Catalyst SD-WAN에서 SSE(Secure Access) 통합 구성 및 문제 해결

목차

소개

이 문서에서는 Catalyst SD-WAN에서 액티브-액티브 SSE 통합을 구성하는 방법을 설명하고 문제 해결을 안내합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco SD-WAN(소프트웨어 정의 WAN)
- 컨피그레이션 그룹
- 정책 그룹

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- C8000V 버전 17.15.02
- vManage 버전 20.15.02

- Cisco Secure Access 계정

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.

Cisco 보안 액세스

Cisco Secure Access는 여러 네트워크 보안 서비스를 통합하는 클라우드 기반 SSE(Security Service Edge) 솔루션으로서 클라우드에서 제공하여 하이브리드 인력을 지원합니다. Cisco SD-WAN Manager는 REST API를 활용하여 Cisco Secure Access에서 정책 정보를 검색하고 이 정보를 Cisco IOS XE SD-WAN 장치에 배포합니다. 이러한 통합을 통해 사용자는 원활하고 투명하며 안전한 DIA(Direct Internet Access)를 사용할 수 있으므로 어떤 장치에서든 어디에서든 안전하게 연결할 수 있습니다.

Cisco SSE를 사용하면 SD-WAN 디바이스에서 IPSec 터널을 사용하여 SSE 제공자와의 연결을 설정할 수 있습니다. 이 문서는 Cisco Secure Access 사용자를 대상으로 합니다.

예비 컨피그레이션

- 디바이스에 대한 도메인 조회 활성화: Configuration Groups(컨피그레이션 그룹) > System Profile(시스템 프로파일) > Global(전역)로 이동하고 Domain Lookup(도메인 조회)을 활성화합니다.

참고: 기본적으로 도메인 조회는 비활성화되어 있습니다.

- DNS 구성: 라우터가 DNS를 확인하고 VPN 0에서 인터넷에 액세스할 수 있습니다.
- NAT DIA 구성: DIA 컨피그레이션은 SSE 터널이 생성된 라우터에 있어야 합니다.

루프백 인터페이스 생성

액티브/액티브 컨피그레이션의 두 터널이 모두 동일한 대상 데이터 센터에 연결되고 소스와 동일한 WAN 인터페이스를 사용하는 경우 두 개의 루프백 IP 주소를 생성해야 합니다.

참고: 두 터널이 동일한 소스와 대상으로 구성된 경우 IKEv2는 로컬 ID와 원격 ID로 구성된 ID 쌍을 형성합니다. 기본적으로 로컬 ID는 터널 소스 인터페이스의 IP 주소입니다. 이 ID 쌍은 고유해야 하며 두 터널 간에 공유할 수 없습니다. IKEv2 상태에서 혼동을 방지하기 위해 각 터널은 서로 다른 루프백 인터페이스를 소스로 사용합니다. IKE 패킷이 DIA 인터페이스에서 변환(NATed)되지만, 로컬 ID는 변경되지 않고 원래 루프백 IP 주소를 유지합니다.

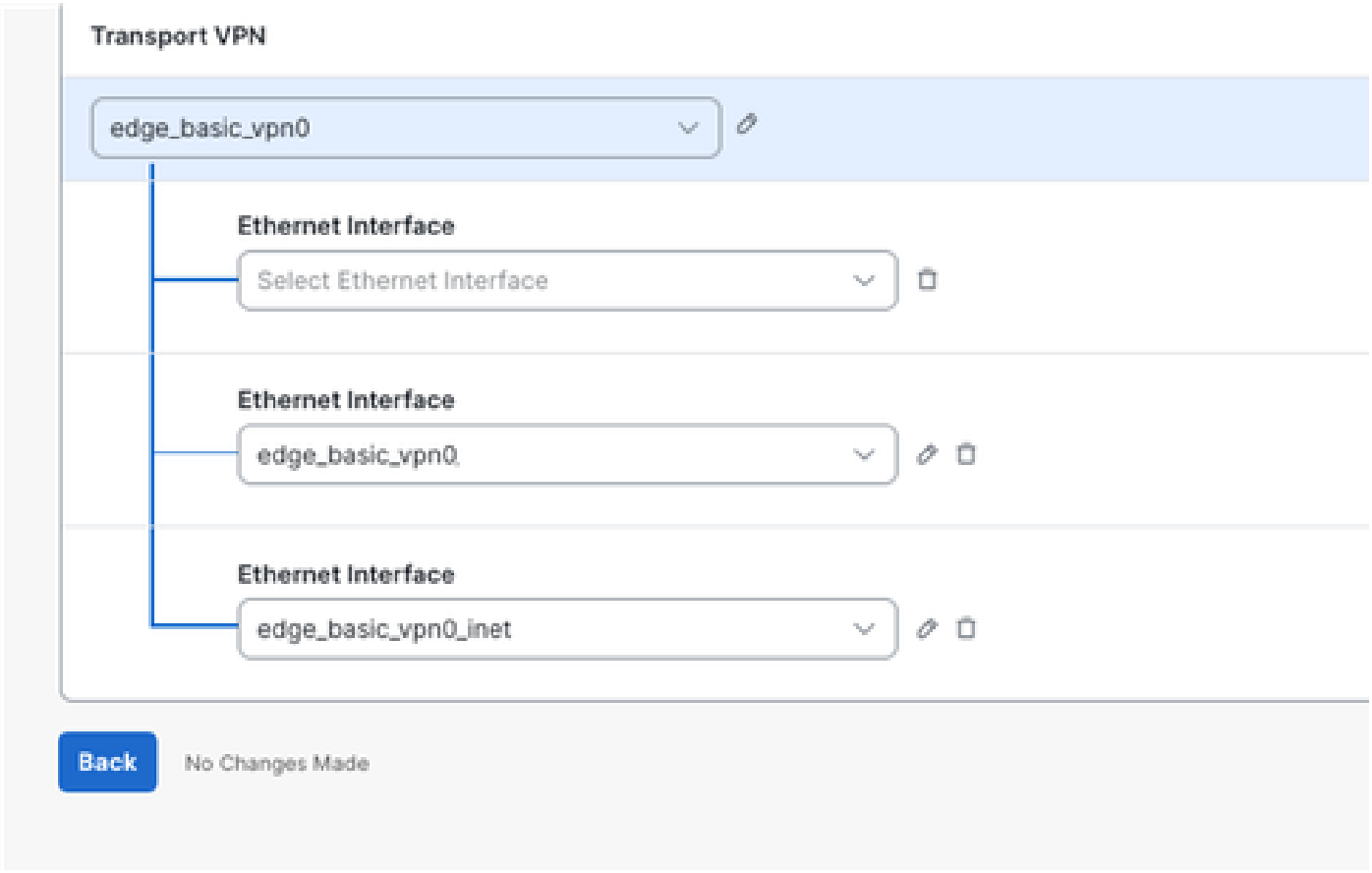
---

1. Configuration(컨피그레이션) > Configuration Groups(컨피그레이션 그룹) > Configuration Group

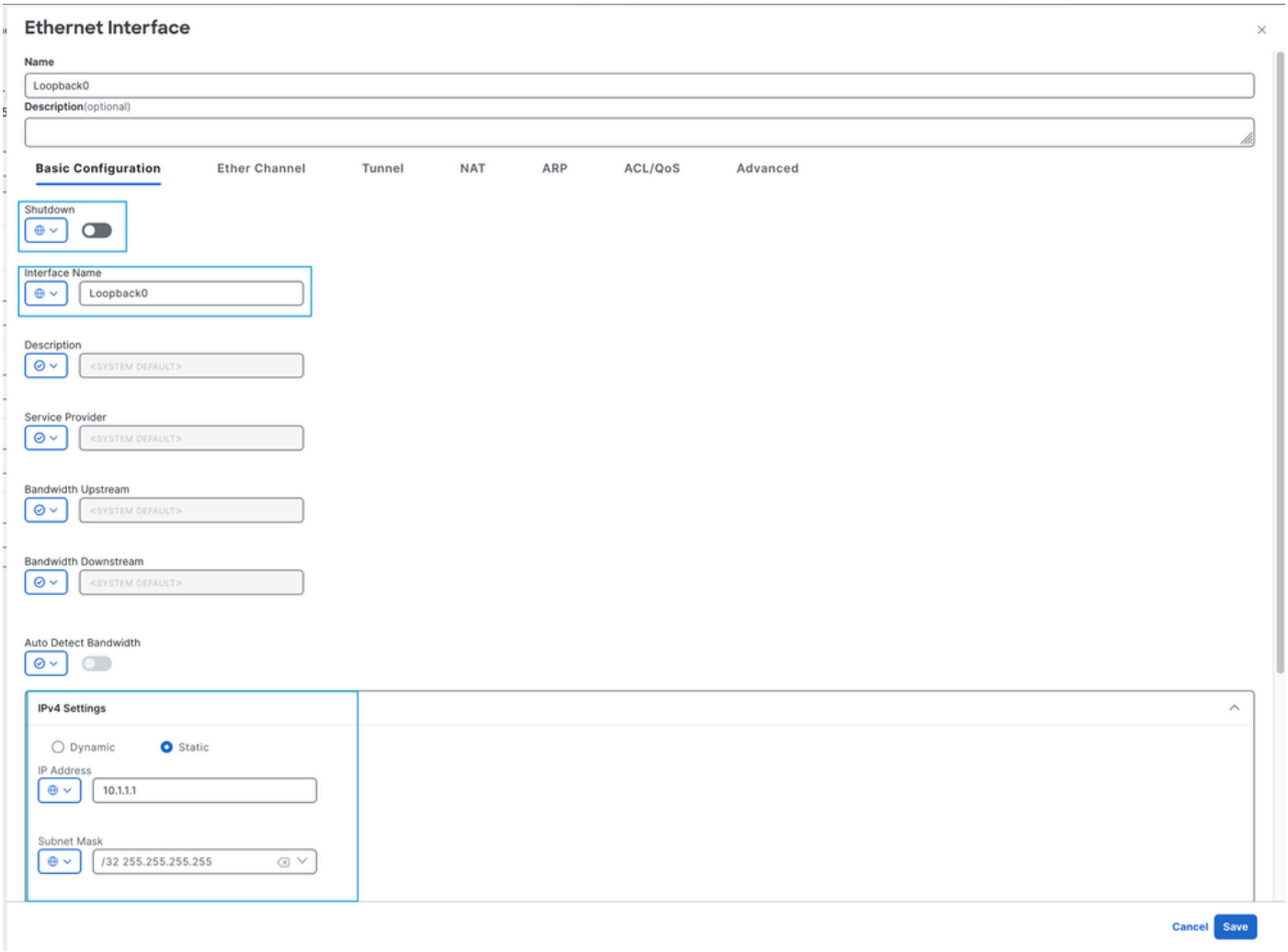
Name(컨피그레이션 그룹 이름)> Transport & Management Profile(전송 및 관리 프로필)로 이동하고 > Edit(수정)를 클릭합니다..

