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

Table des matières

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 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

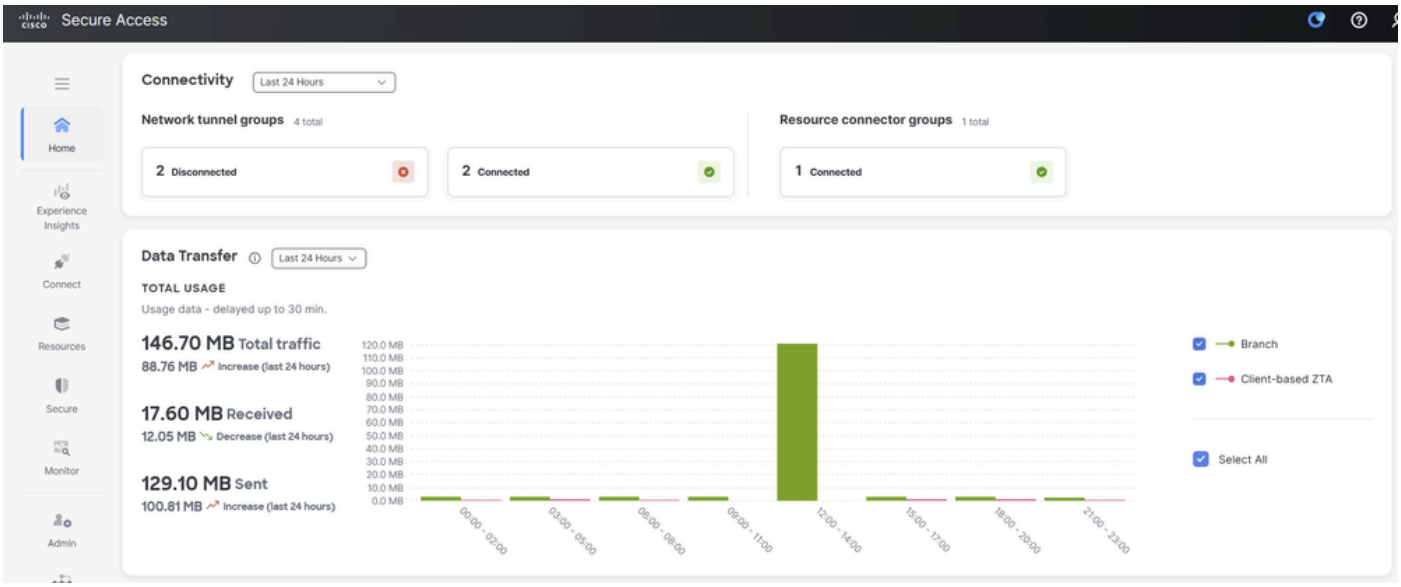
Internet avec l'application de politiques dans le cloud.

- 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.

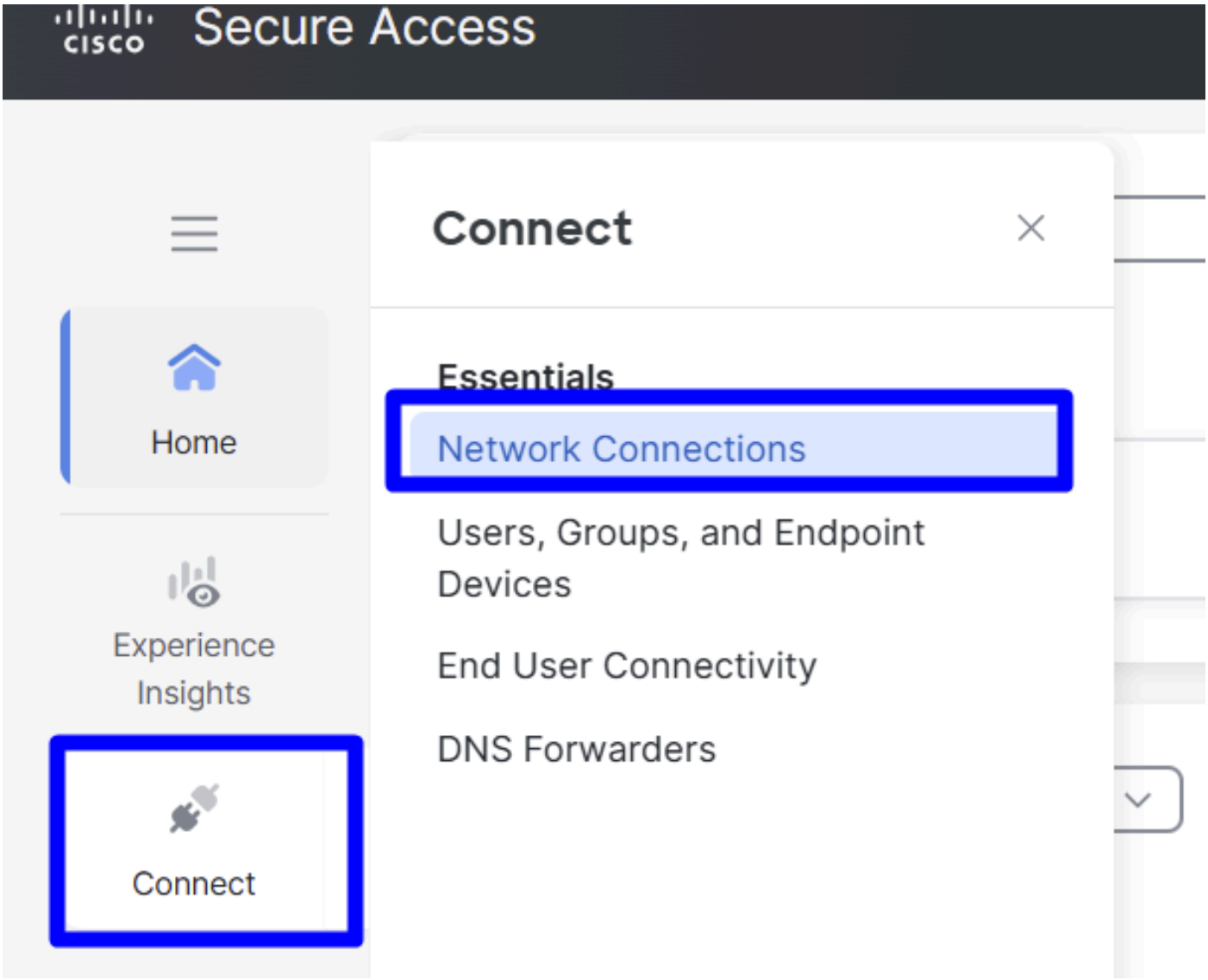
Configurer

Configurer le VPN sur un accès sécurisé

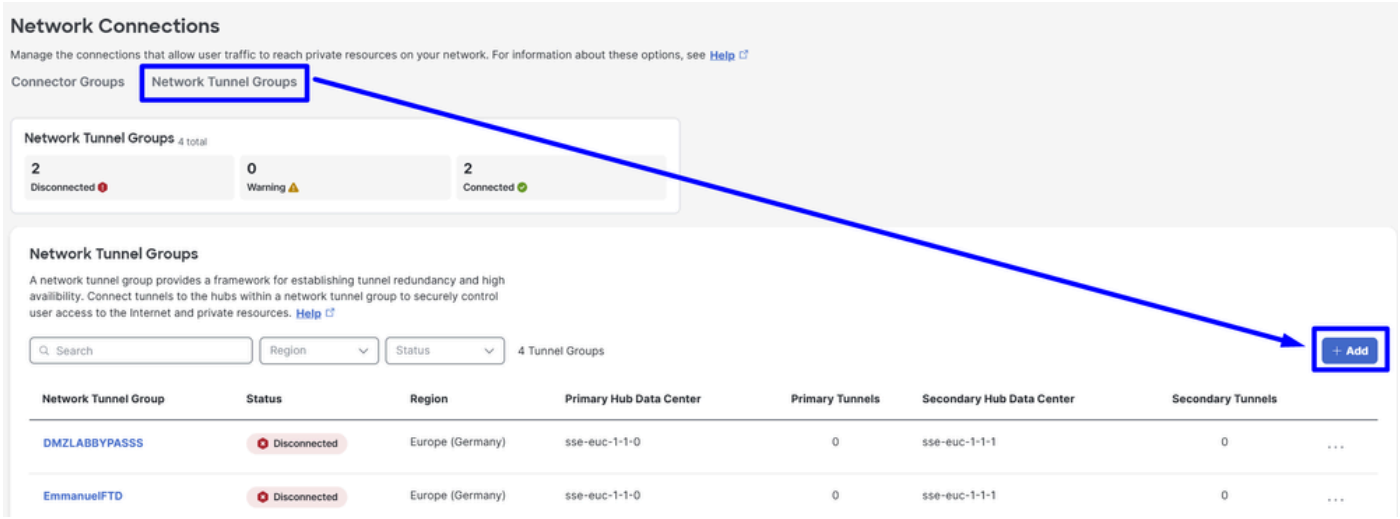
Accédez au panneau d'administration de Secure Access.



