동일한 리전에서 두 개의 허브와 네 개의 스포크를 사용하여 듀얼 ISP 토폴로지 구성

목차

소개

이 문서에서는 SD-WAN 마법사를 사용하여 동일한 지역에 있는 두 개의 허브와 네 개의 스포크로 이중 ISP 토폴로지를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

지원되는 소프트웨어 및 하드웨어 플랫폼

관리자	FTD	지원되는 플랫폼
• FMC >= 7.6.0 및 FMC REST API	• 허브 FTD >= 7.6.0 • 스포크 FTD >= 7.3.0	FMC >= 7.6.0에서 관리할 수 있는 모든 플랫폼

• cdFMC >= 7.6.0 • FDM - 지원되지 않음		

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Firewall 위협 방어
- Cisco Secure Firewall 관리 센터
- 소프트웨어 정의 WAN(SD-WAN)

사용되는 구성 요소

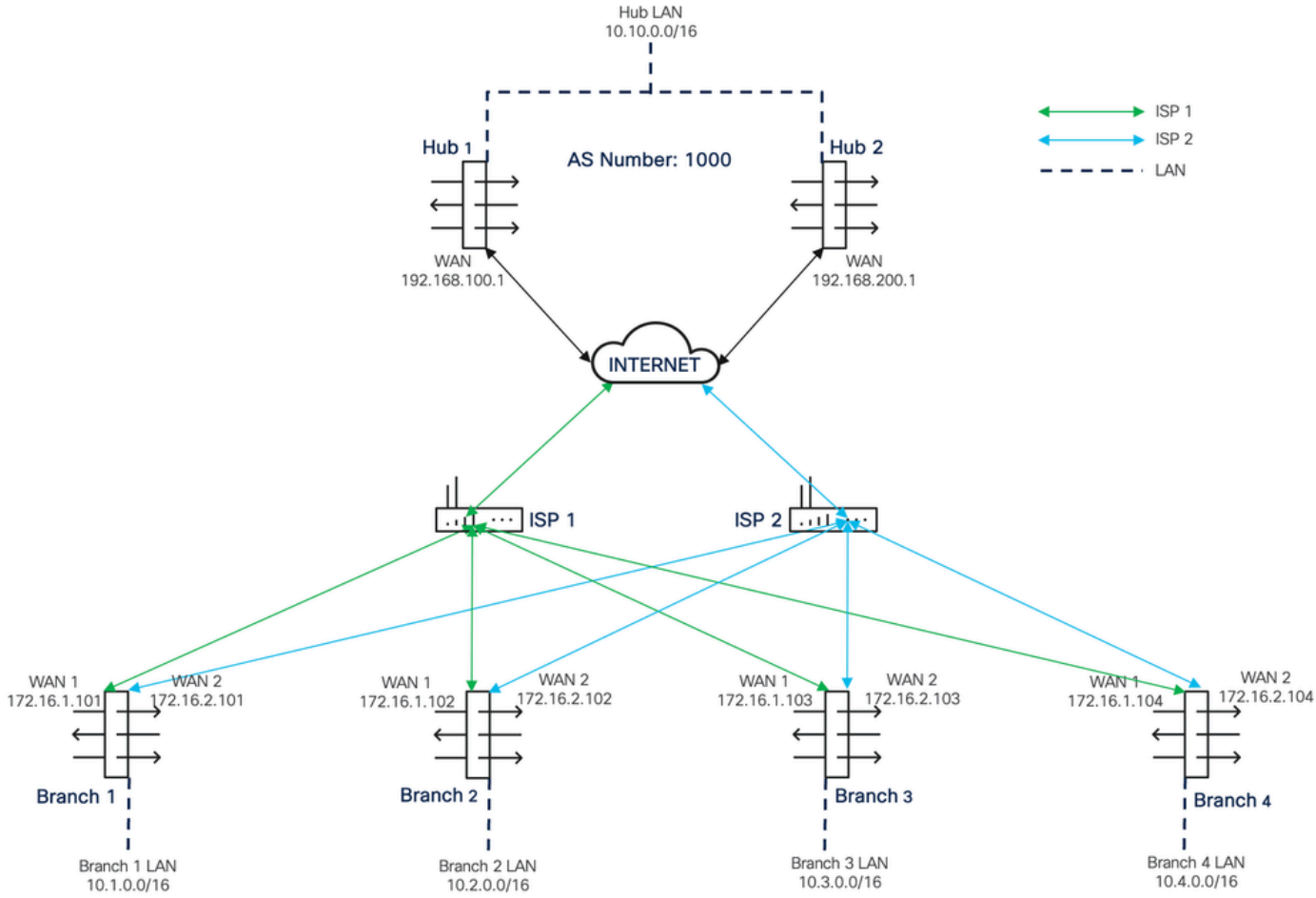
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

