# Secure Private Access를 위한 Catalyst 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
    - 라우팅 구성
- 다음을 확인합니다.
  - 보안 액세스 - 활동 검색
  - 보안 액세스 - 이벤트
  - Catalyst SD-WAN Manager - 네트워크 전반에 걸친 경로 통찰력
- 관련 정보


## 소개

이 문서에서는 Secure Private Access를 위해 Catalyst SD-WAN Automated Tunnels를 사용하여 Secure Access를 구성하는 방법에 대해 설명합니다.


## 배경 정보

조직이 기존의 경계 기반 네트워크를 넘어서면서 프라이빗 리소스에 안전하게 액세스하는 것도 인터넷 트래픽 보안만큼 중요합니다. 애플리케이션은 더 이상 단일 데이터 센터에 국한되지 않으며, 이제 온프레미스 환경, 퍼블릭 클라우드, 하이브리드 아키텍처 전반에 걸쳐 실행됩니다. 이러한 전환에는 프라이빗 액세스에 대한 보다 유연하고 현대적인 접근 방식이 필요합니다.

여기서 SASE 기반 아키텍처와 Cisco Secure Access가 등장합니다. Cisco Secure Access는 레거시 VPN Concentrator 및 플랫 네트워크 액세스에 의존하는 대신 VPNaaS(VPN-as-a-Service)와 ZTNA(Zero Trust Network Access)를 결합하여 클라우드 제공 서비스로서 프라이빗 연결을 제공합니다.

네트워크 레벨 프라이빗 액세스를 위해 Cisco Secure Access는 자동화된 사이트 간 IPsec 터널을 사용하여 SD-WAN과 통합됩니다. 이러한 터널은 프라이빗 트래픽이 Secure Access와 온프레미스 또는 클라우드 네트워크 간에 안전하게 흐르도록 하는 동시에 보안 검사 및 정책 시행을 클라우드에서 중앙 집중화할 수 있도록 합니다. 운영 측면에서는 기존 VPN 헤드엔드를 배포하고 유지 관리할 필요가 없으며 환경의 성장에 따라 확장이 간소화됩니다.

VPNaaS 모델에서 Secure Access는 클라우드의 VPN 종단 지점 역할을 합니다. SD-WAN은 Secure Access를 통해 지능형 라우팅 및 복원력을 처리하며, 프라이빗 리소스에 도달하기 전에 일관된 보안 정책을 통해 트래픽을 보호하고 관리하도록 보장합니다.

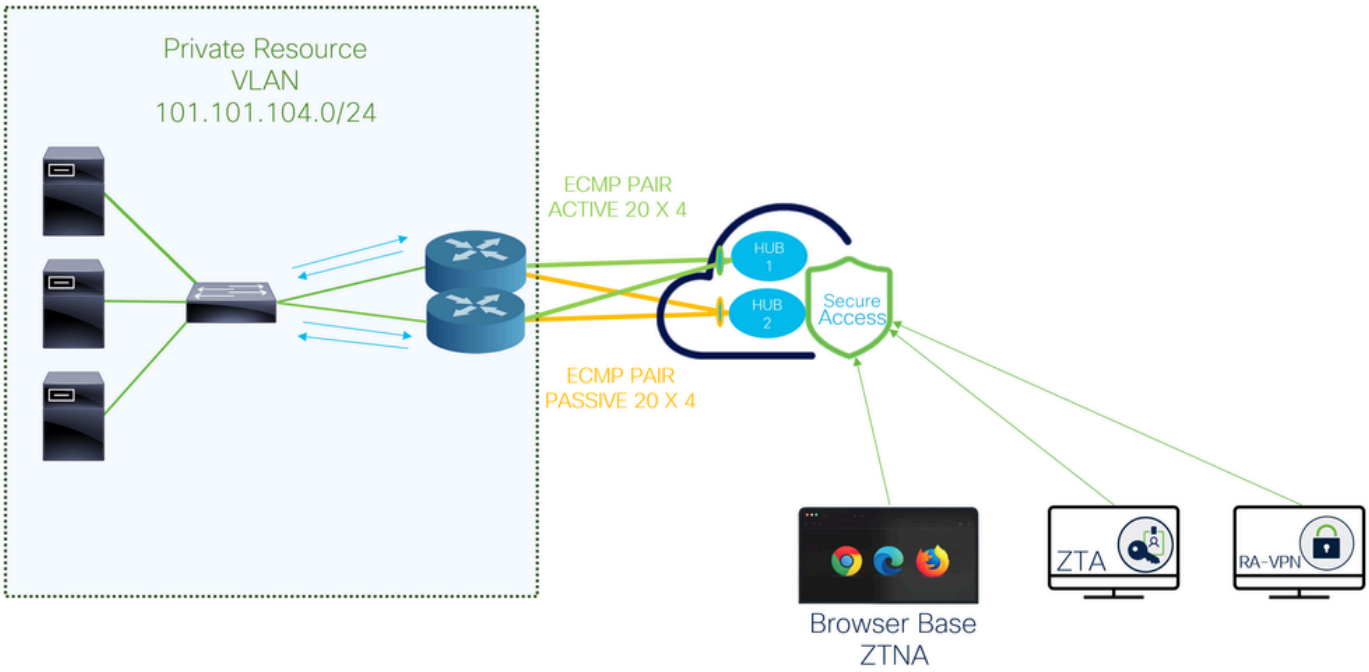
Cisco Secure Access는 또한 다중 지역 백홀을 비롯한 고급 사이트 간 터널 아키텍처를 지원합니다. 이 기능을 통해 조직은 여러 Secure Access 영역에 대한 터널을 동시에 설정하여 지리적 이중화와 고가용성을 제공할 수 있습니다. 서로 다른 지역에 연결하면 지역 중단, 레이턴시 저하 또는 유지 보수 이벤트의 경우 트래픽이 자동으로 장애 조치될 수 있습니다.

예를 들어, 조직은 SD-WAN 환경에서 런던과 독일의 Secure Access 영역으로 사이트 대 사이트 터널을 설정할 수 있습니다. 두 터널 모두 활성 상태로 유지되므로 여러 지역에서 민첩한 프라이빗 액세스가 가능하며, 한 지역을 사용할 수 없게 되더라도 연속성이 보장됩니다. 이 다중 지역 설계는 고가용성을 강화하고 내결함성을 개선하며 엔터프라이즈급 탄력성 요구 사항에 부합합니다.

Cisco Secure Access는 더 세분화된 액세스를 위해 ZTNA(Zero Trust Network Access) 모델을 적용합니다. ZTNA는 사용자에게 폭넓은 네트워크 연결을 허용하는 대신 ID, 디바이스 상태 및 컨텍스트를 기반으로 특정 애플리케이션에만 액세스를 허용합니다. 이 접근 방식은 공격 표면을 크게 줄이고 제로 트러스트 원칙에 부합합니다.

ZTNA 액세스는 Site-to-Site 터널과 Resource Connector의 조합을 통해 활성화됩니다. 리소스 커넥터는 보안 액세스에 대한 아웃바운드 전용 연결을 설정하는 경량 가상 어플라이언스입니다. 즉, 개인 리소스를 인터넷에 직접 노출할 필요가 없습니다.

