Beveiligde toegang configureren met Meraki MX voor bewaking van hoge beschikbaarheid en gezondheid

Inhoud

Inleiding

In dit document wordt beschreven hoe u Cisco Secure Access configureert met Meraki MX voor hoge beschikbaarheid met behulp van gezondheidscontroles.

Voorwaarden

- Bekijk de vereisten voor de IPsec-tunnel met beveiligde toegang
- Beveiligde toegangscomponenten begrijpen
- Begrijp Health Check Functionaliteit in Meraki MX

Vereisten

- Meraki MX moet firmwareversie 19.7.1 of hoger uitvoeren
- Bij het gebruik van Private Access wordt slechts één tunnel ondersteund vanwege een

Meraki-beperking die voorkomt dat de IP-health check wordt gewijzigd, waardoor NAT vereist is voor extra SPA-tunnels (Secure Private Access). Dit geldt niet bij gebruik van SIA (Secure Internet Access).
- Duidelijk definiëren welke interne subnetten of bronnen door de tunnel worden geleid naar Secure Access.

Gebruikte componenten

- Cisco Secure Access
- Meraki MX Security Appliance (firmwareversie 19.7.1 of hoger)
- Meraki-dashboard
- Dashboard voor beveiligde toegang

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Cisco Secure Access is een cloud-native beveiligingsplatform dat veilige toegang tot zowel privé-applicaties (via Private Access) als internetbestemmingen (via Internet Access) mogelijk maakt. Wanneer het wordt geïntegreerd met Meraki MX, kunnen organisaties beveiligde IPsec-tunnels tussen vestigingen en de cloud opzetten, waardoor een gecodeerde verkeersstroom en gecentraliseerde beveiligingshandhaving worden gewaarborgd.

Deze integratie maakt gebruik van statische routing IPsec-tunnels. Meraki MX richt primaire en secundaire IPsec-tunnels op voor Cisco Secure Access en maakt gebruik van de ingebouwde uplink-gezondheidscontroles om automatische failover tussen tunnels uit te voeren. Dit biedt een robuuste configuratie met hoge beschikbaarheid voor connectiviteit met vestigingen.

De belangrijkste elementen van deze implementatie zijn:

- Meraki MX fungeert als een niet-Meraki VPN-peer voor Cisco Secure Access.
- Primaire en secundaire tunnels worden statisch geconfigureerd, waarbij de beschikbaarheid wordt bepaald door gezondheidscontroles.
- Private Access ondersteunt veilige toegang tot interne applicaties via SPA (Secure Private Access), terwijl Internet Access verkeer in staat stelt om op internet gebaseerde bronnen te

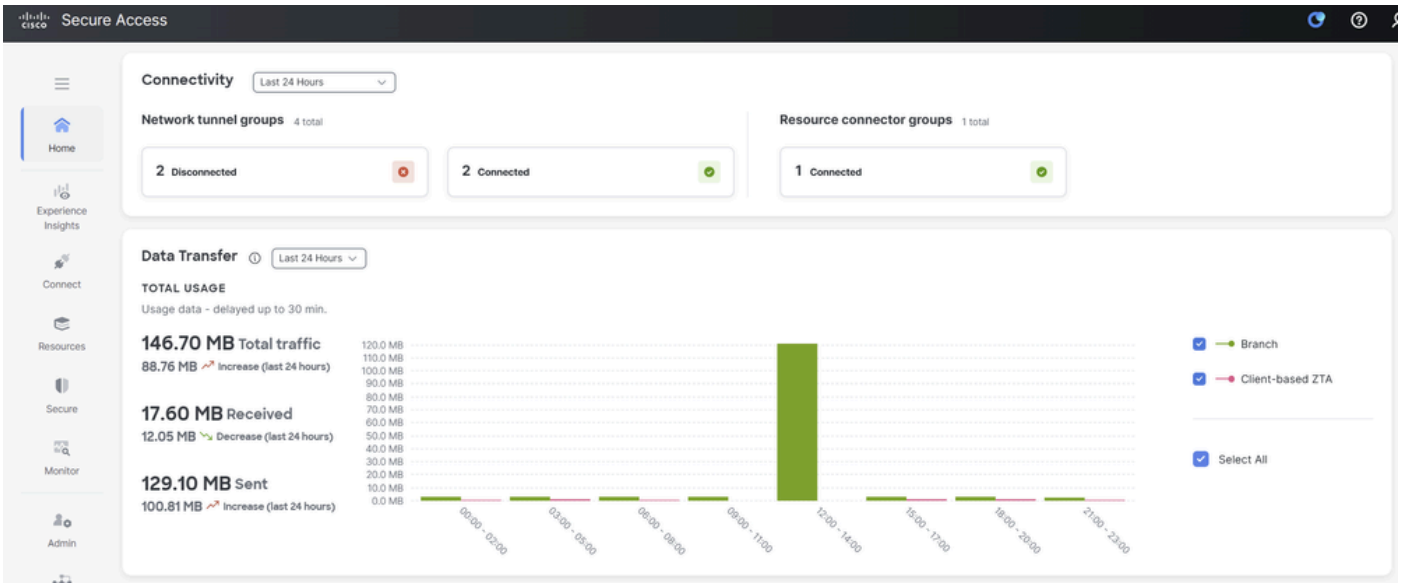
bereiken met beleidshandhaving in de cloud.

- Vanwege de beperkingen van Meraki in de IP-flexibiliteit van de health check wordt slechts één tunnelgroep ondersteund in de modus Privé toegang. Als meerdere Meraki MX-apparaten verbinding moeten maken met Secure Access for Private Access, moet u BGP gebruiken voor dynamische routering of statische tunnels configureren, met dien verstande dat slechts één netwerktunnelgroep gezondheidscontroles en hoge beschikbaarheid kan ondersteunen. Extra tunnels werken zonder gezondheidsbewaking of redundantie.

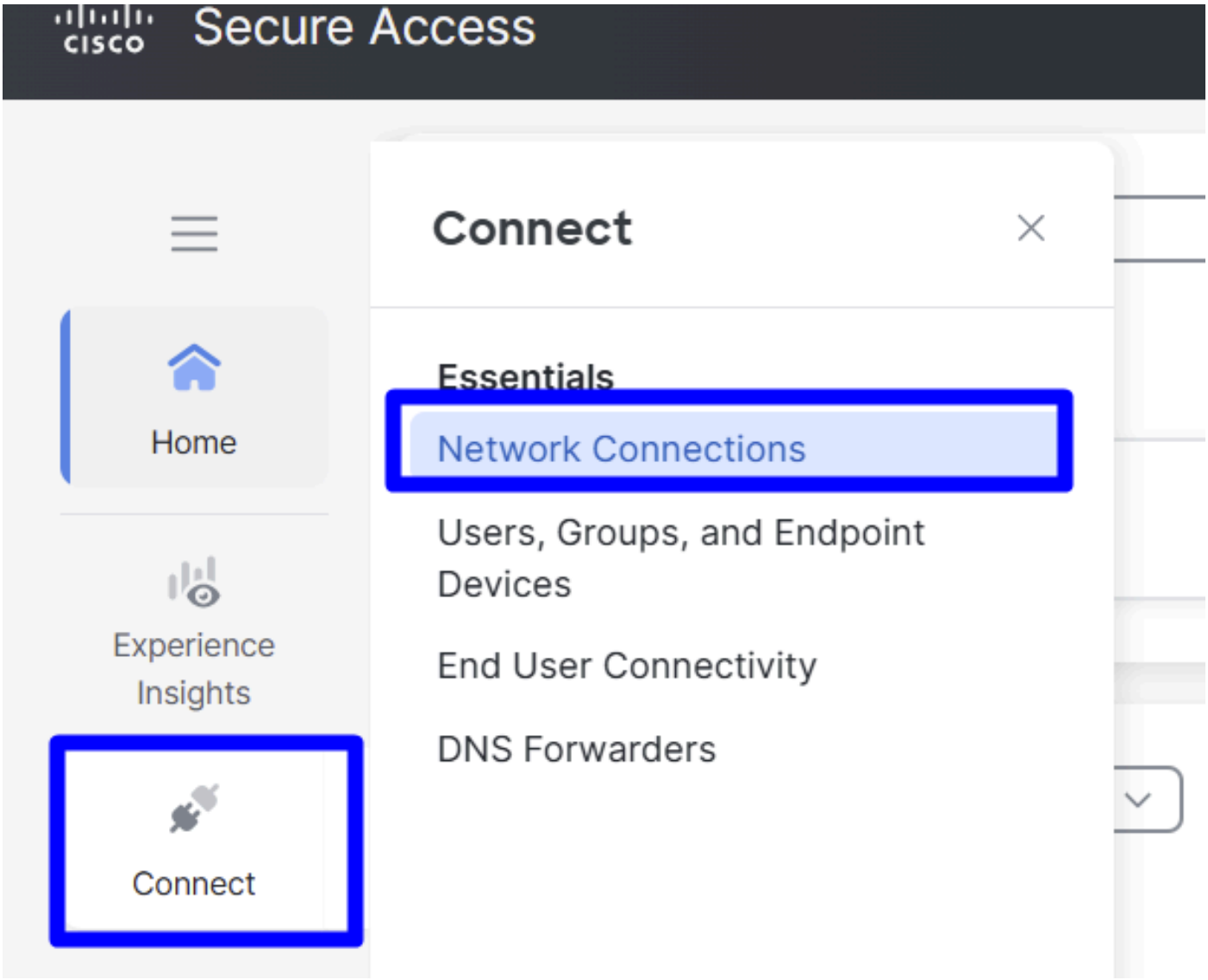
Configureren

VPN configureren voor beveiligde toegang

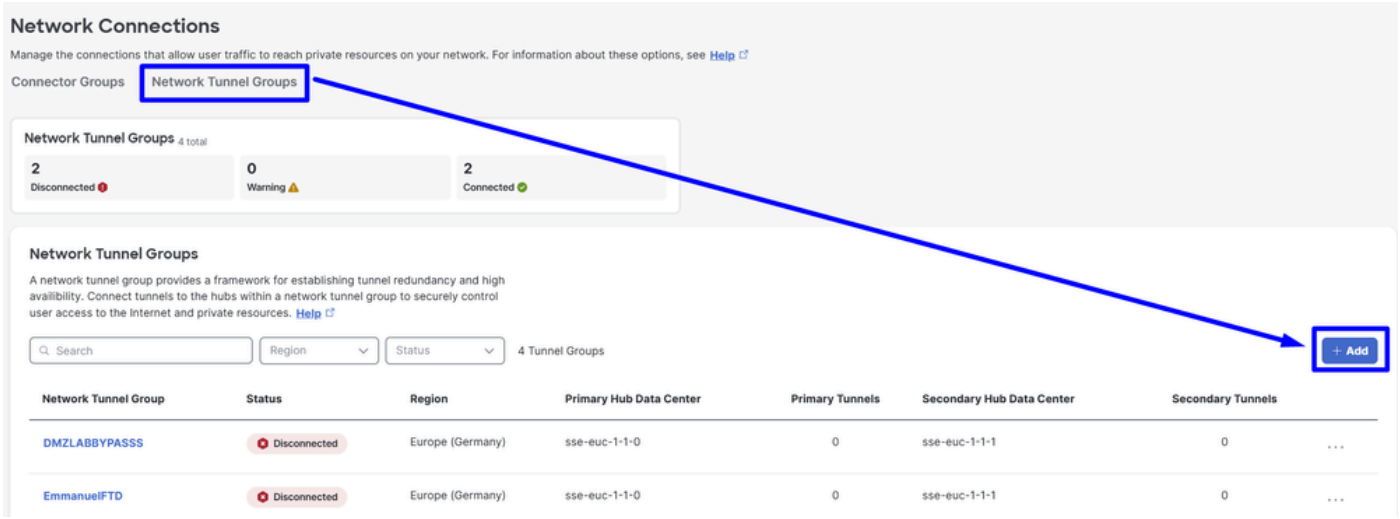
Navigeer naar het beheerderspaneel van Secure Access.



