

Configuration d'un accès sécurisé avec Meraki MX pour une haute disponibilité et une surveillance de l'état

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Configurer le VPN sur un accès sécurisé](#)

[Configuration VPN d'accès sécurisé](#)

[Configuration du VPN sur Meraki MX](#)

[VPN de site à site](#)

[Paramètres VPN](#)

[Homologues VPN non Meraki](#)

[Configuration du tunnel principal](#)

[Configuration du tunnel secondaire](#)

[Configurer le pilotage du trafic \(contournement du trafic en tunnel\)](#)

[Vérifier](#)

[Dépannage](#)

[Vérifier les bilans de santé](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer Cisco Secure Access avec Meraki MX pour la haute disponibilité à l'aide de vérifications d'intégrité.

Conditions préalables

- [Examen des exigences du tunnel IPsec avec accès sécurisé](#)
- Comprendre les composants d'accès sécurisé
- [Comprendre la fonctionnalité de contrôle du fonctionnement dans Meraki MX](#)

Exigences

- Meraki MX doit exécuter la version 19.1.6 ou ultérieure du micrologiciel
- Lors de l'utilisation de l'accès privé, un seul tunnel est pris en charge en raison d'une

limitation de Meraki qui empêche de modifier l'adresse IP du contrôle d'intégrité, rendant la NAT requise pour les tunnels SPA (Secure Private Access) supplémentaires. Cela ne s'applique pas lorsque vous utilisez SIA (Secure Internet Access).

- Définissez clairement quels sous-réseaux ou ressources internes sont routés via le tunnel vers Secure Access.

Composants utilisés

- Accès sécurisé Cisco
- Appliance de sécurité Meraki MX (microprogramme version 19.1.6 ou ultérieure)
- Tableau de bord Cisco Meraki
- Tableau de bord Secure Access

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

CISCO Secure Access



CISCO

Meraki

Cisco Meraki MX

Cisco Secure Access est une plate-forme de sécurité native au cloud qui permet un accès sécurisé aux applications privées (via un accès privé) et aux destinations Internet (via un accès Internet). Lorsqu'elle est intégrée à Meraki MX, elle permet aux entreprises d'établir des tunnels IPsec sécurisés entre les sites des filiales et le cloud, garantissant ainsi un flux de trafic chiffré et une application de sécurité centralisée.

Cette intégration utilise des tunnels IPsec de routage statique. Meraki MX établit des tunnels IPsec principaux et secondaires vers Cisco Secure Access et exploite ses contrôles d'intégrité de liaison ascendante intégrés pour effectuer un basculement automatique entre les tunnels. Cela permet d'obtenir une configuration résiliente et haute disponibilité pour la connectivité des filiales.

Les éléments clés de ce déploiement sont les suivants :

- Meraki MX agissant en tant qu'homologue VPN autre que Meraki pour Cisco Secure Access.
- Tunnels principaux et secondaires configurés de manière statique, avec des contrôles d'intégrité déterminant la disponibilité.
- L'accès privé prend en charge l'accès sécurisé aux applications internes via SPA (Secure Private Access), tandis que l'accès Internet permet au trafic d'atteindre les ressources

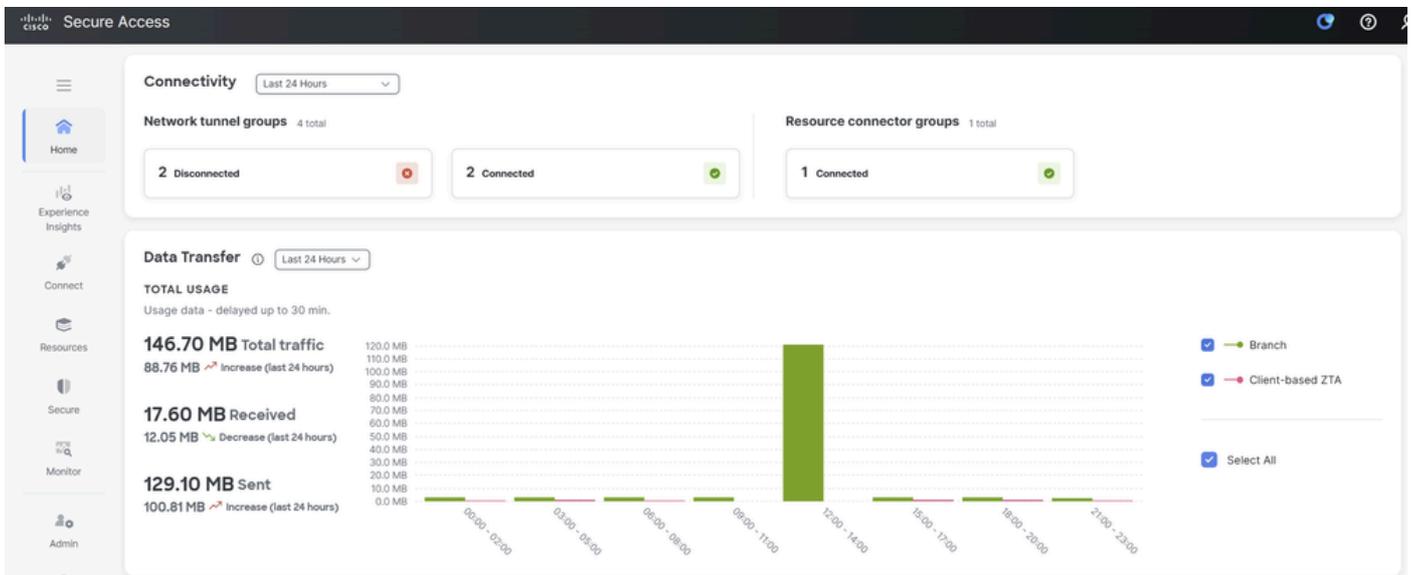
Internet avec l'application de politiques dans le cloud.

