Konfiguration von SD-WAN für Site-to-Site-VPN über sichere Firewall

Inhalt

Einleitung

In diesem Dokument werden routenbasierte VPN-Bereitstellungsszenarien mit BGP-Overlay-Routing unter Verwendung der SD-WAN-Funktion der sicheren Firewall beschrieben.

Voraussetzungen

Auf allen Hubs und Stationen wird FTD 7.6 oder höher ausgeführt, und die Verwaltung erfolgt über dasselbe FMC, auf dem auch Software der Version 7.6 oder höher ausgeführt wird.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- IKEv2
- Routenbasiertes VPN
- Virtuelle Tunnelschnittstellen (VTI)
- IPsec
- BGP

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Informationen zu Funktionen

Das Management Center vereinfacht die Konfiguration von VPN-Tunneln und das Routing zwischen zentralisierten Hauptgeschäftsstellen (Hubs) und Außenstellen (Spokes) mithilfe des neuen SD-WAN-Assistenten.

・ Automatisiert die VPN-Konfiguration durch die Nutzung von DVTI (Dynamic Virtual Tunnel Interface) auf Hubs und SVTI (Static Virtual Tunnel Interface) auf Stationen, wobei das Overlay-Routing über BGP aktiviert wird.

・ Automatische Zuweisung von SVTI-IP-Adressen für Stationen und Übertragung der gesamten VTI-Konfiguration, einschließlich Verschlüsselungsparametern.

・ Einfache Routing-Konfiguration in einem Schritt mit demselben Assistenten zur Aktivierung von BGP für Overlay-Routing

・ Skalierbares und optimales Routing durch Nutzung des Route-Reflector-Attributs für BGP

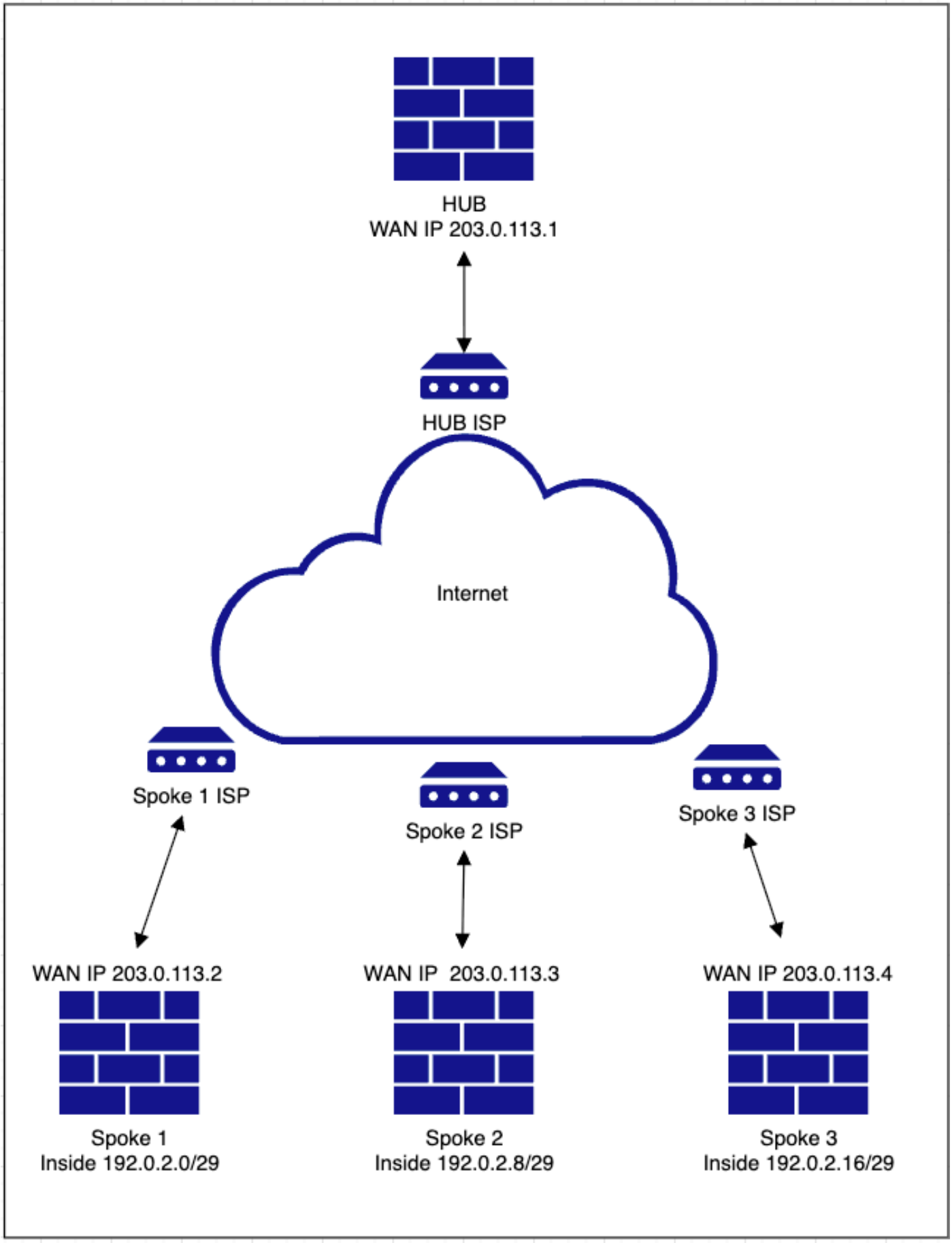
・ Gleichzeitiges Hinzufügen mehrerer Speichen bei minimalem Benutzereingriff

Behandelte Topologien

In diesem Artikel werden mehrere Topologien behandelt, um sicherzustellen, dass Benutzer die verschiedenen Bereitstellungsszenarien kennen.

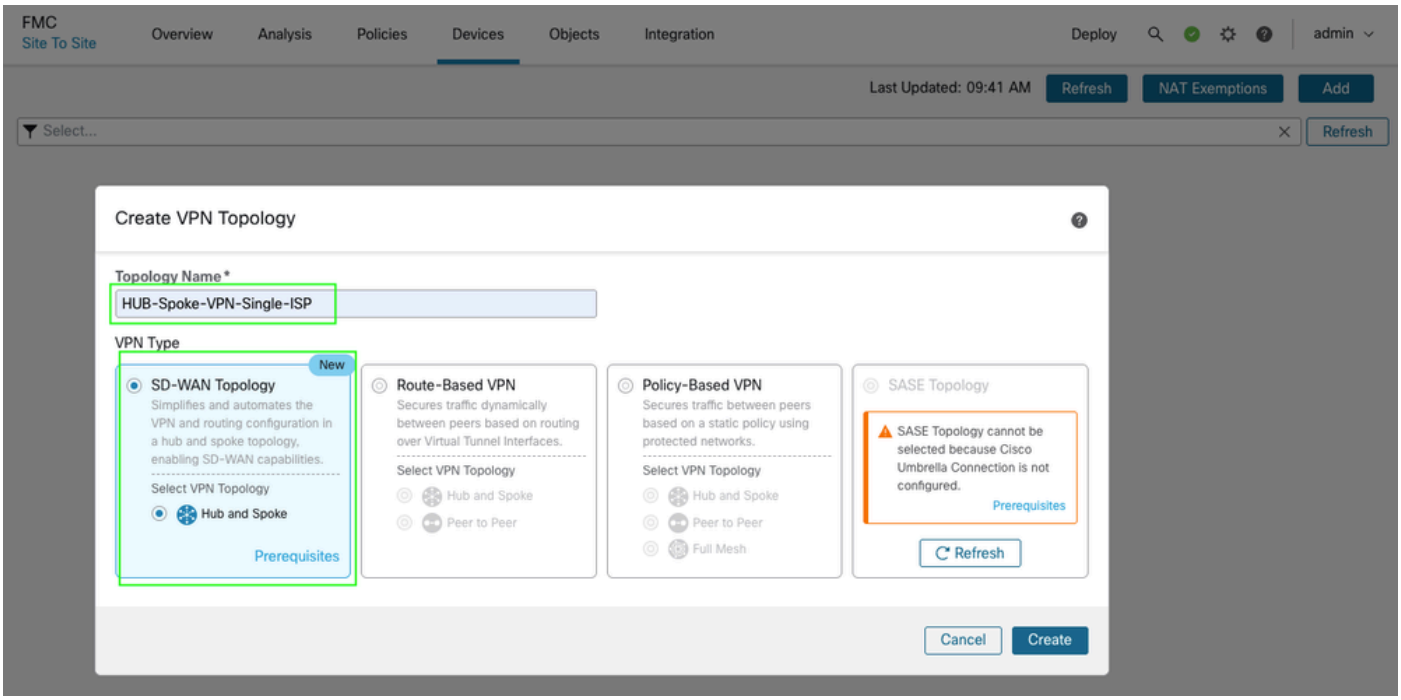
HUB und Spoke (einzelner ISP)

Netzwerkdiagramm

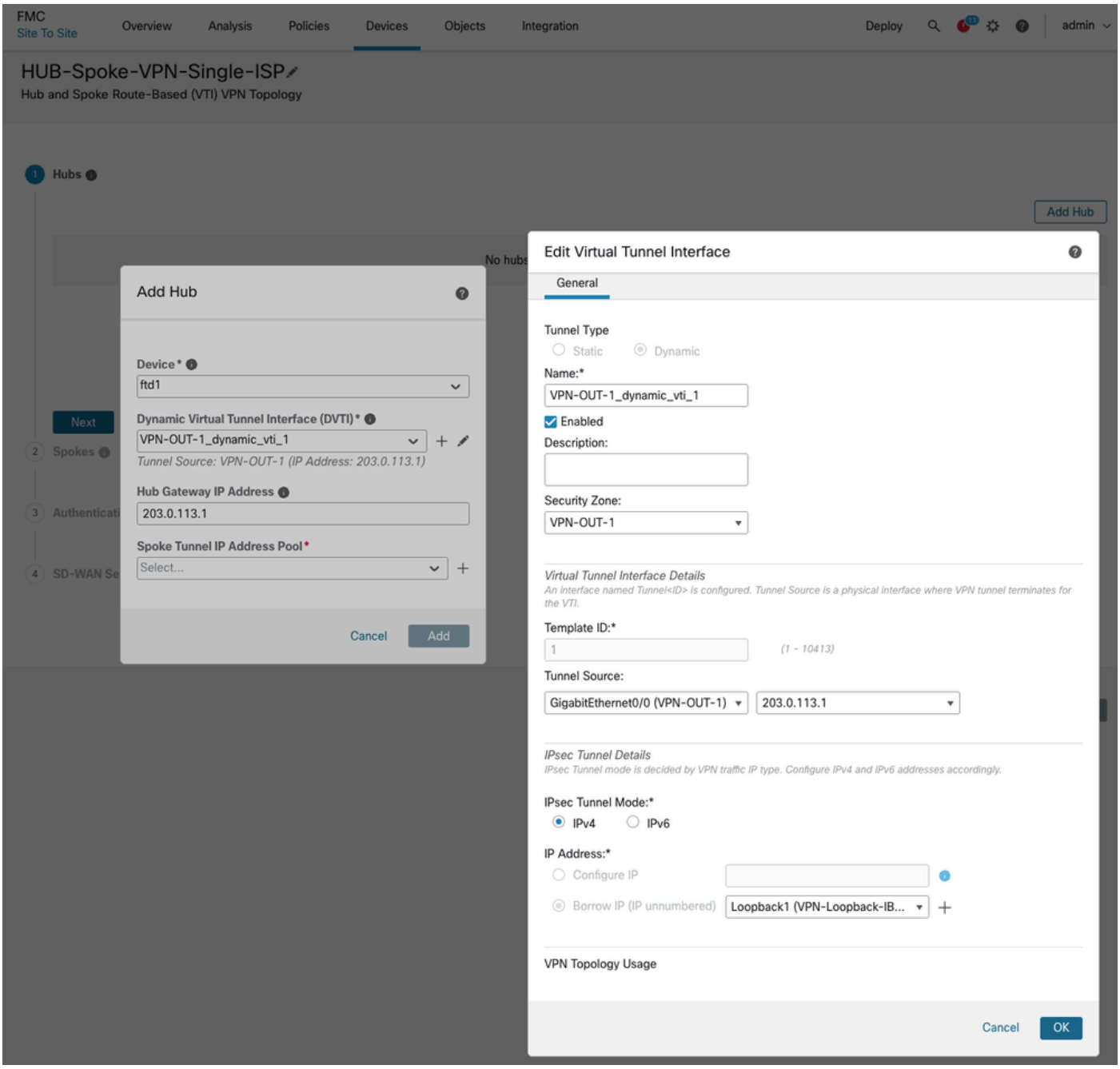


Konfigurationen

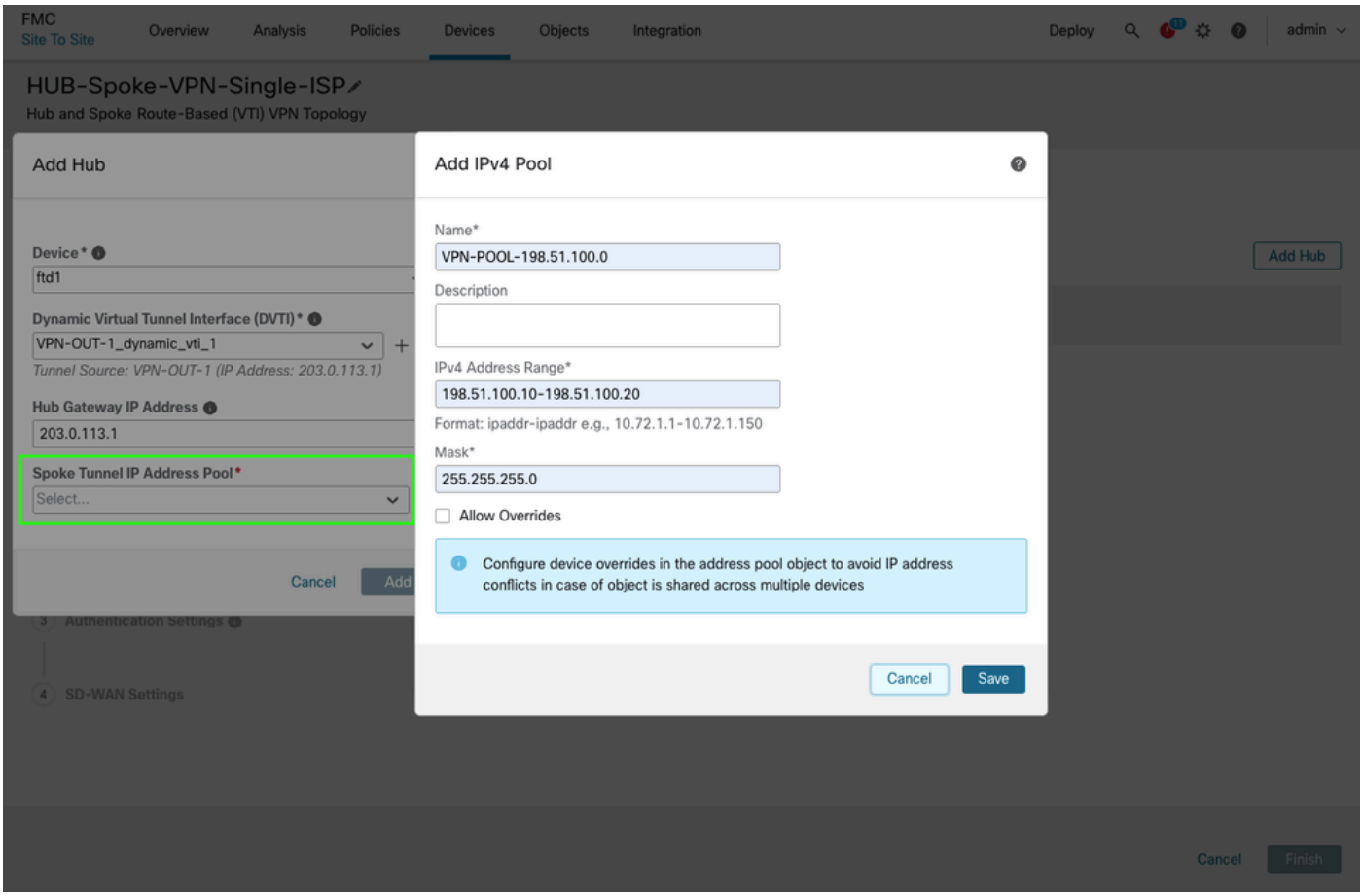
- Navigieren Sie zu Devices > VPN > Site to Site > Add > SD-WAN Topology > > Create.

