고가용성 및 상태 모니터링을 위한 Meraki MX로 보안 액세스 구성

목차

소개

이 문서에서는 상태 확인을 사용하여 고가용성을 위한 Meraki MX로 Cisco Secure Access를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

- 보안 액세스로 IPsec 터널 요구 사항 검토
- 보안 액세스 구성 요소 이해
- Meraki MX의 상태 확인 기능 이해

요구 사항

- Meraki MX는 펌웨어 버전 19.7.1 이상을 실행해야 합니다.
- Private Access를 사용할 경우, 상태 확인 IP를 변경하지 못하게 하는 Meraki 제한 때문에 추가 SPA(Secure Private Access) 터널에 NAT가 필요하기 때문에 터널이 하나만 지원됩니다. SIA(Secure Internet Access)를 사용하는 경우에는 적용되지 않습니다.

- 터널을 통해 보안 액세스로 라우팅되는 내부 서브넷 또는 리소스를 명확하게 정의합니다.

사용되는 구성 요소

- Cisco 보안 액세스
- Meraki MX Security Appliance(펌웨어 버전 19.7.1 이상)
- Meraki 대시보드
- 보안 액세스 대시보드

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

Cisco Secure Access는 프라이빗 애플리케이션(Private Access를 통해) 및 인터넷 대상(Internet Access를 통해) 모두에 대한 보안 액세스를 지원하는 클라우드 네이티브 보안 플랫폼입니다. Meraki MX와 통합할 경우, 조직은 지사 사이트와 클라우드 간에 안전한 IPsec 터널을 설정하여 암

호화된 트래픽 흐름과 중앙 집중식 보안 시행을 보장할 수 있습니다.

이 통합에서는 고정 라우팅 IPsec 터널을 사용합니다. Meraki MX는 Cisco Secure Access에 대한 기본 및 보조 IPsec 터널을 설정하고 내장된 업링크 상태 검사를 활용하여 터널 간의 자동 장애 조치를 수행합니다. 이를 통해 브랜치 연결을 위한 탄력적이고 고가용성 컨피그레이션을 제공합니다.

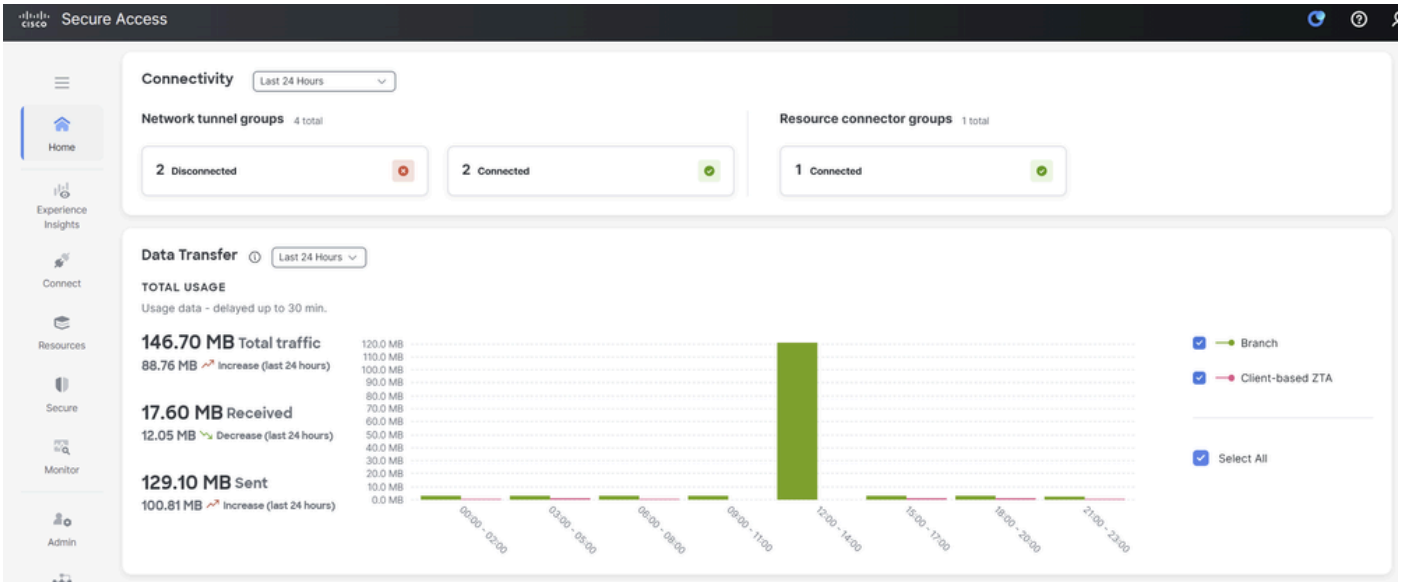
이 구축의 핵심 요소는 다음과 같습니다.

- Meraki MX는 Cisco Secure Access에 대한 비 Meraki VPN 피어 역할을 합니다.
- 기본 및 보조 터널이 정적으로 구성되었으며, 상태 확인으로 가용성을 확인합니다.
- Private Access는 SPA(Secure Private Access)를 통해 내부 애플리케이션에 대한 보안 액세스를 지원하는 반면, Internet Access는 클라우드에서 정책을 시행하여 트래픽이 인터넷 기반 리소스에 도달할 수 있도록 합니다.
- 상태 확인 IP 유연성의 Meraki 제한 사항으로 인해 프라이빗 액세스 모드에서는 터널 그룹이 하나만 지원됩니다. 여러 Meraki MX 디바이스가 Secure Access for Private Access에 연결해야 하는 경우 동적 라우팅을 위해 BGP를 사용하거나, 네트워크 터널 그룹 하나만 상태 확인 및 고가용성을 지원할 수 있음을 이해하고 고정 터널을 구성해야 합니다. 추가 터널은 상태 모니터링 또는 이중화 없이 작동합니다.

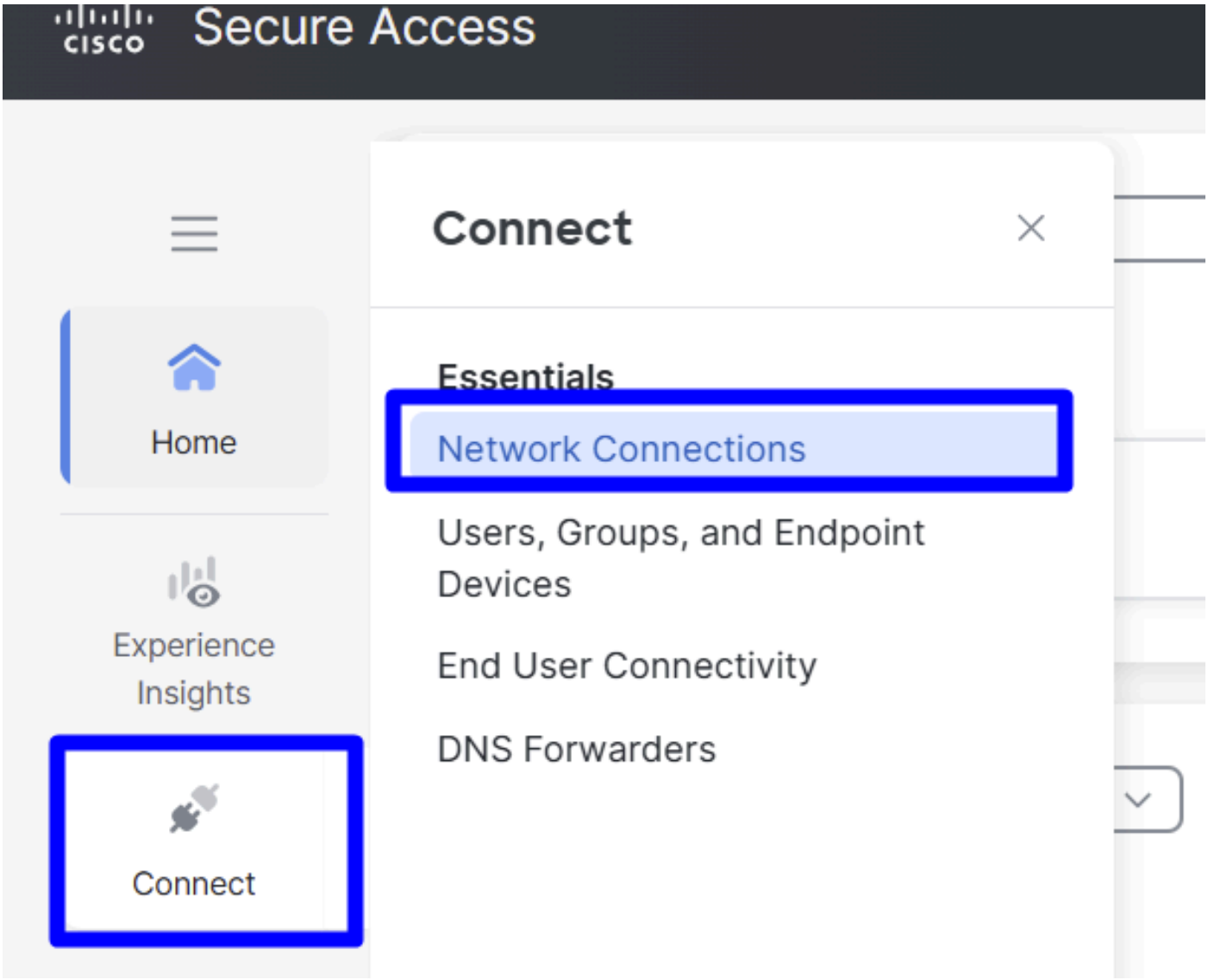
구성

보안 액세스에서 VPN 구성

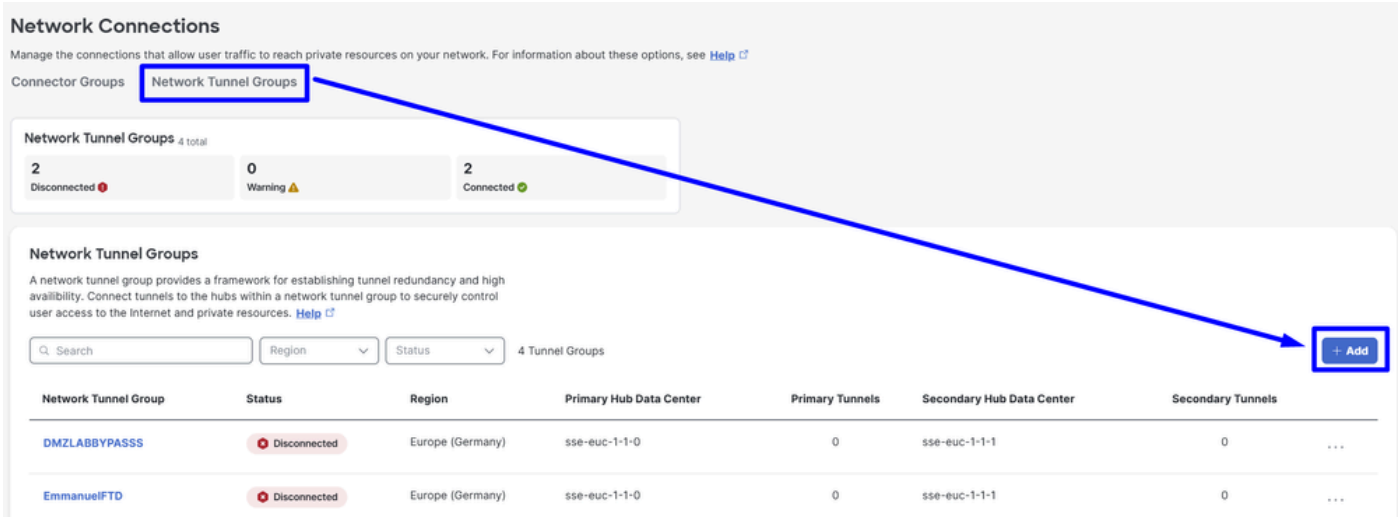
Secure Access의 관리자 패널로 이동합니다.



