Palo Alto Firewall로 보안 액세스 구성

목차

소개

이 문서에서는 Palo Alto Firewall로 Secure Access를 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.

- Palo Alto 11.x 버전 방화벽
- 보안 액세스
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- 클라이언트리스 ZTNA

사용되는 구성 요소

이 문서의 정보는 다음을 기반으로 합니다.

- Palo Alto 11.x 버전 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 - Palo Alto

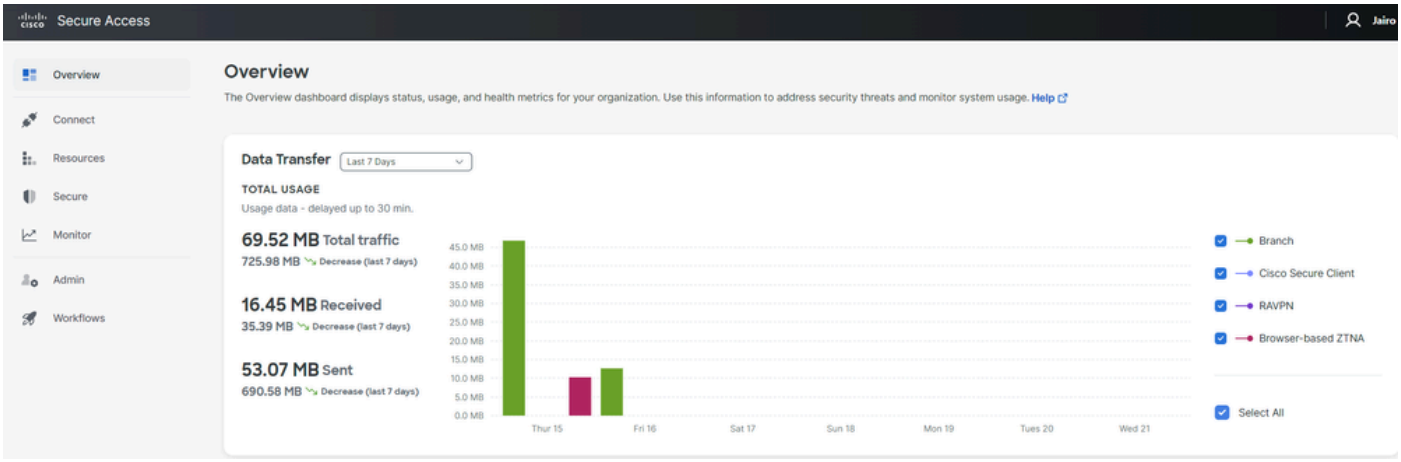
Cisco는 온프레미스 및 클라우드 기반 프라이빗 애플리케이션을 보호하고 액세스를 제공하도록

Secure Access를 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

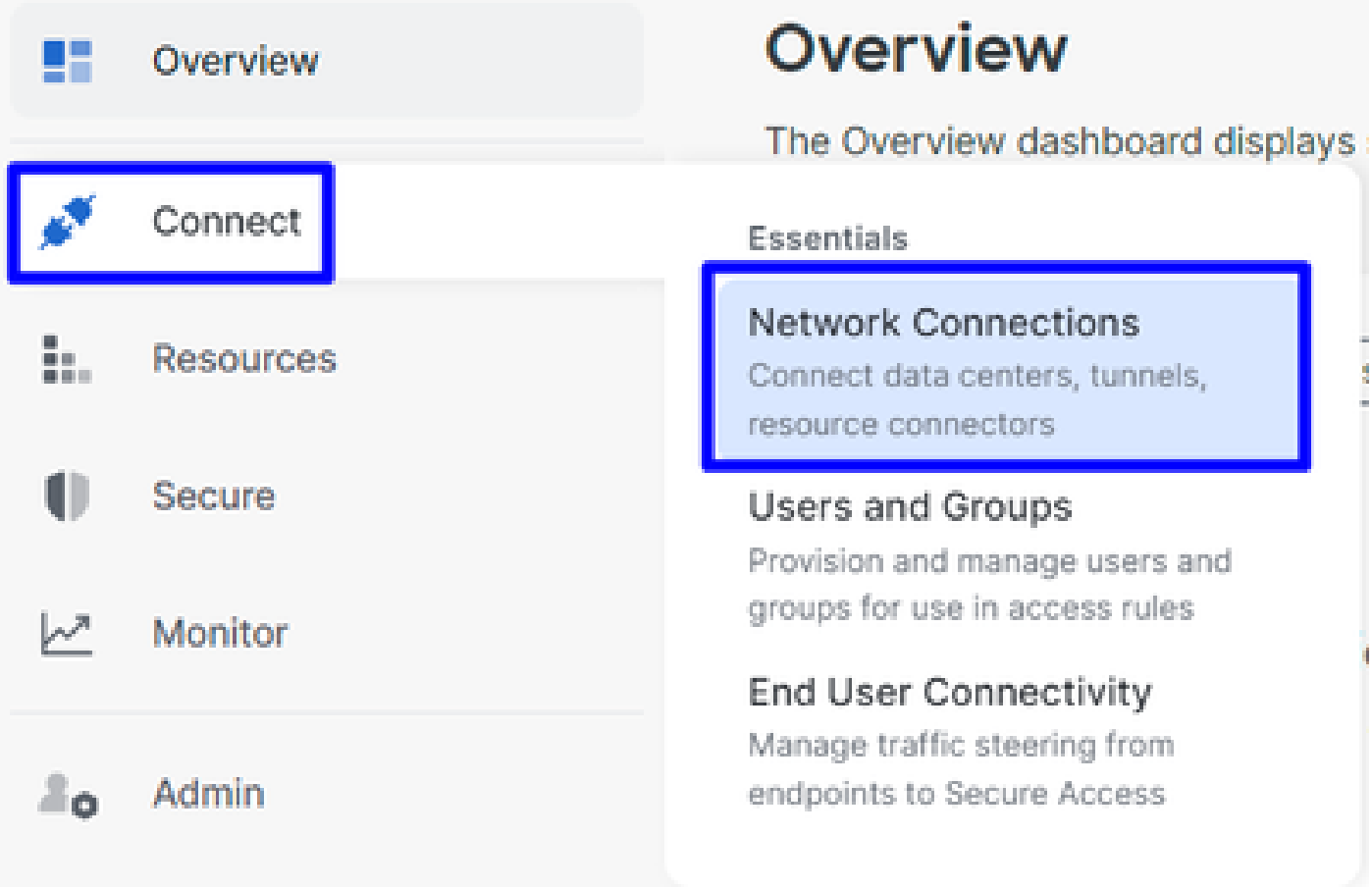
보안 액세스에서 VPN 구성

Secure Access의 관리자 패널로 이동합니다.



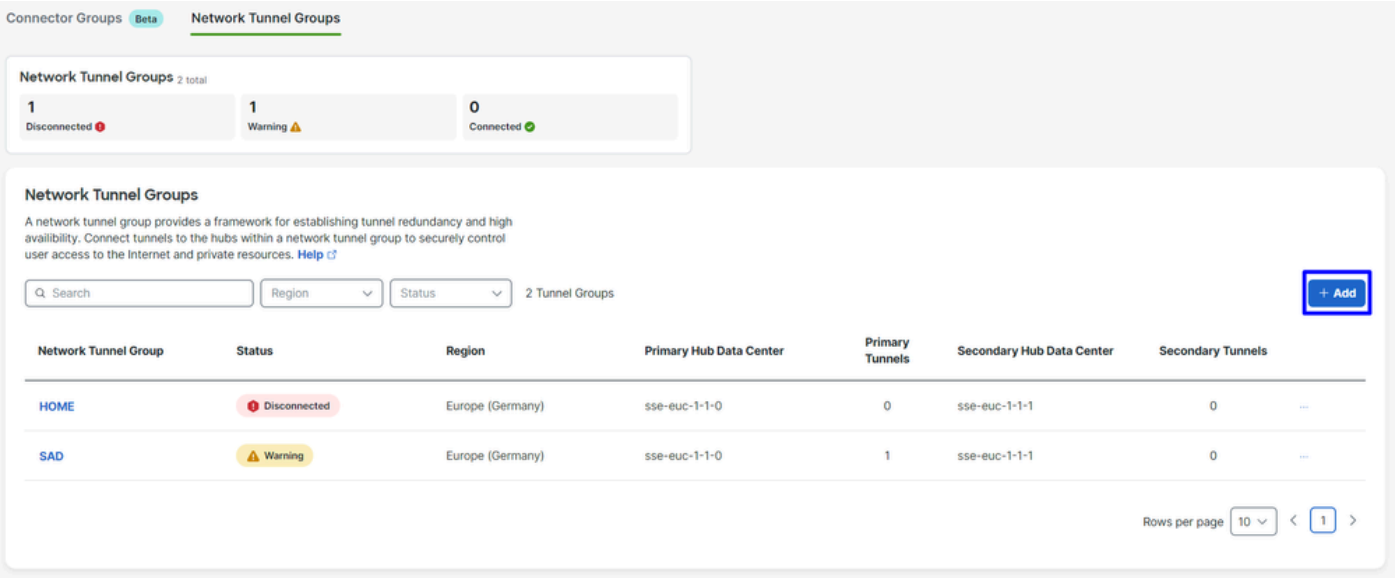
보안 액세스 - 기본 페이지

- 클릭 Connect > Network Connections



보안 액세스 - 네트워크 연결

- 에서 Network Tunnel Groups 클릭 + Add



보안 액세스 - 네트워크 터널 그룹

- 구성Tunnel Group Name, Region 및 Device Type
- 클릭 **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

Palo Alto

Region

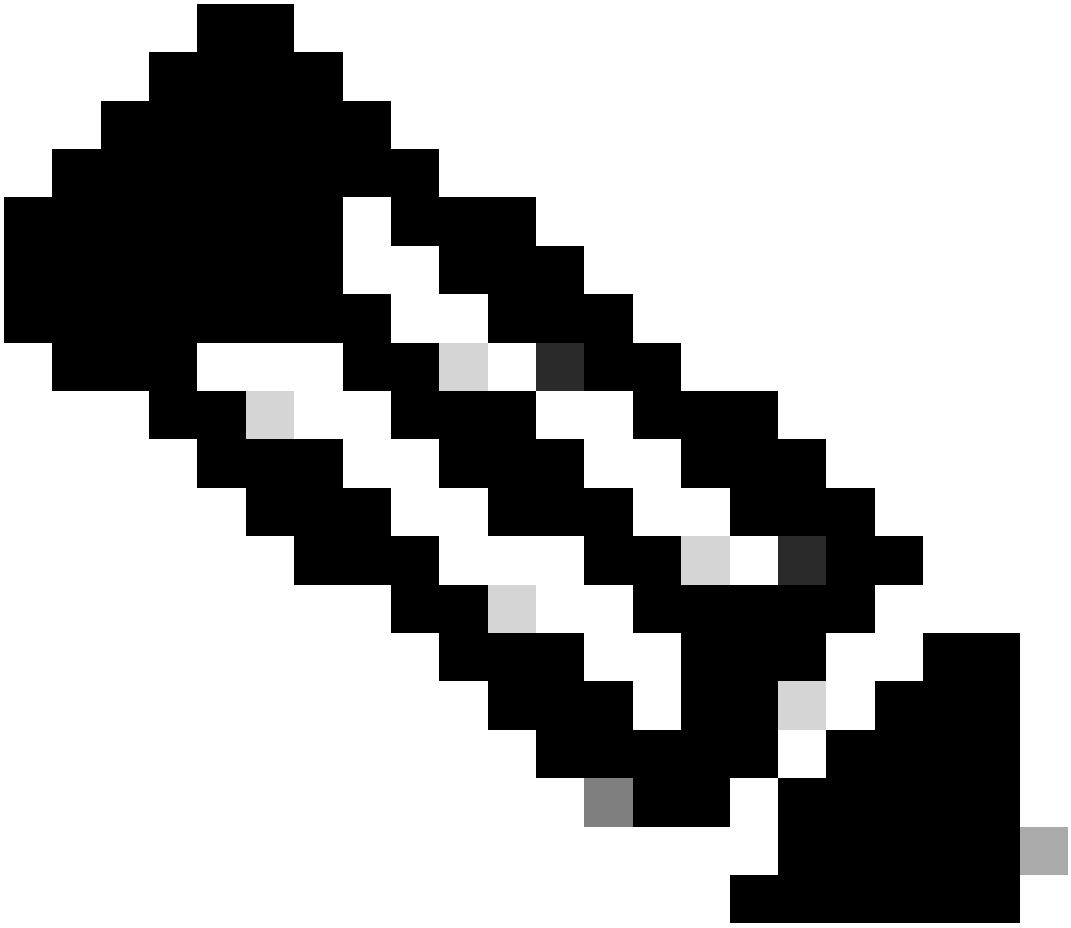
Europe (Germany)

