Konfigurieren von sicherem Zugriff mit Meraki MX für Hochverfügbarkeit und Statusüberwachung

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Cisco Secure Access mit Meraki MX für hohe Verfügbarkeit mithilfe von Statusprüfungen konfigurieren.

Voraussetzungen

- Überprüfen der IPsec-Tunnelanforderungen mit sicherem Zugriff
- Komponenten des sicheren Zugriffs
- Analyse der Funktionalität der Statusprüfung in Meraki MX

Anforderungen

- Auf Meraki MX muss die Firmware-Version 19.7.1 oder höher ausgeführt werden
- Bei Verwendung von Private Access wird aufgrund einer Meraki-Einschränkung, die eine

Änderung der Integritätsprüfung-IP verhindert, nur ein Tunnel unterstützt. Für zusätzliche SPA-Tunnel (Secure Private Access) ist daher NAT erforderlich. Dies gilt nicht bei Verwendung von SIA (Secure Internet Access).
- Legen Sie klar fest, welche internen Subnetze oder Ressourcen durch den Tunnel zu Secure Access geroutet werden.

Verwendete Komponenten

- Sicherer Zugriff von Cisco
- Meraki MX Security Appliance (Firmware-Version 19.7.1 oder höher)
- Meraki-Dashboard
- Dashboard für sicheren Zugriff

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Cisco Secure Access ist eine Cloud-basierte Sicherheitsplattform, die einen sicheren Zugriff auf private Anwendungen (über Private Access) und Internetziele (über Internet Access) ermöglicht. Durch die Integration mit Meraki MX können Organisationen sichere IPsec-Tunnel zwischen Zweigstellen und der Cloud einrichten, wodurch ein verschlüsselter Datenverkehrsfluss und eine zentrale Durchsetzung der Sicherheit gewährleistet werden.

Bei dieser Integration werden IPsec-Tunnel mit statischem Routing verwendet. Meraki MX richtet primäre und sekundäre IPsec-Tunnel zu Cisco Secure Access ein und nutzt die integrierten Uplink-Integritätsprüfungen, um ein automatisches Failover zwischen Tunneln durchzuführen. Dies bietet eine ausfallsichere und hochverfügbare Konfiguration für Zweigstellenverbindungen.

Zu den wichtigsten Elementen dieser Bereitstellung gehören:

- Meraki MX fungiert als Nicht-Meraki-VPN-Peer zu Cisco Secure Access.
- Primäre und sekundäre Tunnel werden statisch konfiguriert, wobei die Verfügbarkeit durch Integritätsprüfungen bestimmt wird.
- Private Access unterstützt den sicheren Zugriff auf interne Anwendungen über SPA (Secure Private Access), während Internet Access den Datenverkehr mit der Durchsetzung von

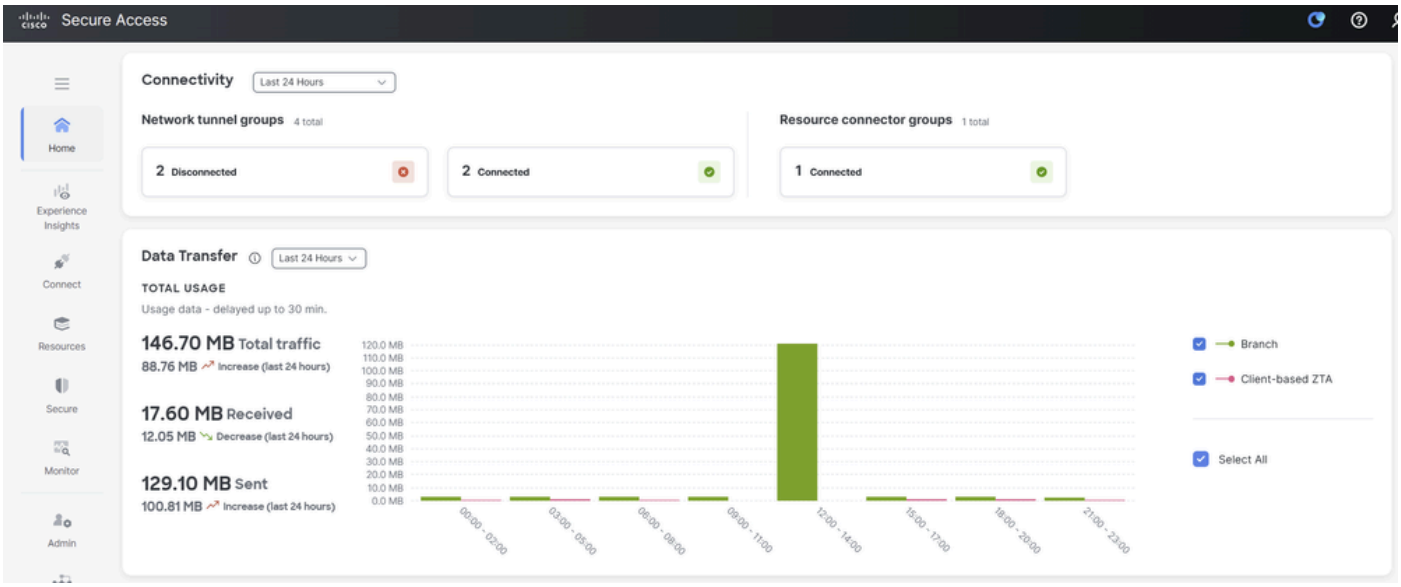
Richtlinien in der Cloud auf internetbasierte Ressourcen zulässt.

- Aufgrund der Einschränkungen von Meraki bei der IP-Flexibilität bei der Integritätsprüfung wird im privaten Zugriffsmodus nur eine Tunnelgruppe unterstützt. Wenn mehrere Meraki MX-Geräte mit Secure Access für privaten Zugriff verbunden werden müssen, müssen Sie entweder BGP für dynamisches Routing verwenden oder statische Tunnel konfigurieren, wobei nur eine Netzwerk-Tunnelgruppe Integritätsprüfungen und Hochverfügbarkeit unterstützen kann. Zusätzliche Tunnel funktionieren ohne Statusüberwachung oder Redundanz.

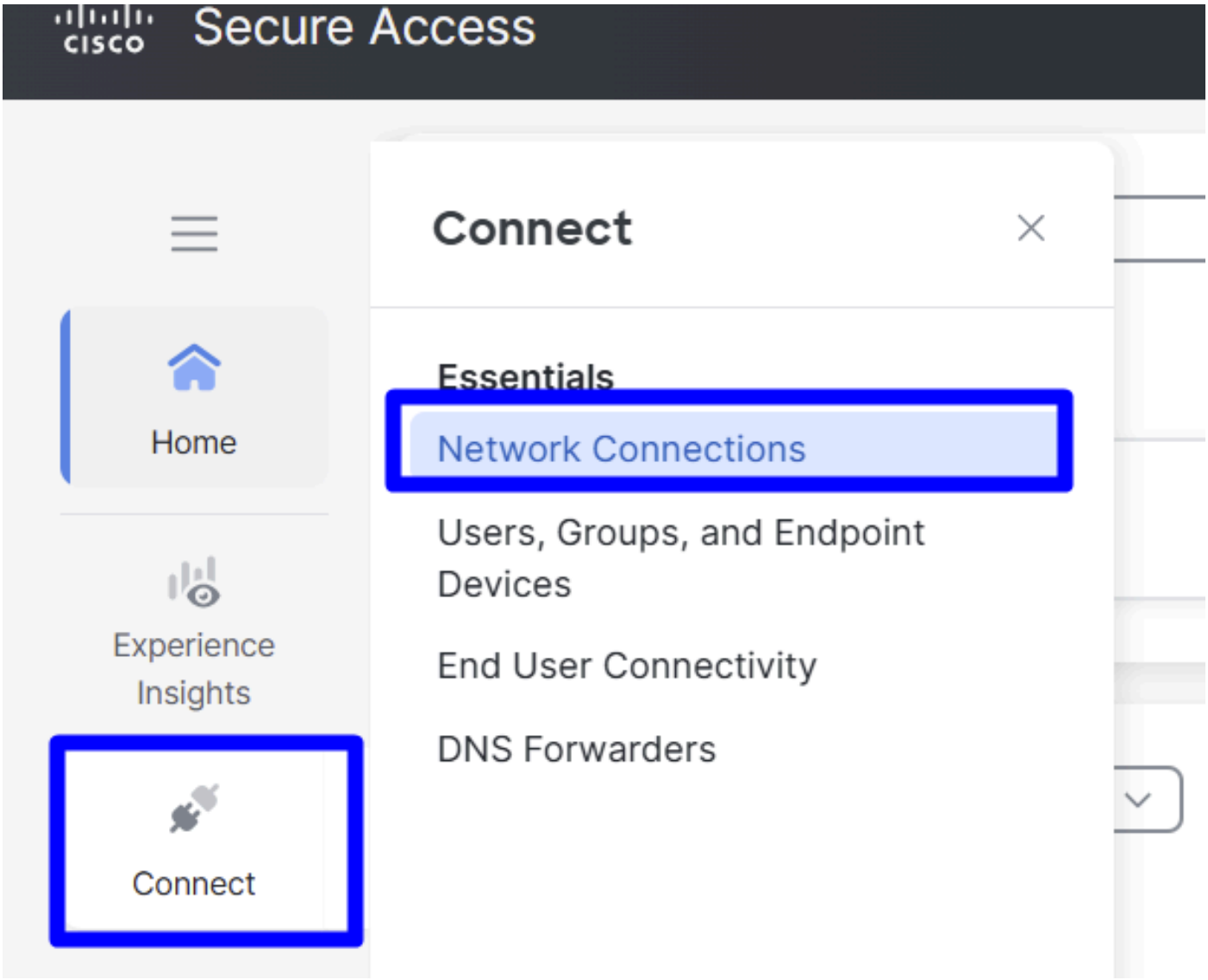
Konfigurieren

Konfigurieren des VPN für sicheren Zugriff

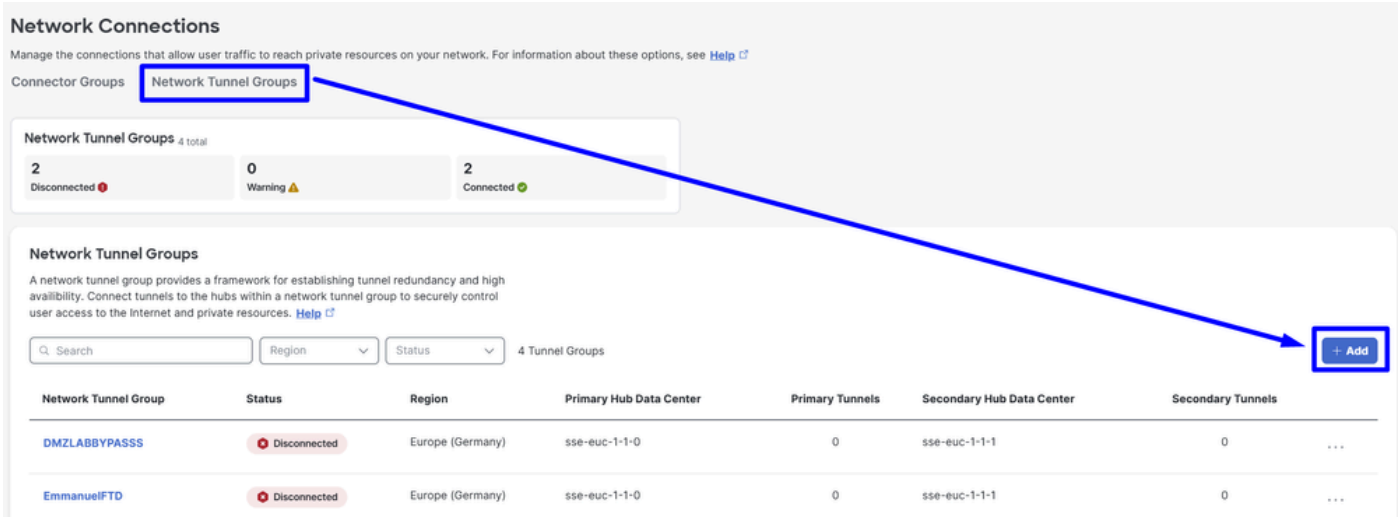
Navigieren Sie zum Admin-Bereich von Secure Access.