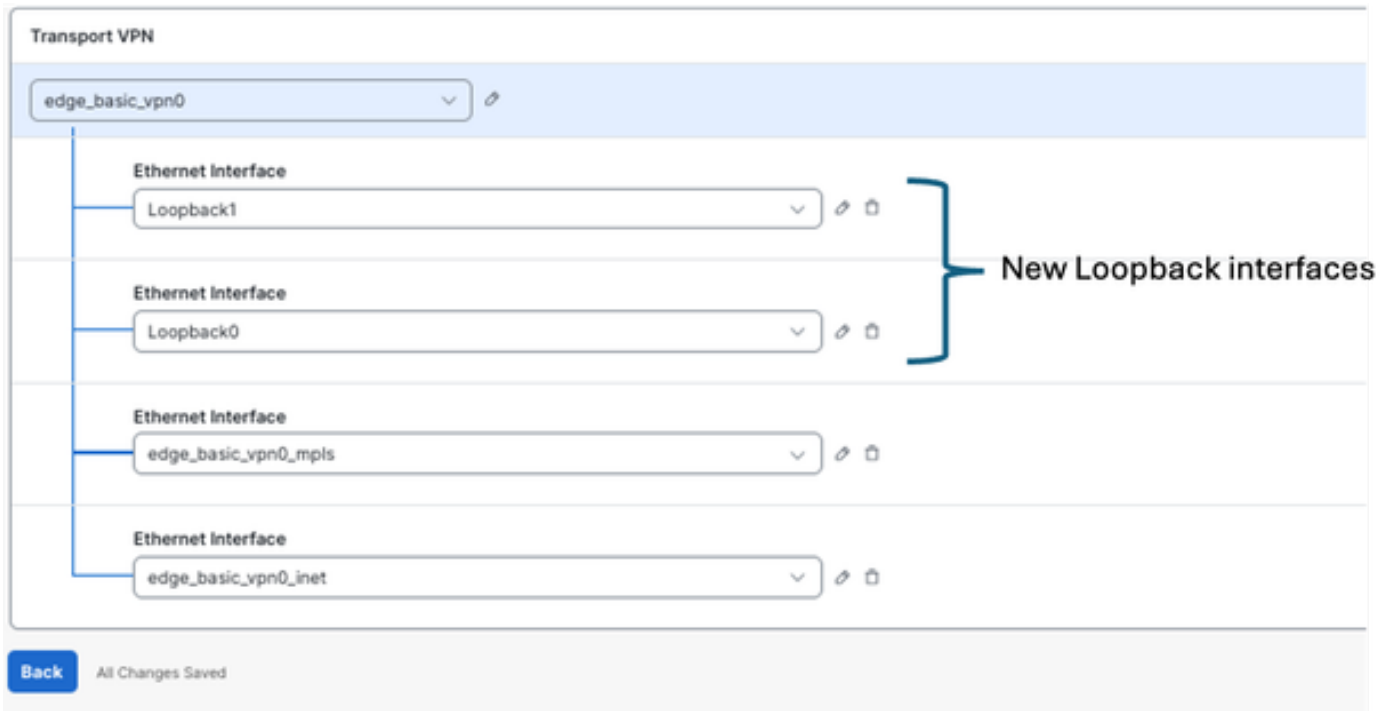
2. 전송 VPN 프로필(기본 프로필)의 오른쪽에 있는 더하기 기호(+)를 클릭합니다. 그러면 맨 오른쪽에 있는 피쳐 추가(Add Feature) 메뉴가 열립니다.

3. 이더넷 인터페이스를 클릭합니다. Transport VPN(전송 VPN)에 새 인터넷 인터페이스를 추가합니다.

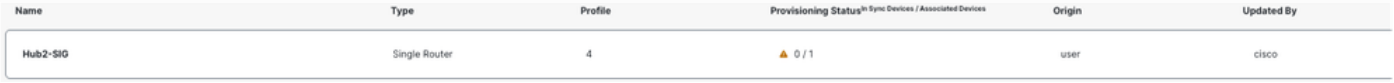


4. 그림의 Loopback 0 예시와 같이 RFC1918 IPv4 주소를 사용하여 두 개의 루프백 인터페이스를 만듭니다.



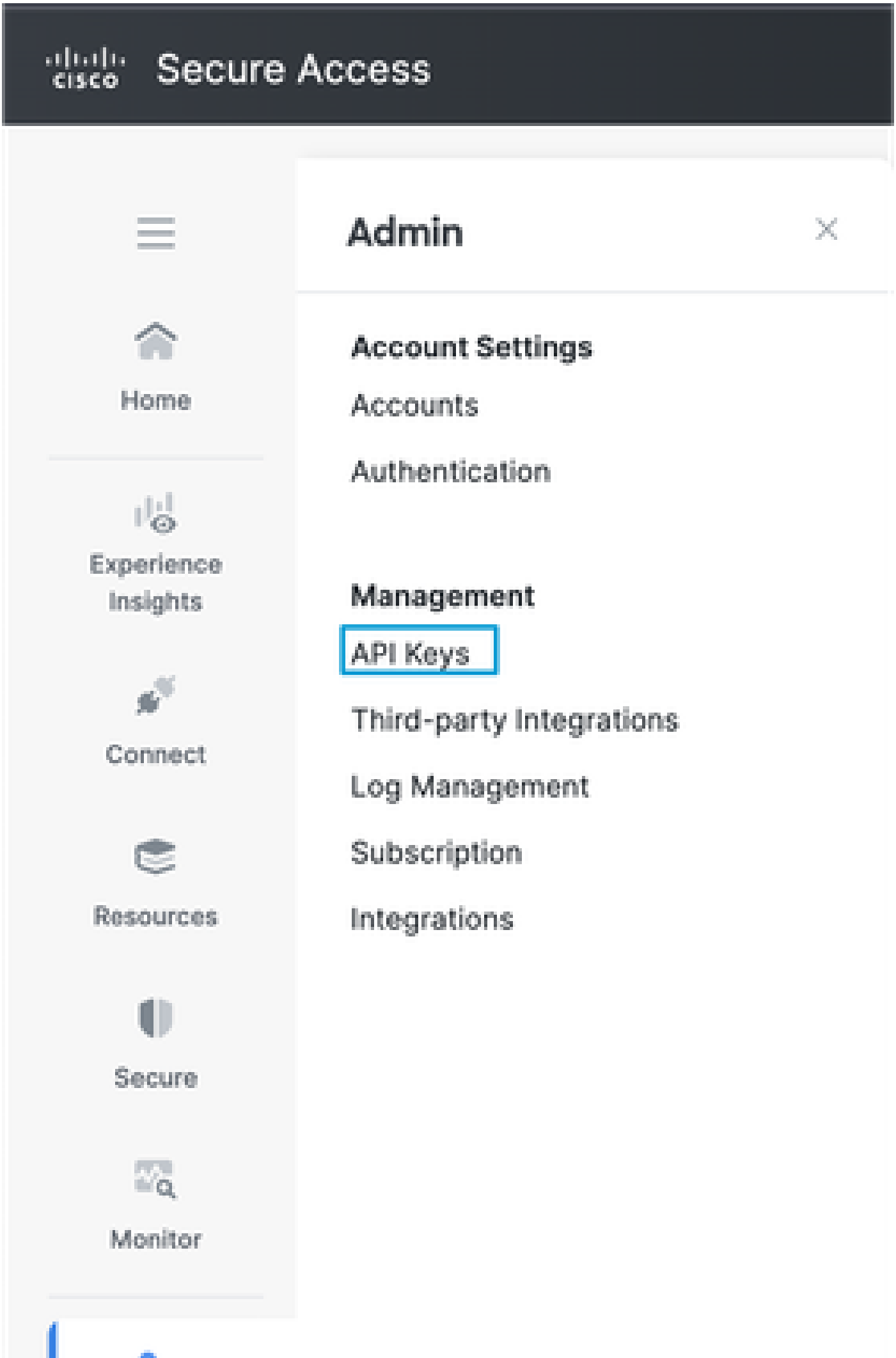


5. 루프백 컨피그레이션을 적용한 후 컨피그레이션 변경 사항을 디바이스에 구축합니다. 프로비저닝 상태가 1/1에서 0/1로 변경됩니다.