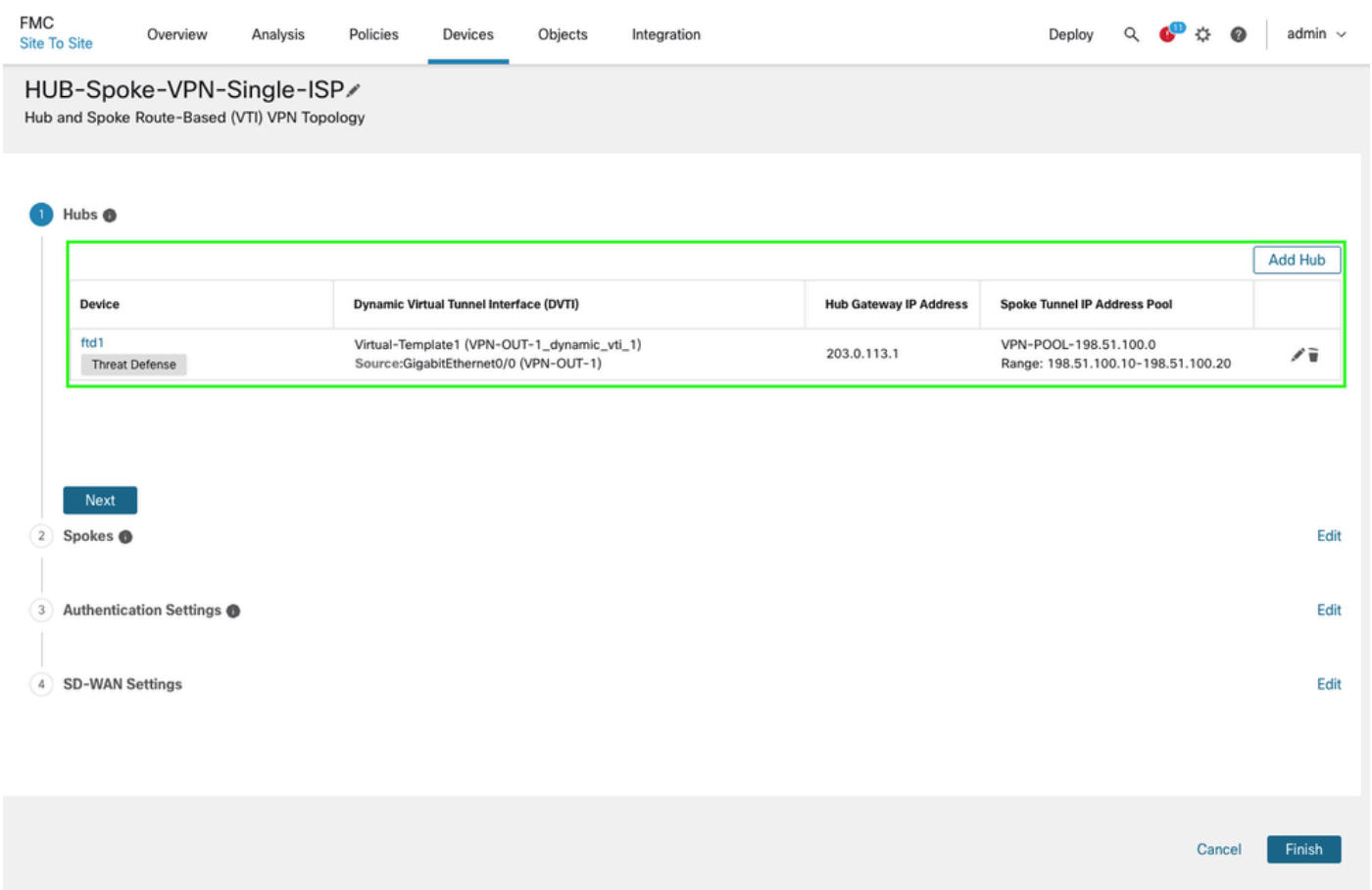


・ Hinzufügen eines Hubs und Erstellen einer DVTI am Hub-Ende Stellen Sie im Rahmen der DVTI-Konfiguration sicher, dass Sie die richtige Tunnel-Quellschnittstelle entsprechend der Topologie auswählen.



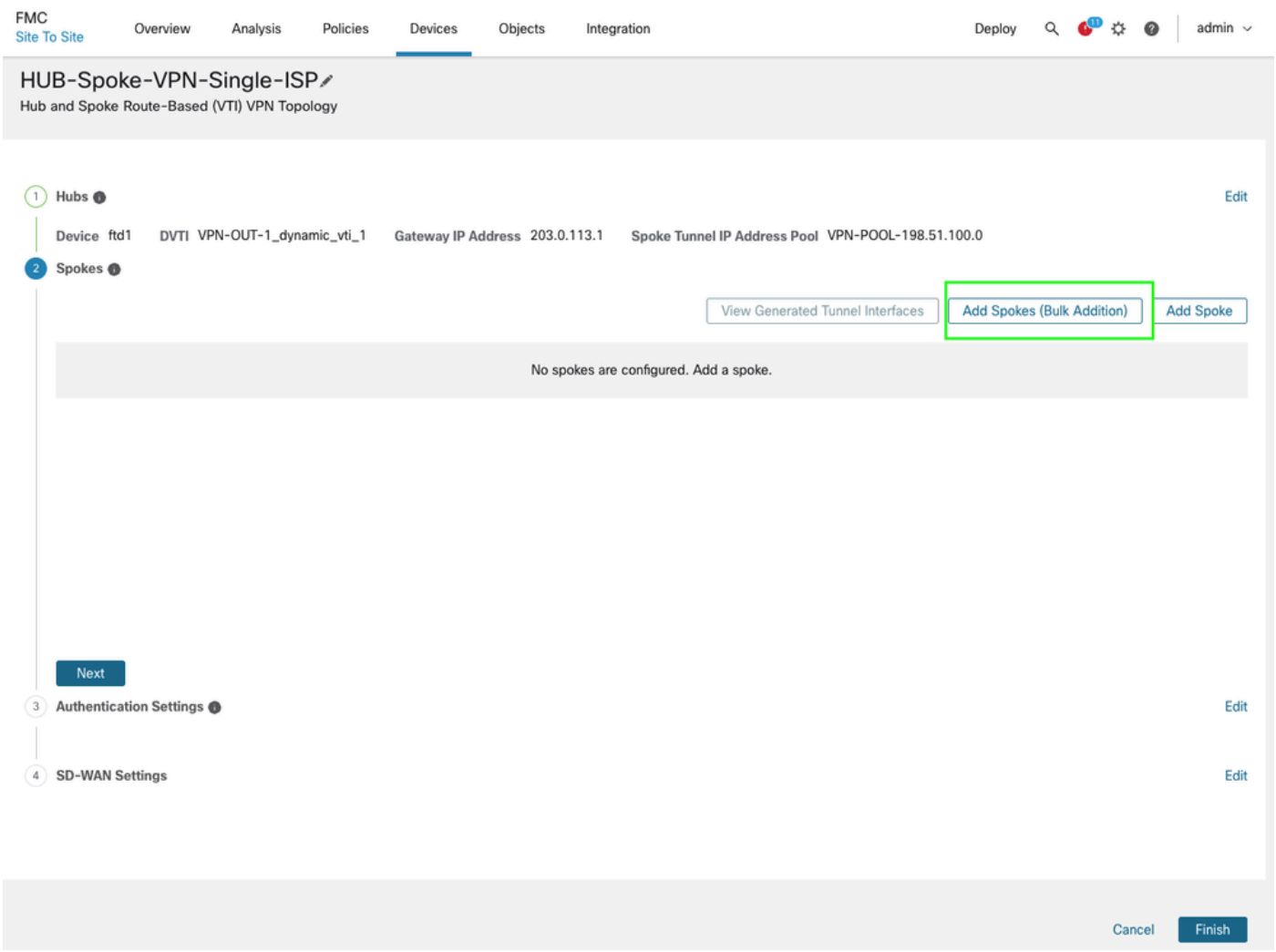
- Erstellen Sie einen IP-Adresspool für den Spoke-Tunnel, und klicken Sie auf Speichern und dann auf Hinzufügen. Der IP-Adresspool wird verwendet, um den Stationen IP-Adressen des VTI-Tunnels zuzuweisen.



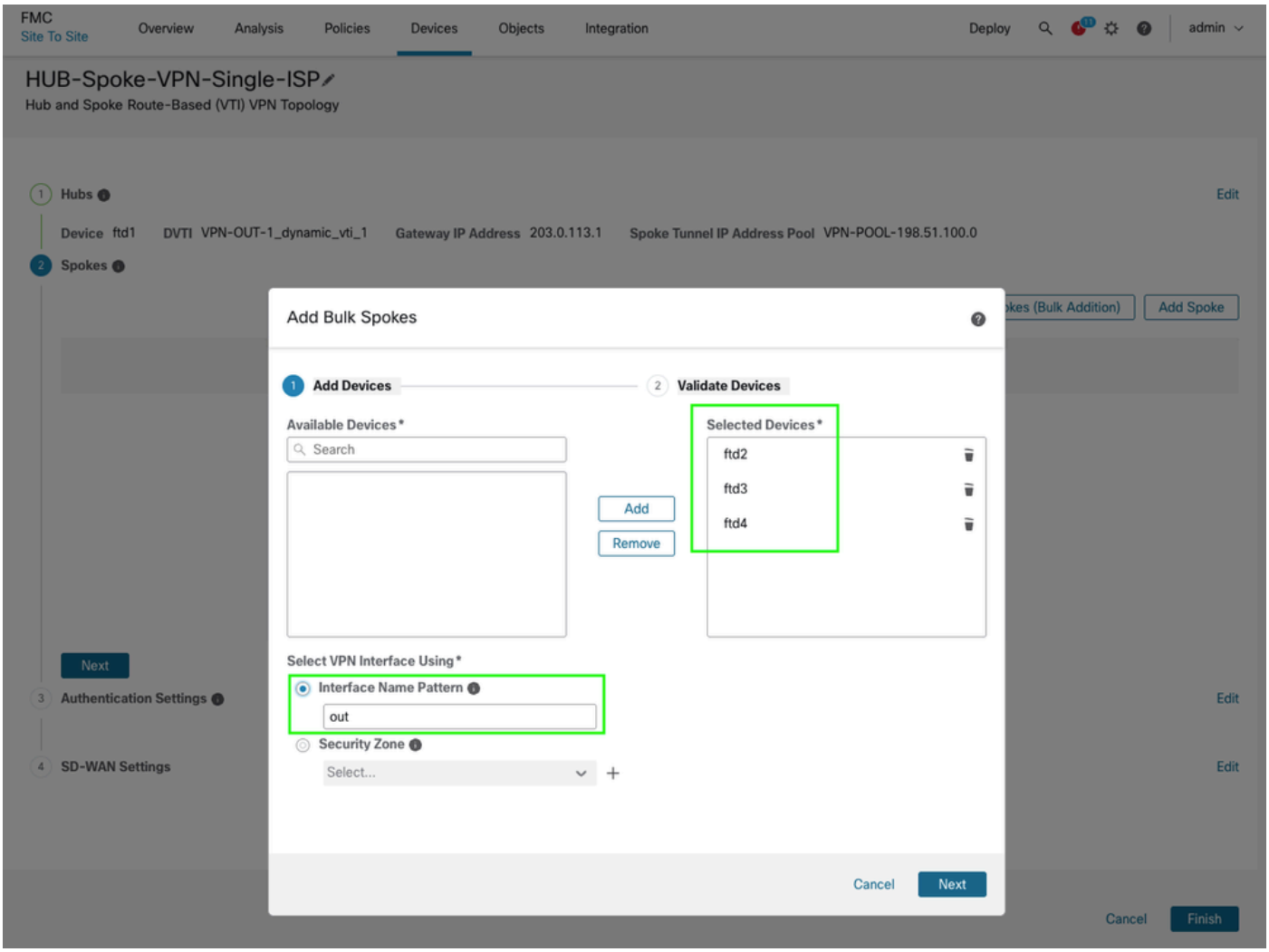


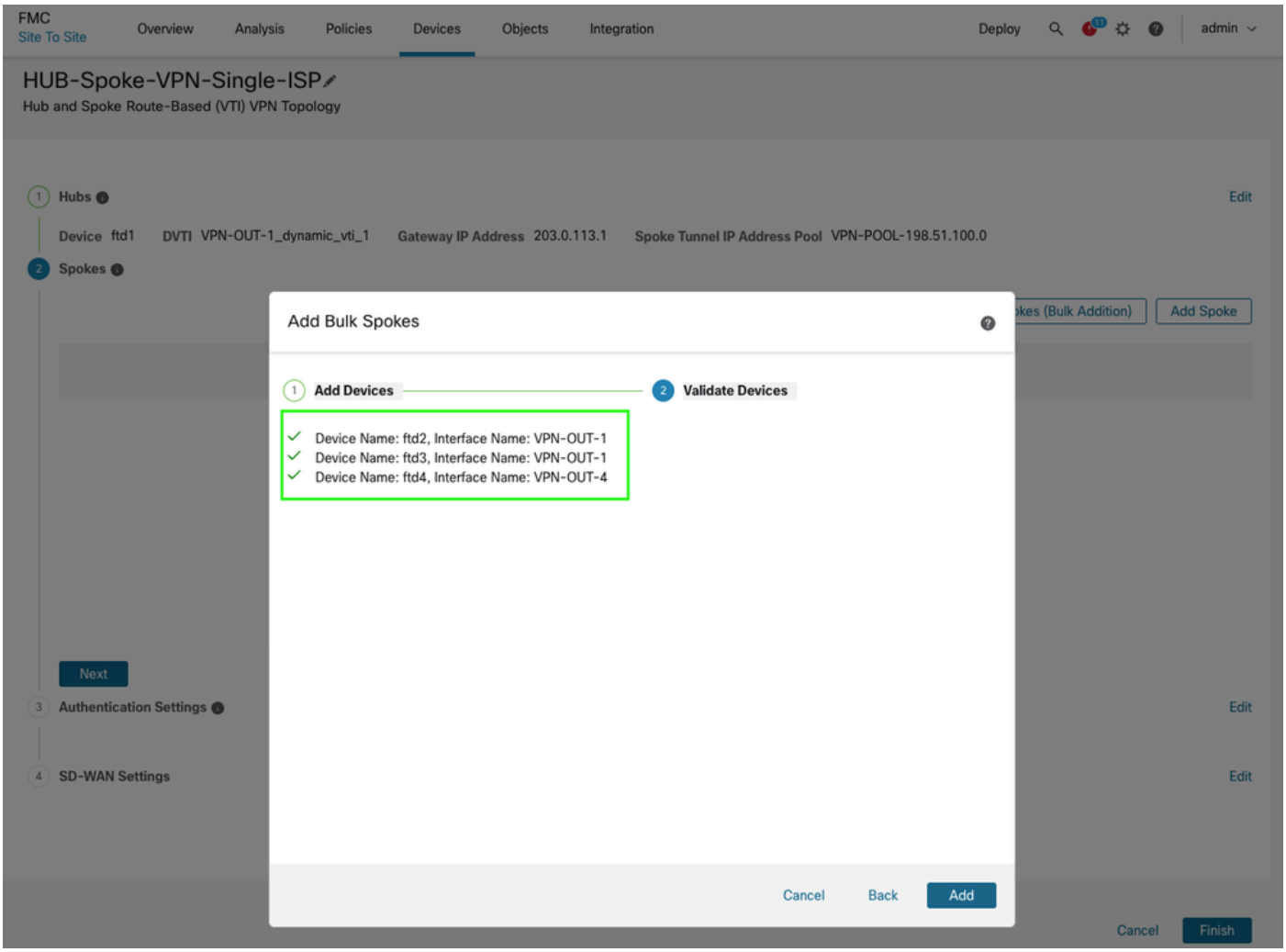
- Klicken Sie auf Weiter, um fortzufahren und die Speichen hinzuzufügen. Sie können entweder eine Bulk-Hinzufügungsoption nutzen, wenn Sie allgemeine Schnittstellen-

/Zonennamen haben, oder Stationen einzeln hinzufügen.