- En raison des limites de Meraki en matière de souplesse IP de contrôle d'intégrité, un seul groupe de tunnels est pris en charge en mode d'accès privé. Si plusieurs périphériques Meraki MX doivent se connecter à un accès sécurisé pour un accès privé, vous devez soit utiliser le protocole [BGP](#) pour le routage dynamique, soit configurer des tunnels statiques, sachant qu'un seul groupe de tunnels réseau peut prendre en charge les vérifications d'intégrité et la haute disponibilité. Les tunnels supplémentaires fonctionnent sans surveillance de l'état ou redondance.

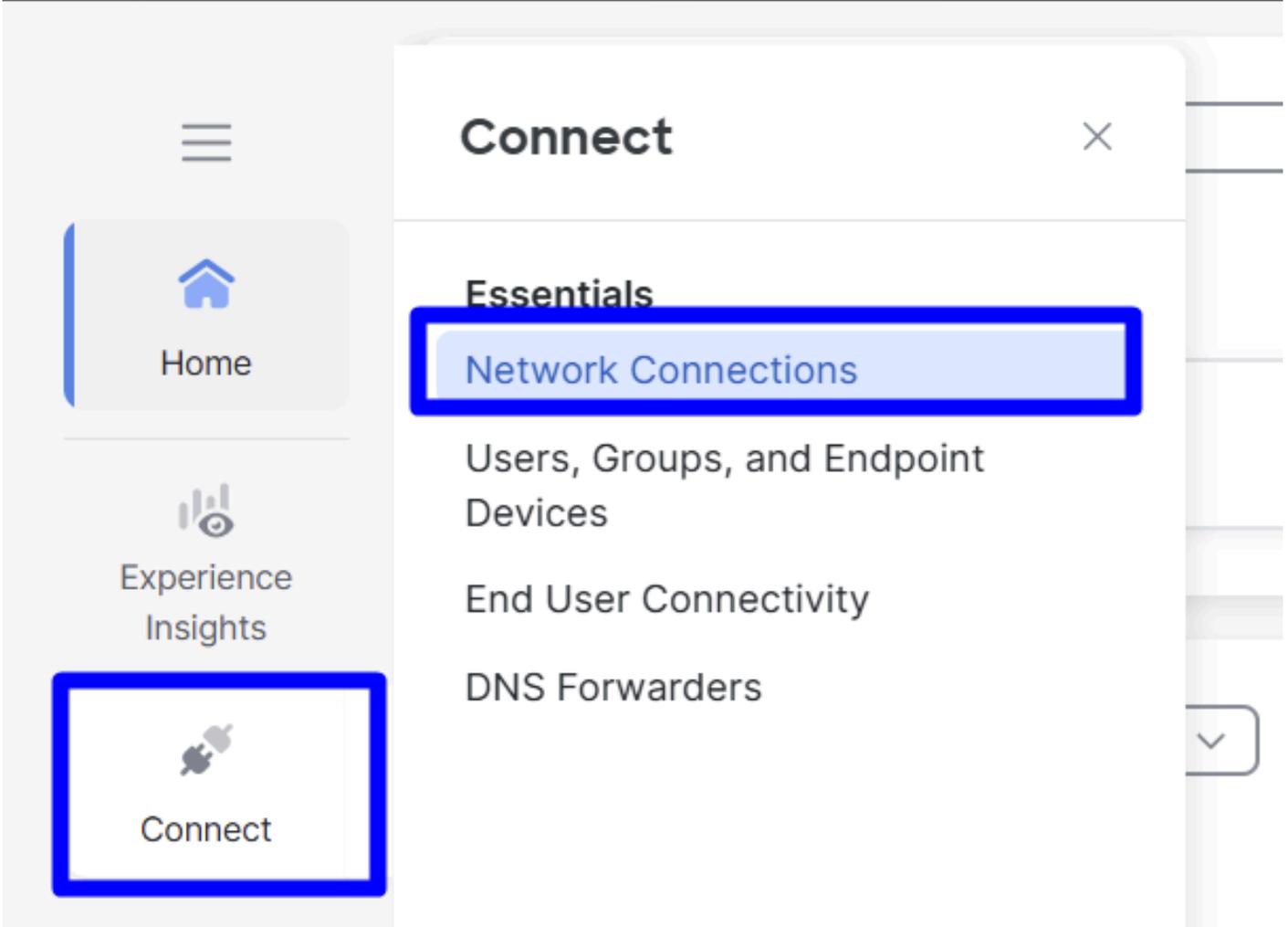
Configurer

Configurer le VPN sur un accès sécurisé

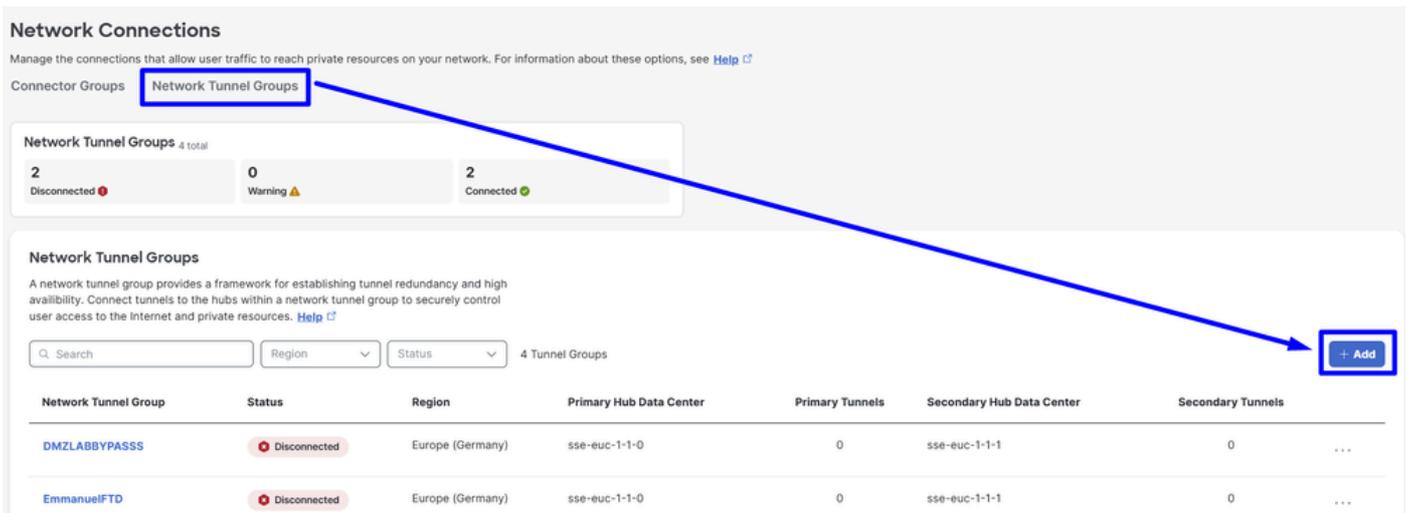
Accédez au panneau d'administration de [Secure Access](#).



