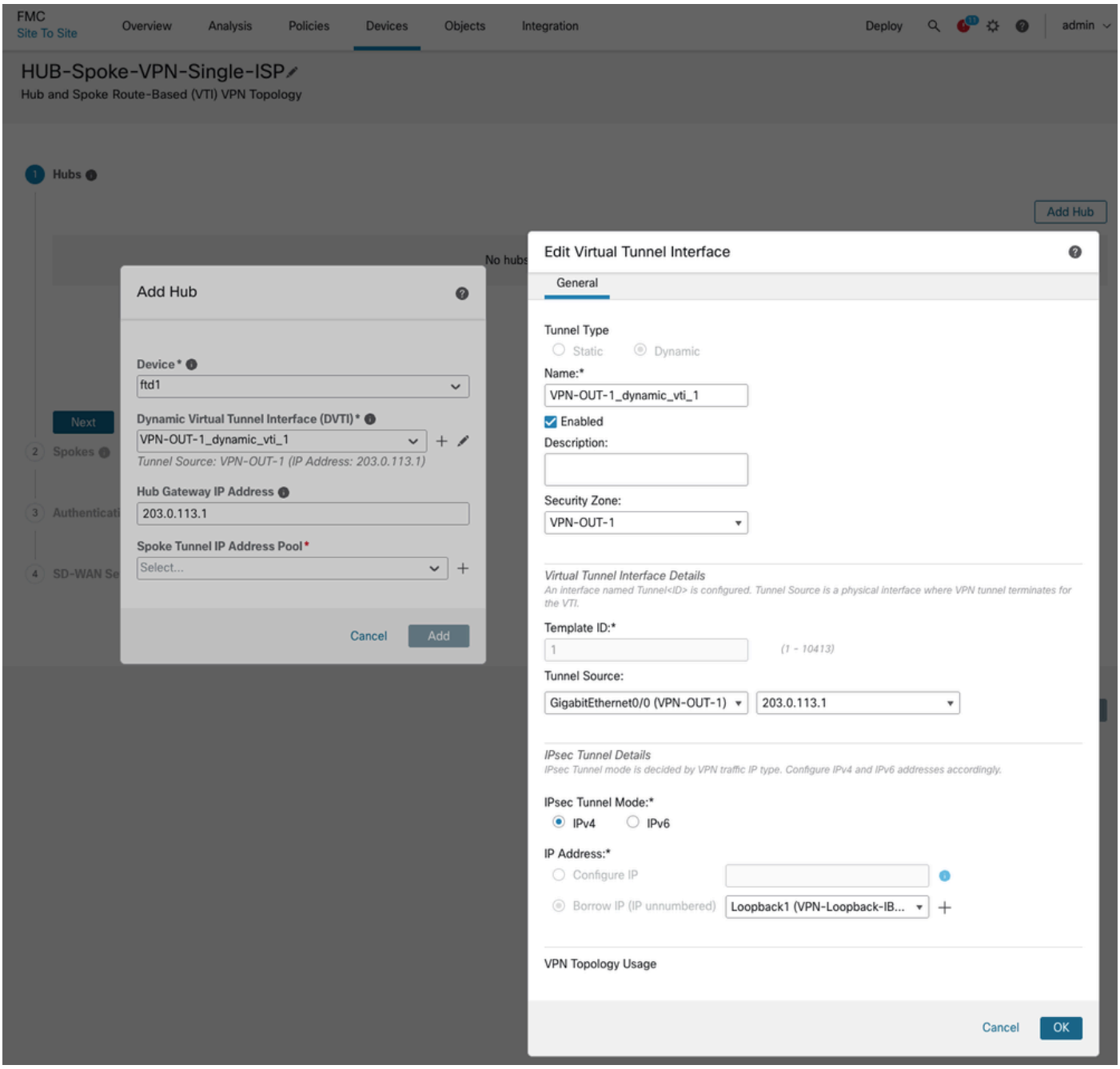


Configurations

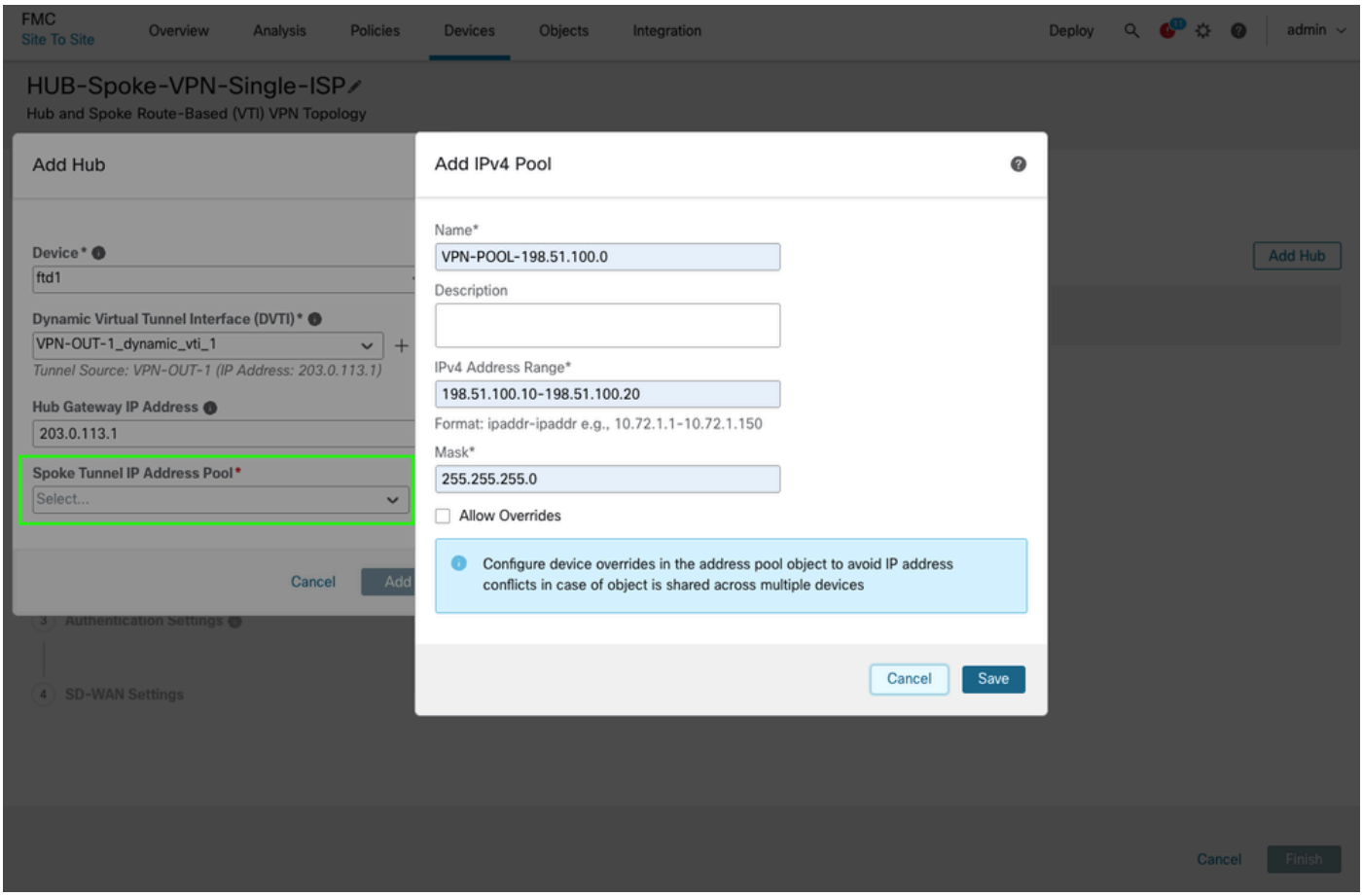
- Accédez à Devices > VPN > Site to Site > Add > SD-WAN Topology > > Create.

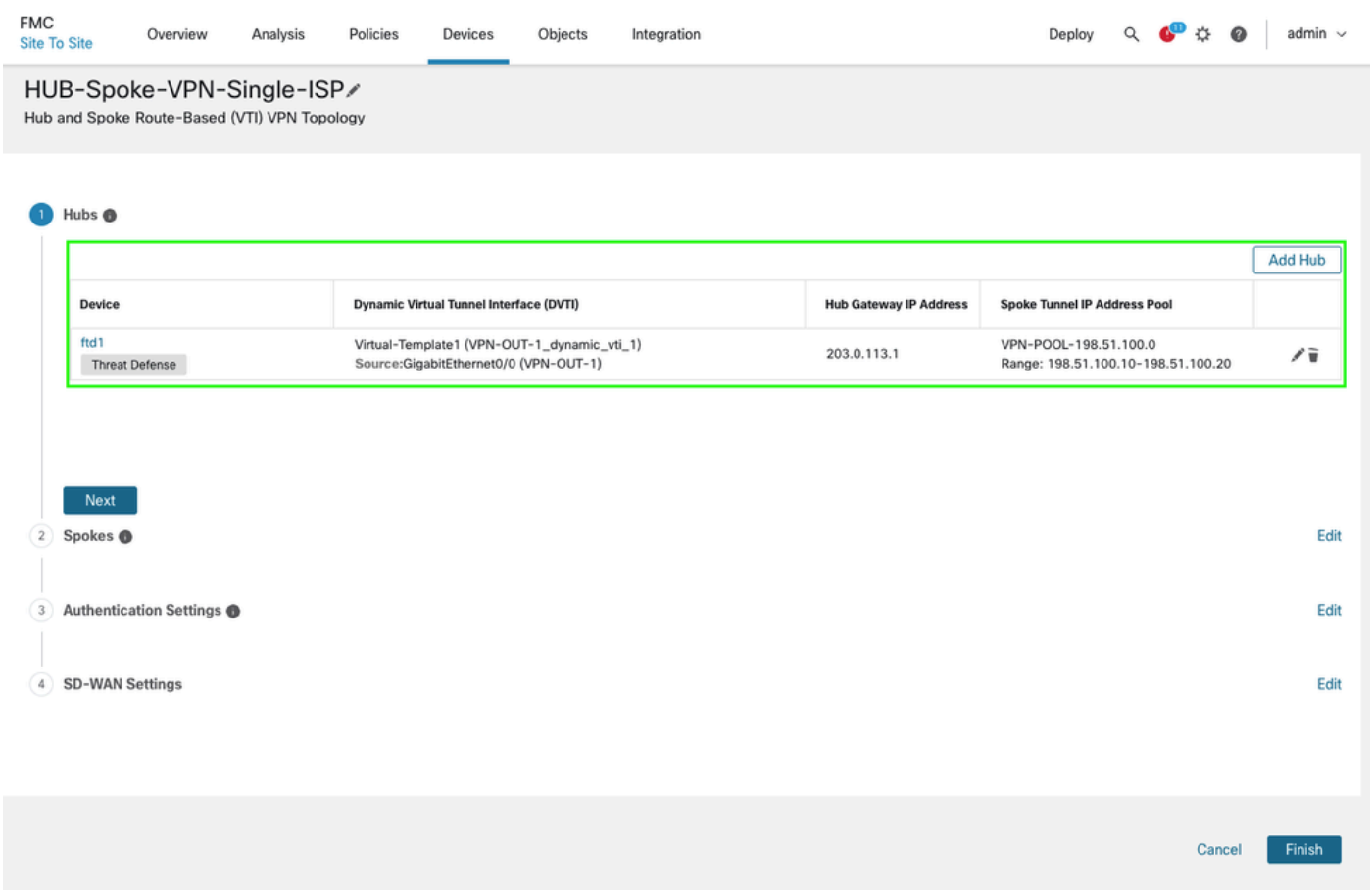


· Ajoutez un concentrateur et créez une interface DVTI à l'extrémité du concentrateur. Dans le cadre de la configuration DVTI, assurez-vous de sélectionner l'interface source de tunnel correcte conformément à la topologie.



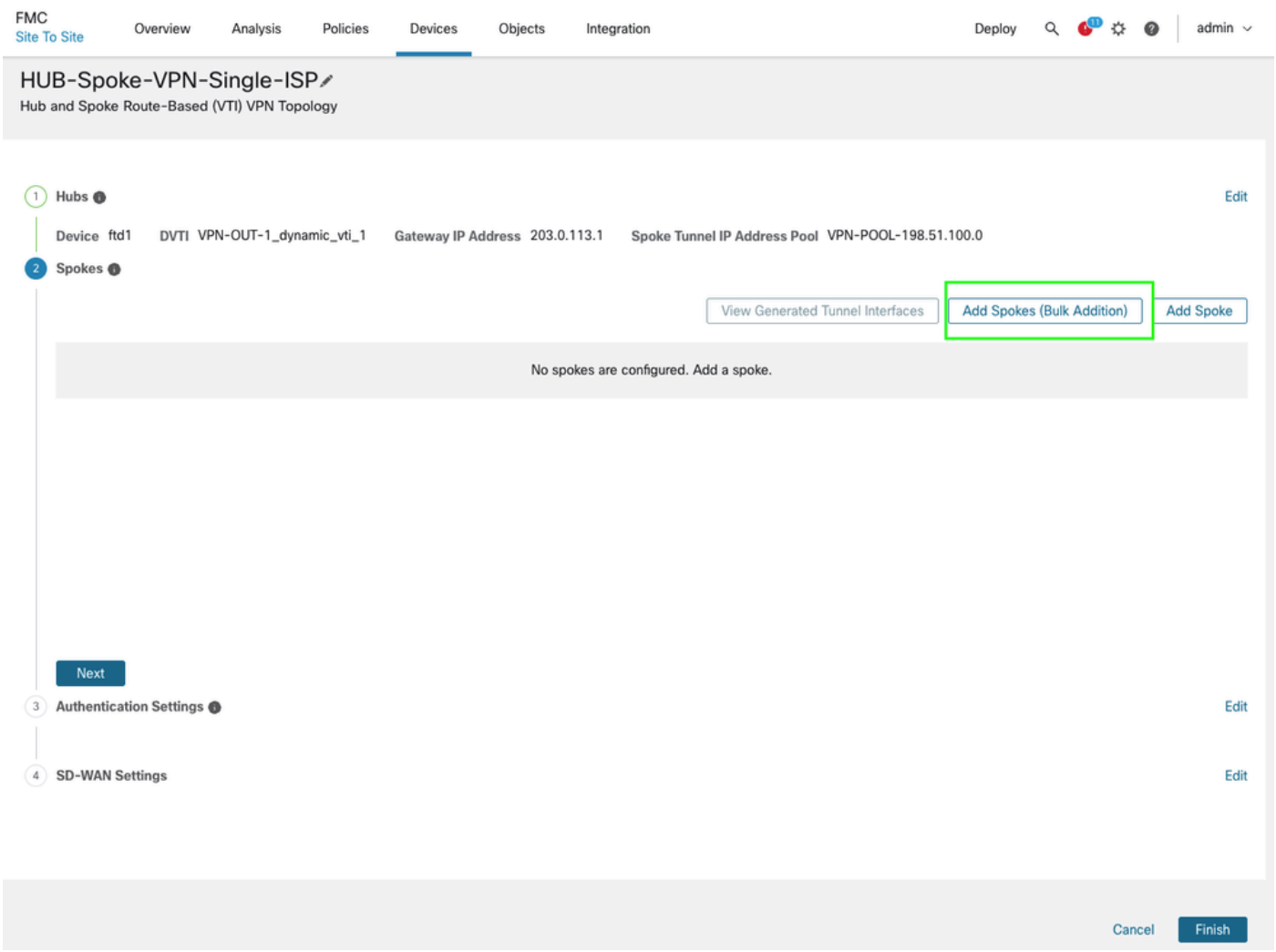
- Créez un pool d'adresses IP de tunnel Spoke et cliquez sur Save puis sur Add. Le pool d'adresses IP est utilisé pour attribuer des adresses IP de tunnel VTI aux rayons.