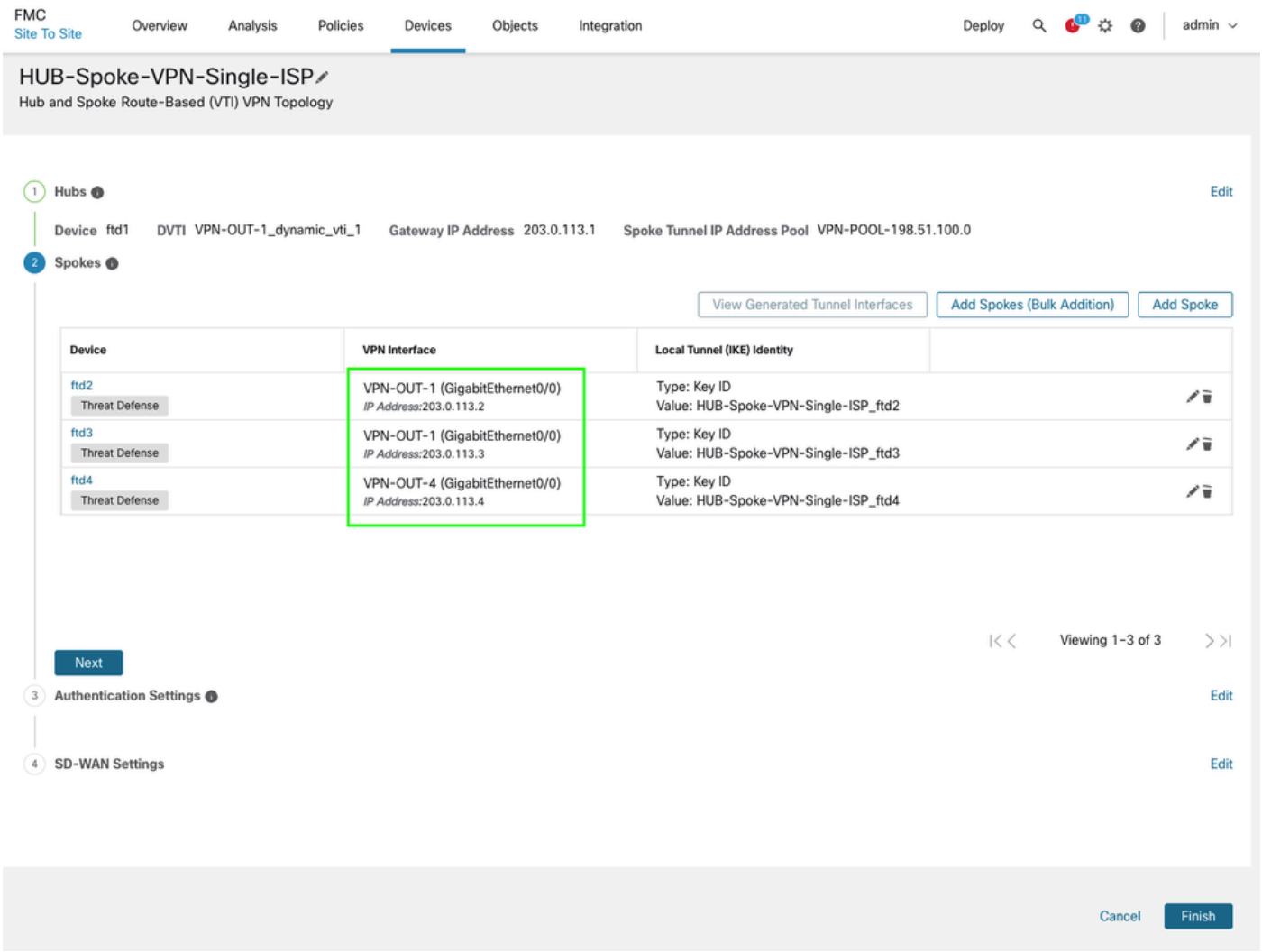


- Wählen Sie die Geräte aus, und geben Sie ein Namensmuster für die WAN-/externe Schnittstelle an. Wenn die Geräte denselben Schnittstellennamen verwenden, ist die Verwendung von Initialen ausreichend. Klicken Sie auf Weiter, und wenn die Validierung erfolgreich ist, klicken Sie auf Hinzufügen. Bei Massenadditionen können Sie den Zonennamen auf die gleiche Weise verwenden.

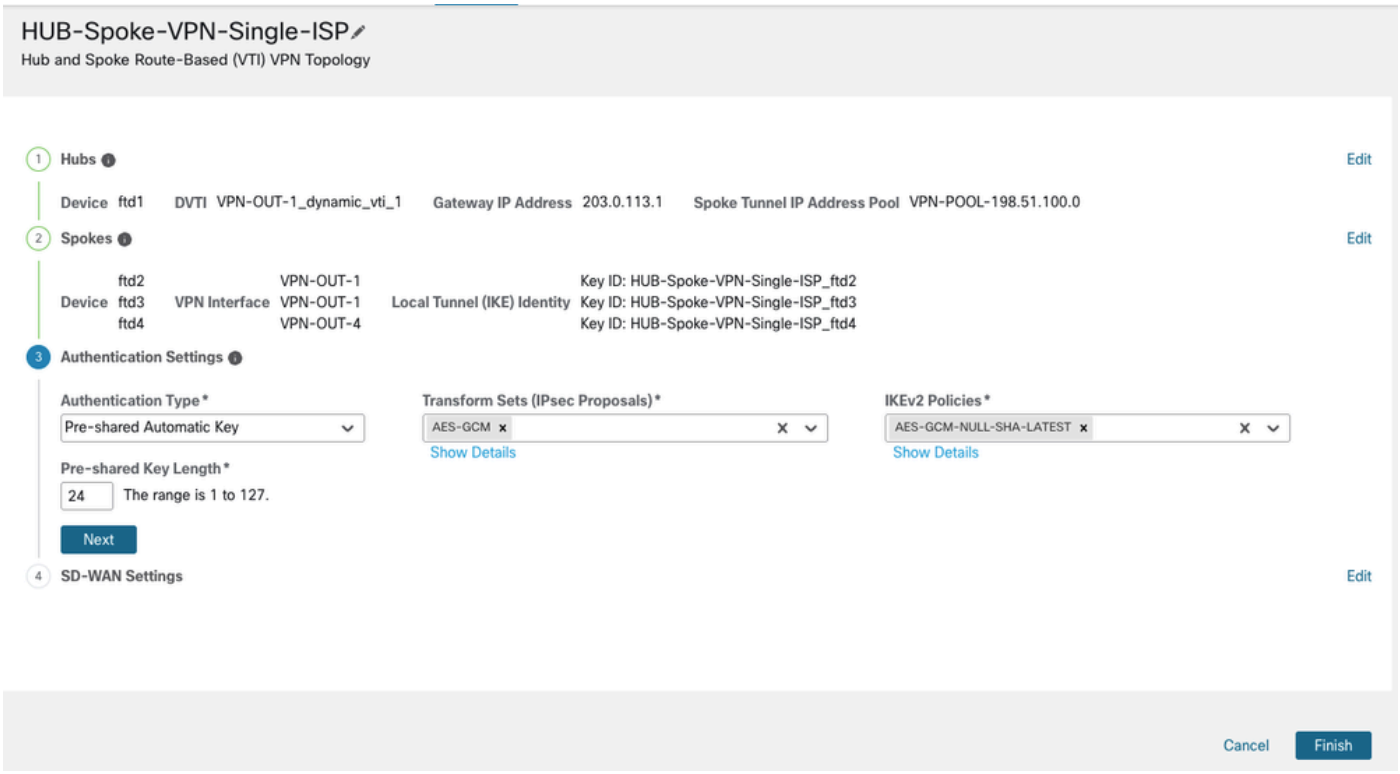

FMC
Site To Site
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
HUB-Spoke-VPN-Single-ISP
Hub and Spoke Route-Based (VTI) VPN Topology
1 Hubs
Edit
Device ftd1
DVTI VPN-OUT-1_dynamic_vti_1
Gateway IP Address 203.0.113.1
Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.0
2 Spokes
Add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



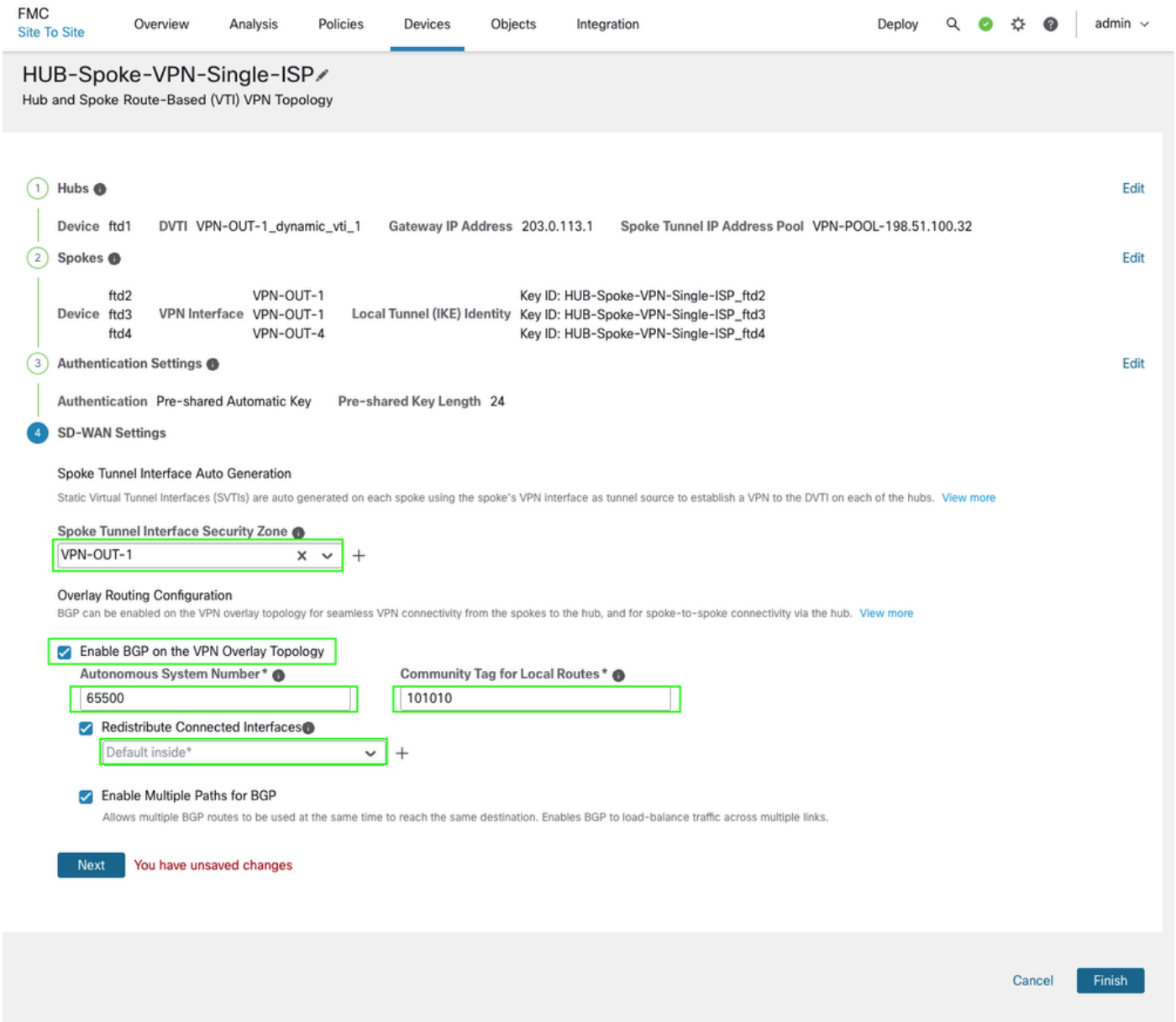
- Überprüfen Sie die Speichen- und Overlay-Schnittstellendetails, um sicherzustellen, dass die richtigen Schnittstellen ausgewählt sind, und klicken Sie dann auf Weiter.



- Sie können entweder die Standardparameter für die IPsec-Konfiguration beibehalten oder nach Bedarf benutzerdefinierte Chiffren angeben. Klicken Sie auf Weiter, um fortzufahren. In diesem Dokument werden die Standardparameter verwendet.



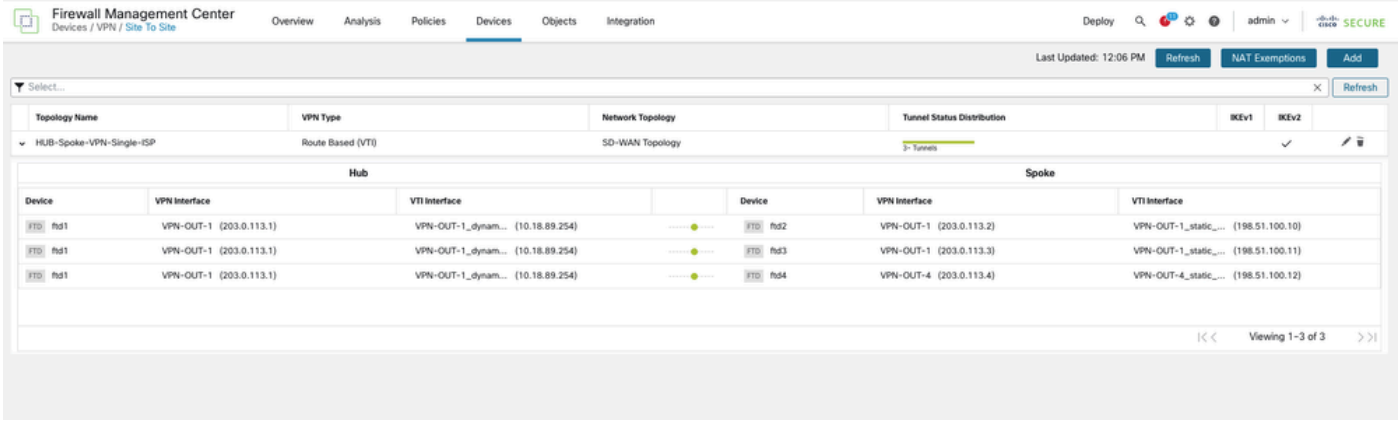
- Schließlich können Sie das Overlay-Routing im selben Assistenten für diese Topologie konfigurieren, indem Sie die entsprechenden BGP-Parameter wie die AS-Nummer, die interne Schnittstellenankündigung und Community-Tags für die Präfixfilterung angeben. Die Sicherheitszone kann bei der Filterung des Datenverkehrs mithilfe von Zugriffskontrollrichtlinien helfen. Sie können außerdem ein Objekt für Schnittstellen erstellen und diese bei der Neuverteilung verbundener Schnittstellen verwenden, wenn der Name nicht der interne Name ist oder nicht symmetrisch zu den Geräten in der Topologie ist.



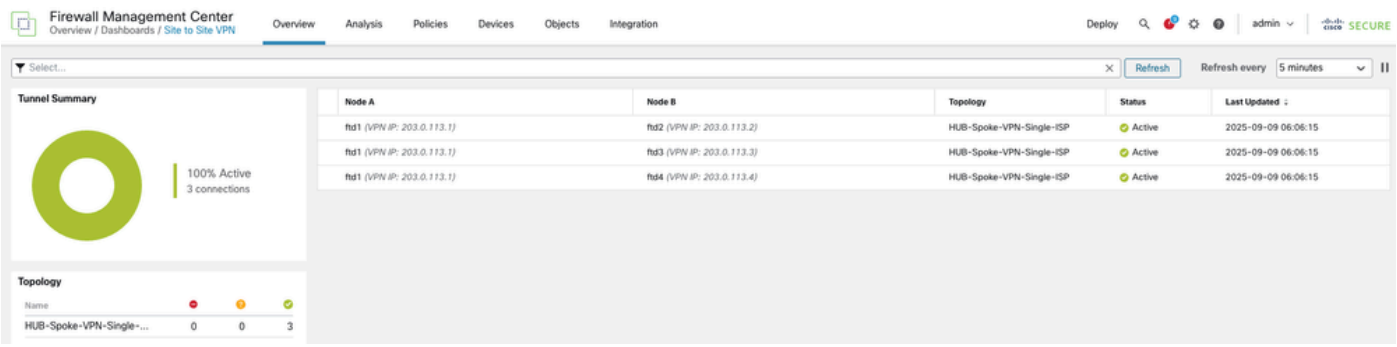
- Klicken Sie auf Weiter, dann auf Fertig stellen und schließlich auf Bereitstellen, um den Prozess abzuschließen.

Verifizierung

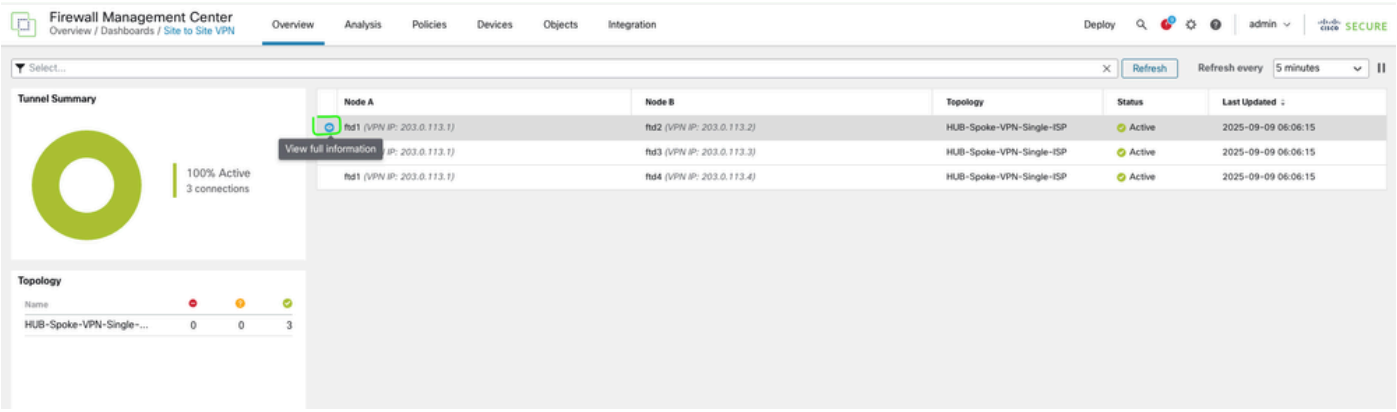
- Sie können den Tunnelstatus überprüfen, indem Sie zu Devices (Geräte) > VPN (VPN) > Site to Site (Site-to-Site) navigieren.