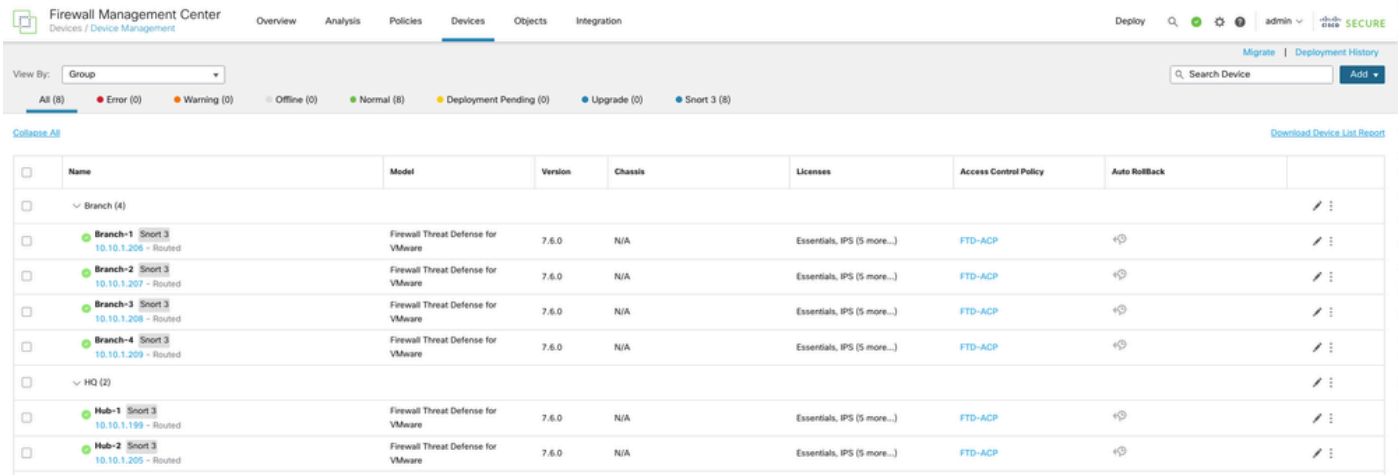
- FTD 버전 7.6.0
- FMC 버전 7.6.0

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

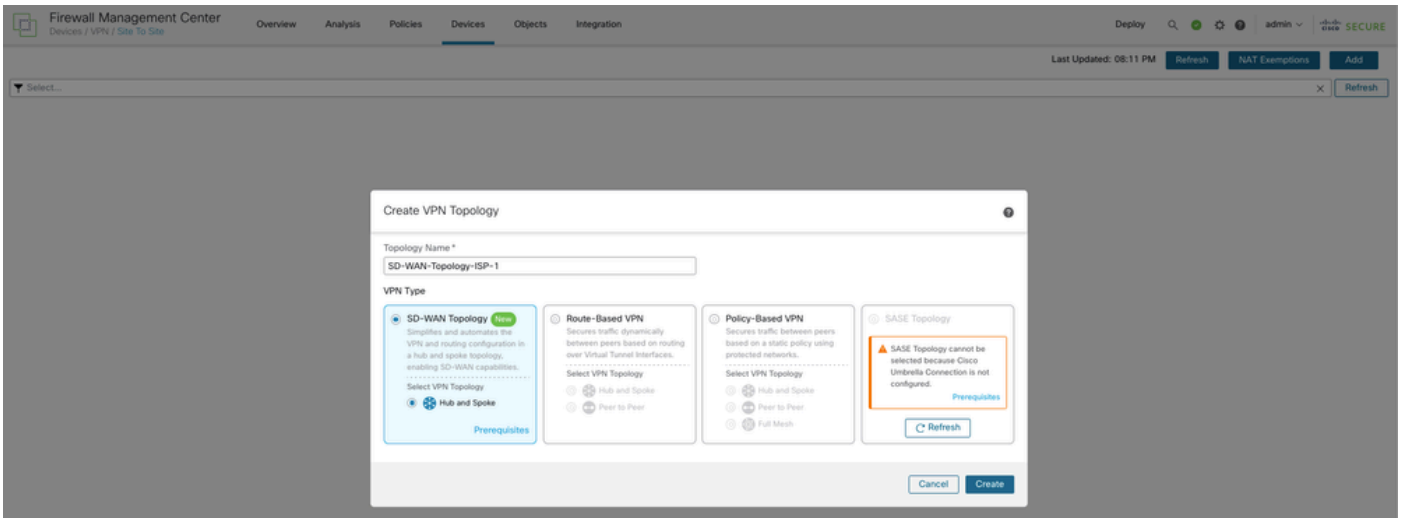
네트워크 다이어그램





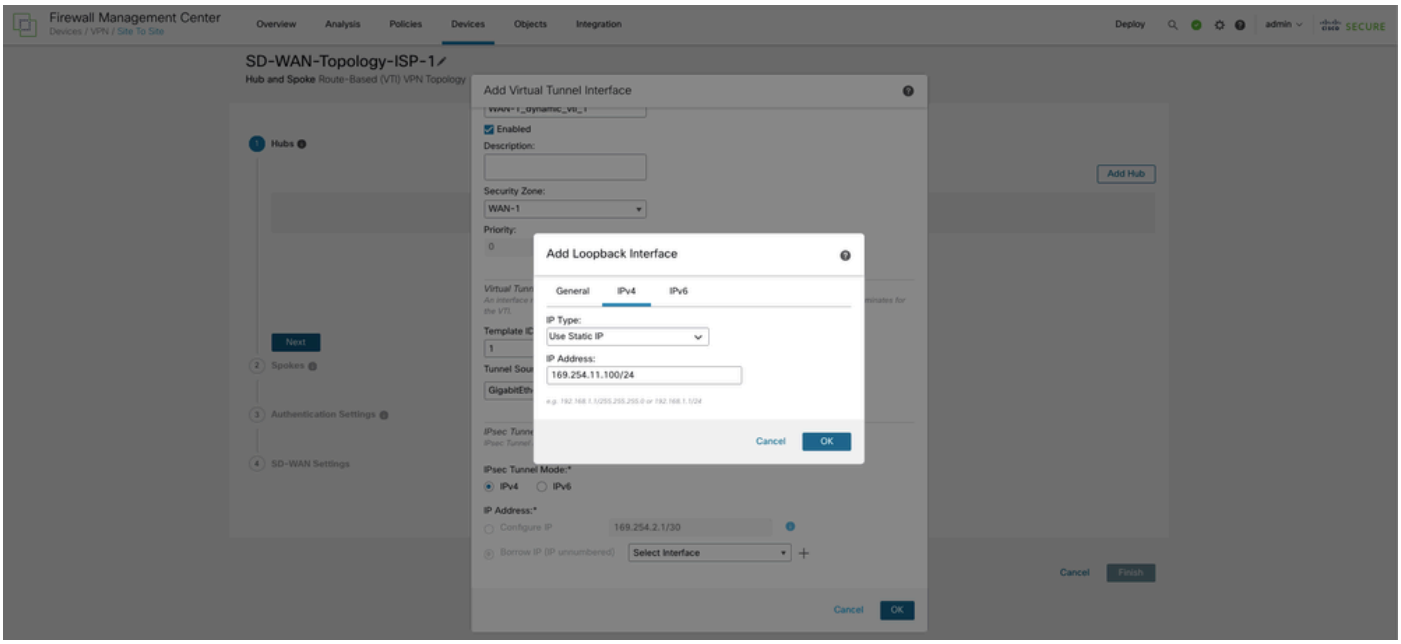
1단계. WAN-1을 VPN 인터페이스로 사용하여 SD-WAN 토폴로지 생성

Devices(디바이스) > VPN > Site To Site(사이트 대 사이트)로 이동합니다. Add(추가)를 선택하고 WAN-1을 VPN 인터페이스로 사용하는 첫 번째 토폴로지에 대한 Topology Name(토폴로지 이름) 필드에 적절한 이름을 입력합니다. SD-WAN Topology(SD-WAN 토폴로지)를 선택하고 Create(생성)를 선택합니다.

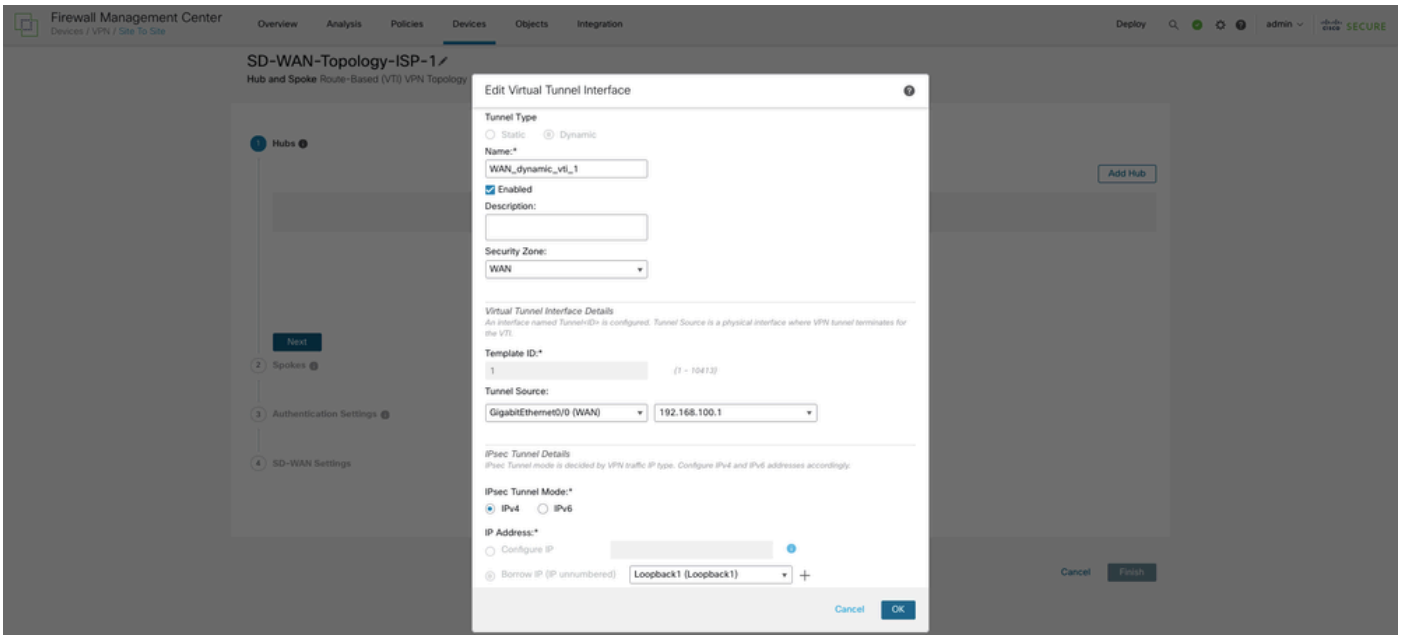


2단계. 기본 허브에 DVTI(Dynamic Virtual Tunnel Interface)를 구성합니다

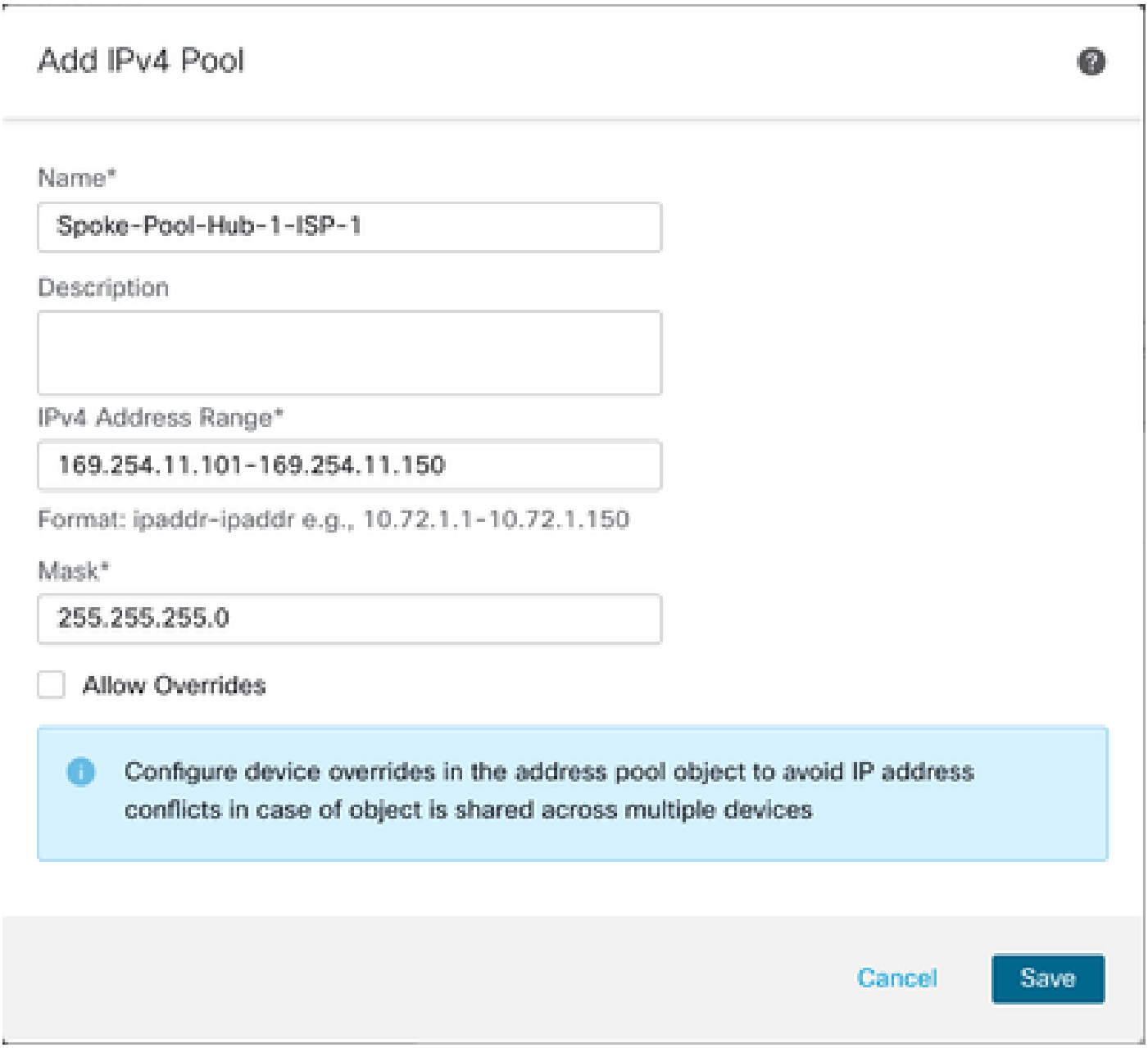
Add Hub(허브 추가)를 선택하고 Device(디바이스) 드롭다운 목록에서 기본 허브를 선택합니다. DVTI(Dynamic Virtual Tunnel Interface) 옆에 있는 + 아이콘을 선택합니다. 이름, 보안 영역 및 템플릿 ID를 구성하고 WAN-1을 DVTI의 터널 소스 인터페이스로 할당합니다.



