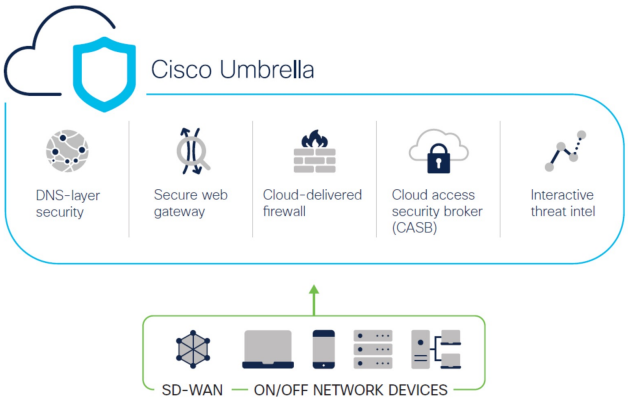
Umbrella 자동 터널을 사용하여 인터넷 트래픽 보호

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 *1: 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.

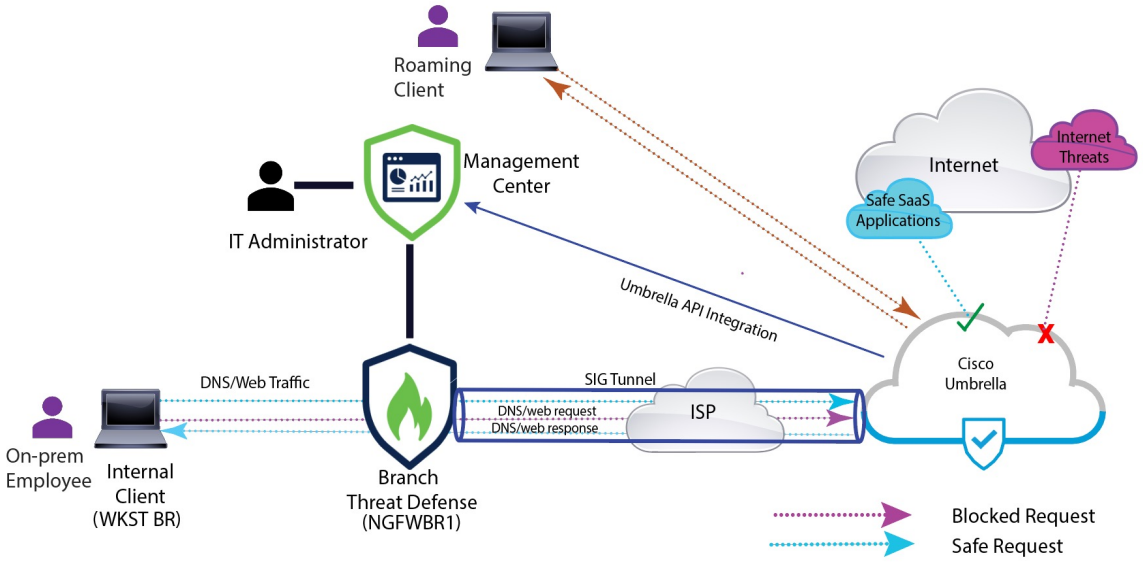
Sally는 일부 웹사이트가 현재 방화벽과 Umbrella에 의해 차단되고 있는 것을 확인합니다.

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 *2: 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.

