Configuración de acceso seguro con Meraki MX para lograr una alta disponibilidad y supervisión del estado

Contenido

Introducción

Este documento describe cómo configurar Cisco Secure Access con Meraki MX para alta disponibilidad mediante comprobaciones de estado.

Prerequisites

- Revisar los requisitos del túnel IPsec con Secure Access
- Comprensión de los componentes de Secure Access
- Comprender la funcionalidad de comprobación de estado en Meraki MX

Requirements

- Meraki MX debe ejecutar la versión de firmware 19.1.6 o posterior
- Al utilizar el acceso privado, solo se admite un túnel debido a una limitación de Meraki que

impide cambiar la IP de comprobación de estado, lo que hace que sea necesaria la NAT para túneles SPA (acceso privado seguro) adicionales. Esto no se aplica cuando se utiliza SIA (acceso seguro a Internet).
- Defina claramente qué subredes o recursos internos se rutean a través del túnel hacia el acceso seguro.

Componentes Utilizados

- Acceso seguro de Cisco
- Appliance de seguridad Meraki MX (versión de firmware 19.1.6 o posterior)
- Tablero Meraki
- Panel de acceso seguro

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cisco Secure Access es una plataforma de seguridad nativa de la nube que permite el acceso seguro tanto a aplicaciones privadas (a través de acceso privado) como a destinos de Internet (a través de acceso a Internet). Al integrarse con Meraki MX, permite a las organizaciones establecer túneles IPsec seguros entre las sucursales y la nube, lo que garantiza el flujo de tráfico cifrado y la aplicación de seguridad centralizada.

Esta integración utiliza túneles IPSec de ruteo estático. Meraki MX establece túneles IPsec primarios y secundarios para Cisco Secure Access, y aprovecha las comprobaciones de estado de enlaces ascendentes integradas para realizar una conmutación por fallo automática entre túneles. Esto proporciona una configuración resistente y de alta disponibilidad para la conectividad de sucursales.

Entre los elementos clave de esta implementación se incluyen:

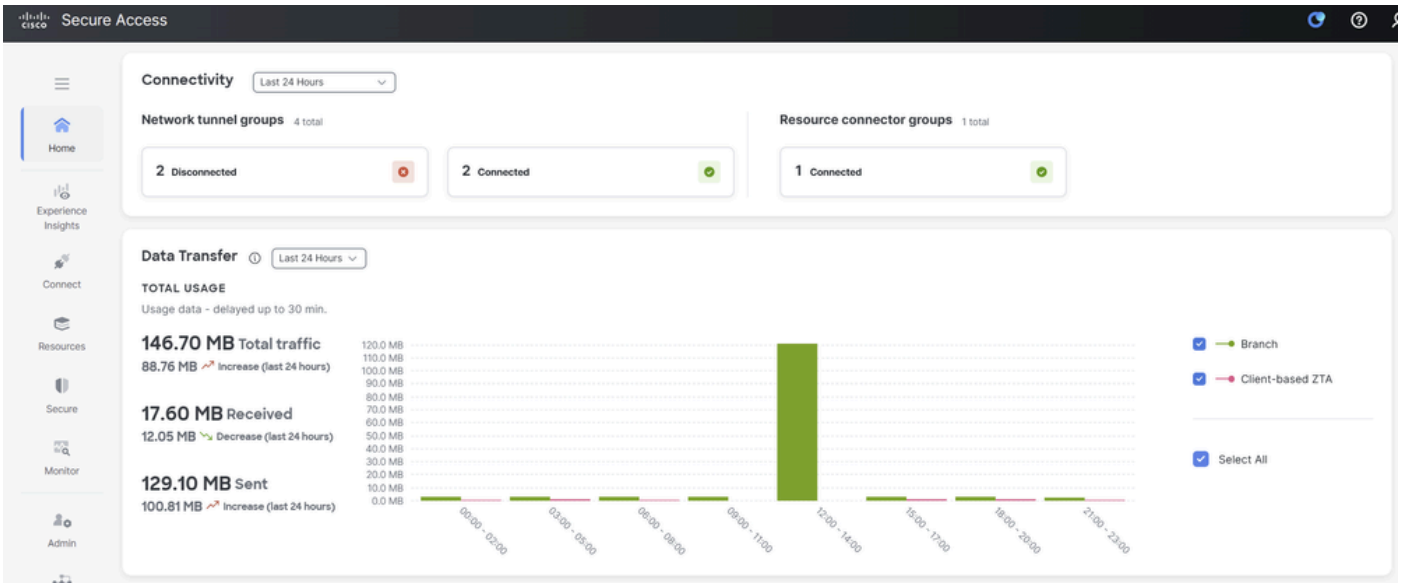
- Meraki MX actúa como una VPN que no es de Meraki asociada a Cisco Secure Access.
- Túneles primario y secundario configurados estáticamente, con comprobaciones de estado que determinan la disponibilidad.
- El acceso privado admite el acceso seguro a las aplicaciones internas a través de SPA

