Sophos XG 방화벽으로 보안 액세스 구성

목차

소개

이 문서에서는 Sophos XG 방화벽으로 보안 액세스를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

- 사용자 프로비저닝 구성
- ZTNA SSO 인증 컨피그레이션
- 원격 액세스 VPN 보안 액세스 구성

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Sophos XG 방화벽
- 보안 액세스
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

- 클라이언트리스 ZTNA

사용되는 구성 요소

이 문서의 정보는 다음을 기반으로 합니다.

- Sophos XG 방화벽
- 보안 액세스
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

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.

배경 정보

보안 액세스 - Sophos

Cisco는 온프레미스 및 클라우드 기반 프라이빗 애플리케이션에 대한 액세스 보호 및 프로비저닝을 보장하기 위해 보안 액세스를 설계했습니다. 또한 네트워크에서 인터넷으로의 연결도 보호합니다. 이는 여러 보안 방법 및 레이어의 구현을 통해 달성되며, 모두 클라우드를 통해 정보에 액세스할 때 정보를 보존하는 데 목적이 있습니다.

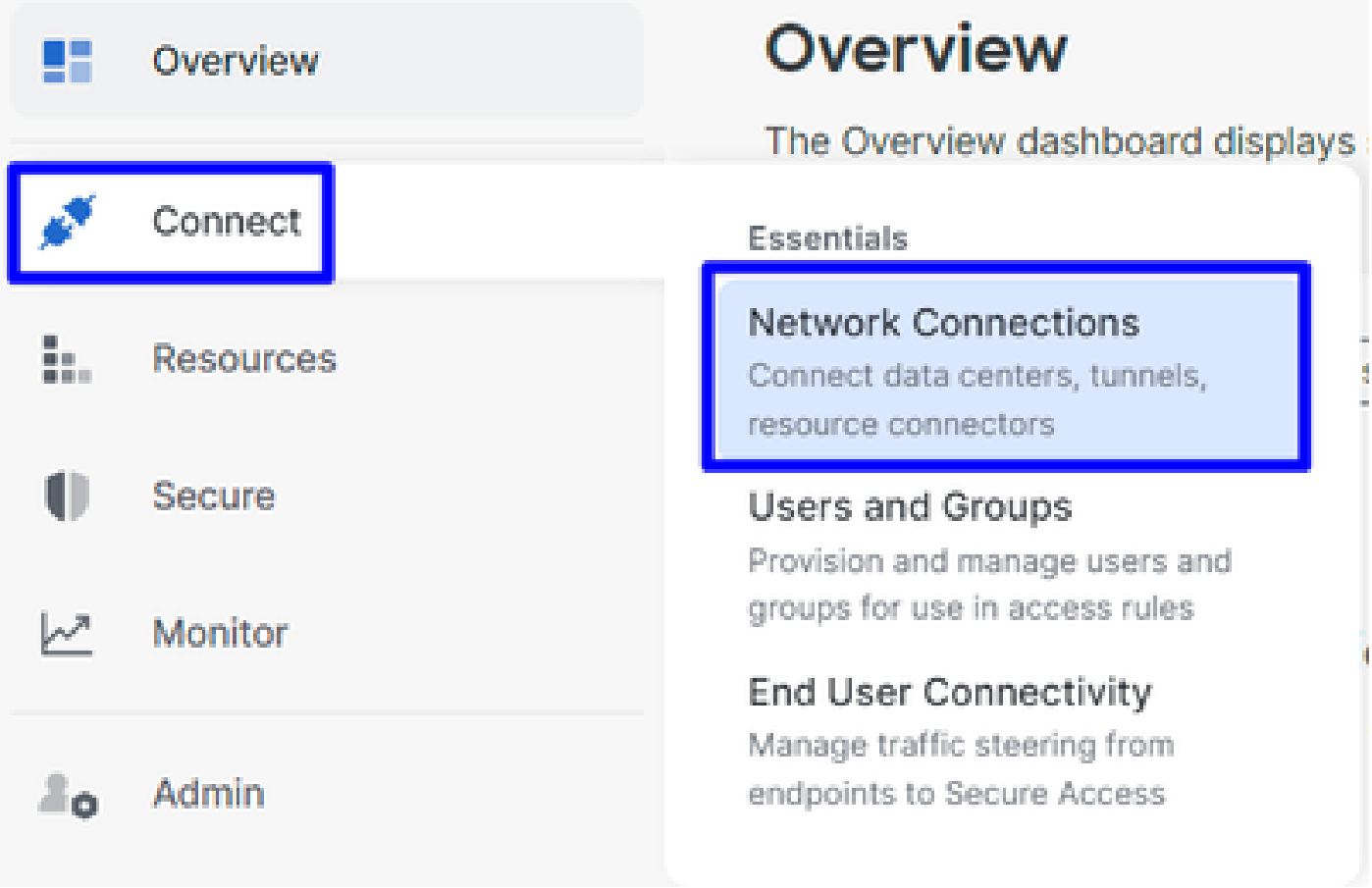
구성

보안 액세스에서 터널 구성

Secure Access의 관리자 패널로 이동합니다.

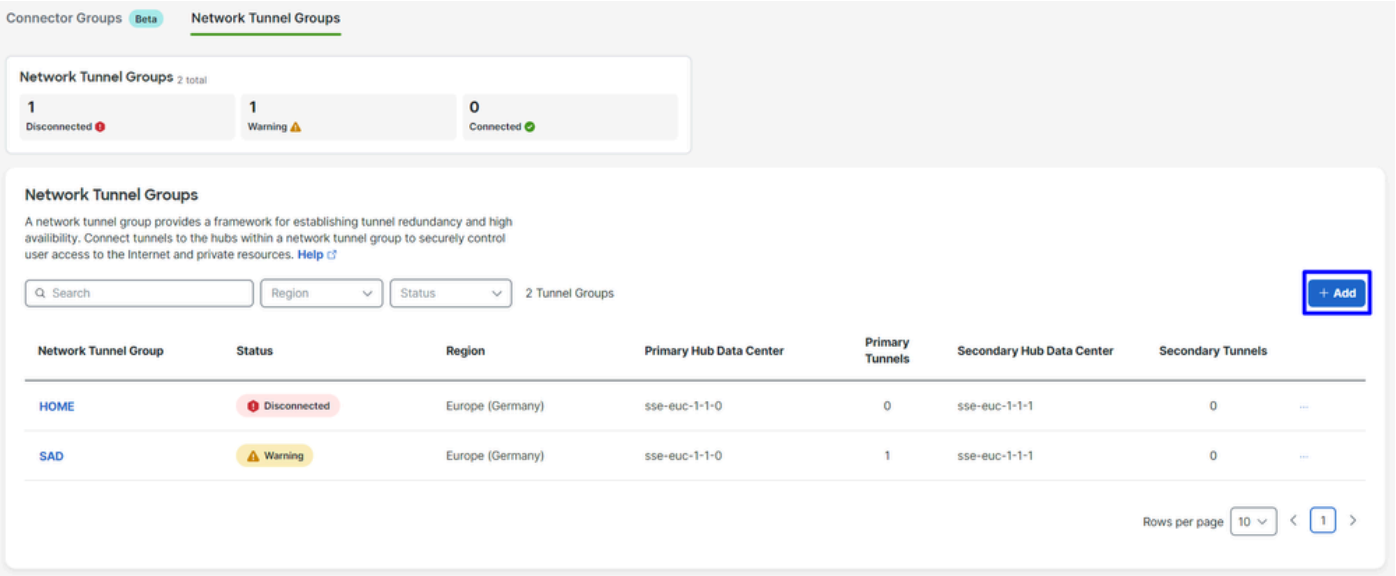
보안 액세스 - 기본 페이지

- 클릭 Connect > Network Connections.



보안 액세스 - 네트워크 연결

- 아래에서 Network Tunnel Groups 를 클릭합니다+ Add.



보안 액세스 - 네트워크 터널 그룹

- 구성Tunnel Group Name, Region 및 Device Type.
- 를 클릭합니다 **Next**.

General Settings

Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.

Tunnel Group Name

SophosFirewall

Region

Europe (Germany)

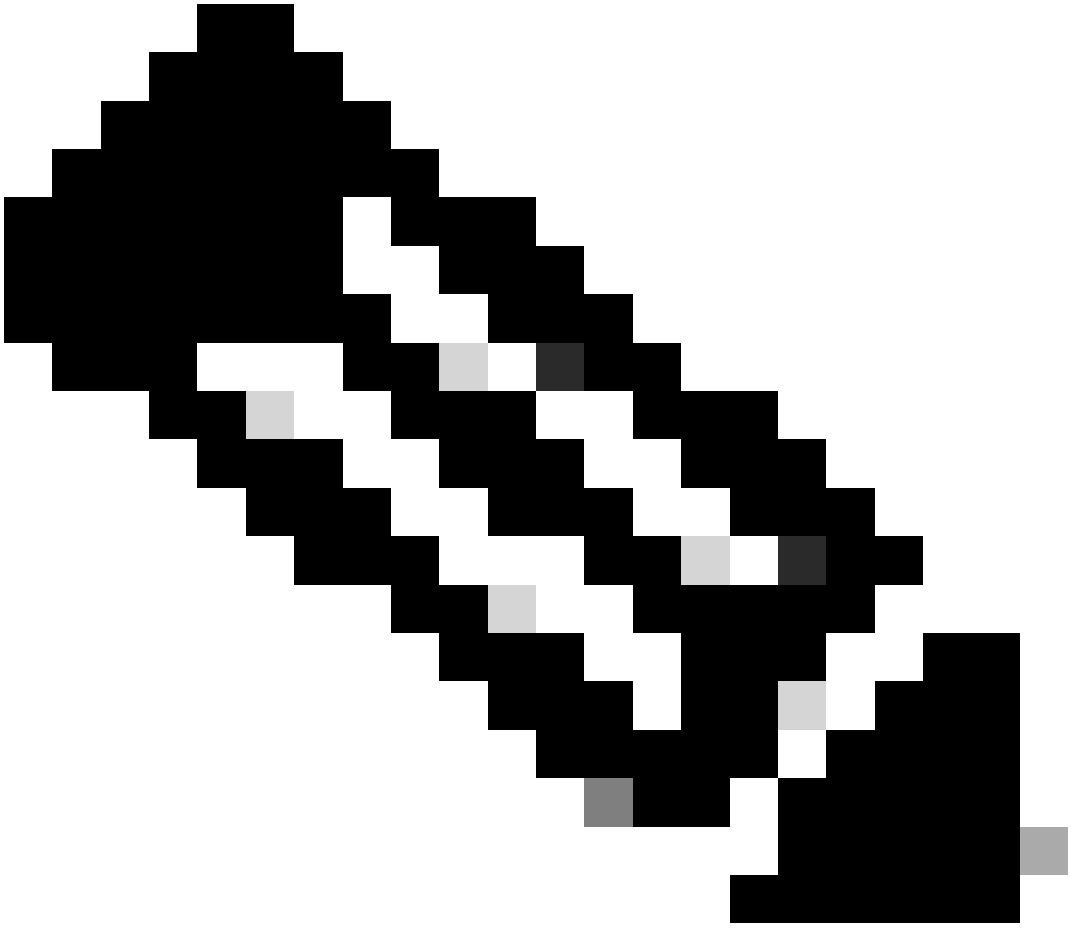
Device Type

Other

Cancel

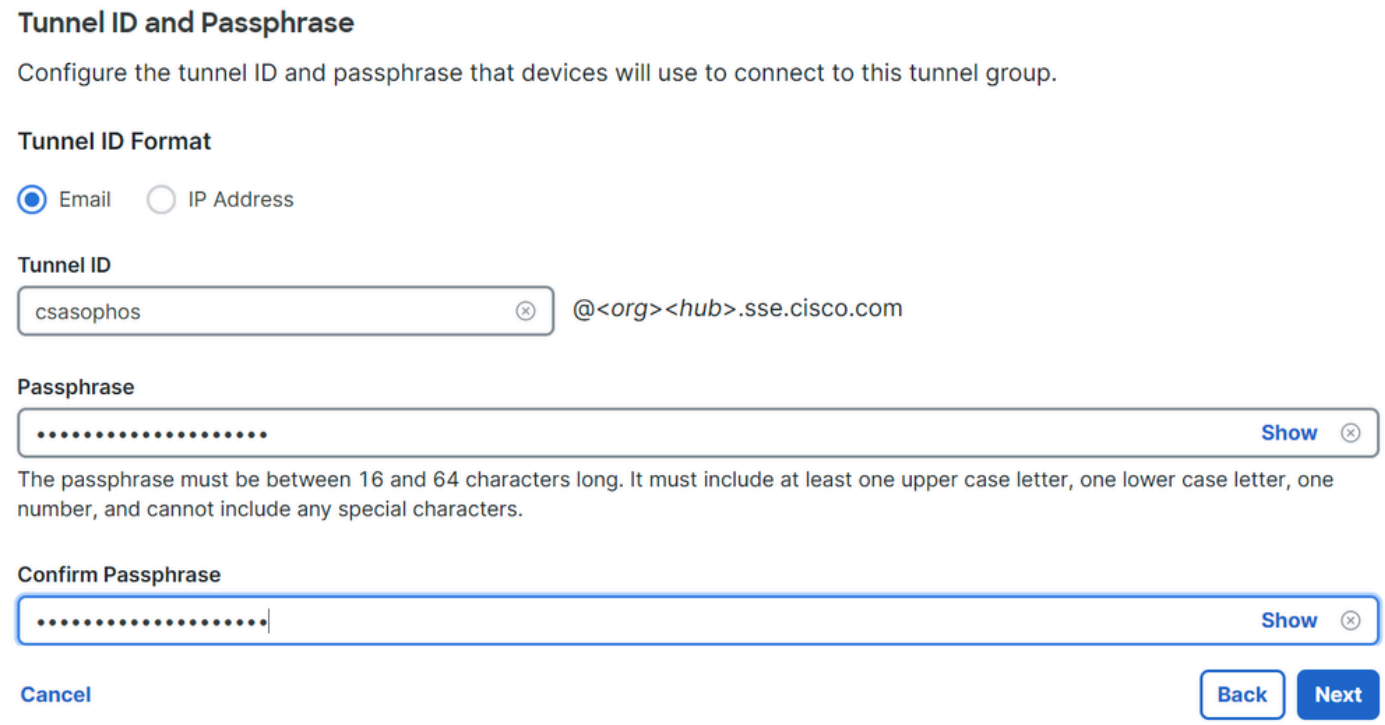
Next

보안 액세스 - 터널 그룹 - 일반 설정



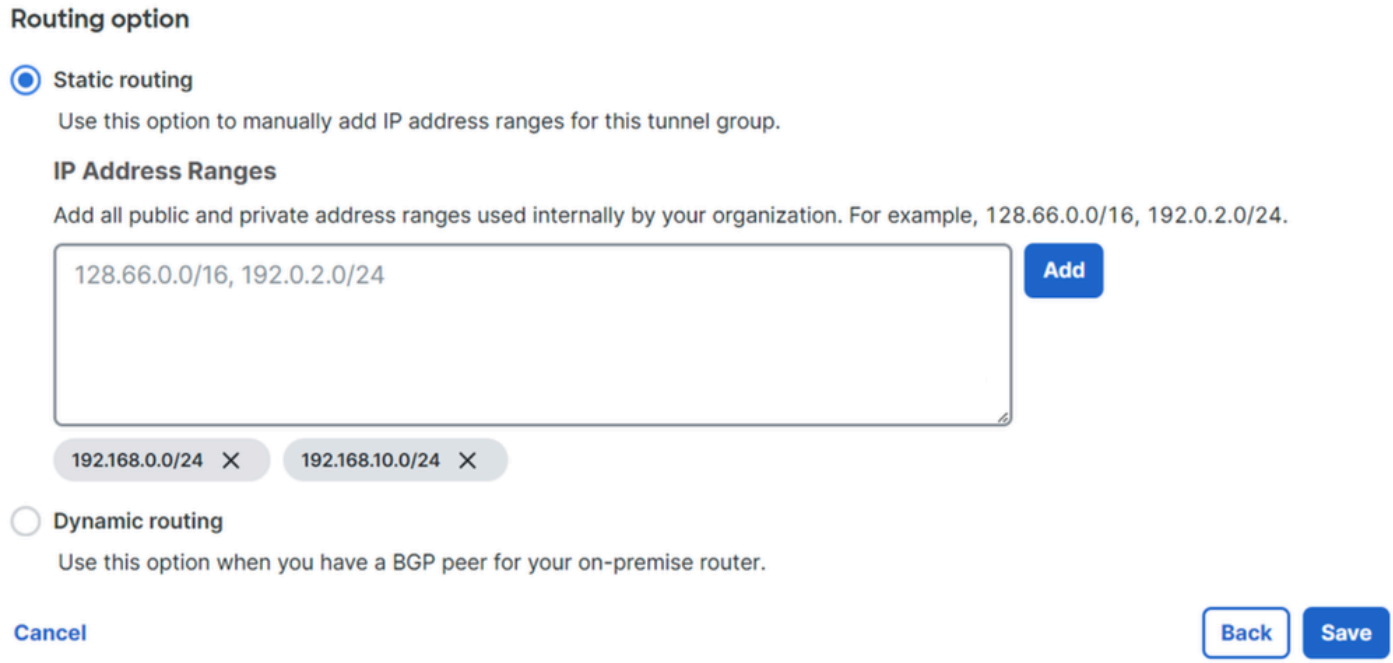
참고: 방화벽 위치에서 가장 가까운 지역을 선택합니다.

- 및 을Tunnel ID Format 구성합니다Passphrase.
- 를 Next 클릭합니다.



보안 액세스 - 터널 그룹 - 터널 *ID* 및 암호

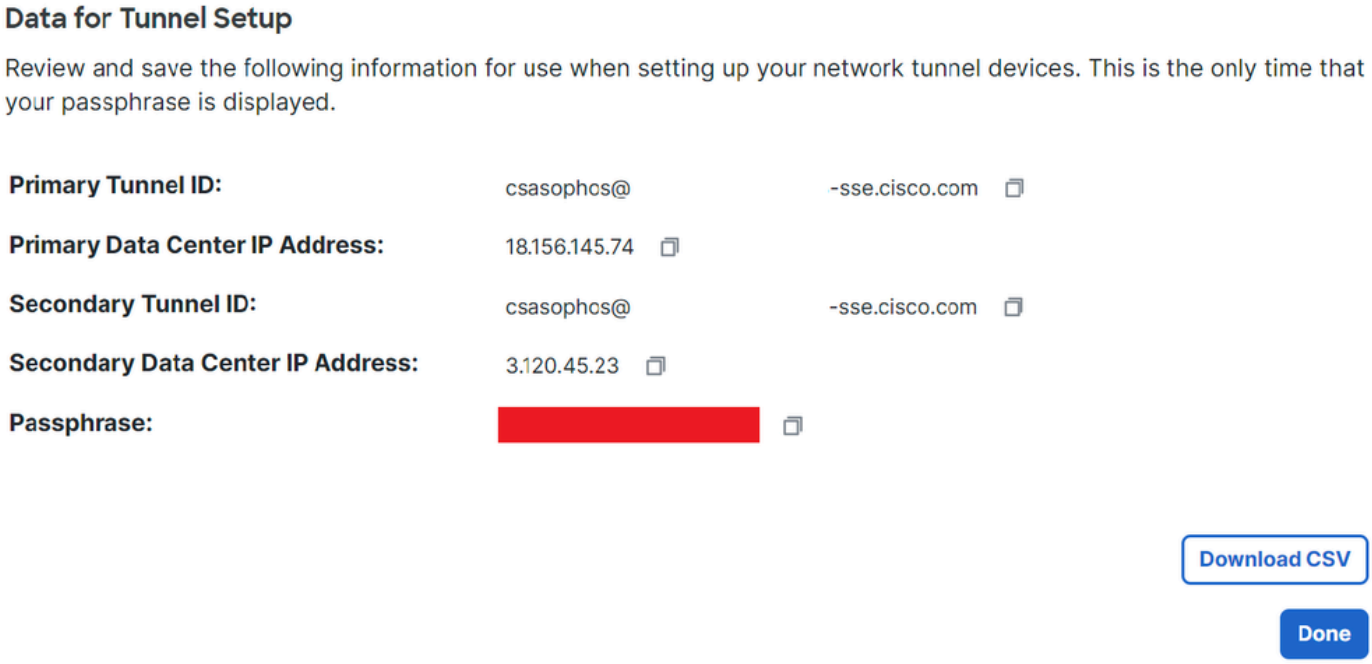
- 네트워크에서 구성했으며 Secure Access를 통해 트래픽을 전달하려는 IP 주소 범위 또는 호스트를 구성합니다.
- 를 **Save**클릭합니다.