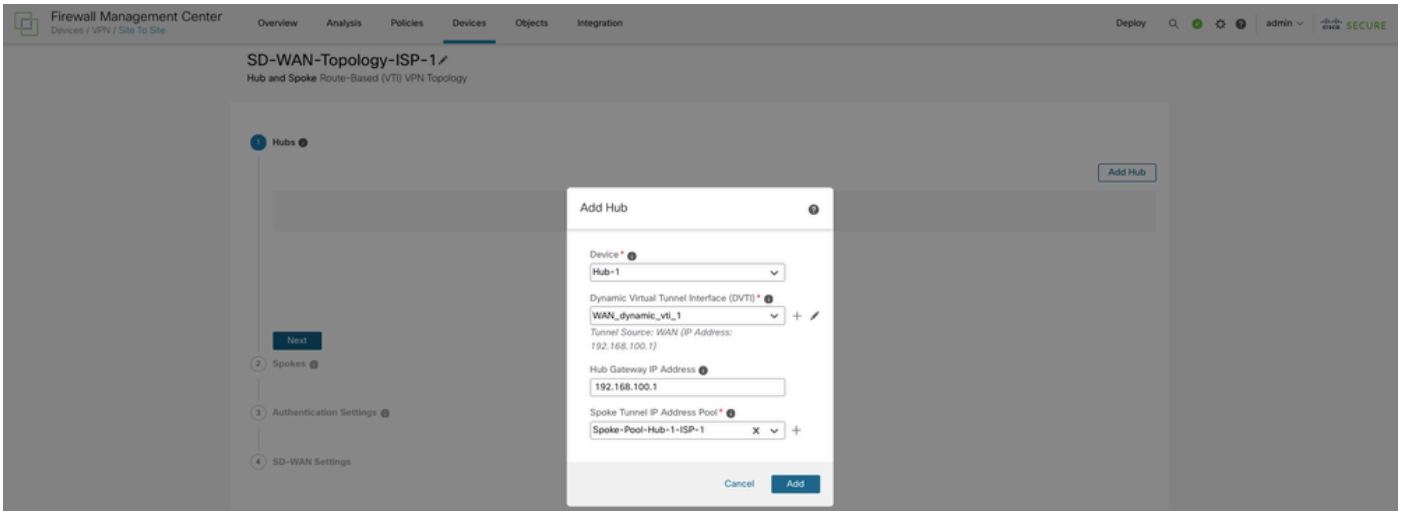
Borrow IP 드롭다운 목록에서 물리적 또는 루프백 인터페이스를 선택합니다. 현재 토폴로지에서 DVTI는 루프백 인터페이스 IP 주소를 상속합니다. 확인을 선택합니다.



주소 풀을 선택하거나 스포크 터널 IP 주소 풀 옆의 + 아이콘을 선택하여 새 주소 풀을 생성합니다. 스포크를 추가하면 마법사가 자동으로 스포크 터널 인터페이스를 생성하고 이 IP 주소 풀에서 이러한 스포크 인터페이스에 IP 주소를 할당합니다.

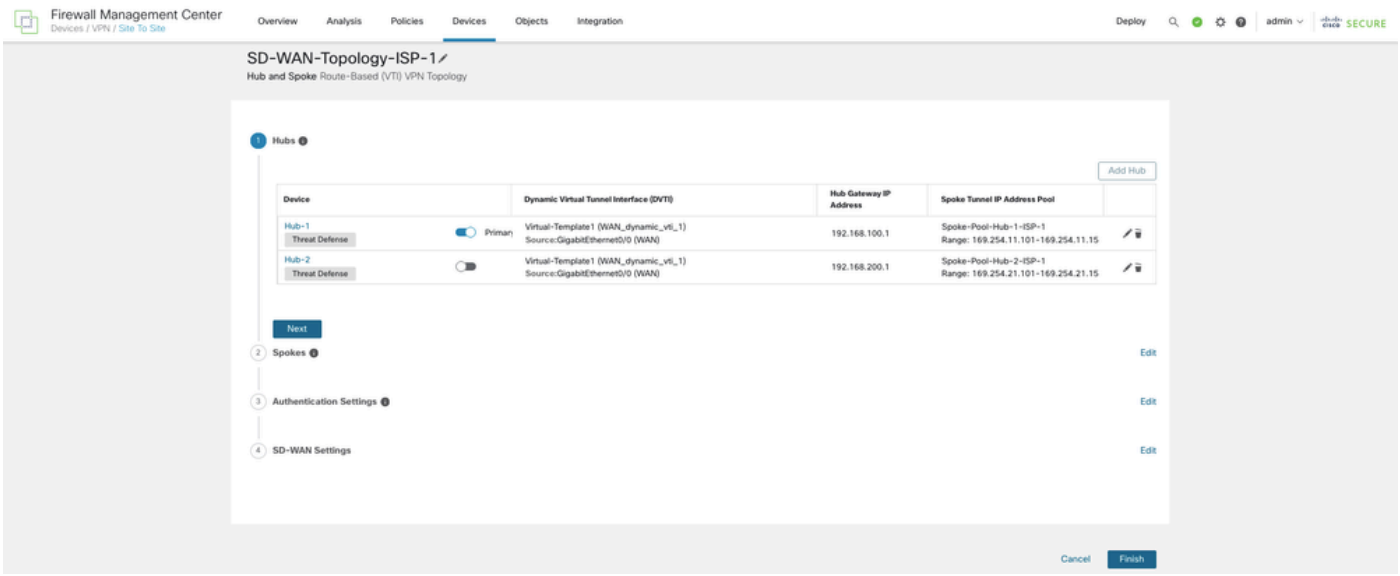


기본 허브 컨피그레이션이 완료되면 Add를 선택하여 토폴로지에 기본 허브를 저장합니다.



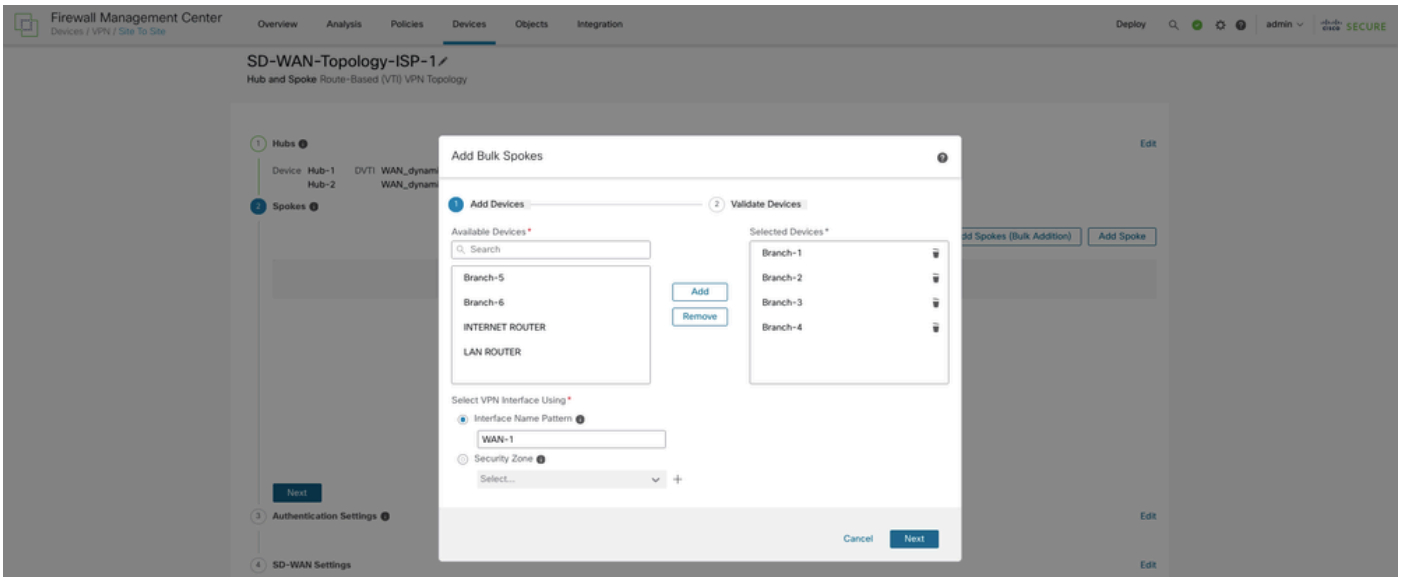
3단계. 보조 허브에서 DVTI(Dynamic Virtual Tunnel Interface)를 구성합니다

이제 Add Hub(허브 추가)를 다시 선택하여 토폴로지의 보조 허브를 WAN-1을 VPN 인터페이스로 구성합니다(단계 1 및 단계 2 반복). Next(다음)를 선택합니다.