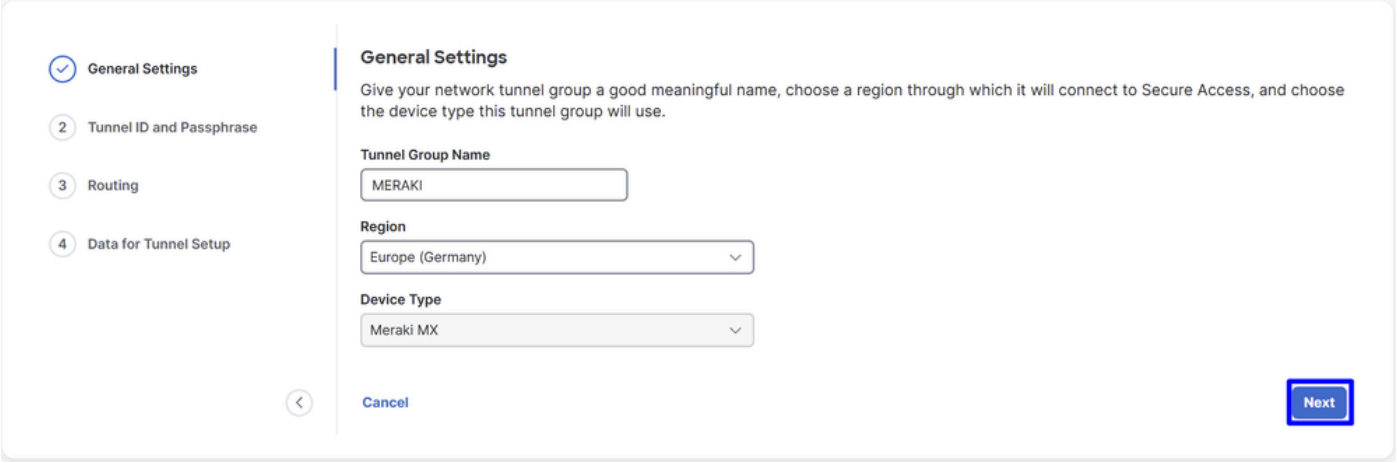
- Klik op Connect > Network Connections



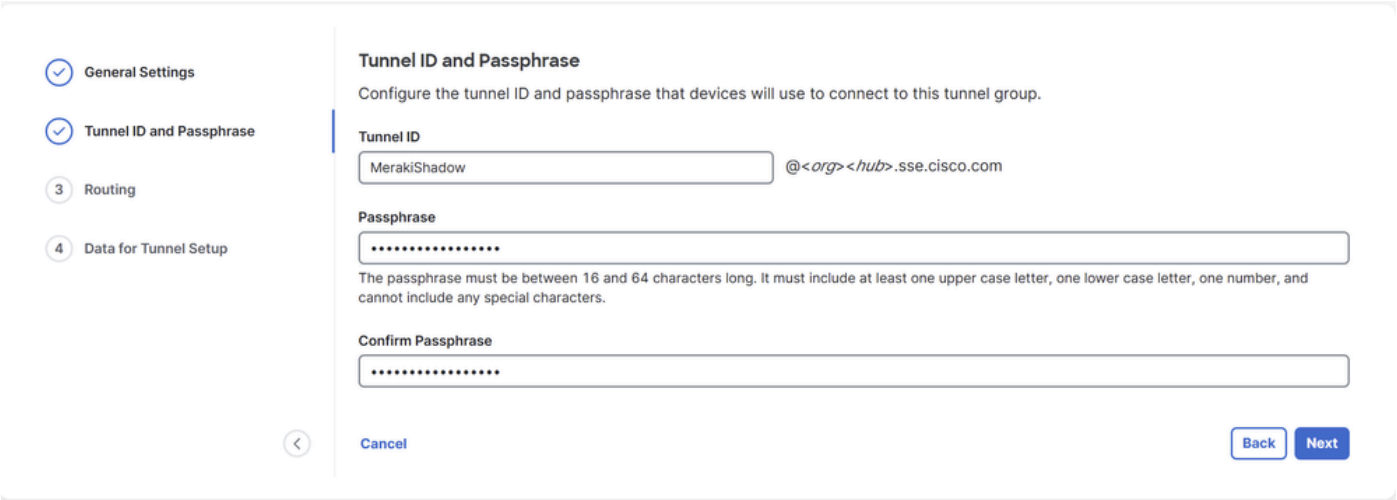
- Onder Network Tunnel Groups klik op + Add



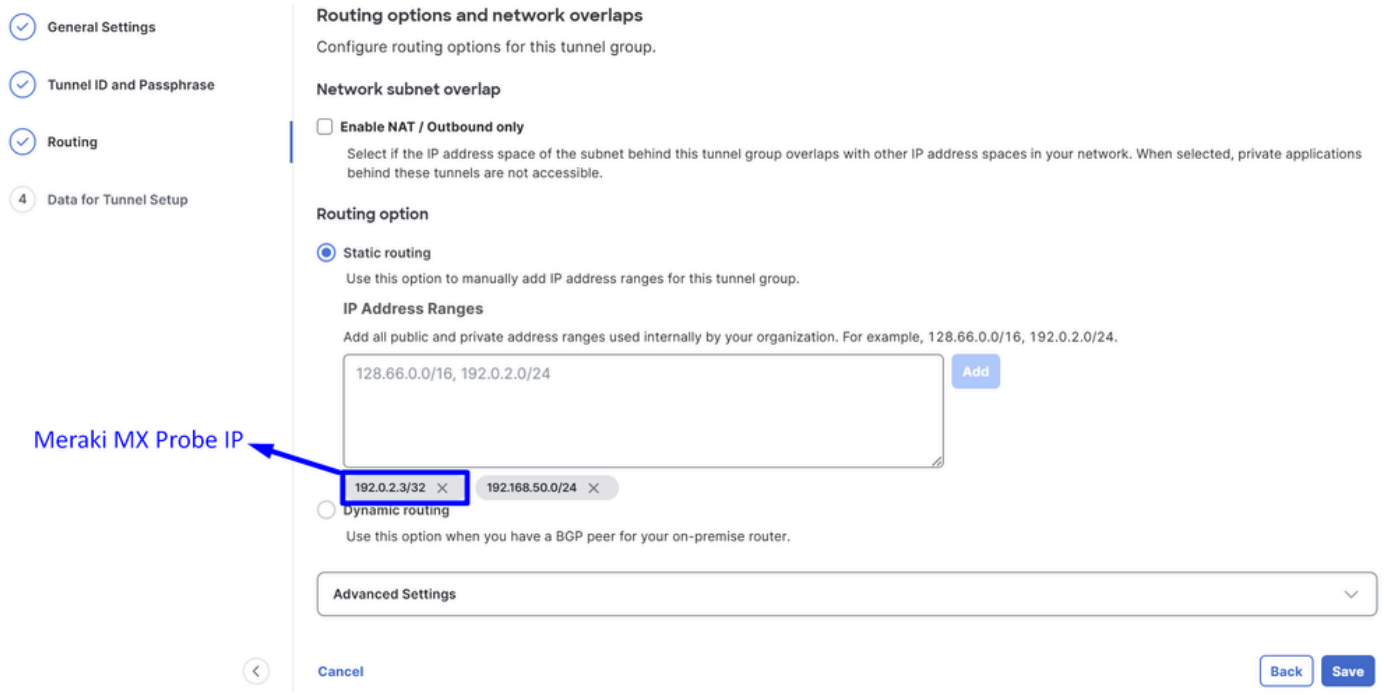
- Configureren Tunnel Group Name, Region en Device Type
- Klik op de knop **Next**

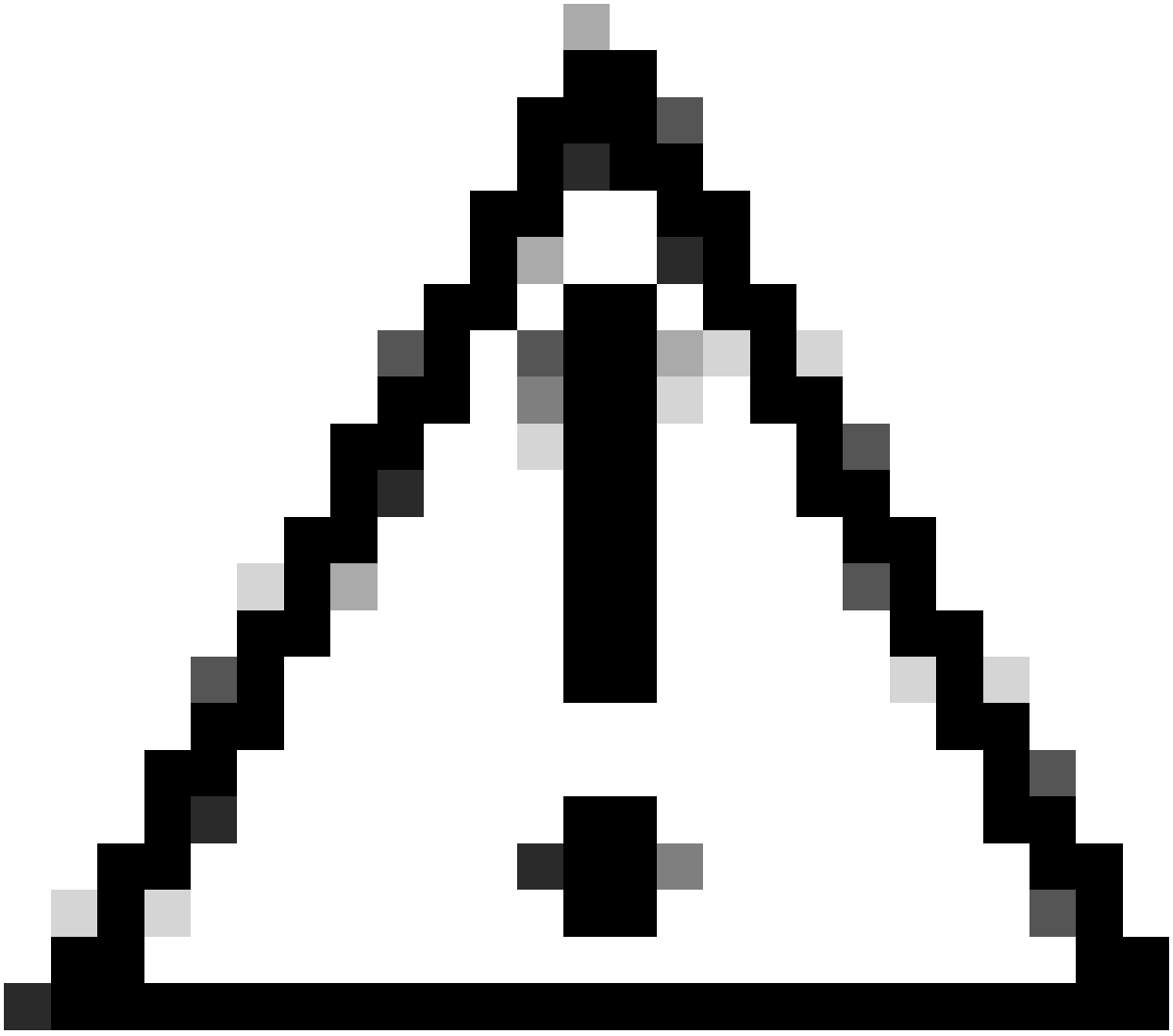


- Configureer deTunnel ID Formaten Passphrase
- Klik op de knop Next



- Configureer de IP-adresbereiken of hosts die u op uw netwerk hebt geconfigureerd en die het verkeer via Secure Access willen doorgeven en zorg ervoor dat u de Meraki-controleprobe IP 192.0.2.3/32 opneemt om retourverkeer van Secure Access terug naar de Meraki MX mogelijk te maken.
- Klik op de knop Save


