セキュアファイアウォールを介したサイト間VPNのためのSD-WANの設定

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[機能情報](#)

[対象トポロジ](#)

- [ハブ&スポーク（単一のISP）](#)
- [デュアルハブアンドスポーク（セカンダリハブとスポーク間のEBGPを介した冗長ハブ用のシングルISP）](#)
- [デュアルハブ&スポーク（冗長ハブ用のデュアルISP、およびセカンダリハブとスポーク間のEBGPを介したISP）](#)

[結論](#)

[関連情報](#)

はじめに

このドキュメントでは、Secure FirewallのSD-WAN機能を使用したBGPオーバーレイルーティングによるルートベースのVPN導入シナリオについて説明します。

前提条件

すべてのハブとスポークでFTD 7.6以降のソフトウェアが稼働しており、これらのハブとスポークは、7.6以降のソフトウェアが稼働している同じFMC経由で管理されます。

要件

次の項目に関する知識があることが推奨されます。

- IKEv2
- ルートベースのVPN
- 仮想トンネルインターフェイス(VTI)
- IPSec
- BGP

使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- Cisco Secure Firewall脅威対策7.7.10
- Cisco Secure Firewall Management Center 7.7.10

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

機能情報

Management Centerは、新しいSD-WANウィザードを使用して、一元化された本社（ハブ）とリモートブランチサイト（スポーク）間のVPNトンネルおよびルーティングの設定を簡素化します。

・ ハブ上でDVTI(Dynamic Virtual Tunnel Interface)を活用し、スポーク上でSVTI(Static Virtual Tunnel Interface)を活用することでVPN設定を自動化します。オーバーレイルーティングはBGPを介して有効にします。