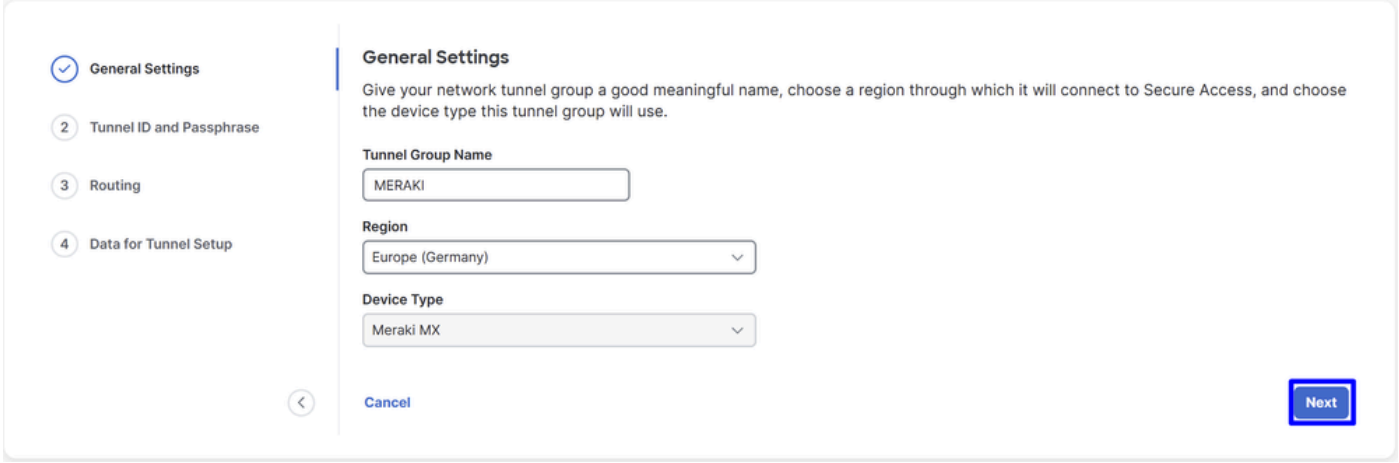
- 클릭 Connect > Network Connections



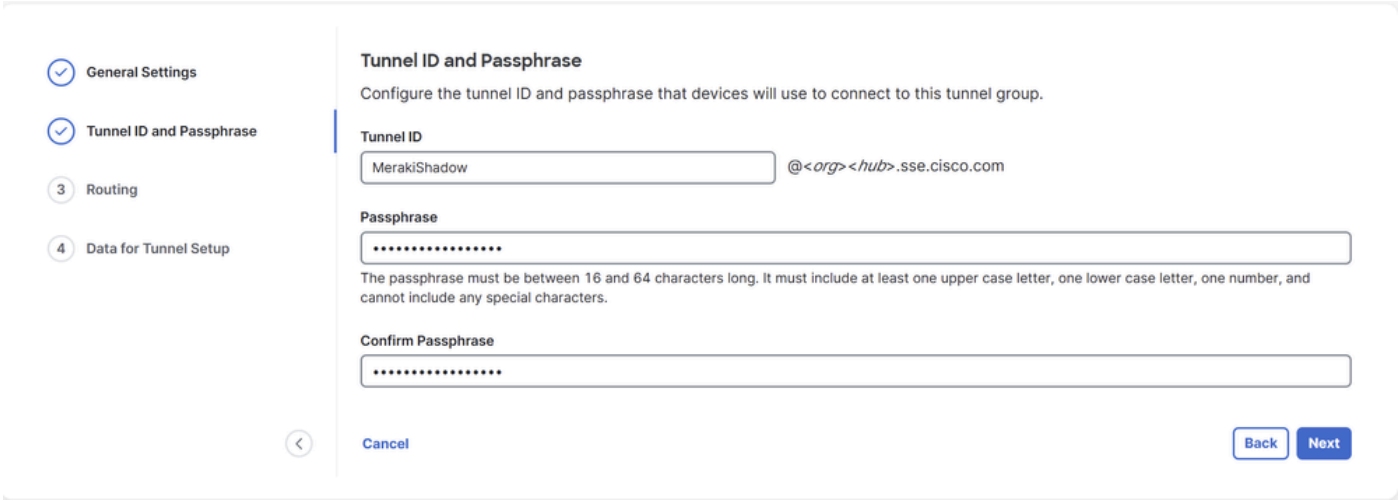
- 에서Network Tunnel Groups클릭 + Add



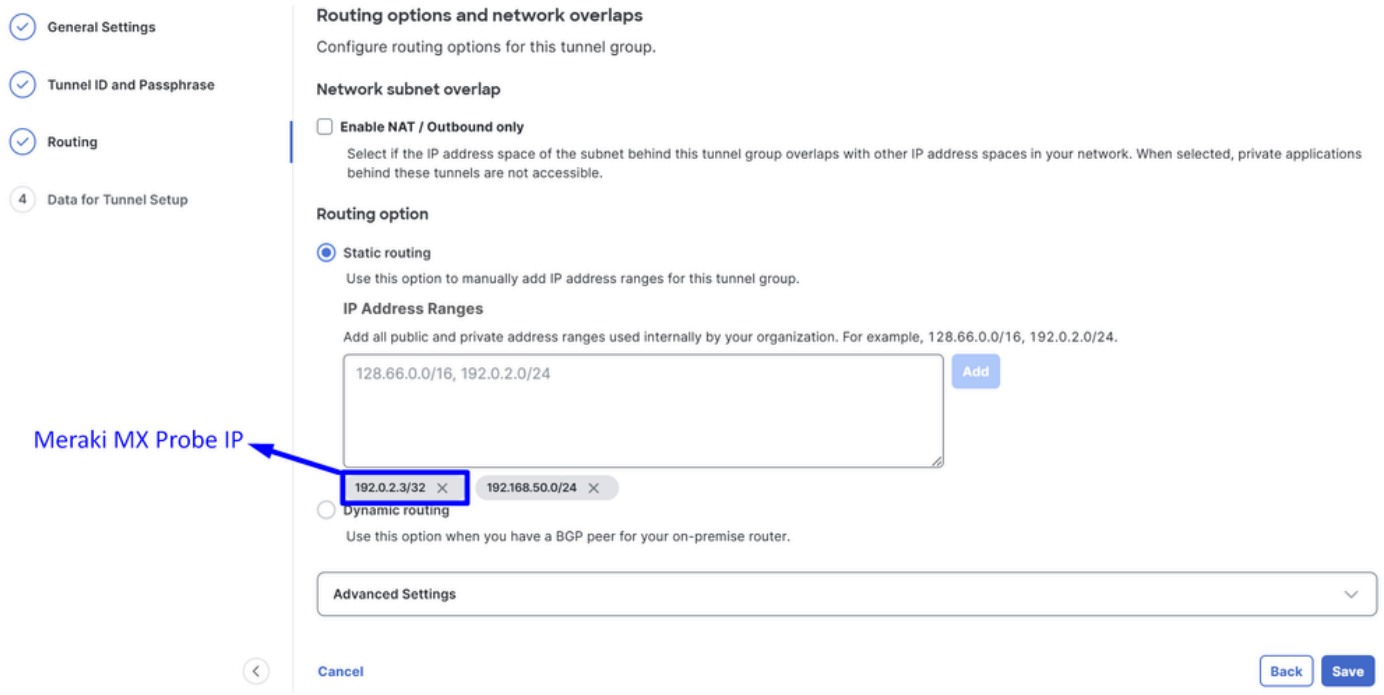
- 구성Tunnel Group Name，Region및Device Type
- 을 클릭합니다 **Next**

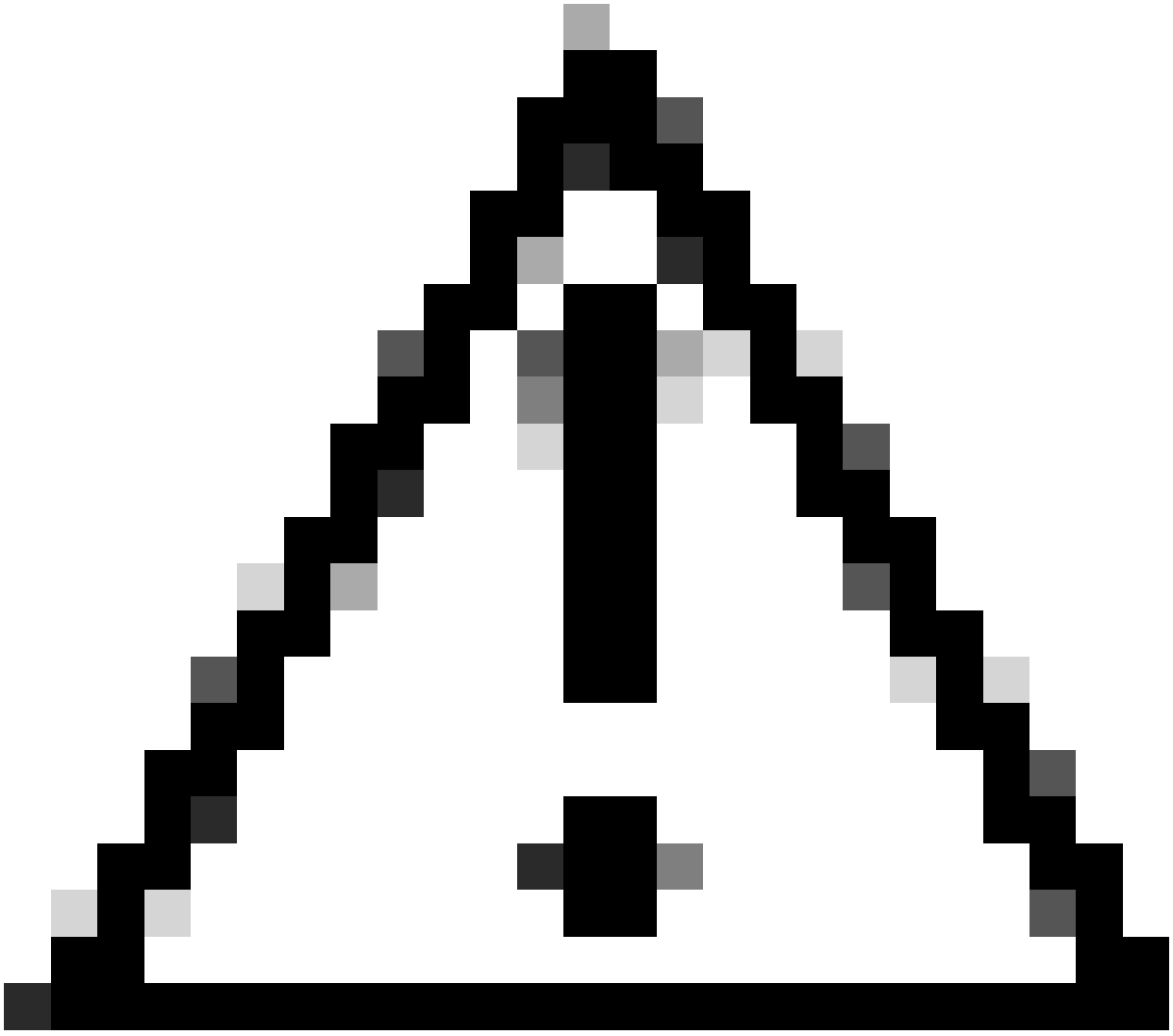


- 및 를Tunnel ID Format구성합니다 Passphrase
- 을 클릭합니다Next



- 네트워크에서 구성했으며 Secure Access를 통해 트래픽을 전달하려는 IP 주소 범위 또는 호스트를 구성하고, Secure Access에서 Meraki MX로 반환되는 트래픽을 허용하도록 Meraki 모니터링 프로브 IP192.0.2.3/32를 포함해야 합니다.
- 을 클릭합니다Save