Device Type

Other

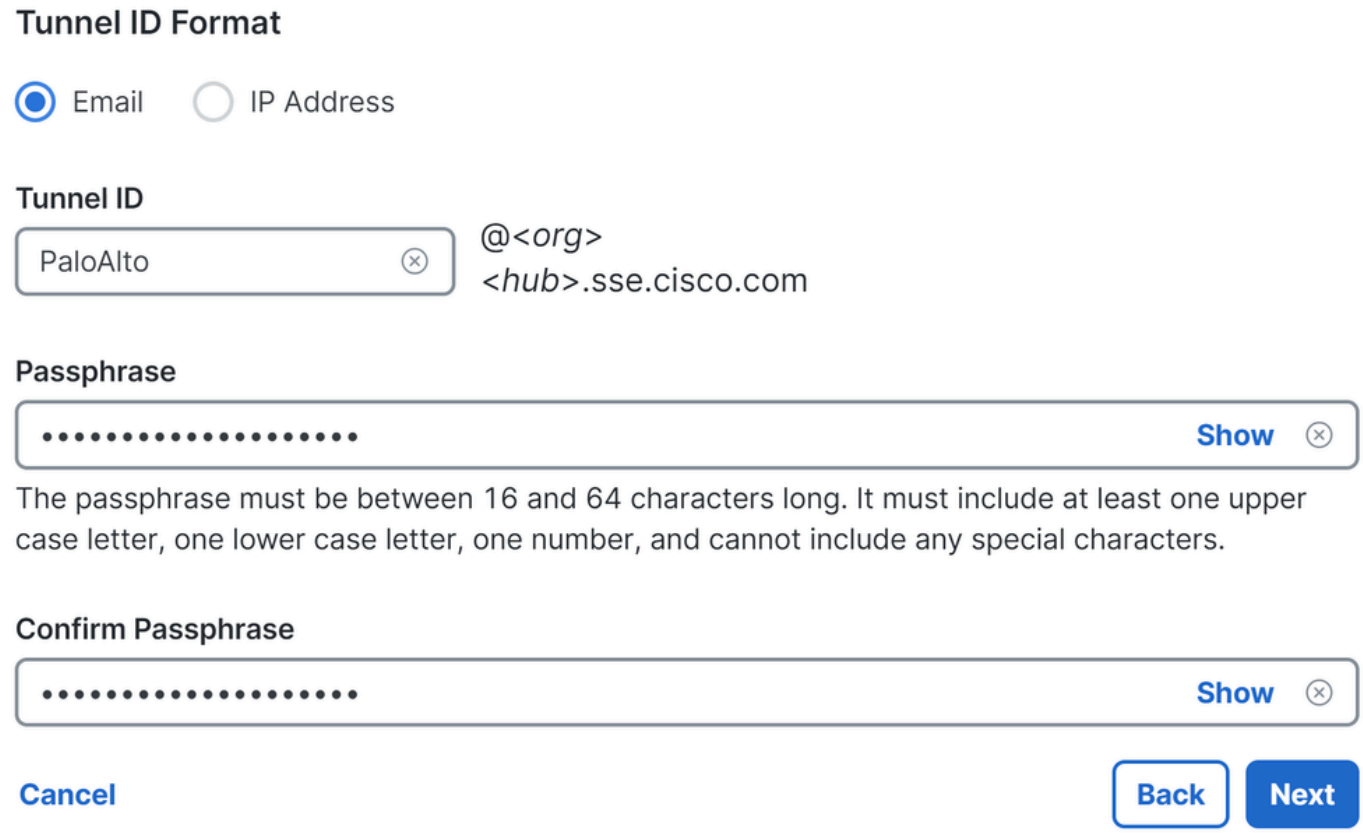
Cancel

Next

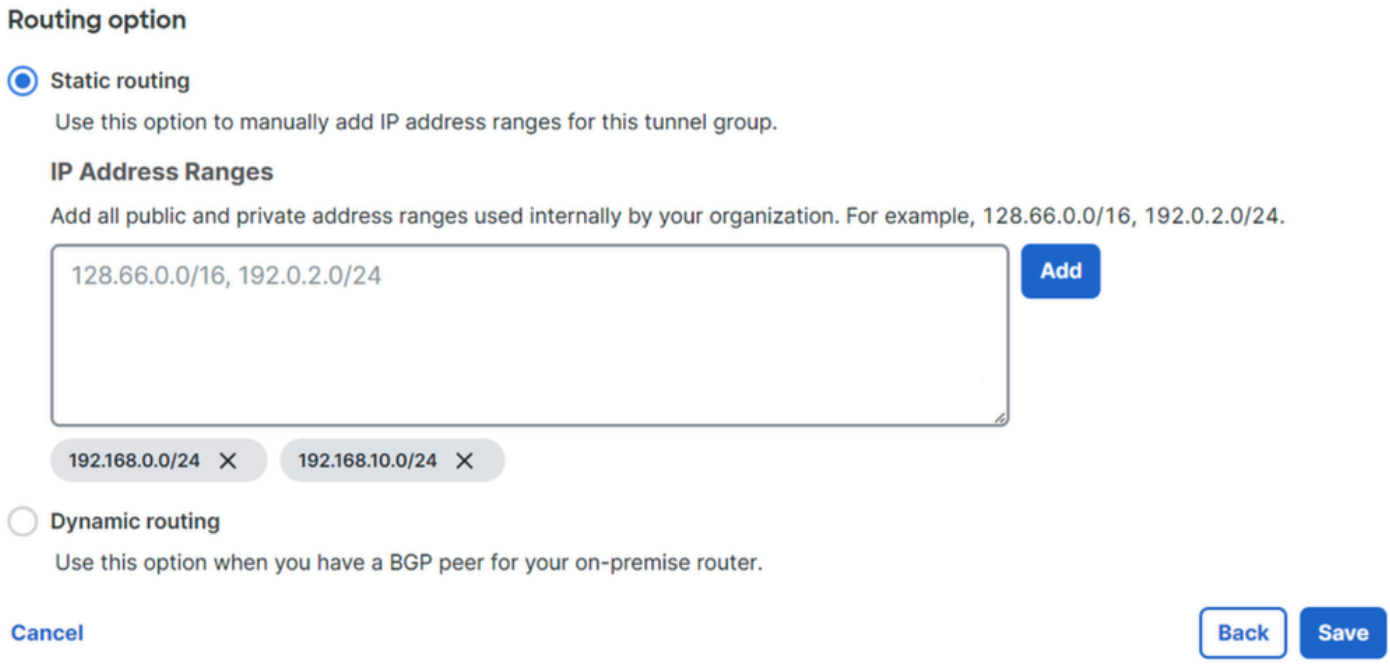


참고: 방화벽 위치에서 가장 가까운 지역을 선택합니다.

- 및 를Tunnel ID Format 구성합니다 Passphrase
- 클릭 Next



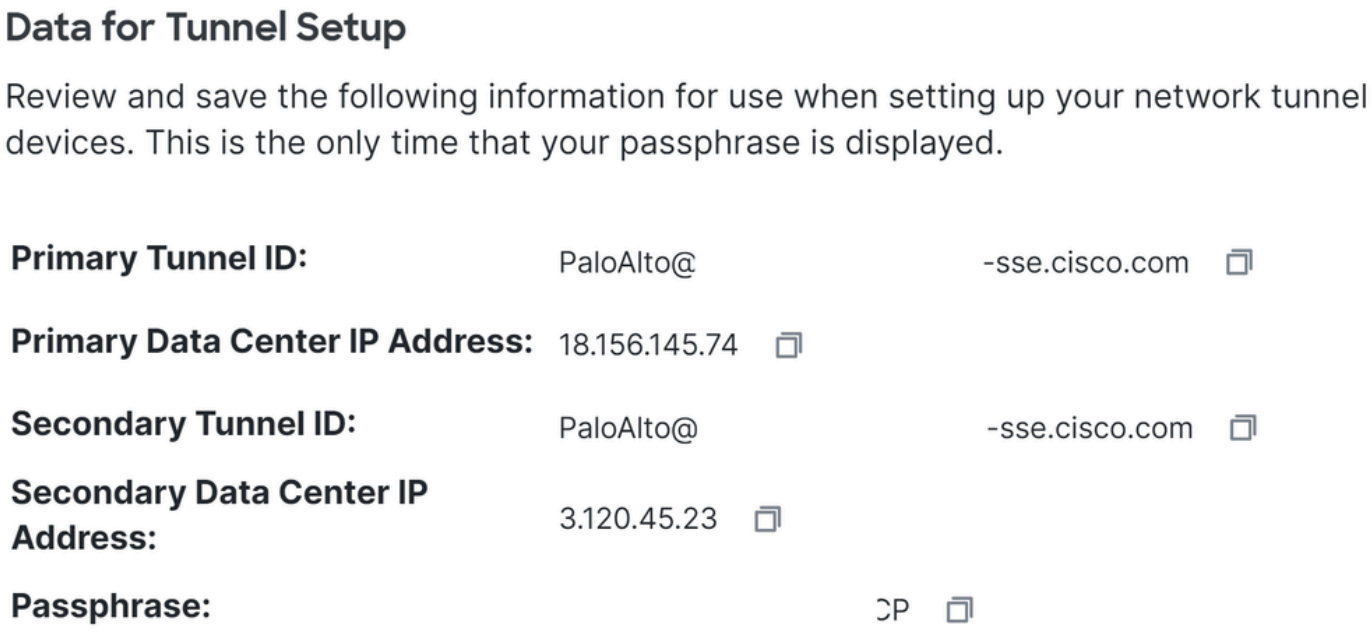
- 네트워크에서 구성했으며 Secure Access를 통해 트래픽을 전달하려는 IP 주소 범위 또는 호스트를 구성합니다
- 클릭 **Save**