・ スポークにSVTI IPアドレスを自動的に割り当て、暗号化パラメータを含む完全なVTI設定をプッシュします。

・ 同じウィザード内で簡単な1ステップのルーティング設定を行い、BGPでオーバーレイルーティングを有効にします。

・ BGPのルートリフレクタアトリビュートを活用することにより、スケーラブルで最適なルーティングを可能にします。

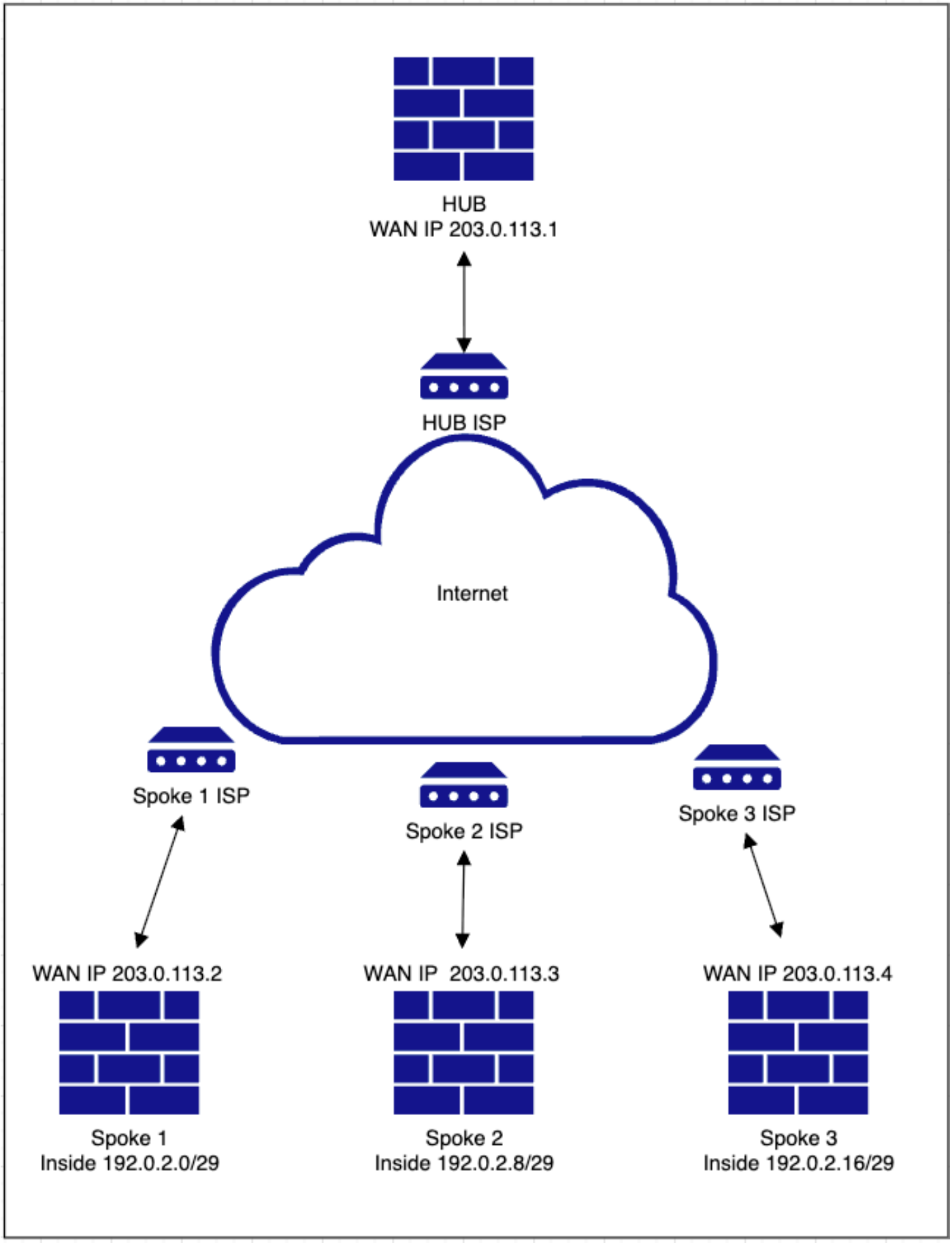
・ 最小限のユーザ操作で複数のスポークを同時に追加できます。

対象トポロジ

この記事では、ユーザがさまざまな導入シナリオを認識できるように、複数のトポロジについて説明します。

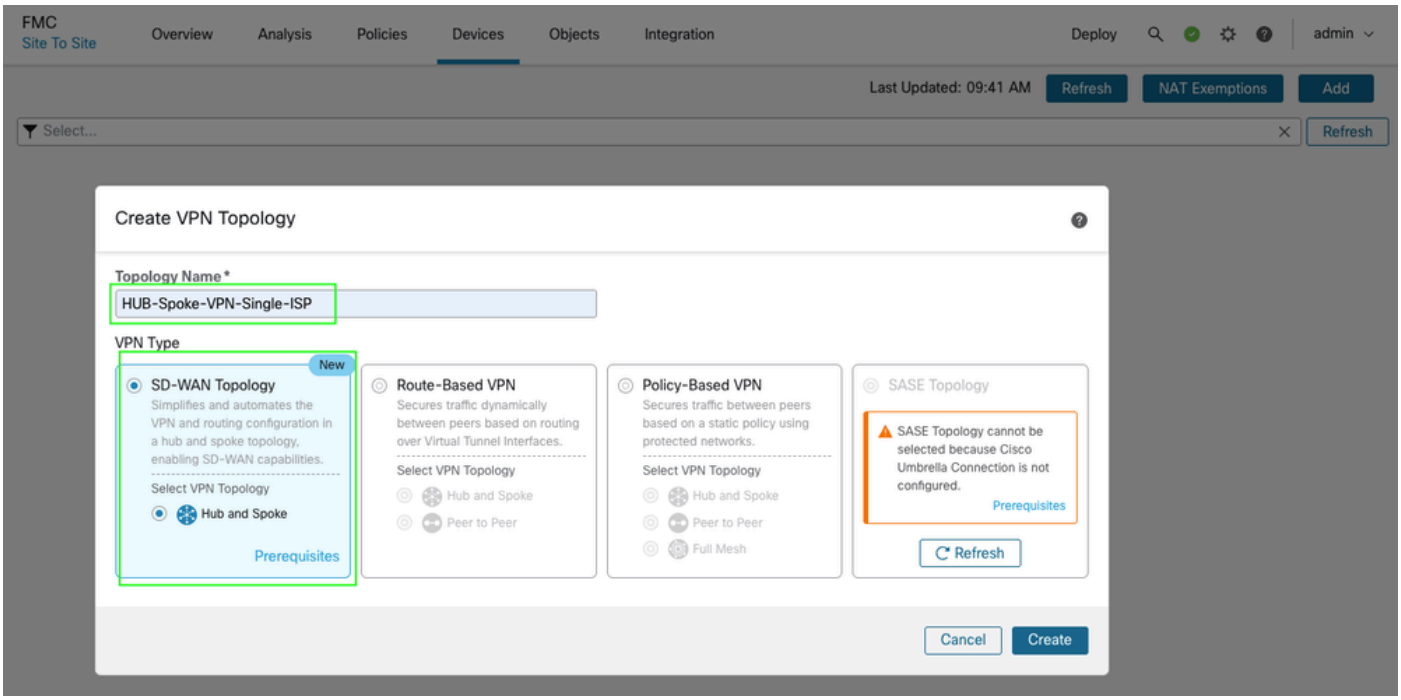
ハブ&スポーク（単一のISP）

ネットワーク図

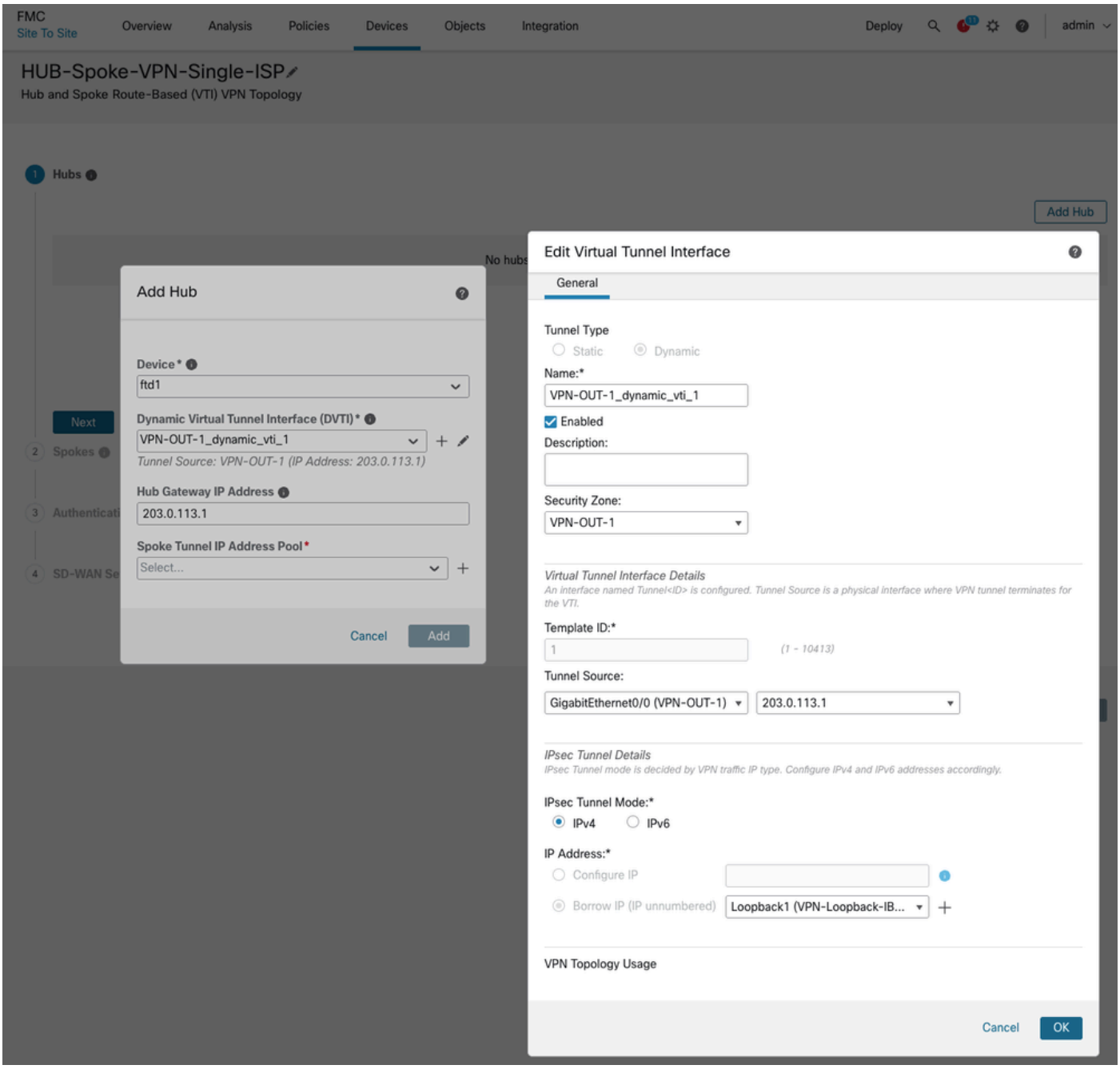


コンフィギュレーション

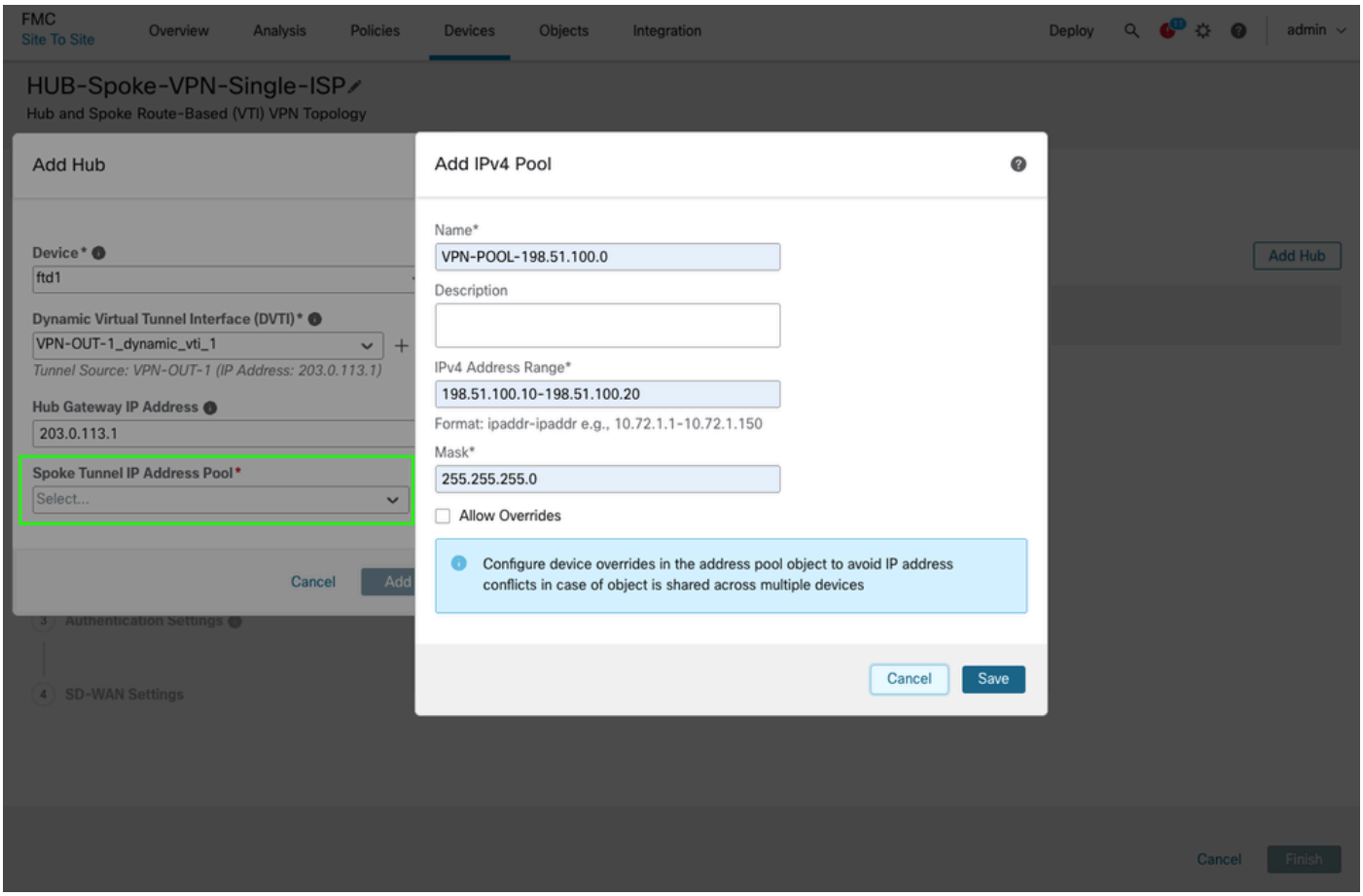
- Devices > VPN > Site to Site > Add > SD-WAN Topology > > Createの順に移動します。