## 네트워크 다이어그램




## 사전 요구 사항

### 요구 사항

- 보안 액세스 지식
- Cisco Catalyst SD-WAN Manager 릴리스 20.18.2 및 Cisco IOS XE Catalyst SD-WAN 릴리스 17.18.2 이상
- 라우팅 및 스위칭에 대한 중간 지식
- ECMP 지식
- VPN 지식
- 이 통합은 가용성이 제어되므로 Cisco Secure Access에서 이 기능을 활성화하도록 요청하는 TAC 케이스를 제출해야 합니다

### 사용되는 구성 요소

- 보안 액세스 테넌트
- Catalyst SD-WAN Manager 릴리스 20.18.2 및 Cisco IOS XE Catalyst SD-WAN 릴리스

17.18.2
- 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

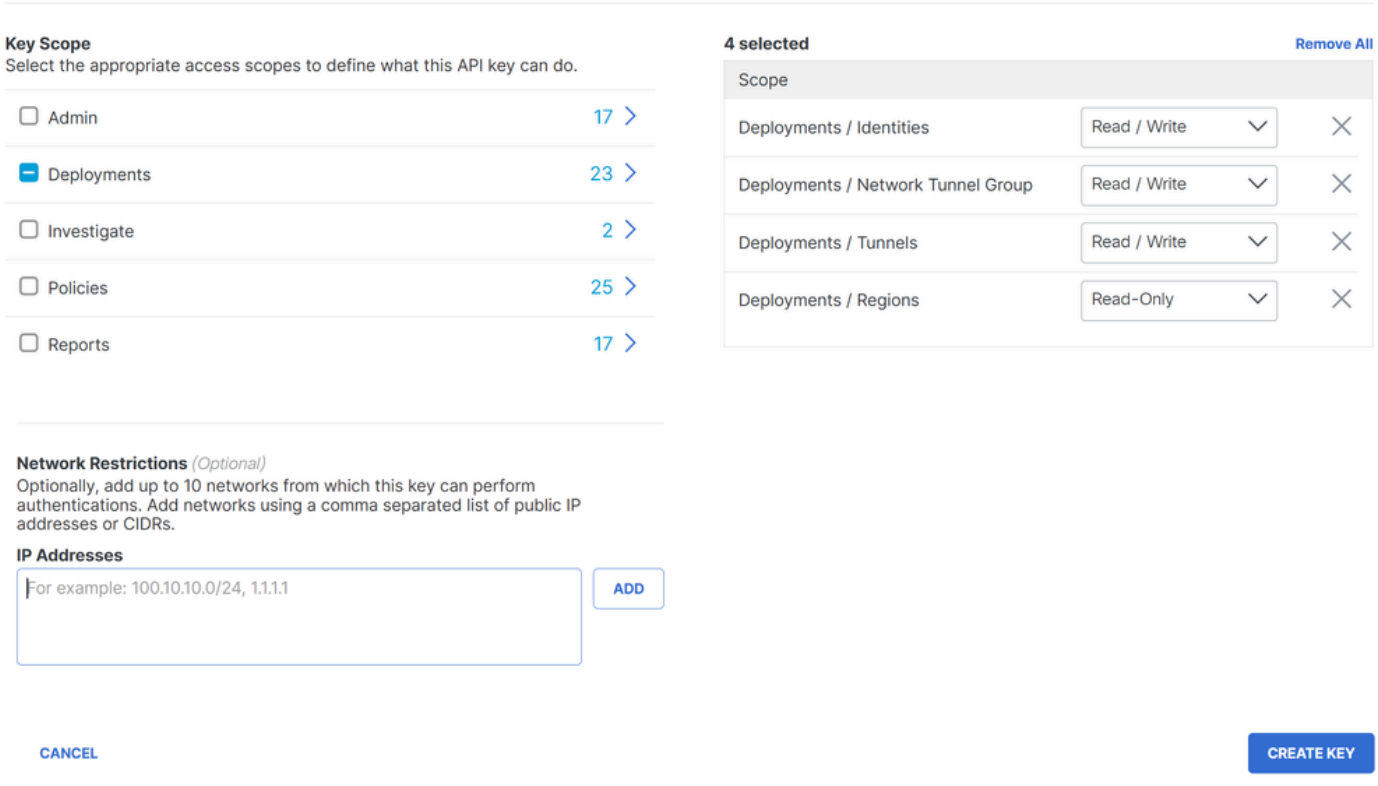
## 보안 액세스 컨피그레이션

### API 생성

Secure Access를 통해 자동 터널을 생성하려면 다음 단계를 확인하십시오.

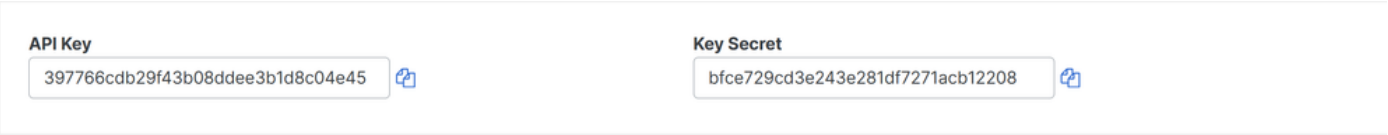
Secure Access Dashboard(보안 액세스 대시보드)로 이동합니다.

- 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.

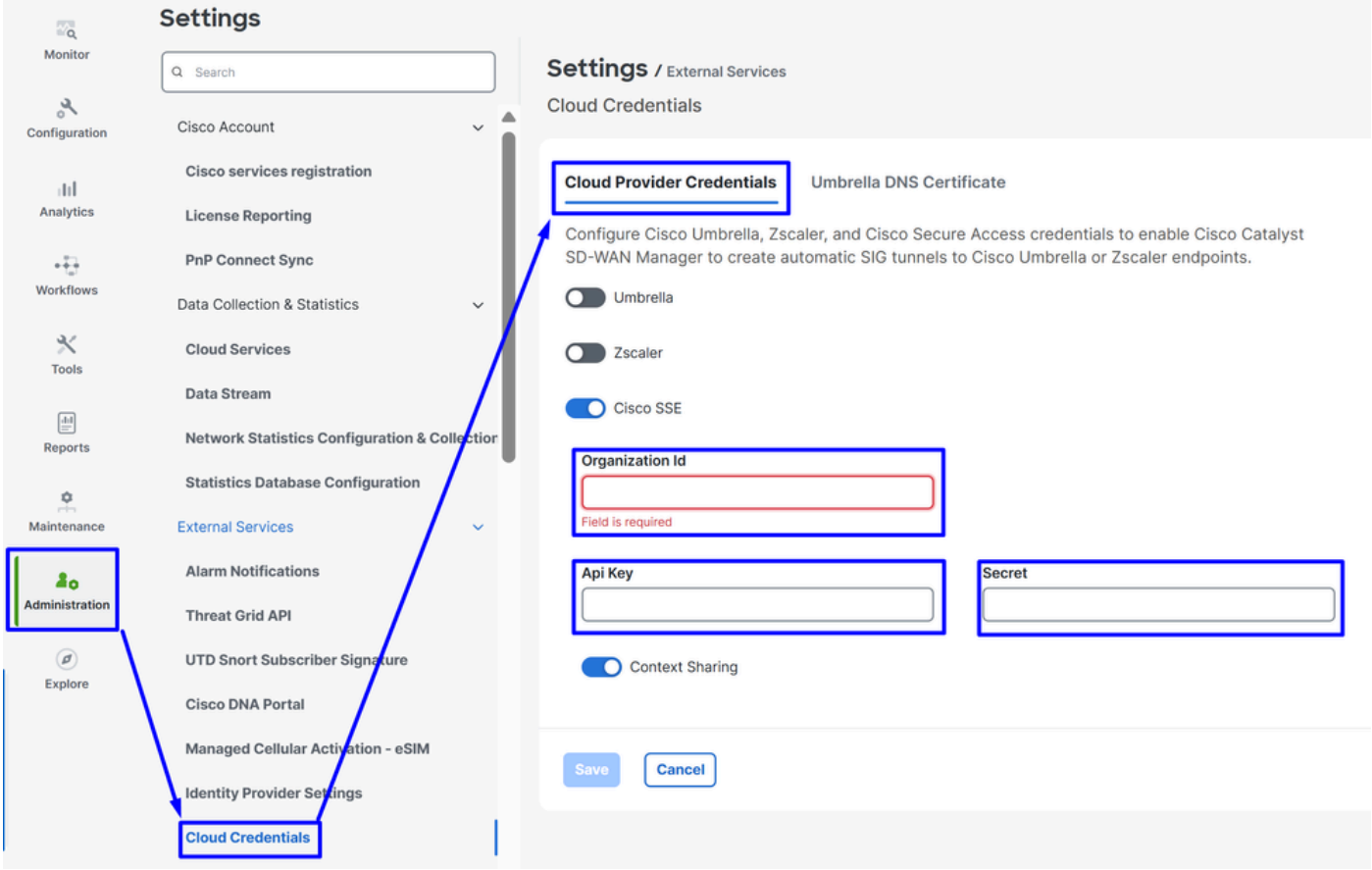
그런 다음 을 클릭하여 마무리합니다ACCEPT AND CLOSE.

