Fortigate 방화벽으로 보안 액세스 구성

목차

소개

이 문서에서는 Fortigate 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.

- Fortigate 7.4.x 버전 방화벽
- 보안 액세스
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- 클라이언트리스 ZTNA

사용되는 구성 요소

이 문서의 정보는 다음을 기반으로 합니다.

- Fortigate 7.4.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.

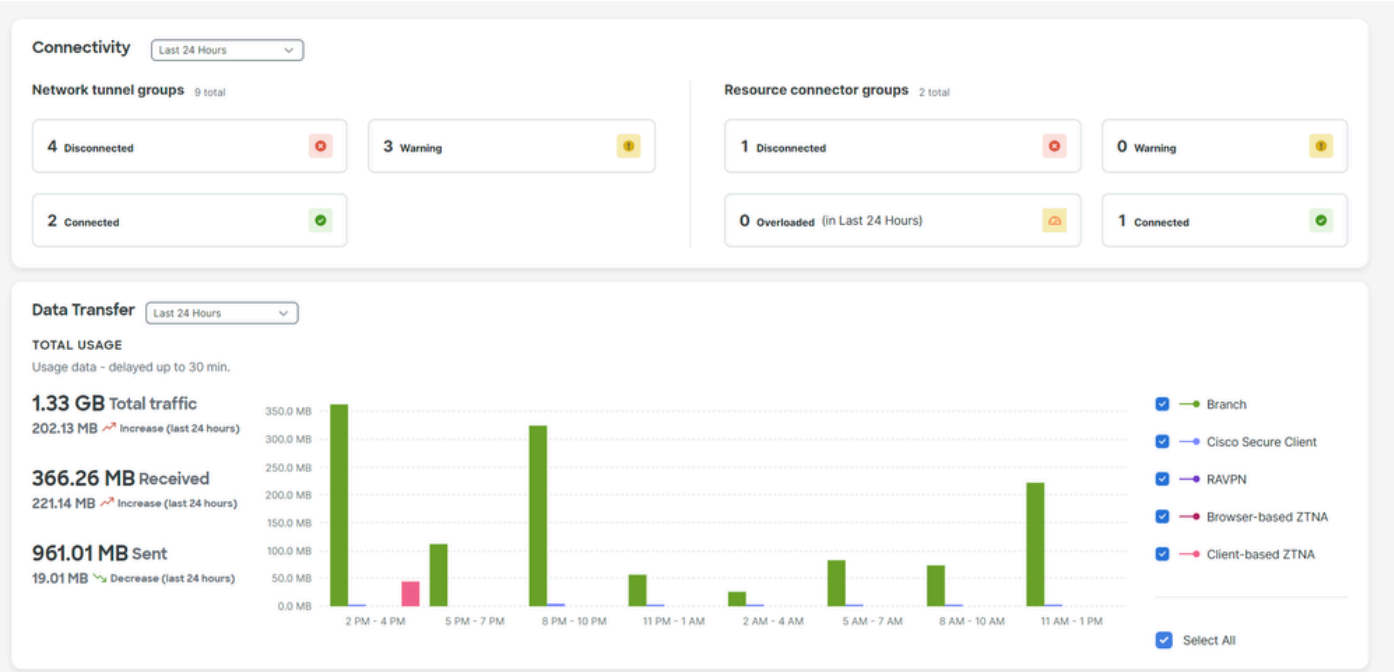
배경 정보

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.

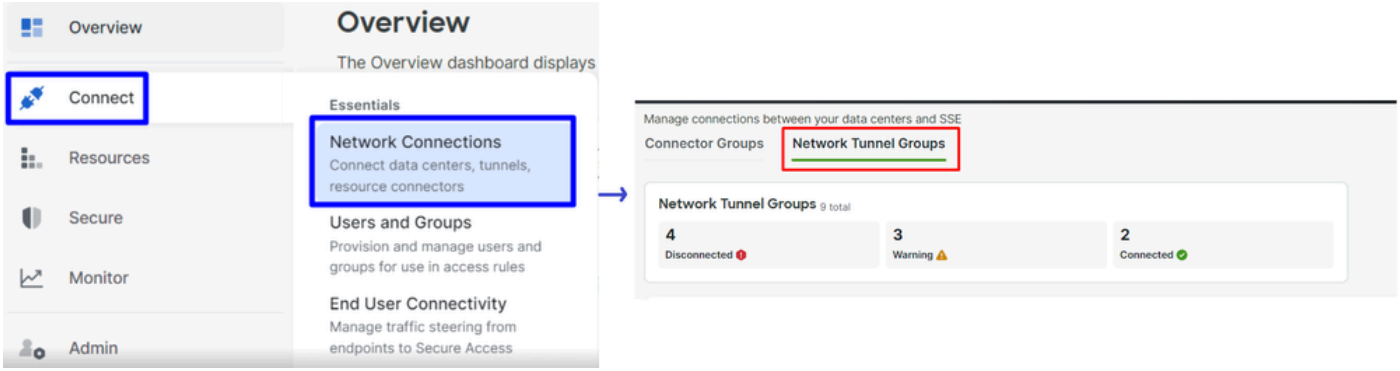
구성

보안 액세스에서 VPN 구성

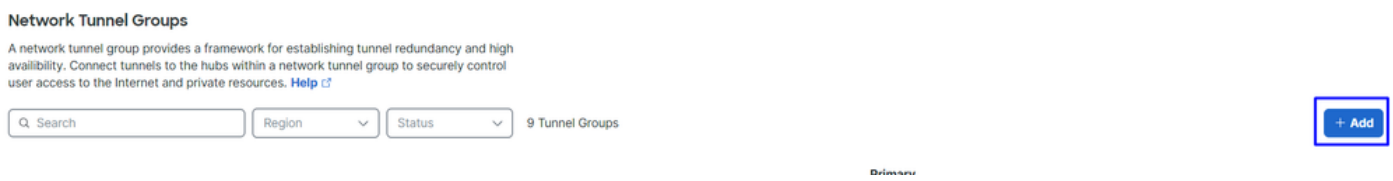
Secure Access의 관리자 패널로 이동합니다.



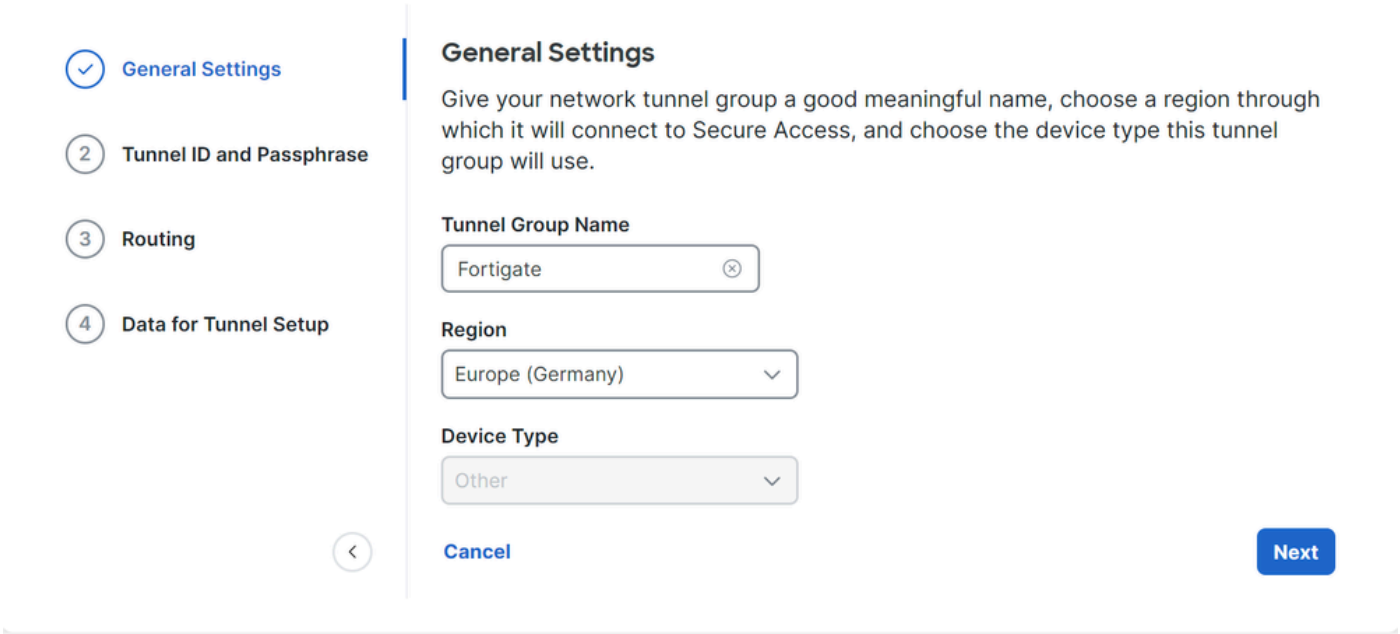
- 클릭 Connect > Network Connections > Network Tunnels Groups