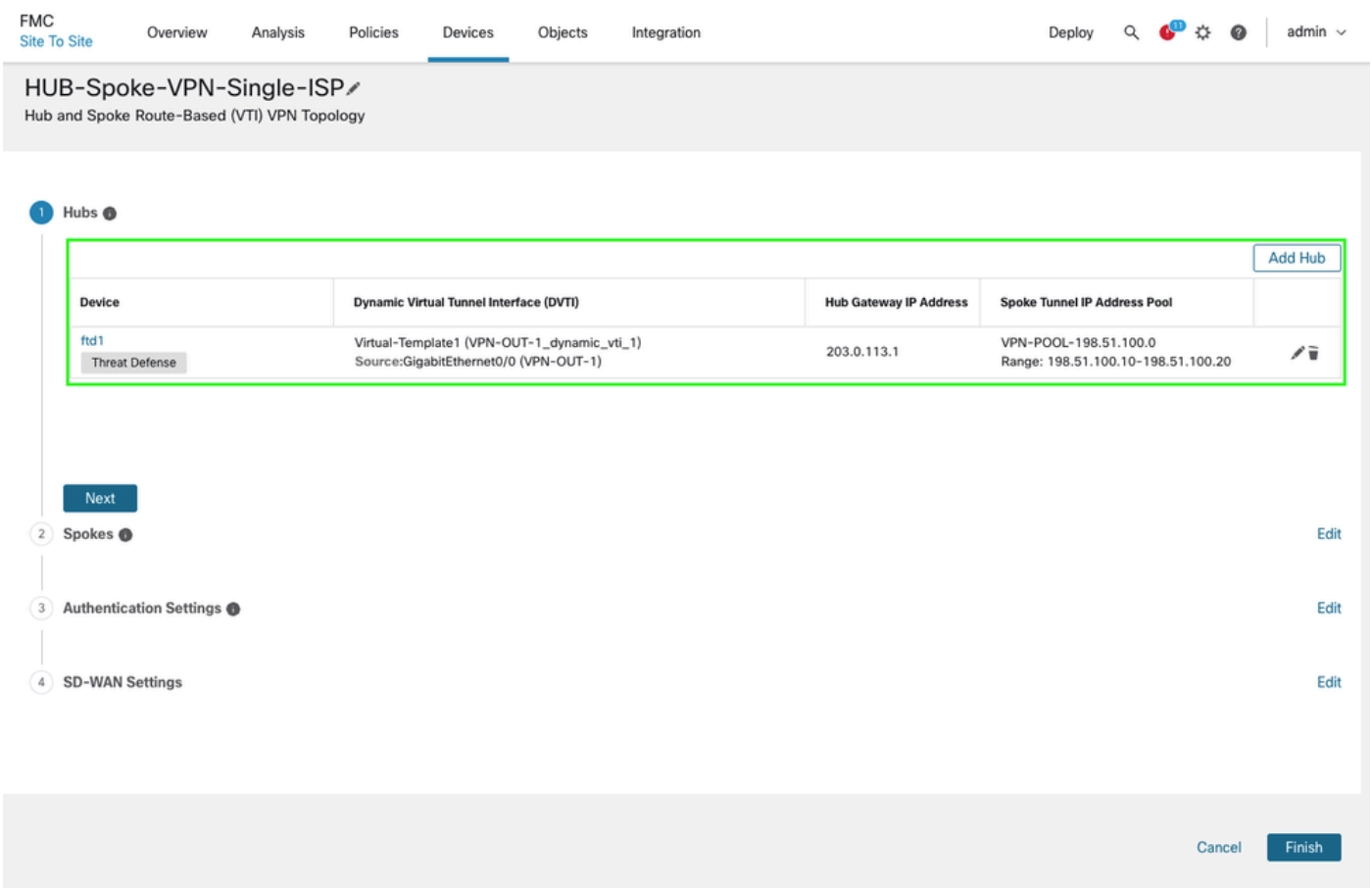


・ ハブを追加し、ハブの終端にDVTIを作成します。DVTI設定の一部として、トポロジに従って正しいトンネル送信元インターフェイスを必ず選択してください。

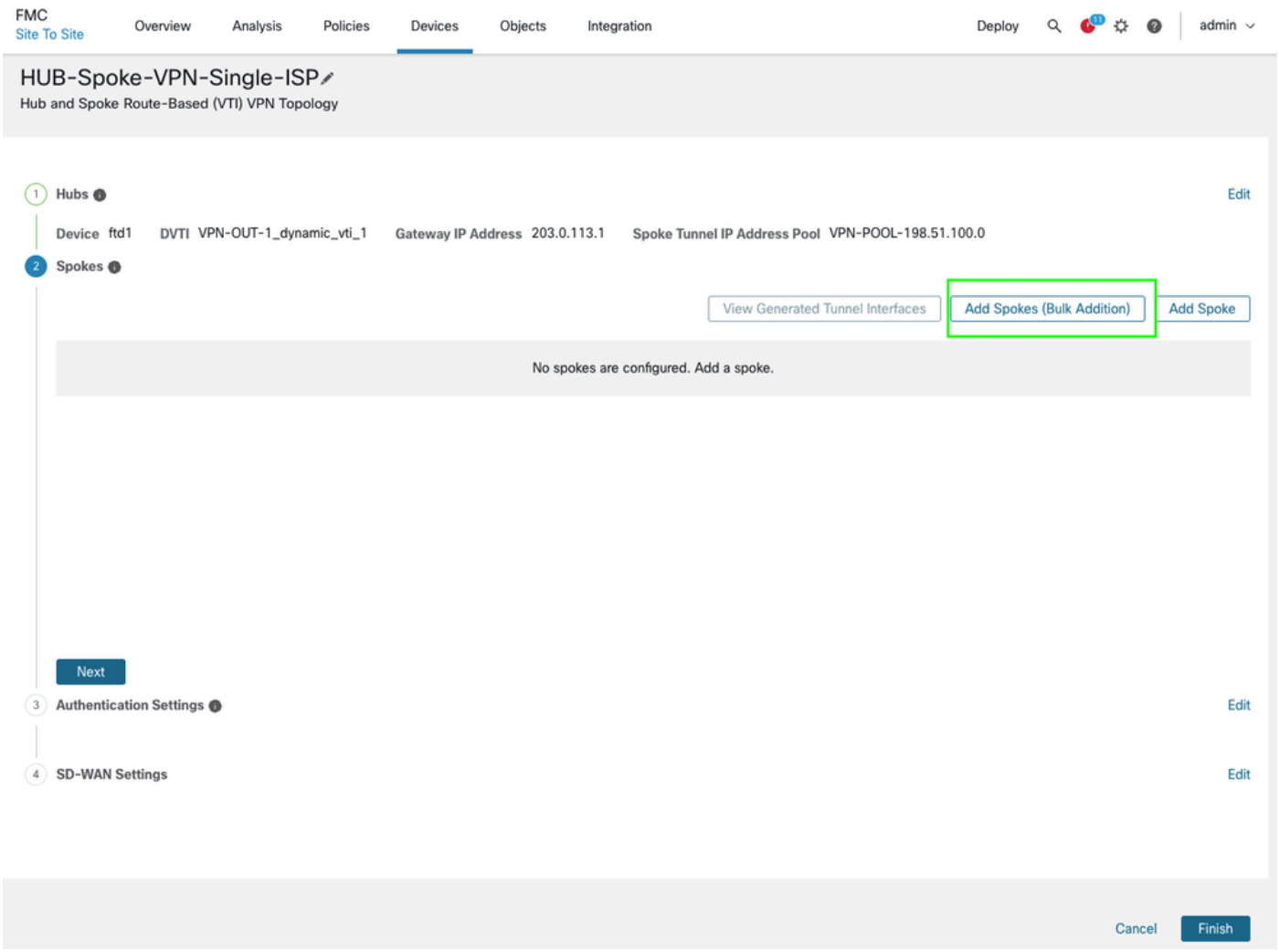


- Spoke Tunnel IP address poolを作成し、SaveをクリックしてからAddをクリックします。IPアドレスプールは、スポークにVTIトンネルIPアドレスを割り当てるために使用されます。