(acceso privado seguro), mientras que el acceso a Internet permite que el tráfico llegue a los recursos basados en Internet con la aplicación de políticas en la nube.
- Debido a las limitaciones de Meraki en cuanto a la flexibilidad de IP de comprobación de estado, solo se admite un grupo de túnel en el modo de acceso privado. Si es necesario conectar varios dispositivos Meraki MX a Secure Access para acceso privado, debe utilizar BGP para el routing dinámico o configurar túneles estáticos, sabiendo que solo un grupo de túnel de red puede admitir comprobaciones de estado y alta disponibilidad. Los túneles adicionales funcionan sin supervisión de estado ni redundancia.

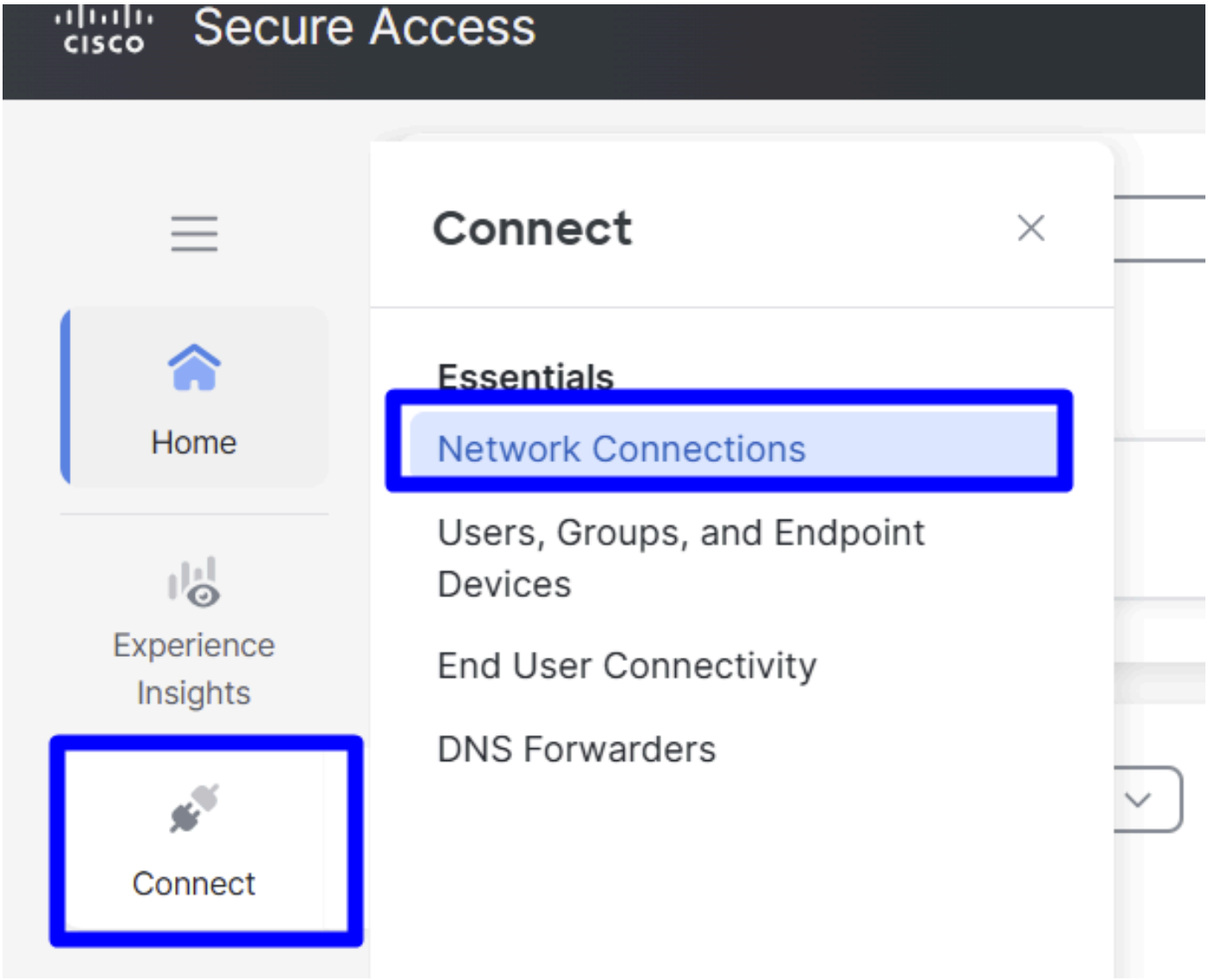
Configurar

Configuración de la VPN en Secure Access

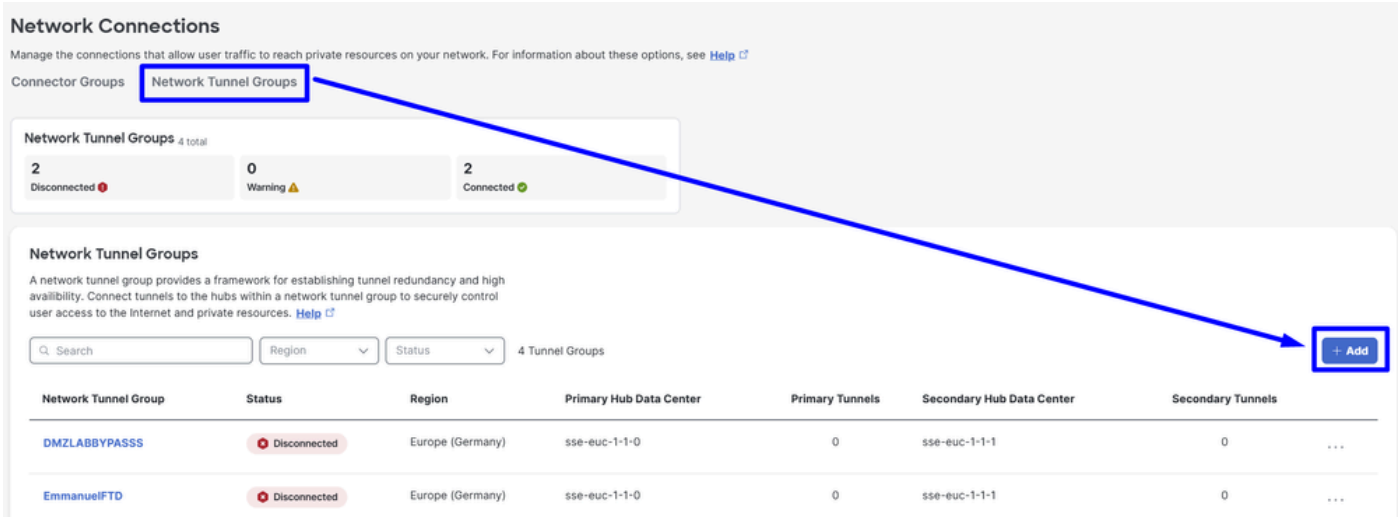
Vaya al panel de administración de Secure Access.



