

Konfigurieren von sicherem Zugriff mit Meraki MX für Hochverfügbarkeit und Statusüberwachung

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Konfigurieren des VPN für sicheren Zugriff](#)

[Konfiguration des VPN für sicheren Zugriff](#)

[Konfigurieren des VPN auf der Meraki MX](#)

[Standortübergreifendes VPN](#)

[VPN-Einstellungen](#)

[Nicht-Meraki VPN-Peers](#)

[Primärtunnel konfigurieren](#)

[Sekundären Tunnel konfigurieren](#)

[Konfigurieren der Datenverkehrssteuerung \(Tunnelumgehung\)](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Integritätsprüfungen überprüfen](#)

[Zugehörige Informationen](#)

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



CISCO

Meraki

Cisco Meraki MX

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

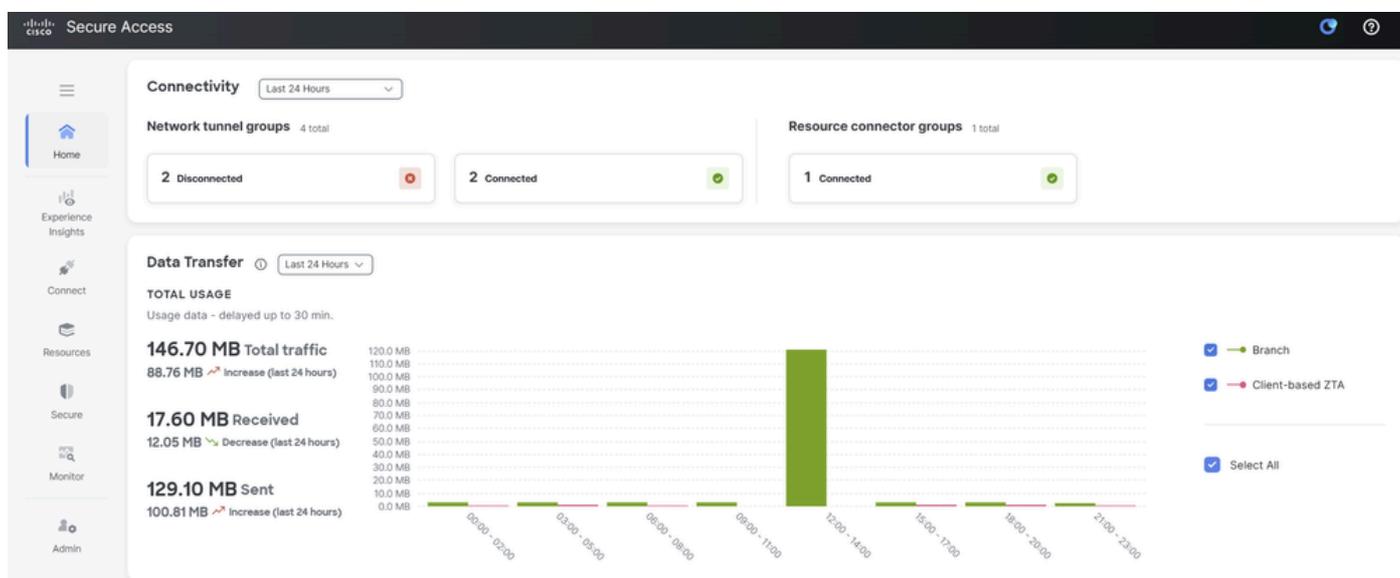
Richtlinien in der Cloud auf internetbasierte Ressourcen zulässt.

- 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.