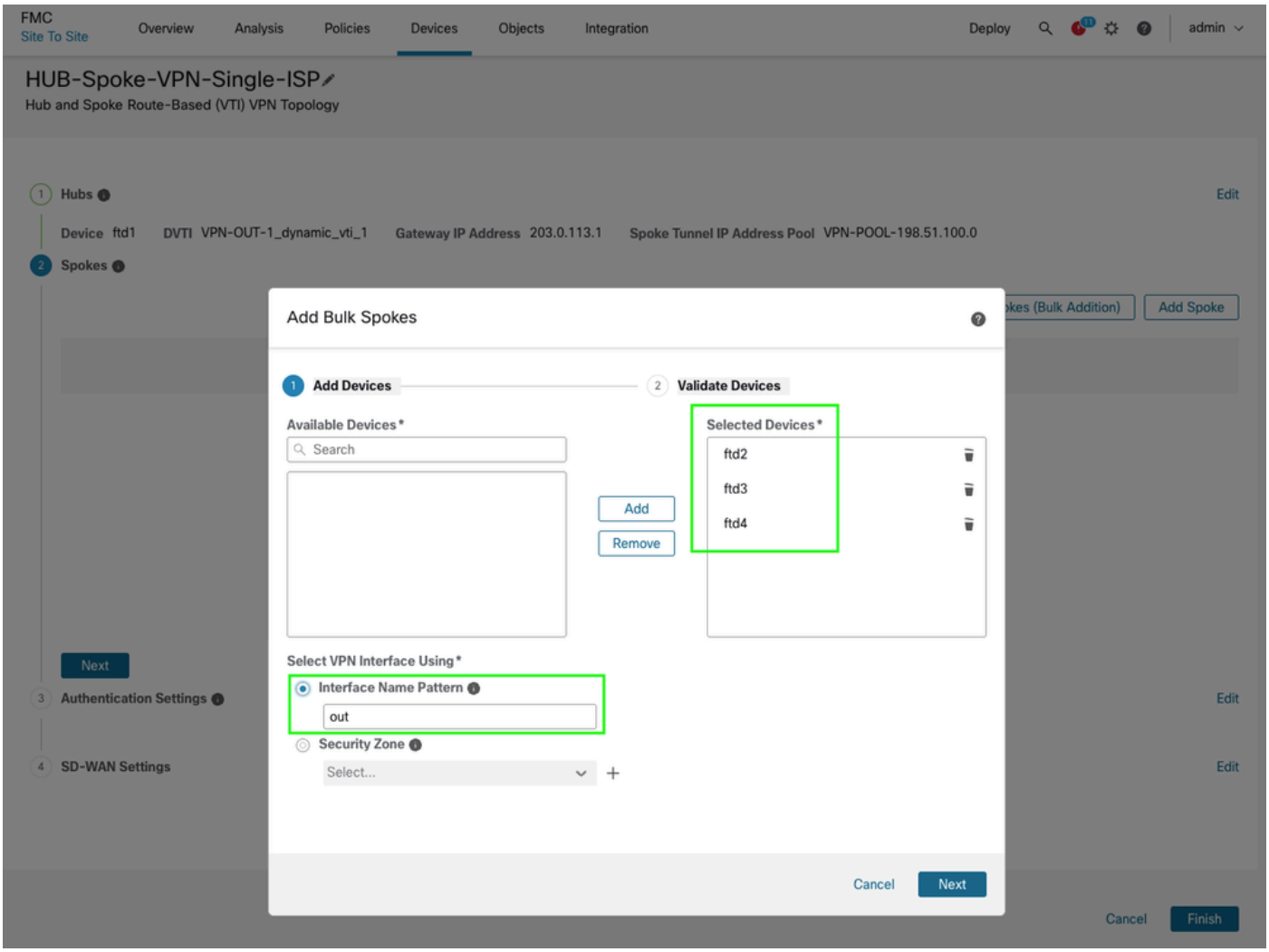


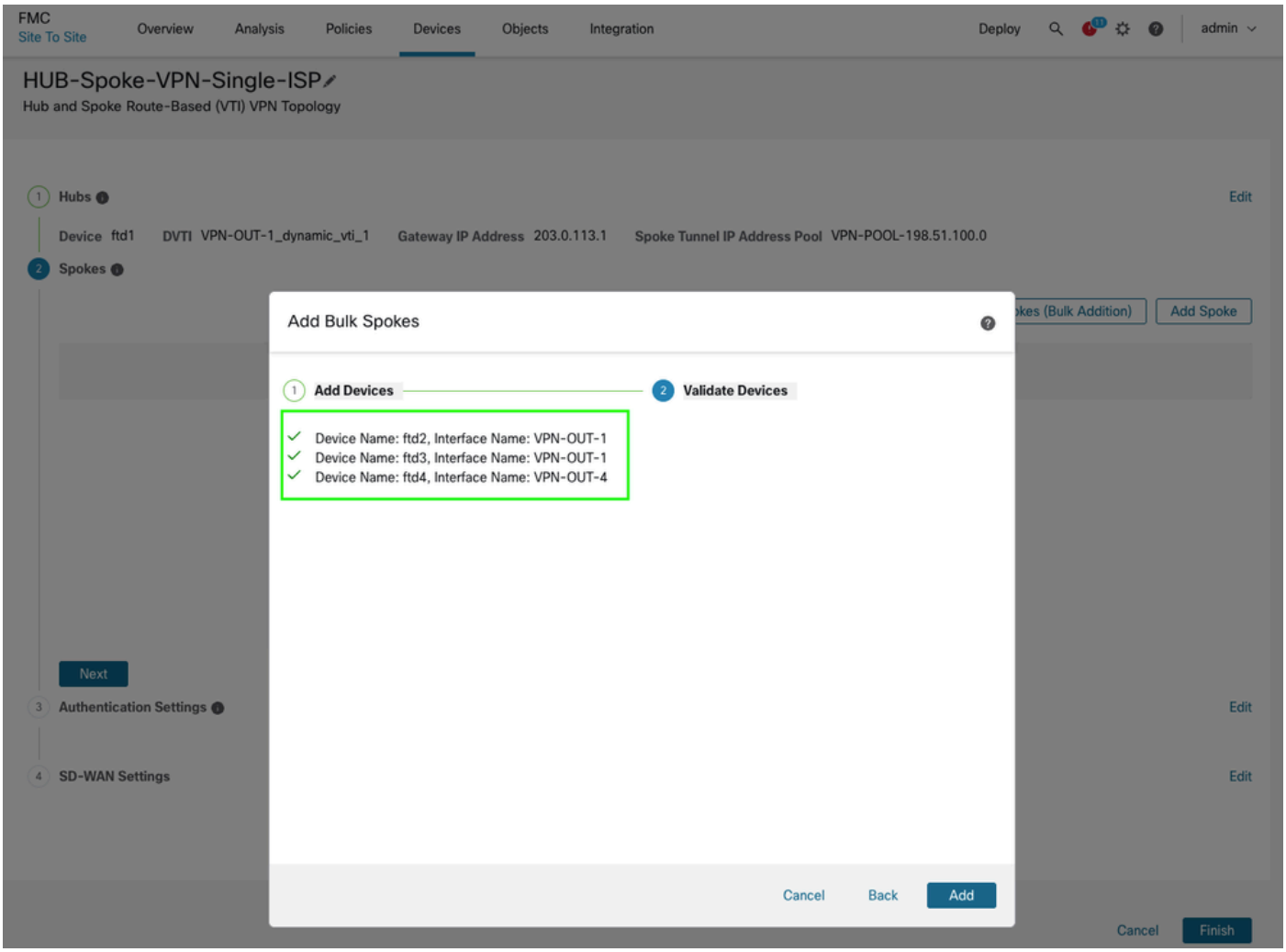
- Cliquez sur Next pour continuer et ajouter les rayons. Vous pouvez utiliser l'option d'ajout en bloc si vous avez des noms d'interface/de zone communs ou ajouter des rayons

individuellement.

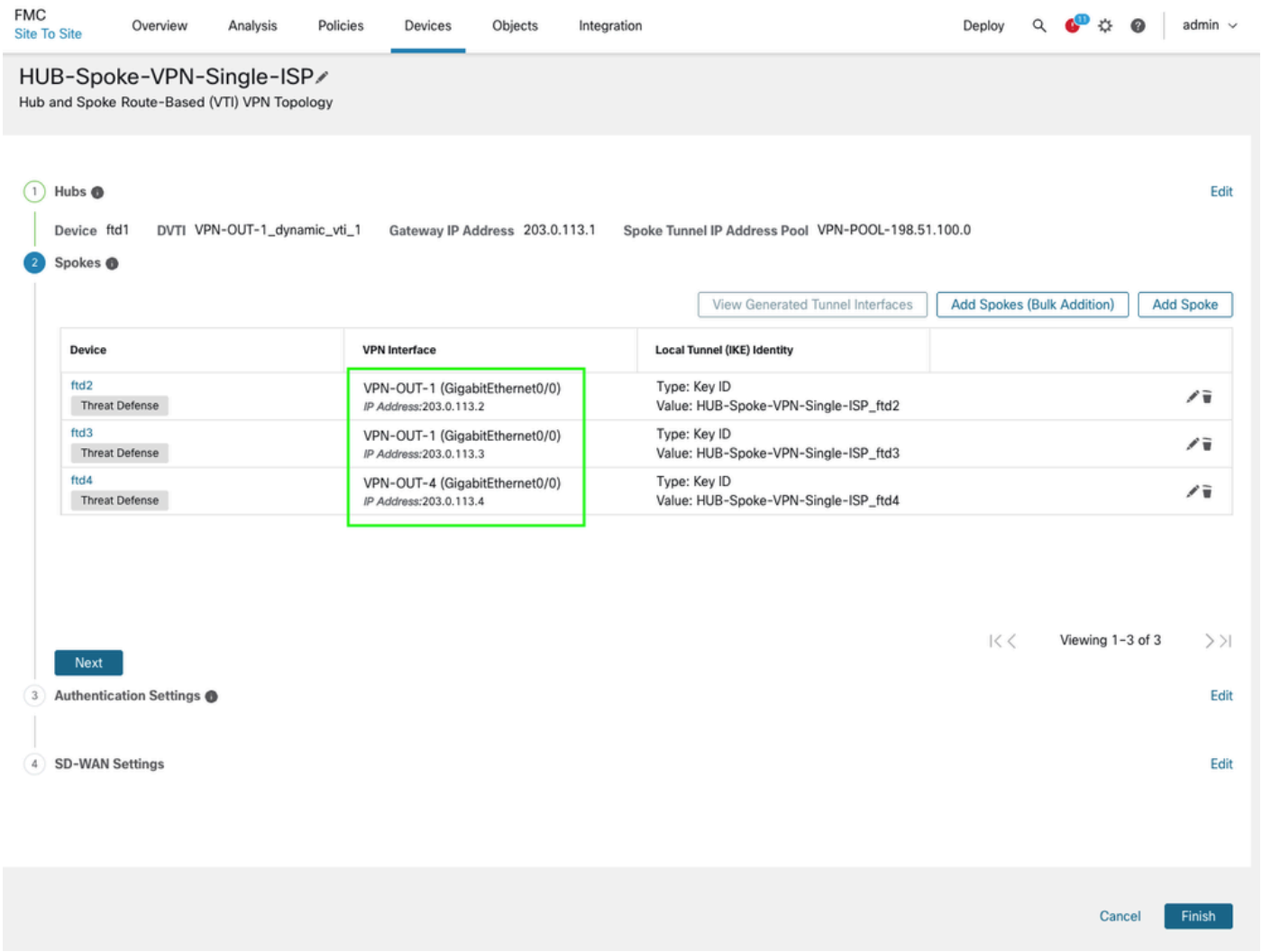


- Sélectionnez les périphériques et spécifiez un modèle d'attribution de noms pour l'interface WAN/externe. Si les périphériques partagent le même nom d'interface, l'utilisation d'initiales est suffisante. Cliquez sur Next, et si la validation est réussie, cliquez sur Add. Pour les ajouts en bloc, vous pouvez également utiliser le nom de la zone de la même manière.

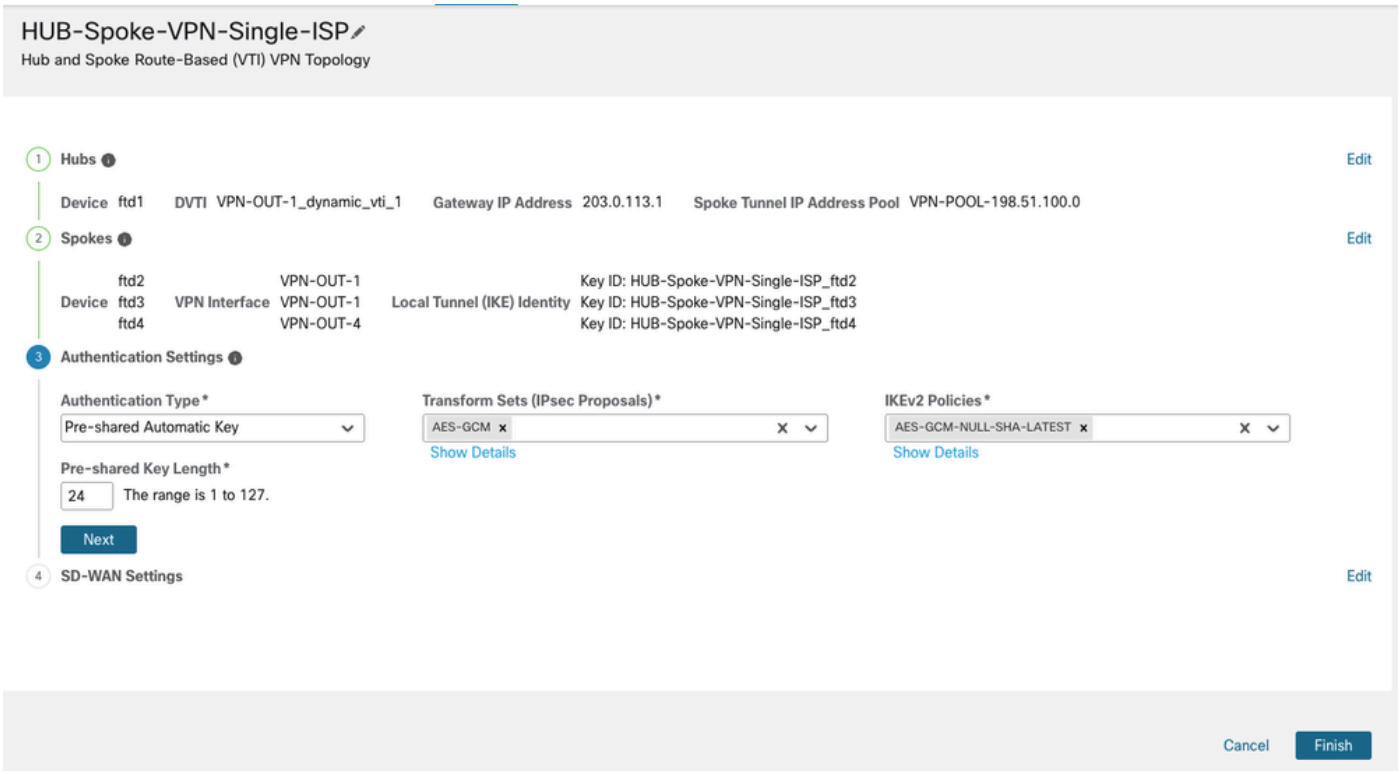

FMC
Site To Site
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
HUB-Spoke-VPN-Single-ISP
Hub and Spoke Route-Based (VTI) VPN Topology
1 Hubs
Edit
Device ftd1
DVTI VPN-OUT-1_dynamic_vti_1
Gateway IP Address 203.0.113.1
Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.0
2 Spokes
Add 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