보안 액세스 - 터널 그룹 - 라우팅 옵션

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

터널 데이터

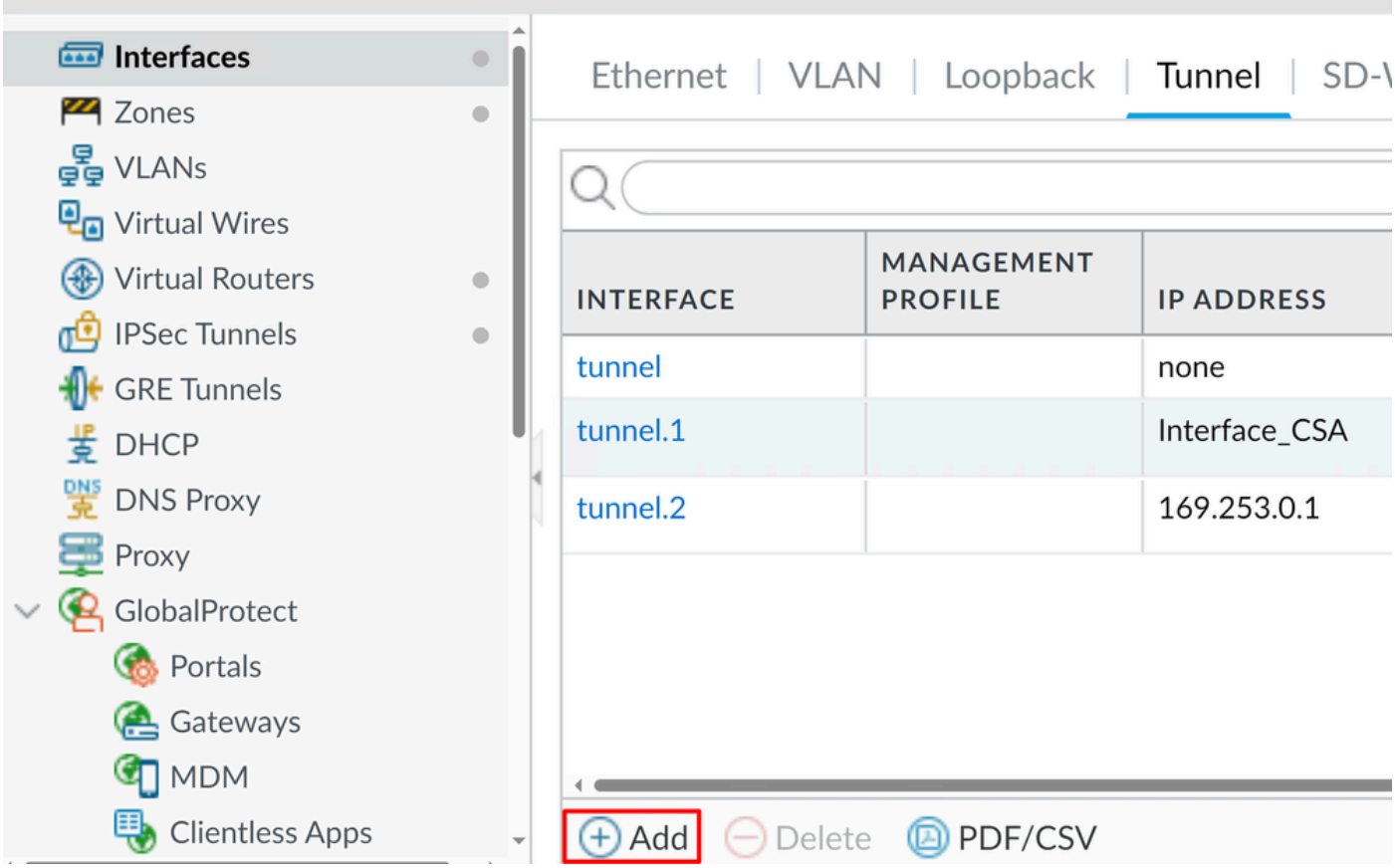


Palo Alto에서 터널 구성

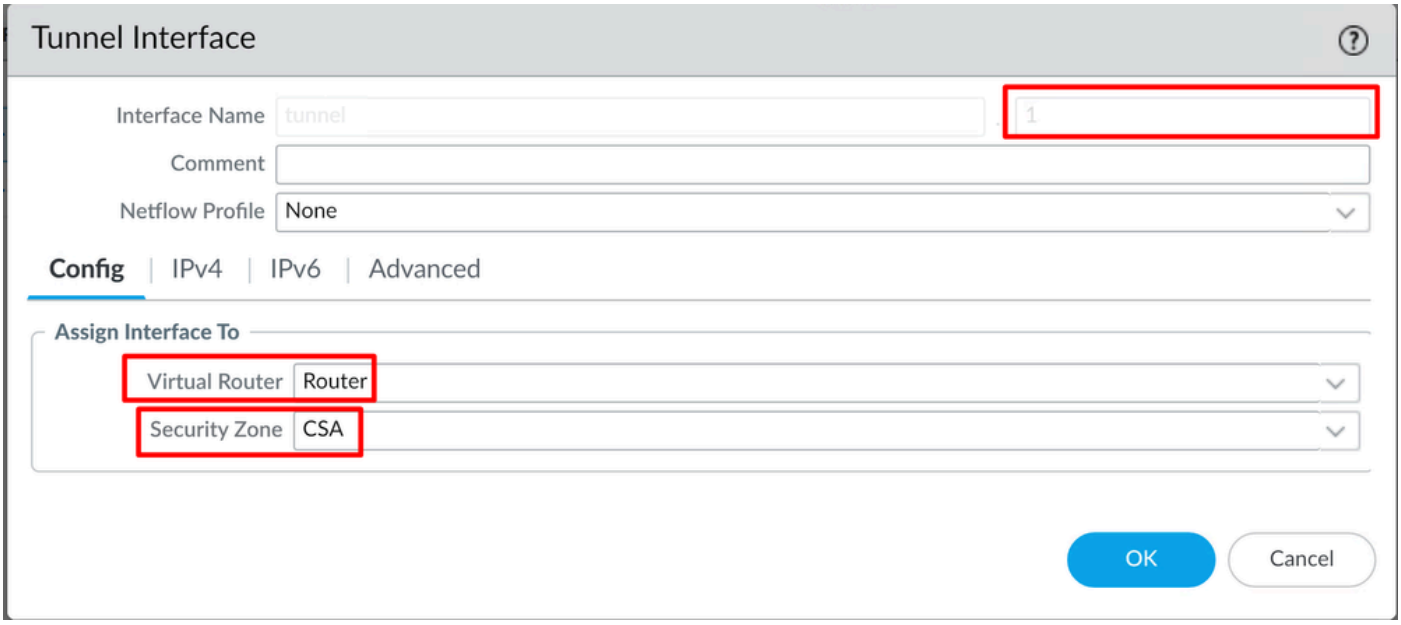
터널 인터페이스 구성

Palo Alto Dashboard(Palo Alto 대시보드)로 이동합니다.

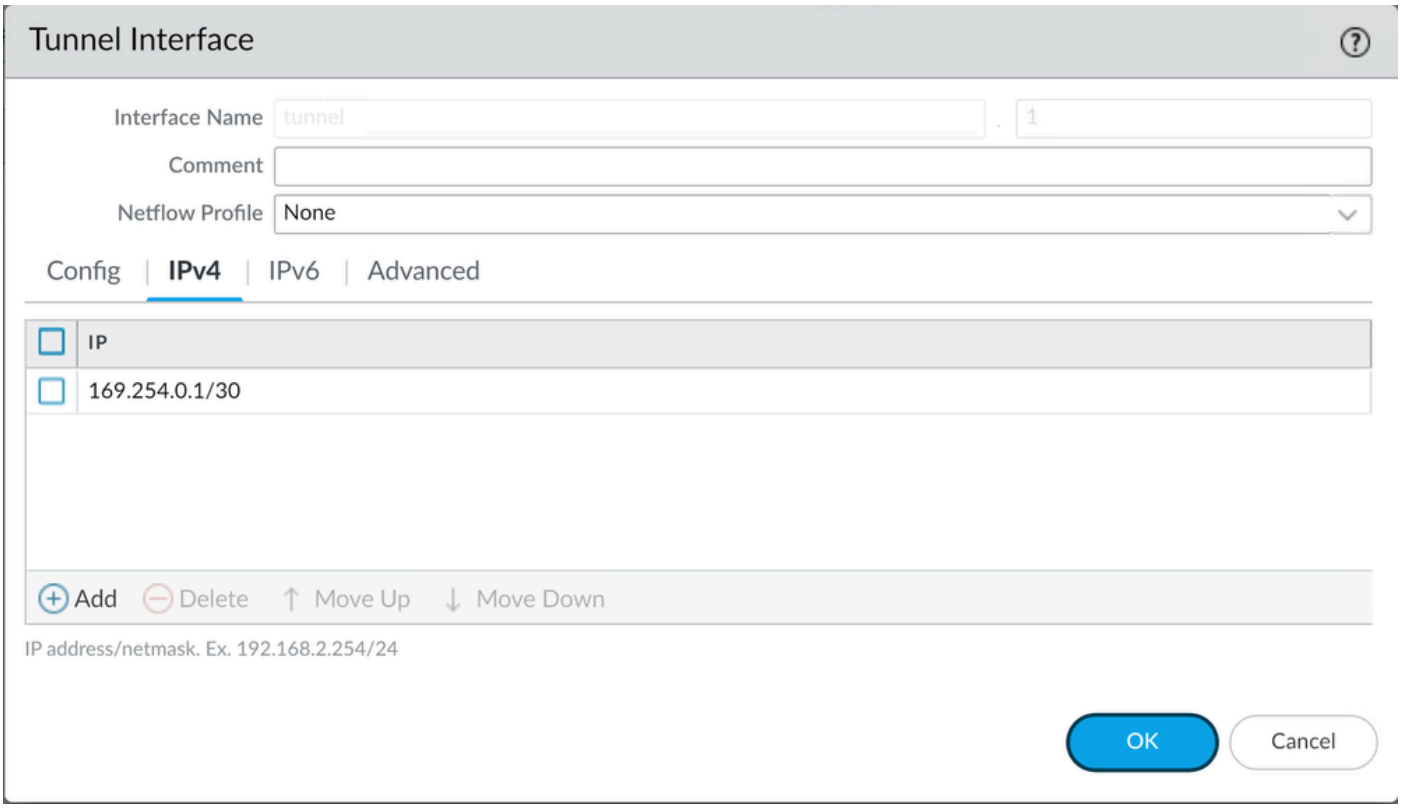
- Network > Interfaces > Tunnel
- Click Add



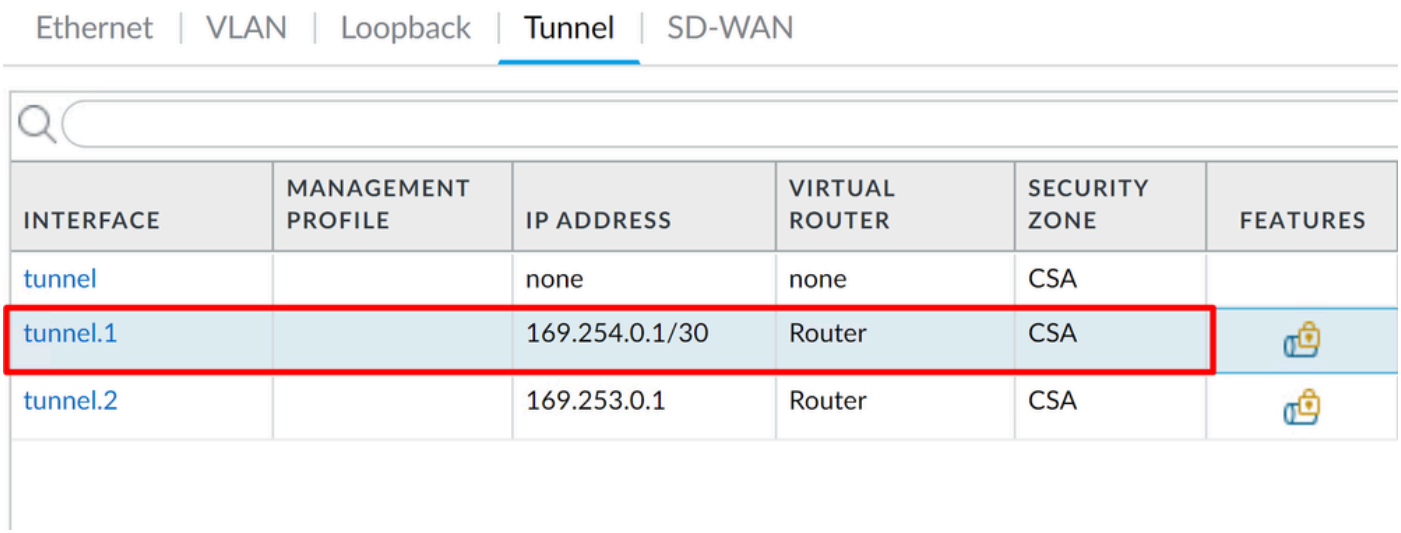
- 메뉴Config 아래에서 Virtual Router, Security Zone를 구성하고Suffix Number



- 에서IPv4 라우팅 불가 IP를 구성합니다. 예를 들어, 169.254.0.1/30
- 클릭OK



그런 다음 다음과 같은 구성을 수행할 수 있습니다.