## 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.

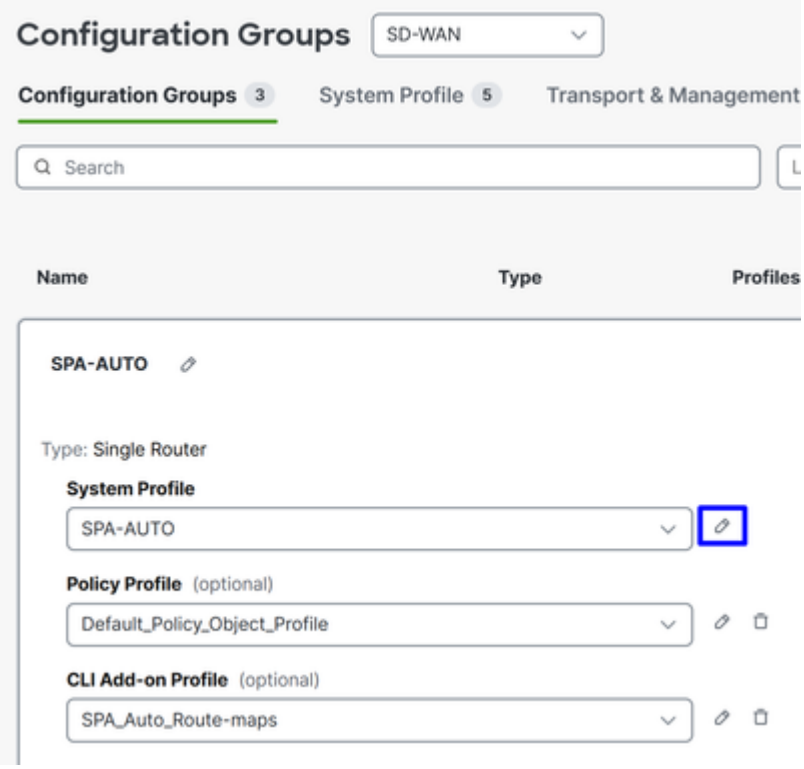
---

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

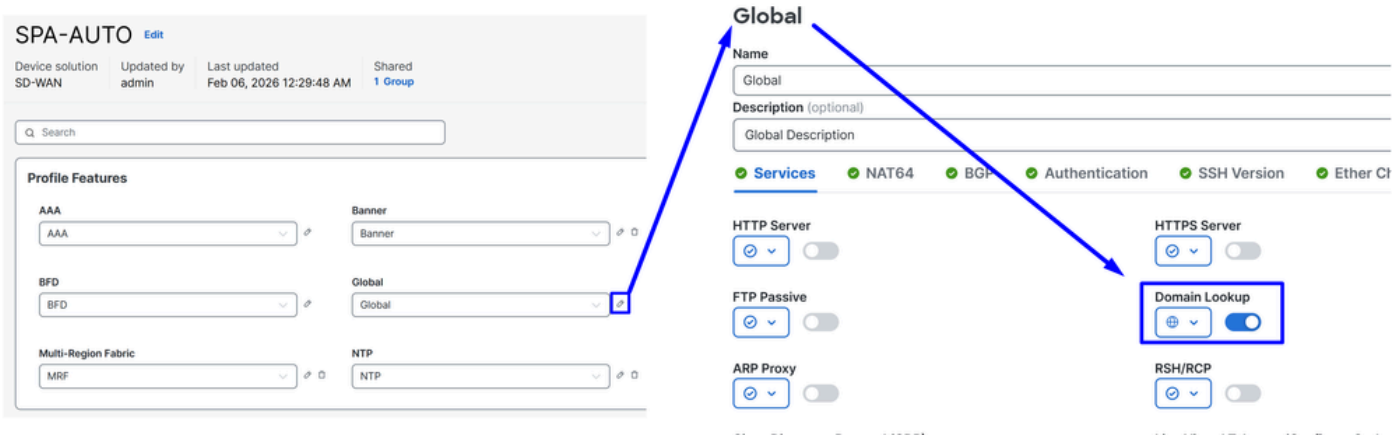
---

DNS-Lookup이 활성화되어 있는지 확인하려면 다음으로 이동하십시오.

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



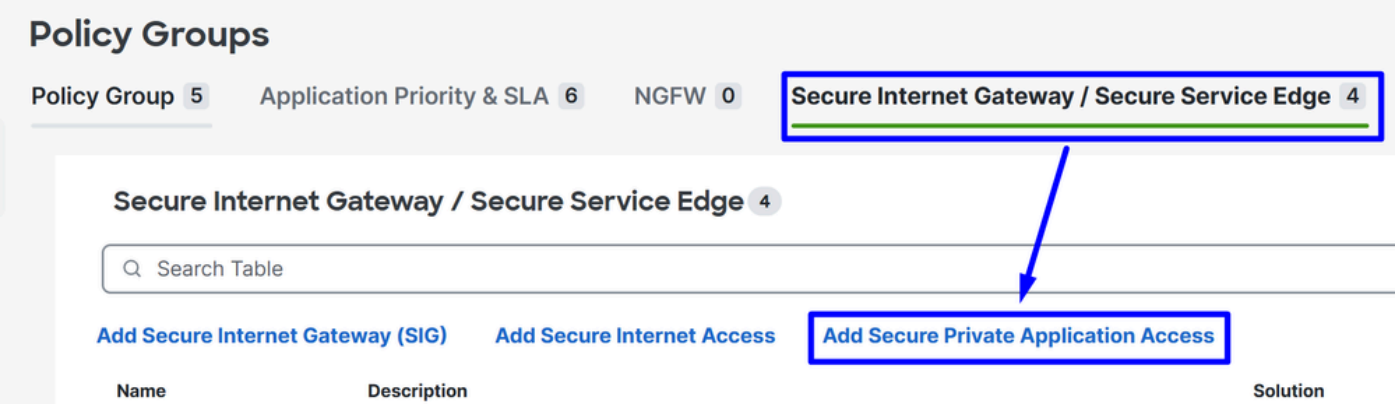

- 그런 다음 Global(전역) 옵션을 수정하고 Domain Resolution(도메인 확인) 옵션이 활성화되었는지 확인합니다



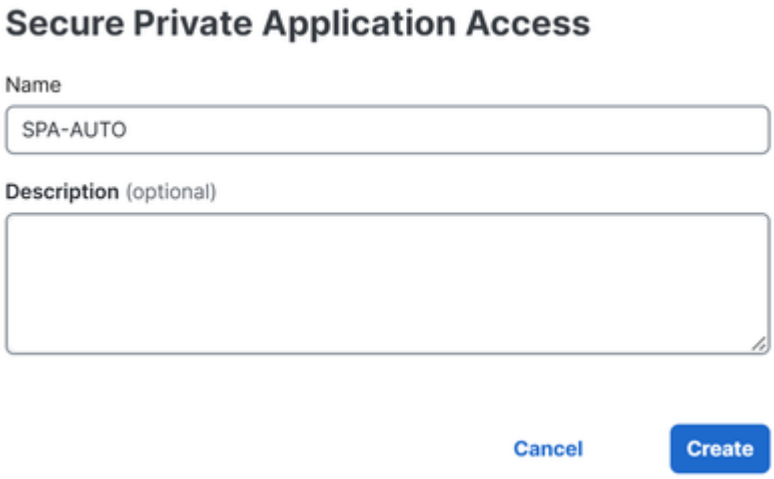

정책 그룹 구성

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

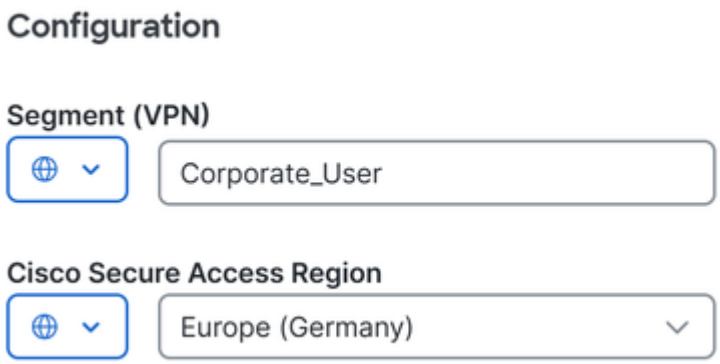
- 클릭 Secure Internet Gateway / Secure Service Edge>*Add Secure Private Access*




