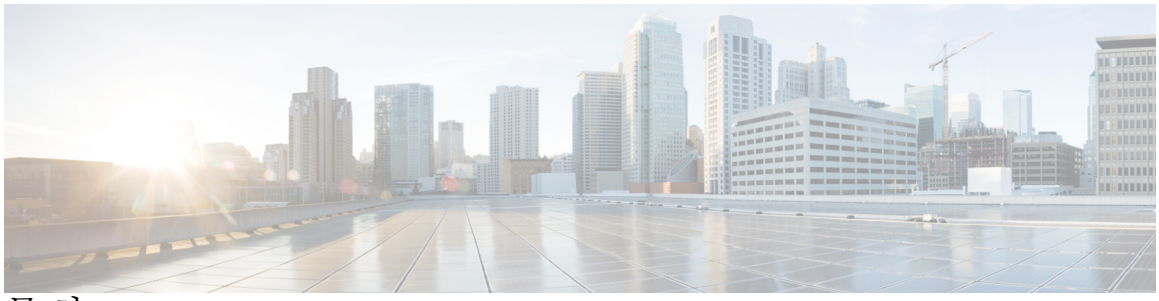
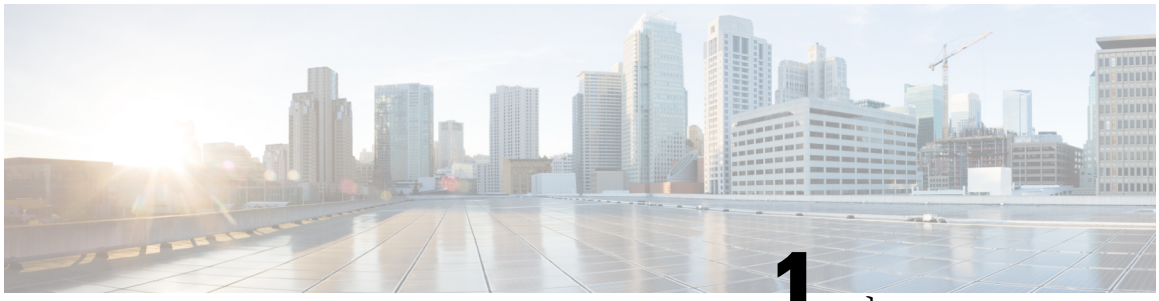
Cisco Secure Firewall의 SD-WAN 기능에 대한 활용 사례

초판: 2023년 4월 4일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차



1 장

시작하기

이 장에서는 Cisco Secure Firewall의 기능 및 지원되는 SD-WAN 기능에 대해 간략하게 설명합니다.

이 발행물에 관하여

이 가이드에서는 Cisco Secure Firewall에서 지원되는 SD-WAN 기능을 사용하는 주요 활용 사례를 자세히 설명합니다.

이러한 접근 방식은 가능한 모든 네트워크 요구 사항을 해결하지는 않습니다. 대신, 네트워크를 패턴화할 수 있는 모델을 제공합니다. 예시에 나와 있는 기능을 사용하지 않도록 선택할 수도 있고, 필요에 더 적합한 기능을 추가 또는 대체할 수도 있습니다.

이 가이드에서는 사용자가 Cisco Secure Firewall에 대해 잘 알고 있다고 가정합니다. 설정에 대한 자세한 정보는 Cisco Secure Firewall Management Center 관리 가이드, 7.3 및 Cisco Secure Firewall Management Center 디바이스 설정 가이드, 7.3을 참조하십시오.

Cisco Secure Firewall

Cisco Secure Firewall은 Snort IPS, URL 필터링, 악성코드 방어 등의 첨단 기능을 갖춘 매우 강력한 방화벽 솔루션입니다.

이 포괄적인 제품은 물리적, 프라이빗 및 퍼블릭 클라우드 환경에서 일관된 보안 정책을 적용하여 위협 방지를 크게 간소화합니다.

또한 네트워크 인프라에 대한 광범위한 가시성을 제공하므로, 잠재적인 위협의 출처와 활동을 신속하게 식별할 수 있습니다. 이러한 정보를 파악하면 운영이 중단되기 전에 공격을 중지하기 위한 조치를 즉시 취할 수 있습니다.

기존 방화벽 기능 외에도 다음과 같은 기능을 제공합니다.

1. AVC(Application Visibility and Control)

2. 사용자 ID 인식 및 제어
3. 침입 방지 및 침입 탐지
4. SSL/TLS 암호 해독
5. 평판 기반 차단
6. 파일 및 악성코드 보호
7. VPN(Virtual Private Network)

네트워크 구축을 더욱 보호하기 위해 Cisco Secure Firewall은 이후 릴리스에서 다음과 같은 추가 보안 기능을 제공합니다.

- EVE(Encrypted Visibility Engine) - 전체 MITM(main-in-the-middle) 암호 해독을 구현할 필요 없이 암호화된 트래픽 검사를 개선합니다.
- 엘리펀트 플로우 탐지 - 엘리펀트 플로우(일반적으로 1GB/10초보다 큰 플로우)를 탐지하고 해결하여 높은 CPU 사용률 및 패킷 삭제를 방지합니다.
- CSDAC(Secure Dynamic Attribute Connector) - 기존 IP/네트워크 기반 정책 구성에 대해 태그와 레이블을 활용하여 보안 정책 관리에 민첩성과 인텔리전스를 제공합니다.

SD-WAN 기능 개요

조직이 여러 브랜치에서 운영을 확장하면서 안전하고 간소화된 연결을 보장하는 것이 무엇보다 중요해졌습니다. 안전한 브랜치 네트워크 인프라 구축에는 복잡한 설정 및 관리 프로세스가 포함되며, 이 프로세스에는 시간이 많이 걸리고 제대로 처리하지 않을 경우 보안 취약점에 노출되기 쉽습니다. 그러나 조직에서는 간소화되고 안전한 브랜치 구축을 위한 보안 방화벽 솔루션을 활용하여 이러한 문제를 해결할 수 있습니다.

이 가이드에서 강력한 방화벽 솔루션을 사용하여 보안 브랜치 구축을 간소화하는 개념을 살펴봅니다. 보안 방화벽을 브랜치 네트워크 아키텍처의 기본 구성 요소로 통합함으로써 조직은 구축 프로세스를 간소화하는 동시에 강력한 보안 베이스라인을 설정할 수 있습니다. 조직에서는 이 접근 방식을 통해 통합 보안 정책을 시행하고 트래픽 라우팅을 최적화하며 복원력 있는 연결을 보장할 수 있습니다.

Cisco Secure Firewall에서 지원되는 일부 SD-WAN 기능은 다음과 같습니다.

- 보안 탄력적 연결:
  - 본사(허브)와 브랜치(스포크) 간 경로 기반(VTI) VPN 터널
  - IPv4 및 IPv6 BGP, IPv4 및 IPv6 OSPFv2/v3, 그리고 IPv4 EIGRP over VTI
  - 정적 또는 동적 IP 스포크에 대한 DVTI 지원
- 네트워크 다운타임이 거의 없는 고가용성:
  - 듀얼 ISP 구성

- 애플리케이션 기반 인터페이스 모니터링을 기반으로 최적의 경로 선택

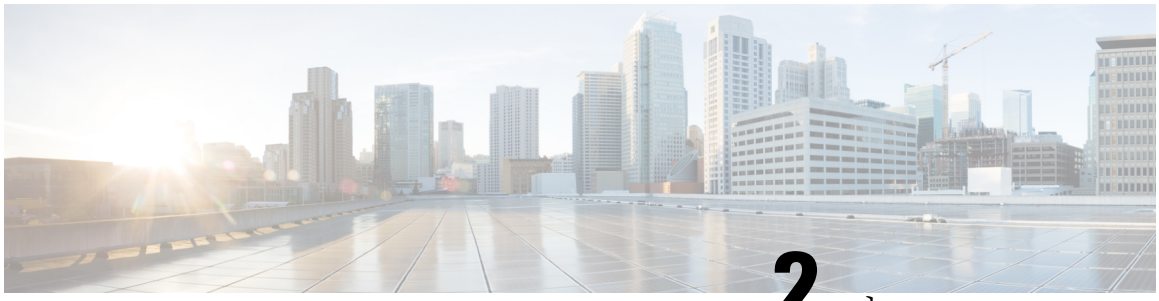
- 사용 가능한 대역폭 증가**:**
  - 여러 ISP 간 로드 밸런싱을 위한 ECMP 지원
  - SVTI에 대한 ECMP 지원
  - PBR을 사용하는 애플리케이션 기반 로드 밸런싱
- 퍼블릭 클라우드 및 게스트 사용자를 위한 직접 인터넷 액세스**:**
  - 애플리케이션을 일치 기준으로 사용하는 정책 기반 라우팅
  - Umbrella용 로컬 터널 ID 지원
- 간소화된 관리**:**
  - SASE Umbrella 자동 터널 구축
  - DVTI 허브 스포크 토폴로지 간소화

기능

이 표에는 일반적으로 사용되는 몇 가지 WAN 기능이 나와 있습니다.

기능	도입 버전
VTI에 대한 루프백 인터페이스 지원	릴리스 7.3
사이트 간 VPN을 통한 동적 VTI(DVTI) 지원	릴리스 7.3
Umbrella 자동 터널	릴리스 7.3
VTI에 대한 IPv4 및 IPv6 BGP, IPv4 및 IPv6 OSPFv2/v3, IPv4 EIGRP 지원	릴리스 7.3
허브 및 스포크 토폴로지를 사용하는 경로 기반 사이트 간 VPN	릴리스 7.2
경로 모니터링을 사용하는 정책 기반 라우팅	릴리스 7.2
사이트 간 VPN 모니터링 대시보드	릴리스 7.1
직접 인터넷 액세스/정책 기반 라우팅	릴리스 7.1
WAN 인터페이스가 있는 ECMP(Equal-Cost-Multi-Path) 영역	릴리스 7.1
VTI 인터페이스를 사용하는 ECMP(Equal-Cost-Multi-Path) 영역	릴리스 7.1
경로 기반 사이트 간 VPN을 위한 백업 VTI	릴리스 7.0

기능	도입 버전
사이트 간 VPN을 통한 정적 VTI(SVTI) 지원	릴리스 6.7



2 장

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.

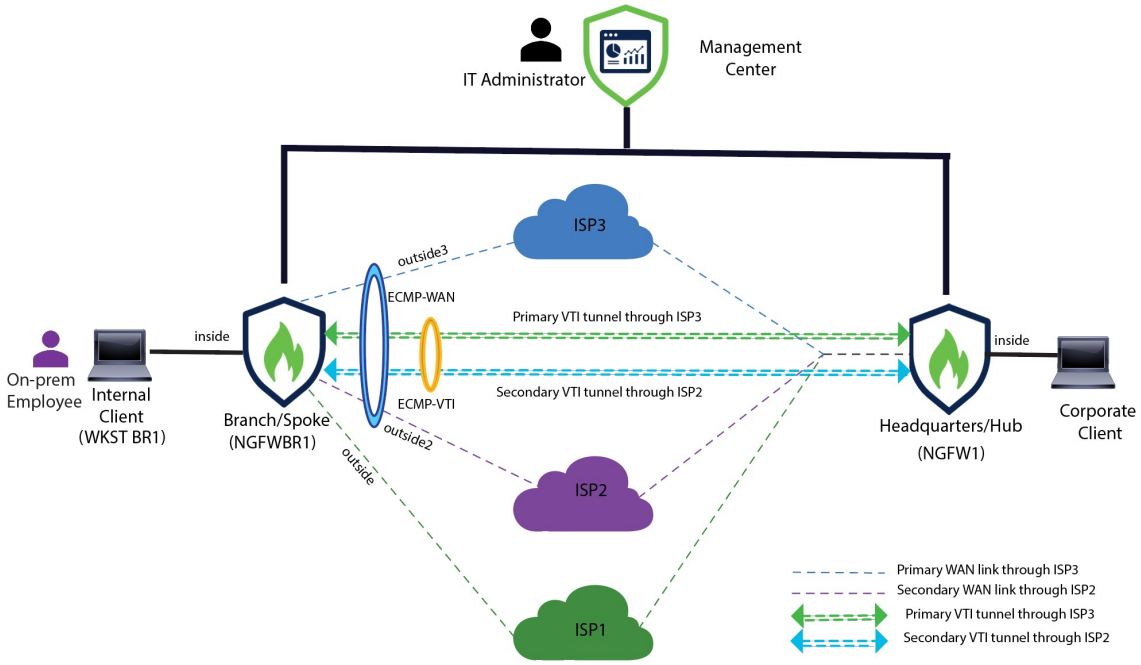
브랜치(스포크)와 본사(허브) 간의 경로 기반 **VPN**은 문제를 어떻게 해결합니까?

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

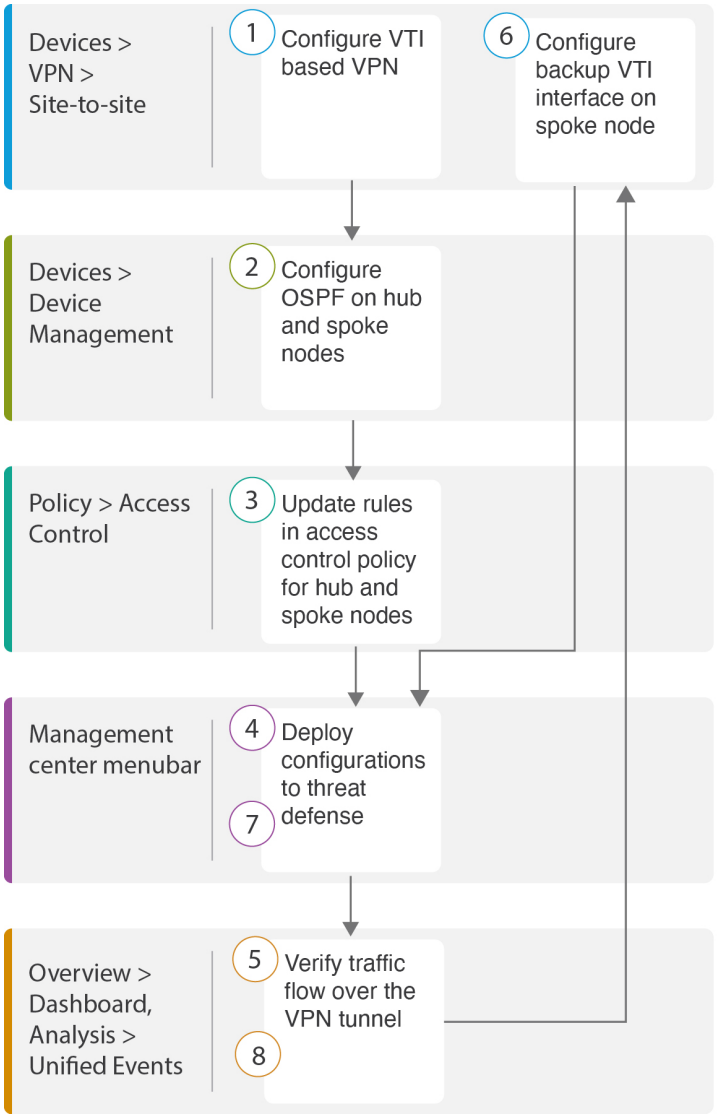
- Secure Firewall Threat Defense가 버전 6.7 이상에서 실행되는지 확인합니다.
- VTI는 라우팅 모드에서만 지원됩니다.
- 루프백 인터페이스에서 동적 인터페이스에 대한 IP 대여를 구성하는 것이 좋습니다.
- VTI를 통한 트래픽을 제어하려면 VTI 인터페이스에 액세스 규칙을 적용해야 합니다.
- VTI 트래픽의 로드 밸런싱을 위해 SVTI에 대한 ECMP 영역을 구성합니다.

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, 10 페이지 • 허브 노드에 대한 엔드포인트 구성, 11 페이지

단계	설명
	• 스포크 노드에 대한 엔드포인트 구성, 13 페이지
2	허브 앤 스포크 노드에서 OSPF를 구성합니다. 확인 • 허브 노드에서 OSPF 구성, 14 페이지 • 스포크 노드에서 OSPF 구성, 16 페이지
3	허브 및 스포크 노드에 대한 액세스 제어 정책에서 규칙을 업데이트합니다. 액세스 제어 정책 구성, 18 페이지의 내용을 참조하십시오.
4	구성을 위협 방어에 구축합니다. 컨피그레이션 구축, 21 페이지의 내용을 참조하십시오.
5	VPN 터널을 통한 트래픽 플로우를 확인합니다. VPN 터널을 통한 트래픽 흐름 확인, 21 페이지의 내용을 참조하십시오.
6	스포크 노드에서 백업 VTI를 구성합니다. 스포크 노드에서 백업 VTI 인터페이스 구성, 24 페이지의 내용을 참조하십시오.
7	구성을 위협 방어에 구축합니다. 컨피그레이션 구축, 21 페이지의 내용을 참조하십시오.
8	보조 터널의 트래픽 플로우를 확인합니다. 기본 및 보조 터널 확인, 27 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, 11 페이지의 내용을 참조하십시오.

단계 **5** 스포크 노드에 대한 엔드포인트를 구성합니다. 스포크 노드에 대한 엔드포인트 구성, 13 페이지의 내용을 참조하십시오.

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

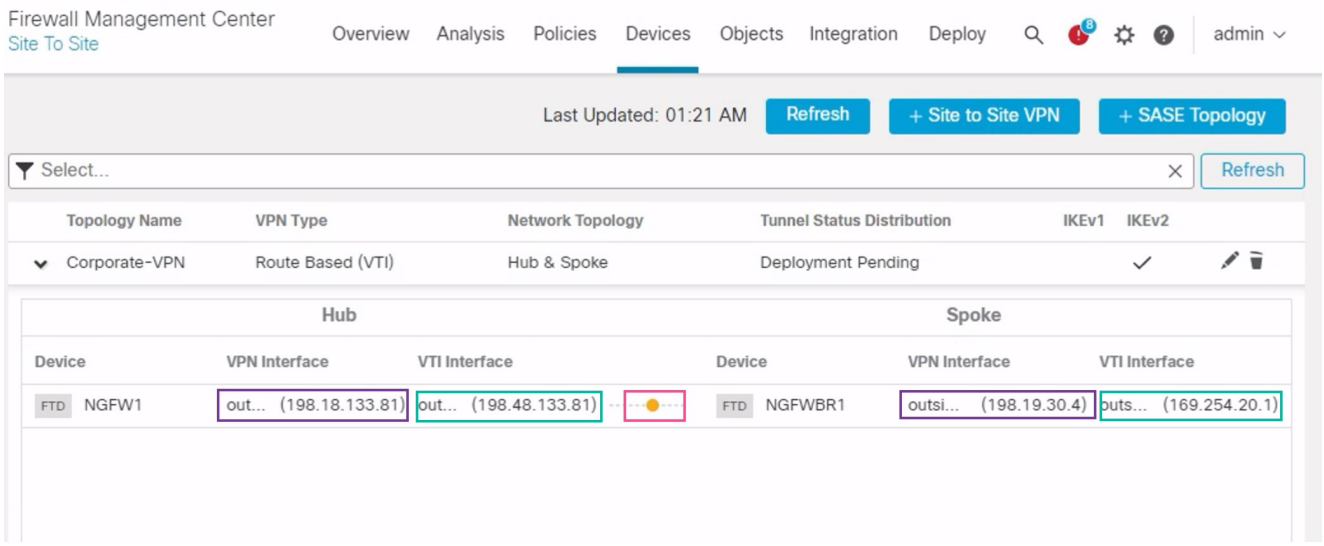
단계 **7** **Save**(저장)를 클릭합니다.

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, 14 페이지 및 스포크 노드에서 OSPF 구성, 16 페이지를 참조하십시오.
- 암호화된 트래픽을 허용하는 액세스 제어 규칙입니다. 액세스 제어 정책 구성, 18 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.

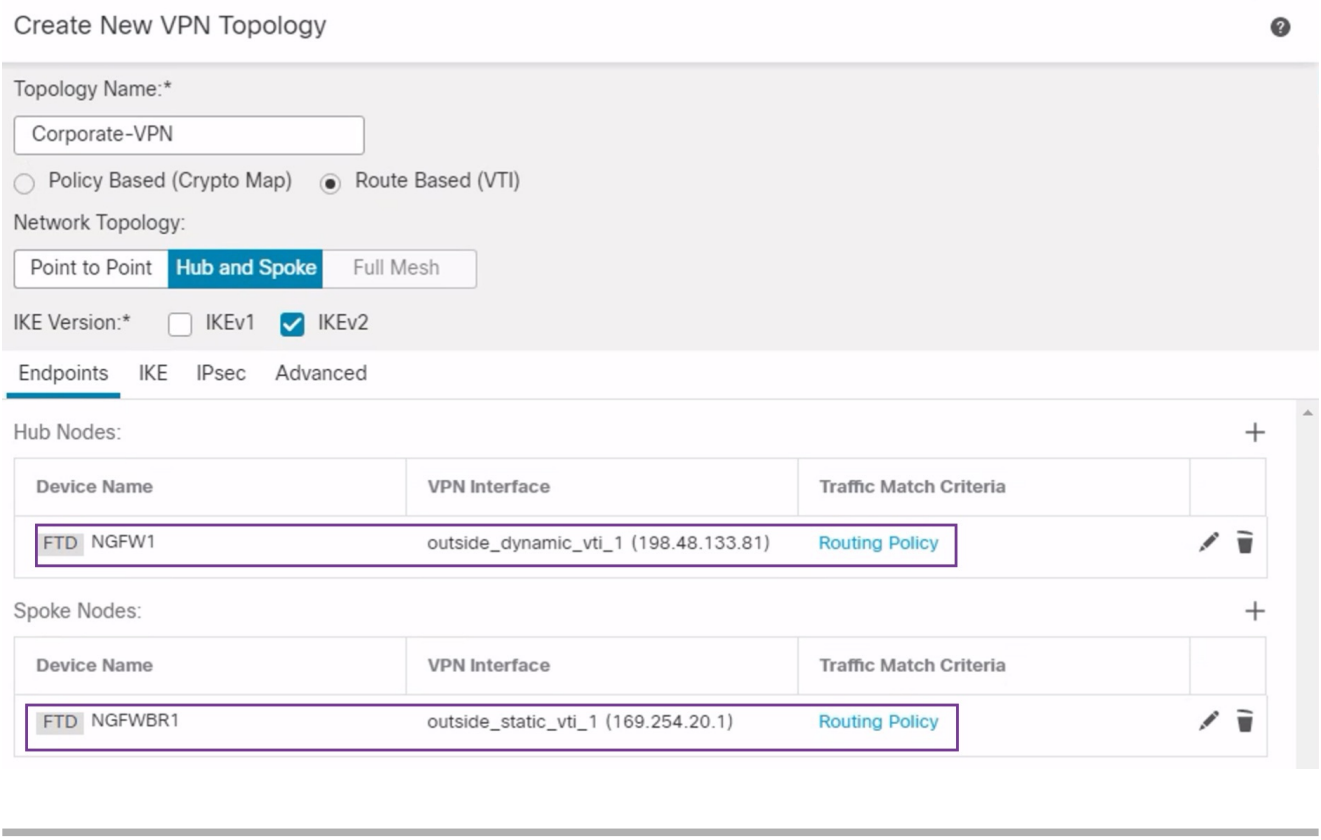
OK(확인**)**를 클릭하여 SVTI를 저장합니다. VTI가 성공적으로 생성되었음을 확인하는 메시지가 표시됩니다. **OK(**확인**)**를 클릭합니다.

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.

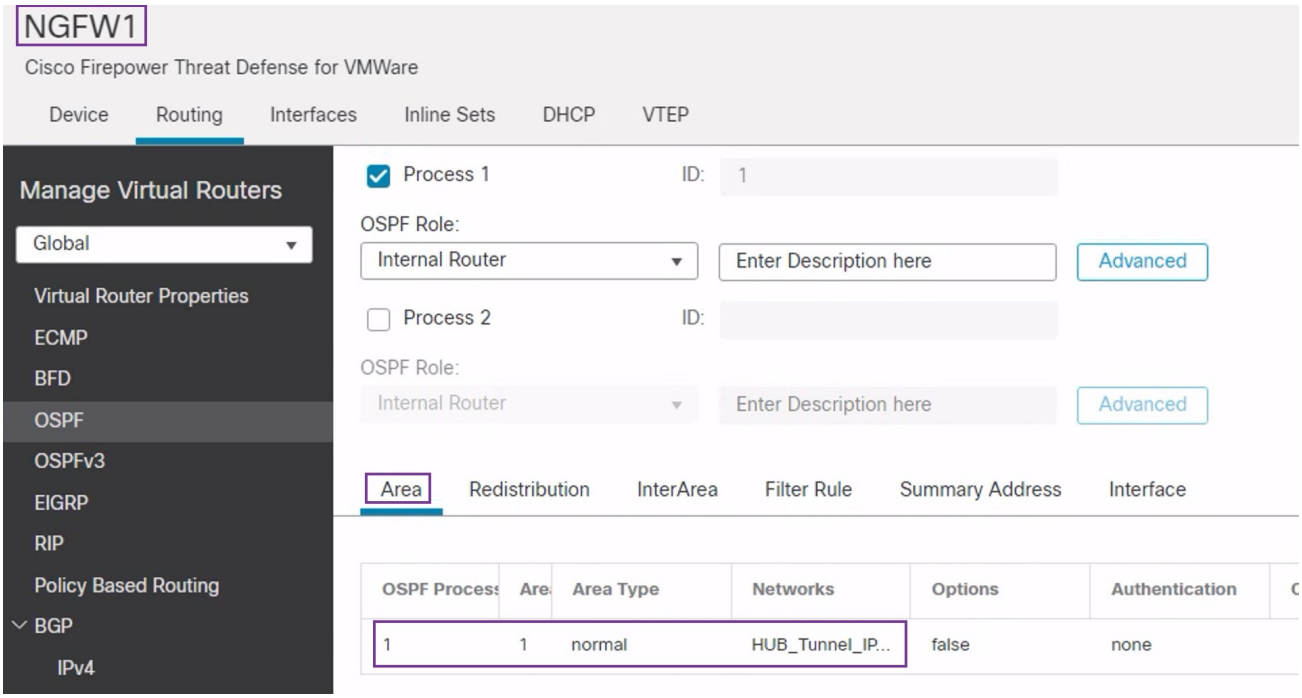
단계 **8** **Area(**영역**)** 탭을 클릭합니다.