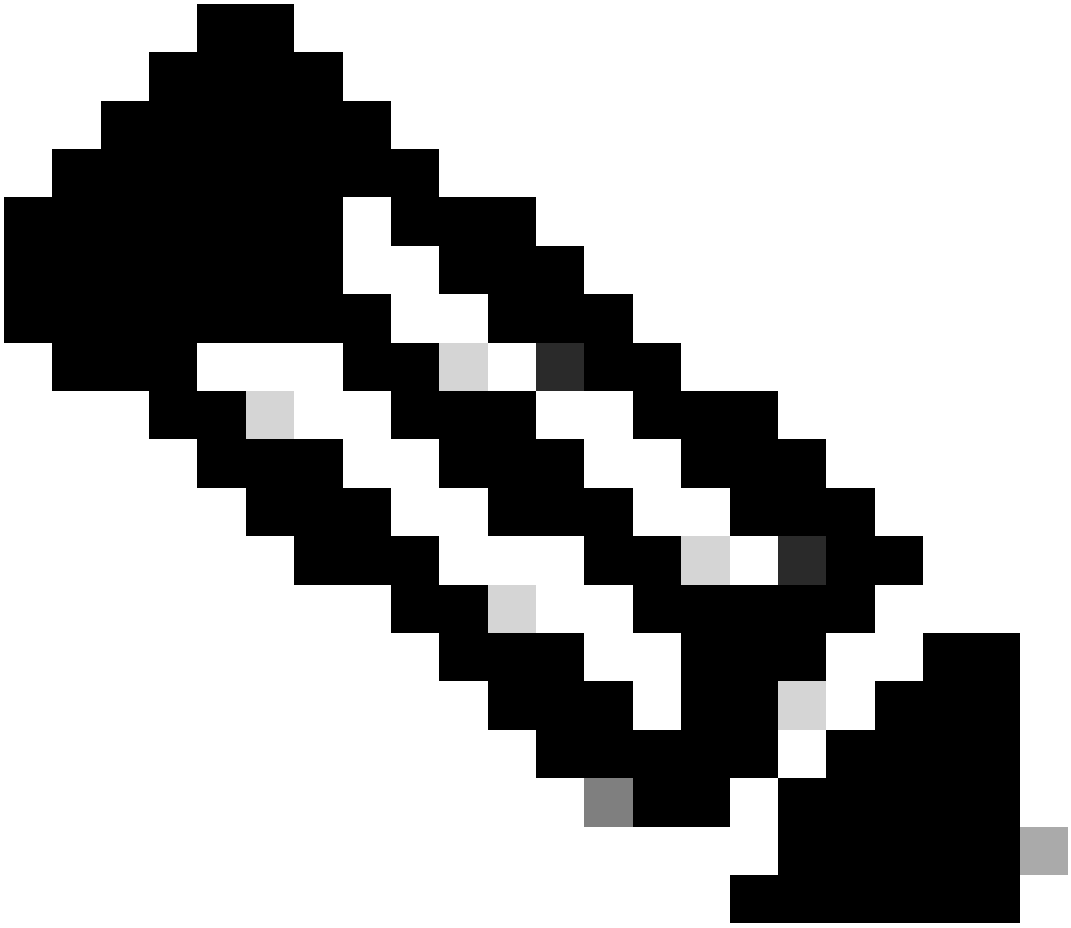


- 에서 Network Tunnel Groups 클릭 + Add



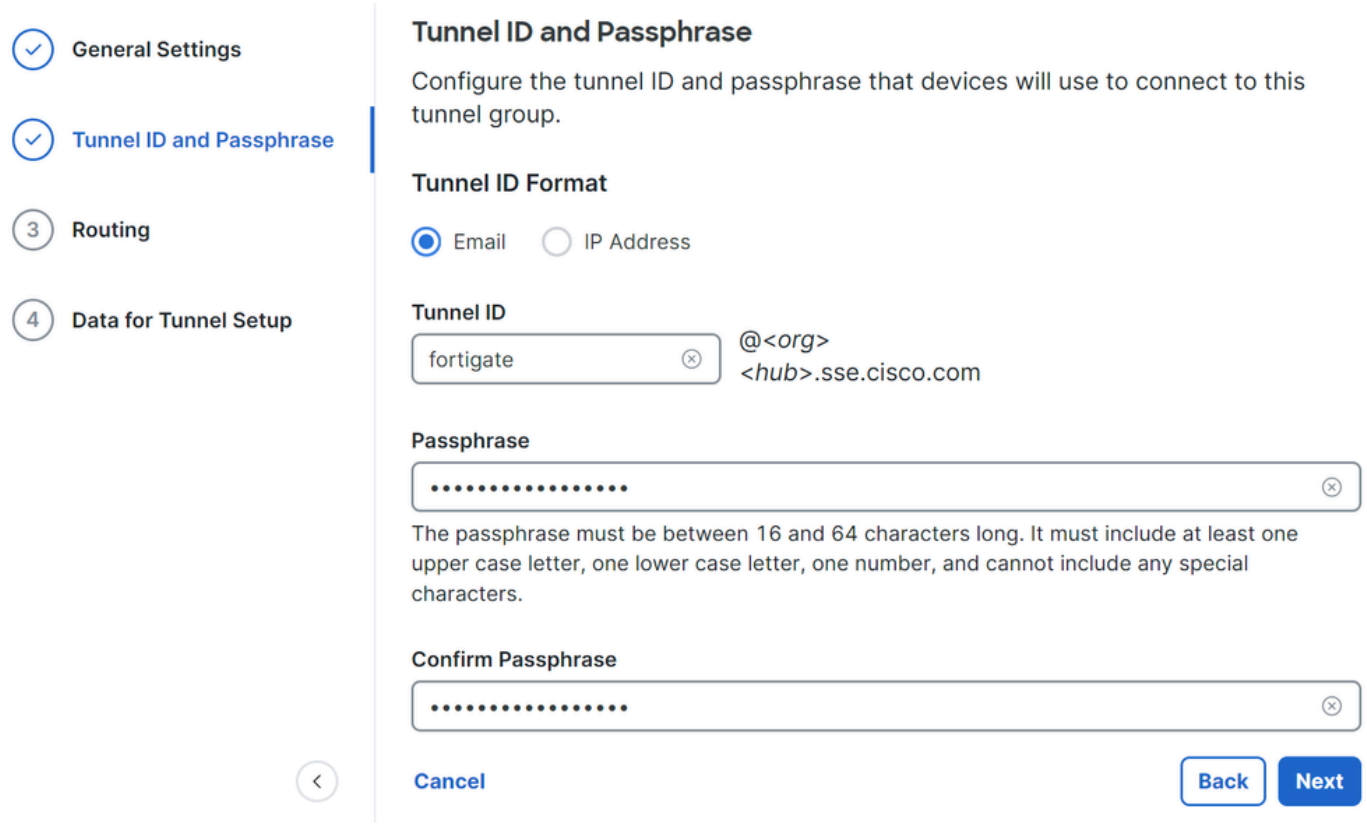
- 구성Tunnel Group Name, Region 및 Device Type
- 클릭 **Next**


General Settings
2
Tunnel ID and Passphrase
3
Routing
4
Data for Tunnel Setup
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
Fortigate
Region
Europe (Germany)
Device Type
Other
Cancel
Next