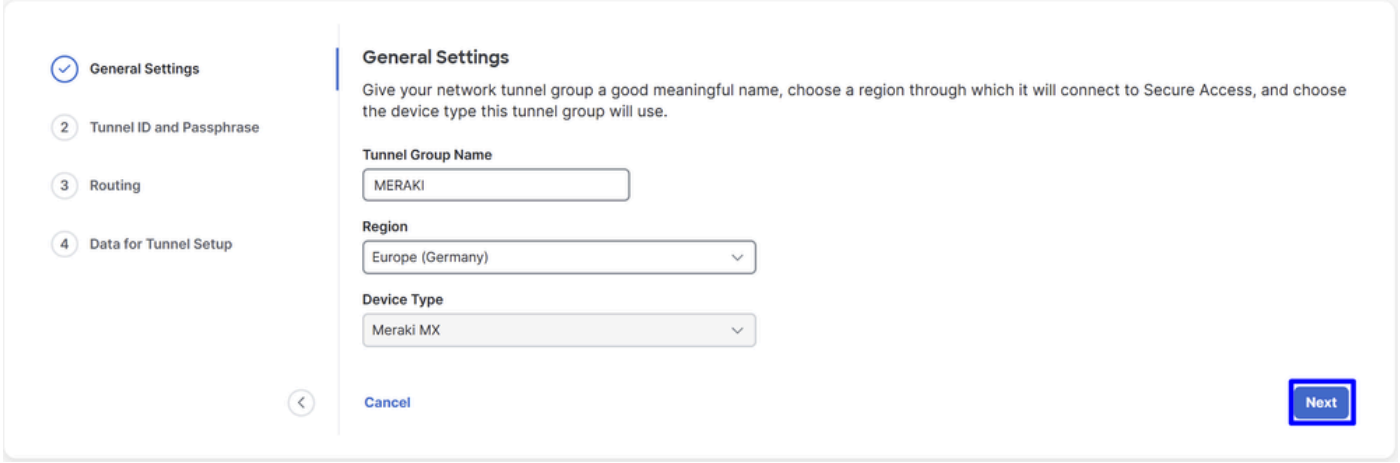
- Cliquez sur Connect > Network Connections



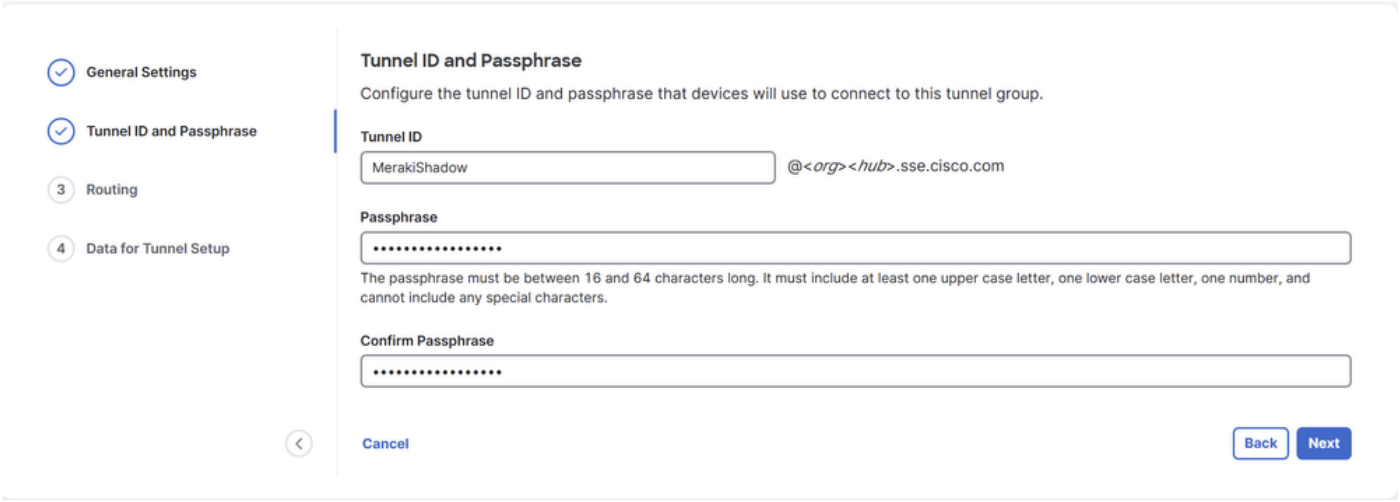
- SousNetwork Tunnel Groupscliquez sur + Add



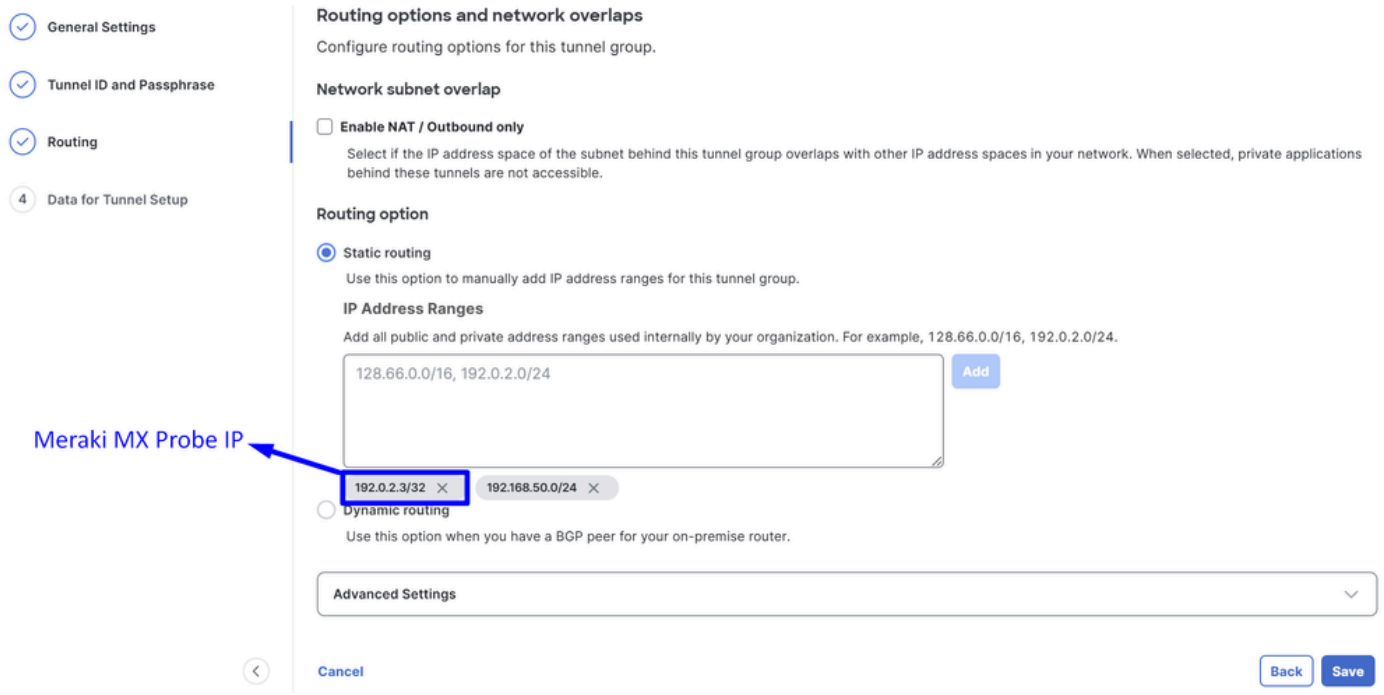
- ConfigurerTunnel Group Name, Regionet Device Type
- Cliquer **Next**