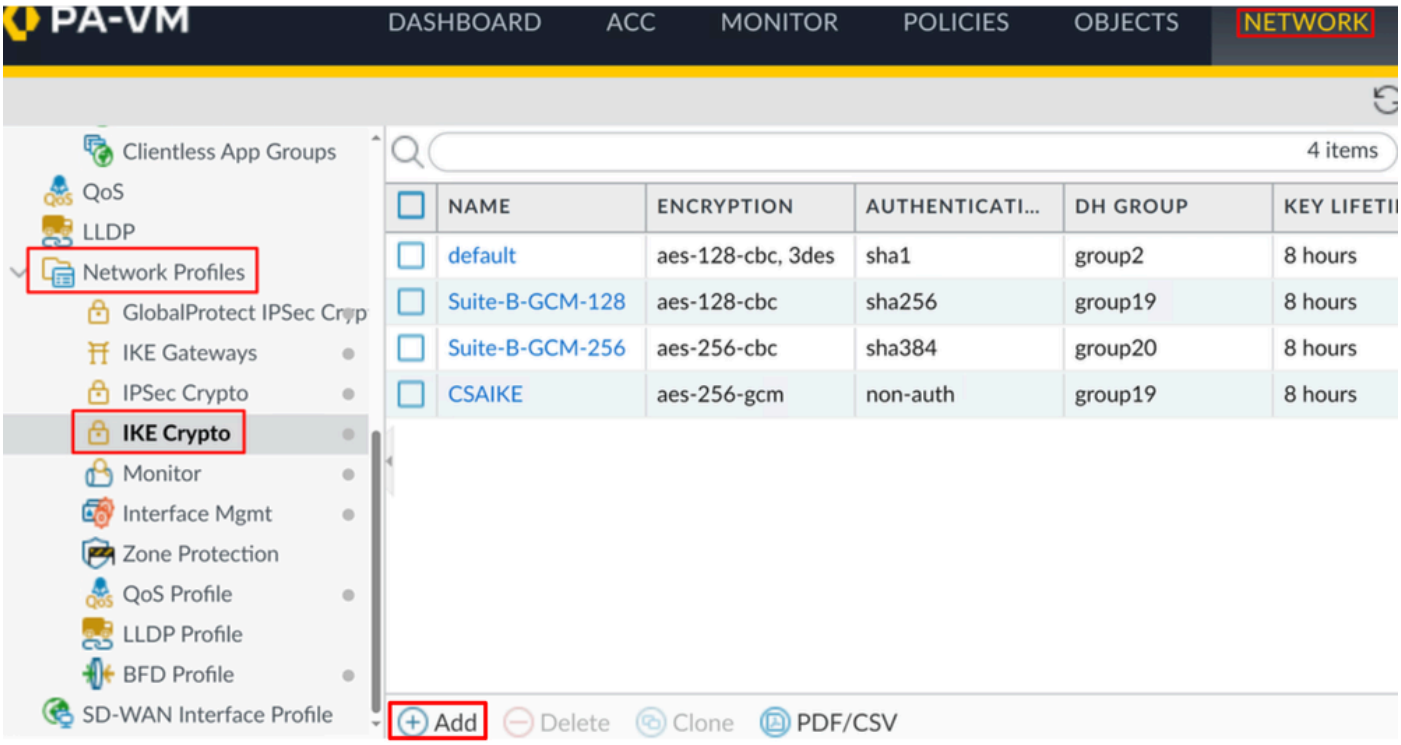


이렇게 구성한 경우 를 클릭하여 컨피그레이션**Commit** 을 저장하고 다음 단계인 를 계속 진행할 수 있습니다Configure IKE Crypto Profile.

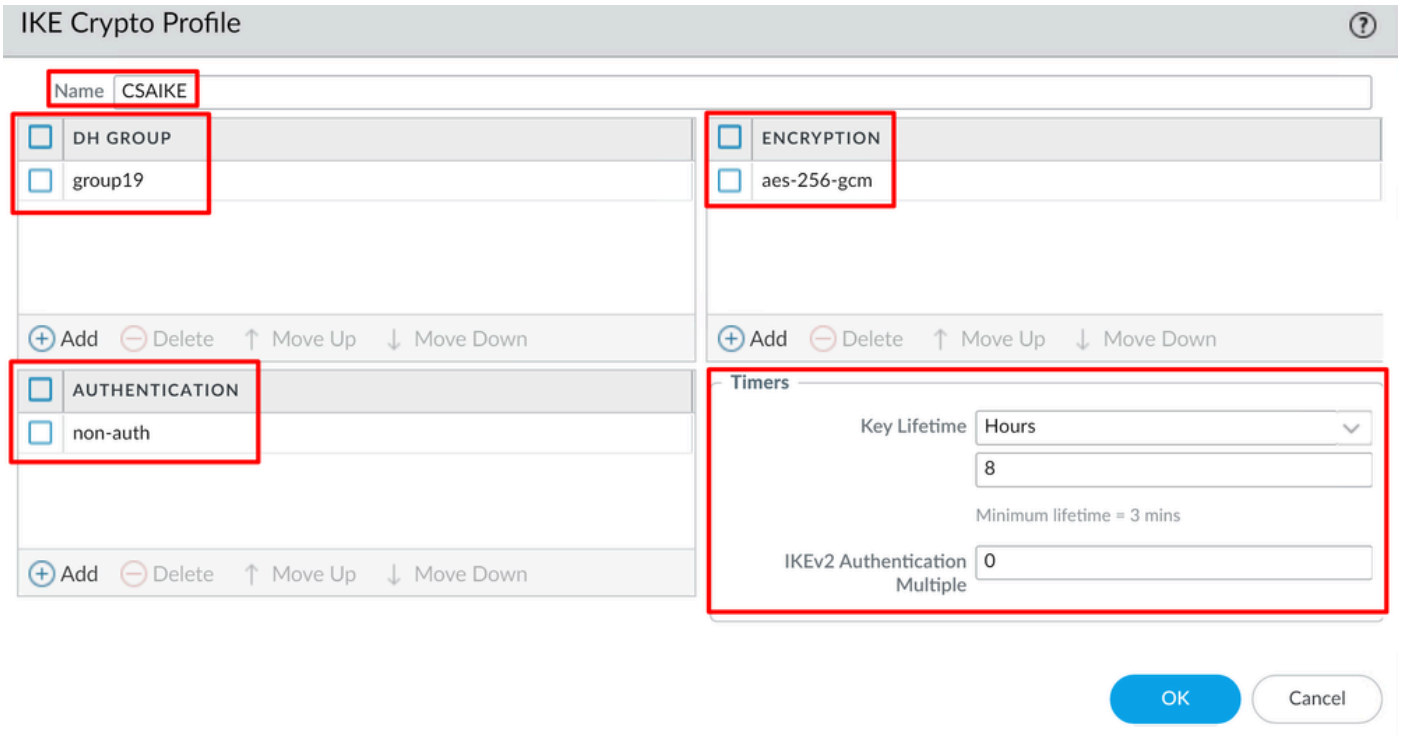
IKE 암호화 프로파일 구성

암호화 프로필을 구성하려면 다음 사이트로 이동합니다.

- Network > Network Profile > IKE Crypto
- 클릭Add



- 다음 매개변수를 구성합니다.
    - **Name**: 프로필을 식별하기 위한 이름을 구성합니다.
        - **DH GROUP**: 그룹19
        - **AUTHENTICATION**: 비 인증
        - **ENCRYPTION**: aes-256-gcm
        - Timers
            - Key Lifetime:8시간
                - **IKEv2 Authentication**:0
- 모든 항목을 구성한 후 **OK**

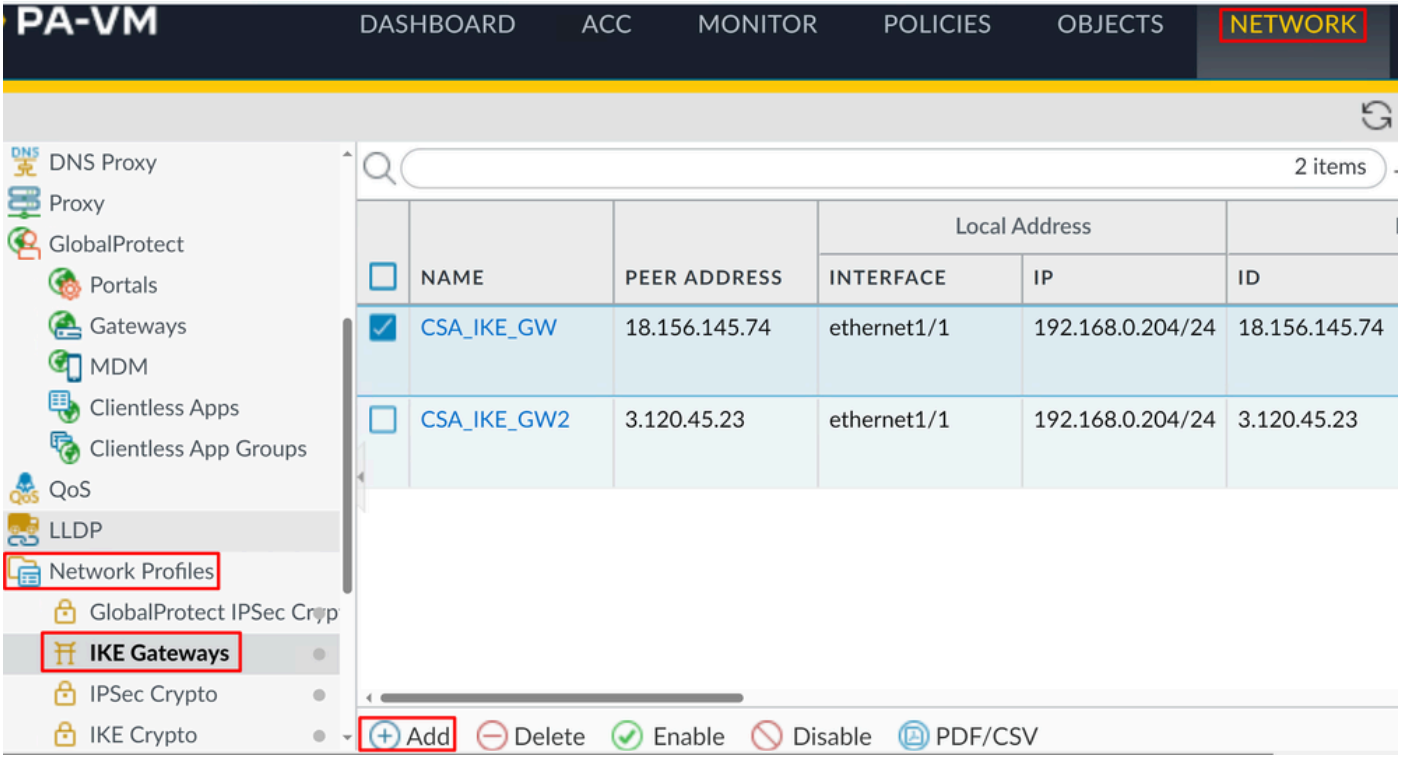


이와 같이 구성한 경우 을 클릭하여 컨피그레이션**Commit** 을 저장하고 다음 단계로 계속 진행할 수 있습니다. Configure IKE Gateways.

