DVTI(Dynamic Virtual Tunnel Interface)를 사용하여 브랜치-허브 통신 간소화

이 장에서는 허브 앤 스포크 토폴로지에서 DVTI를 실제로 적용하는 방법을 살펴봅니다. 활용 사례에서는 시나리오, 네트워크 토폴로지, 모범 사례, 사전 요건에 대해 자세히 설명합니다. 또한 원활한 구현을 위한 포괄적인 엔드 투 엔드 절차를 제공합니다.

허브 앤 스포크 토폴로지의 경로 기반 VPN

Secure Firewall Management Center는 VTI(Virtual Tunnel Interface)라고 하는 라우팅 가능한 논리적 인터페이스를 지원합니다. 이러한 인터페이스를 사용하여 정적 및 동적 라우팅 정책을 적용할 수 있습니다. VTI를 사용할 때는 정적 크립토 맵 액세스 목록을 구성하고 인터페이스에 매핑할 필요가 없습니다. 더 이상 모든 원격 서브넷을 추적하고 암호화 맵 액세스 목록에 포함하지 않아도 됩니다.

VTI를 사용하여 피어 간에 VPN 터널을 생성할 수 있습니다. VTI는 각 터널 끝에 IPsec 프로파일이 연결된 라우팅 기반 VPN을 지원합니다. VTI는 정적 또는 동적 경로를 사용합니다. 위협 방어 디바이스는 터널 인터페이스에서 들어오고 나가는 트래픽을 암호화하거나 암호 해독하고 라우팅 테이블에 따라 전달합니다.

관리 센터는 VTI 또는 경로 기반 VPN을 설정하는 데 기본값을 사용하는 사이트 간 VPN 마법사를 지원합니다.

허브 앤 스포크 토폴로지에서 경로 기반 VPN을 구현하는 경우 DVTI(Dynamic Virtual Tunnel Interface)는 허브에 구성되고 SVTI(Static Virtual Tunnel Interface)는 스포크에 구성됩니다.

동적 VTI는 IPsec 인터페이스의 동적 인스턴스화 및 관리를 위해 가상 템플릿을 사용합니다. 가상 템플릿은 각 VPN 세션에 고유한 가상 액세스 인터페이스를 동적으로 생성합니다. 동적 VTI는 여러 IPsec 보안 연결을 지원하며 스포크에서 제안한 여러 IPsec 선택기를 허용합니다.

Secure Firewall Threat Defense는 링크 이중화를 제공하는 경로 기반(VTI) VPN에 대한 백업 터널 구성을 지원합니다. 기본 VTI(기본 터널)가 트래픽을 라우팅할 수 없는 경우 VPN의 트래픽은 백업 VTI(보조 터널)를 통해 터널링됩니다.

이점

허브 앤 스포크 토폴로지에서 VTI 기반 VPN을 사용하는 경우의 이점은 다음과 같습니다.

1. 설정 간소화: VTI는 터널 자체를 나타내는 논리적 인터페이스를 제공하여 VPN 터널의 설정을 간소화합니다. 따라서 일반적으로 기존 VPN 설정에서와 관련된 복잡한 암호화 맵 또는 액세스 목록 구성이 필요하지 않습니다.
2. 간소화된 관리**:** 대규모 엔터프라이즈 허브 및 스포크 배포를 위한 피어 구성을 쉽게 관리할 수 있습니다. 스포크에 설정된 여러 고정 VTI에 대해 하나의 동적 VTI만 허브에 설정됩니다.
3. 확장성**:** VTI를 사용하면 쉽게 확장할 수 있습니다. 새로운 스포크를 추가할 때 허브에서 추가 VPN 구성이 필요하지 않습니다. 설정에 따라 NAT 및 라우팅 구성을 업데이트해야 할 수 있습니다.
4. 동적 라우팅 지원**:** VTI는 OSPF(Open Shortest Path First)와 같은 동적 라우팅 프로토콜을 지원하므로 VPN 엔드포인트 간의 라우팅 정보 동적 교환이 가능합니다. 따라서 실시간 네트워크 조건을 기반으로 효율적인 라우팅 결정이 가능합니다.
5. 이중 **ISP** 리던던시**:** SVTI는 백업 VTI 터널을 지원합니다.
6. 로드 밸런싱**:** SVTI는 ECMP를 사용하는 VPN 트래픽의 로드 밸런싱을 지원합니다.

이 활용 사례가 귀사에 적합합니까?

DVTI 허브 앤 스포크 구성의 대상에는 조직의 네트워크 인프라 설계 및 관리를 책임지는 네트워크 설계자, IT 관리자 및 네트워킹 전문가가 포함됩니다. 이 활용 사례는 원격 스포크 사이트에 연결하는 보안 터널이 있는 중앙 집중식 허브를 구현하여 네트워크 연결을 최적화하고, 데이터 보안을 보장하며, 네트워크 관리를 간소화하려는 사용자에게 유용합니다.

시나리오

각기 다른 도시에 여러 개의 브랜치 오피스를 보유한 중견 기업은 안전하고 효율적인 네트워크 인프라를 구축하여 이러한 브랜치를 중앙 본사와 연결하고자 합니다. 회사의 IT 관리자인 Alice는 네트워크를 구성하고 관리하는 일을 담당하고 있습니다.

어떤 위험이 있습니까**?**

현재 네트워크 설정에서는 각 브랜치 오피스와 본사 간의 여러 포인트 투 포인트 연결을 수동으로 구성해야 합니다. 이 접근 방식은 시간이 많이 걸리고 오류가 발생하기 쉬우며, 모든 위치 전반에 걸쳐 네트워크 설정에서 일관성을 유지하기가 어렵습니다. Alice는 설정 프로세스를 간소화하고 중앙 집중식 제어를 제공하는 솔루션이 필요했습니다.

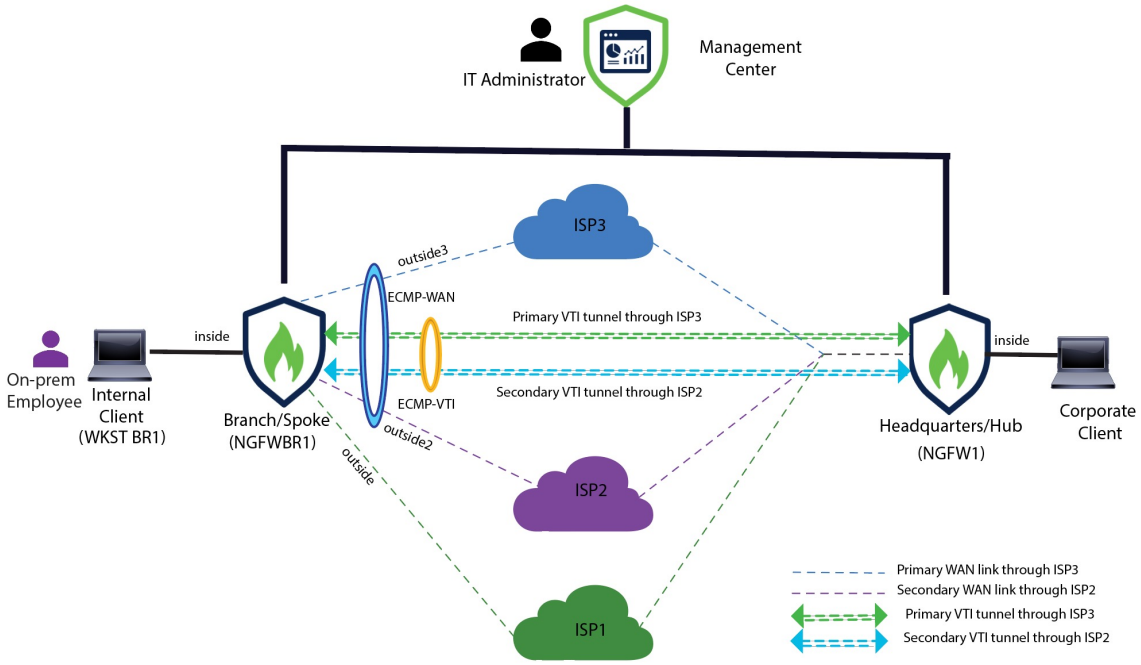
브랜치**(**스포크**)**와 본사**(**허브**)** 간의 경로 기반 **VPN**은 문제를 어떻게 해결합니까**?**

1. 중앙 집중식 구성: Alice는 DVTI 허브 앤 스포크 토폴로지를 구현하여 구성 및 관리를 허브에서 중앙 집중화합니다. 이렇게 하면 모든 위치에서 네트워크 설정이 간소화됩니다.
2. 동적 라우팅: Alice는 라우팅 정보 교환을 자동화하는 동적 라우팅 프로토콜(예: OSPF)을 설정합니다. 정적 경로의 수동 구성이 제거되어 네트워크 관리가 간소화됩니다.
3. 빠른 프로비저닝: Alice는 DVTI를 사용하여 스포크 라우터를 구성하고 허브와의 보안 터널을 설정하여 새 브랜치를 신속하게 프로비저닝할 수 있습니다. 이렇게 하면 프로비저닝 프로세스가 간소화되고 네트워크 확장성이 지원됩니다.

Alice는 DVTI를 구현함으로써 네트워크 구성을 간소화하고, 제어를 중앙 집중화하며, 일관성을 보장하고, 기업 네트워크에서 효율적인 프로비저닝 및 확장성을 지원합니다.

네트워크 토폴로지

이 허브 스포크 토폴로지에서 위협 방어 디바이스는 브랜치 위치에 구축됩니다. 아래 그림에서 내부 클라이언트 또는 브랜치 워크스테이션은 WKST BR 레이블로 표시되고 브랜치(스포크) 위협 방어는 NGFWBR1 레이블로 표시됩니다. 본사(허브)는 NGFW1로 레이블이 지정되고 기업 네트워크에 연결됩니다. NGFWBR1과 NGFW1 사이에 VPN 터널이 구성됩니다. ECMP 영역은 VPN 트래픽의 링크 이중화 및 로드 밸런싱을 위해 브랜치 노드의 기본 및 보조 정적 VTI 인터페이스에 구성됩니다.



모범 사례

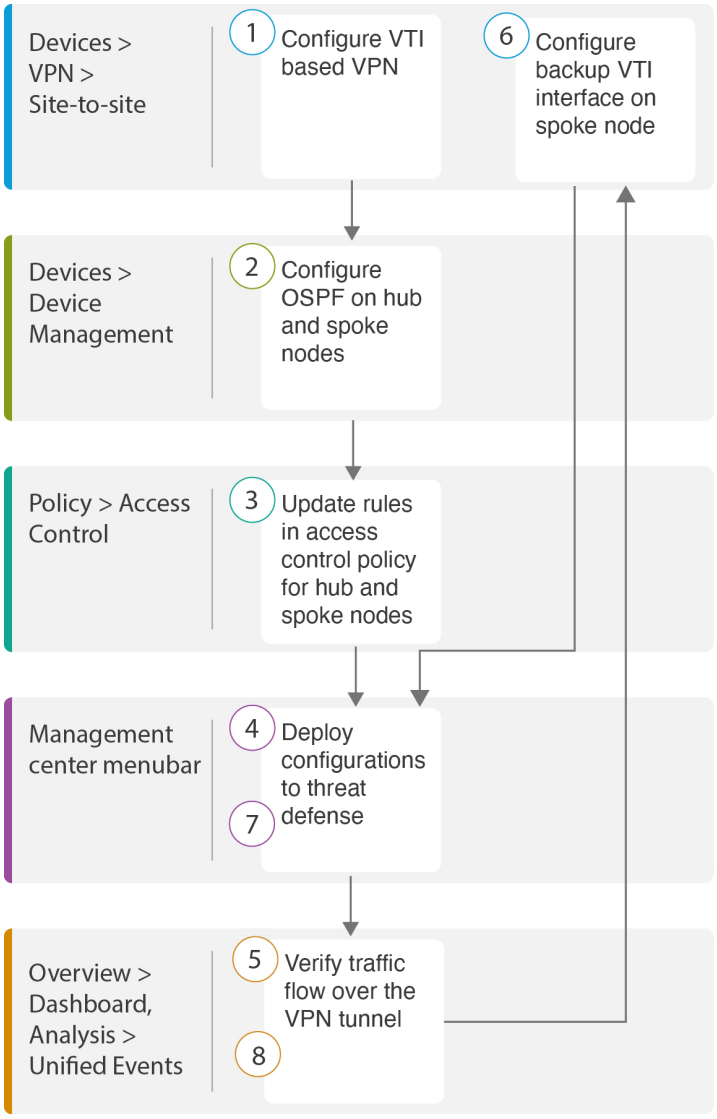
- Secure Firewall Threat Defense가 버전 6.7 이상에서 실행되는지 확인합니다.
- VTI는 라우팅 모드에서만 지원됩니다.
- 루프백 인터페이스에서 동적 인터페이스에 대한 IP 대여를 구성하는 것이 좋습니다.
- VTI를 통한 트래픽을 제어하려면 VTI 인터페이스에 액세스 규칙을 적용해야 합니다.
- VTI 트래픽의 로드 밸런싱을 위해 SVTI에 대한 ECMP 영역을 구성합니다.