SSE 포털에서 새 API 키 구성

1. SSE 포털 https://login.sse.cisco.com/에 액세스
2. Admin(관리) > API Keys(API 키)로 이동합니다


Secure Access
Admin
Account Settings
Accounts
Authentication
Management
API Keys
Third-party Integrations
Log Management
Subscription
Integrations
Home
Experience Insights
Connect
Resources
Secure
Monitor

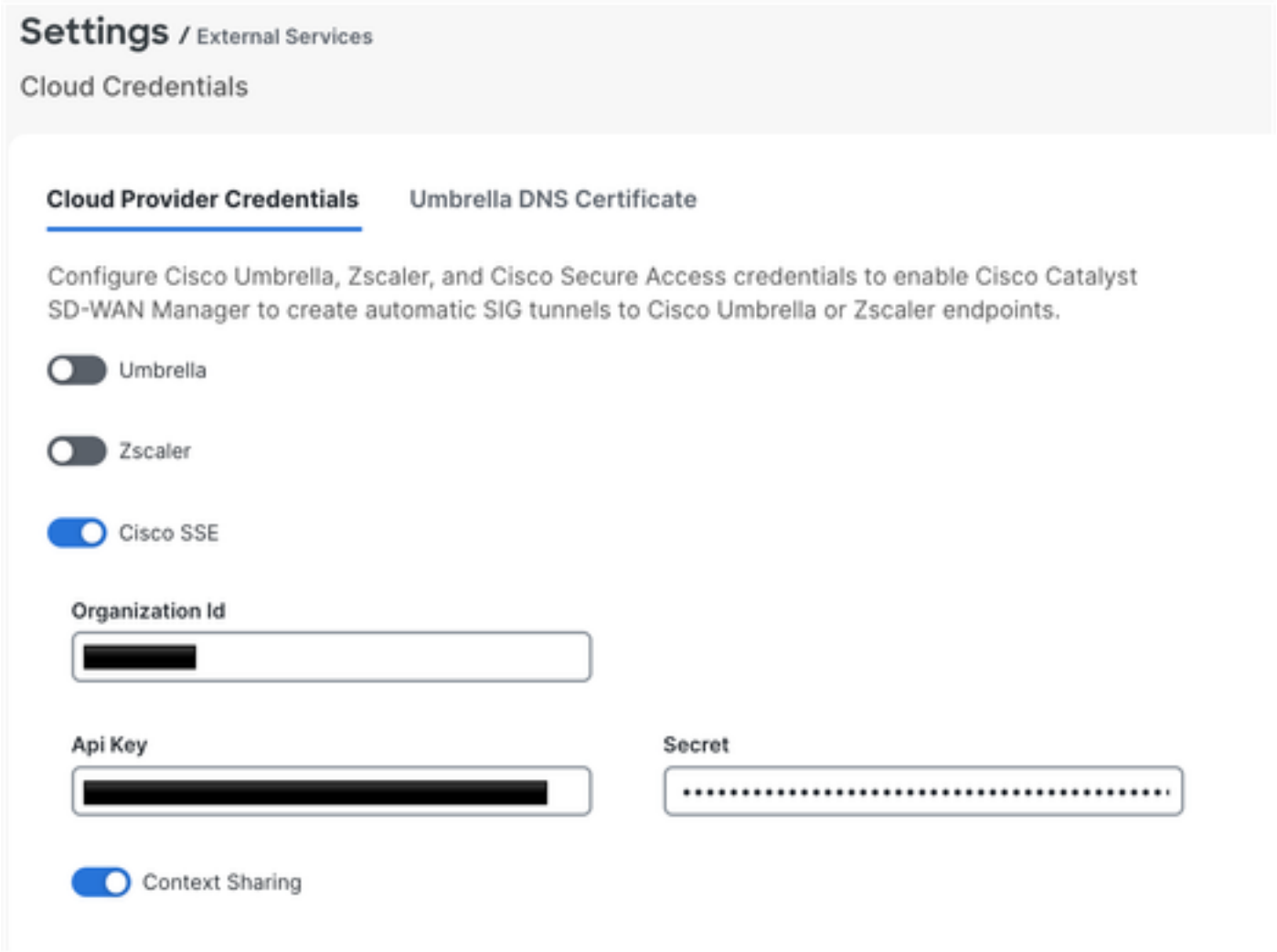
6. API 키와 키 암호를 메모장에 복사하고 수락 및 닫기를 선택합니다

7. URL https://dashboard.sse.cisco.com/#some-numbers#/admin/apikeys 아래#some-numbers#는 조직 ID입니다. 해당 정보를 메모장에도 복사합니다.

Catalyst Manager에서 SSE 구성

클라우드 자격 증명 설정

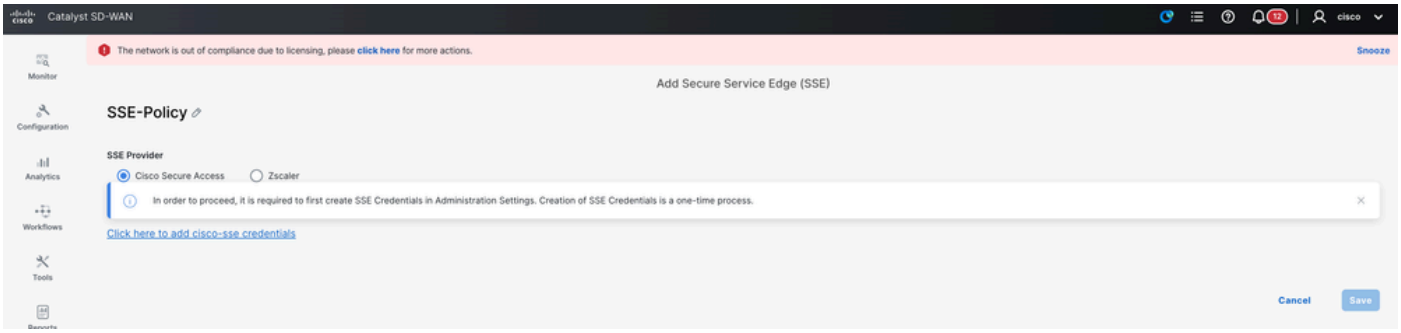
1. Administration(관리) > Settings(설정) > Cloud Credentials(클라우드 자격 증명) > Cloud Provider Credentials(클라우드 제공자 자격 증명)로 이동하여 Cisco Secure Access를 활성화합니다 세부사항을 입력합니다.



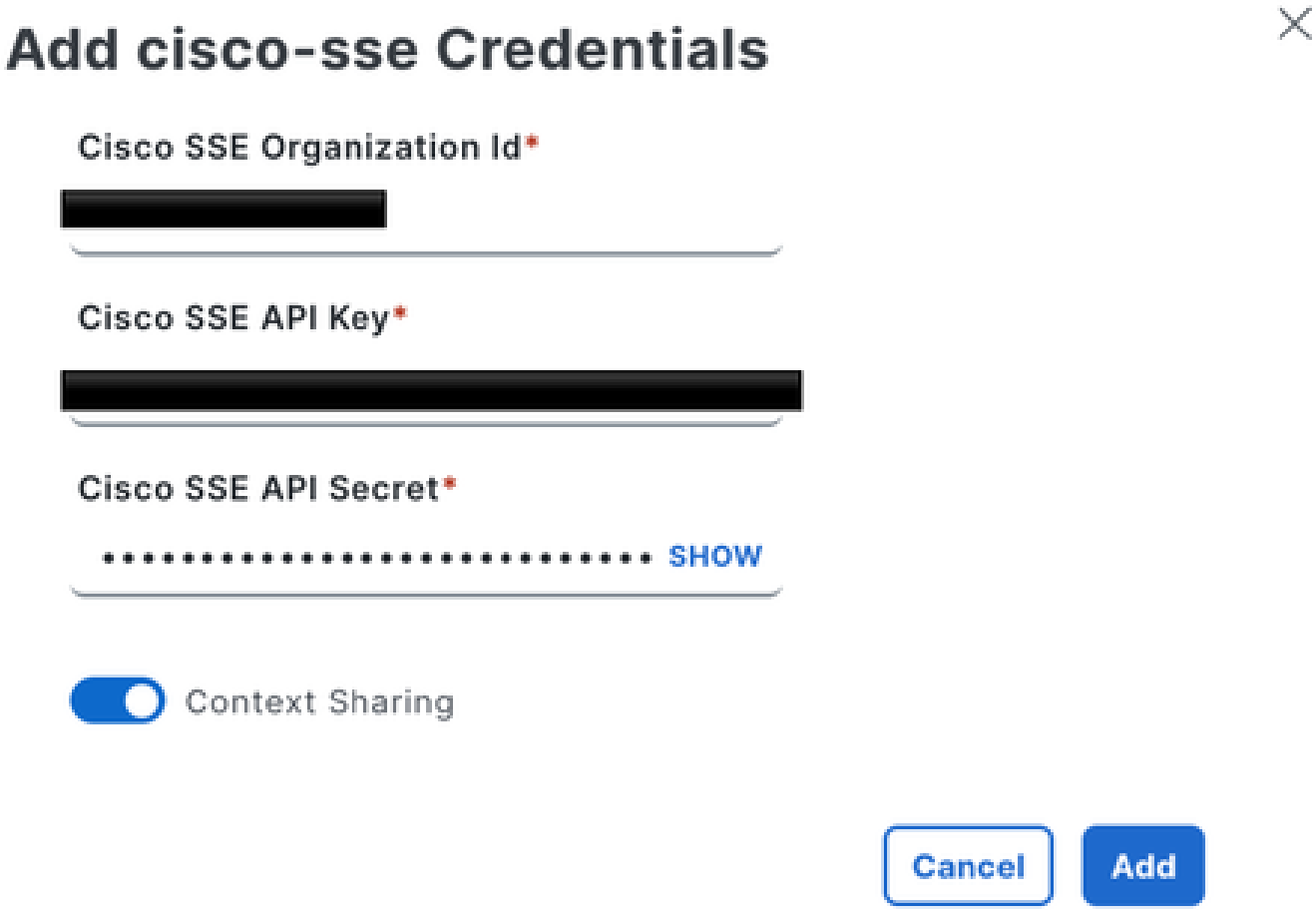
2. 선택 사항 향상된 기능을 위해 컨텍스트 공유를 활성화할 수 있습니다. 자세한 내용은 [컨텍스트 공유에 대한 Cisco SSE 사용 설명서를 참조하십시오](#).

