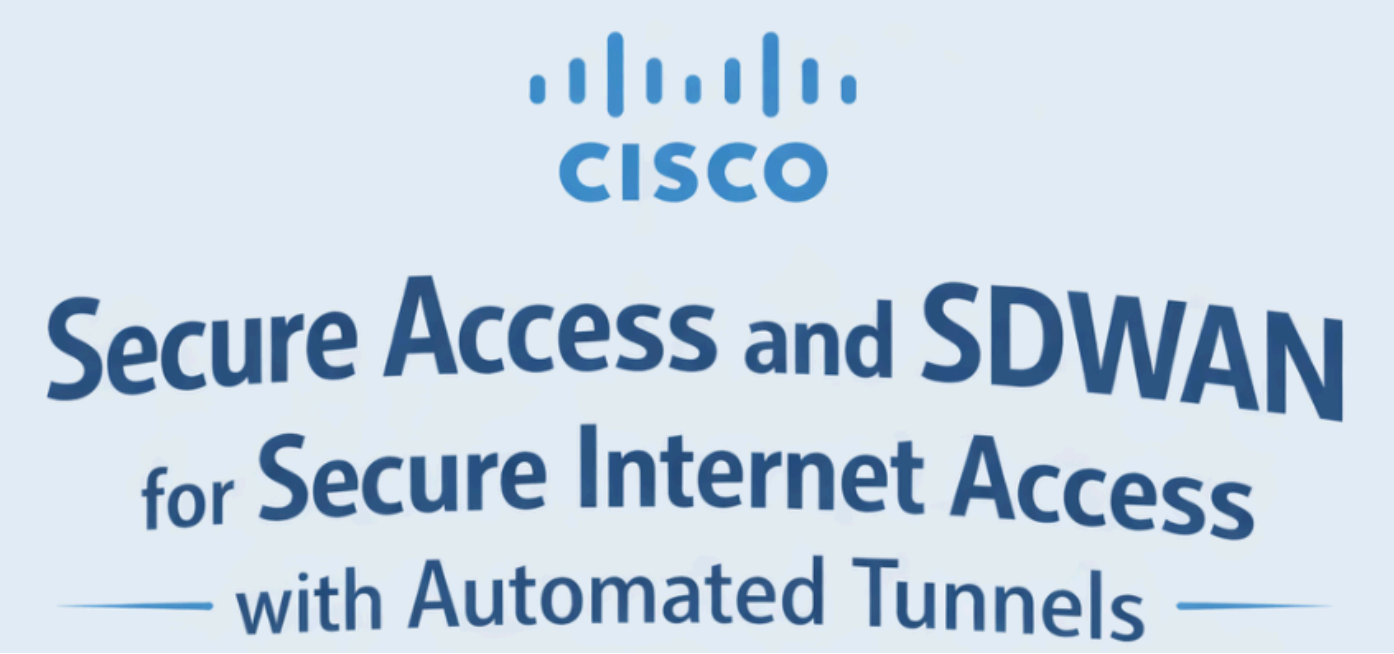
보안 인터넷 액세스를 위한 SD-WAN 자동 터널로 보안 액세스 구성

목차

- 소개
- 배경 정보
- 네트워크 다이어그램
- 사전 요구 사항
  - 요구 사항
  - 사용되는 구성 요소
- 구성
  - 보안 액세스 컨피그레이션
    - API 생성
  - SD-WAN 컨피그레이션
    - API 통합
    - 정책 그룹 구성
  - SD-WAN에서 사용자 지정 Bypass FQDN 또는 앱 만들기(선택 사항)
  - 트래픽 라우팅
- 다음을 확인합니다.
  - 보안 액세스 - 활동 검색
  - 보안 액세스 - 이벤트
  - Catalyst SD-WAN Manager - 네트워크 전반에 걸친 경로 통찰력
- 관련 정보

소개

이 문서에서는 보안 인터넷 액세스를 위해 SD-WAN 자동 터널로 보안 액세스를 구성하는 방법에 대해 설명합니다.



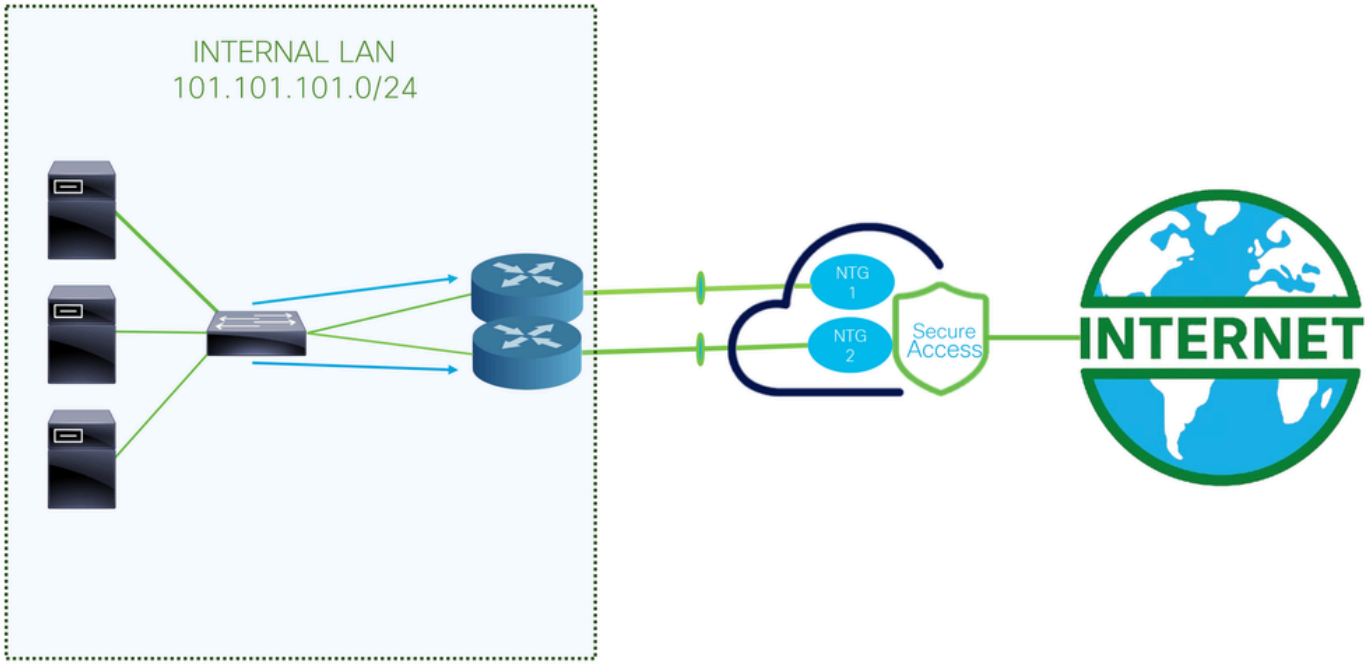
배경 정보

조직에서 클라우드 기반 애플리케이션을 점점 더 많이 채택하고 분산된 인력을 지원함에 따라 네트워크 아키텍처는 리소스에 대한 안전하고 안정적이며 확장 가능한 액세스를 제공하도록 진화해야 합니다. SASE(Secure Access Service Edge)는 네트워킹과 보안을 단일 클라우드 제공 서비스로 통합하는 프레임워크로서, SD-WAN 기능과 보안 원격 액세스를 위한 SWG(Secure Web Gateway), CASB(Cloud Access Security Broker), DNS 레이어 보안, ZTNA(Zero Trust Network Access) 또는 통합 VPN과 같은 고급 보안 기능을 결합합니다.

자동화된 터널을 통해 Cisco Secure Access를 SD-WAN과 통합하면 인터넷 트래픽을 안전하고 효율적으로 라우팅할 수 있습니다. SD-WAN은 지능적인 경로 선택과 분산된 위치 전반에 걸쳐 최적화된 연결을 제공하는 반면, Cisco Secure Access는 모든 트래픽이 인터넷에 도달하기 전에 기업 보안 정책에 따라 검사되고 보호되도록 보장합니다.

SD-WAN 디바이스와 Secure Access 간의 터널 구성을 자동화함으로써 조직은 구축을 간소화하고 확장성을 개선하며 위치에 관계없이 사용자의 일관된 보안 적용을 보장할 수 있습니다. 이러한 통합은 최신 SASE 아키텍처의 핵심 구성 요소로, 지사, 원격 사이트 및 모바일 사용자에게 안전한 인터넷 액세스를 제공합니다.

네트워크 다이어그램



이 컨피그레이션 예에 사용되는 아키텍처입니다. 보시다시피 2개의 에지 라우터가 있습니다.

두 개의 다른 디바이스에 정책을 구축하도록 선택하는 경우 각 라우터에 대해 NTG가 구성되고 NAT가 보안 액세스 측에서 활성화됩니다. 그러면 두 라우터가 터널을 통해 동일한 소스에서 트래픽을 전송할 수 있습니다. 일반적으로 이는 허용되지 않습니다. 그러나 이러한 터널에 대해 NAT 옵션을 활성화하면 두 에지 라우터가 동일한 소스 주소에서 시작되는 트래픽을 전송할 수 있습니다.

사전 요구 사항

요구 사항

- 보안 액세스 지식
- Cisco Catalyst SD-WAN Manager 릴리스 20.15.1 및 Cisco IOS XE Catalyst SD-WAN 릴리스 17.15.1 이상
- 라우팅 및 스위칭에 대한 중간 지식
- ECMP 지식
- VPN 지식

사용되는 구성 요소

- 보안 액세스 테넌트
- Catalyst SD-WAN Manager 릴리스 20.18.1 및 Cisco IOS XE Catalyst SD-WAN 릴리스 17.18.1
- Catalyst SD-WAN Manager

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

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

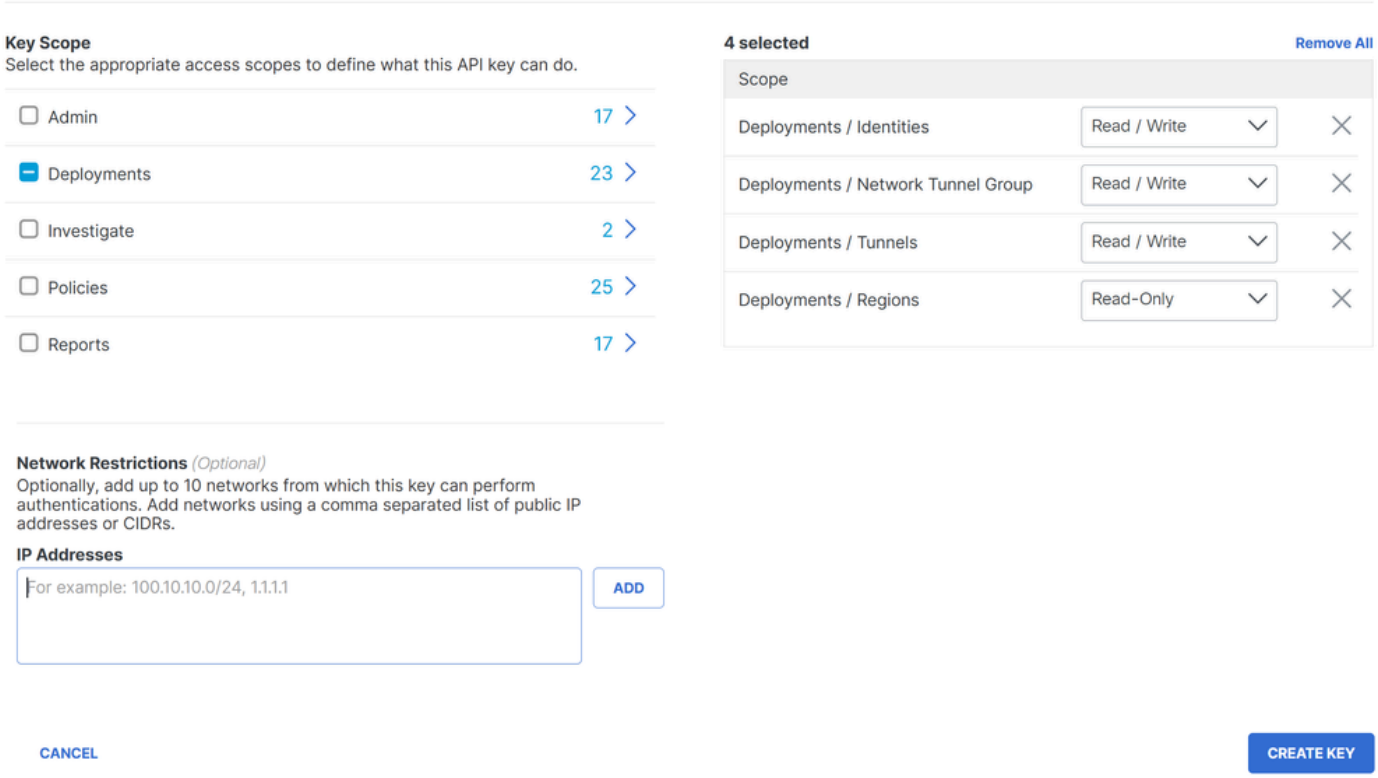
보안 액세스 컨피그레이션

API 생성

Secure Access를 통해 자동 터널을 생성하려면 다음 단계를 확인하십시오.