General Settings
Tunnel ID and Passphrase
Routing
4 Data for Tunnel Setup
Routing options and network overlaps
Configure routing options for this tunnel group.
Network subnet overlap
Enable NAT / Outbound only
Select if the IP address space of the subnet behind this tunnel group overlaps with other IP address spaces in your network. When selected, private applications behind these tunnels are not accessible.
Routing option
Static routing
Use this option to manually add IP address ranges for this tunnel group.
IP Address Ranges
Add all public and private address ranges used internally by your organization. For example, 128.66.0.0/16, 192.0.2.0/24.
128.66.0.0/16, 192.0.2.0/24
Add
Meraki MX Probe IP
192.0.2.3/32
192.168.50.0/24
Dynamic routing
Use this option when you have a BGP peer for your on-premise router.
Advanced Settings
Cancel
Back
Save

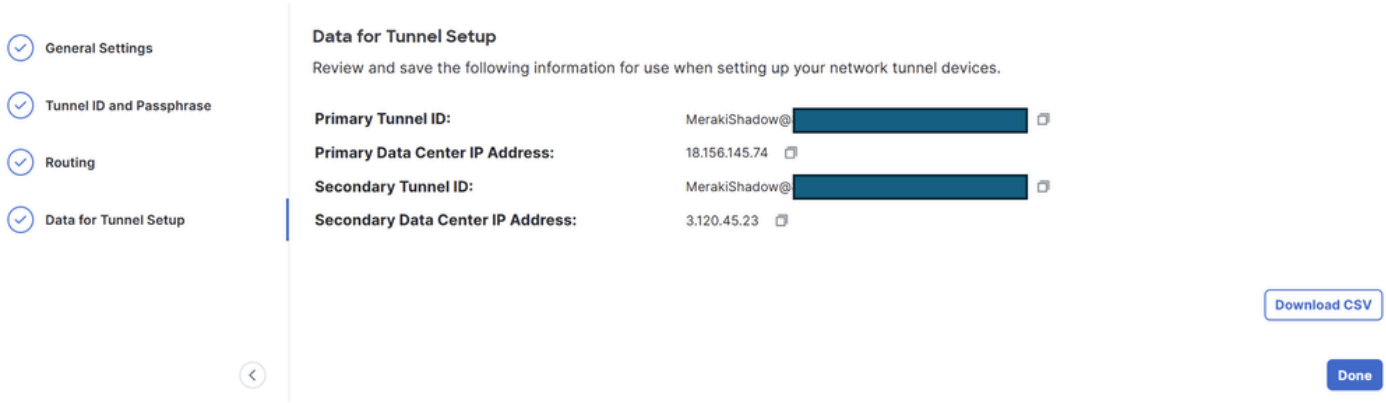


주의: 모니터링 프로브 IP (192.0.2.3/32)를 추가 해야 합니다. 그렇지 않으면 Meraki 디바이스에서 트래픽을 인터넷, VPN 풀 및 ZTNA에서 사용하는 CGNAT 범위 100.64.0.0/10으로 라우팅하는 트래픽 문제가 발생할 수 있습니다.

- 터널에 대한 정보가 표시되면 **Save** 다음 단계를 위해 해당 정보를 저장하십시오. **Configure the tunnel on Meraki MX.**

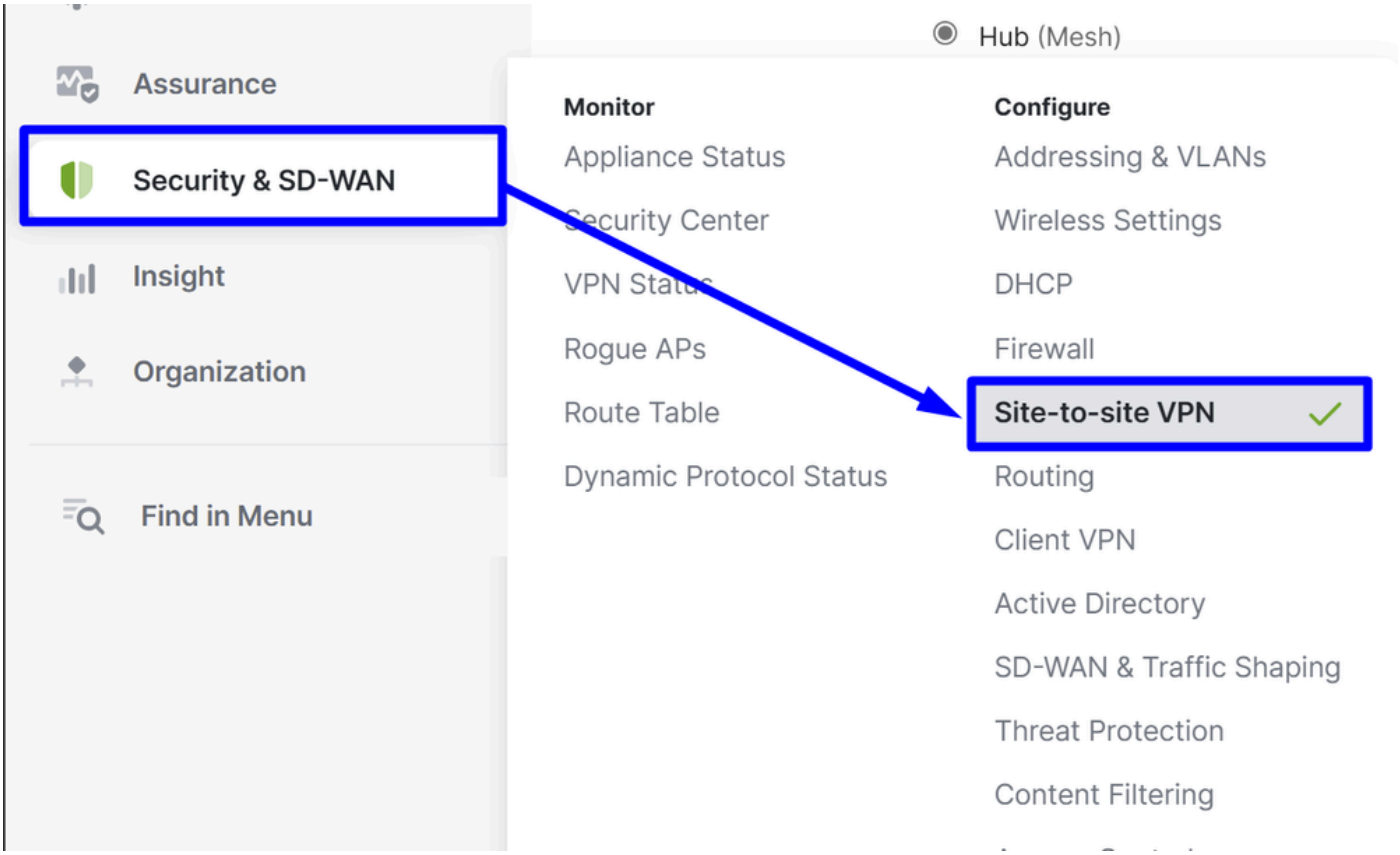
보안 액세스 VPN 구성

메모장에서 터널의 컨피그레이션을 복사합니다. 이 정보를 사용하여 Meraki에서 컨피그레이션을 완료합니다**Non-Meraki VPN Peers**.



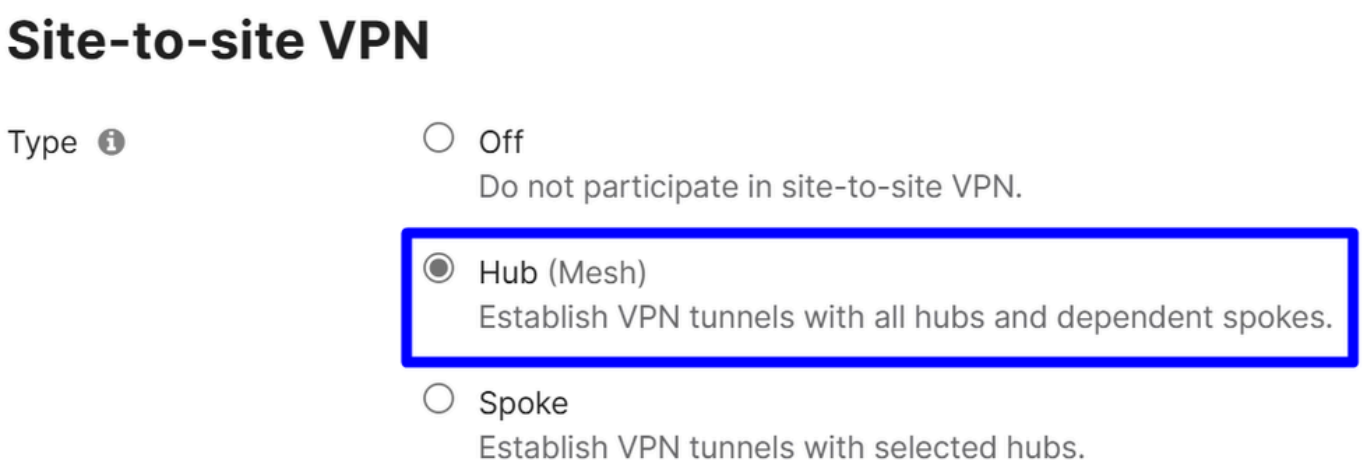
Meraki MX에서 VPN 구성

Meraki MX로 이동하여 **Security & SD-WAN** > Site-to-site VPN



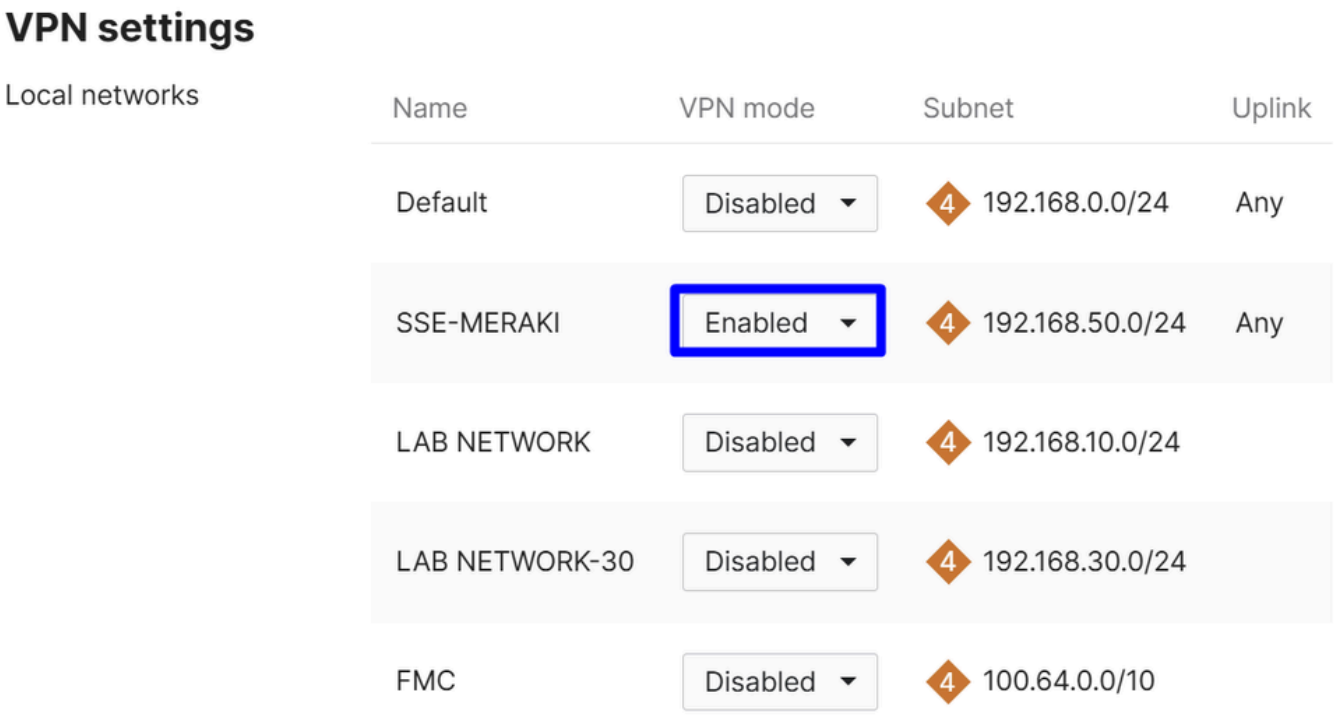
사이트 대 사이트 VPN

선택 Hub.