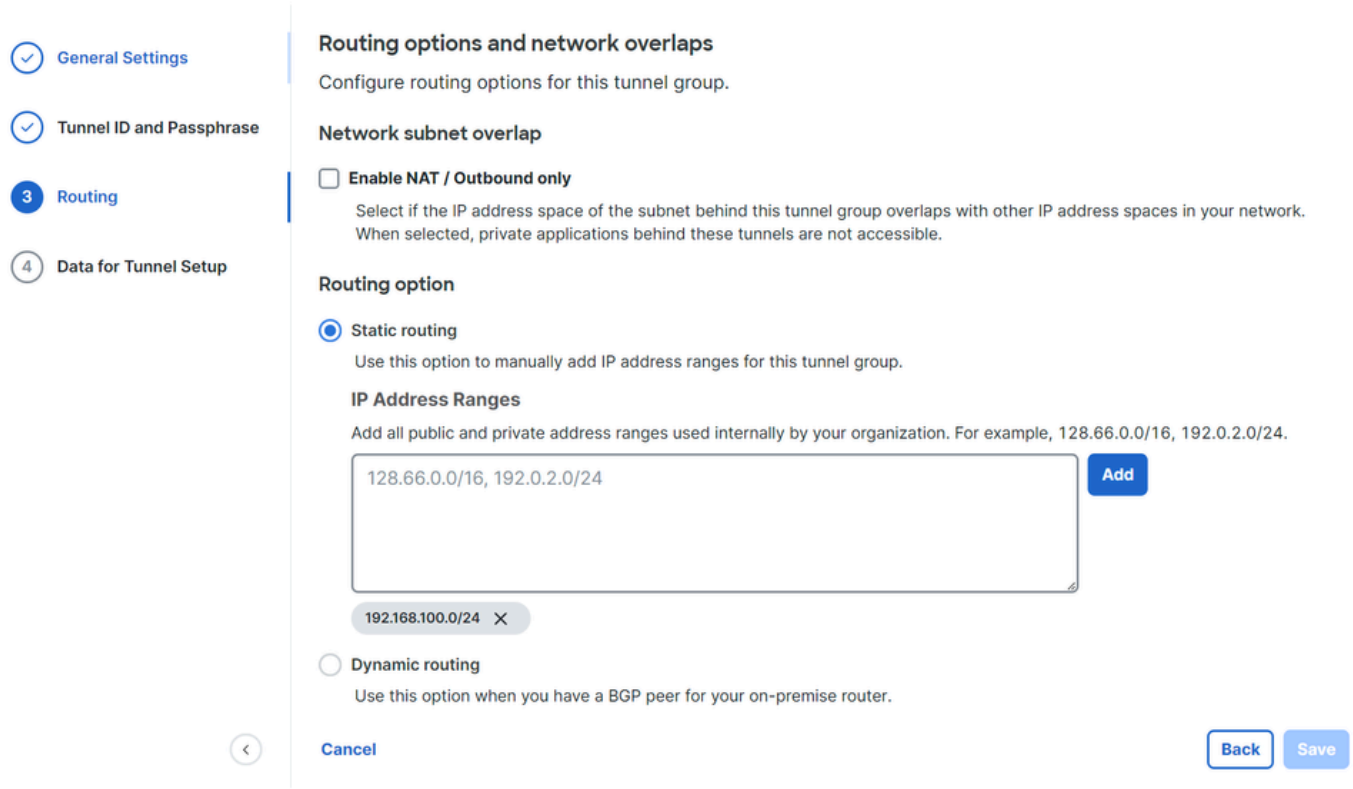


참고: 방화벽 위치에서 가장 가까운 지역을 선택합니다.

- 및 를Tunnel ID Format 구성합니다 Passphrase
- 클릭Next



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



터널에 대한 정보**Save** 가 표시되면 다음 단계를 위해 해당 정보를 저장하십시오. **Configure the VPN Site to Site on Fortigate.**

터널 데이터

Data for Tunnel Setup

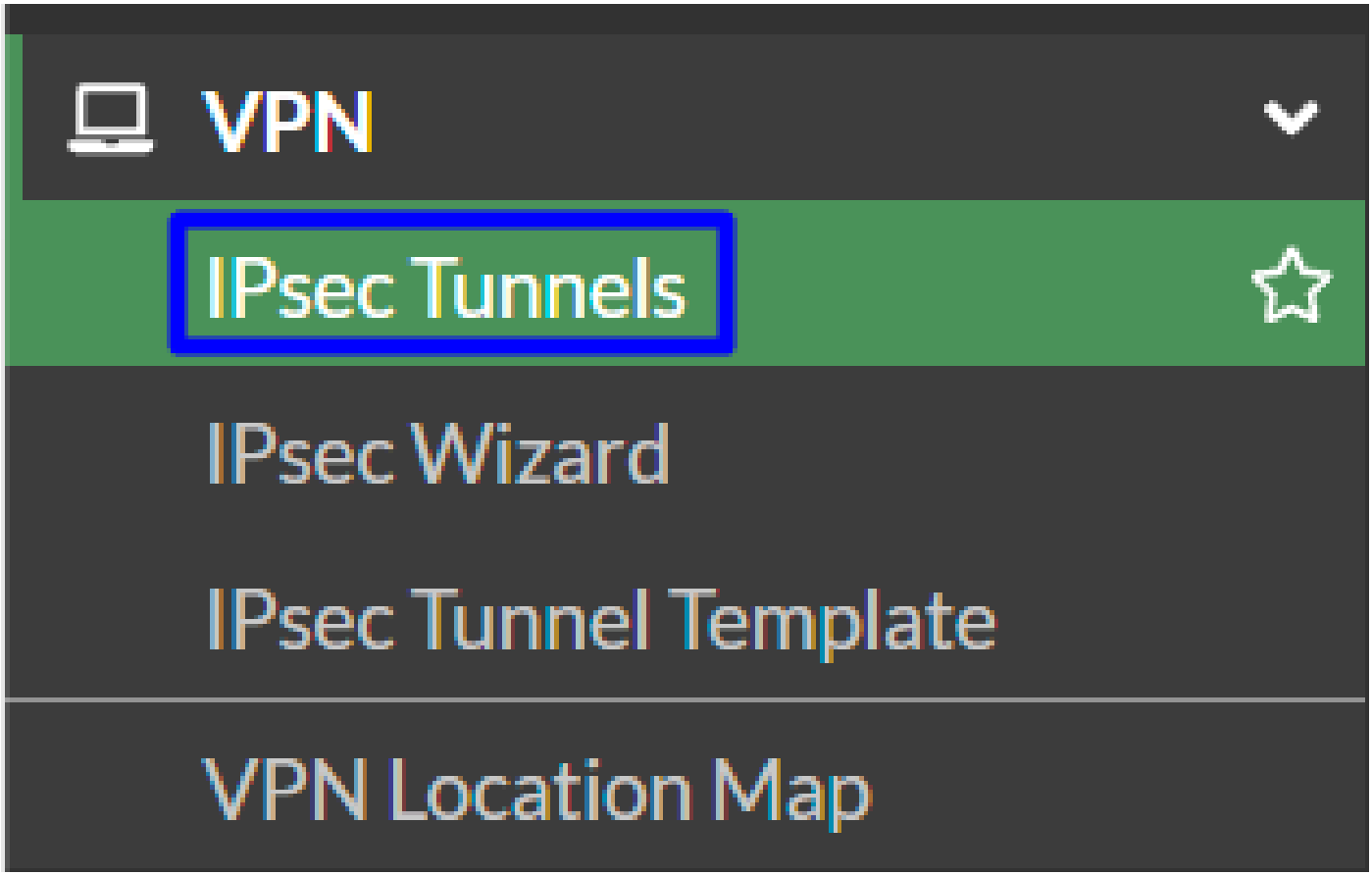
Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

Primary Tunnel ID:	@	-sse.cisco.com
Primary Data Center IP Address:	18.156.145.74	
Secondary Tunnel ID:	@	-sse.cisco.com
Secondary Data Center IP Address:	3.120.45.23	
Passphrase:		CP

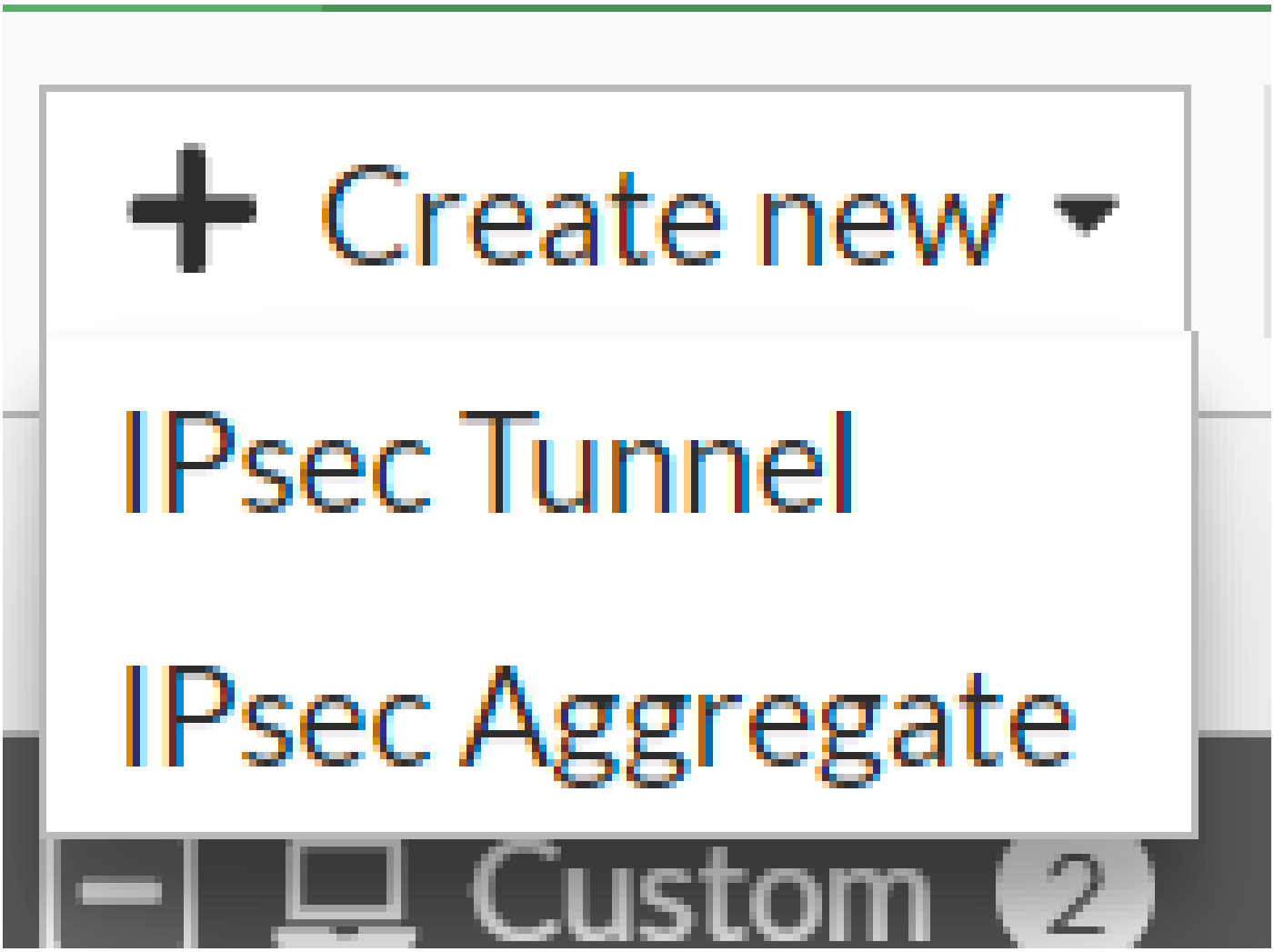
Fortigate에서 VPN 사이트 대 사이트 구성

Fortigate 대시보드로 이동합니다.