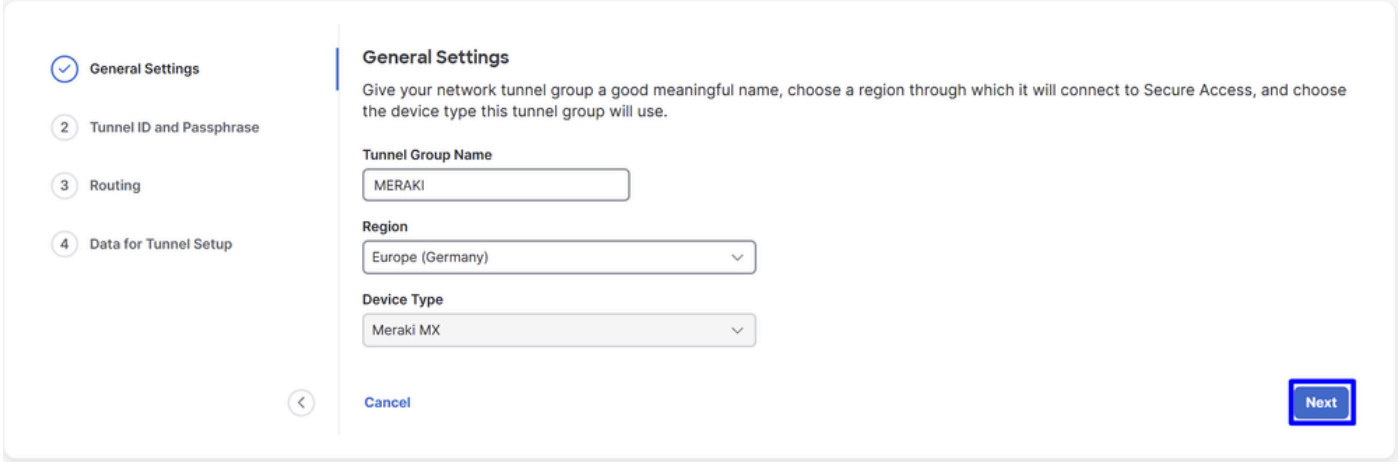
- Klicken Sie Connect > Network Connections



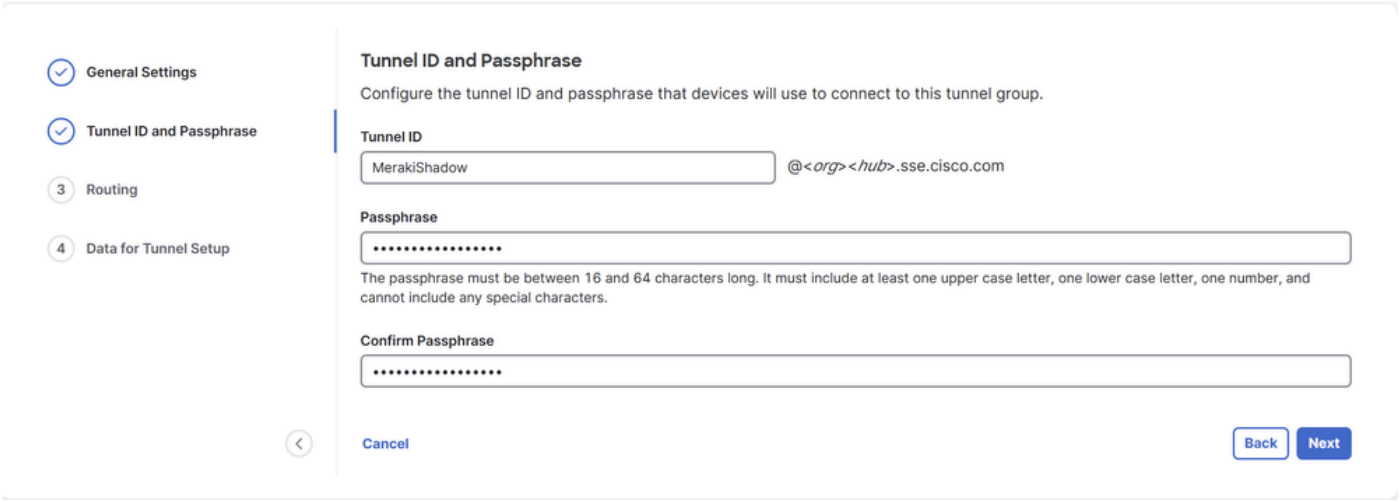
- Klicken Sie unterNetwork Tunnel Groupsauf + Add



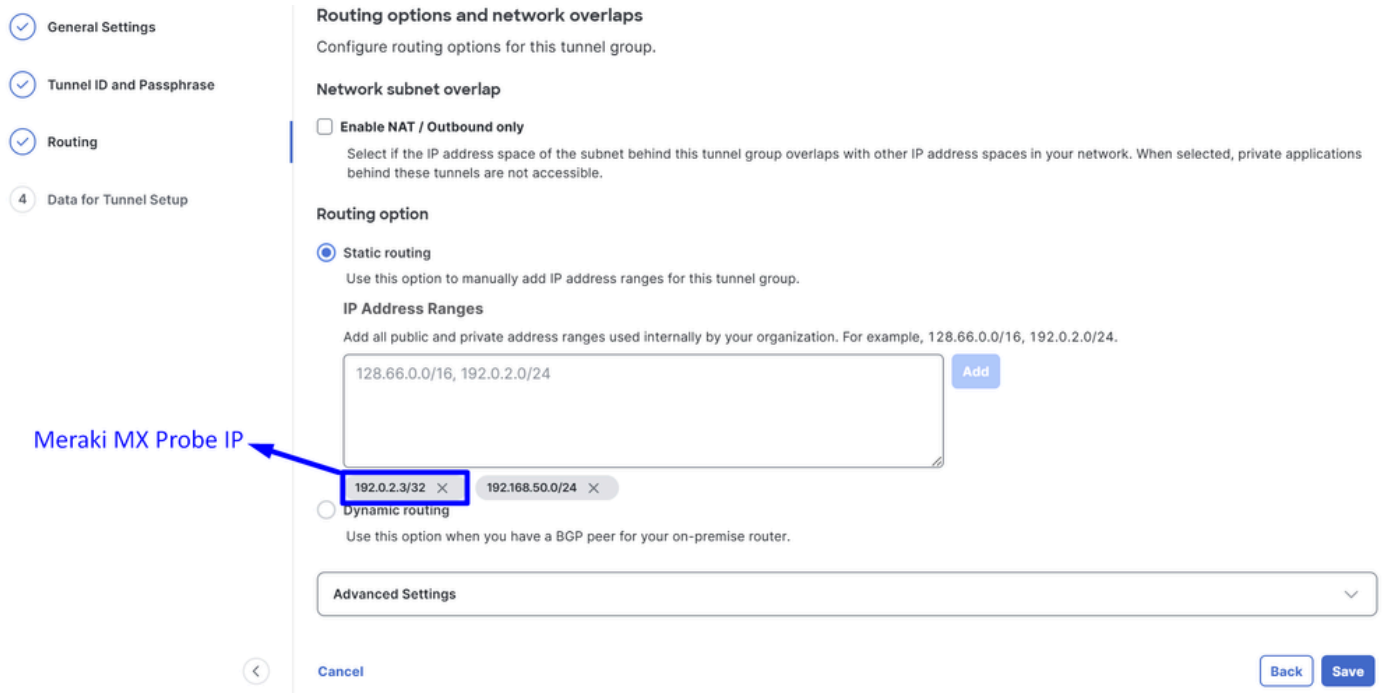
- KonfigurationTunnel Group NameRegionundDevice Type
- Klicken Sie auf **Next**

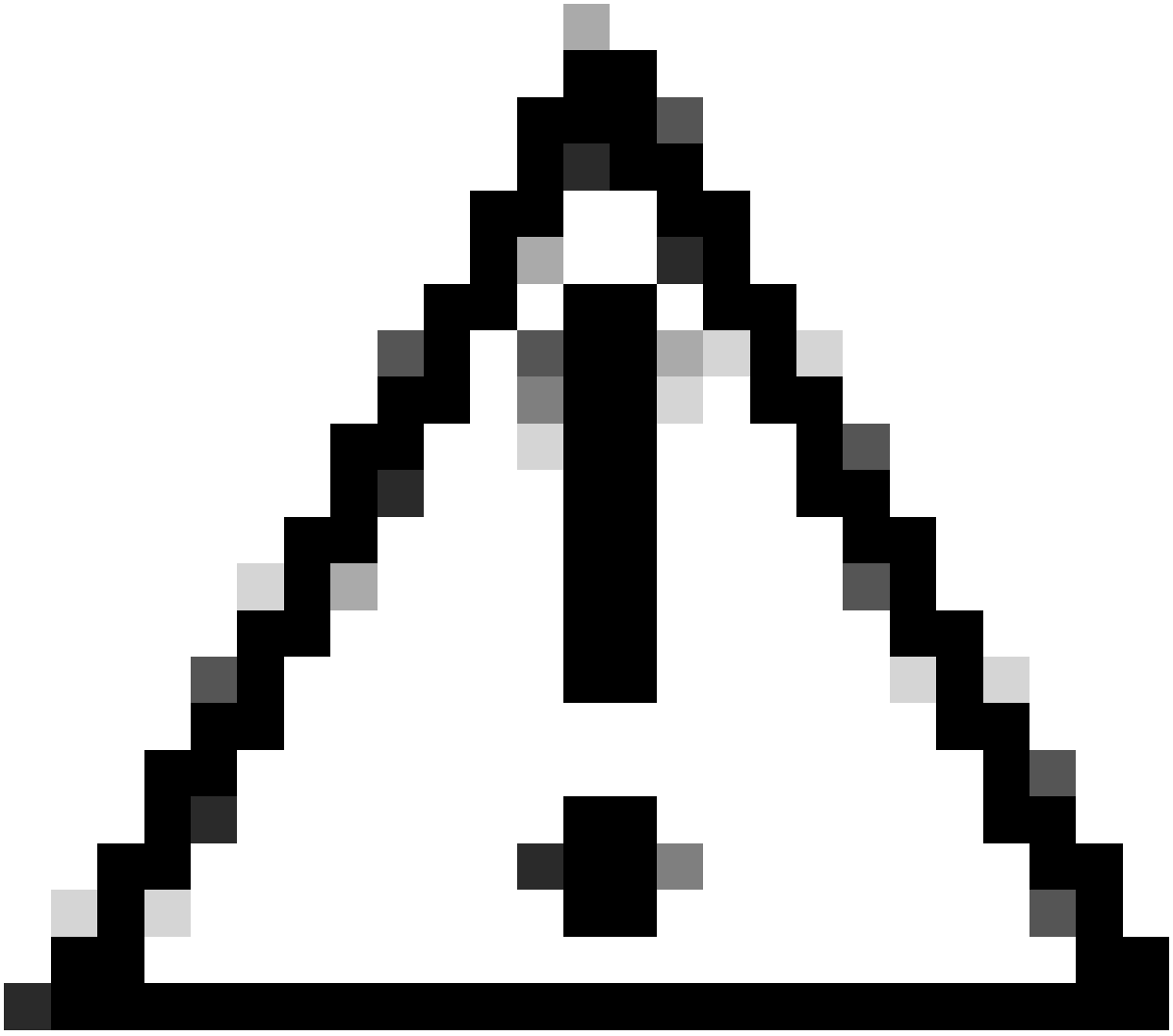


- Konfigurieren Sie dieTunnel ID Formatund Passphrase
- Klicken Sie auf Next



- Konfigurieren Sie die IP-Adressbereiche oder Hosts, die Sie in Ihrem Netzwerk konfiguriert haben und den Datenverkehr über Secure Access weiterleiten möchten, und stellen Sie sicher, dass die IP-Adresse der Meraki-Überwachungssonde enthalten ist, 192.0.2.3/32 um den Rückverkehr von Secure Access zurück zur Meraki MX zuzulassen.
- Klicken Sie auf 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