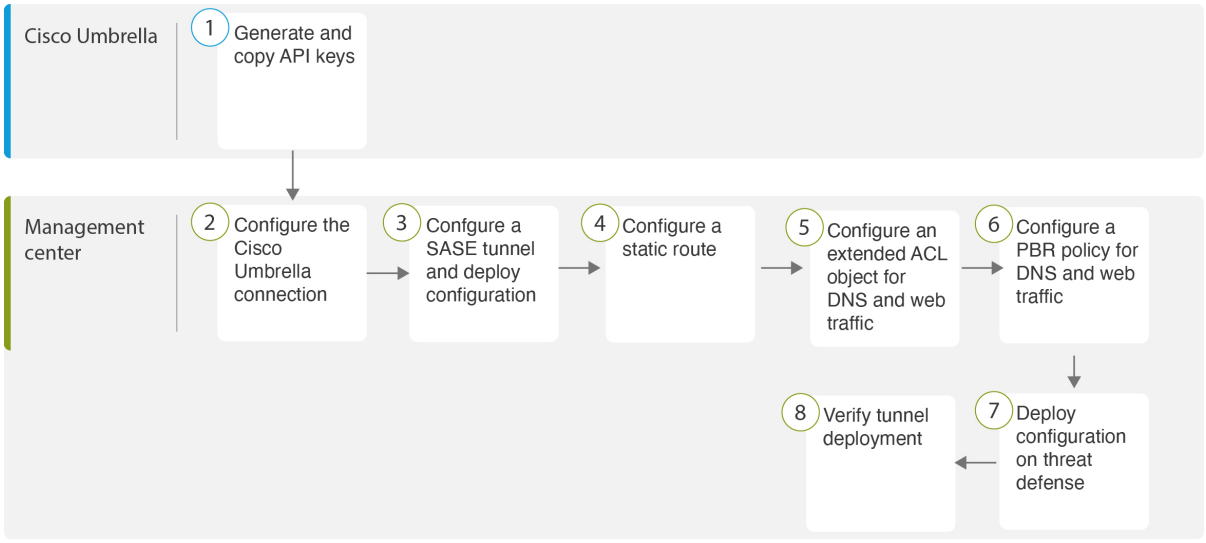
  자세한 내용은 다음 링크를 참조하십시오.

  - 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, 8 페이지의 내용을 참조하십시오.
4	고정 경로를 구성합니다. 고정 경로 구성, 11 페이지의 내용을 참조하십시오.
5	DNS 및 웹 트래픽에 대한 확장 ACL 개체를 구성합니다. DNS 및 웹 트래픽용 확장 ACL 구성, 12 페이지의 내용을 참조하십시오.
6	DNS 및 웹 트래픽에 대한 PBR 정책을 구성합니다. DNS 및 웹 트래픽용 PBR 정책 구성 , 13 페이지의 내용을 참조하십시오.
7	구성을 위협 방어에 구축합니다. 컨피그레이션 구축의 내용을 참조하십시오.
8	터널 구축을 확인합니다. SASE Umbrella 터널 구축 확인, 14 페이지의 내용을 참조하십시오.

Umbrella용 SASE 터널 구성

시작하기 전에

Umbrella SASE 터널 구성을 위한 사전 요건, 5 페이지 및 SASE Umbrella 터널의 모범 사례, 4 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, 11 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.

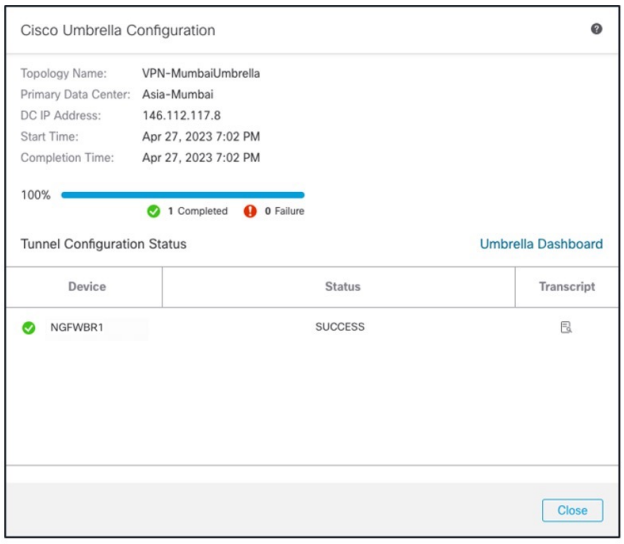
- **Endpoints(**엔드포인트**)** 창: 구성된 위협 방어 엔드포인트의 요약을 표시합니다.
- **Encryption Settings(**암호화 설정**)** 창: SASE 터널의 암호화 설정이 표시됩니다.

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.