IKE 게이트웨이 구성

IKE 게이트웨이를 구성하려면

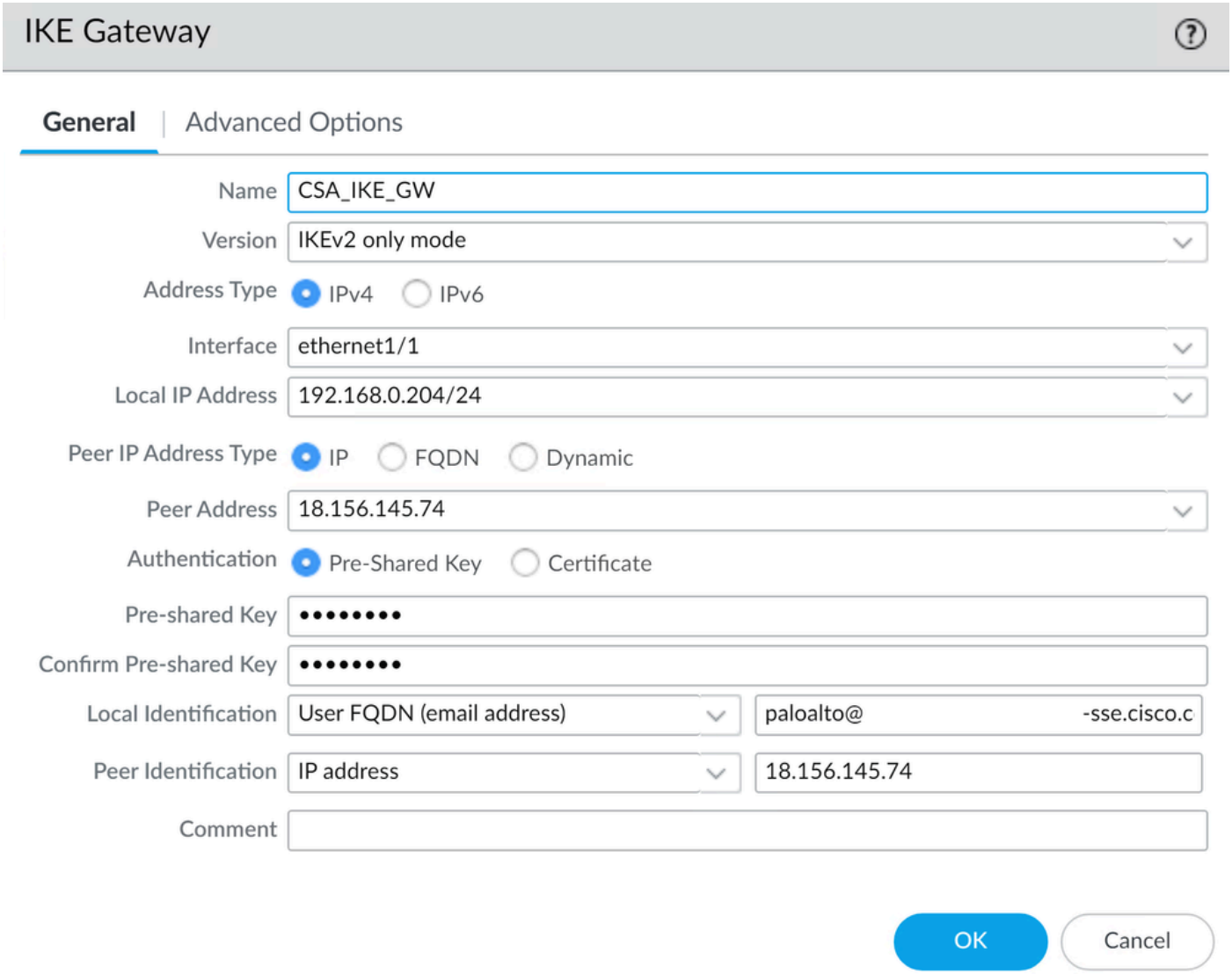
- Network > Network Profile > IKE Gateways
- 클릭Add



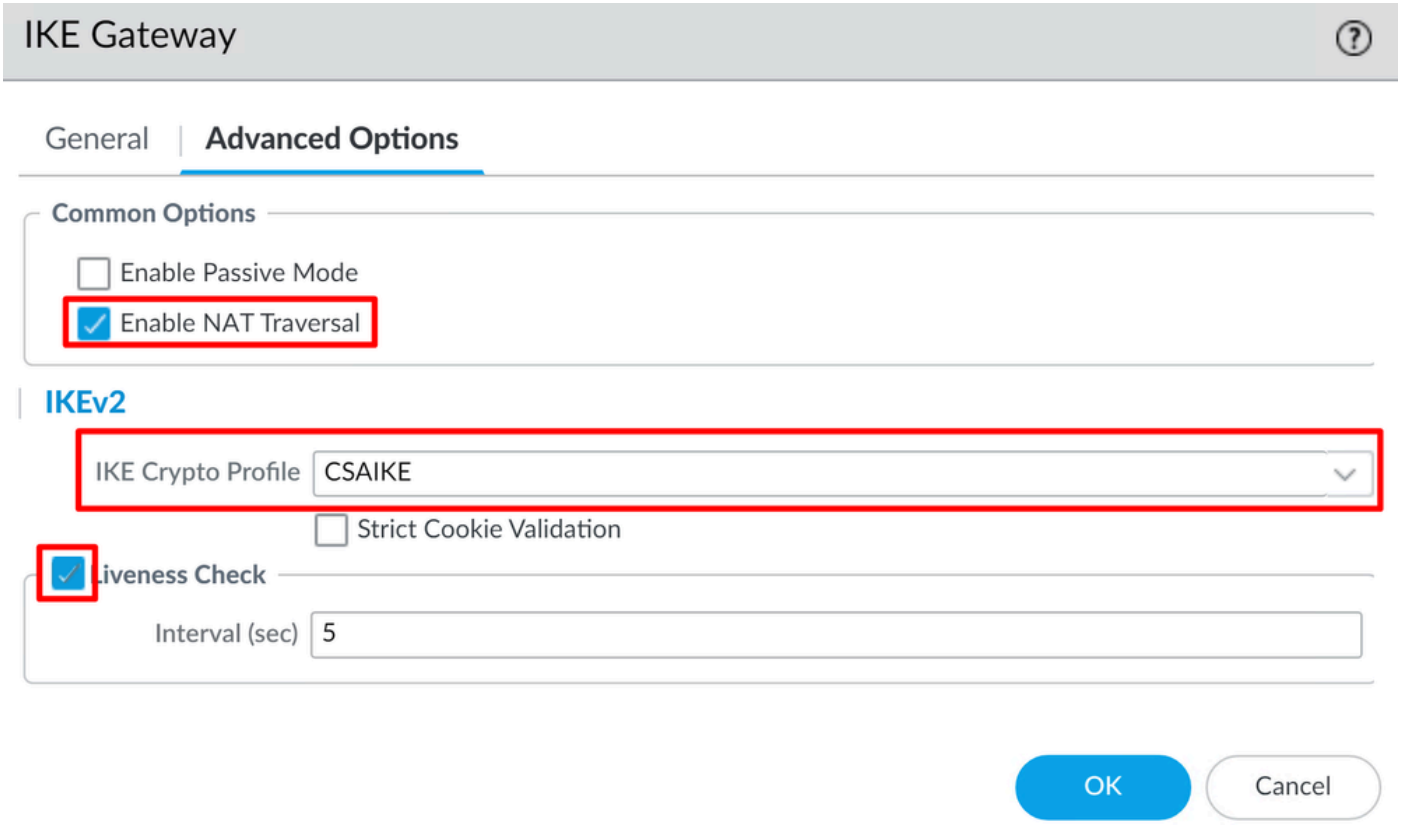
- 다음 매개변수를 구성합니다.

  - Name: Ike 게이트웨이를 식별하기 위한 이름을 구성합니다.

    - **Version** : IKEv2 전용 모드
    - Address Type : IPv4
    - **Interface** : 인터넷 WAN 인터페이스를 선택합니다.
    - Local IP Address: 인터넷 WAN 인터페이스의 IP를 선택합니다.
    - **Peer IP Address Type** :IP
    - Peer Address: 터널 데이터 단계에서 Primary IP Datacenter IP Address지정한 의 IP를 사용합니다.
    - Authentication: 사전 공유 키
    - Pre-shared Key : 터널 데이터 **passphrase** 단계에서 지정된 값을 사용합니다.
    - **Confirm Pre-shared Key** : 터널 데이터 **passphrase** 단계에서 지정된 값을 사용합니다.
    - **Local Identification** : Tunnel Data(데이터 **User FQDN (Email address)** 터널) **Primary Tunnel ID** 단계에서 지정한 항목을 선택하고 사용합니다.
    - **Peer Identification** : IP Address을 선택하고 Primary IP Datacenter IP Address사용합니다.



- 클릭Advanced Options
    - **Enable NAT Traversal**
        - Configure **IKE Crypto Profile** IKE Crypto Profile(IKE 암호화 프로파일 구성) 단계에서 생성한 를 선택합니다
        - 확인란을 선택합니다. **Liveness Check**
        - 클릭 **OK**