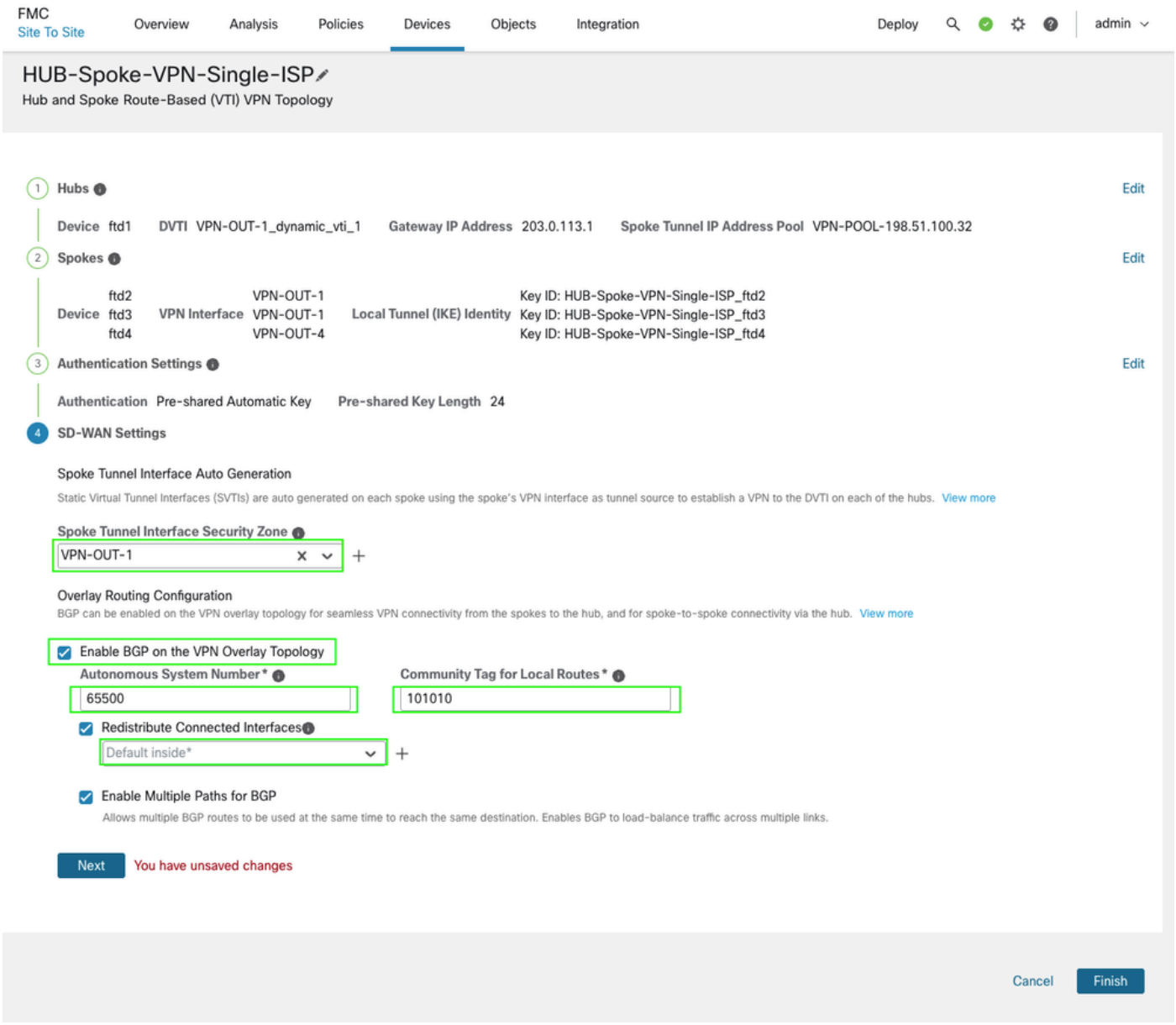
- Vérifiez les détails de l'interface de rayons et de superposition pour vous assurer que les interfaces correctes sont sélectionnées, puis cliquez sur Next.



- Vous pouvez conserver les paramètres par défaut de la configuration IPsec ou spécifier des chiffrements personnalisés, le cas échéant. Cliquez sur Next pour continuer. Dans ce document, vous utilisez les paramètres par défaut.



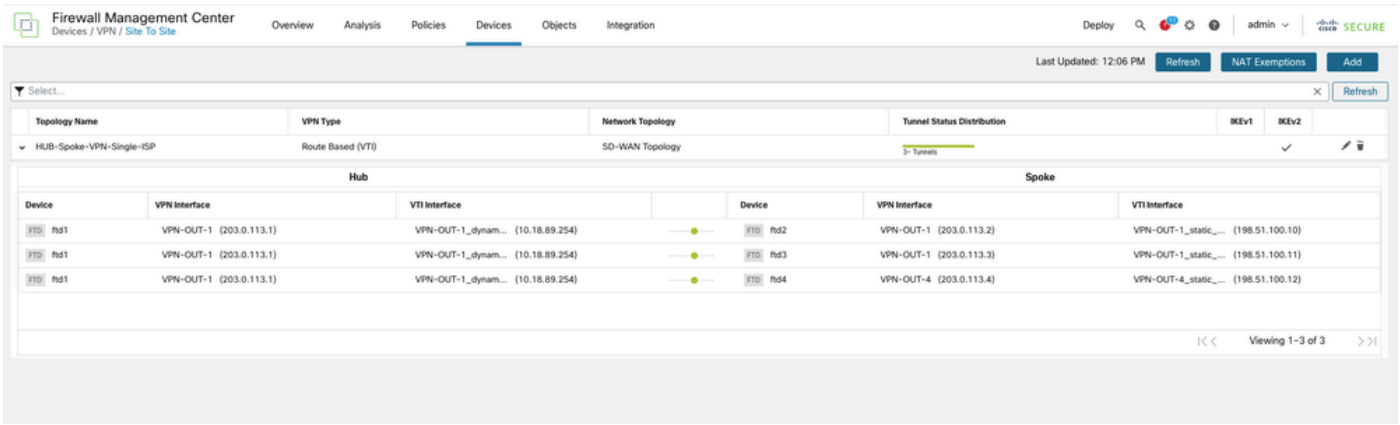
- Enfin, vous pouvez configurer le routage de superposition dans le même assistant pour cette topologie en spécifiant les paramètres BGP appropriés, tels que le numéro de système autonome, l'annonce d'interface interne et les balises de communauté pour le filtrage de préfixe. La zone de sécurité peut aider au filtrage du trafic via des politiques de contrôle d'accès, tandis que vous pouvez également créer un objet pour les interfaces et les utiliser dans la redistribution des interfaces connectées si le nom est différent de celui qui est à l'intérieur ou n'est pas symétrique entre les périphériques dans la topologie.



- Cliquez sur Next, puis sur Finish, et enfin sur Deploy pour terminer le processus.

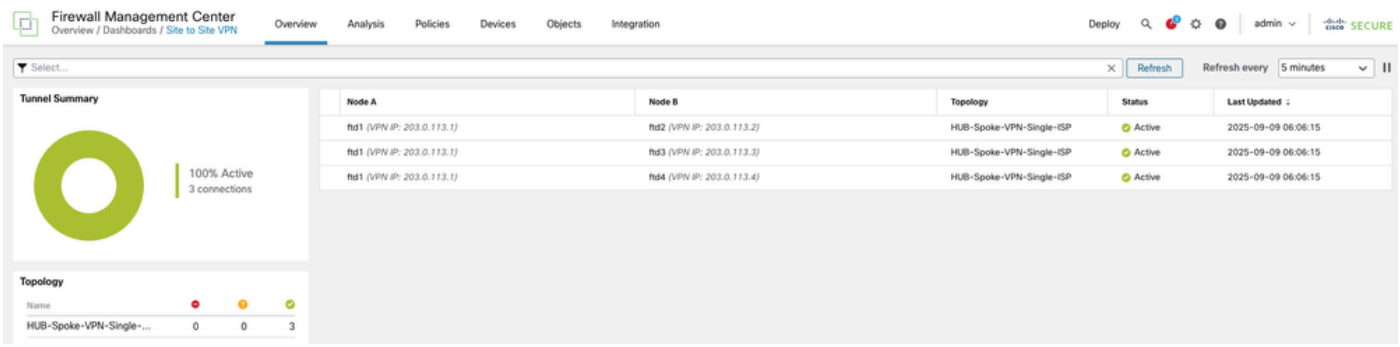
Vérification

- Vous pouvez vérifier l'état du tunnel en naviguant vers Devices > VPN > Site to Site.

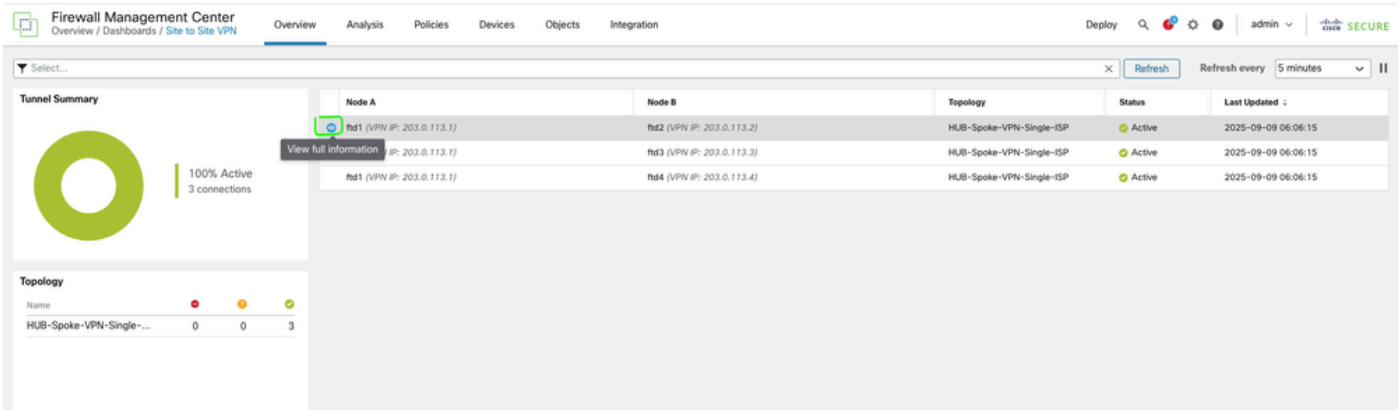


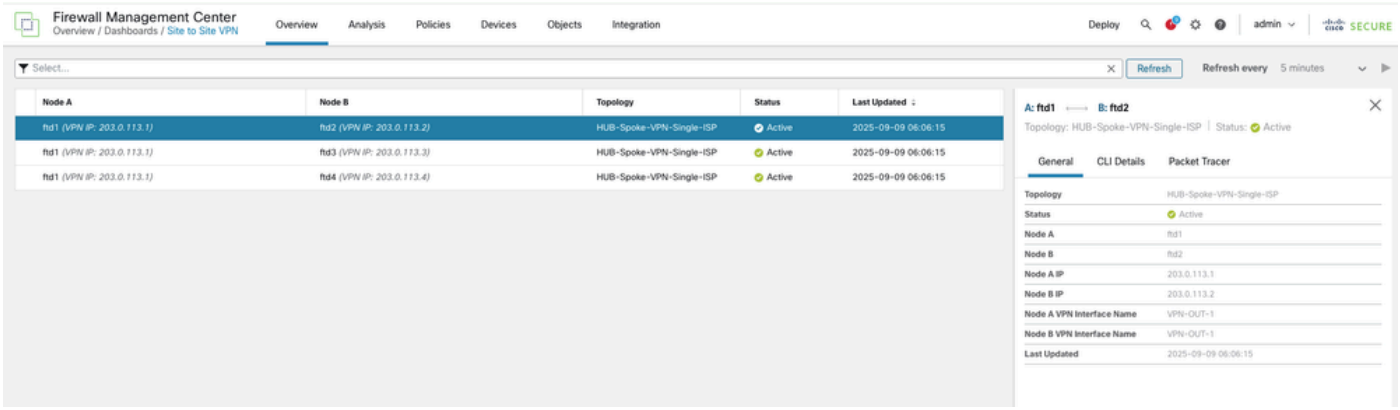
- Vous pouvez vérifier des détails supplémentaires en naviguant vers Overview > Dashboards

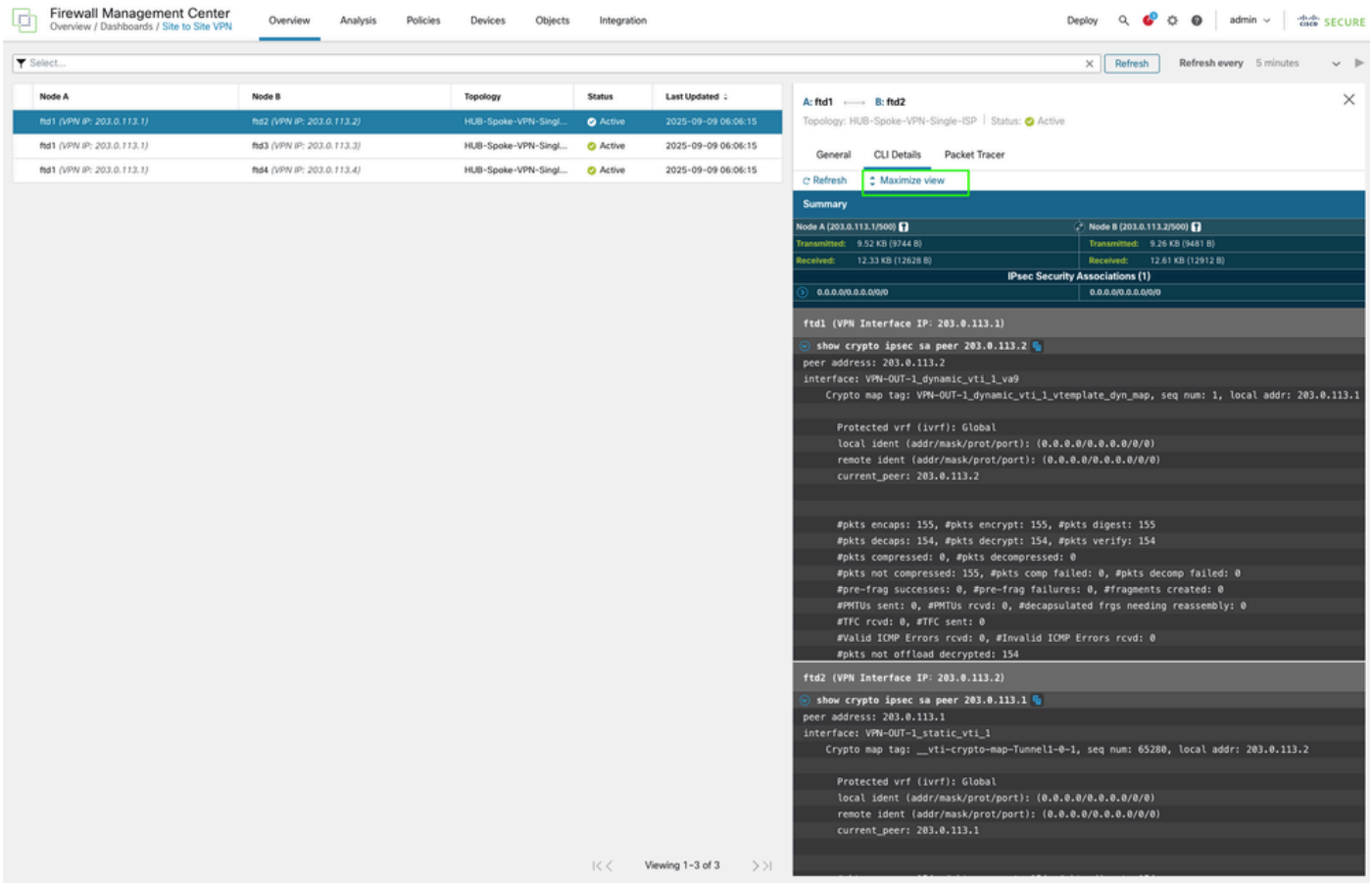
> Site to Site VPN.