사전 요구 사항

- 디바이스 관리자를 사용하여 위협 방어 초기 구성 완료
- 매니지드 디바이스에 라이선스 할당
- 인터넷 액세스용 경로를 추가합니다. 고정 경로 추가를 참조하십시오.
- Threat Defense NAT 구성
- 기본 액세스 제어 정책 만들기

경로 기반 VPN 구성을 위한 엔드 투 엔드 절차(허브 앤 스포크 토폴로지)

다음 순서도에는 Secure Firewall Management Center에서 허브 스포크 토폴로지에 대한 경로 기반 VPN 구성을 위한 워크플로우가 나와 있습니다.



단계	설명
1	VTI 기반 VPN을 구성합니다. 확인 • 라우트 기반 사이트 간 VPN 생성, 6 페이지 • 허브 노드에 대한 엔드포인트 구성, 7 페이지

단계	설명
	• 스포크 노드에 대한 엔드포인트 구성, 9 페이지
2	허브 앤 스포크 노드에서 OSPF를 구성합니다. 확인 • 허브 노드에서 OSPF 구성, 10 페이지 • 스포크 노드에서 OSPF 구성, 12 페이지
3	허브 및 스포크 노드에 대한 액세스 제어 정책에서 규칙을 업데이트합니다. 액세스 제어 정책 구성, 14 페이지의 내용을 참조하십시오.
4	구성을 위협 방어에 구축합니다. 컨피그레이션 구축, 17 페이지의 내용을 참조하십시오.
5	VPN 터널을 통한 트래픽 플로우를 확인합니다. VPN 터널을 통한 트래픽 흐름 확인, 17 페이지의 내용을 참조하십시오.
6	스포크 노드에서 백업 VTI를 구성합니다. 스포크 노드에서 백업 VTI 인터페이스 구성, 20 페이지의 내용을 참조하십시오.
7	구성을 위협 방어에 구축합니다. 컨피그레이션 구축, 17 페이지의 내용을 참조하십시오.
8	보조 터널의 트래픽 플로우를 확인합니다. 기본 및 보조 터널 확인, 23 페이지의 내용을 참조하십시오.

라우트 기반 사이트 간 VPN 생성

두 노드간에 라우트 기반 사이트 간 VPN을 구성할 수 있습니다. VTI 기반 VPN을 구성하려면 터널의 두 노드 모두에 가상 터널 인터페이스가 필요합니다.

매니지드 스포크의 경우 기본 VTI 인터페이스와 함께 백업 정적 VTI 인터페이스를 구성할 수 있습니다.

단계 **1** **Devices**(디바이스) > **VPN** > **Site To Site**(사이트 간)를 선택합니다.

단계 **2** **Topology Name**(토폴로지 이름) 필드에 이름을 **Corporate-VPN**으로 입력합니다.

단계 **3** 토폴로지 유형으로 **VTI(Route Based)**를 선택합니다.

단계 **4** 허브 노드에 대한 엔드포인트를 구성합니다. 허브 노드에 대한 엔드포인트 구성, 7 페이지의 내용을 참조하십시오.

단계 **5** 스포크 노드에 대한 엔드포인트를 구성합니다. 스포크 노드에 대한 엔드포인트 구성, 9 페이지의 내용을 참조하십시오.

단계 **6** **IKE**, **IPsec** 및 **Advanced**(고급) 탭에서는 기본 설정이 사용됩니다.

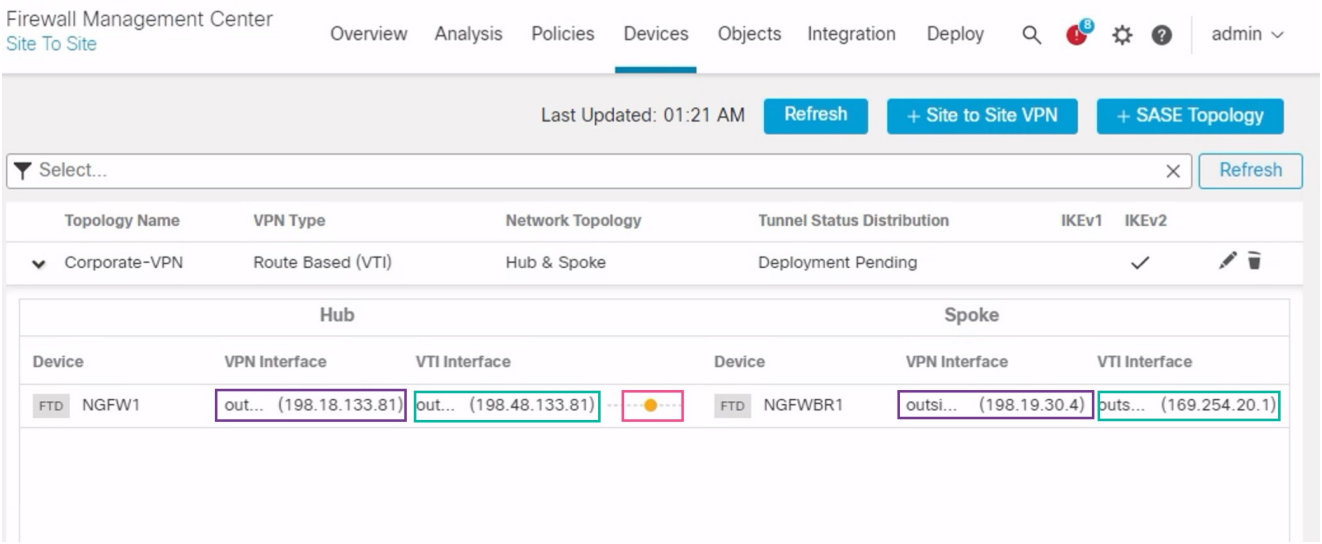
단계 **7** **Save**(저장)를 클릭합니다.

Corporate-VPN 토폴로지가 생성되었습니다.

단계 **8** **Devices(**디바이스**)** > **Site-to-site VPN(**사이트 간 **VPN)**으로 이동하여 사이트 간 VPN 목록 페이지에서 VPN 토폴로지를 볼 수 있습니다.

참고 생성한 VPN 토폴로지가 표시되지 않으면 **Refresh(**새로 고침**)**를 클릭합니다.

단계 **9** 토폴로지의 모든 터널을 보려면 **Corporate-VPN** 노드를 확장합니다. **NGFW1** 허브 및 물리적 소스 및 VTI 인터페이스의 세부 정보와 함께 **NGFWBR1** 스포크가 표시됩니다. 구성이 아직 구축되지 않았으므로 **Deployment Pending(**구축 보류 중**)**으로 표시되고 터널이 황색으로 표시됩니다.



다음에 수행할 작업

두 디바이스에서 VTI 인터페이스 및 VTI 터널을 구성한 후에는 다음을 구성해야 합니다.

- VTI 터널을 통해 디바이스 간에 VTI 트래픽을 라우팅하는 라우팅 프로토콜입니다. 허브 노드에서 OSPF 구성, 10 페이지 및 스포크 노드에서 OSPF 구성, 12 페이지를 참조하십시오.
- 암호화된 트래픽을 허용하는 액세스 제어 규칙입니다. 액세스 제어 정책 구성, 14 페이지의 내용을 참조하십시오.

허브 노드에 대한 엔드포인트 구성

터널 유형을 동적으로 지정하고 관련 매개변수를 구성하면 관리 센터는 동적 가상 템플릿을 생성합니다. 가상 템플릿은 각 VPN 세션에 고유한 가상 액세스 인터페이스를 동적으로 생성합니다.

단계 **1** **Hub Nodes(**허브 노드**)** 섹션에서 +를 클릭합니다. **Add Endpoint(**엔드포인트 추가**)** 대화 상자가 표시됩니다.

단계 **2** **Device(**디바이스**)** 드롭다운 목록에서 허브로 **NGFW1**를 선택합니다.

참고 소프트웨어 버전 7.3 이상에서 실행되는 디바이스여야 합니다.

단계 **3** **Dynamic Virtual Tunnel Interface(**동적 가상 터널 인터페이스**)** 드롭다운 목록 옆의 **+**를 클릭하여 새 동적 VTI를 추가합니다.

다음과 같은 기본 구성이 미리 채워진 **Add Virtual Tunnel Interface(Virtual Tunnel** 인터페이스 추가**)** 대화 상자가 나타납니다.

- **Tunnel Type(**터널 유형**)**은 **Dynamic(**동적**)**으로 자동 채워집니다.
- **Name(**이름**)**은*<tunnel_source interface logical name>*+ dynamic_vti +*<tunnel ID>*로 자동 채워집니다. 예를 들면 **outside_dynamic_vti_1**입니다.
- 기본적으로 **Enabled(**활성화됨**)** 확인란이 선택되어 있습니다.
- **Security Zone(**보안 영역**)** - 이 인터페이스의 보안 영역을 정의하려면 드롭다운 목록에서 **New(**새로 만들기**)**를 선택합니다. **New Security Zone(**새 보안 영역**)** 대화 상자에서 이름으로 **Tunnel_Zone**을 입력하고 **OK(**확인**)**를 클릭합니다. 이 터널 인터페이스의 보안 영역으로 **Tunnel_Zone**을 선택합니다**.**
- **Template ID(**템플릿 **ID)**는 DVTI 인터페이스의 고유 ID로 자동으로 채워집니다.
- **Tunnel Source(**터널 소스**)**는 DVTI의 소스인 물리적 인터페이스이며 기본적으로 자동으로 채워집니다. 이 활용 사례에서는 DVTI에 대해 명시적 터널 소스를 설정하지 않을 것입니다. 드롭다운 목록에서 **Select Interface(**인터페이스 선택**)**를 선택하여 선택을 취소합니다.
- **IPsec Tunnel Mode(IPsec** 터널 모드**)**는 기본적으로 IPv4로 설정됩니다.
- DVTI는 템플릿 인터페이스이므로 **IP** 주소는 고정 IP 주소일 수 없습니다. 루프백 인터페이스에서 동적 인터페이스에 대한 IP 대여를 구성하는 것이 좋습니다. 루프백 인터페이스를 추가하려면 **Burrow IP (IP unnumbered)(IP** 대여**(IP** 번호 없음**))** 드롭다운 목록 옆의 **+**를 클릭합니다. **Add Loopback Interface(**루프백 인터페이스 추가**)** 대화 상자에서 다음을 수행합니다.
  1. **General(**일반**)** 탭에서 **Name(**이름**)**을 **HUB_Tunnel_IP**로 입력하고 **Loopback ID**를 **1**로 입력합니다.
  2. **IPv4** 탭에 IP 주소를 **198.48.133.81/32**로 입력합니다.
  3. **OK(**확인**)**를 클릭하여 루프백 인터페이스를 저장합니다.

  대여 IP는 **Loopback 1(HUB_Tunnel_IP)**로 설정됩니다.

OK(확인**)**를 클릭하여 DVTI를 저장합니다. VTI가 성공적으로 생성되었음을 확인하는 메시지가 표시됩니다. **OK(**확인**)**를 클릭합니다.