- Cliquez sur **Connect > Network Connections**



- Sous Network Tunnel Groups Cliquez sur + Add



- Configurer Tunnel Group Name, Region et Device Type
- Cliquer Next

- Configurez les Tunnel ID Format et Passphrase
- Cliquer Next

- Configurez les plages d'adresses IP ou les hôtes que vous avez configurés sur votre réseau et que vous souhaitez faire passer le trafic via l'accès sécurisé et assurez-vous d'inclure l'adresse IP de la sonde de surveillance Meraki, 192.0.2.3/32 afin de permettre le retour du trafic depuis l'accès sécurisé vers le Meraki MX.
- Cliquer 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

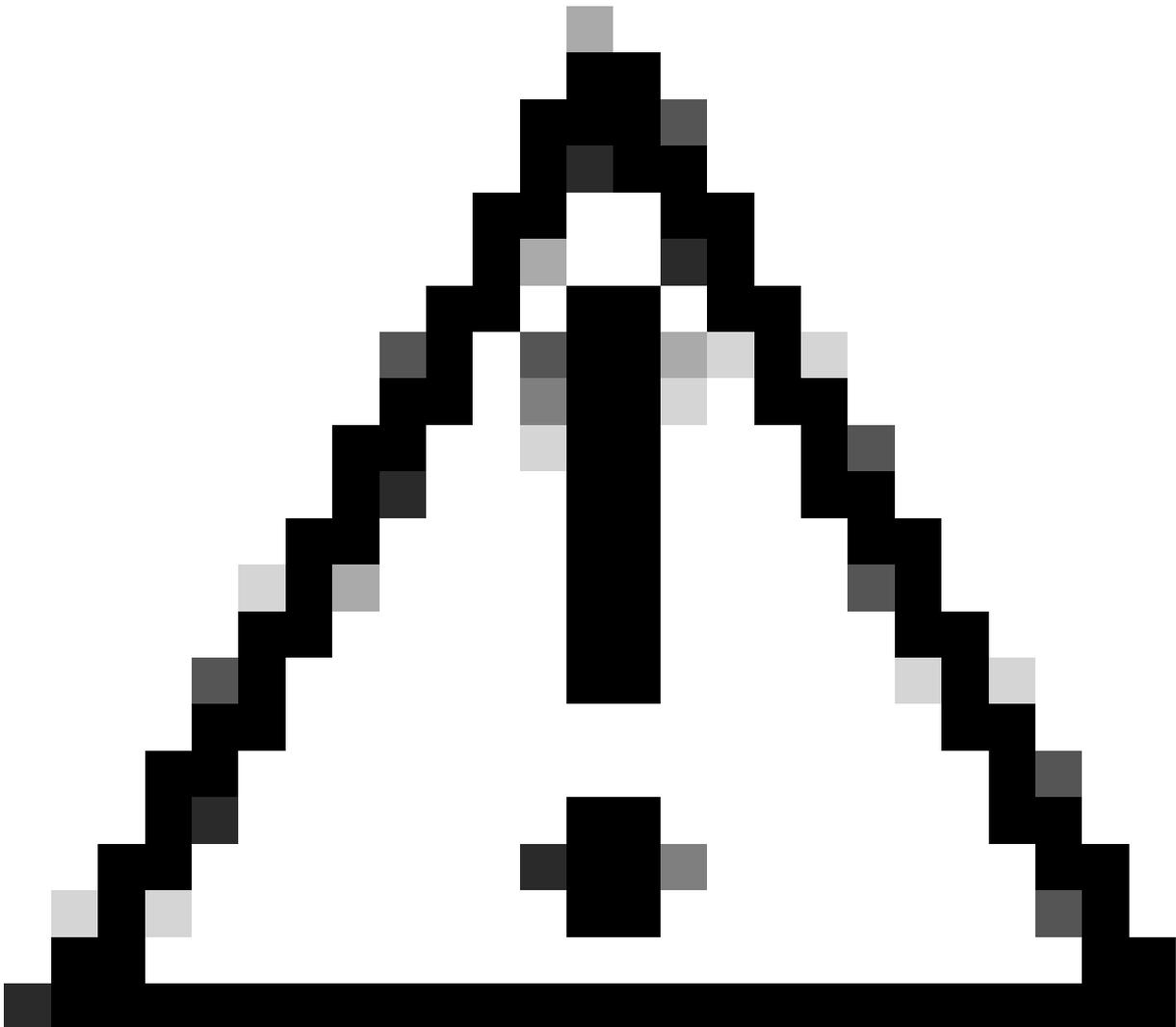
Use this option when you have a BGP peer for your on-premise router.