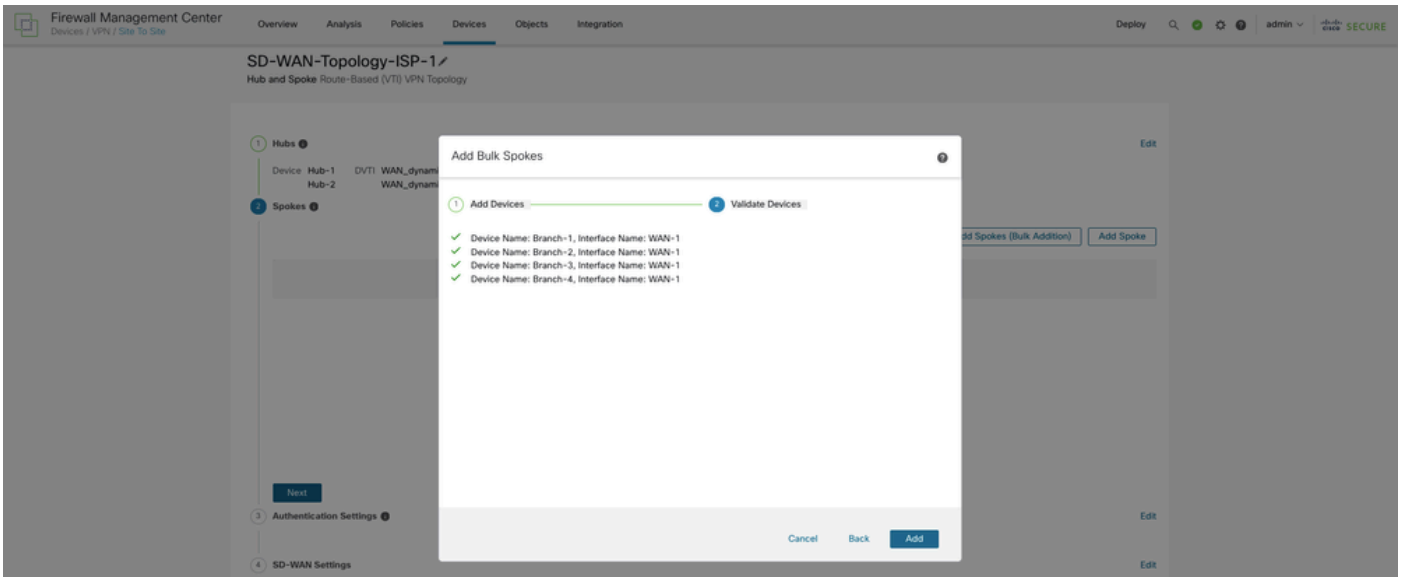


4단계. 스포크 구성

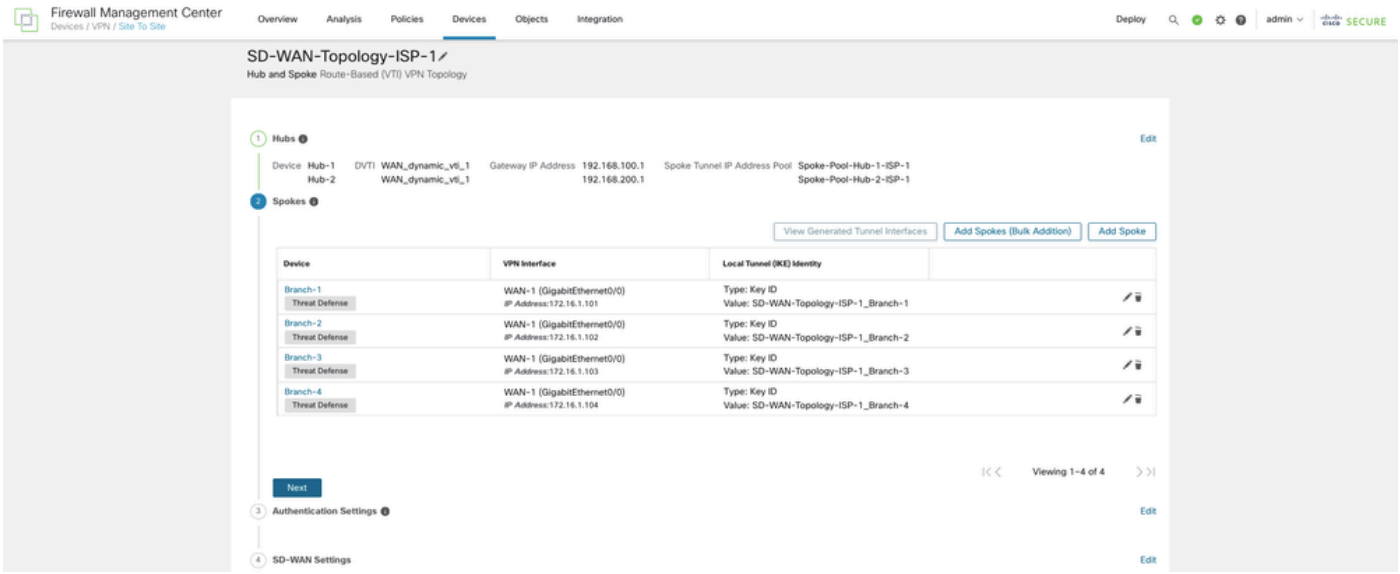
단일 스포크 디바이스를 추가하려면 스포크 추가(Add Spoke)를 선택하고, 토폴로지에 여러 스포크를 추가하려면 스포크 추가(Add Spokes (Bulk Addition))를 클릭합니다. 현재 토폴로지에서는 후자의 옵션을 사용하여 여러 브랜치 FTD를 토폴로지에 추가합니다. 벌크 스포크 추가(Add Bulk Spokes) 대화상자에서 스포크로 추가할 필수 FTD를 선택합니다. 모든 스포크에서 WAN-1의 논리적 이름과 일치하는 공통 인터페이스 이름 패턴 또는 WAN-1과 연결된 보안 영역을 선택합니다.



마법사가 스포크에 지정된 패턴 또는 보안 영역과 인터페이스가 있는지 검증하도록 Next(다음)를 선택합니다.

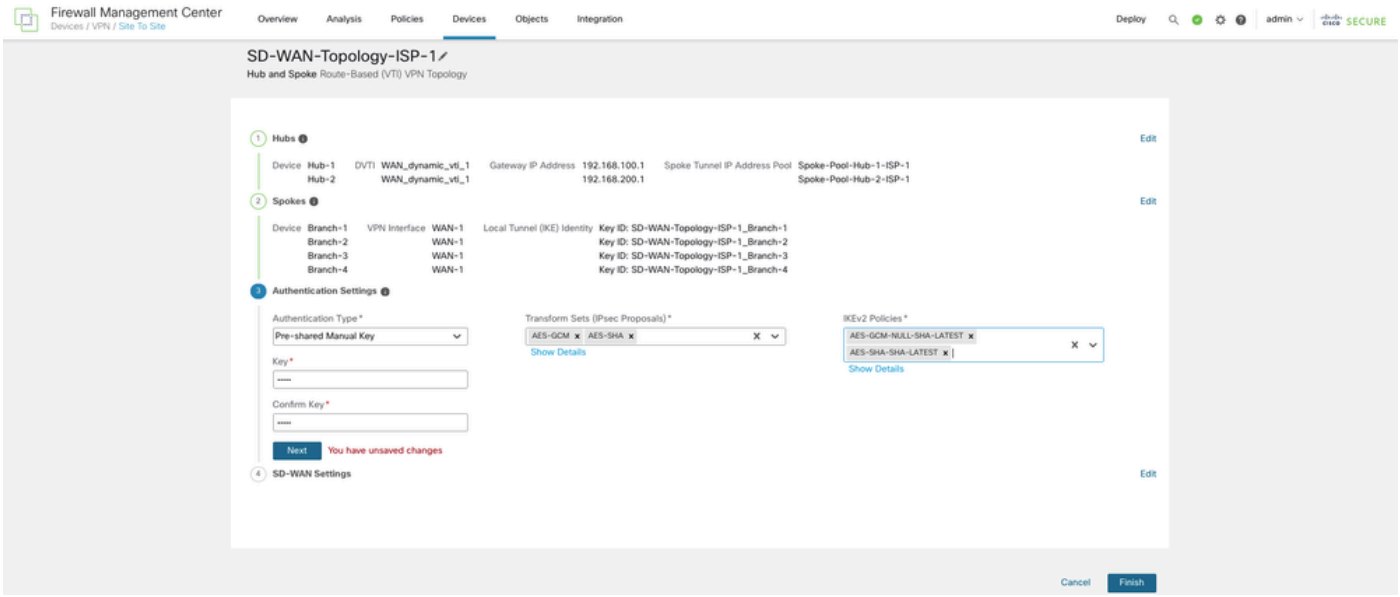


Add(추가)를 선택하면 마법사에서 자동으로 허브 DVTI를 각 스포크의 터널 소스 IP 주소로 선택합니다.



5단계. 인증 설정 구성

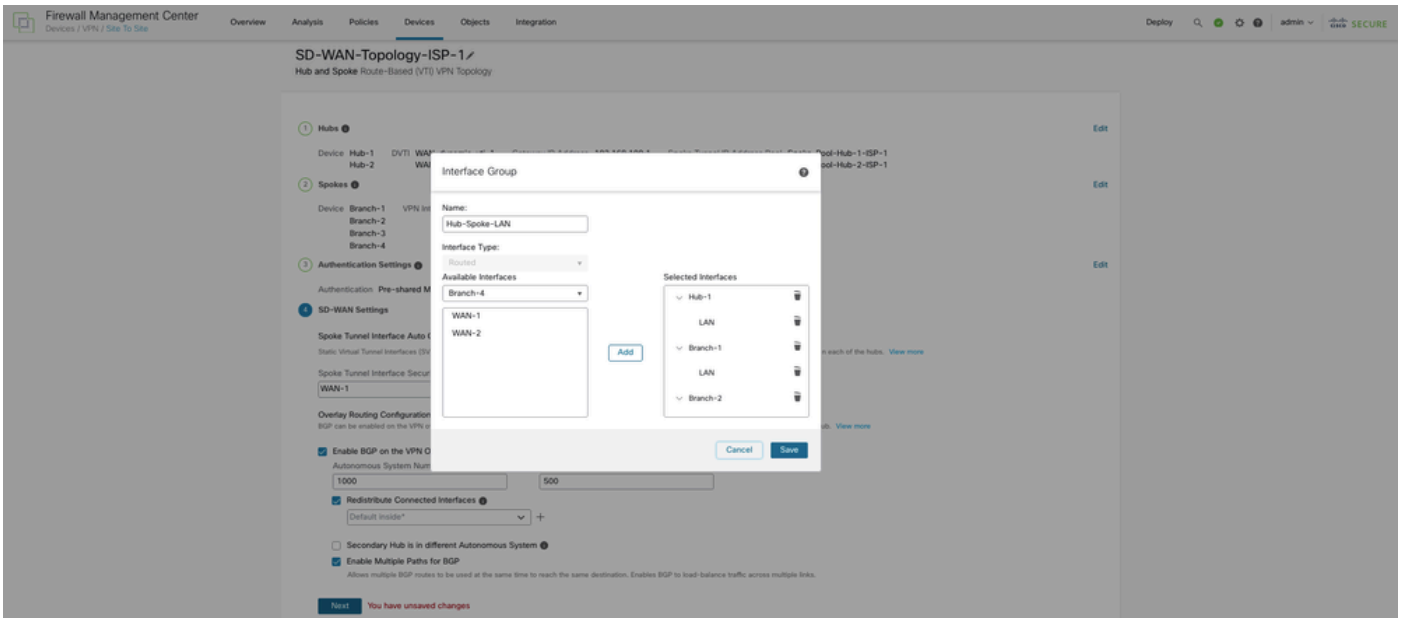
Next(다음)를 선택하여 인증 설정을 구성합니다. 디바이스 인증의 경우 Authentication Type 드롭다운 목록에서 수동 사전 공유 키, 자동 생성 사전 공유 키 또는 인증서를 선택할 수 있습니다. Transform Sets and IKEv2 Policies(변형 집합 및 IKEv2 정책) 드롭다운 목록에서 하나 이상의 알고리즘을 선택합니다.