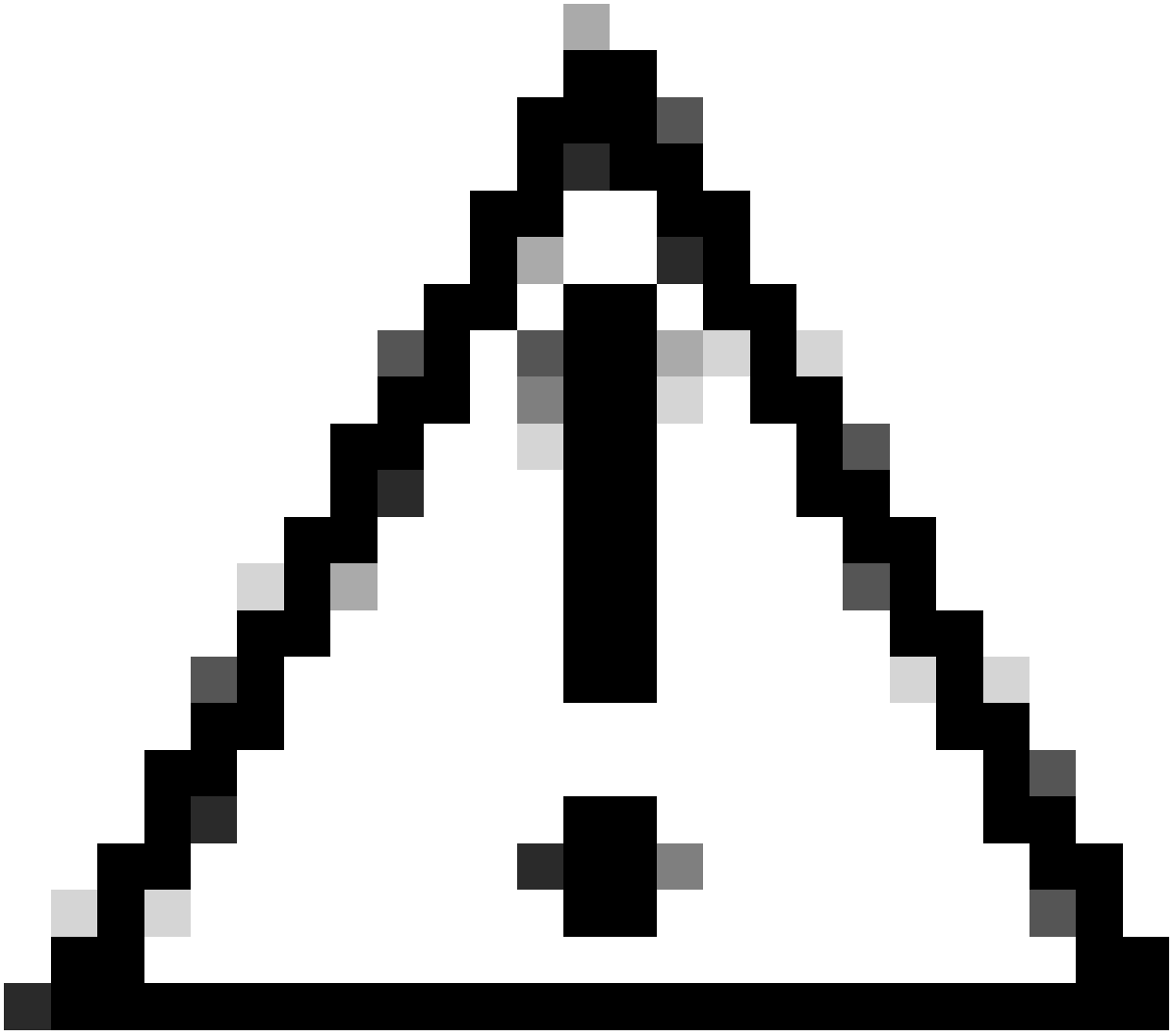


- Configurez lesTunnel ID Formatet Passphrase
- CliquerNext



- 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.
- CliquerSave


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

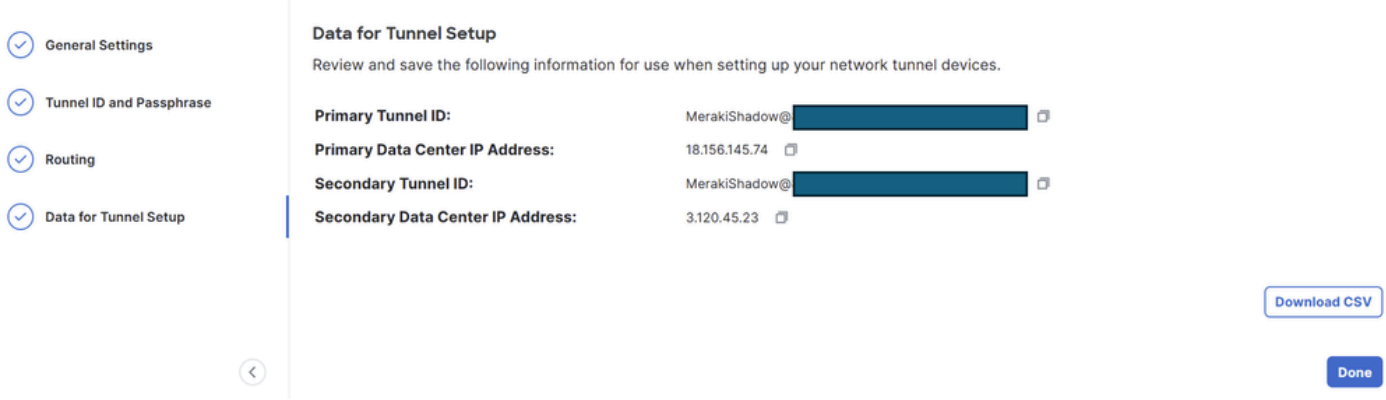


Mise en garde : Veillez à ajouter la sonde de surveillance IP (192.0.2.3/32) ; sinon, vous pouvez rencontrer des problèmes de trafic sur le périphérique Meraki qui achemine le trafic vers Internet, les pools VPN et la plage CGNAT 100.64.0.0/10 utilisée par ZTNA.

- 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.**

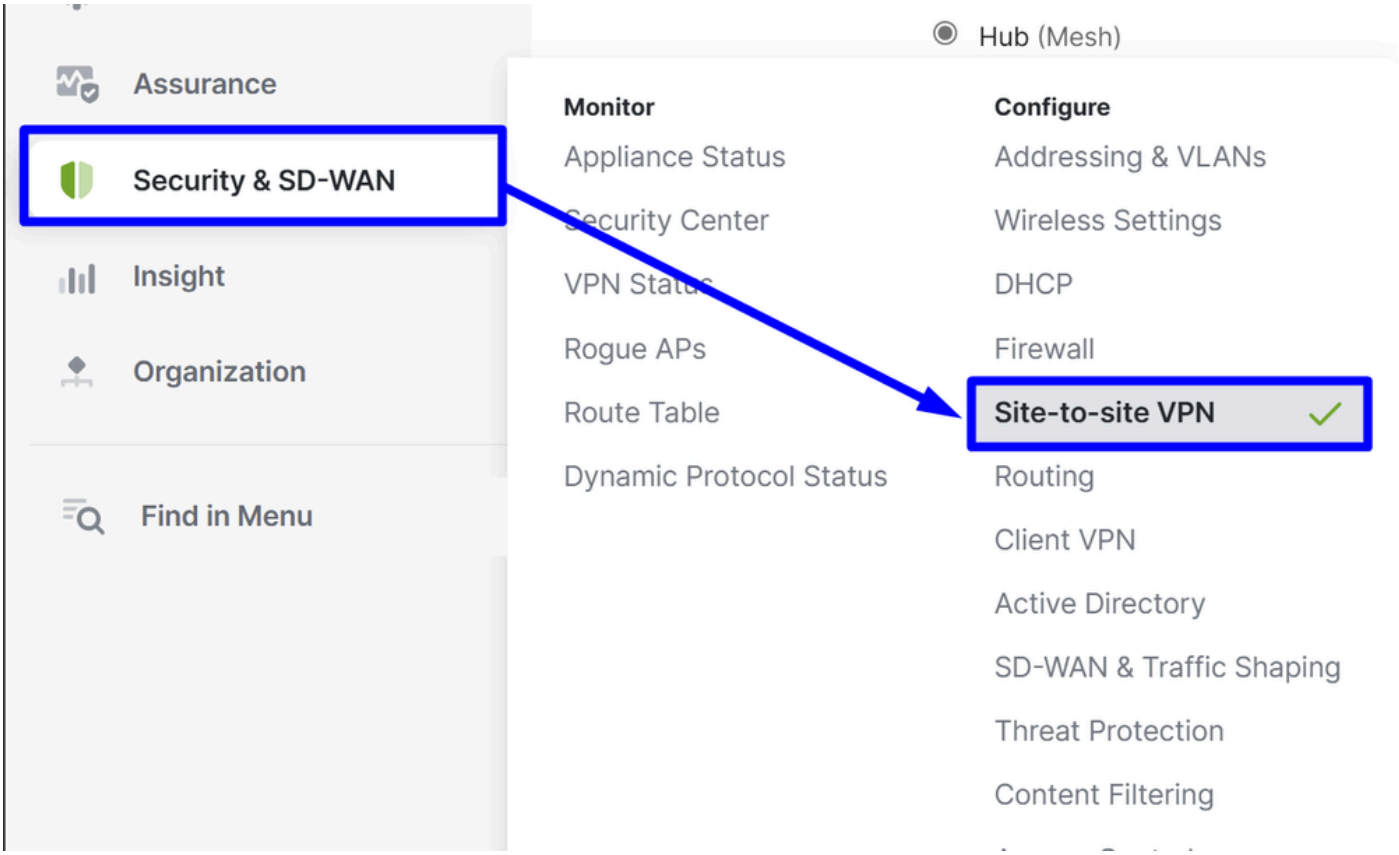
Configuration VPN d'accès sécurisé

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



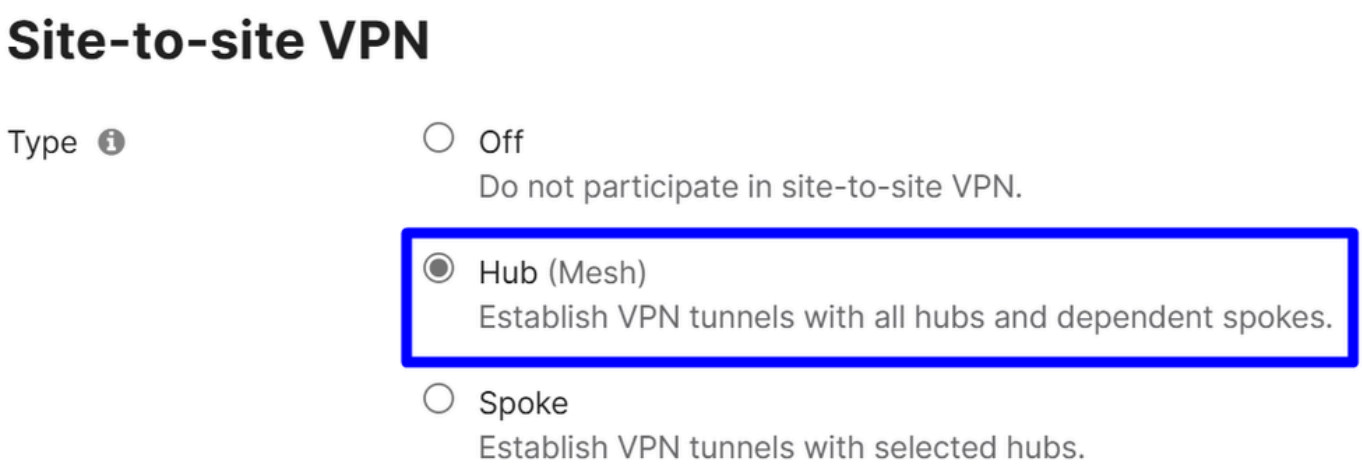
Configuration du VPN sur Meraki MX

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



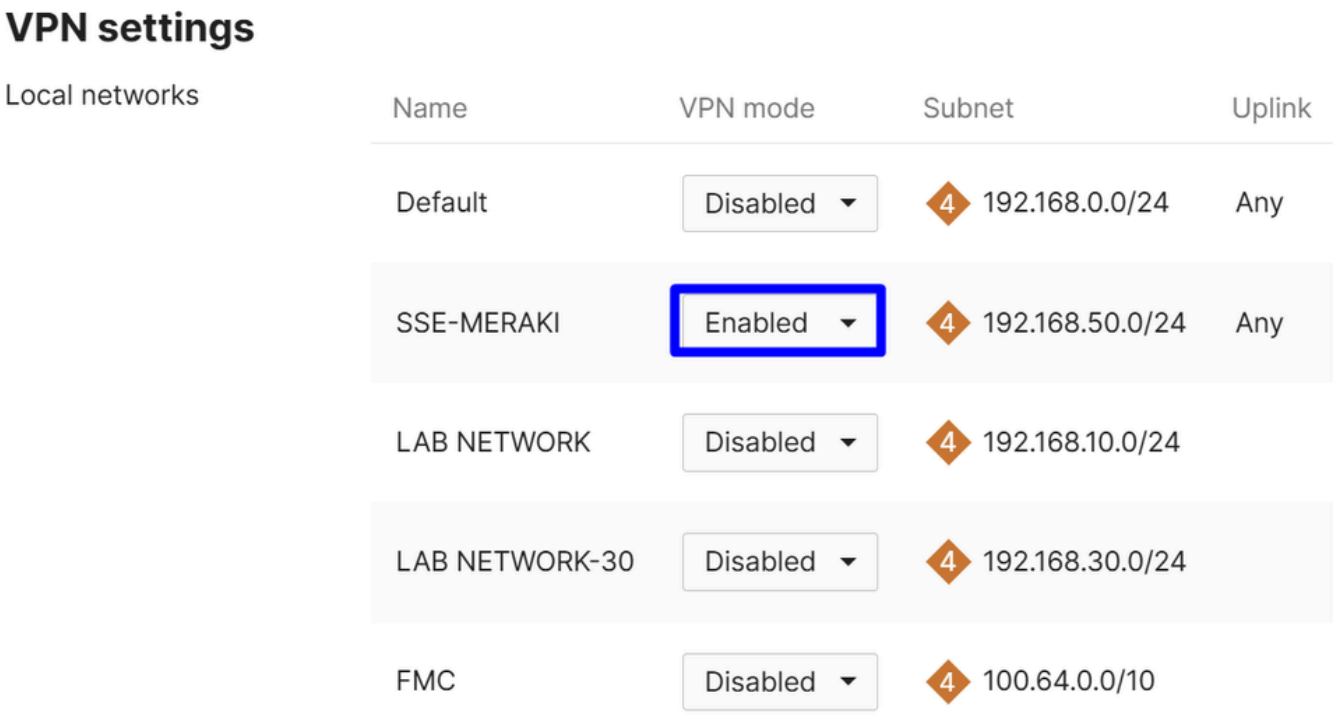
VPN de site à site

Choisir Hub.