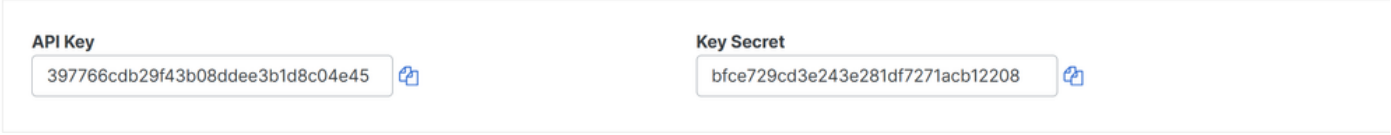
Secure Access Dashboard(보안 액세스 대시보드)로 이동합니다.

- 클릭 Admin > API Keys
- 클릭 Add
- 다음 옵션을 선택합니다.
  - Deployments / Network Tunnel Group: 읽기/쓰기
  - Deployments / Tunnels: 읽기/쓰기
  - Deployments / Regions: 읽기 전용
  - Deployments / Identities: 읽기-쓰기
  - Expiry Date: 만료 안 함



참고: 선택적으로, 이 키가 인증을 수행할 수 있는 최대 10개의 네트워크를 추가합니다. 쉼표로 구분된 공용 IP 주소 또는 CIDR 목록을 사용하여 네트워크를 추가합니다.

- 및 의 생성을 완료하려면CREATE KEY을API Key클릭합니다Key Secret.



⚠ 주의: 클릭하기 전에 복사합니다ACCEPT AND CLOSE. 그렇지 않으면 다시 만들고 복사되지 않은 파일을 삭제해야 합니다.

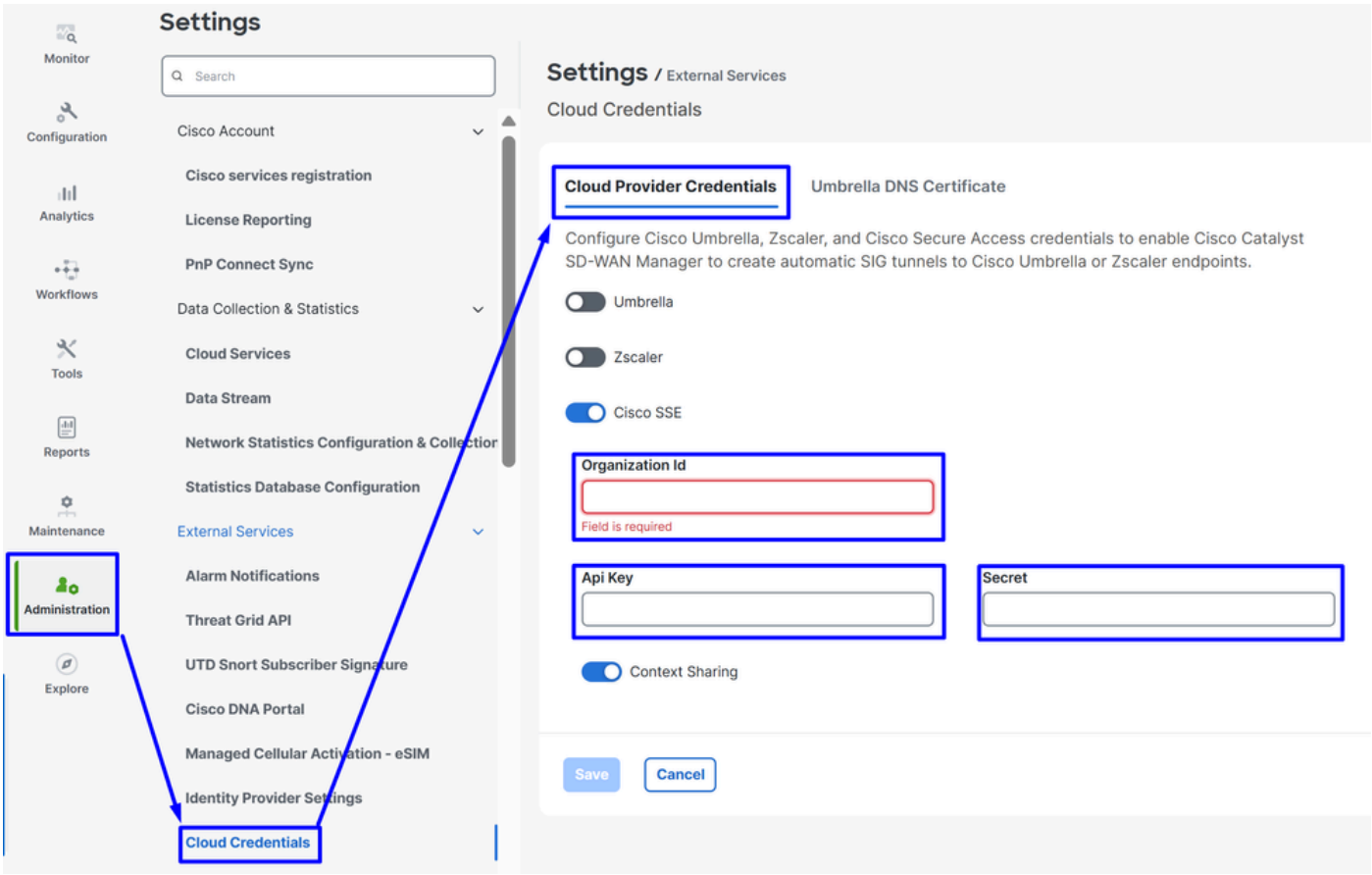
그런 다음 을 클릭하여 마무리합니다ACCEPT AND CLOSE.

SD-WAN 컨피그레이션

API 통합

Catalyst SD-WAN Manager로 이동합니다.

- **Administration** >Settings> Cloud Credentials
- 그런 다음Cloud Provider Credentials클릭하고 APICisco SSE및 조직 설정을 활성화하고 채웁니다



- Organization ID: SSE Dashboard(SSE 대시보드)의 URL에서 가져올 수 있습니다 https://dashboard.sse.cisco.com/org/xxxxx
- Api

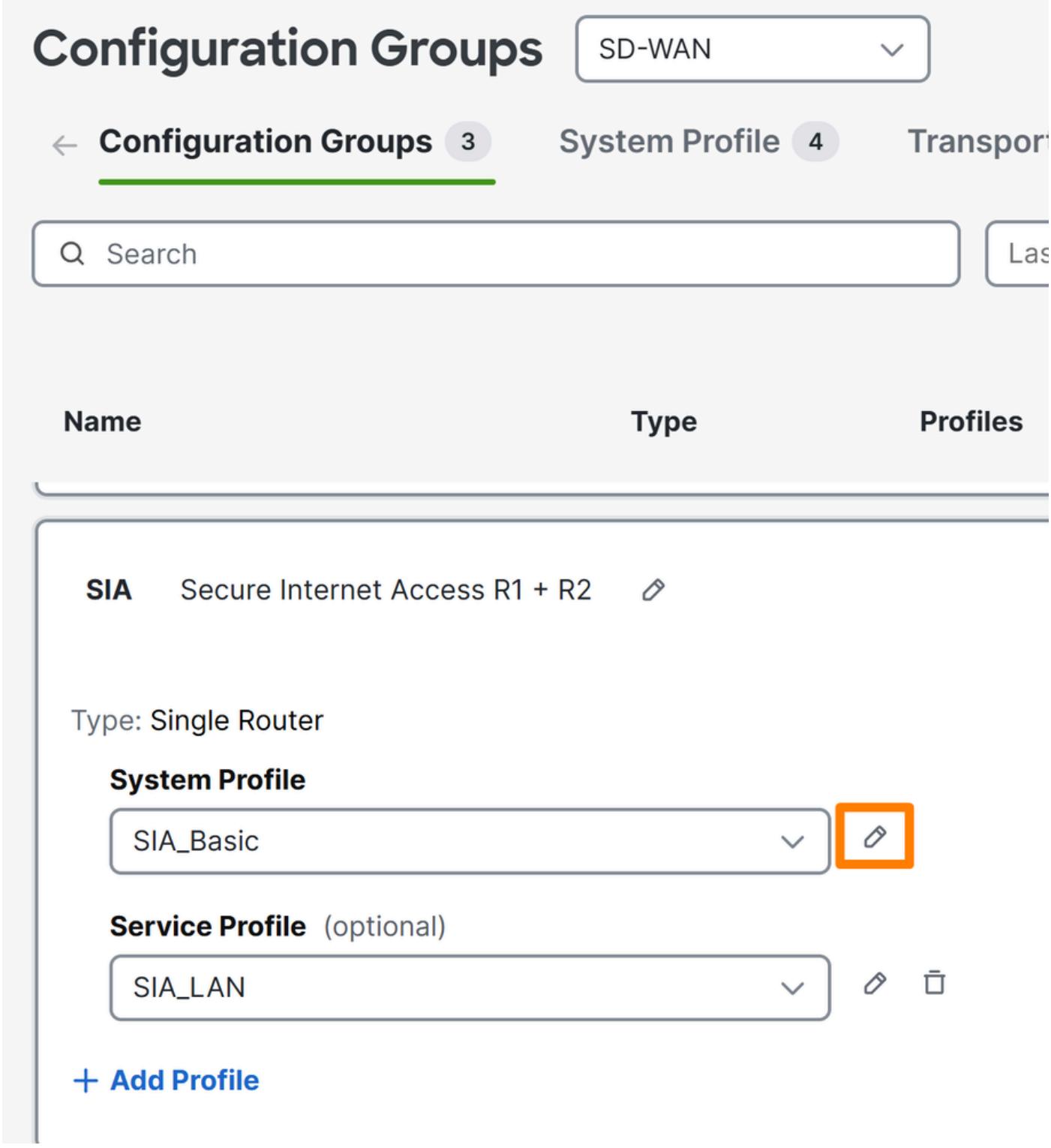
Key: Secure Access Configuration 단계에서 복사합니다.
- Secret: Secure Access Configuration 단계에서 복사합니다.

그런 다음 버튼을Save클릭합니다.