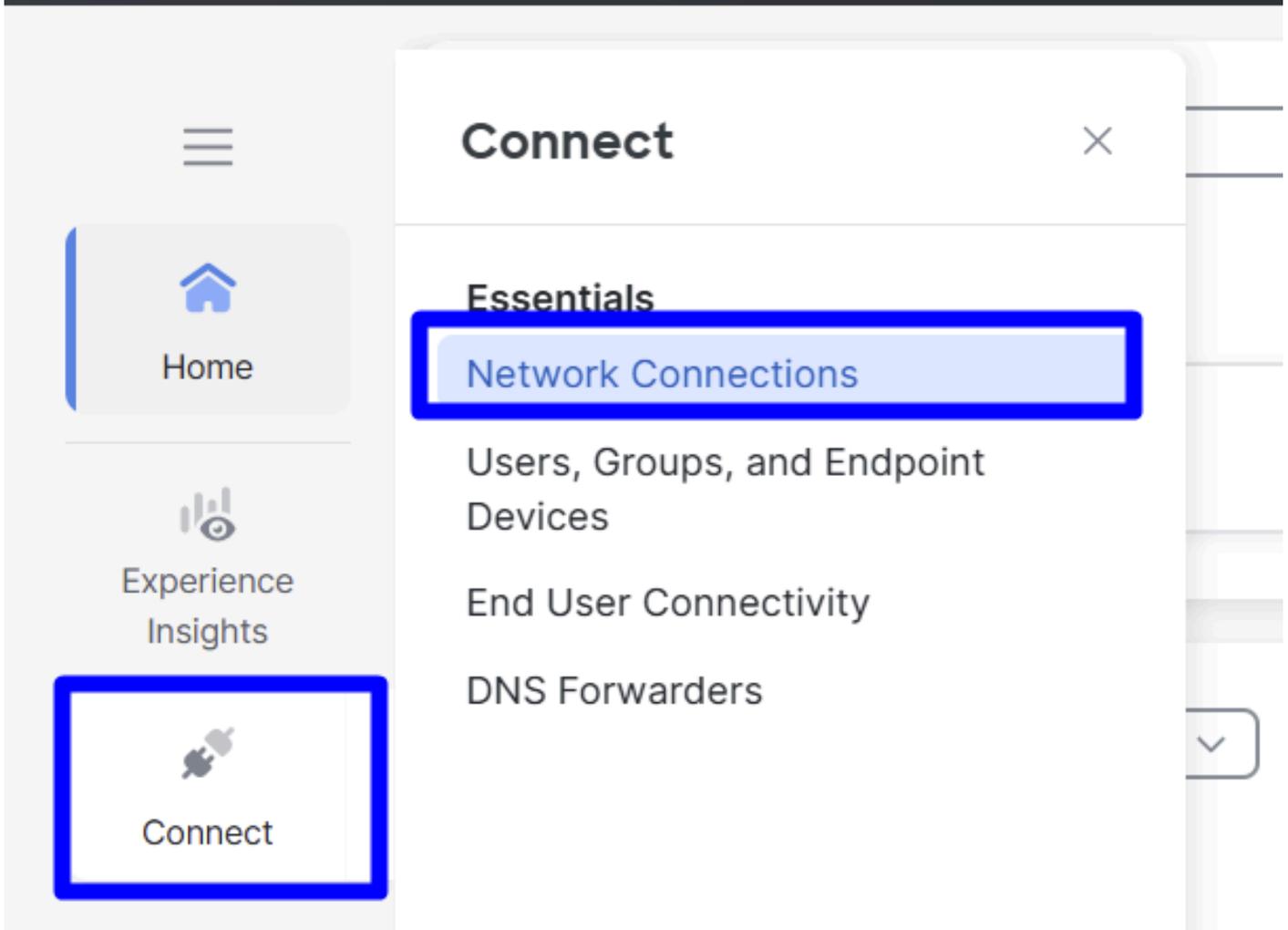
Konfigurieren

Konfigurieren des VPN für sicheren Zugriff

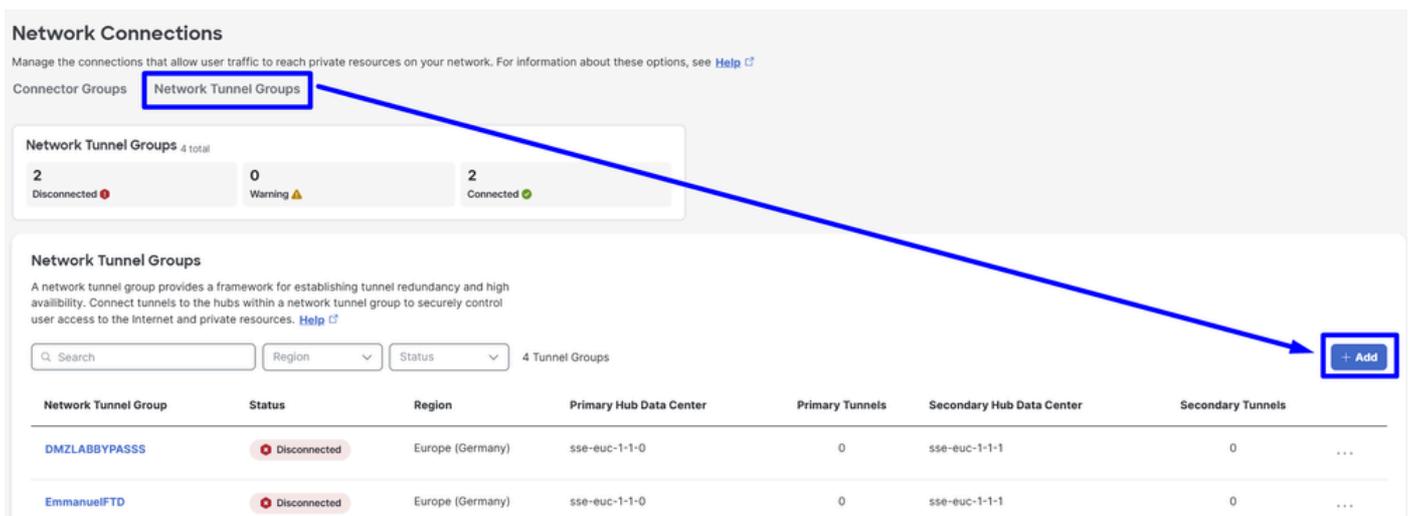
Navigieren Sie zum Admin-Bereich von [Secure Access](#).