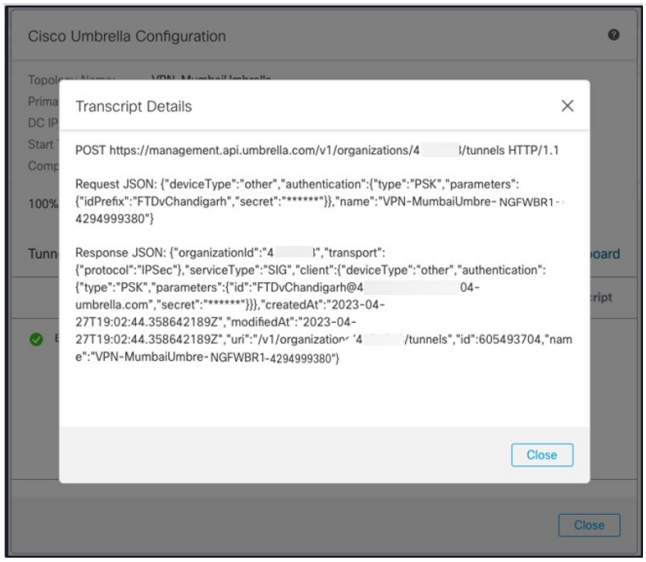
단계 **9** **Save(**저장**)**를 클릭합니다.

이 작업은

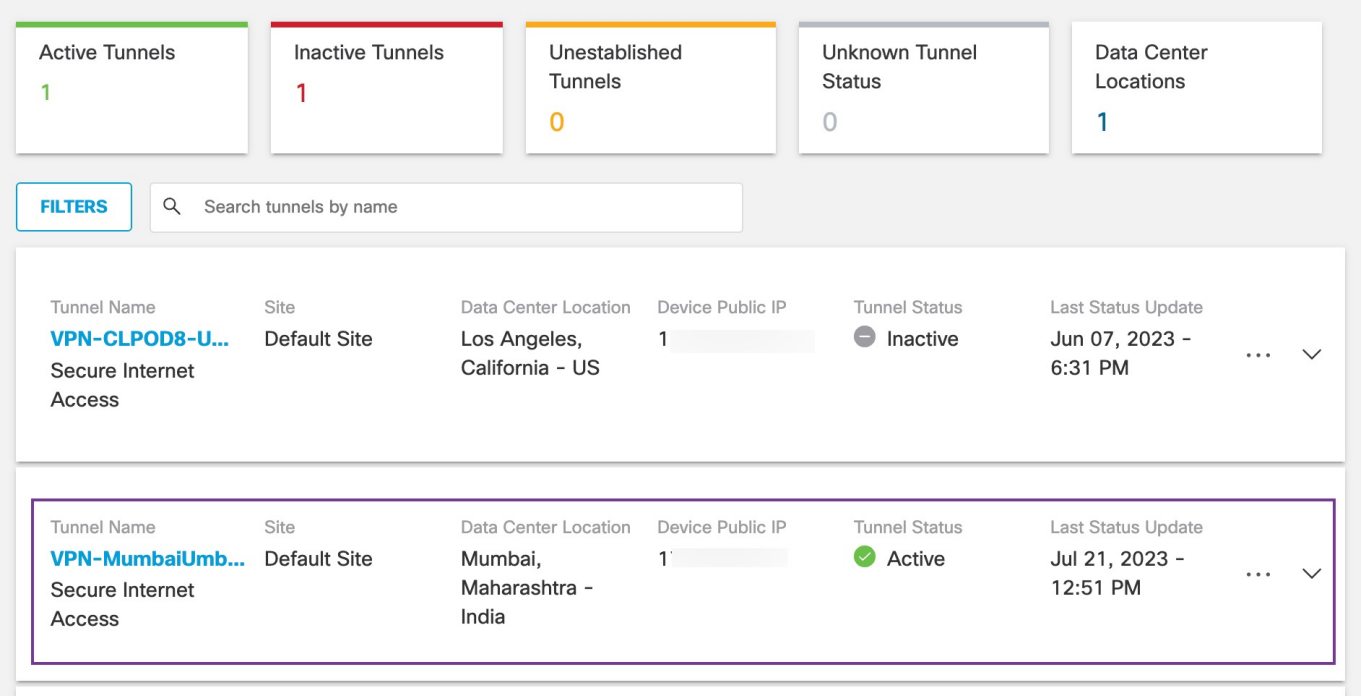
1. 관리 센터에 SASE 토폴로지를 저장합니다.
2. 각 위협 방어 엔드포인트에 대한 네트워크 터널의 Umbrella 구축을 트리거합니다.
3. 옵션이 활성화된 경우 위협 방어 디바이스에 대한 네트워크 터널 구축을 트리거합니다. 이 작업은 디바이스에서 마지막으로 구축한 이후 비 VPN 정책을 포함하여 업데이트된 모든 구성 및 정책을 커밋하고 구축합니다.
4. **Cisco Umbrella Configuration(Cisco Umbrella** 구성**)** 창을 열고 Umbrella에서 터널 구축의 상태를 표시합니다.