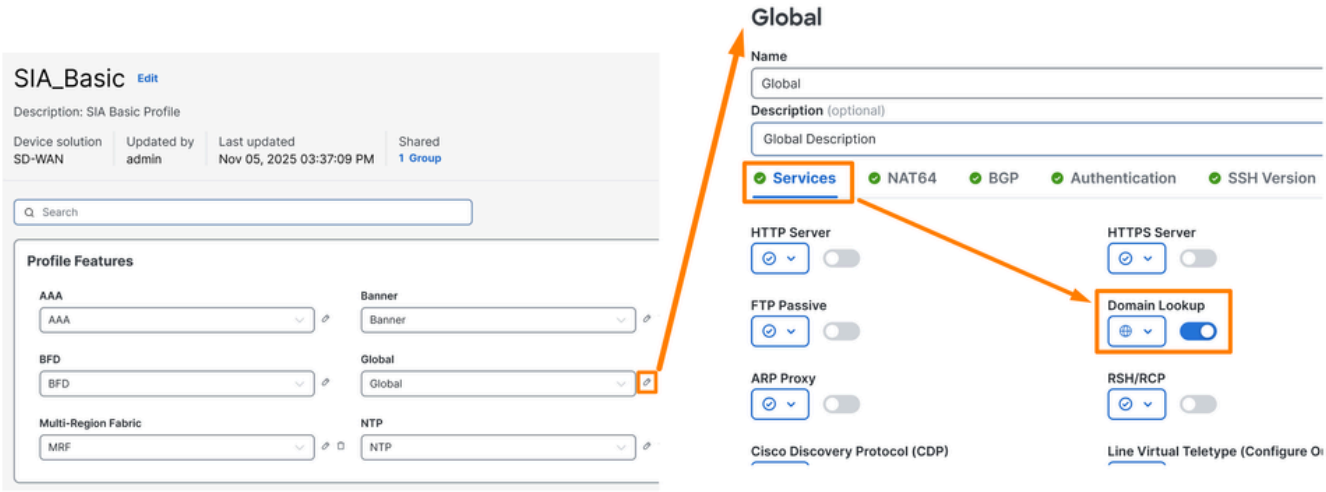
참고: 다음 단계를 진행하기 전에 SD-WAN 관리자 및 Catalyst SD-WAN 에지에 DNS 확인 및 인터넷 액세스가 있는지 확인해야 합니다.

DNS-Lookup이 활성화되어 있는지 확인하려면 다음으로 이동하십시오.

- Configuration(컨피그레이션) > Configuration Groups(컨피그레이션 그룹)를 클릭합니다.
- 에지 디바이스의 프로필을 클릭하고 시스템 프로필을 수정합니다



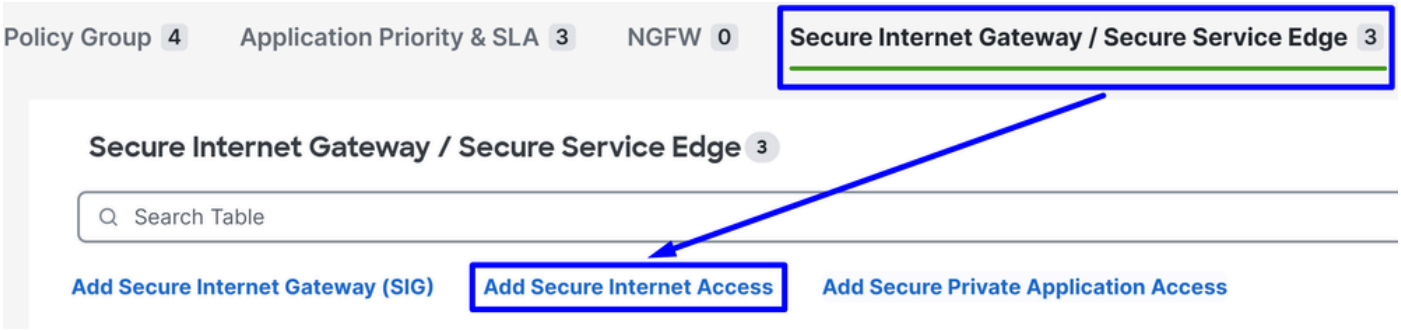
- 그런 다음 Global(전역) 옵션을 수정하고 Domain Resolution(도메인 확인) 옵션이 활성화되었는지 확인합니다



정책 그룹 구성

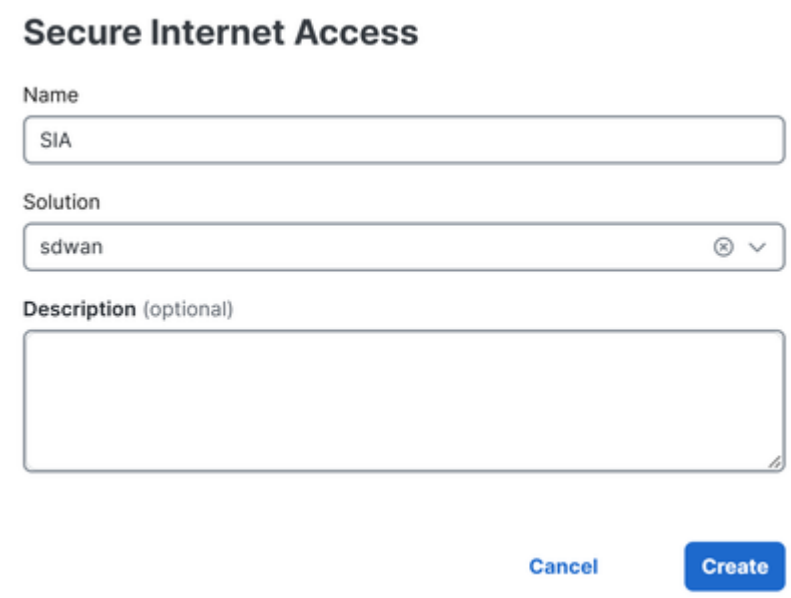
Configuration(컨피그레이션) > Policy Groups(정책 그룹)로 이동합니다.

- Secure Internet Gateway / Secure Service Edge> 를 클릭합니다. *Add Secure Internet Access*

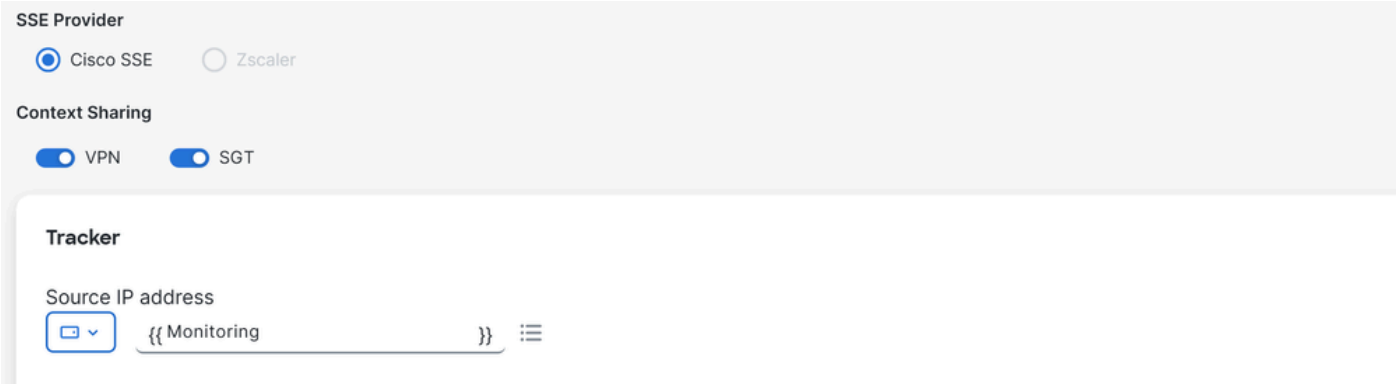


참고: 20.18 이하 릴리스에서는 이 옵션을 SSE(Add Secure Service Edge)라고 합니다.

- 이름, 솔루션을 구성하고 Create

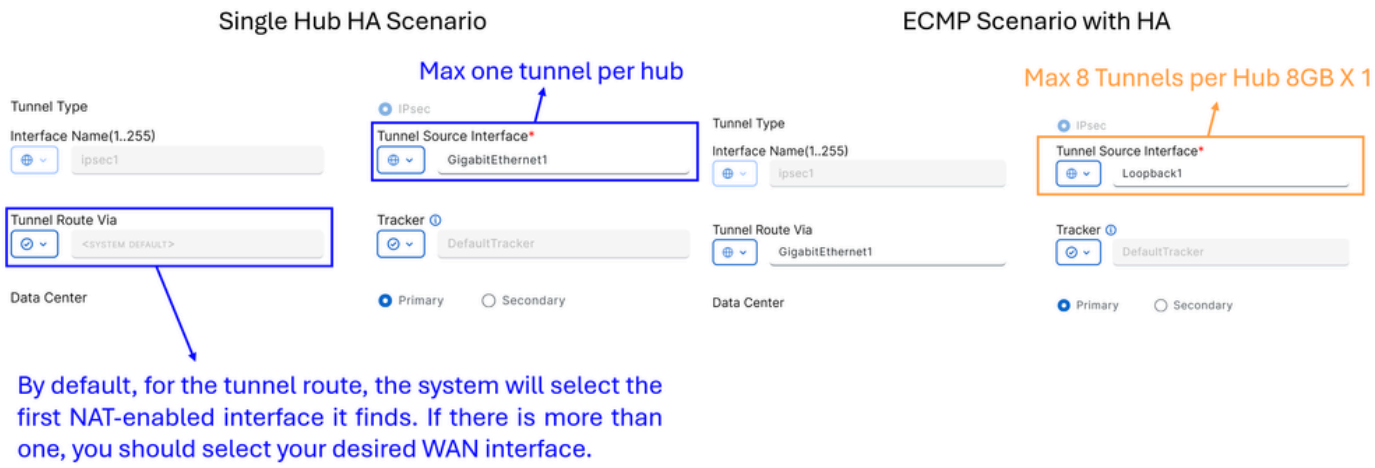


다음 컨피그레이션에서는 Catalyst SD-WAN 에지에서 컨피그레이션을 구축한 후 터널을 생성할 수 있습니다.



- SSE Provider: SSE
- Context Sharing: 필요에 따라 VPN 또는 SGT를 선택합니다.
- Tracker
  - **Source IP Address**: Device Specific(디바이스별)을 선택합니다(이렇게 하면 디바이스별로 수정하고 구축 단계에서 해당 활용 사례를 식별할 수 있음).

이 단계에서Configuration터널을 설정합니다.