- Klicken Sie [Connect > Network Connections](#)



- Klicken Sie unter Network Tunnel Groups auf + Add



- Konfiguration Tunnel Group Name Region und Device Type
- Klicken Sie auf Next

- Konfigurieren Sie die Tunnel ID Format und 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.

Meraki MX Probe IP

192.0.2.3/32 192.168.50.0/24

Dynamic routing

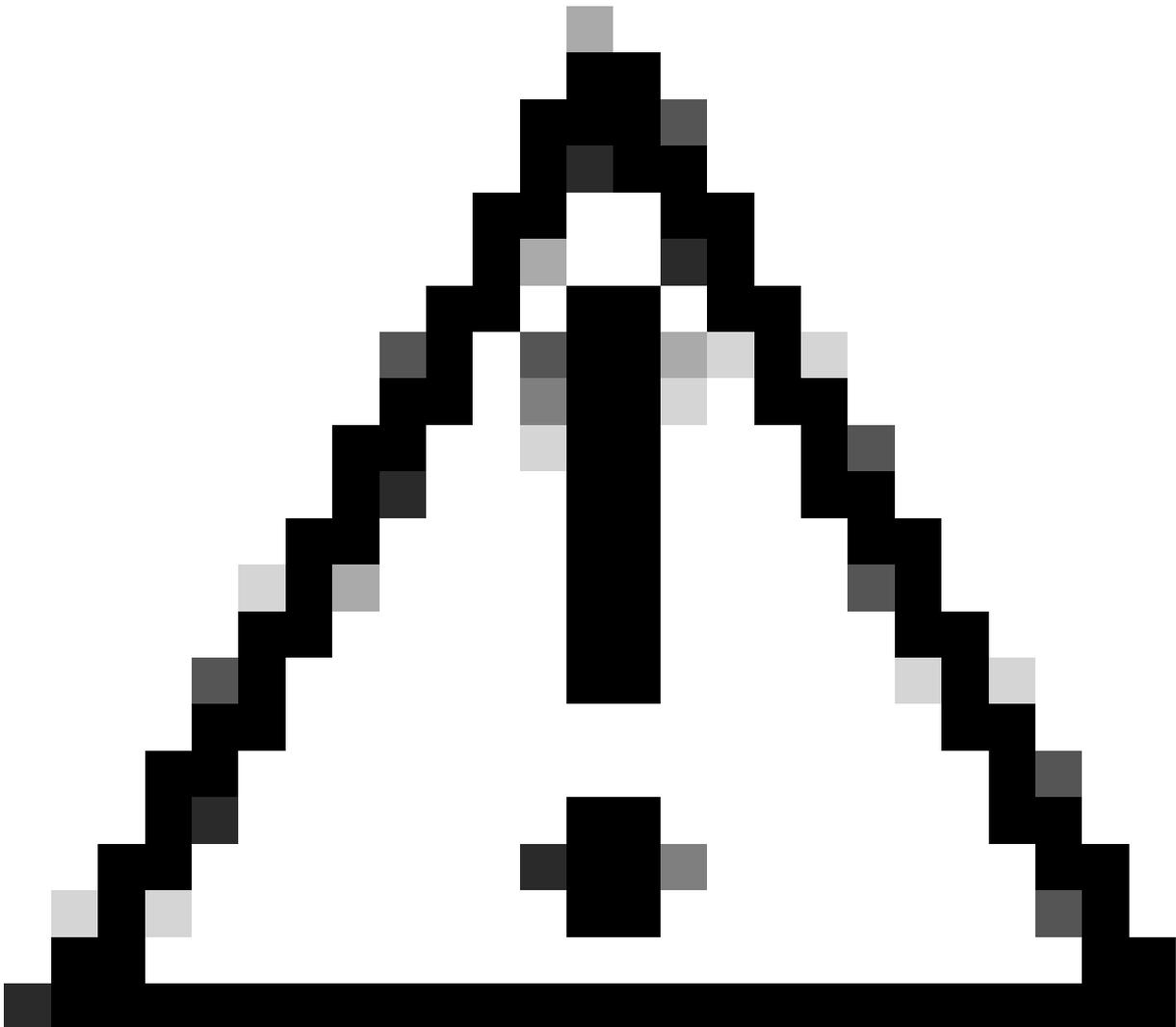
Use this option when you have a BGP peer for your on-premise router.