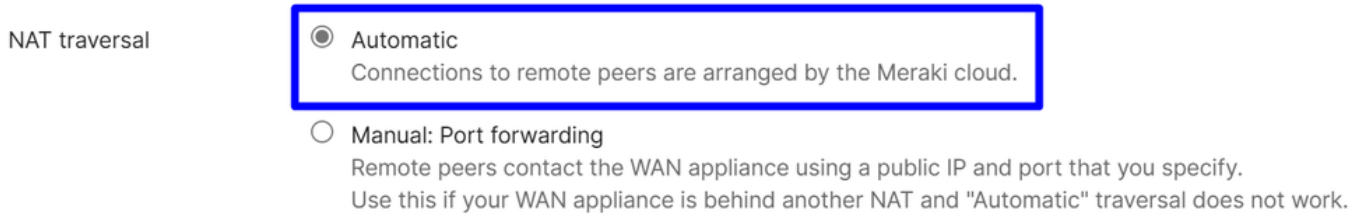


Paramètres VPN

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



Choisir dansNAT TraversalAutomatique



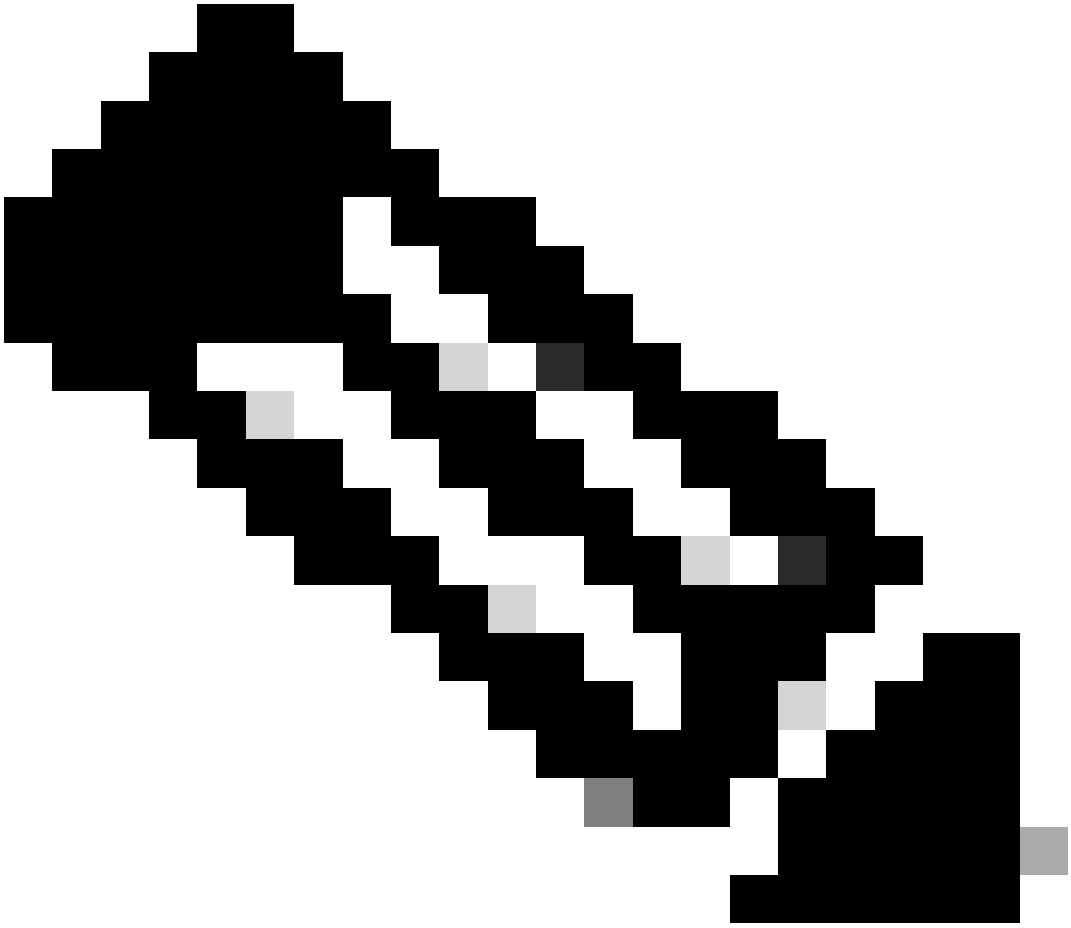
Homologues VPN non Meraki

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

Cliquez sur **Configure Health Checks**

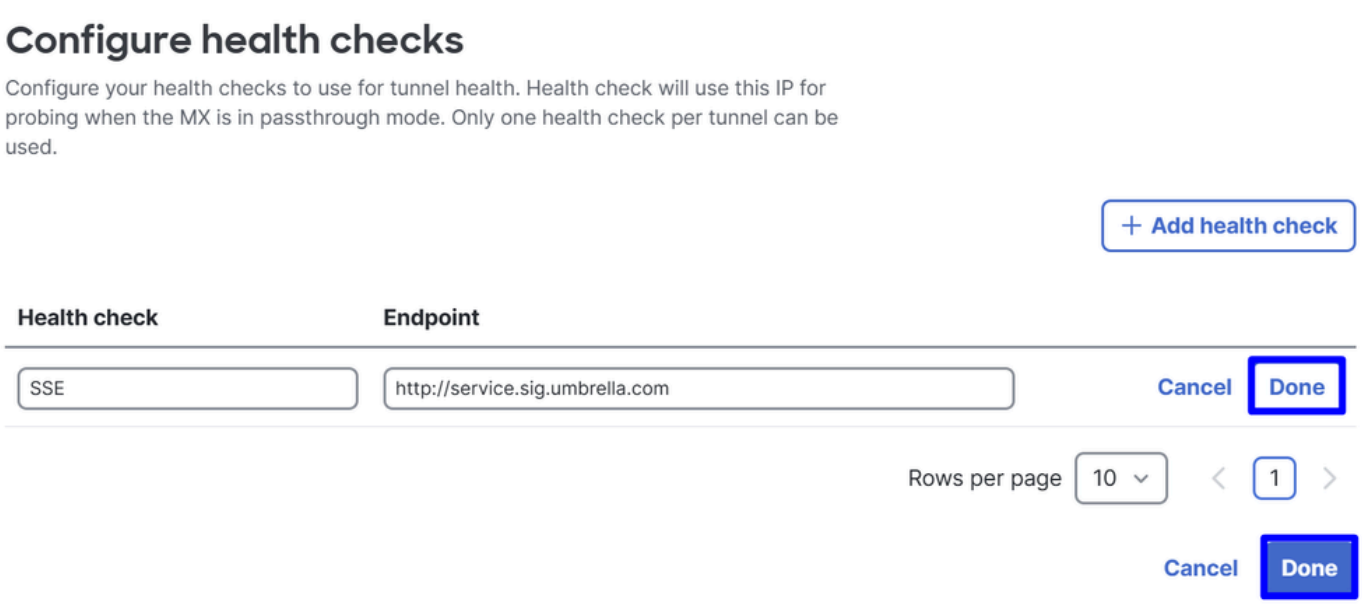
- Cliquez sur **+Add health Check**

- **Health Check**: 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.

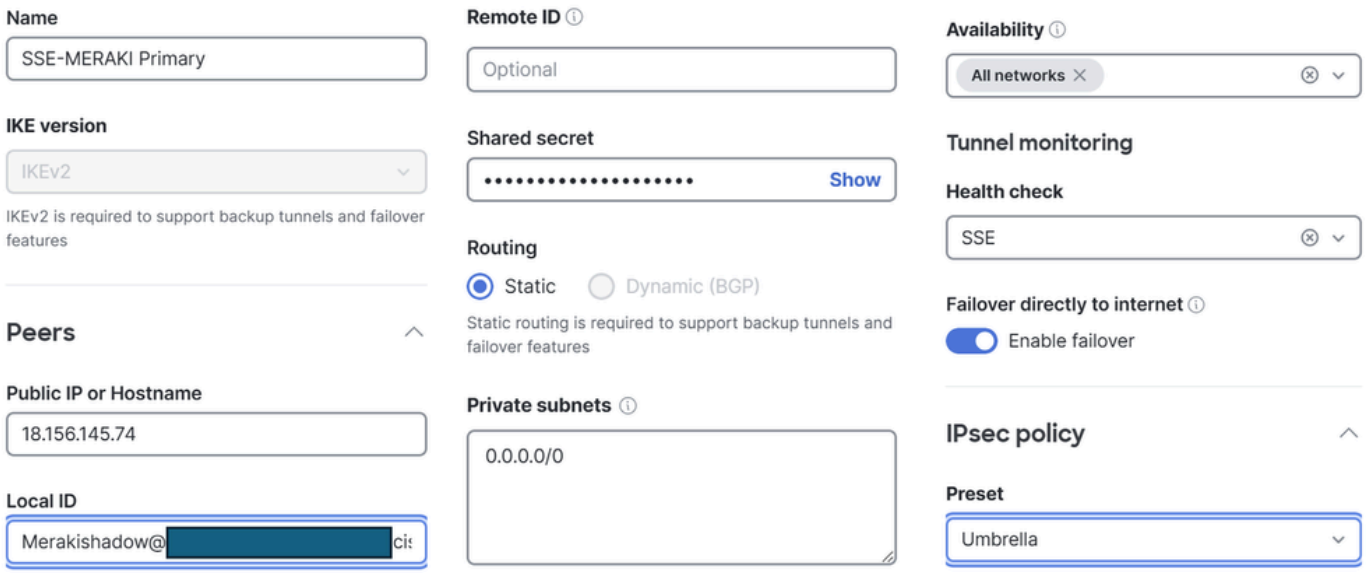
Cliquez ensuite **Done** deux fois pour finaliser.