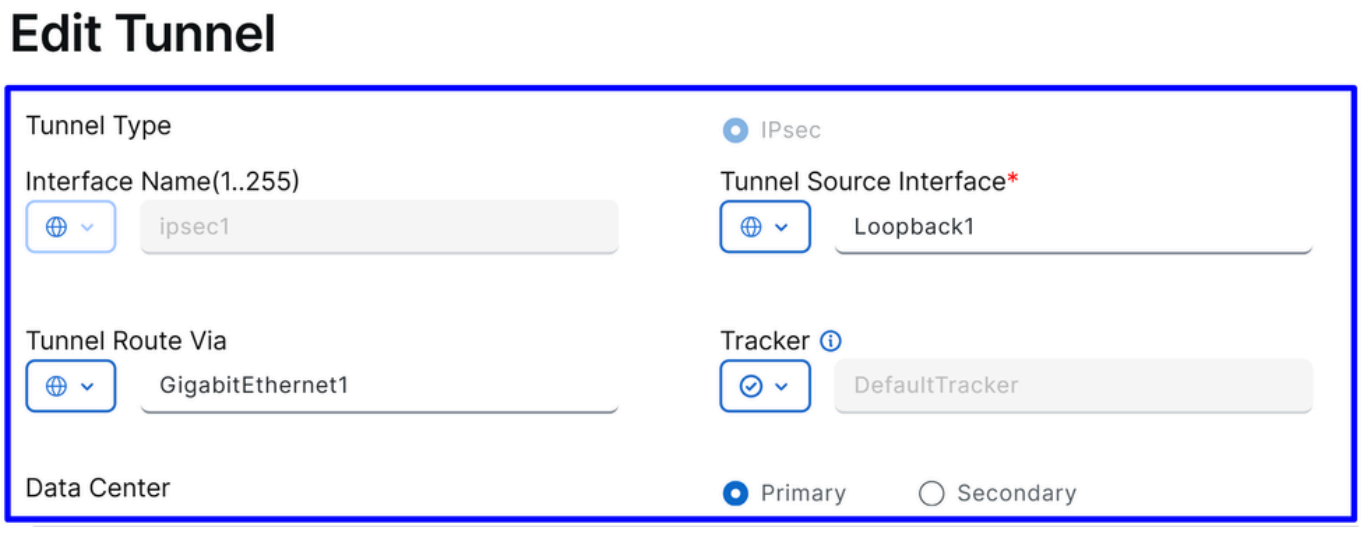


- **Single Hub HA Scenario**: 이 시나리오에서는 하나의 NTG를 액티브로 사용하고 다른 NTG를 패시브로 사용하여 고가용성을 구성할 수 있으며, NTG당 최대 처리량은 1Gbps입니다
- ECMP Scenario with HA: 이 시나리오에서는 허브당 최대 8개의 터널을 구성하여 NTG당 총 16개의 터널을 지원할 수 있습니다. 이 설정을 통해 터널 전반의 처리량이 향상됩니다

참고: 네트워크 인터페이스의 처리량이 1Gbps보다 크고 확장성이 필요한 경우 루프백 인터페이스를 사용해야 합니다. 그렇지 않으면 디바이스에서 표준 인터페이스를 사용할 수 있습니다. 이는 보안 액세스 측에서 ECMP를 활성화하기 위한 것입니다.

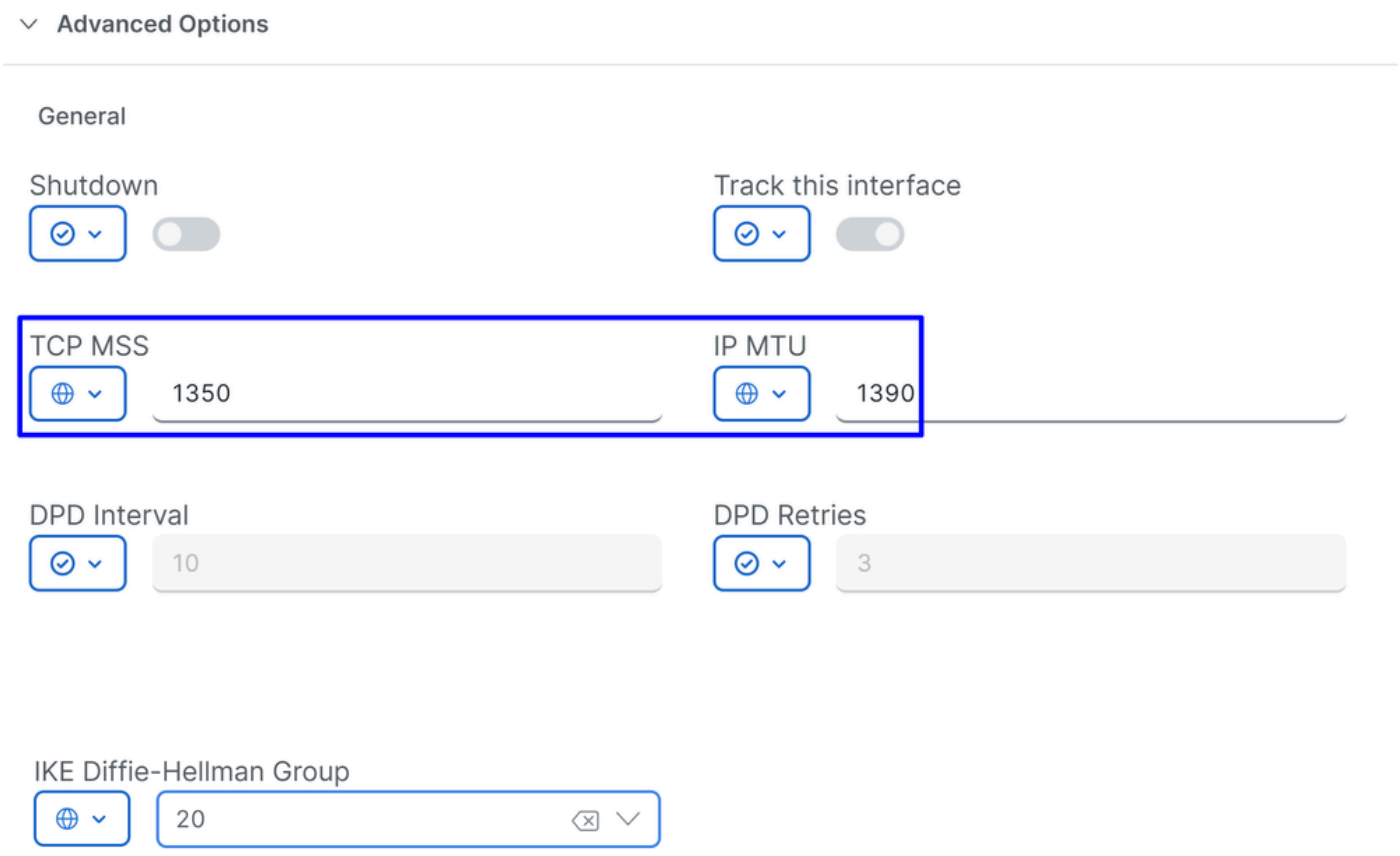
경고: ECMP 시나리오에 대한 루프백 인터페이스를 구성하려면 먼저 >Configuration GroupsTransport & Management Profile에서 라우터에서 사용하는 정책에서 루프백 인터페이스를 설정해야 합니다.

- 클릭Add Tunnel



- Interface Name: ipsec1, ipsec2, ipsec3 등
- Tunnel Source Interface: 루프백 인터페이스 또는 터널을 설정한 특정 인터페이스를 선택합니다
- **Tunnel Route Via**: Loopback(루프백)을 선택하는 경우 트래픽을 라우팅할 물리적 인터페이스를 선택해야 합니다. Loopback(루프백)을 선택하지 않으면 이 옵션이 회색으로 표시되었으며 시스템에서 제공하는 첫 번째 NAT 지원 인터페이스를 사용합니다. 둘 이상인 경우 원하는 WAN 인터페이스를 선택해야 합니다
- **Data Center**: 즉, Secure Access에서 어떤 허브가 연결을 설정하는지를 의미합니다

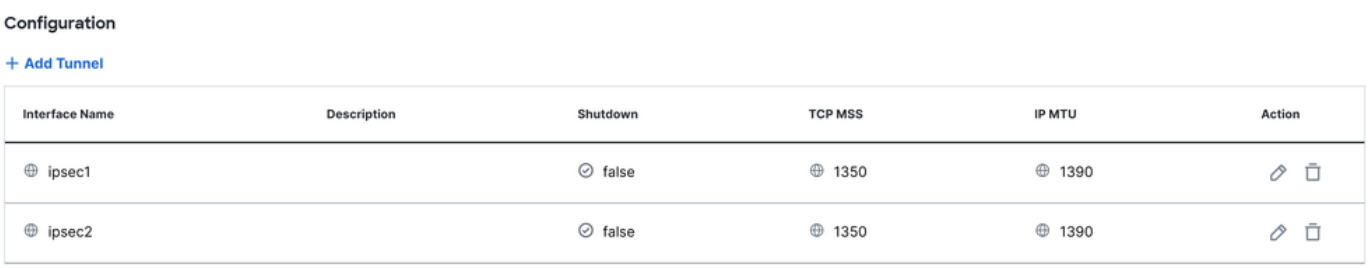
터널 컨피그레이션의 다음 부분에서는 Cisco에서 제공하는 모범 사례를 사용하여 터널을 구성합니다.



- TCP MSS: 1350
- IP MTU: 1390
- IKE Diffie-Hellman Group: 20

그런 다음 보조 데이터 센터를 가리키는 보조 터널을 구성해야 합니다.

단일 허브 HA 시나리오



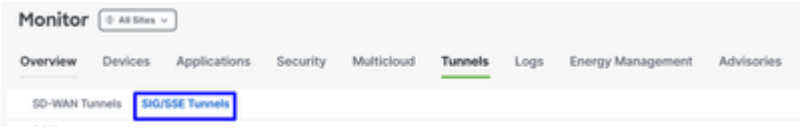
이는 일반 시나리오 구축을 사용할 때의 최종 결과입니다.

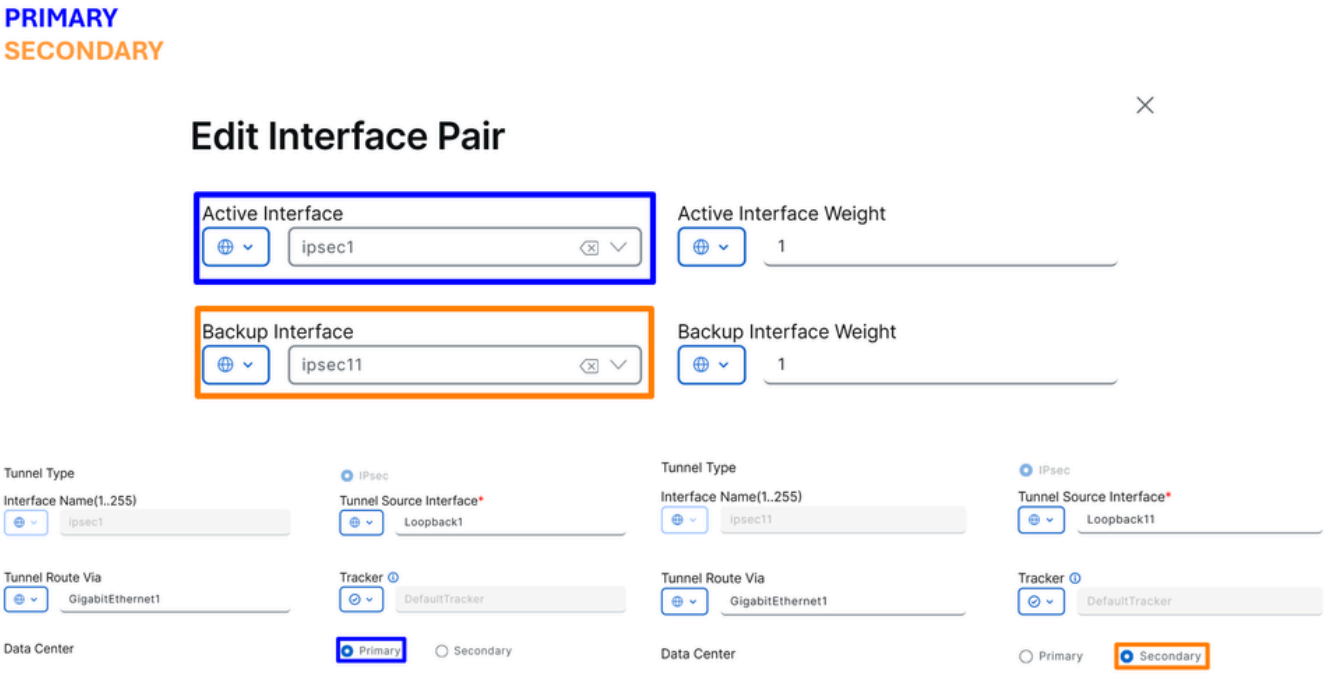
ECMP SCENARIO WITH HA

Interface Name	Description	Shutdown	TCP MSS	IP MTU
ipsec1		false	1350	1390
ipsec2		false	1350	1390
ipsec3	PRIMARY HUB	false	1350	1390
ipsec4		false	1350	1390
ipsec5		false	1350	1390
ipsec11		false	1350	1390
ipsec12		false	1350	1390
ipsec13	SECONDARY HUB	false	1350	1390
ipsec14		false	1350	1390
ipsec15		false	1350	1390

그런 다음 보안 인터넷 정책에서 고가용성을 구성해야 합니다.