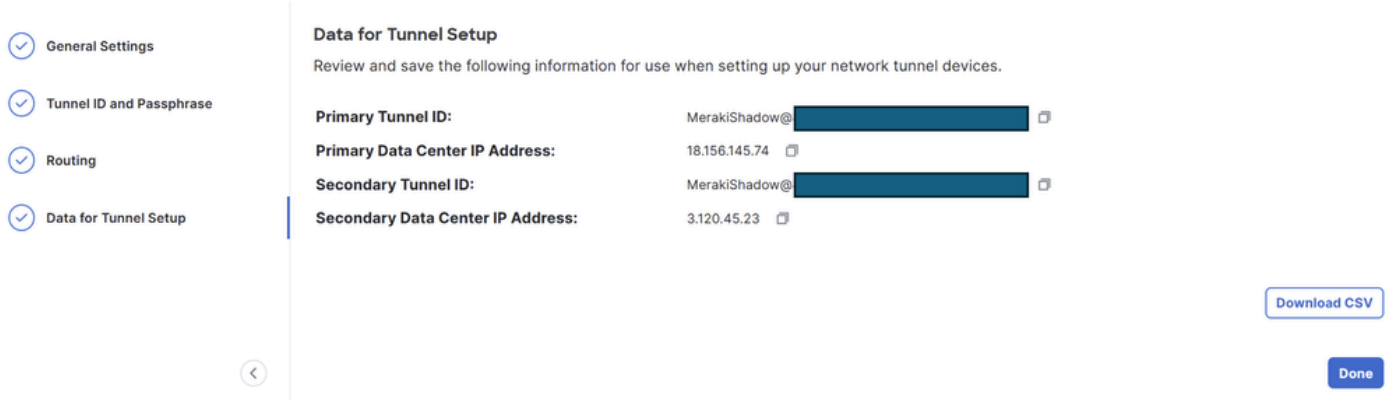


Vorsicht: Stellen Sie sicher, dass Sie die Überwachungssonde IP (192.0.2.3/32) hinzufügen. Andernfalls kann es auf dem Meraki-Gerät zu Datenverkehrsproblemen kommen, die den Datenverkehr an das Internet, die VPN-Pools und den von ZTNA verwendeten CGNAT-Bereich 100.64.0.0/10 weiterleiten.

- Nachdem Sie auf **Save** die Informationen über den Tunnel angezeigt wird, bitte speichern Sie diese Informationen für den nächsten Schritt, **Configure the tunnel on Meraki MX.**

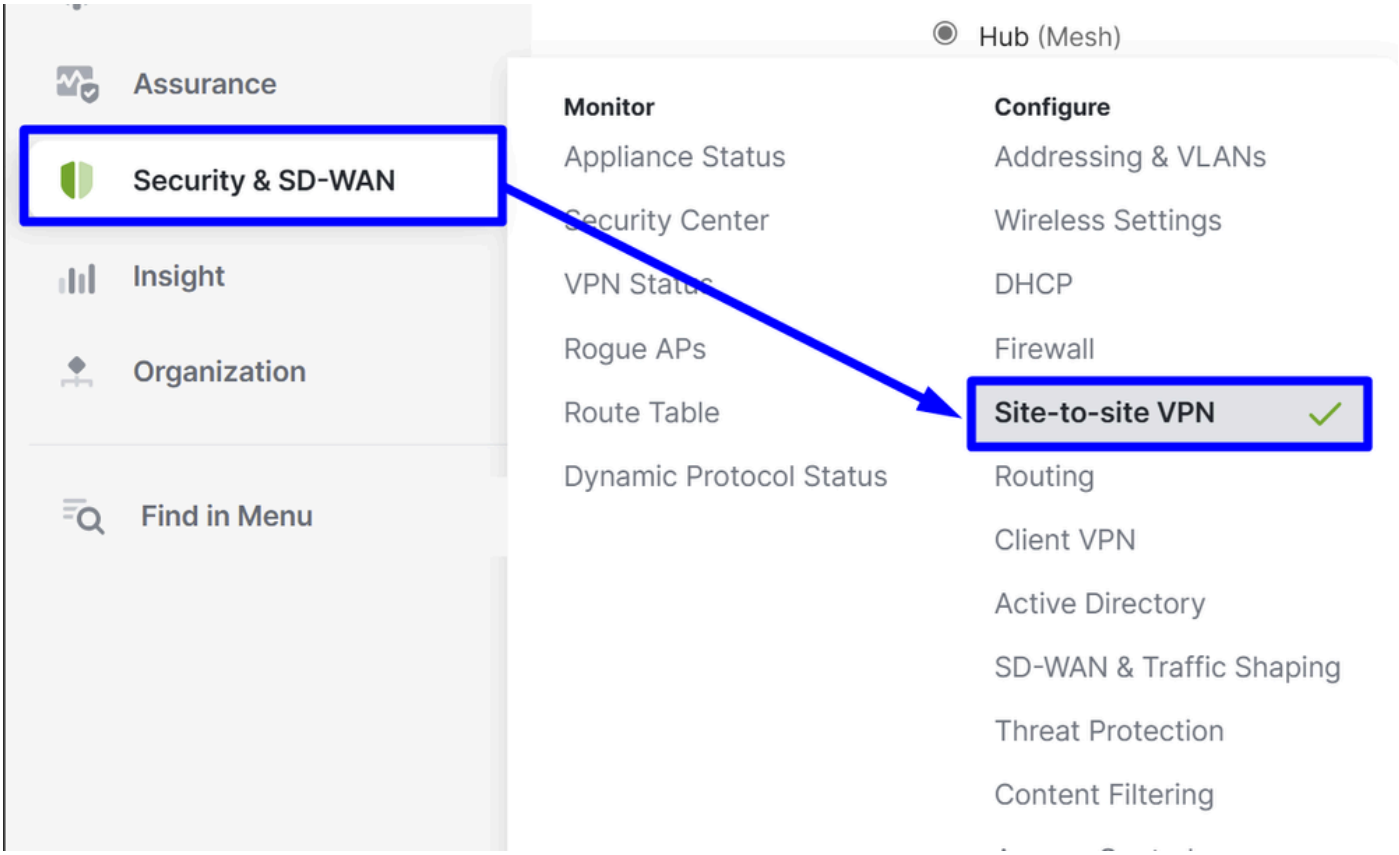
Konfiguration des VPN für sicheren Zugriff

Kopieren Sie die Konfiguration der Tunnel in einen Notizblock. Verwenden Sie diese Informationen, um die Konfiguration in Meraki abzuschließen **Non-Meraki VPN Peers.**



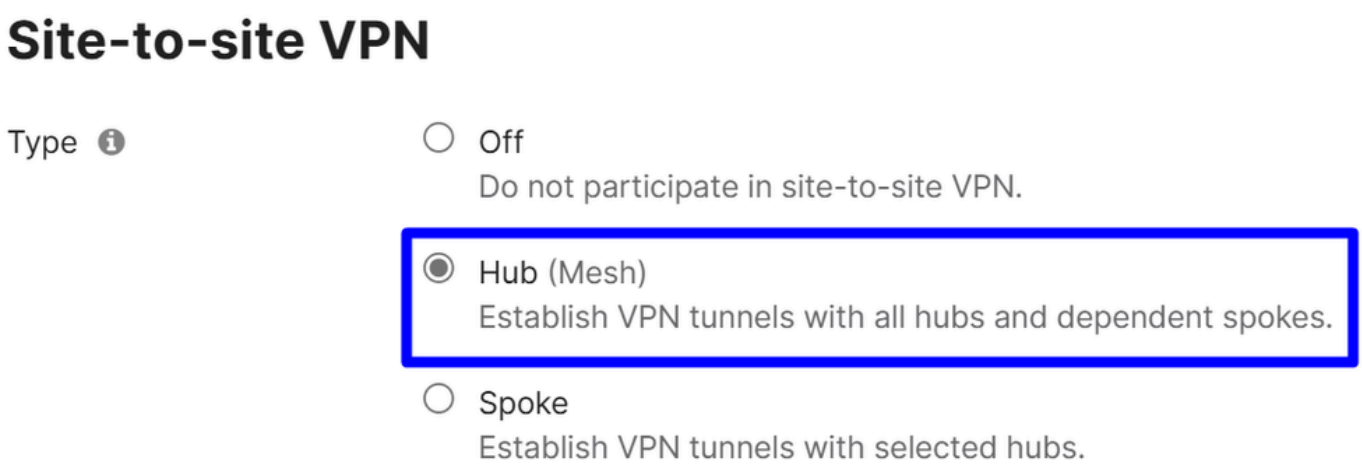
Konfigurieren des VPN auf der Meraki MX

Navigieren Sie zu Ihrer Meraki MX, und klicken Sie auf **Security & SD-WAN >** Site-to-site VPN



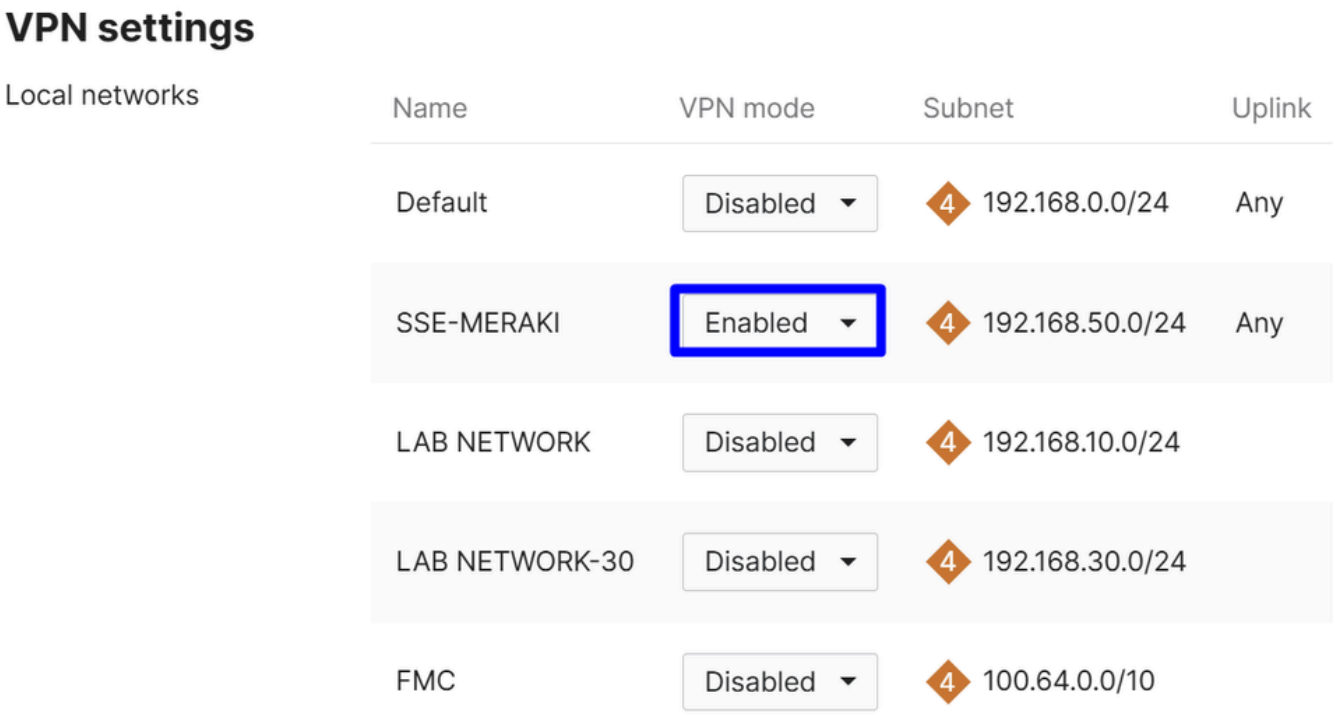
Standortübergreifendes VPN

Auswählen Hub.