동적 Virtual Tunnel Interface는 **outside_dynamic_vti_1(198.48.133.81)**로 설정됩니다.

단계 **4** **Tunnel Source(**터널 소스**)** 드롭다운 목록에서 **GigabitEthernet 0/0(outside)**을 선택합니다. 외부 인터페이스 (**198.18.133.81**)의 IP 주소가 다음 필드에 자동으로 입력됩니다.

단계 **5** 기본 설정을 확인하려면 **Advanced Settings(**고급 설정**)**를 확장합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

NGFW1이 허브 노드로 구성되었습니다.

스포크 노드에 대한 엔드포인트 구성

단계 **1** **Spoke Nodes(**스포크 노드**)** 섹션에서 **+**를 클릭합니다. **Add Endpoint(**엔드포인트 추가**)** 대화 상자가 표시됩니다.

단계 **2** **Device(**디바이스**)** 드롭다운 목록에서 허브로 **NGFWBR1**을 선택합니다.

참고 소프트웨어 버전 7.3 이상에서 실행되는 디바이스여야 합니다.

단계 **3** **Static Virtual Tunnel Interface(**정적 **Virtual Tunnel Interface)** 드롭다운 목록 옆의 **+**를 클릭하여 새 정적 VTI를 추가합니다.

다음과 같은 기본 구성이 미리 채워진 **Add Virtual Tunnel Interface(Virtual Tunnel** 인터페이스 추가**)** 대화 상자가 나타납니다.

- **Tunnel Type(**터널 유형**)**은 **Static(**정적**)**으로 자동 채워집니다.
- **Name(**이름**)**은 *<tunnel_source interface logical name>*+ static_vti +*<tunnel ID>*로 자동 채워집니다. 예: **outside_static_vti_1** .
- 기본적으로 **Enabled(**활성화됨**)** 확인란이 선택되어 있습니다.
- Security Zone(보안 영역) 드롭다운 목록에서 **Tunnel_Zone**을 선택합니다.
- **Tunnel ID(**터널 **ID)**는 값이 1로 자동 채워집니다.
- **Tunnel Source(**터널 소스**)** 드롭다운 목록에서 **GigabitEthernet0/4 (outside3)**를 선택합니다. 외부 3 인터페이스의 IP 주소를 옆에 있는 드롭다운 목록에서 **198.19.30.4**로 선택합니다.
- **IPsec Tunnel Mode(IPsec** 터널 모드**)**는 기본적으로 IPv4로 설정됩니다.
- **IP address(IP** 주소**)**는 고정 IP 주소 또는 대여 IP일 수 있습니다. 루프백 인터페이스에서 정적 인터페이스에 대한 IP 대여를 구성하는 것이 좋습니다. 루프백 인터페이스를 추가하려면 **Burrow IP (IP unnumbered)(IP** 대여 **(IP** 번호 없음**))** 드롭다운 목록 옆의 **+**를 클릭합니다. **Add Loopback Interface(**루프백 인터페이스 추가**)** 대화 상자에서 다음을 수행합니다.
  1. **General(**일반**)** 탭에서 **Name(**이름**)**을 **Spoke_Tunnel_IP**로 입력하고 **Loopback ID**를 **1**로 입력합니다.
  2. **IPv4** 탭에 IP 주소를 **169.254.20.1/32**로 입력합니다.
  3. **OK(**확인**)**를 클릭하여 루프백 인터페이스를 저장합니다.

  대여 IP는 **Loopback 1(Spoke_Tunnel_IP)**로 설정됩니다.

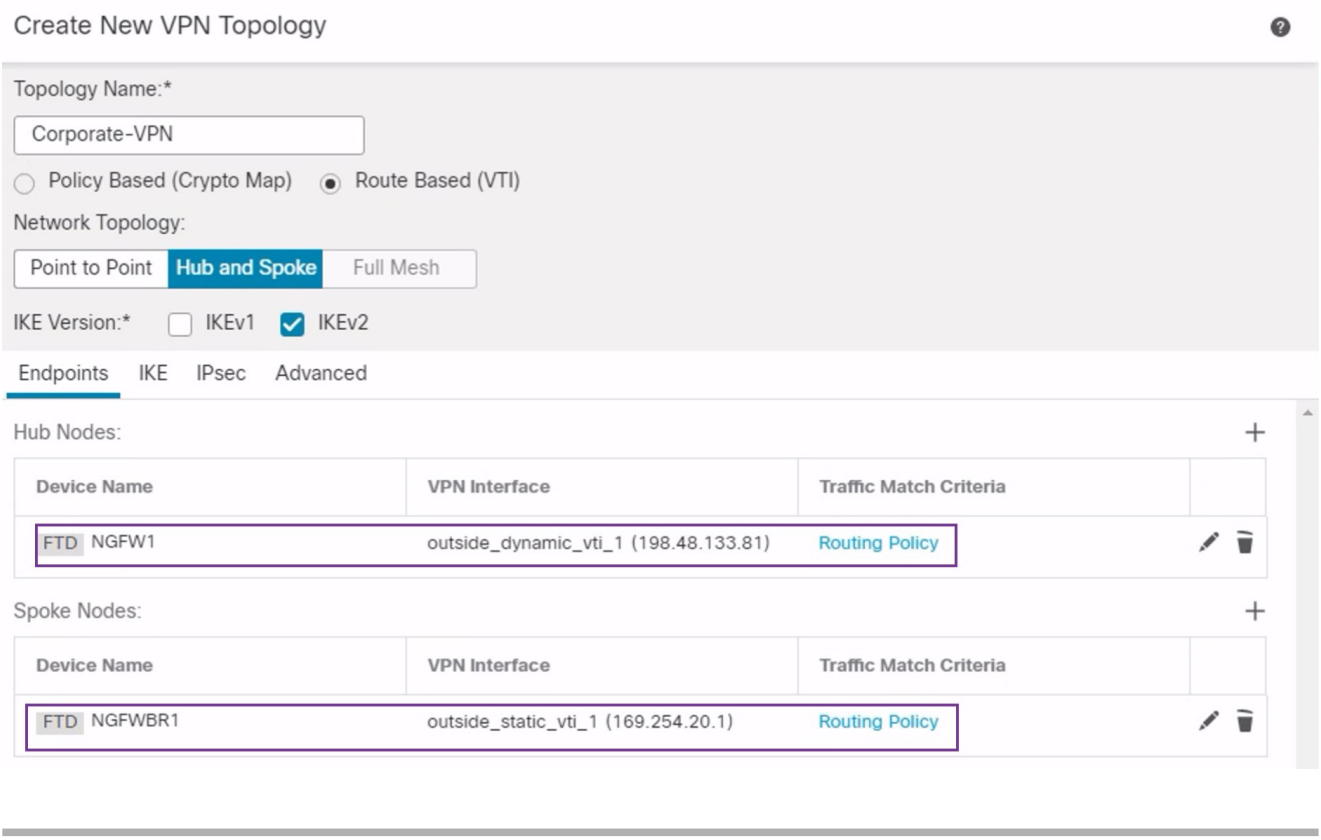
OK(확인**)**를 클릭하여 SVTI를 저장합니다. VTI가 성공적으로 생성되었음을 확인하는 메시지가 표시됩니다. **OK(**확인**)**를 클릭합니다.

정적 Virtual Tunnel Interface는 **outside_static_vti_1(169.254.20.1)**로 설정됩니다.

단계 4 기본 설정을 확인하려면 **Advanced Settings(**고급 설정**)**를 확장합니다. 두 확인란을 모두 선택해야 합니다.

단계 5 **OK(**확인**)**를 클릭합니다.

NGFWBR1이 스포크 노드로 구성되었습니다.



허브 노드에서 OSPF 구성

OSPF는 트래픽이 VPN 터널을 통해 전송될 수 있도록 허브 및 스포크 디바이스 사이에 구성됩니다. 참조에서 정적 라우팅은 스포크-허브 터널이 설정되는 언더레이이며, OSPF는 오버레이로 간주됩니다.

단계 1 허브 노드를 편집하려면 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 NGFW1 노드의 **Edit(**수정**)** (✎) 아이콘을 클릭합니다.

단계 2 **Interfaces(**인터페이스**)** 탭에서 이전에 생성되었으며 DVTI 인터페이스의 IP 주소 역할을 하는 **Loopback1** 인터페이스를 확인합니다.

단계 3 **Routing(**라우팅**)**을 클릭합니다.

단계 4 왼쪽 패널에서 **OSPF**를 클릭합니다.

단계 5 OSPF 인스턴스를 활성화하려면 **Process 1(**프로세스 **1)** 확인란을 선택합니다.

단계 6 **Interface(**인터페이스**)** 탭을 클릭합니다.

단계 **7** **+Add(**추가**)**를 클릭합니다. **Add Interface(**인터페이스 추가**)** 대화 상자가 나타납니다. 다음 필드를 수정합니다.

- **Interface(**인터페이스**)** - 드롭다운 목록에서 **outside_dynamic_vti_1** DVTI 인터페이스를 선택합니다.
- **Point-to-Point(**포인트-투-포인트**)** - VPN 터널을 통해 OSPF 경로를 전하려면 이 확인란을 선택합니다.

  나머지 필드에서는 기본값을 사용합니다.
- **OK(**확인**)**를 클릭합니다.

outside_dynamic_vti_1의 행이 **Interface(**인터페이스**)** 탭에 추가됩니다.

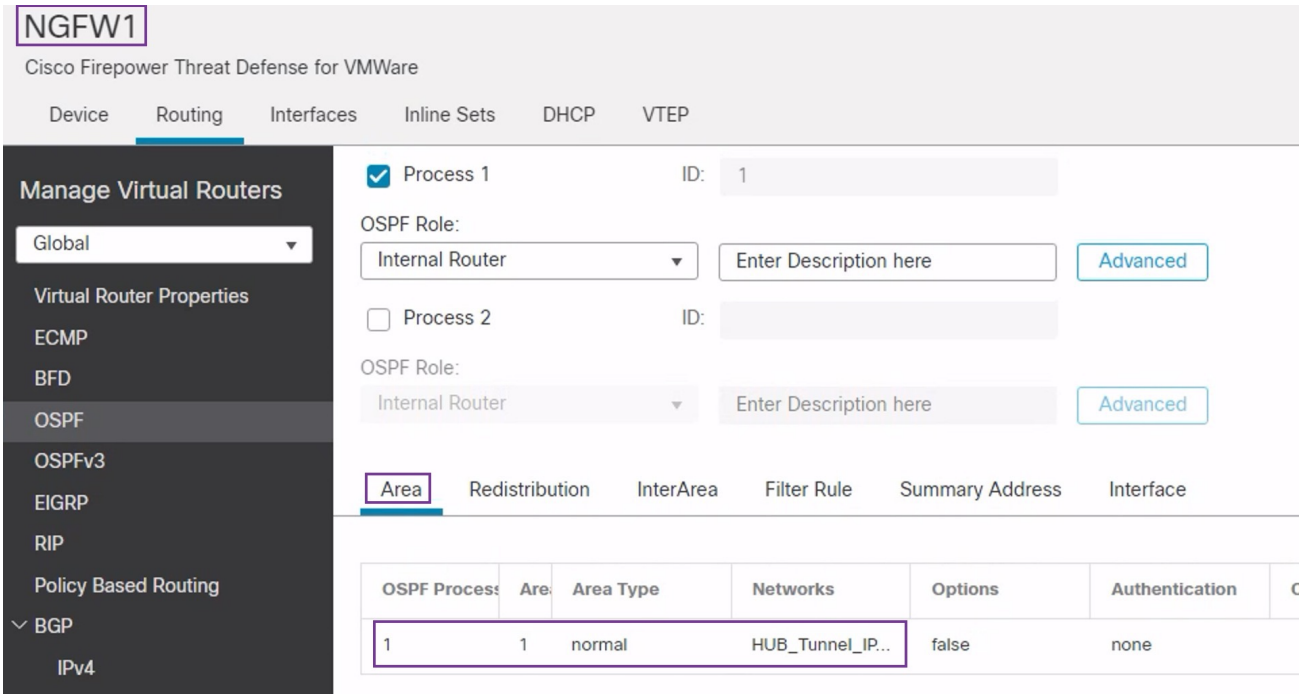
단계 **8** **Area(**영역**)** 탭을 클릭합니다.