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.

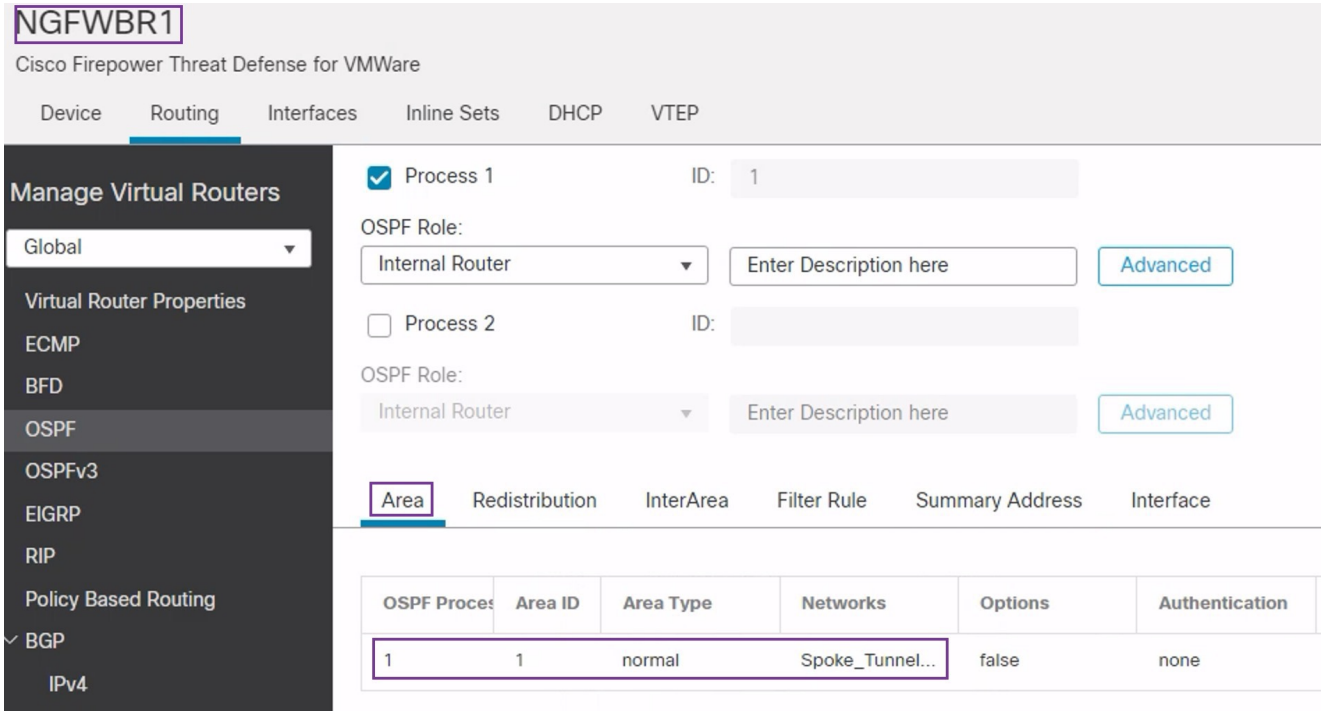
단계 **7** **+Add(**추가**)**를 클릭합니다. **Add Area(**영역 추가**)** 대화 상자가 나타납니다. 다음 필드를 수정합니다.

- **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.

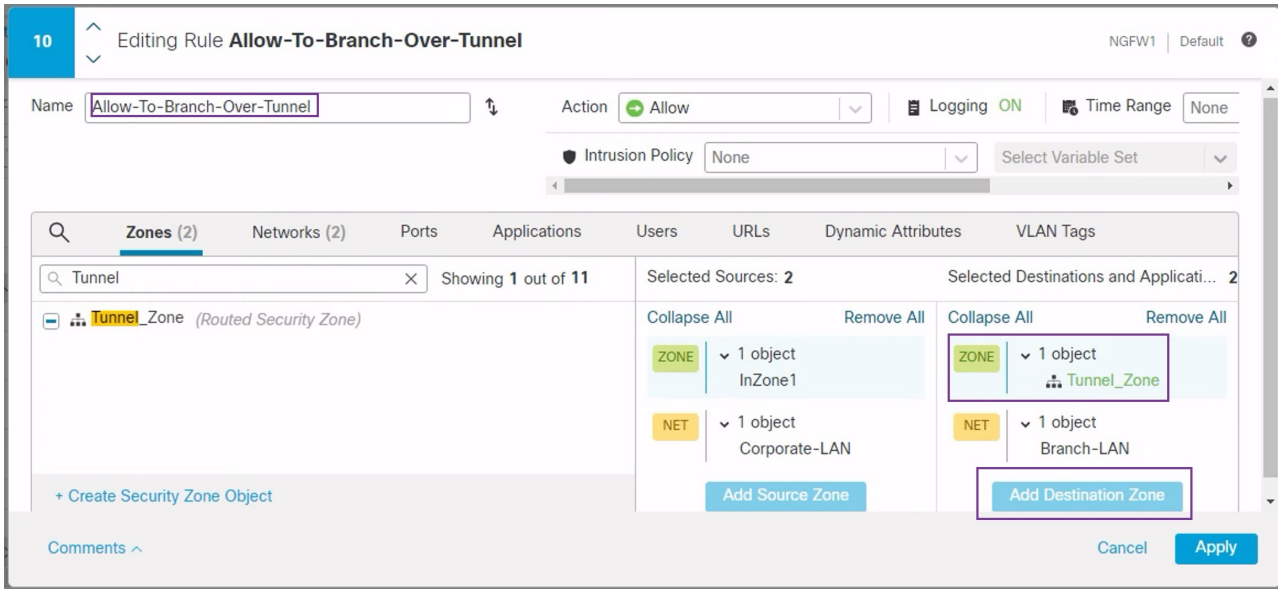
- **NGFW1** - 허브 노드(NGFW1)에 대한 액세스 제어 정책
- 브랜치 액세스 제어 - 스포크 노드(NGFWBR1)에 대한 액세스 제어 정책

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

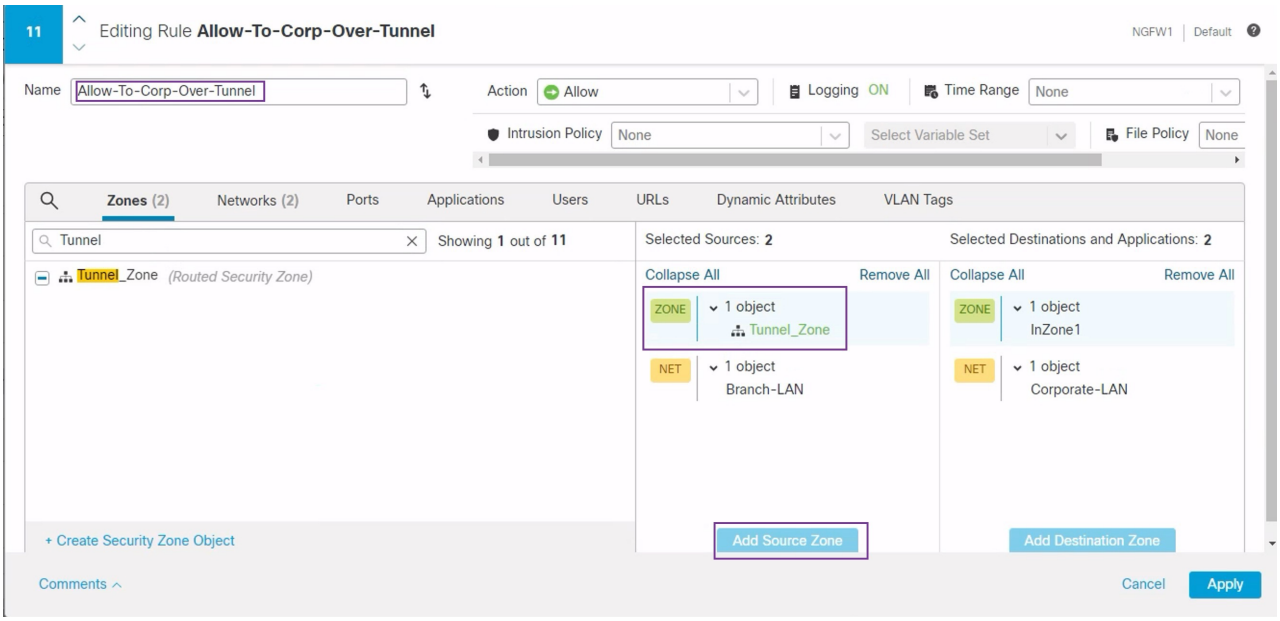
이 활용 사례를 위해 수정해야 하는 기존 규칙은 다음과 같습니다.

- **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.



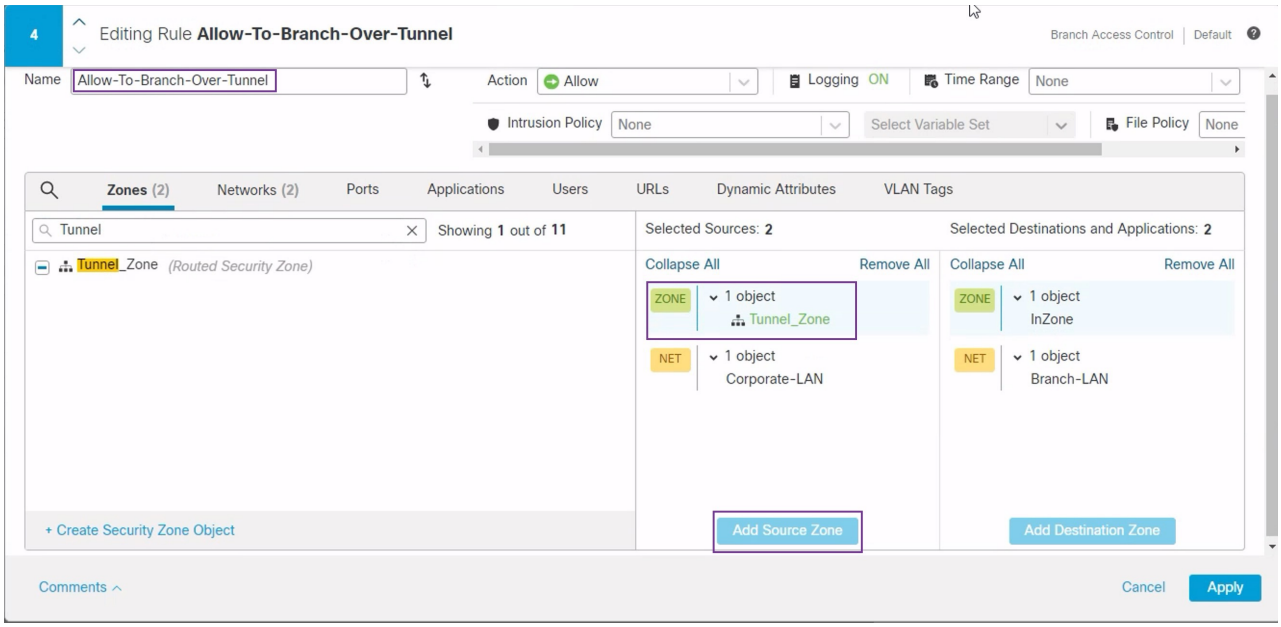
6. **Apply(**적용**)**를 클릭하여 규칙을 저장합니다.
7. NGFW1에서 업데이트된 규칙을 확인합니다.
8. **Save(**저장**)**를 클릭하여 AC 정책을 저장합니다.
9. **Return to Access Conrol Policy Management(**액세스 제어 정책 관리로 돌아가기**)**를 클릭하여 정책 페이지로 돌아갑니다.

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

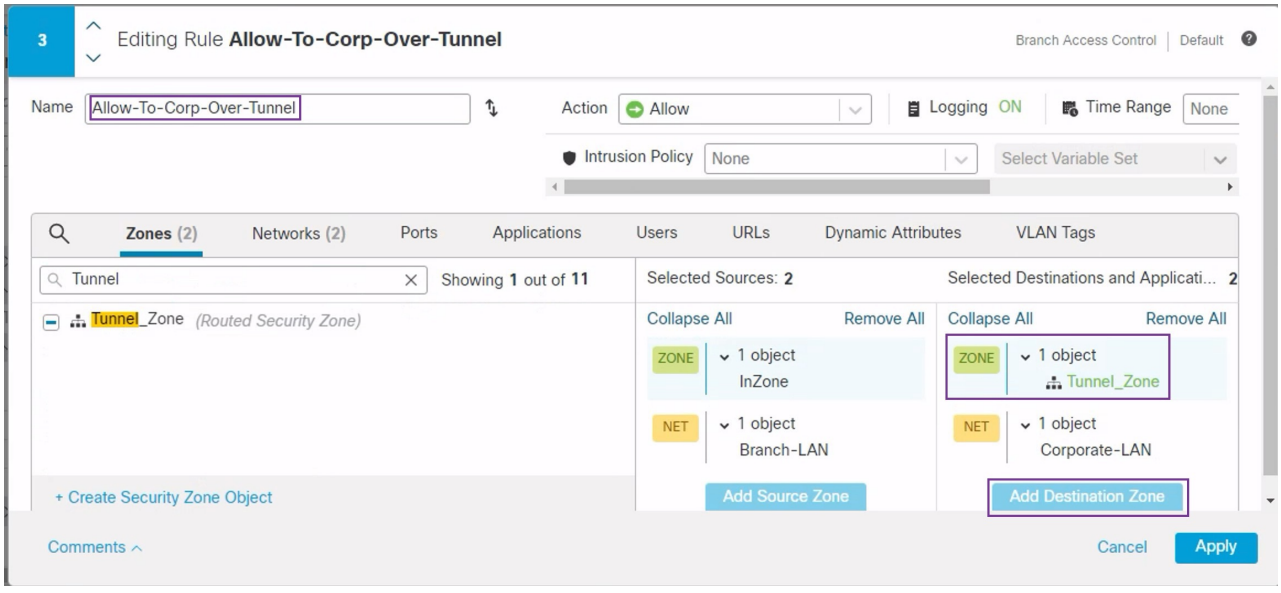
이 예시에서 수정해야 하는 규칙은 다음과 같습니다.

- **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.

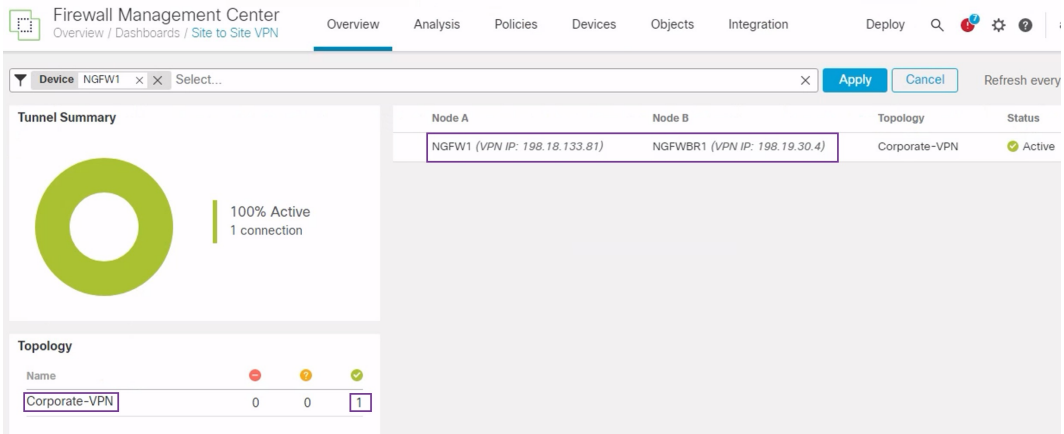
- Proceed with Deploy(구축 계속) - 경고 조건을 해결하지 않고 구축을 계속합니다. 오류가 식별되는 경우 계속 진행할 수 없습니다.
- Close(닫기) -구축하지 않고 종료합니다. 오류 및 경고 조건을 해결하고 컨피그레이션을 재구축합니다.

VPN 터널을 통한 트래픽 흐름 확인

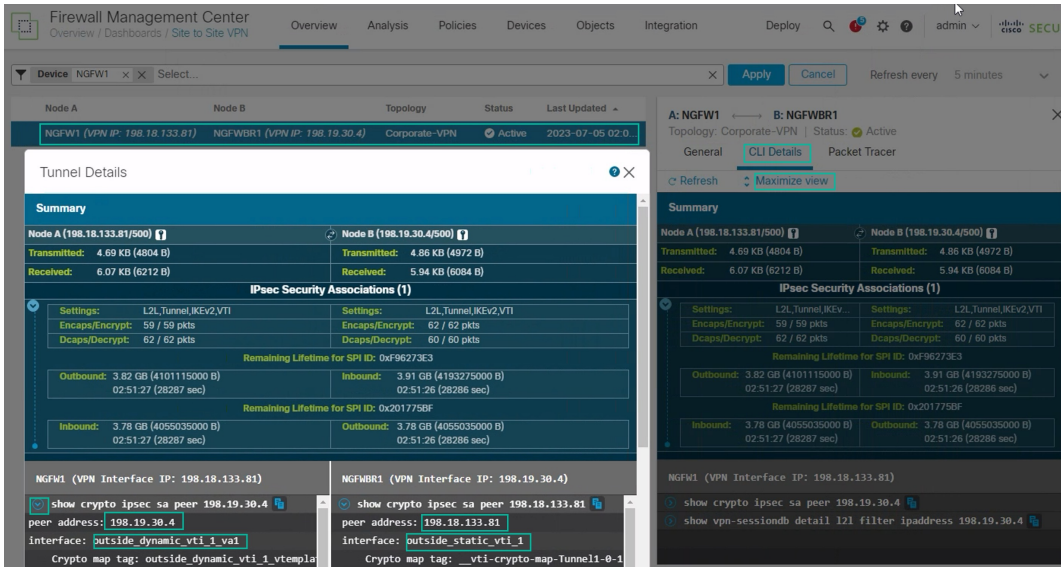
VPN 터널에 대해 다음 확인을 수행합니다.

- 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.



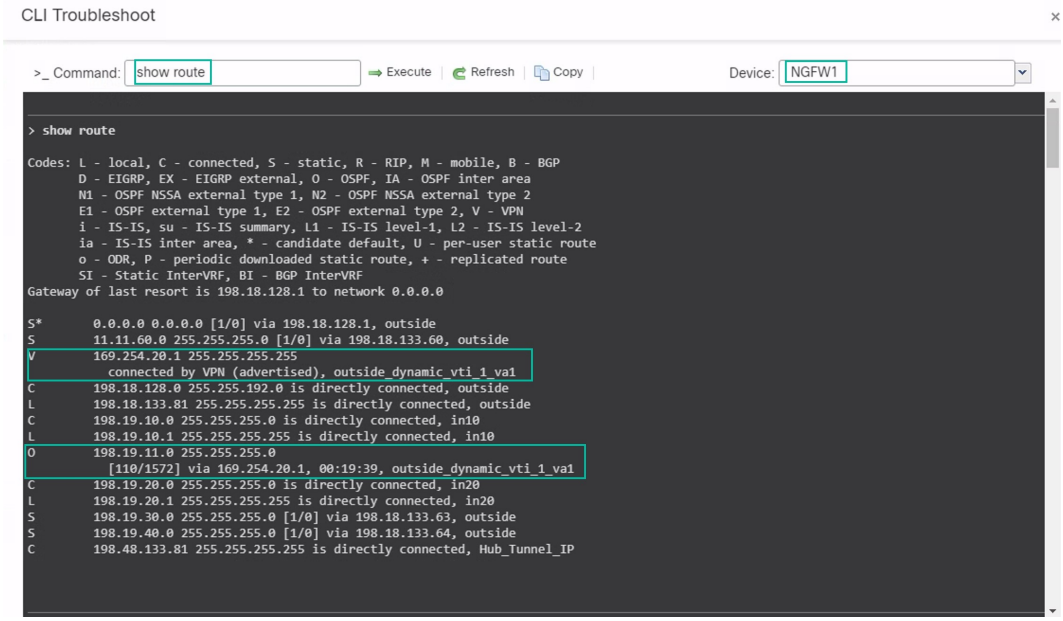
2. NGFW1 위에 마우스 커서를 올려 놓습니다. NGFW1 옆에 **View Full Information(**전체 정보 보기**)** 아이콘이 표시됩니다.
3. **View Full Information(**전체 정보 보기**)** 아이콘을 클릭합니다. 터널 세부 정보 및 추가 작업이 있는 측면 창이 나타납니다.
4. 측면 창에서 **CLI Details(CLI** 세부 정보**)** 탭을 클릭합니다.
5. IPSec 보안 연결의 상세정보가 포함된 최대화된 대화 상자를 표시하려면 **Maximumize View(**보기 최대화**)**를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



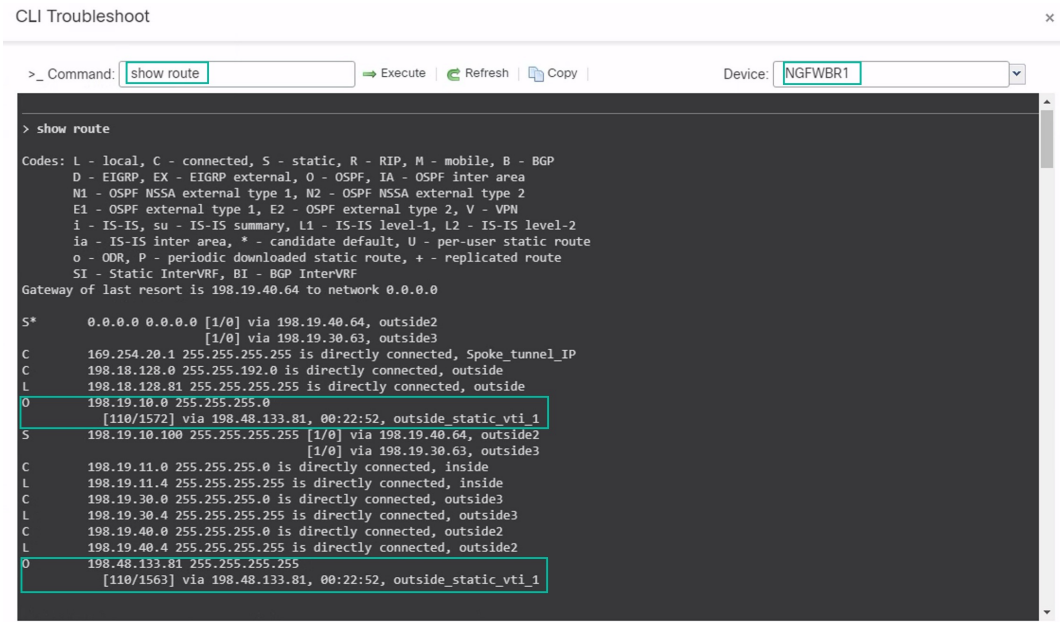
7. **Close(**닫기**)**를 클릭하여 Tunnel Details(터널 상세정보) 창을 종료합니다.

- 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.

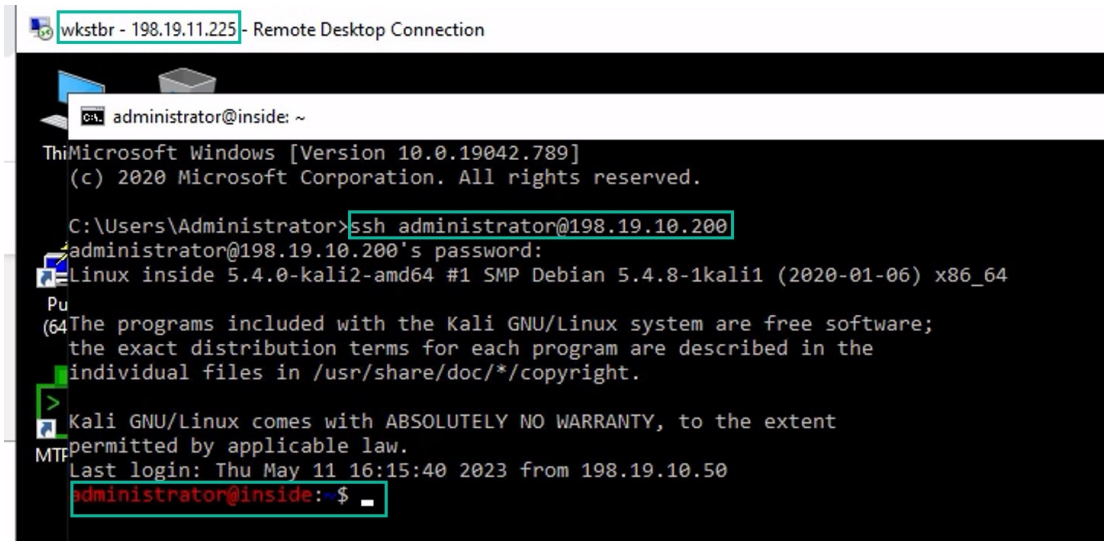


7. NGFWBR1 노드에 대해 2~5단계를 반복합니다.
8. NGFWBR1 노드의 경로를 검토합니다. 아래 그림에 표시된 것과 같이 허브의 VTI IP(198.48.133.81) 및 Corporate_LAN(198.19.10.0/24)에 대해 학습된 OSPF 경로를 확인합니다.