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

Configuration du tunnel principal

- Cliquez sur+Add a peer

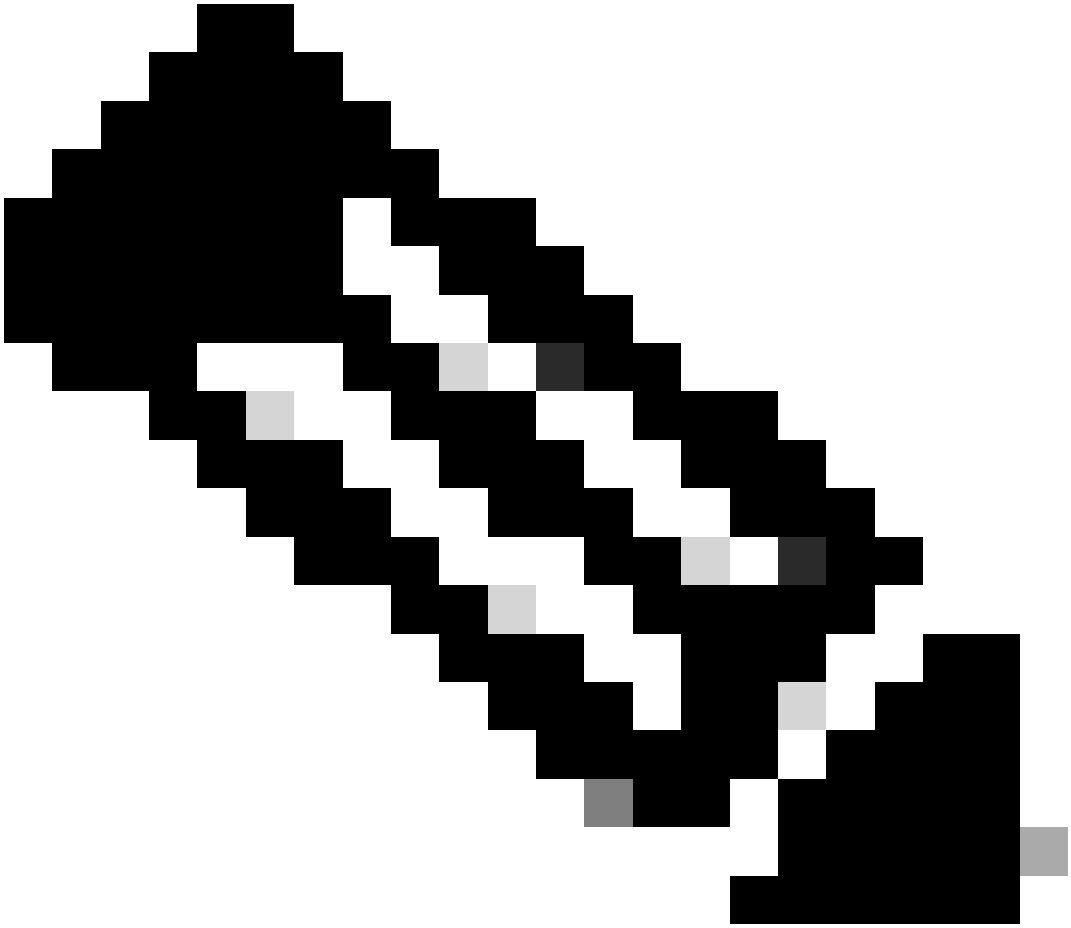


- Ajouter un homologue VPN
  - Name : Configurez un nom pour le VPN pour un accès sécurisé
  - Version IKE : Choisir IKEv2
- Pairs
  - Adresse IP publique ou nom d'hôte : Configurez les données **Primary Datacenter IP** fournies par Secure Access dans l'étape Configurations VPN d'accès sécurisé
  - ID 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'Failover directly to Internet'interface WAN est activée.

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

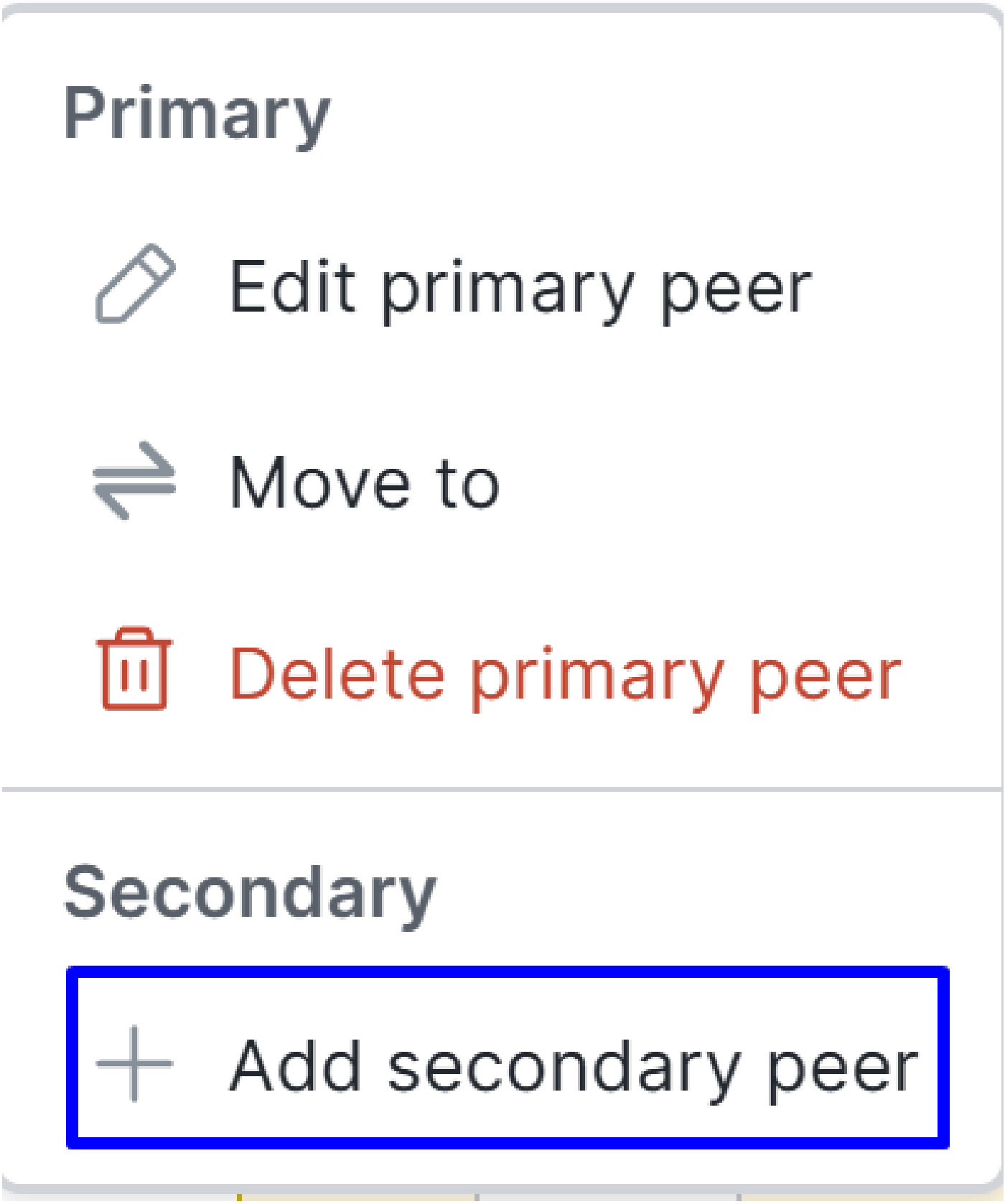
Cliquez ensuite sur **Save**.

Configuration du tunnel secondaire

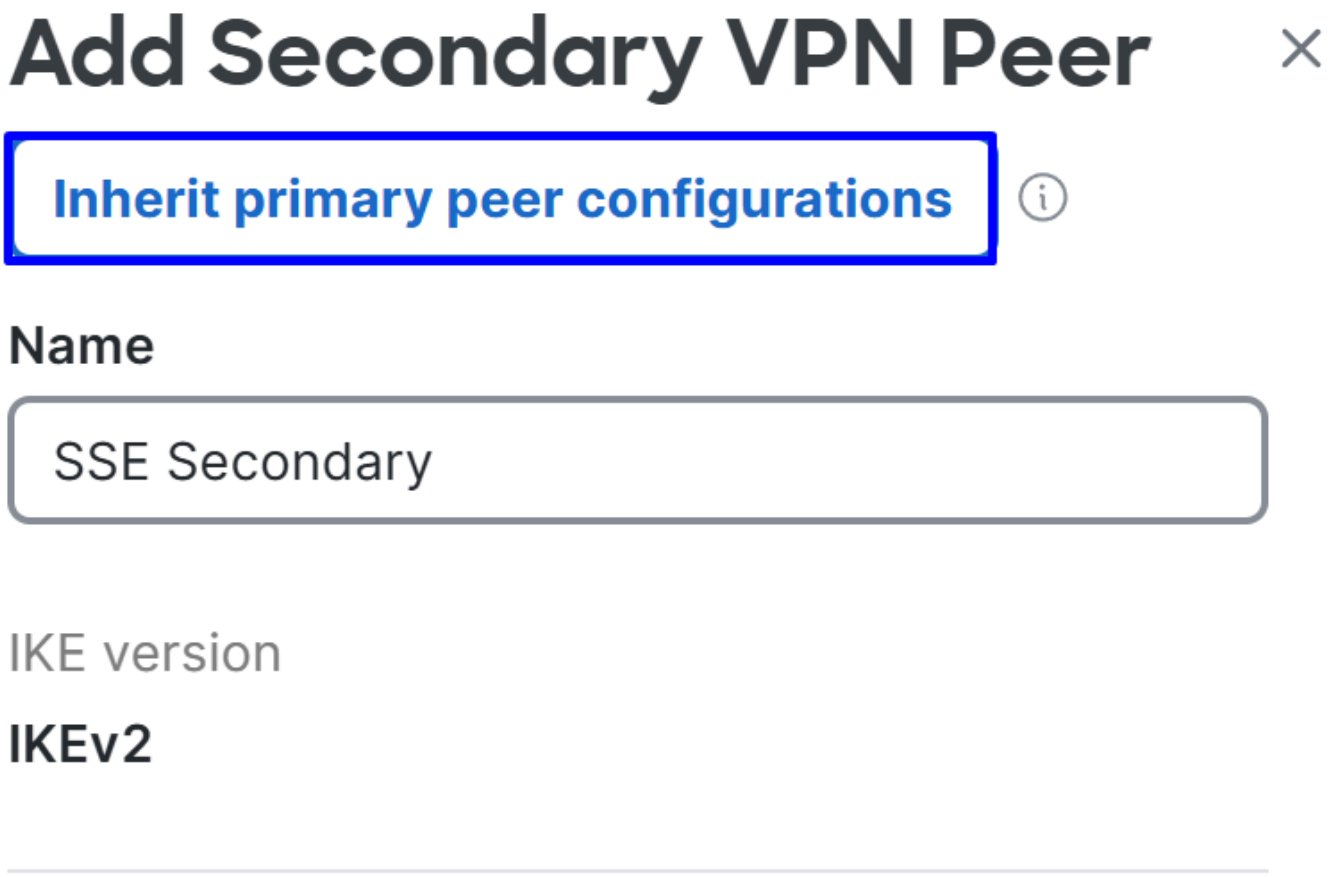
Pour configurer le tunnel secondaire, cliquez sur le menu d'options du tunnel principal :