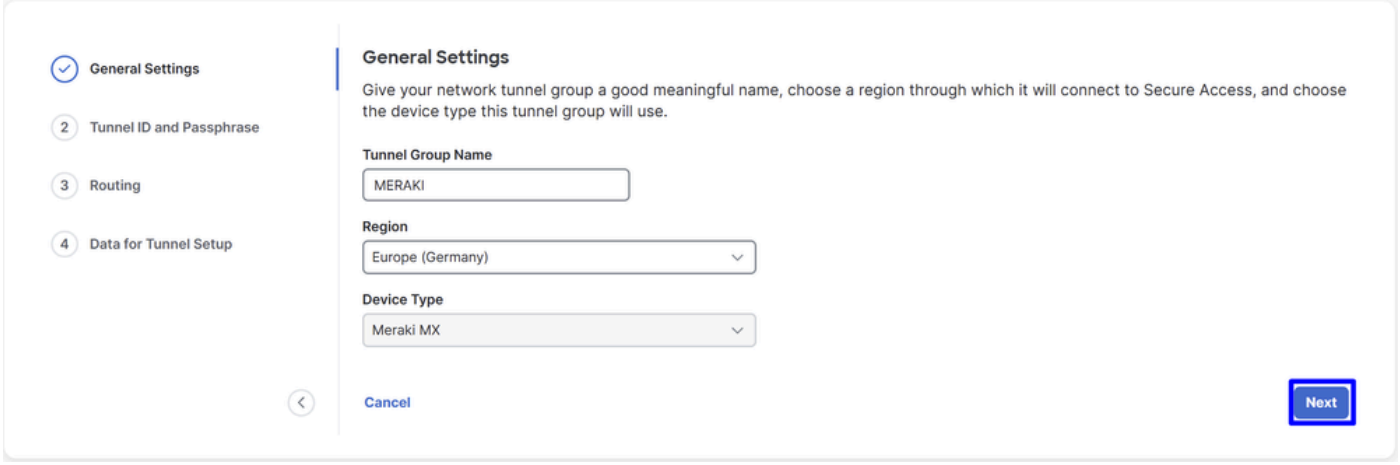
- Haga clic en Connect > Network Connections



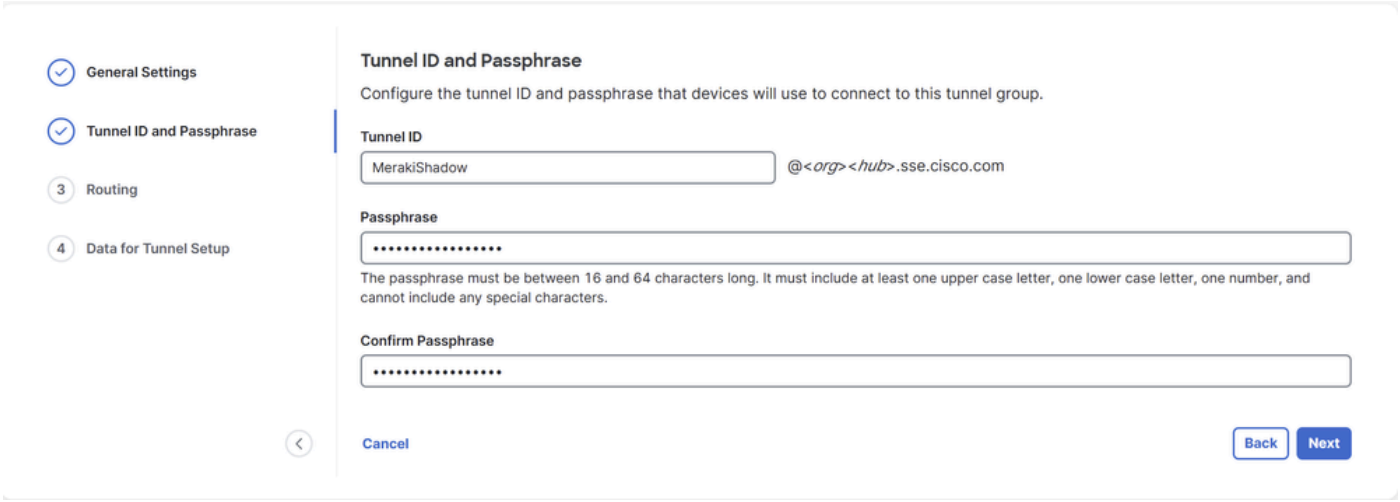
- En Network Tunnel Groups haga clic en + Add