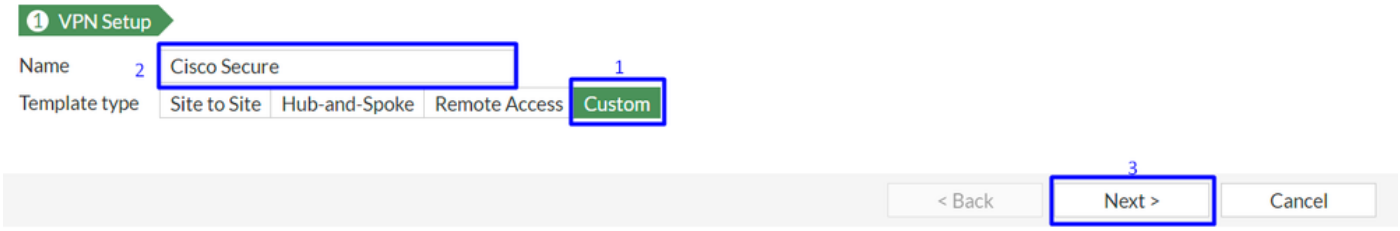
- 클릭 VPN > IPsec Tunnels



- 클릭 Create New > IPsec Tunnels

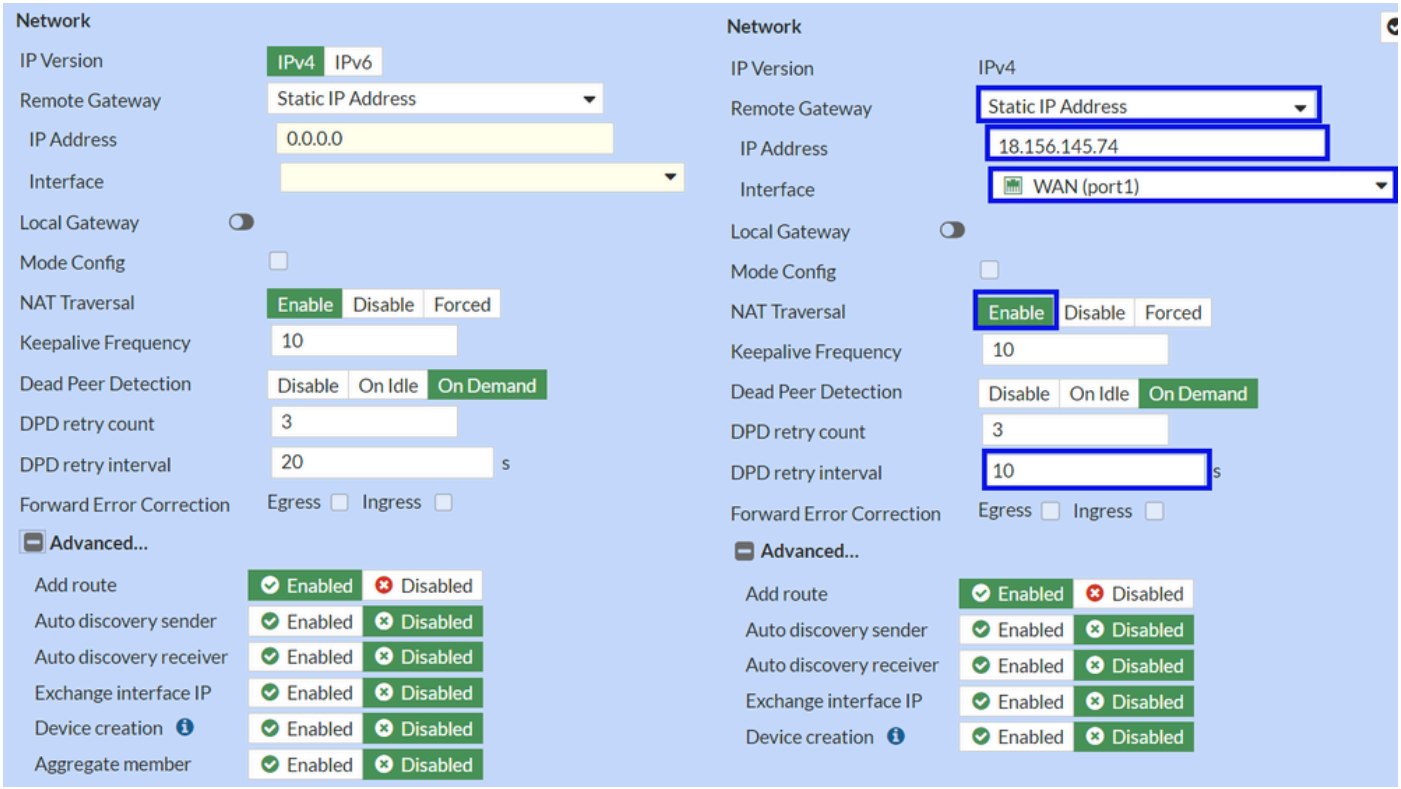


- 를 Custom 클릭하고 을 **Name** 구성한 다음 을 **Next**클릭합니다.



다음 그림에서는 부품에 대한 설정을 구성하는 방법을 **Network** 보여줍니다.

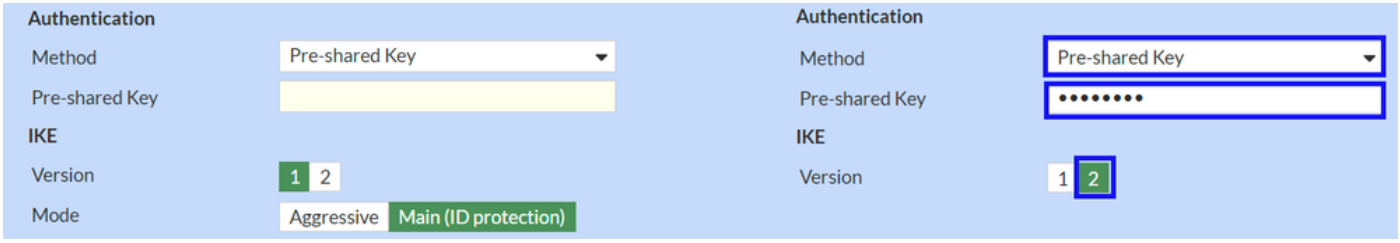
네트워크



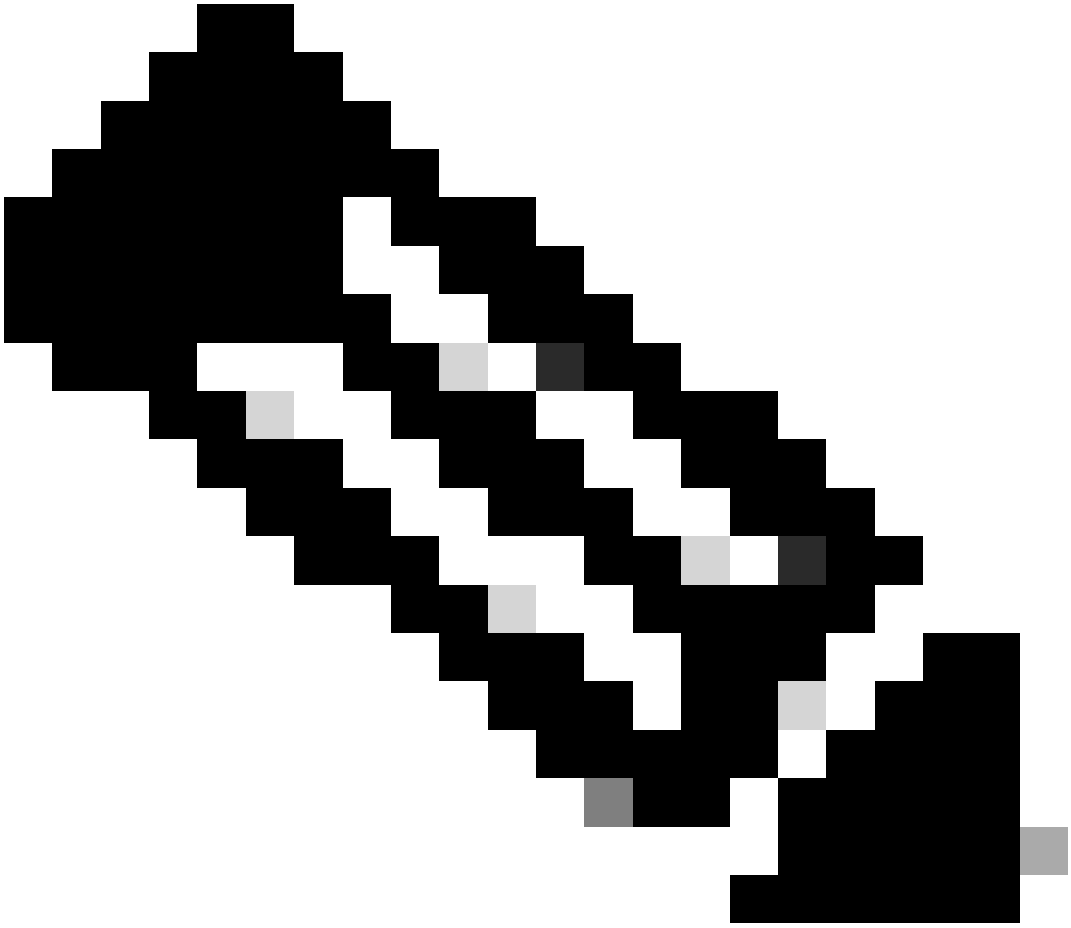
- Network
    - IP Version : IPv4
        - **Remote Gateway** :고정 IP 주소
        - IP Address: 터널 데이터 단계에서 Primary IP Datacenter IP Address,지정된 IP 사용
        - **Interface** : 터널을 설정하기 위해 사용하려는 WAN 인터페이스를 선택합니다
        - **Local Gateway** : 기본값으로 사용 안 함
        - **Mode Config** : 기본값으로 사용 안 함
        - **NAT Traversal** : 사용
        - **Keepalive Frequency** :10
        - Dead Peer Detection : 온디맨드
        - **DPD retry count** :3
        - **DPD retry interval** :10
        - **Forward Error Correction** : 확인란을 선택하지 마십시오.
        - **Advanced...**: 이미지로 구성합니다.