Cancel

Back

Save



Mise en garde : Veillez à ajouter la sonde de surveillance IP (192.0.2.3/32) ; sinon, vous pouvez rencontrer des problèmes de trafic sur le périphérique Meraki qui achemine le trafic vers Internet, les pools VPN et la plage CGNAT 100.64.0.0/10 utilisée par ZTNA.

- Après avoir cliqué sur **save** les informations sur le tunnel s'affiche, veuillez enregistrer ces informations pour l'étape suivante, **Configure the tunnel on Meraki MX**.

Configuration VPN d'accès sécurisé

Copiez la configuration des tunnels dans un bloc-notes. Utilisez ces informations pour terminer la configuration dans Meraki **Non-Meraki VPN Peers**.

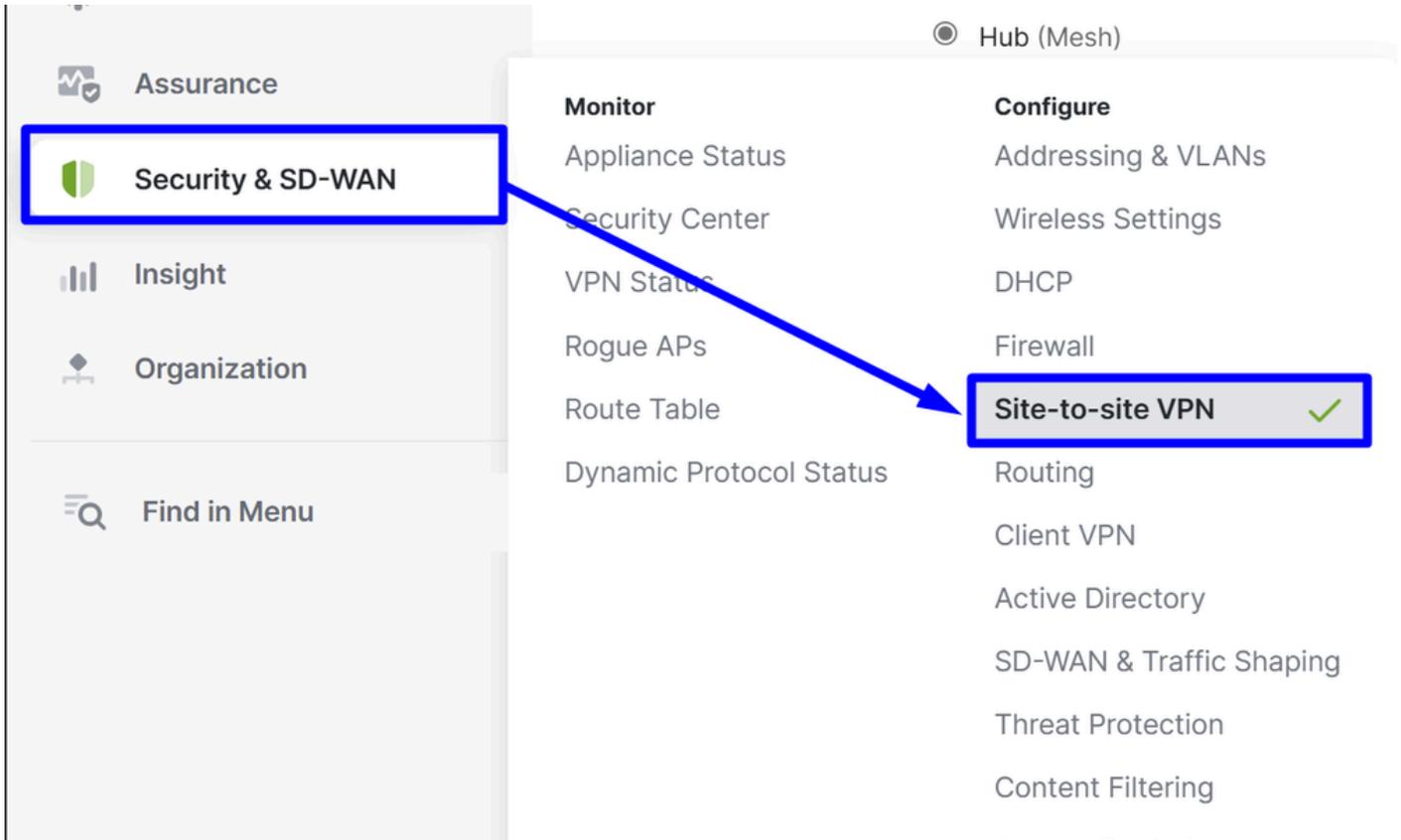
The screenshot shows the 'Data for Tunnel Setup' section of the Meraki configuration interface. On the left, a sidebar contains four menu items: 'General Settings', 'Tunnel ID and Passphrase', 'Routing', and 'Data for Tunnel Setup', each with a checkmark icon. The main content area is titled 'Data for Tunnel Setup' and includes the instruction: 'Review and save the following information for use when setting up your network tunnel devices.' Below this, there are four fields for configuration data:

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

At the bottom right of the configuration area, there are two buttons: 'Download CSV' (outlined) and 'Done' (solid blue).

Configuration du VPN sur Meraki MX

Accédez à votre Meraki MX et cliquez sur **Security & SD-WAN > Site-to-site VPN**



VPN de site à site

Choisir 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.

Paramètres VPN

Choisissez les réseaux que vous avez sélectionnés pour envoyer le trafic vers l'accès sécurisé :

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	

Choisir dans NAT Traversal Automatique

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.

Homologues VPN non Meraki

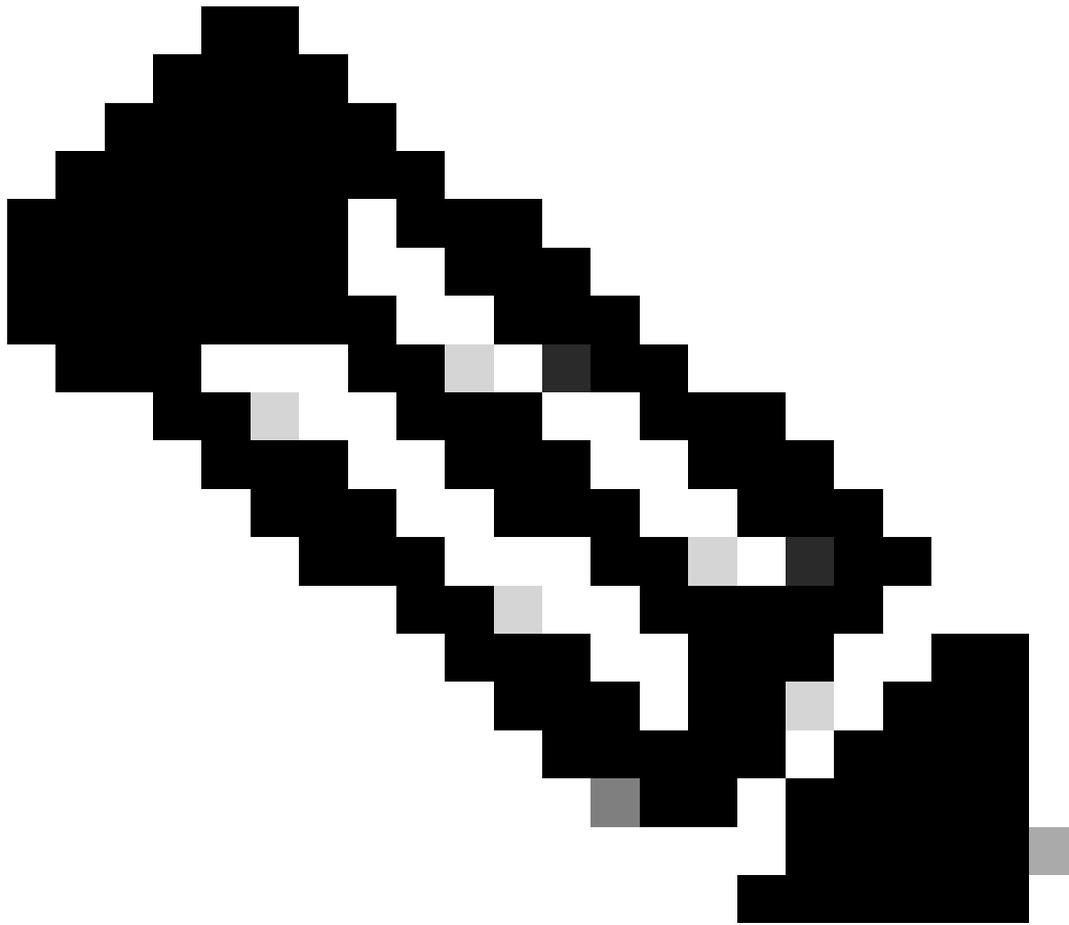
Vous devez configurer les contrôles d'intégrité que Meraki utilise pour acheminer le trafic vers Secure Access :

Cliquez sur **Configure Health Checks**

- Cliquez sur **+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:** Configurez un nom pour le test
- **Endpoint:** Utilisez celle recommandée par Secure Access <http://service.sig.umbrella.com>



Remarque : Ce domaine répond uniquement lorsqu'il est accessible via un tunnel de site à site avec un accès sécurisé ou un parapluie : les tentatives d'accès en dehors de ces tunnels échouent.

Cliquez ensuite **Done** deux fois pour finaliser.