- 이름을 구성하고 다음을 클릭합니다. Create



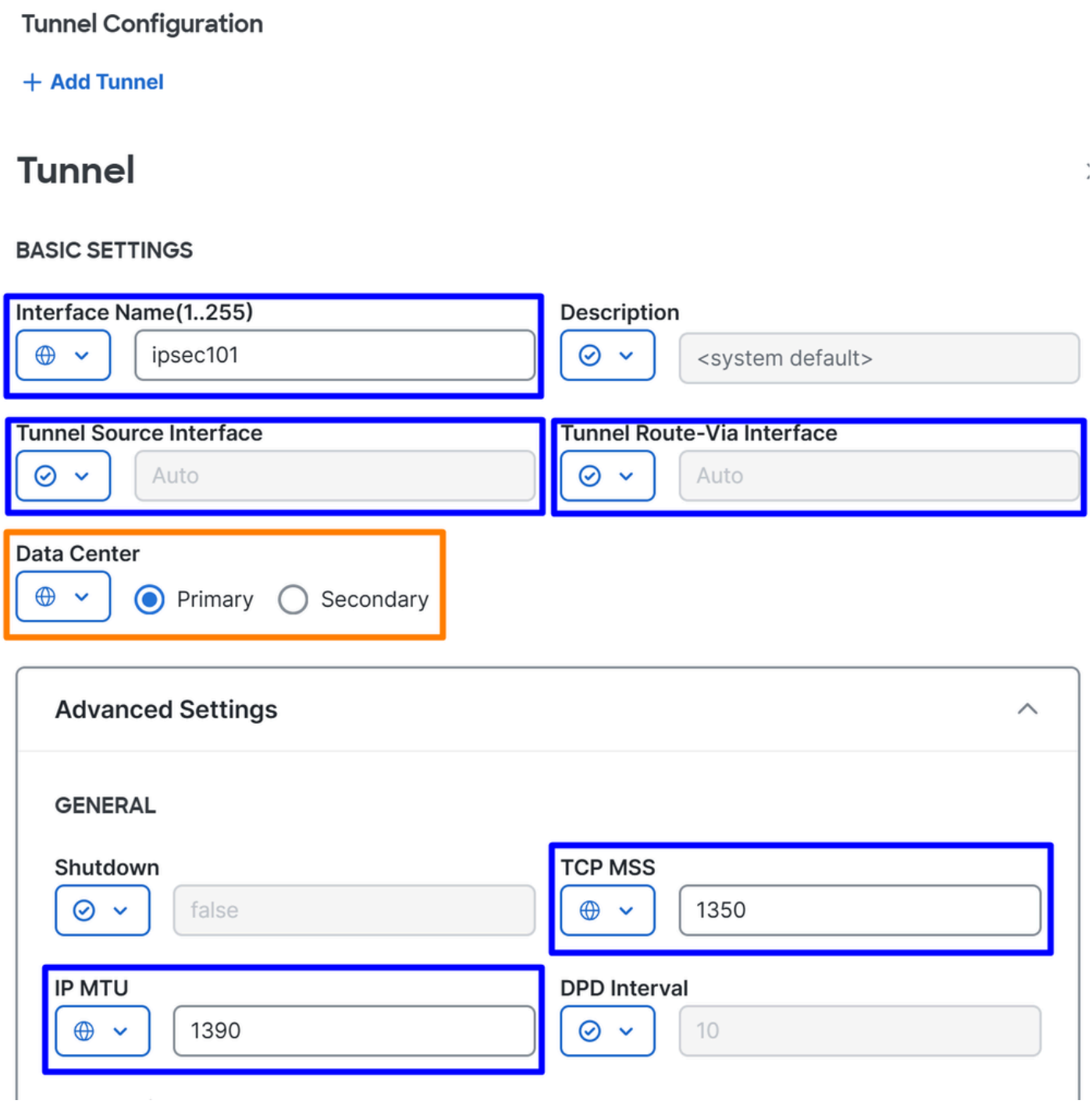

다음 컨피그레이션에서는 Catalyst SD-WAN 에지에서 컨피그레이션을 구축한 후 터널을 생성할 수 있습니다.




- Configuration
  - Segment (VPN): Secure Access를 통해 액세스할 애플리케이션을 호스팅하는 VRF를 선택합니다
  - Cisco Secure Access Region: 애플리케이션이 호스팅되는 SD-WAN 허브 또는 브랜치와 가장 가까운 지역을 선택합니다

다음으로 터널 컨피그레이션을 정의합니다. 기본 Secure Access 데이터 센터에 생성된 터널은 활성 상태이며, 보조 Secure Access 데이터 센터에 생성된 터널은 백업으로 작동합니다.

아래에서Tunnel Configuration다음을 클릭합니다+ Add Tunnel.




- Tunnel
  - Interface Name: 터널 이름을 지정합니다. 새 터널이 추가될 때마다 자동으로 업데이트됩니다.
  - Tunnel Source Interface: 이 설정은 변경할 필요가 없습니다. 그대로 두면Auto시스템은 /31 마스크가 있는 루프백 인터페이스를 자동으로 만듭니다.
  - Tunnel Route-Via Interface: 이 설정을 변경할 필요가 없습니다. 기본적으로 에지 라우터에서 첫 번째 NATed 물리적 WAN 인터페이스를 사용하지만, 특정 WAN 인터페이스가 필요한 경우 변경할 수 있습니다
  - Data Center: Primary(기본) 또는 Secondary(보조)를 선택합니다. 기본 터널이 이미 구성된 경우 Secondary(보조)를 선택합니다. 일반적인 시나리오에서는 터널 하나를 기본으로,

다른 터널을 보조로 구성할 수 있습니다

- Advanced Settings
  - IP MTU: 1390 사용
  - TCP MSS: 1350 사용

---

참고: ECMP를 활성화하고 터널 용량을 늘리기 위해 여러 터널을 생성하려는 경우 라우터당 최대 10개의 활성/10개의 백업 터널을 구성할 수 있습니다. 이는 NTG당 최대 10×4Gbps를 제공합니다.