단계 **9** **+Add(**추가**)**를 클릭합니다. **Add Area(**영역 추가**)** 대화 상자가 나타납니다. 다음 필드를 수정합니다.

- **OSPF Process(OSPF** 프로세스**)** - 프로세스 ID를 1로 선택합니다.
- **Area ID(**영역 **ID)** - 값이 1인지 확인합니다.

  나머지 필드에서는 기본값을 사용합니다.
- **Available Network(**사용 가능한 네트워크**)** - 터널을 통해 광고할 네트워크를 추가하려면 다음을 수행합니다.
  - 네트워크 개체를 새로 추가하려면 ＋을 클릭합니다. 다음 세부사항을 입력합니다.
    - **Name(**이름**)** - 이름을 **HUB_Tunnel_IP**로 입력합니다.
    - **Network(**네트워크**)** - **Host(**호스트**)** 옵션을 선택하고 호스트 IP를 **198.48.133.81**로 입력합니다.
    - **Save(**저장**)**를 클릭합니다.
  - **Available Network(**사용 가능한 네트워크**)** 필드의 검색 영역에 **HUB**를 입력합니다. 새로 추가된 네트워크 개체(**HUB_Tunnel_IP**)가 나열됩니다. 개체를 선택하고 **Add(**추가**)**를 클릭하여 **Selected Network(**선택한 네트워크**)** 목록에 추가합니다.
  - **Available Network(**사용 가능한 네트워크**)** 필드의 검색 영역에 **Corporate**를 입력합니다. **Corporate_LAN** 네트워크 개체가 나열됩니다. 개체를 선택하고 **Add(**추가**)**를 클릭하여 **Selected Network(**선택한 네트워크**)** 목록에 추가합니다.
- **OK(**확인**)**를 클릭합니다.

Area(영역**)** 탭에 행이 추가됩니다.



단계 **10** 허브 노드에 대한 OSPF 구성을 저장하려면 **Save(**저장**)**를 클릭합니다.

스포크 노드에서 **OSPF** 구성

단계 **1** 스포크 노드를 수정하려면 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 NGFWBR1 노드의 **Edit(**수정**)** (✎) 아이콘을 클릭합니다.

단계 **2** **Interface(**인터페이스**)** 탭에서:

- 스포크 구성에서 이전에 생성한 **Tunnel1** 인터페이스의 세부 정보를 확인합니다.
- Tunnel1의 이전에 생성되어 IP 주소 역할을 하는 **Loopback1** 인터페이스의 세부 정보를 확인합니다.

단계 **3** **Routing(**라우팅**)**을 클릭합니다.

단계 **4** 왼쪽 패널에서 **OSPF**를 클릭합니다.

단계 **5** OSPF 인스턴스를 활성화하려면 **Process 1(**프로세스 **1)** 확인란을 선택합니다.

단계 **6** **Area(**영역**)** 탭을 클릭합니다.

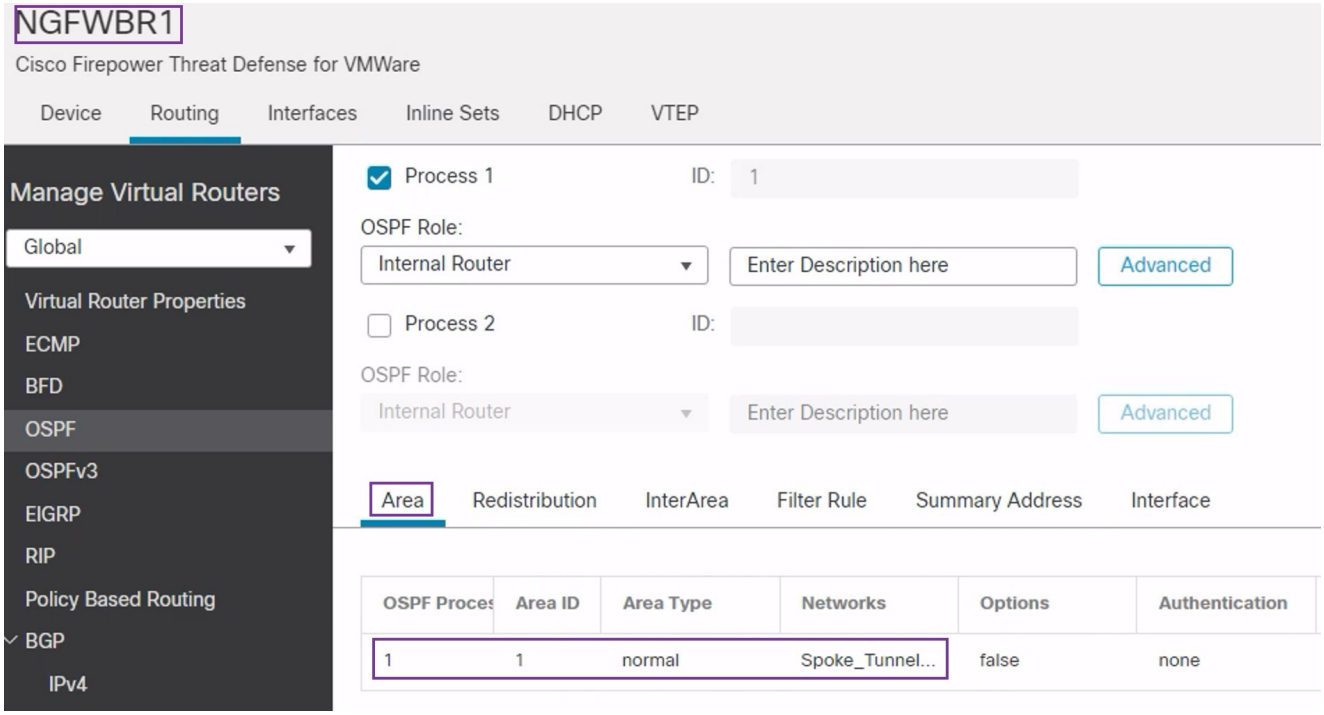
단계 **7** **+Add(**추가**)**를 클릭합니다. **Add Area(**영역 추가**)** 대화 상자가 나타납니다. 다음 필드를 수정합니다.

- **OSPF Process(OSPF** 프로세스**)** - 프로세스 ID를 1로 선택합니다.
- **Area ID(**영역 **ID)** - 값이 1인지 확인합니다.

  나머지 필드에서는 기본값을 사용합니다.

- **Available Network(**사용 가능한 네트워크**)** - 터널을 통해 광고할 네트워크를 추가하려면 다음을 수행합니다.
  - 네트워크 개체를 새로 추가하려면 ＋을 클릭합니다. 다음 세부사항을 입력합니다.
    - **Name(**이름**)** - 이름을 **Spoke_Tunnel_IP**로 입력합니다.
    - **Network(**네트워크**)** - **Host(**호스트**)** 옵션을 선택하고 호스트 IP를 **169.254.20.1**로 입력합니다.
    - **Save(**저장**)**를 클릭합니다.
  - **Available Network(**사용 가능한 네트워크**)** 필드의 검색 영역에 **Spoke**를 입력합니다. 새로 추가된 네트워크 개체(**Spoke_Tunnel_I**)가 나열됩니다. 개체를 선택하고 **Add(**추가**)**를 클릭하여 **Selected Network(**선택한 네트워크**)** 목록에 추가합니다.
  - **Available Network(**사용 가능한 네트워크**)** 필드의 검색 영역에 **Branch**를 입력합니다. **Branch_LAN** 네트워크 개체가 나열됩니다. 개체를 선택하고 **Add(**추가**)**를 클릭하여 **Selected Network(**선택한 네트워크**)** 목록에 추가합니다.
- **OK(**확인**)**를 클릭합니다.

Area(영역**)** 탭에 행이 추가됩니다.



단계 **8** 스포크 노드에 대한 OSPF 구성을 저장하려면 **Save(**저장**)**를 클릭합니다.

액세스 제어 정책 구성

계속 진행하기 전에 **NGFW1** 및 **NGFWBR1** 노드의 VTI 인터페이스가 **Tunnel_Zone**으로 레이블이 지정된 새 영역에 연결되어 있는지 확인합니다.

Policies(정책) > Access Control(액세스 제어)로 이동하여 액세스 제어 정책을 검토합니다. 터널을 오가는 VPN 트래픽을 허용하려면 허브 및 스포크 모두에 대해 다음 액세스 제어 정책을 업데이트해야 합니다.

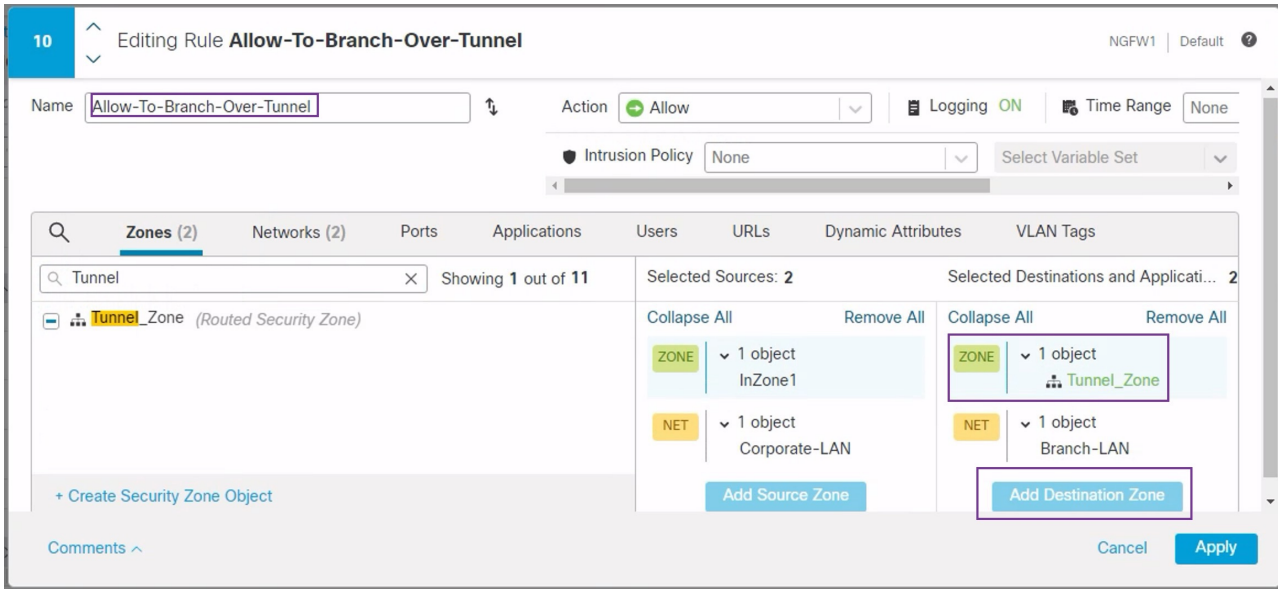
- **NGFW1** - 허브 노드(NGFW1)에 대한 액세스 제어 정책
- 브랜치 액세스 제어 - 스포크 노드(NGFWBR1)에 대한 액세스 제어 정책

단계 **1** 허브 노드(NGFW1) AC 정책을 편집하려면 **Edit(수정)** (✎) 아이콘을 클릭합니다.