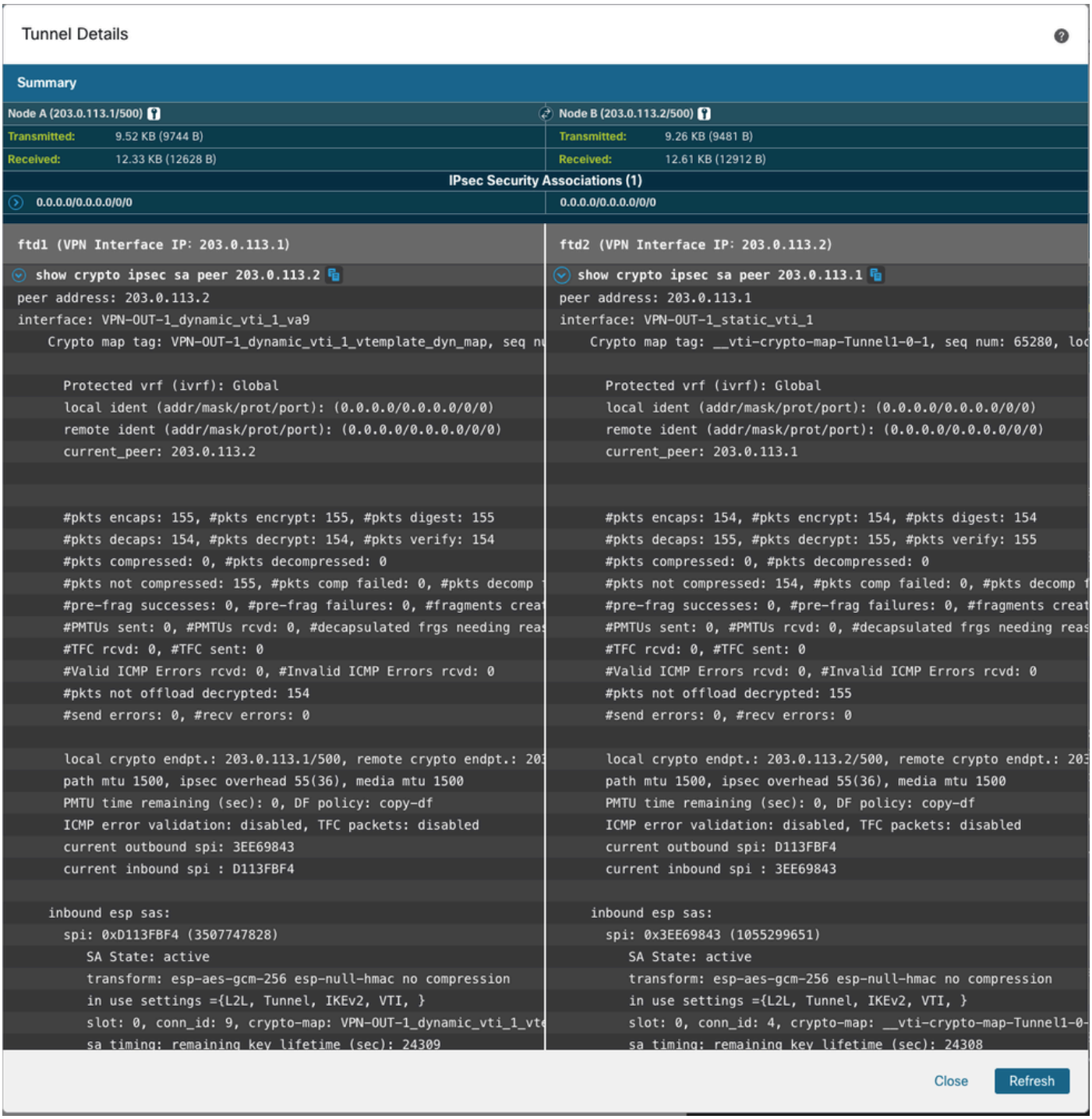
- Pour plus d'informations, sélectionnez le tunnel et cliquez sur View Full Information.







- Le résultat est affiché directement à partir de l'interface de ligne de commande FTD et peut être actualisé pour afficher des compteurs mis à jour et des informations importantes, telles que les détails de l'index des paramètres de sécurité (SPI).



- L'interface de ligne de commande FTD peut également être utilisée pour vérifier les informations de routage et l'état d'appairage BGP.

Côté concentrateur

<#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
```

Côté Rayon

La même vérification peut également être effectuée sur les périphériques en étoile. Voici un exemple de l'un des rayons.

<#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
```

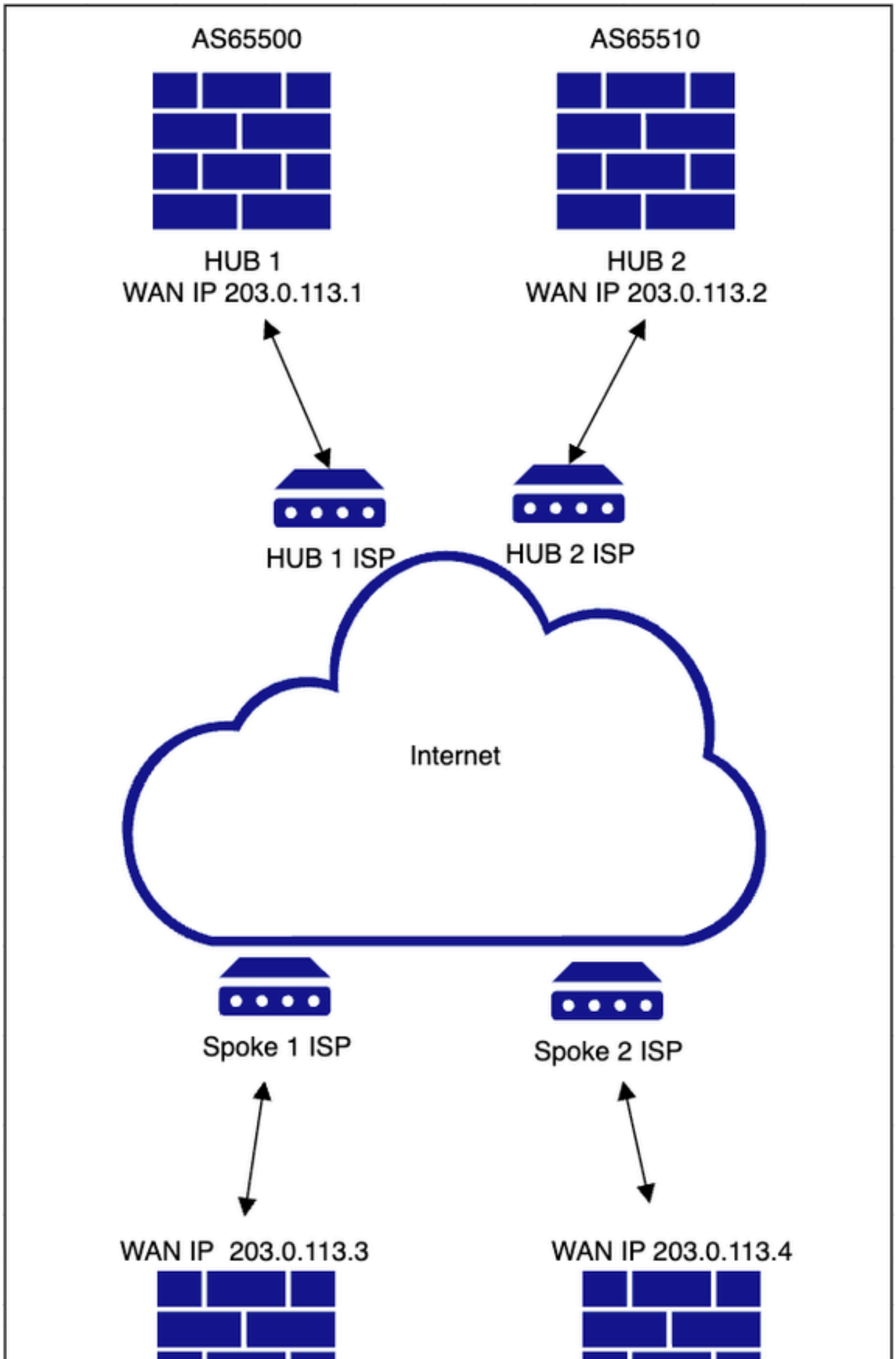
<<<<<< spoke 2 inside network

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

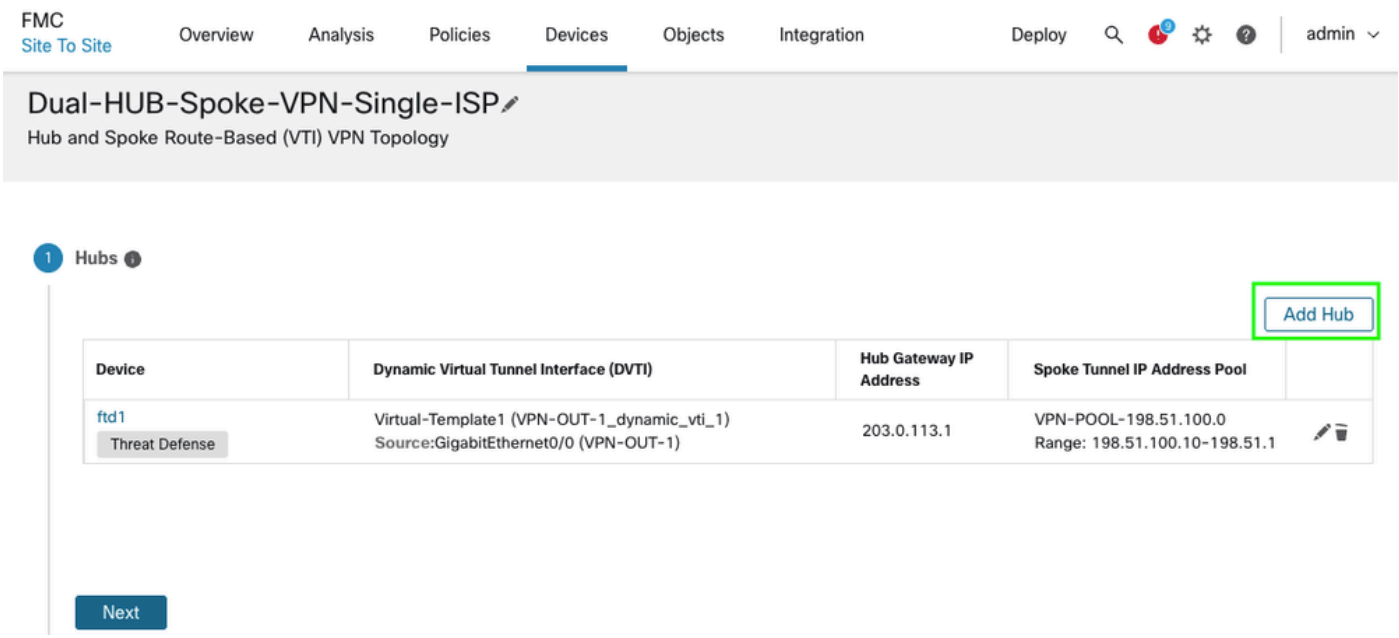
<<<<<< spoke 3 inside network

Double HUB & Spoke (ISP unique pour concentrateur redondant via EBGP entre concentrateur secondaire et satellites)