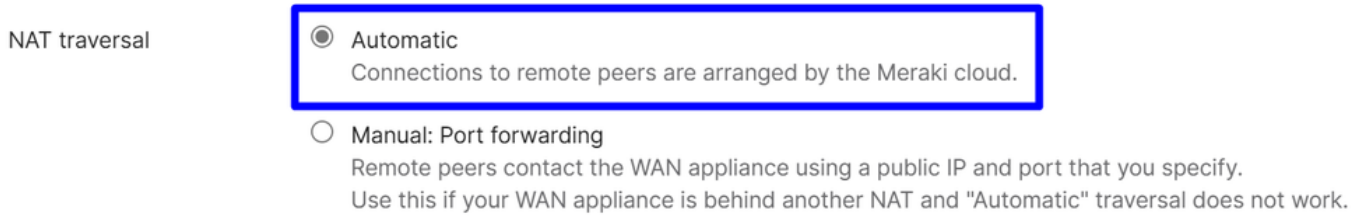


VPN 설정

Secure Access에 트래픽을 보내도록 선택한 네트워크를 선택합니다.



자동에서NAT Traversal선택



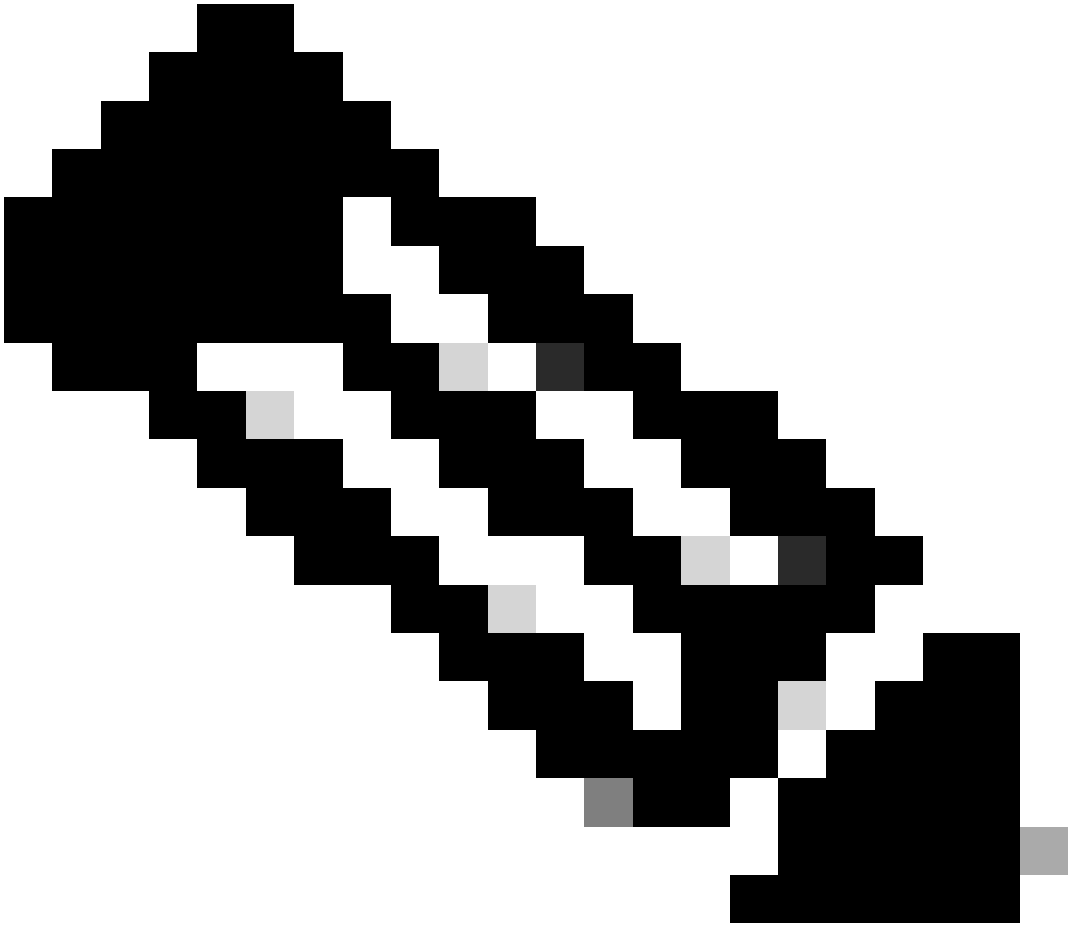
비 Meraki VPN 피어

Meraki에서 Secure Access로 트래픽을 라우팅하는 데 사용하는 상태 검사를 구성해야 합니다.

클릭 **Configure Health Checks**

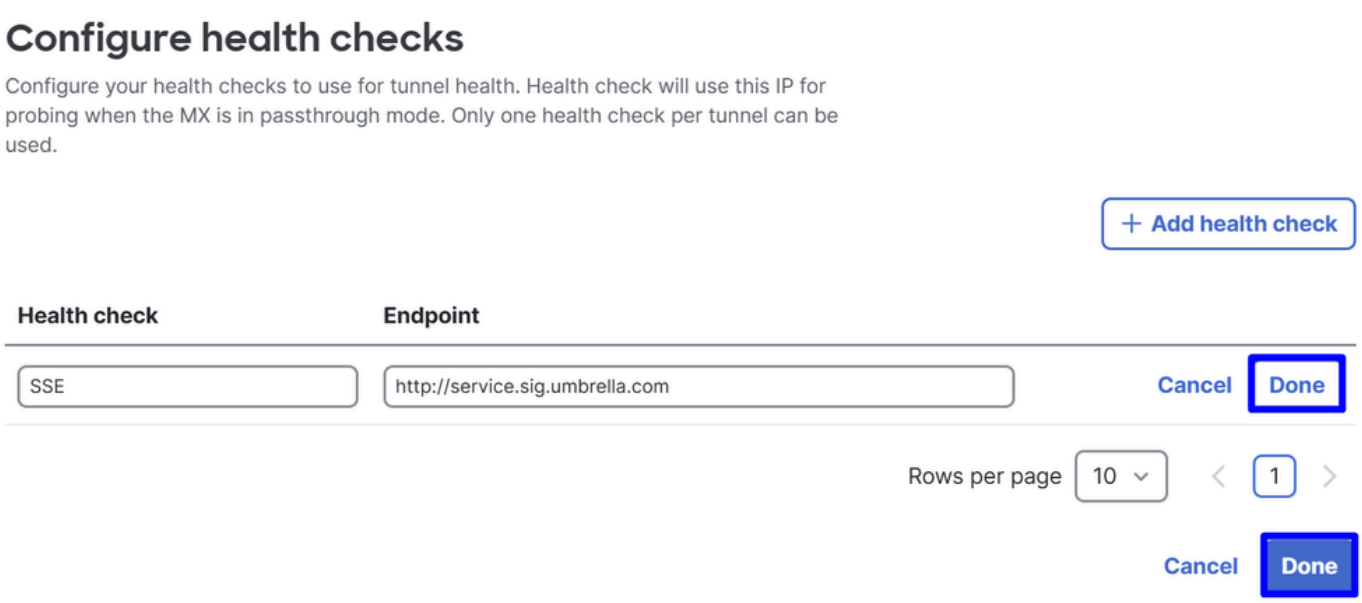
- 클릭 **+Add health Check**

- **Health Check**: 테스트 이름 구성
- **Endpoint**: Secure Access에서 권장하는 방법 사용 http://service.sig.umbrella.com



참고: 이 도메인은 Secure Access 또는 Umbrella를 사용하여 사이트 대 사이트 터널을 통해 액세스할 때만 응답합니다. 이러한 터널 외부에서 액세스를 시도하면 실패합니다.

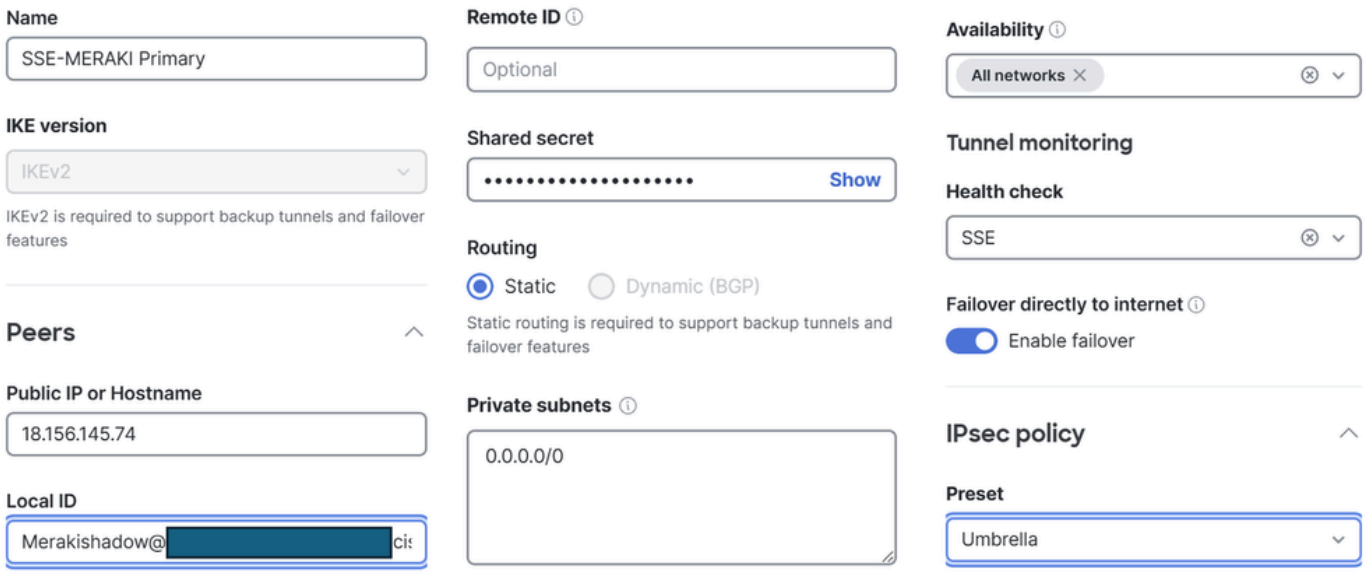
그런 다음 **Done** 두 번 클릭하여 마무리합니다.