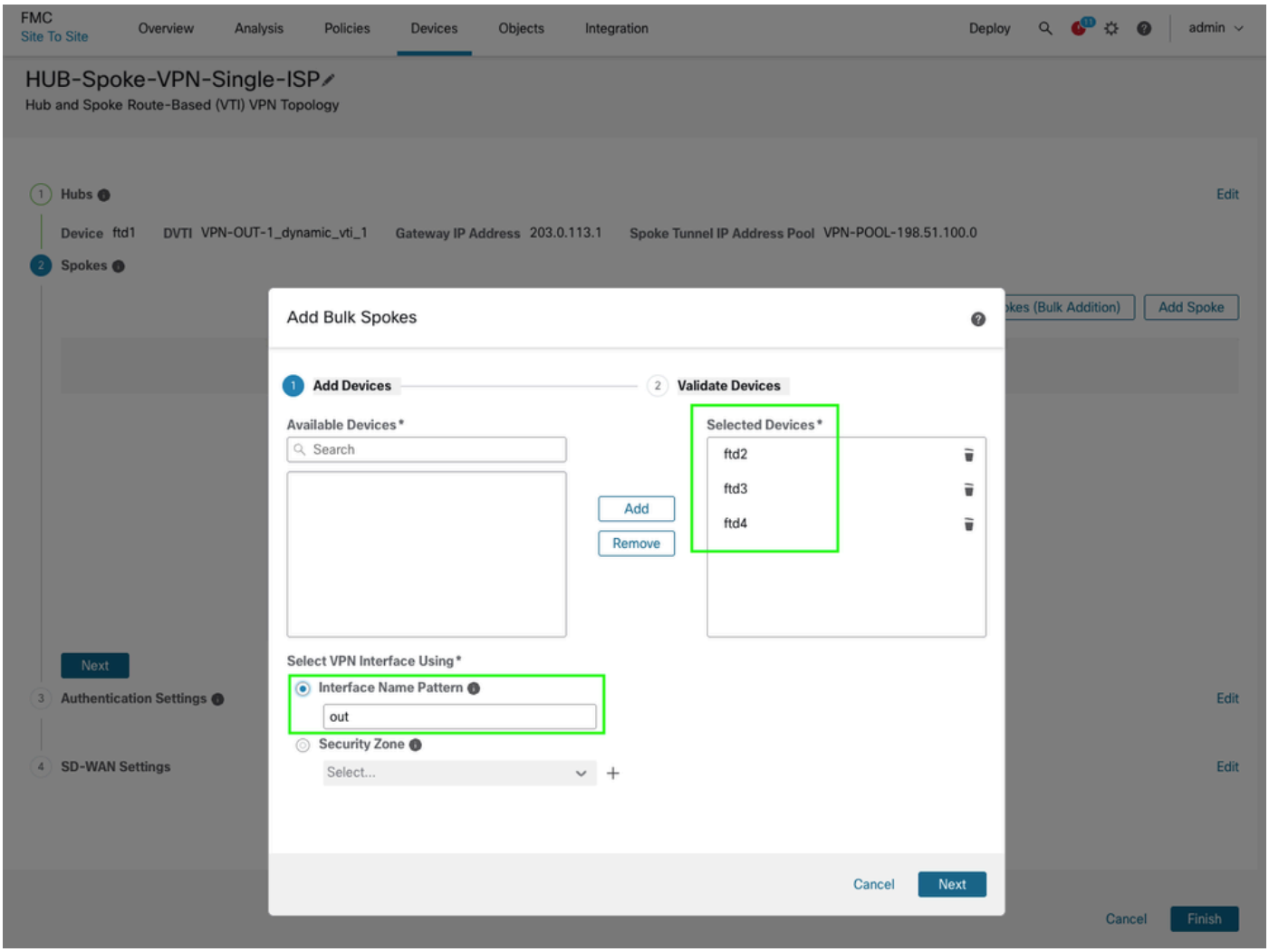


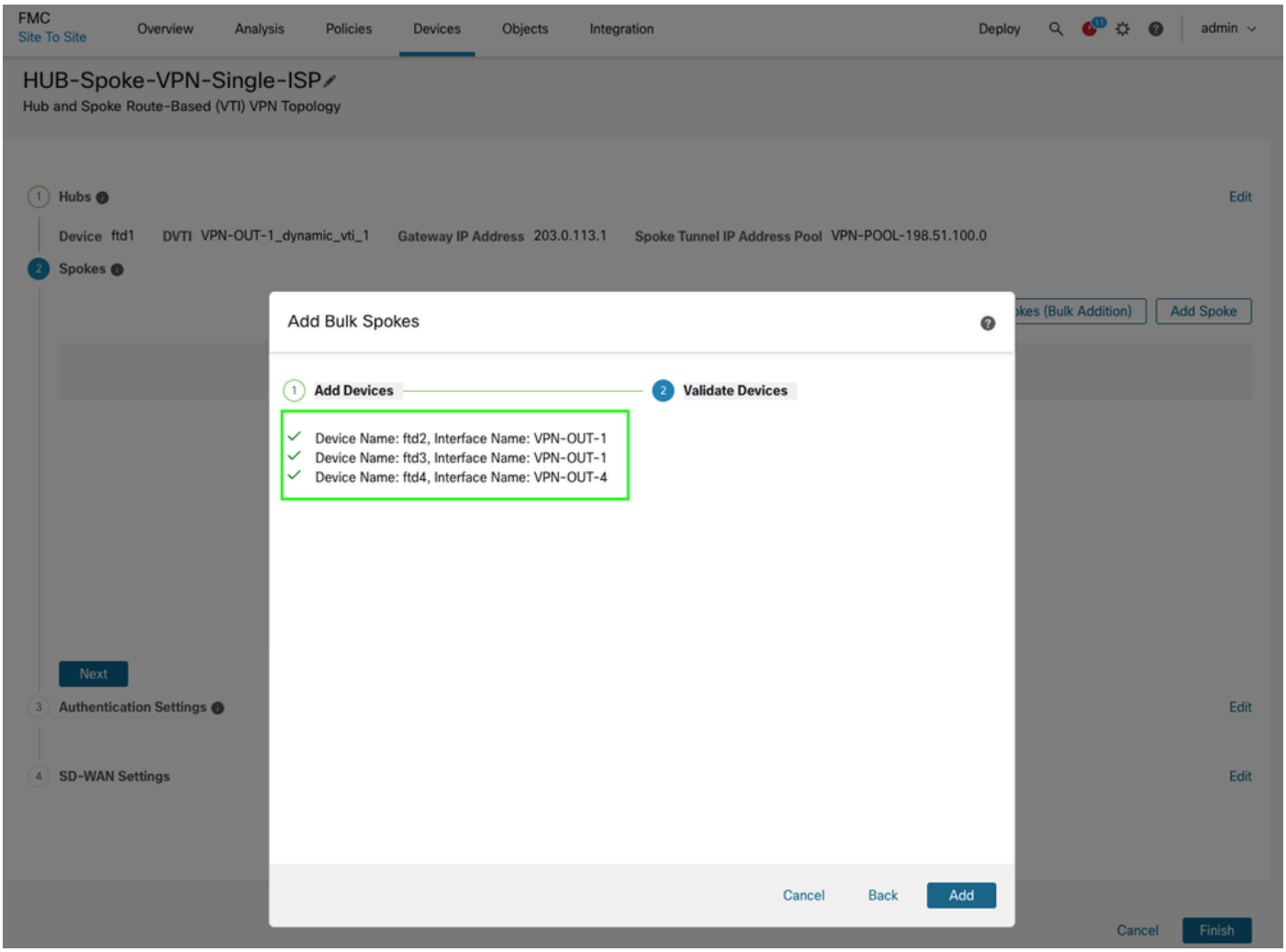


- Nextをクリックして続行し、スポークを追加します。共通のインターフェイス/ゾーン名がある場合、またはスポークを個別に追加する場合は、一括追加オプションを利用できます。