정책 그룹을 사용하여 SSE 터널 구성

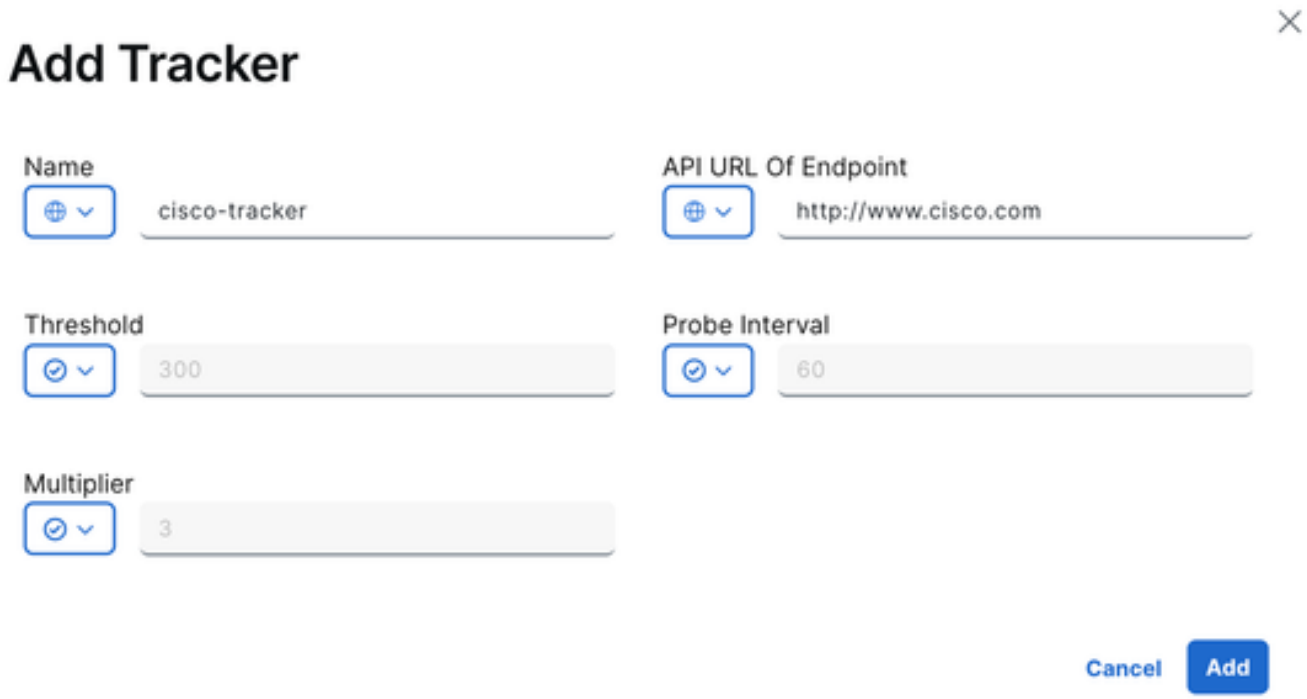
SD-WAN Manager에서 Configuration(컨피그레이션) > Policy Groups(정책 그룹) > Secure Internet Gateway/Secure Service Edge(보안 인터넷 게이트웨이/보안 서비스 에지)로 이동하고 Add Secure Service Edge (SSE)(보안 서비스 에지 추가)를 클릭합니다.

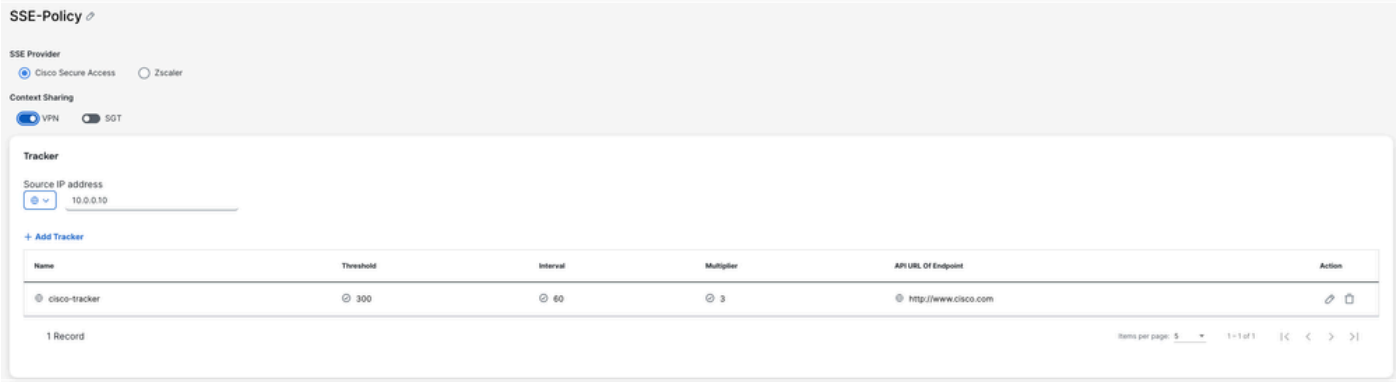


참고: 클라우드 자격 증명이 아직 구성되지 않은 경우 이 단계에서 추가할 수 있습니다. 자격 증명이 이미 구성된 경우 자동으로 로드됩니다.



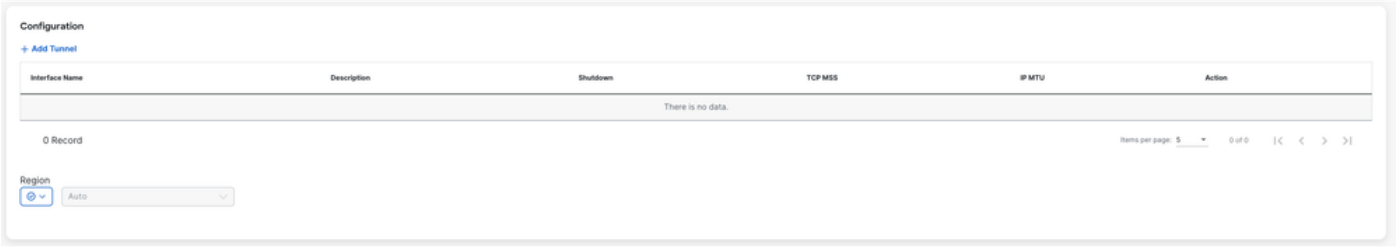
1. SSE 추적기를 구성합니다. 이 예에서는 추적기 URL이 http://www.cisco.com으로 설정되고 소스 IP 주소가 루프백 인터페이스 중 하나에서 할당됩니다.



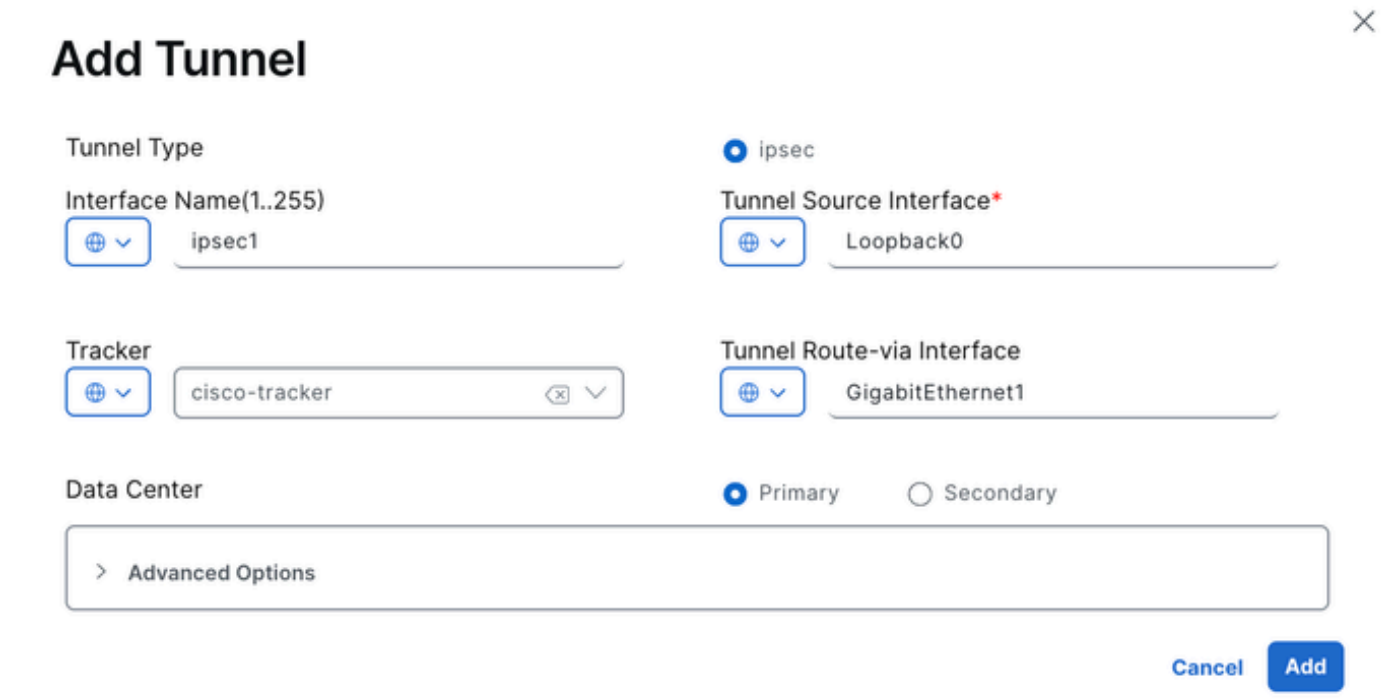


선택적으로, 클라우드 자격 증명이 구성될 때 컨텍스트 공유가 활성화되었으므로 VPN이 이 예의 옵션으로 선택됩니다.