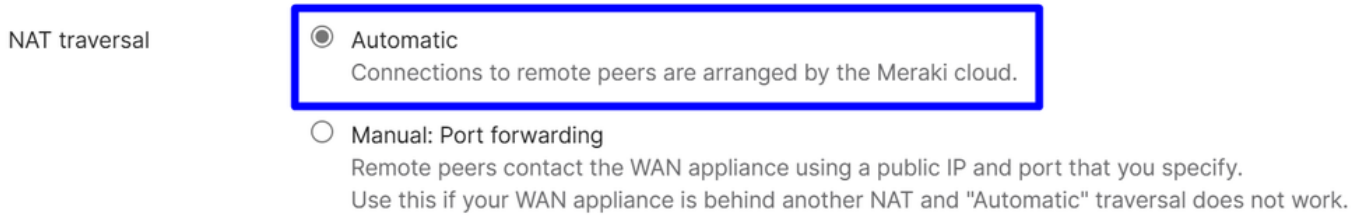


VPN-Einstellungen

Wählen Sie die Netzwerke aus, die Sie ausgewählt haben, um Datenverkehr an sicheren Zugriff zu senden:



Auswahl unterNAT TraversalAutomatisch



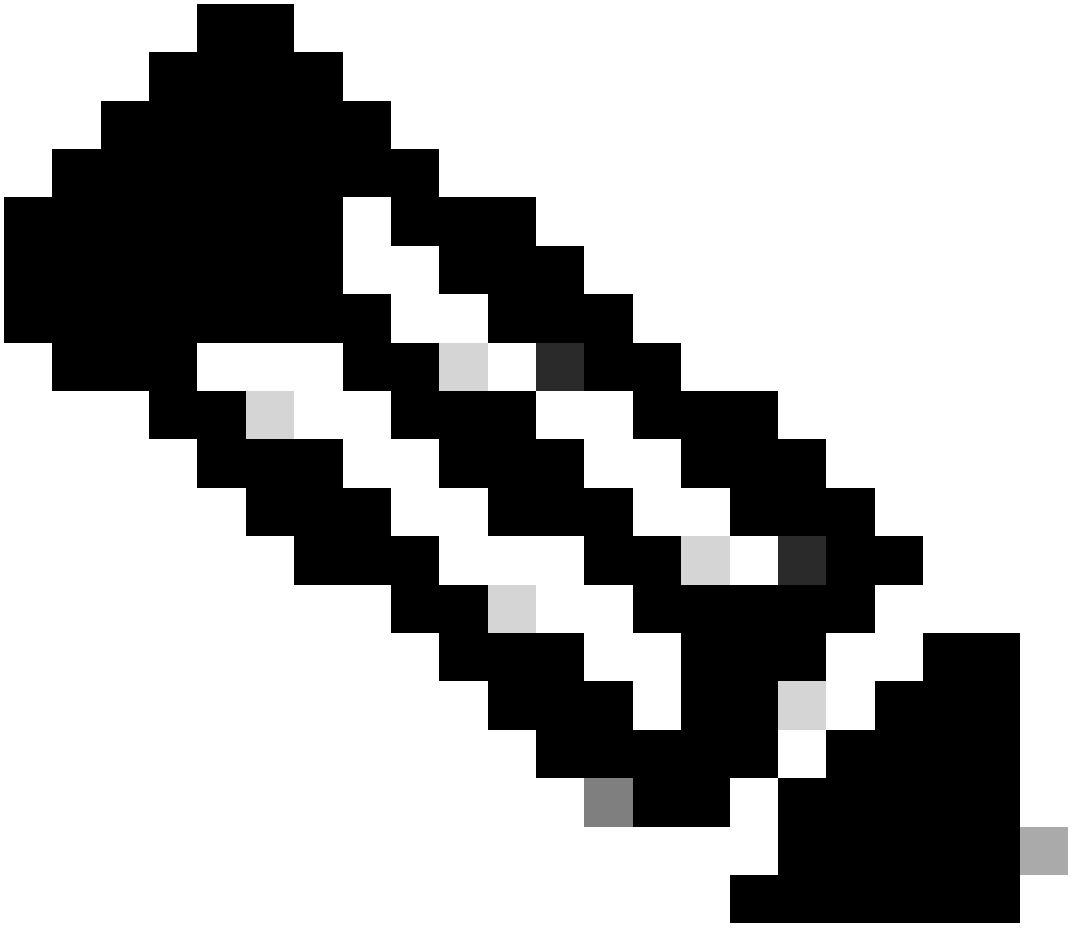
Nicht-Meraki VPN-Peers

Sie müssen die Integritätsprüfungen konfigurieren, die Meraki verwendet, um Datenverkehr an Secure Access weiterzuleiten:

Klicken Sie **Configure Health Checks**

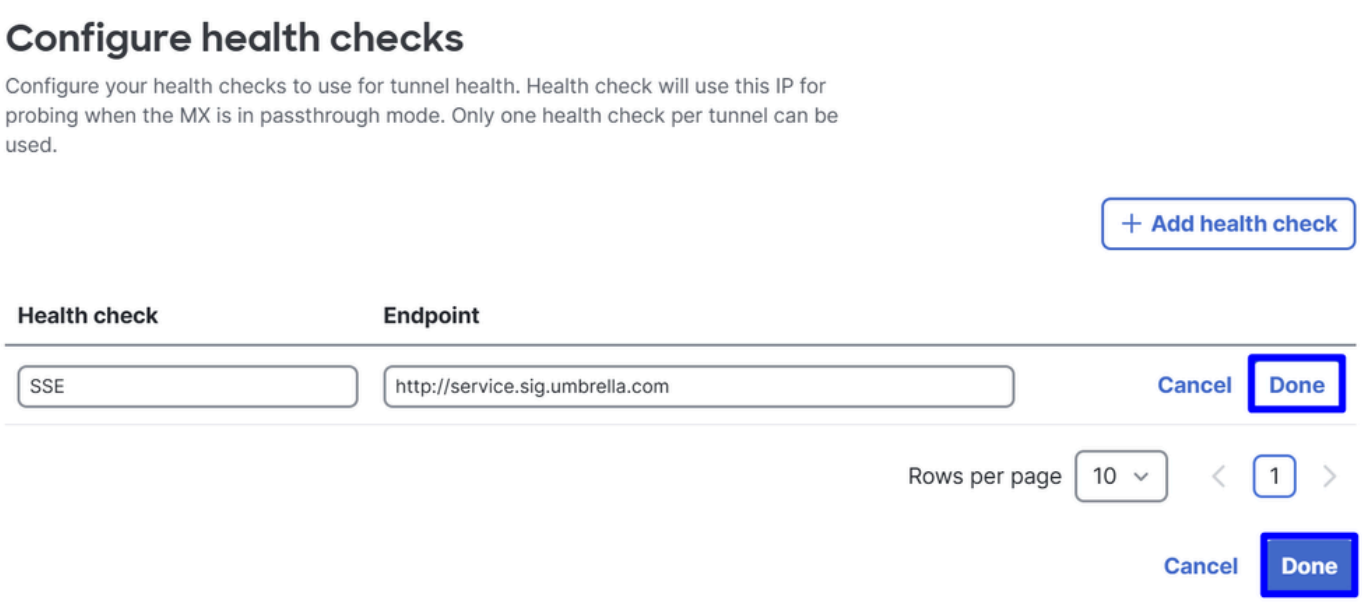
- Klicken Sie **+Add health Check**

- **Health Check**: Konfigurieren eines Testnamens
- **Endpoint**: Verwenden Sie die von Secure Access empfohlene http://service.sig.umbrella.com



Anmerkung: Diese Domäne reagiert nur, wenn der Zugriff über einen Site-to-Site-Tunnel mit sicherem Zugriff oder Umbrella erfolgt: Zugriffsversuche von außerhalb dieser Tunnel schlagen fehl.

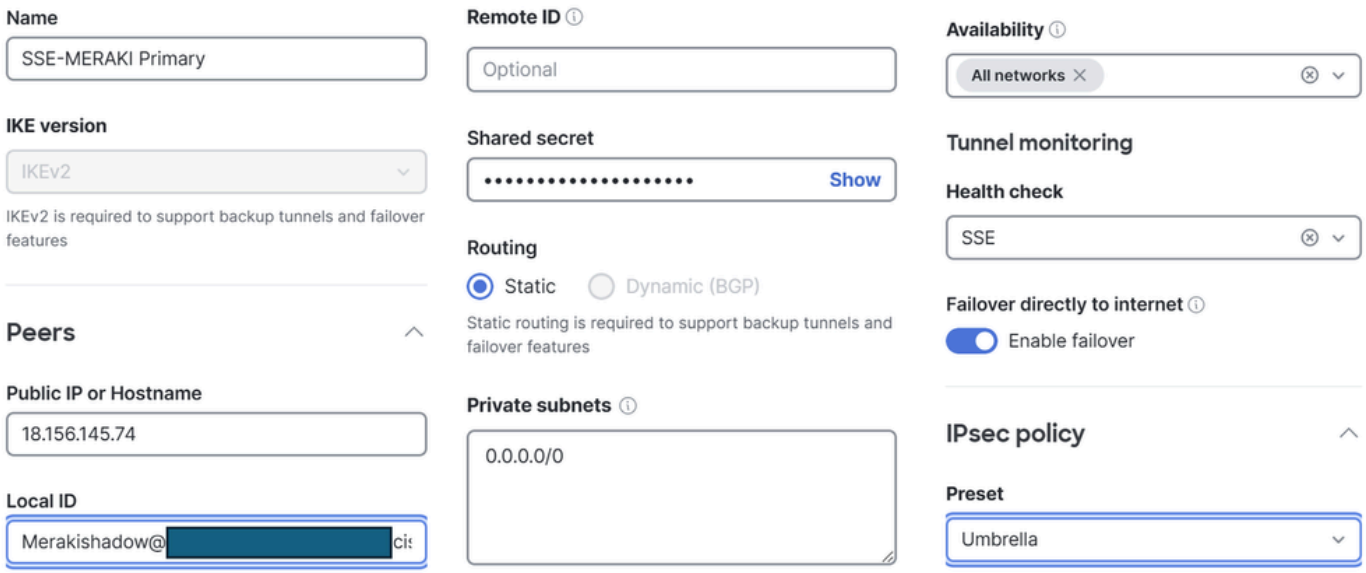
Klicken Sie dann zwei Mal auf**Done**, um den Vorgang abzuschließen.