- Cliquez sur les trois points

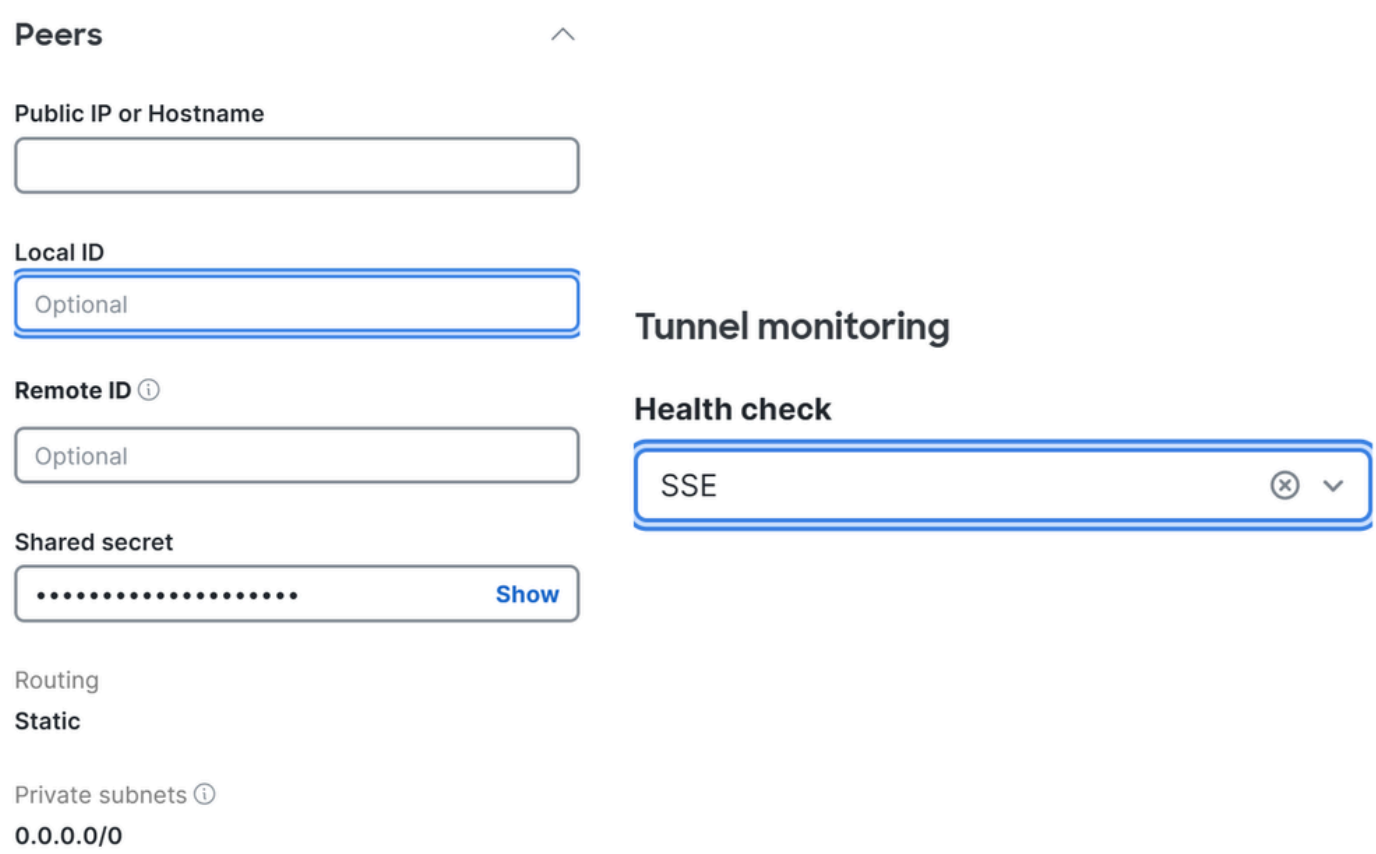
- Cliquez sur + Add Secondary peer



- Cliquez surInherit primary peer configurations

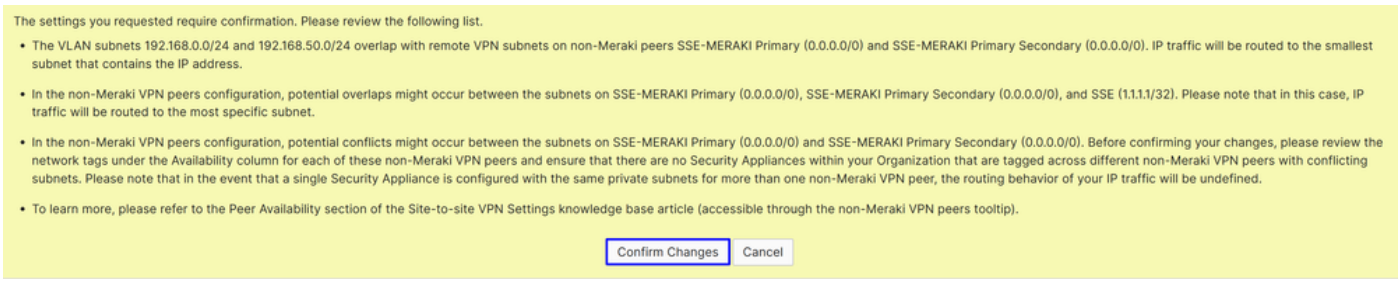


Vous remarquerez ensuite que certains champs sont remplis automatiquement. Vérifiez-les, apportez les modifications nécessaires et complétez le reste manuellement :



- 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 :

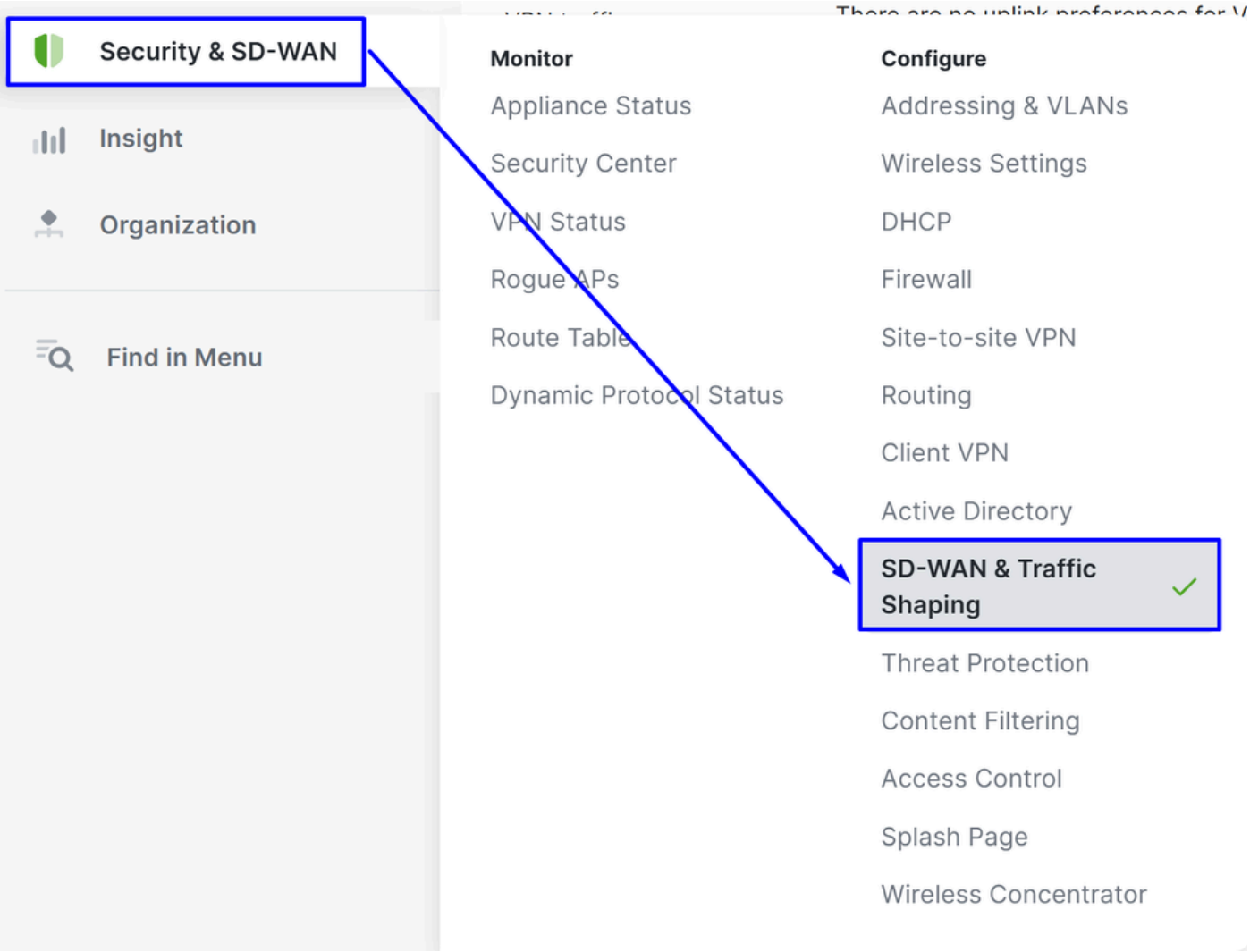


Ne vous inquiétez pas et cliquez **Confirm Changes**.