보안 액세스 - 터널 그룹 - 라우팅 옵션

터널에 대한 정보**Save** 가 표시되면 다음 단계를 위해 해당 정보를 저장하십시오**Configure the tunnel on Sophos**.

터널 데이터



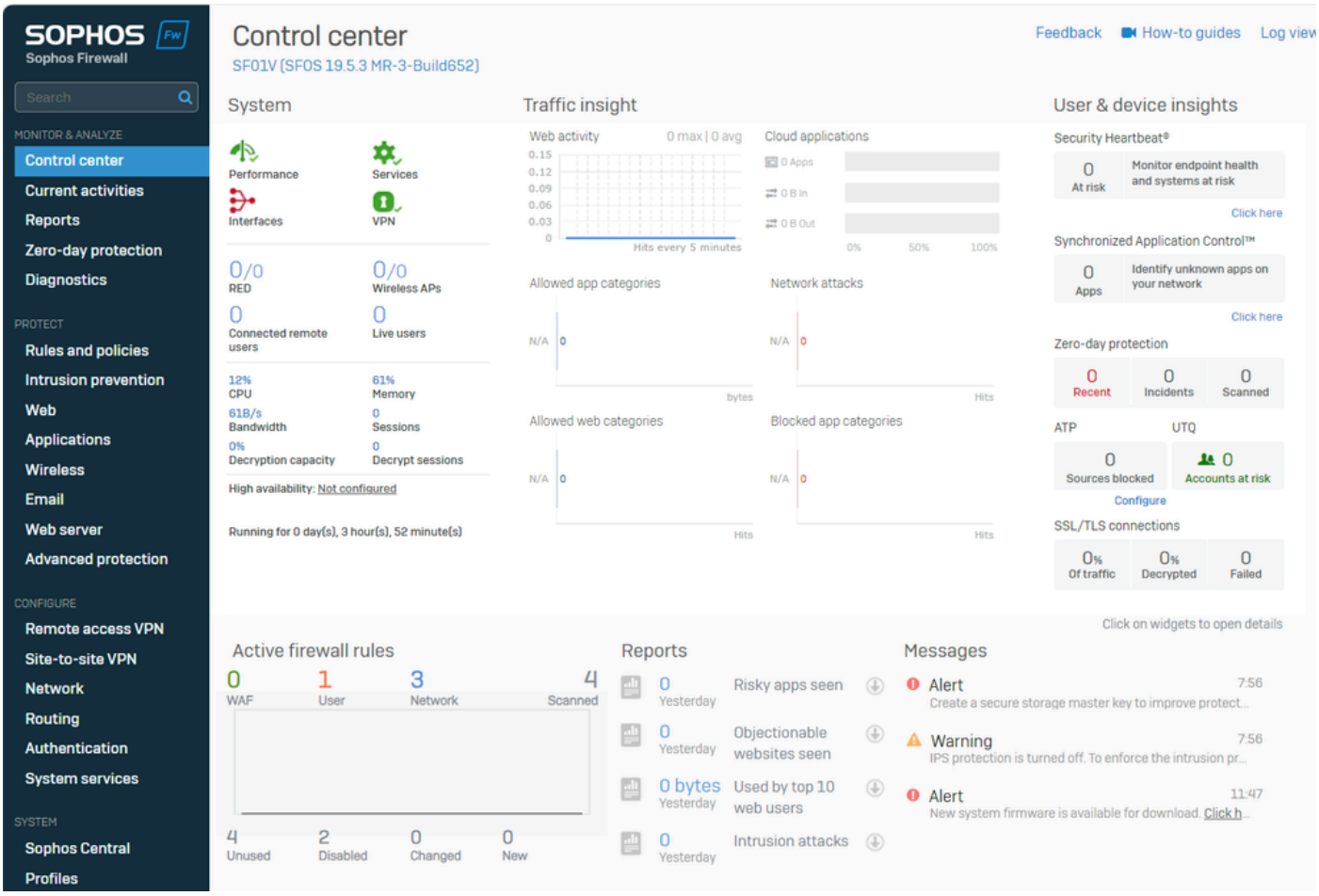
보안 액세스 - 터널 그룹 - 컨피그레이션 재개

Sophos에서 터널 구성

IPsec 프로필 구성

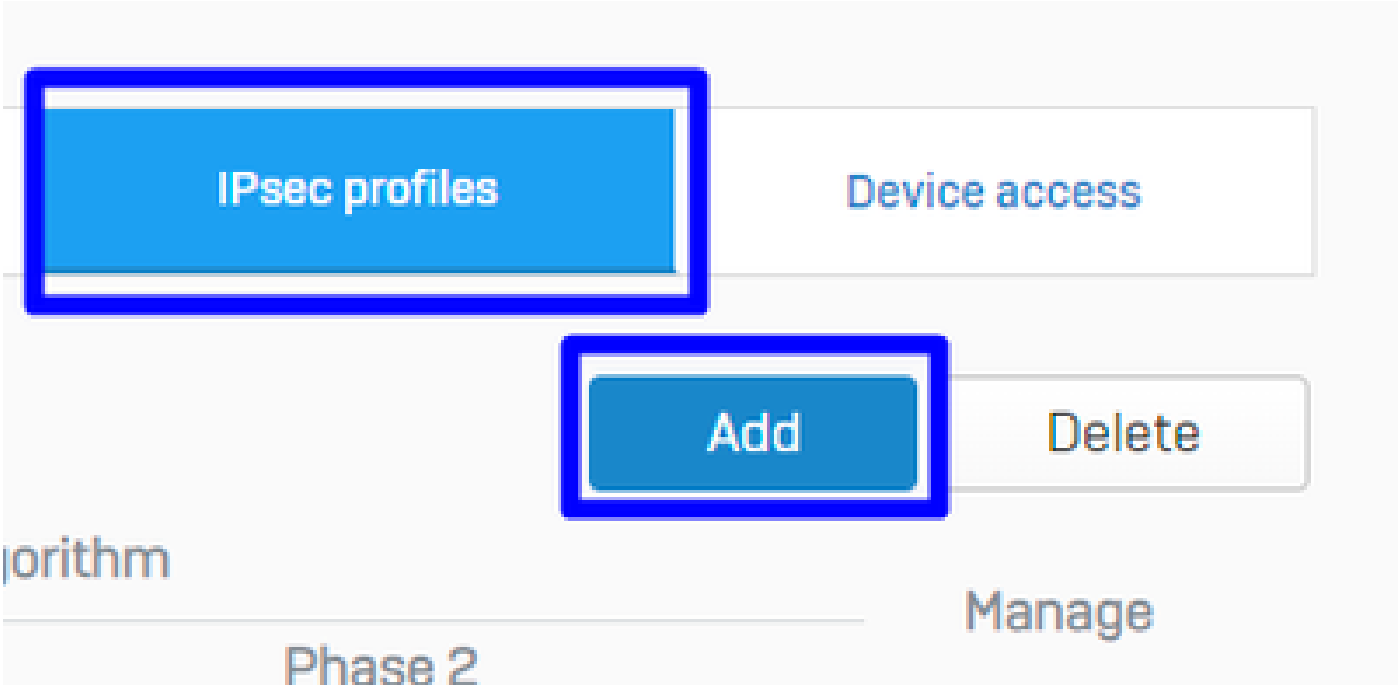
IPsec 프로필을 구성하려면 Sophos XG Firewall(Sophos XG 방화벽)로 이동합니다.

다음과 유사한 정보를 얻을 수 있습니다.



Sophos - 관리 패널

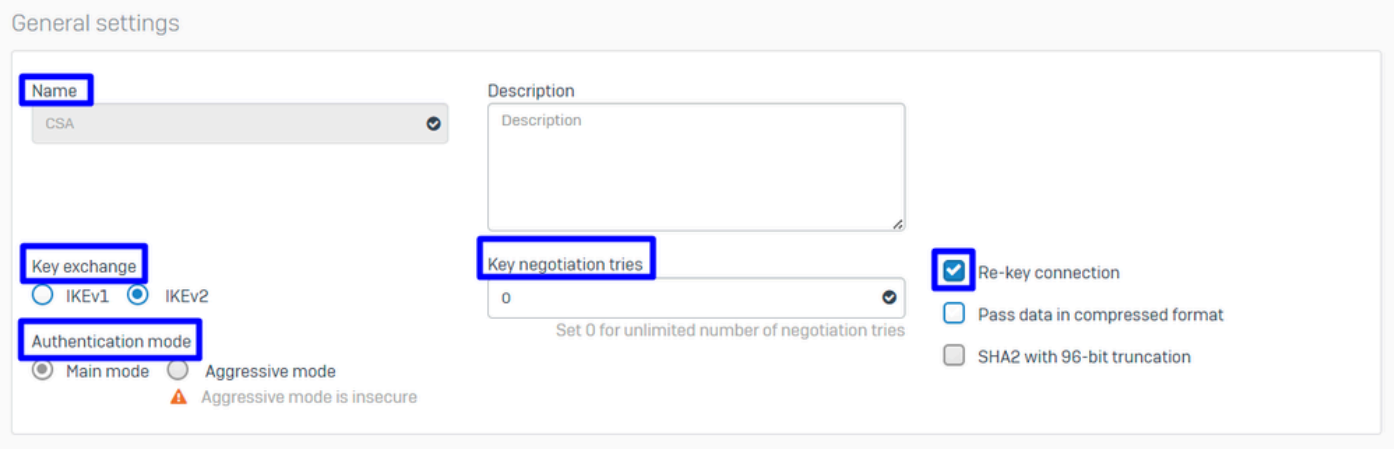
- 탐색 Profiles
- 클릭 **IPsec Profiles** 후 클릭Add



Sophos - IPsec 프로필

구성 **General Settings** 아래에서:

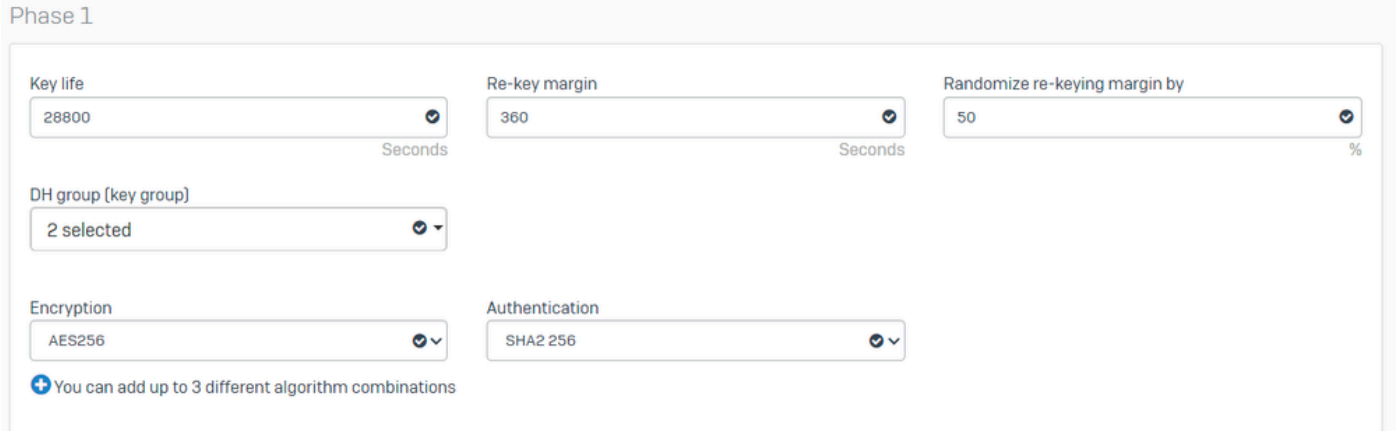
- **Name**: Cisco 보안 액세스 정책에 대한 참조 이름입니다.
- **Key Exchange**: IKEv2
- **Authentication Mode**:기본 모드
- **Key Negotiation Tries**:0
- **Re-Key connection**: 옵션을 선택합니다.



Sophos - IPsec 프로필 - 일반 설정

구성 **Phase 1** 아래에서:

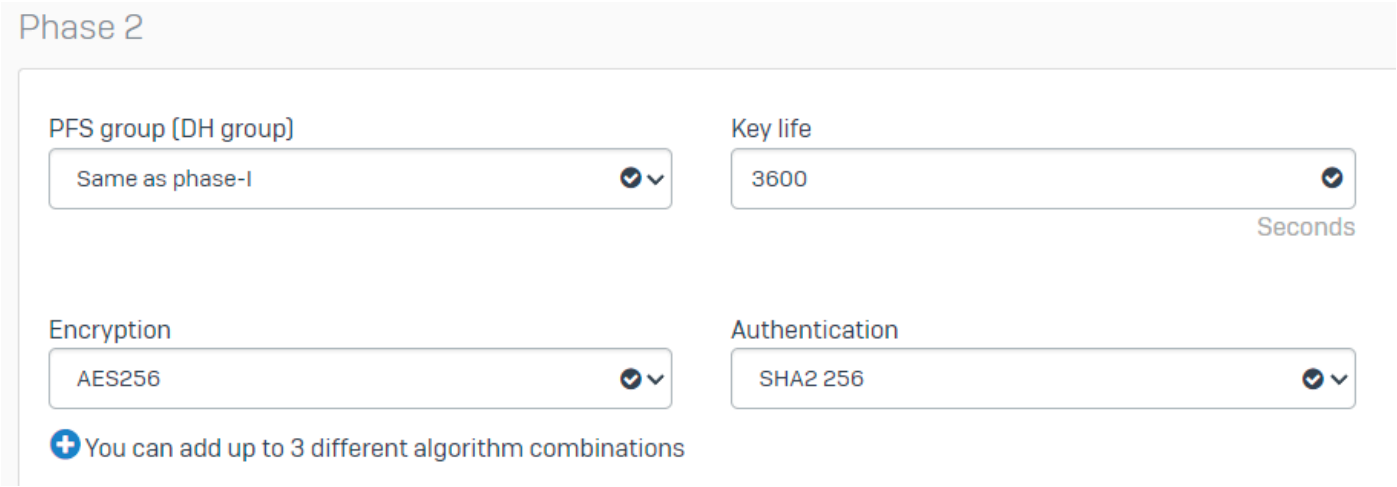
- **Key Life**:28800
- **DH group(key group)**: 19 및 20 선택
- **Encryption**: AES256
- **Authentication**: SHA2 256
- Re-key margin: 360(기본값)
- **Randomize re-keying margin by**: 50(기본값)



Sophos - IPsec 프로필 - 1단계

구성 **Phase 2** 아래에서:

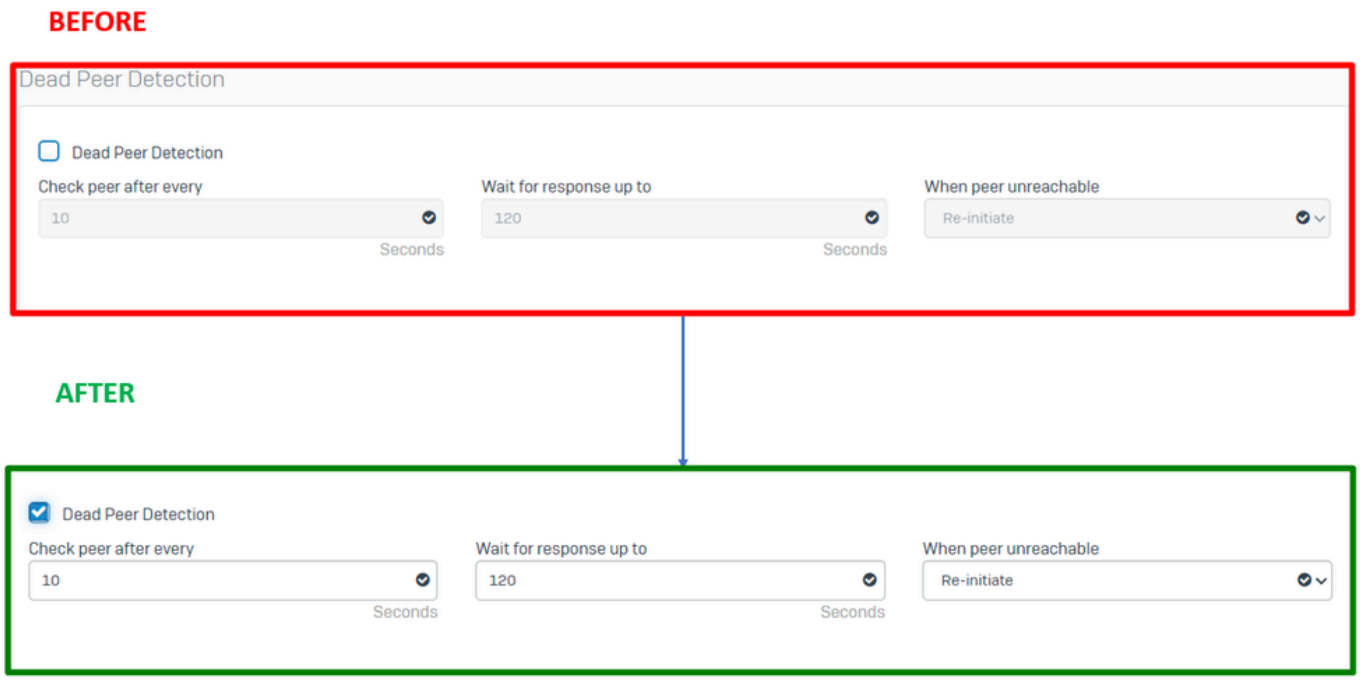
- PFS group (DH group): I단계와 동일
- **Key life**:3600
- **Encryption**: AES 256
- Authentication: SHA2 256



Sophos - IPsec 프로필 - 2단계

구성 **Dead Peer Detection** 아래에서:

- **Dead Peer Detection**: 옵션을 선택합니다.
- **Check peer after every**:10
- **Wait for response up to**: 120(기본값)
- **When peer unreachable**: 다시 시작(기본값)

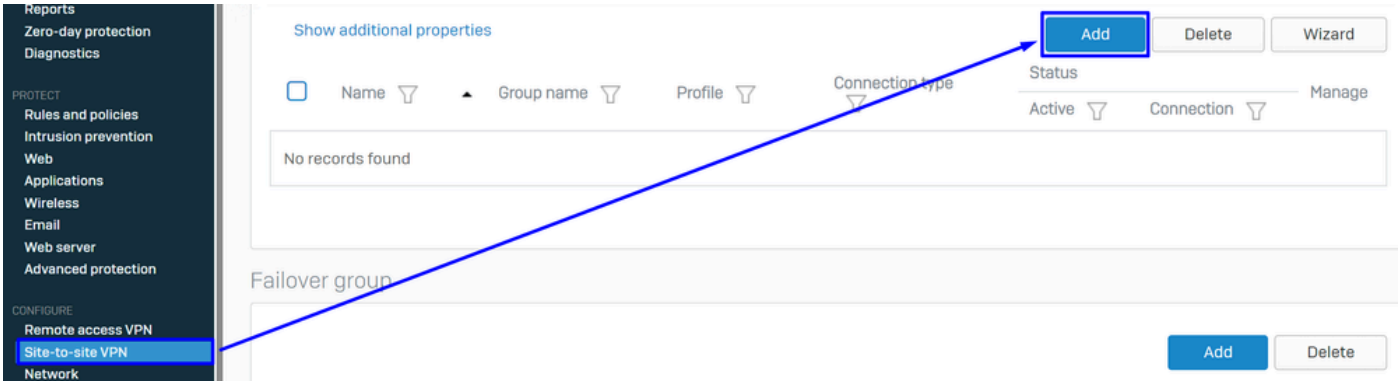


Sophos - IPsec 프로필 - 데드 피어 감지

그런 다음 을 **Save** and proceed with the next step, Configure Site-to-site VPN클릭합니다.