2. Add Tunnel(터널 추가)을 클릭합니다.

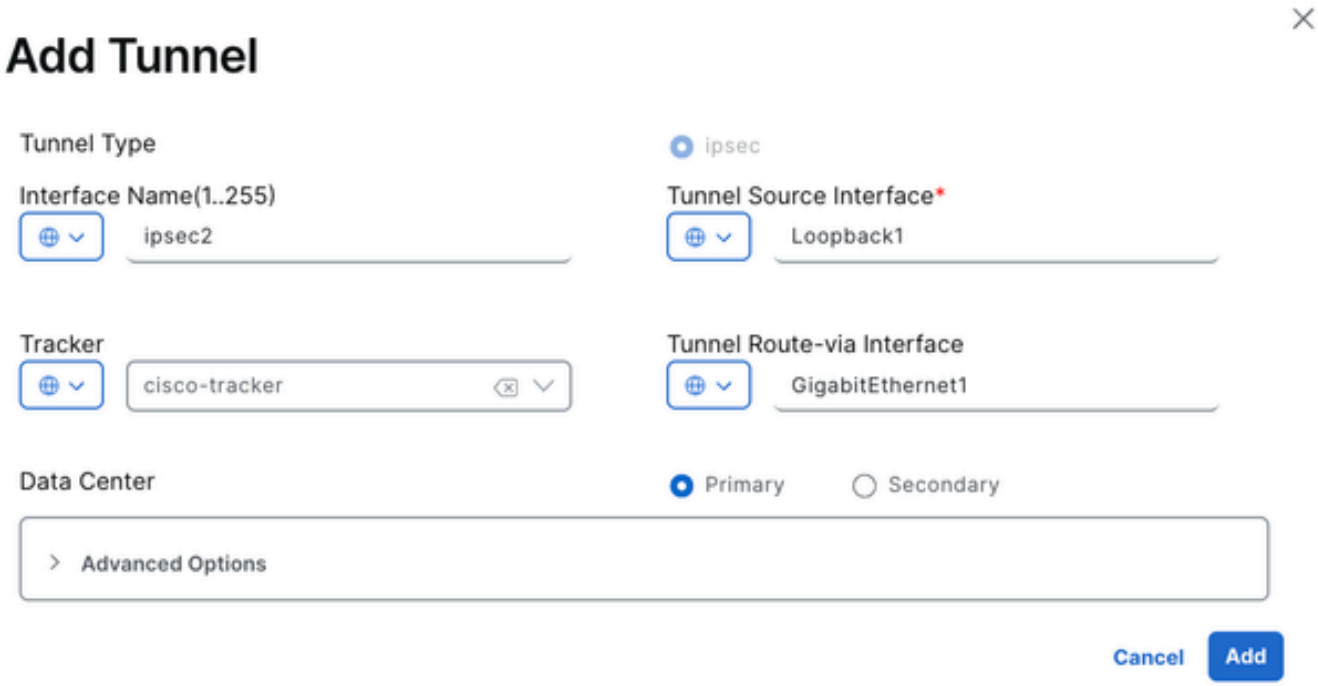


3. 이 예에서는 Loopback0 인터페이스가 터널 소스로 사용되는 반면, GigabitEthernet1 인터페이스는 트래픽을 라우팅하는 WAN 인터페이스로 사용됩니다.



이 예에서 추적기가 구성되었으므로 설정이 Global로 변경되고 사전 구성된 cisco-tracker가 선택됩니다.

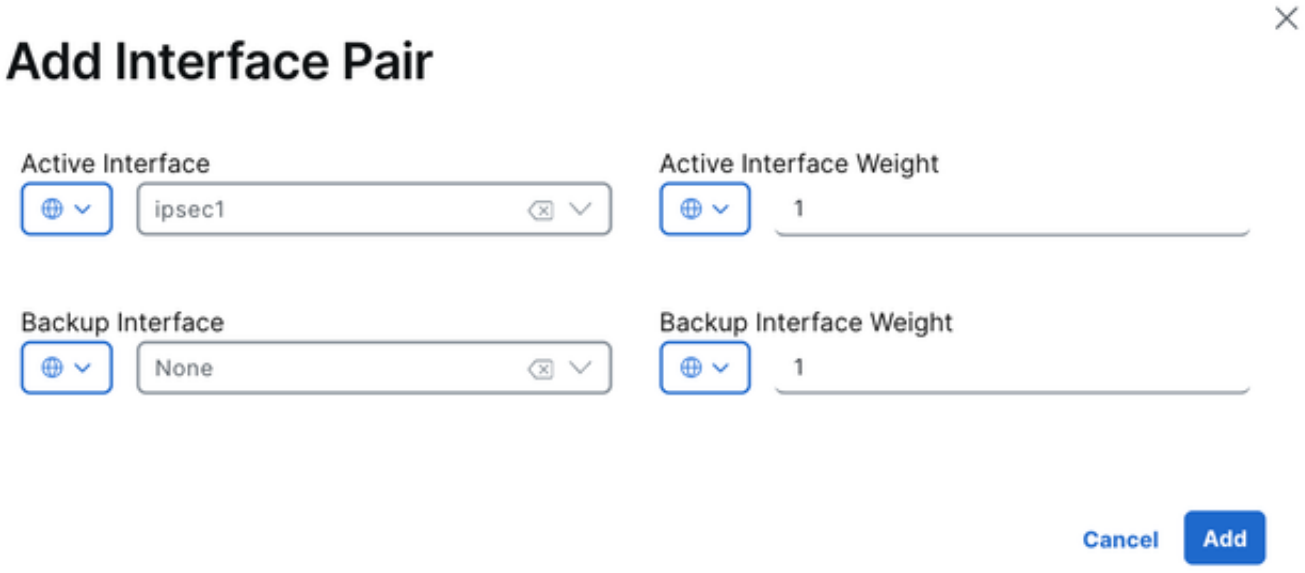
4. 두 번째 터널의 경우 동일한 매개변수를 사용하여 동일한 단계를 반복하되 인터페이스 이름을 ipsec1에서 ipsec2로, 소스 인터페이스 이름을 루프백1으로 변경합니다.



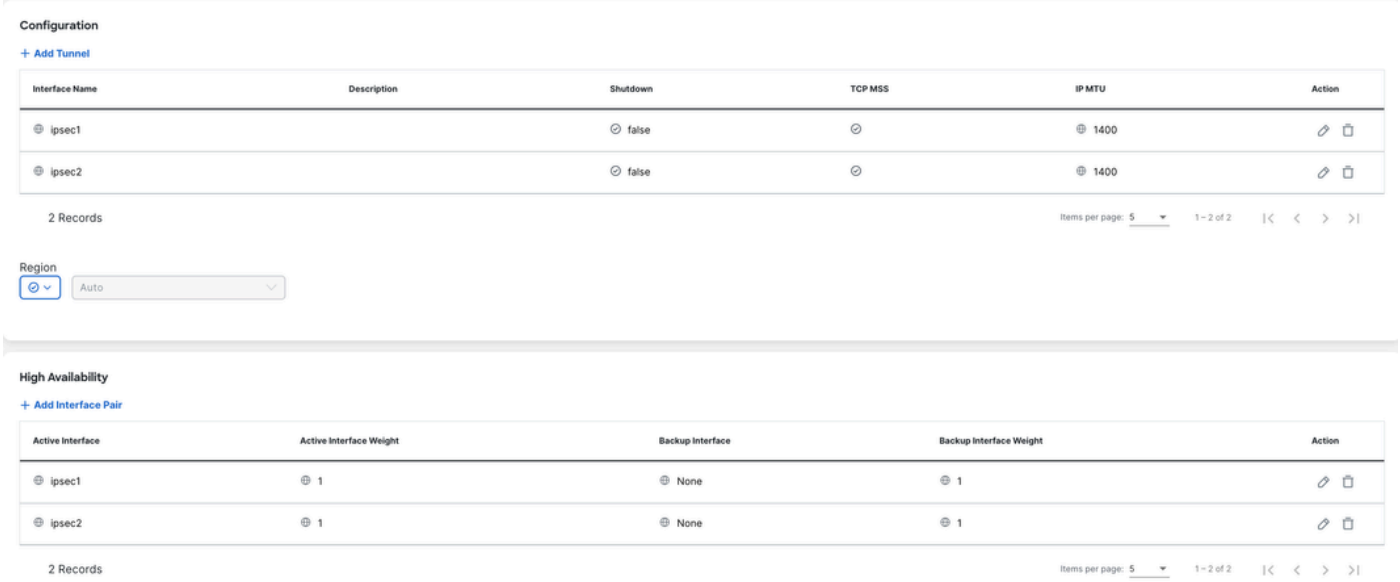
두 터널 모두 백업 없이 동시에 활성화되도록 구성됩니다.

5. Add Interface Pair(인터페이스 쌍 추가)를 클릭합니다.

6. 추가를 클릭합니다. 활성 인터페이스가 ipsec1로 설정되며 백업 인터페이스가 지정되지 않습니다.