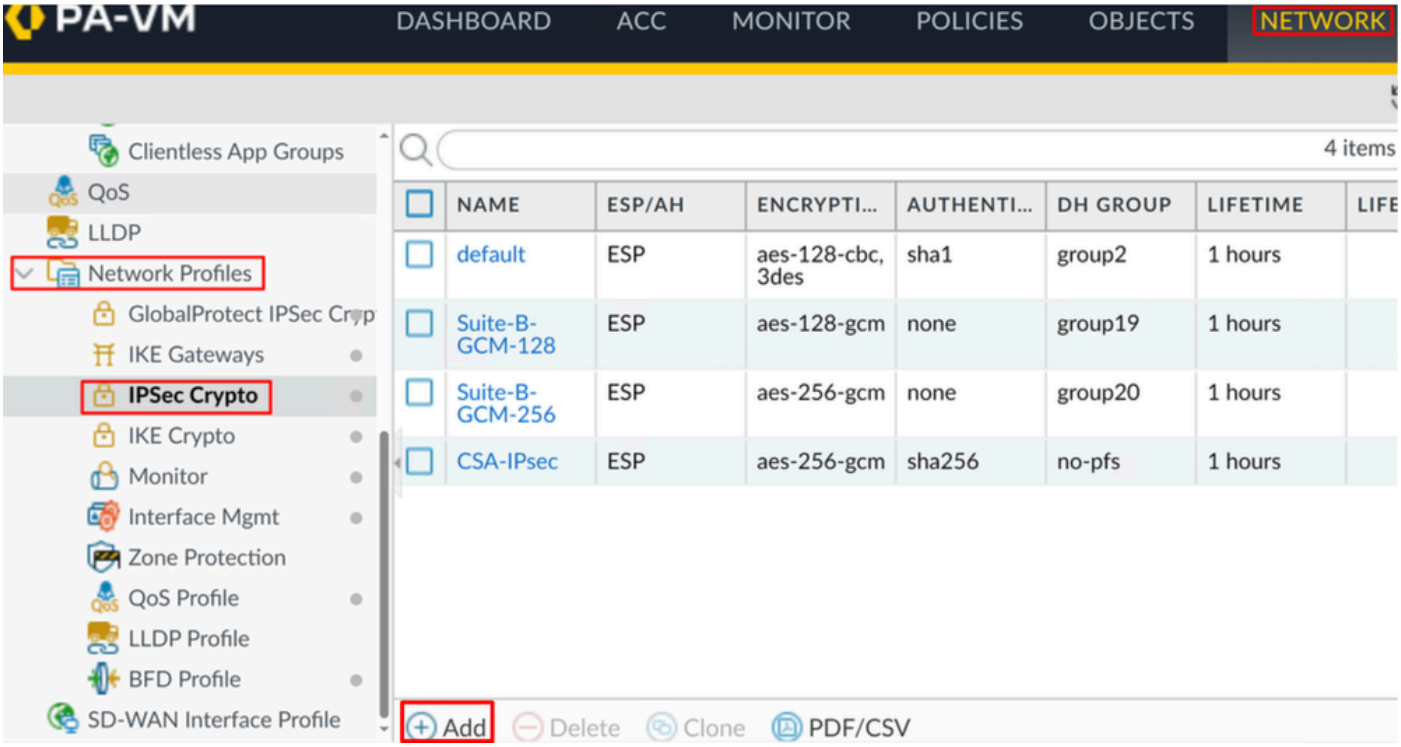


이와 같이 구성한 경우 을 클릭하여 컨피그레이션**Commit** 을 저장하고 다음 단계로 계속 진행할 수 있습니다. Configure IPSEC Crypto.

IPSEC 암호화 프로파일 구성

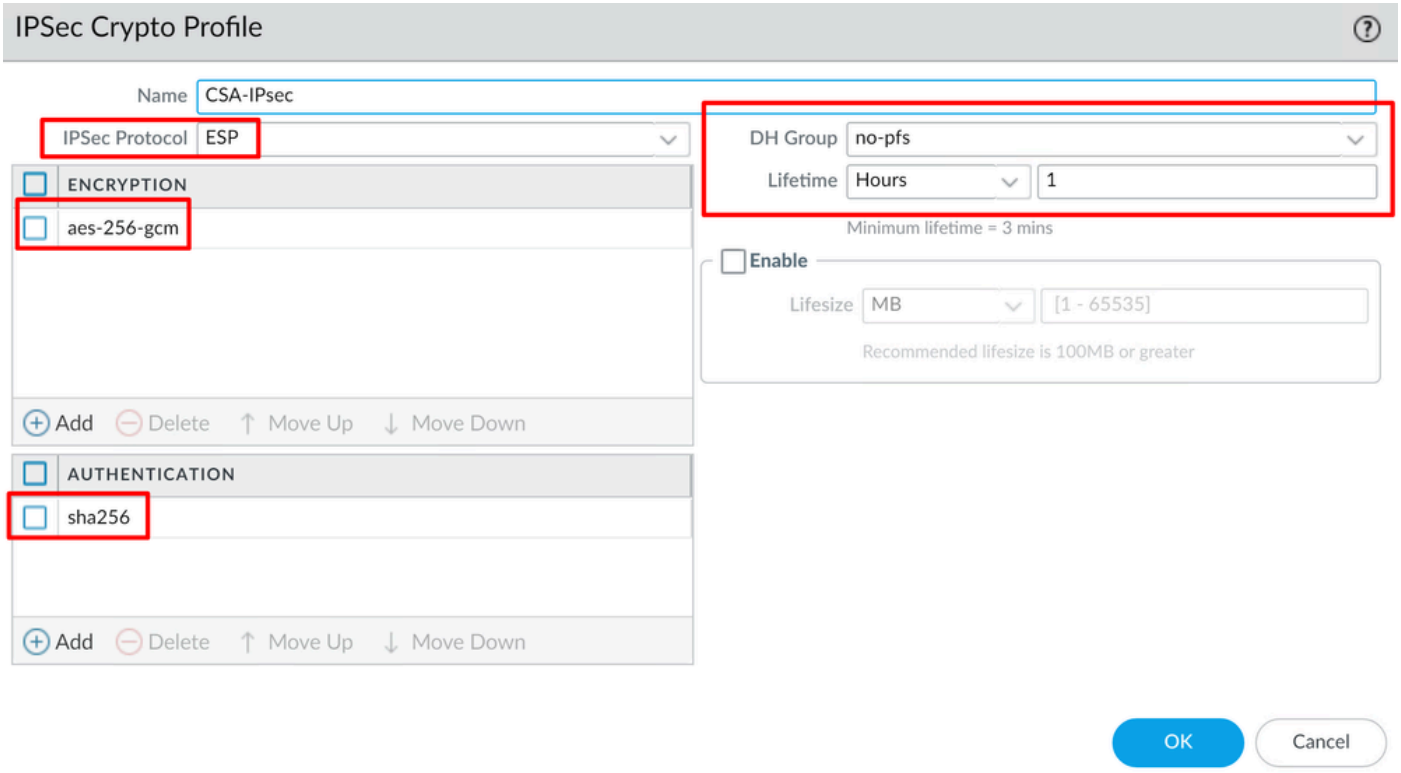
IKE 게이트웨이를 구성하려면 Network > Network Profile > IPSEC Crypto

- 클릭Add



- 다음 매개변수를 구성합니다.
  - **Name**: 이름을 사용하여 보안 액세스 IPsec 프로필을 식별합니다.
    - IPSec Protocol: ESP
    - **ENCRYPTION**: aes-256-gcm
    - DH Group: no-pfs, 1시간

- 클릭 OK

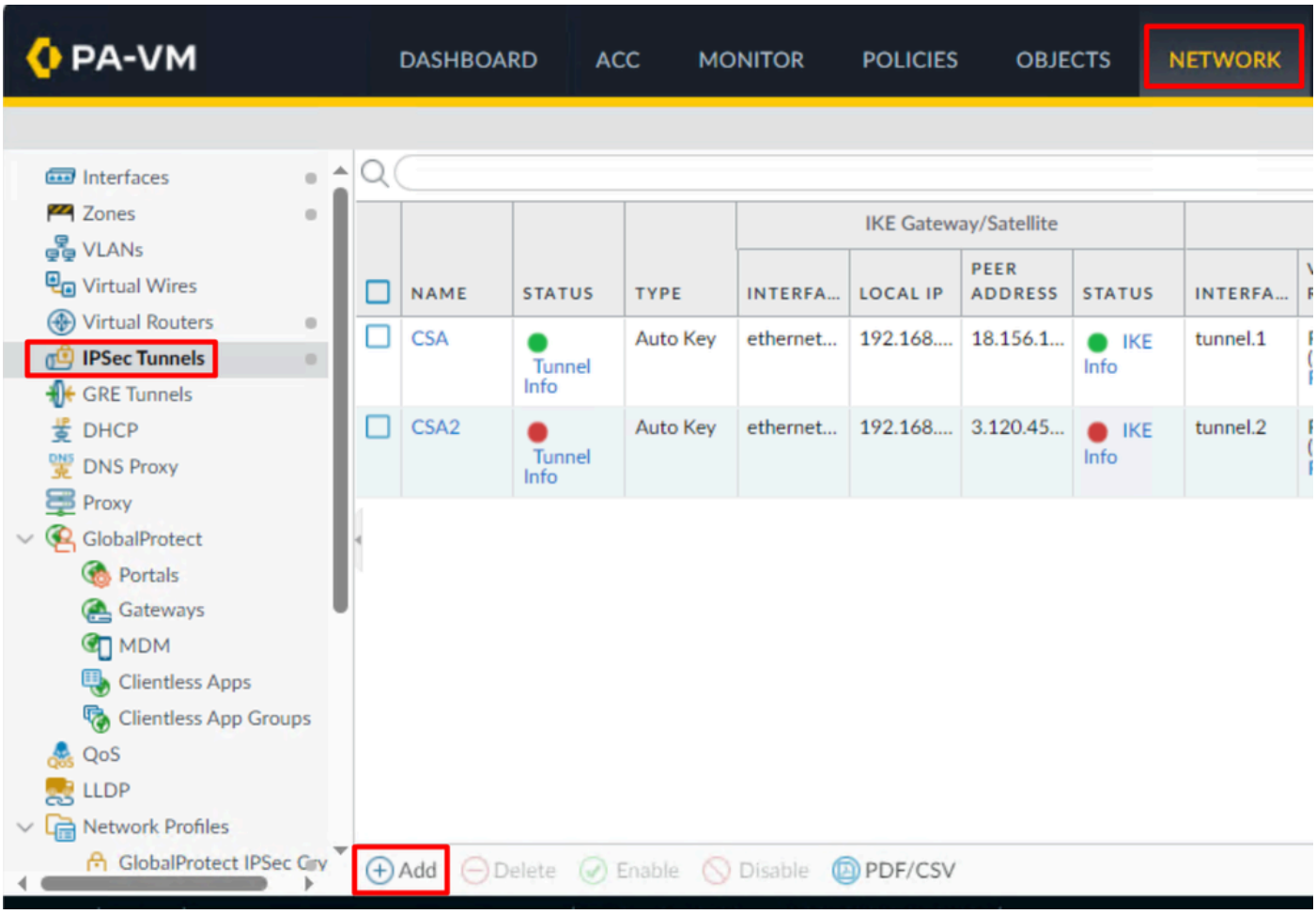


이와 같이 구성한 경우 을 클릭하여 컨피그레이션**Commit** 을 저장하고 다음 단계로 계속 진행할 수 있습니다. Configure IPSec Tunnels.

IPSec 터널 구성

구성하려면 **IPSec Tunnels**로 이동합니다Network > IPSec Tunnels.