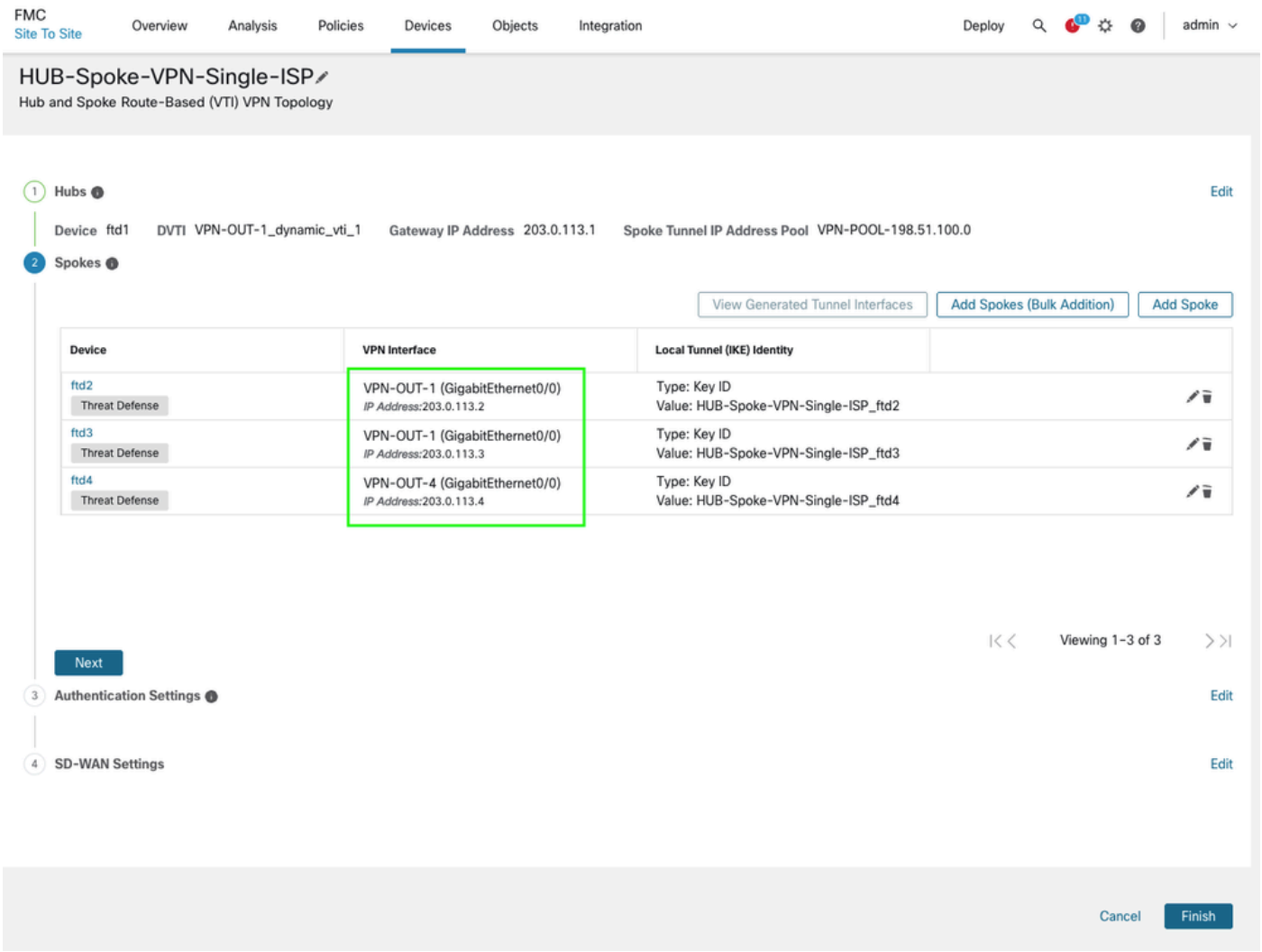


- デバイスを選択し、WAN/Outsideインターフェイスの命名パターンを指定します。デバイスが同じインターフェイス名を共有する場合は、イニシャルを使用するだけで十分です。Nextをクリックし、検証が正常に終了したらAddをクリックします。一括追加の場合も、同じ方法でゾーン名を使用できます。

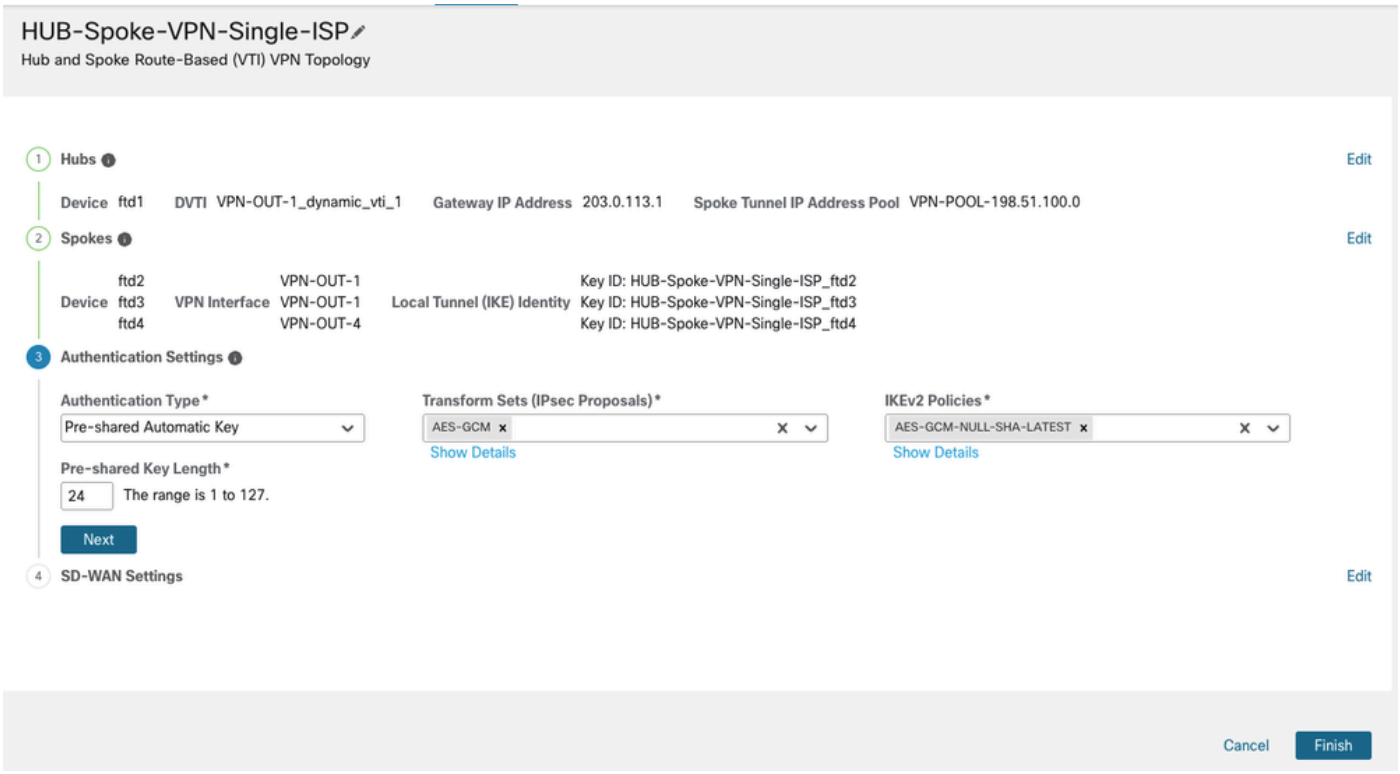

FMC
Site To Site
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
HUB-Spoke-VPN-Single-ISP
Hub and Spoke Route-Based (VTI) VPN Topology
1 Hubs
Edit
Device ftd1
DVTI VPN-OUT-1_dynamic_vti_1
Gateway IP Address 203.0.113.1
Spoke Tunnel IP Address Pool VPN-POOL-198.51.100.0
2 Spokes
Add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