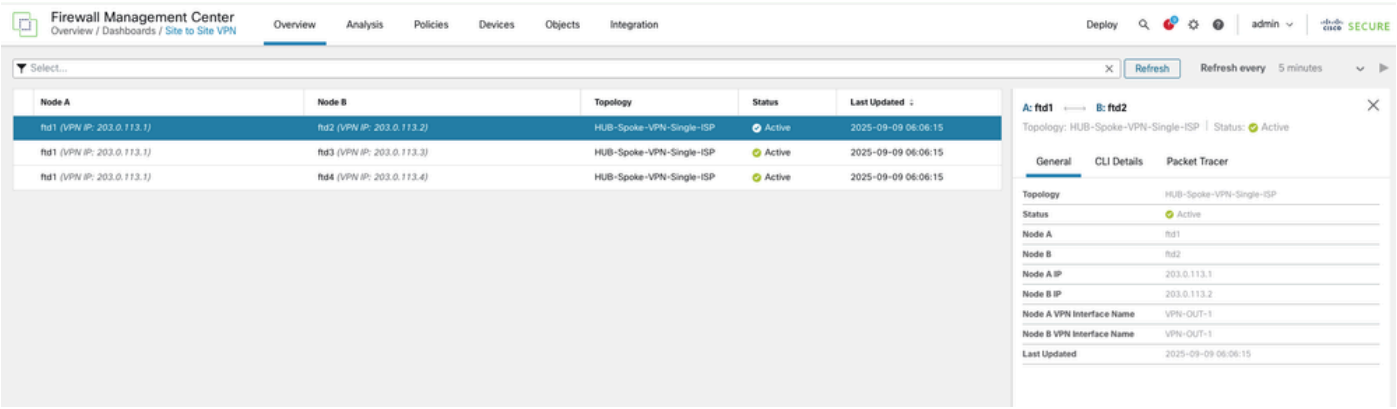


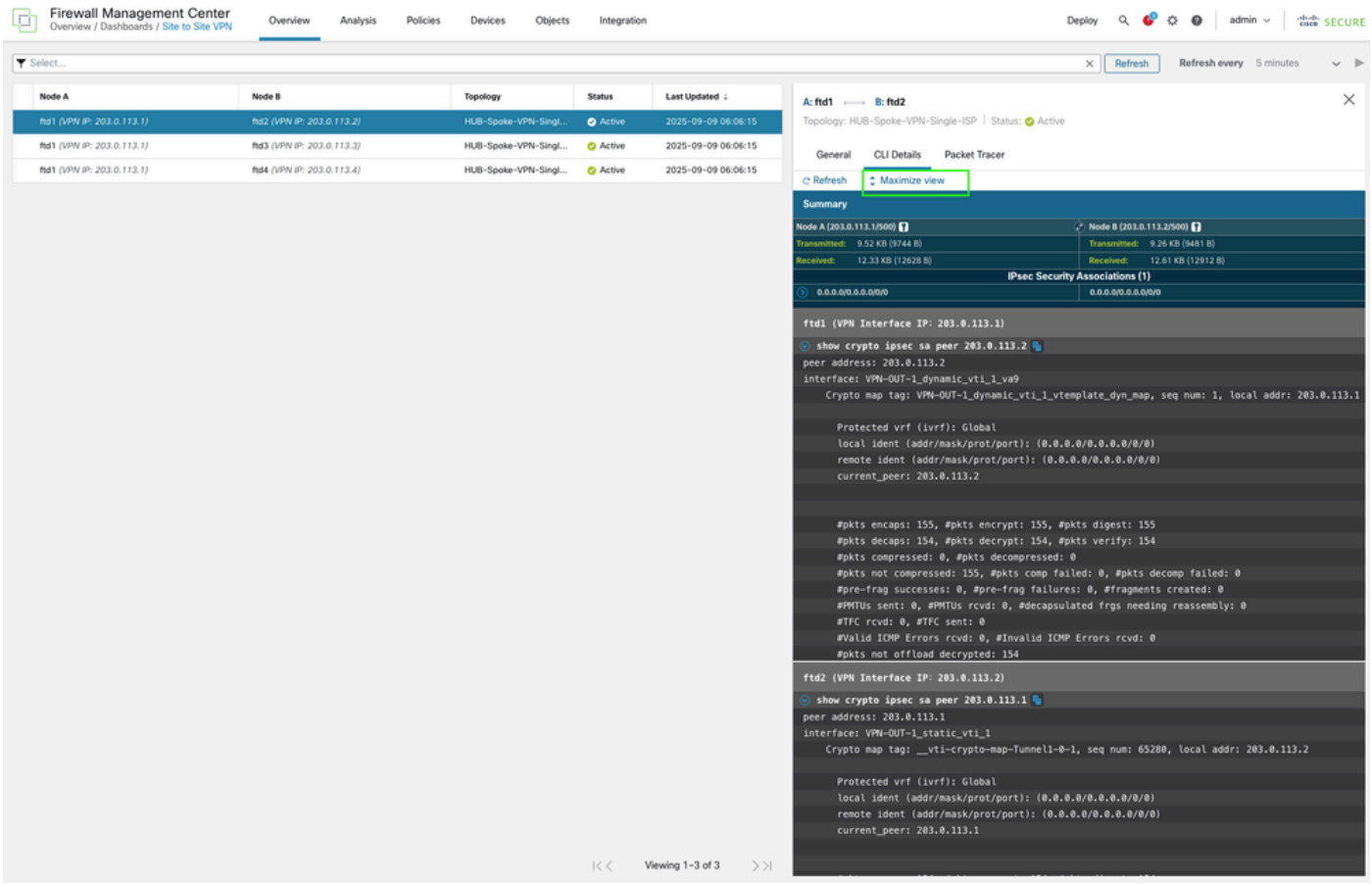
- Weitere Details können unter Übersicht > Dashboards > Site-to-Site-VPN überprüft werden.



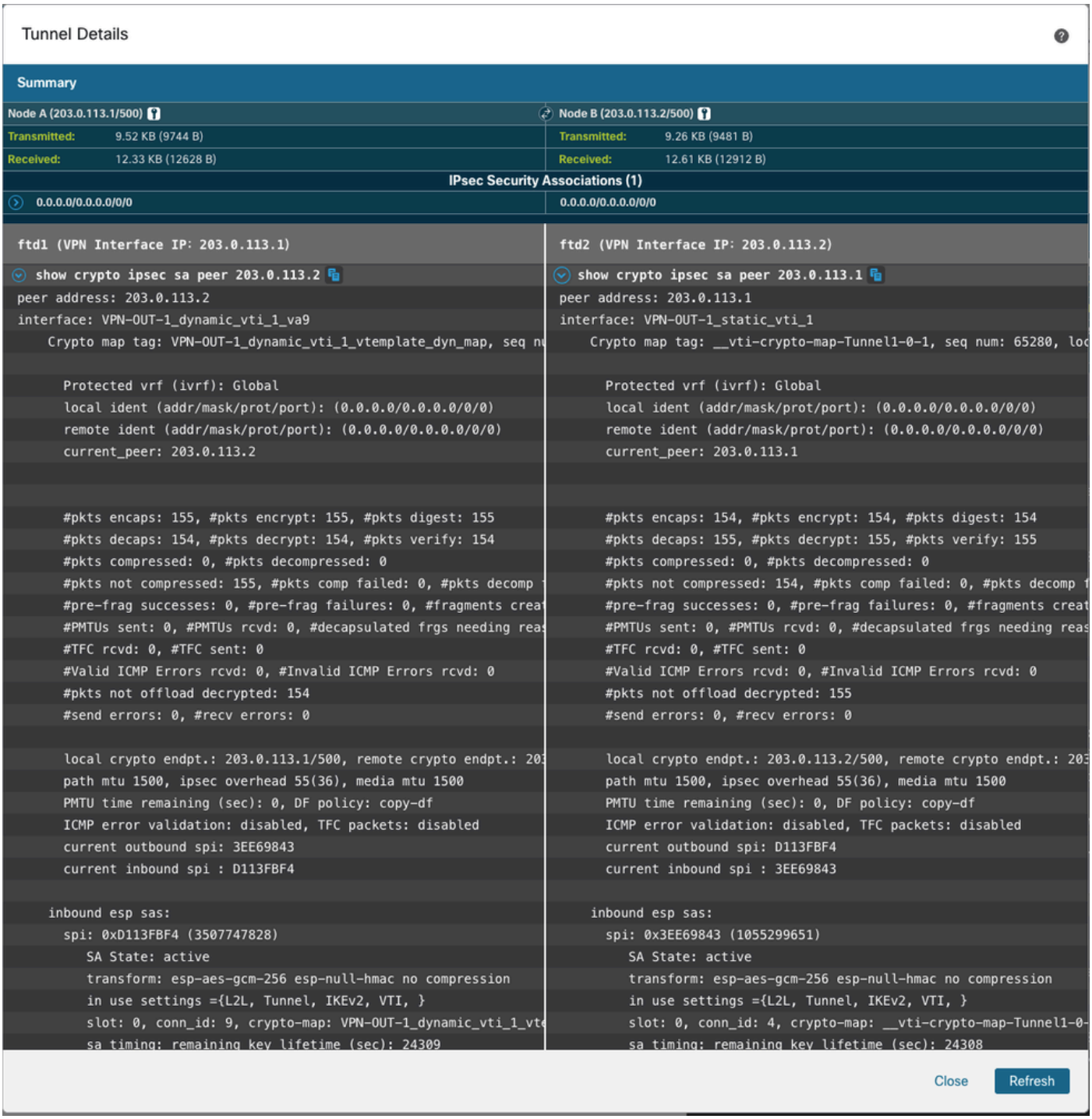
- Um weitere Einblicke zu erhalten, wählen Sie den Tunnel aus, und klicken Sie auf Vollständige Informationen anzeigen.







- Die Ausgabe wird direkt über die FTD-CLI angezeigt und kann aktualisiert werden, um aktualisierte Zähler und wichtige Informationen anzuzeigen, z. B. Details zum Sicherheitsparameterindex (SPI).



- Die FTD-CLI kann auch verwendet werden, um Routing-Informationen und den BGP-Peering-Status zu überprüfen.

HUB-seitig

<#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
```

auf Spoke-Seite

Die gleiche Überprüfung kann auch an den Spoke-Geräten durchgeführt werden. Hier ist ein Beispiel aus einer der Speichen.

<#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
```

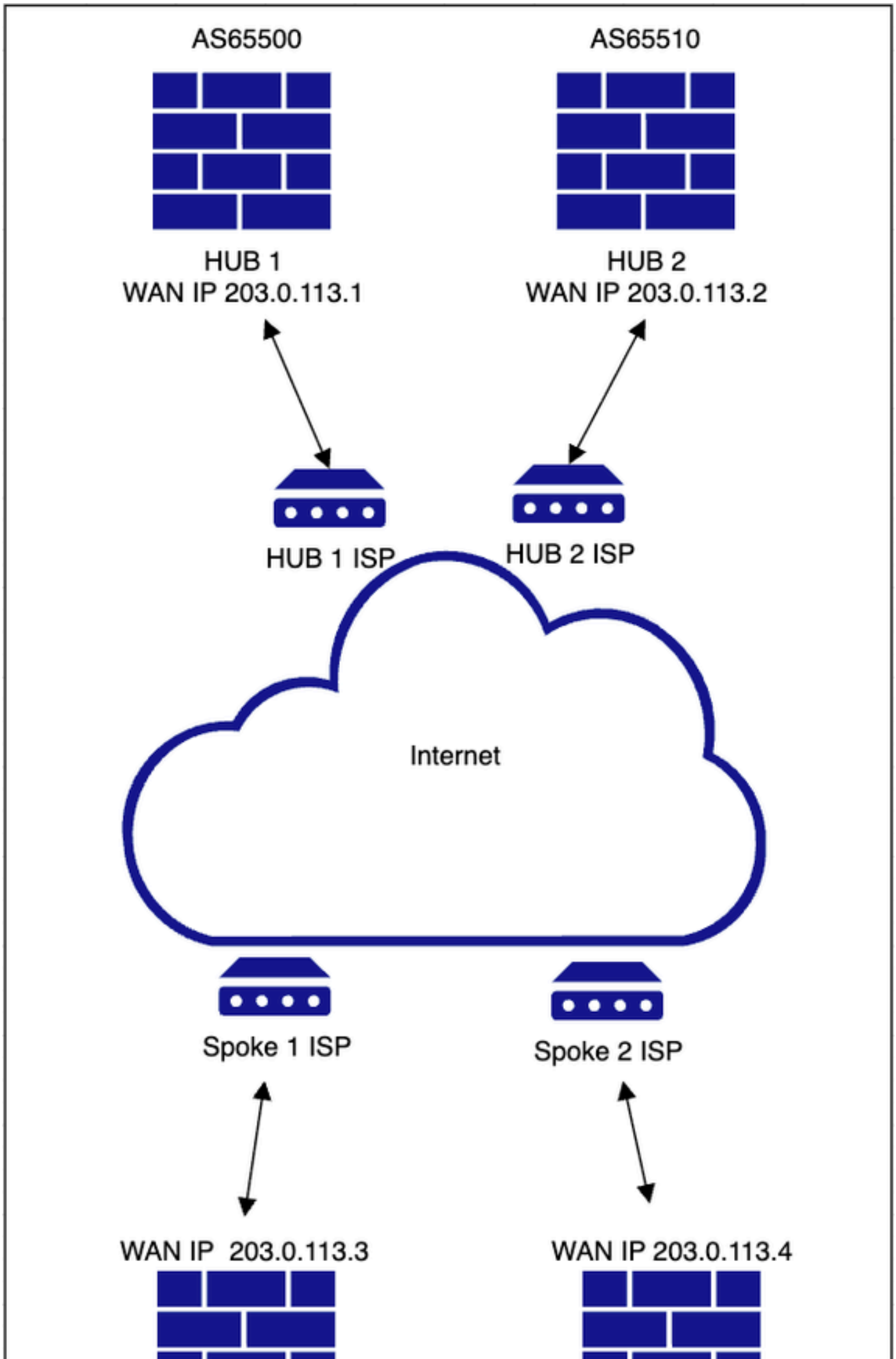
<<<<<< spoke 2 inside network

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

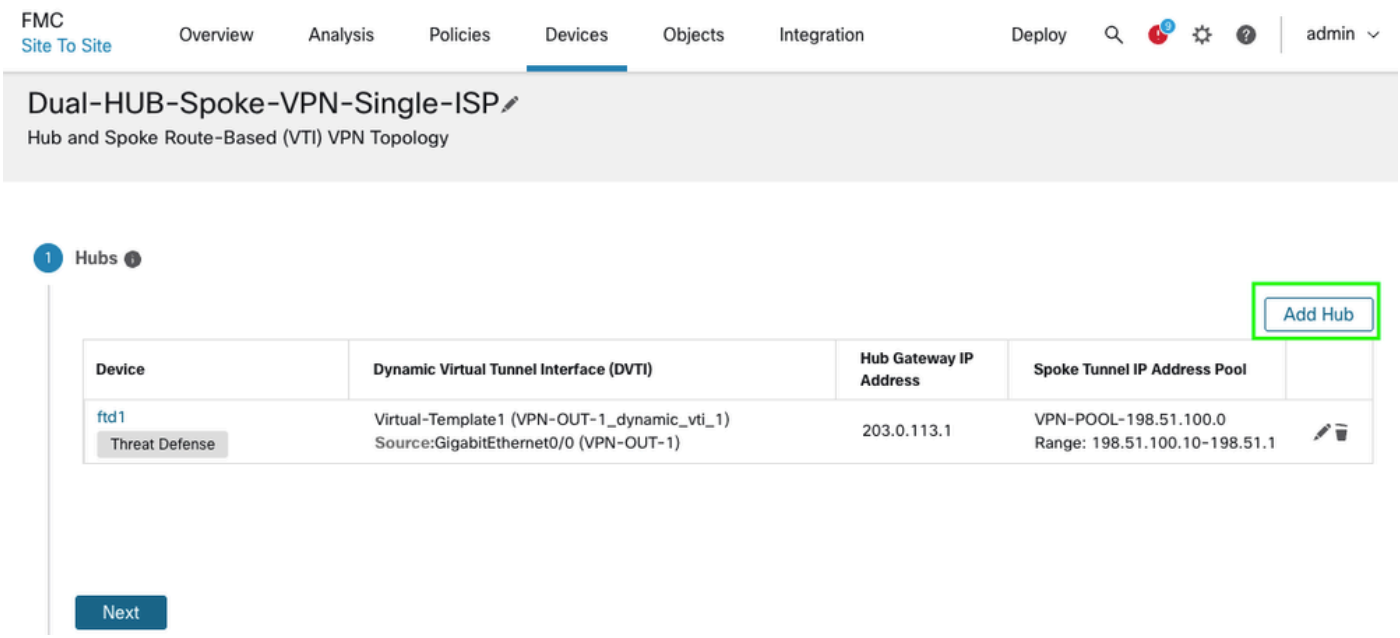
<<<<<< spoke 3 inside network

Dual-HUB und -Spoke (Single-ISP für redundanten HUB über EBGP zwischen sekundären HUB und Spokes)