---

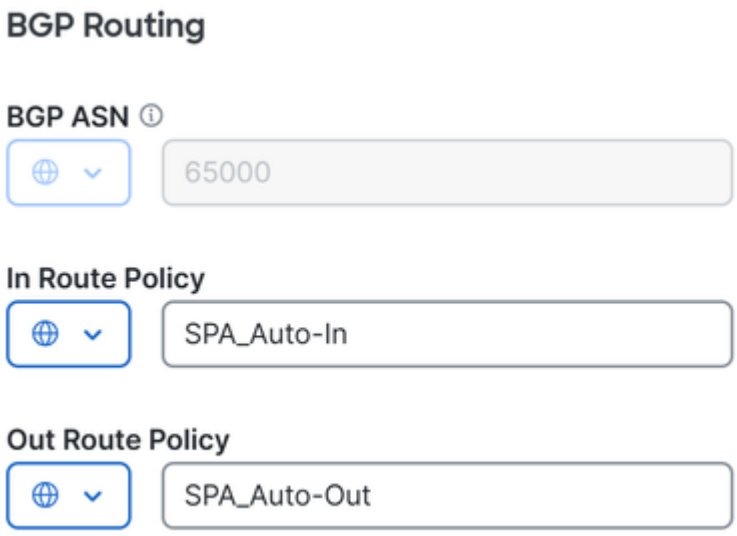
| Interface Name | Description | Tunnel Source Interface | Tunnel Route-Via Interface | Data Center | Action | |
|---|---|---|---|---|---|---|
| ipsec101 | | Auto | Auto | Primary | | |
| ipsec102 | | Auto | Auto | Secondary | | |
| ipsec103 | | Auto | Auto | Primary | | |
| ipsec104 | | Auto | Auto | Secondary | | |
| ipsec105 | | Auto | Auto | Primary | | |
| ipsec106 | | Auto | Auto | Secondary | | |
| ipsec107 | | Auto | Auto | Primary | | |
| ipsec108 | | Auto | Auto | Secondary | | |
| ipsec109 | | Auto | Auto | Primary | | MAXIMUM OF 10 TUNNELS PER HUB |
| ipsec110 | | Auto | Auto | Secondary | | 10 x 1 Primary |
| ipsec111 | | Auto | Auto | Primary | | 10 x 1 Secondary |
| ipsec112 | | Auto | Auto | Secondary | | |
| ipsec113 | | Auto | Auto | Primary | | |
| ipsec114 | | Auto | Auto | Secondary | | |
| ipsec115 | | Auto | Auto | Primary | | |
| ipsec116 | | Auto | Auto | Secondary | | |
| ipsec117 | | Auto | Auto | Primary | | |
| ipsec118 | | Auto | Auto | Secondary | | |
| ipsec119 | | Auto | Auto | Primary | | |
| ipsec120 | | Auto | Auto | Secondary | | |

---

참고:라우터당 여러 터널을 구축할 경우 전송 인터페이스가 결합된 모든 활성 터널의 종합 대역폭을 유지할 수 있는지 확인하십시오. 예를 들어 2개의 터널이 각각 최대 1Gbps를 전송해야 하는 경우 전송 링크는 최소 2Gbps의 처리량을 지원해야 합니다.

---

터널이 구성되면 BGP 컨피그레이션을 진행합니다.




- **BGP Routing**
  - BGP ASN: SD-WAN 허브의 AS 번호를 지정합니다. AS 64512은 보안 액세스용으로 예약되어 있으므로 사용할 수 없습니다. BGP에 대한 자세한 내용은 를 참조하십시오.
  - In Route Policy: 라우팅 문제를 방지하기 위해 시스템에서 명령문을 사용하여deny all이 인바운드 경로 정책을 자동으로 생성합니다. 적절한 경로를 허용/거부하려면 를 통해CLI Add-On Template수동으로 수정해야 합니다.
  - Out Route Policy: 라우팅 문제를 방지하기 위해 시스템이 명령문을 사용하여 이 아웃바운드deny all경로 정책을 생성합니다. 적절한 경로를 허용/거부하려면 를 통해 수동으로CLI Add-On Template편집해야 합니다.

---

경고: 2025년 11월부터 새로 생성된 모든 Secure Access 조직은 네트워크 터널 그룹의 BGP 피어링32644 대해 기본적으로 공용 ASN 인터페이스를 사용합니다. 2025년 11월 이전에 설립된 기존 조직에서는 이전에 Secure Access BGP 64512을 위해 예약한 프라이빗 ASN Service를 계속 사용합니다. 사설 AS 번호 64512이 네트워크의 디바이스에 할당된 경우, 피어(보안 액세스) BGP AS 64512에 대해 구성된 네트워크 터널 그룹으로 피어링할 수 없습니다.

---

에서 새 정책을 수행한 후 모든 BGP 네이버에 대해 다음BGProute-mapDeploy및 컨피그레이션이 자동으로Policy Group생성됩니다.

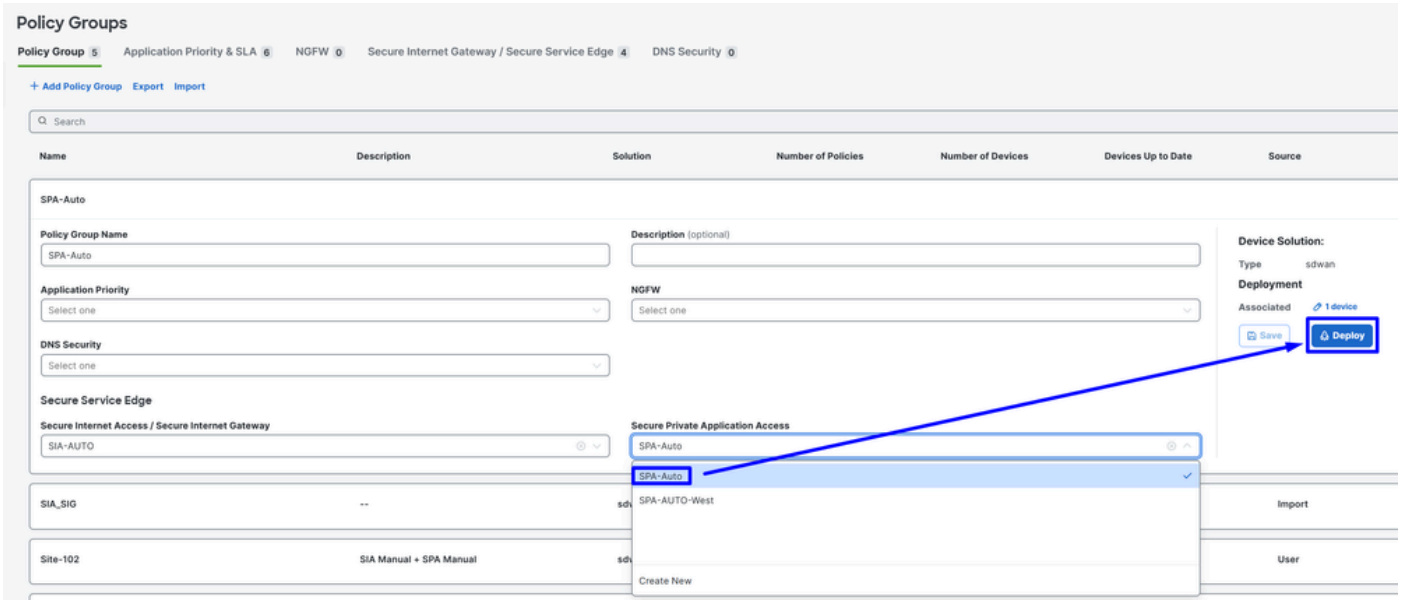
```
route-map SPA_Auto-In deny 65534
 description Default Deny Configured from Secure Private Application Access feature
route-map SPA_Auto-Out deny 65534
 description Default Deny Configured from Secure Private Application Access feature

R104#sh run | s r b
router bgp 65000
bgp log-neighbor-changes
!
address-family ipv4 vrf 10
 neighbor 169.254.0.3 remote-as 64512
```

```
 neighbor 169.254.0.3 activate
 neighbor 169.254.0.3 send-community both
 neighbor 169.254.0.3 route-map SPA_Auto-In in
 neighbor 169.254.0.3 route-map SPA_Auto-Out out
 ...
 maximum-paths 32
exit-address-family
```

Save그런 다음 을 클릭하고 정책 구축을 진행하여 터널을 가동합니다.

- Configuration> 를 클릭합니다. Policy Groups
- Policy>Secure Service Edge>Secure Private Application Access아래에서 선택하고 SPA를 위해 생성된 최근 프로필을 클릭합니다.
- 마무리하려면Deploy클릭하십시오.




에서Secure Access확인하려면 다음 단계를 수행하십시오.