Site-to-Site VPN 구성

VPN의 컨피그레이션을 시작하려면 을 클릭한 다음 **Site-to-site VPN** 을 **Add**클릭합니다.

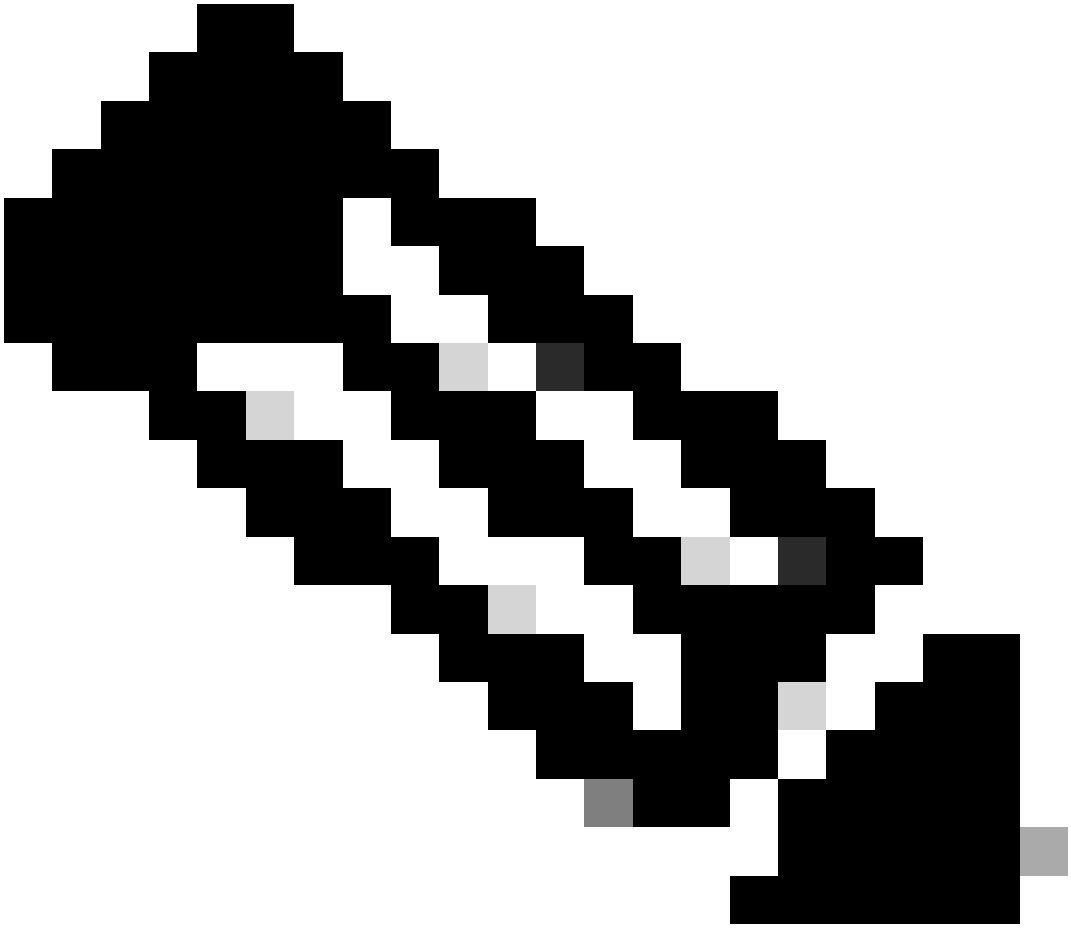


Sophos - 사이트 간 VPN

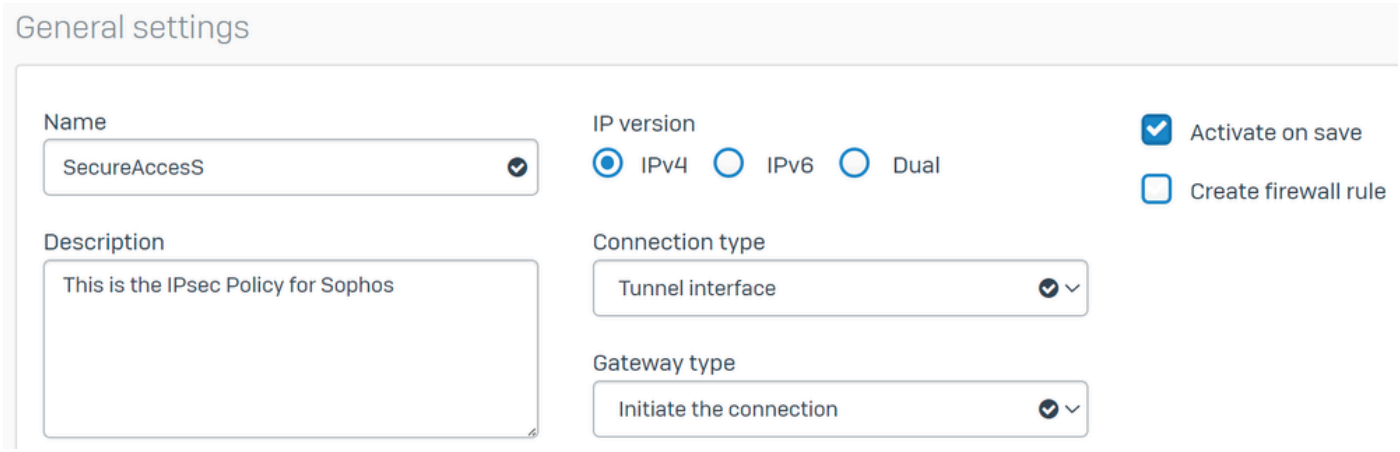
구성 **General Settings** 아래에서:

- **Name**: Cisco Secure Access IPsec 정책에 대한 참조 이름입니다.
- IP version: IPv4
- Connection type: 터널 인터페이스
- Gateway type: 연결 시작

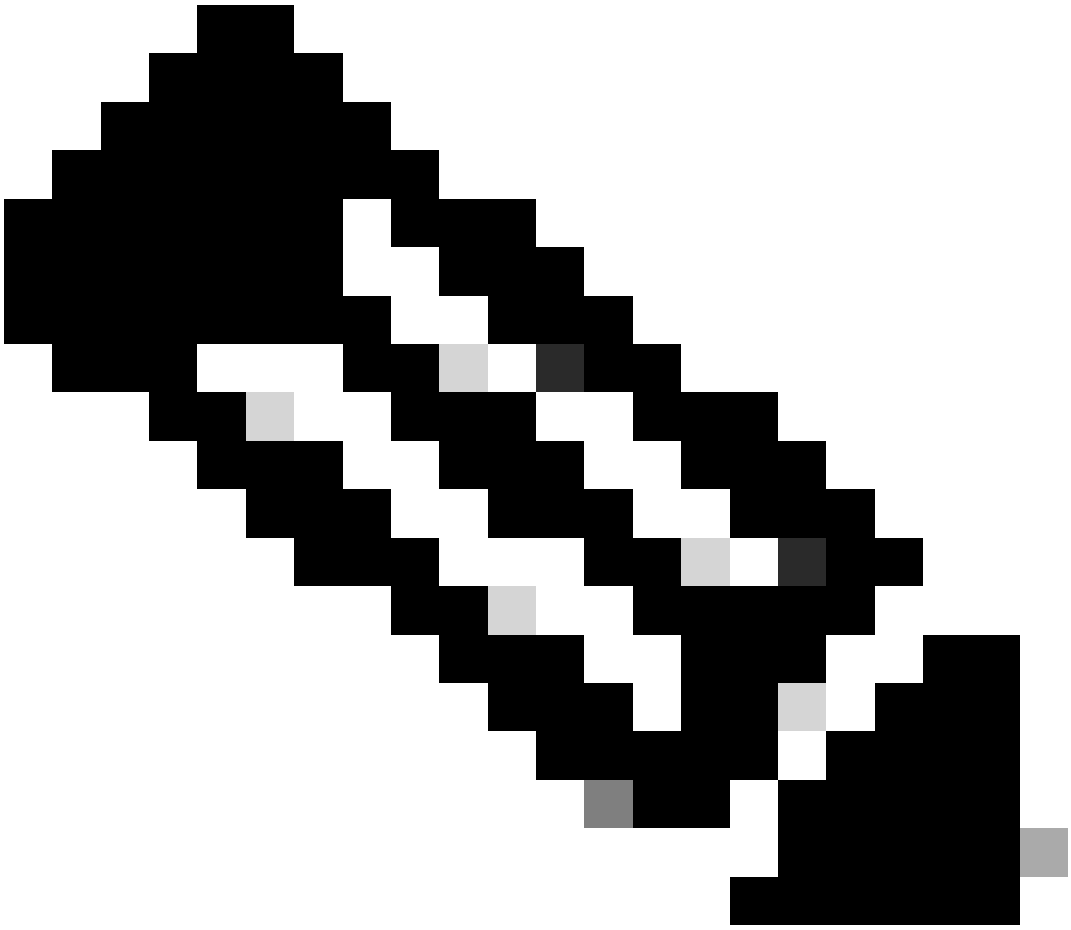
- Active on save: 옵션을 선택합니다.



참고: 이 옵션은 **Active on save** 사용자가 사이트 간 VPN을 구성한 후 VPN을 자동으로 활성화합니다.



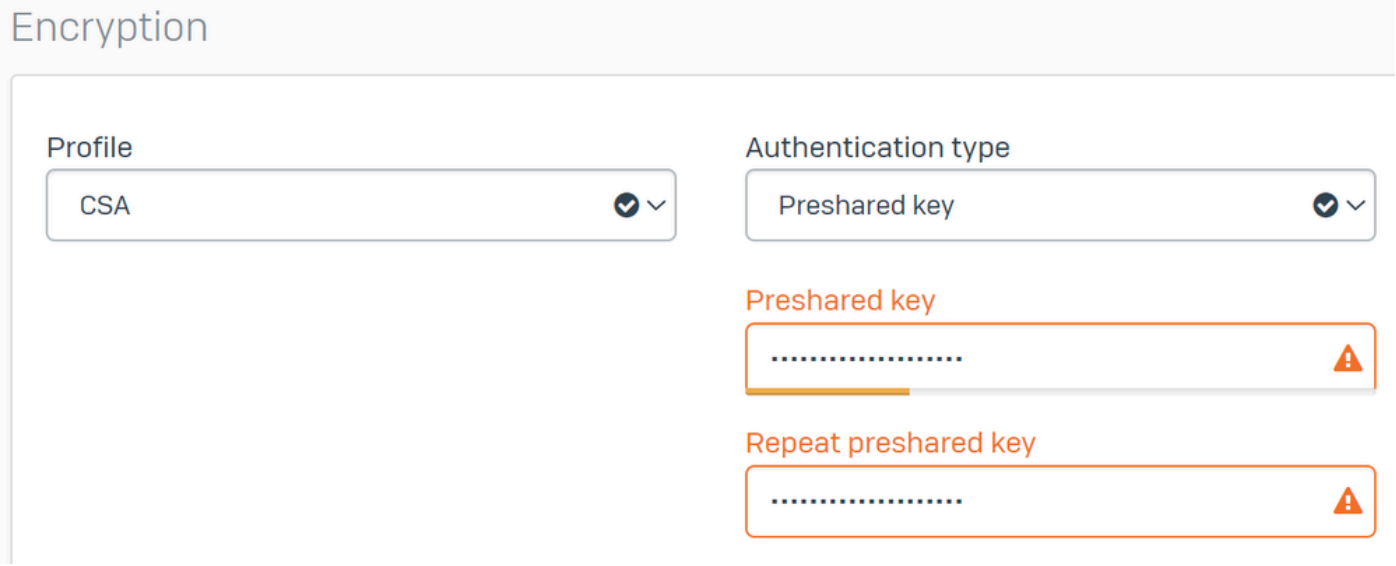
Sophos - Site-to-Site VPN - 일반 설정



참고: 터널 인터페이스 옵션은 XFRM이라는 이름으로 Sophos XG 방화벽에 대한 가상 터널 인터페이스를 생성합니다.

구성 **Encryption** 아래에서:

- **Profile**: 단계에서 생성한 프로파일입니다. **Configure IPsec Profile**
- **Authentication type**: 사전 공유 키
- **Preshared key**: 단계에서 구성하는 키입니다. Configure the Tunnel on Secure Access
- **Repeat preshared key**: **Preshared key**

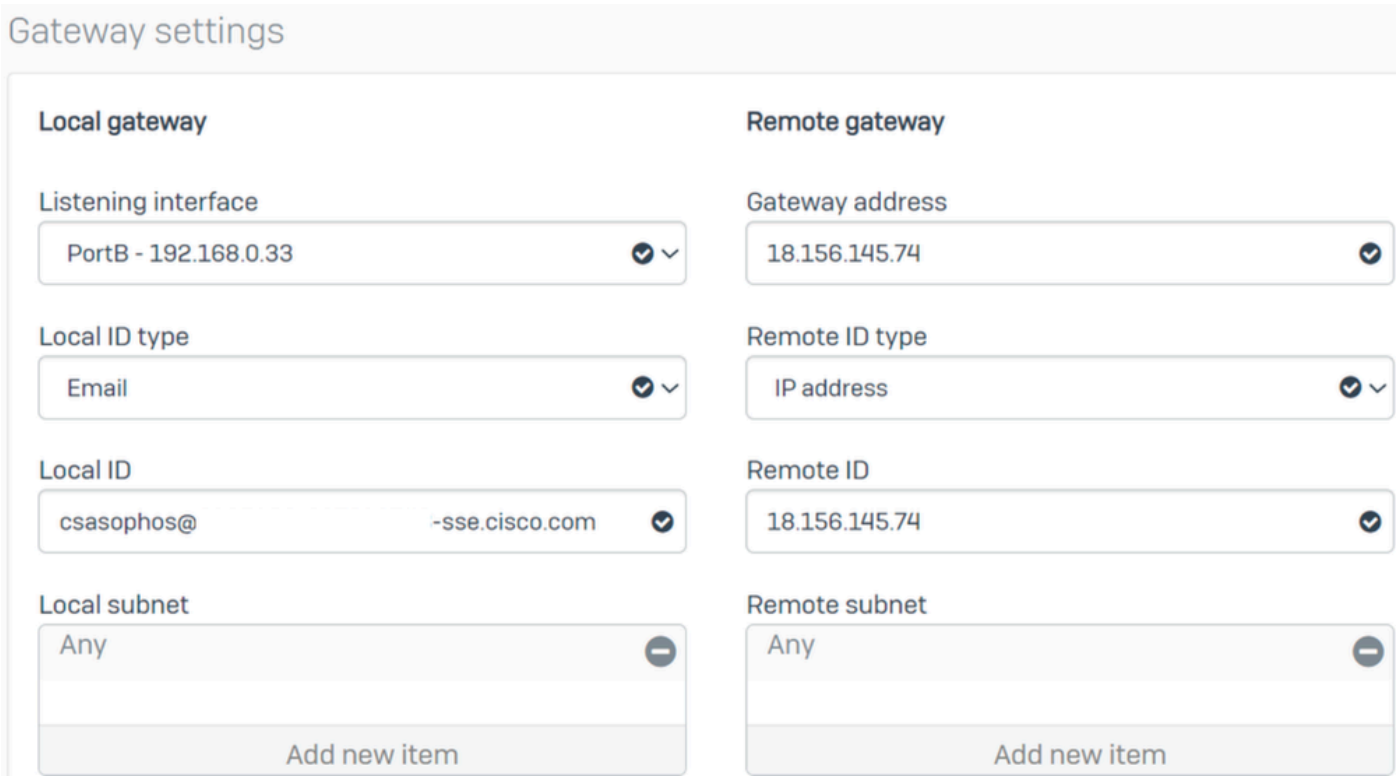


Sophos - Site-to-Site VPN - 암호화

configure **Gateway Settings** Local Gateway and optionsRemote Gateway 아래에서 이 테이블을 참조로 사용합니다.

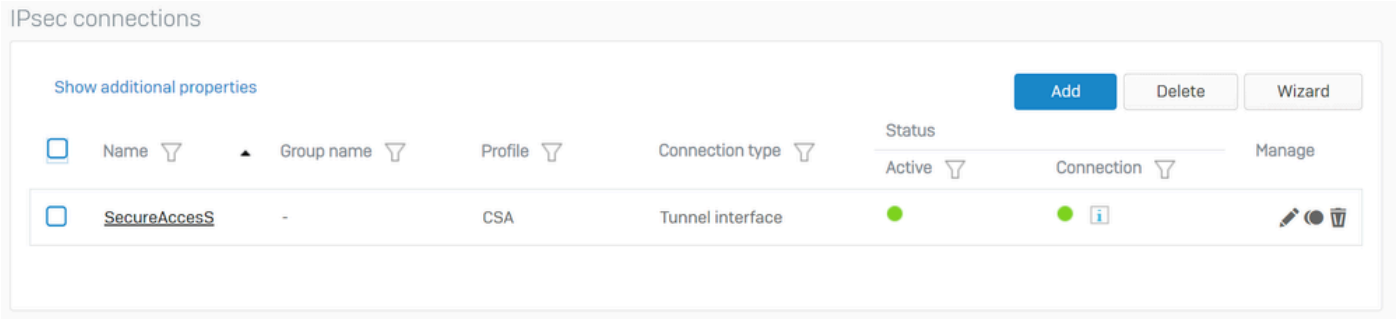
로컬 게이트웨이	원격 게이트웨이
수신 인터페이스 Wan-인터넷 인터페이스	게이트웨이 주소 단계에서 생성된 퍼블릭 IP, **Tunnel Data**
로컬 ID 유형 Email	원격 ID 유형 IP 주소

로컬 ID 이 단계에서 생성된 이메일, Tunnel Data	원격 ID 단계에서 생성된 퍼블릭 IP, Tunnel Data
로컬 서브넷 모두	원격 서브넷 모두

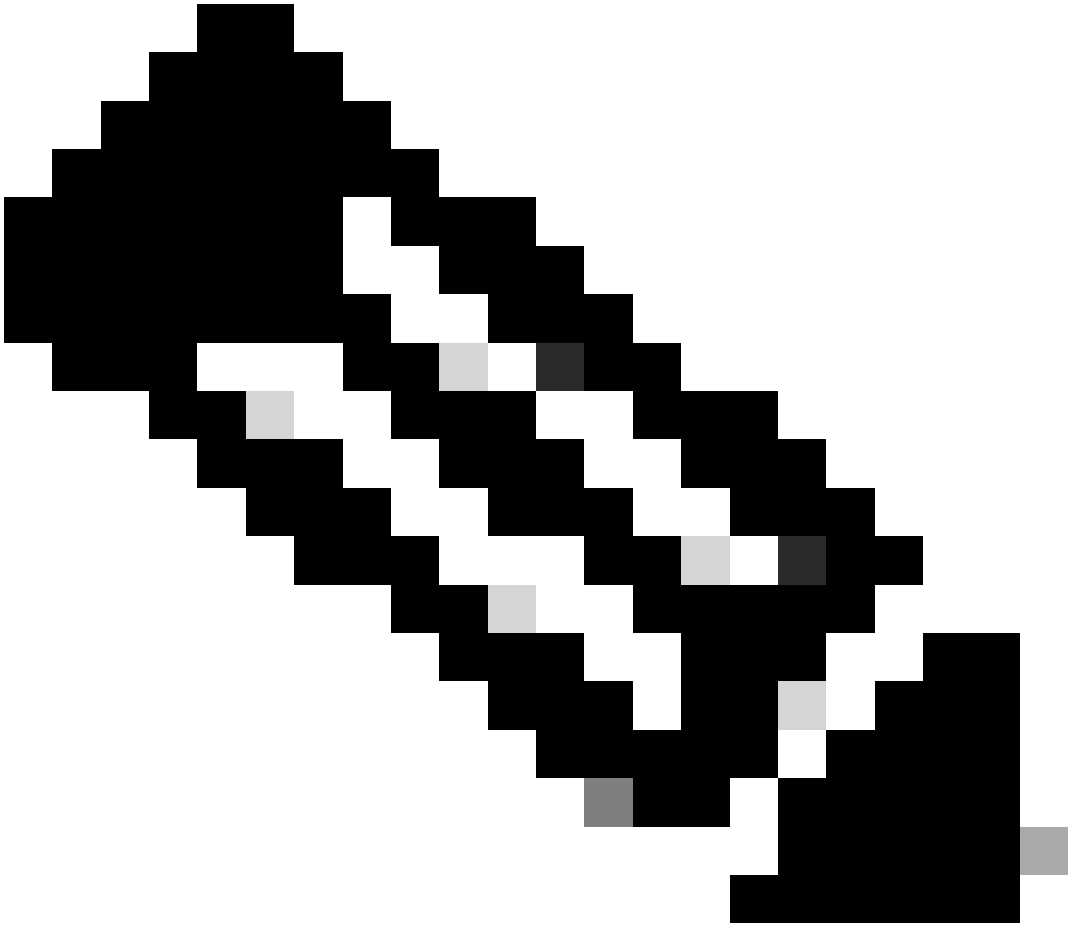


Sophos - Site-to-Site VPN - 게이트웨이 설정

그런 다음 클릭하면 **Save**터널이 생성된 것을 확인할 수 있습니다.