Jetzt sind Ihre Statusprüfungen konfiguriert, und Sie können die **Peer:**

Primärtunnel konfigurieren

- Klicken Sie+Add a peer

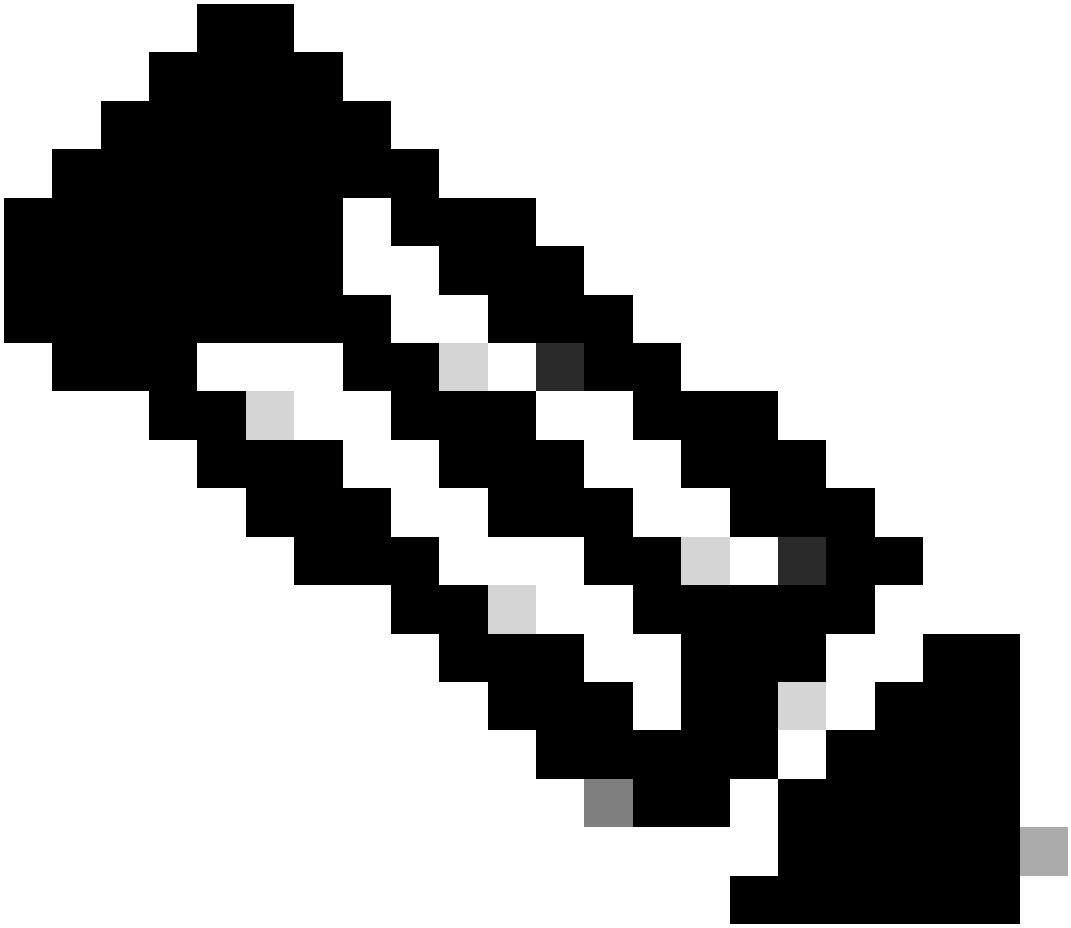


- VPN-Peer hinzufügen
  - Name: Konfigurieren Sie einen Namen für das sichere VPN.
  - IKE-Version: IKEv2 auswählen
- Peers
  - Öffentliche IP oder Hostname: Konfigurieren Sie die **Primary Datacenter IP** unter Sicherer Zugriff im Schritt Sicherer Zugriff VPN-Konfigurationen angegebenen
  - Lokale ID: Konfigurieren Sie die **Primary Tunnel ID** unter Sicherer Zugriff im Schritt Sicherer Zugriff VPN-Konfigurationen angegebenen
  - Remote-ID: –
  - Shared Secret: Konfigurieren Sie die **Passphrase** unter Sicherer Zugriff im Schritt Sicherer

Zugriff VPN-Konfigurationen

- Routing: Statisch auswählen
- Private Subnetze: Wenn Sie sowohl Internetzugang als auch privaten Zugang konfigurieren möchten, verwenden Sie **0.0.0.0/0** als Ziel. Wenn Sie nur privaten Zugriff für diesen VPN-Tunnel konfigurieren, geben Sie den **Remote Access VPN IP Pool** und den CGNAT-Bereich **100.64.0.0/10** als Zielnetzwerke an.
- Verfügbarkeit: Wenn Sie nur ein Meraki-Gerät haben, können Sie auswählen **All Networks**. Wenn Sie über mehrere Geräte verfügen, stellen Sie sicher, dass Sie nur das Meraki-Netzwerk auswählen, in dem Sie den Tunnel konfigurieren.

- Tunnelüberwachung
  - Statusprüfung: Zuvor konfigurierte Integritätsprüfung zur Überwachung der Tunnelverfügbarkeit
  - Direktes Failover auf das Internet: Wenn Sie diese Option aktivieren und Tunnel 1 und Tunnel 2 die Statusprüfung nicht bestehen, wird der Datenverkehr an die WAN-Schnittstelle umgeleitet, um einen Verlust des Internetzugriffs zu verhindern.



Integritätsprüfung:Wenn Tunnel 1 überwacht wird und die Integritätsprüfung fehlschlägt,

---

wird automatisch ein Failover des Datenverkehrs zu Tunnel 2 durchgeführt. Wenn Tunnel 2 ebenfalls fehlschlägt und die Failover directly to Internet Option aktiviert ist, wird der Datenverkehr über die WAN-Schnittstelle des Meraki-Geräts geleitet.

- IPsec-Richtlinie
  - Voreinstellung: Auswählen **Umbrella**

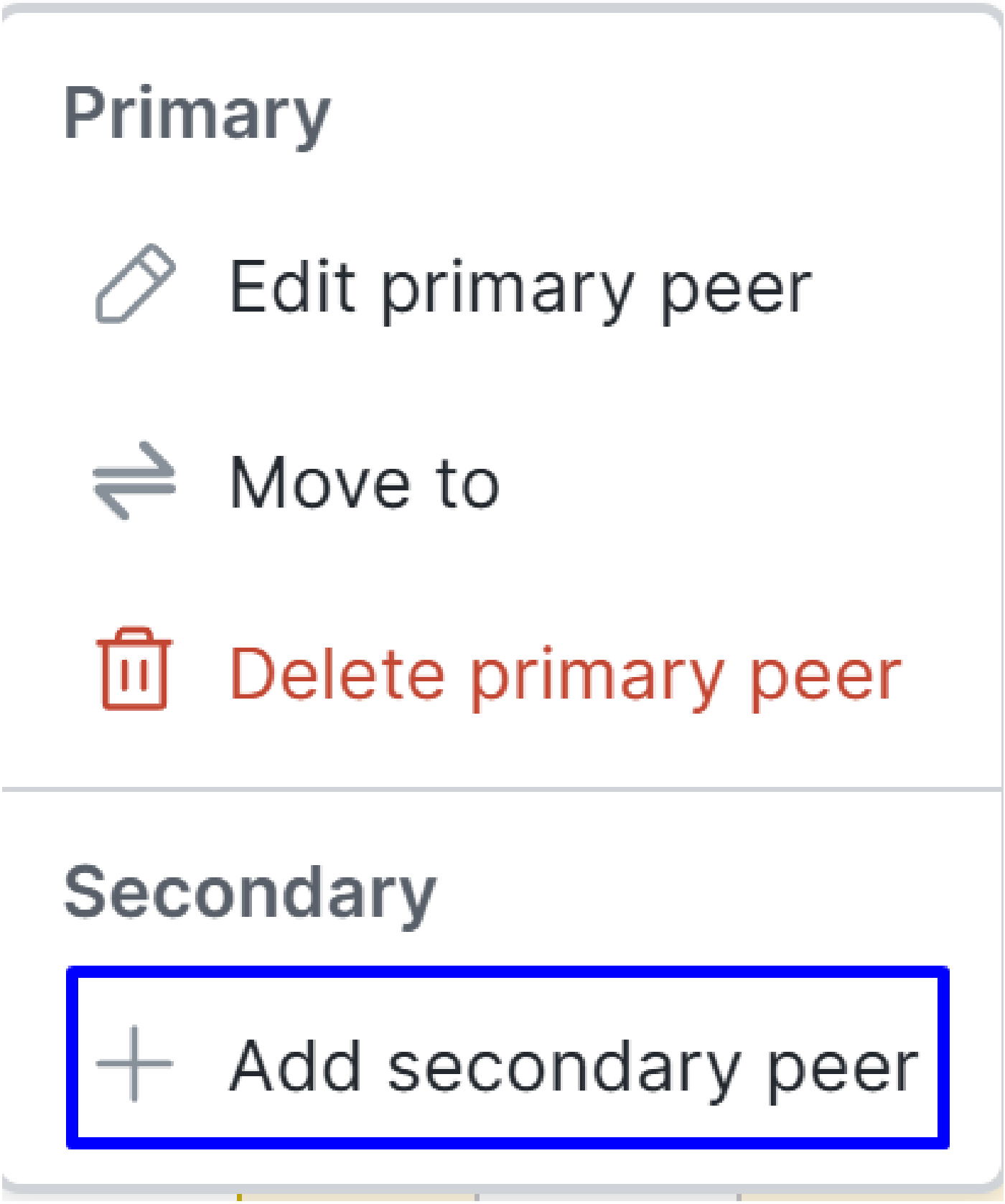
Klicken Sie anschließend auf **Save**.

Sekundären Tunnel konfigurieren

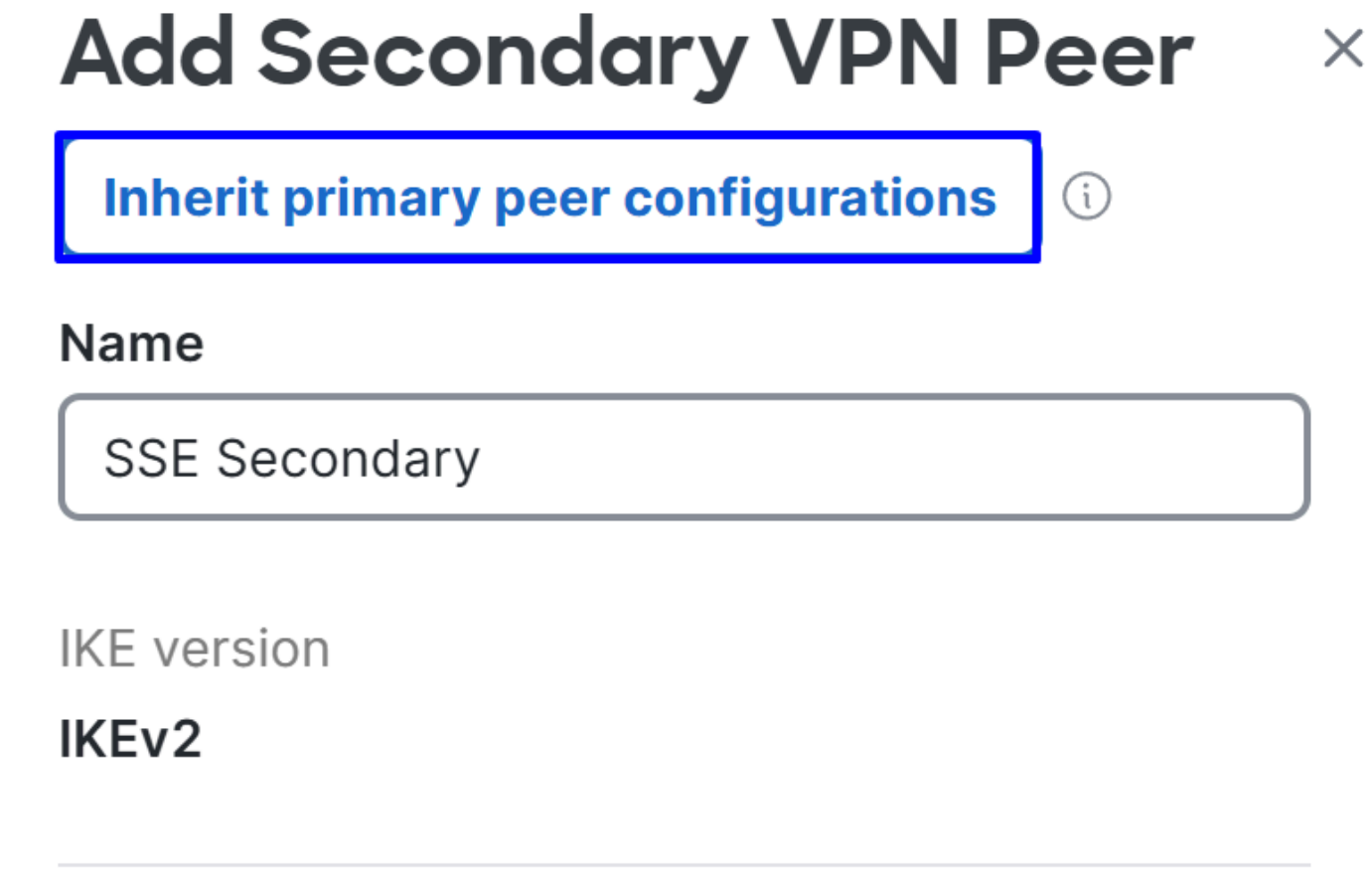
Um den sekundären Tunnel zu konfigurieren, klicken Sie auf das Optionsmenü des primären Tunnels:

- Klicken Sie auf die drei Punkte

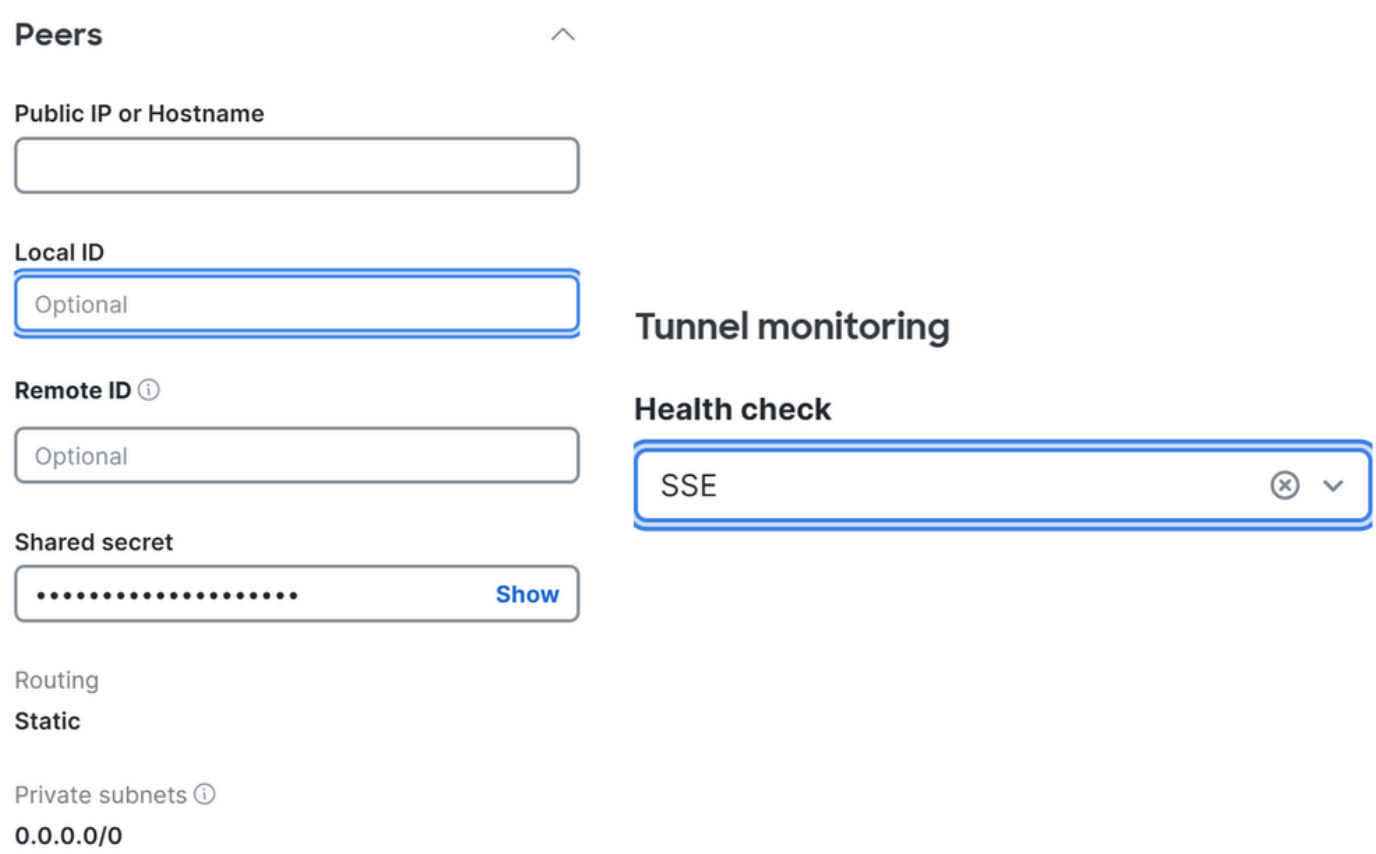
- Klicken Sie + Add Secondary peer



- Klicken SieInherit primary peer configurations

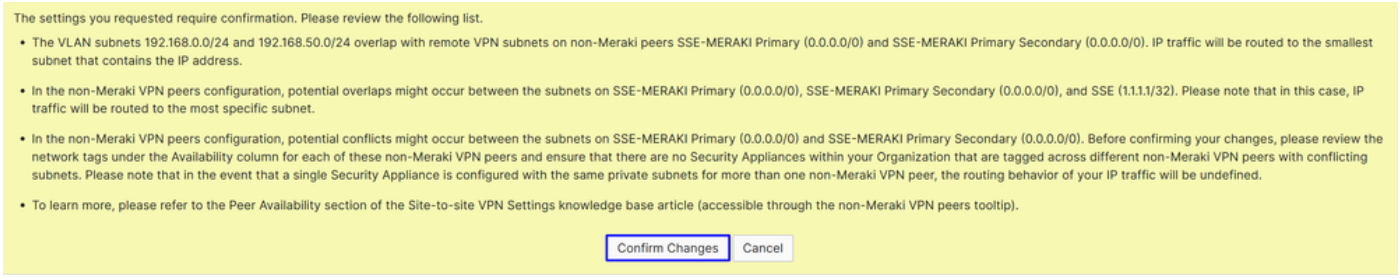


Einige Felder werden dann automatisch ausgefüllt. Überprüfen Sie sie, nehmen Sie die erforderlichen Änderungen vor, und führen Sie den Rest manuell aus:



- Peers
  - Öffentliche IP oder Hostname: Konfigurieren Sie die **Secondary Datacenter IP** unter Sicherer Zugriff im Schritt Sicherer Zugriff VPN-Konfigurationen angegebenen
  - Lokale ID: Konfigurieren Sie die **Secondary Tunnel ID** unter Sicherer Zugriff im Schritt Sicherer Zugriff VPN-Konfigurationen angegebenen
  - Remote-ID: –
  - Shared Secret: Konfigurieren Sie die **Passphrase** unter Sicherer Zugriff im Schritt Sicherer Zugriff VPN-Konfigurationen
- Tunnelüberwachung
  - Statusprüfung: Zuvor konfigurierte Integritätsprüfung zur Überwachung der Tunnelverfügbarkeit

Anschließend können Sie auf klicken, **Save**und die nächste Warnmeldung wird angezeigt:

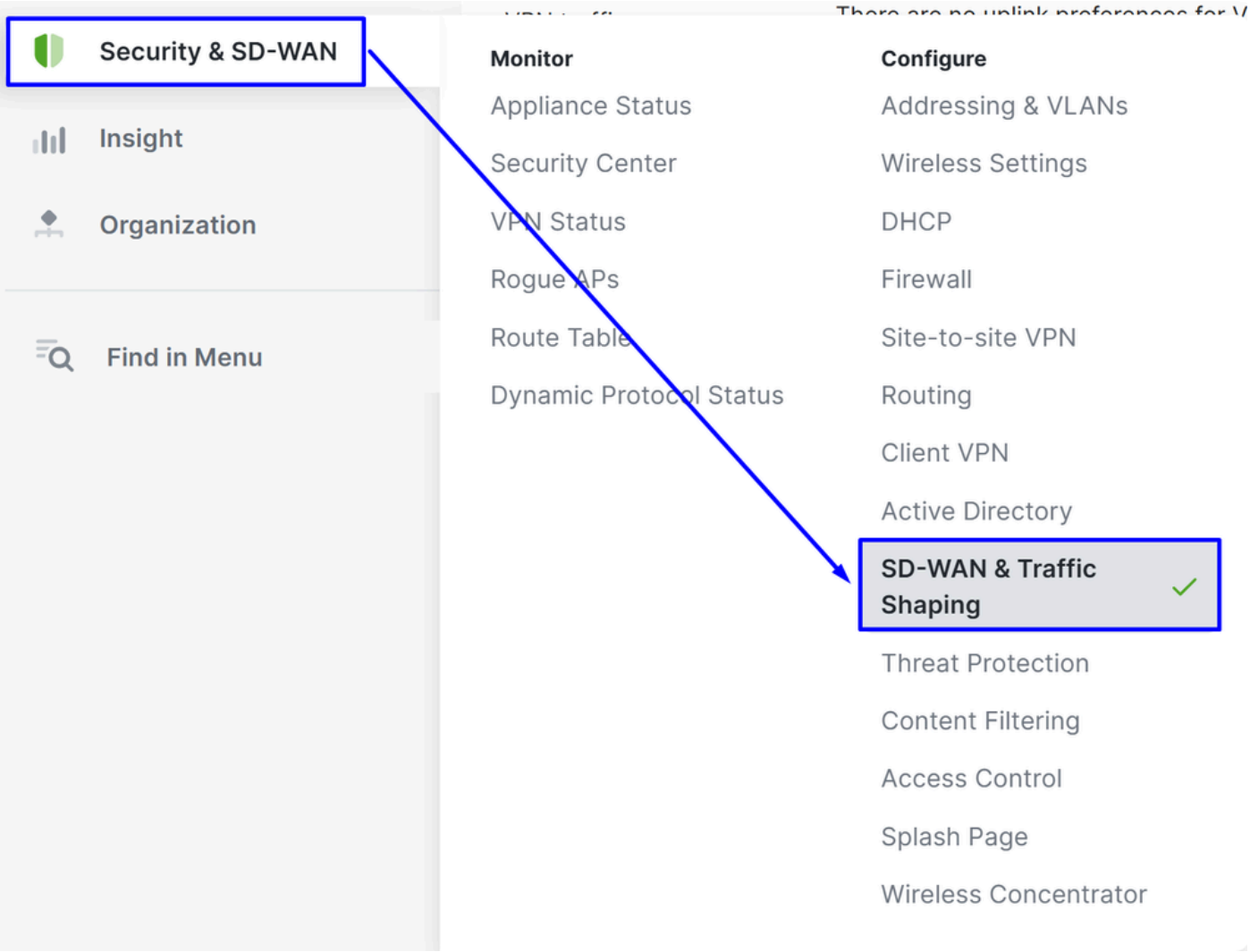


Keine Sorge, klicken Sie auf **Confirm Changes**.