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**.

The screenshot shows the 'Data for Tunnel Setup' section of a Meraki configuration page. On the left, there is a sidebar with four menu items: 'General Settings', 'Tunnel ID and Passphrase', 'Routing', and 'Data for Tunnel Setup' (which is currently selected). The main content area is titled 'Data for Tunnel Setup' and contains the following information:

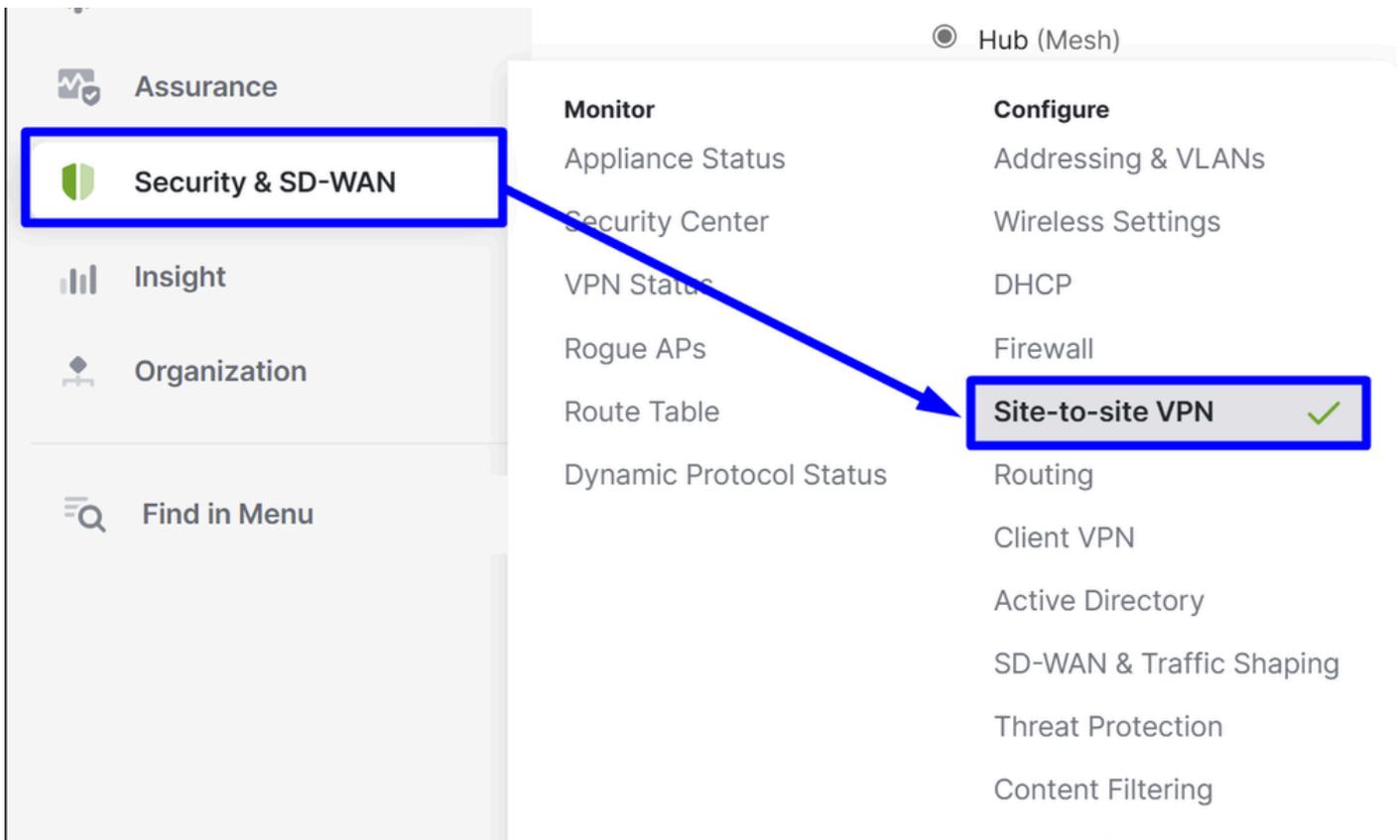
Review and save the following information for use when setting up your network tunnel devices.