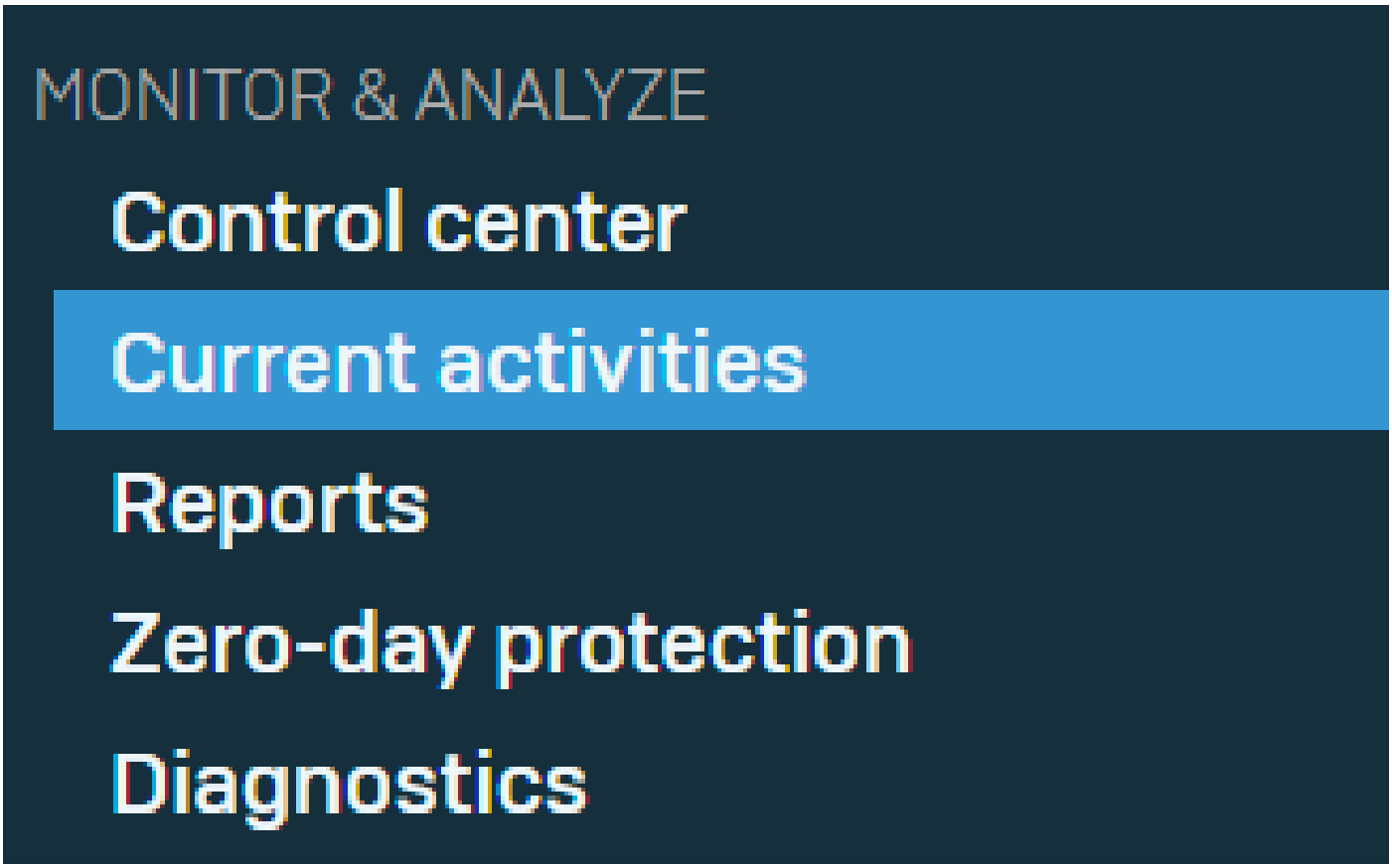


Sophos - Site-to-Site VPN - IPsec 연결

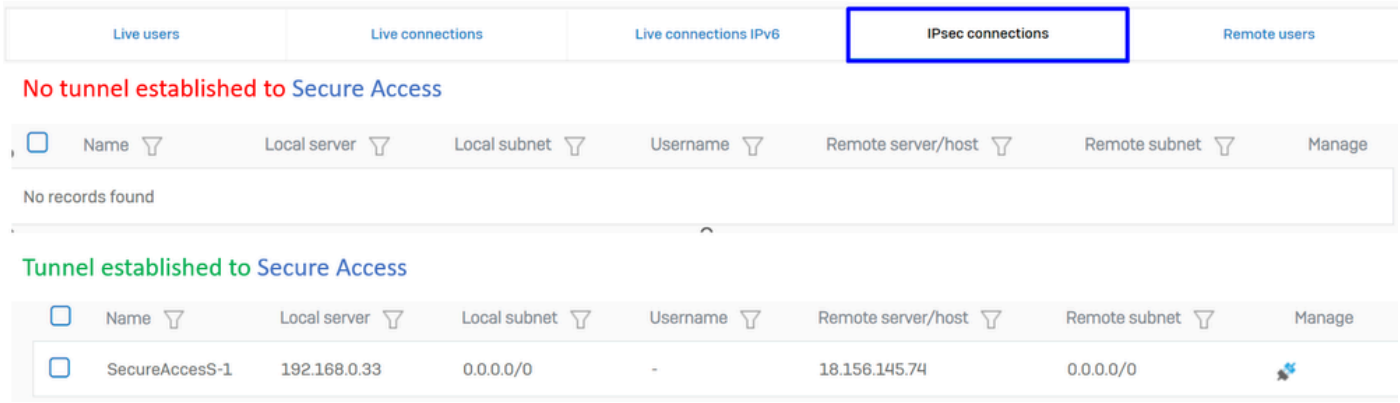


참고: 마지막 이미지에서 터널이 올바르게 활성화되었는지 확인하려면 **Connection** 상태(녹색인 경우)를 확인할 수 있습니다. 녹색이 아닌 경우 터널이 연결됨 터널이 연결되지 않았습니다.

터널이 설정되었는지 확인하려면 로 **Current Activities** > **IPsec Connections**이동합니다.



Sophos - 모니터링 및 분석 - *IPsec*



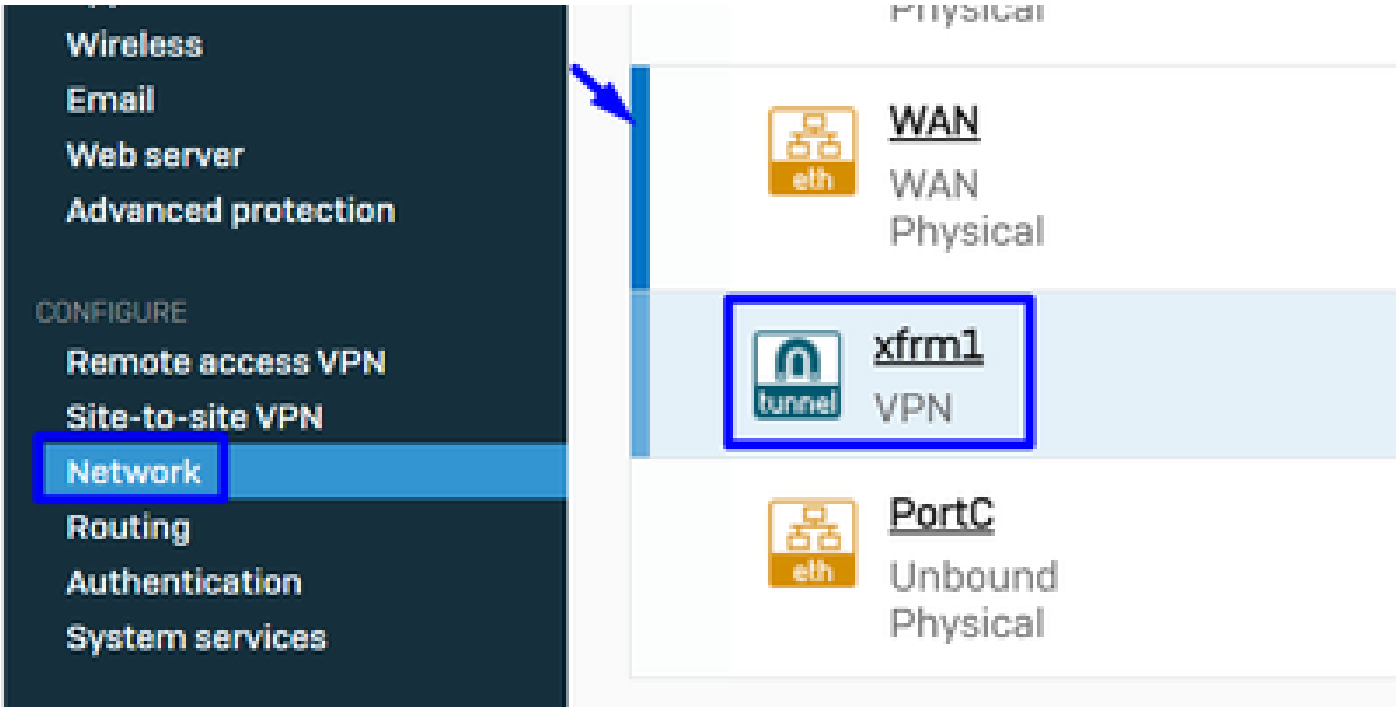
Sophos - 모니터링 및 분석 - 전후 *IPsec*

그런 다음 단계를 계속 진행할 수 있습니다 **Configure Tunnel Interface Gateway**.

터널 인터페이스 구성

이름으로 가상 터널 **Network** 인터페이스를 편집하려면 VPN에 구성된 인터페이스로 이동하여WAN 확인합니다xfrm.

- 인터페이스를 **xfrm** 클릭합니다.



Sophos - 네트워크 - 터널 인터페이스

- 네트워크에서 라우팅 불가 IP로 인터페이스를 구성합니다. 예를 들어 라우팅 불가 공간의 IP인 169.254.x.x/30을 사용할 수 있습니다. 이 예에서는 169.254.0.1/30을 사용합니다

Sophos - 네트워크 - 터널 인터페이스 - 컨피그레이션

게이트웨이 구성

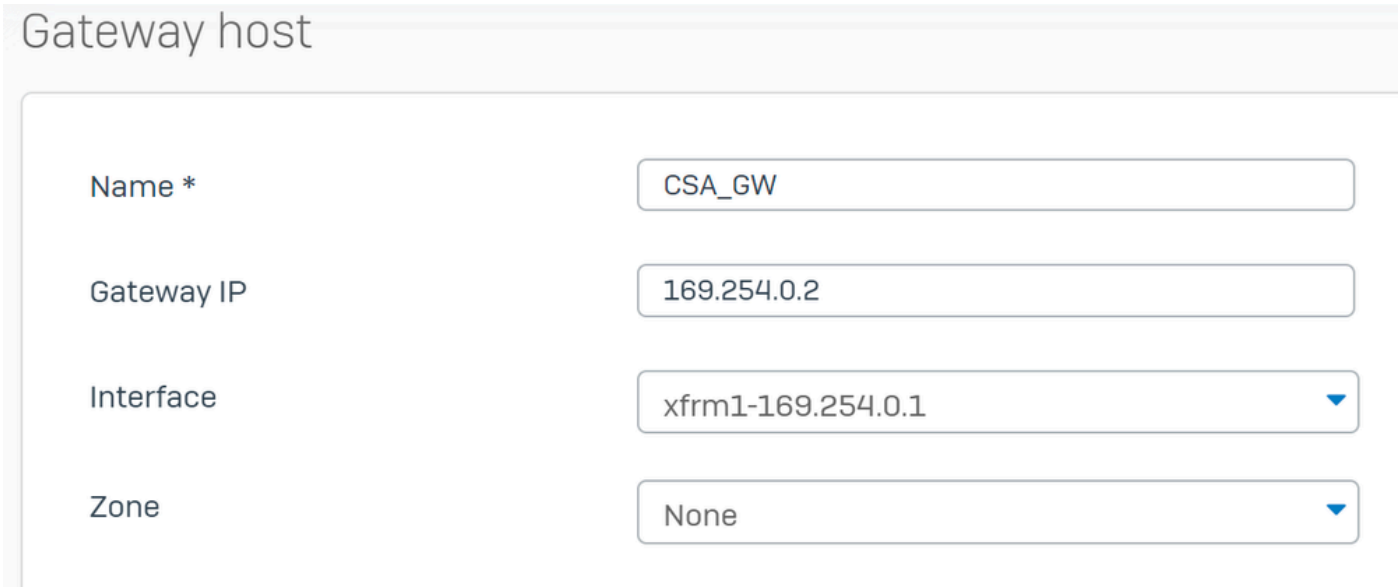
가상 인터페이스(xfrm)에 대한 게이트웨이를 구성하려면

- 탐색 Routing > Gateways
- 클릭 Add

Sophos - 라우팅 - 게이트웨이

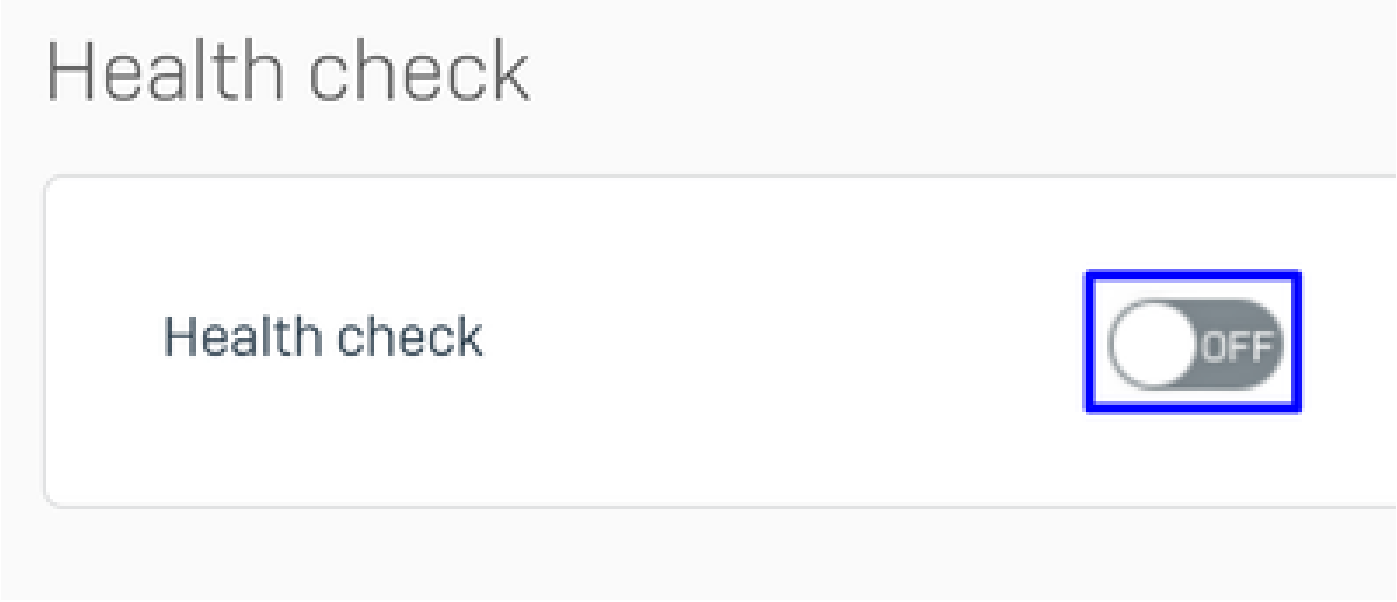
구성 **Gateway host** 아래에서:

- **Name**: VPN에 대해 생성된 가상 인터페이스를 참조하는 이름
- **Gateway IP**: 우리의 경우 169.254.0.2는 이미 단계에서 할당한 네트워크 169.254.0.1/30의 IP입니다. Configure Tunnel Interface
- Interface: VPN 가상 인터페이스
- **Zone**: 없음(기본값)



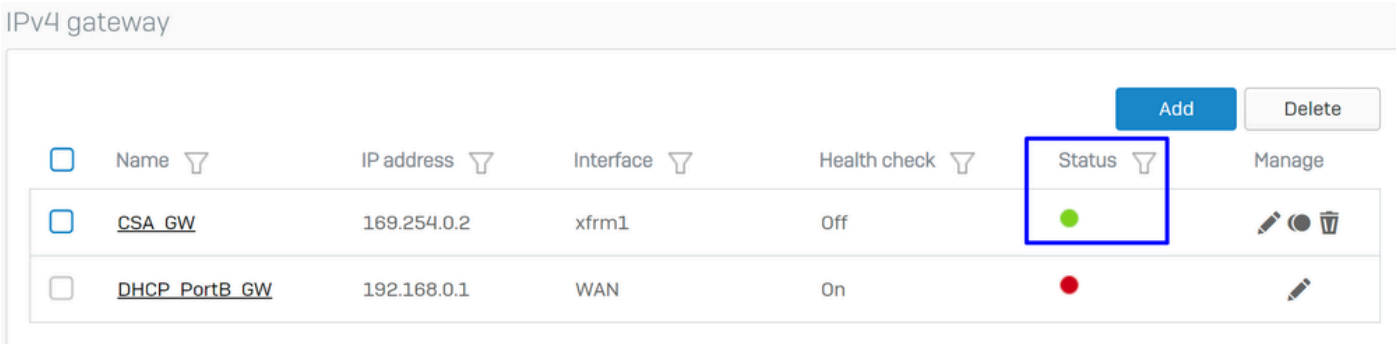
Sophos - 라우팅 - 게이트웨이 - 게이트웨이 호스트

- 비활성화 **Health check** 상태에서 확인
- 클릭 **Save**



Sophos - 라우팅 - 게이트웨이 - 상태 확인

컨피그레이션을 저장한 후 게이트웨이의 상태를 관찰할 수 있습니다.