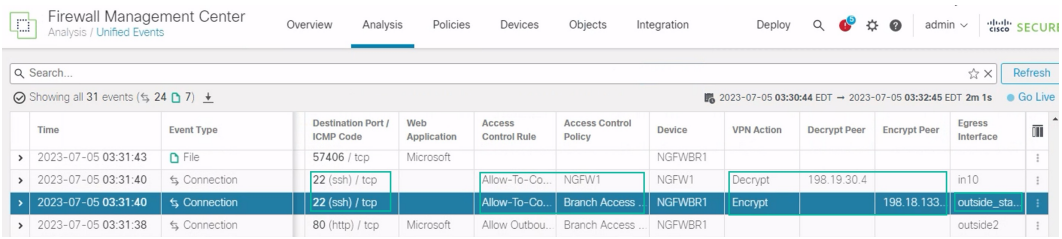
- 스포크 및 허브 노드 뒤의 보호되는 네트워크 간의 트래픽 확인

  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.

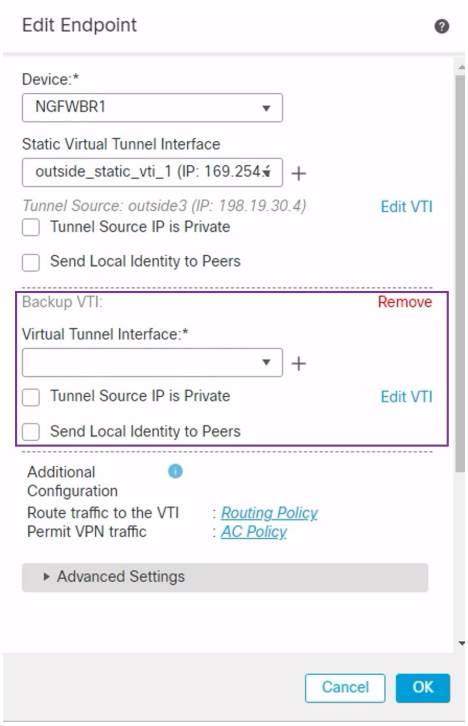
스포크 노드에서 백업 **VTI** 인터페이스 구성

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.

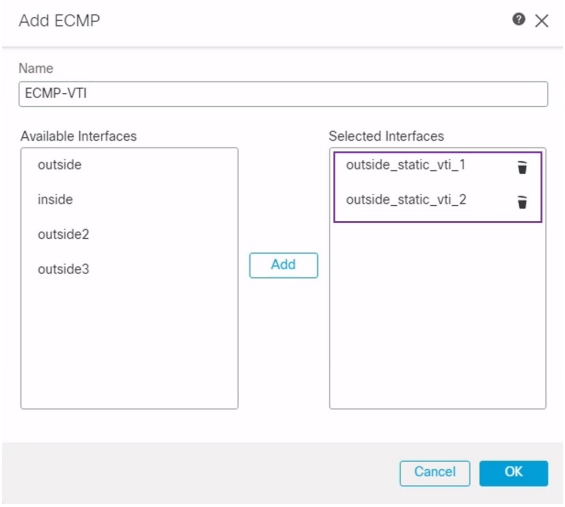
단계 **2** NGFWBR1의 인터페이스 보기에서 **Routing(**라우팅**)** 탭을 클릭합니다.

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.

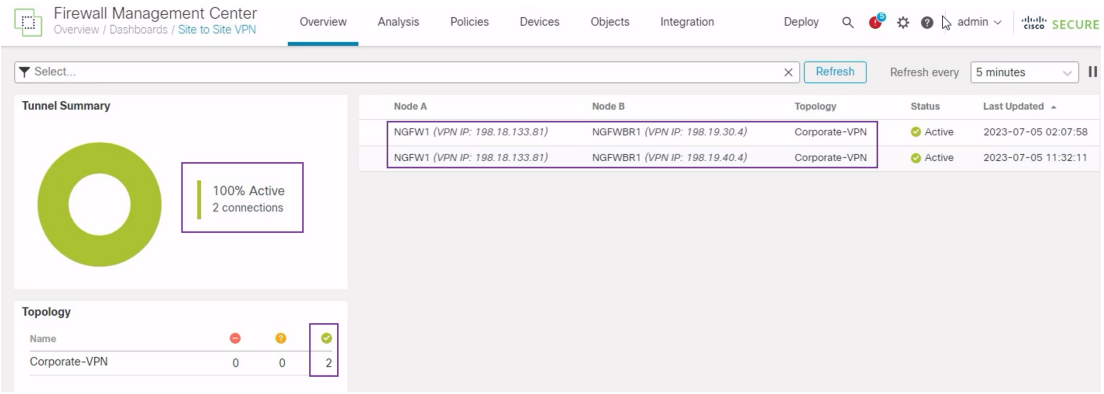
단계 **8** **Save(**저장**)**를 클릭합니다.

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

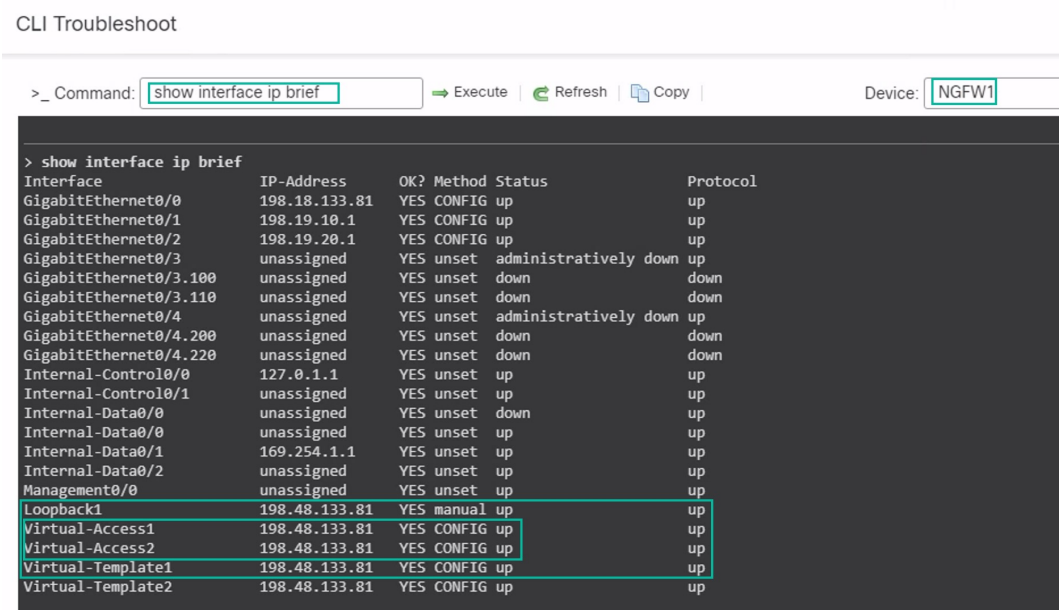
  VPN 터널이 작동 중이며 녹색인지 확인하려면 **Overview(**개요**)** > **Dashboards(**대시보드**)** > **Site-to-site VPN(**사이트 간 **VPN)**을 선택합니다.



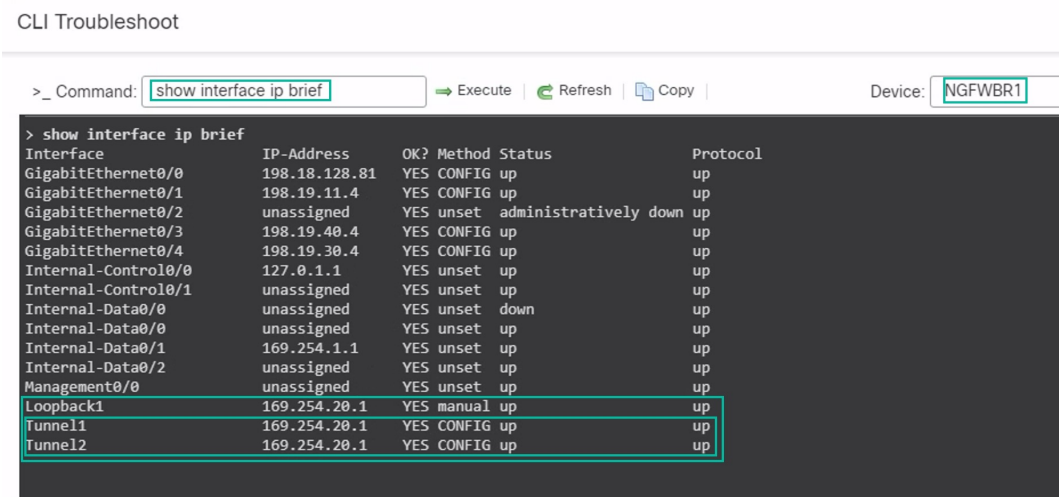
- 허브 및 브랜치 노드의 라우팅 확인

  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.

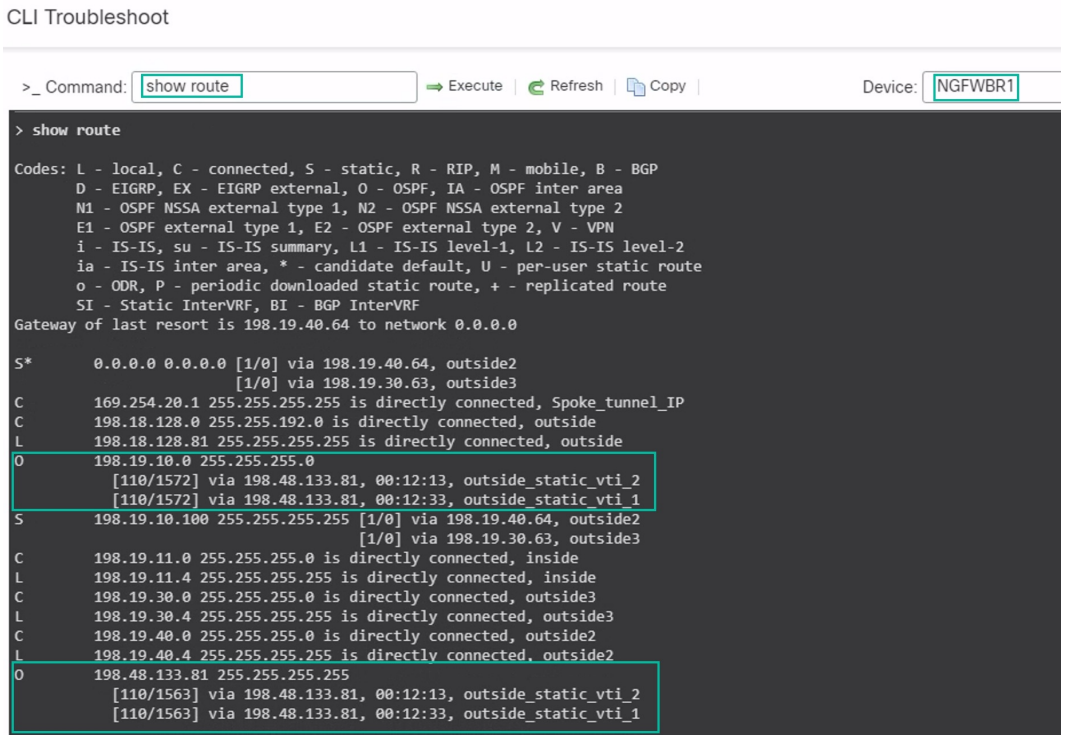
참고 **NGFWBR1**이 보조 VTI 연결을 통해 NGFW1에 연결되는 경우 동일한 DVTI에서 Virtual-Access2 인터페이스가 생성됩니다.



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.



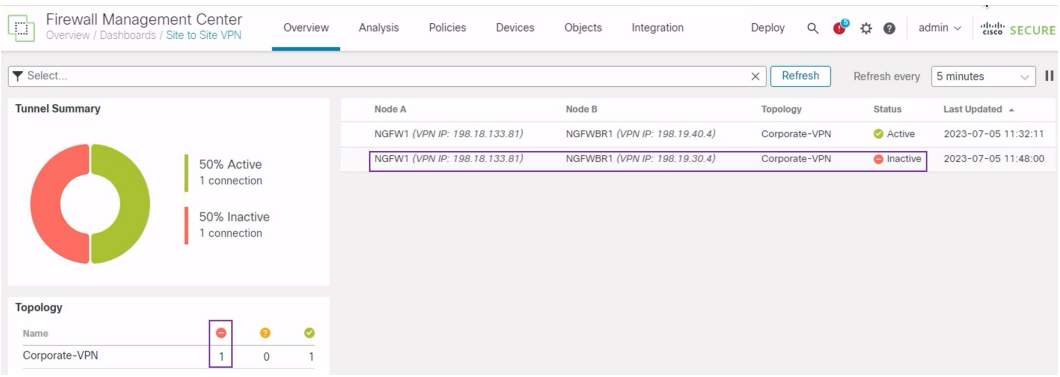
- **Corporate_LAN**(198.19.10.0/24)은 기본(**outside_static_vti_1**) 및 보조(**outside_static_vti_2**) VTI 모두에서 OSPF를 통해 학습되었습니다.
- DVTI 터널 IP(198.48.133.81)는 기본 및 보조 VTI 모두에서 OSPF를 통해서도 학습되었습니다.

- 기본 터널 중단 시 보조 터널에 대한 페일오버 확인

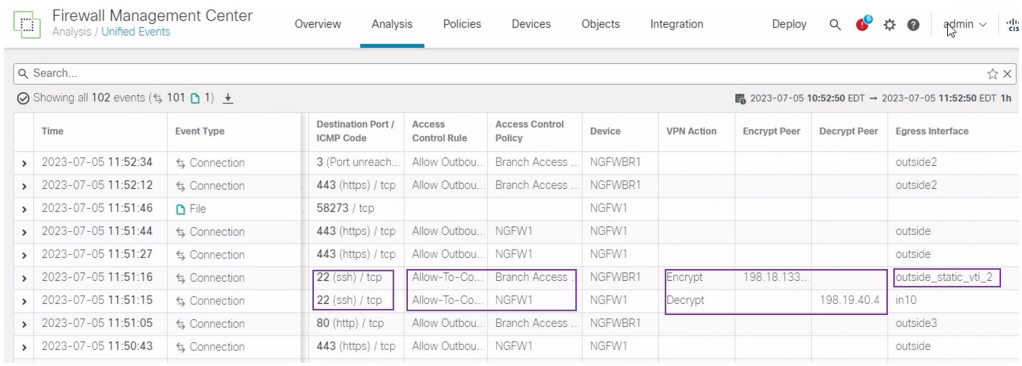
1. 이 예에서는 보조 터널에 대한 페일오버를 검증하기 위해 업스트림 디바이스의 액세스 제어 목록을 통해 인터넷으로 이동하는 outside3 인터페이스에서 제공되는 아웃바운드 트래픽을 제한하거나 다음의 위협 방어를 위해 outside3 인터페이스를 종료하여 패킷 손실을 유도할 수 있습니다.

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

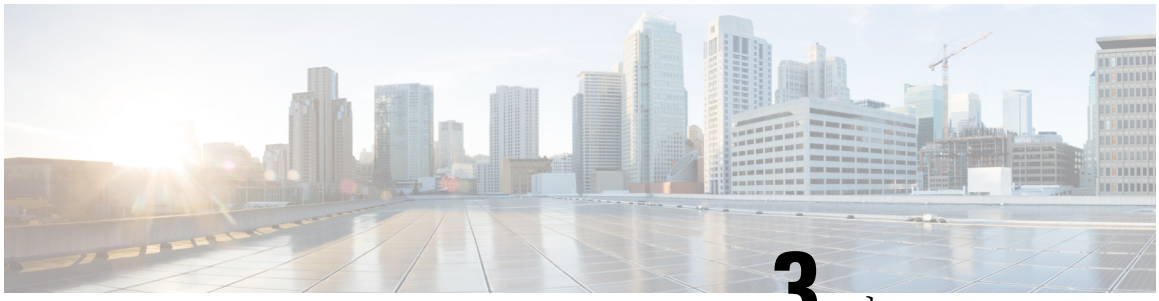
구축 후 다음 CLI를 사용하여 Secure Firewall Threat Defense에서 경로 기반 VPN 터널과 관련된 문제를 디버깅합니다.

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



3 장

DIA(Direct Internet Access)를 사용하여 브랜치에서 인터넷으로 애플리케이션 트래픽 라우팅

이 장에서는 두 가지 활용 사례를 사용하여 DIA(Direct Internet Access)를 실제로 적용하는 방법을 살펴봅니다. 각 활용 사례에서는 시나리오, 네트워크 토폴로지, 모범 사례, 사전 요건에 대해 자세히 설명합니다. 또한 원활한 구현을 위한 포괄적인 엔드 투 엔드 절차를 제공합니다.

직접 인터넷 액세스

디지털 혁신은 기업이 운영하고, 커뮤니케이션하고, 고객과 상호 작용하는 방식을 혁신하고 있습니다. 이제는 협업 및 고객 경험을 개선하며 높은 대역폭 및 낮은 레이턴시 연결이 요구되는 새로운 애플리케이션 및 기술이 생성되었습니다.

기존 네트워크의 당면 과제

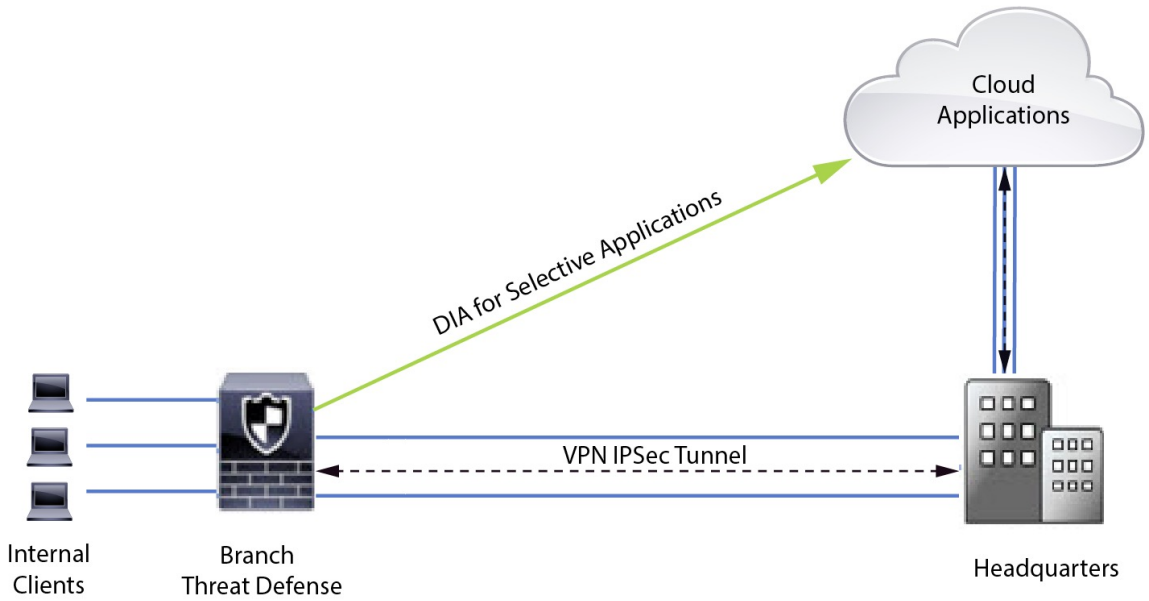
일반적으로 네트워크 구축은 중앙 사이트의 경계 방화벽을 활용하여 로컬 및 브랜치 사용자에 대한 보안 액세스를 제공합니다. 이 아키텍처는 원하는 연결성을 제공하지만, 모든 인터넷 트래픽을 VPN 터널을 통해 암호화된 트래픽으로 중앙 사이트에 전송하므로 패킷 레이턴시, 삭제 및 지터가 발생합니다. 또한, 네트워크는 높은 비용과 대역폭 사용률로 인해 구축 및 복잡한 네트워크 관리와 관련된 문제를 지속적으로 해결해야 합니다.

솔루션

이러한 문제를 해결하는 방법 중 하나는 DIA(직접 인터넷 액세스)를 사용하는 것입니다. DIA는 Cisco Secure Firewall의 브랜치 간소화 기능의 구성 요소입니다. DIA는 정책 기반 라우팅(PBR)을 사용합니다. DIA는 애플리케이션 인식 라우팅이라고도 합니다.

DIA 토폴로지에서는 브랜치 오피스의 애플리케이션 트래픽이 인터넷으로 직접 라우팅되므로 인터넷 바인딩 트래픽을 본사로 터널링하는 레이턴시를 우회합니다. Secure Firewall Threat Defense 브랜치는 인터넷 종료점을 포함하여 구성되어 있습니다. PBR 정책은 확장된 액세스 제어 목록에 정의된 애플리케이션을 기반으로 트래픽을 식별하기 위해 인그레스 인터페이스에 적용됩니다. 따라서 트래픽은 이그레스 인터페이스를 통해 인터넷으로 직접 전달됩니다.

그림 *1:* 특정 이그레스 인터페이스를 통한 직접 인터넷 액세스



정책 기반 라우팅을 사용하는 이유

PBR을 사용하여 지정된 애플리케이션에 대한 트래픽을 분류하고 안전하게 분할할 수 있습니다. 또한 특정 트래픽에 대한 경로를 지정할 수 있습니다. Secure Firewall Management Center 사용자 인터페이스에서 애플리케이션이 직접 액세스하도록 허용하는 PBR 정책을 구성할 수 있습니다.

PBR 및 경로 모니터링

일반적으로 PBR에서 트래픽은 구성된 우선순위 값(인터페이스 비용)에 따라 이그레스 인터페이스를 통해 전달됩니다. Secure Firewall Management Center 버전 7.2 이상 버전에서 PBR은 경로 모니터링을 사용하여 이그레스 인터페이스의 성과 측정(RTT, 지터, 패킷 손실 및 MOS)을 수집합니다. PBR은 메트릭을 사용하여 트래픽을 전달하기 위한 최적의 경로(이그레스 인터페이스)를 결정합니다. 경로 모니터링은 메트릭이 변경되면 모니터링되는 인터페이스에 대해 주기적으로 PBR에 알립니다. PBR은 경로 모니터링 데이터베이스에서 모니터링되는 인터페이스에 대한 최신 메트릭 값을 검색하고 데이터 경로를 업데이트합니다.

인터페이스에 대한 경로 모니터링을 활성화하고, 이그레스 인터페이스의 모니터링 유형을 구성한 후 메트릭 값을 사용하는 경로 모니터링을 활용하도록 애플리케이션 트래픽을 구성해야 합니다.

경로 모니터링에 대한 내용은 시나리오 2: 경로 모니터링을 사용한 직접 인터넷 액세스, 40 페이지의 내용을 참조하십시오.

이점

DIA 사용의 이점은 다음과 같습니다.

- 인터넷 속도 및 브랜치 오피스 사용자 환경을 개선합니다.
- 복잡성 감소로 네트워크 관리를 더 쉽고 저렴하게 할 수 있습니다.
- 대역폭 사용량을 줄이고 고가의 하드웨어가 필요하지 않으므로 비용 효율적입니다.
- 실시간 메트릭을 사용하는 동적 경로 선택합니다.
- 수동 개입 없이 최상의 이그레스 경로가 보장됩니다.
- 링크 상태 및 네트워크 상태에 대한 지속적인 모니터링.
- 민첩성 증가로 조직이 변화하는 비즈니스 요구에 빠르게 적응할 수 있습니다.

이 활용 사례가 귀사에 적합합니까?

이 활용 사례의 대상은 브랜치에서 직접 인터넷 바인딩 트래픽을 로컬로 분리할 수 있도록 각 원격 사이트 내에서 직접 인터넷 액세스를 구현하려는 네트워크 설계 엔지니어, 네트워크 운영 담당자, 보안 운영 담당자입니다.

직접 인터넷 액세스를 위한 구성 요소

브랜치 방화벽이 DIA에 사용하는 몇 가지 중요한 구성 요소는 다음과 같습니다.