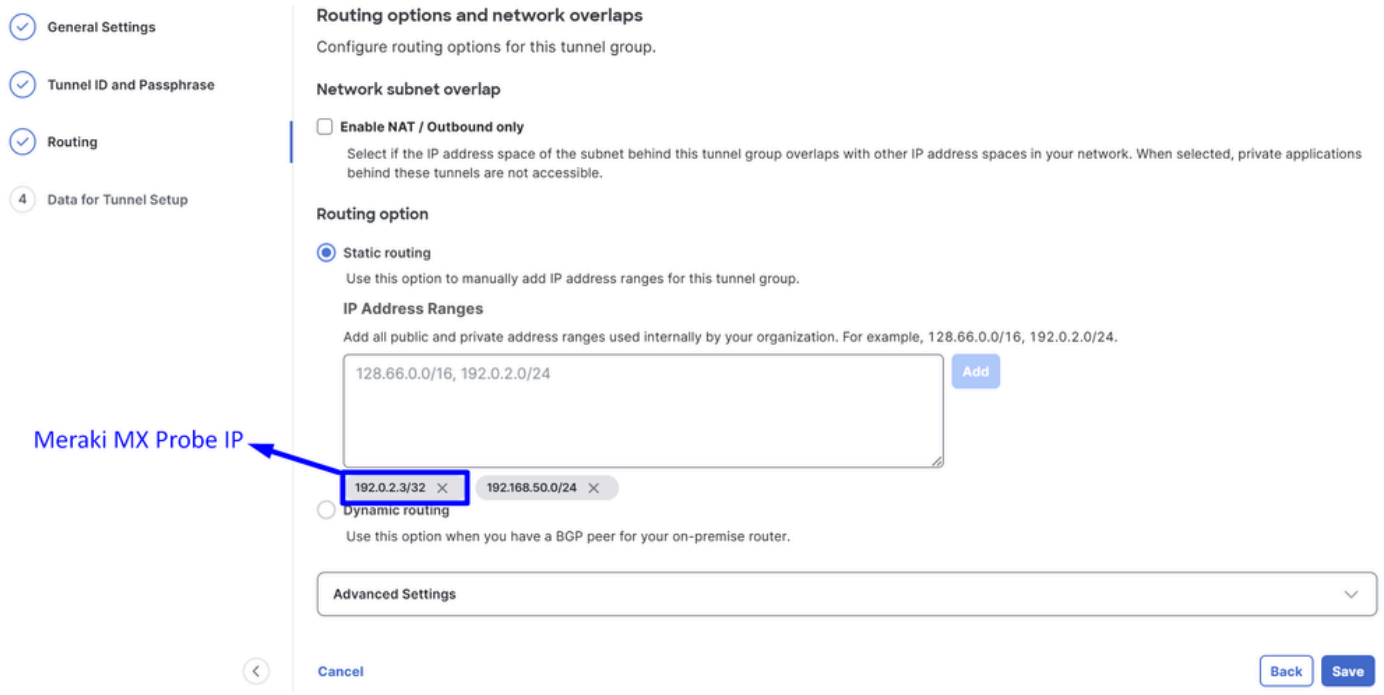
- Configurar Tunnel Group Name, Region y Device Type
- Haga clic en **Next**