이제 IKE를 **Authentication**구성합니다.

인증



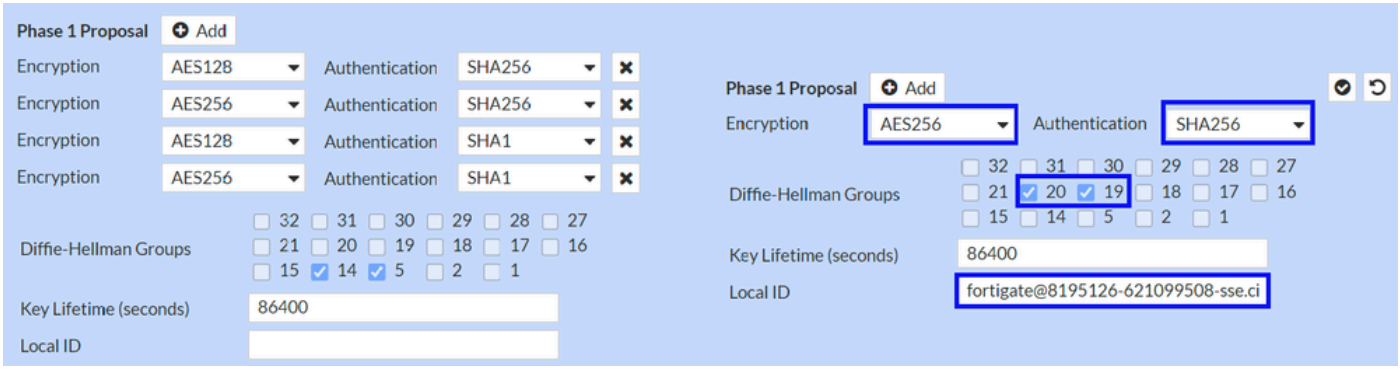
- **Authentication**
  - **Method** : 사전 공유 키를 기본값으로
    - **Pre-shared Key** : 터널 데이터 **Passphrase**단계에서 지정된 데이터 사용
- **IKE**
  - Version : 버전 2를 선택합니다.



참고: 보안 액세스는 IKEv2만 지원합니다

이제 를 **Phase 1 Proposal**구성합니다.

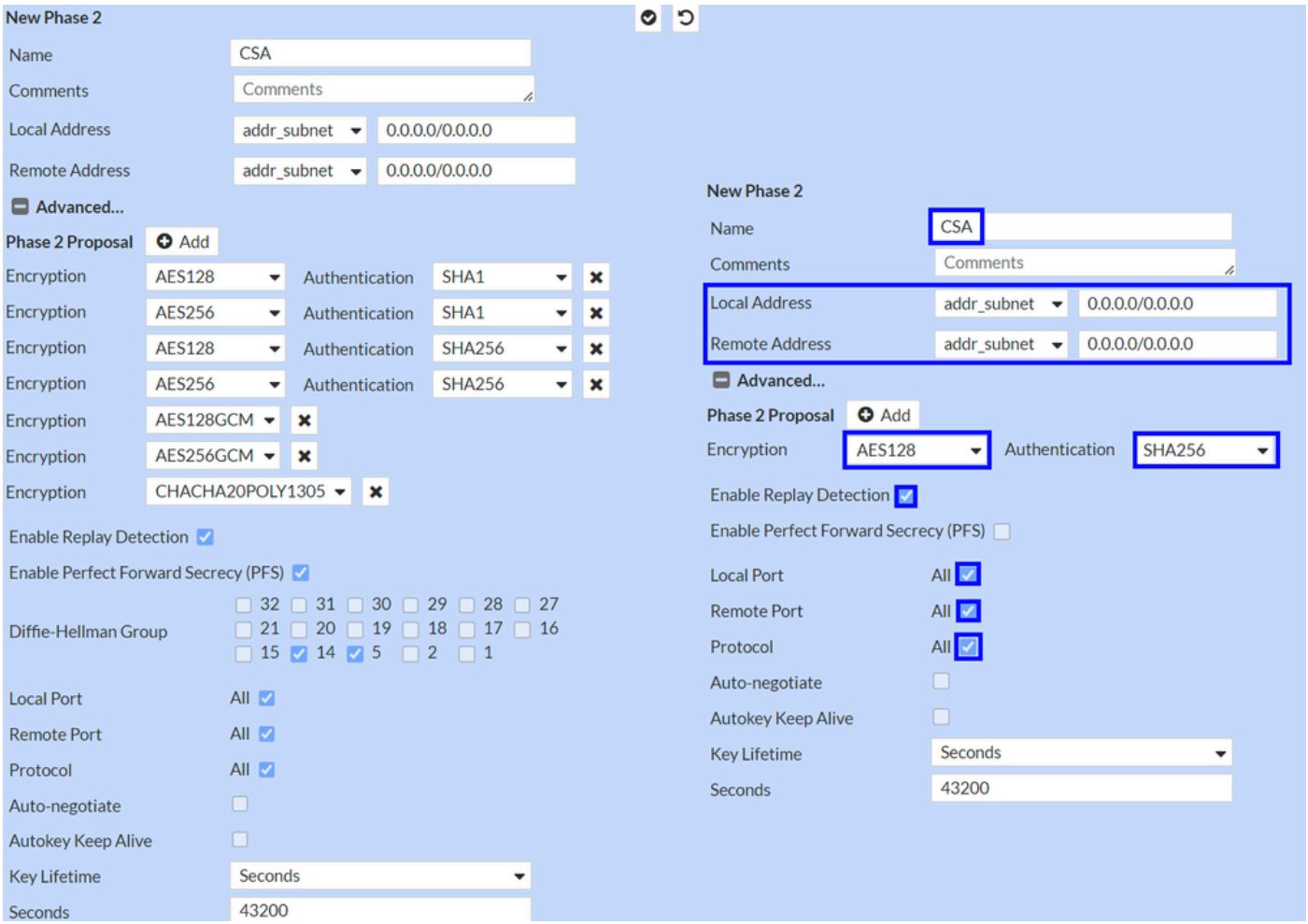
1단계 제안



- Phase 1 Proposal
  - Encryption : AES256 선택
    - Authentication : SHA256 선택
    - Diffie-Hellman Groups : 확인란 19 및 20을 선택합니다.
    - Key Lifetime (seconds) : 기본값으로 86400
    - Local ID : 터널 데이터 Primary Tunnel ID 단계에서 제공된 을 사용합니다.

이제 를 **Phase 2 Proposal**구성합니다.