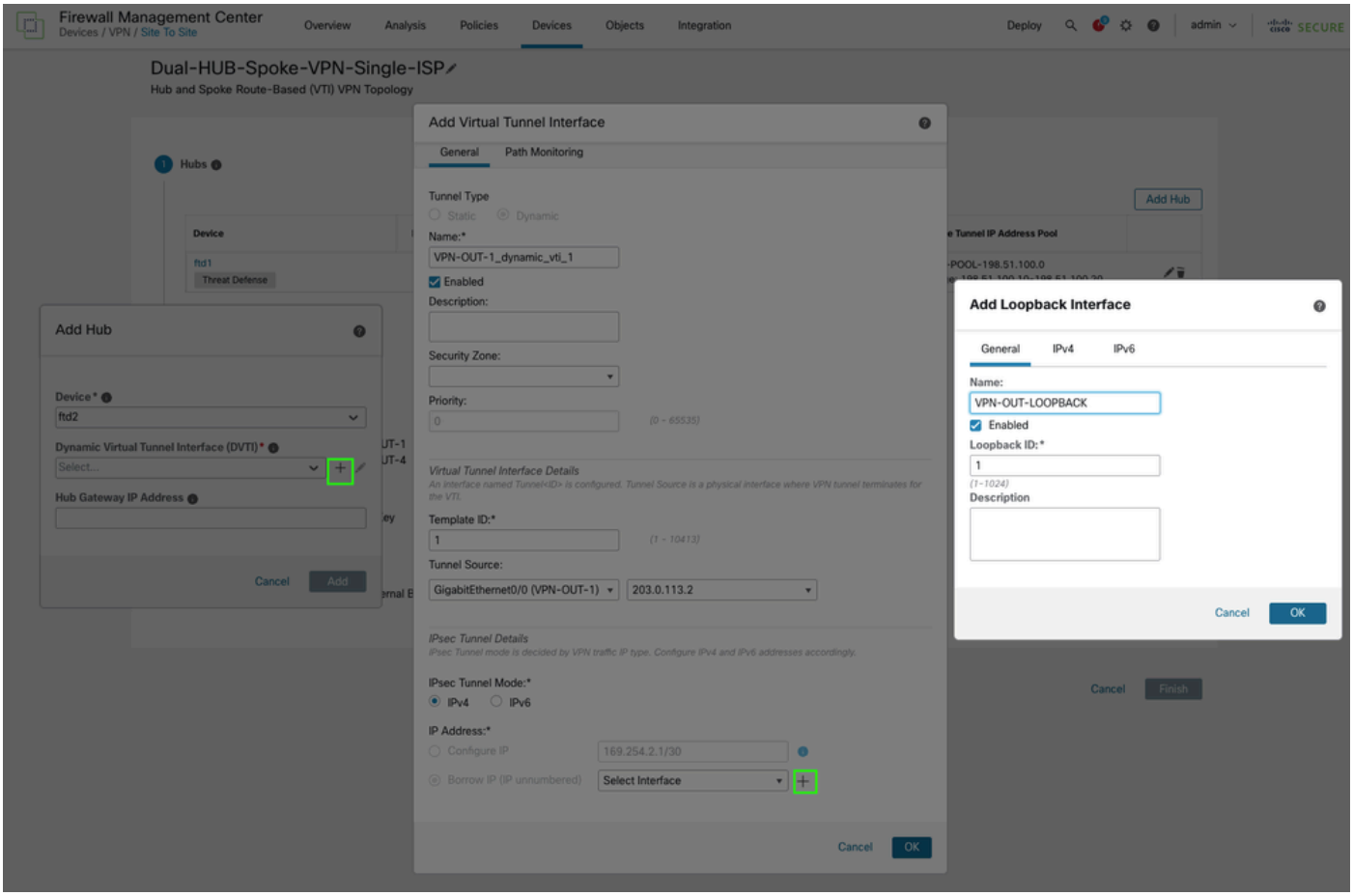
Diagramme du réseau


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

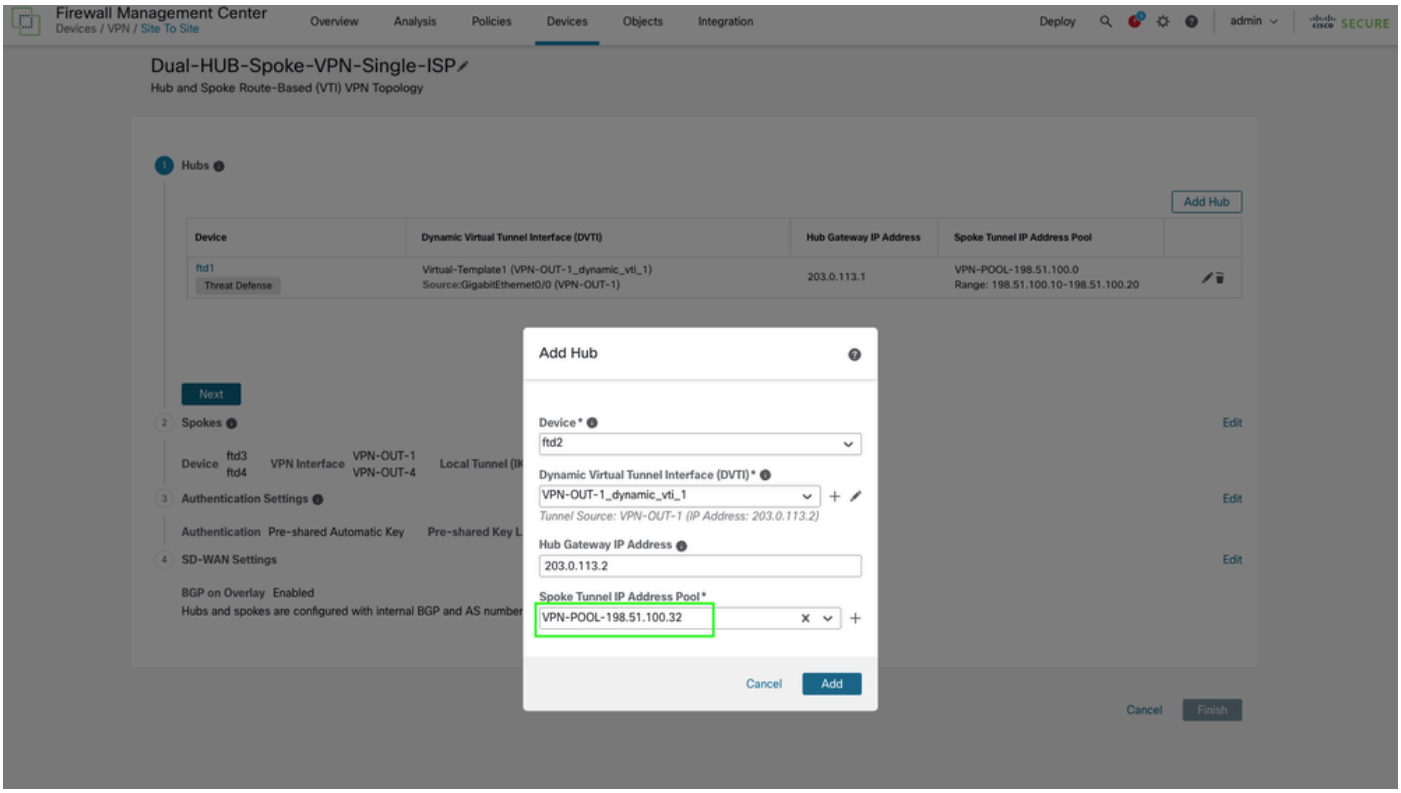
Après avoir ajouté le premier concentrateur, ajoutez le second en suivant les mêmes étapes que pour le concentrateur 1.

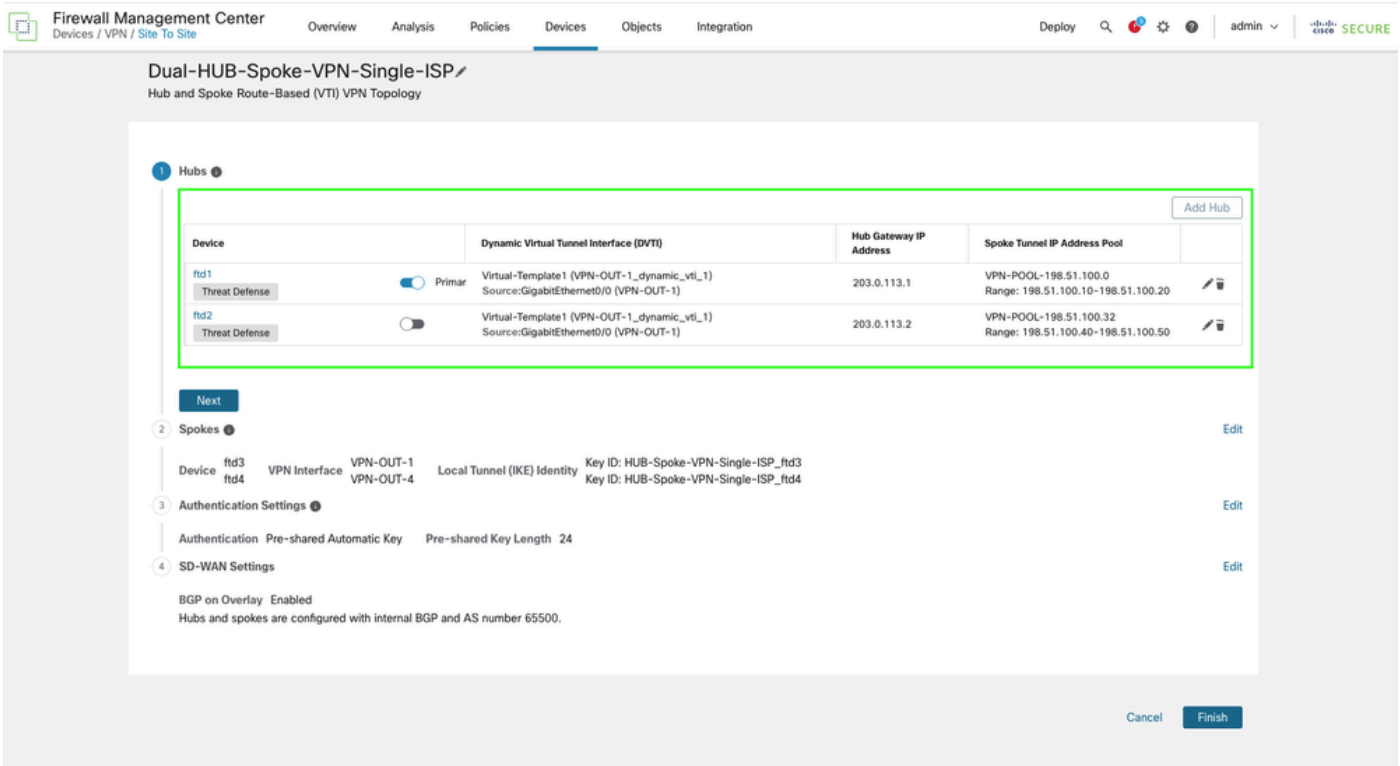


- Créez l'interface DVTI (Dynamic Virtual Tunnel Interface).



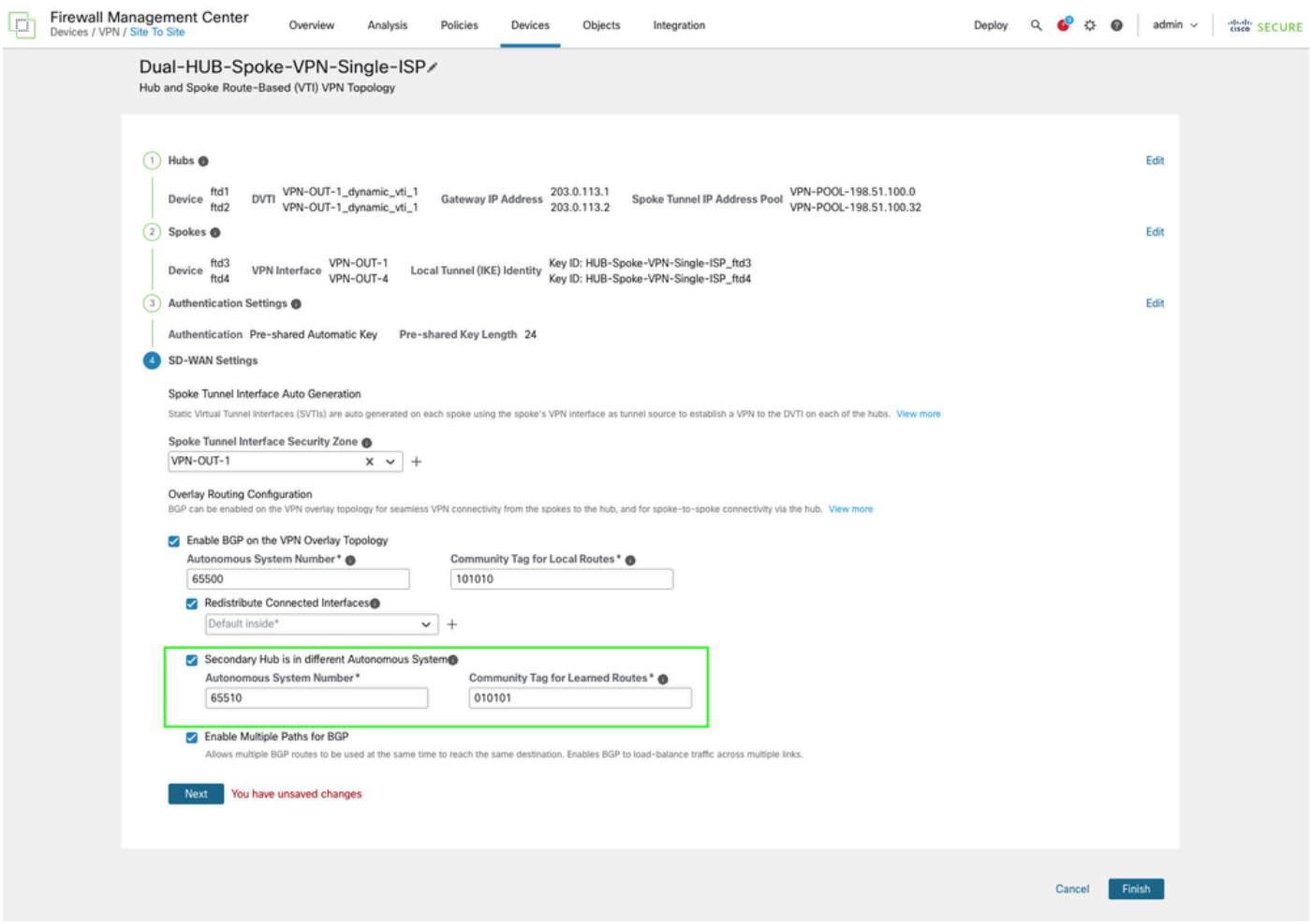
- Un nouveau pool d'adresses IP est requis pour les tunnels VTI du HUB 2 côté satellite. Créez et configurez le nouveau pool, puis enregistrez les modifications.





- Pour configurer l'appairage eBGP entre le deuxième concentrateur et les rayons, modifiez les paramètres SD-WAN à l'étape finale. Activez l'option Secondary HUB is in a different Autonomous System et spécifiez le numéro de système autonome (AS) pour le HUB secondaire. IBGP peut également être utilisé s'il n'y a aucune limitation à l'utilisation d'un numéro de système autonome différent sur votre environnement en laissant l'option Secondary HUB is in a different Autonomous System décochée. Cela permet d'envoyer la même balise de communauté et le même numéro de système autonome pour le concentrateur secondaire également. L'article se concentre sur eBGP pour la configuration

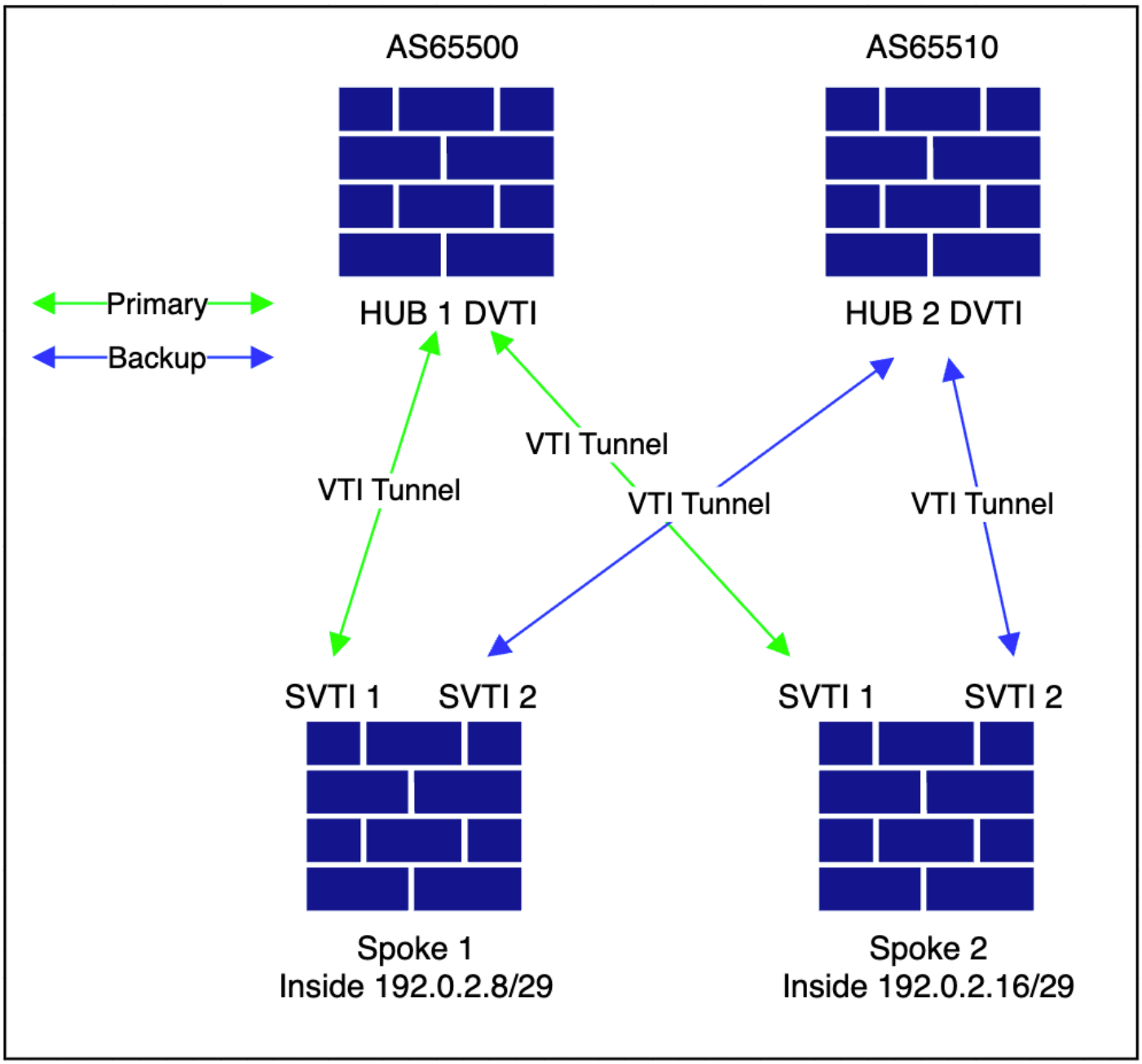
actuelle.