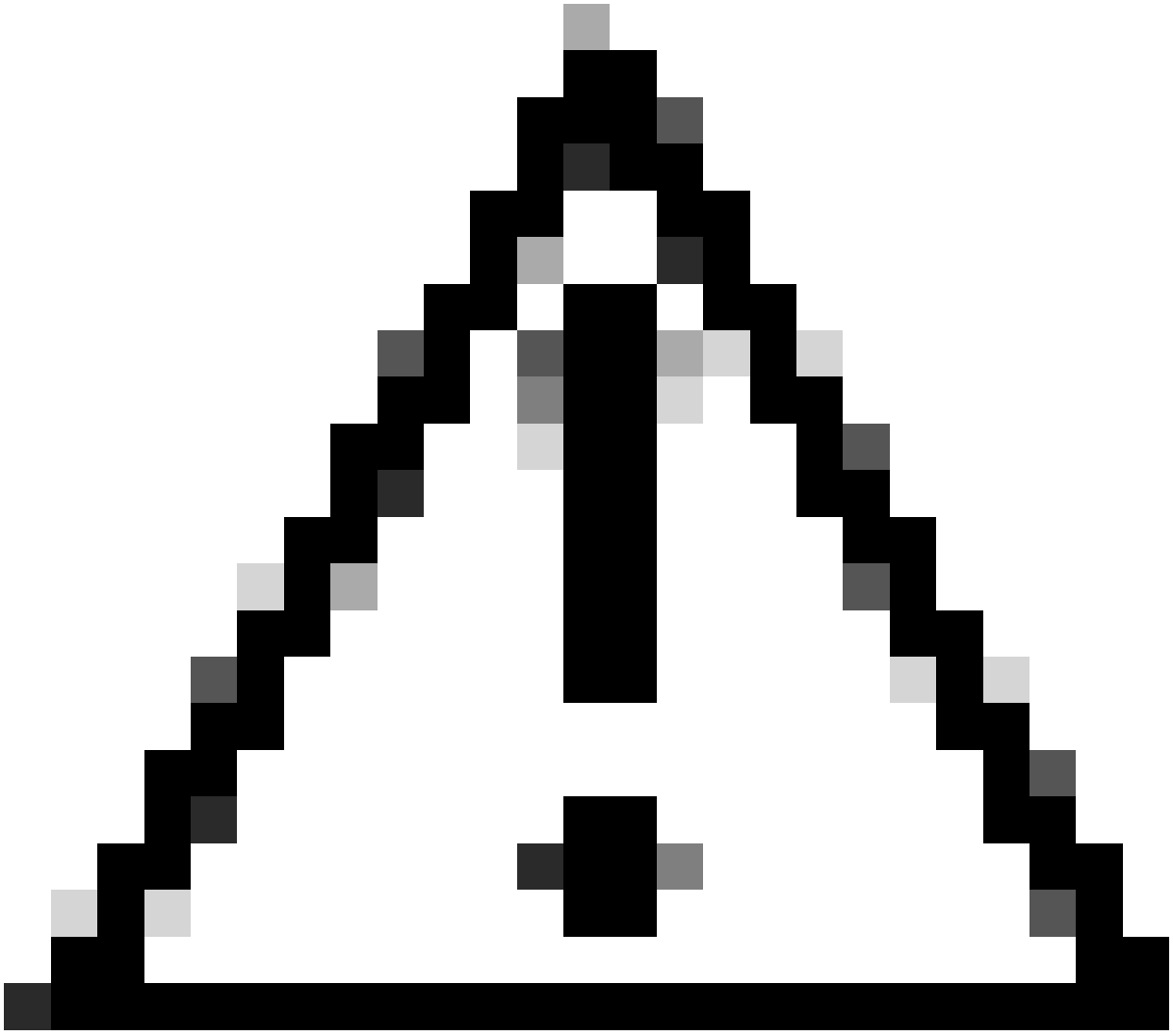


- Configure elTunnel ID Formaty Passphrase
- Haga clic enNext



- Configure los rangos de direcciones IP o los hosts que ha configurado en su red y que desea que el tráfico pase a través de Secure Access y Cisco, y asegúrese de incluir la IP de sondeo de supervisión de Meraki 192.0.2.3/32 para permitir el retorno del tráfico de Secure Access al Meraki MX.
- Haga clic enSave