- 신뢰할 수 있는 **DNS** 서버 — DIA 기능의 애플리케이션 탐지는 DNS 스누핑을 사용하여 애플리케이션 또는 애플리케이션 그룹을 확인합니다. DNS 요청이 비인가 DNS 서버에 의해 확인되지 않고 원하는 DNS 서버에 고정되도록 하기 위해 관리 센터에서 위협 방어를 위해 신뢰할 수 있는 DNS 서버를 구성할 수 있습니다.
- 인터페이스 우선순위 - Cisco Secure Firewall은 인터페이스 우선순위를 사용하여 최적의 인터넷 경로를 결정합니다. 우선 순위는 낮을수록 트래픽을 인터넷으로 전송할 때 특정 ISP의 기본 설정을 결정합니다. 관리 센터에서 위협 방어의 인터페이스 우선순위를 구성할 수 있습니다.
- 네트워크 서비스 - 정책 기반 라우팅 내에서 사용되는 특정 애플리케이션과 관련된 개체입니다. 이 개체는 자동으로 생성됩니다.
- **NSG(Network Service Group)** - 네트워크 서비스 그룹은 방화벽에서 설정을 기반으로 경로를 결정하는 데 사용하는 애플리케이션 그룹입니다. 여러 네트워크 서비스 개체가 단일 NSG의 일부일 수 있습니다. 관리 센터는 정책 기반 라우팅을 위해 구성된 확장된 액세스 목록을 기반으로 NSG를 자동 생성합니다.

모범 사례

- Secure Firewall Threat Defense는 버전 7.1 이상을 실행해야 합니다.
- 애플리케이션 트래픽 흐름을 지원하기 위해 신뢰할 수 있는 DNS 서버를 통해 DNS 스누핑이 수행되도록 하려면 신뢰할 수 있는 DNS 서버를 구성해야 합니다.
- Threat Defense를 통과하는 DNS 요청은 DNS 스누핑을 통해 PBR 플로우를 지원하도록 암호화되지 않은 일반 텍스트 형식이어야 합니다.
- 애플리케이션 트래픽의 활성/활성 로드 밸런싱을 위해 ECMP 영역을 구성해야 합니다.
- ECMP는 라우팅 방화벽 모드에서만 지원되며, 디바이스는 최대 256개의 ECMP 영역을 가질 수 있습니다.
- 라우팅 인터페이스만 사용해야 합니다. 각 인터페이스는 단일 ECMP 영역에만 속해야 합니다.
- 인터페이스가 ECMP가 구성되는 가상 라우터에 속해 있는지 확인하십시오.
- ECMP 영역 설정에 사용된 인터페이스에는 인터페이스 설정 내에 논리적 이름이 정의되어 있어야 합니다.
- Secure Firewall Threat Defense에서 PBR에 대해 ECMP 영역당 8개의 인터페이스가 구성되어 있는지 확인합니다.
- PBR은 이 모드에서 지원되지 않으므로 Secure Firewall Threat Defense는 클러스터에 구축해서는 안 됩니다.
- PBR은 사용자 정의 가상 라우터에서 지원되지 않으므로 전역 가상 라우터에 대해 구성해야 합니다.
- PBR 내 인그레스 및 이그레스 인터페이스에 사용되는 인터페이스가 라우팅된 인터페이스 또는 관리 전용이 아닌 인터페이스이고, 전역 가상 라우터에 속해 있는지 확인합니다.

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

시나리오 1: 직접 인터넷 액세스

Bob은 어카운트 매니저이고 Ann은 헬프데스크 전문가입니다. 두 사람은 모두 대기업의 브랜치 오피스에서 근무합니다. 최근에는 Webex와 같은 웹 컨퍼런싱 툴 및 YouTube 같은 스트리밍 플랫폼을 사용하면서 레이턴시 문제를 경험하고 있습니다.

어떤 위험이 있습니까**?**

네트워크 레이턴시 및 네트워크 혼잡으로 인해 웹 컨퍼런싱 및 스트리밍 세션의 성능 및 사용자 경험이 감소합니다. 이는 브랜치 오피스 직원의 생산성과 효율성에 영향을 미쳐 전체 비즈니스 운영에 부정적인 영향을 미칠 수 있습니다.

PBR이 있는 **DIA**는 이 문제를 어떻게 해결합니까**?**

IT 관리자인 Alice는 네트워크의 레이턴시를 줄이기 위해 DIA와 함께 정책 기반 라우팅을 사용했습니다.

직접 인터넷 액세스를 사용하면 브랜치 오피스가 중앙 사이트나 데이터 센터를 통해 트래픽을 라우팅하지 않고 직접 인터넷에 액세스할 수 있습니다. 그 결과 브랜치 사용자에게 더욱 직접적이고 최적화된 인터넷 연결을 제공하여 레이턴시를 줄였습니다.

정책 기반 라우팅은 서로 다른 이그레스 인터페이스에서 Webex 트래픽과 YouTube 트래픽을 분리했습니다. 이를 통해 트래픽이 다른 경로를 통해 전달되어 단일 인터페이스에 대한 부담이 감소하고 애플리케이션 성능이 향상되었습니다.

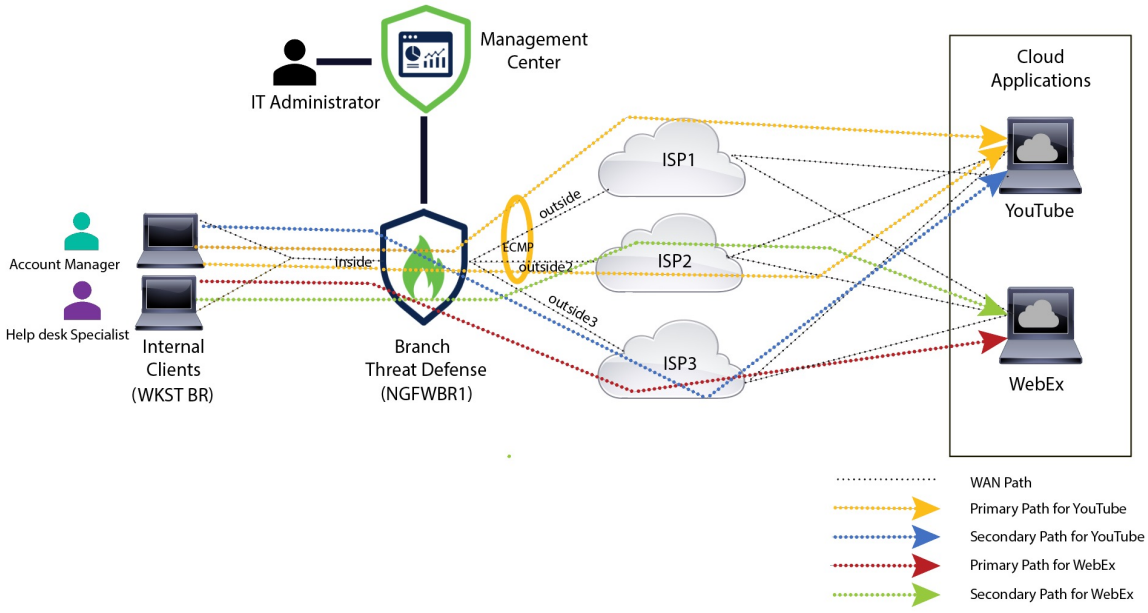
DIA용 네트워크 토폴로지

이 토폴로지에서 위협 방어 디바이스는 3개의 이그레스 인터페이스가 있는 브랜치 위치에 구축됩니다. 디바이스가 PBR을 사용하여 DIA에 대해 구성됩니다.

아래 그림에서 내부 클라이언트 또는 브랜치 워크스테이션은 **WKST BR** 레이블로 표시되고 브랜치 위협 방어는 **NGFWBR1** 레이블로 표시됩니다. **NGFWBR1**의 인그레스 인터페이스는 **inside**로 이름이 지정되고 이그레스 인터페이스는 **outside**, **outside2**, **outside3**으로 각각 지정됩니다.

outside 및 **outside2** 인터페이스 간의 로드 밸런싱은 ECMP 영역 및 정적 경로를 구성하여 수행합니다.

그림 2: 직접 인터넷 액세스 토폴로지

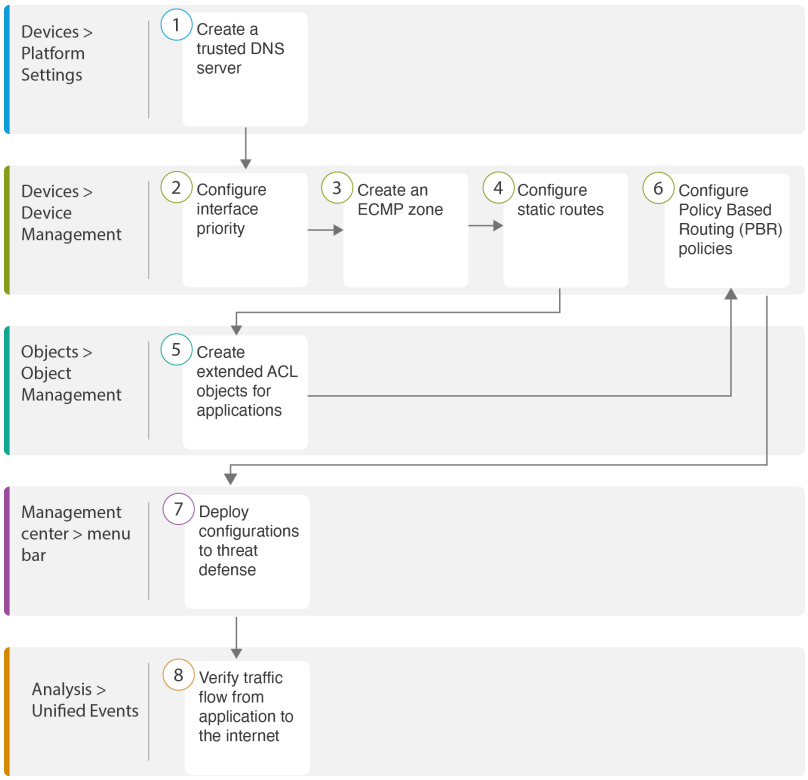


DIA를 사용하면 브랜치 방화벽 뒤에 있는 사용자가 다음에 액세스할 수 있습니다.

1. 2개의 이그레스 인터페이스(**outside** 및 **outside2**)를 사용하여 로드 밸런싱되는 소셜 미디어 애플리케이션 트래픽(예: **YouTube**). 두 인터페이스 모두에서 장애가 발생하면 트래픽은 세 번째 이그레스 인터페이스(**outside3**)로 폴백됩니다.
2. 협업 애플리케이션 트래픽(예: **WebEx**)은 **outside3** 인터페이스를 통해 전달되며 이 링크에 장애가 발생하면 트래픽은 **outside2** 인터페이스를 통해 전달됩니다.

DIA 구성을 위한 엔드 투 엔드 절차

다음 순서도에는 Secure Firewall Management Center에서 DIA 설정을 위한 워크플로우가 나와 있습니다.



단계	설명
1	(사전 요건) 신뢰할 수 있는 DNS 서버를 구성합니다. 신뢰할 수 있는 DNS 서버 구성, 43 페이지의 내용을 참조하십시오.
2	(사전 요건) 인터페이스 우선순위를 구성합니다. 인터페이스 우선순위 설정, 44 페이지의 내용을 참조하십시오.
3	(사전 요건) ECMP 영역을 생성합니다. ECMP 영역 생성, 44 페이지의 내용을 참조하십시오.
4	(사전 요건) 정적 경로를 구성합니다. 동일 비용 정적 경로 구성, 45 페이지의 내용을 참조하십시오.
5	애플리케이션의 확장 ACL 개체를 구성합니다. 확인 • YouTube의 확장 ACL 개체 구성, 46 페이지 • WebEx의 확장 ACL 개체 구성, 47 페이지
6	애플리케이션의 PBR 정책을 구성합니다. 확인 • YouTube용 정책 기반 라우팅 정책 구성, 47 페이지 • WebEx에 대한 정책 기반 라우팅 정책 구성, 48 페이지

단계	설명
7	구성을 위협 방어에 구축합니다. 컨피그레이션 구축, 51 페이지의 내용을 참조하십시오.
8	YouTube 및 WebEx 트래픽 흐름을 확인합니다. 애플리케이션 트래픽 흐름 확인, 51 페이지의 내용을 참조하십시오.

시나리오 2: 경로 모니터링을 사용한 직접 인터넷 액세스

Ann은 헬프데스크 전문가이며 대기업의 지사에서 근무합니다. Ann은 WebEx를 사용하는 동안 연결이 끊기고 지연이 발생하는 문제를 경험했습니다.

어떤 위험이 있습니까?

WebEx 미팅은 미팅 호스트와 참석자 간의 오디오 및 비디오 스트림을 포함한 실시간 데이터 전송을 사용합니다. 이 실시간 데이터는 네트워크 레이턴시 및 패킷 손실에 민감합니다. 네트워크에서 높은 패킷 손실이 발생하는 경우, 중단, 지연과 같은 오디오 및 비디오 품질 문제가 발생하여 미팅 경험에 부정적인 영향을 줄 수 있습니다.

경로 모니터링 기능이 있는 **PBR**이 문제를 어떻게 해결합니까?

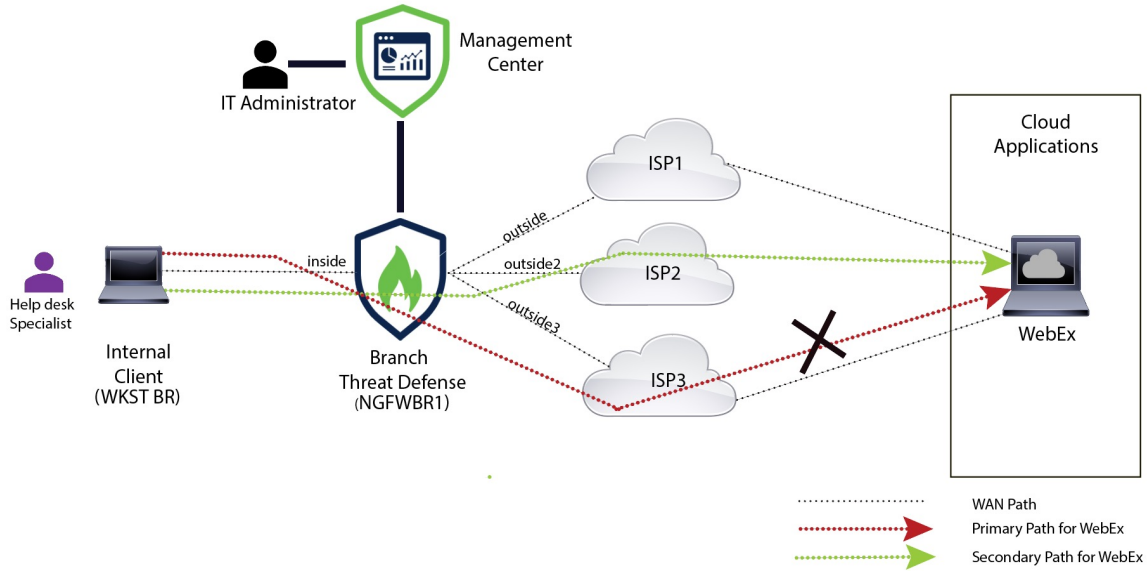
IT 관리자인 Grace는 경로 모니터링이 있는 정책 기반 라우팅을 사용하여 최소한의 패킷 손실로 이그레스 인터페이스를 통해 인터넷으로 WebEx 애플리케이션 트래픽을 조정하여 참석자에게 최상의 미팅 경험을 보장했습니다.

네트워크 토폴로지-DIA(경로 모니터링 포함)

이 토폴로지에서 위협 방어 디바이스는 3개의 이그레스 인터페이스가 있는 브랜치 위치에 구축됩니다. 디바이스가 정책 기반 라우팅을 사용하는 직접 인터넷 액세스용으로 구성되어 있습니다.

아래 그림에서 내부 클라이언트 또는 브랜치 워크스테이션은 **WKST BR** 레이블로 표시되고 브랜치 위협 방어는 **NGFWBR1** 레이블로 표시됩니다. **NGFWBR1**의 인그레스 인터페이스는 **inside**로 이름이 지정되고 이그레스 인터페이스는 **outside**, **outside2**, **outside3**으로 각각 지정됩니다.

그림 *3:* 직접 인터넷 액세스 토폴로지*(*경로 모니터링 사용*)*



outside2 및 **outside3** 이그레스 인터페이스는 경로 모니터링을 통해 활성화됩니다. WebEx용 PBR 정책은 최소한의 패킷 손실로 트래픽이 이그레스 인터페이스로 라우팅되도록 구성됩니다.

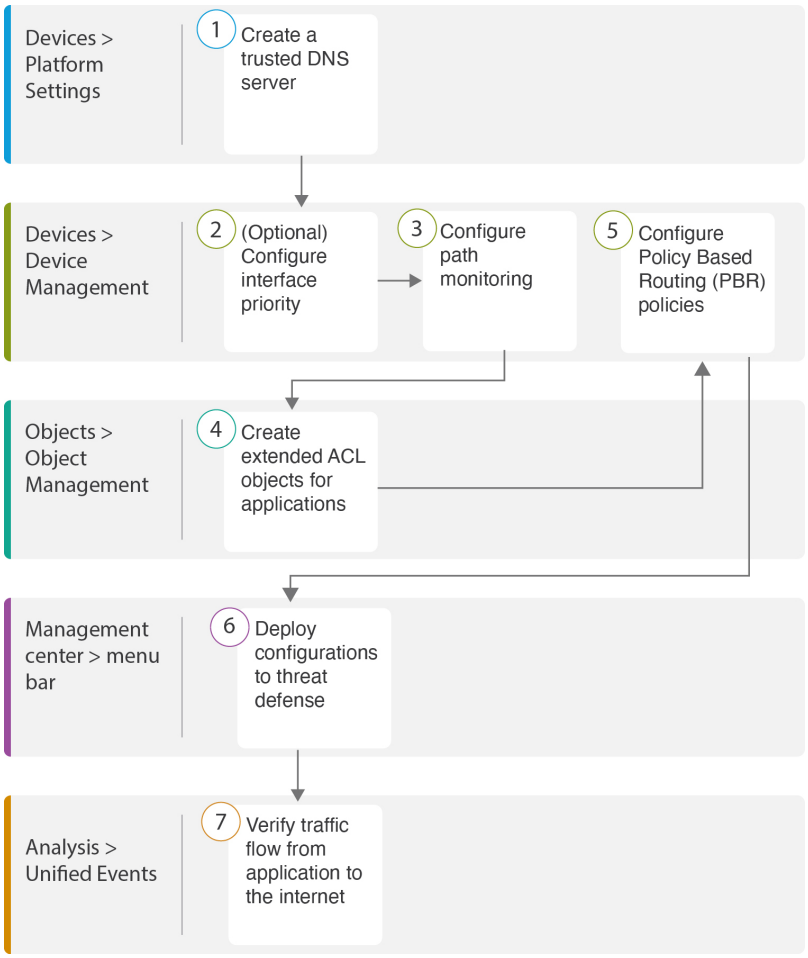
이 시나리오에서는 경로 모니터링을 검증하기 위해 업스트림 디바이스의 액세스 제어 목록을 통해 인터넷으로 이동하는 **outside3** 인터페이스에서 소싱되는 아웃바운드 트래픽을 제한하거나 Firewall Management Center에서 Secure Firewall Threat Defense에 대한 **outside3** 인터페이스를 종료하여 패킷 손실을 유발할 수 있습니다.

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

패킷 손실의 결과로 **outside3** 인터페이스와 연결된 링크가 중단됩니다. 협업 애플리케이션 트래픽은 **outside3** 인터페이스 대신 **outside2** 인터페이스를 통해 전달됩니다.

경로 모니터링을 통해 DIA를 구성하기 위한 엔드 투 엔드 절차

다음 순서도에는 Secure Firewall Management Center에서 경로 모니터링을 사용하여 DIA를 설정하는 워크플로우가 나와 있습니다.



단계	설명
1	(사전 요건) 신뢰할 수 있는 DNS 서버를 구성합니다. 신뢰할 수 있는 DNS 서버 구성, 43 페이지의 내용을 참조하십시오.
2	[사전 요건 (선택 사항)] 인터페이스 우선순위를 구성합니다. 인터페이스 우선순위 설정, 44 페이지의 내용을 참조하십시오.
3	경로 모니터링을 구성합니다. 경로 모니터링 설정 구성, 45 페이지의 내용을 참조하십시오.
4	애플리케이션의 확장 ACL 개체를 구성합니다. WebEx의 확장 ACL 개체 구성, 47 페이지의 내용을 참조하십시오.
5	애플리케이션에 대한 PBR 정책을 구성합니다. Webex용 경로 모니터링을 사용하여 정책 기반 라우팅 정책 구성, 49 페이지의 내용을 참조하십시오.
6	구성을 위협 방어에 구축합니다. 컨피그레이션 구축, 51 페이지의 내용을 참조하십시오.

단계	설명
7	WebEx 트래픽 흐름을 확인합니다. 애플리케이션 트래픽 흐름 확인, 51 페이지의 내용을 참조하십시오.

신뢰할 수 있는 DNS 서버 구성

직접 인터넷 액세스 기능의 애플리케이션 탐지는 DNS 스누핑을 사용하여 애플리케이션 또는 애플리케이션 그룹을 탐지하기 위해 애플리케이션 도메인을 IP에 매핑합니다. DNS 요청이 비인가 DNS 서버에 의해 확인되지 않고 실제로 원하는 DNS 서버에 잠기도록 Cisco Secure Firewall Management Center를 사용하여 Cisco Secure Firewall Threat Defense에 신뢰할 수 있는 DNS 서버를 구성할 수 있습니다. 따라서 방화벽은 신뢰할 수 있는 DNS 서버로 이동하는 트래픽만 스누핑합니다. 신뢰할 수 있는 DNS 서버를 구성하는 것 외에도 DNS 서버 그룹, DHCP 풀, DHCP 릴레이 및 DHCP 클라이언트에 이미 구성된 서버를 신뢰할 수 있는 DNS 서버로 포함할 수 있습니다.

Trusted DNS Servers(신뢰할 수 있는 DNS 서버) 탭을 사용하여 DNS 스누핑에 대해 신뢰할 수 있는 DNS 서비스를 구성할 수 있습니다.

참고 애플리케이션 기반 PBR의 경우 신뢰할 수 있는 DNS 서버를 구성해야 합니다. 또한 도메인을 확인하여 애플리케이션을 탐지할 수 있도록 DNS 트래픽이 일반 텍스트 형식(암호화된 DNS는 지원하지 않음)으로 위협 방어를 통과하는지 확인해야 합니다.

시작하기 전에

- 하나 이상의 DNS 서버 그룹을 만들었는지 확인합니다. 자세한 내용은 DNS 서버 그룹 개체 생성을 참조하십시오.
- DNS 서버에 연결할 인터페이스 개체를 생성했는지 확인합니다.
- 관리 디바이스에 DNS 서버에 액세스하기 위한 적절한 정적 또는 동적 경로가 있는지 확인합니다.

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 위협 방어 정책을 편집합니다.

단계 **2** **Edit(**수정**)** (✎) 아이콘을 클릭합니다.

단계 **3** **DNS**를 클릭합니다.

단계 **4** 신뢰할 수 있는 DNS 서버를 구성하려면 **Trusted DNS Servers(**신뢰할 수 있는 **DNS** 서버**)** 탭을 클릭합니다.

단계 **5** 기존 호스트 개체에서 **DNS_Server**를 선택하려면 **Available Host Objects(**사용 가능한 호스트 개체**)**에서 검색 필드를 사용하여 해당 호스트를 검색하고 **Add(**추가**)**를 클릭하여 **Selected DNS Servers(**선택한 **DNS** 서버**)** 목록에 포함합니다.

참고 **DNS_Server**는 이 예에 구성된 DNS 서버입니다.

단계 **6** **Save(**저장**)**를 클릭합니다. 추가된 DNS 서버가 **Trusted DNS Servers(**신뢰할 수 있는 **DNS** 서버**)** 페이지에 표시됩니다.

단계 **7** **NGFWBR1**이 **Selected Devices(**선택한 디바이스**)** 목록에 이미 있는지 확인하려면 **Policy Assignments(**정책 할당**)**를 클릭합니다.

단계 **8** **OK(**확인**)**를 클릭하여 변경 사항을 확인합니다.

단계 **9** 플랫폼 설정에 대한 변경 사항을 기록하려면 **Save(**저장**)**를 클릭합니다.

인터페이스 우선순위 설정

Cisco Secure Firewall Threat Defense는 인터페이스 우선순위를 사용하여 최적의 인터넷 경로를 결정합니다. 우선순위의 범위는 0~65535이며, 트래픽을 인터넷으로 전송할 때 특정 ISP의 우선순위를 결정합니다. 인터페이스의 우선순위에 따라 트래픽이 전달됩니다. 트래픽은 우선 순위 값이 가장 낮은 인터페이스로 라우팅됩니다. 인터페이스를 사용할 수 없는 경우 트래픽은 다음으로 낮은 우선순위 값을 가진 인터페이스로 전달됩니다. 예를 들어 outside2 및 outside3가 우선 순위 값 10과 20으로 각각 설정되어 있다고 가정합니다. 트래픽은 outside2로 전달됩니다. outside2를 사용할 수 없게 되면 트래픽은 outside3으로 전달됩니다.

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** **Policy Based Routing(**정책 기반 라우팅**)**을 클릭합니다.

단계 **4** **Configure Interface Priority(**인터페이스 우선순위 구성**)**를 클릭합니다.

단계 **5** 대화 상자에서 인터페이스에 대한 우선순위 번호를 입력합니다.