이제 상태 확인이 구성되었으며 **Peer:**

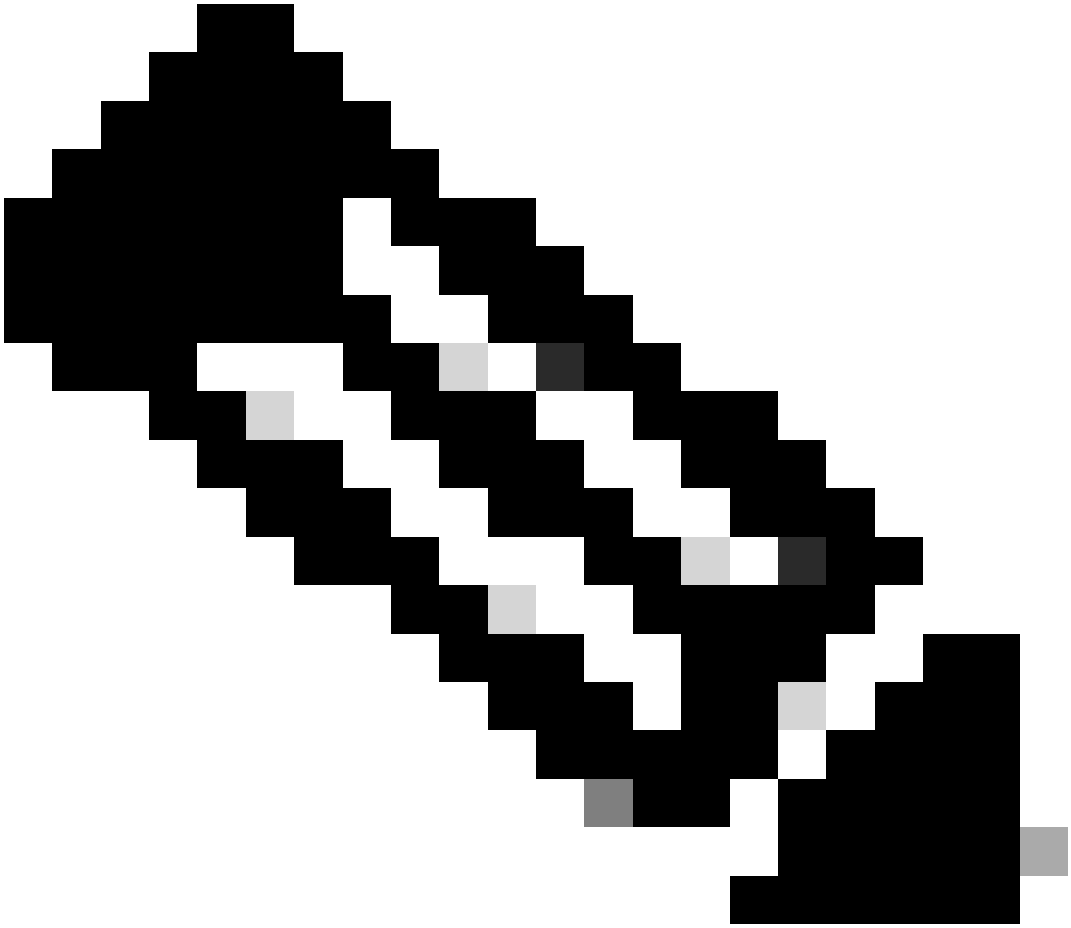
기본 터널 구성

- 클릭+Add a peer



- VPN 피어 추가
  - 이름: 보안 액세스에 대한 VPN의 이름 구성
  - IKE 버전: IKEv2 선택
- 피어
  - 공용 IP 또는 호스트 이름: Secure **Primary Datacenter IP** Access VPN Configurations(보안 액세스 VPN 컨피그레이션) 단계에서 Secure Access가 제공한 를 구성합니다
  - 로컬 ID: Secure **Primary Tunnel ID** Access VPN Configurations(보안 액세스 VPN 컨피그레이션) 단계에서 Secure Access가 제공한 를 구성합니다
  - 원격 ID: 해당 없음
  - 공유 암호: Secure Access VPN Configurations(보안 액세스 VPN **Passphrase** 컨피그레이

션) 단계에서 Secure Access가 제공한 를 구성합니다
    - 라우팅: 정적 선택
    - 프라이빗 서브넷: 인터넷 액세스와 프라이빗 액세스를 모두 구성하려는 경우 를 대상 **0.0.0.0/0**으로 사용합니다. 해당 VPN 터널에 대한 Private Access만 구성하는 경우 및 CGNAT **Remote Access VPN IP Pool** 범위를 대상 네트워크**100.64.0.0/10**로 지정합니다
    - 가용성: Meraki 디바이스가 하나만 있는 경우 선택할 수 **All Networks**있습니다. 디바이스가 여러 개인 경우 터널을 구성할 특정 Meraki 네트워크만 선택해야 합니다.
- 터널 모니터링
    - 상태 확인: 이전에 구성한 상태 확인을 사용하여 터널 가용성을 모니터링합니다
    - 인터넷으로 직접 장애 조치:이 옵션을 활성화한 상태에서 터널 1과 터널 2의 상태 확인이 모두 실패하면 인터넷 액세스 손실을 방지하기 위해 트래픽이 WAN 인터페이스로 리디렉션됩니다.



상태 확인 기능:터널 1을 모니터링 중이며 해당 상태 확인이 실패하면 트래픽이 자동으로 터널 2로 장애 조치됩니다. 터널 2도 실패하고 옵션이 활성화된 경우 트래픽은Failover directly to InternetMeraki 디바이스의 WAN 인터페이스를 통해 라우팅됩니다.

- IPsec 정책
  - 사전 설정: 선택 **Umbrella**

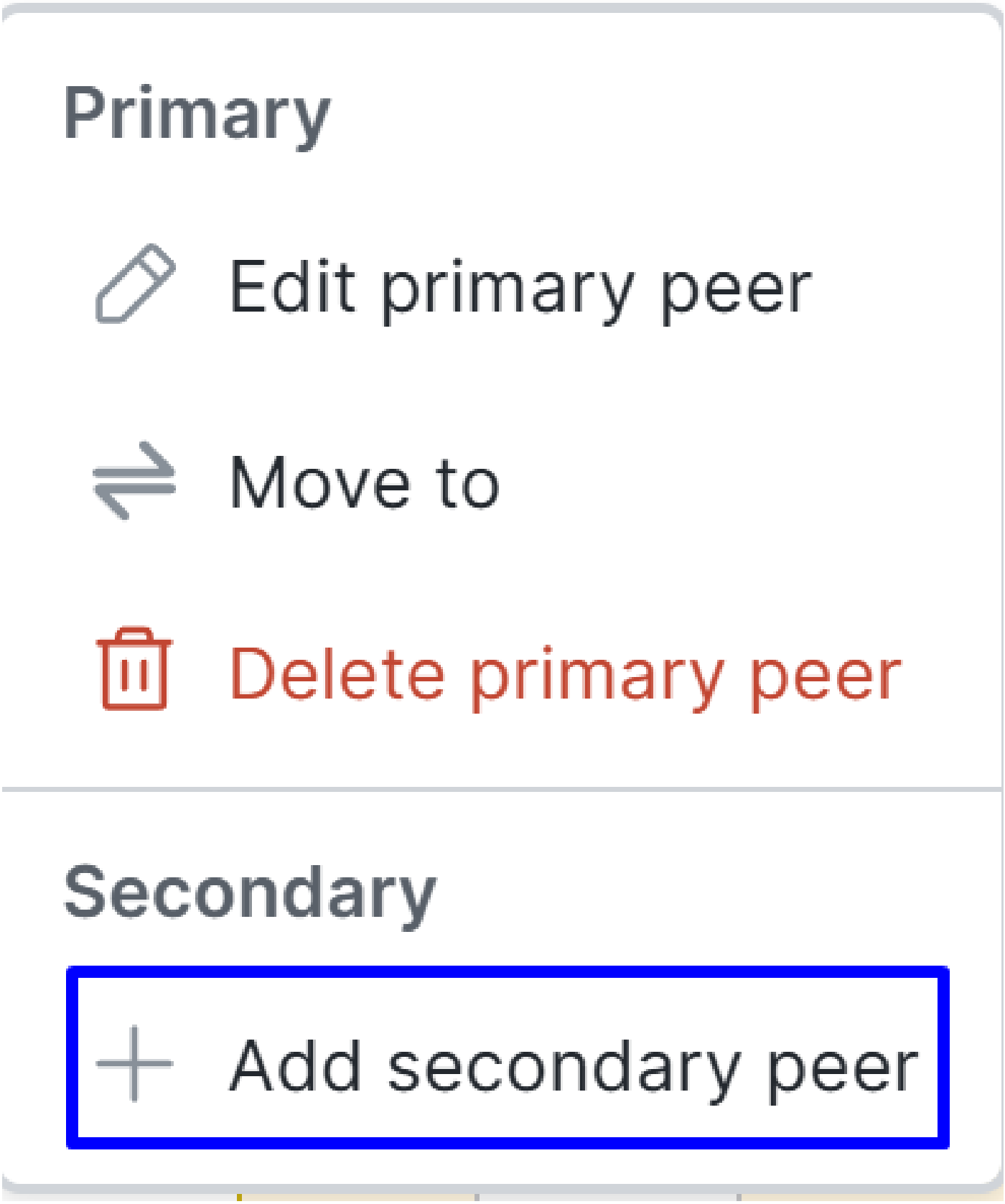
그런 다음 을 **Save**클릭합니다.

보조 터널 구성

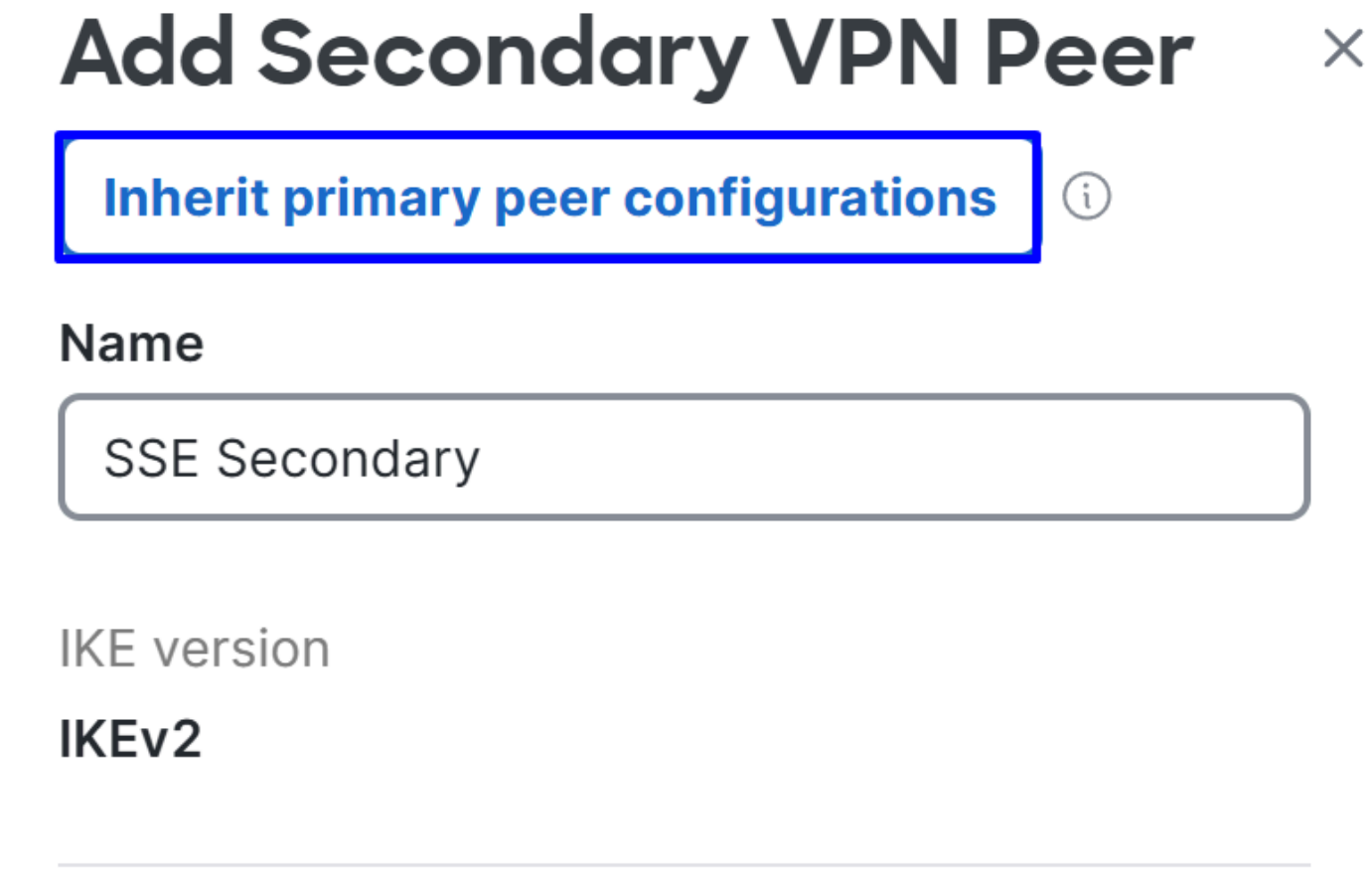
보조 터널을 구성하려면 기본 터널의 옵션 메뉴를 클릭합니다.

- 세 개의 점을 클릭합니다.