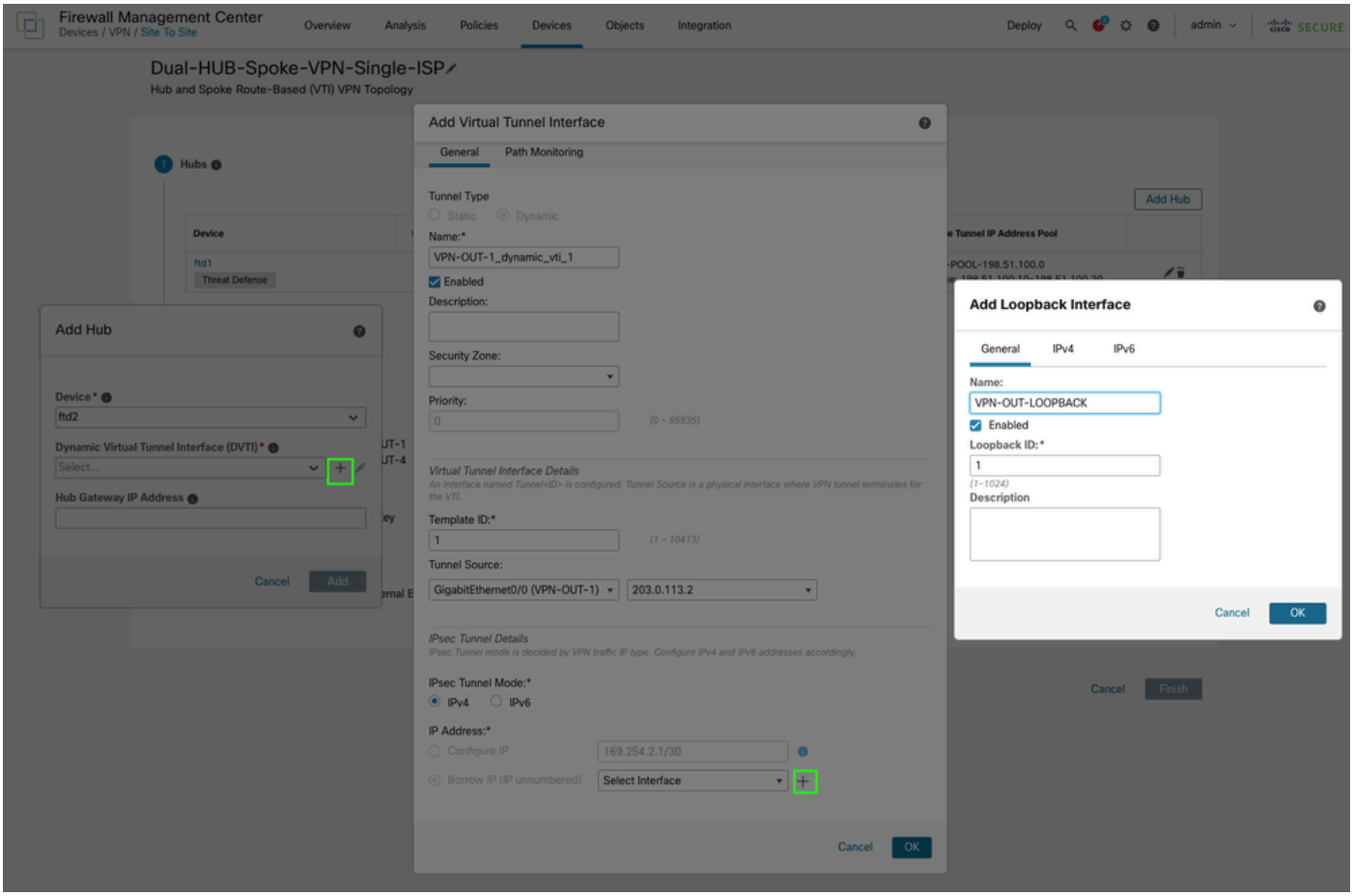
Netzwerkdiagramm


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

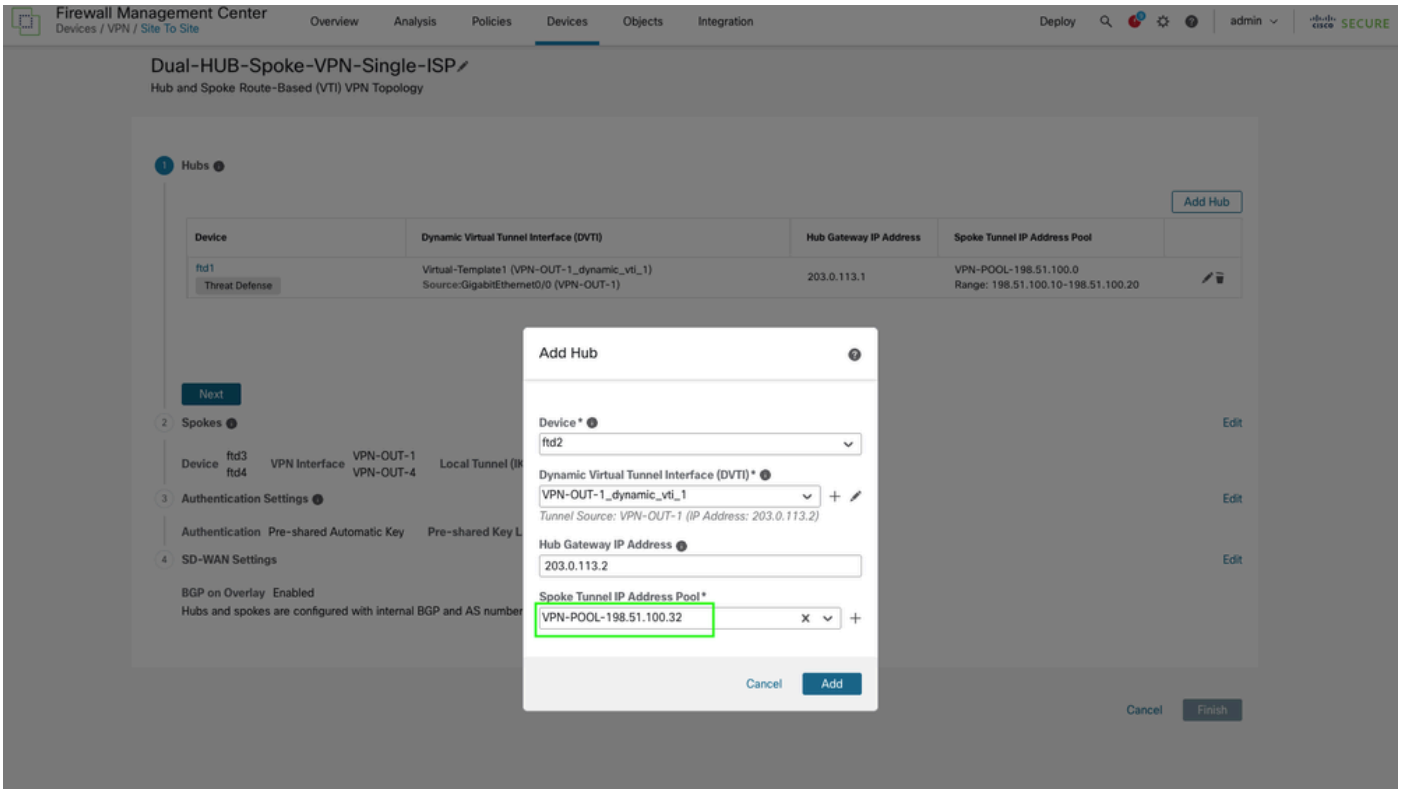
Fahren Sie nach dem Hinzufügen des ersten HUB mit dem Hinzufügen des zweiten HUB fort. Gehen Sie dabei wie zuvor für HUB1 beschrieben vor.

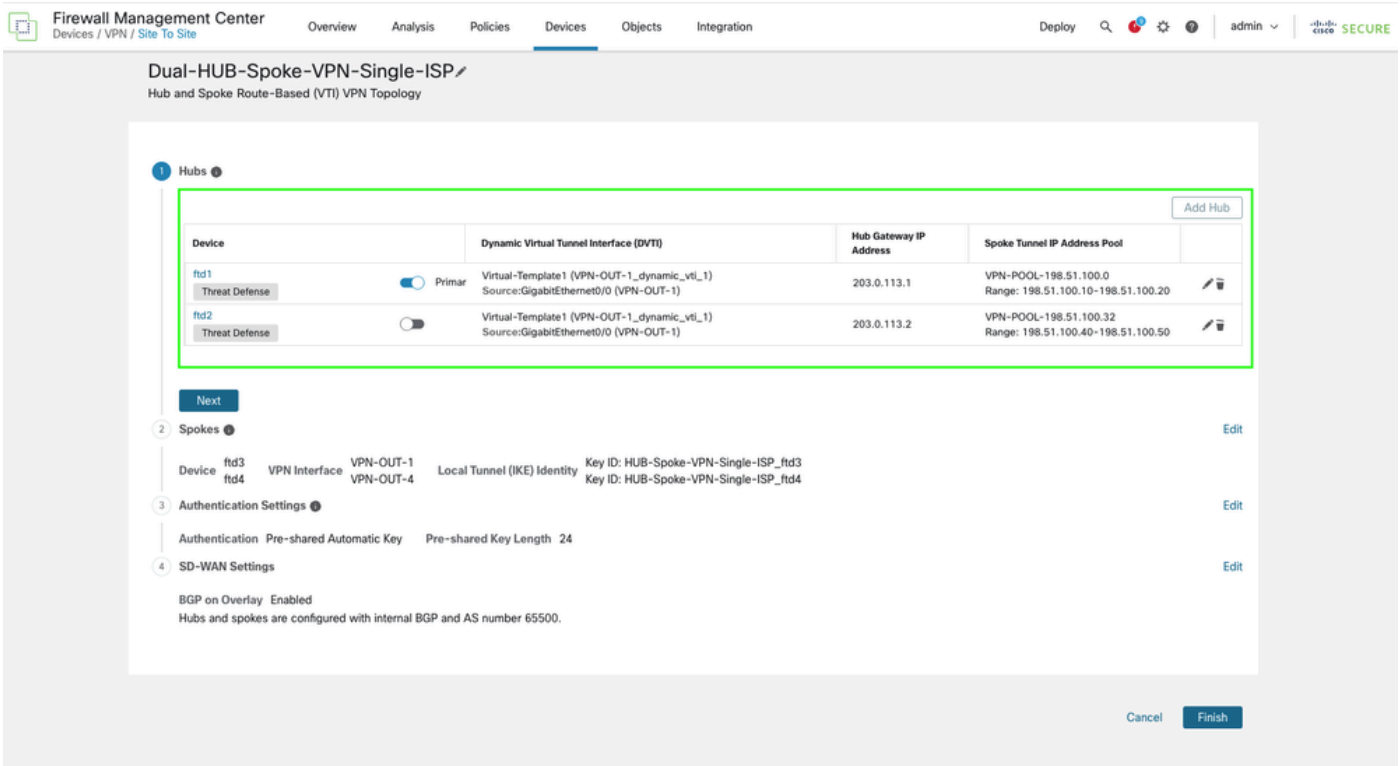


- Fahren Sie mit der Erstellung des DVTI (Dynamic Virtual Tunnel Interface) fort.



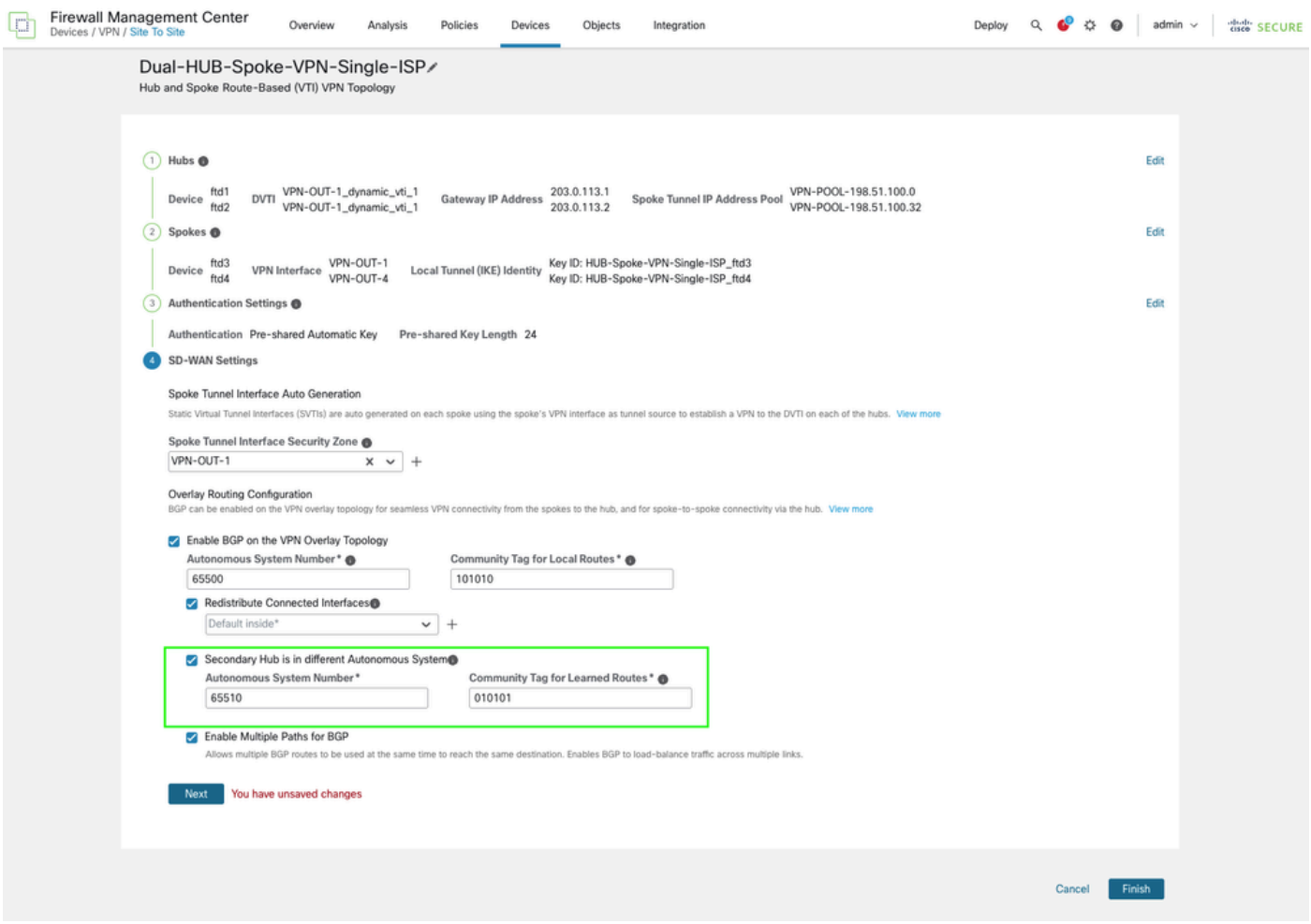
- Für HUB 2 VTI-Tunnel auf der Spoke-Seite ist ein neuer IP-Adresspool erforderlich. Erstellen und konfigurieren Sie den neuen Pool, und speichern Sie die Änderungen.