모든 인터페이스에 대해 우선순위 값이 동일한 경우 트래픽이 인터페이스 간에 균형을 이룹니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

ECMP 영역 생성

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-WAN**을 입력합니다.

단계 **6** 인터페이스를 연결하려면 **Available Interface(**사용 가능한 인터페이스**)** 상자에서 인터페이스를 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

이제 ECMP 페이지에 새로 생성된 ECMP 영역이 표시됩니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

동일 비용 정적 경로 구성

전역 및 사용자 정의 가상 라우터의 인터페이스를 디바이스의 ECMP 영역에 할당할 수 있습니다.

시작하기 전에

- 인터페이스에 대해 동일 비용 고정 경로를 구성하려면 이를 ECMP 영역과 연결해야 합니다. ECMP 영역 생성, 44 페이지의 내용을 참조하십시오.
- 인터페이스를 ECMP 영역과 연결하지 않고는 대상 및 메트릭이 동일한 인터페이스에 대해 정적 경로를 정의할 수 없습니다.

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

단계 **2** 라우팅 탭을 클릭합니다.

단계 **3** 드롭다운 목록에서 인터페이스가 ECMP 영역과 연결된 가상 라우터를 선택합니다.

단계 **4** 인터페이스에 대해 동일 비용 고정 경로를 구성하려면 **Static Route(**고정 경로**)**를 클릭합니다.

단계 **5** **Add Route(**경로 추가**)**를 클릭하여 새 경로를 추가하거나 기존 경로에 대해 **Edit(**수정**)** ( )를 클릭합니다.

단계 **6** **Interface(**인터페이스**)** 드롭다운에서 가상 라우터 및 ECMP 영역에 속한 인터페이스를 선택합니다.

단계 **7** **Available Networks(**사용 가능한 네트워크**)** 상자에서 대상 네트워크를 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **8** 네트워크의 게이트웨이를 입력합니다.

단계 **9** 메트릭 값을 입력합니다. 1~254 범위의 숫자일 수 있습니다.

단계 **10** 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

단계 **11** 동일 비용 고정 라우팅을 구성하려면 동일한 대상 네트워크 및 메트릭 값을 사용하여 동일한 ECMP 영역에서 다른 인터페이스에 대한 고정 경로를 구성하는 단계를 반복합니다. 다른 게이트웨이를 제공해야 합니다.

경로 모니터링 설정 구성

PBR 정책은 트래픽에 가장 적합한 라우팅 경로를 식별하기 위해 인터페이스의 RTT(왕복 시간), 지터, MOS(평균 의견 점수) 및 패킷 손실과 같은 유연한 메트릭을 사용합니다. 경로 모니터링은 지정된

인터페이스에서 이러한 메트릭을 수집합니다. **Interfaces(**인터페이스**)** 페이지에서 메트릭 수집을 위해 프로브를 전송하도록 경로 모니터링에 대한 설정을 사용하여 인터페이스를 구성할 수 있습니다.

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 위협 방어 디바이스(**NGFWBR1**)에 대한 **Edit(**수정**)** (✎)를 클릭합니다.

단계 **2** 편집할 인터페이스의 **Edit(**수정**)** (✎)을 클릭합니다(외부).

단계 **3** **Path Monitoring(**경로 모니터링**)** 탭을 클릭합니다.

단계 **4** **Enable IP based Path Monitoring(IP** 기반 경로 모니터링 활성화**)** 확인란을 선택합니다.

단계 **5** **Monitoring Type(**모니터링 유형**)** 드롭다운 목록에서 관련 옵션을 선택합니다. 이 예시에서는 기본값인 인터페이스에서 기본 경로의 다음 홉**(**자동**)**을 사용합니다.

단계 **6** **Ok(**확인**)**를 클릭합니다.

단계 **7** **outside2** 및 **outside3** 인터페이스에 대해 2 ~ 8단계를 반복합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

YouTube의 확장 ACL 개체 구성

YouTube 트래픽이 정책 기반 라우팅을 사용하여 다른 이그레스 인터페이스에서 인터넷으로 향하도록 조정되도록 액세스 목록이 구성됩니다.

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하고 목차에서 **Access Lists(**액세스 목록**)** > **Extended(**확장**)**를 선택합니다.

단계 **2** **Add Extended Access List(**확장된 액세스 목록 추가**)**를 클릭하여 소셜 미디어 트래픽에 대한 확장된 액세스 목록을 생성합니다.

단계 **3** Extended ACL Object(확장된 ACL 개체) 대화 상자에서 개체의 이름(**DIA_SocialMedia**)을 입력합니다.

단계 **4** **Add(**추가**)**를 클릭하여 새 확장된 액세스 목록을 생성합니다.

단계 **5** 다음 액세스 제어 속성을 구성합니다.

1. 작업을 선택하여 트래픽 조건을 허용(일치)합니다.
2. **Application(**애플리케이션**)** 탭을 클릭하고 **Available Applications(**사용 가능한 애플리케이션**)** 목록에서 **YouTube**를 검색합니다.
3. **YouTube**를 선택하고 **Add to Rule(**규칙에 추가**)**을 클릭합니다.
4. 개체에 해당 항목을 추가하려면 **Add(**추가**)**를 클릭합니다.
5. **Save(**저장**)**를 클릭합니다.

WebEx의 확장 ACL 개체 구성

WebEx 트래픽이 정책 기반 라우팅을 사용하여 다른 이그레스 인터페이스에서 인터넷으로 향하도록 조정되도록 액세스 목록이 구성됩니다.

단계 **1** **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하고 목차에서 **Access Lists(**액세스 목록**)** > **Extended(**확장**)**를 선택합니다.

단계 **2** **Add Extended Access List(**확장된 액세스 목록 추가**)**를 클릭하여 협업 트래픽에 대한 확장된 액세스 목록을 생성합니다.

단계 **3** Extended ACL Object(확장된 ACL 개체) 대화 상자에서 개체의 이름(**DIA_Collaboration**)을 입력합니다.

단계 **4** **Add(**추가**)**를 클릭하여 새 확장된 액세스 목록을 생성합니다.

단계 **5** 다음 액세스 제어 속성을 구성합니다.

1. 작업을 선택하여 트래픽 조건을 허용(일치)합니다.
2. **Application(**애플리케이션**)** 탭을 클릭하고 **Available Applications(**사용 가능한 애플리케이션**)** 목록에서 **Webex**를 검색합니다.
3. **Webex**를 선택하고 **Add to Rule(**규칙에 추가**)**을 클릭합니다.
4. 개체에 해당 항목을 추가하려면 **Add(**추가**)**를 클릭합니다.
5. **Save(**저장**)**를 클릭합니다.

YouTube용 정책 기반 라우팅 정책 구성

YouTube 트래픽을 라우팅할 인그레스 인터페이스, 일치 기준(확장된 액세스 제어 목록) 및 이그레스 인터페이스를 지정하여 Policy Based Routing(정책 기반 라우팅) 페이지에서 PBR 정책을 구성할 수 있습니다.

YouTube 트래픽은 **outside** 및 **outside2** 인터페이스 간에 로드 밸런싱되고 두 링크 모두 실패하면 **outside3**으로 폴백됩니다.

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** **Policy Based Routing(**정책 기반 라우팅**)**을 클릭합니다.

Policy Based Routing(정책 기반 라우팅) 페이지에 구성된 정책이 표시됩니다. 그리드에 인그레스 인터페이스 목록과 정책 기반 경로 액세스 목록 및 이그레스 인터페이스의 조합이 표시됩니다.

단계 **4** 정책을 구성하려면 **Add(**추가**)**를 클릭합니다.

단계 **5** **Add Policy Based Route(**정책 기반 경로 추가**)** 대화 상자의 **Ingress Interface(**인그레스 인터페이스**)** 드롭다운 목록에서 **inside**를 선택합니다.

참고 논리적 이름이 있고 전역 가상 라우터에 속하는 인터페이스만 드롭다운에 나열됩니다.

단계 **6** 정책에서 일치 기준 및 전달 작업을 지정하려면 **Add(**추가**)**를 클릭합니다.

단계 **7** **Add Forwarding Actions(**전달 작업 추가**)** 대화 상자에서 다음을 수행합니다.

a) **Match ACL(ACL** 일치**)** 드롭다운에서 **DIA_SocialMedia**를 선택합니다.

b) 구성된 인터페이스를 선택하려면 **Send To(**전송 대상**)** 드롭다운 목록에서 **Egress Interfaces(**이그레스 인터페이스**)**를 선택합니다.

c) **Interface Ordering(**인터페이스 순서 지정**)** 드롭다운 목록에서 **By Priority(**우선순위별**)**를 선택합니다.

트래픽은 우선 순위 값이 가장 낮은 인터페이스로 라우팅됩니다. 인터페이스를 사용할 수 없는 경우 트래픽은 다음으로 낮은 우선순위 값을 가진 인터페이스로 전달됩니다. 예를 들어 outside2 및 outside3가 우선 순위 값 10과 20으로 각각 설정되어 있다고 가정합니다. 트래픽은 outside2로 전달됩니다. outside2를 사용할 수 없게 되면 트래픽은 outside3으로 전달됩니다.

d) **Available Interfaces(**사용 가능한 인터페이스**)** 상자에 우선순위 값과 함께 모든 인터페이스가 나열됩니다. **Add(**추가**)** (+) 아이콘을 클릭하여 선택한 이그레스 인터페이스를 추가합니다.

이 시나리오의 경우:

1. Available Interfaces(사용 가능한 인터페이스)에서 **outside** 및 **outside2** 인터페이스에 인접한 **Add(**추가**)** (+) 아이콘을 클릭하여 이를 **Selected Egress Interfaces(**선택한 이그레스 인터페이스**)**로 이동합니다.

2. 그런 다음 **outside3** 인터페이스 옆의 **Add(**추가**)** (+) 아이콘을 클릭하여 이를 **Selected Egress Interfaces(**선택한 이그레스 인터페이스**)**로 이동합니다.

e) **Save(**저장**)**를 클릭하여 일치 기준에 대한 변경 사항을 기록합니다.

f) 구성을 검토하고 **Save(**저장**)**를 클릭하여 정책 기반 라우팅에 대한 모든 구성 변경 사항을 씁니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

WebEx에 대한 정책 기반 라우팅 정책 구성

WebEx 애플리케이션 트래픽을 라우팅할 인그레스 인터페이스, 일치 기준(확장된 액세스 제어 목록) 및 이그레스 인터페이스를 지정하여 Policy Based Routing(정책 기반 라우팅) 페이지에서 PBR 정책을 구성할 수 있습니다.

WebEx 애플리케이션 트래픽은 **outside3**으로 라우팅되고 기본 링크가 실패하면 **outside2**로 폴백됩니다.

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** **Policy Based Routing(**정책 기반 라우팅**)**을 클릭합니다.

Policy Based Routing(정책 기반 라우팅) 페이지에 구성된 정책이 표시됩니다. 그리드에 인그레스 인터페이스 목록과 정책 기반 경로 액세스 목록 및 이그레스 인터페이스의 조합이 표시됩니다.

단계 **4** 정책을 편집하려면 **Edit(**수정**)** (✎) 아이콘을 클릭합니다.

단계 **5** 정책에서 일치 기준 및 전달 작업을 지정하려면 **Add(**추가**)**를 클릭합니다.

단계 **6** **Add Forwarding Actions(**전달 작업 추가**)** 대화 상자에서 다음을 수행합니다.

a) **Match ACL(ACL** 일치**)** 드롭다운에서 **DIA_Coloperation**을 선택합니다.

b) 구성된 인터페이스를 선택하려면 **Send To(**전송 대상**)** 드롭다운 목록에서 **Egress Interfaces(**이그레스 인터페이스**)**를 선택합니다.

c) **Interface Ordering(**인터페이스 순서 지정**)** 드롭다운 목록에서 **Order(**순서**)**를 선택합니다.

여기에 지정된 인터페이스의 순서에 따라 트래픽이 전달됩니다.

d) **Available Interfaces(**사용 가능한 인터페이스**)** 상자에 우선순위 값과 함께 모든 인터페이스가 나열됩니다. **Add(**추가**)** (+) 아이콘을 클릭하여 선택한 이그레스 인터페이스를 추가합니다.

이 시나리오의 경우:

1. Available Interfaces(사용 가능한 인터페이스)에서 **outside3** 인터페이스 옆의 **Add(**추가**)** (+) 아이콘을 클릭하여 이를 **Selected Egress Interfaces(**선택한 이그레스 인터페이스**)**로 이동합니다.
2. 그런 다음 **outside2** 인터페이스에 인접한 **Add(**추가**)** (+) 아이콘을 클릭하여 **Selected Egress Interfaces(**선택한 이그레스 인터페이스**)**로 이동합니다.

e) **Save(**저장**)**를 클릭하여 일치 기준에 대한 변경 사항을 기록합니다.

f) 구성을 검토하고 **Save(**저장**)**를 클릭하여 정책 기반 라우팅에 대한 모든 구성 변경 사항을 씁니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

Webex용 경로 모니터링을 사용하여 정책 기반 라우팅 정책 구성

Policy Based Routing(정책 기반 라우팅) 페이지에서 경로 모니터링을 사용하여 PBR 정책을 구성할 수 있습니다. 이 예에서 WebEx 애플리케이션 트래픽은 트래픽 손실이 가장 적은 인터페이스에 전달됩니다.

시작하기 전에

이그레스 인터페이스에 대한 트래픽 전달 우선순위를 구성하기 위해 경로 모니터링 메트릭을 사용하려면 인터페이스에 대한 경로 모니터링 설정을 구성해야 합니다. 경로 모니터링 설정 구성, 45 페이지의 내용을 참조하십시오.

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** **Policy Based Routing(**정책 기반 라우팅**)**을 클릭합니다.

Policy Based Routing(정책 기반 라우팅) 페이지에 구성된 정책이 표시됩니다. 그리드에 인그레스 인터페이스 목록과 정책 기반 경로 액세스 목록 및 이그레스 인터페이스의 조합이 표시됩니다.

단계 **4** 정책을 구성하려면 **Add(**추가**)**를 클릭합니다.

단계 **5** **Add Policy Based Route(**정책 기반 경로 추가**)** 대화 상자의 **Ingress Interface(**인그레스 인터페이스**)** 드롭다운 목록에서 **inside**를 선택합니다.

참고 논리적 이름이 있고 전역 가상 라우터에 속하는 인터페이스만 드롭다운에 나열됩니다.

단계 **6** 정책에서 일치 기준 및 전달 작업을 지정하려면 **Add(**추가**)**를 클릭합니다.

단계 **7** **Add Forwarding Actions(**전달 작업 추가**)** 대화 상자에서 다음을 수행합니다.

a) **Match ACL(ACL** 일치**)** 드롭다운에서 **DIA_Coloperation**을 선택합니다.

b) 구성된 인터페이스를 선택하려면 **Send To(**전송 대상**)** 드롭다운 목록에서 **Egress Interfaces(**이그레스 인터페이스**)**를 선택합니다.

c) **Interface Ordering(**인터페이스 순서 지정**)** 드롭다운 목록에서 **Minimal Packet Loss(**최소 패킷 손실**)**를 선택합니다.

트래픽이 패킷 손실이 최소인 인터페이스로 전달됩니다.

d) **Available Interfaces(**사용 가능한 인터페이스**)** 상자에 모든 인터페이스가 나열됩니다. 인터페이스 목록에서 **Add(**추가**)** (+) 아이콘을 클릭하여 선택한 이그레스 인터페이스를 추가합니다.

이 시나리오의 경우:

1. Available Interfaces(사용 가능한 인터페이스)에서 **outside3** 인터페이스 옆의 **Add(**추가**)** (+) 아이콘을 클릭하여 이를 **Selected Egress Interfaces(**선택한 이그레스 인터페이스**)**로 이동합니다.
2. 그런 다음 **outside2** 인터페이스에 인접한 **Add(**추가**)** (+) 아이콘을 클릭하여 **Selected Egress Interfaces(**선택한 이그레스 인터페이스**)**로 이동합니다.

e) **Save(**저장**)**를 클릭하여 일치 기준에 대한 변경 사항을 기록합니다.

f) 구성을 검토하고 **Save(**저장**)**를 클릭하여 정책 기반 라우팅에 대한 모든 구성 변경 사항을 씁니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

컨피그레이션 구축

모든 구성을 완료한 후 매니지드 디바이스에 구축합니다.

단계 **1** 관리 센터 메뉴 바에서 **Deploy(**구축**)**를 클릭합니다.

단계 **2** 구성 변경 사항을 구축할 NGFWBR1 옆의 확인란을 선택합니다.

단계 **3** **Deploy(**구축**)**를 클릭합니다.

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.

애플리케이션 트래픽 흐름 확인

단계 **1** 관리 센터 인터페이스에서 **Analysis(**분석**) - Unified Events(**통합 이벤트**)**를 선택합니다.

단계 **2** **Web Application(**웹 애플리케이션**)** 및 **Egress Interface(**이그레스 인터페이스**)**를 선택하고 **Apply(**적용**)**를 클릭하여 열 선택기를 사용하여 열을 맞춤화합니다.

단계 **3** 쉽게 확인할 수 있도록 열 순서를 변경합니다.

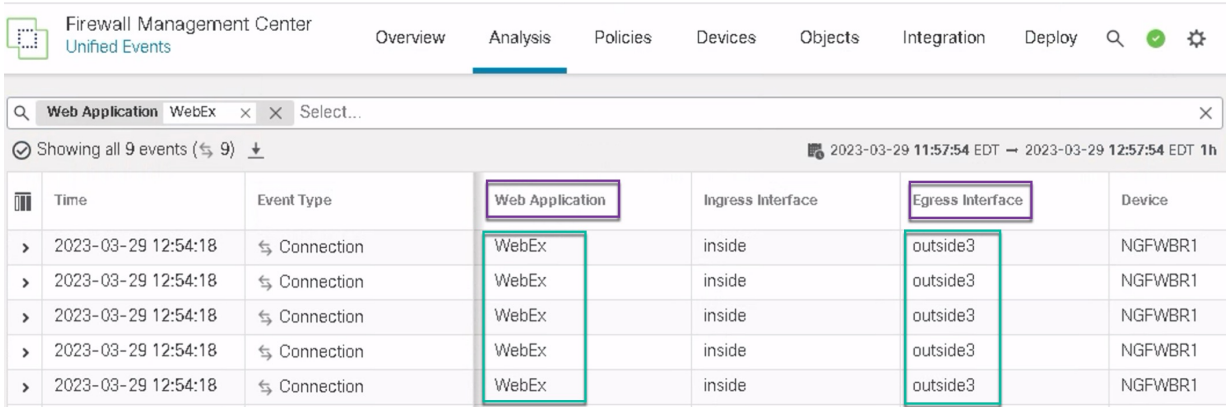
단계 **4** **Web Application(**웹 애플리케이션**)** 필터 내에서 **WebEx** 이름을 입력하고 **Apply(**적용**)**를 클릭합니다.

단계 **5** **Web Application(**웹 애플리케이션**)** 필터 내에서 **YouTube** 이름을 입력하고 **Apply(**적용**)**를 클릭합니다.

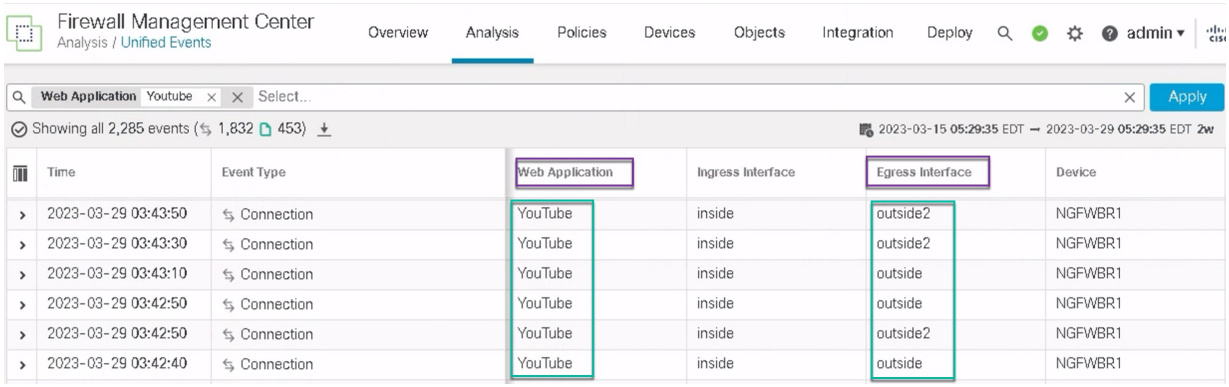
단계 **6** Secure Firewall 뒤에 있는 호스트에서 **YouTube** 및 **WebEx** 애플리케이션에 대한 트래픽을 시작합니다. 이 시나리오에서는 Google Chrome 브라우저를 실행하고 https://youtube.com으로 이동한 다음 브랜치 워크스테이션 **WKST BR1**의 다른 탭에 있는 https://webex.com으로 이동합니다.

단계 **7** 관리 센터에서 두 애플리케이션의 트래픽 흐름을 확인합니다.

1. DIA의 경우:
   - **WebEx** 애플리케이션 트래픽은 아래 그림에 표시된 것과 같이 설정에 따라 **outside3** 인터페이스를 통해 전송됩니다.

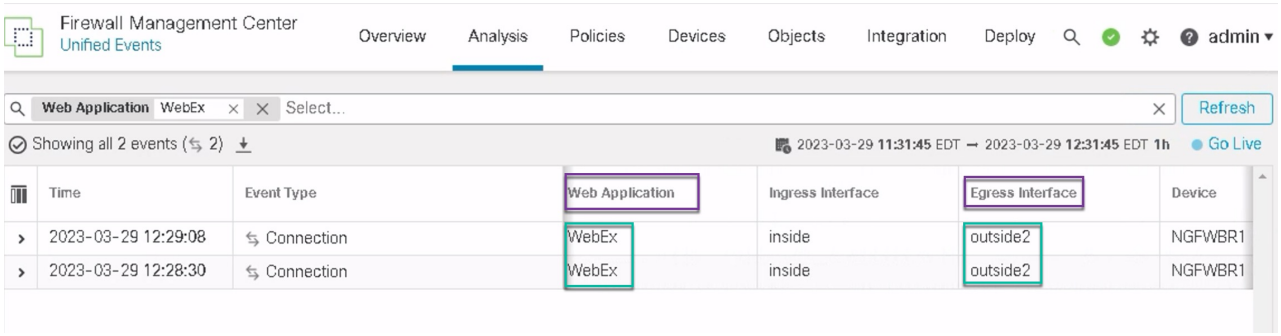


- **YouTube** 애플리케이션 트래픽은 아래 그림에 표시된 설정에 따라 **outside** 및 **outside2** 인터페이스 사이에서 로드 밸런싱됩니다.



2. 경로 모니터링을 사용하는 DIA의 경우:

   아래 그림에서 볼 수 있듯이 **outside3** 인터페이스에서 패킷 손실이 있으므로 **WebEx** 애플리케이션 트래픽은 **outside2** 인터페이스를 통해 전송됩니다.



정책 기반 라우팅 모니터링 및 문제 해결

구축 후 다음 CLI를 사용하여 Secure Firewall Threat Defense에서 정책 기반 라우팅과 관련된 문제를 모니터링하고 해결합니다.