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 Done

Rows per page < >

[Cancel](#) [Done](#)

Vos contrôles d'intégrité sont maintenant configurés et vous êtes prêt à configurer le Peer:

Configuration du tunnel principal

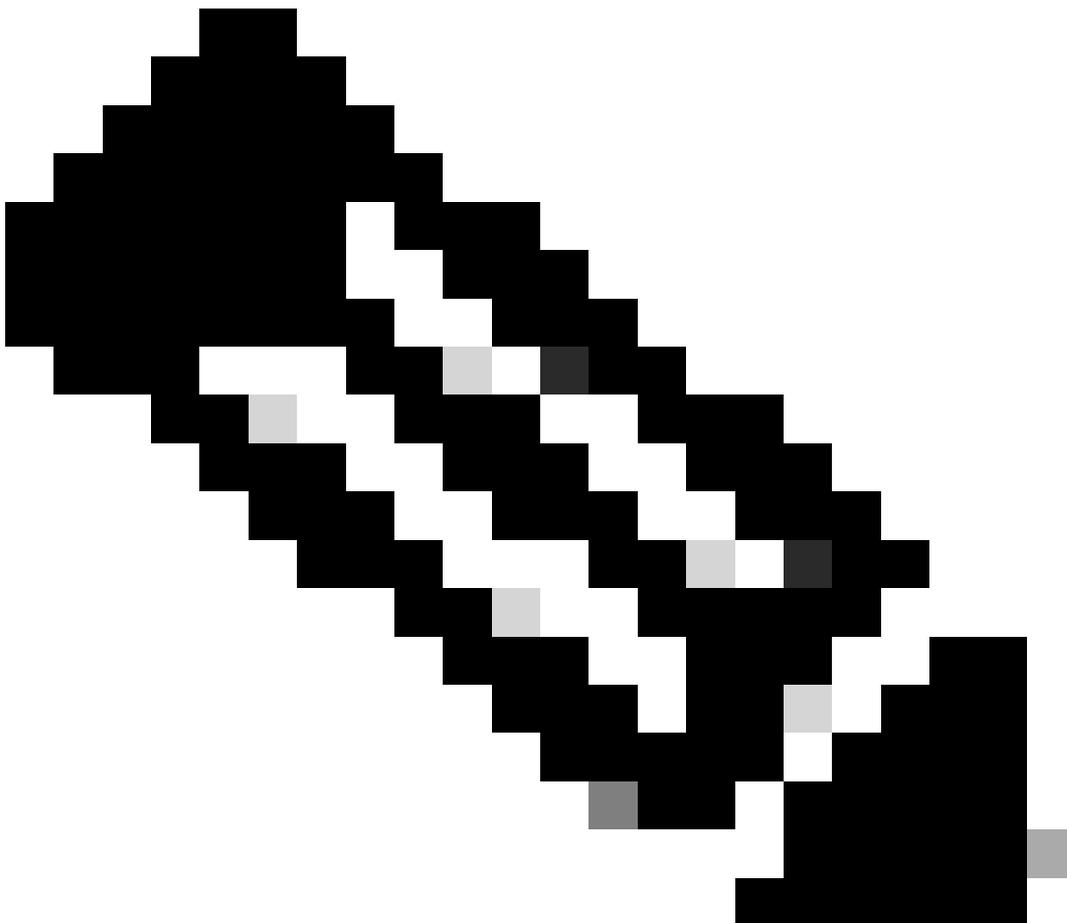
- Cliquez sur [+Add a peer](#)

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="....."/> 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"/>

- Ajouter un homologue VPN
 - Name : Configurez un nom pour le VPN pour un accès sécurisé
 - Version IKE : Choisir IKEv2
- Pairs
 - Adresse IP publique ou nom d'hôte : Configurez les données **Primary Datacenter IP** fournies par Secure Access dans l'étape [Configurations VPN d'accès sécurisé](#)
 - ID local : Configurez les données **Primary Tunnel ID** fournies par Secure Access dans l'étape [Configurations VPN d'accès sécurisé](#)
 - ID distant : S/O
 - Shared secret : configurez les données **Passphrase** fournies par Secure Access à l'étape

Secure Access VPN Configurations

- Routage : Choisir statique
 - Sous-réseaux privés : si vous prévoyez de configurer à la fois l'accès Internet et l'accès privé, utilisez 0.0.0.0/0 comme destination. Si vous configurez uniquement l'accès privé pour ce tunnel VPN, spécifiez le **Remote Access VPN IP Pool** et la plage CGNAT comme réseaux 100.64.0.0/10 de destination
 - Disponibilité : si vous n'avez qu'un seul appareil Meraki, vous pouvez sélectionner **All Networks**. Si vous disposez de plusieurs périphériques, veillez à sélectionner uniquement le réseau Meraki spécifique sur lequel vous configurez le tunnel.
 - Surveillance du tunnel
 - Vérification du fonctionnement : Utilisez le contrôle d'intégrité précédemment configuré pour surveiller la disponibilité du tunnel
 - Basculement direct vers Internet : Si vous activez cette option et que les vérifications de l'intégrité du tunnel 1 et du tunnel 2 échouent, le trafic est redirigé vers l'interface WAN pour empêcher la perte de l'accès à Internet.
-



Fonctionnalité de vérification de l'intégrité : Si le tunnel 1 est surveillé et que sa vérification

de l'intégrité échoue, le trafic bascule automatiquement vers le tunnel 2. Si le tunnel 2 échoue également et que l'option est activée, le trafic est acheminé via l'interface WAN du périphérique Meraki et l'option `Failover directly to Internet` l'interface WAN est activée.