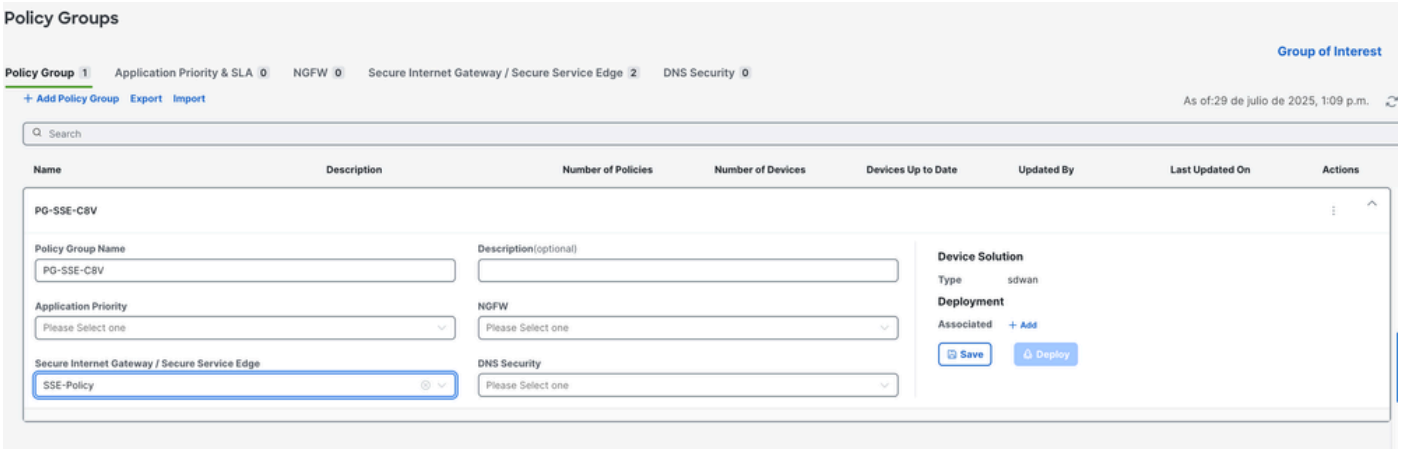
7. 두 번째 터널인 ipsec2에 대해 동일한 작업이 반복됩니다.



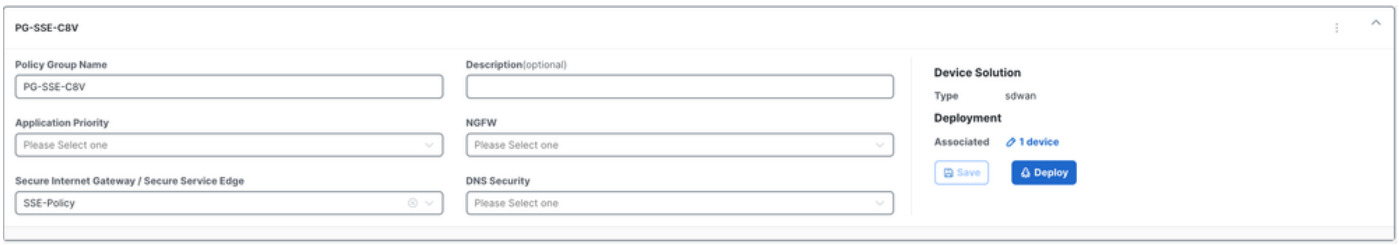
8. 구성을 저장합니다.

정책 그룹 구성

1. 정책 그룹 내에서 이전에 생성한 정책을 선택하고 저장할 수 있습니다.



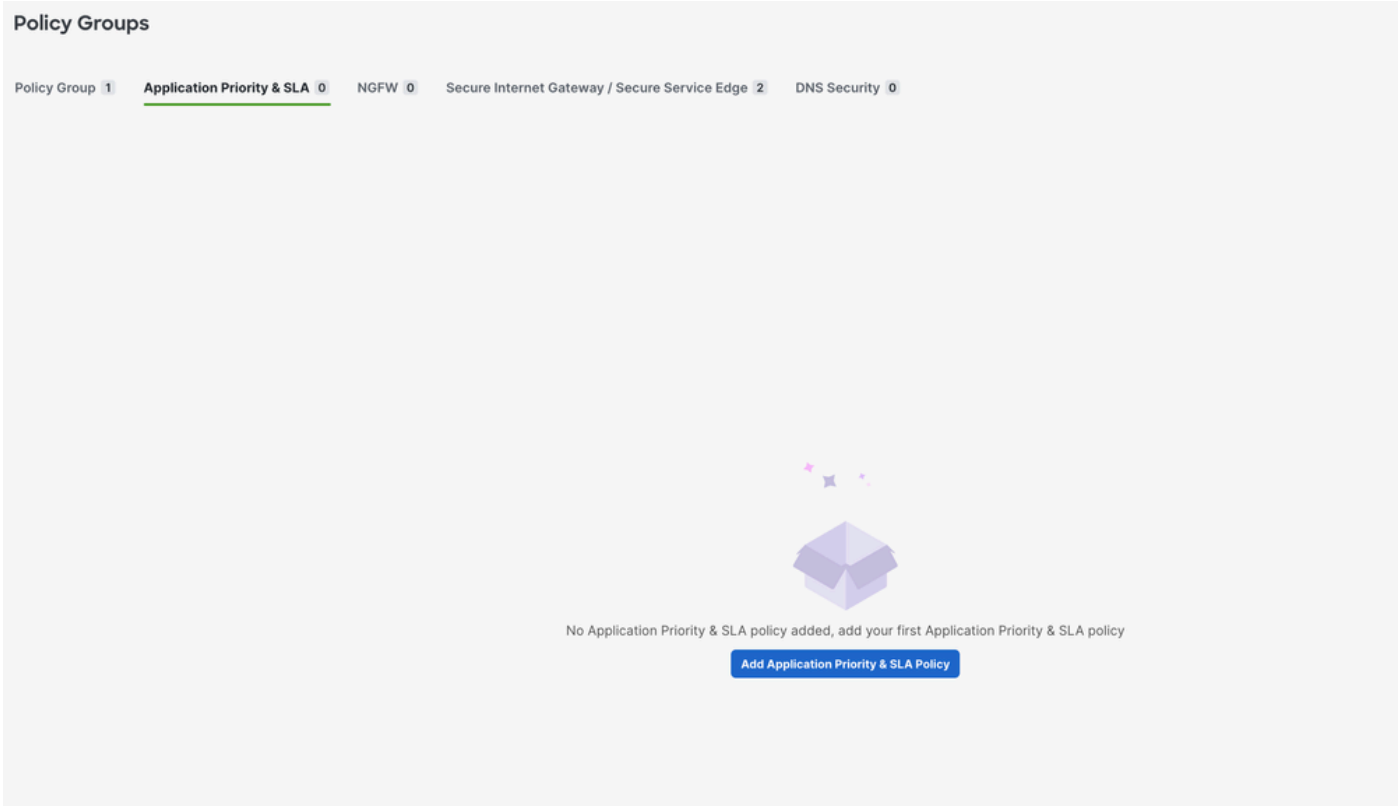
2. 디바이스 또는 디바이스가 정책 그룹과 연결되면 정책 그룹을 구축합니다.



트래픽을 SSE로 리디렉션하도록 정책 그룹 구성

1. SD-WAN Manager에서 Configuration(컨피그레이션) > Policy Groups(정책 그룹) > Application Priority & SLA(애플리케이션 우선순위 및 SLA)로 이동합니다.

- Add Application Priority & SLA Policy(애플리케이션 우선순위 및 SLA 정책 추가)를 선택합니다.
- 정책의 이름을 지정합니다.

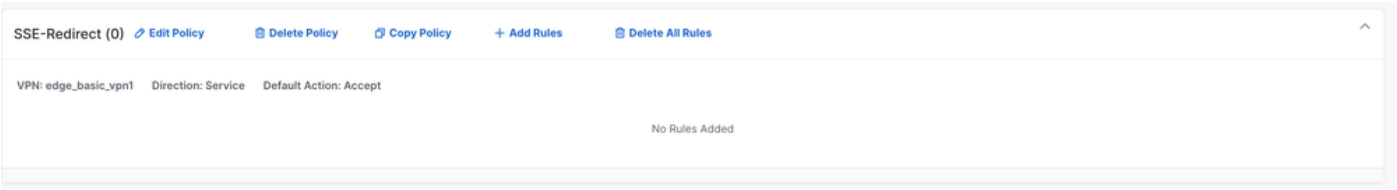


2. 새 정책이 표시되면 고급 레이아웃 토글을 선택합니다.