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

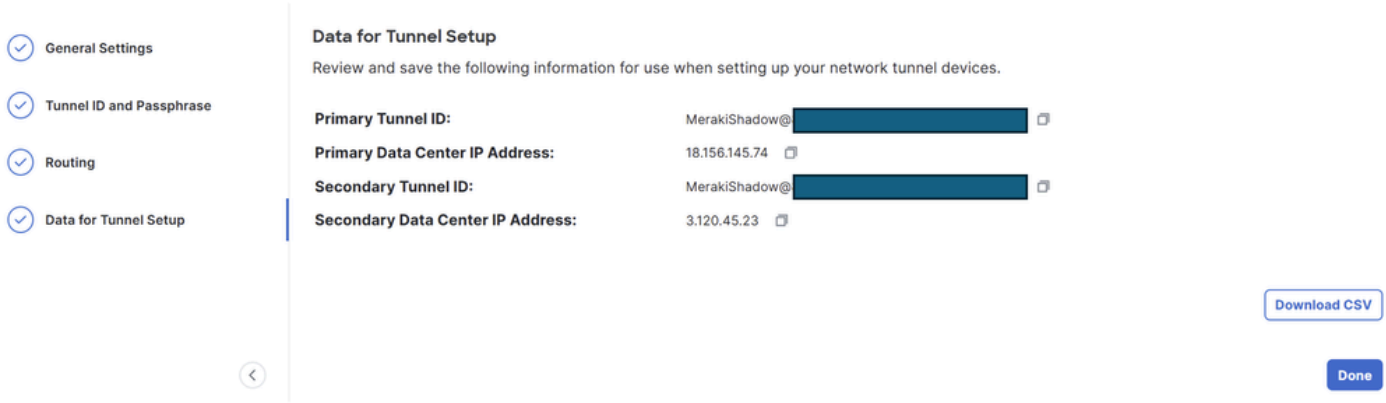


Let op: Zorg ervoor dat u de controleprobe IP (192.0.2.3/32) toevoegt; anders kunt u verkeersproblemen ondervinden op het Meraki-apparaat dat het verkeer naar internet, VPN-pools en CGNAT-bereik 100.64.0.0/10 leidt dat wordt gebruikt door ZTNA.

- Nadat u hebt geklikt op **Save** de informatie over de tunnel die wordt weergegeven, kunt u die informatie opslaan voor de volgende stap, **Configure the tunnel on Meraki MX.**

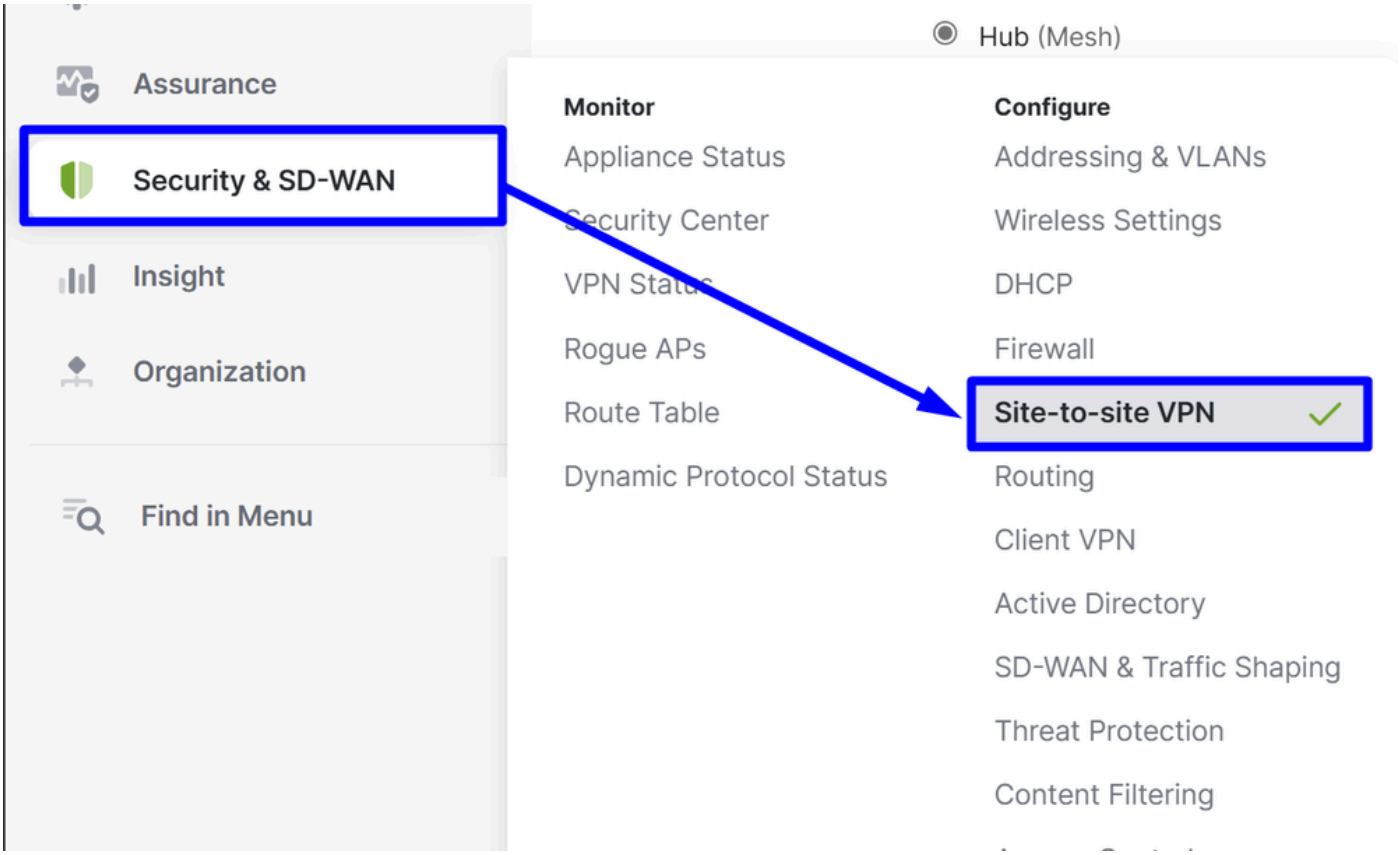
VPN-configuratie met beveiligde toegang

Kopieer de configuratie van de tunnels in een notitieblok, Gebruik deze informatie om de configuratie in Meraki te **Non-Meraki VPN Peers**voltooien.



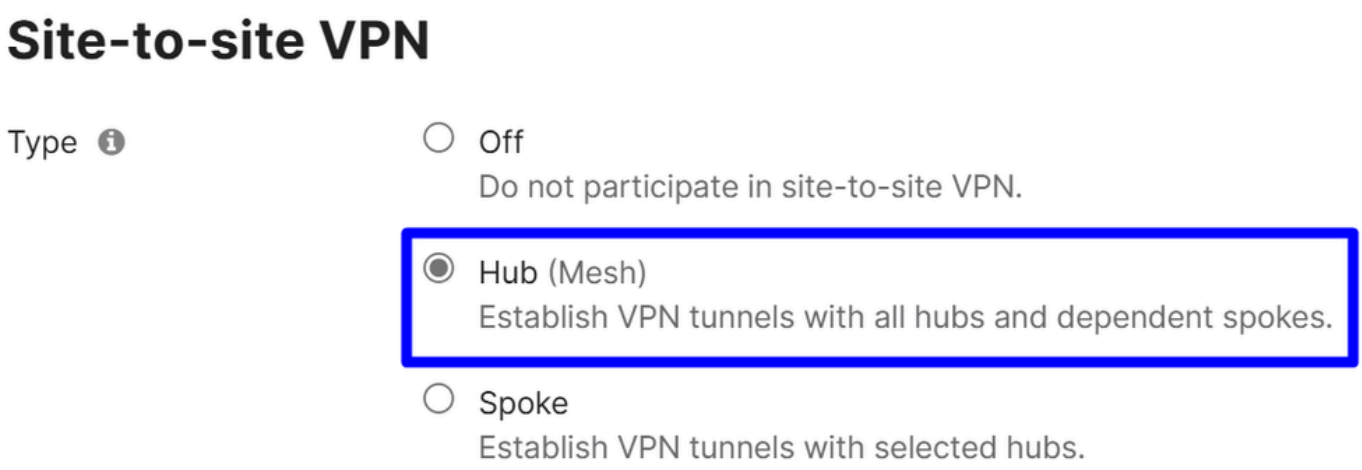
Configureer de VPN op Meraki MX

Navigeer naar je Meraki MX en klik op **Security & SD-WAN** > Site-to-site VPN



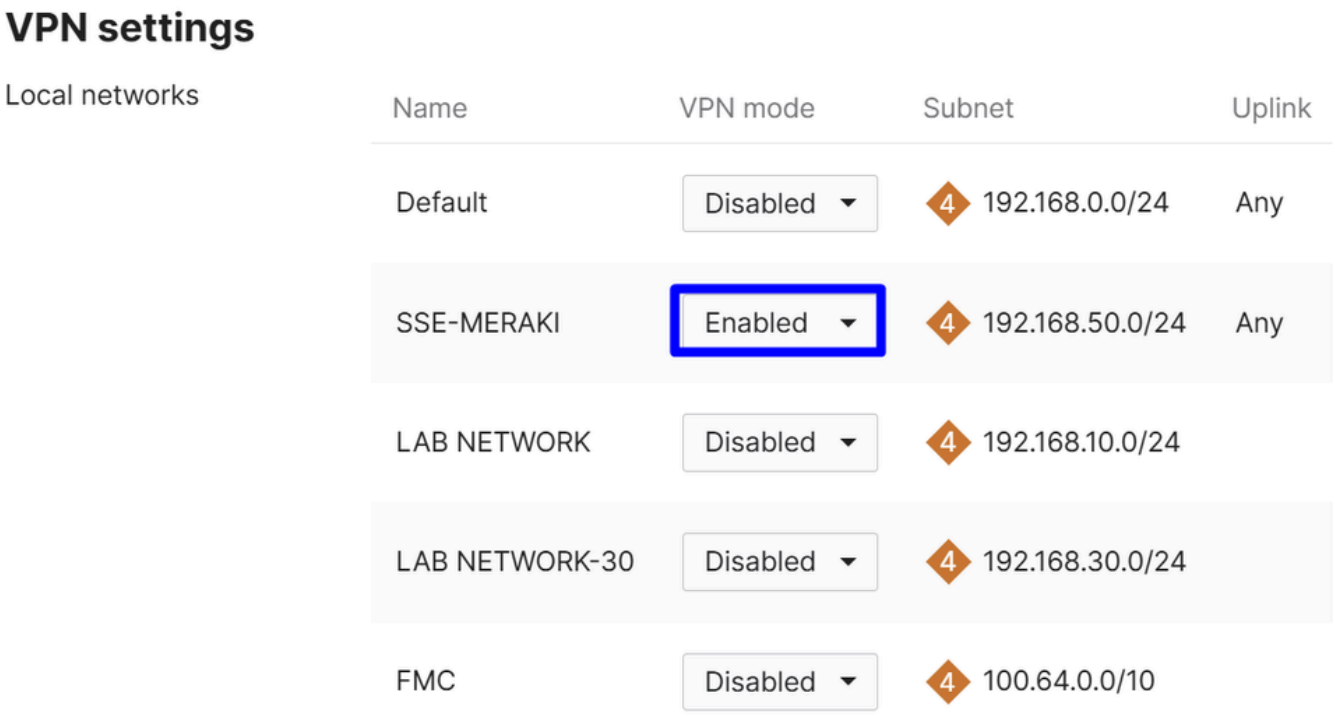
Site-to-site VPN

kiezen Hub.