Add Interface Pair(인터페이스 쌍 추가):



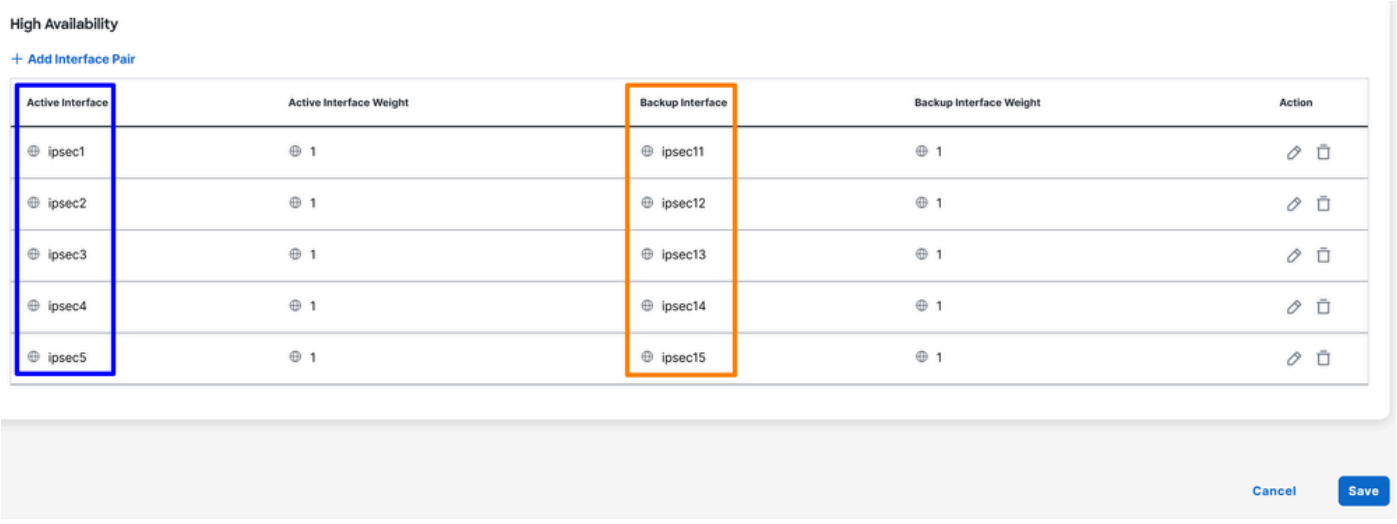


이 단계에서는 설정 중인 각 터널 쌍에 대해 기본 및 보조 터널을 구성해야 합니다. 즉, 각 터널에는 고유한 백업이 있습니다. 이러한 터널은 이러한 용도로 Primary 및 Secondary로 생성되었습니다. "Active interface"은 기본 터널을 나타내고 "Backup interface"은 보조 터널을 나타냅니다.

- Active Interface: 기본
- Backup Interface: 보조

경고: 이 단계를 건너뛰면 터널이 나타나지 않으며 라우터에서 Secure Access로의 연결이 설정되지 않습니다.

터널에 대해 High Availability가 구성되면 아래 이미지와 같이 설정이 표시됩니다. 이 가이드에 사용된 랩 예에서는 HA에 5개의 터널이 표시되어 있습니다. 필요에 따라 터널 수를 조정할 수 있습니다.



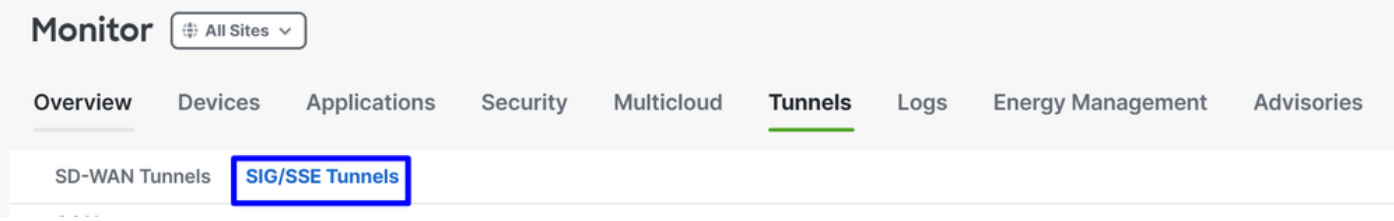
참고: 최대 8개의 터널 쌍(터널 16개: 8 기본 및 8 보조)는 SD-WAN Catalyst vManage에서 구성할 수 있습니다. Cisco Secure Access는 최대 10개의 터널 쌍을 지원합니다.

- 을 클릭합니다 Save

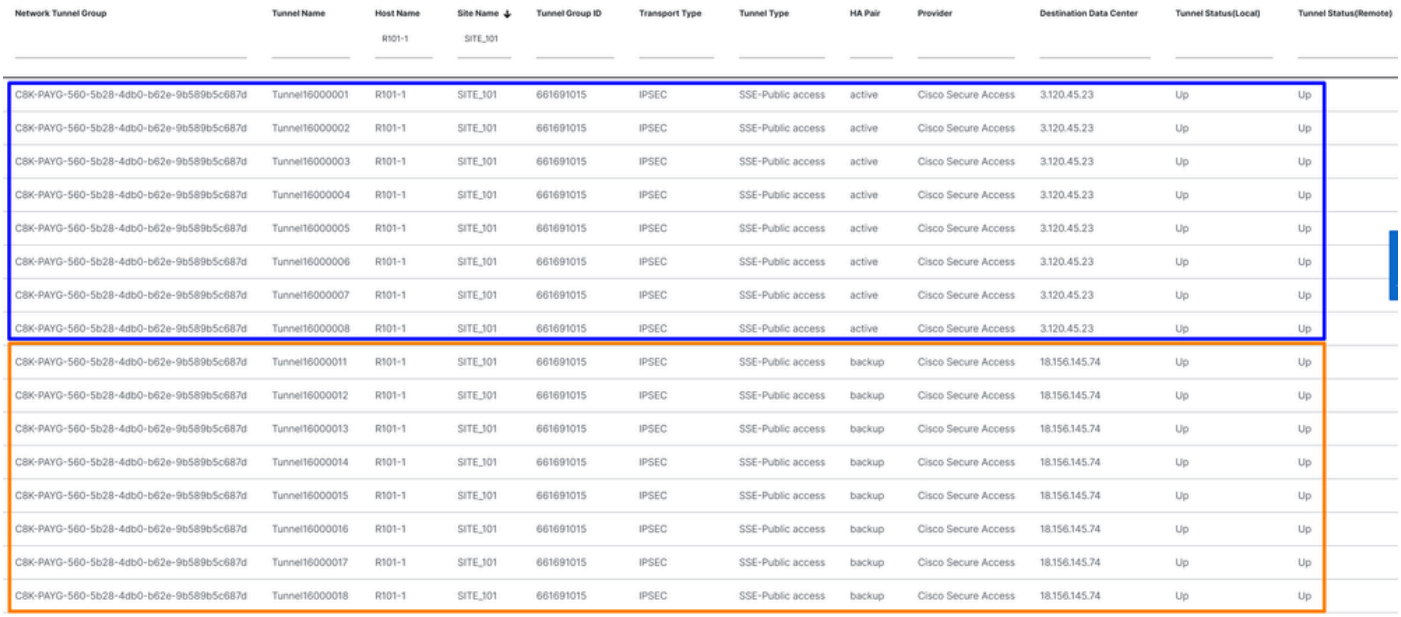
이 시점 이후에 모든 것이 올바르게 구성된 경우 터널은 SD-WAN 관리자 및 보안 액세스에서 UP로 표시됩니다.

SD-WAN에서 확인하려면 다음 단계를 확인하십시오.

- Monitor> 를 클릭합니다. Tunnels
- 그런 다음SIG/SSE Tunnels



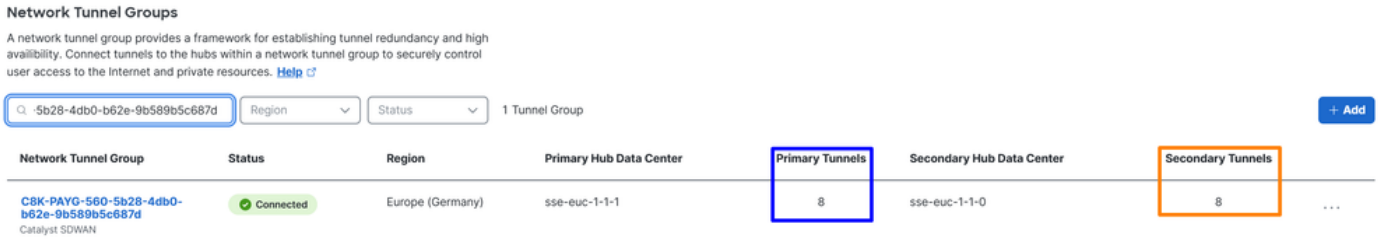
Cisco Secure Access UP에 설정된 터널이 표시되는지 확인할 수 있습니다.



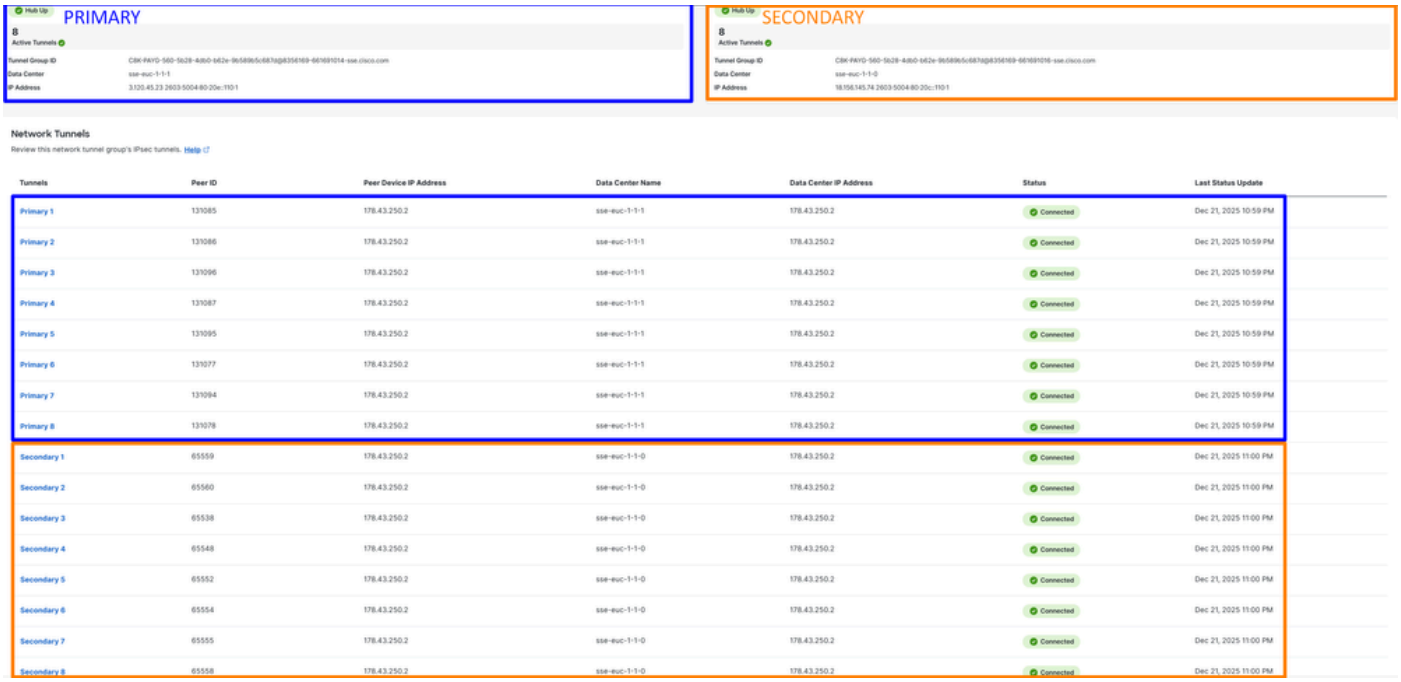
Network Tunnel Group	Tunnel Name	Host Name	Site Name	Tunnel Group ID	Transport Type	Tunnel Type	HA Pair	Provider	Destination Data Center	Tunnel Status(Local)	Tunnel Status(Remote)
		R101-1	SITE_101								
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000001	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000002	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000003	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000004	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000005	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000006	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000007	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000008	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	active	Cisco Secure Access	3.120.45.23	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000011	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000012	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000013	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000014	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000015	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000016	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000017	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up
C8K-PAYG-560-5b28-4db0-b62e-9b589b5c687d	Tunnel16000018	R101-1	SITE_101	661691015	IPSEC	SSE-Public access	backup	Cisco Secure Access	18.156.145.74	Up	Up

에서 확인하려면Secure Access다음 단계를 확인하십시오.