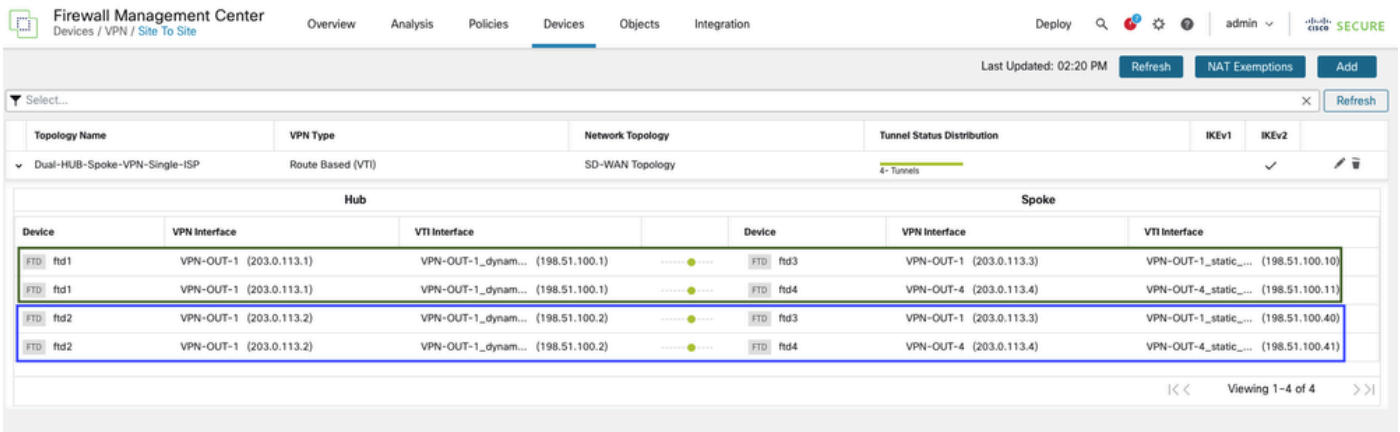
Assurez-vous que le numéro de système autonome (AS) et l'étiquette de communauté sont uniques dans cette configuration.

Vérification

Ce schéma illustre la topologie de superposition.



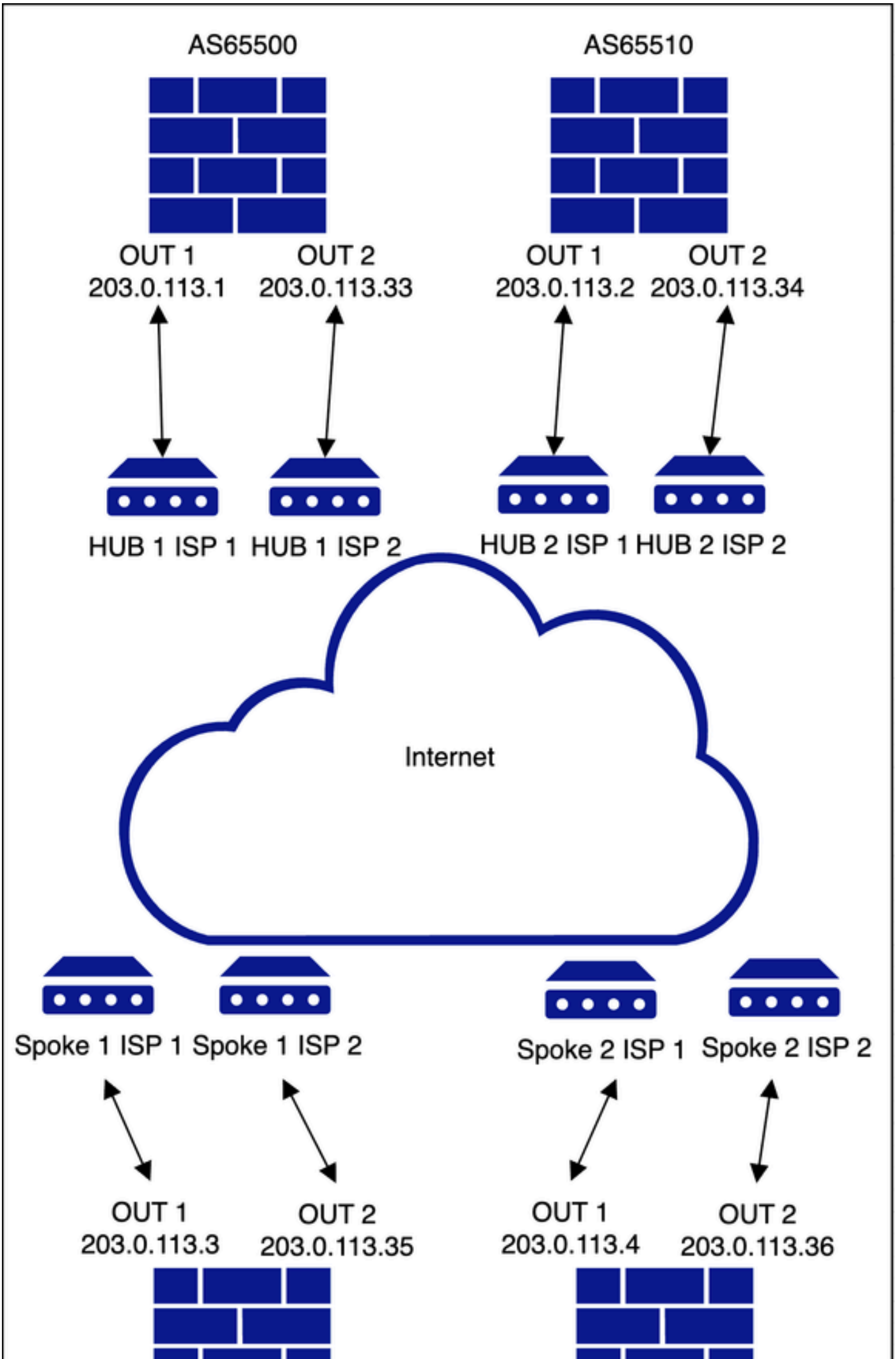
- Dans le FMC, accédez à Devices > VPN > Site to Site.



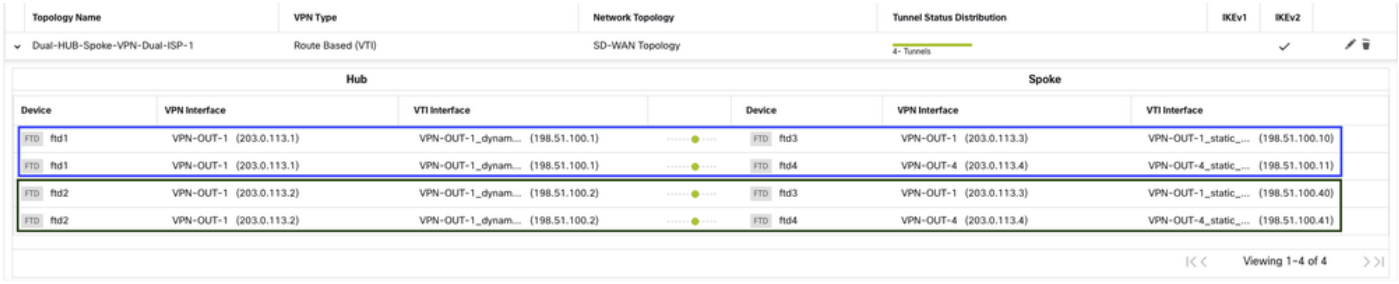
- Toutes les autres étapes restent inchangées.

Double concentrateur et satellite (double FAI pour concentrateur redondant et FAI via EBGP entre concentrateur secondaire et satellites)

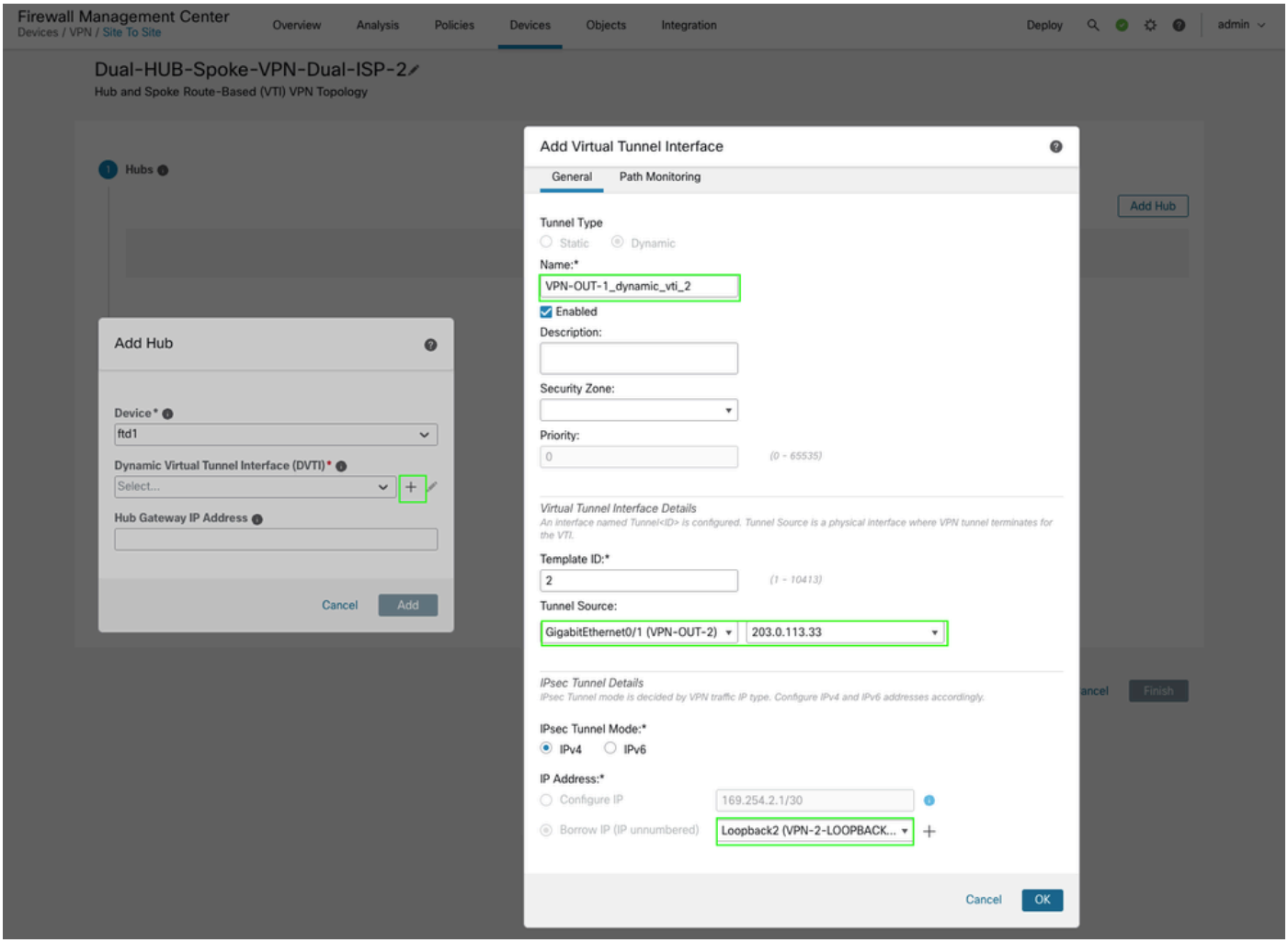
Diagramme du réseau


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

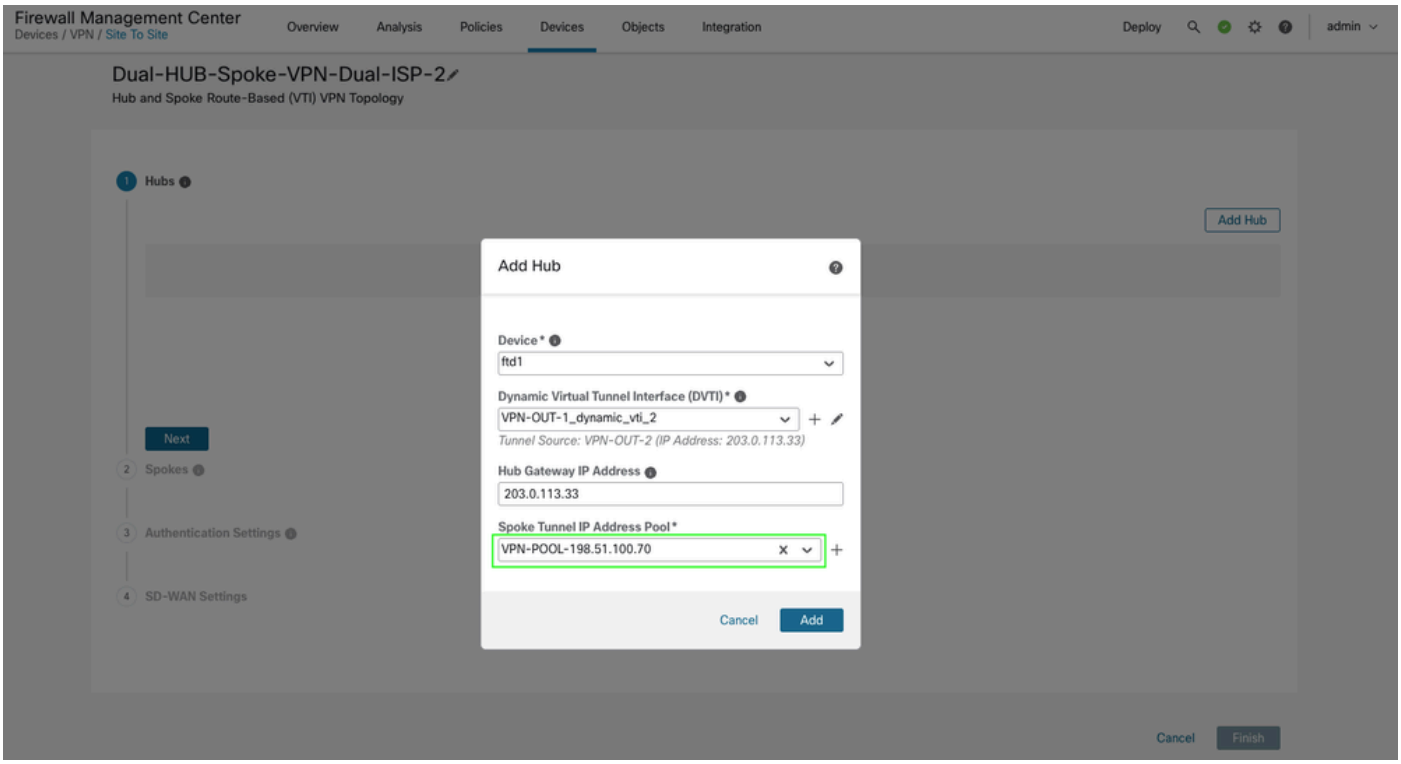
Le déploiement de cette topologie est ignoré à l'aide du premier FAI, car il est traité dans la topologie précédente.