- Ändern Sie im letzten Schritt die SD-WAN-Einstellungen, um das eBGP-Peering zwischen dem zweiten HUB und den Stationen zu konfigurieren. Aktivieren Sie die Option Sekundärer HUB befindet sich in einem anderen autonomen System, und geben Sie die AS-Nummer (Autonomous System) für den sekundären HUB an. IBGP kann auch verwendet werden, wenn die Verwendung unterschiedlicher AS-Nummern in Ihrer Umgebung nicht eingeschränkt ist, indem die Option "Sekundärer HUB" in einem anderen autonomen System deaktiviert wird. Dadurch werden dieselbe Community-Tag- und AS-Nummer auch für das sekundäre HUB verwendet. Der Schwerpunkt dieses Artikels liegt auf eBGP für die aktuelle

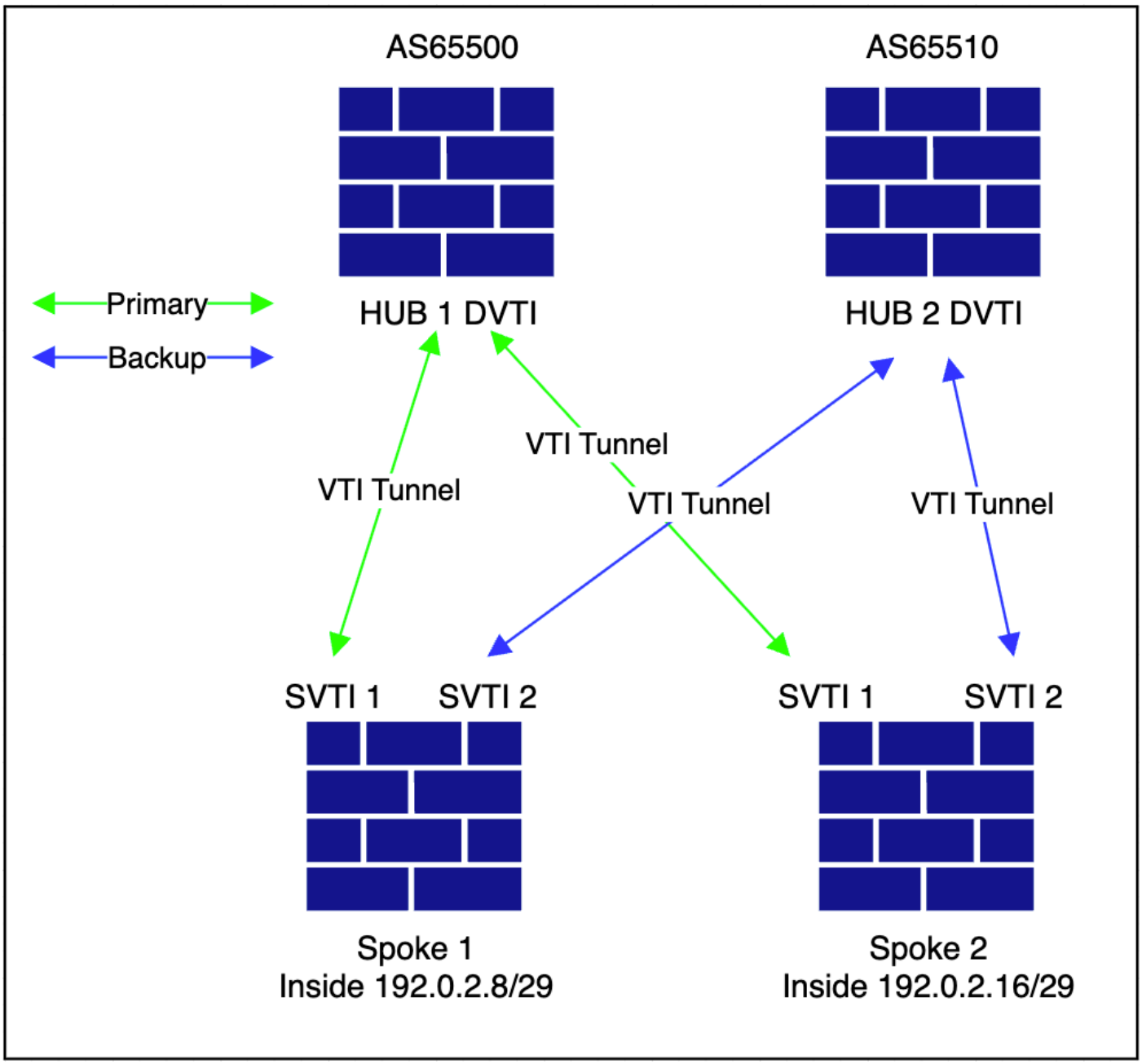
Konfiguration.



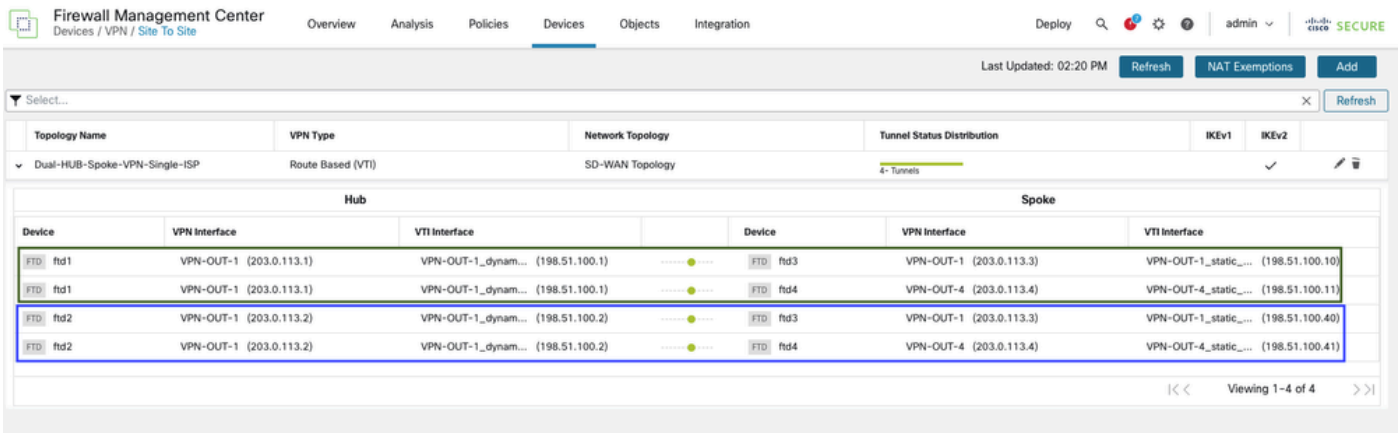
Stellen Sie sicher, dass sowohl die AS-Nummer (Autonomous System) als auch das Community-Tag in dieser Konfiguration eindeutig sind.

Verifizierung

Dieses Diagramm zeigt die Overlay-Topologie.



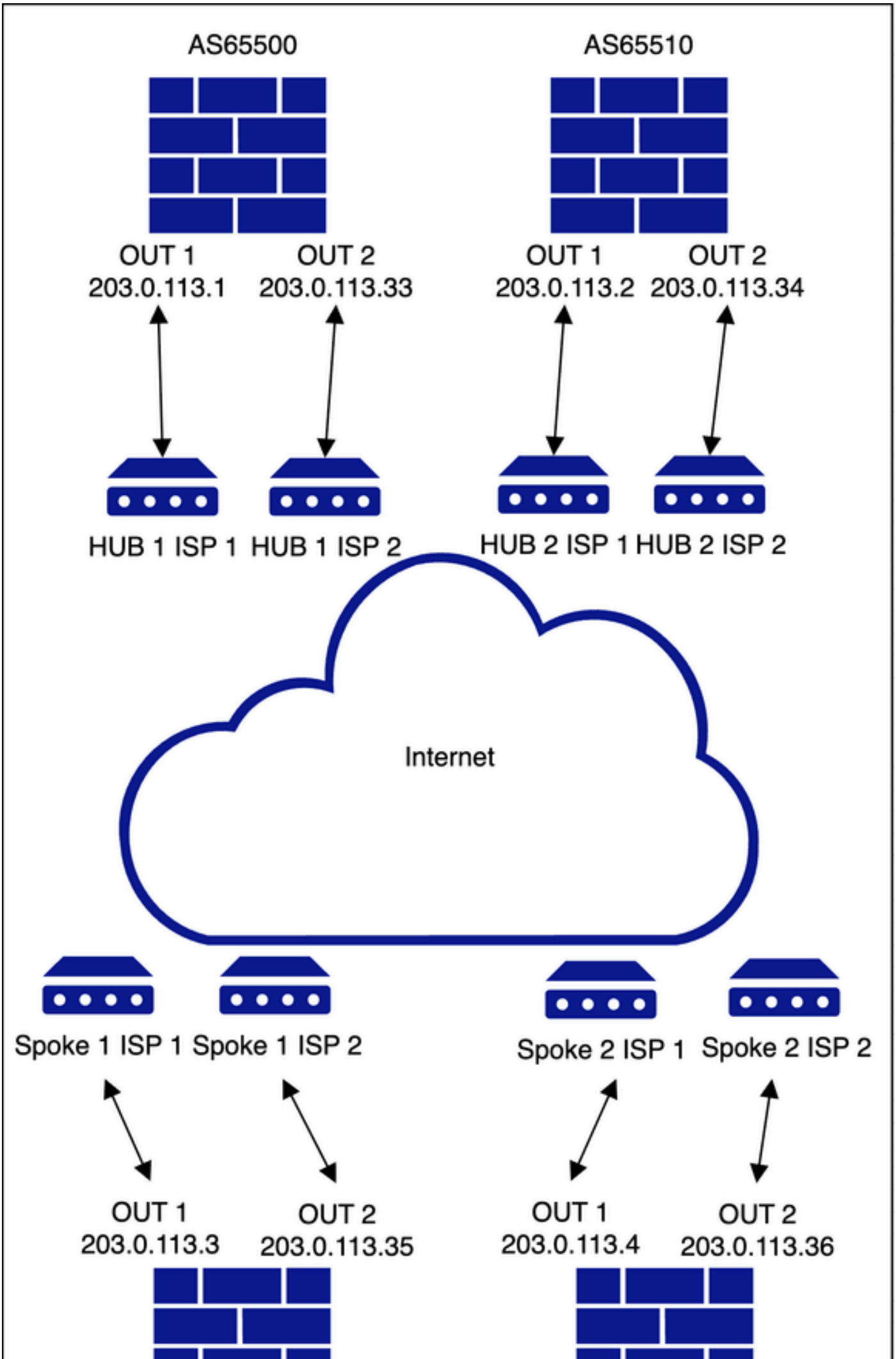
- Navigieren Sie im FMC zu Devices > VPN > Site to Site.



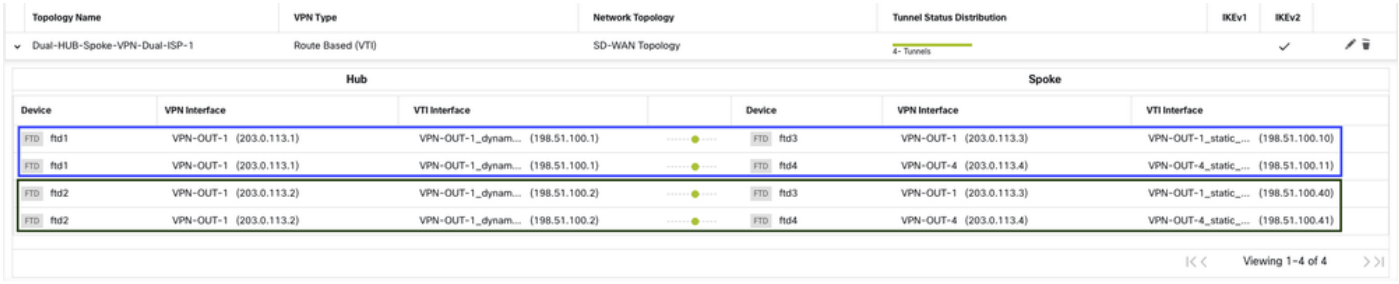
- Alle anderen Schritte bleiben unverändert.

Dual-HUB und -Spoke (Dual-ISP für redundante HUBs und ISPs über EBGP zwischen sekundären HUBs und Spokes)

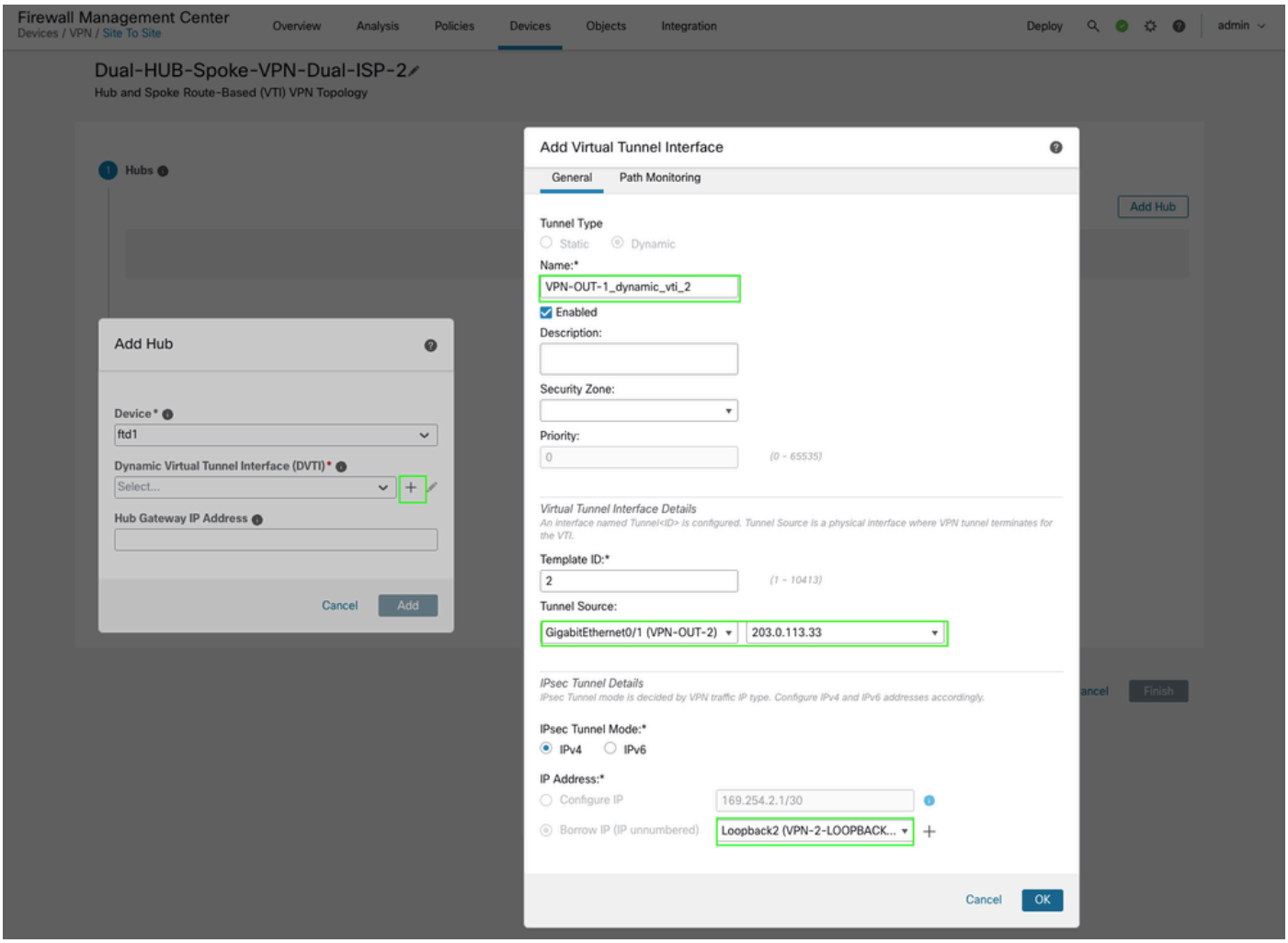
Netzwerkdiagramm


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

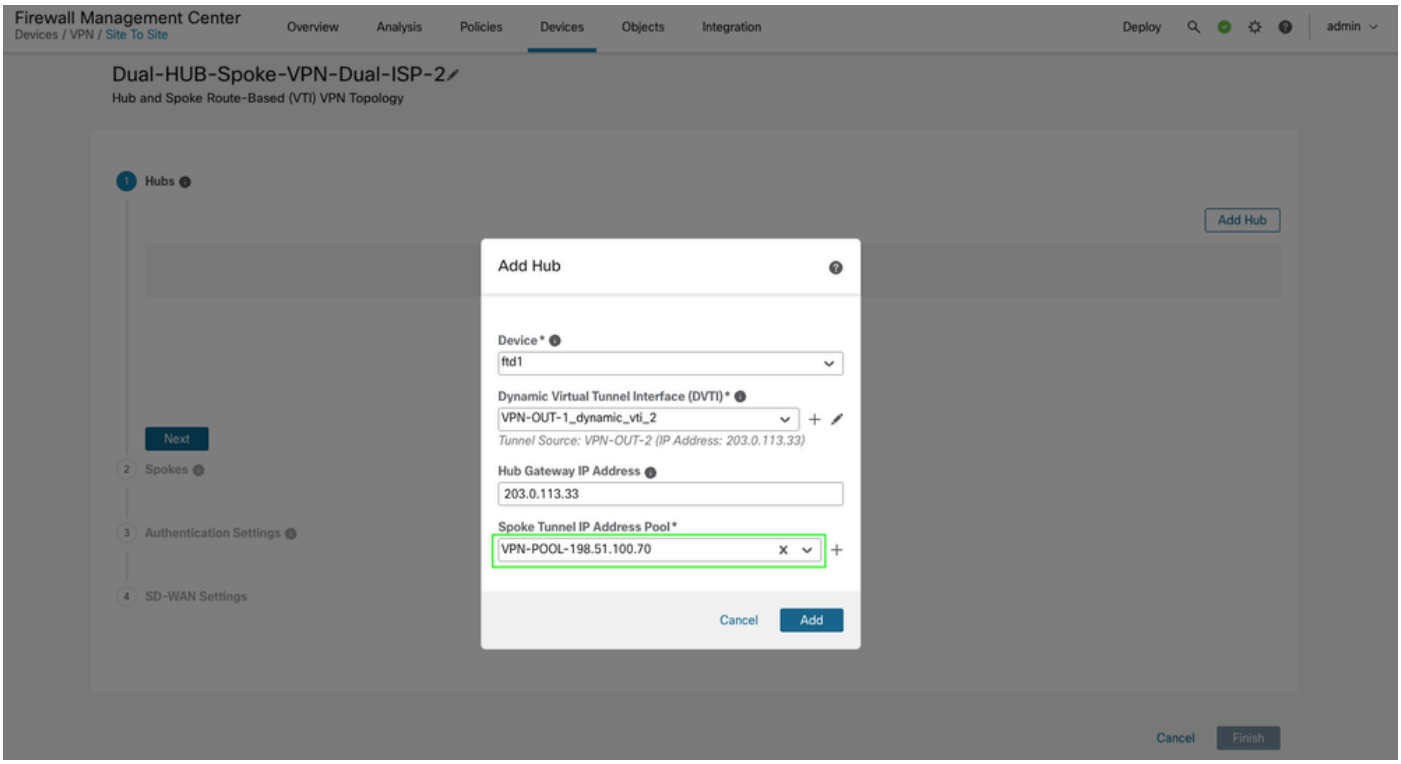
Die Bereitstellung für diese Topologie wird mit dem ersten ISP übersprungen, da dies in der vorherigen Topologie behandelt wurde.