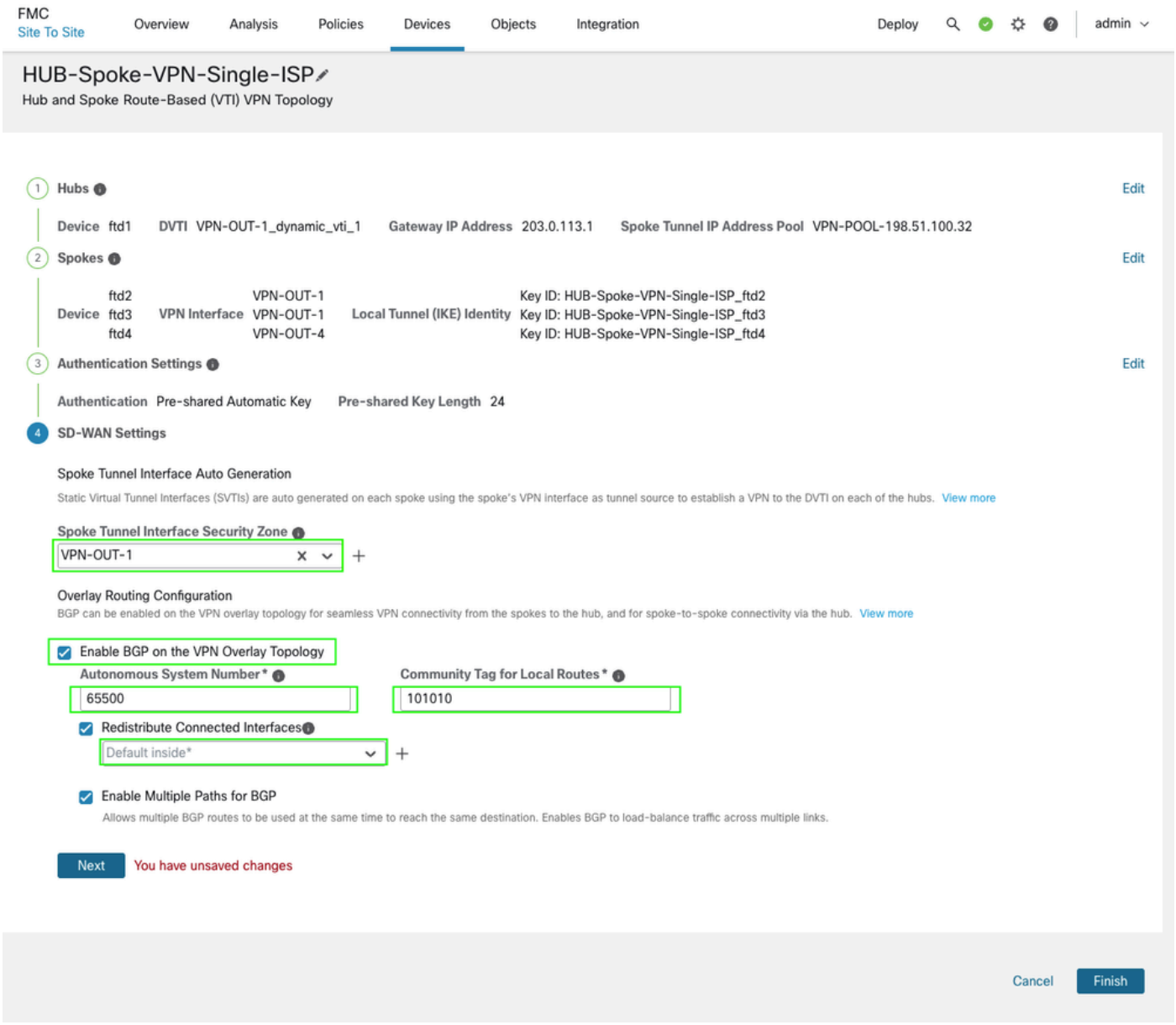
- スポークとオーバーレイインターフェイスの詳細を確認して正しいインターフェイスが選択されていることを確認し、Nextをクリックします。



- IPSec設定のデフォルトパラメータをそのまま使用することも、必要に応じてカスタム暗号を指定することもできます。Next をクリックして続けます。このドキュメントでは、デフォルトのパラメータを使用しています。



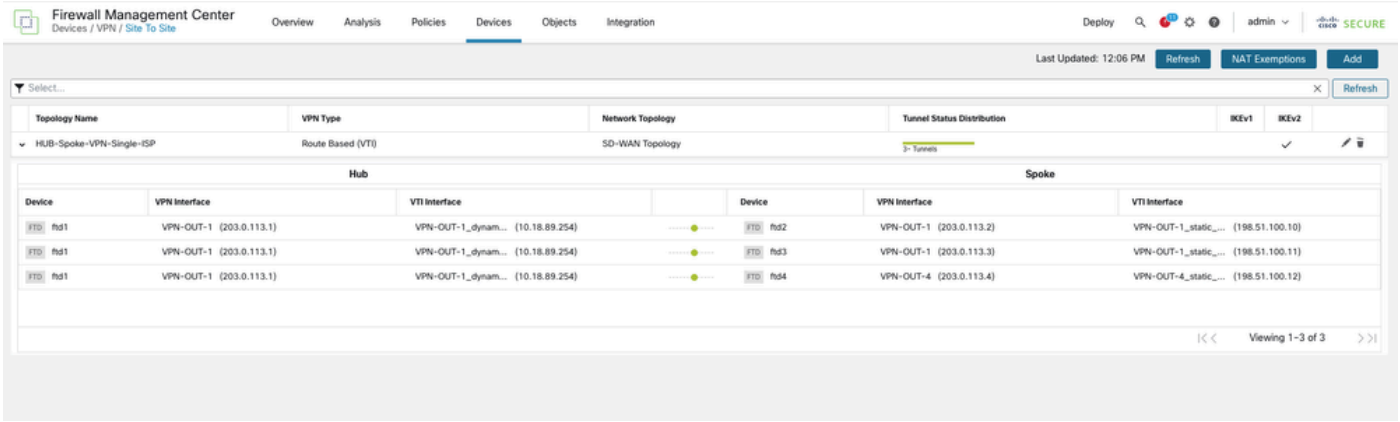
- 最後に、AS番号、内部インターフェイスアドバタイズメント、プレフィクスフィルタリングのコミュニティタグなどの適切なBGPパラメータを指定することで、このトポロジに対して同じウィザード内でオーバーレイルーティングを設定できます。セキュリティゾーンは、アクセスコントロールポリシーによるトラフィックフィルタリングに役立ちます。また、インターフェイスのオブジェクトを作成し、名前がトポロジ内のデバイス間で内部と異なる場合、または名前がトポロジ内のデバイス間で対称でない場合は、接続されたインターフェイスの再配布でそれらを使用することもできます。