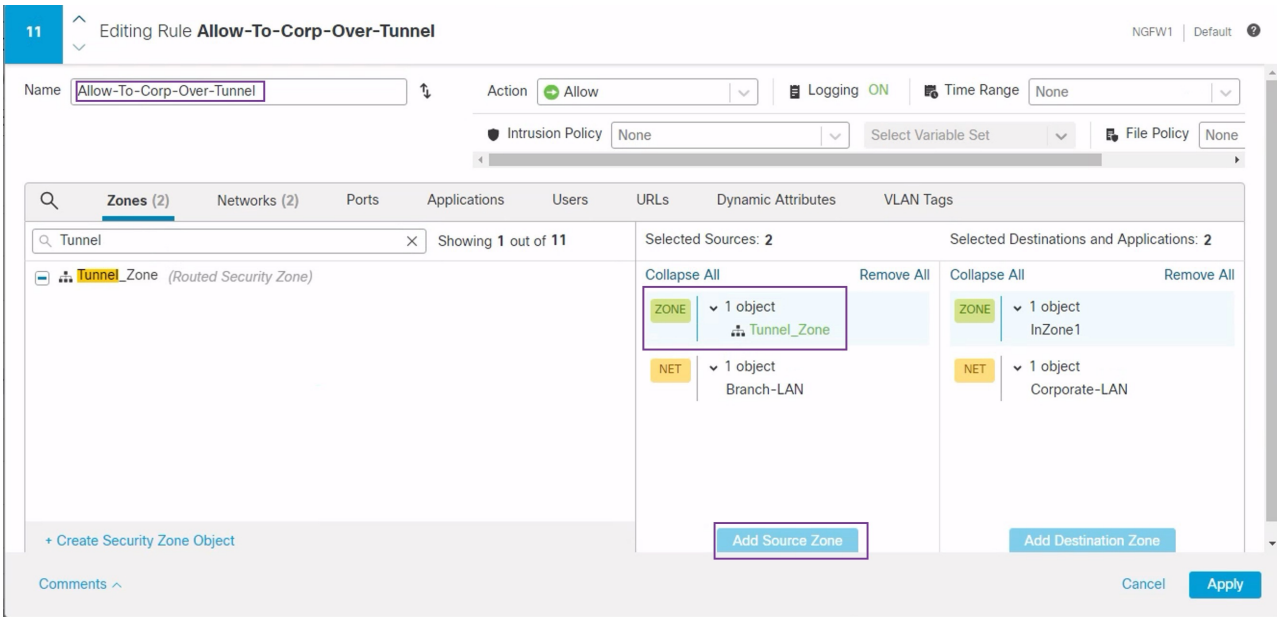
이 활용 사례를 위해 수정해야 하는 기존 규칙은 다음과 같습니다.

- **Allow-To-Branch-Over-Tunnel**
- **Allow-To-Corp-Over-Tunnel**

1. **Allow-To-Branch-Over-Tunnel** 정책을 수정하려면 **Edit(수정)** (✎) 아이콘을 클릭합니다.
2. **Zones(영역)** 탭에서 **Tunnel_Zone**을 검색하여 선택한 다음 **Add Destination Zone(대상 영역 추가)**을 클릭합니다.



3. **Apply(적용)**를 클릭하여 규칙을 저장합니다.
4. **Allow-To-Corp-Over-Tunnel** 정책을 편집하려면 **Edit(수정)** (✎) 아이콘을 클릭합니다.
5. **Zones(영역)** 탭에서 **Tunnel_Zone**을 검색하여 선택한 다음 **Add Source Zone(소스 영역 추가)**을 클릭합니다.



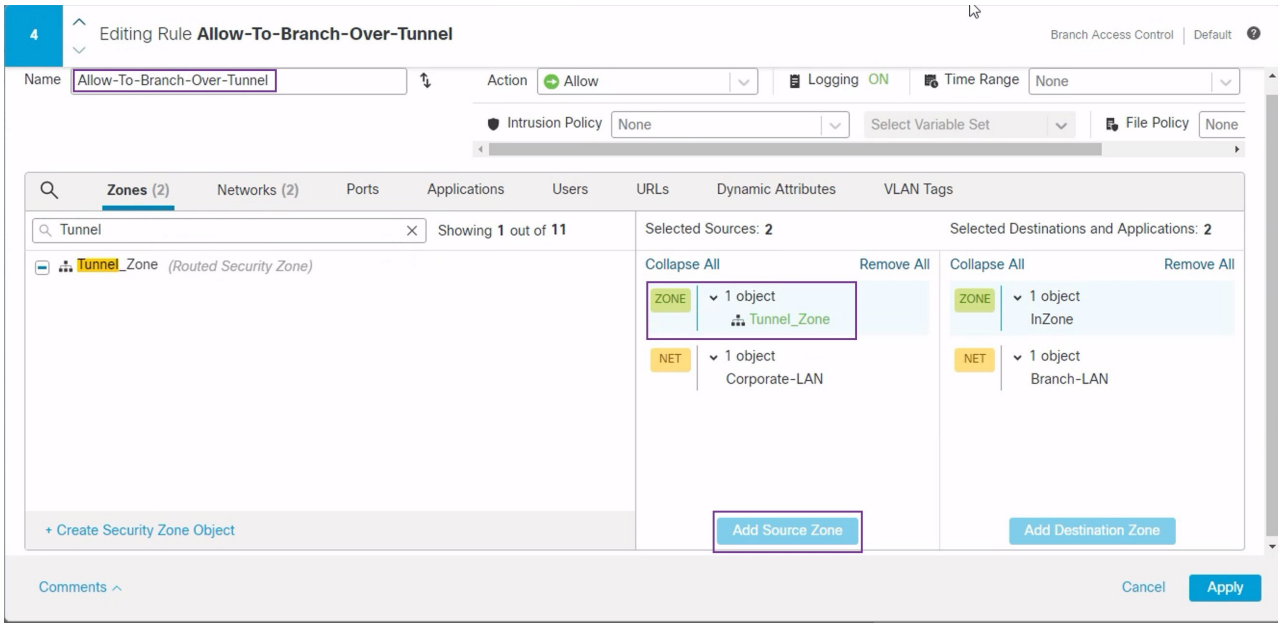
6. **Apply(**적용**)**를 클릭하여 규칙을 저장합니다.
7. NGFW1에서 업데이트된 규칙을 확인합니다.
8. **Save(**저장**)**를 클릭하여 AC 정책을 저장합니다.
9. **Return to Access Conrol Policy Management(**액세스 제어 정책 관리로 돌아가기**)**를 클릭하여 정책 페이지로 돌아갑니다.

단계 **2** 스포크 노드(NGFWBR1) AC 정책을 수정하려면 **Edit(**수정**)** (✎) 아이콘을 클릭합니다.

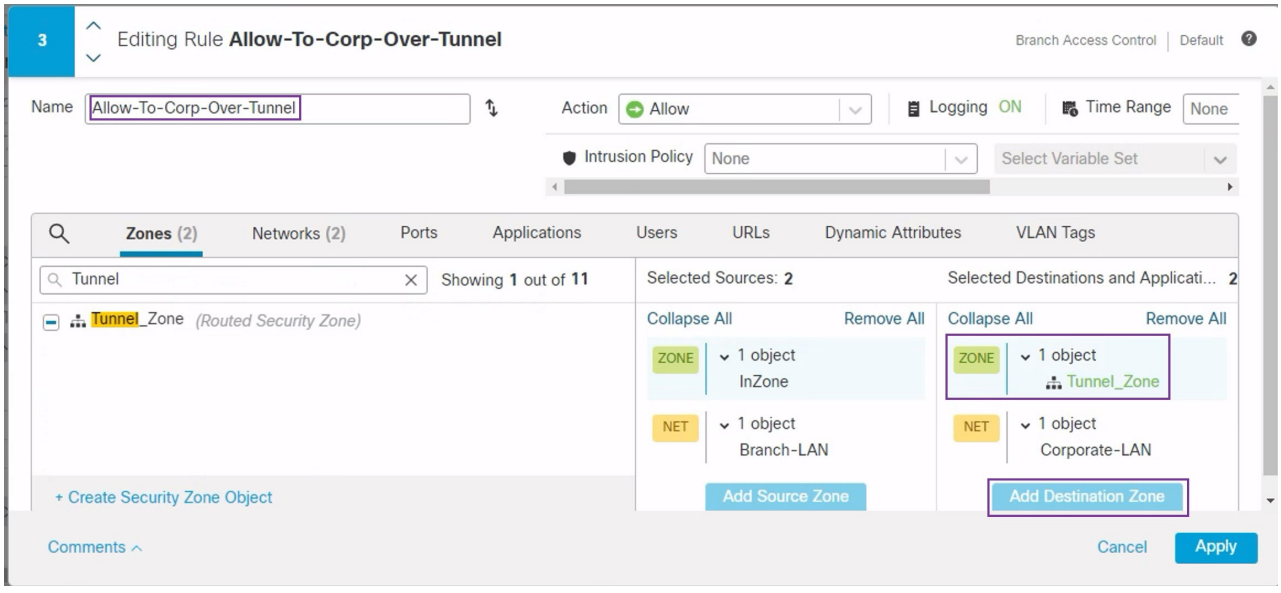
이 예시에서 수정해야 하는 규칙은 다음과 같습니다.

- **Allow-To-Branch-Over-Tunnel**
- **Allow-To-Corp-Over-Tunnel**

1. **Allow-To-Branch-Over-Tunnel** 정책을 수정하려면 **Edit(**수정**)** (✎) 아이콘을 클릭합니다.
2. **Zones(**영역**)** 탭에서 **Tunnel_Zone**을 검색하여 선택한 다음 **Add Soce Zone(**소스 영역 추가**)**을 클릭합니다.



3. **Apply(**적용**)**를 클릭하여 규칙을 저장합니다.
4. **Allow-To-Corp-Over-Tunnel** 정책을 편집하려면 **Edit(**수정**)** (✎) 아이콘을 클릭합니다.
5. **Zones(**영역**)** 탭에서 **Tunnel_Zone**을 검색하여 선택한 다음 **Add Destination Zone(**대상 영역 추가**)**을 클릭합니다.



6. **Apply(**적용**)**를 클릭하여 규칙을 저장합니다.
7. NGFWBR1에서 업데이트된 규칙을 확인합니다.

8. **Save(**저장**)**를 클릭하여 AC 정책을 저장합니다.

컨피그레이션 구축

모든 구성을 완료한 후 매니지드 디바이스에 구축합니다.

단계 **1** 관리 센터 메뉴 바에서 **Deploy(**구축**)**를 클릭합니다. 그러면 구축 준비가 완료된 디바이스의 목록이 표시됩니다.

단계 **2** 구성 변경 사항을 구축하려는 NGFWBR1 및 NGFW1 옆의 확인란을 선택합니다.

단계 **3** **Deploy(**구축**)**를 클릭합니다. Deploy(구축) 대화 상자에서 구축이 Completed(완료)로 표시될 때까지 기다립니다.

단계 **4** 구축할 변경 사항에서 오류나 경고를 식별하면 시스템은 **Validation Messages(**검증 메시지**)** 또는 **Validation Warnings(**검증 경고**)** 창에 이를 표시합니다. 전체 세부 정보를 보려면 Validation Errors(검증 오류) 또는 Validation Warnings(검증 경고) 링크를 클릭합니다.

다음 옵션을 이용할 수 있습니다.

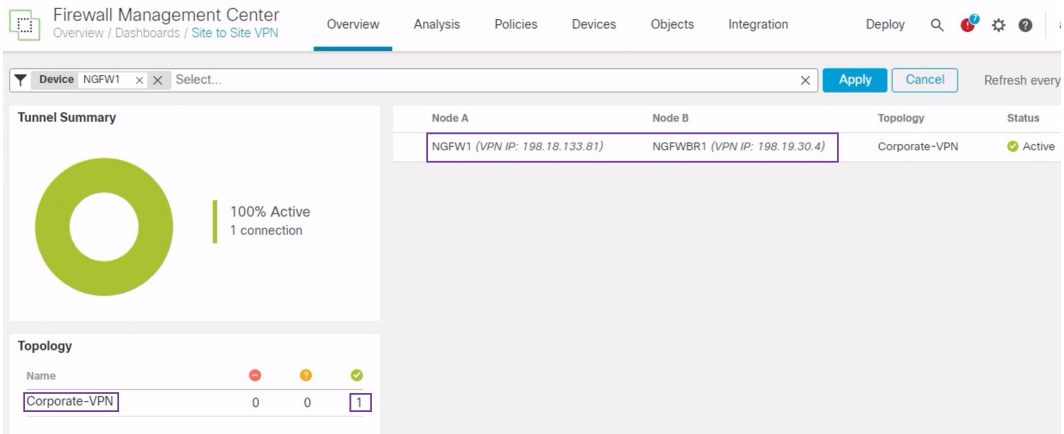
- Proceed with Deploy(구축 계속) - 경고 조건을 해결하지 않고 구축을 계속합니다. 오류가 식별되는 경우 계속 진행할 수 없습니다.
- Close(닫기) -구축하지 않고 종료합니다. 오류 및 경고 조건을 해결하고 컨피그레이션을 재구축합니다.