3. Add Traffic Policy List를 선택합니다.

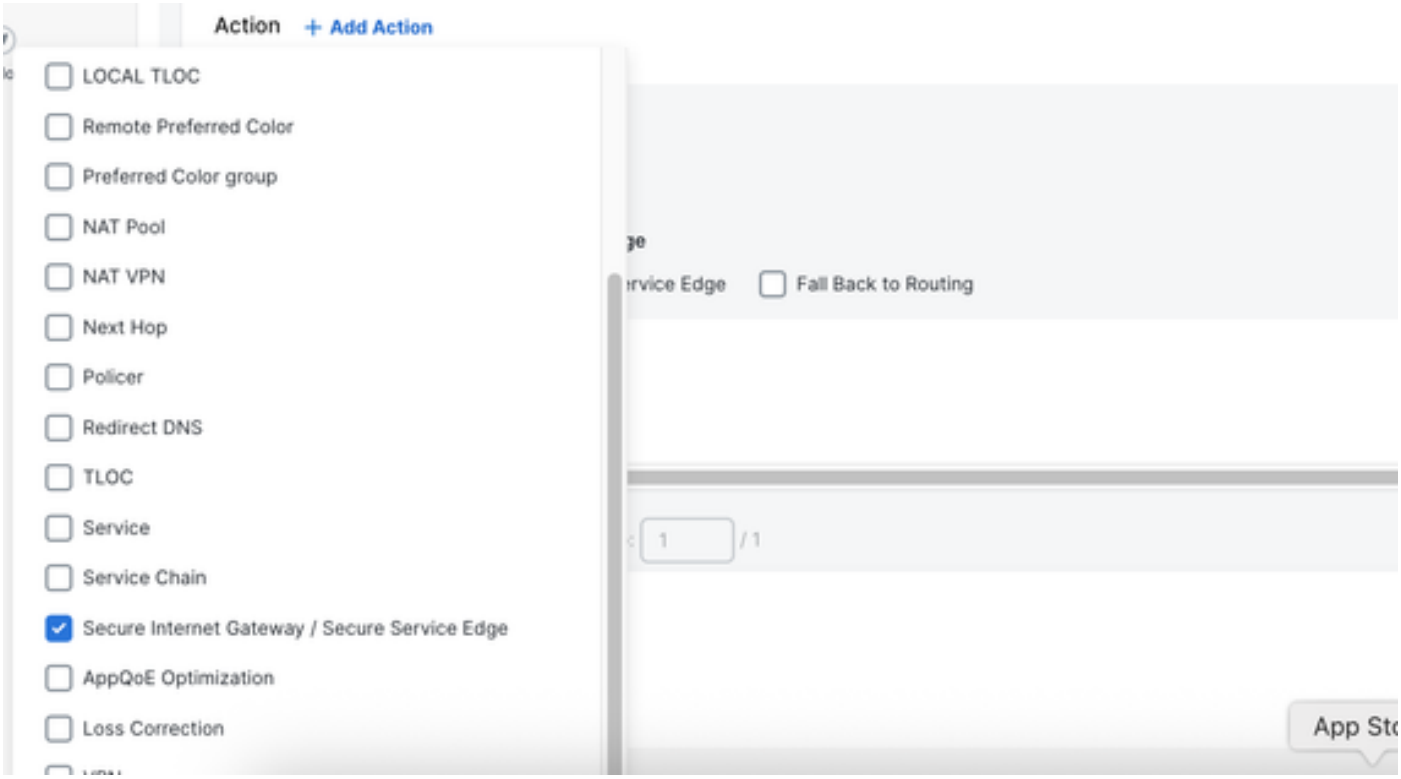
- SSE 터널로 트래픽을 리디렉션하도록 VPN을 구성합니다.
- 필요에 따라 Direction(방향) 및 Default Action(기본 작업)을 설정하고 저장합니다.

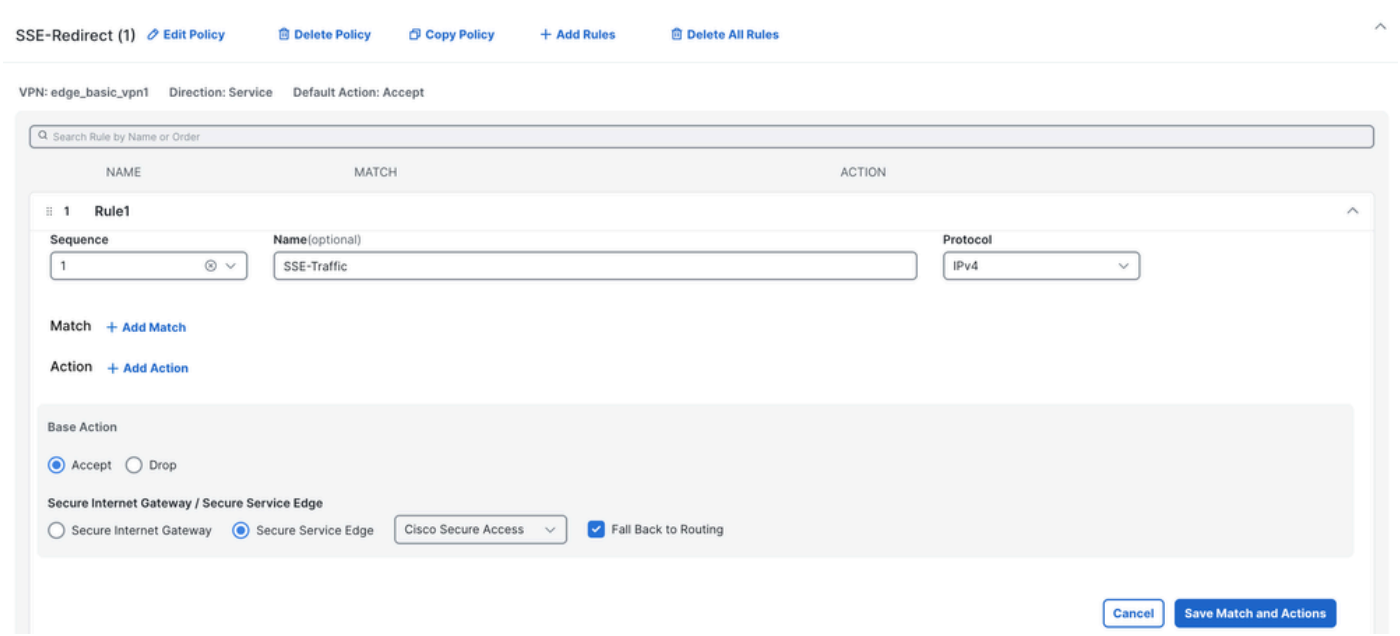
4. + 규칙 추가를 선택합니다.



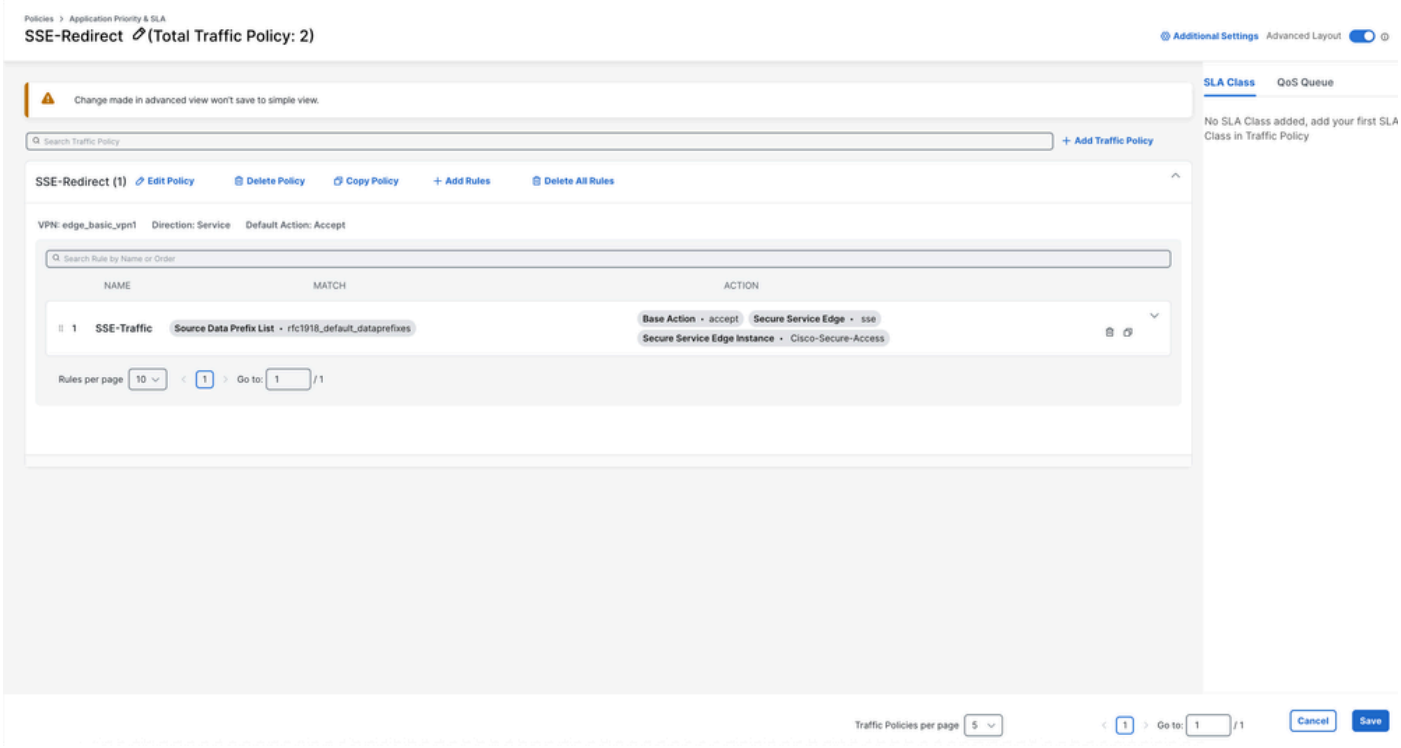
5. SSE로 트래픽을 리디렉션하도록 일치 트래픽 기준을 구성합니다.
6. 기본 조치로 수락을 선택한 다음 + 조치를 클릭합니다.

7. Secure Internet Gateway/Secure Service Edge 작업을 찾아 Secure Service Edge로 설정합니다
.



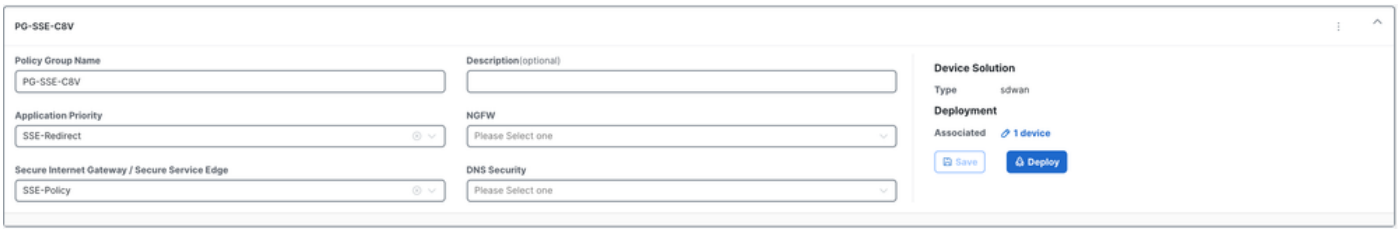


8. Save Match and Actions(일치 및 작업 저장)를 클릭합니다.



9. 저장을 클릭합니다.