Primary Tunnel ID:	MerakiShadow@ [redacted]
Primary Data Center IP Address:	18.156.145.74
Secondary Tunnel ID:	MerakiShadow@ [redacted]
Secondary Data Center IP Address:	3.120.45.23

At the bottom right of the configuration area, there are two buttons: 'Download CSV' and 'Done'.

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.

Site-to-site VPN

Type ⓘ

- Off
Do not participate in site-to-site VPN.
- Hub (Mesh)
Establish VPN tunnels with all hubs and dependent spokes.
- Spoke
Establish VPN tunnels with selected hubs.

VPN-Einstellungen

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

VPN settings

Local networks

Name	VPN mode	Subnet	Uplink
Default	Disabled ▾	4 192.168.0.0/24	Any
SSE-MERAKI	Enabled ▾	4 192.168.50.0/24	Any
LAB NETWORK	Disabled ▾	4 192.168.10.0/24	
LAB NETWORK-30	Disabled ▾	4 192.168.30.0/24	
FMC	Disabled ▾	4 100.64.0.0/10	

Auswahl unter NAT Traversal Automatisch

NAT traversal

- Automatic
Connections to remote peers are arranged by the Meraki cloud.
- Manual: Port forwarding
Remote peers contact the WAN appliance using a public IP and port that you specify.
Use this if your WAN appliance is behind another NAT and "Automatic" traversal does not work.

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	Endpoint	
<input type="text"/>	<input type="text" value="http://"/>	<input type="button" value="Cancel"/> <input type="button" value="Done"/>
<div style="border: 1px solid #ccc; padding: 5px; background-color: #f8d7da;">✖ Health check name can't be blank.</div>		

- **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.

Configure health checks

Configure your health checks to use for tunnel health. Health check will use this IP for probing when the MX is in passthrough mode. Only one health check per tunnel can be used.

+ Add health check

Health check	Endpoint	
<input type="text" value="SSE"/>	<input type="text" value="http://service.sig.umbrella.com"/>	Cancel <input type="button" value="Done"/>