- Next、Finish、最後にDeployの順にクリックして、プロセスを完了します。

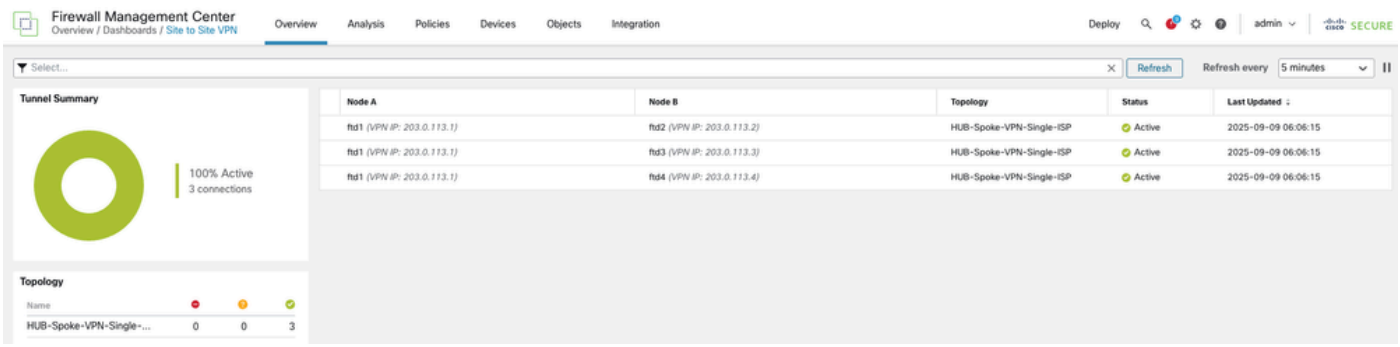
検証

- Devices > VPN > Site to Siteの順に選択して、トンネルのステータスを確認できます。

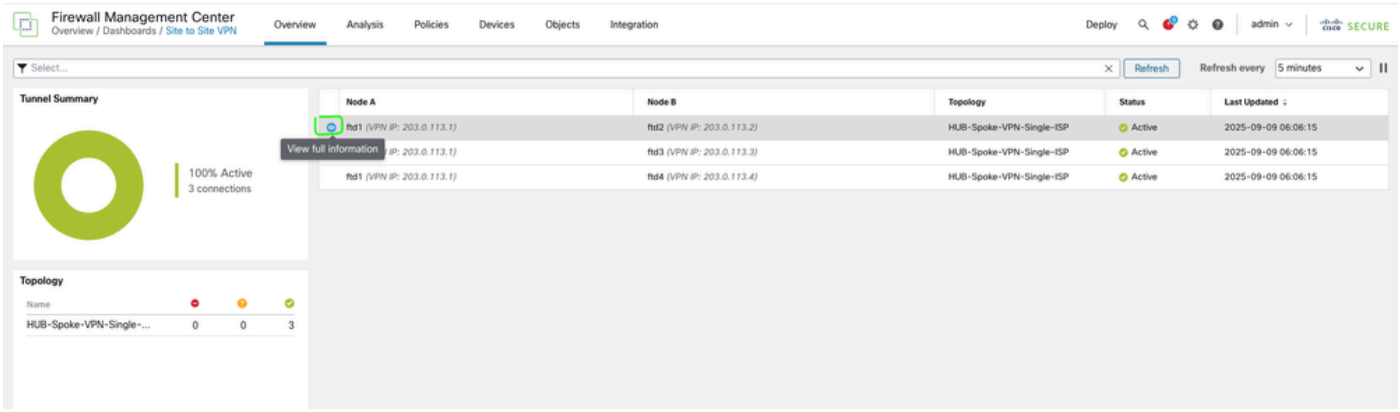


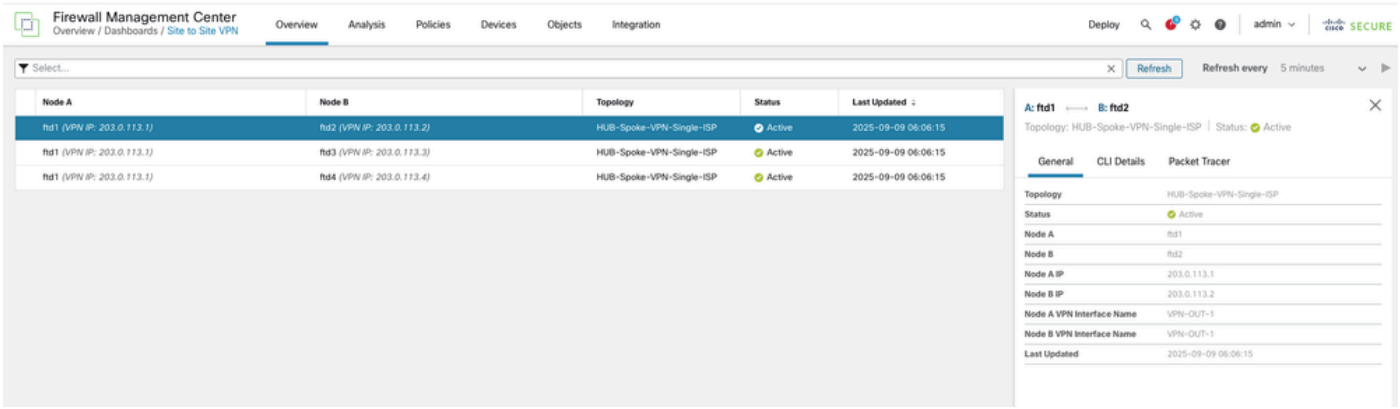
- その他の詳細については、Overview > Dashboards > Site to Site VPNの順に移動して確認で