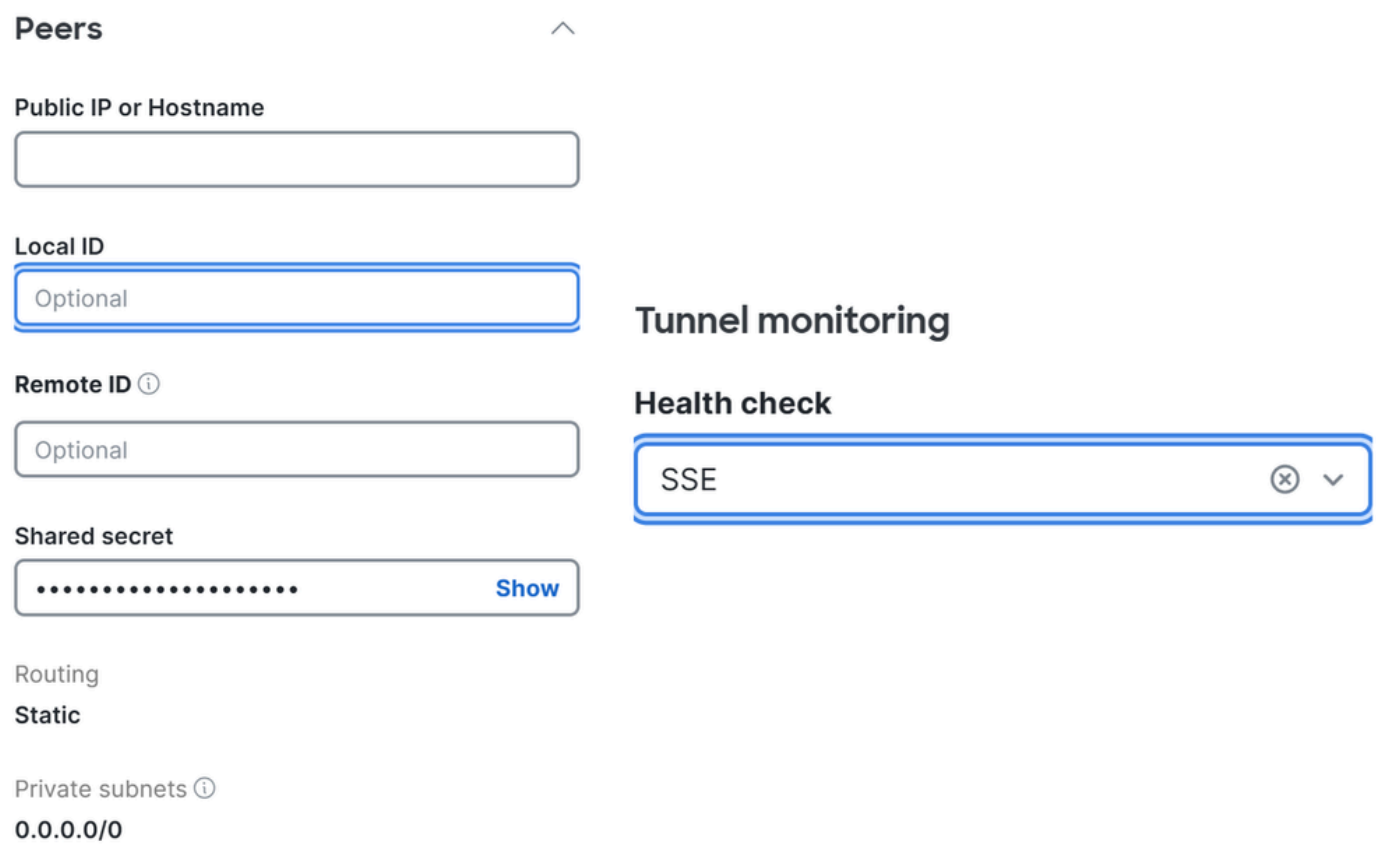
- 클릭 + Add Secondary peer



- 클릭Inherit primary peer configurations

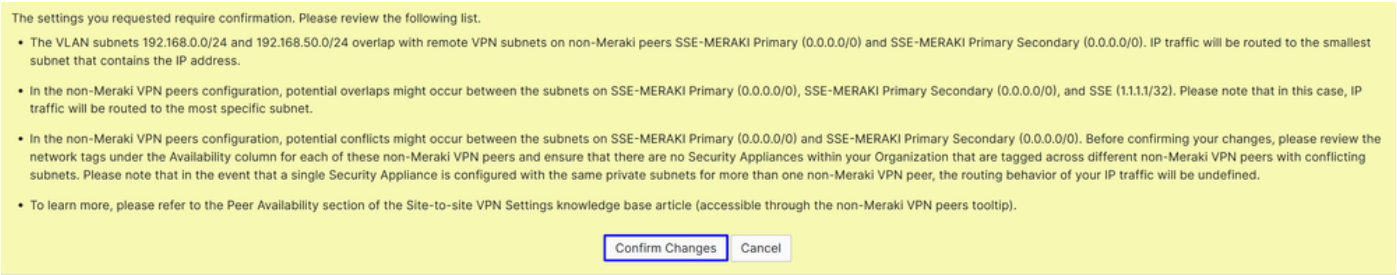


그러면 일부 필드가 자동으로 채워집니다. 검토 후 필요한 사항을 변경하고 나머지는 수동으로 완료합니다.



- 피어
  - 공용 IP 또는 호스트 이름: Secure **Secondary Datacenter IP** Access VPN Configurations(보안 액세스 VPN 컨피그레이션) 단계에서 Secure Access가 제공한 를 구성합니다
  - 로컬 ID: Secure **Secondary Tunnel ID** Access VPN Configurations(보안 액세스 VPN 컨피그레이션) 단계에서 Secure Access가 제공한 를 구성합니다
  - 원격 ID: 해당 없음
  - 공유 암호: Secure Access VPN Configurations(보안 액세스 VPN **Passphrase** 컨피그레이션) 단계에서 Secure Access가 제공한 를 구성합니다
- 터널 모니터링
  - 상태 확인: 이전에 구성한 상태 확인을 사용하여 터널 가용성을 모니터링합니다

그런 다음 을 클릭하면 **Save**다음 알림이 나타납니다.

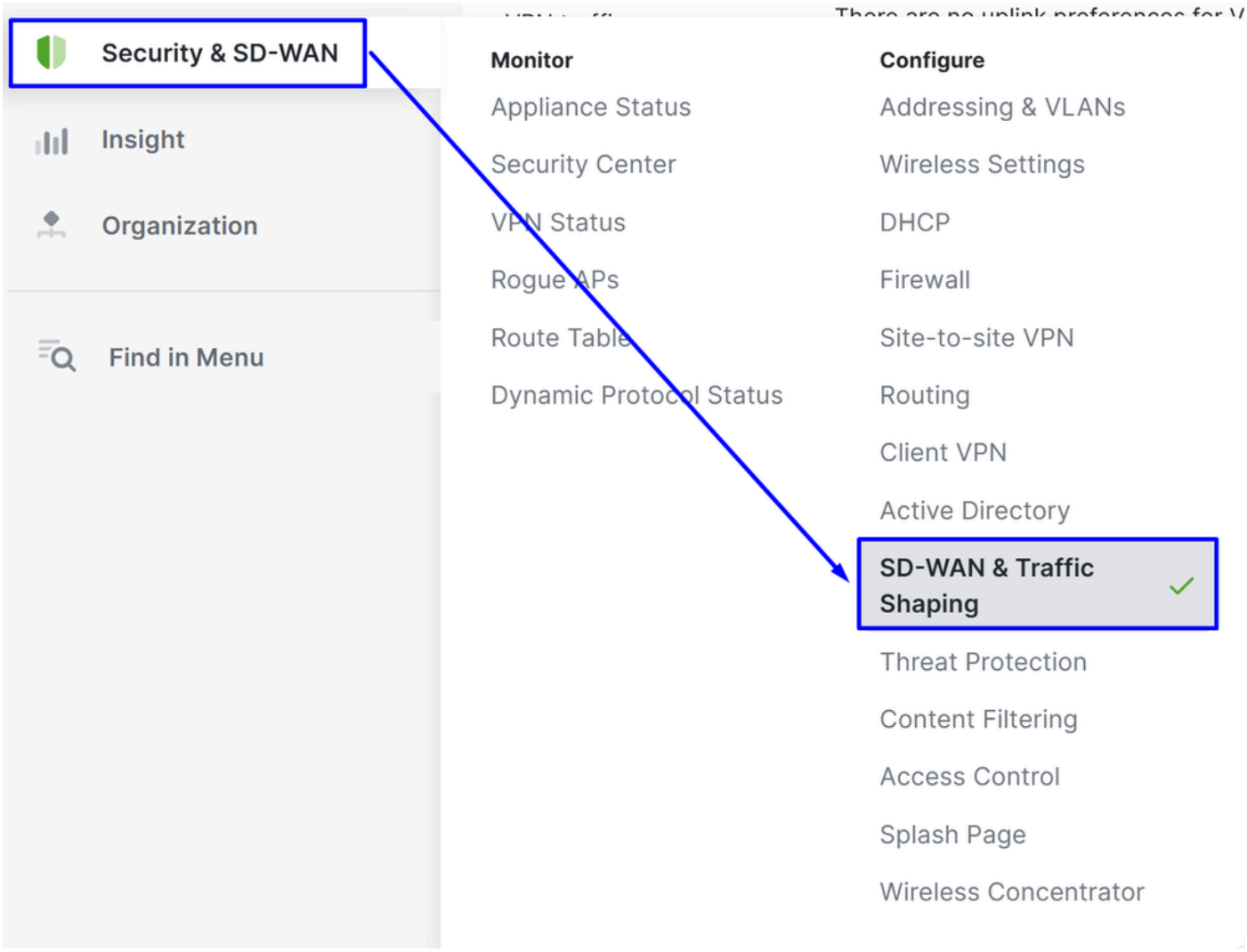


걱정하지 말고 클릭하십시오. **Confirm Changes**.

트래픽 조정 구성(터널 트래픽 바이패스)

이 기능을 사용하면 SD-WAN Bypass 컨피그레이션에서 도메인 또는 IP 주소를 정의하여 터널에서 특정 트래픽을 우회할 수 있습니다.

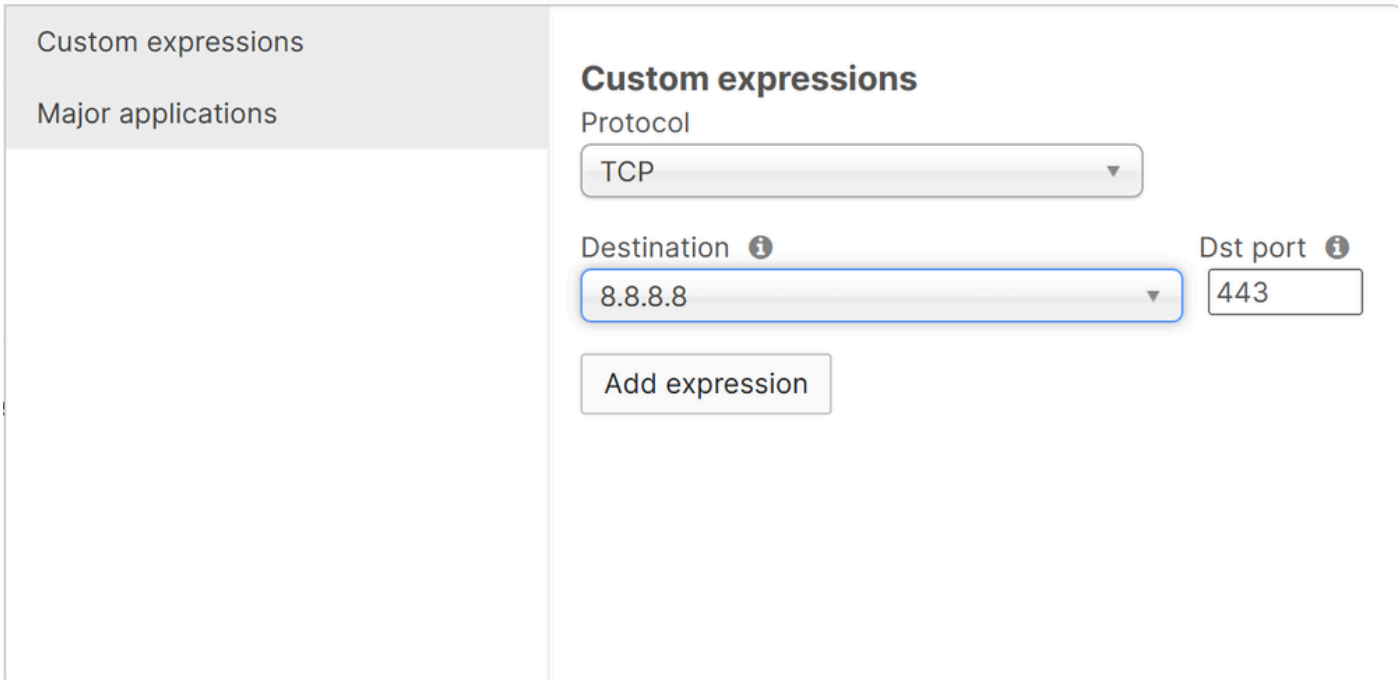
- >으로 **Security & SD-WAN** 이동합니다. SD-WAN & Traffic Shaping