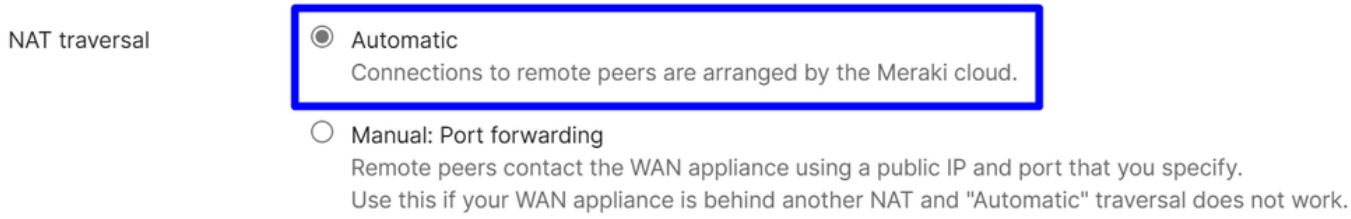


VPN-instellingen

Kies de netwerken die u hebt geselecteerd voor het verzenden van verkeer naar Secure Access:



Kiezen in**NAT Traversal**Automatisch



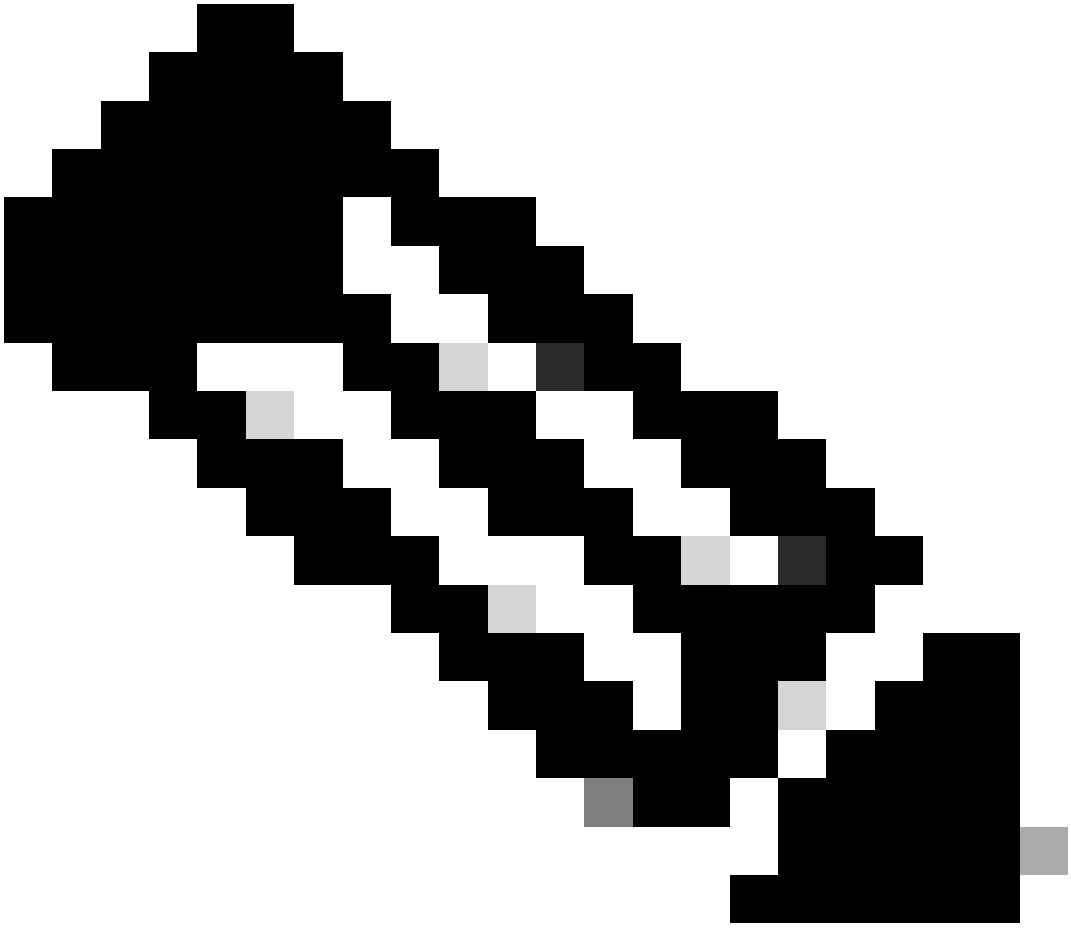
Niet-Meraki VPN-peers

U moet de gezondheidscontroles configureren die Meraki gebruikt om verkeer naar Secure Access te leiden:

Klik op **Configure Health Checks**

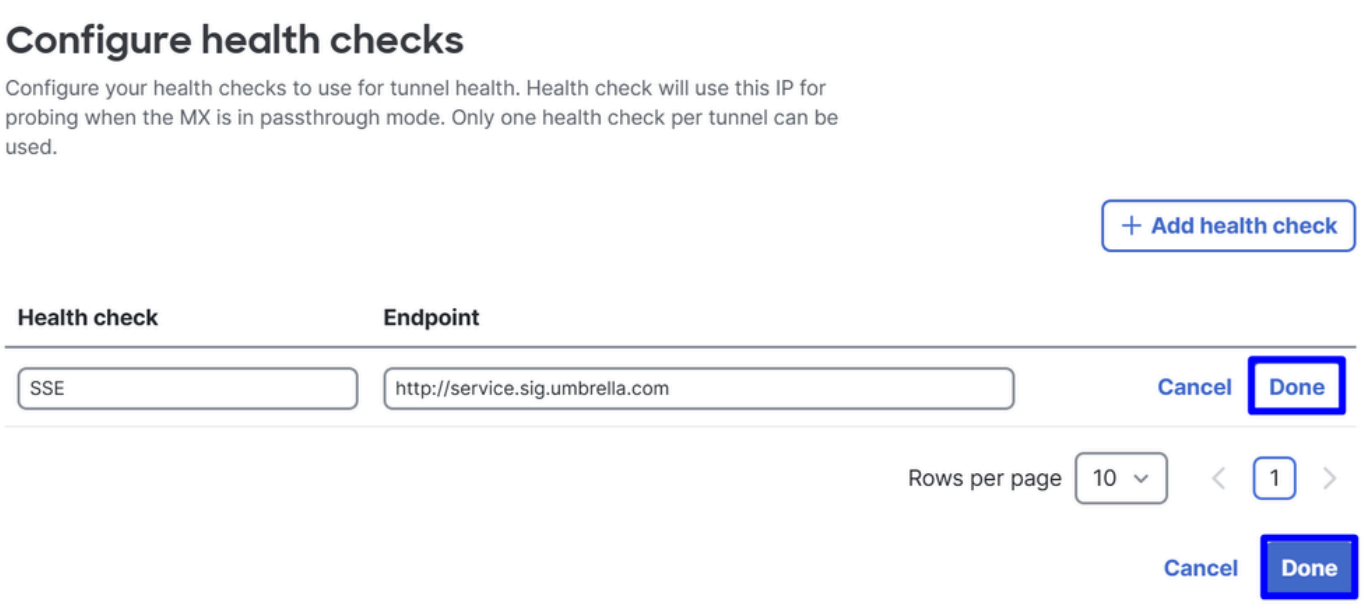
- Klik op **+Add health Check**

- **Health Check**: Configureer een naam voor de test
- **Endpoint**: Gebruik degene die wordt aanbevolen door Secure Access **http://service.sig.umbrella.com**



Opmerking: dit domein reageert alleen wanneer het wordt geopend via een site-to-site tunnel met beveiligde toegang of paraplu: toegangspogingen van buiten deze tunnels mislukken.

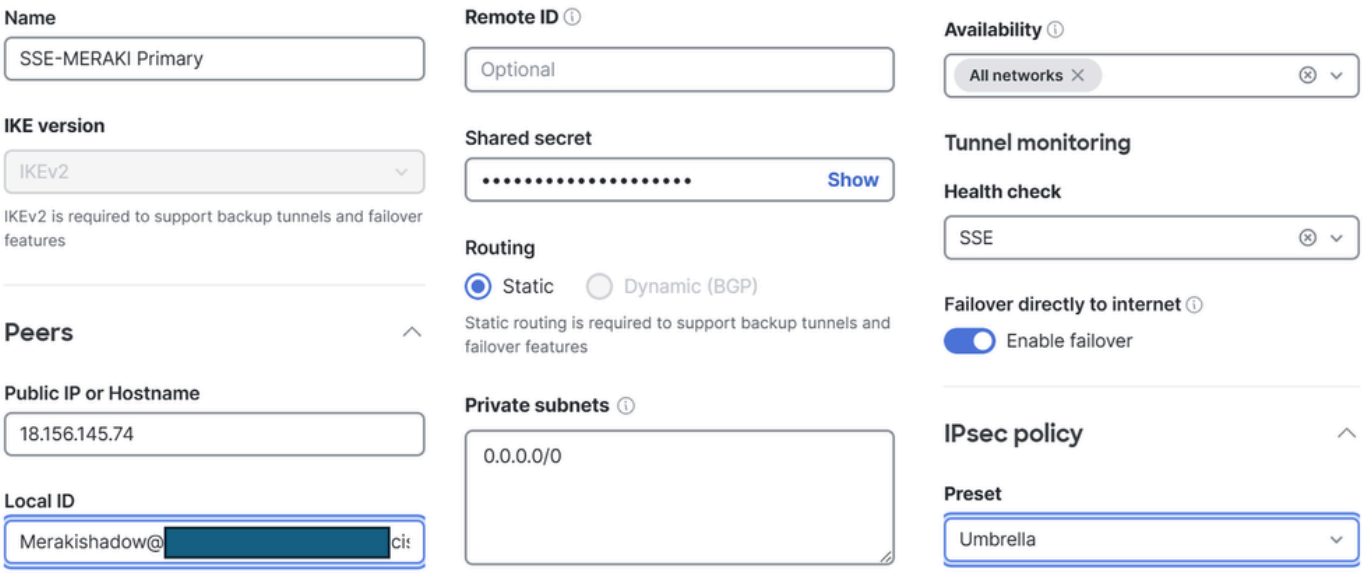
Klik vervolgens **Done** twee keer om te voltooien.