- 클릭Connect> Network Connections

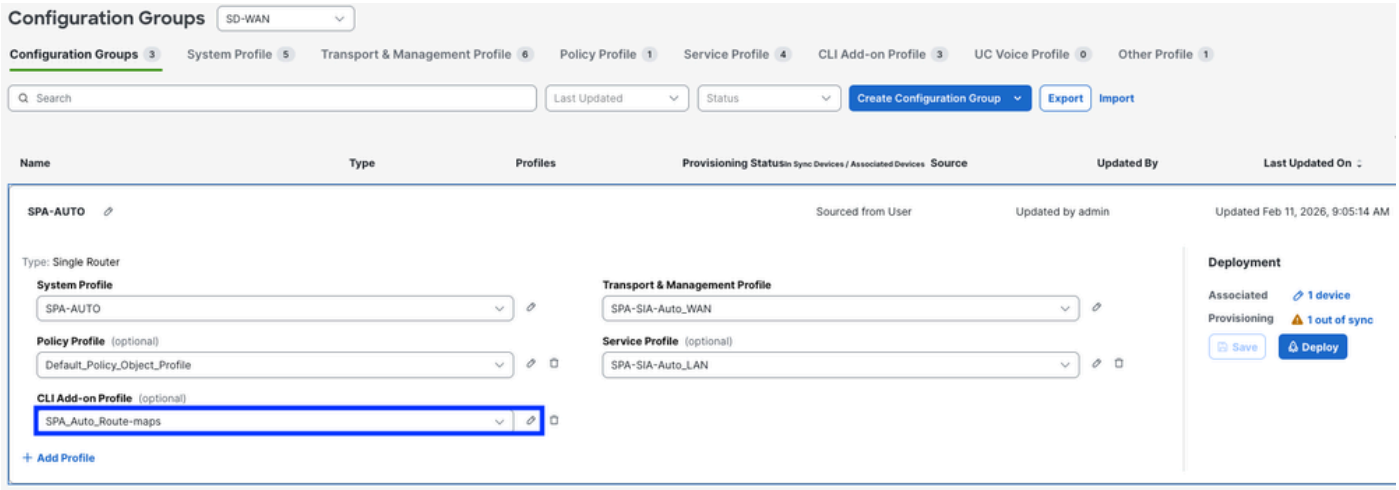
터널 설정


라우팅 구성

Configure

> 로 이동합니다. Configuration Groups

- 를 클릭하고Configuration GroupCreate/Edit CLI Add-on Profile




BGP 경로 교환을 허용하려면 이전에 구성한In Route Policy및 를 **Out Route Policy**사용합니다. 경로 컨피그레이션의 기본 예를 찾을 수CLI Add-On있습니다. 이 템플릿은 시작점을 제공하며 필요에 따라 사용자 정의해야 합니다.

```
ip bgp-community new-format
ip prefix-list ALL-ROUTES seq 5 permit 0.0.0.0/0 le 32

route-map SPA_Auto-In permit 10
match ip address prefix-list ALL-ROUTES
route-map SPA_Auto-In deny 65534
description Default Deny Configured from Secure Private Application Access feature

route-map SPA_Auto-Out permit 10
match ip address prefix-list ALL-ROUTES
description Default Deny Configured from Secure Private Application Access feature
route-map SPA_Auto-Out deny 65534
description Default Deny Configured from Secure Private Application Access feature

router bgp 65000
bgp log-neighbor-changes
!
address-family ipv4 vrf 10
network 172.16.104.0 mask 255.255.255.0
```

---

경고: BGP 경로 맵을 통해 들어오고 나가는 네트워크를 정의할 때는 신중한 계획이 필요합니다. 위의 예에서 보여주는 것처럼 모든 경로를 허용하면 의도하지 않은 라우팅 동작이 발생할 수 있습니다. 최적의 구축을 위해 경로 맵에서 필요한 네트워크만 명시적으로 지정하여 제어 및 예측 가능한 라우팅 결과를 보장합니다

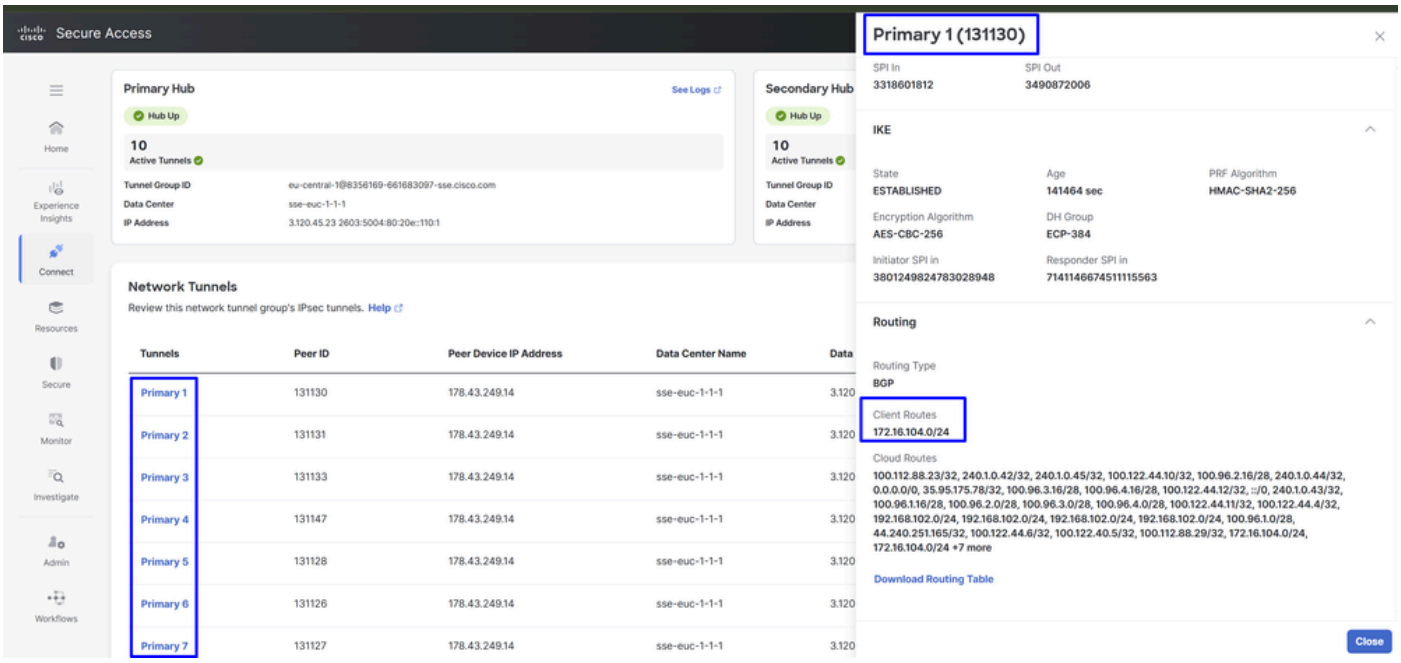
---

이제 다음 작업을 수행할 수 있습니다. Deploy the changes

BGP 경로가 수신되는지 확인하려면Secure Access다음 단계를 확인하십시오.

- Connect>Network ConnectionsNetwork Tunnel Groups> 를 클릭하고 NTG 이름을select클릭합니다.

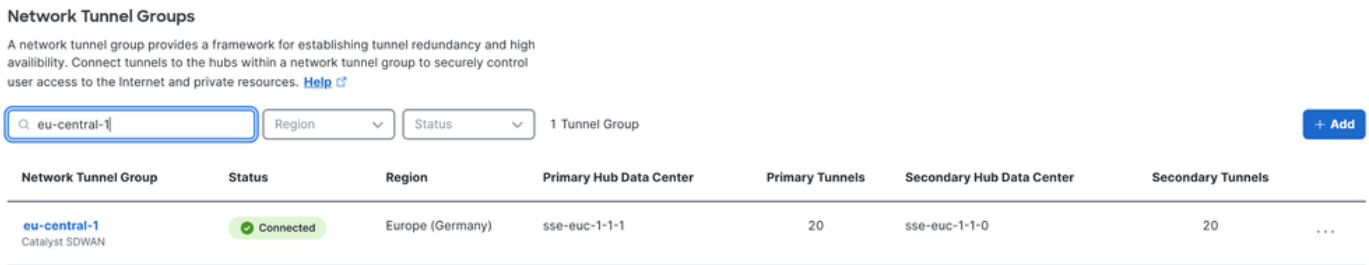
경로 설정




참고: 이 예에서는 기업 사용자 서브넷 172.16.104.0/24이 BGP를 통해 Secure Access로 광고됩니다. 이를 통해 Catalyst SD-WAN과 SSE 환경 간에 적절한 라우팅을 수행할 수 있습니다.