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

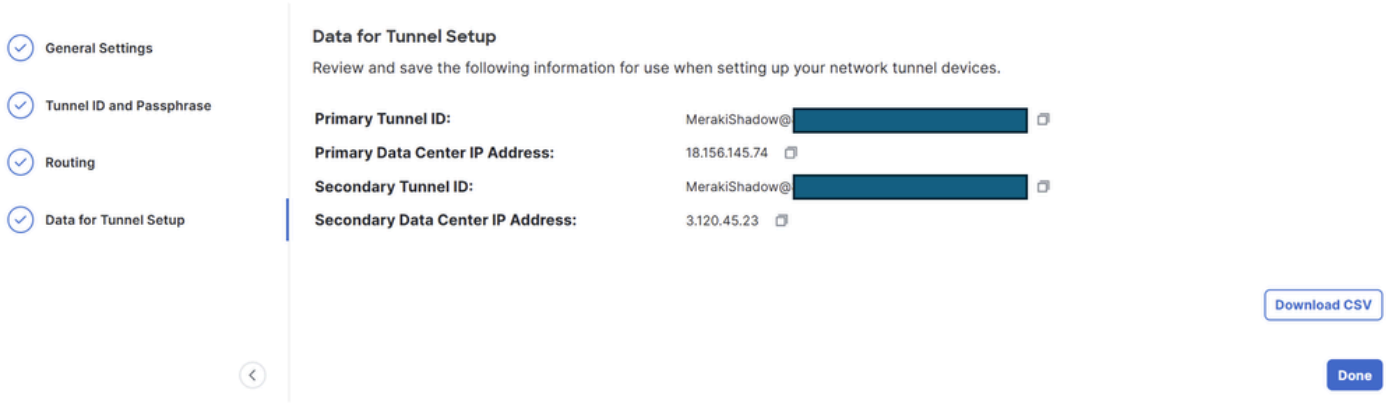


Precaución: Asegúrese de agregar la IP de la sonda de supervisión (192.0.2.3/32); de lo contrario, puede experimentar problemas de tráfico en el dispositivo Meraki que enrutan el tráfico a Internet, los grupos VPN y el rango CGNAT 100.64.0.0/10 que utiliza ZTNA.

- Después de hacer clic en **Save** la información sobre el túnel se muestra, por favor, guarde esa información para el siguiente paso, **Configure the tunnel on Meraki MX.**