Rows per page < >

Cancel

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

Primärtunnel konfigurieren

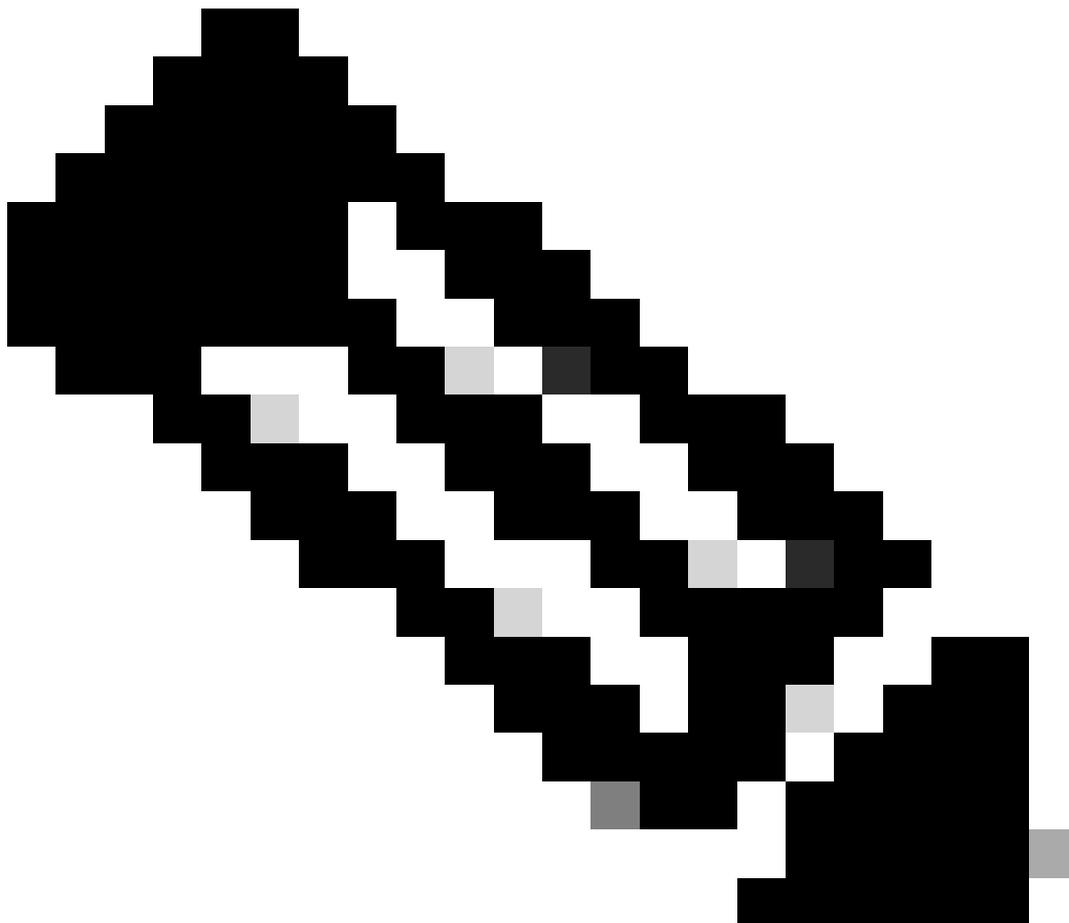
- Klicken Sie +Add a peer

Name <input type="text" value="SSE-MERAKI Primary"/>	Remote ID ⓘ <input type="text" value="Optional"/>	Availability ⓘ <input type="text" value="All networks"/>
IKE version <input type="text" value="IKEv2"/> <small>IKEv2 is required to support backup tunnels and failover features</small>	Shared secret <input type="text" value="....."/> <input type="button" value="Show"/>	Tunnel monitoring
Peers ^	Routing <input checked="" type="radio"/> Static <input type="radio"/> Dynamic (BGP) <small>Static routing is required to support backup tunnels and failover features</small>	Health check <input type="text" value="SSE"/>
Public IP or Hostname <input type="text" value="18.156.145.74"/>	Private subnets ⓘ <input type="text" value="0.0.0.0/0"/>	Failover directly to internet ⓘ <input checked="" type="checkbox"/> Enable failover
Local ID <input type="text" value="Merakishadow@...cit"/>		IPsec policy ^
		Preset <input type="text" value="Umbrella"/>

- 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 angegebene](#)
 - Lokale ID: Konfigurieren Sie die **Primary Tunnel ID** unter Sicherer Zugriff im Schritt [Sicherer Zugriff VPN-Konfigurationen angegebene](#)
 - 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

#	Name	IKE version	IPsec policies	Public IP or Hostname	Local ID	Remote ID	IPsec subnets	Health check	Preshared secret	Availability/Network
> 1	SSE-MERAKI Primary	IKEv2	Umbrella	18.156.145.74	merakijairo@8195126-646082001-sse.cisco.com	—	0.0.0.0/0	SSE	All networks

1-1 of 1 Rows per page 10 < 1 >

- Klicken Sie **+ Add Secondary peer**

Primary



Edit primary peer



Move to



Delete primary peer

Secondary



Add secondary peer

- Klicken Sie **Inherit** primary peer configurations

Add Secondary VPN Peer



Inherit primary peer configurations



Name

SSE Secondary

IKE version

IKEv2

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

Peers



Public IP or Hostname

Local ID

Remote ID ⓘ

Shared secret

 [Show](#)

Routing

Static

Private subnets ⓘ

0.0.0.0/0

Tunnel monitoring

Health check

 ⊗ ▾

- Peers

- Öffentliche IP oder Hostname: Konfigurieren Sie die **Secondary Datacenter IP** unter Sicherer Zugriff im Schritt [Sicherer Zugriff VPN-Konfigurationen angegebene](#)
- Lokale ID: Konfigurieren Sie die **Secondary Tunnel ID** unter Sicherer Zugriff im Schritt [Sicherer Zugriff VPN-Konfigurationen angegebene](#)
- 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:

The settings you requested require confirmation. Please review the following list.