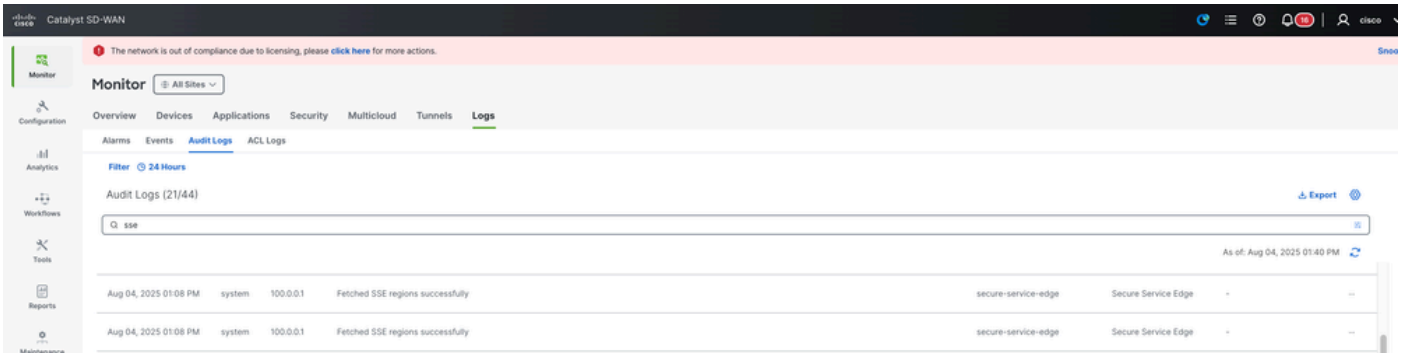
10. Configuration(컨피그레이션) > Policy Groups(정책 그룹)로 이동하고 방금 생성한 애플리케이션 우선순위 정책을 선택합니다. 저장 후 구축합니다.



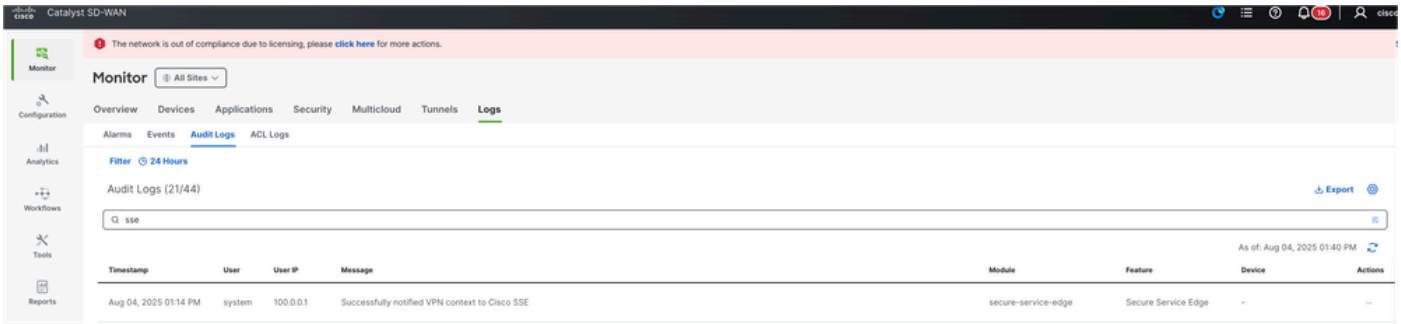
다음을 확인합니다.

관리자

1. 모니터 > 로그 > 감사 로그 및 "sse"를 검색 합니다.

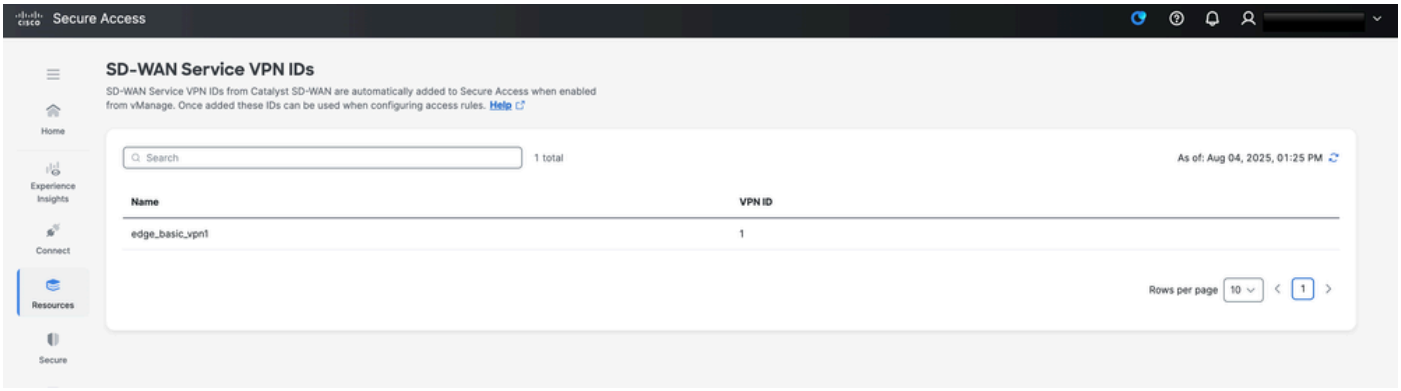


2. 관리자를 확인하여 컨텍스트 공유 VPN이 성공적으로 활성화되었는지 확인할 수 있습니다.



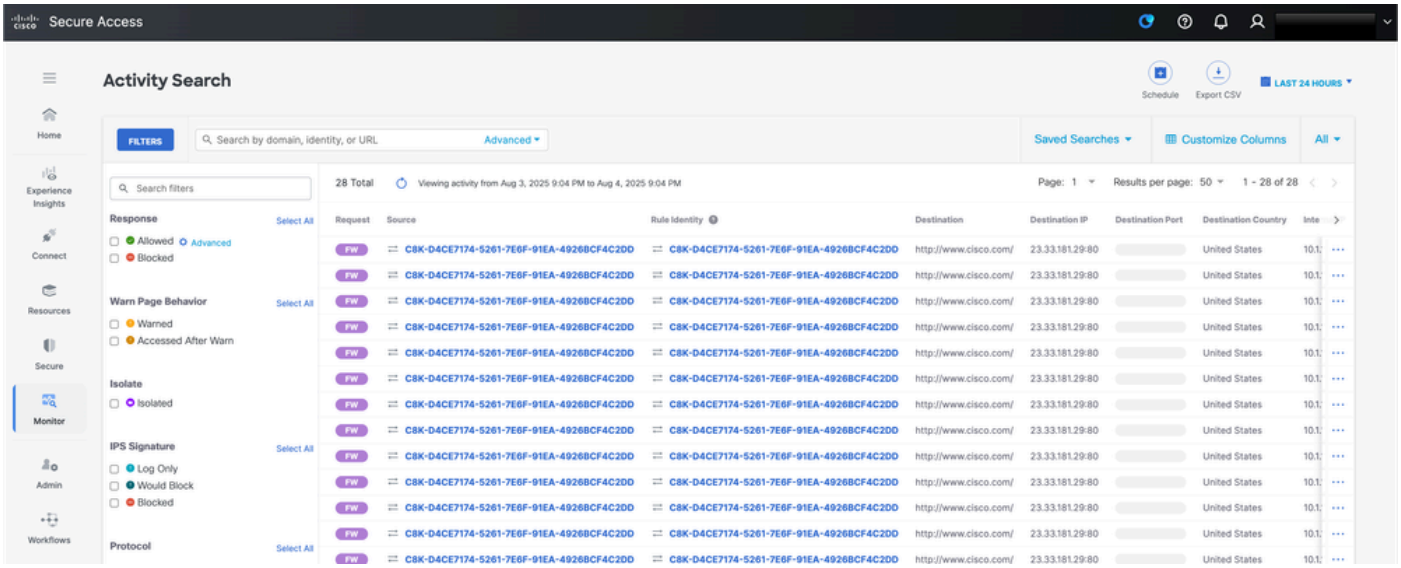
보안 액세스 대시보드

컨텍스트 공유
SSE 대시보드를 확인하여 컨텍스트 공유 VPN이 성공적으로 활성화되었는지 확인할 수 있습니다 .리소스 > SD-WAN Service VPN ID



위로 터널

터널이 가동되고 터널을 통해 흐르는 트래픽과 함께 추적기가 작동하는 경우 Monitor(모니터) > Activity Search(활동 검색)로 이동하여 이를 검증할 수 있습니다. 이 화면에서는 터널을 통과하는 트래픽(예: 추적기에서 생성한 www.cisco.com에 대한 요청)이 표시됩니다. 이 가시성은 추적기가 작동 중임을 확인하고 터널을 통과하는 트래픽을 능동적으로 모니터링합니다



CLI(Command Line Interface) 명령

<#root>

```
Hub2-SIG#show sse all
**************************************
SSE Instance Cisco-Secure-Access
**************************************
Tunnel name : Tunnel16000001
Site id: 2
Tunnel id: 655184839
SSE tunnel name: C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD
HA role: Active
```

Local state: Up

Tracker state: Up

```
Destination Data Center: 44.217.195.188
Tunnel type: IPSEC
Provider name: Cisco Secure Access
Context sharing: CONTEXT_SHARING_SRC_VPN
```

관련 정보

- 컨텍스트 공유 SD-WAN 구성
- Cisco Secure Access와 SD-Routing의 통합
- 기술 지원 및 문서 – Cisco Systems

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.