Nu zijn uw gezondheidscontroles geconfigureerd en bent u klaar om de **Peer:**

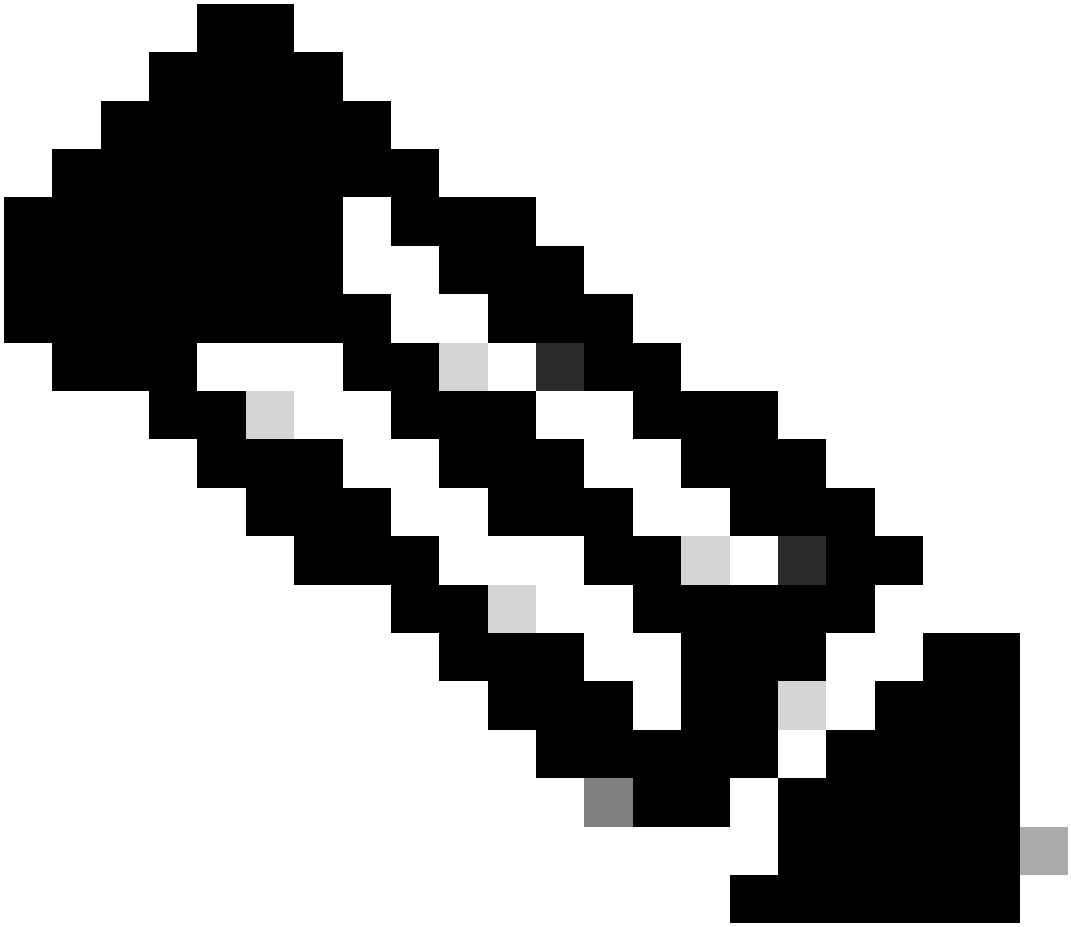
Primaire tunnel configureren

- Klik op+Add a peer



- VPN-peer toevoegen
  - Naam: Configureer een naam voor de VPN naar Secure Access
  - IKE-versie: kies IKEv2
- gelijken
  - Publieke IP of Hostname: Configureer het **Primary Datacenter IP** gegeven door Secure Access in de stap Secure Access VPN Configurations
  - Lokale ID: Configureer de informatie **Primary Tunnel ID** die wordt gegeven door Secure Access in de stap Beveiligde toegang VPN-configuraties
  - Externe ID: niet beschikbaar
  - Gedeeld geheim: Configureer de informatie **Passphrase** die wordt gegeven door Secure

Access in de stap Beveiligde toegang VPN-configuraties
    - Routering: Statisch kiezen
    - Privé-subnetten: Als u van plan bent om zowel Internet Access als Private Access te configureren, gebruikt u deze **0.0.0.0/0** als bestemming. Als u alleen Private Access voor die VPN-tunnel configureert, specificeert u het bereik **Remote Access VPN IP Pool** en het CGNAT-bereik **100.64.0.0/10** als bestemmingsnetwerken
    - Beschikbaarheid: Als u slechts één Meraki-apparaat hebt, kunt u **All Networks**selecteren. Als u meerdere apparaten hebt, moet u alleen het specifieke Meraki-netwerk selecteren waar u de tunnel configureert.
- tunnelbewaking
    - Gezondheidscontrole: gebruik de eerder geconfigureerde gezondheidscontrole om de beschikbaarheid van de tunnel te controleren
    - Failover rechtstreeks naar internet: Als u deze optie inschakelt en zowel Tunnel 1 als Tunnel 2 hun gezondheidscontroles niet uitvoeren, wordt het verkeer omgeleid naar de WAN-interface om verlies van internettoegang te voorkomen.



Health Check Functionaliteit: Als Tunnel 1 wordt bewaakt en de health check mislukt, gaat

---

het verkeer automatisch over naar Tunnel 2. Als ook Tunnel 2 uitvalt en de optie Failover directly to Internet is ingeschakeld, wordt het verkeer via de WAN-interface van het Meraki-apparaat geleid.

- IPsec-beleid
  - voorinstelling: kiezen **Umbrella**

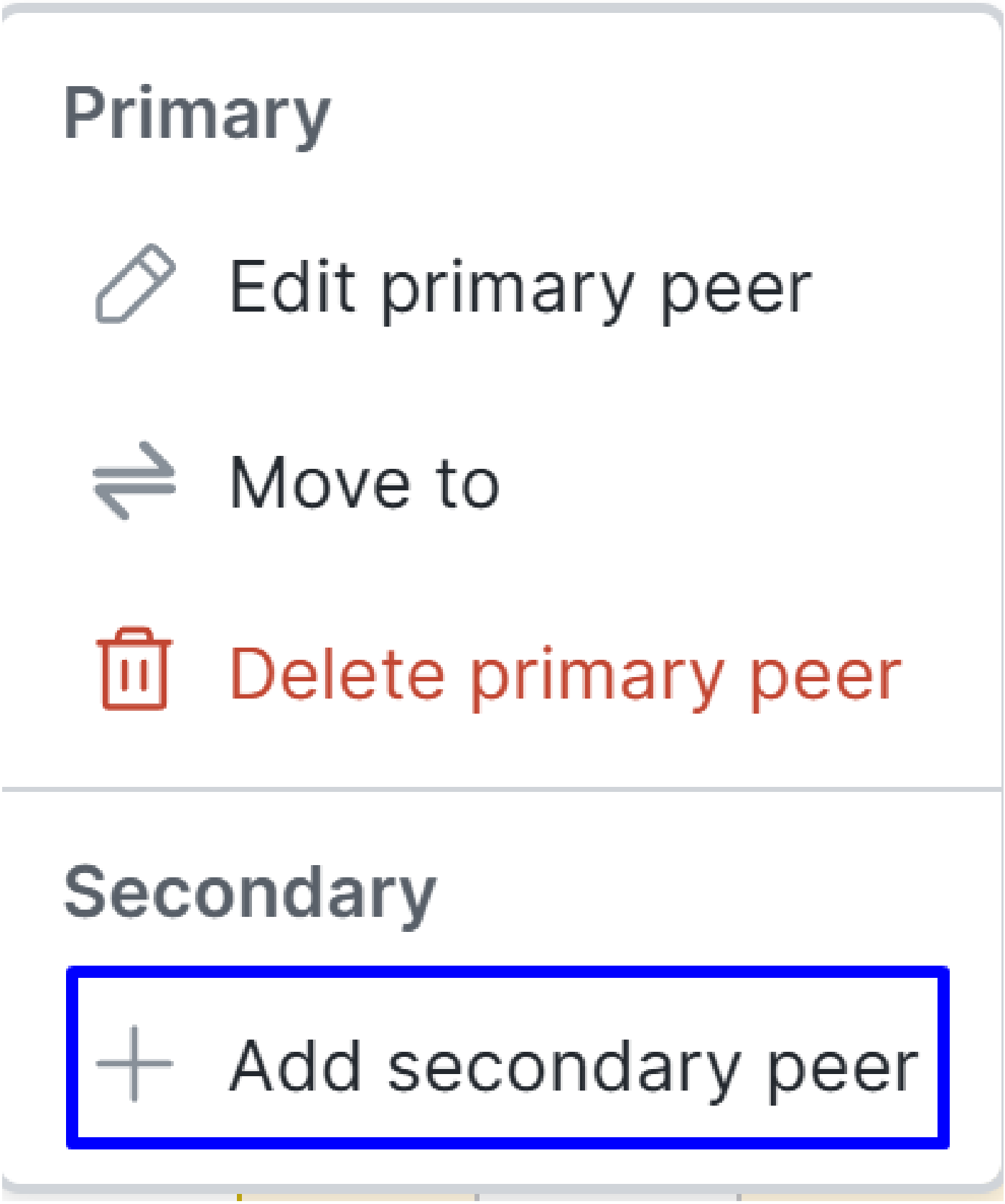
Klik vervolgens **Save** op.

Secundaire tunnel configureren

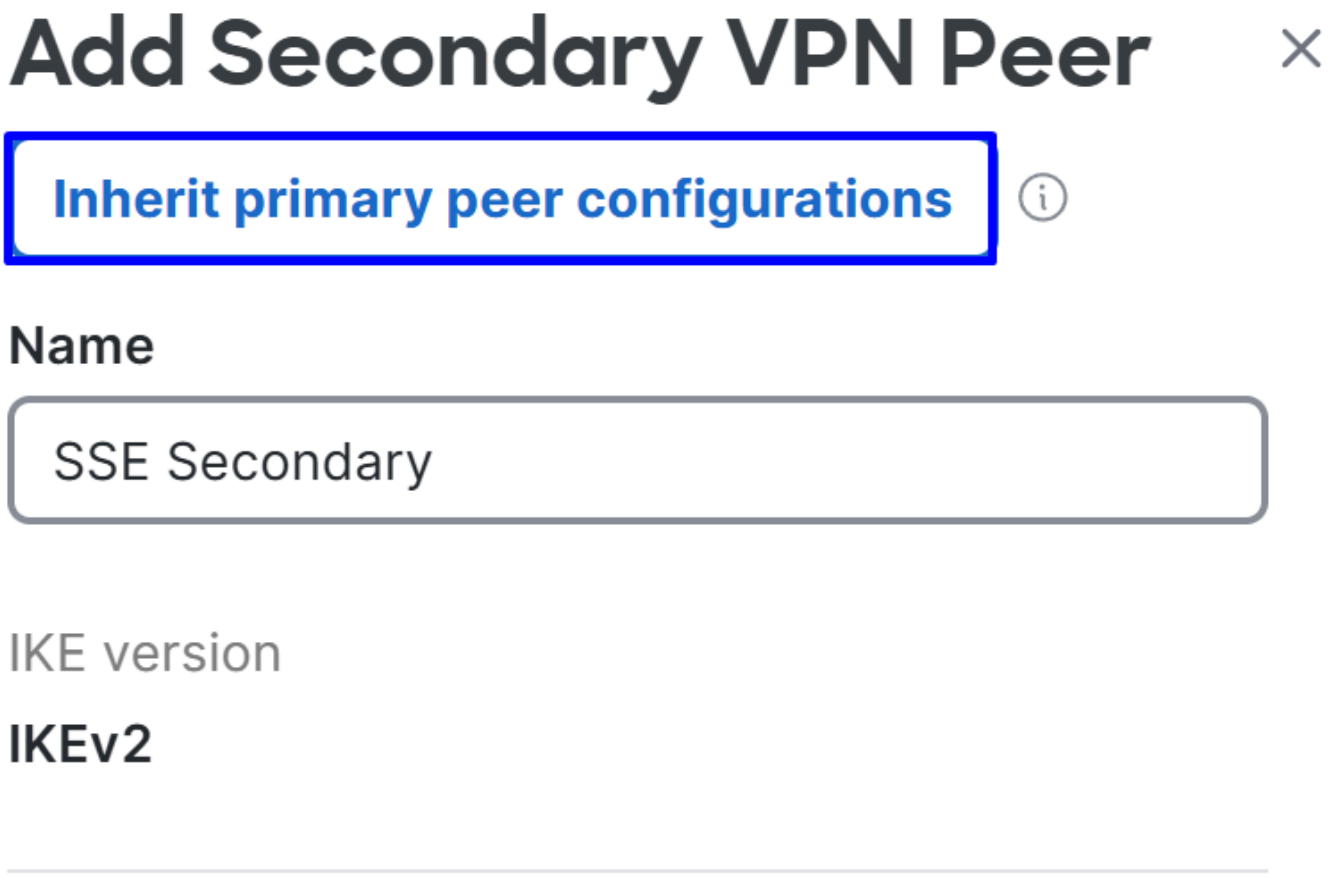
Als u de secundaire tunnel wilt configureren, klikt u op het optiemenu van de primaire tunnel:

- Klik op de drie puntjes

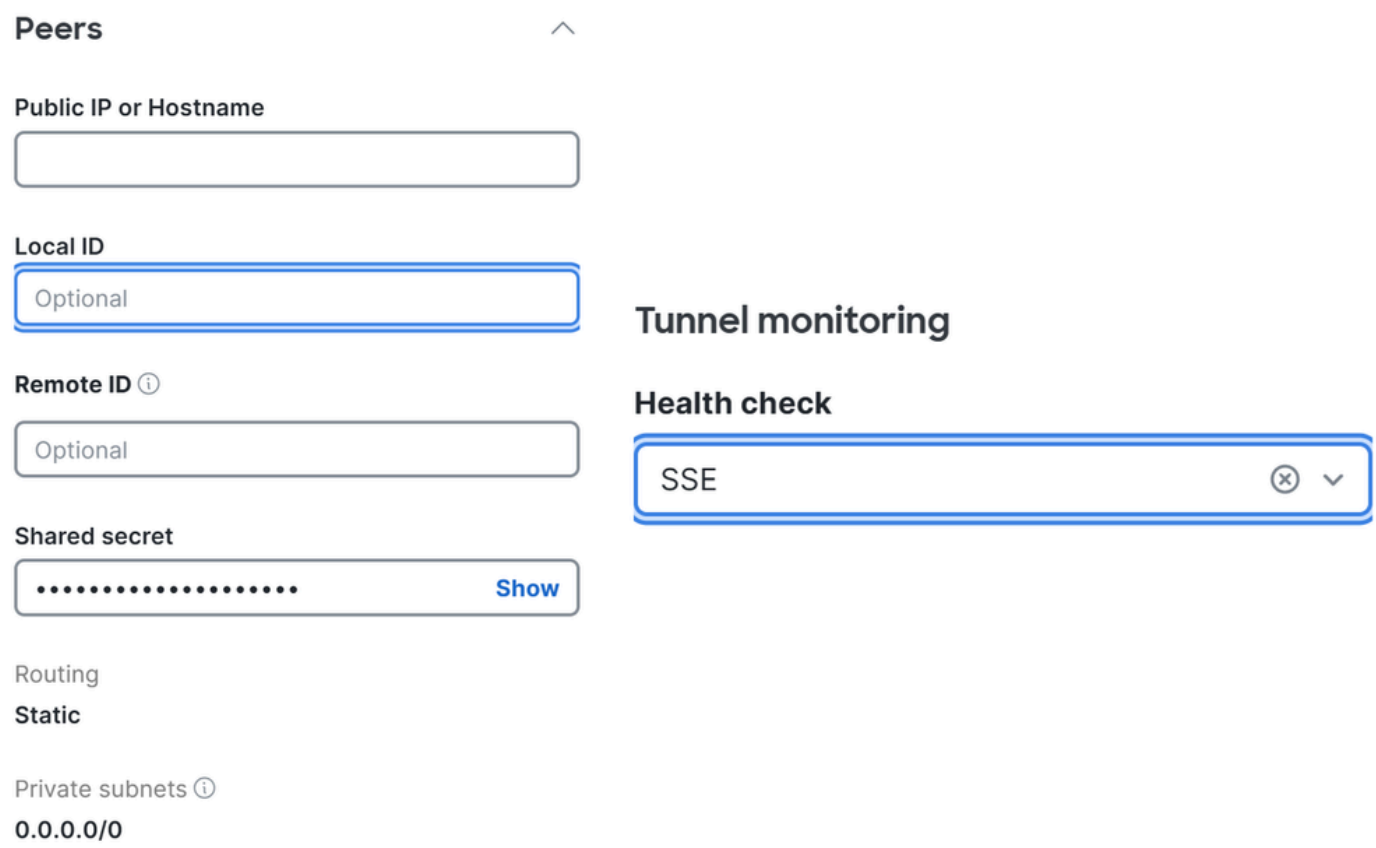
- Klik op + Add Secondary peer



- Klik opInherit primary peer configurations

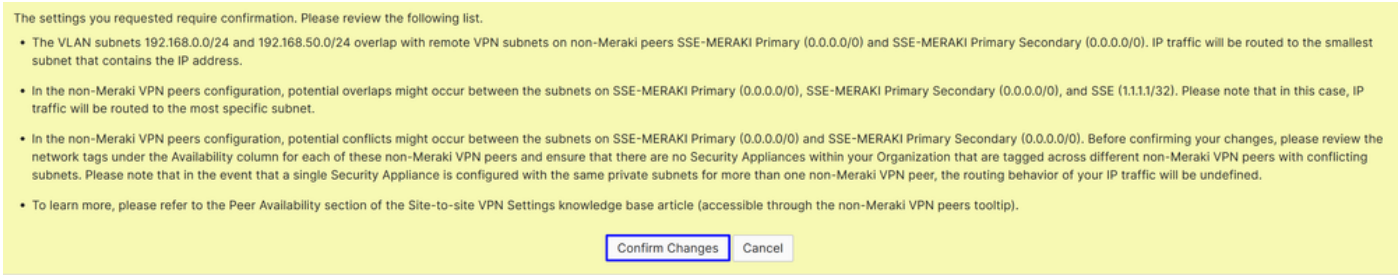


Dan merk je dat sommige velden automatisch worden ingevuld. Bekijk ze, breng de nodige wijzigingen aan en vul de rest handmatig in:



- gelijken
  - Publieke IP of Hostname: Configureer het **Secondary Datacenter IP** gegeven door Secure Access in de stap Secure Access VPN Configurations
  - Lokale ID: Configureer de informatie **Secondary Tunnel ID** die wordt gegeven door Secure Access in de stap Beveiligde toegang VPN-configuraties
  - Externe ID: niet beschikbaar
  - Gedeeld geheim: Configureer de informatie **Passphrase** die wordt gegeven door Secure Access in de stap Beveiligde toegang VPN-configuraties
- tunnelbewaking
  - Gezondheidscontrole: gebruik de eerder geconfigureerde gezondheidscontrole om de beschikbaarheid van de tunnel te controleren

Daarna kunt u klikken **Save**en de volgende waarschuwing wordt weergegeven:

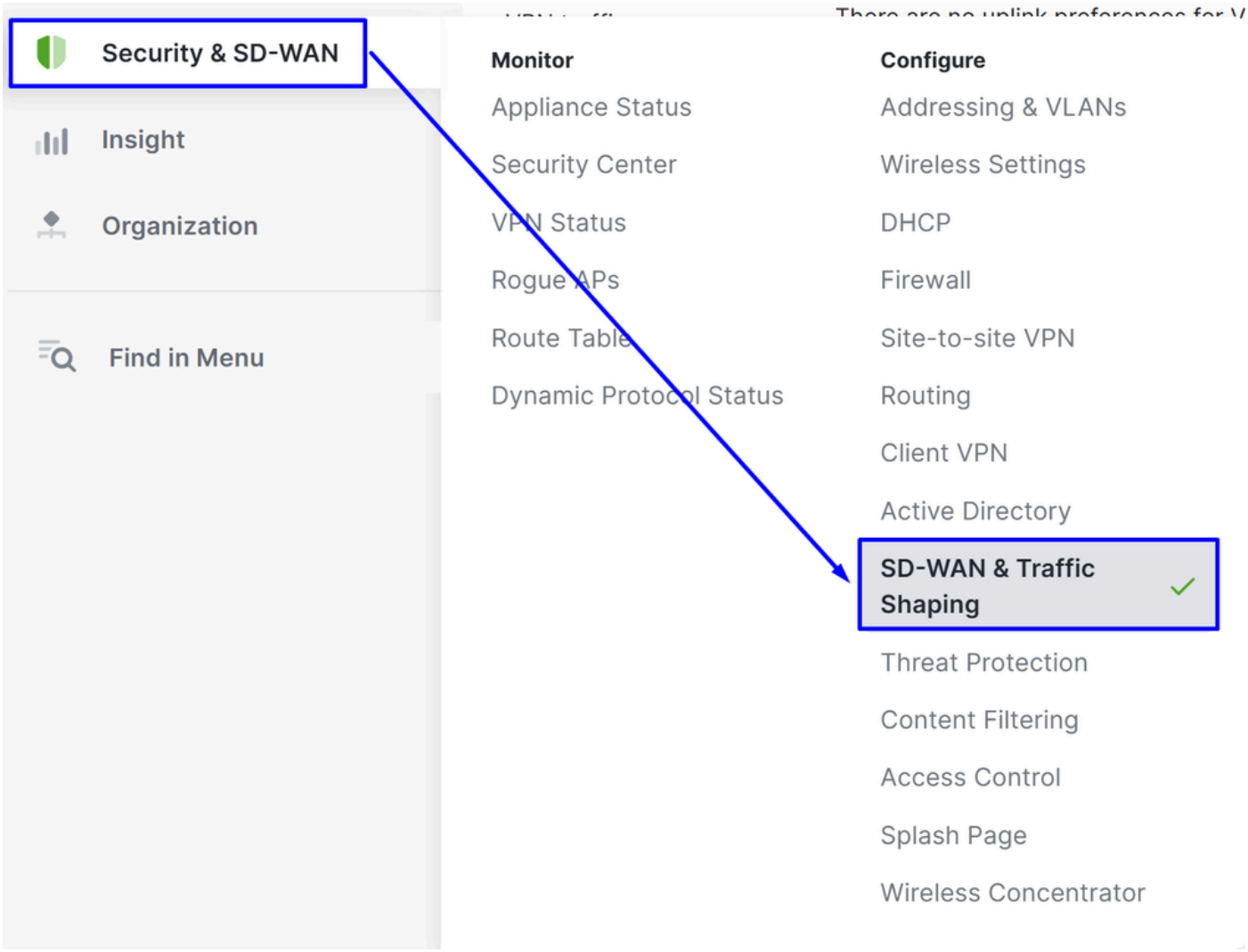


Maak je geen zorgen over een klik **Confirm Changes**.