- The VLAN subnets 192.168.0.0/24 and 192.168.50.0/24 overlap with remote VPN subnets on non-Meraki peers SSE-MERAKI Primary (0.0.0.0/0) and SSE-MERAKI Primary Secondary (0.0.0.0/0). IP traffic will be routed to the smallest subnet that contains the IP address.
- In the non-Meraki VPN peers configuration, potential overlaps might occur between the subnets on SSE-MERAKI Primary (0.0.0.0/0), SSE-MERAKI Primary Secondary (0.0.0.0/0), and SSE (1.1.1.1/32). Please note that in this case, IP traffic will be routed to the most specific subnet.
- In the non-Meraki VPN peers configuration, potential conflicts might occur between the subnets on SSE-MERAKI Primary (0.0.0.0/0) and SSE-MERAKI Primary Secondary (0.0.0.0/0). Before confirming your changes, please review the network tags under the Availability column for each of these non-Meraki VPN peers and ensure that there are no Security Appliances within your Organization that are tagged across different non-Meraki VPN peers with conflicting subnets. Please note that in the event that a single Security Appliance is configured with the same private subnets for more than one non-Meraki VPN peer, the routing behavior of your IP traffic will be undefined.
- To learn more, please refer to the Peer Availability section of the Site-to-site VPN Settings knowledge base article (accessible through the non-Meraki VPN peers tooltip).

[Confirm Changes](#)

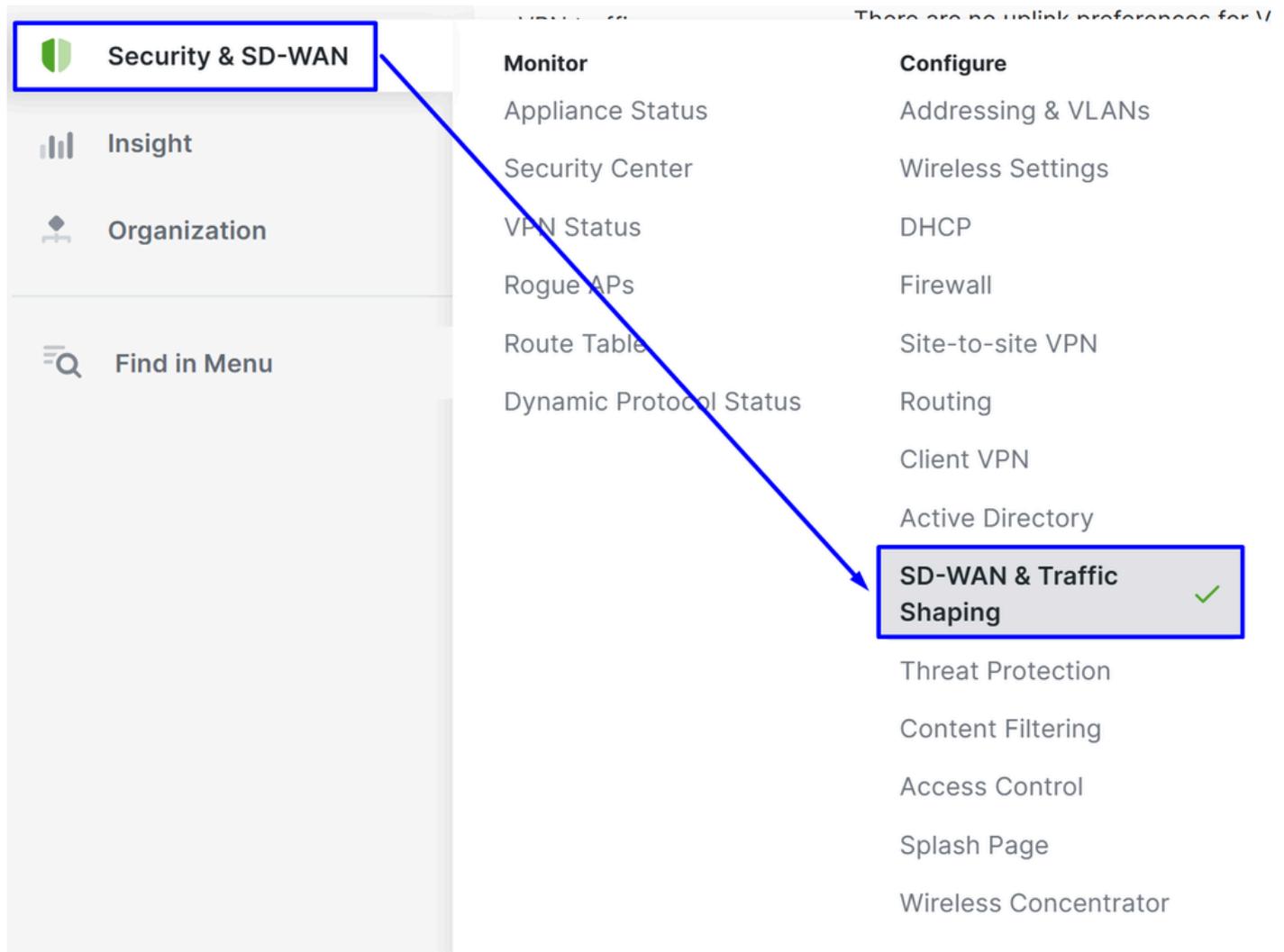
[Cancel](#)