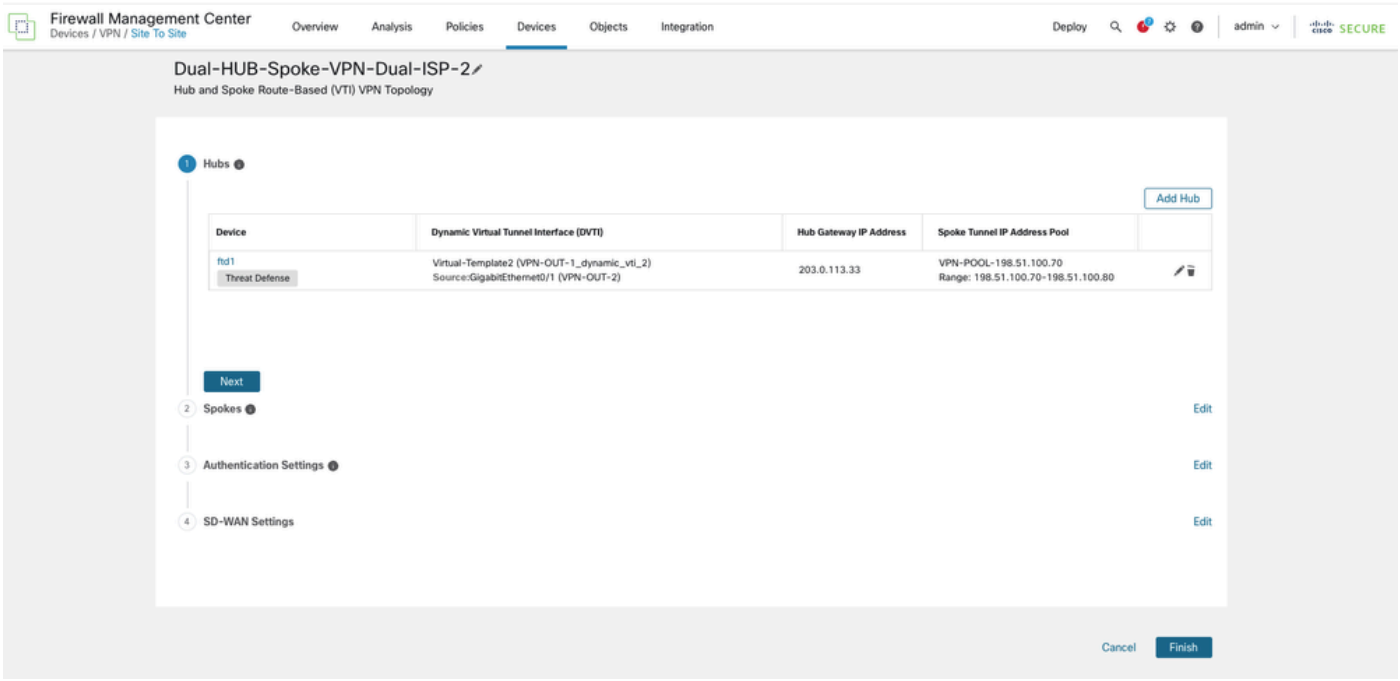


- Als Nächstes fügen Sie die zweite Topologie hinzu, indem Sie zwei zusätzliche DVTI-Schnittstellen pro HUB erstellen, die jeweils die Underlay-Schnittstelle für ISP 2 (VPN-OUT-2) nutzen.

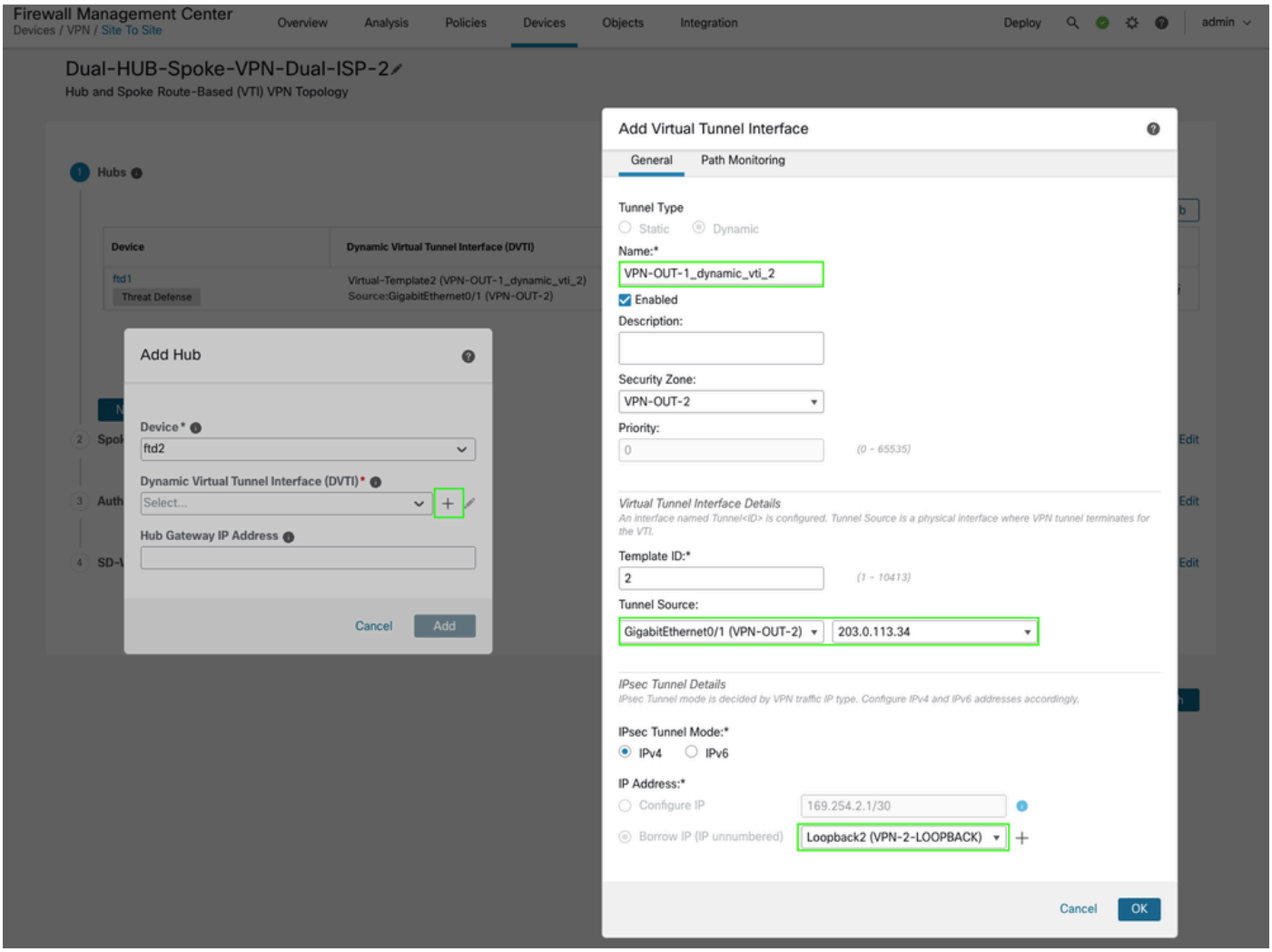


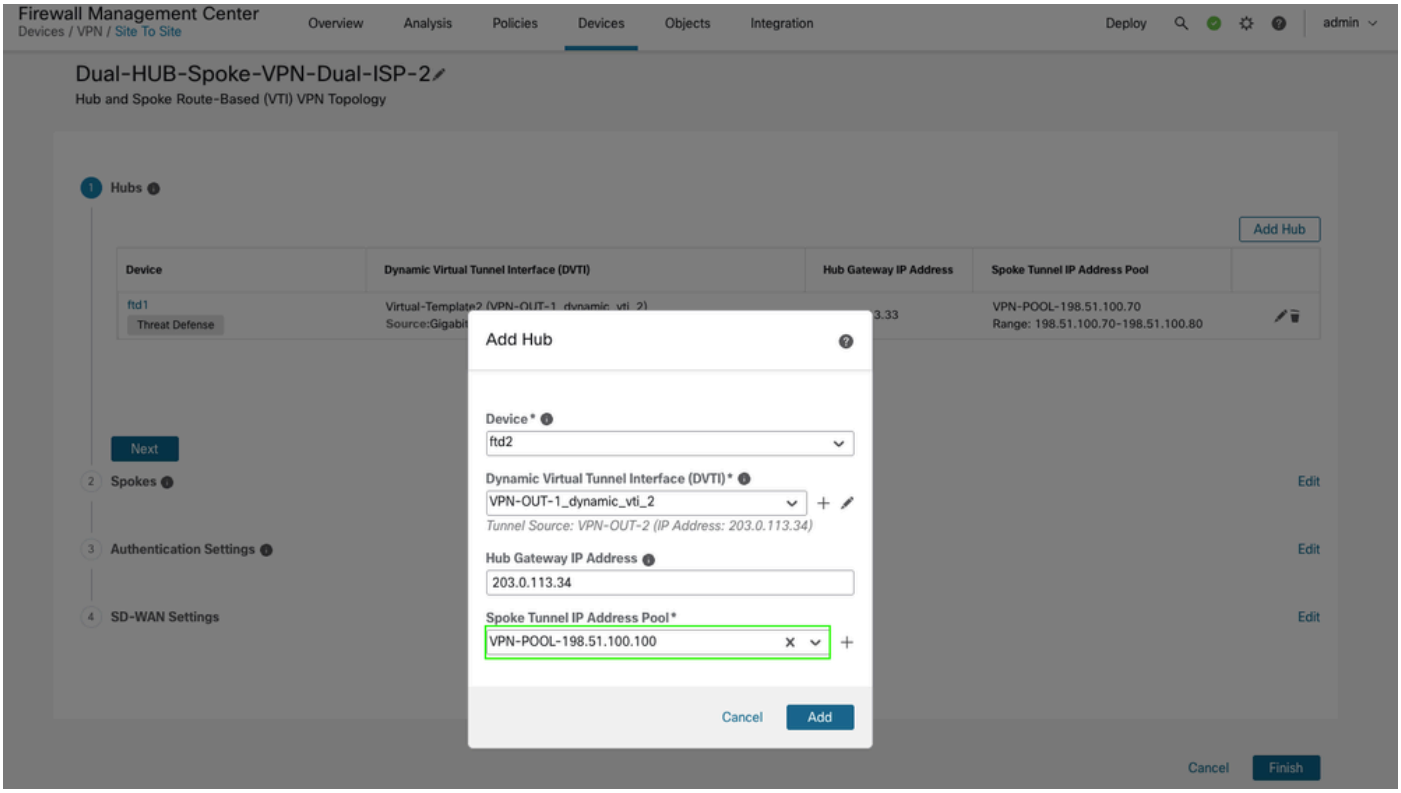
- Speziell für Spoke Virtual Tunnel Interface (VTI)-Adressen wird ein zusätzlicher VPN-IP-Adresspool bereitgestellt.





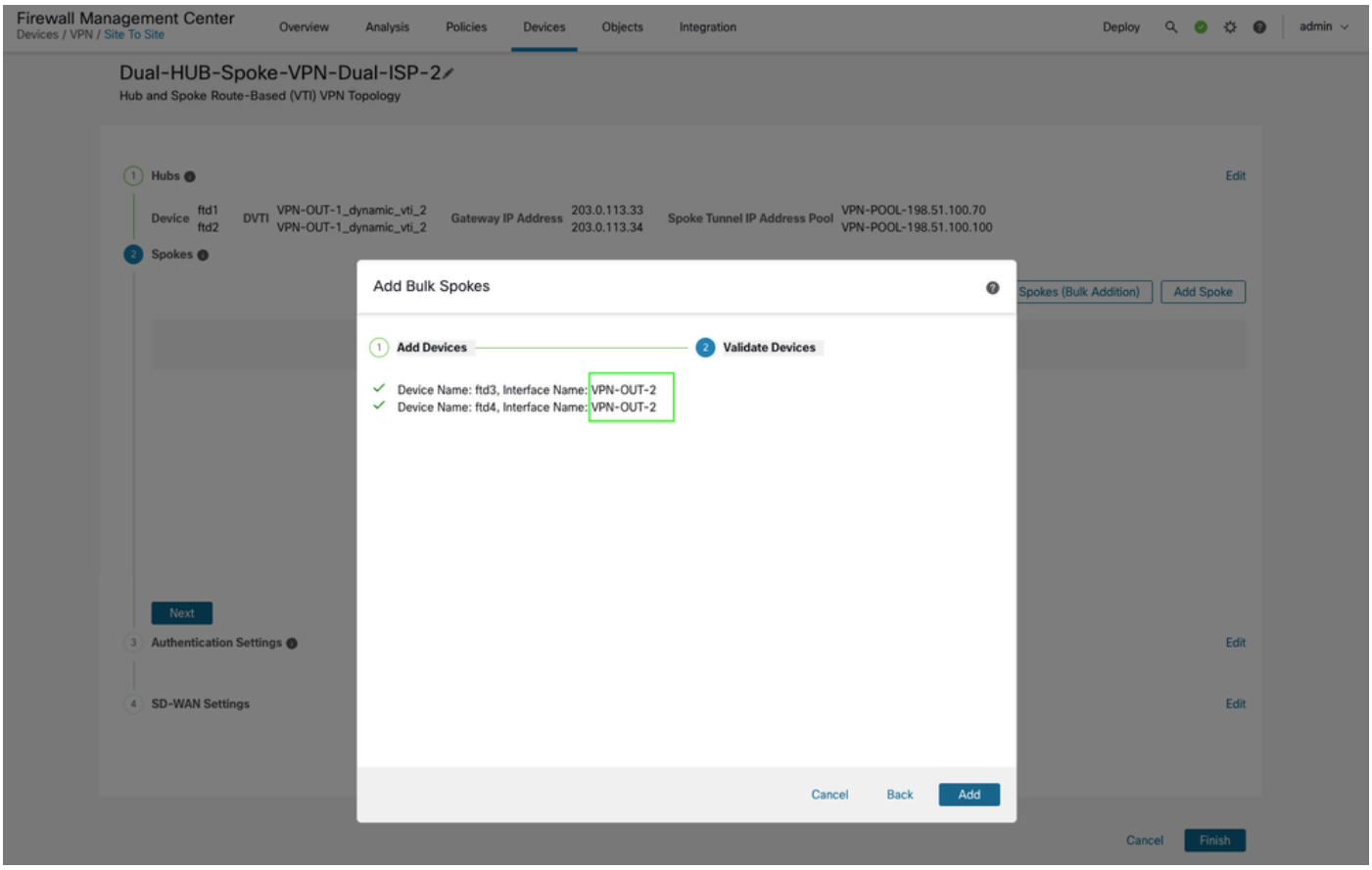
- Um einen sekundären Hub hinzuzufügen, wiederholen Sie den Vorgang, indem Sie DVTI 2 über die sekundäre ISP-Schnittstelle (VPN-OUT-2) erstellen, und konfigurieren Sie einen zusätzlichen IP-Pool für Spoke-End-VTI-Adressen.