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.

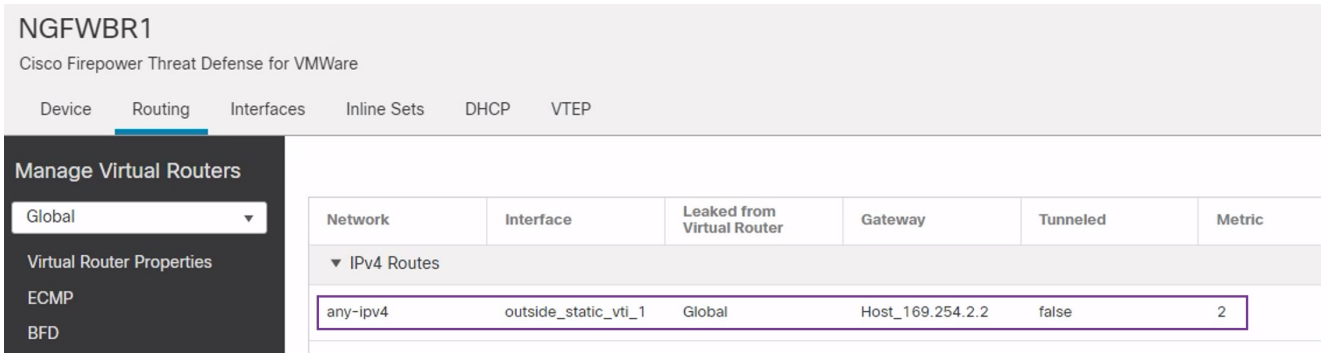
단계 **6** **Available Networks(**사용 가능한 네트워크**)** 상자에서 대상 네트워크로 **any-ipv4**를 선택하고 **Add(**추가**)**를 클릭합니다.

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.

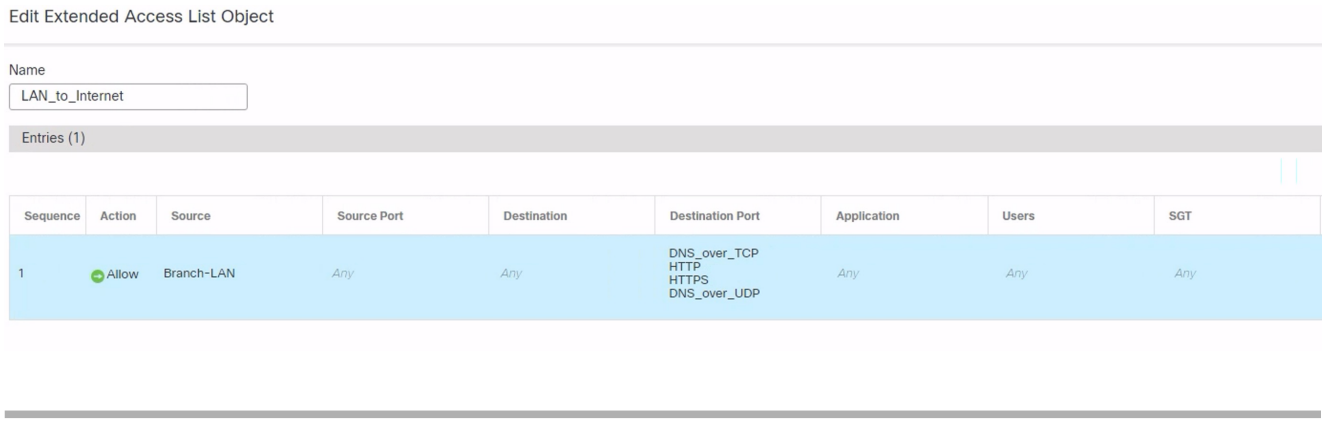
단계 5 다음 액세스 제어 속성을 구성합니다.