Sophos - 라우팅 - 게이트웨이 - 상태

SD-WAN 경로 구성

컨피그레이션 프로세스를 완료하려면 트래픽을 Secure Access로 전달할 수 있는 경로를 만들어야 합니다.

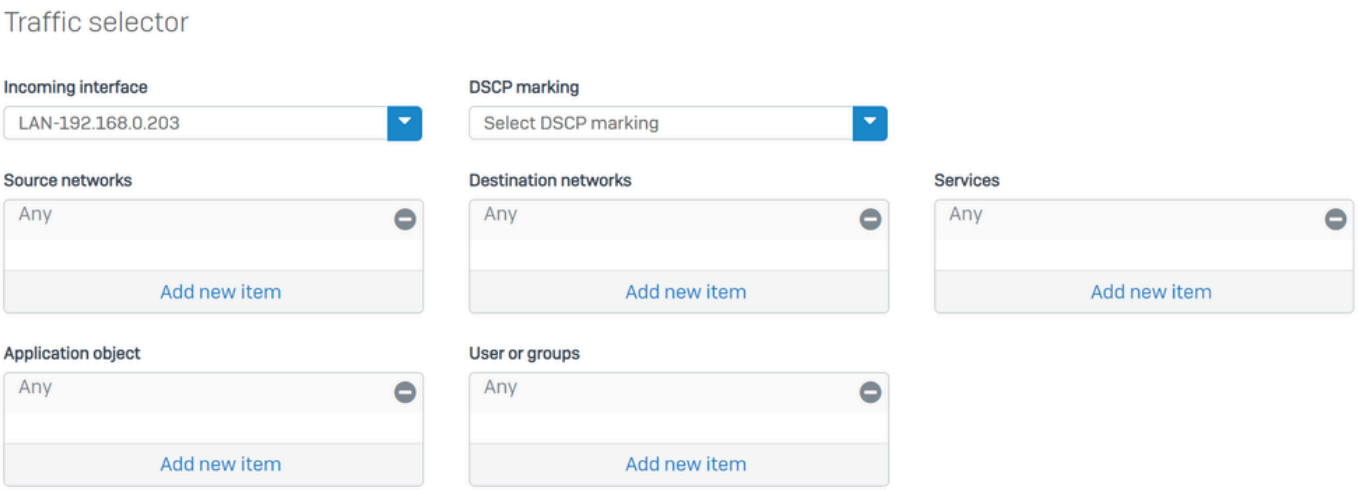
탐색 **Routing > SD-WAN routes.**

- 클릭 **Add**

Sophos - SD-Wan 경로

구성 **Traffic Selector** 아래에서:

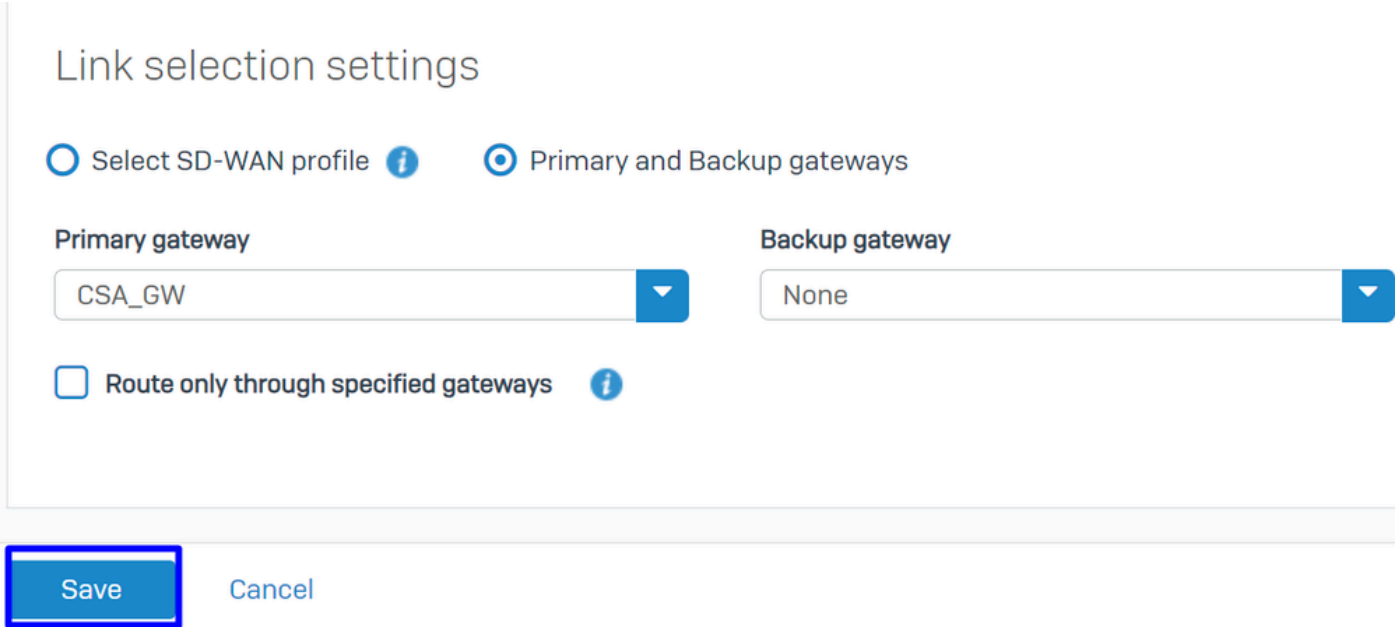
- Incoming interface: RA-VPN, ZTNA 또는 Clientless-ZTNA에서 액세스하는 사용자 또는 트래픽을 보낼 인터페이스를 선택합니다
- DSCP marking: 이 예제에 대한 내용이 없습니다.
- **Source networks**: 터널을 통해 라우팅할 주소를 선택합니다
- **Destination networks**: 모든 또는 대상을 지정할 수 있습니다.
- **Services**: 모두 또는 서비스를 지정할 수 있습니다.
- **Application object**: 객체가 구성된 경우 응용 프로그램입니다.
- User or groups: 트래픽을 Secure Access로 라우팅하기 위해 특정 사용자 그룹을 추가하려는 경우



Sophos - SD-Wan 경로 - 트래픽 선택기

게이트웨이 **Link selection settings** 구성 아래에서 다음을 수행합니다.

    - Primary and Backup gateways: 옵션을 선택합니다.
- **Primary gateway**: 단계에서 구성된 게이트웨이를 선택합니다. Configure the Gateways
- 클릭 **Save**



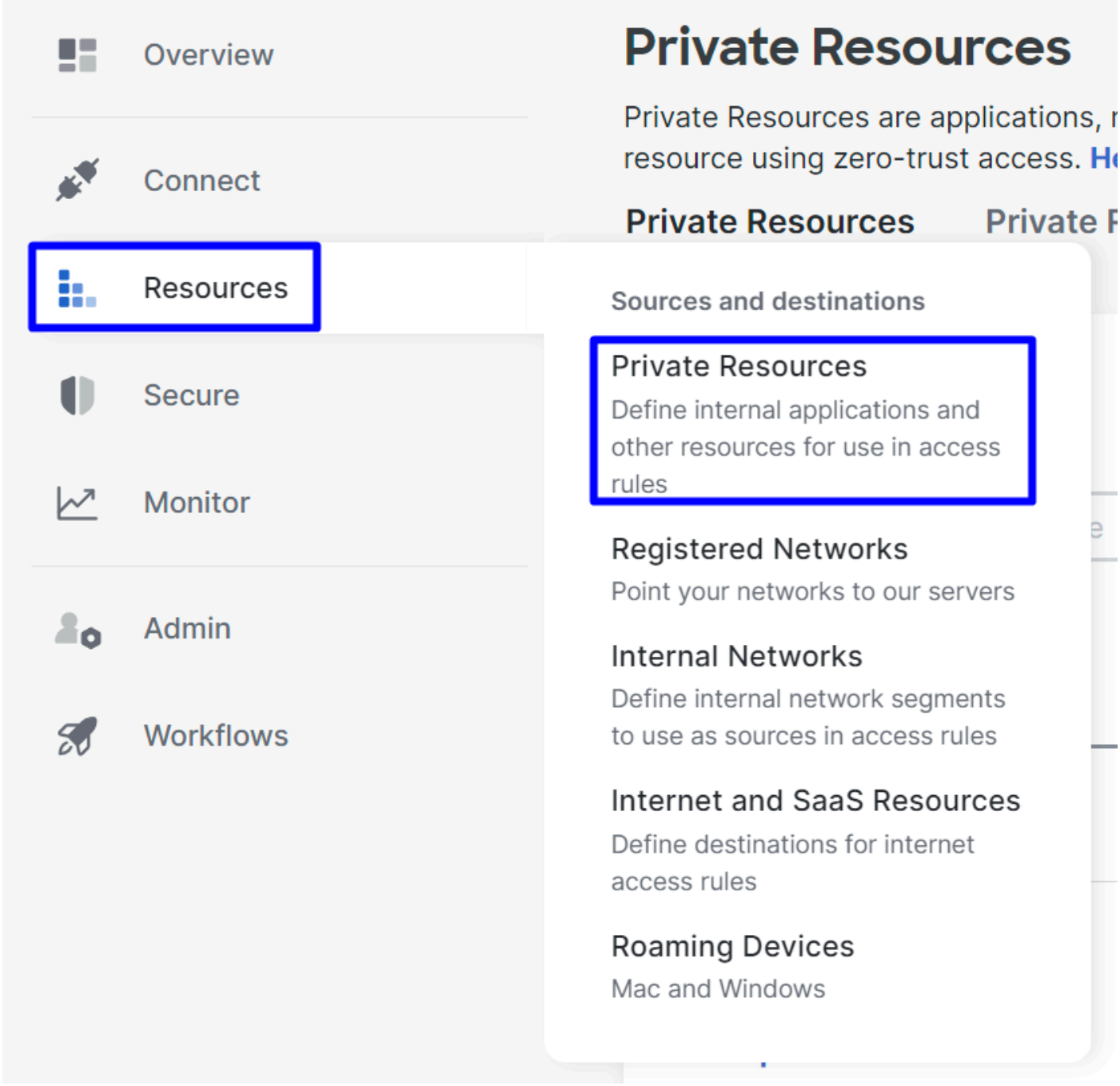
Sophos - SD-Wan 경로 - 트래픽 선택기 - 기본 및 백업 게이트웨이

Sophos XG 방화벽에서 컨피그레이션을 마무리한 후 다음 단계를 진행할 수 있습니다. **Configure Private App.**

프라이빗 앱 구성

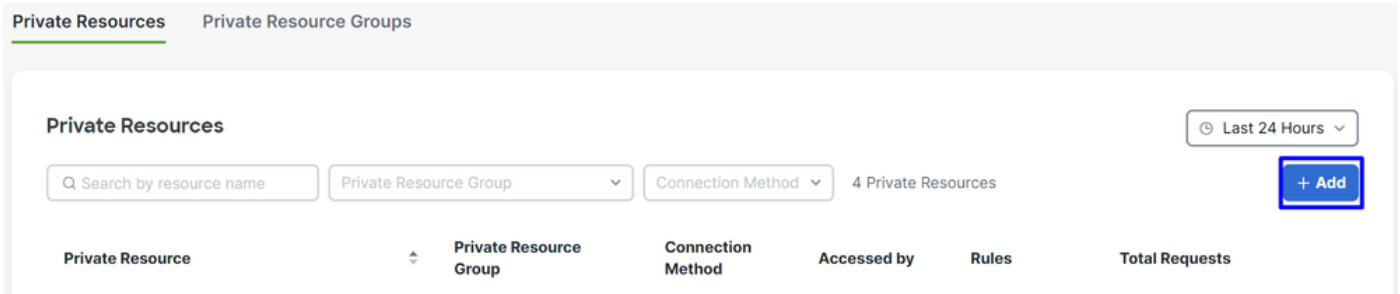
프라이빗 앱 액세스를 구성하려면 관리 포털에 로그인합니다.

- 탐색 **Resources** > **Private Resources**



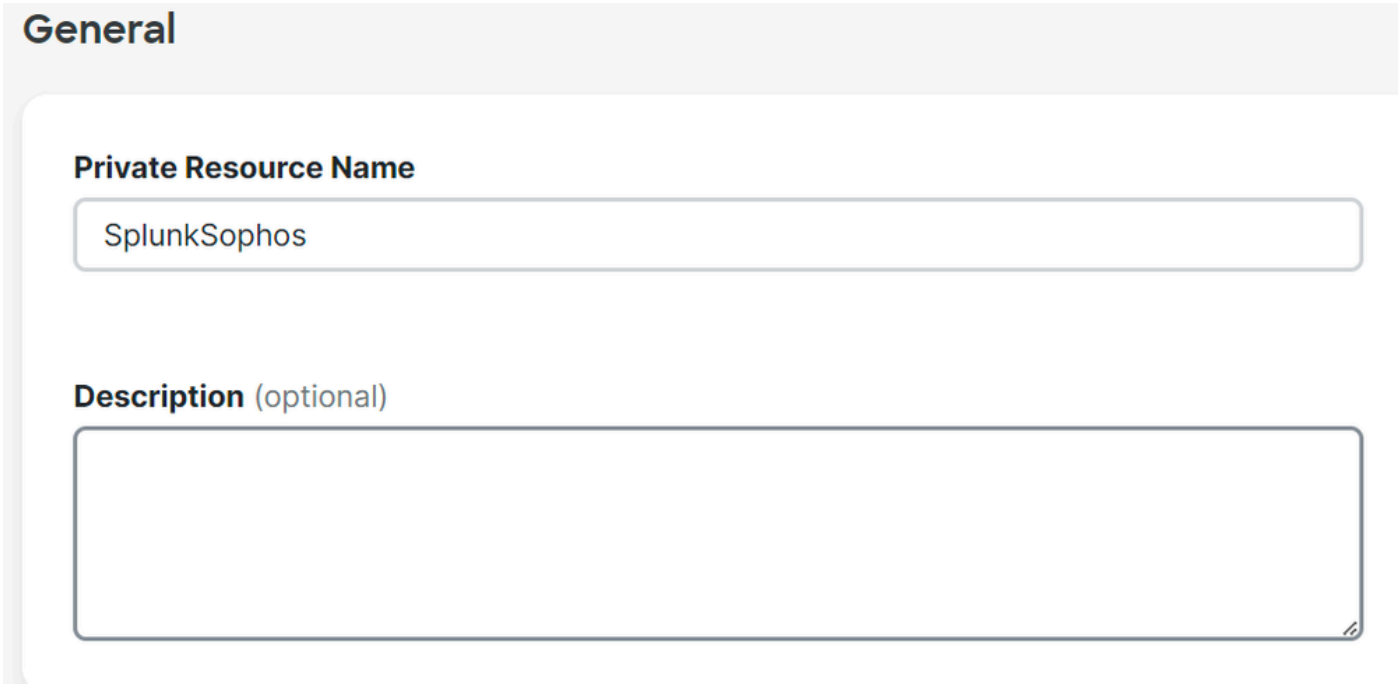
보안 액세스 - 프라이빗 리소스

- 클릭 + Add



보안 액세스 - 프라이빗 리소스 2

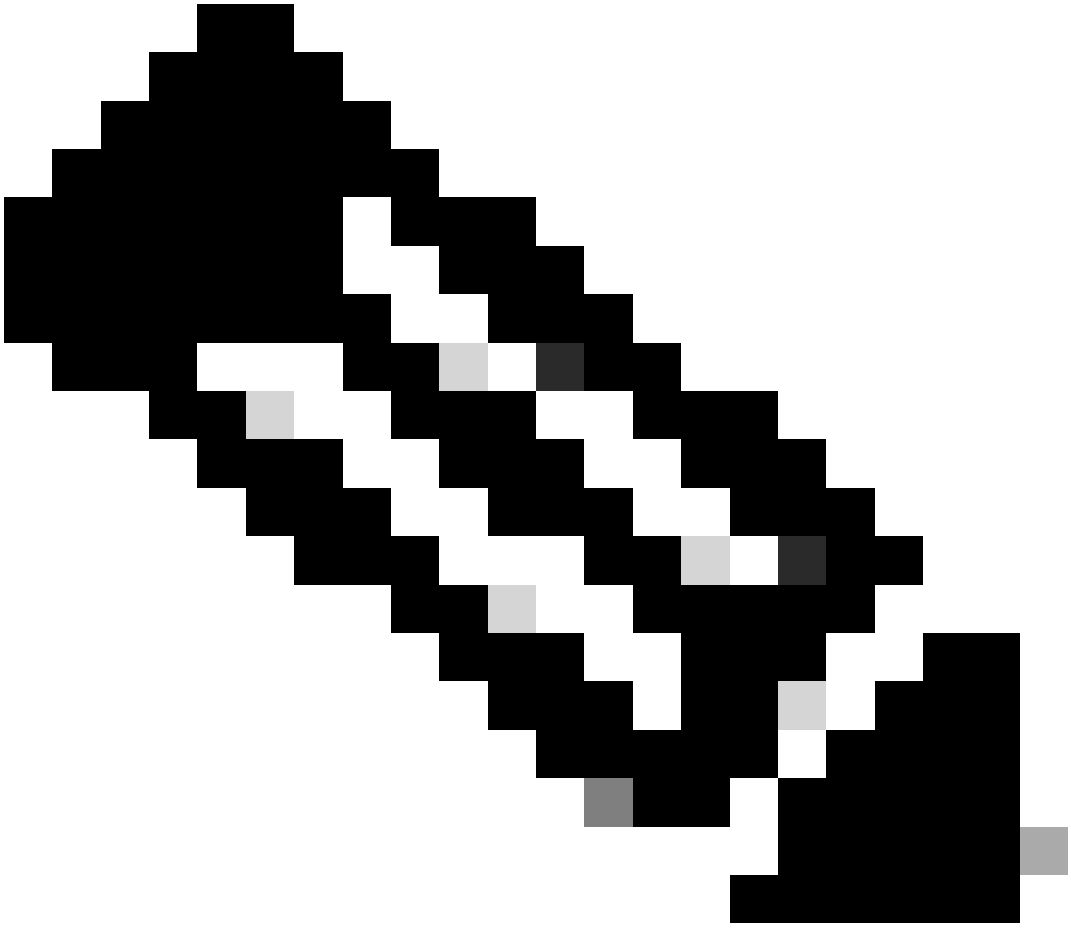
- 구성 **General** 아래에서 **Private Resource Name**



보안 액세스 - 프라이빗 리소스 - 일반

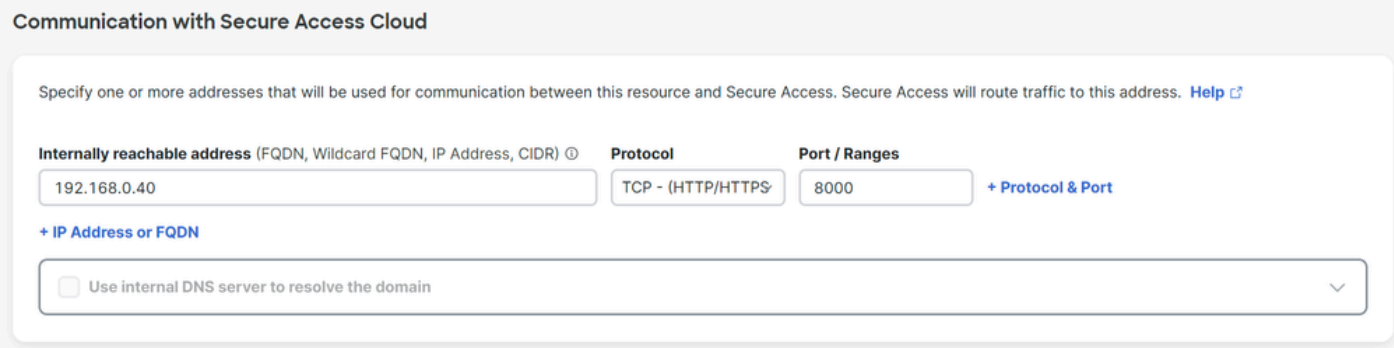
구성 **Communication with Secure Access Cloud** 아래에서:

- **Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR)**: 액세스하려는 리소스를 선택합니다.