- Stratégie IPsec
 - Préréglage : Choisir **Umbrella**

Cliquez ensuite sur `Save`.

Configuration du tunnel secondaire

Pour configurer le tunnel secondaire, cliquez sur le menu d'options du tunnel principal :

- Cliquez sur les trois points

#	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	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 >

- Cliquez sur `+ Add Secondary peer`

Primary



Edit primary peer



Move to



Delete primary peer

Secondary



Add secondary peer

- Cliquez sur `Inherit` primary peer configurations

Add Secondary VPN Peer



Inherit primary peer configurations



Name

SSE Secondary

IKE version

IKEv2

Vous remarquerez ensuite que certains champs sont remplis automatiquement. Vérifiez-les, apportez les modifications nécessaires et complétez le reste manuellement :

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

 ⓘ ▾

- Pairs

- Adresse IP publique ou nom d'hôte : Configurez les données **Secondary Datacenter IP** fournies par Secure Access dans l'étape [Configurations VPN d'accès sécurisé](#)
- ID local : Configurez les données **Secondary Tunnel ID** fournies par Secure Access dans l'étape [Configurations VPN d'accès sécurisé](#)
- ID distant : S/O
- Shared secret : configurez les données **Passphrase** fournies par Secure Access à l'étape [Secure Access VPN Configurations](#)

- Surveillance du tunnel

- Vérification du fonctionnement : Utilisez le contrôle d'intégrité précédemment configuré pour surveiller la disponibilité du tunnel

Ensuite, vous pouvez cliquer sur **Save**, et l'alerte suivante apparaît :

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).

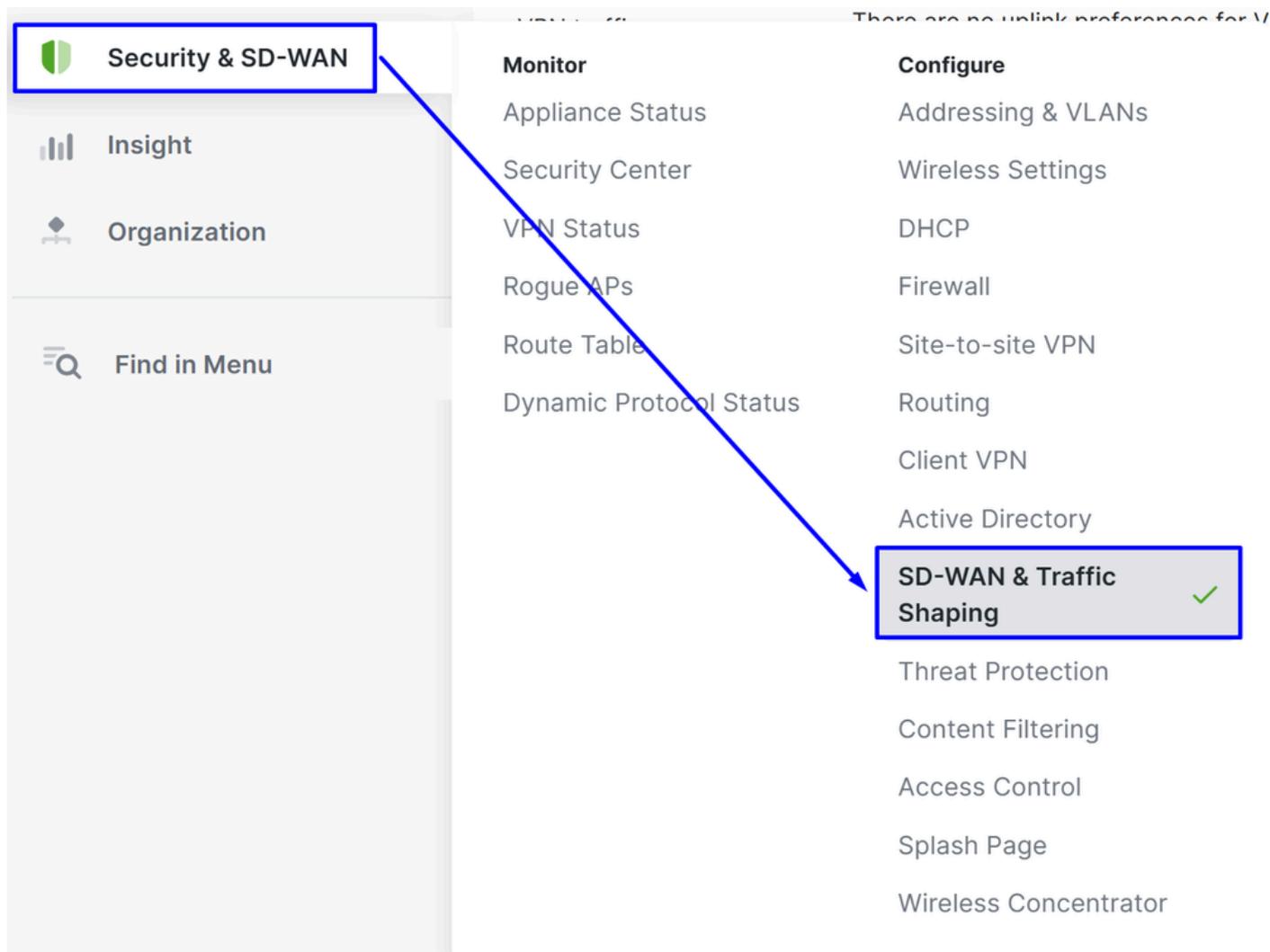
[Confirm Changes](#) [Cancel](#)

Ne vous inquiétez pas et cliquez **Confirm Changes**.