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.

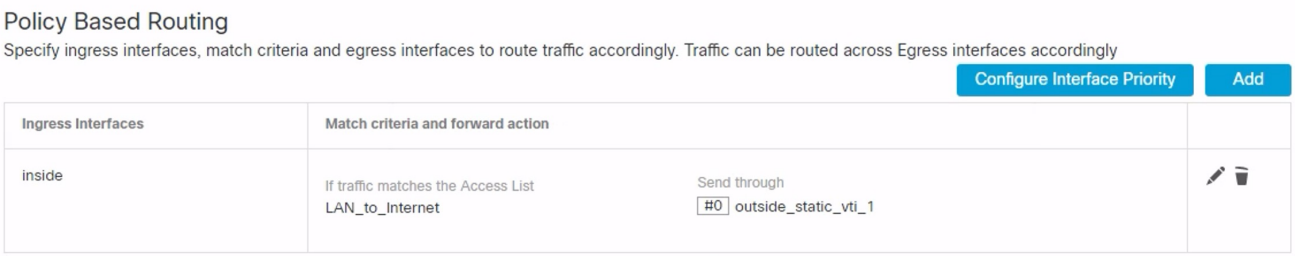
c) **Available Interfaces(**사용 가능한 인터페이스**)**에서 **Outside_static_vti_1** 인터페이스에 인접한 **Add(**추가**)** (+) 아이콘을 클릭하여 이를 **Selected Egress Interfaces(**선택한 이그레스 인터페이스**)**로 이동합니다.

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.

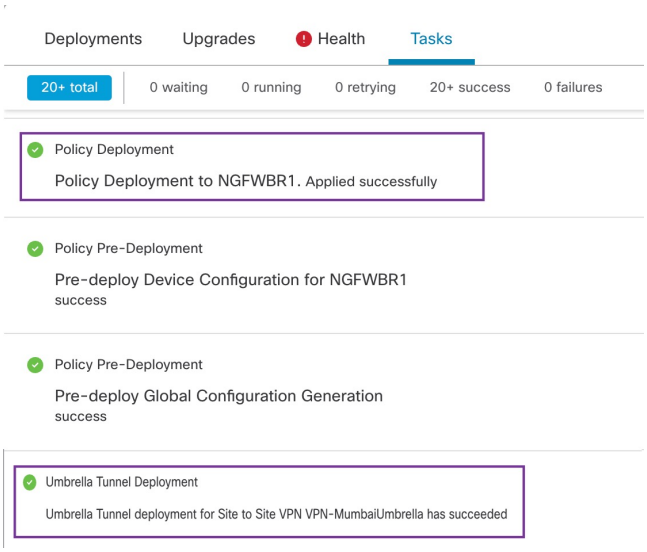
단계 **4** 구축할 변경 사항에서 오류나 경고를 식별하면 시스템은 **Validation Messages(**검증 메시지**)** 또는 **Validation Warnings(**검증 경고**)** 창에 이를 표시합니다. 전체 세부 정보를 보려면 Validation Errors(검증 오류) 또는 Validation Warnings(검증 경고) 링크를 클릭합니다.

다음 옵션을 이용할 수 있습니다.