Verkeerssturing configureren (tunnelverkeersomgeving)

Met deze functie kunt u specifiek verkeer uit de tunnel omzeilen door domeinen of IP-adressen in de SD-WAN-bypassconfiguratie te definiëren:

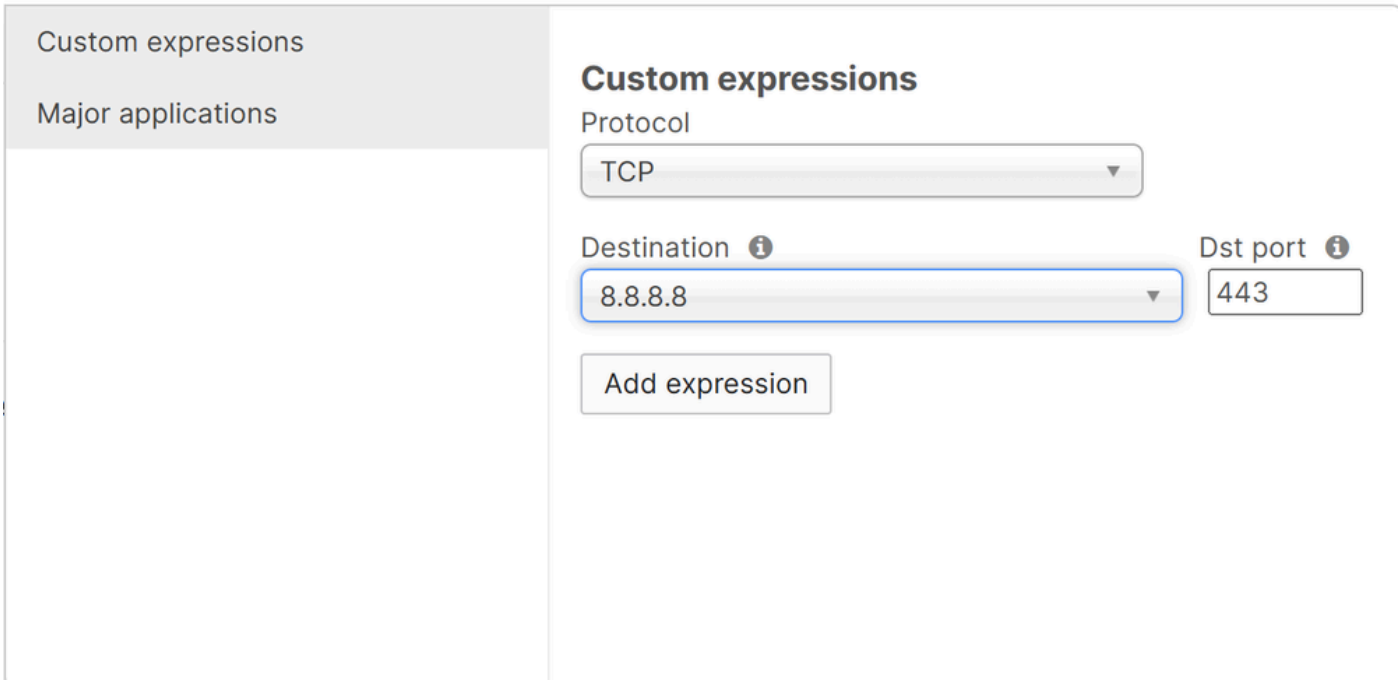
- Navigeer naar **Security & SD-WAN** > SD-WAN & Traffic Shaping



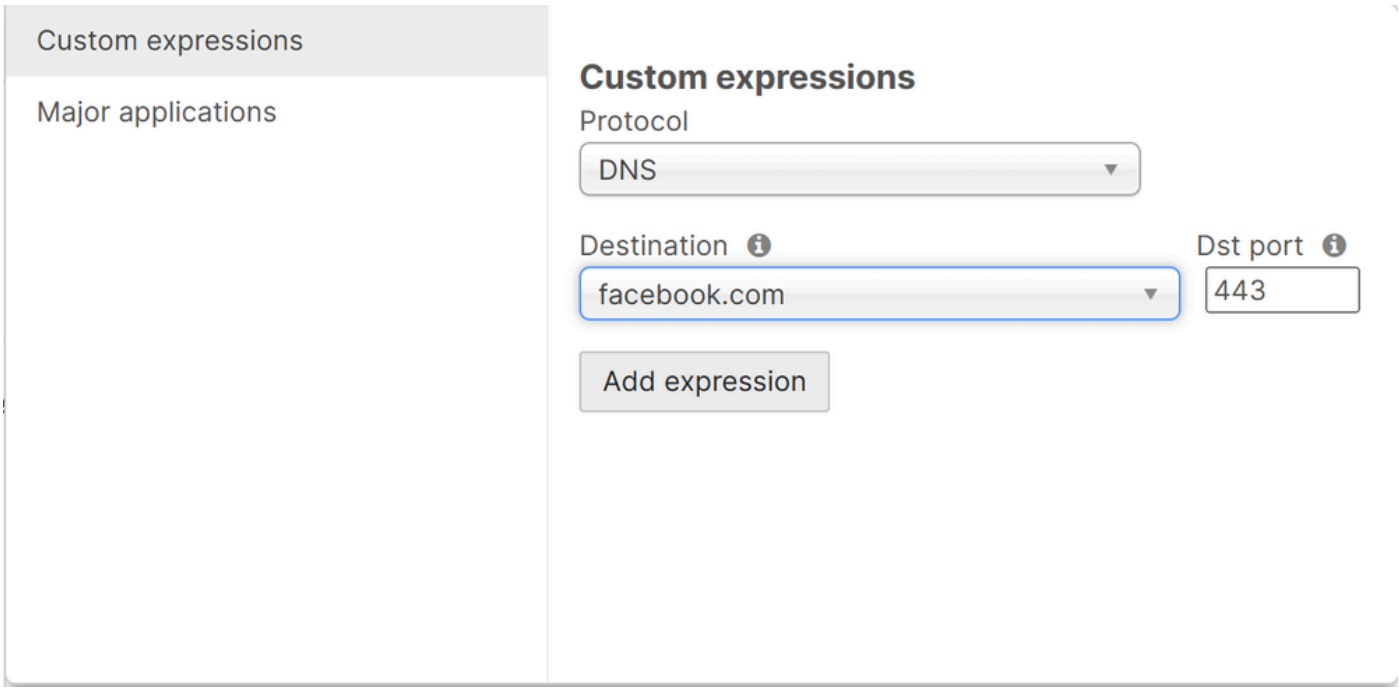
- Scroll naar beneden naar het **Local Internet Breakout** gedeelte en klik op **Add+**

Vervolgens maakt u de bypass op basis van **Custom Expressions** of **Major Applications**:

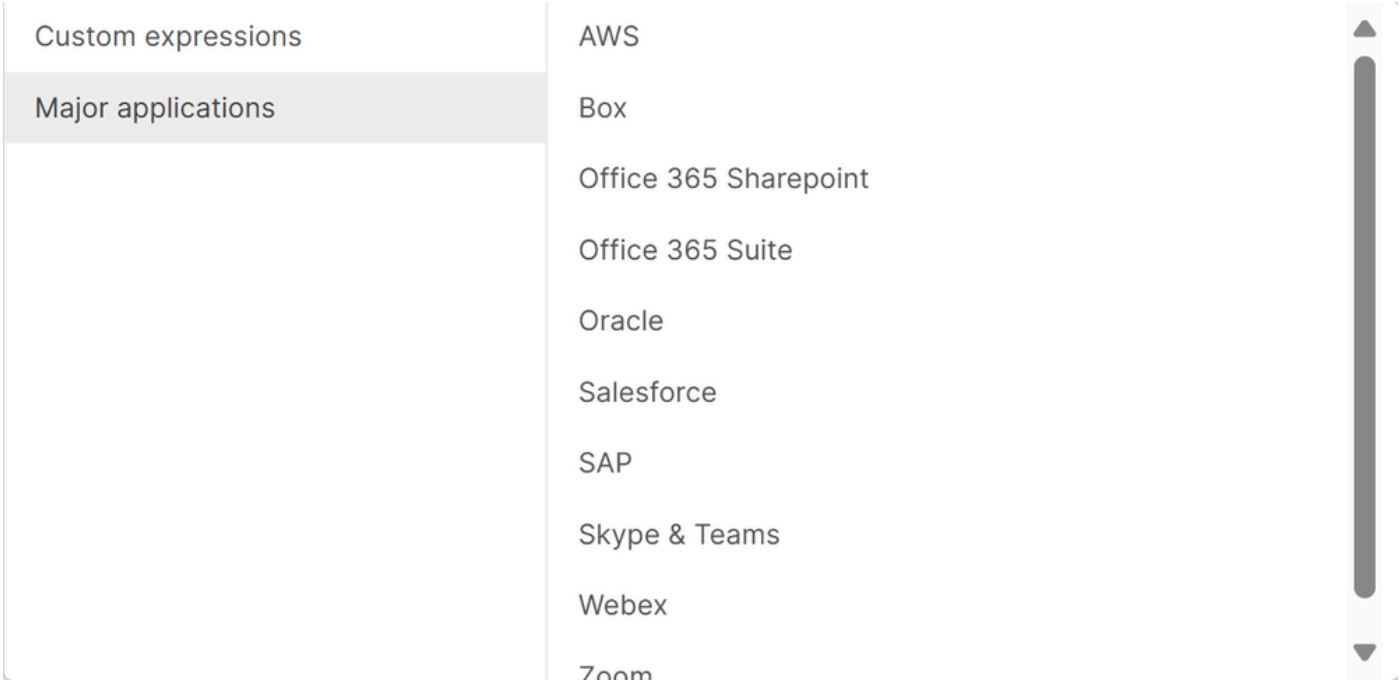
Custom Expressions - Protocol



Custom Expressions - DNS



Major Applications

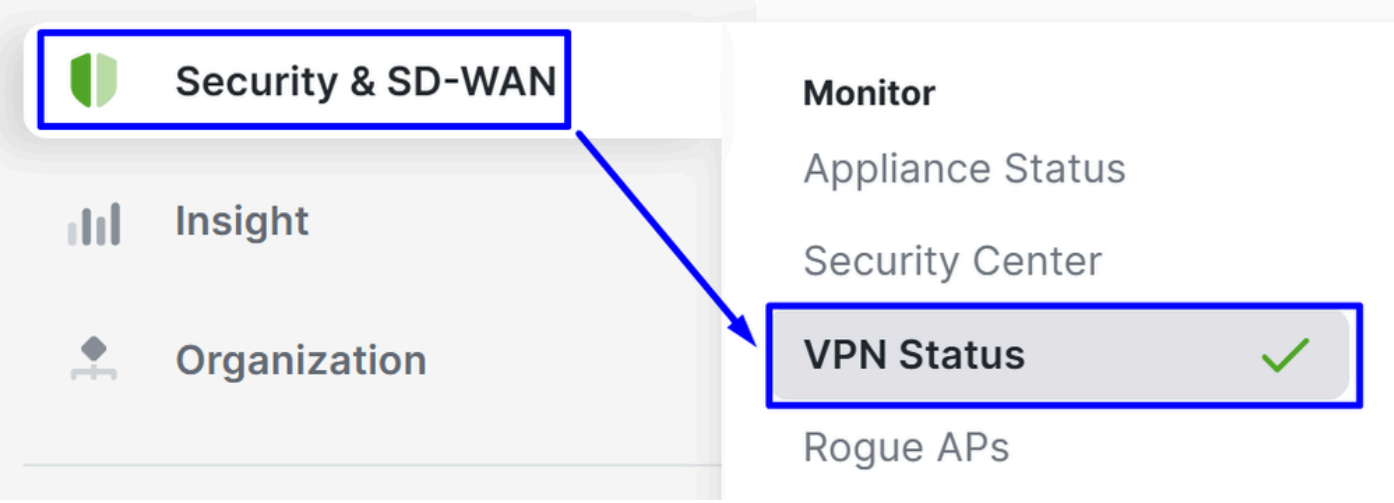


Ga voor meer informatie naar: [VPN-uitsluitingsregels configureren (IP/Port/DNS/APP)]

Verifiëren

Om te controleren of de tunnels zijn geopend, moet u de status controleren in:

- Klik opSecurity & SD-WAN**> VPN Status** op het Meraki Dashboard.