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 :

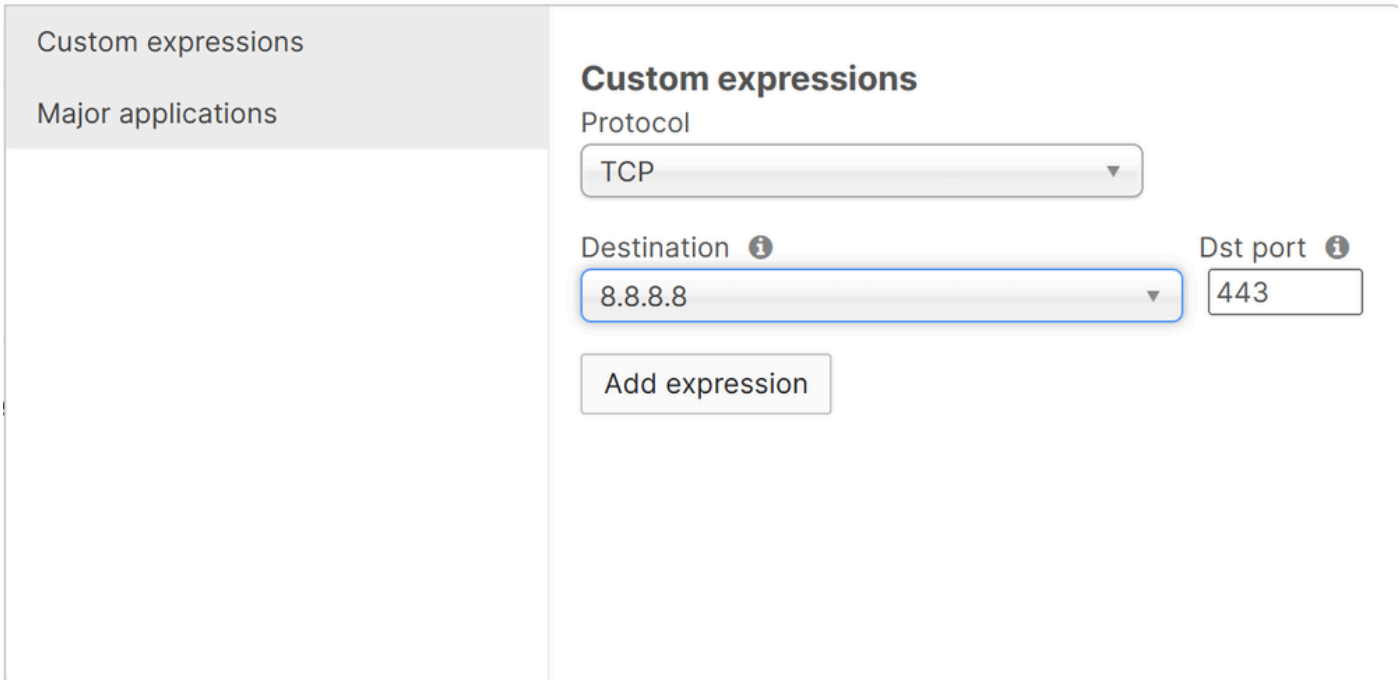
- Accédez à **Security & SD-WAN** > SD-WAN & Traffic Shaping



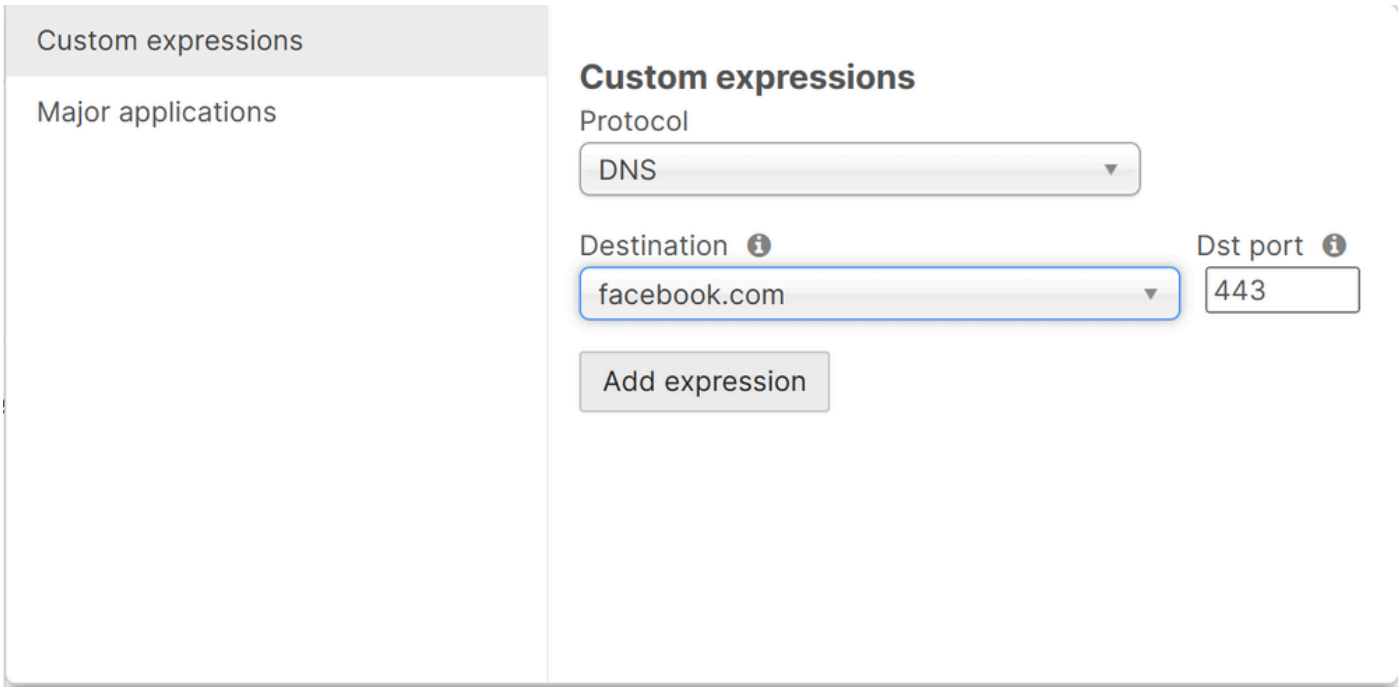
- Faites défiler jusqu'à la **Local Internet Breakout** section et cliquez sur **Add+**

Créez ensuite le contournement en fonction de **Custom Expressions** ou de **Major Applications**:

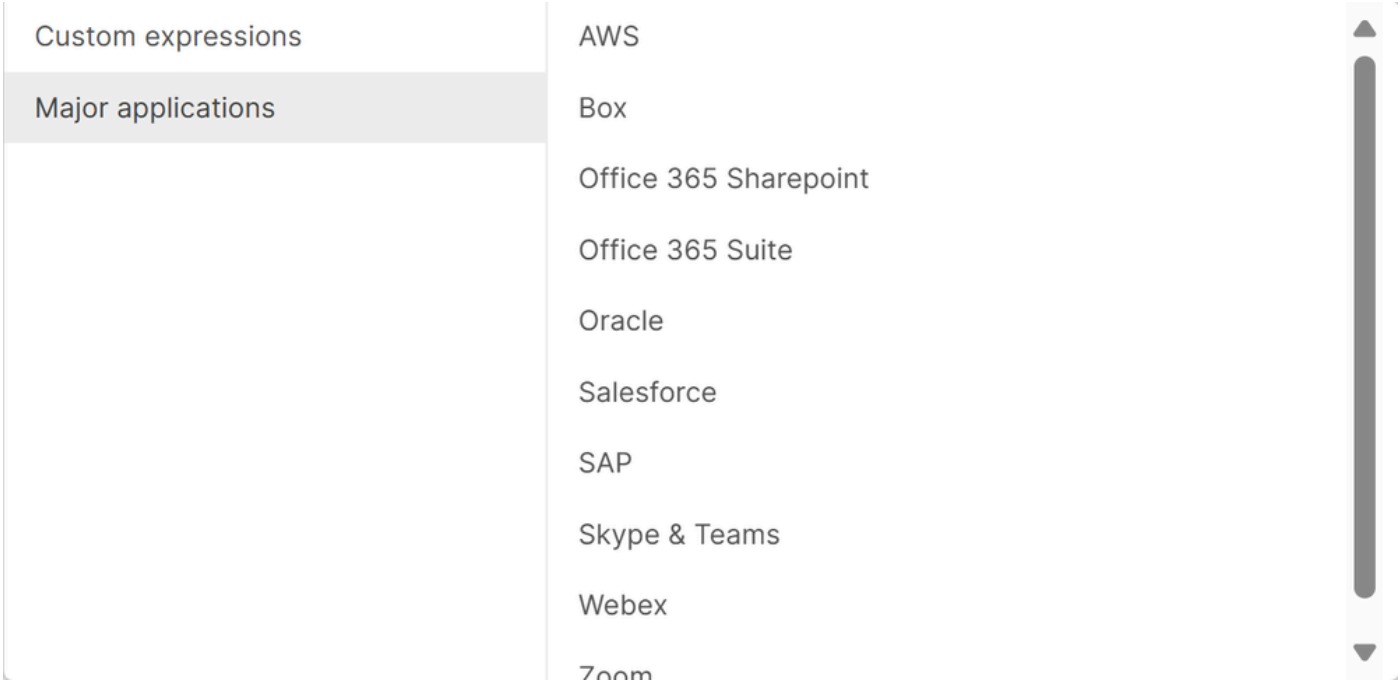
Custom Expressions - Protocol



Custom Expressions - DNS



Major Applications

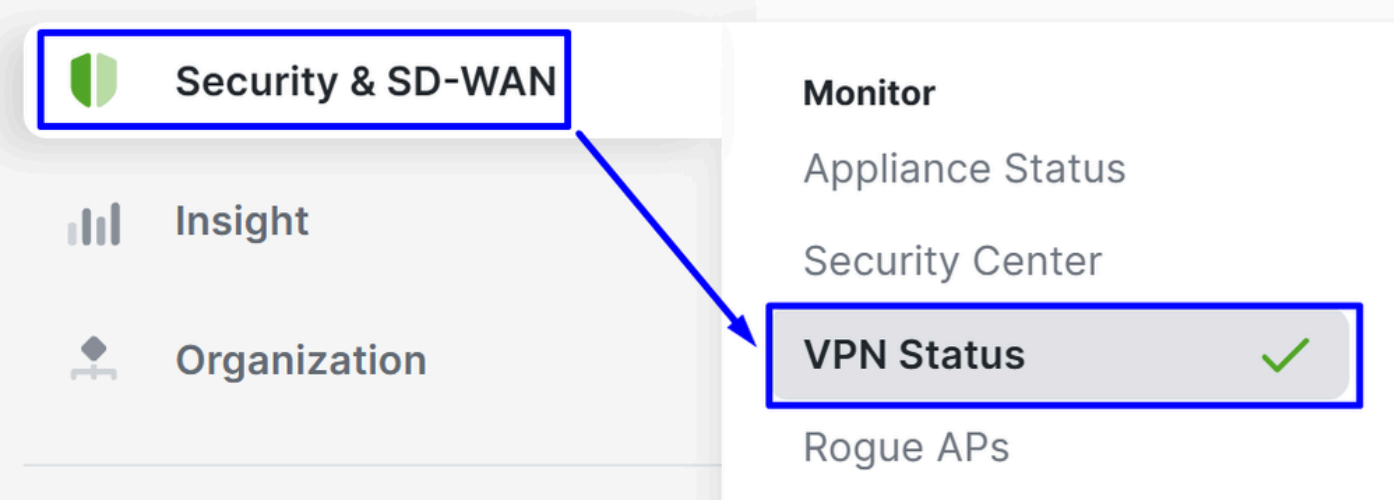


Pour plus d'informations, consultez : [Configuration des règles d'exclusion VPN (IP/Port/DNS/APP)]