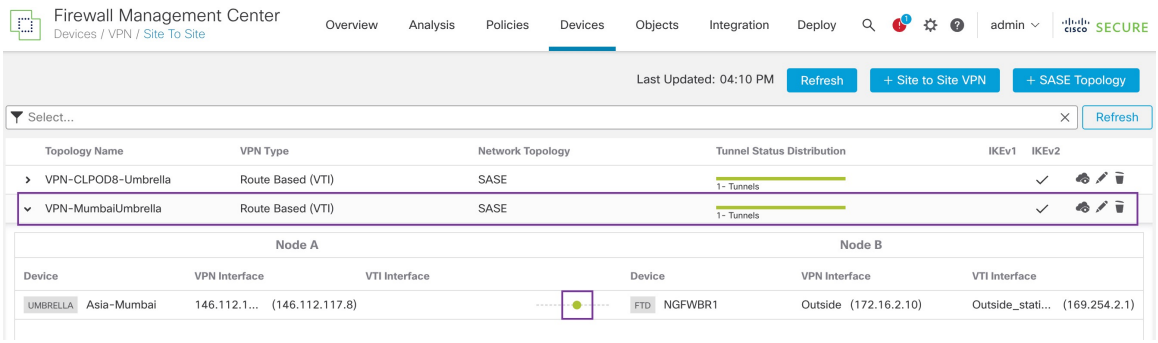
- Proceed with Deploy(구축 계속) - 경고 조건을 해결하지 않고 구축을 계속합니다. 오류가 식별되는 경우 계속 진행할 수 없습니다.
- Close(닫기) -구축하지 않고 종료합니다. 오류 및 경고 조건을 해결하고 컨피그레이션을 재구축합니다.

SASE Umbrella 터널 구축 확인

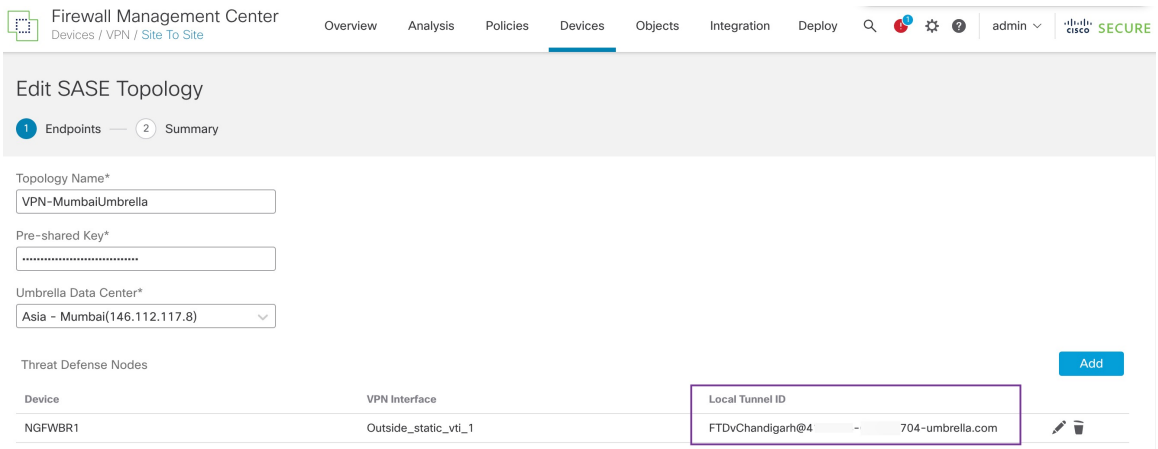
관리 센터에서 위협 방어 디바이스(NGFWBR1)에서 Umbrella 터널 구축 및 정책 구축 상태를 확인하려면 **Notifications(**알림**) - Task(**작업**)**로 이동합니다.