2단계 제안



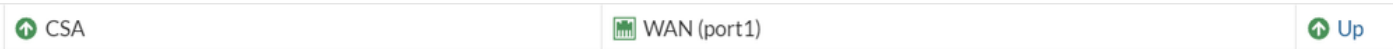
- New Phase 2
  - **Name** : 기본값으로 설정합니다(VPN 이름에서 가져옴).
    - **Local Address** : 기본값으로 설정(0.0.0.0/0.0.0.0)
    - **Remote Address** : 기본값으로 설정(0.0.0.0/0.0.0.0)

- Advanced
  - **Encryption** : AES128 선택
    - **Authentication** : SHA256 선택
    - **Enable Replay Detection** : 기본값으로 설정(활성화됨)
    - **Enable Perfect Forward Secrecy (PFS)** : 확인란 선택을 취소합니다.
    - **Local Port** :

기본값으로 설정(활성화됨)

- **Remote Port**: 기본값으로 설정(활성화됨)
- **Protocol** : 기본값으로 설정(활성화됨)
- **Auto-negotiate** : 기본값으로 설정(표시 안 함)
- **Autokey Keep Alive** : 기본값으로 설정(표시 안 함)
- **Key Lifetime** : 기본값으로 설정(초)
- **Seconds** : 기본값으로 설정(43200)

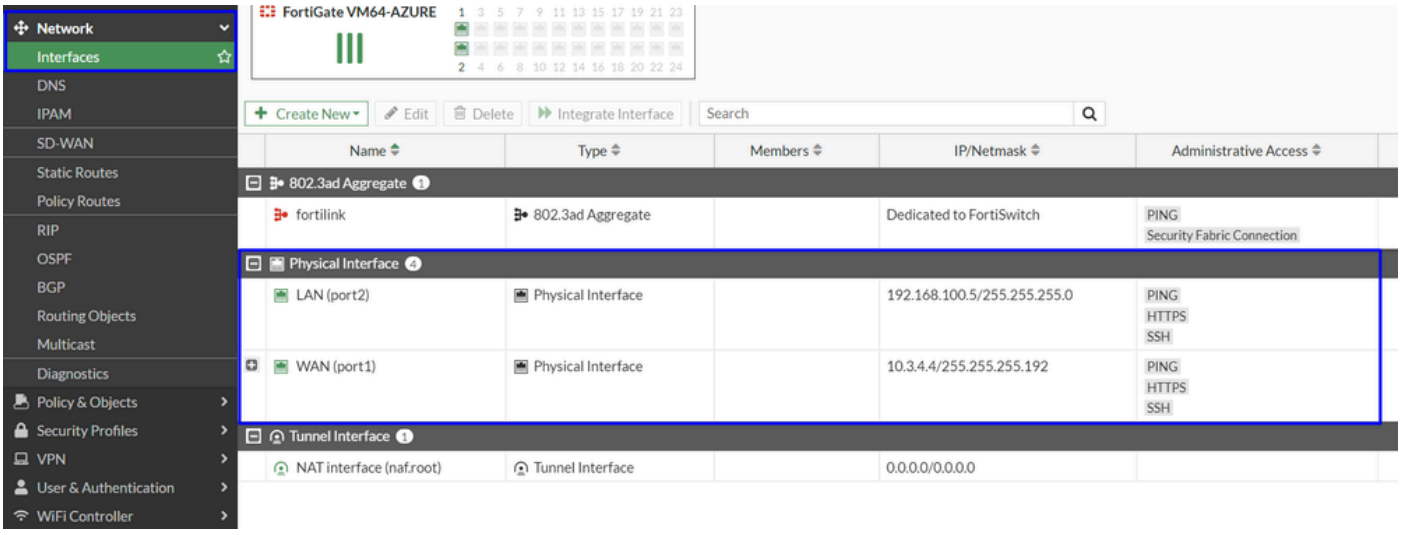
그런 다음 확인을 클릭합니다. 몇 분 후 Secure Access를 통해 VPN이 설정되었음을 확인할 수 있으며 다음 단계로 계속할 수 있습니다 . **Configure the Tunnel Interface.**



터널 인터페이스 구성

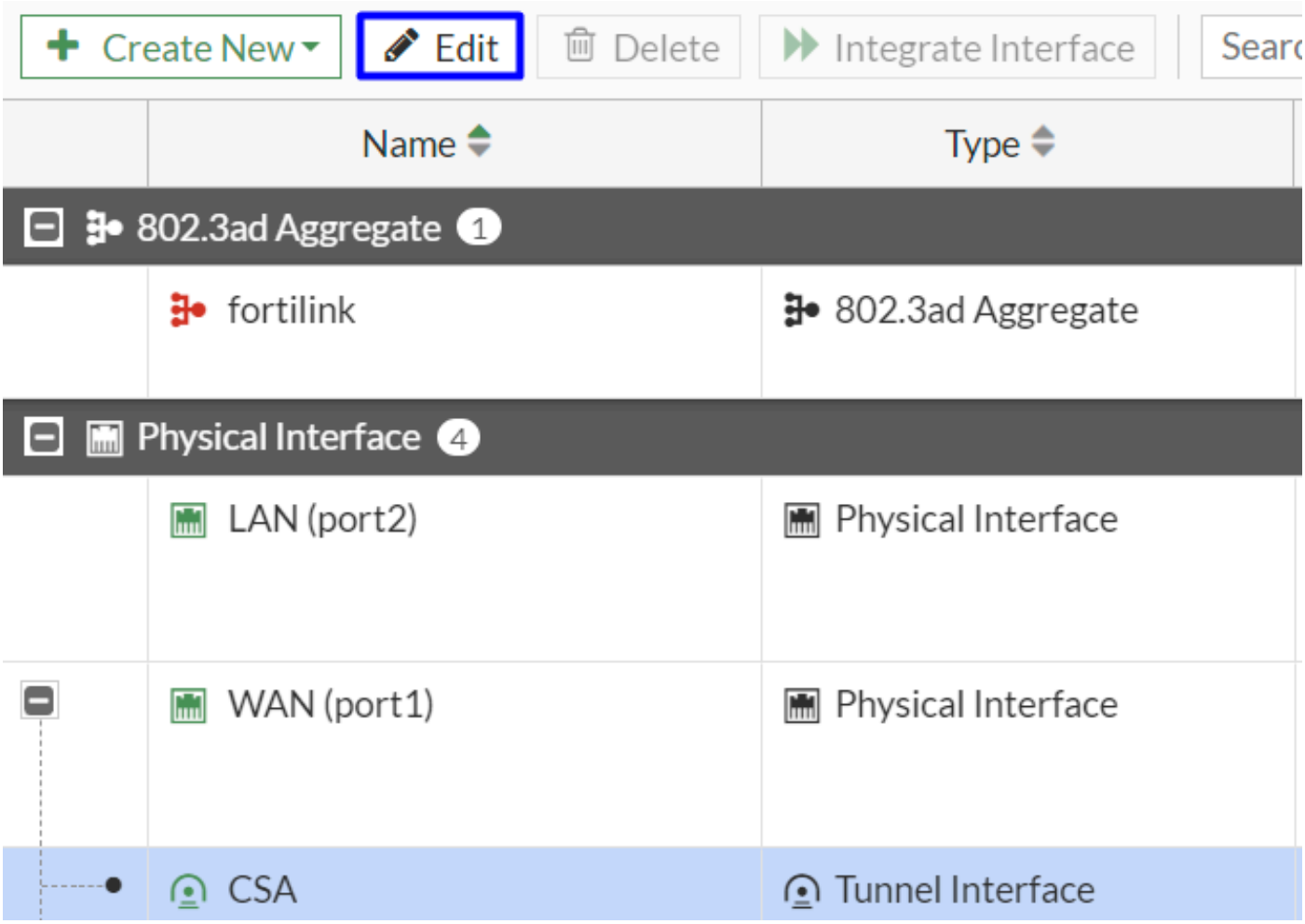
터널이 생성되면 Secure Access와 통신하기 위해 WAN 인터페이스로 사용 중인 포트 뒤에 새 인터페이스가 있음을 알 수 있습니다.

확인하려면 로 이동하십시오 **Network** > **Interfaces**.

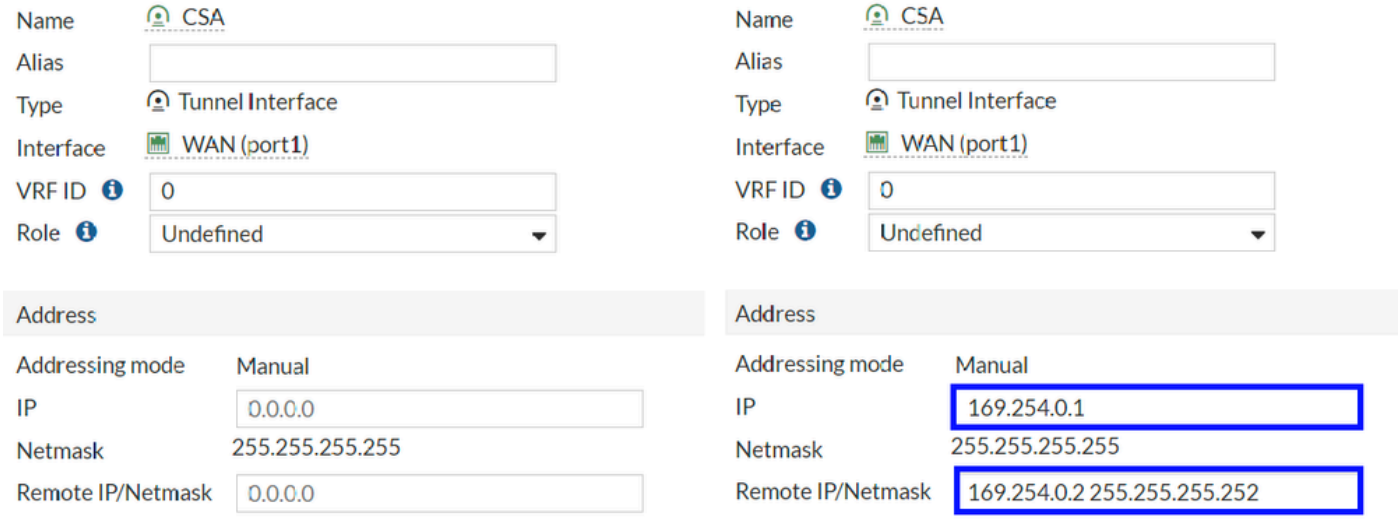


Secure Access와 통신하는 데 사용하는 포트를 확장합니다. 이 경우 인터페이스가 **WAN** 확장됩니다.