Catalyst SD-WAN 허브의 두 WAN 에지에 동일한 정책을 적용할 수 있으므로 20개의 활성 터널과 20개의 대기 터널이 생성됩니다. 총 터널 수는 각 에지에 구성된 개수에 따라 다릅니다. 두 Secure Access 허브(허브 1 및 허브 2)에 모두 연결된 라우터는 설정된 모든 터널에 ECMP 쌍을 형성합니다.

예를 들어 Catalyst SD-WAN Edge 1에 10개의 터널이 있고 Catalyst SD-WAN Edge 2에 10개의 터널이 있는 경우 Secure Access는 20개의 활성 터널 전반에 ECMP를 형성합니다. 보조 SSE 허브에도 동일한 동작이 적용됩니다.

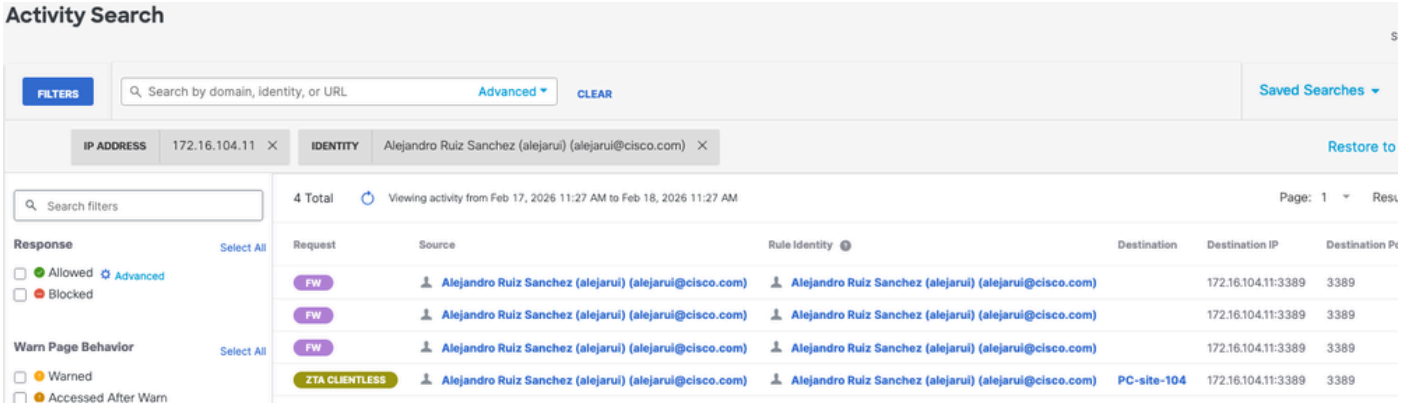


# 다음을 확인합니다.

트래픽이 Cisco Secure Access를 통과하는지 확인하려면 터널 ID로EventsActivity SearchNetwork-Wide Path Insights탐색하거나 필터링합니다.

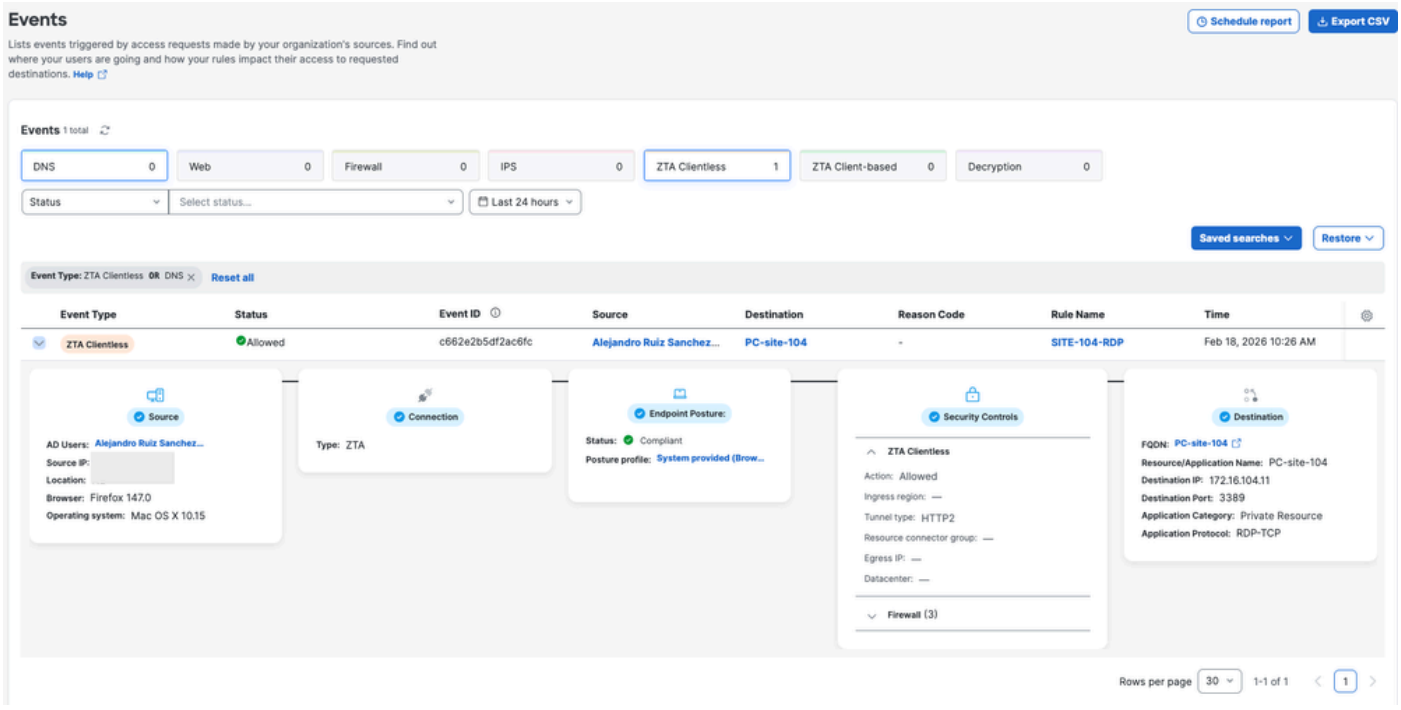
## 보안 액세스 - 활동 검색

탐색Monitor>Activity Search :




## 보안 액세스 - 이벤트

다음으로Monitor이동합니다Events.