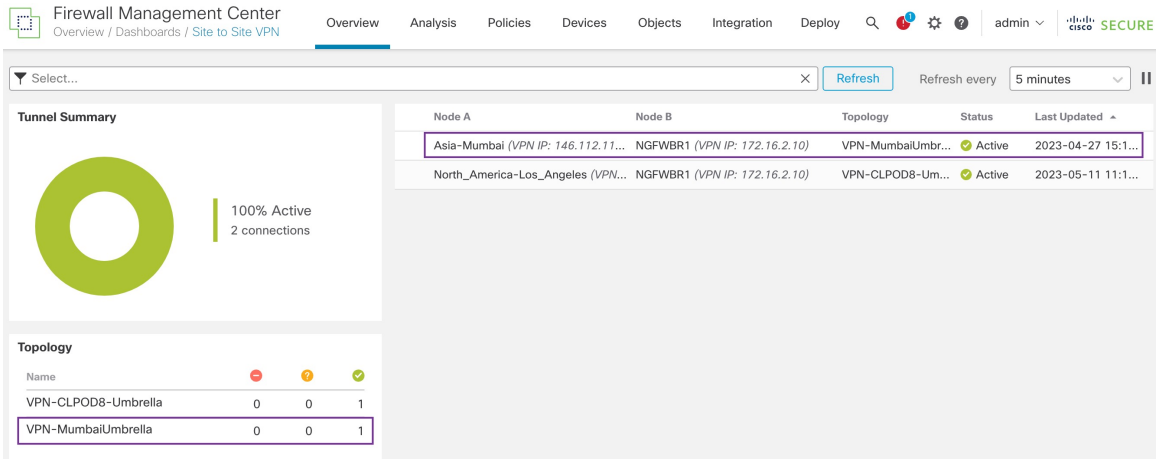
관리 센터에서 SASE 자동 터널 상태를 확인하려면 **Devices(**디바이스**)** → **VPN(VPN)** → **Site To Site(**사이트 간**)**를 선택합니다.



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.