방법	**CLI** 명령
Secure Firewall Threat Defense Lina CLI에 로그인하는 방법	**system support diagnostic-cli**
구축 중에 관리 센터에서 위협 방어로 푸시된 사전 정의된 네트워크 서비스 개체를 보는 방법	• **show object network-service** • **show object network-service detail**
설정된 애플리케이션과 관련된 특정 NSG(네트워크 서비스 개체) 보는 방법	• **show object id YouTube** • **show object id WebEx**
Secure Firewall로 푸시된 네트워크 서비스 그룹(NSG)을 확인하는 방법	**show run object-group network-service**
정책 기반 라우팅에 연결된 경로 맵을 보는 방법	**show run route-map**
인터페이스 이름 및 인터페이스 우선순위와 같은 인터페이스 구성 세부 정보를 확인하는 방법	**show run interface**
신뢰할 수 있는 DNS 서버 설정을 확인하는 방법	**show dns**
트래픽이 사용된 경로를 확인하는 방법	**debug policy-route** 중요 debug 명령은 트래픽에 따라 자세한 정보가 표시될 수 있으므로 프로덕션 환경에서 신중하게 실행합니다.
경로 디버깅을 중지하는 방법	**undebug all**

사전 정의된 네트워크 서비스 개체를 보려면 다음 명령을 사용합니다.

```
ngfwbr1# show object network-service
object network-service "ADrive" dynamic
 description Online file storage and backup.
 app-id 17
 domain adrive.com (bid=0) ip (hitcnt=0)
object network-service "Amazon" dynamic
 description Online retailer of books and most other goods.
 app-id 24
 domain amazon.com (bid=0) ip (hitcnt=0)
 domain amazon.jobs (bid=0) ip (hitcnt=0)
 domain amazon.in (bid=0) ip (hitcnt=0)
.
.
.
```

```
output snipped
.
.
.
object network-service "Logitech" dynamic
 description Company develops Computer peripherals and accessories.
 app-id 4671
 domain logitech.com (bid=0) ip (hitcnt=0)
object network-service "Lenovo" dynamic
 description Company manufactures/markets computers, software and related services.
 app-id 4672
 domain lenovo.com (bid=0) ip (hitcnt=0)
 domain lenovo.com.cn (bid=0) ip (hitcnt=0)
 domain lenovomm.com (bid=0) ip (hitcnt=0)
ngfwbr1#
```

YouTube 및 WebEx와 같은 특정 네트워크 서비스 개체를 보려면 다음 명령을 사용합니다.

```
ngfwbr1# show object id YouTube
object network-service "YouTube" dynamic
 description A video-sharing website on which users can upload, share, and view videos.
 app-id 929
 domain youtubei.googleapis.com (bid=592729) ip (hitcnt=0)
 domain yt3.ggpht.com (bid=709809) ip (hitcnt=102)
 domain youtube.com (bid=830871) ip (hitcnt=101)
 domain ytimg.com (bid=1035543) ip (hitcnt=93)
 domain googlevideo.com (bid=1148165) ip (hitcnt=466)
 domain youtu.be (bid=1247981) ip (hitcnt=0)
ngfwbr1# show object id WebEx
object network-service "WebEx" dynamic
 description Cisco's online meeting and web conferencing application.
 app-id 905
 domain files-prod-us-east-2.webexcontent.com (bid=182837) ip (hitcnt=0)
 domain webex.com (bid=290507) ip (hitcnt=30)
 domain avatar-prod-us-east-2.webexcontent.com (bid=452667) ip (hitcnt=0)
ngfwbr1#
```

NSG가 Threat Defense로 푸시되었는지 확인하려면 다음 명령을 사용합니다.

```
ngfwbr1# show run object-group network-service
object-group network-service FMC_NSG_292057776181
 network-service-member "WebEx"
object-group network-service FMC_NSG_292057776200
 network-service-member "YouTube"
ngfwbr1#
```

PBR과 연결된 경로 맵을 확인하려면 다음 명령을 사용합니다.

```
ngfwbr1# show run route-map
!
route-map FMC_GENERATED_PBR_1678091359817 permit 5
 match ip address DIA_Collaboration
 set interface outside3 outside2

!
route-map FMC_GENERATED_PBR_1678091359817 permit 10
 match ip address DIA_SocialMedia
 set adaptive-interface cost outside outside2 outside3
!
ngfwbr1#
```

인터페이스 설정 및 인터페이스 우선순위 세부정보를 확인하려면 다음 명령을 사용합니다.

```
ngfwbr1# show run interface
!
```

```
interface GigabitEthernet0/0
 nameif outside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
  zone-member ECMP-WAN
 ip address 198.18.128.81 255.255.192.0
 policy-route cost 10
!
interface GigabitEthernet0/1
 nameif inside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 198.19.11.4 255.255.255.0
 policy-route route-map FMC_GENERATED_PBR_1678091359817
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 nameif outside2
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 zone-member ECMP-WAN
 ip address 198.19.40.4 255.255.255.0
 policy-route cost 10
!
interface GigabitEthernet0/4
 nameif outside3
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 198.19.30.4 255.255.255.0
 policy-route cost 20
!
interface Management0/0
 management-only
 nameif diagnostic
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 no ip address
ngfwbr1#
```

신뢰할 수 있는 DNS 설정을 확인하려면 다음 명령을 사용합니다.

```
ngfwbr1# show dns

DNS Trusted Source enabled for DHCP Server Configured
DNS Trusted Source enabled for DHCP Client Learned
DNS Trusted Source enabled for DHCP Relay Learned
DNS Trusted Source enabled for DNS Server Configured
DNS Trusted Source not enabled for Trust-any
DNS Trusted Source: Type: IPs : Interface : Idle/Timeout (sec)
```

```
    DNS Server Configured: 198.19.10.100: <ifc-not-specified> : N/A
Trusted Source Configured: 198.19.10.100: <ifc-not-specified> : N/A
DNS snooping IP cache: 0 in use, 37 most used
Address                                 Idle(sec) Timeout(sec) Hit-count          Branch(es)
ngfwbr1#
```

정책 경로를 디버깅하려면 다음 명령을 사용합니다.

```
ngfwbr1# debug policy-route
debug policy-route  enabled at level 1
ngfwbr1# pbr: policy based route lookup called for 198.19.11.225/58119 to 198.19.10.100/53
 proto 17 sub_proto 0 received on interface inside, NSGs, nsg_id=none
pbr: no route policy found; skip to normal route lookup
.
output-snipped
.
pbr: policy based route lookup called for 198.19.11.225/61482 to 63.140.48.151/443 proto 6
 sub_proto 0 received on interface inside
                                                                , NSGs, nsg_id=1
pbr: First matching rule from ACL(2)
pbr: route map FMC_GENERATED_PBR_1678091359817, sequence 5, permit; proceed with policy
routing
pbr: evaluating interface outside3
pbr: policy based routing applied; egress_ifc = outside3 : next_hop = 198.19.30.63

ngfwbr1#
```

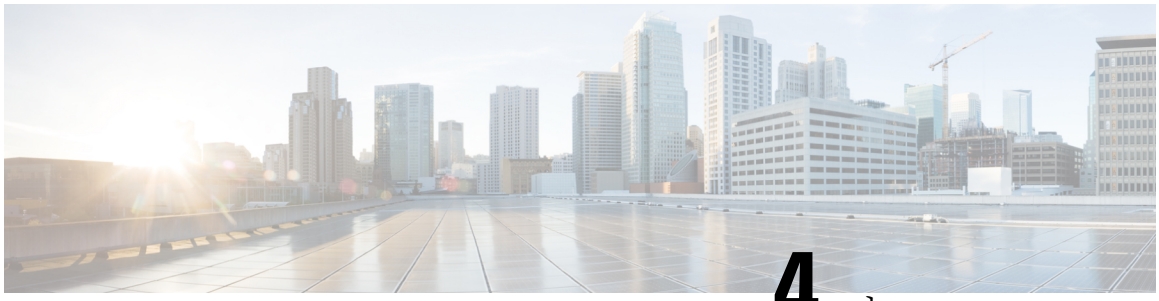
위의 디버그 예는 WebEx 트래픽에 대한 것입니다. PBR이 outside2 인터페이스에 대한 라우팅 경로를 변경하기 전에 트래픽은 outside3 인터페이스를 통해 라우팅됩니다.

디버그 프로세스를 중지하려면 다음 명령을 사용합니다.

```
ngfwbr1# undebug all
```

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



4 장

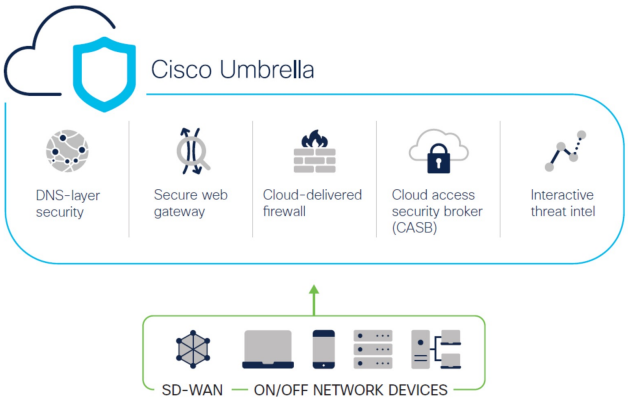
Umbrella 자동 터널을 사용하여 인터넷 트래픽 보호

이 장에서는 Umbrella 자동 터널의 실제 애플리케이션에 대해 자세히 설명합니다. 활용 사례에서는 시나리오, 네트워크 토폴로지, 모범 사례, 사전 요건에 대해 자세히 설명합니다. 또한 원활한 구현을 위한 포괄적인 엔드 투 엔드 절차를 제공합니다.

Cisco Umbrella 자동 터널

DNS(Domain Name System)는 공격에 자주 사용되는 인터넷 프로토콜입니다. 악성코드의 90%가 DNS를 사용합니다(출처: Cisco Security Research 보고서). 하지만 많은 조직에서는 DNS를 모니터링하거나 DNS 중심 보안을 사용하지 않습니다.

그림 *4: Cisco Umbrella*



Cisco Umbrella는 인터넷 기반 위협에 대한 여러 수준의 방어를 제공하는 클라우드 기반 보안 인터넷 게이트웨이 플랫폼입니다. Umbrella는 DNS 레이어 보안, CASB(Cloud Access Security Border) 기능, 클라우드 제공 방화벽 및 보안 웹 게이트웨이를 통합하여 브랜치 리소스와 무관하게 확장성이 뛰어난 보안을 제공합니다. 인터넷 바인딩 트래픽은 인터넷에 대한 액세스가 허용되거나 거부되기 전에 검사를 위해 브랜치에서 가장 가까운 Umbrella 접속 지점으로 자동 전송될 수 있습니다.

릴리스 7.3부터 Secure Firewall Management Center는 Umbrella SIG(Secure Internet Gateway) 통합을 위한 자동 터널 구성을 지원합니다. 이 구성을 사용하면 네트워크 디바이스에서 SIG 터널을 통한 검사 및 필터링을 위해 DNS 및 웹 트래픽을 Umbrella SIG에 전달할 수 있습니다.

Cisco Umbrella 내에 정의된 DNS 및 웹 정책을 Secure Firewall을 통한 연결에 적용할 수 있습니다. 도메인 이름을 기준으로 요청을 적용하고 검증할 수 있습니다.

관리 센터는 이 터널을 구축할 수 있도록 새롭게 간소화된 직관적인 마법사 기반 인터페이스를 제공하므로 Firewall Threat Defense 및 Cisco Umbrella에서 설정 단계가 최소화됩니다.

관리 센터는 Umbrella API를 활용하여 Cisco Umbrella 연결 설정의 매개변수를 사용하여 네트워크 터널을 설정합니다. 그런 다음 관리 센터는 Umbrella 데이터 센터 목록을 가져와 SASE 토폴로지에서 허브로 선택할 수 있도록 사용자 인터페이스에 이를 표시합니다. 네트워크 터널은 위협 방어 디바이스에 구축되고, 관리 센터에서 구축이 완료되고 나면 Cisco Umbrella에서 자동으로 생성됩니다. 이렇게 하면 온프레미스 사용자와 로밍 사용자에게 균일한 DNS 및 웹 정책을 적용할 수 있습니다.

이점

Cisco Umbrella를 사용하여 인터넷 트래픽을 보호하면 다음과 같은 이점이 있습니다.

- 연결을 설정하기 전에 DNS 레이어에서 사용자와 애플리케이션을 보호하면 그에 따른 패킷 처리가 감소하여 보호 속도가 빨라집니다.
- 균일한 DNS 제어 정책이 하이브리드 사용자(온프레미스 사용자 및 로밍 사용자)에 적용됩니다.
- Umbrella는 연결이 설정되기 전에도 웹 요청은 물론 멀웨어, 랜섬웨어, 피싱 시도 및 봇넷에 대한 요청을 차단하여 위협이 네트워크 또는 엔드포인트에 도달하기 전에 차단합니다. 따라서 교정해야 하는 감염 및 알림 수가 크게 감소합니다.

- URL 필터링 및 TLS 암호 해독과 같은 고급 방화벽 기능에 대한 필요성을 제거합니다.
- 자동 터널을 설정하려면 관리 센터에서 최소한의 설정이 필요합니다.
- Umbrella 대시보드의 자동 네트워크 터널 구성입니다.

이 활용 사례가 귀사에 적합합니까**?**

Umbrella SASE 자동 터널 구성의 대상은 조직의 네트워크 인프라 관리 및 보안을 책임지는 IT 팀, 네트워크 관리자, 보안 전문가입니다. 이들은 보안 원격 액세스를 위한 고급 솔루션을 탐색하고 보안 터널의 설정 및 관리를 간소화하는 데 관심이 있습니다. Umbrella SASE 자동 터널 설정 설명은 네트워크 보안을 강화하고, 원격 연결을 간소화, 조직의 원격 인력에 대한 전반적인 사용자 환경을 개선하고자 하는 사용자의 관심을 끌 수 있습니다.

시나리오

IT 관리자인 Alice는 조직의 IT 인프라 관리 및 보안 보장을 담당합니다. Alice는 사이버 공간에서 증가하는 위협을 인지하고 있으며, 악성코드, 랜섬웨어, 피싱과 같은 잠재적인 사이버 공격을 방지하기 위한 강력한 보안 조치를 구현하고자 합니다.

Sally는 지사에서 근무하며 조직의 네트워크를 사용하여 업무 관련 활동을 위해 인터넷에 액세스하는 직원입니다.

어떤 위험이 있습니까**?**

적절한 보안 조치가 없으면 직원이 의도치 않게 악의적인 웹사이트에 액세스하여 유해한 소프트웨어를 다운로드하여 조직의 네트워크 보안 및 데이터 개인 정보를 침해할 수 있습니다.

SIG 통합이 문제를 어떻게 해결합니까**?**

Alice는 브랜치 방화벽과 Cisco Umbrella를 사용하여 2레이어 보안 접근 방식을 구현했습니다. 방화벽은 웹 및 비 웹 기반 공격으로부터 네트워크에 대한 인바운드 보안을 제공했습니다. Umbrella는 DNS 및 웹 레이어에서 악의적인 도메인, IP 및 URL을 차단하여 아웃바운드 보안을 제공합니다.

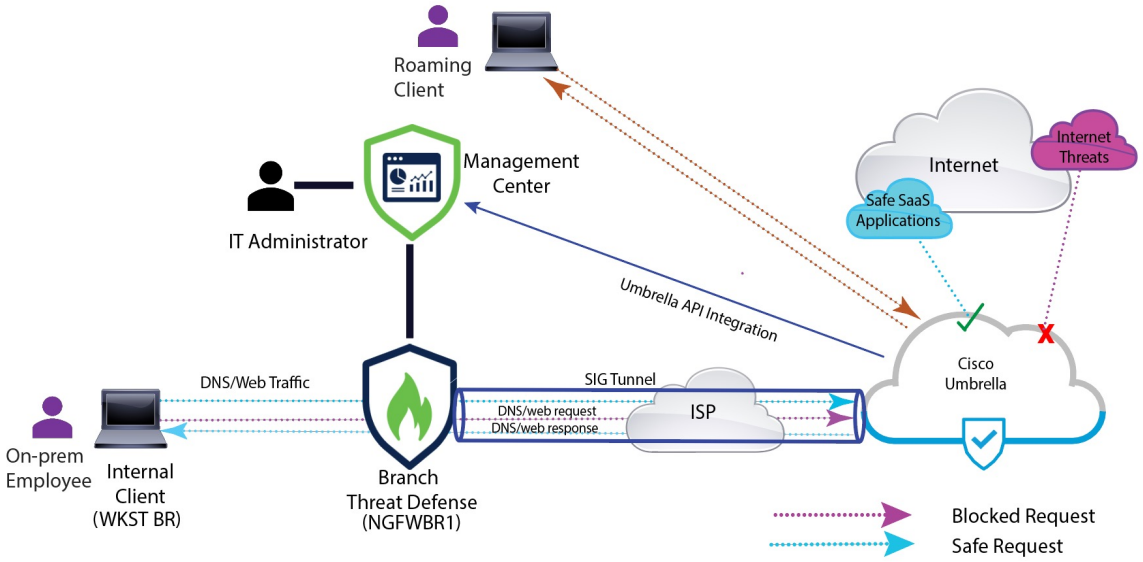
Sally는 일부 웹사이트가 현재 방화벽과 Umbrella에 의해 차단되고 있는 것을 확인합니다.

온프레미스 사용자 및 원격 사용자 모두 Umbrella 대시보드 내에 정의된 것과 동일한 DNS 및 웹 정책의 적용을 받습니다. 이 구현의 결과로, 조직의 네트워크는 이제 더욱 안전해지고 잠재적인 사이버 공격으로부터 보호됩니다.

네트워크 토폴로지

이 토폴로지에서 위협 방어 디바이스는 브랜치 위치에 구축됩니다. 아래 그림에서 내부 클라이언트 또는 브랜치 워크스테이션은 WKST BR 레이블로 표시되고 브랜치 위협 방어는 NGFWBR1 레이블로 표시됩니다. SIG 자동 터널은 NGFWBR1과 Cisco Umbrella 사이에 설정됩니다.

그림 *5: Umbrella* 자동 터널 구성을 위한 네트워크 토폴로지



모든 DNS 및 웹 트래픽은 SIG 터널을 통해 Cisco Umbrella로 전송되어 Umbrella DNS 및 웹 정책에 따라 검증 및 허용 또는 차단됩니다. 이는 두 가지 보호 레이어를 제공합니다. 하나는 Cisco Secure Threat Defense에 의해 로컬로 적용되고 다른 레이어는 Cisco Umbrella에 의해 클라우드에서 제공됩니다.

DNS 트래픽의 경우:

1. Cisco Umbrella는 분류되지 않은 도메인에 대한 DNS 요청을 탐지하는 경우 도메인의 평판을 쿼리합니다.
2. 도메인이 악의적인 것으로 분류된 경우 DNS 요청이 차단되고 최종 사용자는 웹사이트에 액세스할 수 없습니다.
3. 도메인이 안전한 것으로 분류되는 경우 DNS 요청이 확인되며 최종 사용자가 웹사이트에 액세스할 수 있습니다.

SASE Umbrella 터널의 모범 사례

- 관리 센터에서 기본 라이선스가 내보내기 제어 기능으로 활성화되어 있는지 확인합니다.
- 인터넷과 연결되는 위협 방어 인터페이스의 경우에는 **outside**로 이름을 지정하거나 접두사를 지정하는 것이 좋습니다.
- SASE 토폴로지에 대해 Umbrella 구축이 실행 중인 경우 SASE 토폴로지를 수정하거나 삭제하지 마십시오.
- 백업 Umbrella DC를 구성하려면 백업 Umbrella DC를 사용하여 동일한 위협 방어 엔드포인트로 동일한 토폴로지를 복제합니다.
- 위협 방어 엔드포인트에서 백업 인터페이스를 구성하려면 백업 인터페이스에서 VTI를 사용하여 동일한 Umbrella DC와 동일한 위협 방어 엔드포인트로 동일한 토폴로지를 복제합니다.

Umbrella SASE 터널 구성을 위한 사전 요건

- 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
- Cisco Umbrella SIG(Secure Internet Gateway) Essentials 서브스크립션 또는 무료 SIG 평가판이 있어야 합니다.
- 관리 센터에서 Umbrella의 터널을 구축하려면 내보내기 제어 기능을 사용하여 스마트 라이선스 어카운트를 활성화해야 합니다.
- http://login.umbrella.com에서 Umbrella에 로그인하고 Cisco Umbrella 연결을 설정하는 데 필요한 정보를 얻습니다. 관리 센터가 management.api.umbrella.com에 연결할 수 있는지 확인합니다.
- 관리 센터에 Cisco Umbrella 조직을 등록하고 Cisco Umbrella 연결 고급 설정에서 관리 키 및 관리 암호를 구성해야 합니다. 이렇게 하면 Cisco Umbrella 클라우드에서 데이터 센터 세부 정보를 가져옵니다. 또한 Cisco Umbrella 연결 일반 설정에서 조직 ID, 네트워크 디바이스 키, 네트워크 디바이스 암호 및 레거시 네트워크 디바이스 토큰을 구성해야 합니다.

  자세한 내용은 다음 링크를 참조하십시오.

  - Cisco Umbrella 연결 설정 구성
  - Management Center Umbrella 매개변수 및 Cisco Umbrella API 키 맵
- 위협 방어에서 Umbrella 데이터 센터에 연결할 수 있는지 확인합니다.
- 위협 방어가 로컬 터널 ID 지원(버전 7.1.0 이상)을 통해 경로 기반 VPN을 지원하는지 확인합니다. 관리 센터 버전 7.3.0 이상에서 로컬 터널 ID가 지원되는 SASE 터널을 구축할 수 있습니다.

SASE Umbrella 터널의 모범 사례

- 관리 센터에서 기본 라이선스가 내보내기 제어 기능으로 활성화되어 있는지 확인합니다.
- 인터넷과 연결되는 위협 방어 인터페이스의 경우에는 **outside**로 이름을 지정하거나 접두사를 지정하는 것이 좋습니다.
- SASE 토폴로지에 대해 Umbrella 구축이 실행 중인 경우 SASE 토폴로지를 수정하거나 삭제하지 마십시오.
- 백업 Umbrella DC를 구성하려면 백업 Umbrella DC를 사용하여 동일한 위협 방어 엔드포인트로 동일한 토폴로지를 복제합니다.

- 위협 방어 엔드포인트에서 백업 인터페이스를 구성하려면 백업 인터페이스에서 VTI를 사용하여 동일한 Umbrella DC와 동일한 위협 방어 엔드포인트로 동일한 토폴로지를 복제합니다.

Umbrella SASE 터널 구성을 위한 사전 요건

- 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
- Cisco Umbrella SIG(Secure Internet Gateway) Essentials 서브스크립션 또는 무료 SIG 평가판이 있어야 합니다.
- 관리 센터에서 Umbrella의 터널을 구축하려면 내보내기 제어 기능을 사용하여 스마트 라이선스 어카운트를 활성화해야 합니다.
- http://login.umbrella.com에서 Umbrella에 로그인하고 Cisco Umbrella 연결을 설정하는 데 필요한 정보를 얻습니다. 관리 센터가 management.api.umbrella.com에 연결할 수 있는지 확인합니다.
- 관리 센터에 Cisco Umbrella 조직을 등록하고 Cisco Umbrella 연결 고급 설정에서 관리 키 및 관리 암호를 구성해야 합니다. 이렇게 하면 Cisco Umbrella 클라우드에서 데이터 센터 세부 정보를 가져옵니다. 또한 Cisco Umbrella 연결 일반 설정에서 조직 ID, 네트워크 디바이스 키, 네트워크 디바이스 암호 및 레거시 네트워크 디바이스 토큰을 구성해야 합니다.

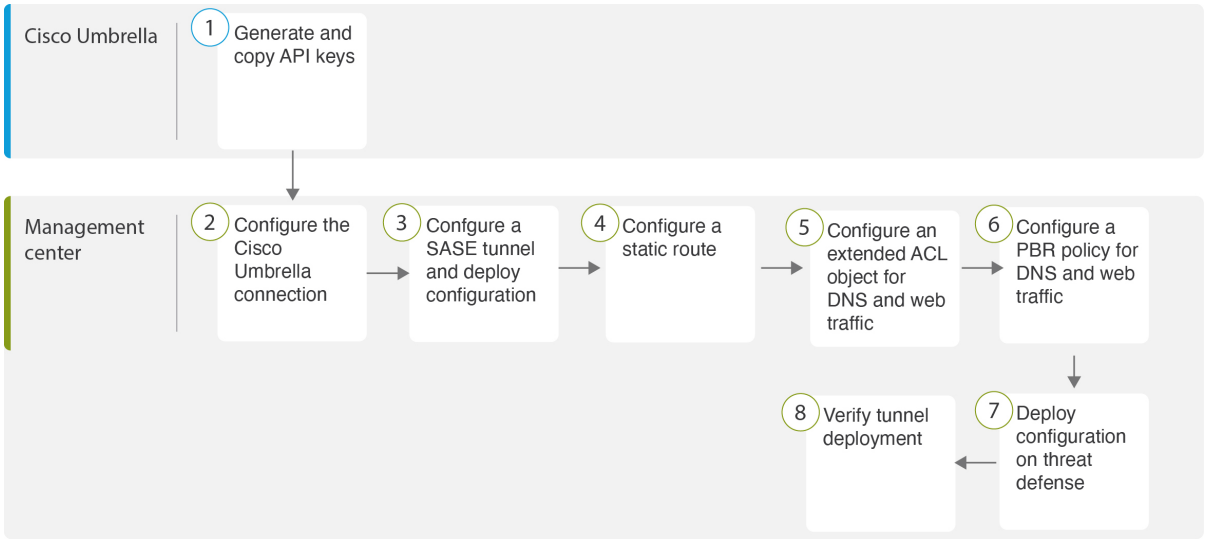
  자세한 내용은 다음 링크를 참조하십시오.

  - Cisco Umbrella 연결 설정 구성
  - Management Center Umbrella 매개변수 및 Cisco Umbrella API 키 맵

- 위협 방어에서 Umbrella 데이터 센터에 연결할 수 있는지 확인합니다.
- 위협 방어가 로컬 터널 ID 지원(버전 7.1.0 이상)을 통해 경로 기반 VPN을 지원하는지 확인합니다. 관리 센터 버전 7.3.0 이상에서 로컬 터널 ID가 지원되는 SASE 터널을 구축할 수 있습니다.

Umbrella 자동 터널 구성을 위한 엔드 투 엔드 절차

다음 순서도에는 Secure Firewall Management Center에서 SASE 터널을 구성하는 워크플로우가 나와 있습니다.



단계	설명
1	(사전 요건) Cisco Umbrella에서 API 키를 생성하고 복사합니다. Management Center Umbrella 매개변수 및 Cisco Umbrella API 키 맵을 참조하십시오.
2	(사전 요건) Cisco Umbrella 연결을 구성합니다. Cisco Umbrella 연결 설정 구성을 참조하십시오.
3	SASE 터널을 생성하고 위협 방어에 대한 구성을 구축합니다. Umbrella용 SASE 터널 구성, 64 페이지의 내용을 참조하십시오.
4	고정 경로를 구성합니다. 고정 경로 구성, 67 페이지의 내용을 참조하십시오.
5	DNS 및 웹 트래픽에 대한 확장 ACL 개체를 구성합니다. DNS 및 웹 트래픽용 확장 ACL 구성, 68 페이지의 내용을 참조하십시오.
6	DNS 및 웹 트래픽에 대한 PBR 정책을 구성합니다. DNS 및 웹 트래픽용 PBR 정책 구성 , 69 페이지의 내용을 참조하십시오.
7	구성을 위협 방어에 구축합니다. 컨피그레이션 구축, 21 페이지의 내용을 참조하십시오.
8	터널 구축을 확인합니다. SASE Umbrella 터널 구축 확인, 70 페이지의 내용을 참조하십시오.