6단계. SD-WAN 설정 구성

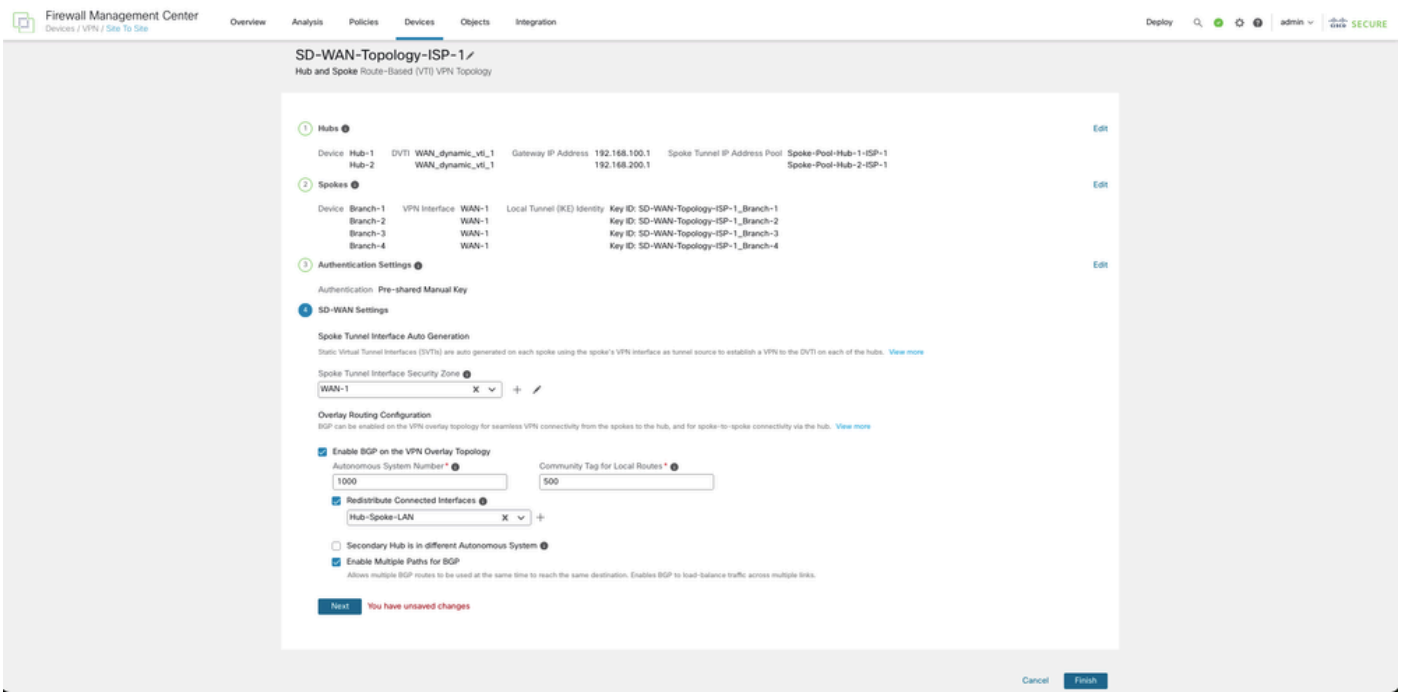
SD-WAN 설정을 구성하려면 Next(다음)를 선택합니다. 이 단계에서는 스포크 터널 인터페이스의 자동 생성 및 오버레이 네트워크의 BGP 컨피그레이션이 포함됩니다. Spoke Tunnel Interface Security Zone 드롭다운 목록에서 보안 영역을 선택하거나 +를 선택하여 마법사가 자동으로 생성한 스포크의 SVTI(Static Virtual Tunnel Interfaces)를 자동으로 추가할 보안 영역을 생성합니다.

오버레이 터널 인터페이스 간의 BGP 구성을 자동화하려면 [VPN 오버레이 토폴로지에서 BGP 사용] 확인란을 선택합니다. Autonomous System Number 필드에 AS(Autonomous System) 번호를 입력합니다. Redistribute Connected Interfaces(연결된 인터페이스 재배포) 확인란을 선택하고 드롭다운 목록에서 인터페이스 그룹을 선택하거나 +를 선택하여 오버레이 토폴로지에서 BGP 경로 재배포를 위한 허브 및 스포크의 연결된 LAN 인터페이스로 인터페이스 그룹을 생성합니다.

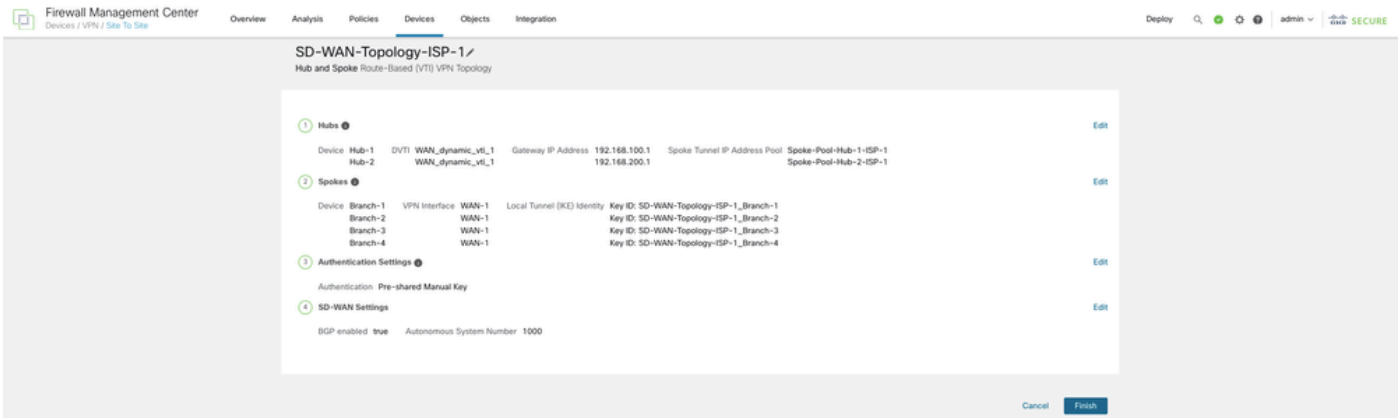


Community Tag for Local Routes 필드에 BGP 커뮤니티 특성을 입력하여 연결된 로컬 경로와 재배포된 로컬 경로를 태그합니다. 이 특성을 사용하면 경로 필터링이 쉬워집니다. 다른 AS에 보조 허브가 있는 경우 Secondary Hub is the Different Autonomous System 확인란을 선택합니다. 마지막으

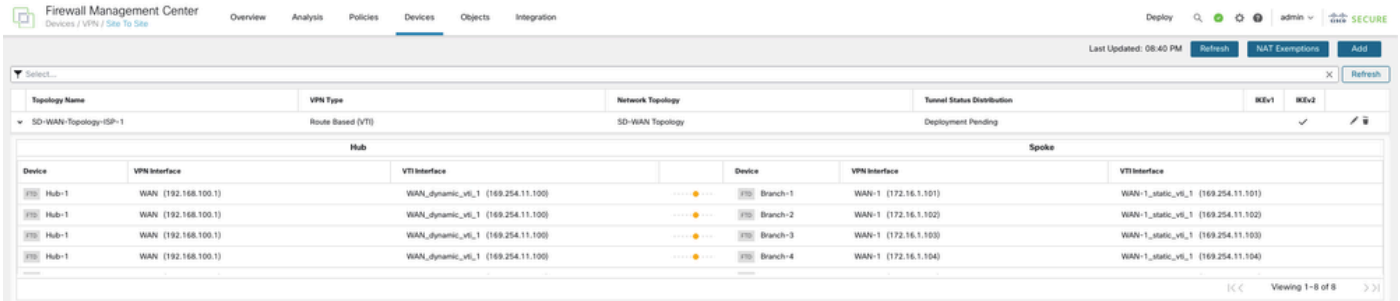
로, Enable Multiple Paths for BGP(BGP에 대해 여러 경로 활성화) 확인란을 선택하여 BGP가 여러 링크에서 트래픽을 로드 밸런싱하도록 합니다.



SD-WAN 토폴로지를 저장하고 검증하려면 Finish(마침)를 클릭합니다.



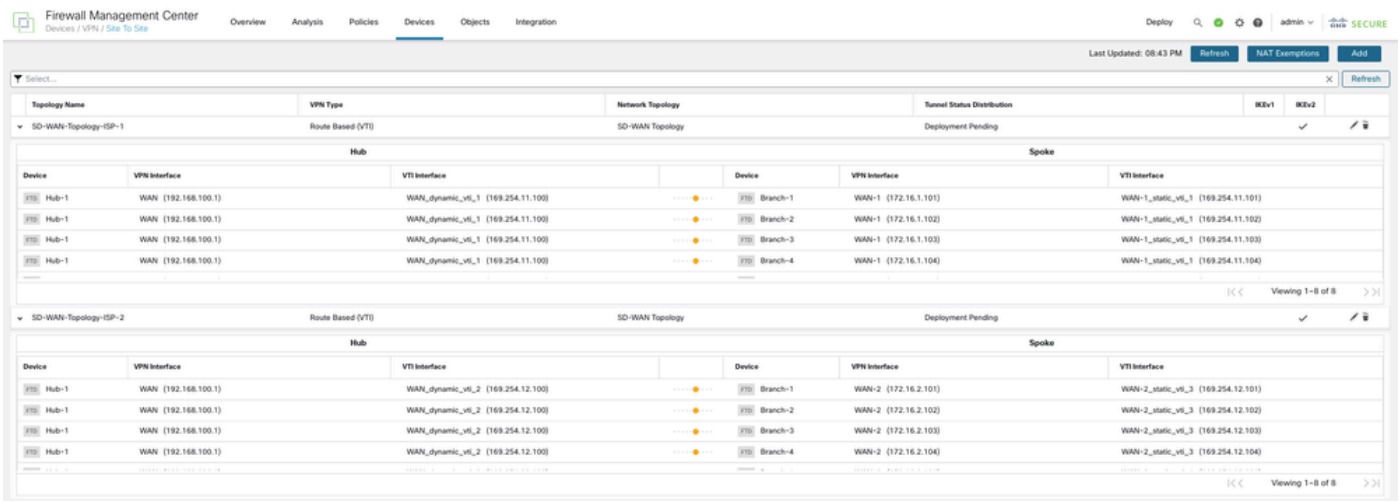
Devices(디바이스) > Site-to-site VPN(사이트 대 사이트 VPN)에서 토폴로지를 볼 수 있습니다. 첫 번째 SD-WAN 토폴로지의 총 터널 수는 8개입니다.