VPN 터널을 통한 트래픽 흐름 확인

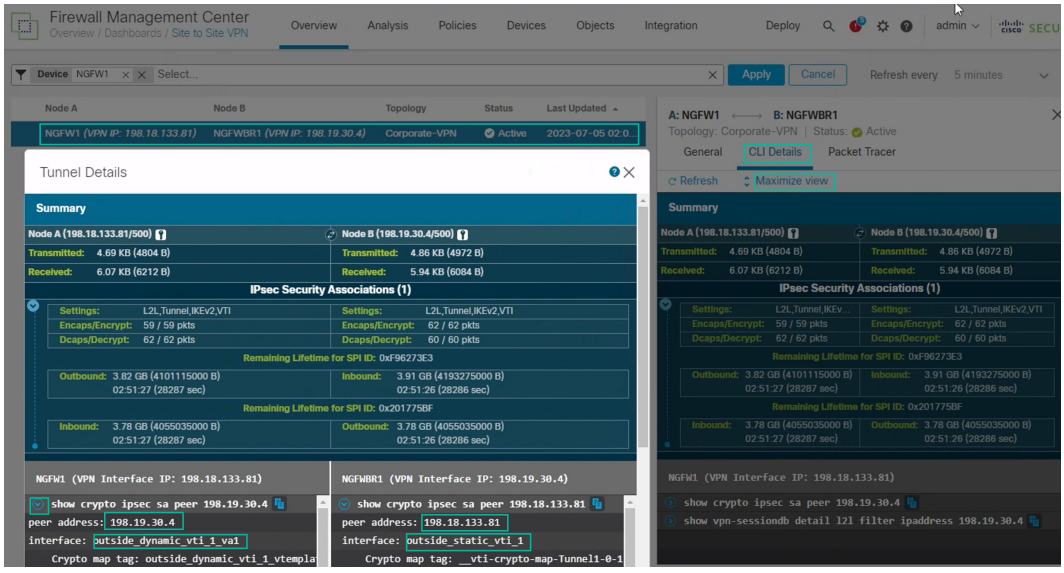
VPN 터널에 대해 다음 확인을 수행합니다.

- 사이트 간 **VPN** 대시보드의 터널 상태 확인

1. VPN 터널이 작동 중이며 녹색인지 확인하려면 **Overview(**개요**)** > **Dashboards(**대시보드**)** > **Site-to-site VPN(**사이트 간 **VPN)**을 선택합니다.



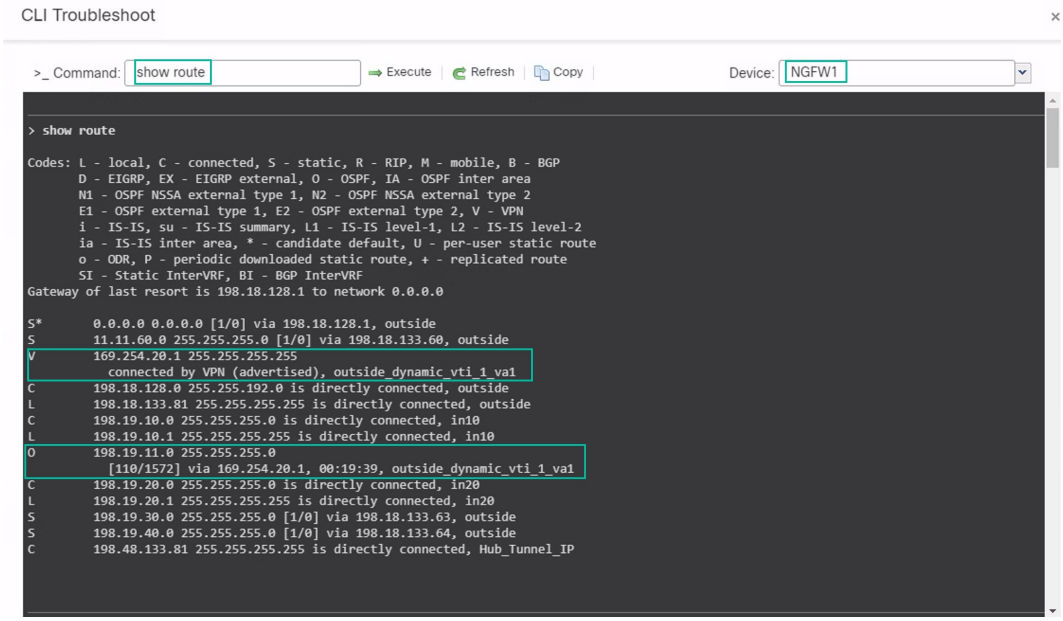
2. NGFW1 위에 마우스 커서를 올려 놓습니다. NGFW1 옆에 **View Full Information(**전체 정보 보기**)** 아이콘이 표시됩니다.
3. **View Full Information(**전체 정보 보기**)** 아이콘을 클릭합니다. 터널 세부 정보 및 추가 작업이 있는 측면 창이 나타납니다.
4. 측면 창에서 **CLI Details(CLI** 세부 정보**)** 탭을 클릭합니다.
5. IPSec 보안 연결의 상세정보가 포함된 최대화된 대화 상자를 표시하려면 **Maximumize View(**보기 최대화**)**를 클릭합니다.
6. 대화 상자의 하단에서 show 명령에 대한 CLI를 확장하여 디바이스의 VTI 인터페이스를 볼 수 있습니다.



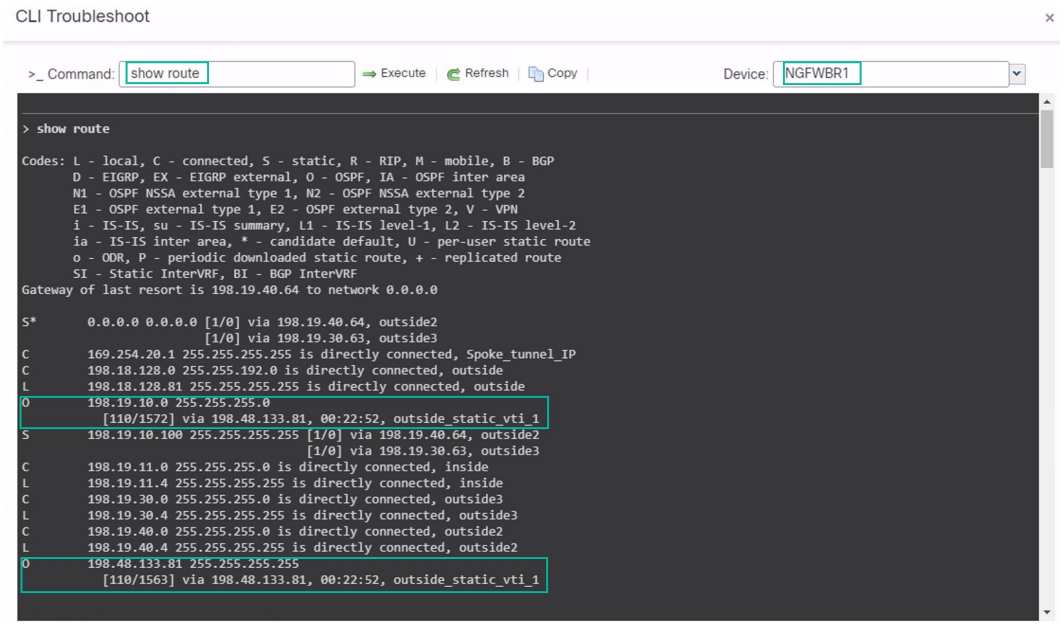
7. **Close(**닫기**)**를 클릭하여 Tunnel Details(터널 상세정보) 창을 종료합니다.

- 허브 및 브랜치 노드에서 라우팅 확인 - **NGFW1** 및 **NGFWBR1** 노드에서 OSPF 경로가 올바르게 학습되었는지 확인합니다.

1. **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.
2. NGFW1을 편집하려면 **Edit(**수정**)** (✎) 아이콘을 클릭합니다.
3. **Device(**디바이스**)** 탭을 클릭합니다.
4. **General(**일반**)** 카드에서 **CLI** 버튼을 클릭합니다. **CLI Troubleshoot(CLI** 문제 해결**)** 창이 나타납니다.
5. **Command(**명령**)** 필드에 **show route**를 입력하고 **Execute(**실행**)**를 클릭합니다.
6. 아래 그림에 표시된 것과 같이 NGFW1 노드에서 경로를 검토하고 스포크의 VTI IP(169.254.20.1)에 대한 VPN 경로와 브랜치_LAN에 대한 OSPF 학습 경로(198.19.11.0/24)를 확인합니다.

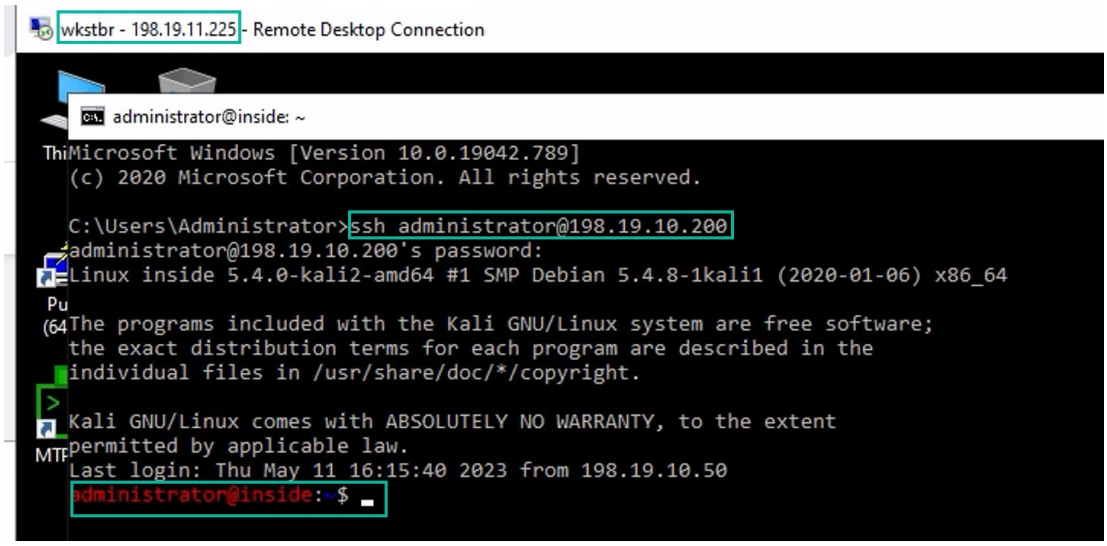


7. NGFWBR1 노드에 대해 2~5단계를 반복합니다.
8. NGFWBR1 노드의 경로를 검토합니다. 아래 그림에 표시된 것과 같이 허브의 VTI IP(198.48.133.81) 및 Corporate_LAN(198.19.10.0/24)에 대해 학습된 OSPF 경로를 확인합니다.



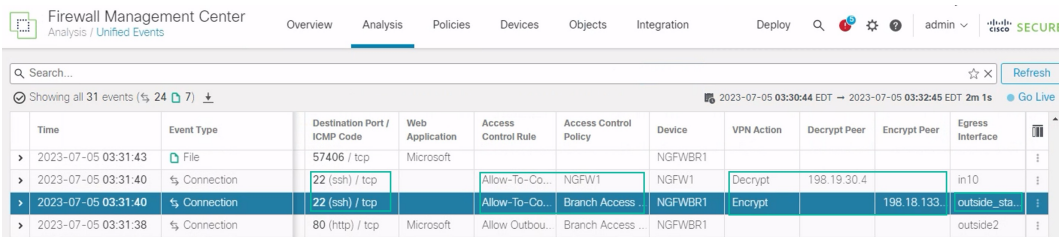
- 스포크 및 허브 노드 뒤의 보호되는 네트워크 간의 트래픽 확인

  WKST BR 워크스테이션(198.19.11.225)에 로그인하고 NGFW1 뒤의 호스트(198.19.10.200)에 SSH를 연결합니다. 호스트에 SSH로 성공적으로 연결할 수 있는지 확인합니다.