- Connect> 를 클릭합니다. Network Connections



자세히 보기에서 터널의 이름을 클릭합니다.



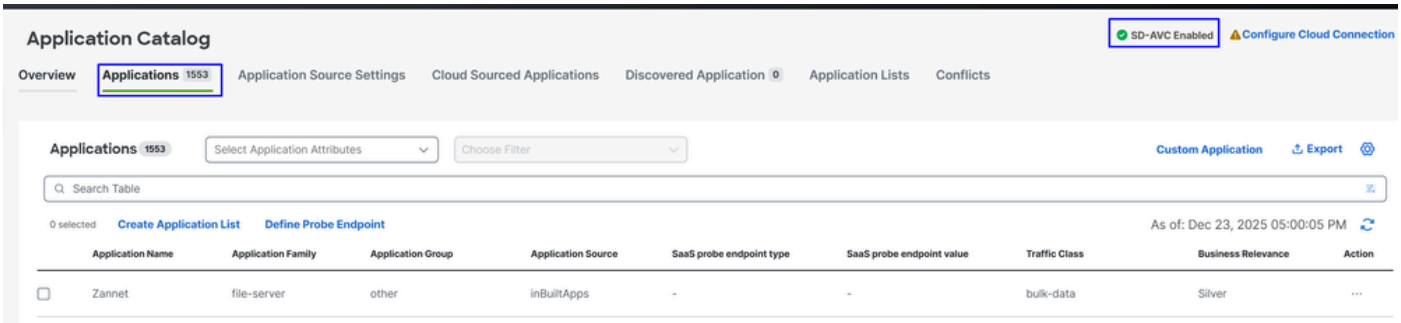
그 다음에는 해당 단계로 이동하여 Create your Custom Bypass FQDN or APP in SD-WAN

SD-WAN에서 사용자 지정 Bypass FQDN 또는 앱 만들기(선택 사항)

라우팅 정책에 적용할 수 있는 Application Bypass 및 FQDN 또는 IP를 만들어야 하는 특별한 사용 사례가 있습니다.

SD-WAN Manager 포털로 이동합니다.

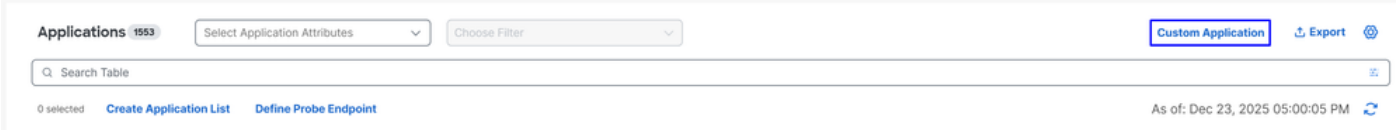
- Configuration>Application Catalog를 클릭합니다. Applications



팁: 20.15보다 낮은 버전을 실행하는 경우 정책 목록에서 맞춤형 애플리케이션을 생성할 수 있습니다

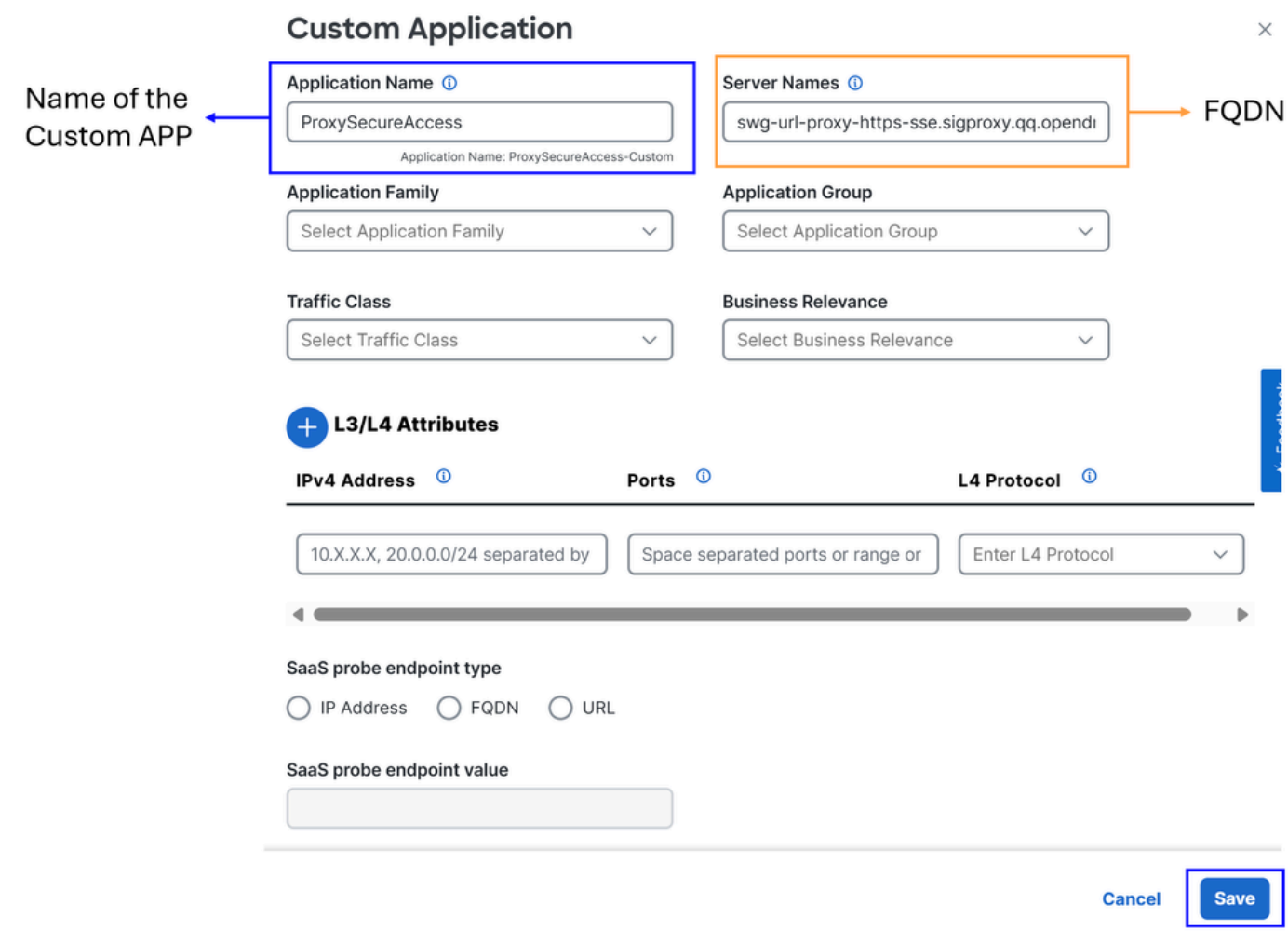
참고: 애플리케이션 카탈로그에 액세스하려면 SD-AVC를 활성화해야 합니다.

- 클릭 Custom Application



이 단계에서는 Secure Client - Umbrella Module SWG FQDN을 사용하여 기본 제외가 구성됩니다.

ProxySecureAccess

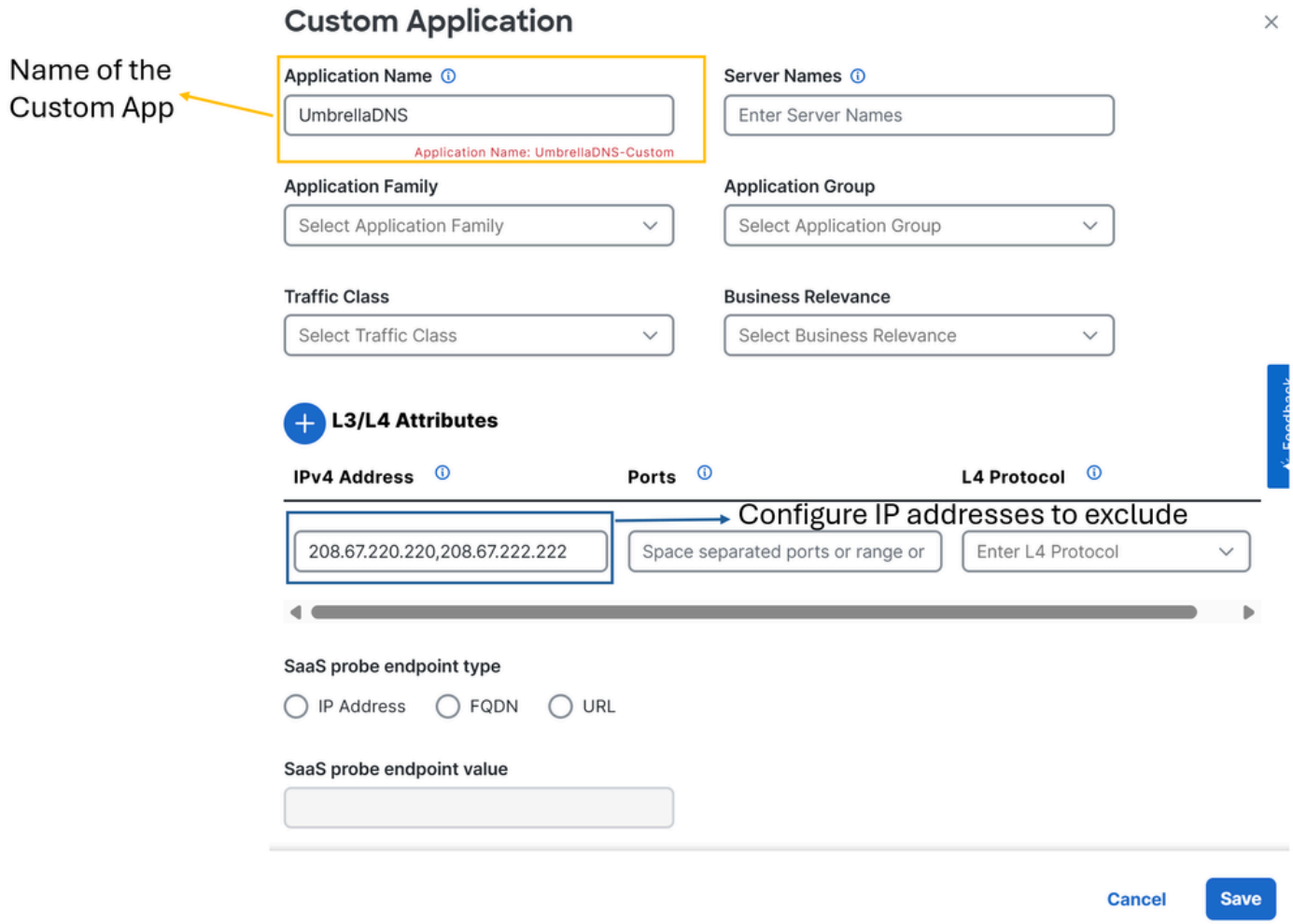


- Server Name: 우회하려는 FQDN을 사용합니다(이 예에서는 SWG의 FQDN이 구성됨).
  - swg-url-proxy-https-sse.sigproxy.qq.opendns.com을 참조하십시오.
  - swg-url-proxy-https-ORGID.sseproxy.qq.opendns.com을 참조하십시오.
- 클릭 Save

참고: SSE 조직 번호로 ORGID를 변경합니다.