Konfigurieren der Datenverkehrssteuerung (Tunnelumgehung)

Mit dieser Funktion können Sie bestimmten Datenverkehr aus dem Tunnel umgehen, indem Sie in der Konfiguration "SD-WAN Bypass" Domänen oder IP-Adressen definieren:

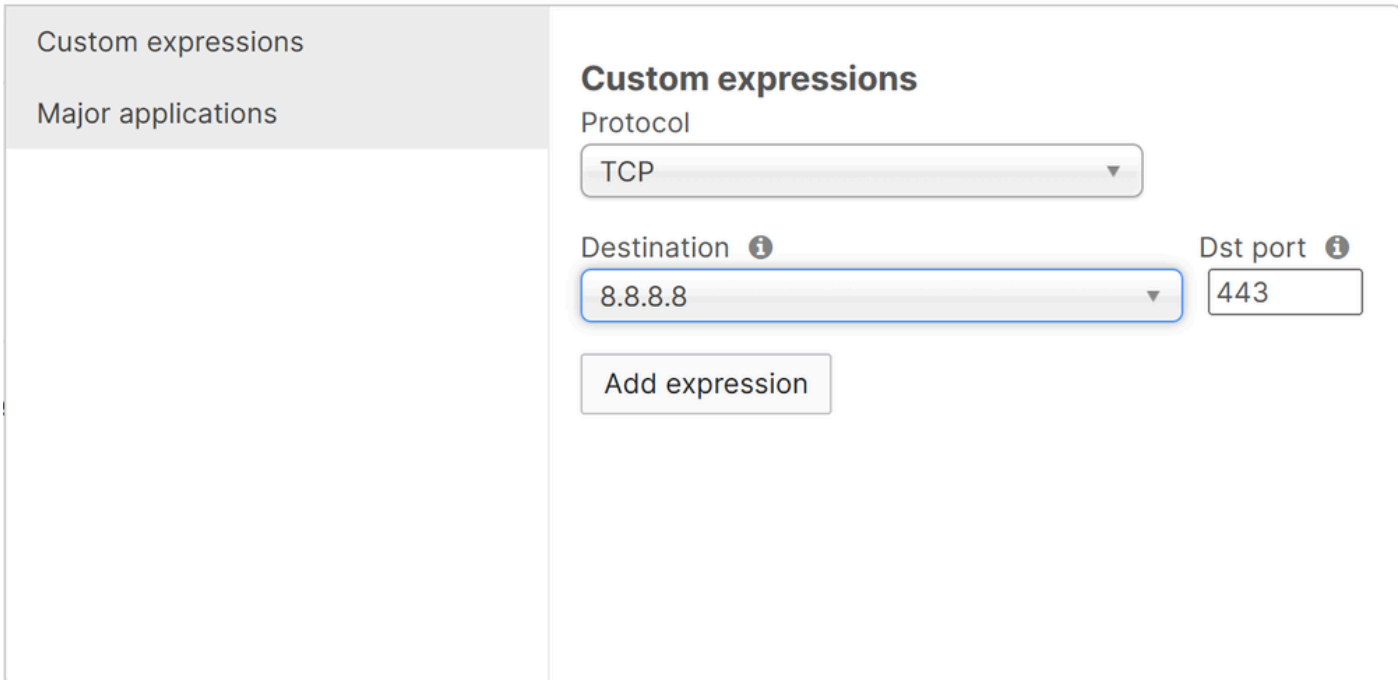
- Navigieren Sie zu **Security & SD-WAN** > SD-WAN & Traffic Shaping



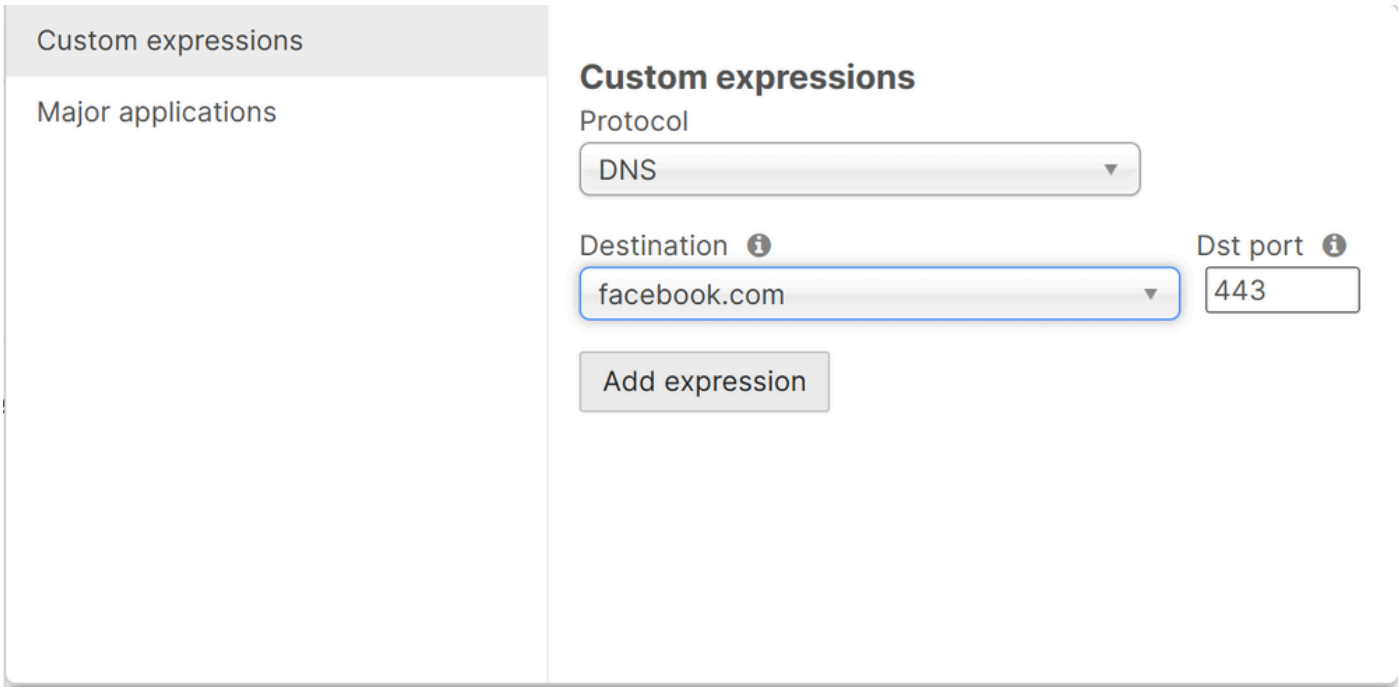
- Blättern Sie nach unten zum **Local Internet Breakout** Abschnitt, und klicken Sie auf **Add+**

Erstellen Sie dann den Bypass basierend auf **Custom Expressions** oder **Major Applications**:

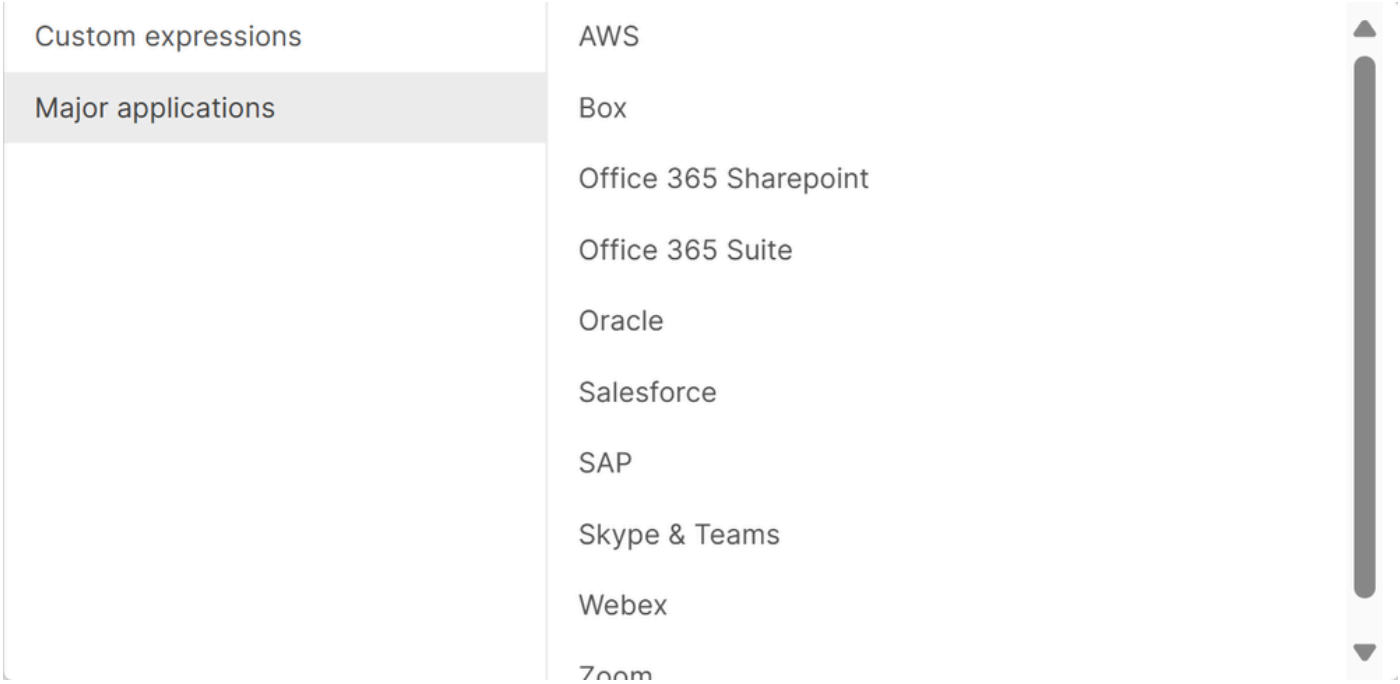
Custom Expressions - Protocol



Custom Expressions - DNS



Major Applications

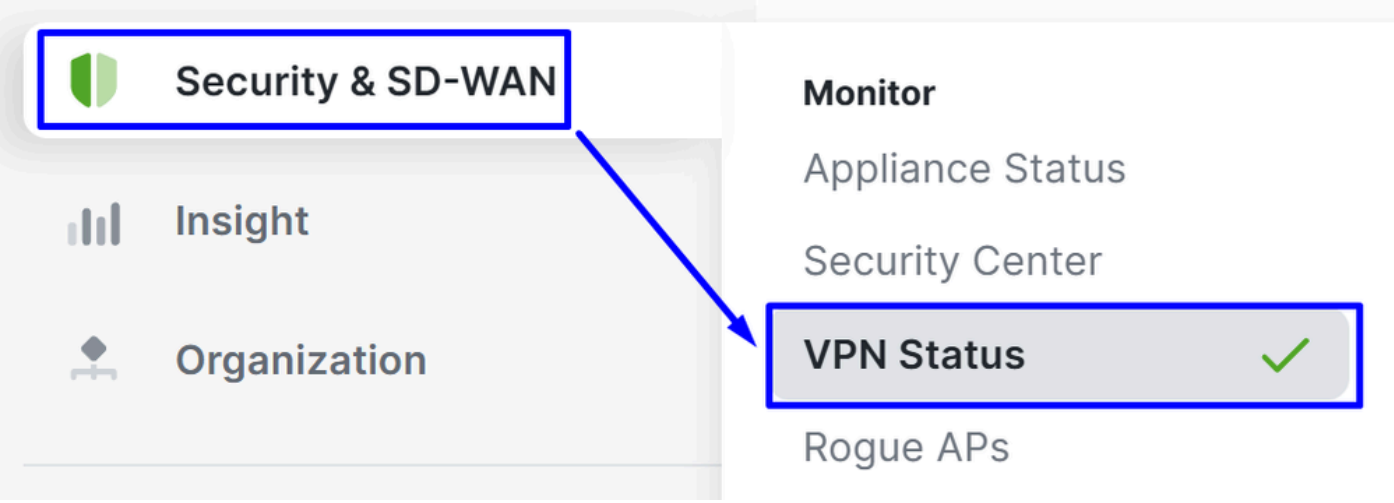


Weitere Informationen finden Sie unter: [Konfigurieren von VPN-Ausschlussregeln (IP/Port/DNS/APP)]

Überprüfung

Um zu überprüfen, ob die Tunnel in Betrieb sind, überprüfen Sie den Status unter:

- Klicken Sie auf Security & SD-WAN > **VPN Status** im Meraki Dashboard.