- 를 클릭하고 **Tunnel Interface** 다음을 클릭합니다. **Edit**



- 구성해야 하는 다음 이미지가 있습니다.

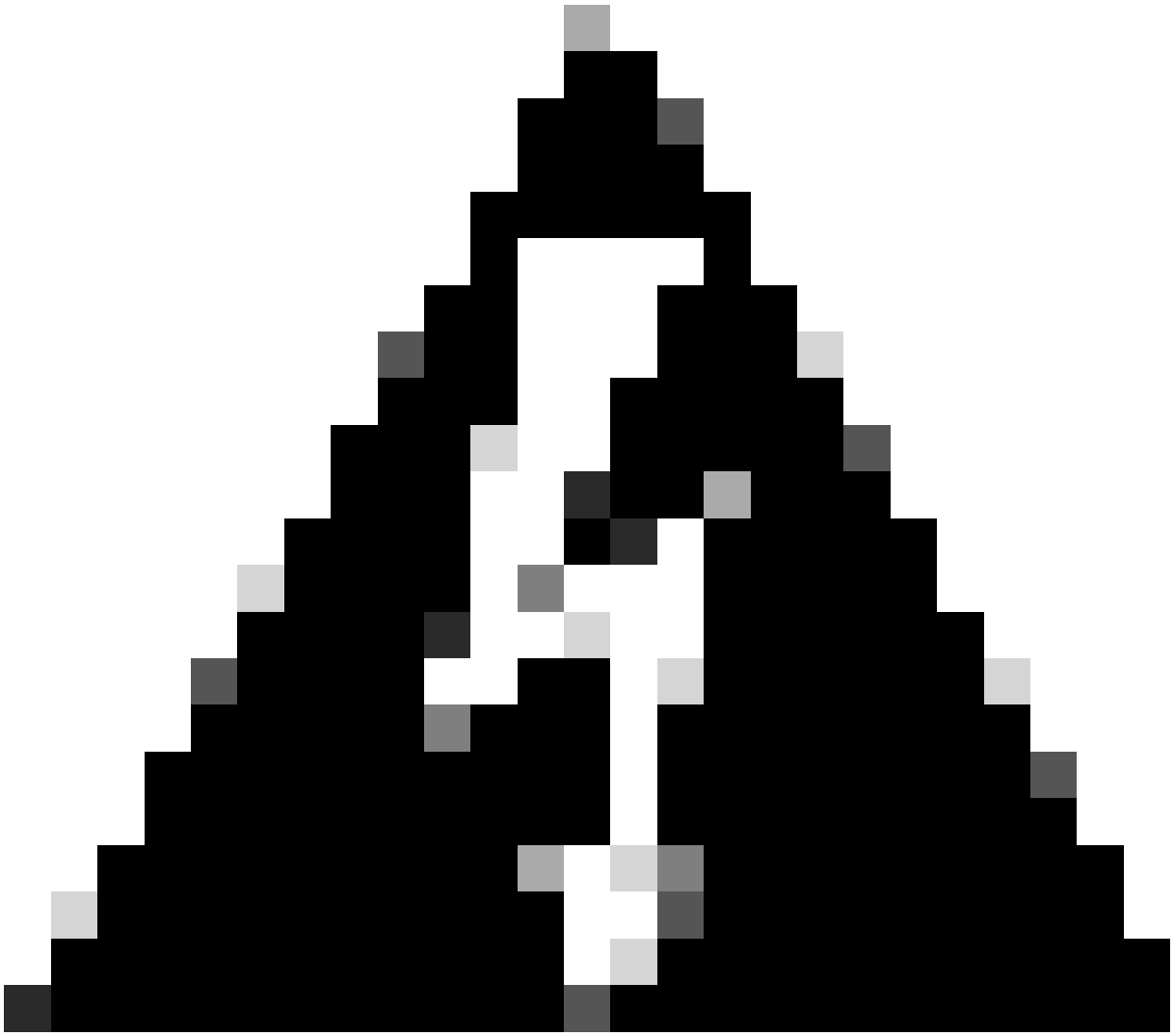


- Interface Configuration

- IP : 네트워크에 없는 라우팅 불가 IP를 구성합니다(169.254.0.1).

- Remote IP/Netmask : 원격 IP를 인터페이스 IP의 다음 IP로 구성하고 넷마스크 30(169.254.0.2 255.255.255.252)을 사용합니다.

그런 다음 **OK** 을 클릭하여 컨피그레이션을 저장하고 다음 단계(Configure Policy Route Origin-based routing)를 진행합니다.

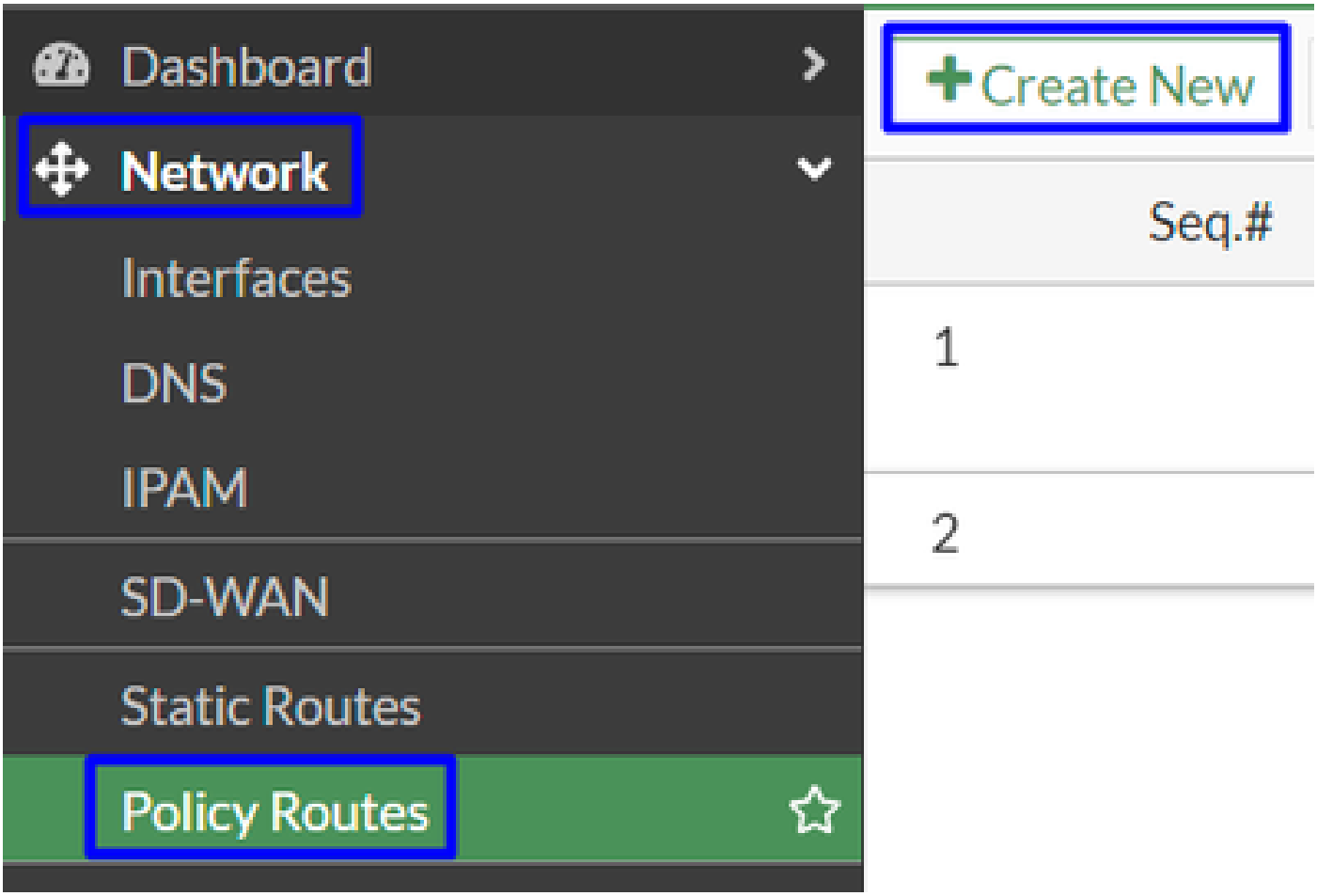


경고: 이 부분이 끝나면 디바이스에서 보안 액세스로, 보안 액세스에서 트래픽을 라우팅하려는 네트워크에 대한 트래픽을 허용하거나 허용하려면 FortiGate에서 방화벽 정책을 구성해야 합니다.