- 통합 이벤트를 사용하여 브랜치 및 스포크 노드 간 연결 확인

1. **Analysis(**분석**) > Unified Events(**통합 이벤트**)**를 선택합니다.
2. 열 선택기를 사용하여 **VPN Action, Encrypt Peer, Decrypt Peer(VPN** 작업**,** 피어 암호화**,** 피어 암호 해독**)** 및 **Egress Interface(**이그레스 인터페이스**)** 열을 추가합니다.
3. 아래 그림에 표시된 것과 같이 열, 대상 포트**/ICMP** 코드**,** 액세스 제어 규칙**,** 액세스 제어 정책 및 디바이스와 함께 새 열의 순서를 변경하고 크기를 조정합니다.



4. **WKST BR**에서 회사 호스트로의 SSH 연결과 관련된 이벤트를 보려면 **Destination Port/ICMP Code(**대상 포트**/ICMP** 코드**)** 열에서 **22(ssh/tcp)**가 있는 행을 선택합니다. 위의 그림에 나와 있는 것처럼 **outside_static_vti_1** 인터페이스를 통해 **NGFWBR1**의 **Encrypt(**암호화**)** 작업을 수행한 다음 **NGFW1**에서 **Decrypt(**암호 해독**)** 작업이 수행됩니다.

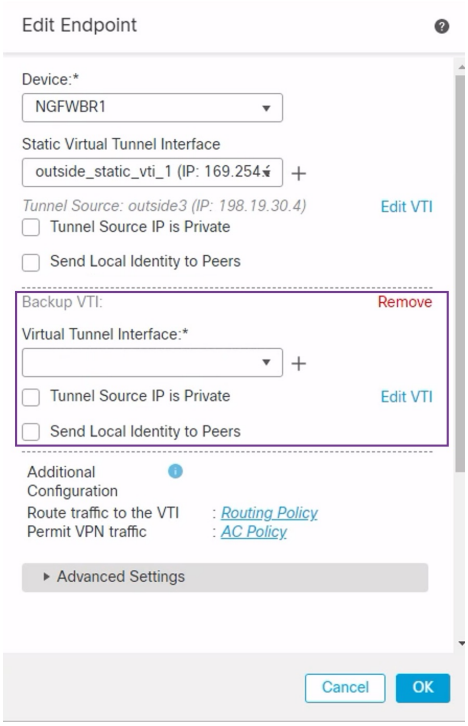
스포크 노드에서 백업 **VTI** 인터페이스 구성

Secure Firewall Threat Defense는 경로 기반(VTI) VPN에 대한 백업 터널 구성을 지원합니다. 기본 VTI가 트래픽을 라우팅할 수 없는 경우 VPN의 트래픽은 백업 VTI를 통해 터널링됩니다.

단계 **1** **Devices(**디바이스**)** > **Site-to-site VPN(**사이트 간 **VPN)**을 선택하여 구성된 기업-VPN VPN 토폴로지를 확인하고 **Edit(**수정**)** (✎) 아이콘을 클릭합니다. Edit VPN Topology(VPN 토폴로지 편집) 창이 나타납니다.

단계 **2** Spoke Nodes(스포크 노드) 섹션에서 **NGFWBR1** 노드의 **Edit(**수정**)** (✎) 아이콘을 클릭합니다. **Edit Endpoint(**엔드포인트 편집**)** 대화 상자가 나타납니다.

단계 **3** 보조 VTI 터널을 추가하려면 **Add Backup VTI(**백업 **VTI** 추가**)** 링크를 클릭합니다. 링크에 Backup VTI(백업 VTI) 섹션이 표시됩니다.



단계 **4** **Virtual Tunnel Interface** 드롭다운 목록 옆의 **+**를 클릭하여 새 VTI를 추가합니다.

다음과 같은 기본 구성이 미리 채워진 **Add Virtual Tunnel Interface(Virtual Tunnel** 인터페이스 추가**)** 대화 상자가 나타납니다.

- **Tunnel Type(**터널 유형**)**은 **Static(**정적**)**으로 자동 채워집니다.
- **Name(**이름**)**은 *<tunnel_source interface logical name>*+ static_vti +*<tunnel ID>*로 자동 채워집니다. 예: **outside_static_vti_2** .
- 기본적으로 **Enabled(**활성화됨**)** 확인란이 선택되어 있습니다.
- Security Zone(보안 영역) 드롭다운 목록에서 **Tunnel_Zone**을 선택합니다.
- **Tunnel ID(**터널 **ID)**는 값이 2로 자동 채워집니다.
- **Tunnel Source(**터널 소스**)** 드롭다운 목록에서 **GigabitEthernet0/3 (outside2)**를 선택합니다. 외부 3 인터페이스의 IP 주소를 옆에 있는 드롭다운 목록에서 **198.19.40.4**로 선택합니다.
- **IPsec Tunnel Mode(IPsec** 터널 모드**)**는 기본적으로 IPv4로 설정됩니다.

- **IP address(IP** 주소**)**는 고정 IP 주소 또는 대여 IP일 수 있습니다. 루프백 인터페이스에서 정적 인터페이스에 대한 IP 대여를 구성하는 것이 좋습니다. 루프백 인터페이스를 추가하려면 드롭다운 목록에서 **Loopback 1(Spoke_Tunnel_IP)**을 클릭합니다.

OK(확인**)**를 클릭하여 VTI를 저장합니다. VTI가 성공적으로 생성되었음을 확인하는 메시지가 표시됩니다. **OK(**확인**)**를 클릭합니다.

백업 VTI 인터페이스는 **outside_static_vti_2(169.254.20.1)**로 설정됩니다.

단계 **5** **OK(**확인**)**를 클릭하여 스포크 구성을 저장합니다.

단계 **6** **Save(**저장**)**를 클릭하여 VPN 토폴로지를 저장합니다.

기본 및 보조 VTI 인터페이스에 대한 ECMP 영역 구성

링크 이중화 및 VPN 트래픽 로드 밸런싱을 위해 브랜치 노드의 기본 및 보조 정적 VTI 인터페이스에서 ECMP를 구성합니다.

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 위협 방어 디바이스(**NGFWBR1**)를 편집합니다.

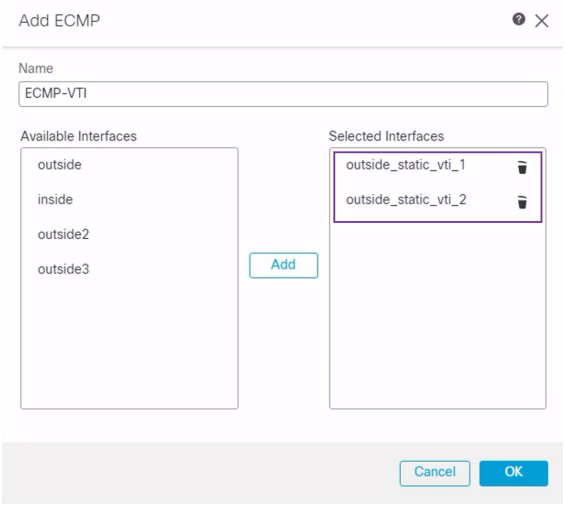
단계 **2** NGFWBR1의 인터페이스 보기에서 **Routing(**라우팅**)** 탭을 클릭합니다.

단계 **3** **ECMP**를 클릭합니다.

단계 **4** **Add(**추가**)**를 클릭합니다.

단계 **5** **Add ECMP(ECMP** 추가**)** 상자에 ECMP 영역의 이름인 **ECMP-VTI**를 입력합니다.

단계 **6** 인터페이스를 연결하려면 **Available Interfaces(**사용 가능한 인터페이스**)** 상자에서 **outside_static_vti_1** 및 **outside_static_vti_2** 인터페이스를 선택한 다음 **Add(**추가**)**를 클릭합니다.



단계 **7** **OK(**확인**)**를 클릭합니다.

이제 ECMP 페이지에 새로 생성된 ECMP 영역이 표시됩니다.

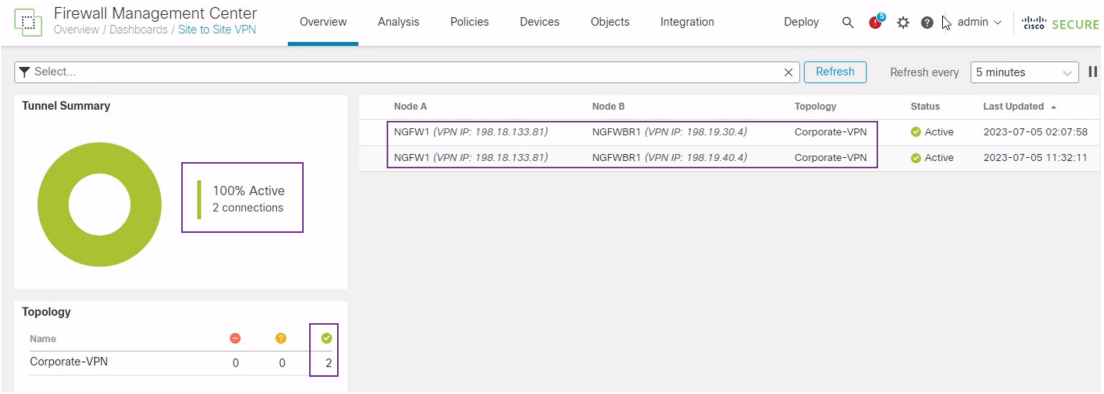
단계 **8** **Save(**저장**)**를 클릭합니다.

기본 및 보조 터널 확인

브랜치 노드와 허브 노드 간의 기본 및 보조 VTI 터널이 모두 설정되어 작동 중이며 활성 상태인지 확인합니다.

- 사이트 간 **VPN** 대시보드의 터널 상태 확인

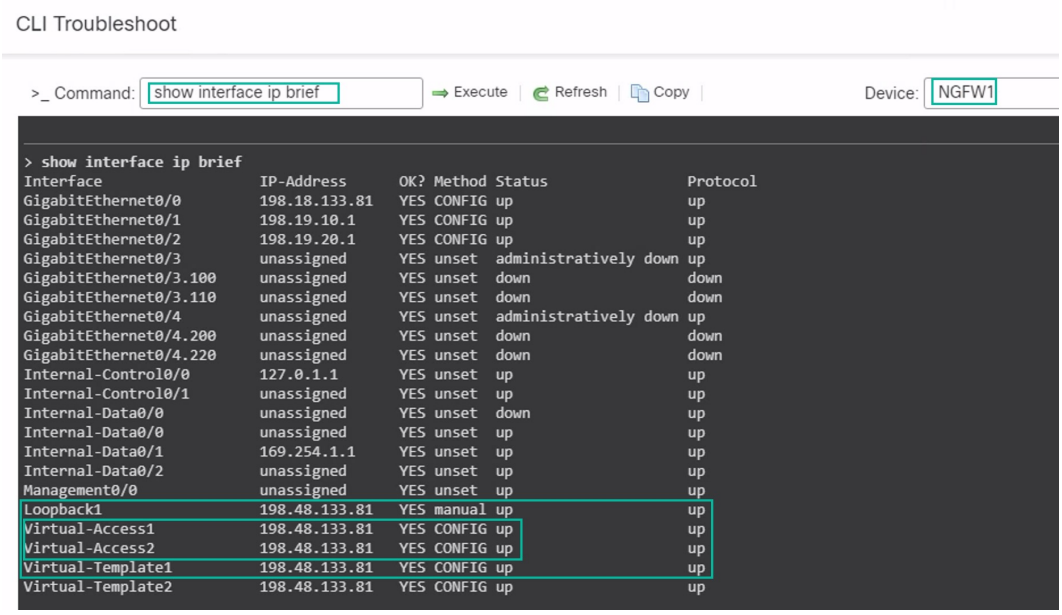
  VPN 터널이 작동 중이며 녹색인지 확인하려면 **Overview(**개요**)** > **Dashboards(**대시보드**)** > **Site-to-site VPN(**사이트 간 **VPN)**을 선택합니다.