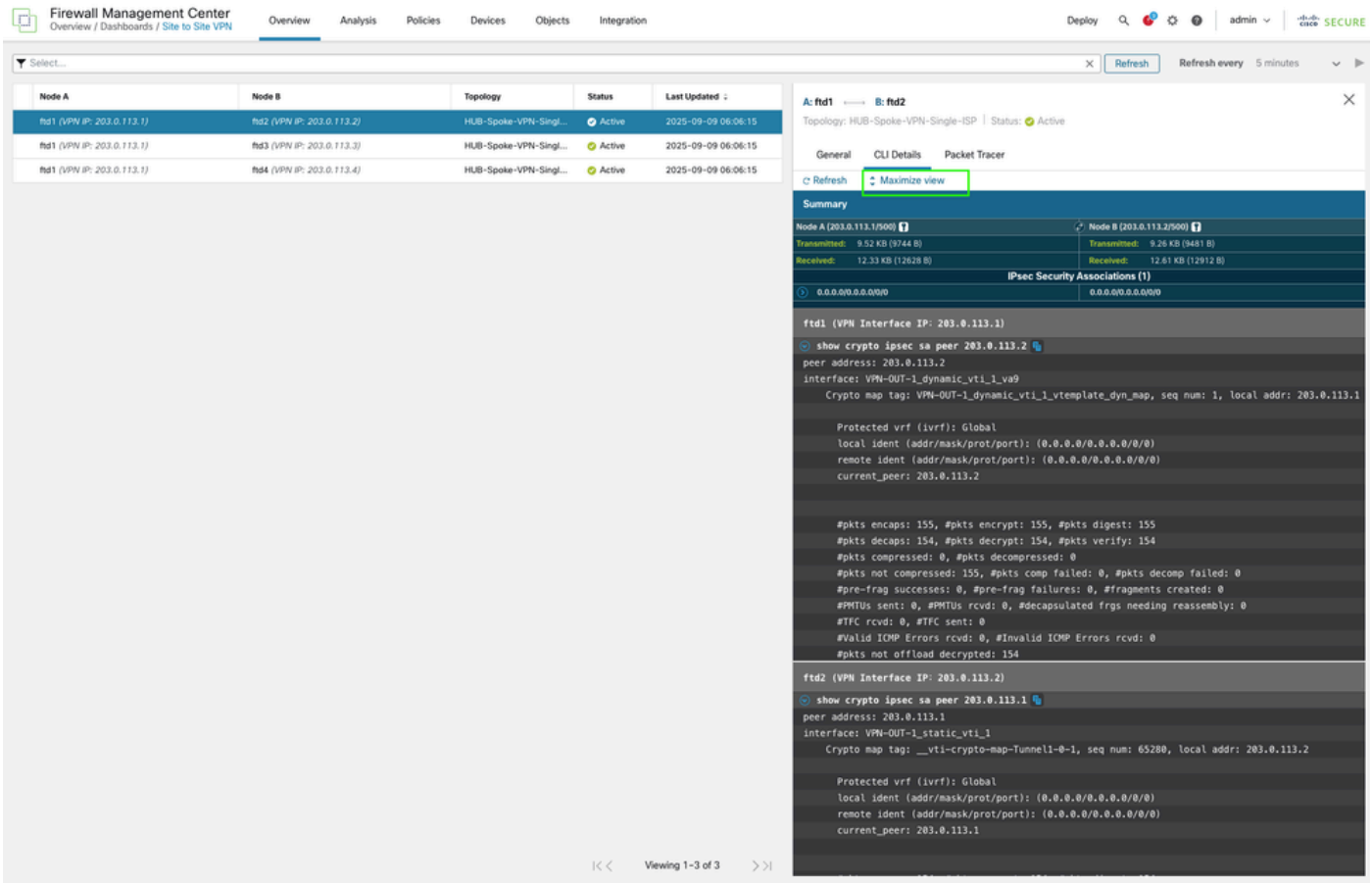
きます。



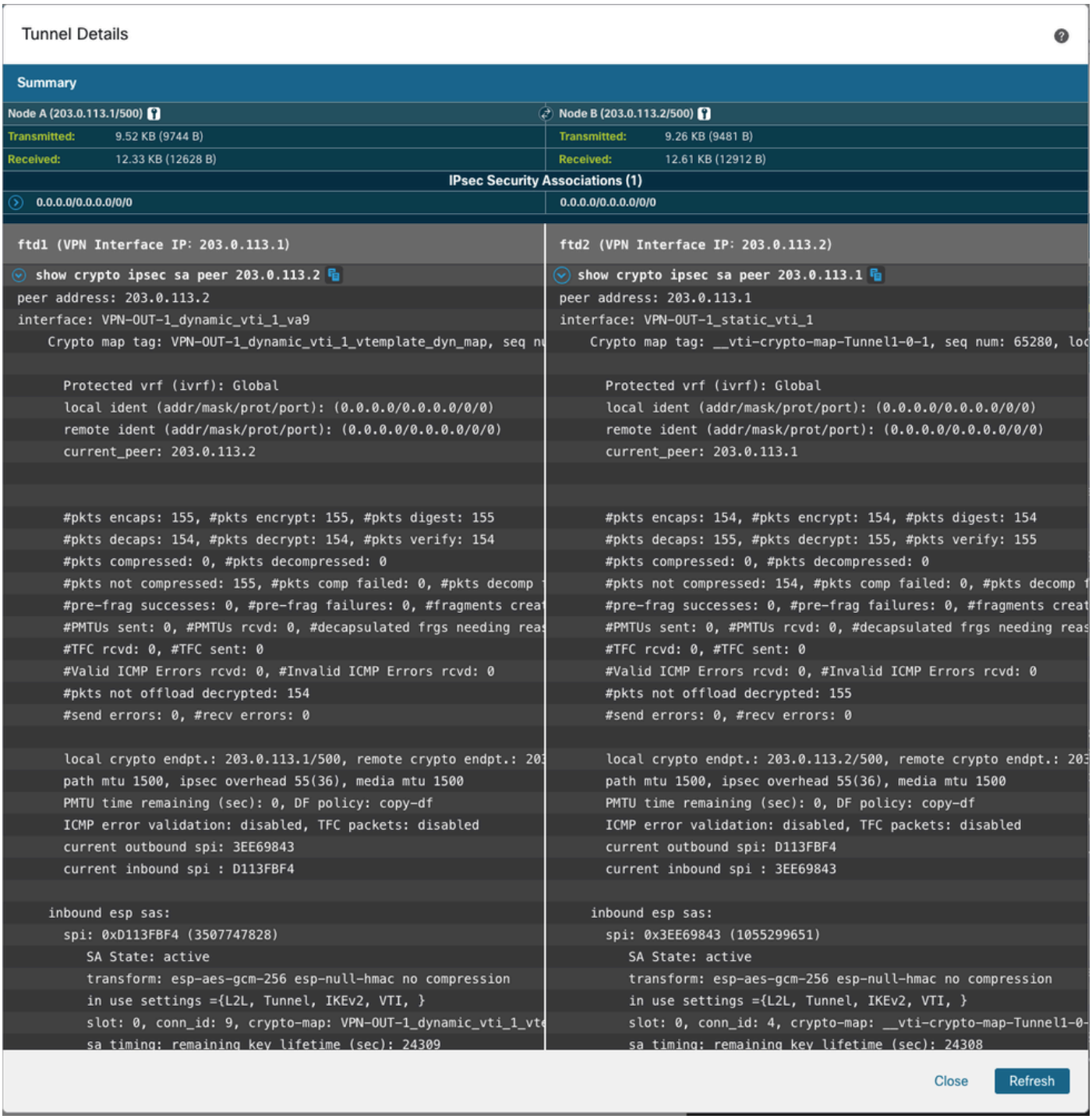
- さらに詳しい情報については、トンネルを選択して、View Full Informationをクリックしてください。







- 出力はFTD CLIから直接表示され、更新されたカウンタやセキュリティパラメータインデックス(SPI)の詳細などの重要な情報を表示するために更新できます。



- FTD CLIを使用して、ルーティング情報とBGPピアリングステータスを確認することもできます。

ハブ側

<#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
```

スポーク側

同じ検証をスポークデバイスでも実行できます。スポークの1つの例を次に示します。

<#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
```

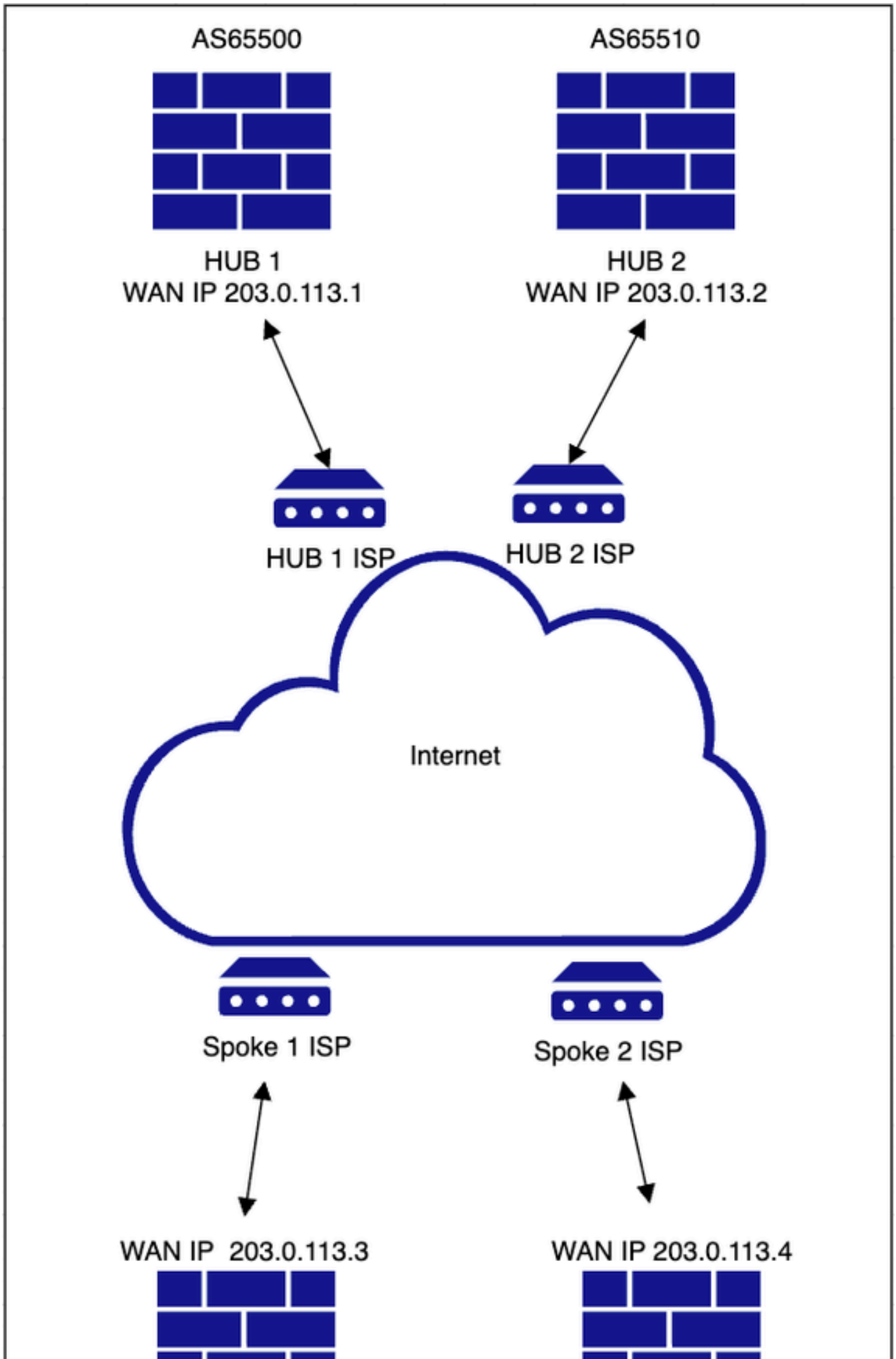
<<<<<< spoke 2 inside network

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

<<<<<< spoke 3 inside network

デュアルハブアンドスポーク（セカンダリハブとスポーク間のEBGPを介した冗長ハブ用のシングルISP）

ネットワーク図


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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。