Configurer le pilotage du trafic (contournement du trafic en tunnel)

Cette fonctionnalité vous permet de contourner le trafic spécifique du tunnel en définissant des domaines ou des adresses IP dans la configuration de contournement SD-WAN :

- Accédez à **Security & SD-WAN** > **SD-WAN & Traffic Shaping**



- Faites défiler jusqu'à la **Local Internet Breakout** section et cliquez sur **Add+**

Local internet breakout

VPN exclusion rules

Add +

Créez ensuite le contournement en fonction de **Custom Expressions** OU de **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

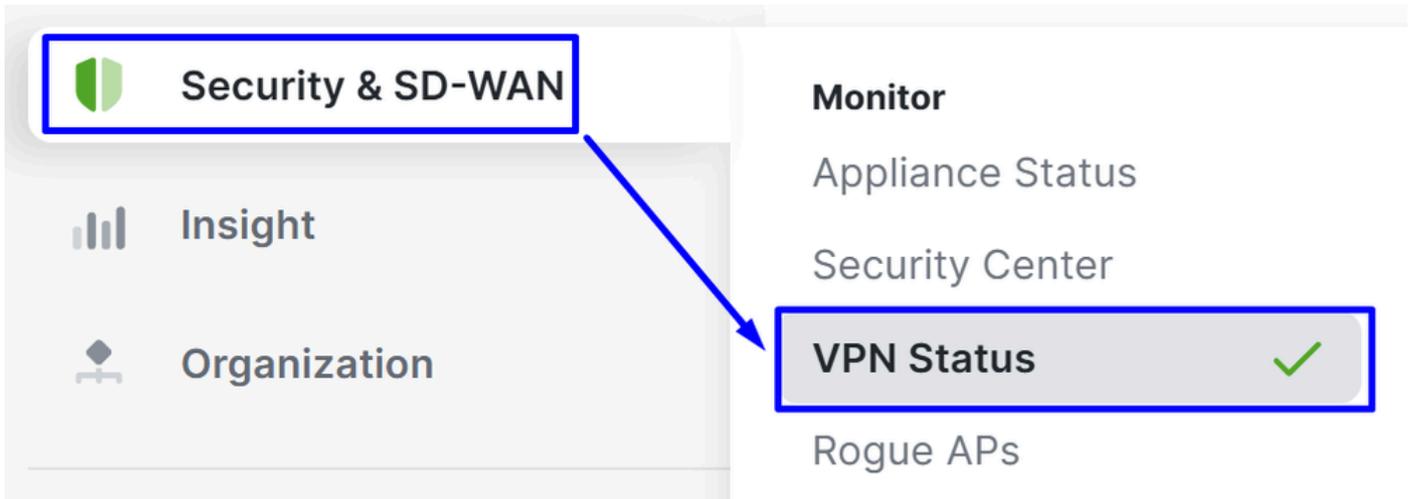
- AWS
- Box
- Office 365 Sharepoint
- Office 365 Suite
- Oracle
- Salesforce
- SAP
- Skype & Teams
- Webex
- Zoom

Pour plus d'informations, consultez : [Configuration des règles d'exclusion VPN \(IP/Port/DNS/APP\)](#)

Vérifier

Pour vérifier si les tunnels sont actifs, vérifiez l'état dans :

- Cliquez sur **Security & SD-WAN** > dans **VPN Status** le tableau de bord Meraki.



- Cliquez sur 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				

Si les deux états VPN principal et secondaire sont affichés en vert, cela signifie que les tunnels sont actifs et actifs.

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

Dépannage

Vérifier les bilans de santé

Pour vérifier si les contrôles d'intégrité Meraki pour le VPN fonctionnent correctement, accédez à :

- Cliquez sur **Assurance** > Event Log

Event log

Client:

Before: (PDT)

Event type include:

Event type ignore:

[Reset filters](#)

Sous **Event Type Include**, sélectionnez **Non-Meraki VPN Healthcheck**

Event log

Client:

Before: (PDT)

Event type include:

Event type ignore:

[Reset filters](#)



Client:

Before: (PDT)

Event type include:

Event type ignore:

[Reset filters](#)

Lorsque le tunnel principal vers Cisco Secure Access est actif, les paquets arrivant par le tunnel secondaire sont abandonnés pour maintenir un chemin de routage cohérent.

Le tunnel secondaire reste en veille et n'est utilisé qu'en cas de panne sur le tunnel principal, soit du côté Meraki, soit dans Secure Access, comme déterminé par le mécanisme de contrôle d'intégrité.

Event log

Client: **Before:** (PDT)

Event type include: **Event type ignore:**

[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

- Le contrôle d'intégrité du tunnel principal indique l'état : up, ce qui signifie qu'il est actuellement en train de transmettre et de transférer activement le trafic.
- Le contrôle d'intégrité du tunnel secondaire indique l'état : inactif, non pas parce que le tunnel n'est pas disponible, mais parce que le primaire est sain et en cours d'utilisation. Ce comportement est attendu, car le trafic n'est autorisé qu'à traverser le tunnel 1, ce qui entraîne l'échec du contrôle d'intégrité du tunnel secondaire.

Informations connexes

- [Assistance technique de Cisco et téléchargements](#)
- [Centre d'aide Cisco Secure Access](#)
- [Guide de configuration de Cisco Secure Access Meraki BGP](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.