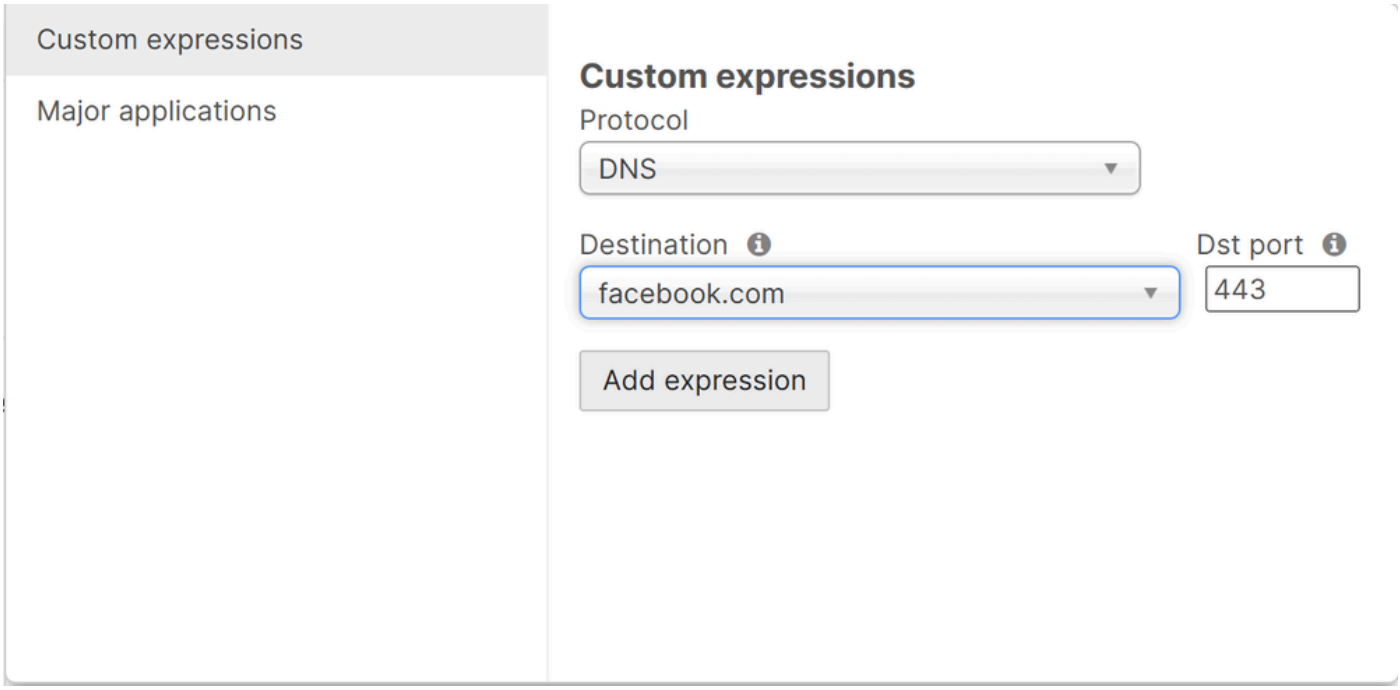
- 아래로 스크롤하여 섹션으로 **Local Internet Breakout** 이동한 다음 **Add+**

그런 다음 또는 을 기반으로 우회**Custom Expressions**를 **Major Applications**생성합니다.

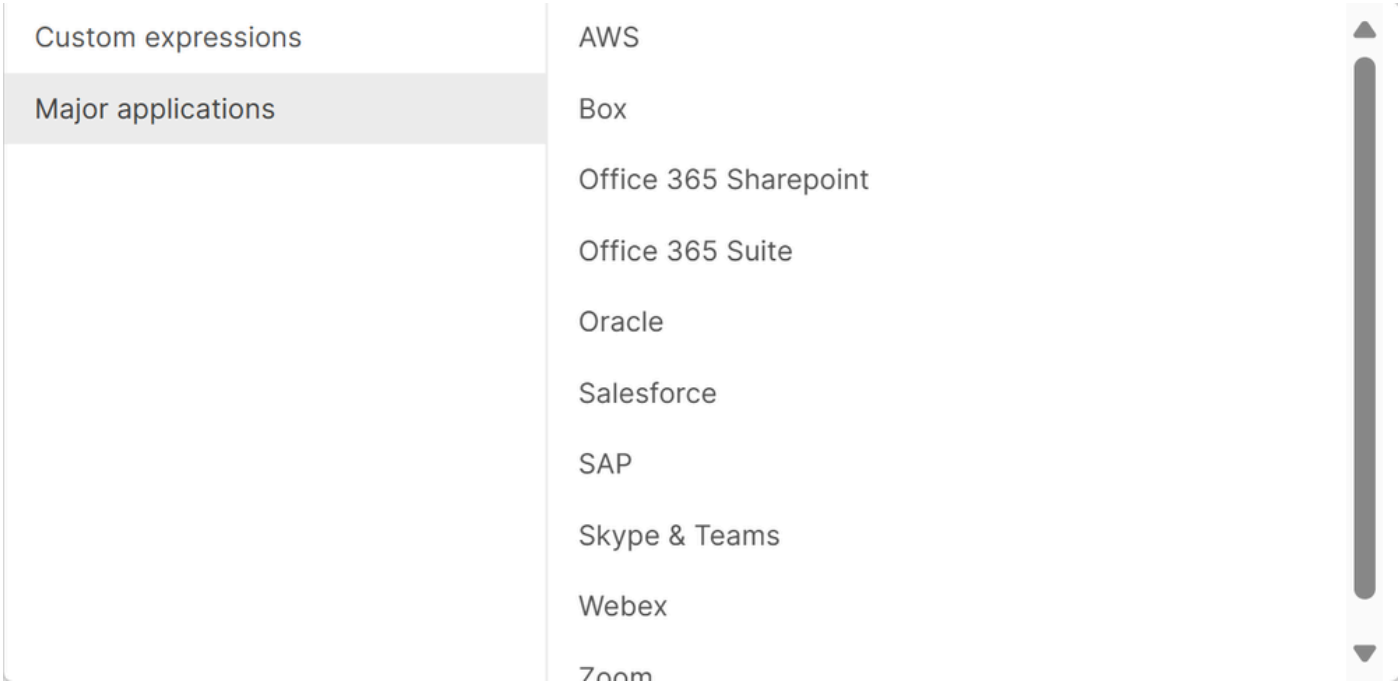
Custom Expressions - Protocol



Custom Expressions - DNS



Major Applications

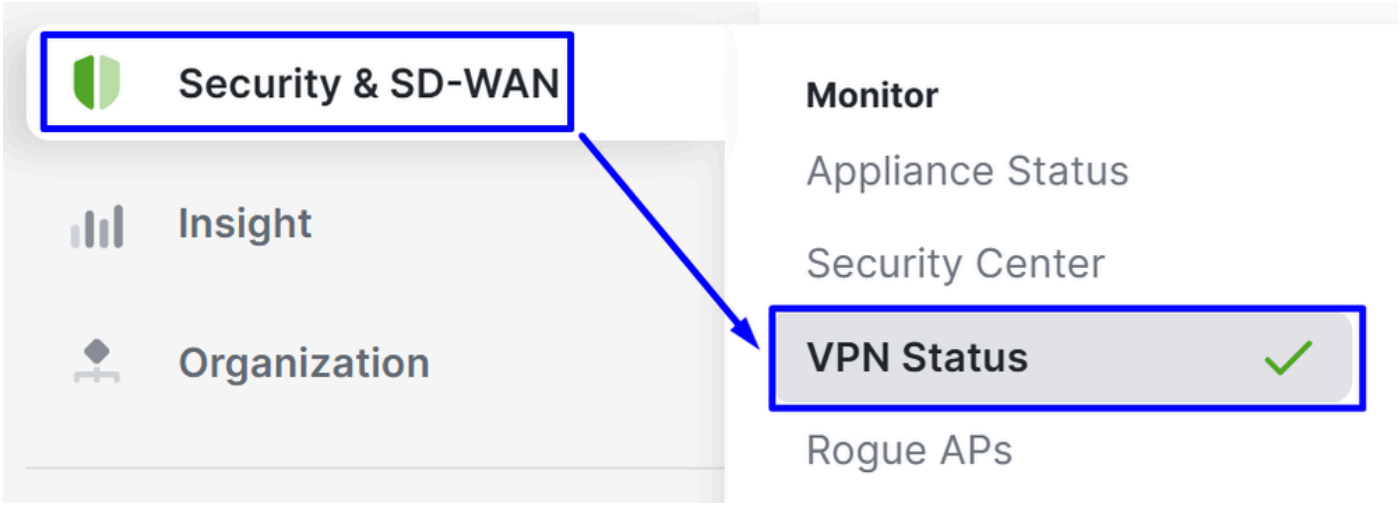


자세한 내용은 VPN 제외 규칙 구성(IP/포트/DNS/APP)을 참조하십시오.

다음을 확인합니다.

터널이 작동 중인지 확인하려면 의 상태를 확인하십시오.

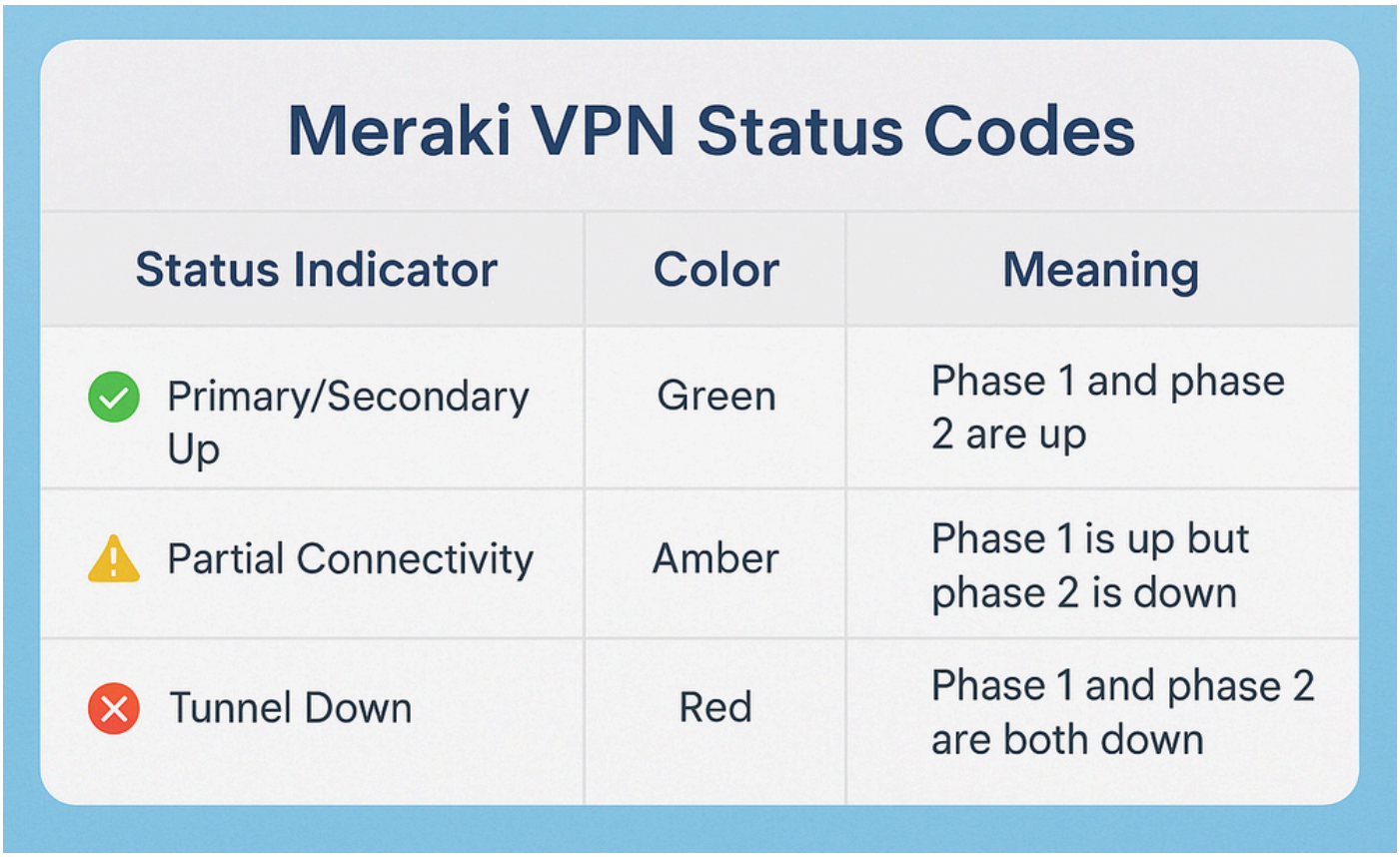
- Meraki Dashboard(Meraki 대시보드)에서Security & SD-WAN> **VPN Status** 을(를) 클릭합니다.