Umbrella용 SASE 터널 구성

시작하기 전에

Umbrella SASE 터널 구성을 위한 사전 요건, 61 페이지 및 SASE Umbrella 터널의 모범 사례, 60 페이지 항목을 검토하십시오.

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

단계 2 **+ SASE Topology(+ SASE** 토폴로지**)**를 클릭하여 SASE 토폴로지 마법사를 엽니다.

단계 3 고유한 **Topology Name(**토폴로지 이름**)**을 입력합니다. 이 예에서는 **VPN-MumbaiUmbrella**를 입력합니다.

단계 4 사전 공유 키: 이 키는 Umbrella PSK 요구 사항에 따라 자동으로 생성됩니다.

디바이스와 Umbrella는 이 비밀 키를 공유하며 IKEv2는 이를 인증에 사용합니다. 자동 생성된 키를 재정의할 수 있습니다. 이 키를 구성하려면 길이가 16~64자여야 하며 최소 하나의 대문자, 하나의 소문자, 하나의 숫자를 포함해야 하며 특수 문자가 없어야 합니다. 각 토폴로지에는 고유한 사전 공유 키가 있어야 합니다. 토폴로지에 여러 터널이 있는 경우 모든 터널에 동일한 사전 공유 키가 있습니다.

단계 5 **Umbrella** 데이터 센터 드롭다운 목록에서 데이터 센터를 선택합니다. Umbrella 데이터 센터는 지역 및 IP 주소로 자동으로 채워집니다.

단계 6 **Add(**추가**)**를 클릭하여 위협 방어 노드를 SASE 토폴로지에 엔드포인트로 추가합니다.

a) **Device(**디바이스**)** 드롭다운 목록에서 위협 방어 디바이스(**NGFWBR1**)를 선택합니다.

b) **VPN Interface(VPN** 인터페이스**)** 드롭다운 목록에서 정적 VTI 인터페이스를 선택합니다.

새 정적 VTI 인터페이스(예: **Outside_static_vti_1**)를 생성하려면 **+**를 클릭합니다. 다음과 같은 기본 구성이 미리 채워진 **Add Virtual Tunnel Interface(Virtual Tunnel** 인터페이스 추가**)** 대화 상자가 나타납니다.

- Tunnel Type(터널 유형)은 기본적으로 **Static(**고정**)**으로 설정됩니다.
- 이름은 <*tunnel_source interface logical name*>+ static_vti +<*tunnel ID*>입니다. 예: Outside_static_vti_1.
- 터널은 기본적으로 **Enabled(**활성화됨**)** 상태입니다.
- 보안 영역은 기본적으로 **Outside(**외부**)**로 구성됩니다.
- 터널 ID는 고유한 ID로 자동으로 채워집니다.
- 터널 소스 인터페이스는 'outside' 접두사가 있는 인터페이스로 자동으로 채워집니다.

  참고 터널 소스가 **GigabitEthernet0/0**으로 설정되어 있는지 확인합니다.

  참고 터널 소스 인터페이스를 다른 인터페이스로 설정할 수도 있습니다.

- IPsec 터널 모드는 기본적으로 IPv4입니다.
- 미사용 IP 주소는 169.254.xx/30 프라이빗 IP 주소 범위에서 선택됩니다. 이 예에서는 **169.254.2.1/30**이 선택되었습니다.

참고 /30 서브넷을 사용하는 경우에는 2개의 IP 주소만 사용할 수 있습니다. 첫 번째 IP 주소는 자동 터널 VTI IP이고 두 번째 IP 주소는 Umbrella DC에 대한 정적 경로를 설정하는 동안 다음 홉 IP로 사용됩니다. 이 예에서 169.254.2.1은 VTI IP이고 169.254.2.2는 정적 경로에 사용됩니다. 고정 경로 구성, 67 페이지의 내용을 참조하십시오.

- **OK(**확인**)**를 클릭합니다.

VPN Interface(VPN 인터페이스) 드롭다운 목록에서 **outside_static_vti_1**을 선택합니다.

c) **Local Tunnel ID(**로컬 터널 **ID)** 필드에 로컬 터널 ID의 접두사를 입력합니다.

접두사는 최소 8자에서 최대 100자까지 사용할 수 있습니다. Umbrella는 관리 센터에서 Umbrella에 터널을 구축한 후 전체 터널 ID(<*prefix*>@<*umbrella-generated-ID*>-umbrella.com)를 생성합니다. 그런 다음 관리 센터는 전체 터널 ID를 검색 및 업데이트하여 위협 방어 디바이스에 구축합니다. 각 터널에는 고유한 로컬 터널 ID가 있습니다.

d) **Save(**저장**)**를 클릭하여 엔드포인트 디바이스를 토폴로지에 추가합니다.

단계 **7** Umbrella SASE 터널 구성의 요약을 보려면 **Next(**다음**)**를 클릭합니다.

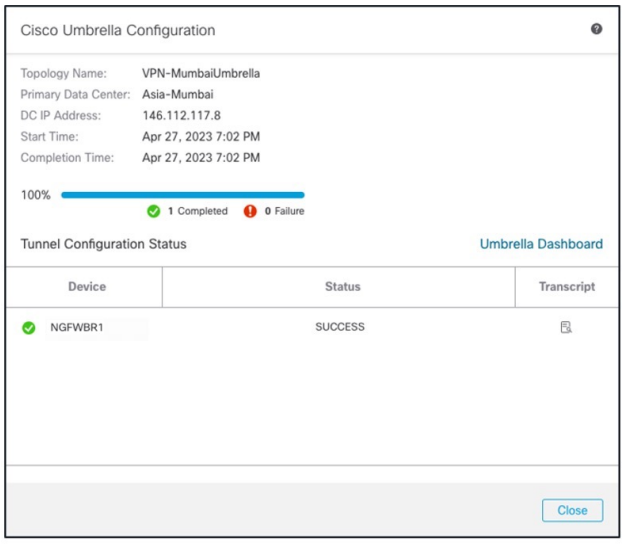
- **Endpoints(**엔드포인트**)** 창: 구성된 위협 방어 엔드포인트의 요약을 표시합니다.
- **Encryption Settings(**암호화 설정**)** 창: SASE 터널의 암호화 설정이 표시됩니다.

단계 **8** **Deploy configuration on threat Defense nodes(**위협 방어 노드에서 컨피그레이션 구축**)** 확인란을 선택하여 위협 방어에 대한 네트워크 터널 구축을 트리거합니다. 이 구축은 터널이 Umbrella에 구축된 후에만 수행됩니다. 위협 방어 구축에는 로컬 터널 ID가 필요합니다.

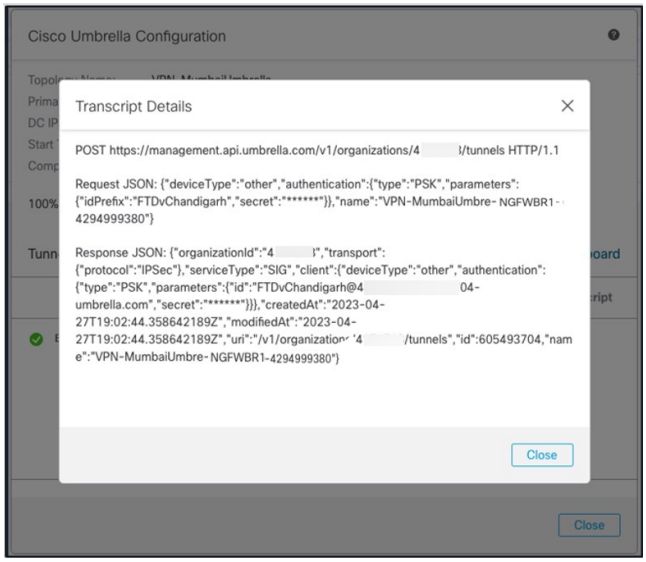
단계 **9** **Save(**저장**)**를 클릭합니다.

이 작업은

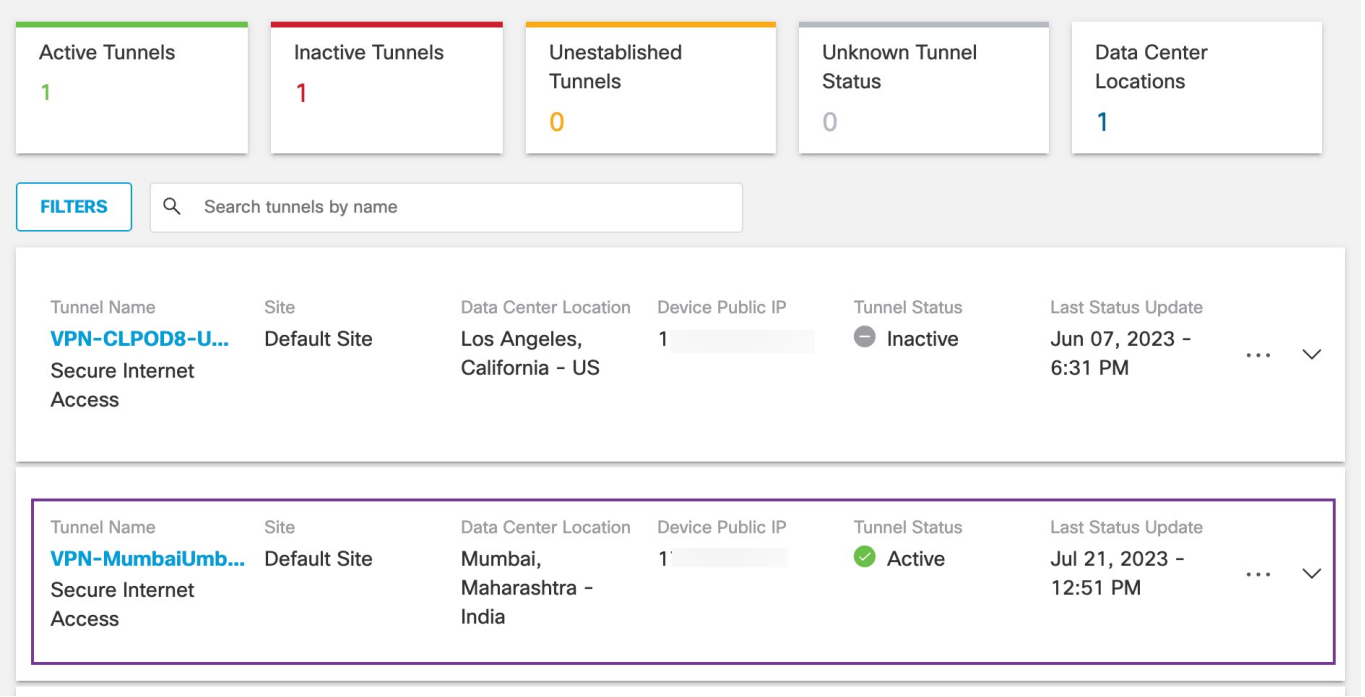
1. 관리 센터에 SASE 토폴로지를 저장합니다.
2. 각 위협 방어 엔드포인트에 대한 네트워크 터널의 Umbrella 구축을 트리거합니다.
3. 옵션이 활성화된 경우 위협 방어 디바이스에 대한 네트워크 터널 구축을 트리거합니다. 이 작업은 디바이스에서 마지막으로 구축한 이후 비 VPN 정책을 포함하여 업데이트된 모든 구성 및 정책을 커밋하고 구축합니다.
4. **Cisco Umbrella Configuration(Cisco Umbrella** 구성**)** 창을 열고 Umbrella에서 터널 구축의 상태를 표시합니다.



구축의 세부 정보를 보려면 **Transcript(**기록**)** 버튼을 클릭하여 API, 요청 페이로드 및 Umbrella에서 수신한 응답 등의 기록 세부 정보를 확인합니다.



Umbrella Dashboard(Umbrella 대시보드**)**를 클릭하여 Umbrella에서 네트워크 터널 페이지를 확인합니다.



다음에 수행할 작업

SASE 터널을 통과하도록 의도된 트래픽의 경우, VTI를 통해 트래픽을 전송하도록 특정 일치 기준을 사용하여 PBR 정책을 구성합니다.

고정 경로 구성

자동 터널에서 Umbrella DC로의 정적 경로를 구성해야 합니다.

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

단계 **2** 라우팅 탭을 클릭합니다.

단계 **3** **Static Route(**정적 경로**)**를 클릭합니다.

단계 **4** **Add Route(**경로 추가**)**를 클릭하여 새 경로를 추가합니다.

단계 **5** **Interface(**인터페이스**)** 드롭다운 목록에서 인터페이스로 **outside_static_vti_1**을 선택합니다.

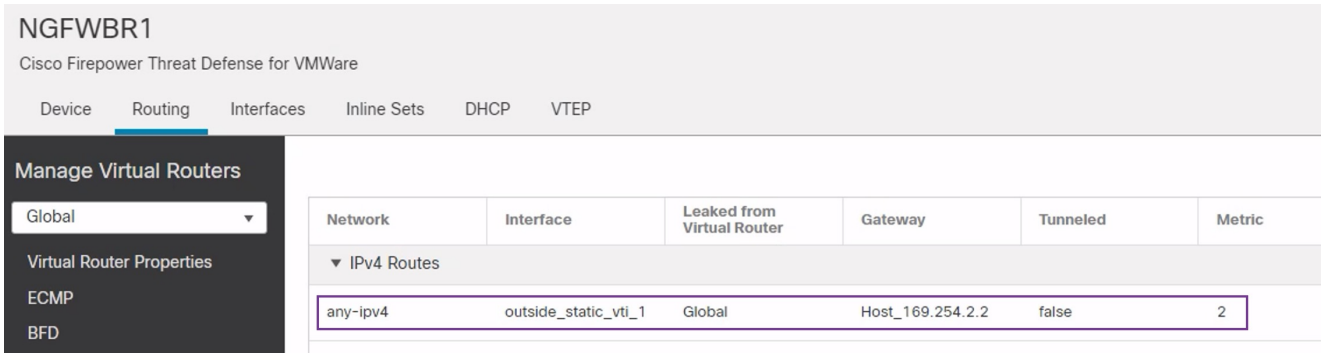
단계 **6** **Available Networks(**사용 가능한 네트워크**)** 상자에서 대상 네트워크로 **any-ipv4**를 선택하고 **Add(**추가**)**를 클릭합니다.

단계 **7** 네트워크의 게이트웨이를 입력합니다. 이 예시에서는 **169.254.2.2**를 입력합니다.

단계 **8** 메트릭 값을 입력합니다. 1~254 범위의 숫자일 수 있습니다. 이 예시에서는 값을 2로 입력합니다.

단계 9 설정을 저장하려면 **Save(**저장**)**를 클릭합니다.

아래 그림과 같이 정적 경로가 생성됩니다.



DNS 및 웹 트래픽용 확장 ACL 구성

액세스 목록은 DNS 및 웹 트래픽이 정책 기반 라우팅을 통해 이그레스 인터페이스에서 인터넷으로 조정되도록 구성됩니다.

단계 1 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하고 목차에서 **Access Lists(**액세스 목록**)** > **Extended(**확장**)**를 선택합니다.

단계 2 **Add Extended Access List(**확장된 액세스 목록 추가**)**를 클릭하여 소셜 미디어 트래픽에 대한 확장된 액세스 목록을 생성합니다.

단계 3 Extended ACL Object(확장된 ACL 개체) 대화 상자에서 개체의 이름(**LAN_to_Internet**)을 입력합니다.

단계 4 **Add(**추가**)**를 클릭하여 새 확장된 액세스 목록을 생성합니다.

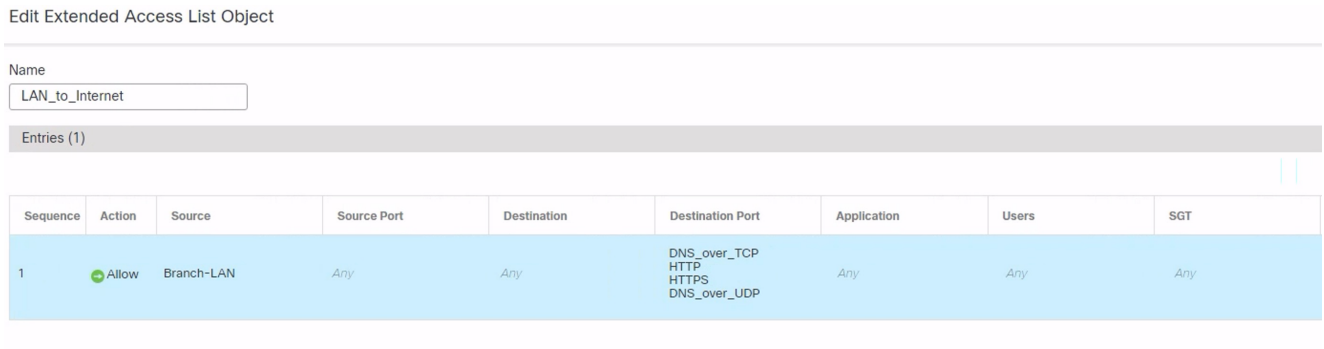
단계 5 다음 액세스 제어 속성을 구성합니다.

1. 작업을 선택하여 트래픽 조건을 허용(일치)합니다.
2. **Port(**포트**)** 탭을 클릭하고 **Available Ports(**사용 가능한 포트**)** 목록에서 **HTTP, HTTPS, DNS_over_UDP, DNS_over_TCP**를 검색합니다.
3. 포트를 선택하고 **Add to Destination(**대상에 추가**)**을 클릭합니다.
4. **Network(**네트워크**)** 탭을 클릭하고 **Available Networks(**사용 가능한 네트워크**)** 목록에서 브랜치 LAN을 검색합니다.

   참고 이 예에서 네트워크는 **Branch-LAN**입니다.

5. **Branch-LAN**을 선택하고 **Add to Source(**소스에 추가**)**를 클릭합니다.
6. 개체에 해당 항목을 추가하려면 **Add(**추가**)**를 클릭합니다.
7. **Save(**저장**)**를 클릭합니다.

아래 그림과 같이 ACL 개체가 생성됩니다.



DNS 및 웹 트래픽용 PBR 정책 구성

DNS 및 웹 트래픽을 라우팅할 인그레스 인터페이스, 일치 기준(확장된 액세스 제어 목록) 및 이그레스 인터페이스를 지정하여 Policy Based Routing(정책 기반 라우팅) 페이지에서 PBR 정책을 구성할 수 있습니다.

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** **Policy Based Routing(**정책 기반 라우팅**)**을 클릭합니다.

단계 **4** **Add Policy Based Route(**정책 기반 경로 추가**)** 대화 상자의 드롭다운 목록에서 **Ingress Interface(**인그레스 인터페이스**)**를 선택합니다.

단계 **5** 정책에서 일치 기준 및 전달 작업을 지정하려면 **Add(**추가**)**를 클릭합니다.

단계 **6** **Add Forwarding Actions(**전달 작업 추가**)** 대화 상자에서 다음을 수행합니다.

a) **Match ACL(ACL** 일치**)** 드롭다운에서 **LAN_to_Internet**을 선택합니다.

b) 구성된 인터페이스를 선택하려면 **Send To(**전송 대상**)** 드롭다운 목록에서 **Egress Interfaces(**이그레스 인터페이스**)**를 선택합니다.

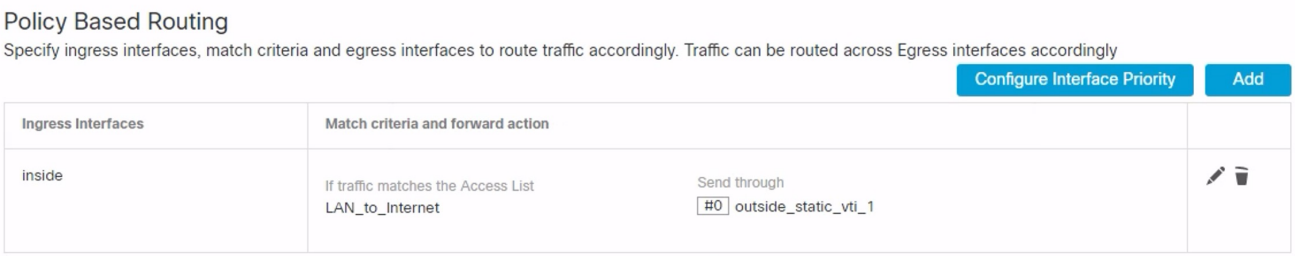
c) **Available Interfaces(**사용 가능한 인터페이스**)**에서 **Outside_static_vti_1** 인터페이스에 인접한 **Add(**추가**)** (+) 아이콘을 클릭하여 이를 **Selected Egress Interfaces(**선택한 이그레스 인터페이스**)**로 이동합니다.

d) **Save(**저장**)**를 클릭하여 일치 기준에 대한 변경 사항을 기록합니다.

e) 구성을 검토하고 **Save(**저장**)**를 클릭하여 정책 기반 라우팅에 대한 모든 구성 변경 사항을 씁니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

아래 그림과 같이 PBR 정책이 생성됩니다.



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.

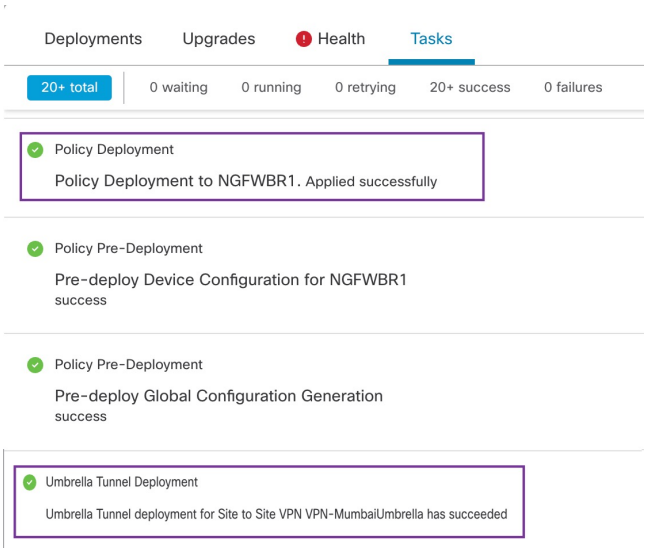
단계 **4** 구축할 변경 사항에서 오류나 경고를 식별하면 시스템은 **Validation Messages(**검증 메시지**)** 또는 **Validation Warnings(**검증 경고**)** 창에 이를 표시합니다. 전체 세부 정보를 보려면 Validation Errors(검증 오류) 또는 Validation Warnings(검증 경고) 링크를 클릭합니다.

다음 옵션을 이용할 수 있습니다.

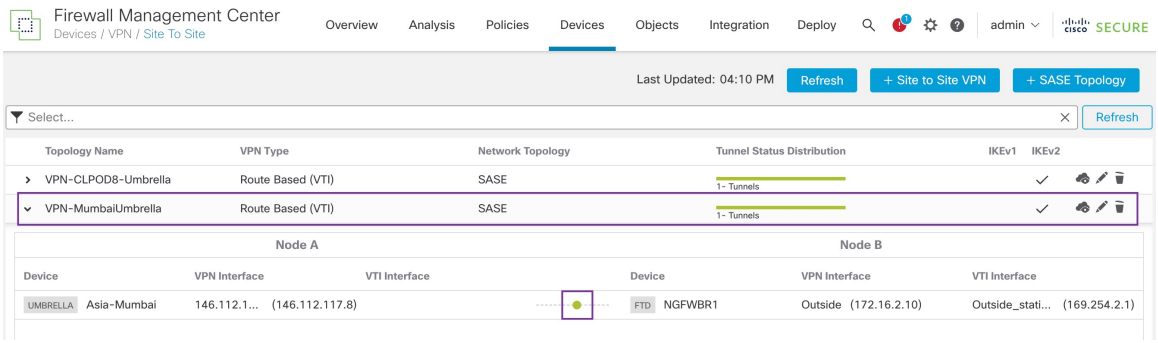
- Proceed with Deploy(구축 계속) - 경고 조건을 해결하지 않고 구축을 계속합니다. 오류가 식별되는 경우 계속 진행할 수 없습니다.
- Close(닫기) -구축하지 않고 종료합니다. 오류 및 경고 조건을 해결하고 컨피그레이션을 재구축합니다.