- Klicken Sie 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				

Wenn sowohl der primäre als auch der sekundäre VPN-Status grün angezeigt werden, bedeutet dies, dass die Tunnel aktiv sind.

Meraki VPN Status Codes

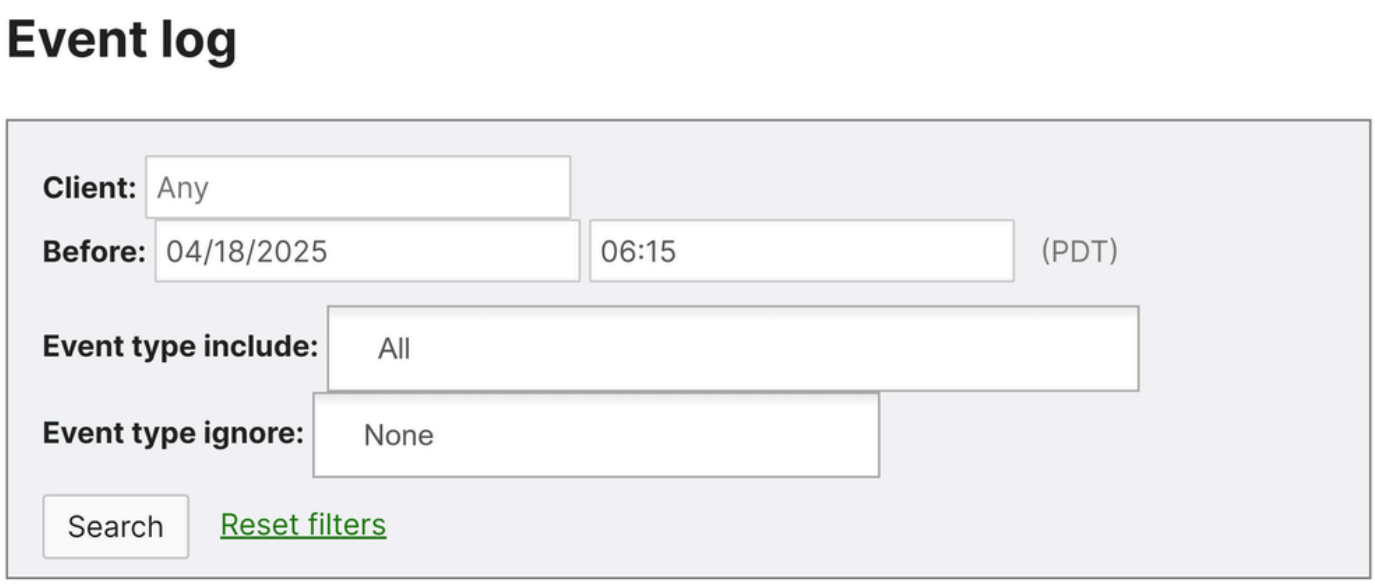
Status Indicator	Color	Meaning
Primary/Secondary Up	Green	Phase 1 and phase 2 are up
Partial Connectivity	Amber	Phase 1 is up but phase 2 is down
Tunnel Down	Red	Phase 1 and phase 2 are both down

Fehlerbehebung

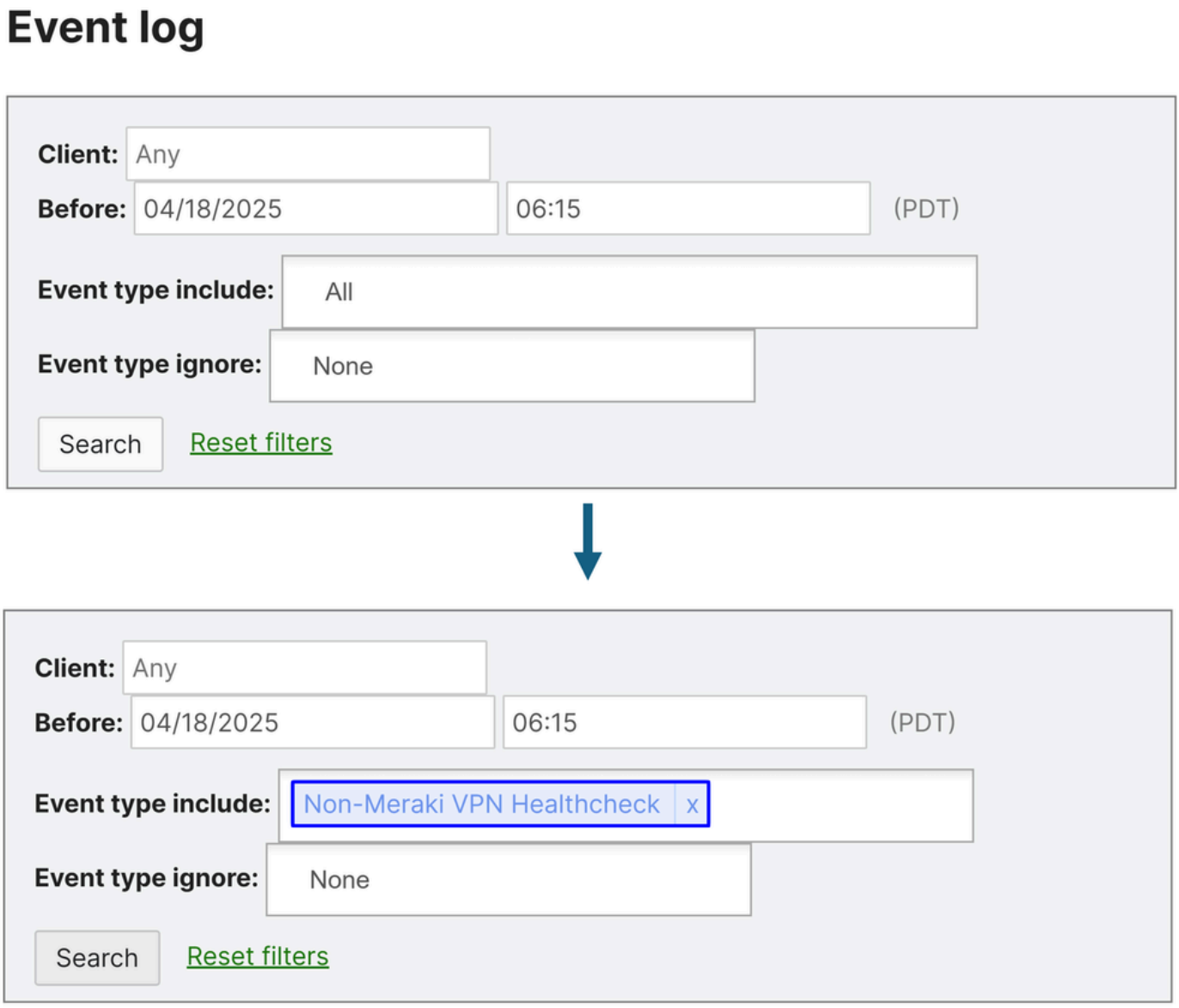
Integritätsprüfungen überprüfen

Navigieren Sie zu den folgenden Seiten, um zu überprüfen, ob die Zustandsprüfungen von Meraki für das VPN ordnungsgemäß funktionieren:

- Klicken Sie auf **Assurance** > Event Log

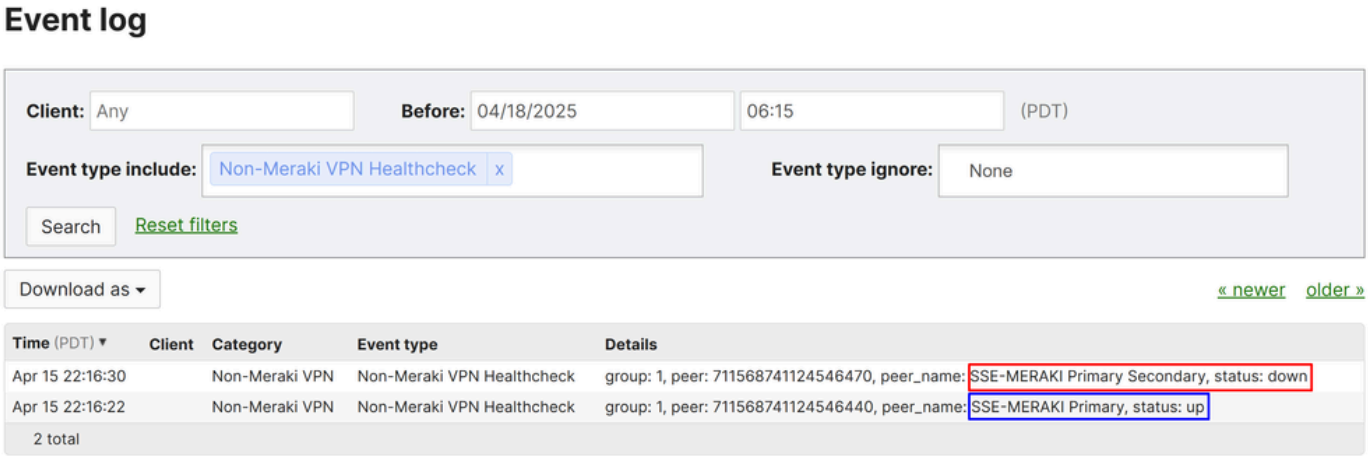


Wählen Sie **Event Type Include**unter Non-Meraki VPN Healthcheck



Wenn der primäre Tunnel zu Cisco Secure Access aktiv ist, werden Pakete, die über den sekundären Tunnel eingehen, verworfen, um einen konsistenten Routing-Pfad aufrechtzuerhalten.

Der sekundäre Tunnel bleibt im Standby-Modus und wird nur verwendet, wenn auf dem primären Tunnel ein Fehler auftritt, entweder von der Meraki-Seite oder innerhalb von Secure Access, wie durch den Health Check-Mechanismus festgelegt.



- Die Statusüberprüfung des primären Tunnels zeigt den Status an: aktiv, d. h. der Datenverkehr wird derzeit weitergeleitet und weitergeleitet.
- Die Statusüberprüfung des sekundären Tunnels zeigt den Status an: nicht, weil der Tunnel nicht verfügbar ist, sondern weil der Primärtunnel gesund ist und aktiv genutzt wird. Dieses Verhalten wird erwartet, da der Datenverkehr nur durch Tunnel 1 geleitet werden darf, was dazu führt, dass die Statusüberprüfung des sekundären Tunnels fehlschlägt.

Zugehörige Informationen

- Technischer Support und Downloads von Cisco
- Cisco Secure Access-Hilfecenter
- Cisco Secure Access Meraki BGP-Konfigurationsleitfaden

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.