- Klik op 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				

Als zowel de primaire als de secundaire VPN-status groen wordt weergegeven, betekent dit dat de tunnels actief zijn.

Meraki VPN Status Codes

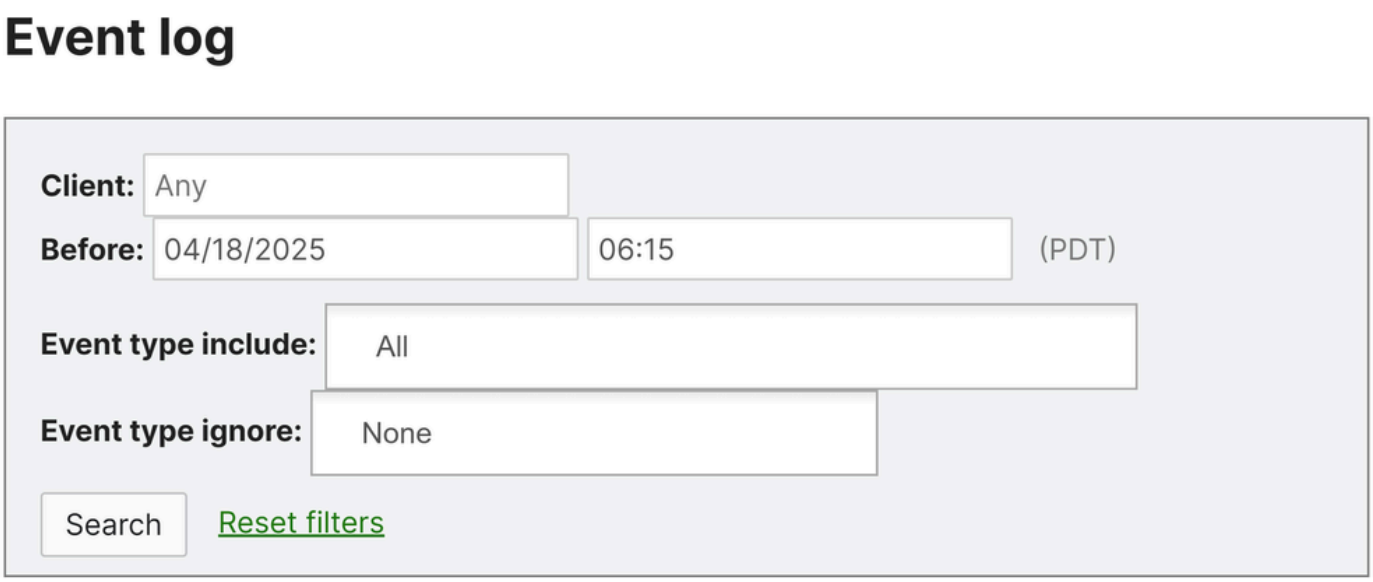
Status Indicator	Color	Meaning
Primary/Secondary Up	Green	Phase 1 and phase 2 are up
Partial Connectivity	Amber	Phase 1 is up but phase 2 is down
Tunnel Down	Red	Phase 1 and phase 2 are both down

Problemen oplossen

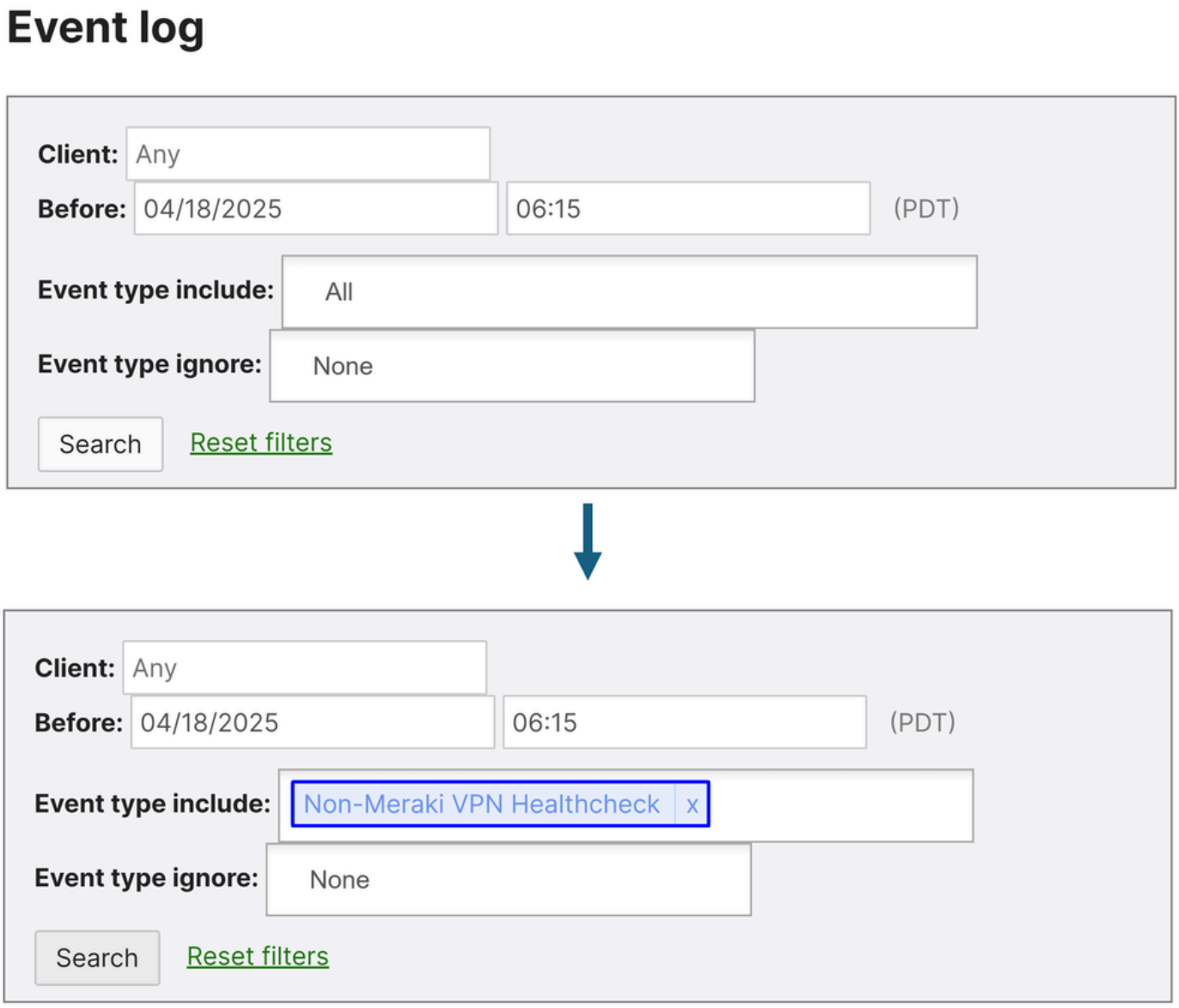
Controles controleren

Om te controleren of de gezondheidscontroles van Meraki voor de VPN goed werken, navigeert u naar:

- Klik op de link **Assurance** > Event Log

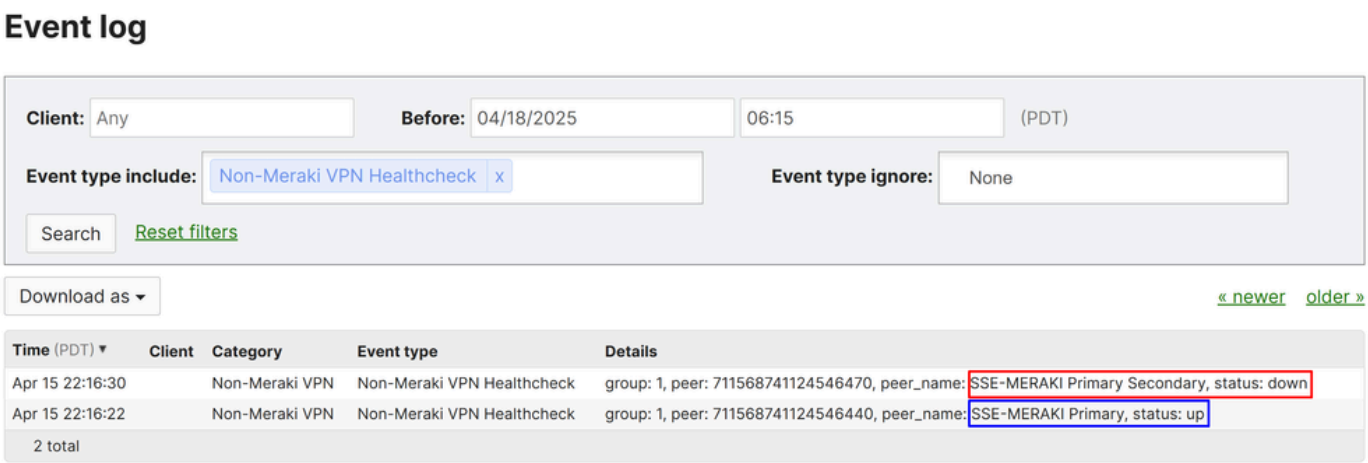


Onder **Event Type Include**kies Non-Meraki VPN Healthcheck



Wanneer de primaire tunnel naar Cisco Secure Access actief is, worden pakketten die door de secundaire tunnel aankomen, weggelaten om een consistent routeringspad te behouden.

De secundaire tunnel blijft in stand-by en wordt alleen gebruikt als er een storing optreedt in de primaire tunnel, hetzij vanaf de Meraki-zijde of binnen Secure Access, zoals bepaald door het gezondheidscontrolemechanisme.



- De primaire tunnelgezondheidscontrole toont status: omhoog, wat betekent dat het momenteel verkeer doorgeeft en actief doorstuurt.
- De secundaire tunnelgezondheidscontrole toont de status: down, niet omdat de tunnel niet beschikbaar is, maar omdat de primaire gezond is en actief in gebruik. Dit gedrag wordt verwacht, omdat het verkeer alleen door tunnel 1 mag, waardoor de gezondheidscontrole van de secundaire tunnel mislukt.

Gerelateerde informatie

- Cisco Technical Support en downloads
- Cisco Secure Access Help Center
- Configuratiegids Cisco Secure Access Meraki BGP

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.