SASE Umbrella 터널 구축 확인

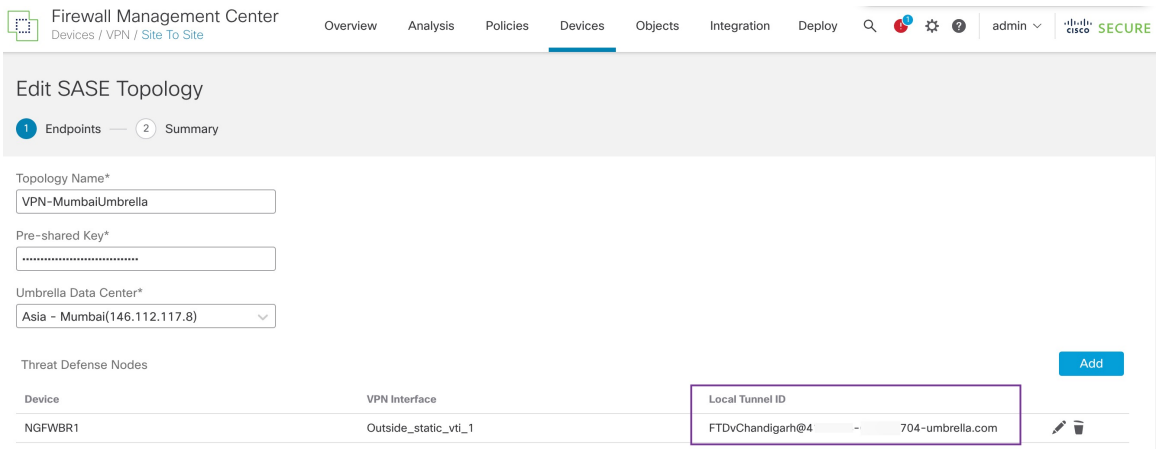
관리 센터에서 위협 방어 디바이스(NGFWBR1)에서 Umbrella 터널 구축 및 정책 구축 상태를 확인하려면 **Notifications(**알림**) - Task(**작업**)**로 이동합니다.



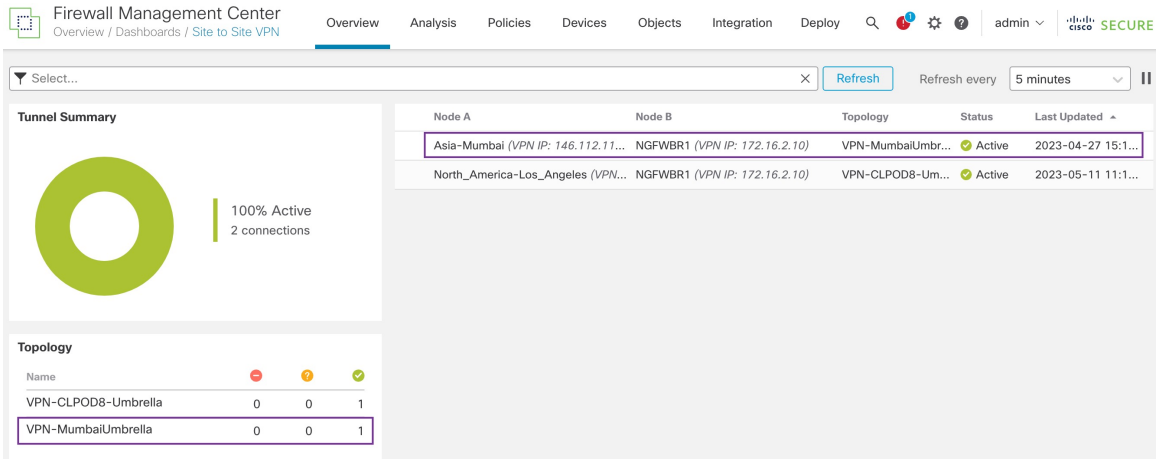
관리 센터에서 SASE 자동 터널 상태를 확인하려면 **Devices(**디바이스**)** → **VPN(VPN)** → **Site To Site(**사이트 간**)**를 선택합니다.



관리 센터에서 업데이트된 SASE 토폴로지를 확인하려면 **Devices(**디바이스**) > VPN > Site To Site(**사이트 간**) > Edit SASE Topology(SASE** 토폴로지 편집**)**를 선택합니다. 로컬 터널 ID는 Umbrella에 구축 후 업데이트됩니다.



관리 센터에서 Site To Site VPN(사이트 간 VPN) 대시보드를 보려면 **Overview(개요) > Dashboard(대시보드) > Site to Site VPN(사이트 간 VPN)**을 선택합니다.



위협 방어에 대한 SASE Umbrella 터널을 확인하려면 다음 CLI 명령을 사용합니다.

- SASE 터널의 세부 정보를 확인하려면 다음 명령을 사용합니다.

```
> show running-config interface tunnel 1
!
interface Tunnel1
 nameif Outside_static_vti_1
 ip address 169.254.2.1 255.255.255.252
 tunnel source interface Outside
 tunnel destination 146.112.117.8
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

- IPSec 프로파일 및 관련 제안을 확인하려면 다음 명령을 사용합니다.

```
> show running-config crypto ipsec
crypto ipsec ikev2 ipsec-proposal CSM_IP_1
 protocol esp encryption aes-gcm-256
 protocol esp integrity sha-256
crypto ipsec profile FMC_IPSEC_PROFILE_1
 set ikev2 ipsec-proposal CSM_IP_1
 set ikev2 local-identity email-id FTDvChandigarh@41xxxxx-xxxxxxxxx-umbrella.com
 set reverse-route
crypto ipsec security-association pmtu-aging infinite
```

- IKEV2 정책 집합을 확인하려면 다음 명령을 사용합니다.

```
> show running-config crypto ikev2
crypto ikev2 policy 15
 encryption aes-gcm-256
 integrity null
 group 20 19
 prf sha256
 lifetime seconds 86400
crypto ikev2 enable Outside
```

- Tx 및 Rx 데이터를 포함한 터널 통계를 확인하려면 다음 명령을 사용합니다.

```
> show vpn-sessiondb l2l
Session Type: LAN-to-LAN
Connection   : 146.112.117.8
Index        : 19                     IP Addr      : 146.112.117.8
Protocol     : IKEv2 IPsecOverNatT
Encryption   : IKEv2: (1)AES-GCM-256  IPsecOverNatT: (1)AES-GCM-256
Hashing      : IKEv2: (1)none  IPsecOverNatT: (1)none
Bytes Tx     : 234                      Bytes Rx     : 446
Login Time   : 19:14:51 UTC Thu Apr 27 2023
Duration     : 0h:55m:16s
Tunnel Zone  : 0
```

- 터널 상태를 확인하려면 다음 명령을 사용합니다.

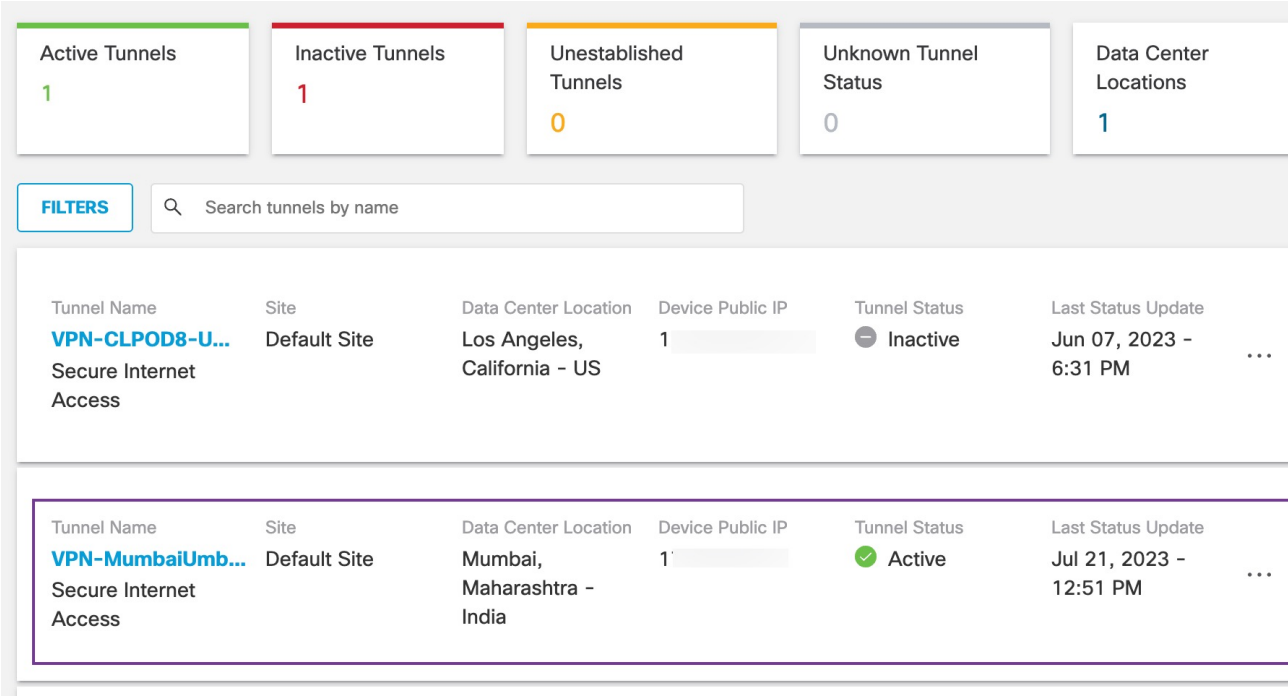
```
> show interface ip brief

Interface                  IP-Address      OK? Method Status                Protocol
Internal-Control0/0        127.0.1.1       YES unset  up                    up
Internal-Control0/1        unassigned      YES unset  up                    up
Internal-Data0/0           unassigned      YES unset  down                  up
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           169.254.1.1     YES unset  up                    up
Internal-Data0/2           unassigned      YES unset  up                    up
Management0/0              203.0.113.130   YES unset  up                    up
TenGigabitEthernet0/0      172.16.2.10     YES manual up                    up
TenGigabitEthernet0/1      172.16.3.10     YES manual up                    up
TenGigabitEthernet0/2      unassigned      YES unset  administratively down up
Tunnel1                    169.254.2.1     YES manual up                    up
```

- VTI 터널과 연결된 IPSec SA를 확인하려면 다음 명령을 사용합니다.

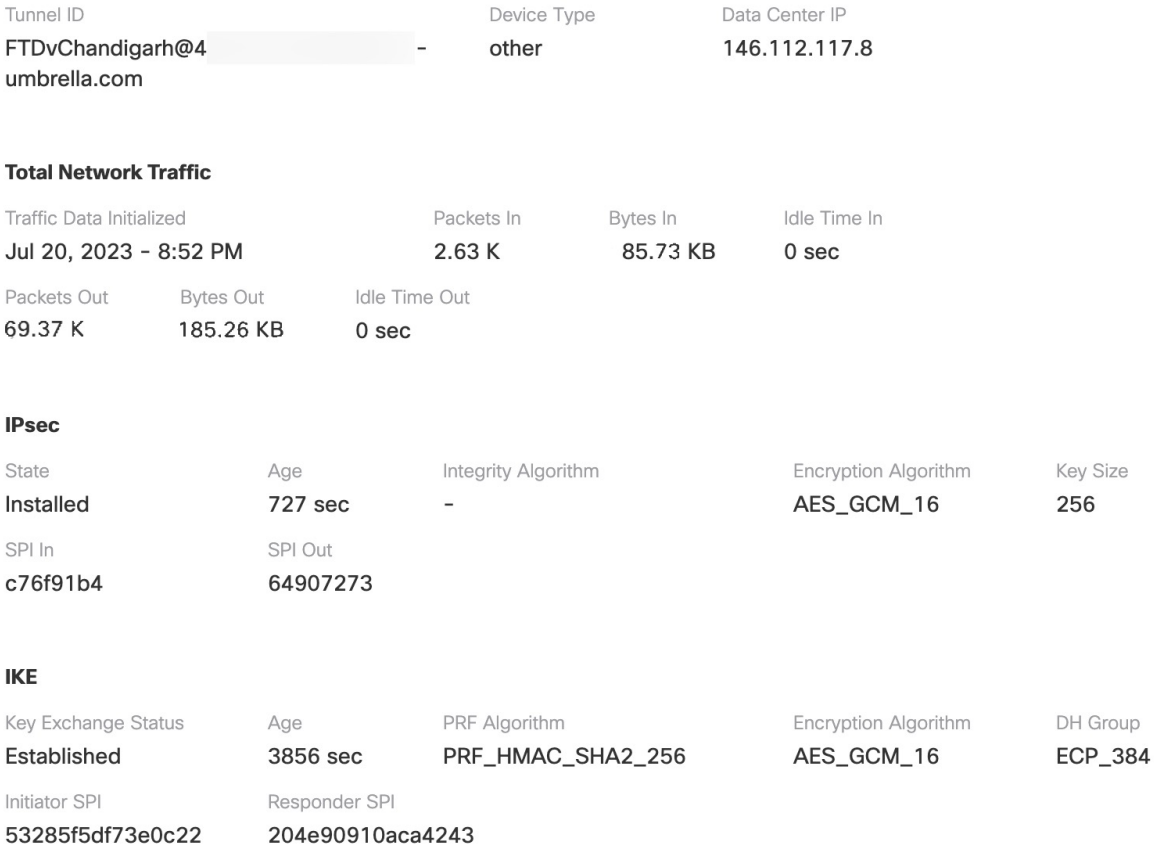
```
> show crypto ipsec sa
interface: outside_static_vti_1
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr:
198.18.128.81

      Protected vrf (ivrf): Global
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer: 146.112.117.8


      #pkts encaps: 705, #pkts encrypt: 705, #pkts digest: 705
      #pkts decaps: 743, #pkts decrypt: 743, #pkts verify: 743
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 705, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

     local crypto endpt.: 198.18.128.81/4500, remote crypto endpt.: 146.112.117.8/4500

      path mtu 1500, ipsec overhead 63(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: C76F91B4
```

```
  current inbound spi : 64907273

inbound esp sas:
  spi: 0x2BF92601 (737748481)
     SA State: active
     transform: esp-aes-gcm-256 esp-null-hmac no compression
     in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, VTI, }
     slot: 0, conn_id: 32, crypto-map: __vti-crypto-map-Tunnel1-0-1
     sa timing: remaining key lifetime (kB/sec): (4331520/27987)
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0x00000000 0x00000001
outbound esp sas:
  spi: 0xCA2DC006 (3391995910)
     SA State: active
     transform: esp-aes-gcm-256 esp-null-hmac no compression
     in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, VTI, }
     slot: 0, conn_id: 32, crypto-map: __vti-crypto-map-Tunnel1-0-1
     sa timing: remaining key lifetime (kB/sec): (4101072/27987)
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0x00000000 0x00000001
```

Umbrella에서 SASE 터널을 보려면 Cisco Umbrella에 로그인하고 **Deployments(**구축**) - Core Identities(**코어 **ID) - Network Tunnel(**네트워크 터널**)**로 이동합니다. 위협 방어에서 Umbrella로의 네트워크 터널이 아래 그림과 같이 표시됩니다.



터널의 상세정보를 보려면 섹션을 확장합니다.



Umbrella 자동 터널 문제 해결

구축 후 다음 CLI를 사용하여 Secure Firewall Threat Defense에서 Umbrella 자동 터널과 관련된 문제를 디버깅합니다.

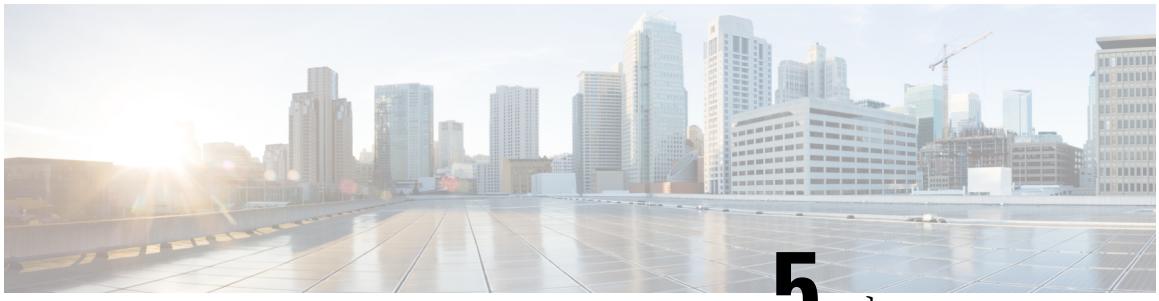
참고 프로덕션 환경의 위협 방어 디바이스에서 디버그 명령을 실행할 때는 주의하십시오. 자세한 정보 표시 출력이 있을 수 있는 디바이스에서 다양한 디버그 레벨을 설정할 수 있습니다.

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**

방법	CLI 명령
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



5 장

보안 연결로 원격 근무자의 권한 강화: DIA, Umbrella 자동 터널, DVTI 활용

이 장에서는 DIA, Umbrella 자동 터널 및 DVTI 사용에 대한 실제 애플리케이션에 대해 자세히 설명합니다. 활용 사례에서는 원활한 구현을 위한 시나리오, 네트워크 토폴로지 및 엔드 투 엔드 절차에 대해 자세히 설명합니다.

DIA, Umbrella SASE 자동 터널 및 DVTI를 사용하여 원격 근무자를 위한 연결성 및 보안 향상

오늘날과 같이 상호 연결된 원격 근무 환경에서 조직은 분산되어 있는 인력을 위해 끊김 없는 연결성, 안전한 액세스, 최적화된 성능을 제공해야 하는 과제에 직면해 있습니다. 이 활용 사례에서는 네트워크 연결 문제를 해결하고, 협업을 개선하며, 민감한 정보를 보호하고, 원격 사용자가 어디서든 효율적으로 작업할 수 있도록 역량을 강화하기 위한 DIA(직접 인터넷 액세스), Umbrella SASE 자동 터널 및 DVTI(Dynamic Virtual Tunnel Interface) 기술을 구현하는 방법을 살펴봅니다.

이 활용 사례가 귀사에 적합합니까?

이 활용 사례의 대상 독자는 네트워크 인프라의 관리 및 보안을 책임지는 IT 전문가, 네트워크 관리자, 의사 결정권자, 그리고 원격으로 근무하는 직원을 위해 연결 및 보안을 최적화하고자 하는 조직입니다. 이 문서에서는 DIA, Umbrella SASE 자동 터널 및 DVTI 기술의 구현에 대한 인사이트를 제공

하고, 원격 근무자가 당면한 문제를 해결하는 데 있어 이러한 기술이 제공하는 이점을 중점적으로 살펴봅니다.

시나리오

Sally는 실시간 협업 및 데이터 액세스에 대한 의존도가 높은 글로벌 기업에서 원격 영업 담당자로 일하고 있습니다. 그녀는 다른 클라이언트 위치를 자주 방문하지만, 판매 데이터에 액세스하고 동료와 커뮤니케이션하는 데 문제가 있습니다.

어떤 위험이 있습니까**?**

이 회사의 기존 네트워크 인프라는 여러 위치에서 끊김 없는 연결 및 보안 액세스를 제공할 수 없어 지연, 데이터 불일치, 통신 단절이 발생하고 있습니다.

허브 앤 스포크 토폴로지에서 **DIA, Umbrella** 자동 터널 및 **DVTI**로 구성된 솔루션은 문제를 어떻게 해결합니까**?**

Sally와 같은 재택근무 근로자가 당면한 문제를 해결하기 위해 그녀의 회사는 DIA, Umbrella SASE 자동 터널 및 DVTI를 사용하는 포괄적인 솔루션을 구현합니다.

1. **DIA**: DIA를 사용하면 Sally는 기업 네트워크를 통해 라우팅하지 않고 인터넷에 직접 연결할 수 있습니다. 이를 통해 더 빠르고 안정적인 인터넷 액세스가 제공되어 클라우드 기반 애플리케이션 및 서비스에 빠르게 액세스할 수 있습니다. 기업 네트워크의 네트워크 트래픽을 오프로드하여 혼잡을 줄이고 성능을 최적화합니다.
2. **Umbrella** 자동 터널**:** Sally의 회사는 Umbrella 자동 터널 설정을 활용하여 Sally가 원격으로 연결되어 있는지 또는 브랜치 방화벽 뒤에 있는지에 관계없이 트래픽에 균일한 보안 정책이 적용되도록 보장합니다. 이를 통해 VPN 연결을 수동으로 구성할 필요가 없으며, 기존 터널 설정과 관련된 복잡성 및 잠재적 오류가 감소합니다. 이 기술은 Sally를 비롯한 조직 내의 원격 근무자들에게 단순성, 편의성, 강화된 보안을 제공합니다.
3. **DVTI:** 허브 앤 스포크 토폴로지의 DVTI를 사용하면 지사와 기업 네트워크 간에 보안 IPsec 터널을 동적으로 생성할 수 있습니다. 이러한 터널은 데이터 전송을 암호화하므로 원격으로 작업하는 동안 기업 리소스에 안전하게 액세스할 수 있습니다. 또한 DVTI는 가장 효율적인 경로를 통해 트래픽을 지능적으로 라우팅하고 중단 없는 연결을 위한 이중화를 제공하여 네트워크 성능을 최적화합니다.

Sally의 회사는 DIA, Umbrella SASE 자동 터널 및 DVTI를 결합하여 재택근무 직원의 연결성, 보안, 생산성을 향상시킵니다. 클라우드 애플리케이션에 빠르게 액세스하고, 동료와 원활하게 협업하며, 위치에 상관없이 기업 리소스에 안전하고 안정적으로 연결합니다. IT 팀은 중앙 집중식 보안 관리, 네트워크 복잡성 감소, 원격 작업자 활동에 대한 향상된 가시성의 이점을 활용합니다.

토폴로지

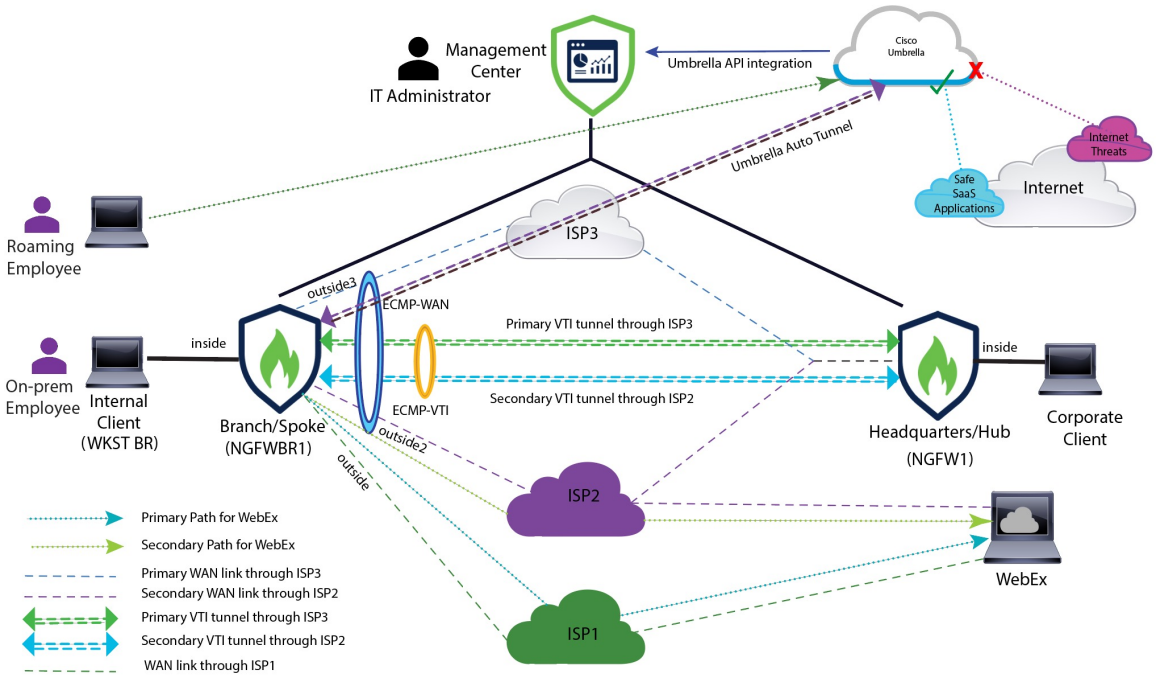
이 토폴로지에서 내부 클라이언트 또는 브랜치 워크스테이션은 WKST BR로 레이블이 지정되고 NGFWBR1로 레이블이 지정된 브랜치 위협 방어에 연결됩니다. 본사 위협 방어에는 NGFW1이라는 레이블이 지정됩니다. 기업 네트워크는 NGFW1을 통해 연결할 수 있습니다. NGFWBR1의 인그레스

인터페이스는 inside로 이름이 지정되고 이그레스 인터페이스는 outside, outside2, outside3으로 각각 지정됩니다.

Umbrella 자동 터널은 NGFWBR1과 Cisco Umbrella 사이에 설정됩니다.

모든 DNS 및 웹 트래픽은 Umbrella 자동 터널을 통해 Cisco Umbrella로 전송되어 Umbrella DNS 및 웹 정책에 따라 허용되거나 차단됩니다. 이는 두 가지 보호 레이어를 제공합니다. 하나는 Cisco Secure Threat Defense에 의해 로컬로 적용되고 다른 레이어는 Cisco Umbrella에 의해 클라우드에서 제공됩니다.

허브 스포크 구성의 경우 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.



DIA, Umbrella 자동 터널 및 **DVTI** 구성을 위한 엔드 투 엔드 절차

DIA, Umbrella SASE 자동 터널 및 DVTI를 사용하여 솔루션을 구성하려면 다음을 수행합니다.

- 직접 인터넷 액세스 구성: 경로 모니터링을 통해 DIA를 구성하기 위한 엔드 투 엔드 절차, 41 페이지
- **Umbrella SIG** 자동 터널 구성: Umbrella 자동 터널 구성을 위한 엔드 투 엔드 절차, 62 페이지
- **DVTI** 허브 앤 스포크 토폴로지 구성: 경로 기반 VPN 구성을 위한 엔드 투 엔드 절차(허브 앤 스포크 토폴로지), 9 페이지

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