참고: 단계에서 내부적으로 연결 가능한 주소가 할당되었음을 **Configure the Tunnel on Secure Access**기억하십시오.

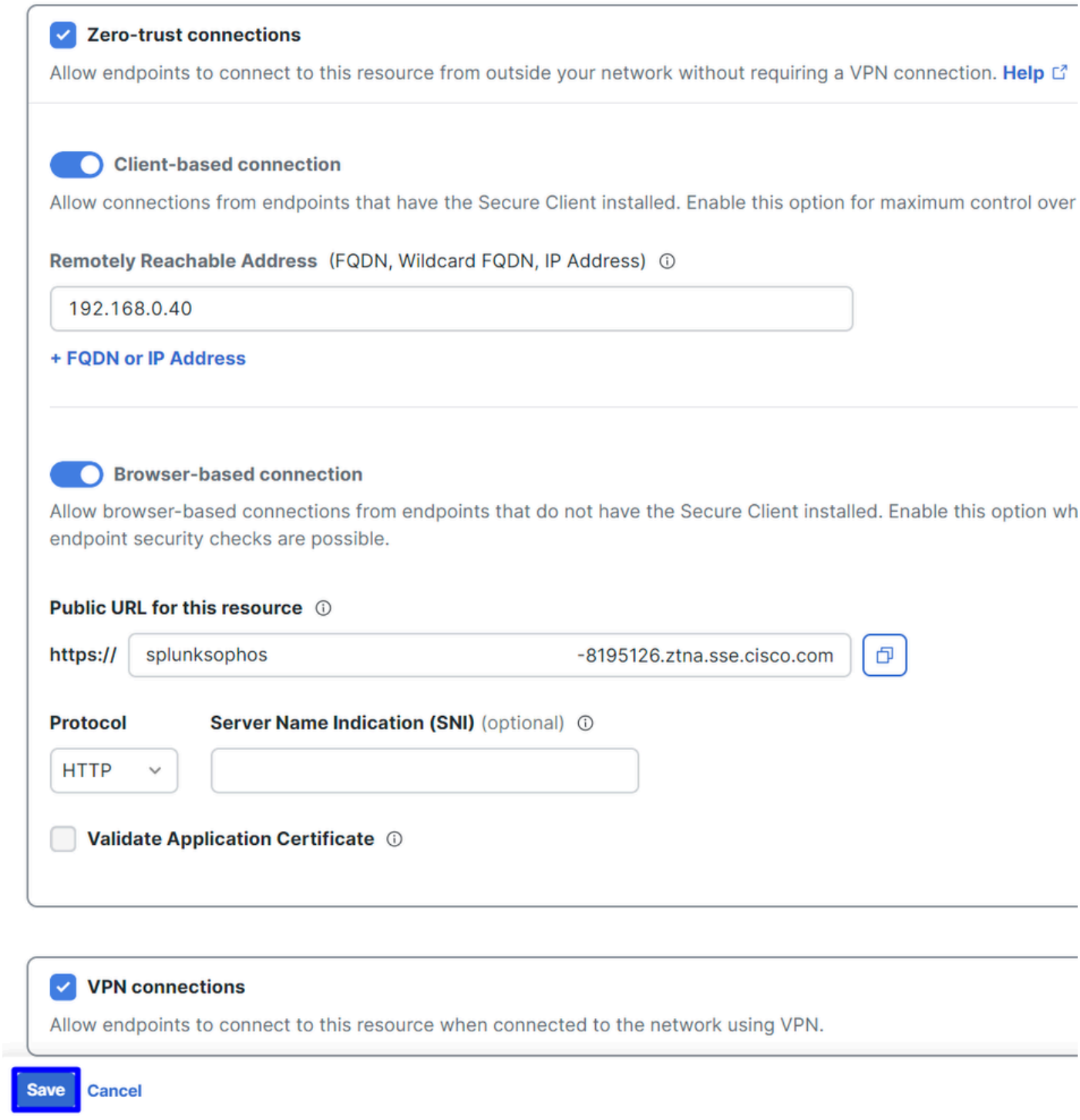
- **Protocol**: 해당 리소스에 액세스하는 데 사용하는 프로토콜을 선택합니다
- Port / Ranges : 앱에 액세스하기 위해 활성화해야 하는 포트를 선택합니다



보안 액세스 - 프라이빗 리소스 - *Secure Access Cloud*와의 통신

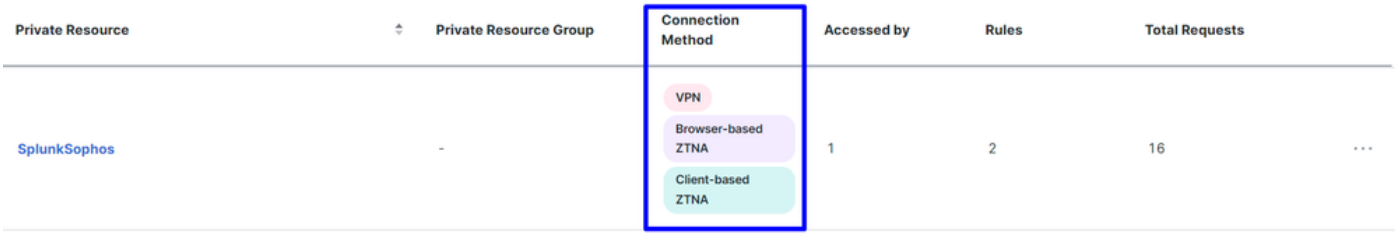
내에서 **Endpoint Connection Methods** Secure Access를 통해 프라이빗 리소스에 액세스할 수 있는 모든 방법을 구성하고 환경에 사용할 방법을 선택합니다.

- **Zero-trust connections**: ZTNA 액세스를 활성화하려면 확인란을 선택합니다.
    - **Client-based connection**: 클라이언트 기본 ZTNA를 허용하는 단추를 활성화합니다.
        - **Remotely Reachable Address**: 개인 앱의 IP를 구성합니다
    - **Browser-based connection**: 버튼을 활성화하여 브라우저 기반 ZTNA를 허용합니다.
        - Public URL for this resource: ztna.sse.cisco.com 도메인과 함께 사용할 이름을 추가합니다.
            - Protocol: 브라우저를 통해 액세스하기 위한 프로토콜로 HTTP 또는 HTTPS를 선택합니다.
    - **VPN connections**: RA-VPN 액세스를 활성화하려면 확인란을 선택합니다.
- 클릭 **Save**



보안 액세스 - 프라이빗 리소스 - *Secure Access Cloud*와의 통신 2

컨피그레이션이 완료되면 다음과 같은 결과가 나타납니다.

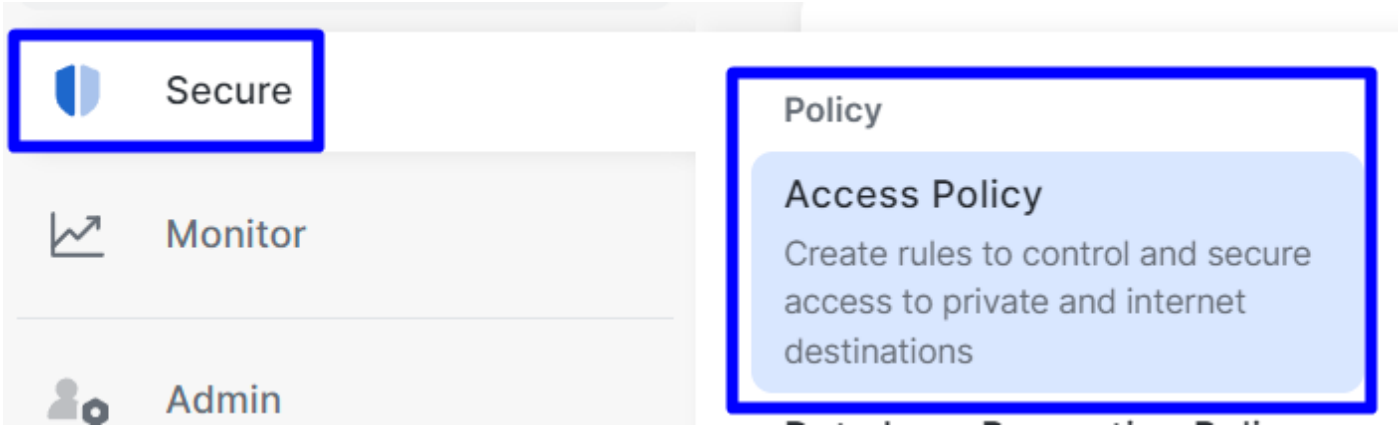


보안 액세스 - 프라이빗 리소스 구성

이제 단계를 진행할 수 있습니다 **Configure the Access Policy**.

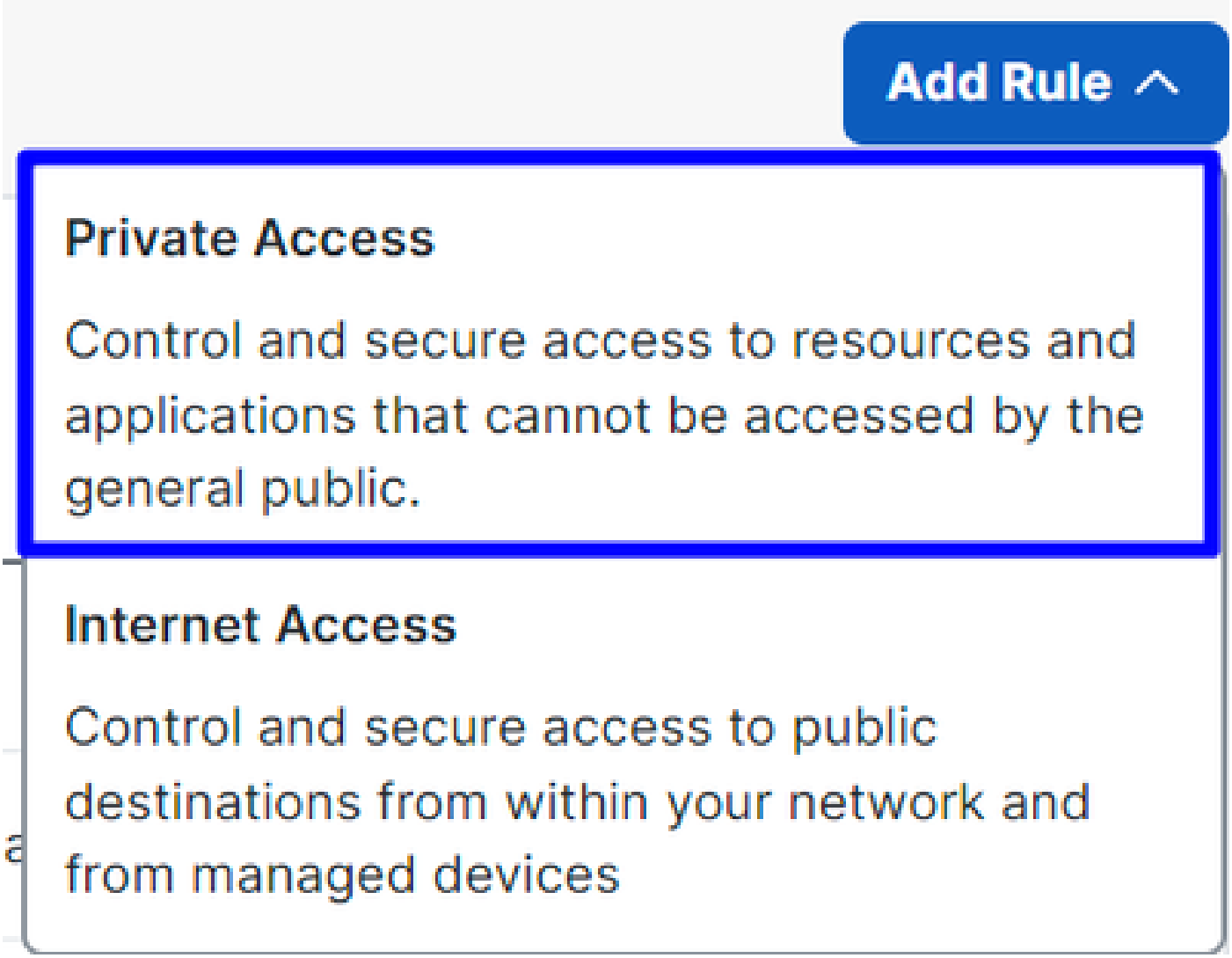
액세스 정책 구성

액세스 정책을 구성하려면 로 Secure > Access Policy 이동합니다.



보안 액세스 - 액세스 정책

- 클릭 **Add Rule** > **Private Access**

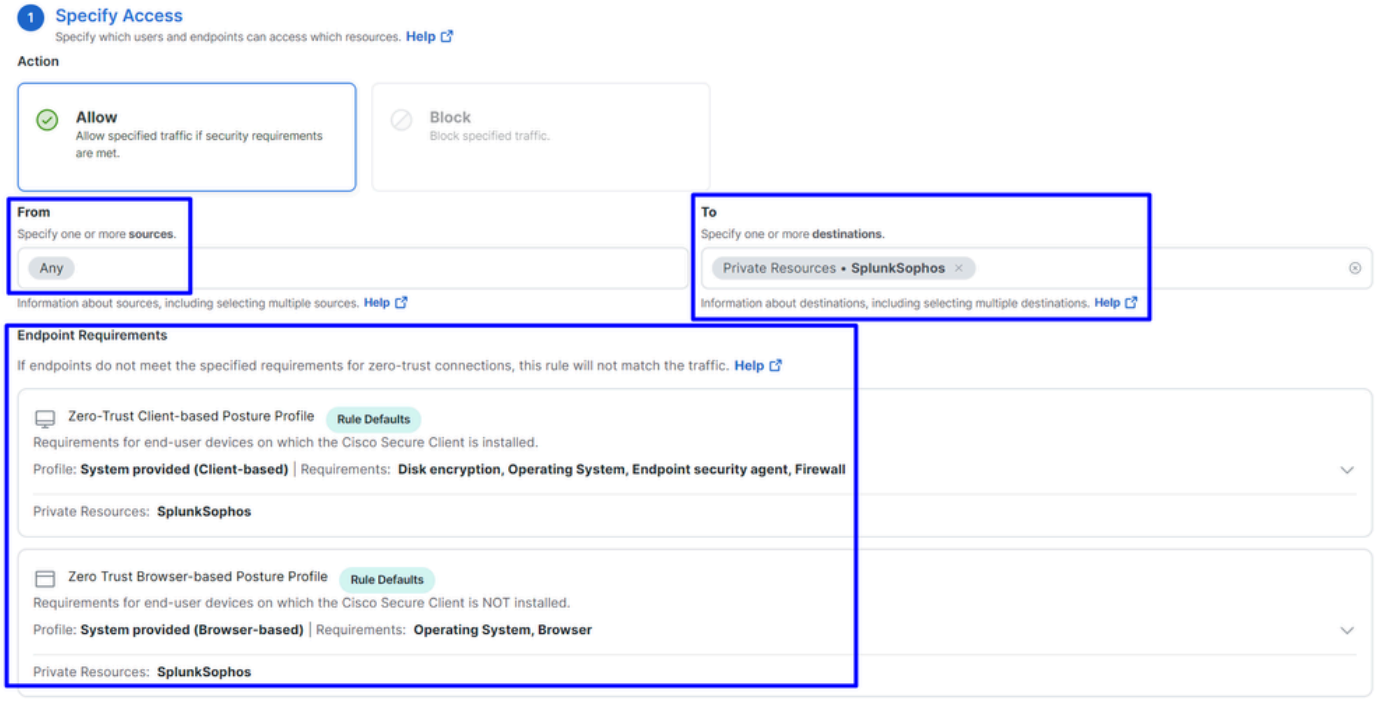


보안 액세스 - 액세스 정책 - 개인 액세스

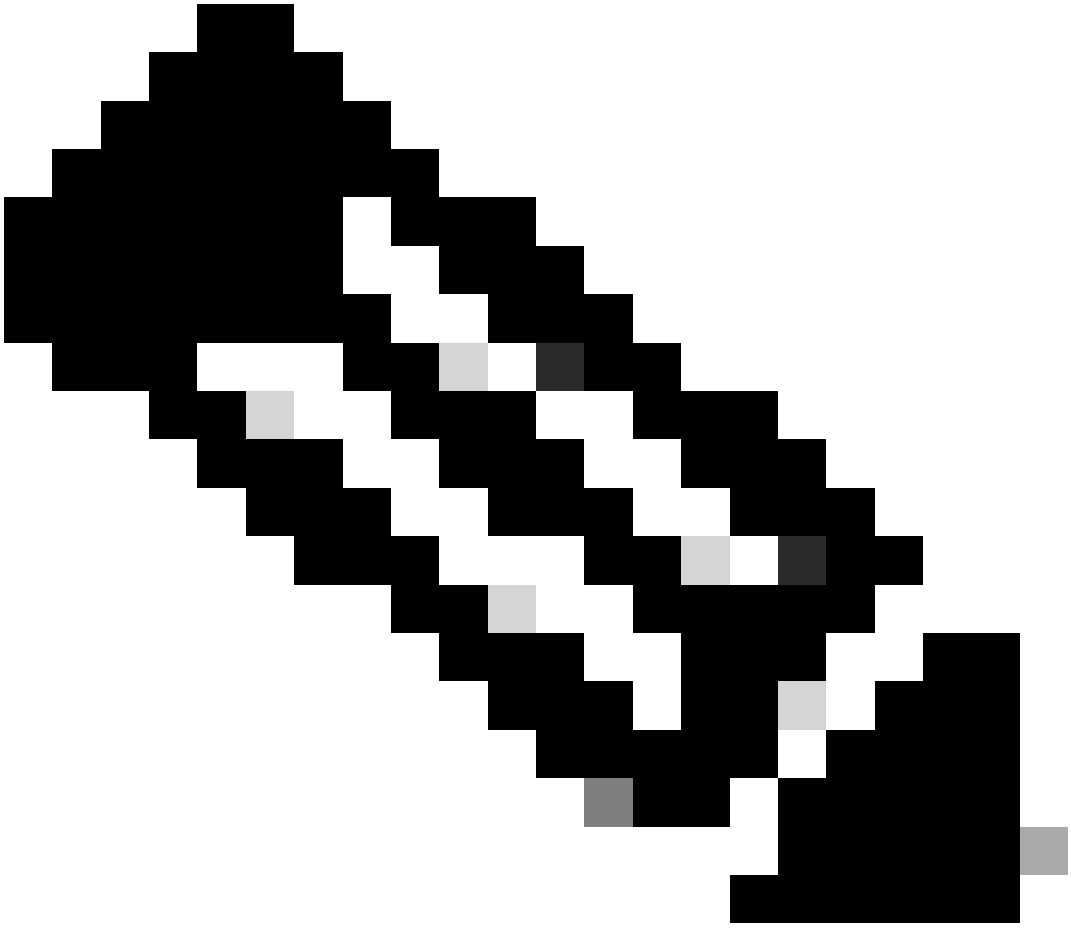
여러 인증 방법을 통해 액세스를 제공하려면 다음 옵션을 구성합니다.