- 클릭 Non-Meraki peers:

Status ▲	Name	Public IP	Subnets	+
●	SSE-MERAKI Primary	18.156.145.74	0.0.0.0/0	
●	SSE-MERAKI Primary Secondary	3.120.45.23	0.0.0.0/0	
2 total				

기본 및 보조 VPN 상태가 모두 녹색으로 표시되면 터널이 작동 및 활성 상태임을 의미합니다.

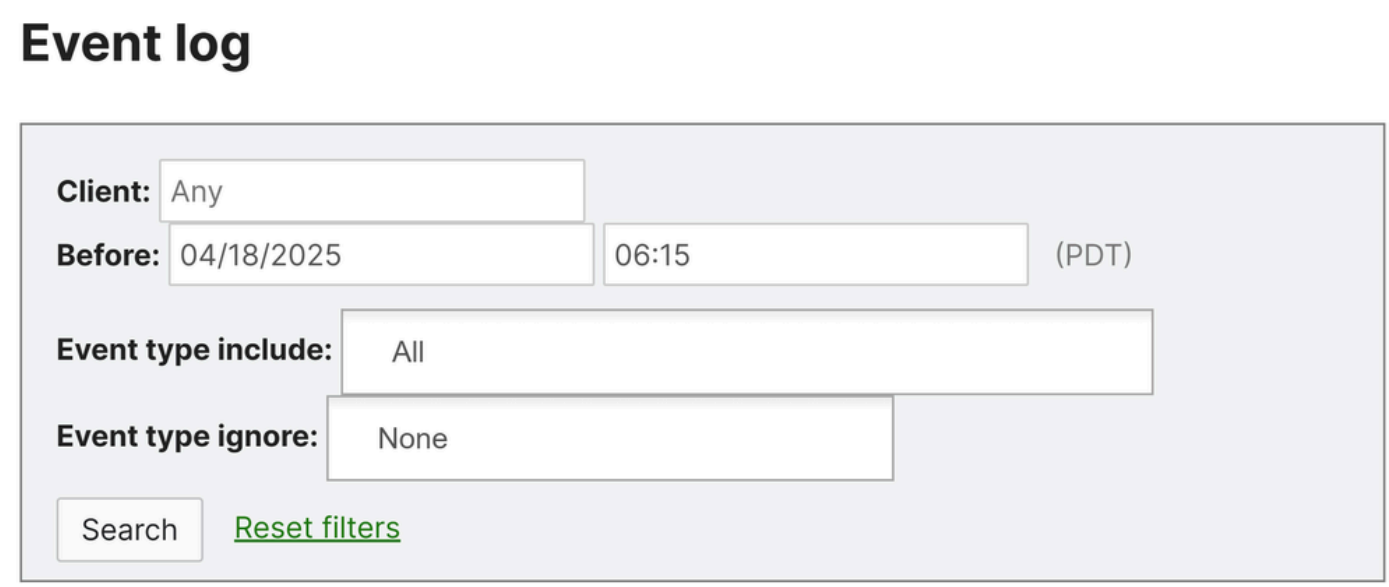


문제 해결

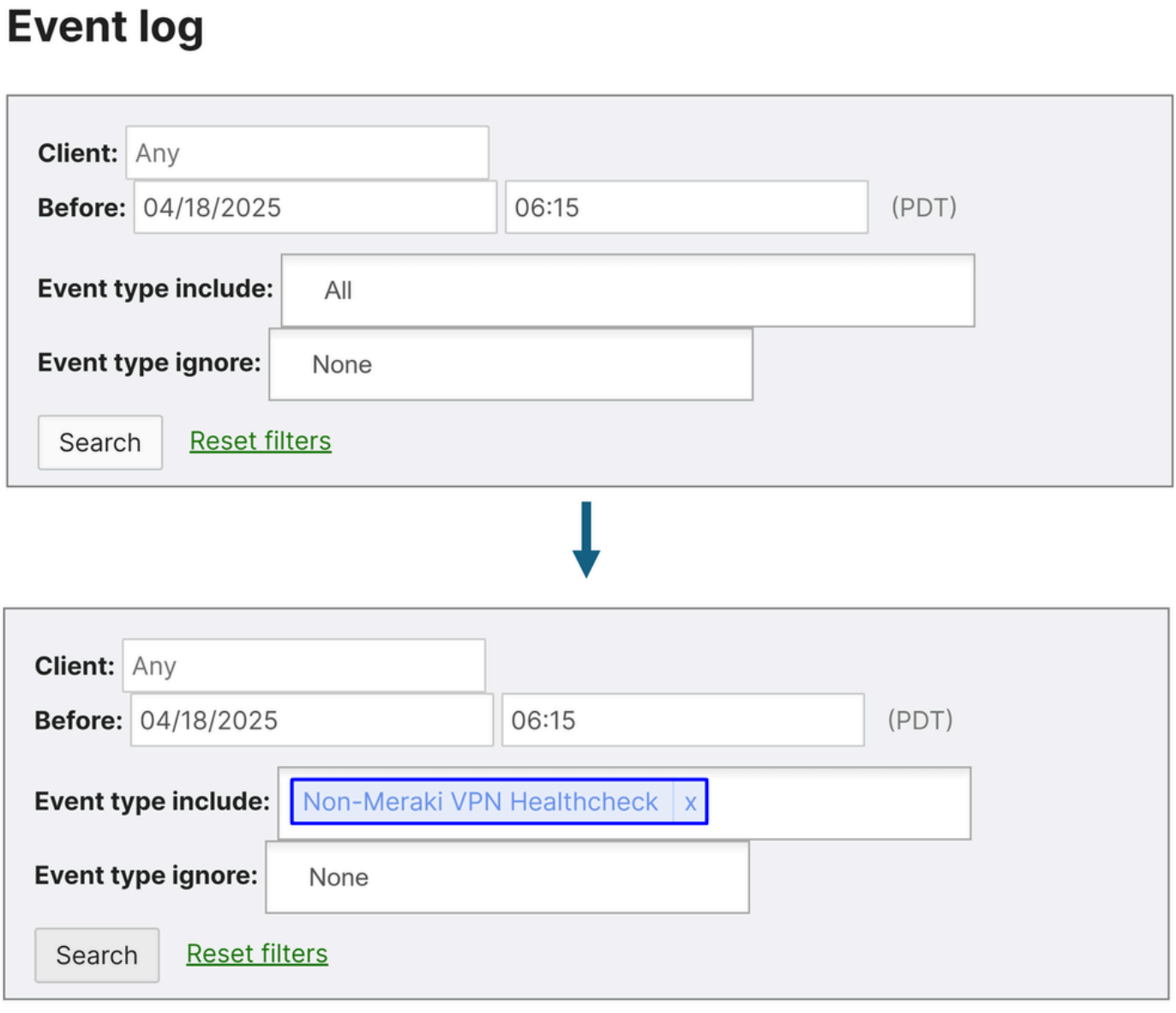
상태 확인

VPN에 대한 Meraki 상태 확인이 제대로 작동하는지 확인하려면 다음으로 이동합니다.

- 클릭 **Assurance** > Event Log

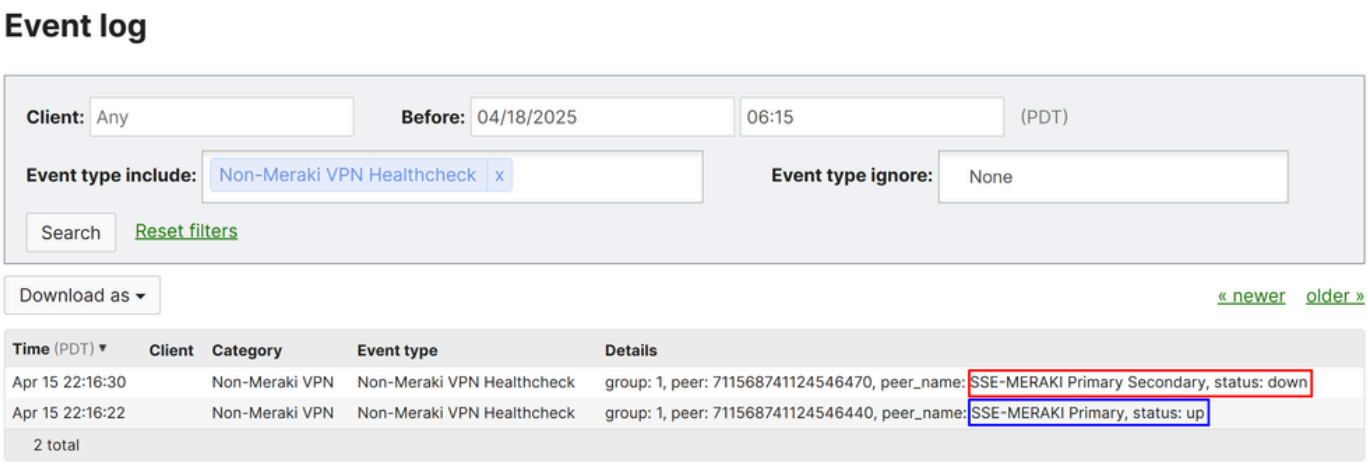


에서 **Event Type Include**을 선택합니다. Non-Meraki VPN Healthcheck



Cisco Secure Access에 대한 기본 터널이 활성 상태일 경우, 일관된 라우팅 경로를 유지하기 위해 보조 터널을 통해 도착하는 패킷이 삭제됩니다.

보조 터널은 스탠바이 상태로 유지되며, 상태 확인 메커니즘에 따라 Meraki 측에서 또는 Secure Access 내에서 기본 터널에 장애가 발생한 경우에만 사용됩니다.



- 기본 터널 상태 확인에는 상태가 표시됩니다. 즉, 현재 트래픽이 전달되고 있으며 능동적으로 트래픽을 전달합니다.
- 보조 터널 상태 확인에는 상태가 표시됩니다. 작동이 중지된 이유는 터널을 사용할 수 없기 때문이 아니라 기본 터널이 정상적이고 활발하게 사용되고 있기 때문입니다. 트래픽이 터널 1을 통과하도록 허용되어 보조 터널의 상태 확인에 실패하므로 이 동작이 예상됩니다.

관련 정보

- Cisco 기술 지원 및 다운로드
- Cisco Secure Access Help Center
- Cisco Secure Access Meraki BGP 컨피그레이션 가이드

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.