다음으로, 기본 제외가 생성됩니다. 이 경우 Umbrella DNS 서버는 다음을 수행합니다.

UmbrellaDNS



이제 라우팅 정책의 컨피그레이션을 진행할 수 있습니다.

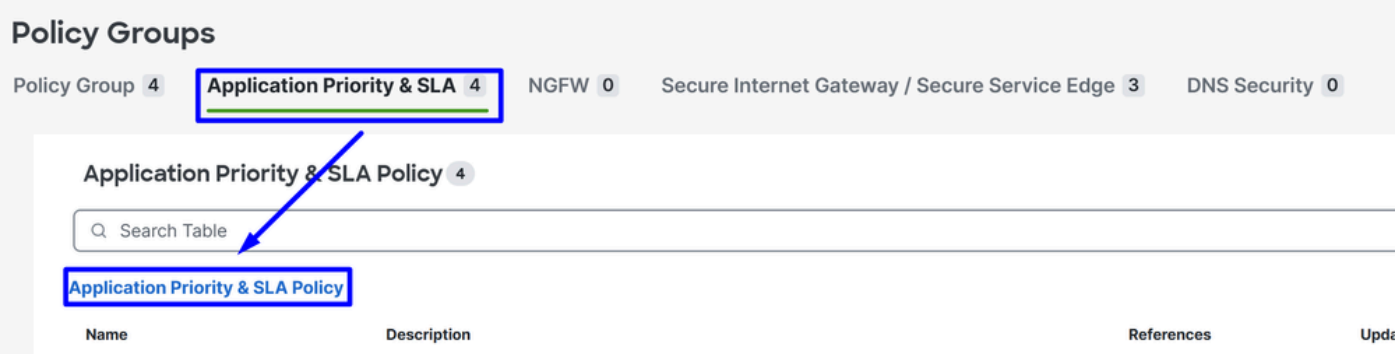
트래픽 라우팅

이 단계에서는 터널을 통해 인터넷 트래픽을 라우팅하여 Cisco Secure Access를 통해 보호해야 합니다. 이 경우 특정 트래픽 지원을 우회하여 원치 않는 트래픽을 Secure Access를 통해 전송하지 못하게 하거나 잠재적인 악영향을 방지하는 유연한 라우팅 정책을 사용합니다.
먼저 사용할 수 있는 두 가지 라우팅 방법을 정의하도록 합니다.

- Configuration >Configuration Groups>Service Profile>Service Route: 이 방법은 Secure Access로의 라우팅을 제공하지만 유연성이 부족합니다.
- **Configuration** >Policy Groups>Application Priority & SLA: 이 방법은 SD-WAN 내에서 다양한 라우팅 옵션을 제공하며, 가장 중요한 것은 특정 트래픽을 우회하여 Secure Access를 통해 전송되지 않도록 하는 것입니다.

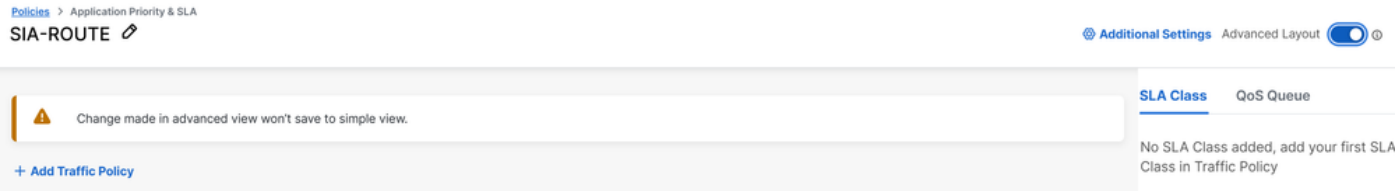
유연하고 모범 사례에 맞게 조정하기 위해 다음 컨피그레이션을 사용합니다Application Priority & SLA.

- 클릭 **Configuration** >Policy Groups> Application Priority & SLA
- 그런 다음 Application Priority & SLA Policy



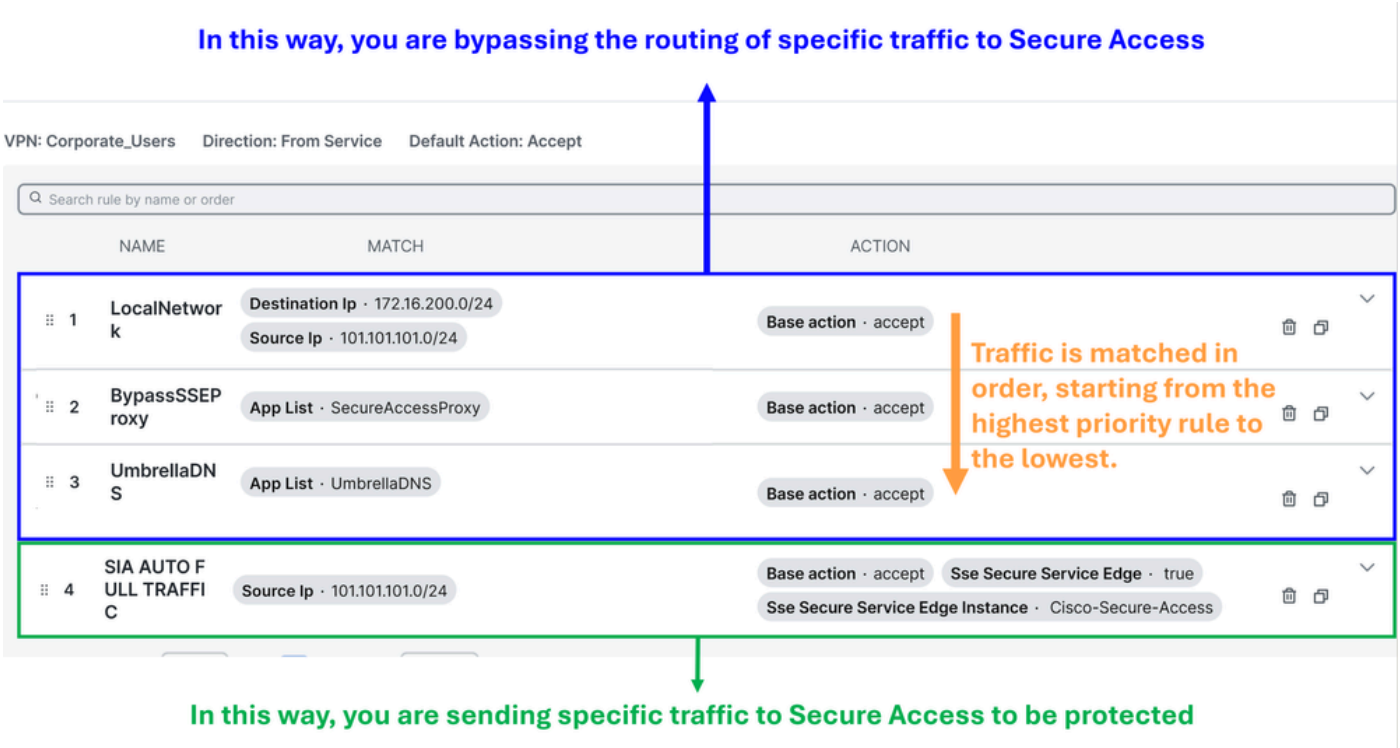
- 정책 이름을 구성하고 Create

- Enable Advanced Layout
- 클릭 + Add Traffic Policy



- Policy Name: 이 트래픽 정책 목록의 목적에 맞게 조정하는 이름
- VPN(s): 트래픽을 라우팅하는 위치에서 사용자의 서비스 VPN을 선택합니다
- **Direction**: 서비스에서
- Default action: 수락

그런 다음 트래픽 정책 생성을 시작할 수 있습니다.



1. Local Network Policy (Optional): 소스 101.101.101.0/24, 대상 172.16.200.0/24. 이 경로는 네트워크 내 트래픽이 Cisco Secure Access로 전송되지 않도록 합니다. 일반적으로 내부 라우팅은 SD-WAN 구축의 배포 라우터에서 처리하므로 고객은 이 작업을 수행하지 않습니다. 이 컨피그레이션을 사용하면 시나리오에 따라 이러한 서브넷 간의 내부 트래픽이 보안 액세스로 라우팅되

지 않습니다(선택 사항, 네트워크 환경에 따라 다름)

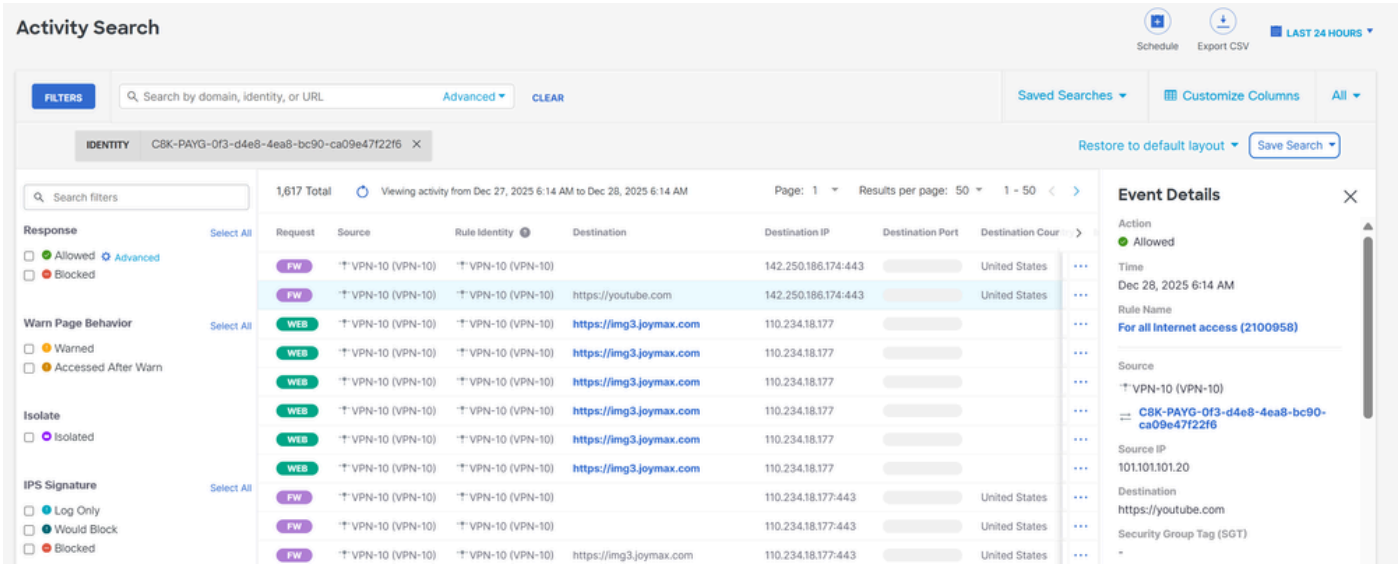
2. **BypassSSEProxy (Optional)**: 이 정책은 Secure Client 및 SWG에서 Cisco Umbrella 모듈이 활성화된 내부 컴퓨터가 프록시 트래픽을 클라우드로 다시 전송하지 못하도록 합니다. 프록시 트래픽을 클라우드로 다시 라우팅하는 것은 모범 사례로 간주되지 않습니다.
3. UmbrellaDNS (Best Practice): 이 정책은 인터넷을 목적지로 하는 DNS 쿼리가 터널을 통해 전송되지 않도록 합니다. 터널을 통해 Umbrella 확인자(208.67.222.222,208.67.220.220)에 DNS 쿼리를 보내지 않는 것이 좋습니다.
4. SIA AUTO FULL TRAFFIC: 이 정책은 이전에 생성한 SSE 터널을 통해 소스 101.101.101.0/24의 모든 트래픽을 인터넷으로 라우팅하여 이 트래픽이 클라우드에서 보호되도록 합니다.