7단계. WAN-2를 VPN 인터페이스로 사용하여 SD-WAN 토폴로지 생성

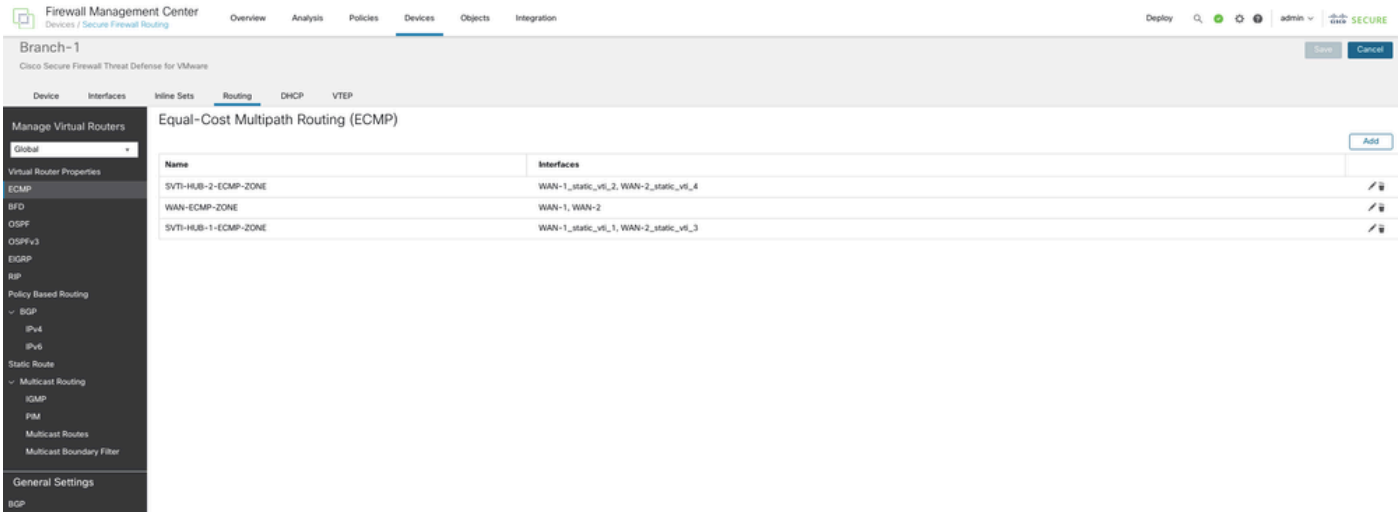
WAN-2를 VPN 인터페이스로 사용하는 SD-WAN 토폴로지를 구성하려면 1~6단계를 반복합니다.

두 번째 SD-WAN 토폴로지의 총 터널 수는 8개입니다. 최종 토폴로지는 아래 그림과 같아야 합니다
.



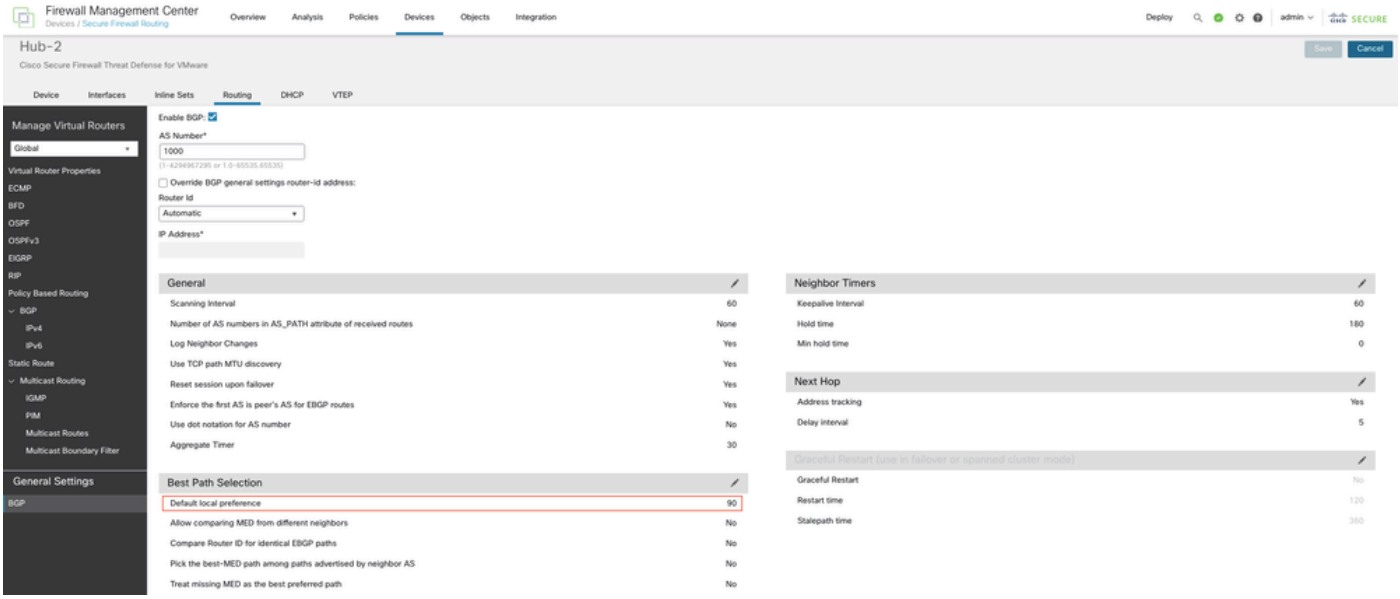
8단계. ECMP 영역 구성

각 브랜치에서 Routing(라우팅) > ECMP로 이동하고 아래와 같이 기본 및 보조 허브에 연결하는 WAN 인터페이스 및 SVTI에 대한 ECMP(Equal-Cost Multi-Path) 영역을 구성합니다. 이를 통해 링크 이중화를 제공하고 VPN 트래픽의 로드 밸런싱을 활성화할 수 있습니다.



9단계. 허브에서 BGP 로컬 환경 설정 수정

보조 허브에서 Routing(라우팅) > General Settings(일반 설정) > BGP로 이동합니다. Enable BGP(BGP 활성화)를 선택하고 AS Number(AS 번호)를 구성하며 Best Path Selection(최적 경로 선택) 아래의 기본 로컬 환경 설정 값을 기본 허브에 구성된 값보다 낮은 값으로 설정합니다. 저장을 선택합니다. 이렇게 하면 기본 허브에 대한 경로가 보조 허브에 대한 경로보다 우선합니다. 기본 허브가 다운되면 보조 허브에 대한 경로가 이어받습니다.

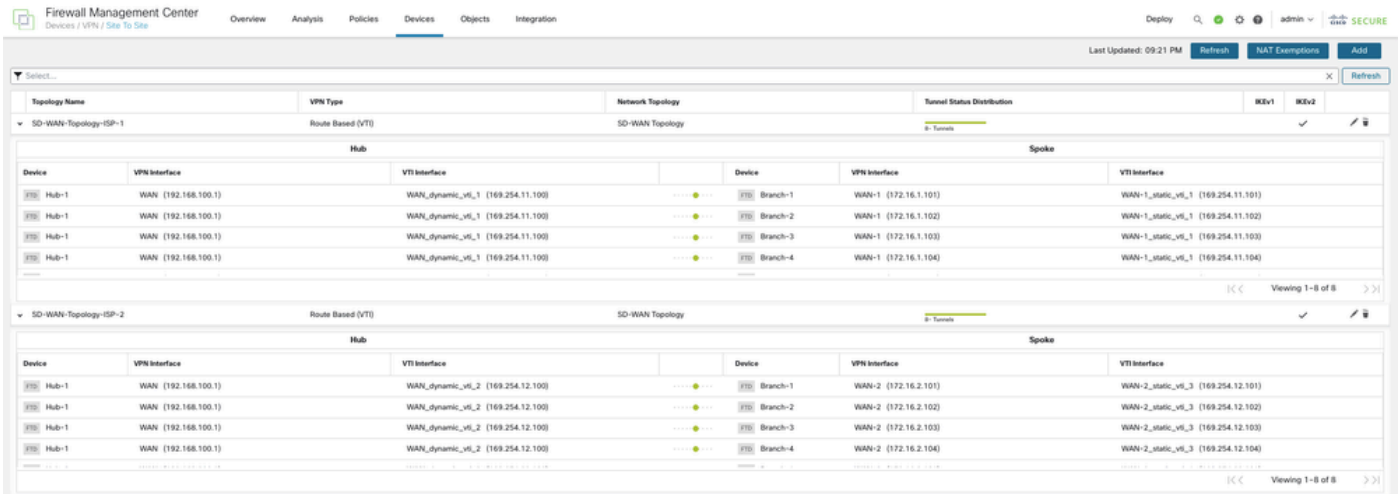


모든 디바이스에 컨피그레이션을 구축합니다.

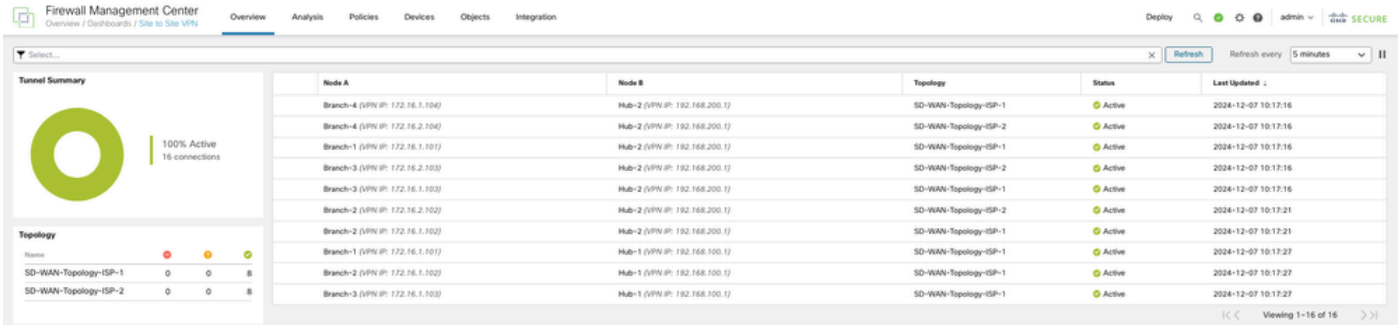
다음을 확인합니다.

터널 상태 확인

SD-WAN 토폴로지의 VPN 터널이 작동 중인지 확인하려면 Device(디바이스) > VPN > Site-to-Site(사이트 대 사이트)를 선택합니다.