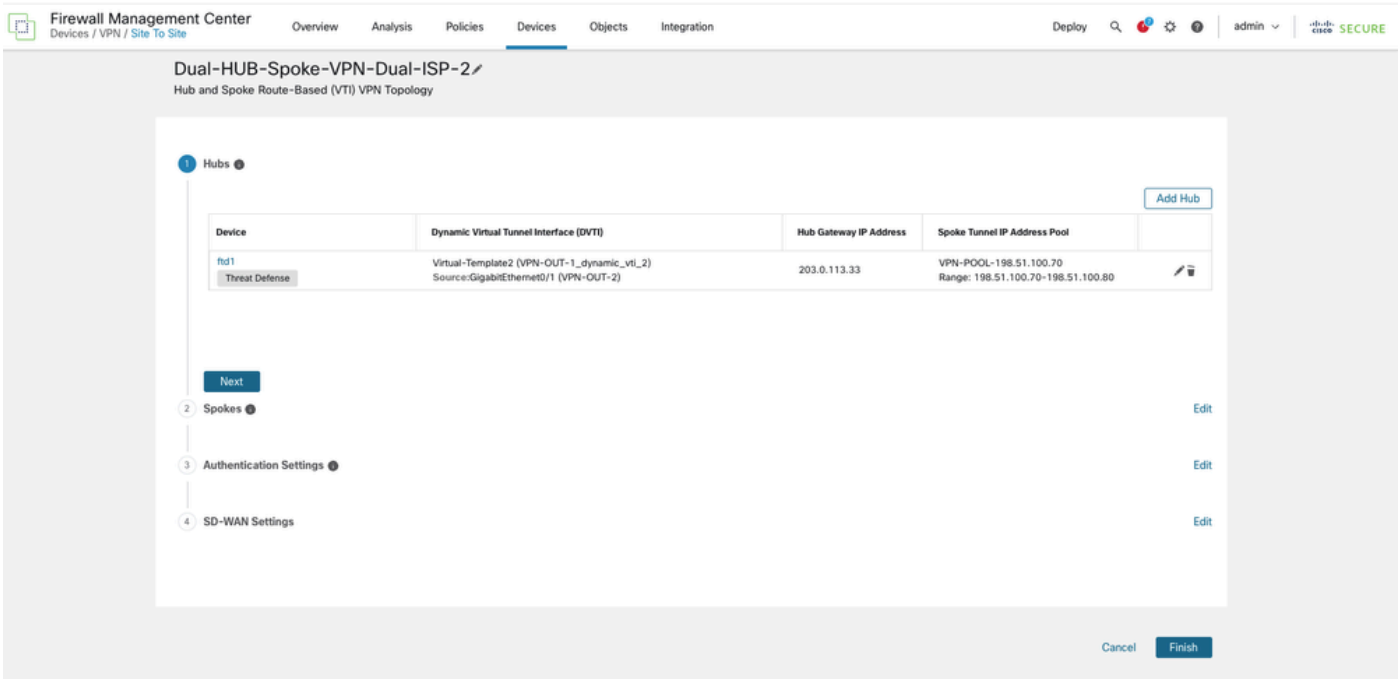


- Ensuite, ajoutez la deuxième topologie en créant deux interfaces DVTI supplémentaires par concentrateur, chacune utilisant l'interface sous-jacente pour ISP 2 (VPN-OUT-2).

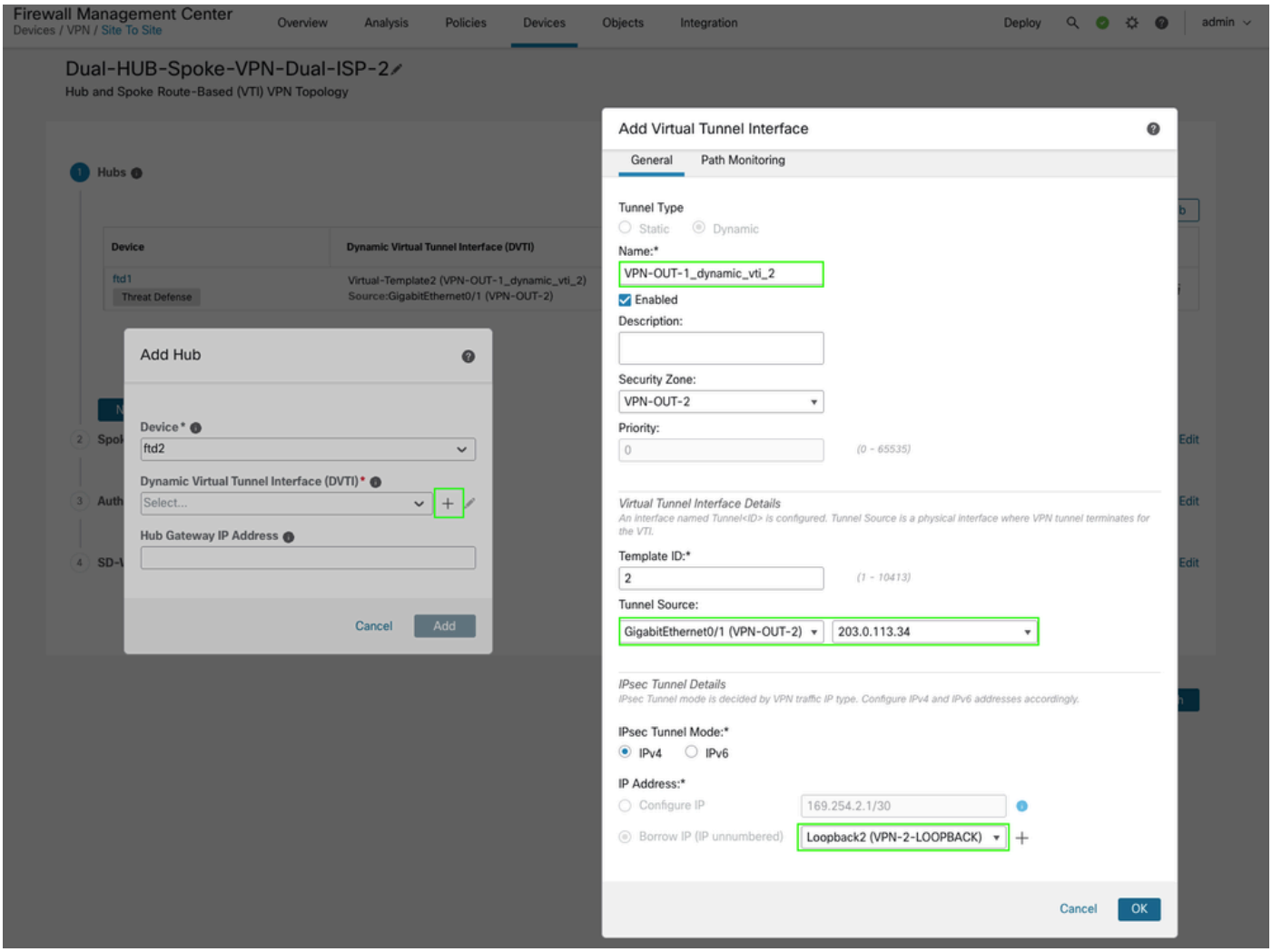


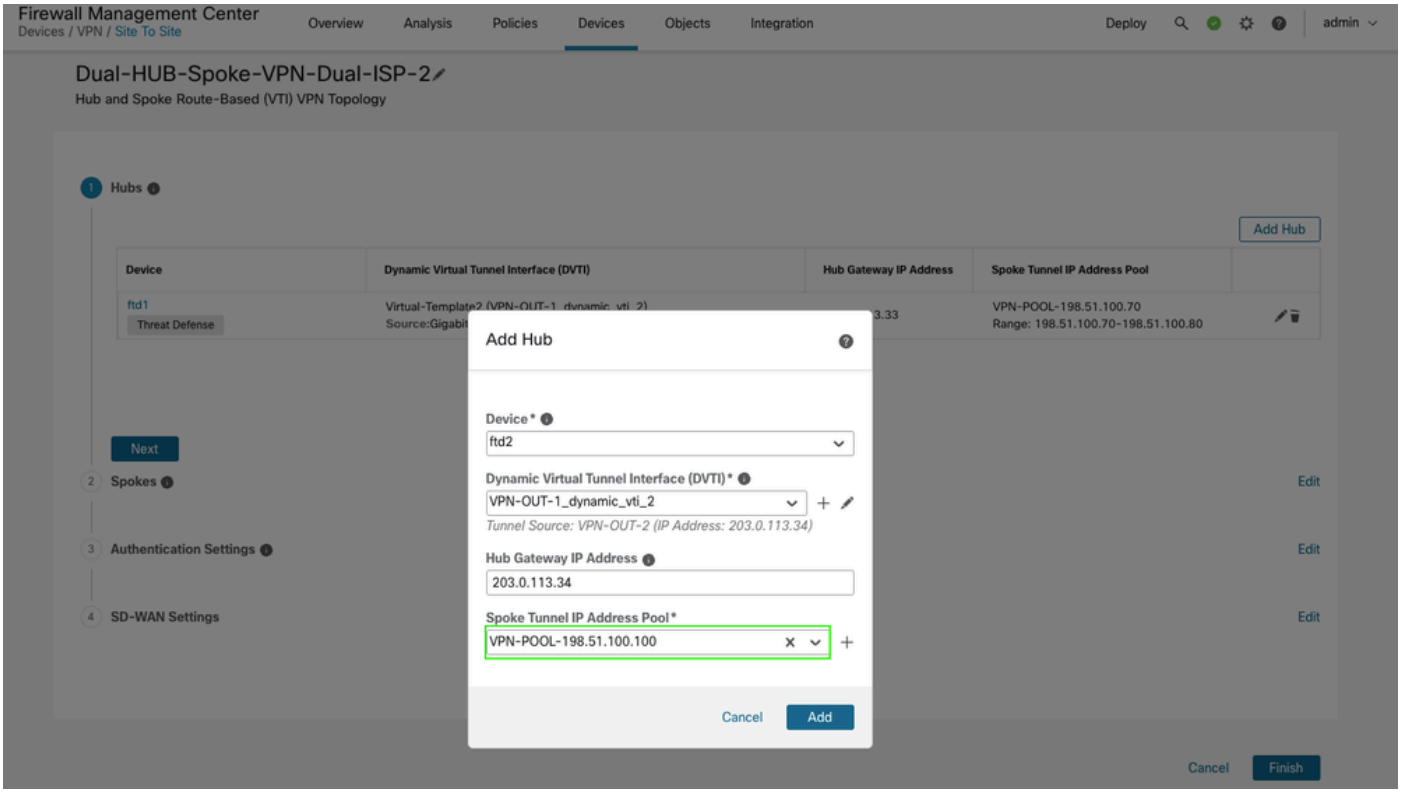
- Un pool d'adresses IP VPN supplémentaire est configuré spécifiquement pour les adresses VTI (Virtual Tunnel Interface) en étoile.





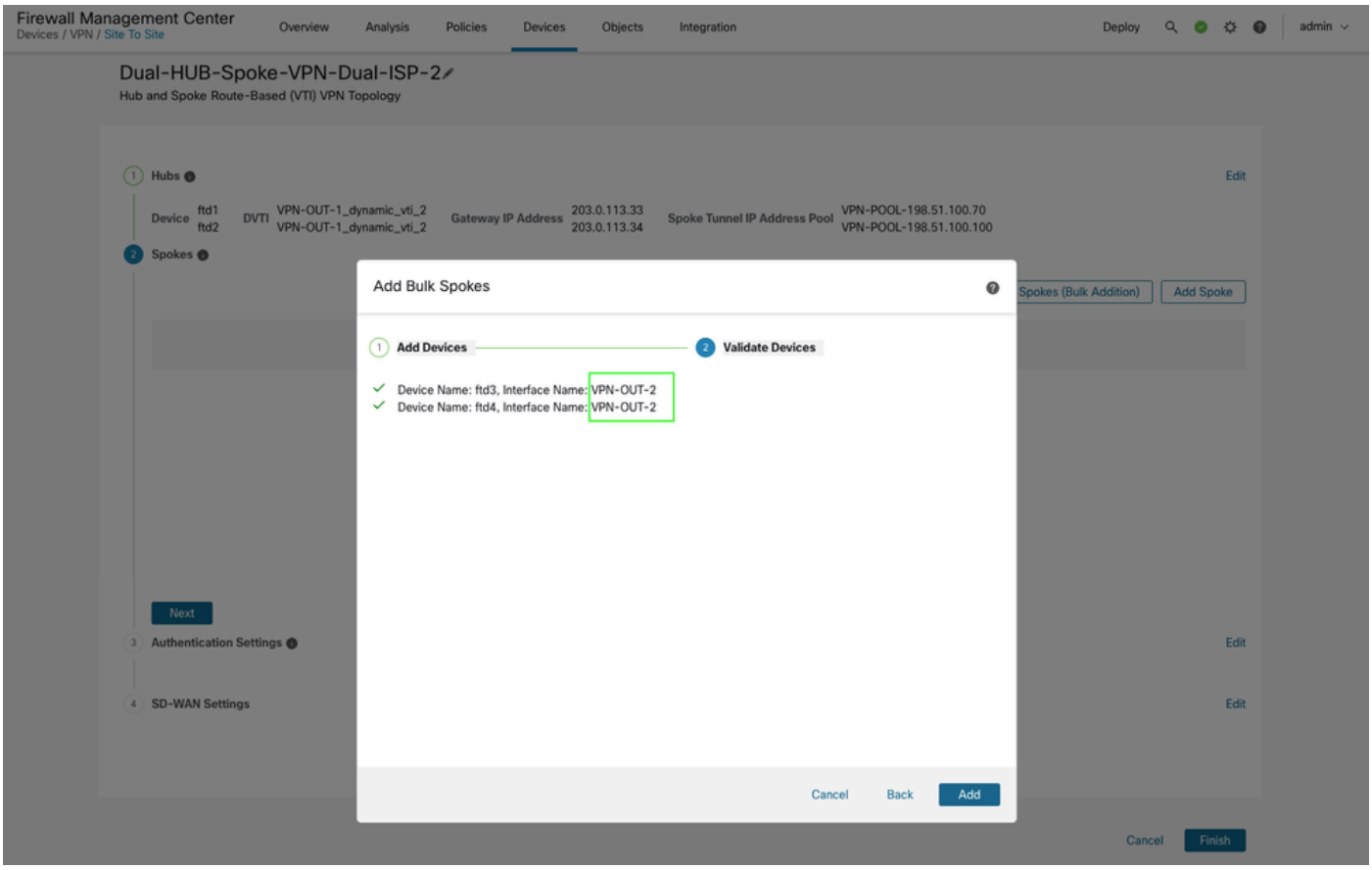
- Pour ajouter un concentrateur secondaire, répétez le processus en créant DVTI 2 à l'aide de l'interface ISP secondaire (VPN-OUT-2) et configurez un pool d'adresses IP supplémentaires pour les adresses VTI en étoile.