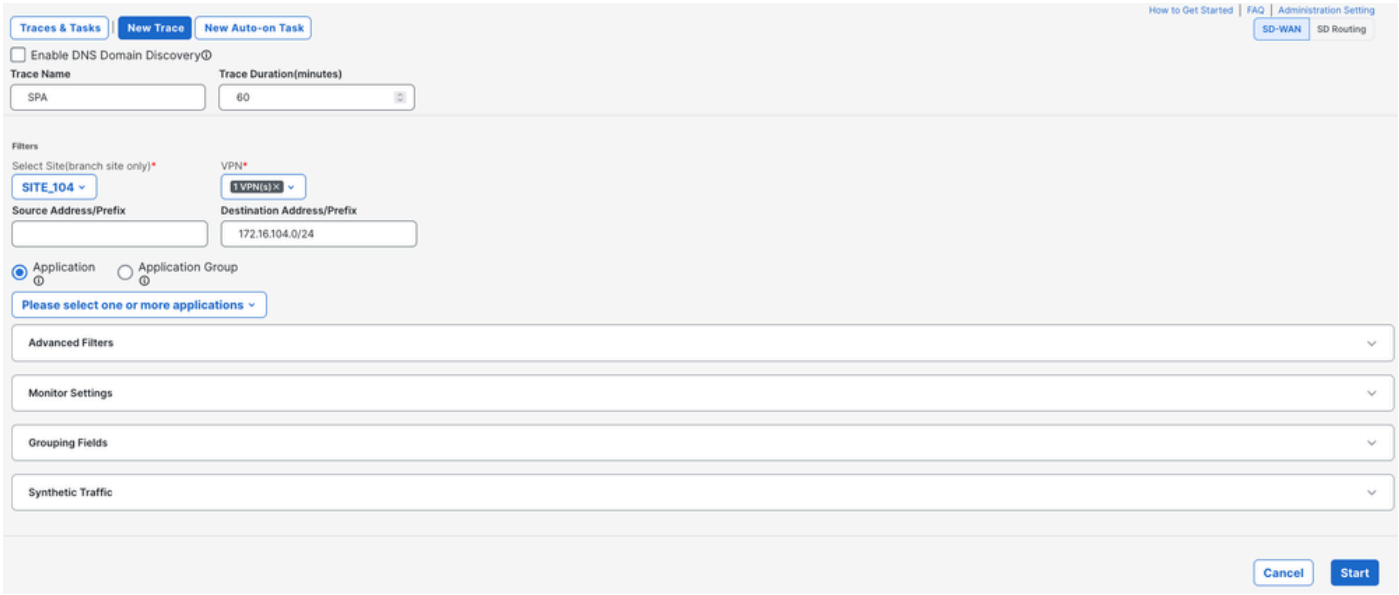



참고: 로깅이 활성화된 기본 정책이 있어야 합니다. 기본적으로 비활성화되어 있습니다.

## Catalyst SD-WAN Manager - 네트워크 전반에 걸친 경로 통찰력

Catalyst SD-WAN Manager로 이동합니다.

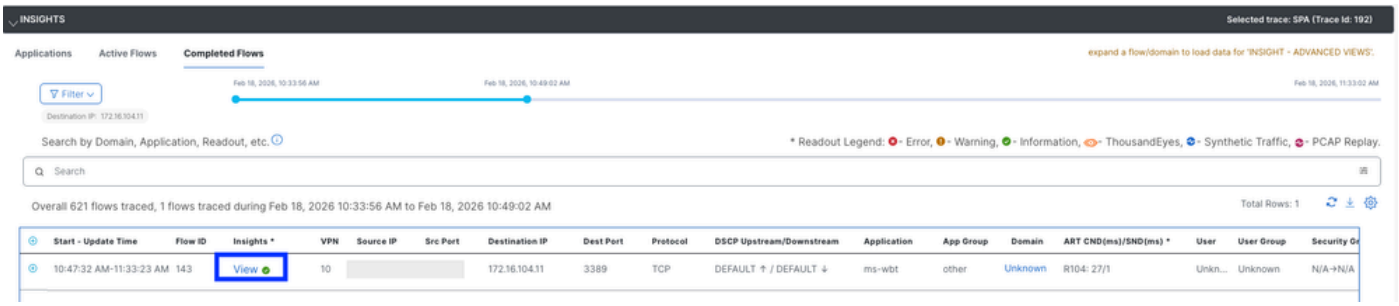
- 클릭Tools> Network-Wide Path Insights
- 클릭 New Trace



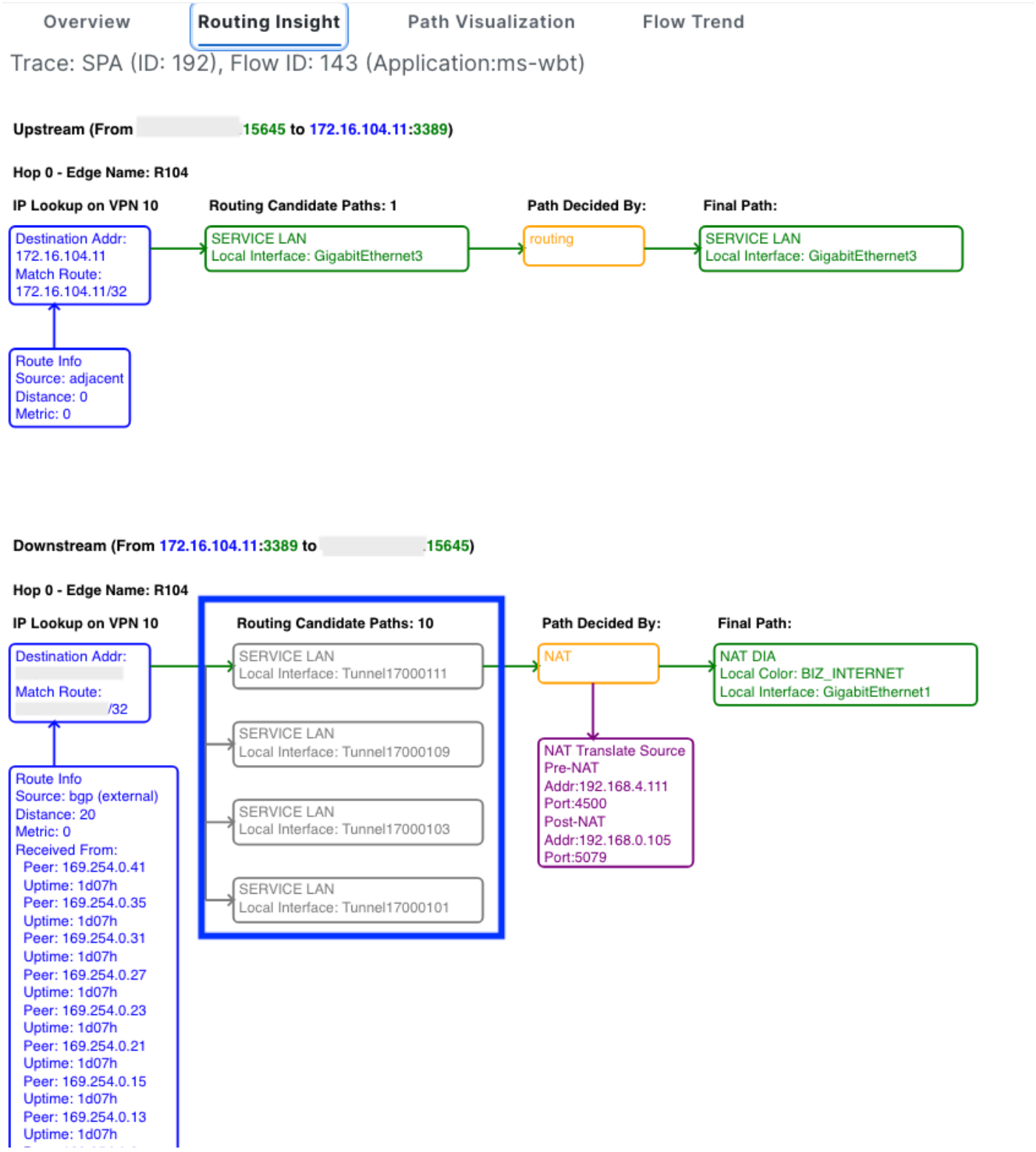

- Trace Name: (선택 사항) 추적 이름 지정
- Site: 프라이빗 리소스가 있는 사이트 선택
- VPN: 프라이빗 리소스가 있는 VPN ID를 선택합니다
- Source/Destination Address: (선택 사항) IP를 입력하거나 디스크에 남겨 두어 기준으로 필터링된 모든 트래픽을 캡처하고 SiteVPN선택합니다

추적 시작

트래픽 흐름을 찾고 Insights 열에서 View를 클릭합니다.




Routing Insights 열에는 후보 경로가 표시되고 Secure Access에 대한 IPSec 터널이 표시됩니다




## 관련 정보

- Cisco 기술 지원 및 다운로드
- Cisco Secure Access Help Center
- Cisco ISE 설계 가이드
- 보안 인터넷 액세스를 위한 SD-WAN 자동 터널로 보안 액세스 구성
- 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.