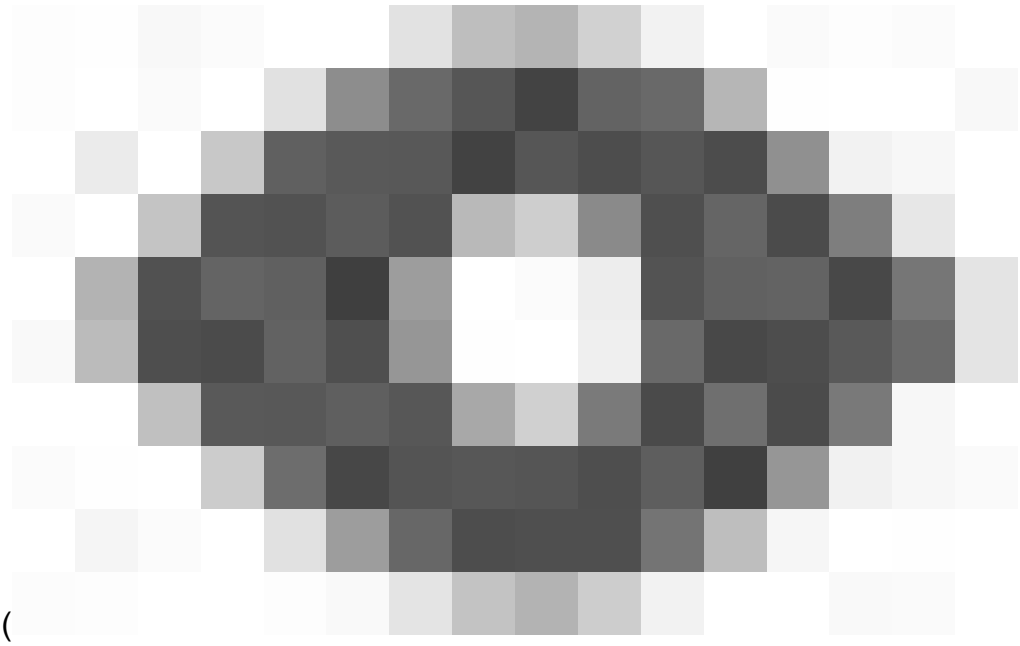


SD-WAN VPN 터널의 세부 정보를 보려면 Overview > Dashboards > Site-to-site VPN을 선택합니다.



각 VPN 터널의 세부 정보를 보려면

1. 터널 위에 마우스 커서를 올려 놓습니다.



2. View Full Information(
) 아이콘. 터널 세부사항 및 추가 작업이 포함된 창이 나타납니다.

3. IPsec 보안 연결의 show 명령 및 세부사항을 보려면 측면 창에서 CLI Details(CLI 세부사항) 탭을 선택합니다.

A: Branch-1 ⟷ B: Hub-1

Topology: SD-WAN-Topology-ISP-2 | Status: Active

General | CLI Details | Packet Tracer

Refresh | Maximize view

Summary

Node A (172.16.2.101/500)		Node B (192.168.100.1/500)	
Transmitted:	8.46 KB (8664 B)	Transmitted:	5.98 KB (6123 B)
Received:	27.73 KB (28400 B)	Received:	7.68 KB (7868 B)

IPsec Security Associations (2)

0.0.0.0/0.0.0.0/0/0		0.0.0.0/0.0.0.0/0/0	
Settings:	L2L,Tunnel,IKEv2,...	Settings:	L2L,Tunnel,IKEv2,VTI
Encaps/Encrypt:	140 / 140 pkts	Encaps/Encrypt:	92 / 92 pkts
Dcaps/Decrypt:	232 / 232 pkts	Dcaps/Decrypt:	96 / 96 pkts

Remaining Lifetime for SPI ID: 0x5B2983A9

Outbound:	3.69 GB (3962871000 B) 12:47:26 (26246 sec)	Inbound:	3.65 GB (3916794000 B) 12:50:26 (26426 sec)

Remaining Lifetime for SPI ID: 0x0F4EA9C0

Inbound:	3.99 GB (4285416000 B) 12:47:26 (26246 sec)	Outbound:	3.69 GB (3962874000 B) 12:50:26 (26426 sec)

0.0.0.0/0.0.0.0/0/0		
Settings:	L2L,Tunnel,IKEv2,...	
Encaps/Encrypt:	96 / 96 pkts	Info is not available for Extranet device
Dcaps/Decrypt:	92 / 92 pkts	

Remaining Lifetime for SPI ID: 0x1DEFCB21

Outbound:	4.03 GB (4331514000 B) 12:50:25 (26425 sec)	Inbound:	No data

Remaining Lifetime for SPI ID: 0x53B1AE47

Inbound:	3.65 GB (3916794000 B) 12:50:25 (26425 sec)	Outbound:	No data

Branch-1 (VPN Interface IP: 172.16.2.101)

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

이중화 및 허브 레벨 이중화를 확인하기 위해 브랜치 1에서 허브로 이동하는 트래픽만 사용됩니다. 설정 세부 정보는 다음과 같습니다.

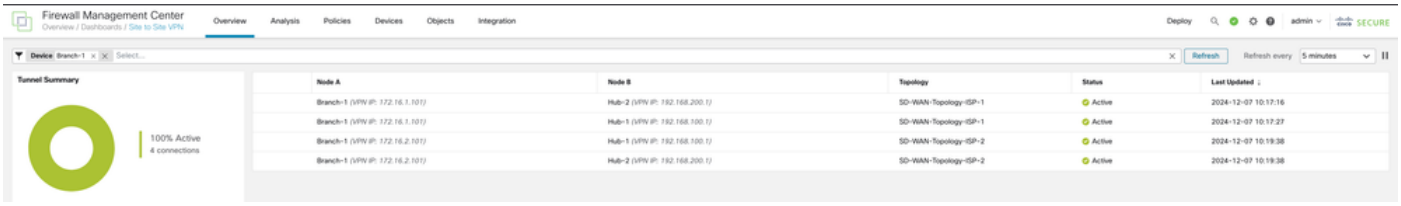
10.1.0.0.100 - 브랜치 1 연결 네트워크의 클라이언트

10.10.0.0.100 - 허브 연결 네트워크의 클라이언트

WAN-1_static_vti_1 - ISP 1을 통해 허브 1로 SVTI
WAN-2_static_vti_3 - ISP 2를 통해 허브 1로 SVTI
WAN-1_static_vti_2 - ISP 1을 통해 허브 2로 SVTI
WAN-2_static_vti_4 - ISP 2를 통해 허브 2로 SVTI

VPN 트래픽의 로드 밸런싱 확인

터널 상태는 Site to Site VPN(사이트 대 사이트 VPN) 대시보드에서 확인할 수 있습니다. 모든 터널은 액티브 상태여야 하는 것이 좋습니다.



기본 허브에 대한 경로가 우선합니다. Branch 1의 show route 명령은 VPN 트래픽이 ISP 1 및 ISP 2의 두 SVTI 간에 로드 밸런싱되어 기본 허브에 있음을 나타냅니다.