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+**

Local internet breakout

VPN exclusion rules

Add +

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

Custom Expressions - Protocol

Custom expressions	Custom expressions
Major applications	Protocol
	TCP
	Destination ⓘ
	8.8.8.8
	Dst port ⓘ
	443
	Add expression

Custom Expressions - DNS

Custom expressions

Major applications

Custom expressions

Protocol
DNS

Destination ⓘ facebook.com

Dst port ⓘ 443

Add expression

Major Applications

Custom expressions

Major applications

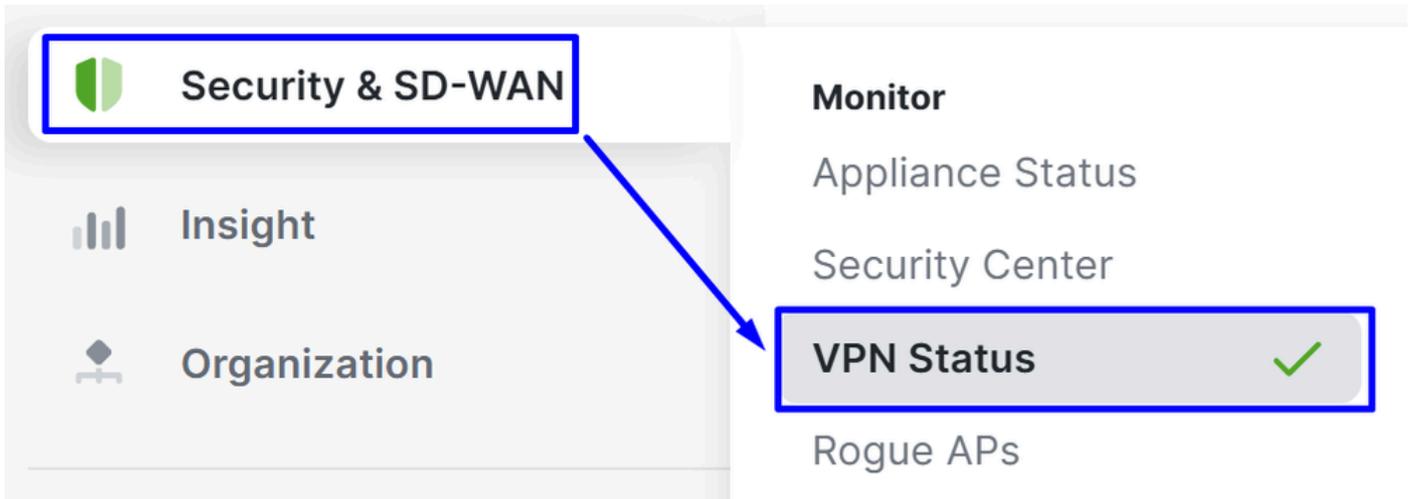
- AWS
- Box
- Office 365 Sharepoint
- Office 365 Suite
- Oracle
- Salesforce
- SAP
- Skype & Teams
- Webex
- Zoom

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

Event log

Client:

Before: (PDT)

Event type include:

Event type ignore:

[Reset filters](#)

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

Event log

Client: Any

Before: 04/18/2025 06:15 (PDT)

Event type include: All

Event type ignore: None

[Reset filters](#)



Client: Any

Before: 04/18/2025 06:15 (PDT)

Event type include: Non-Meraki VPN Healthcheck x

Event type ignore: None

[Reset filters](#)

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.

Event log

Client: Any **Before:** 04/18/2025 06:15 (PDT)

Event type include: Non-Meraki VPN Healthcheck x **Event type ignore:** None

[Reset filters](#)

Download as

[« newer](#) [older »](#)

Time (PDT) ▼	Client	Category	Event type	Details
Apr 15 22:16:30	Non-Meraki VPN	Non-Meraki VPN	Non-Meraki VPN Healthcheck	group: 1, peer: 711568741124546470, peer_name: SSE-MERAKI Primary Secondary, status: down
Apr 15 22:16:22	Non-Meraki VPN	Non-Meraki VPN	Non-Meraki VPN Healthcheck	group: 1, peer: 711568741124546440, peer_name: SSE-MERAKI Primary, status: up

2 total

- 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.