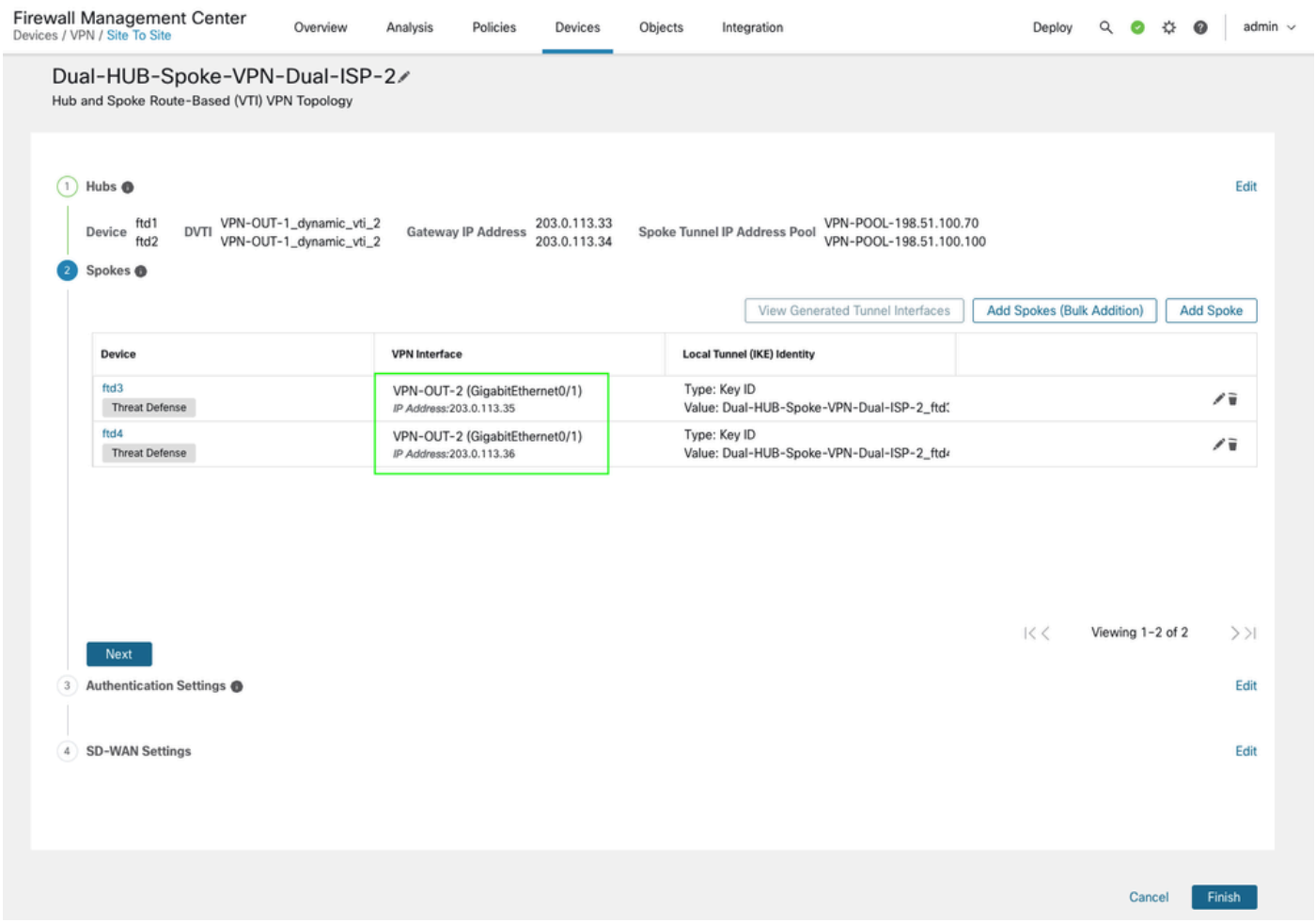




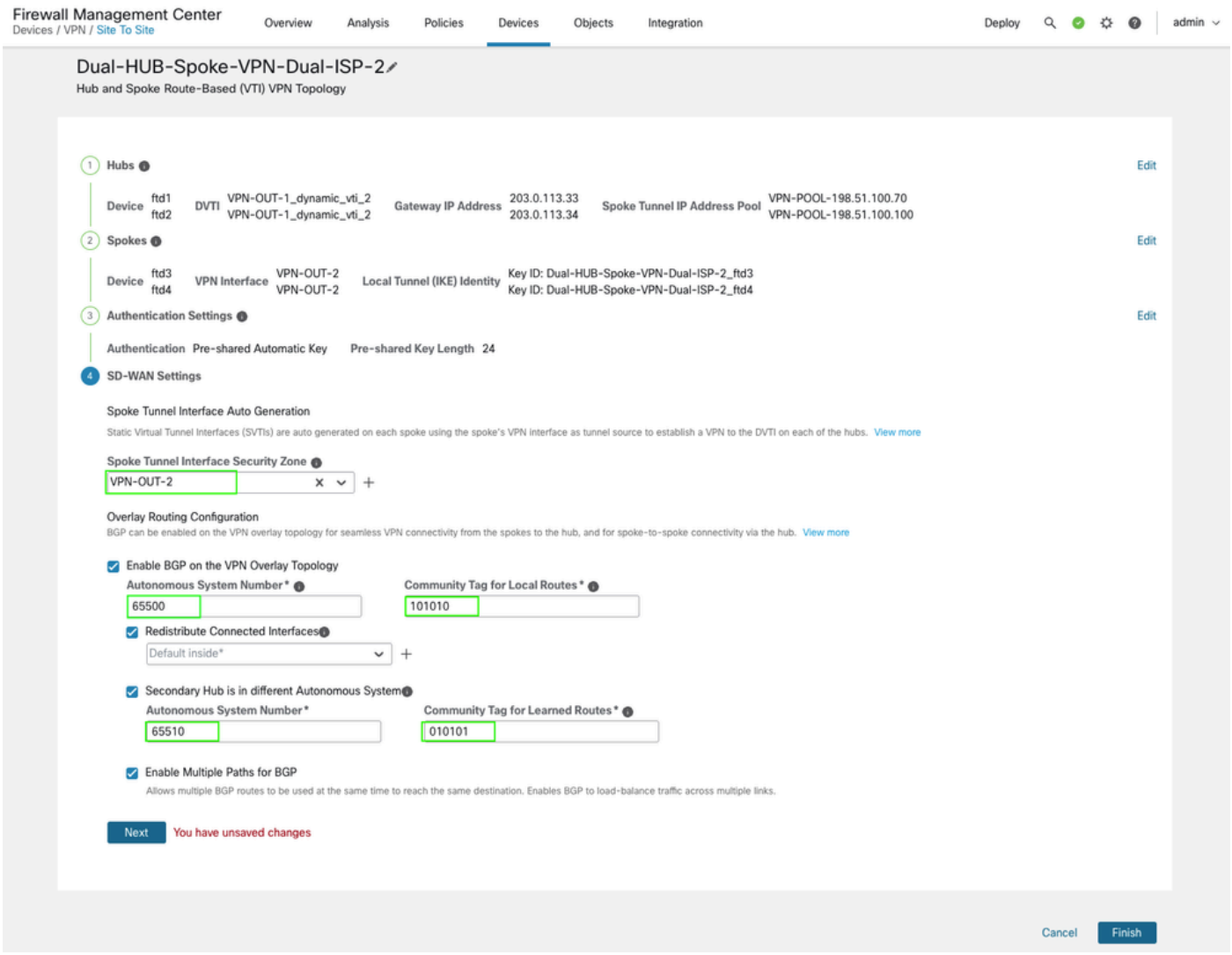
- Achten Sie beim Hinzufügen einer Speiche darauf, dass die richtige Underlay-/WAN-Schnittstelle für die VTI-Tunnel festgelegt ist. Diese Topologie verwendet die sekundäre ISP-

Schnittstelle VPN-OUT-2.





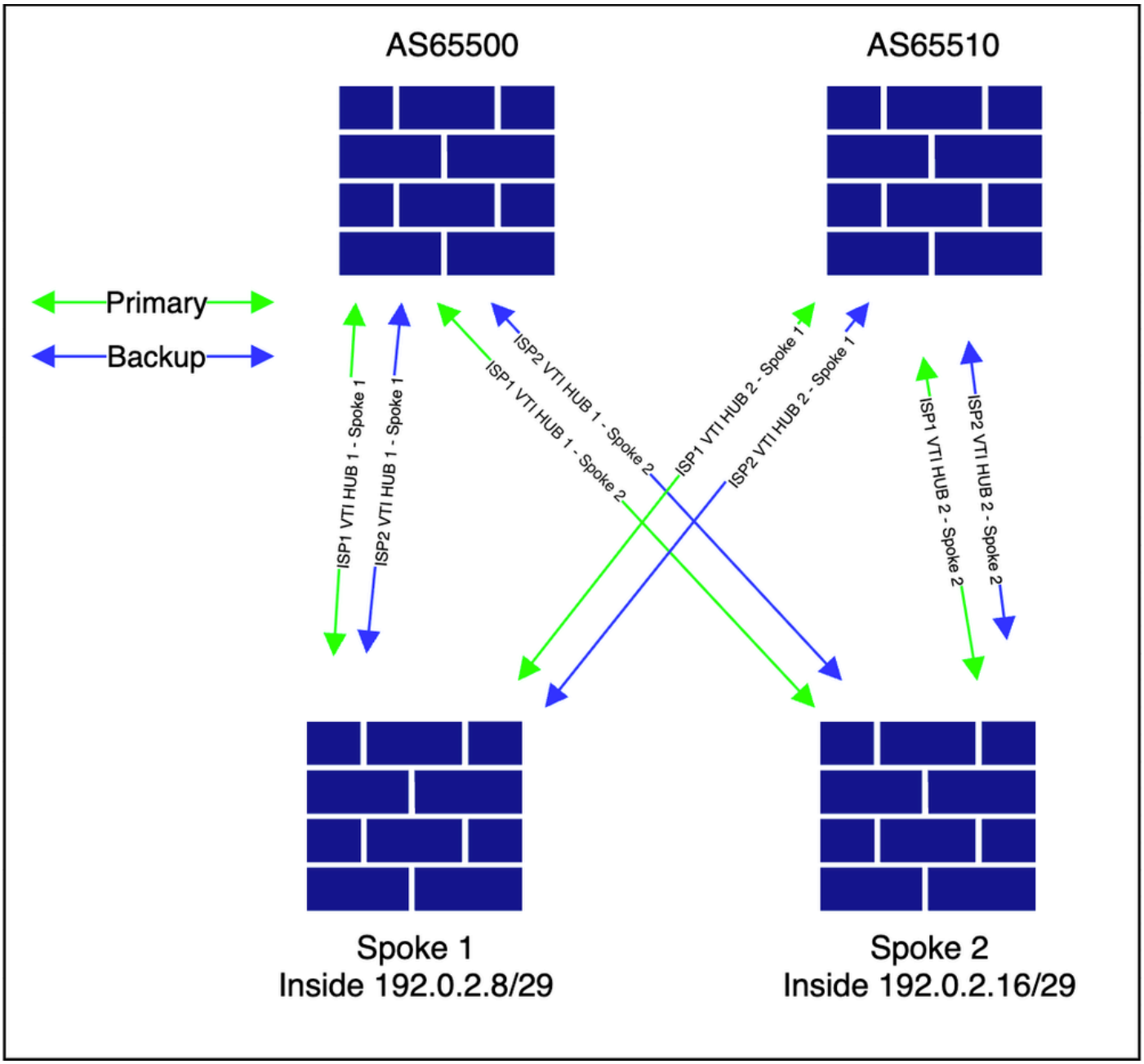
- Stellen Sie beim Konfigurieren des Routings sicher, dass die Community-Tags und AS-Nummern für beide HUBs in dieser Topologie mit den Tags übereinstimmen, die in der vorherigen ISP1-Topologie verwendet wurden. Die Topologie nutzt unterschiedliche Sicherheitszonen, die verbleibenden Konfigurationen (AS-Nummern für primäre und sekundäre HUBs sowie Community-Tags) sind jedoch identisch. Dies ist erforderlich, damit die Benutzeroberfläche die Topologieprüfung abschließen kann.



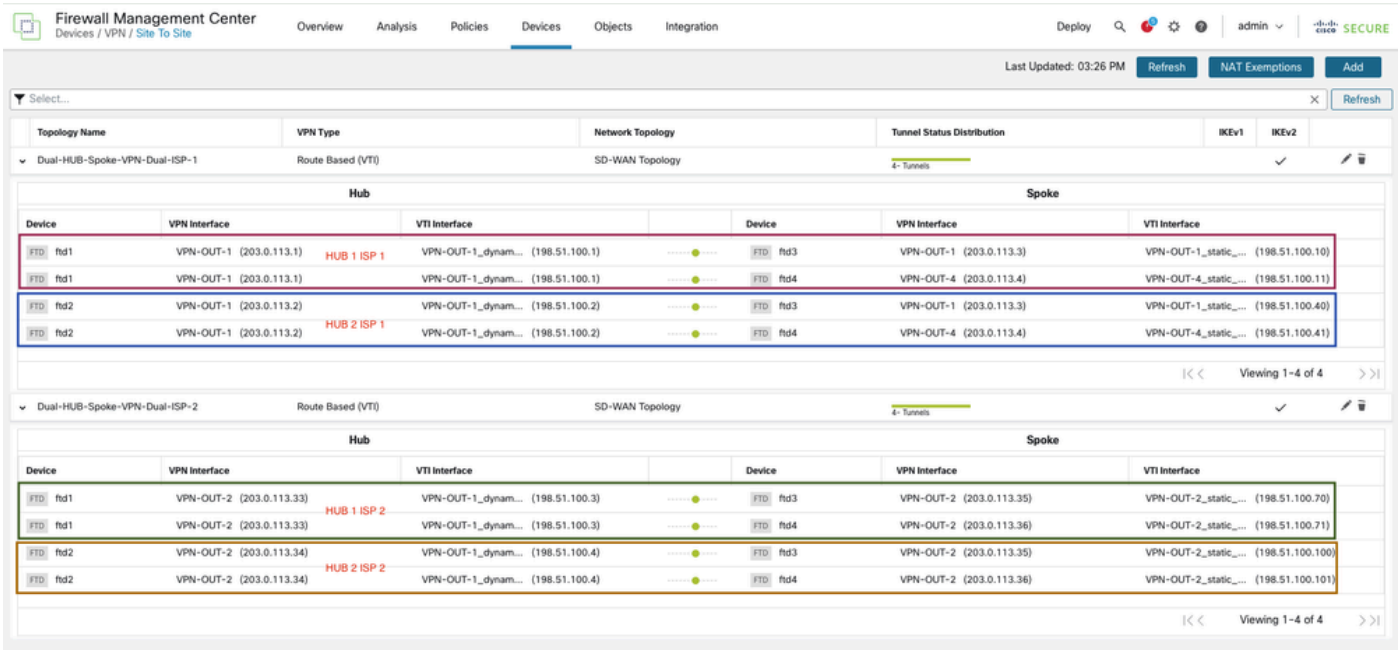
- Alle anderen Einstellungen bleiben unverändert. Schließen Sie den Assistenten ab, und fahren Sie mit der Bereitstellung fort.

Verifizierung

- Die Topologie wird wie dargestellt angezeigt.



- Navigieren Sie zu Devices > VPN > Site to Site, um die Topologie anzuzeigen.



Diese Konfiguration führt zu vier BGP-Peerings pro Gerät, und jede Spoke verfügt über die geeigneten Routen, um andere Spokes zu erreichen. Als Beispiel können Sie die Ausgabe von einem der Spokes abrufen.

Für Speiche 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
```

Die Routing-Tabelle wird wie dargestellt angezeigt. Sie bestätigt, dass ein Load Balancing des Datenverkehrs zwischen den beiden Verbindungen auf der Spoke-Seite stattfindet.

<#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
```

Schlussfolgerung

In diesem Artikel werden verschiedene Bereitstellungsszenarien erläutert, die mit einem einzigen Setup-Assistenten einfach implementiert werden können.

Zugehörige Informationen

- Weitere Unterstützung erhalten Sie beim TAC. Ein gültiger Support-Vertrag ist erforderlich:Cisco Worldwide Support Contacts
- Sie können hier auch die Cisco VPN Community besuchen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.