- 1. Specify Access
  - Action:허용
    - **Rule name**: 액세스 규칙의 이름을 지정합니다.
    - **From**: 액세스 권한을 부여한 사용자
    - **To**: 액세스를 허용하려는 애플리케이션
    - Endpoint Requirements: (기본값)

- 클릭 **Next**

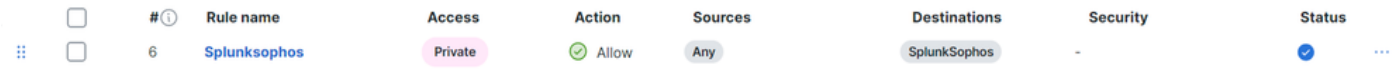


보안 액세스 - 액세스 정책 - 액세스 지정



참고: 필요에 **2. Configure Security** 따라 단계에서 또는 을(를) **Intrusion Prevention (IPS)**활성화하지 **Tenant Control Profile**않았습니다.

- 다음Save 항목을 클릭하면 됩니다.



보안 액세스 - 구성된 액세스 정책

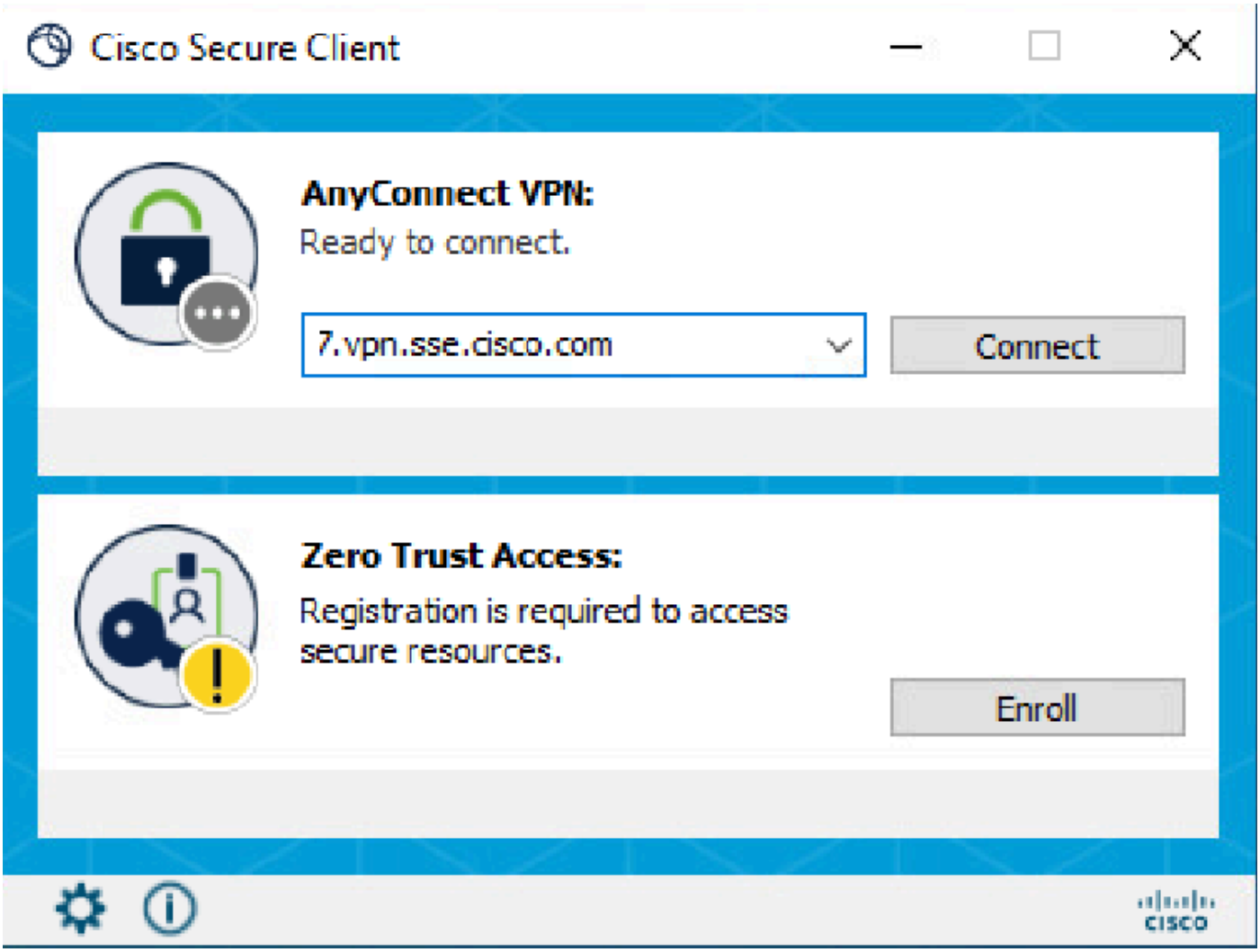
그런 다음 단계를 진행할 수 Verify 있습니다.

다음을 확인합니다.

액세스를 확인하려면 소프트웨어 다운로드 - Cisco Secure Client에서 다운로드할 수 있는 Cisco Secure Client의 에이전트를 설치해야 합니다.

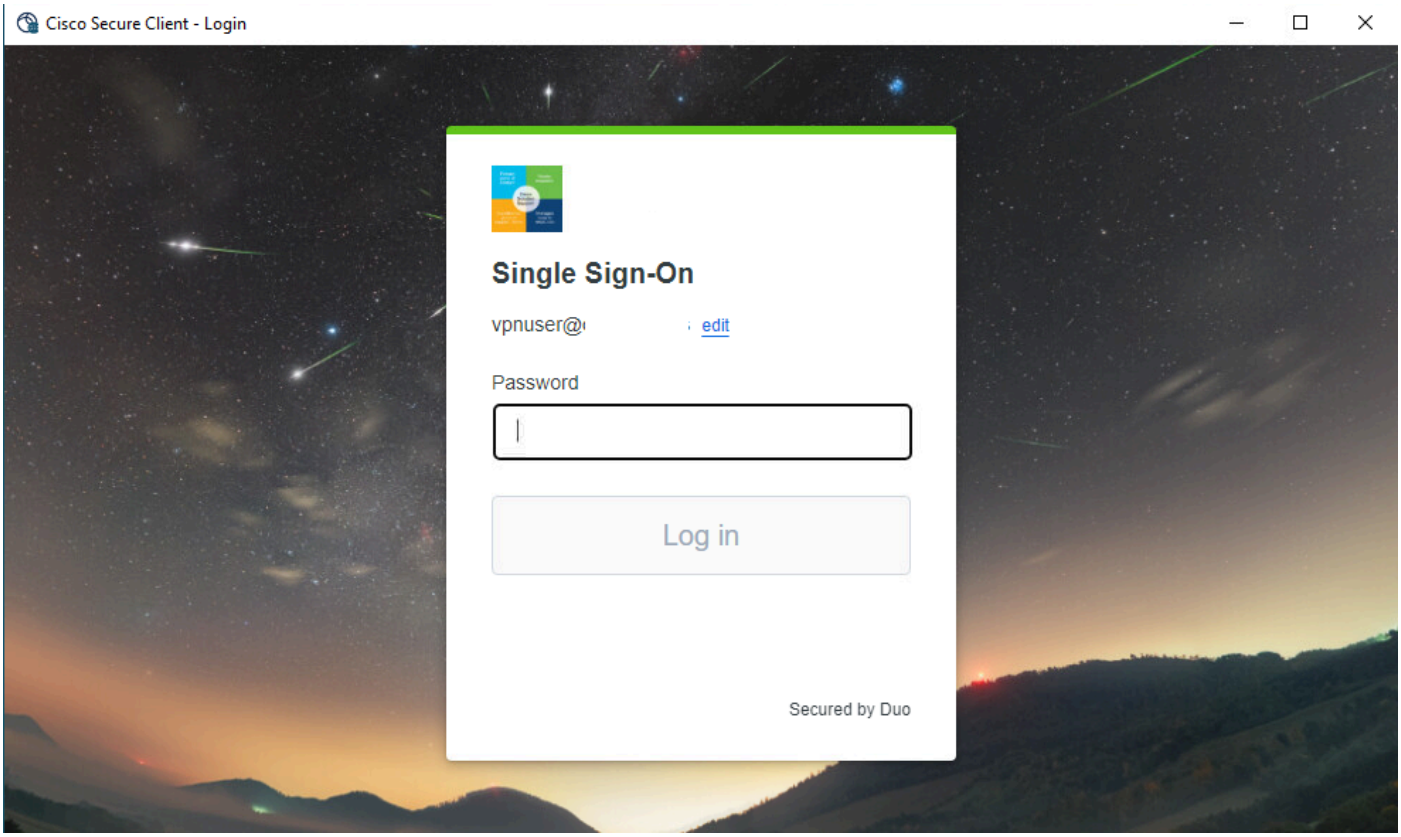
RA-VPN

Cisco Secure Client Agent-VPN을 통해 로그인합니다.



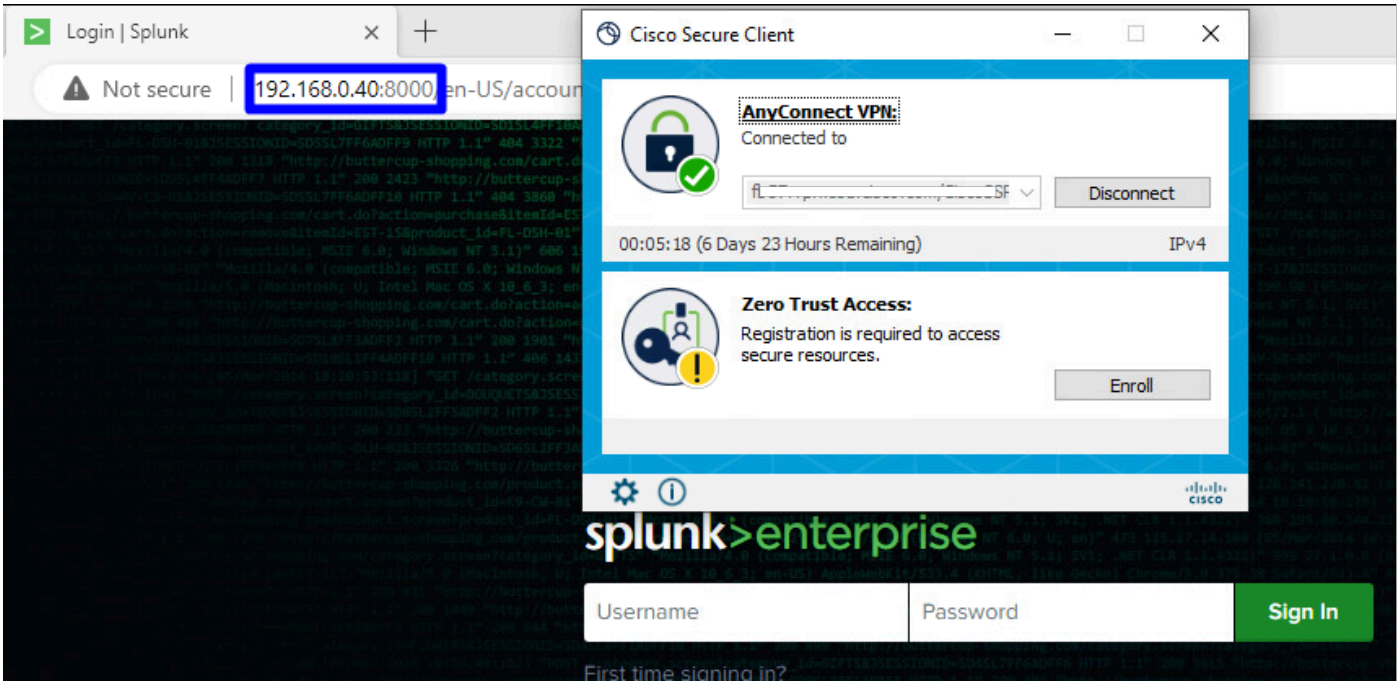
보안 클라이언트 - *VPN*

- SSO 공급자를 통해 인증



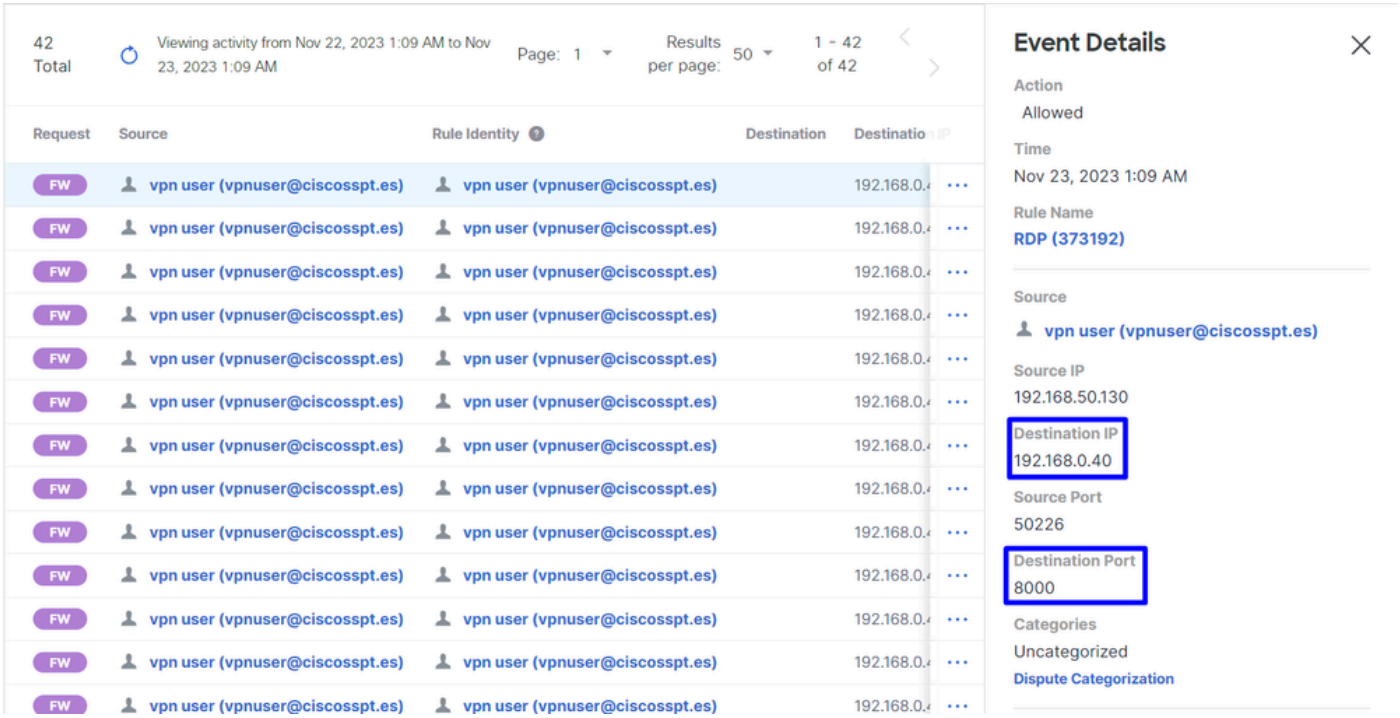
보안 액세스 - *VPN - SSO*

- 인증된 후 리소스에 액세스합니다.



보안 액세스 - *VPN* - 인증

다음으로 이동합니다.Monitor > Activity Search

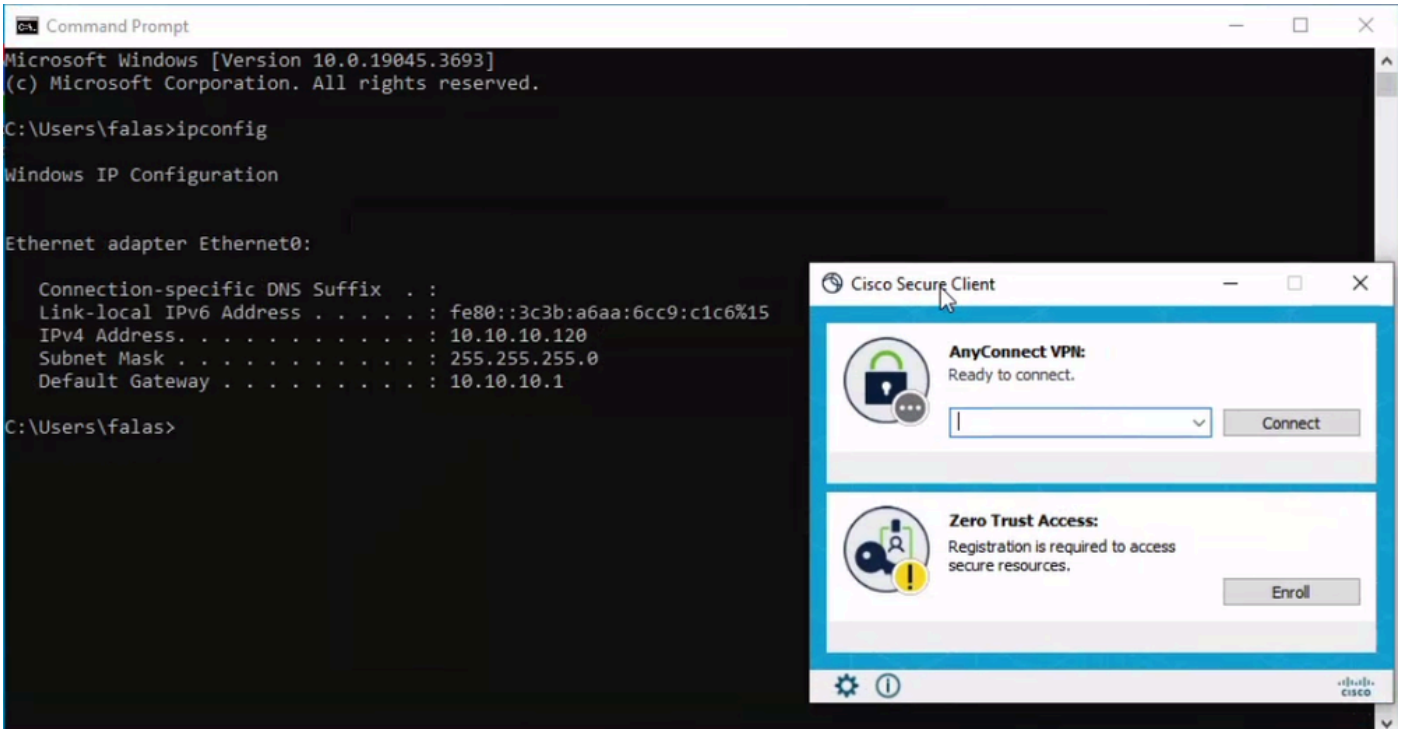


보안 액세스 - 활동 검색 - *RA-VPN*

사용자가 RA-VPN을 통해 인증하도록 허용되었음을 확인할 수 있습니다.