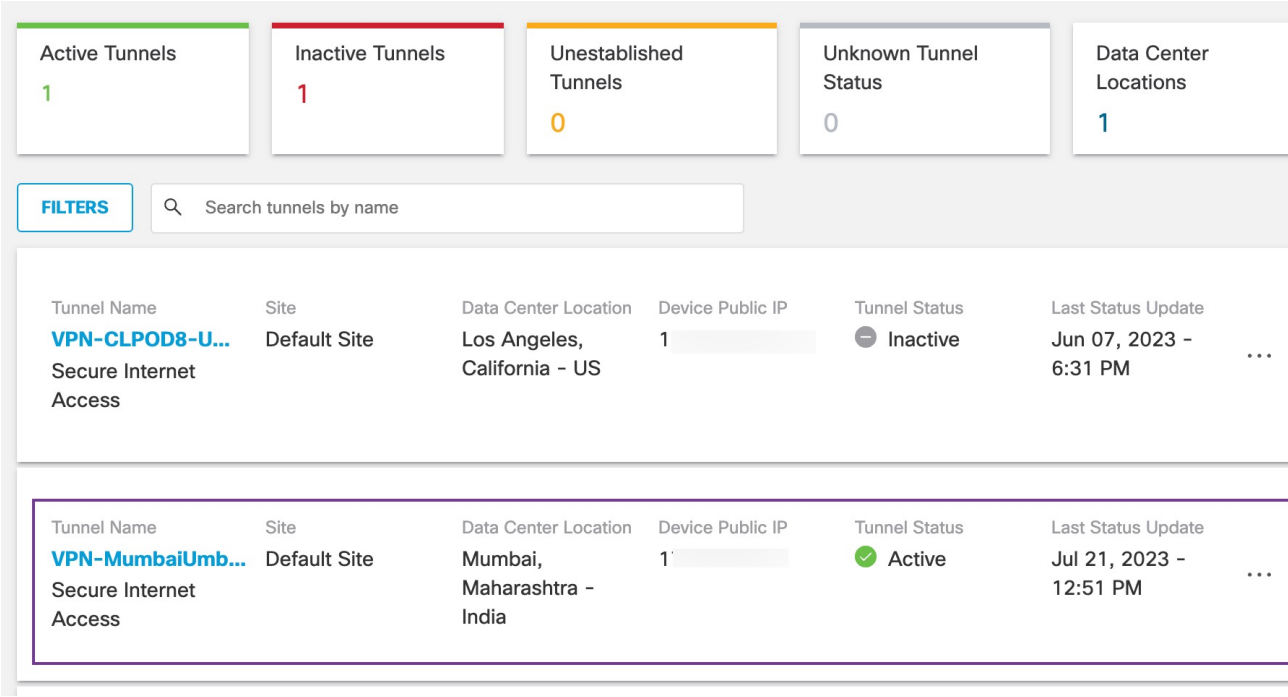
```
> show interface ip brief

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.

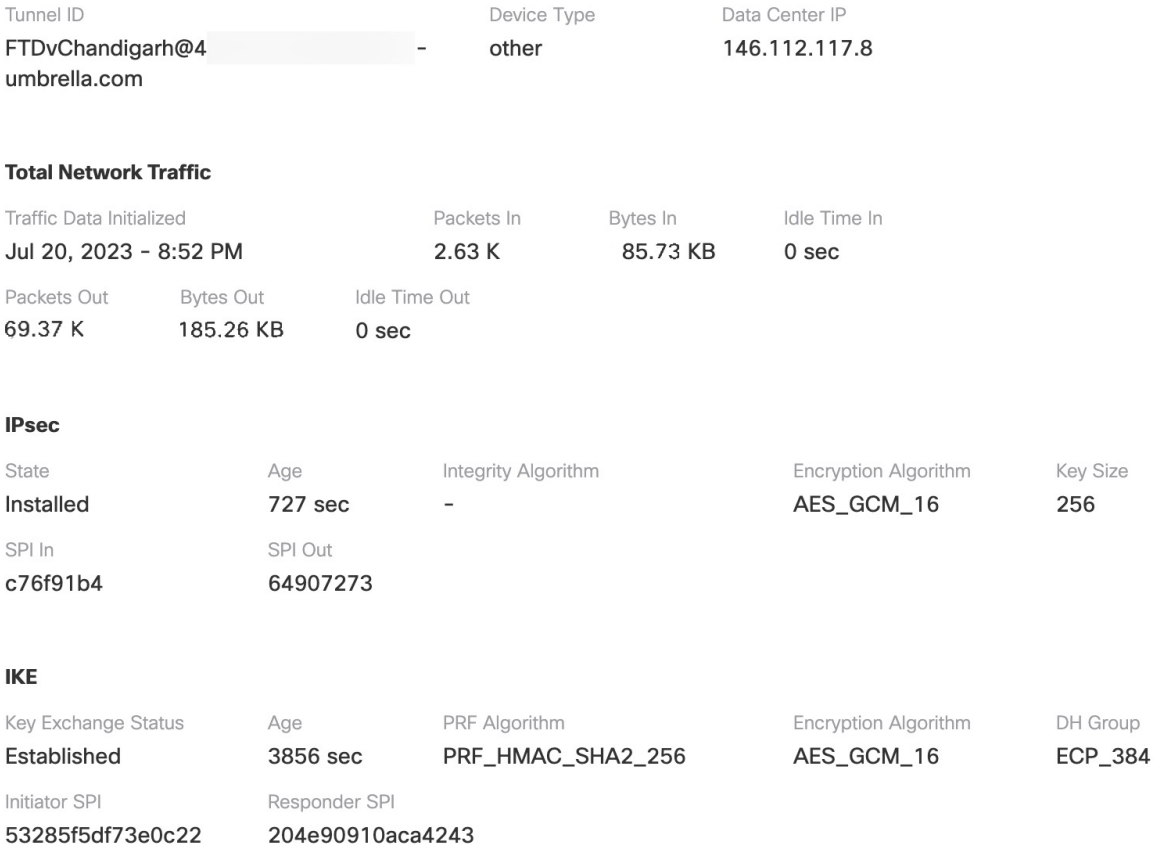
```
> show crypto ipsec sa
interface: outside_static_vti_1
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr:
198.18.128.81

      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