다음을 확인합니다.

트래픽이 이미 Cisco Secure Access를 통해 플러딩되고 있는지 확인하려면 터널 ID로EventsActivity SearchNetwork-Wide Path Insights로 이동하거나 필터링합니다.

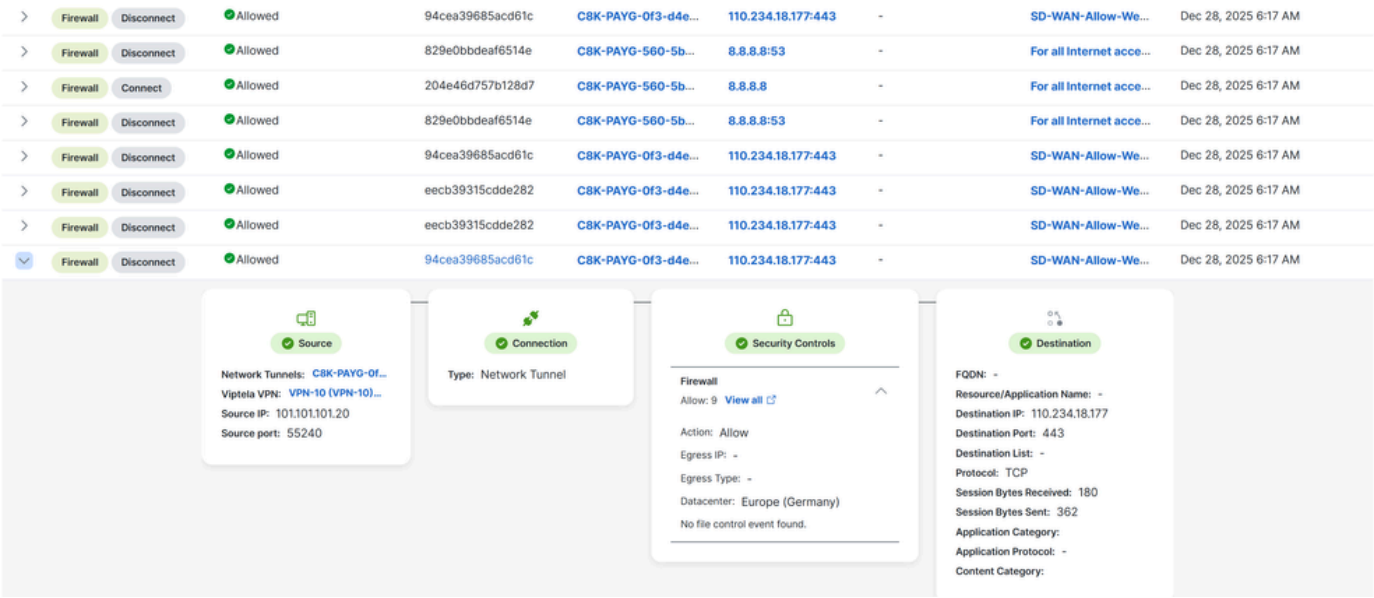
보안 액세스 - 활동 검색

Monitor> 로 이동합니다Activity Search.



보안 액세스 - 이벤트

Monitor> 로 이동합니다Events.

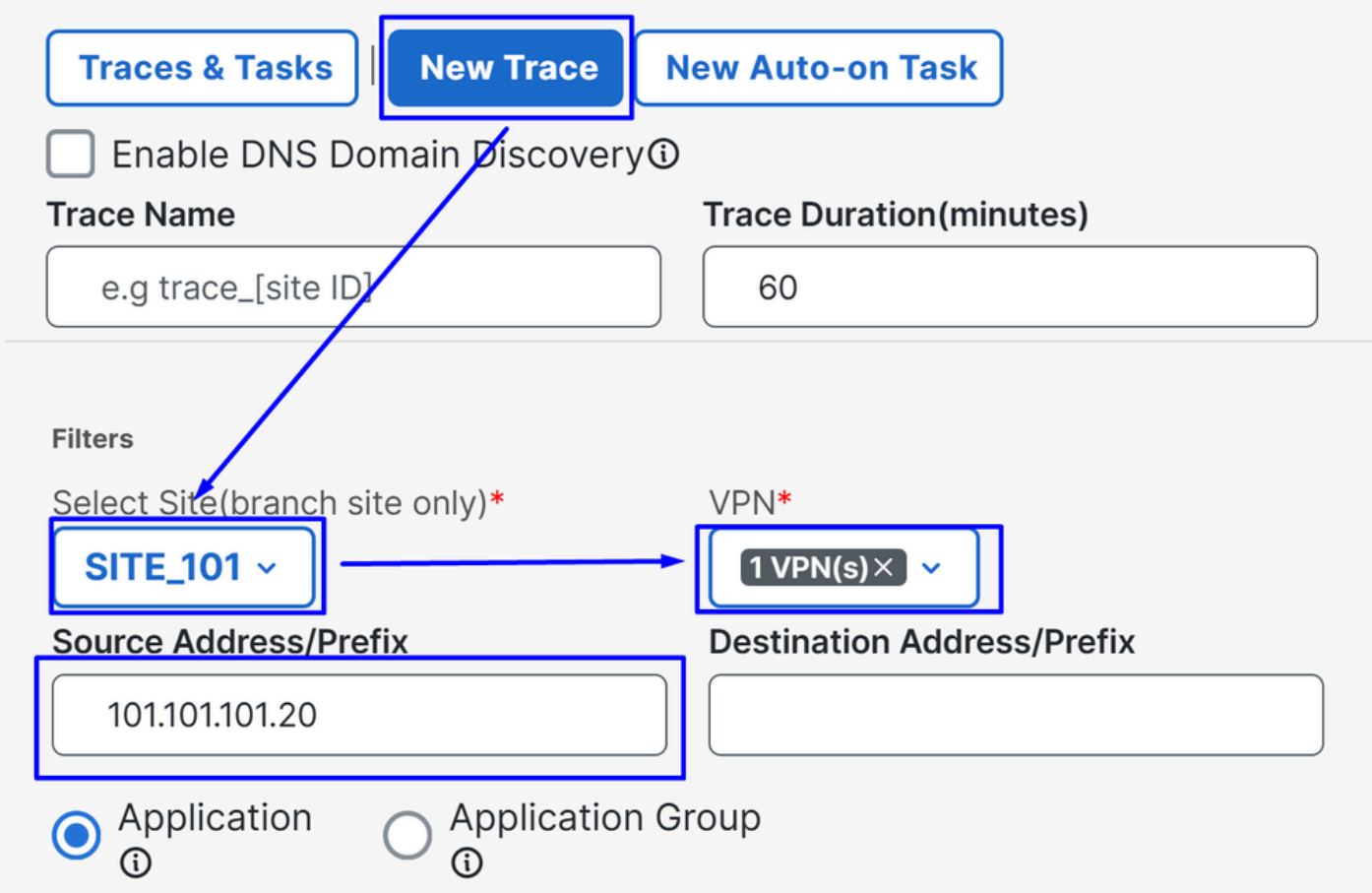


참고: 로깅이 활성화된 기본 정책이 있어야 합니다. 기본적으로 비활성화되어 있습니다.

Catalyst SD-WAN Manager - 네트워크 전반에 걸친 경로 통찰력

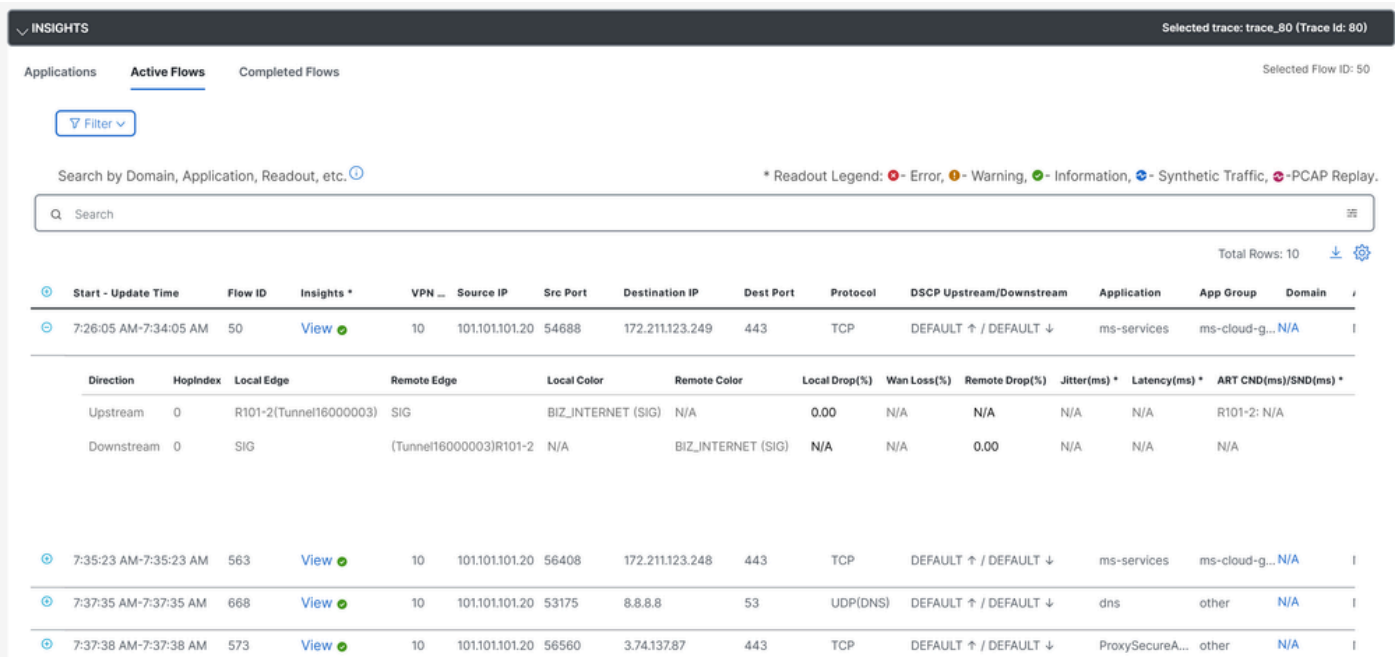
Catalyst SD-WAN Manager로 이동합니다.

- Tools> 를 클릭합니다. Network-Wide Path Insights
- 클릭 New Trace



- Site: 트래픽이 증가하는 사이트를 선택합니다.
- VPN: 트래픽이 증가하고 있는 서브넷의 VPN ID를 선택합니다
- Source: IP를 넣거나 차단하여 로 필터링한 모든 트래픽을 필터링한 다음Site을VPN선택합니다

그런 다음 Insights에서 터널을 통해 트래픽이 플러딩되고 Secure Access로 이동하는 트래픽 유형을 확인할 수 있습니다.



관련 정보

- Cisco 기술 지원 및 다운로드
- Cisco Secure Access Help Center
- Cisco ISE 설계 가이드
- Cisco Catalyst SD-WAN 보안 컨피그레이션 가이드, Cisco IOS XE Catalyst SD-WAN 릴리스 17.x
- Cisco ISE 솔루션: Cisco Secure Access At-a-Glance와 통합된 Cisco Catalyst SD-WAN

이 번역에 관하여

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