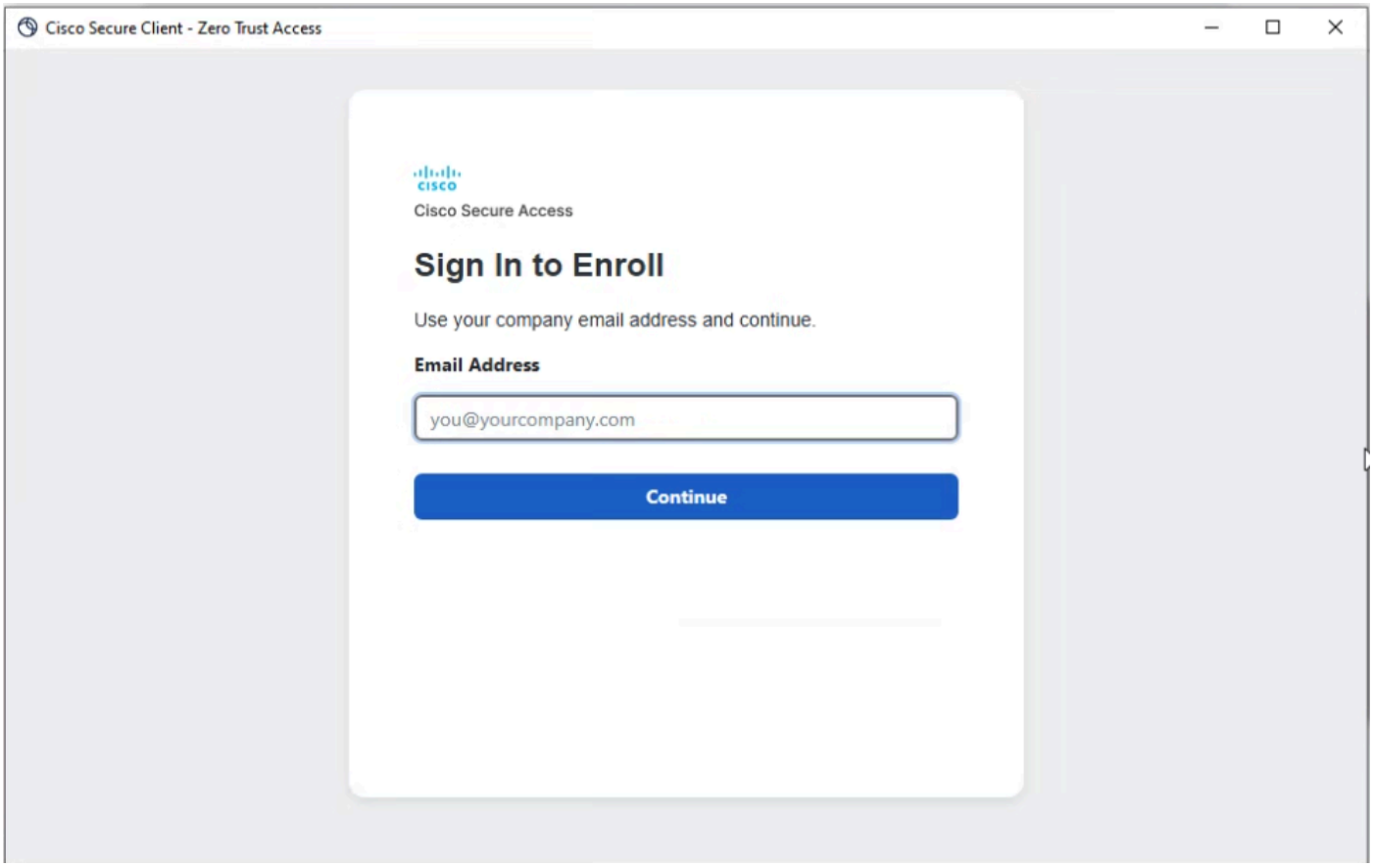
클라이언트 기반 ZTNA

Cisco Secure Client Agent - ZTNA를 통해 로그인합니다.



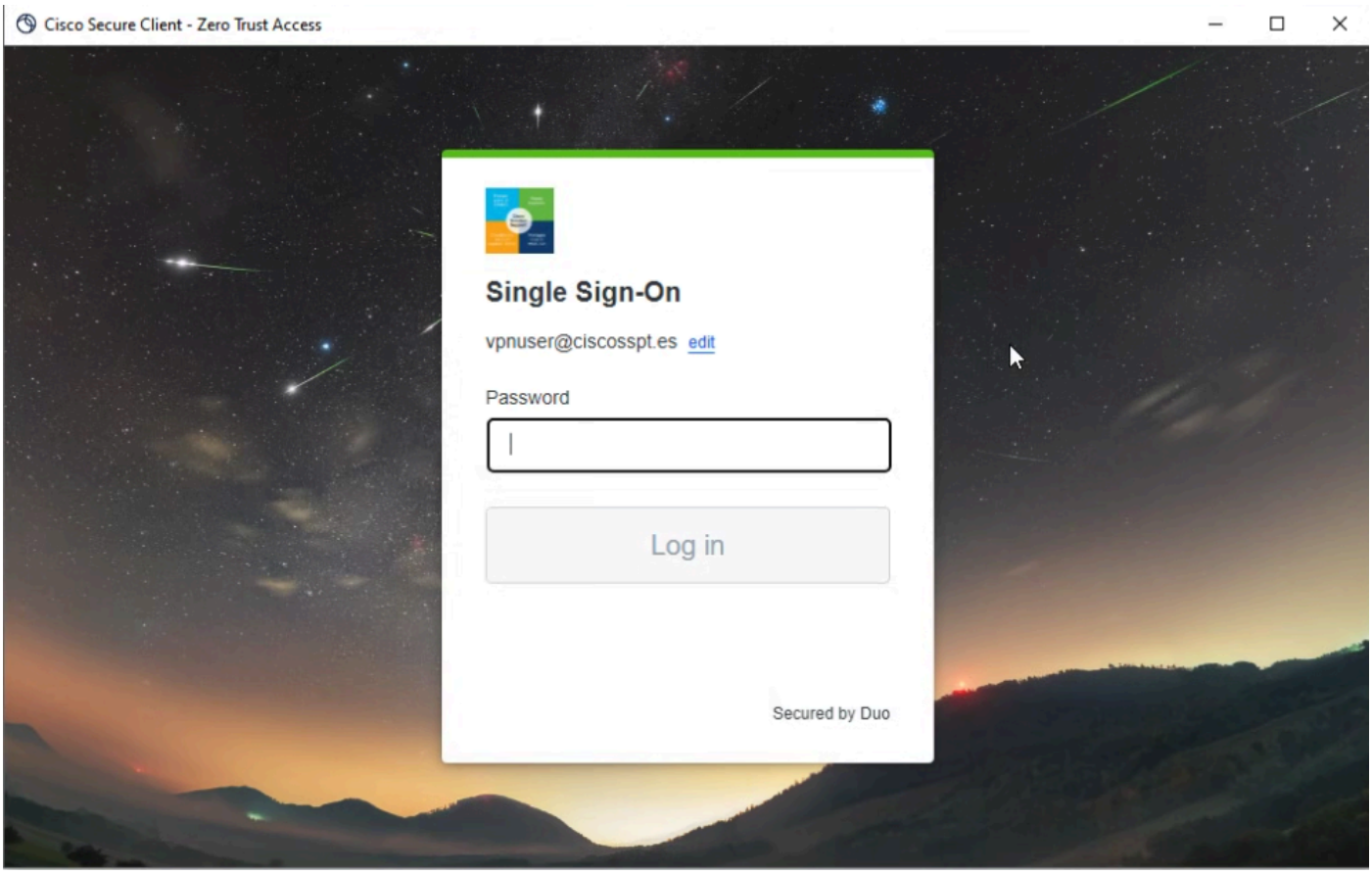
보안 클라이언트 - *ZTNA*

- 사용자 이름으로 등록합니다.



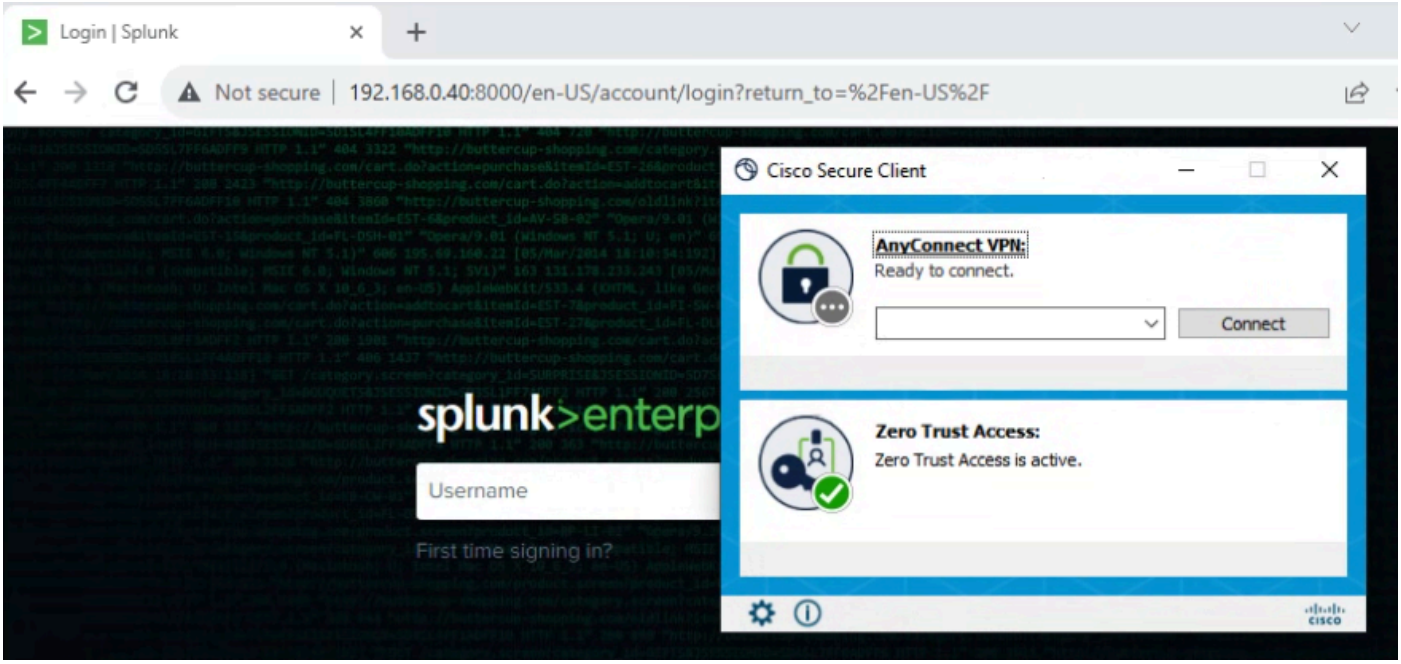
보안 클라이언트 - *ZTNA* - 등록

- SSO 제공자에서 인증



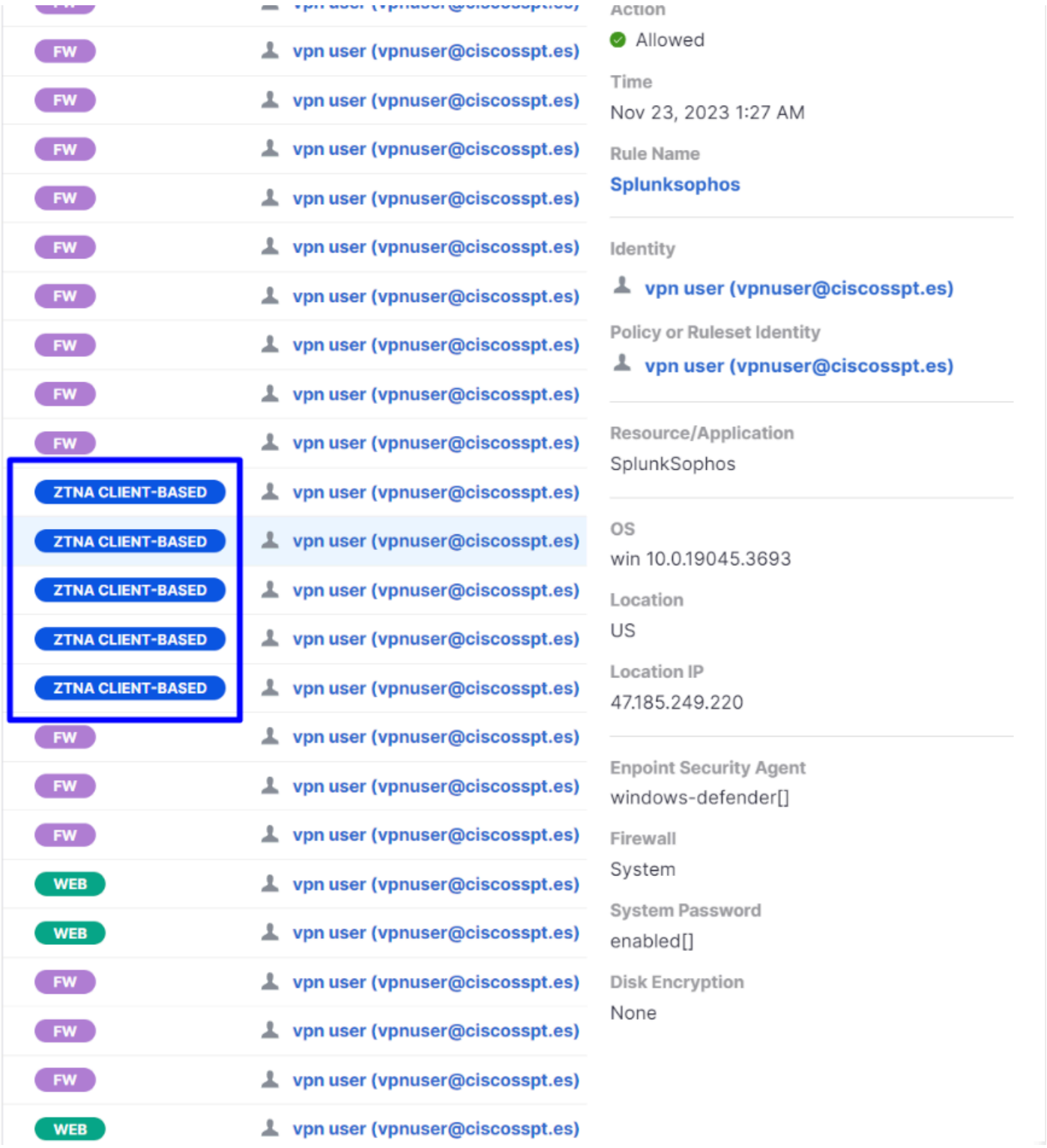
보안 클라이언트 - *ZTNA* - *SSO* 로그인

- 인증된 후 리소스에 액세스합니다.



보안 액세스 - *ZTNA* - 기록됨

다음으로 이동합니다.Monitor > Activity Search

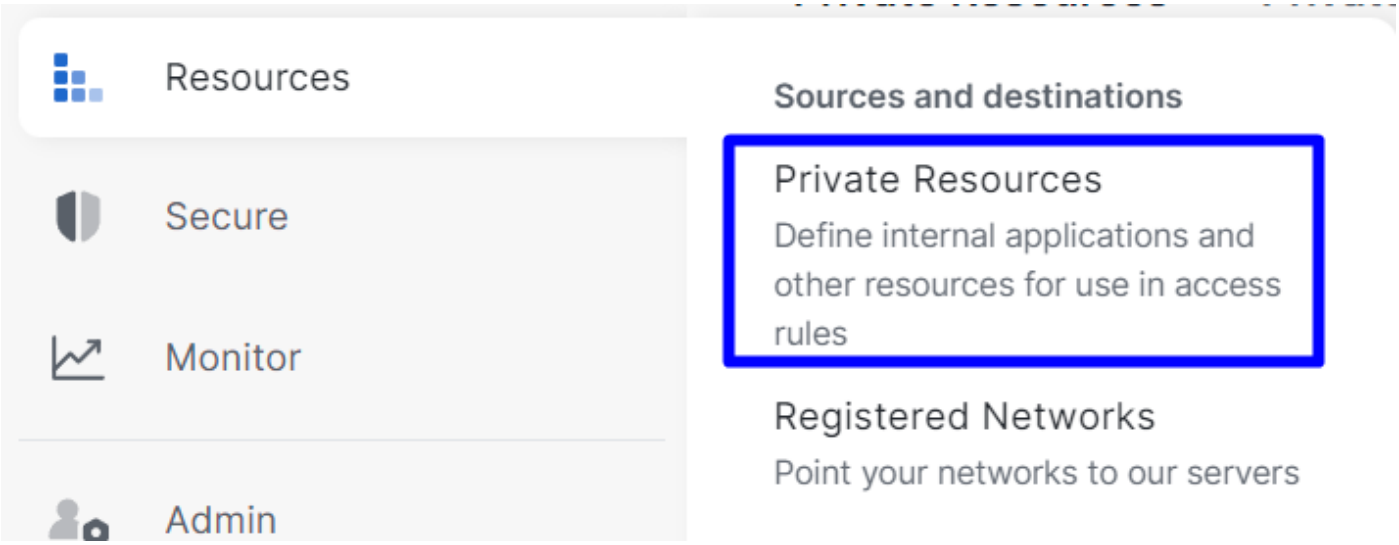


보안 액세스 - 활동 검색 - *ZTNA* 클라이언트 기반

사용자가 클라이언트 기반 ZTNA를 통해 인증하도록 허용되었음을 확인할 수 있습니다.

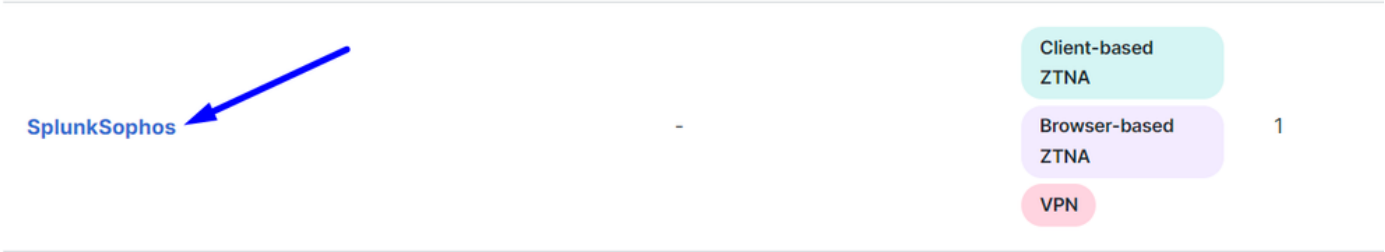
브라우저 기반 ZTNA

URL을 가져오려면 로 이동해야 합니다**Resources** > **Private Resources**.



보안 액세스 - 프라이빗 리소스

- 정책을 클릭합니다.



보안 액세스 - 프라이빗 리소스 - *SplunkSophos*

- 아래로 스크롤

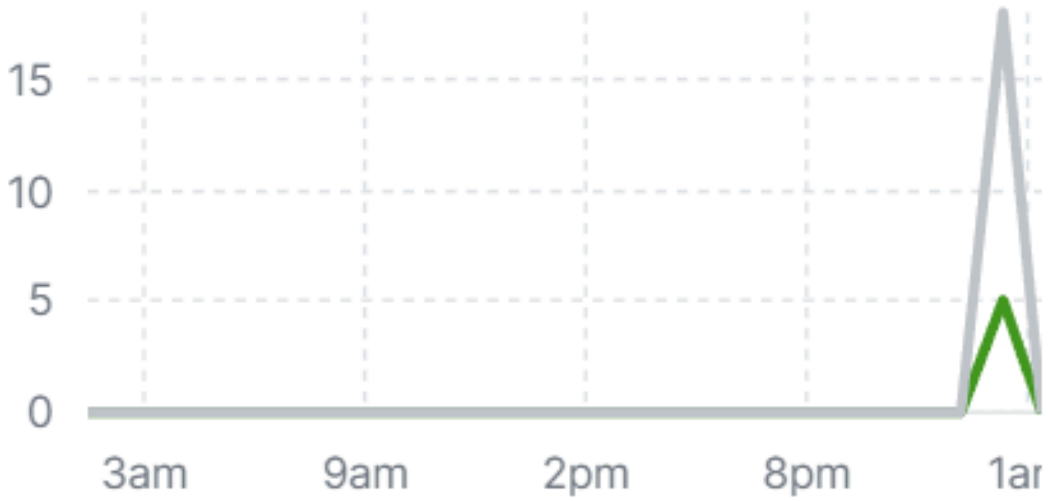
SplunkSophos

Client-based ZTNA Browser-based ZTNA

VPN

Total Requests

23 44% from previous 24 hours



TOTAL REQUESTS BY STATUS

Status	
Success	5
Blocked	18

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.