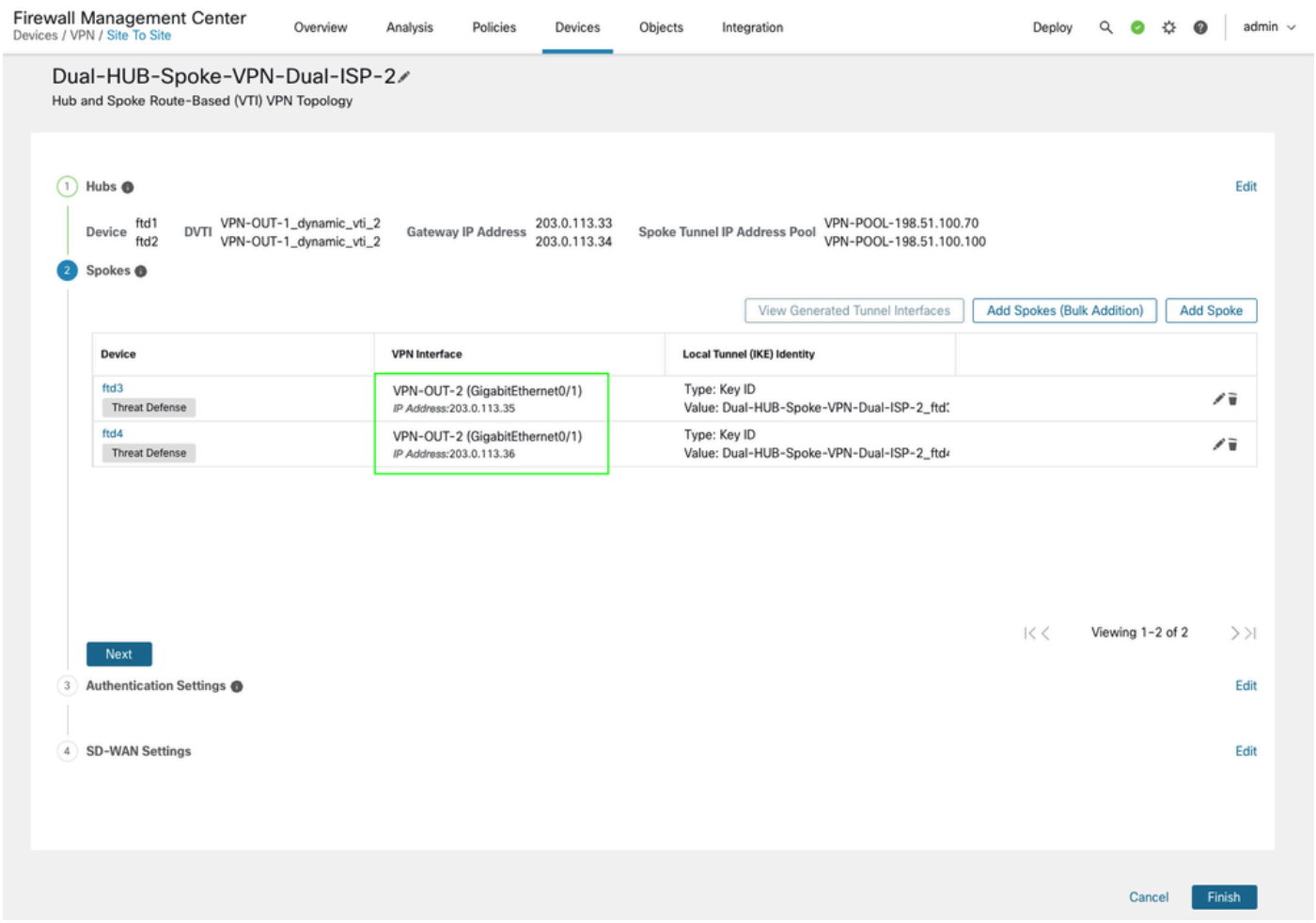




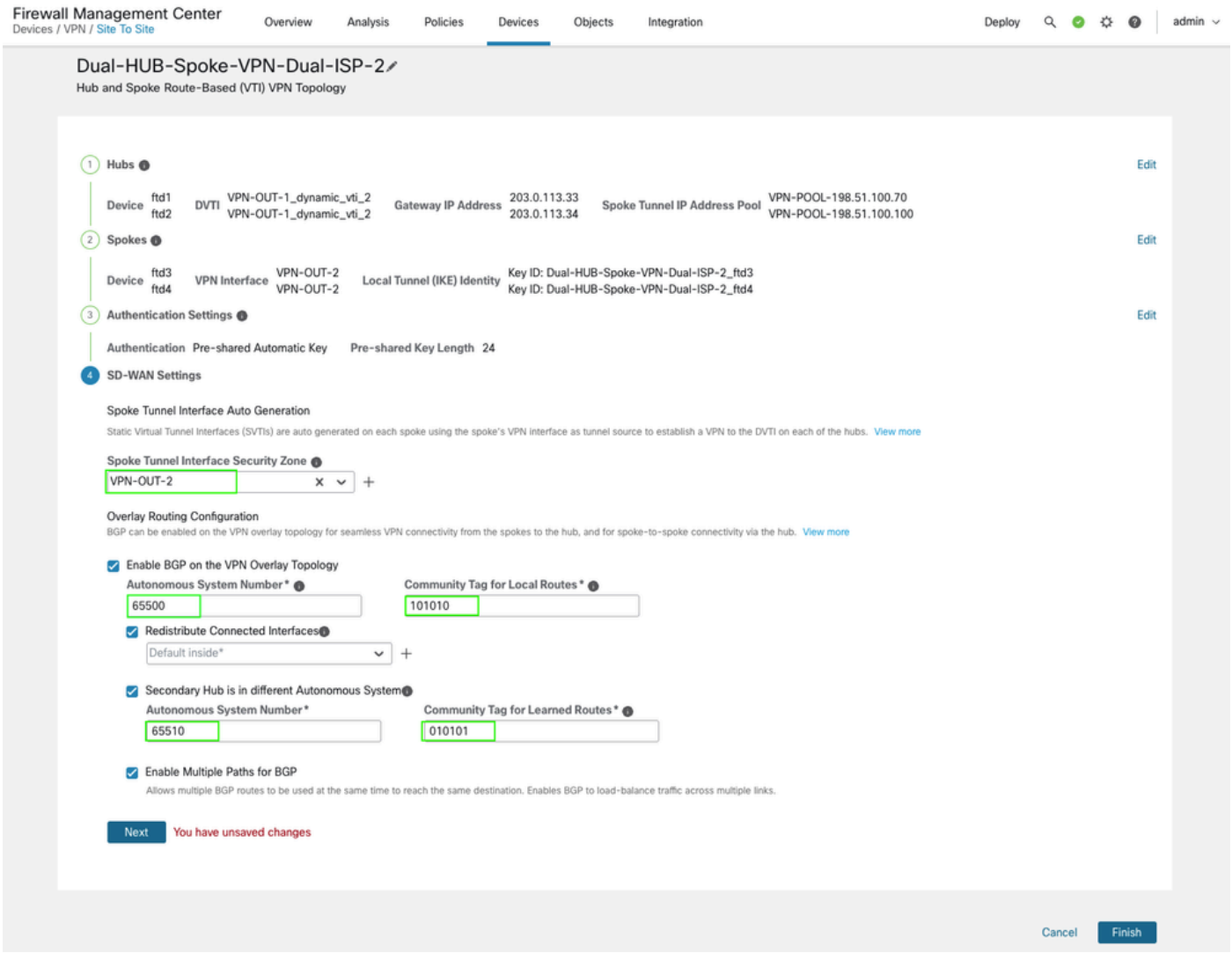
- Lors de l'ajout d'un rayon, assurez-vous que l'interface sous-jacente / WAN correcte est spécifiée pour les tunnels VTI. Cette topologie utilise l'interface VPN-OUT-2 de l'ISP

secondaire.


Firewall Management Center
Devices / VPN / Site To Site
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
Dual-HUB-Spoke-VPN-Dual-ISP-2
Hub and Spoke Route-Based (VTI) VPN Topology
Hubs
Edit
Device ftd1 ftd2
DVTI VPN-OUT-1_dynamic_vti_2 VPN-OUT-1_dynamic_vti_2
Gateway IP Address 203.0.113.33 203.0.113.34
Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.70 VPN-POOL-198.51.100.100
Spokes
Add Bulk Spokes
Add Devices
Validate Devices
Device Name: ftd3, Interface Name: VPN-OUT-2
Device Name: ftd4, Interface Name: VPN-OUT-2
Spokes (Bulk Addition)
Add Spoke
Cancel
Back
Add
Next
Authentication Settings
SD-WAN Settings
Cancel
Finish


Firewall Management Center
Devices / VPN / Site To Site
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
Dual-HUB-Spoke-VPN-Dual-ISP-2
Hub and Spoke Route-Based (VTI) VPN Topology
Hubs
Edit
Device ftd1 ftd2
DVTI VPN-OUT-1_dynamic_vti_2 VPN-OUT-1_dynamic_vti_2
Gateway IP Address 203.0.113.33 203.0.113.34
Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.70 VPN-POOL-198.51.100.100
Spokes
View Generated Tunnel Interfaces
Add Spokes (Bulk Addition)
Add Spoke
Device
VPN Interface
Local Tunnel (IKE) Identity
ftd3
Threat Defense
VPN-OUT-2 (GigabitEthernet0/1)
IP Address:203.0.113.35
Type: Key ID
Value: Dual-HUB-Spoke-VPN-Dual-ISP-2_ftd
ftd4
Threat Defense
VPN-OUT-2 (GigabitEthernet0/1)
IP Address:203.0.113.36
Type: Key ID
Value: Dual-HUB-Spoke-VPN-Dual-ISP-2_ftd
Viewing 1-2 of 2
Next
Authentication Settings
Edit
SD-WAN Settings
Edit
Cancel
Finish

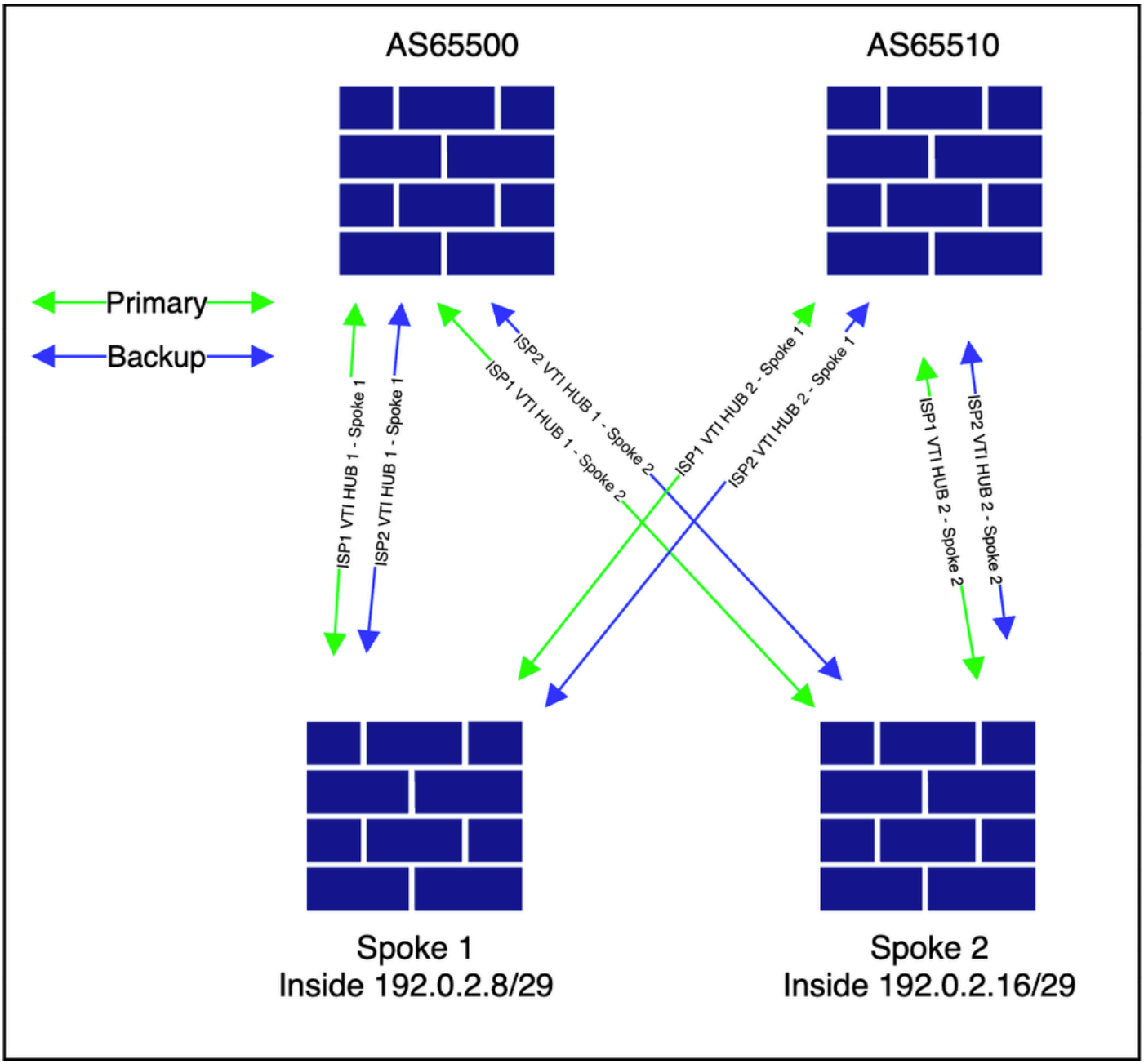
- Lors de la configuration du routage, assurez-vous que les balises de communauté et les numéros de système autonome des deux concentrateurs de cette topologie sont cohérents avec ceux utilisés dans la topologie précédente du routeur ISP1. La topologie utilise différentes zones de sécurité, mais les configurations restantes, telles que les numéros de système autonome pour les concentrateurs principal et secondaire, ainsi que les balises de communauté sont identiques. Cette opération est obligatoire pour que l'interface utilisateur puisse valider la topologie.



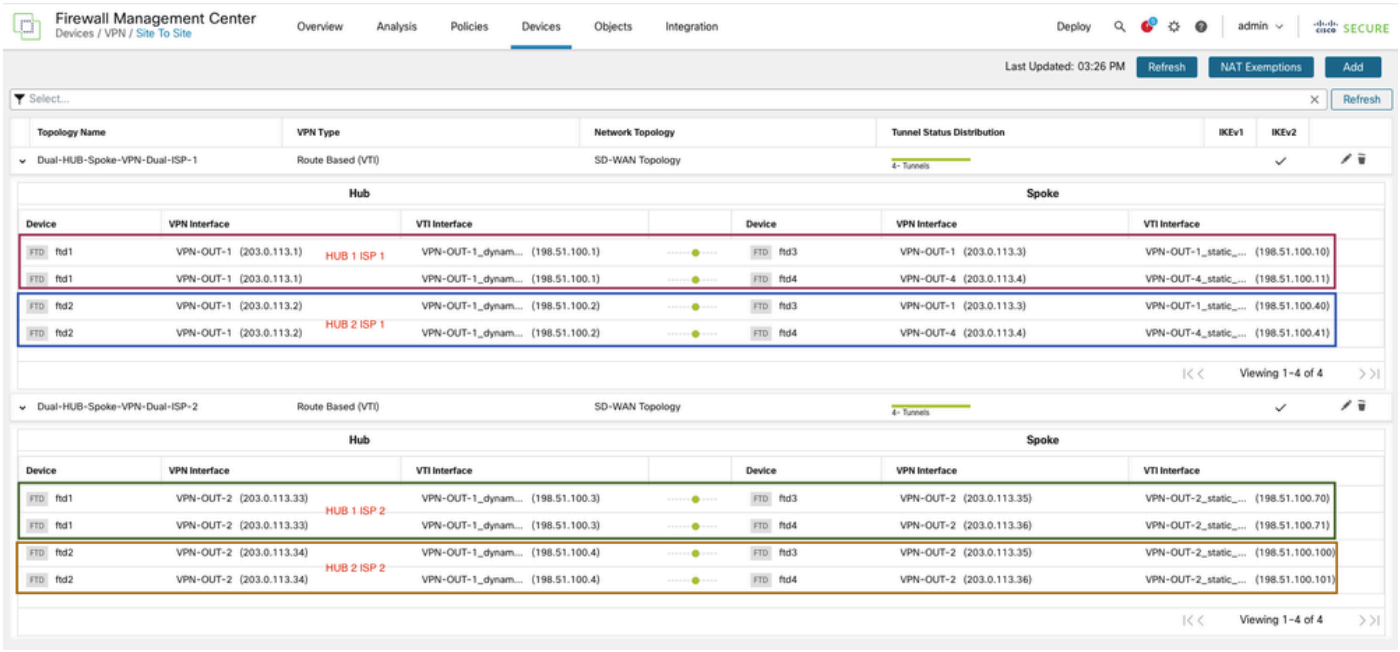
- Tous les autres paramètres restent inchangés. Terminez l'Assistant et poursuivez le déploiement.

Vérification

- La topologie apparaît comme illustré.



- Accédez à Devices > VPN > Site to Site pour afficher la topologie.



Cette configuration entraîne quatre appairages BGP par périphérique, et chaque rayon possède les routes appropriées pour atteindre les autres rayons. Par exemple, vous pouvez récupérer la sortie de l'un des rayons.

Pour le satellite 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 table de routage apparaît comme indiqué, ce qui confirme que la charge du trafic est équilibrée entre les deux liaisons côté satellite.

```
<#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
```

Conclusion

L'objectif de cet article est d'expliquer divers scénarios de déploiement qui peuvent être facilement mis en oeuvre à l'aide d'un seul assistant de configuration.

Informations connexes

- Pour obtenir de l'aide supplémentaire, contactez le TAC. Un contrat d'assistance valide est requis :Contacts d'assistance internationale Cisco.
- Vous pouvez également visiter la communauté VPN Cisco ici.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.