Vérifier

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

- Cliquez surSecurity & 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

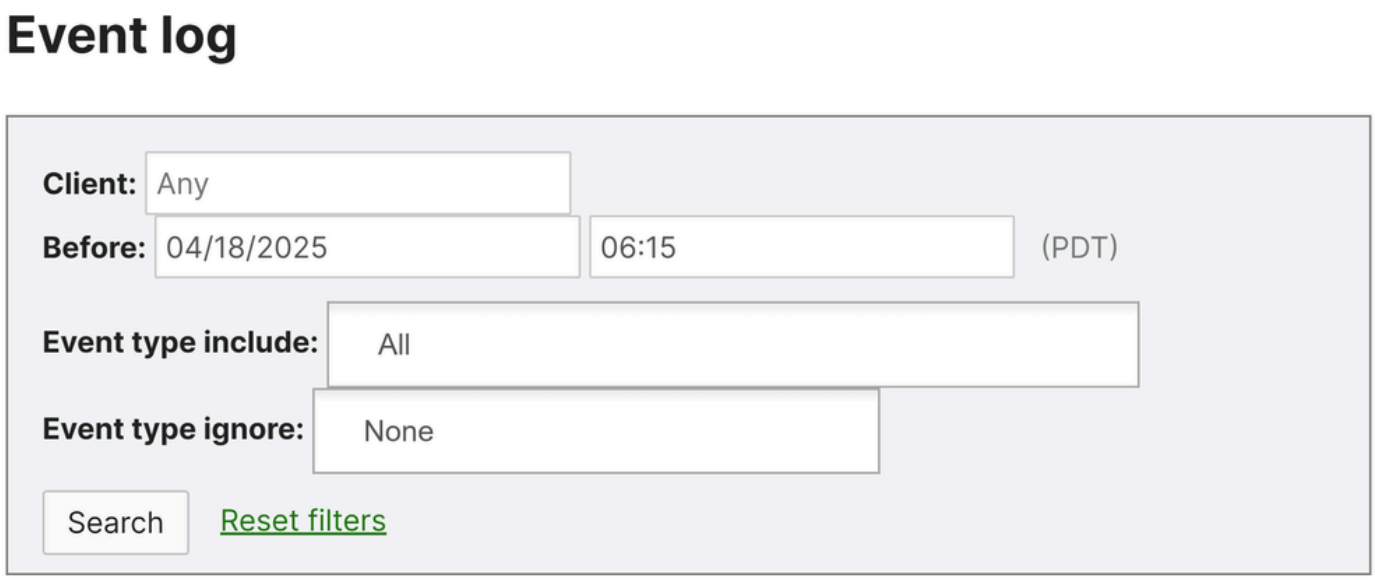
Status Indicator	Color	Meaning
Primary/Secondary Up	Green	Phase 1 and phase 2 are up
Partial Connectivity	Amber	Phase 1 is up but phase 2 is down
Tunnel Down	Red	Phase 1 and phase 2 are both down

Dépannage

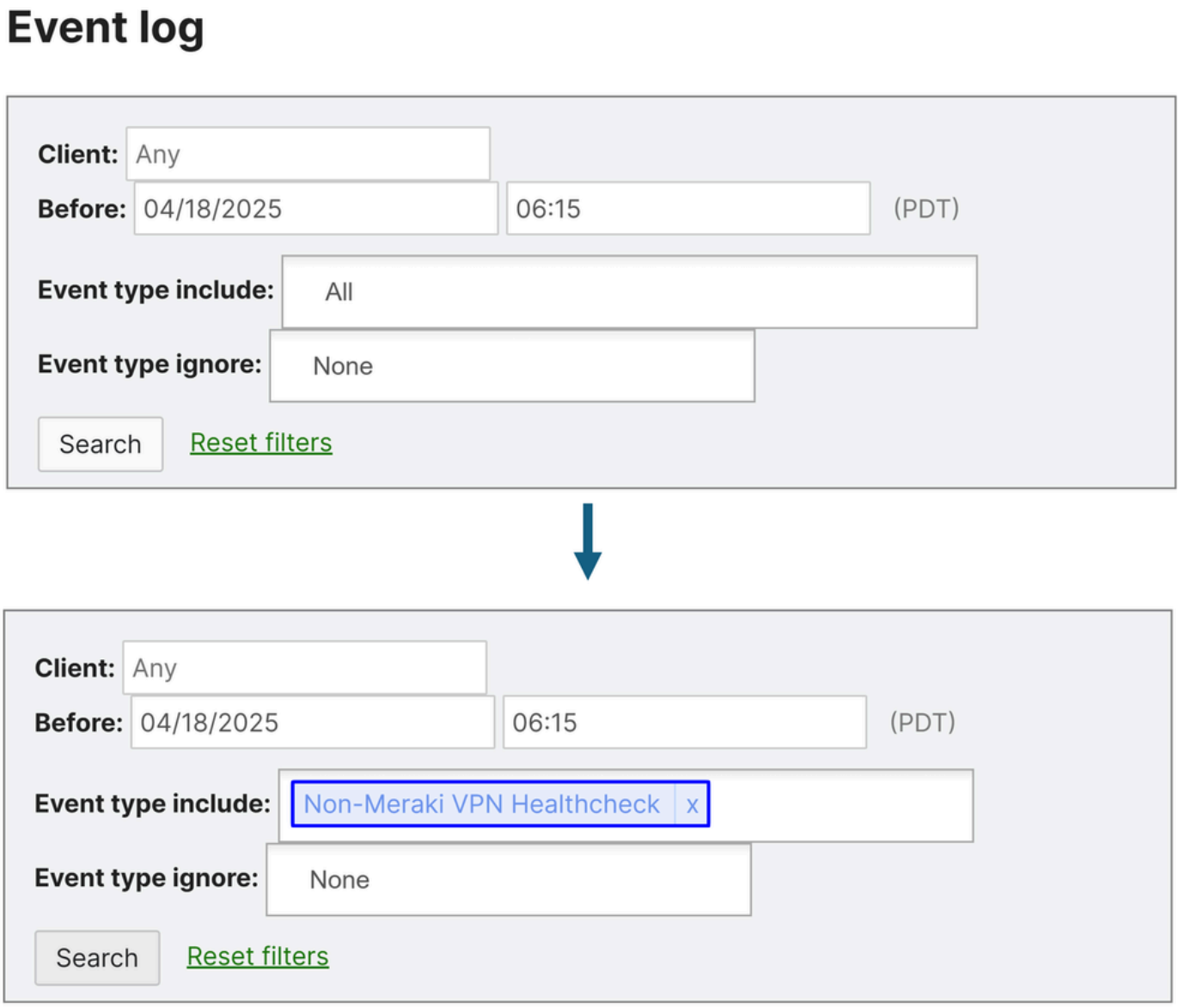
Vérifier les bilans de santé

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

- Cliquez sur **Assurance** > Event Log

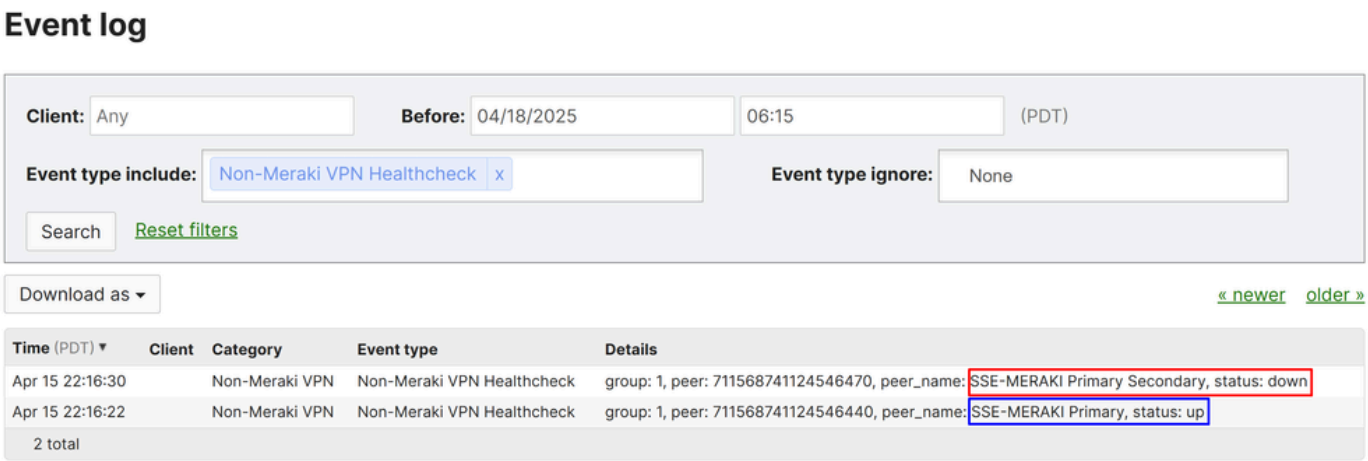


Sous **Event Type Include**, sélectionnez Non-Meraki VPN Healthcheck



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.



- 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.