- 클릭 Add



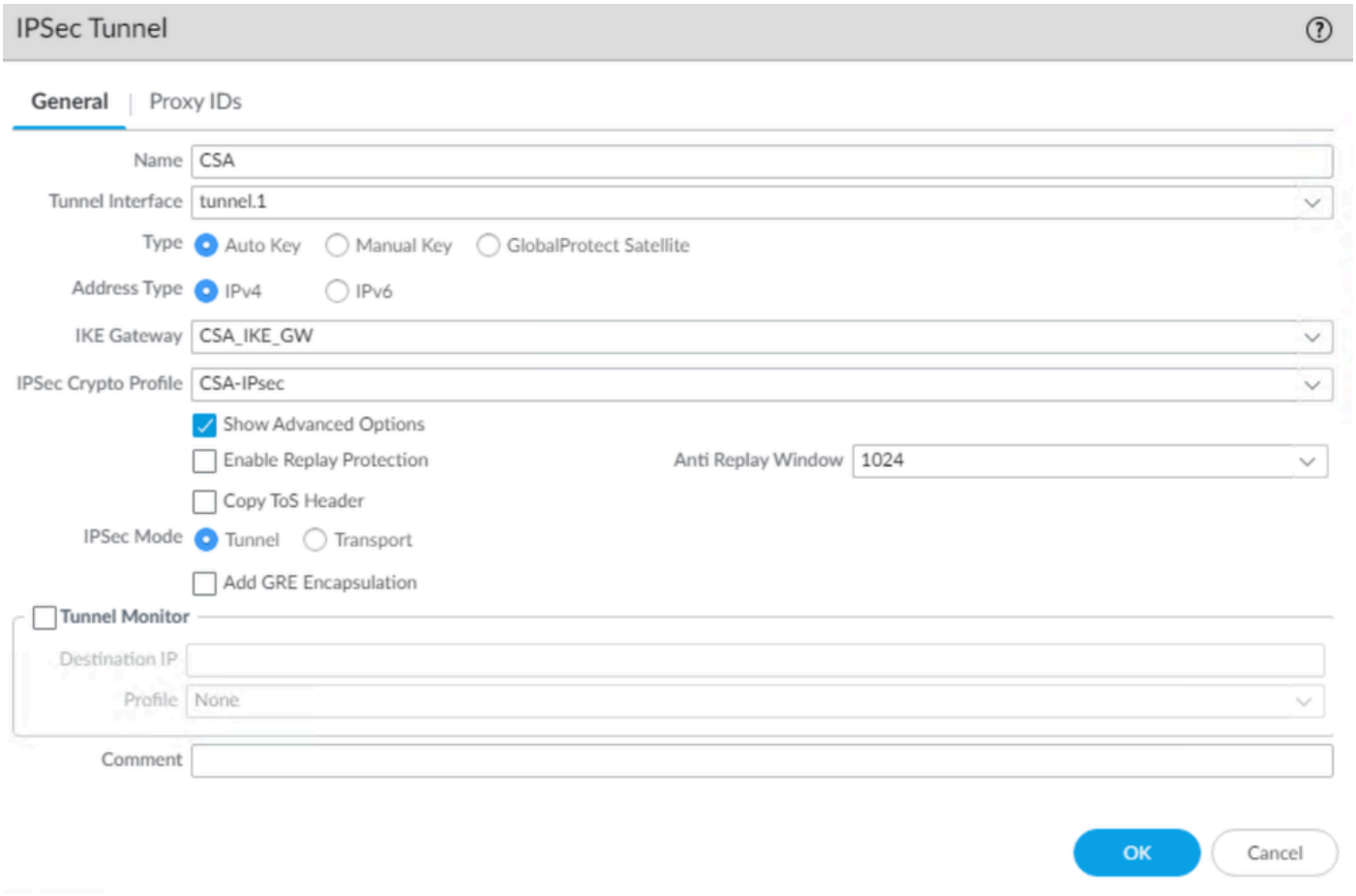
- 다음 매개변수를 구성합니다.

  - **Name**: 이름을 사용하여 보안 액세스 터널을 식별합니다.

    - **Tunnel Interface**: 단계에서 구성된 터널 인터페이스, 터널 인터페이스 구성을 선택합니다.
    - **Type**: 자동 키
    - **Address Type**: IPv4
    - **IKE Gateways**: 단계에서 구성된 IKE 게이트웨이, IKE 게이트웨이 구성을 선택합니다.
    - **IPsec Crypto Profile**: 단계에서 구성된 IKE 게이트웨이, IPSEC 암호화 프로파일 구성을 선택합니다
    - 확인란을 선택합니다. **Advanced Options**

      - **IPSec Mode Tunnel**: 터널을 선택합니다.

- 클릭 OK

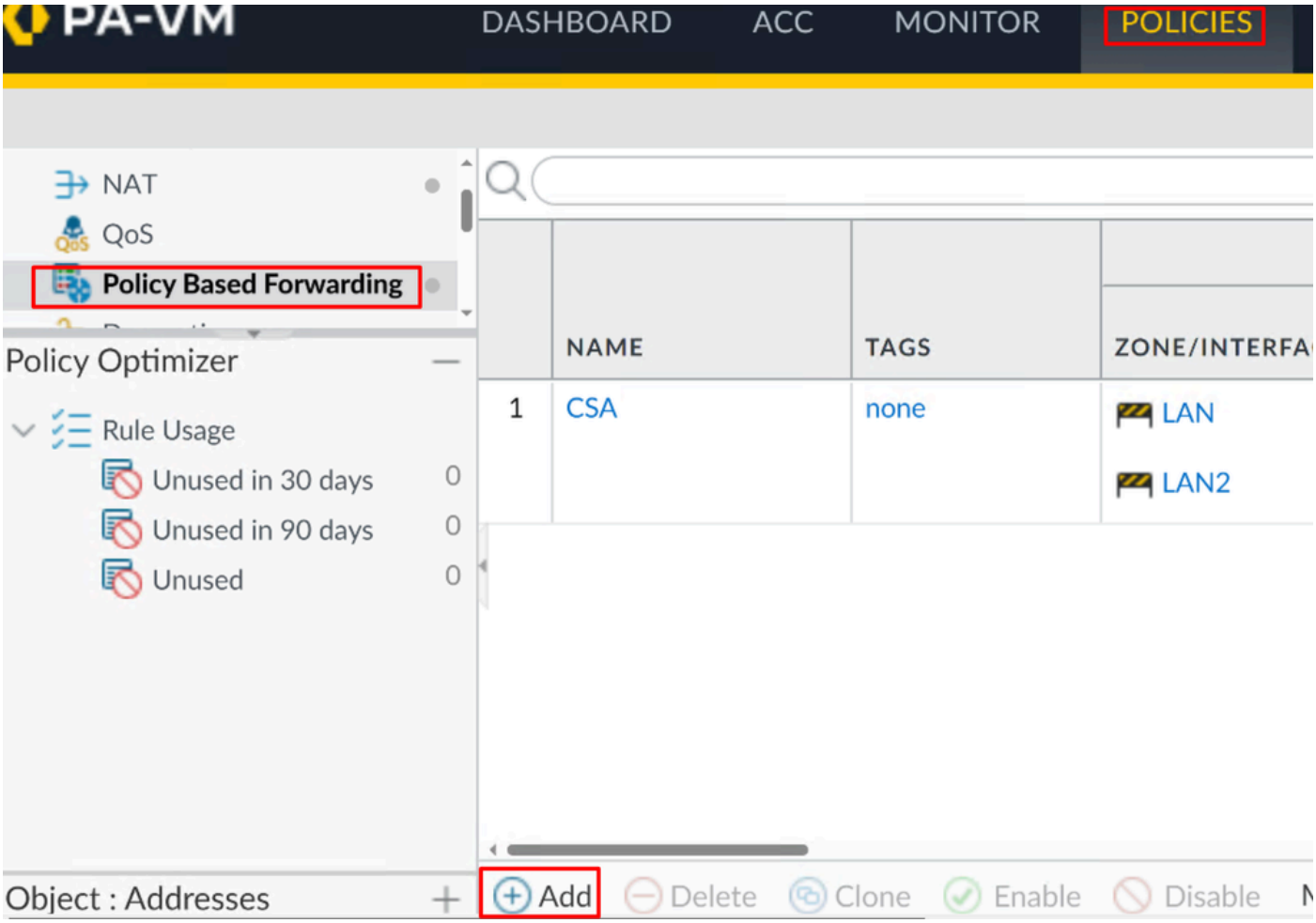


이제 VPN이 성공적으로 생성되었으므로, 단계를 진행할 수 있습니다 **Configure Policy Based Forwarding**.

정책 기반 전달 구성

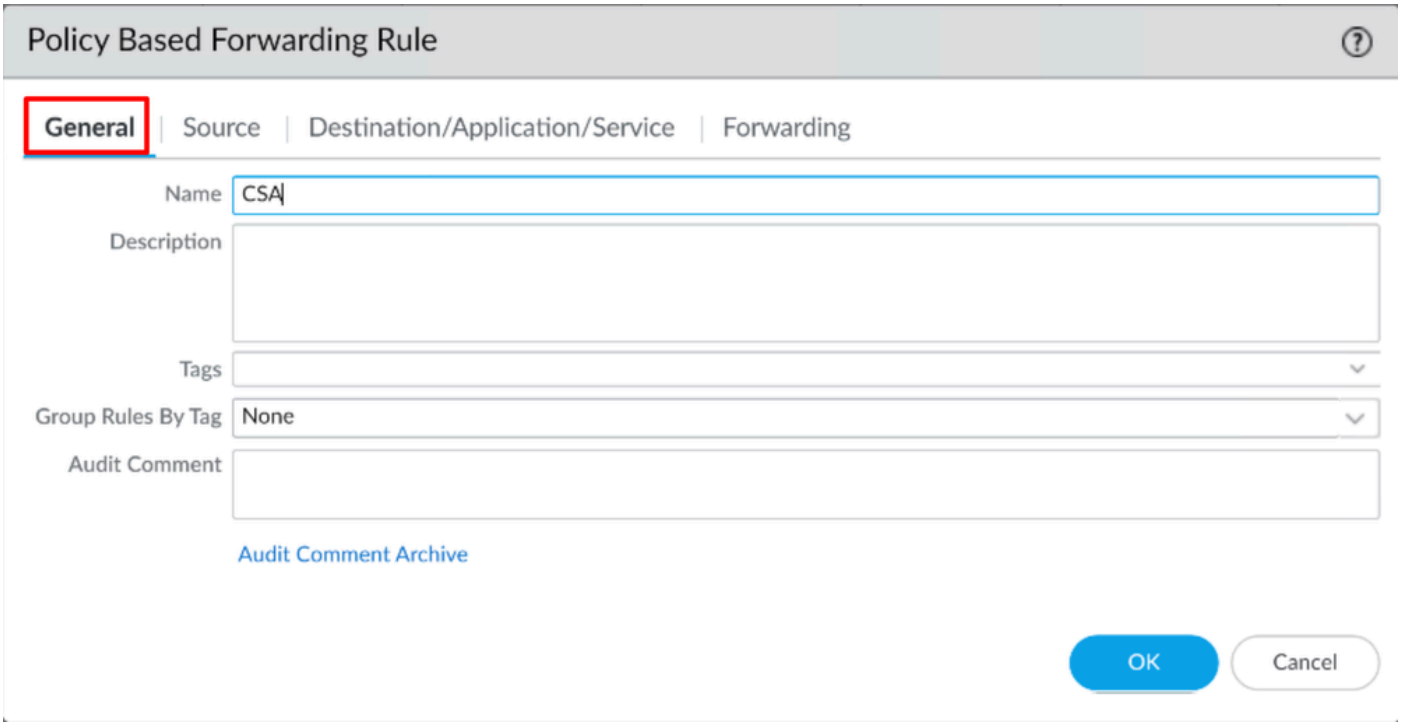
구성하려면 다음 **Policy Based Forwarding**으로 이동하십시오. Policies > Policy Based Forwarding.