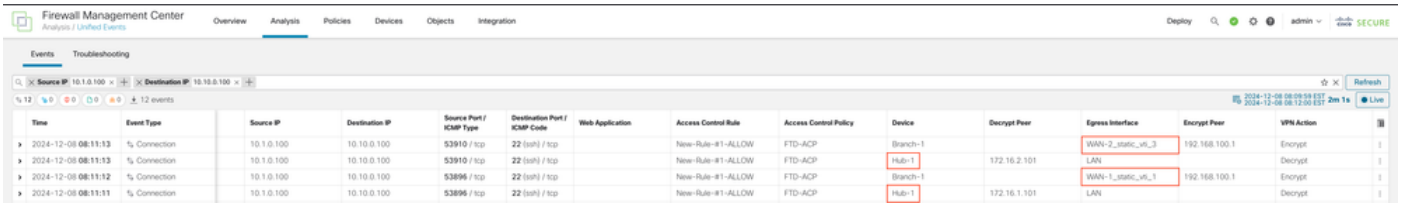
CLI Troubleshoot

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

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set

C        10.1.0.0 255.255.0.0 is directly connected, LAN
L        10.1.0.1 255.255.255.255 is directly connected, LAN
B        10.10.0.0 255.255.0.0 [200/1] via 169.254.12.100, 01:41:02
                               [200/1] via 169.254.11.100, 01:41:02
C        169.254.11.0 255.255.255.0 is directly connected, WAN-1_static_vti_1
V        169.254.11.100 255.255.255.255
           connected by VPN (advertised), WAN-1_static_vti_1
L        169.254.11.101 255.255.255.255
           is directly connected, WAN-1_static_vti_1
C        169.254.12.0 255.255.255.0 is directly connected, WAN-2_static_vti_3
V        169.254.12.100 255.255.255.255
           connected by VPN (advertised), WAN-2_static_vti_3
L        169.254.12.101 255.255.255.255
           is directly connected, WAN-2_static_vti_3
C        169.254.21.0 255.255.255.0 is directly connected, WAN-1_static_vti_2
V        169.254.21.100 255.255.255.255
           connected by VPN (advertised), WAN-1_static_vti_2
L        169.254.21.101 255.255.255.255
           is directly connected, WAN-1_static_vti_2
C        169.254.22.0 255.255.255.0 is directly connected, WAN-2_static_vti_4
V        169.254.22.100 255.255.255.255
           connected by VPN (advertised), WAN-2_static_vti_4
L        169.254.22.101 255.255.255.255
           is directly connected, WAN-2_static_vti_4
C        172.16.1.0 255.255.255.0 is directly connected, WAN-1
L        172.16.1.101 255.255.255.255 is directly connected, WAN-1
C        172.16.2.0 255.255.255.0 is directly connected, WAN-2
L        172.16.2.101 255.255.255.255 is directly connected, WAN-2
D        192.168.1.0 255.255.255.0 [90/768] via 172.16.1.1, 02:03:26, WAN-1
D        192.168.2.0 255.255.255.0 [90/768] via 172.16.2.1, 02:03:26, WAN-2
D        192.168.100.0 255.255.255.0 [90/1024] via 172.16.2.1, 02:03:26, WAN-2
                                     [90/1024] via 172.16.1.1, 02:03:26, WAN-1
D        192.168.200.0 255.255.255.0 [90/1024] via 172.16.2.1, 02:03:26, WAN-2
                                     [90/1024] via 172.16.1.1, 02:03:26, WAN-1
```

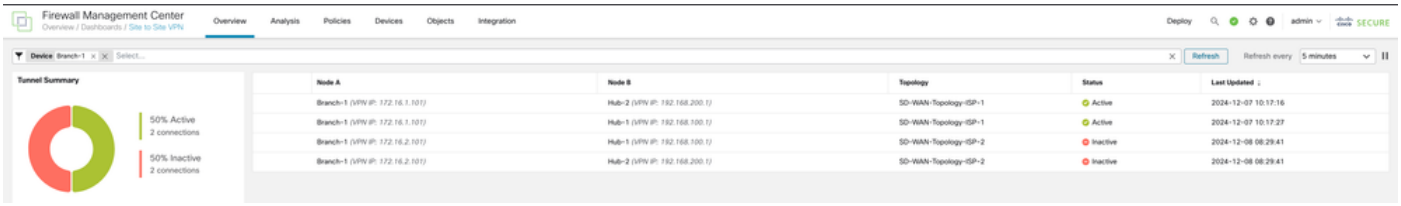
Close

실제 VPN 트래픽에 대해 사용된 이그레스 인터페이스는 다음과 같은 Unified Events에서 볼 수 있습니다.



이중 ISP 이중화 확인

ISP-2가 작동 중지되면 터널 상태는 ISP-1을 통한 터널이 활성 상태임을 나타냅니다.



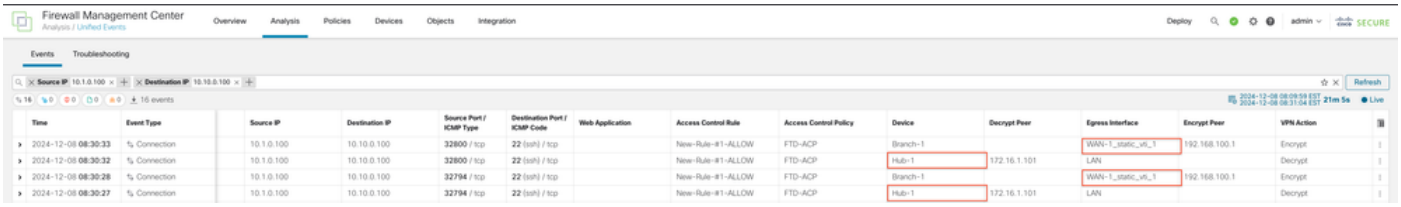
기본 허브에 대한 경로가 우선합니다. Branch 1의 show route 명령은 VPN 트래픽이 ISP-1의 SVTI를 통해 기본 허브로 라우팅됨을 나타냅니다.

CLI Troubleshoot

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

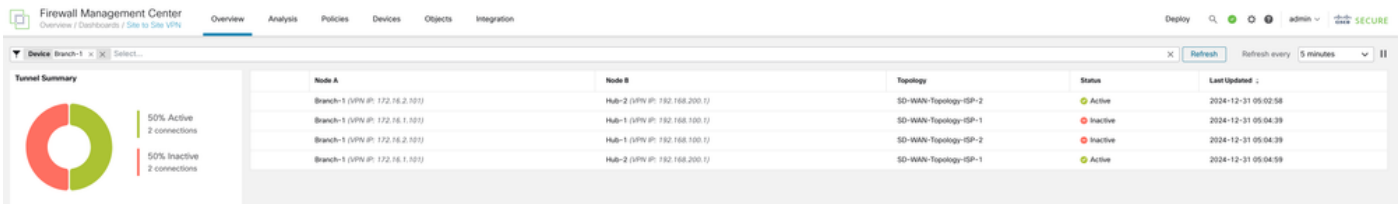
```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set

C        10.1.0.0 255.255.0.0 is directly connected, LAN
L        10.1.0.1 255.255.255.255 is directly connected, LAN
B        10.10.0.0 255.255.0.0 [200/1] via 169.254.11.100, 00:04:02
C        169.254.11.0 255.255.255.0 is directly connected, WAN-1_static_vti_1
V        169.254.11.100 255.255.255.255
           connected by VPN (advertised), WAN-1_static_vti_1
L        169.254.11.101 255.255.255.255
           is directly connected, WAN-1_static_vti_1
C        169.254.21.0 255.255.255.0 is directly connected, WAN-1_static_vti_2
V        169.254.21.100 255.255.255.255
           connected by VPN (advertised), WAN-1_static_vti_2
L        169.254.21.101 255.255.255.255
           is directly connected, WAN-1_static_vti_2
C        172.16.1.0 255.255.255.0 is directly connected, WAN-1
L        172.16.1.101 255.255.255.255 is directly connected, WAN-1
D        172.16.2.0 255.255.255.0 [90/1280] via 172.16.1.1, 00:04:03, WAN-1
D        192.168.1.0 255.255.255.0 [90/768] via 172.16.1.1, 22:12:57, WAN-1
D        192.168.2.0 255.255.255.0 [90/1024] via 172.16.1.1, 00:04:03, WAN-1
D        192.168.100.0 255.255.255.0 [90/1024] via 172.16.1.1, 00:04:03, WAN-1
D        192.168.200.0 255.255.255.0 [90/1024] via 172.16.1.1, 00:04:03, WAN-1
```

실제 VPN 트래픽에 대해 사용된 이그레스 인터페이스는 다음과 같은 Unified Events에서 볼 수 있습니다.

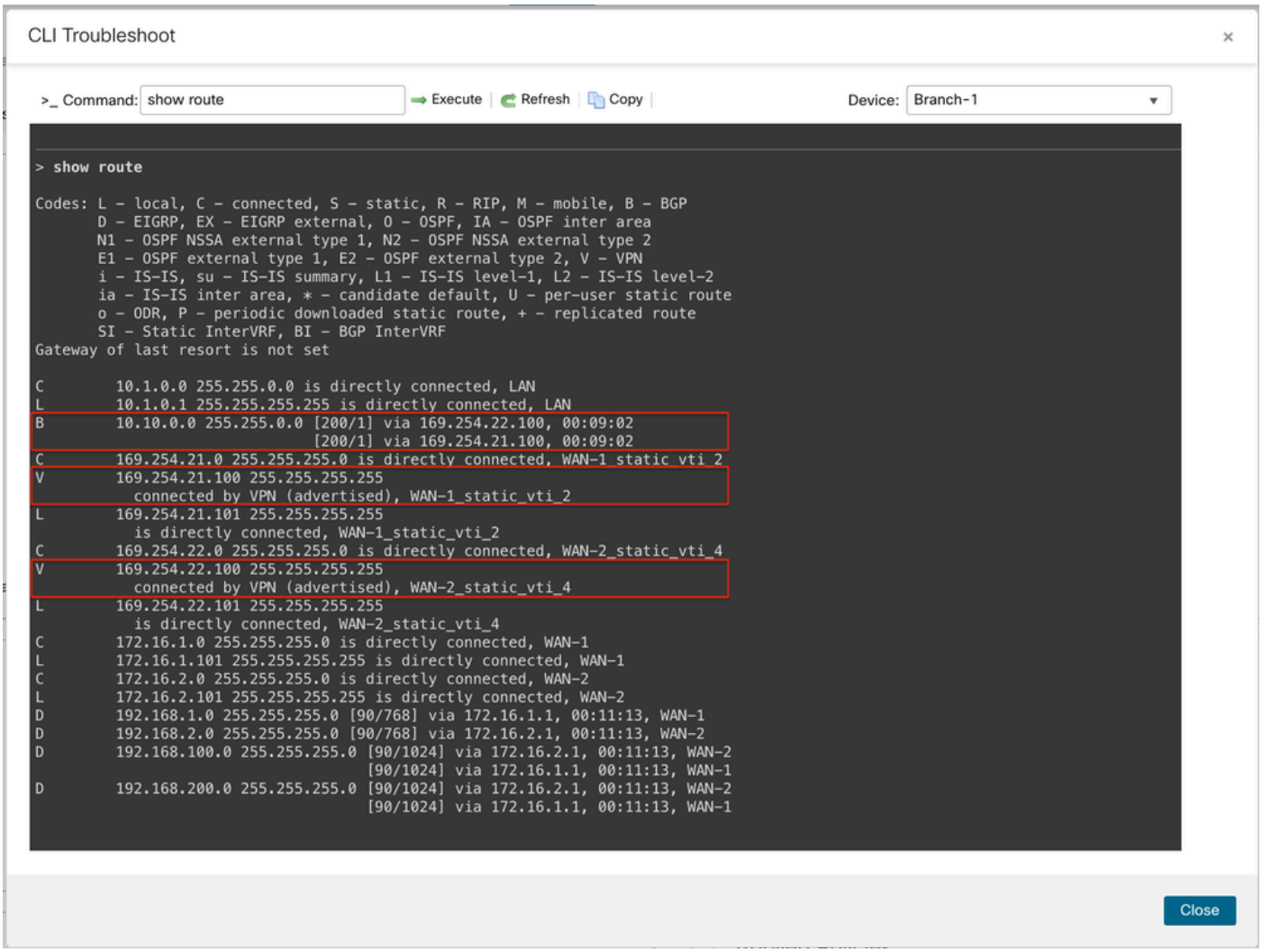


허브 레벨 이중화 확인

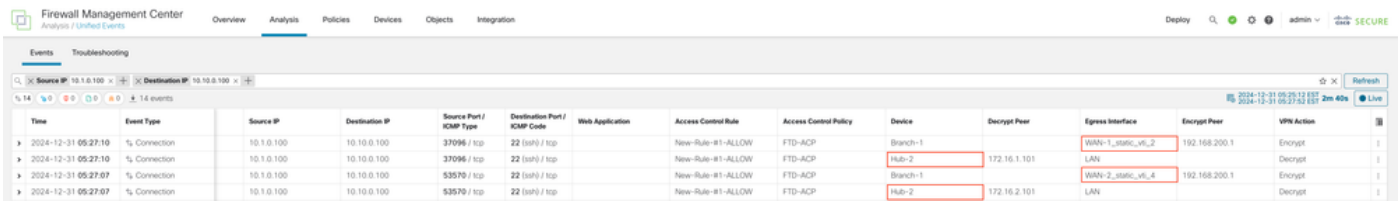
기본 허브가 다운된 경우 터널 상태는 보조 허브에 대한 터널이 활성 상태임을 나타냅니다.



기본 허브가 다운되었으므로 보조 허브에 대한 경로가 우선합니다. Branch 1의 show route 명령은 VPN 트래픽이 ISP 1의 두 SVTI와 ISP 2의 두 SVTI 간에 보조 허브로 로드 밸런싱됨을 나타냅니다.



실제 VPN 트래픽에 대해 사용된 이그레스 인터페이스는 다음과 같은 Unified Events에서 볼 수 있습니다.



이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.