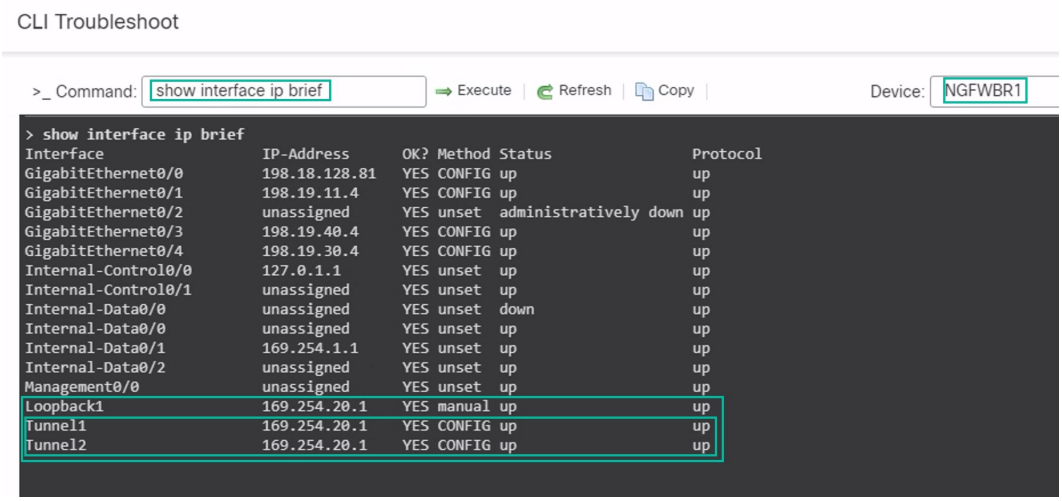
- 허브 및 브랜치 노드의 라우팅 확인

  1. **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.
  2. NGFW1을 수정하려면 Edit(편집) 아이콘을 클릭합니다.
  3. **Device(**디바이스**)** 탭을 클릭합니다.
  4. **General(**일반**)** 카드에서 **CLI** 버튼을 클릭합니다. **CLI Troubleshoot(CLI** 문제 해결**)** 창이 나타납니다.
  5. **Command(**명령**)** 필드에 **show interface ip brief**를 입력하고 **Execute(**실행**)**를 클릭하여 허브의 DVTI에서 생성된 동적 가상 액세스 인터페이스를 확인합니다.

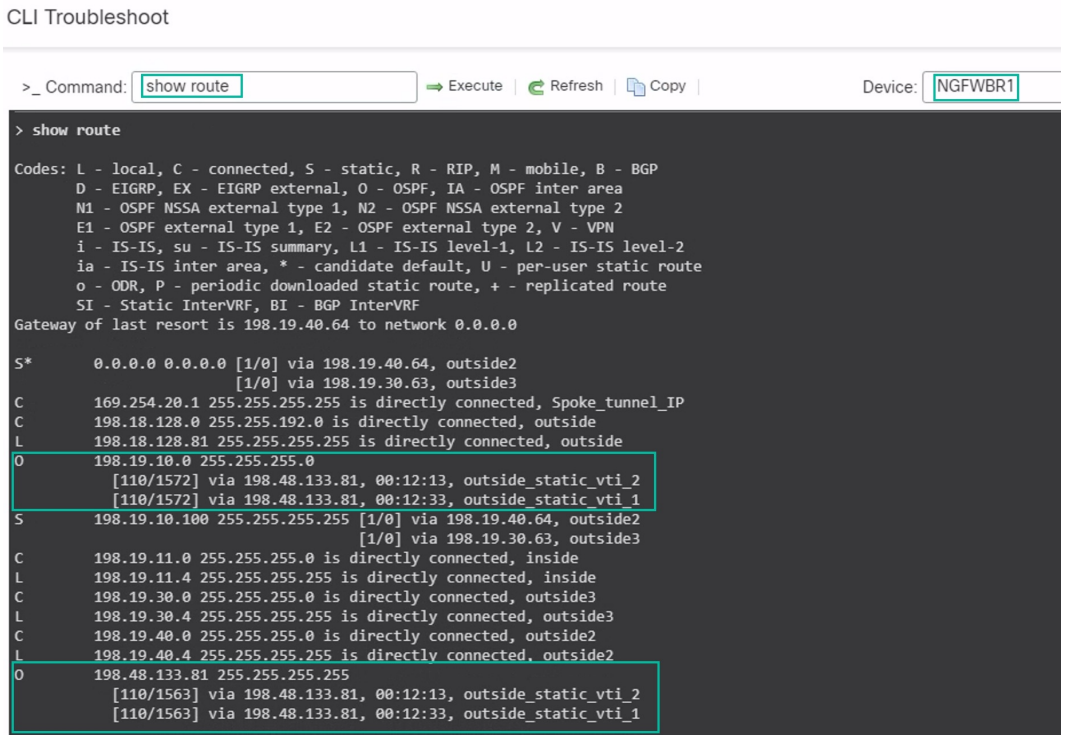
참고 **NGFWBR1**이 보조 VTI 연결을 통해 NGFW1에 연결되는 경우 동일한 DVTI에서 Virtual-Access2 인터페이스가 생성됩니다.



6. NGFWBR1 노드에 대해 2~5단계를 반복하여 아래 그림에 표시된 것과 같이 정적 VTI 인터페이스 **Tunnel1** 및 **Tunnel2**를 확인합니다.



7. **Command(**명령**)** 필드에 **show route**를 입력하고 **Execute(**실행**)**를 클릭하여 보조 VTI 터널을 추가한 후 경로를 확인합니다.



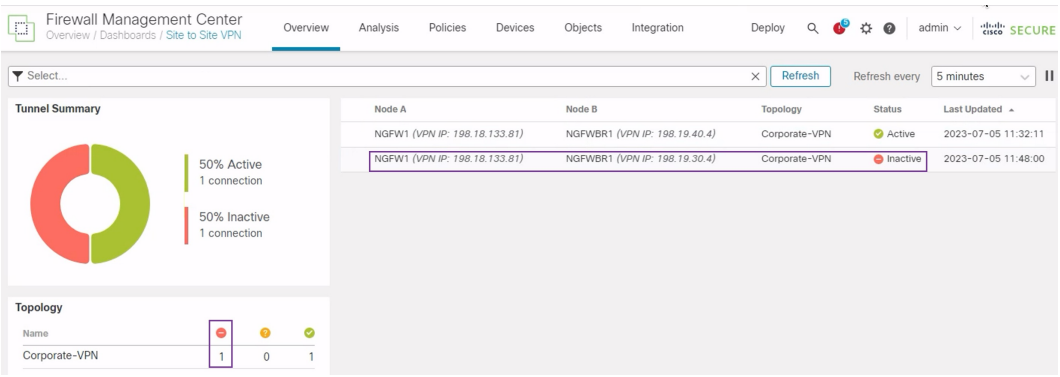
- **Corporate_LAN**(198.19.10.0/24)은 기본(**outside_static_vti_1**) 및 보조(**outside_static_vti_2**) VTI 모두에서 OSPF를 통해 학습되었습니다.
- DVTI 터널 IP(198.48.133.81)는 기본 및 보조 VTI 모두에서 OSPF를 통해서도 학습되었습니다.

- 기본 터널 중단 시 보조 터널에 대한 페일오버 확인

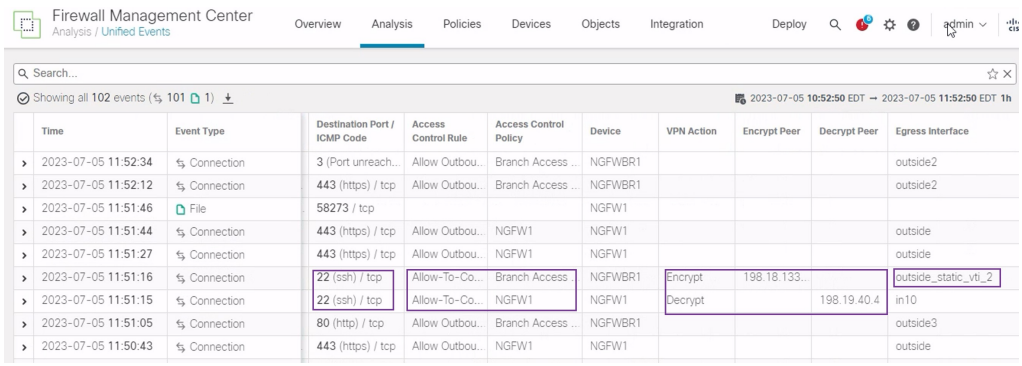
1. 이 예에서는 보조 터널에 대한 페일오버를 검증하기 위해 업스트림 디바이스의 액세스 제어 목록을 통해 인터넷으로 이동하는 outside3 인터페이스에서 제공되는 아웃바운드 트래픽을 제한하거나 다음의 위협 방어를 위해 outside3 인터페이스를 종료하여 패킷 손실을 유도할 수 있습니다.

참고 인터페이스를 종료하는 것은 네트워크를 방해하므로 프로덕션 네트워크에서 시도해서는 안 됩니다.

2. 사이트 간 VPN 대시보드에서 아래 그림과 같이 기본 터널이 다운된 상태입니다.



3. 브랜치에서 허브로의 트래픽을 시작합니다. WKST BR 워크스테이션에 로그인하고 NGFW1 뒤의 호스트에 SSH를 연결합니다. 호스트에 SSH로 성공적으로 연결할 수 있는지 확인합니다.
4. 통합 이벤트 뷰어를 사용하여 트래픽의 이그레스 경로를 확인합니다.
   1. **Analysis(분석) > Unified Events(통합 이벤트)**를 선택합니다.
   2. 열 선택기를 사용하여 **VPN Action, Encrypt Peer, Decrypt Peer(VPN** 작업**,** 피어 암호화**,** 피어 암호 해독**)** 및 **Egress Interface(**이그레스 인터페이스**)** 열을 추가합니다.
   3. 아래 그림에 표시된 것과 같이 열, 대상 포트**/ICMP** 코드**,** 액세스 제어 규칙**,** 액세스 제어 정책 및 디바이스와 함께 새 열의 순서를 변경하고 크기를 조정합니다.



SSH(포트 22)에 대한 **NGFWBR1**의 이그레스 인터페이스가 이제 보조 인터페이스 **(outside_static_vti_2**)로 표시됩니다.

경로 기반 **VPN** 터널 문제 해결

구축 후 다음 CLI를 사용하여 Secure Firewall Threat Defense에서 경로 기반 VPN 터널과 관련된 문제를 디버깅합니다.

참고 프로덕션 환경의 위협 방어 디바이스에서 디버그 명령을 실행할 때는 주의하십시오. 자세한 정보 표시 출력이 있을 수 있는 디바이스에서 다양한 디버그 레벨을 설정할 수 있습니다.

방법	**CLI** 명령
특정 피어에 대해 조건부 디버깅 활성화	**debug crypto condition peer <peer-IP>**
가상 터널 인터페이스 정보 디버그	**debug vti 255**
IKEv2 프로토콜 관련 트랜잭션 디버그	**debug crypto ikev2 protocol 255**
IKEv2 플랫폼 관련 트랜잭션 디버그	**debug crypto ikev2 platform 255**
일반 IKE 관련 트랜잭션 디버그	**debug crypto ike-common 255**
IPSec 관련 트랜잭션 디버그	**debug crypto ipsec 255**

추가 리소스

리소스	**URL**
Secure Firewall Threat Defense 릴리스 노트	https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html
모든 신규 및 지원 중단된 기능	http://www.cisco.com/go/whatsnew-fmc
Cisco.com의 보안 방화벽	http://www.cisco.com/go/firewall
유튜브의 Secure Firewall	https://www.youtube.com/cisco-netsec
Secure Firewall 기초	https://secure.cisco.com/secure-firewall

추가 리소스