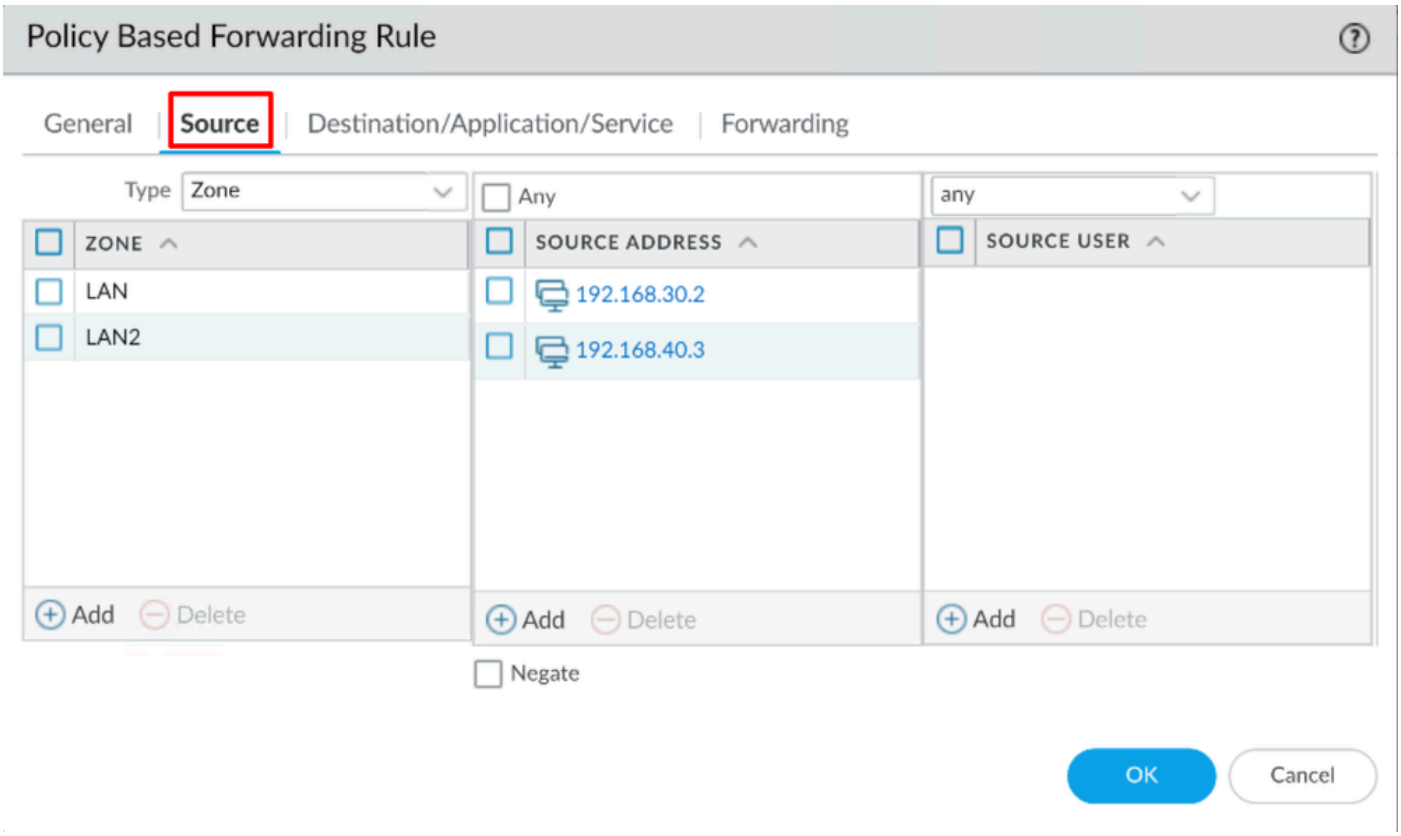
- 클릭 Add

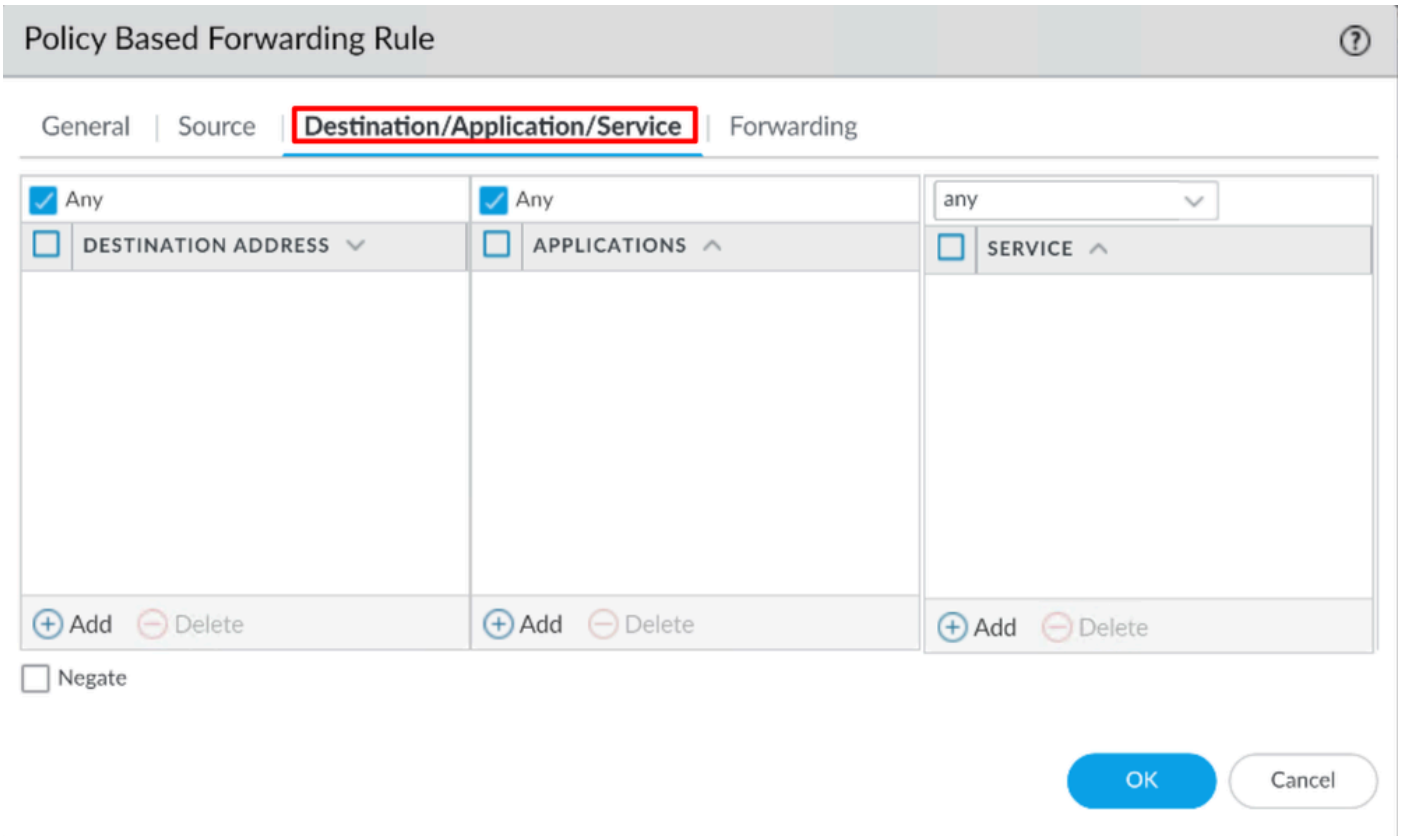


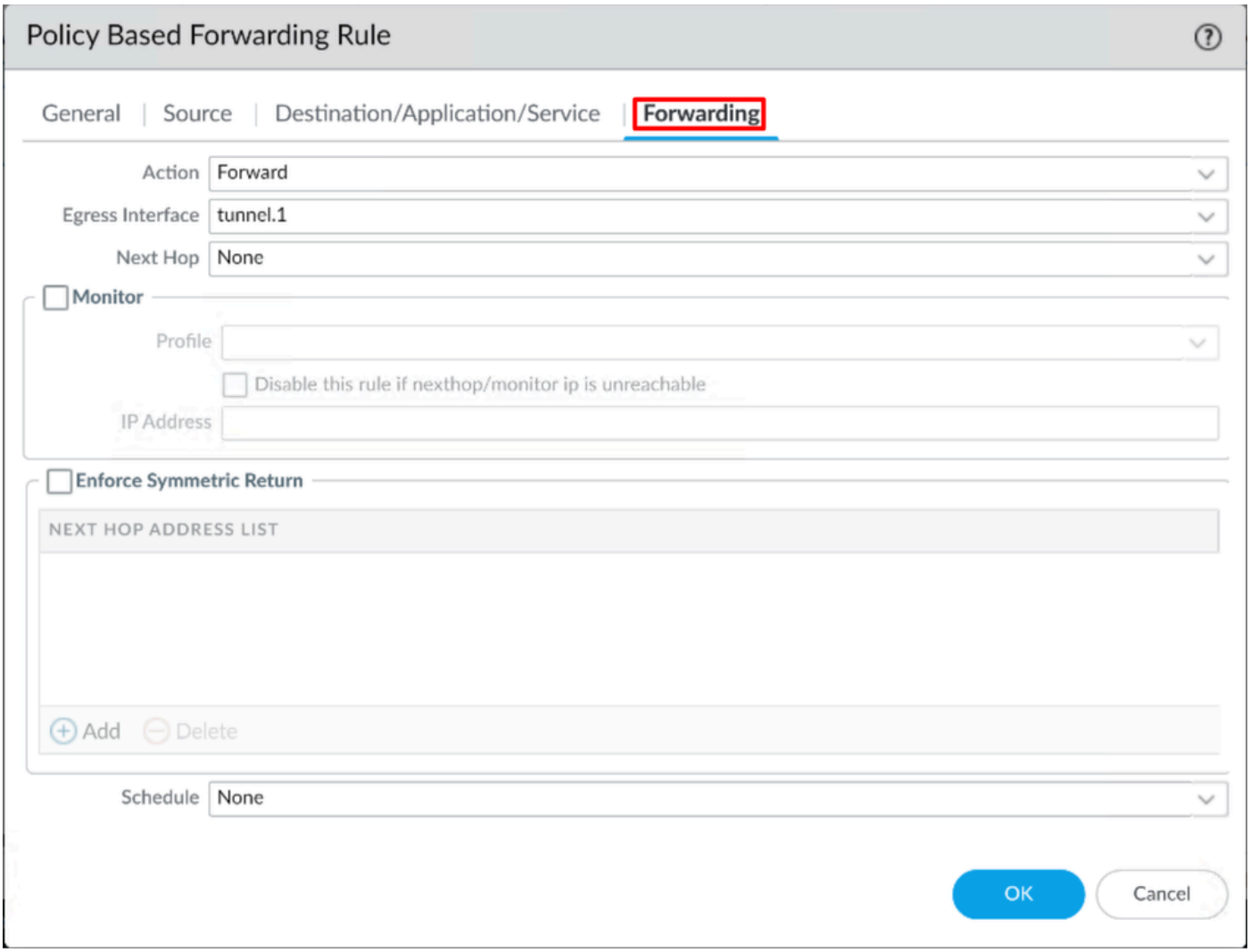
- 다음 매개변수를 구성합니다.
  - General
    - **Name**: 이름을 사용하여 보안 액세스, 정책 기반 전달(발신지별 라우팅)을 식별합니다.
- Source
  - **Zone**: 출발지를 기준으로 트래픽을 라우팅할 계획이 있는 Zones를 선택합니다
    - **Source Address**: 소스로 사용할 호스트를 구성합니다.
    - Source Users: 트래픽을 라우팅할 사용자를 구성합니다(해당되는 경우에만).

- Destination/Application/Service
    - Destination Address: Any로 남겨두거나 Secure Access(100.64.0.0/10)의 주소 범위를 지정할 수 있습니다.
- Forwarding
    - **Action**: 앞으로
        - **Egress Interface**: 단계에서 구성된 터널 인터페이스, 터널 인터페이스 구성을 선택합니다.
        - **Next Hop**:None
- 클릭OK 및 Commit




Policy Based Forwarding Rule
General
Source
Destination/Application/Service
Forwarding
Type
Zone
Any
any
ZONE
SOURCE ADDRESS
SOURCE USER
LAN
LAN2
192.168.30.2
192.168.40.3
Add
Delete
Add
Delete
Add
Delete
Negate
OK
Cancel


Policy Based Forwarding Rule
General
Source
Destination/Application/Service
Forwarding
Any
Any
any
DESTINATION ADDRESS
APPLICATIONS
SERVICE
Add
Delete
Add
Delete
Add
Delete
Negate
OK
Cancel



이제 모든 것이 Palo Alto에 구성되어 있습니다. 경로를 구성한 후 터널을 설정할 수 있으며, Secure Access Dashboard에서 RA-VPN, 브라우저 기반 ZTA 또는 클라이언트 기반 ZTA를 계속 구성해야 합니다.

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.