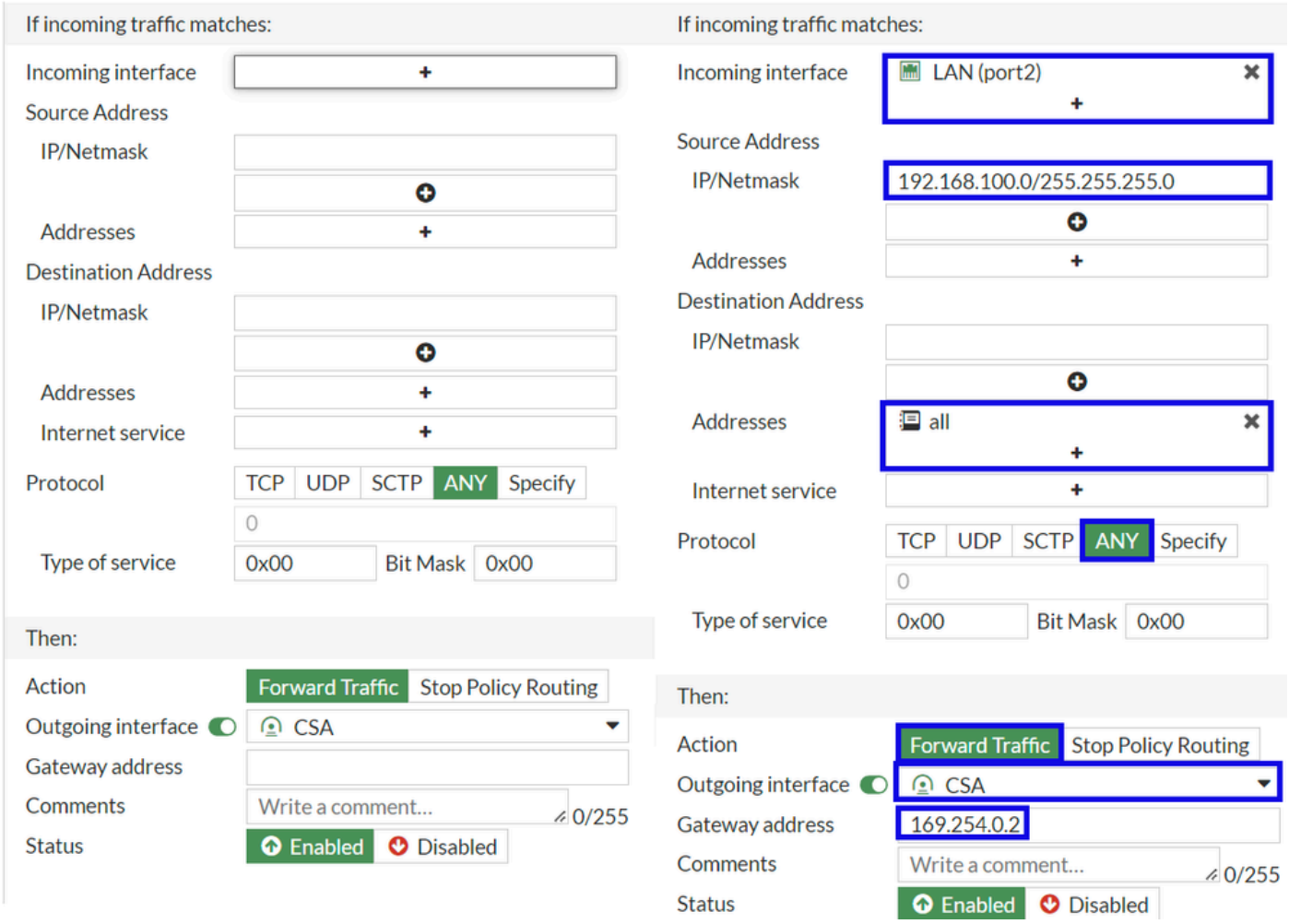
정책 경로 구성

이 시점에서는 VPN이 보안 액세스로 구성 및 설정되어 있습니다. 이제 트래픽을 보안 액세스로 다시 라우팅하여 트래픽을 보호하거나 FortiGate 방화벽 뒤에서 개인 애플리케이션에 액세스해야 합니다.

- 탐색 Network > Policy Routes



- 정책 구성



- If Incoming traffic matches
  - Incoming Interface : 트래픽을 Secure Access(Origin of traffic)로 다시 라우팅할 인터페이스를 선택합니다.
- Source Address
  - IP/Netmask : 인터페이스의 서브넷만 라우팅하는 경우 이 옵션을 사용합니다.
    - Addresses : 객체가 생성되고 트래픽 소스가 여러 인터페이스 및 여러 서브넷에서 오는 경우 이 옵션을 사용합니다
- Destination Addresses
  - Addresses: 선택 all

- Protocol: 선택 **ANY**

- Then
  - Action: **Choose Forward Traffic**

- Outgoing Interface : Configure Tunnel Interface(터널 인터페이스 구성) 단계에서 수정한 터널 인터페이스를 선택합니다
- Gateway Address: RemoteIPNetmask 단계에서 구성한 원격 IP를 구성합니다
- Status : Enabled(활성화됨)를 선택합니다.

컨피그레이션**OK** 을 저장하려면 클릭합니다. 이제 디바이스 트래픽이 Secure Access로 다시 라우팅되었는지 확인할 준비가 되었습니다.

다음을 확인합니다.

컴퓨터의 트래픽이 Secure Access로 다시 라우팅되었는지 확인하려면 인터넷에 접속하여 공용 IP를 확인하거나 다음 명령을 curl로 실행할 수 있는 두 가지 옵션이 있습니다.

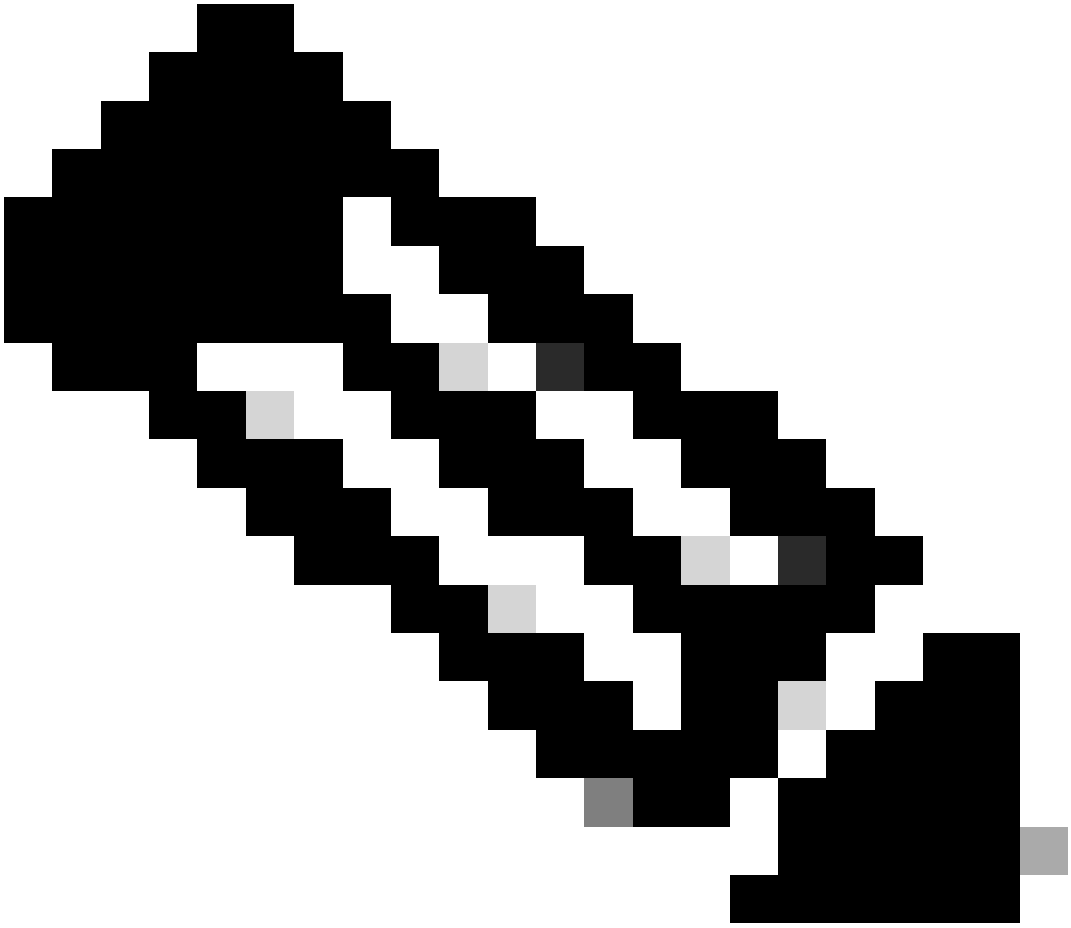
<#root>

```
C:\Windows\system32>curl ipinfo.io { "ip": "151.186.197.1", "city": "Frankfurt am Main", "region": "Hes
```

트래픽을 볼 수 있는 공개 범위는 다음과 같습니다.

Min Host:151.186.176.1

Max Host :151.186.207.254



참고: 이러한 IP는 변경될 수 있으며, 이는 Cisco가 향후 이 범위를 확장할 가능성이 있음을 의미합니다.

공용 IP가 변경되면 Secure Access에 의해 보호됩니다. 이제 Secure Access 대시보드에서 프라이빗 애플리케이션을 구성하여 VPNaaS 또는 ZTNA에서 애플리케이션에 액세스할 수 있습니다.

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.