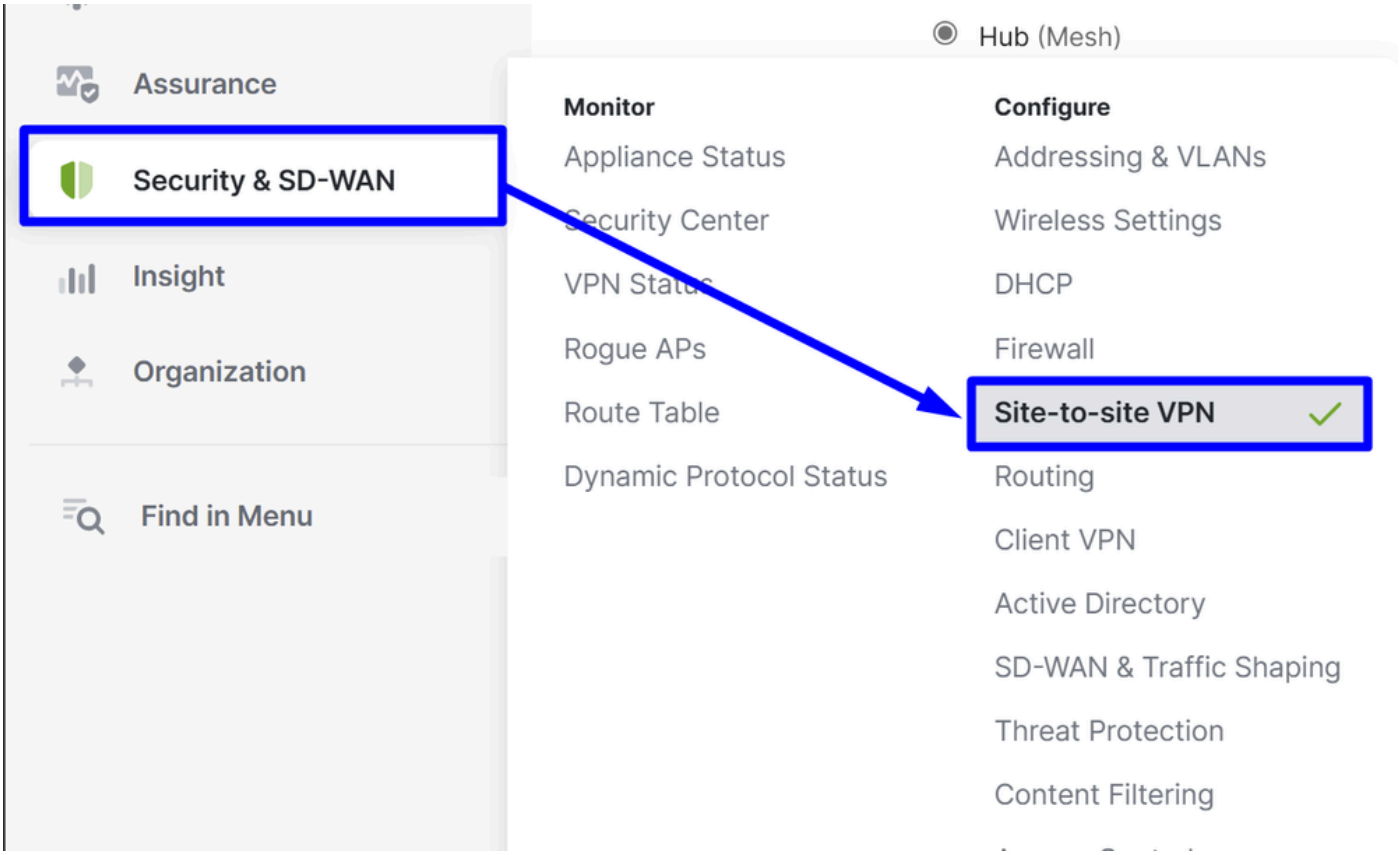
Configuración de VPN de acceso seguro

Copie la configuración de los túneles en un bloc de notas. Utilice esta información para completar la configuración en Meraki **Non-Meraki VPN Peers**.



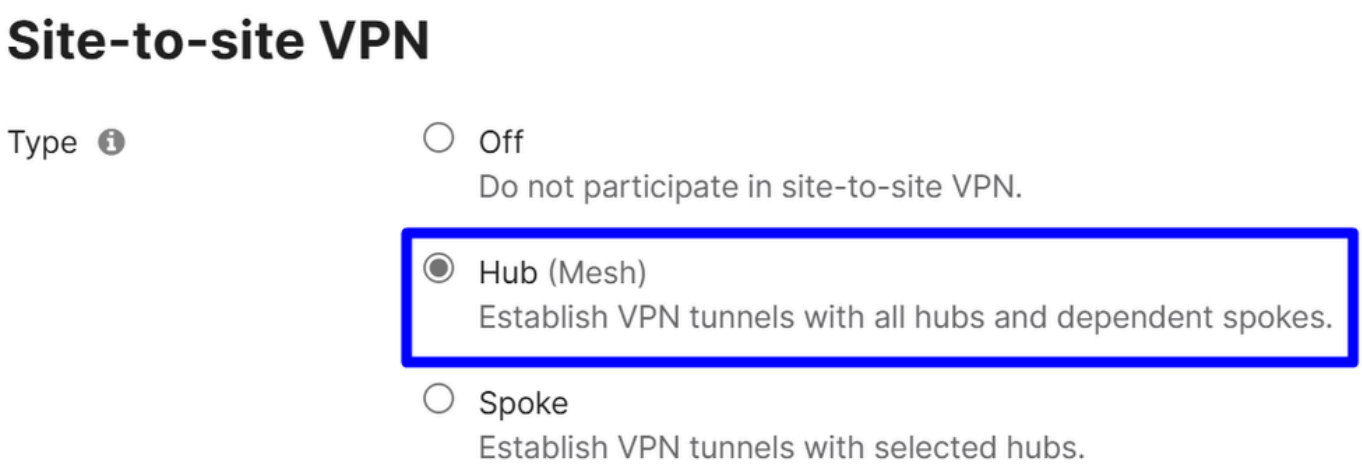
Configuración de la VPN en Meraki MX

Navegue hasta Meraki MX y haga clic en **Security & SD-WAN** > Site-to-site VPN



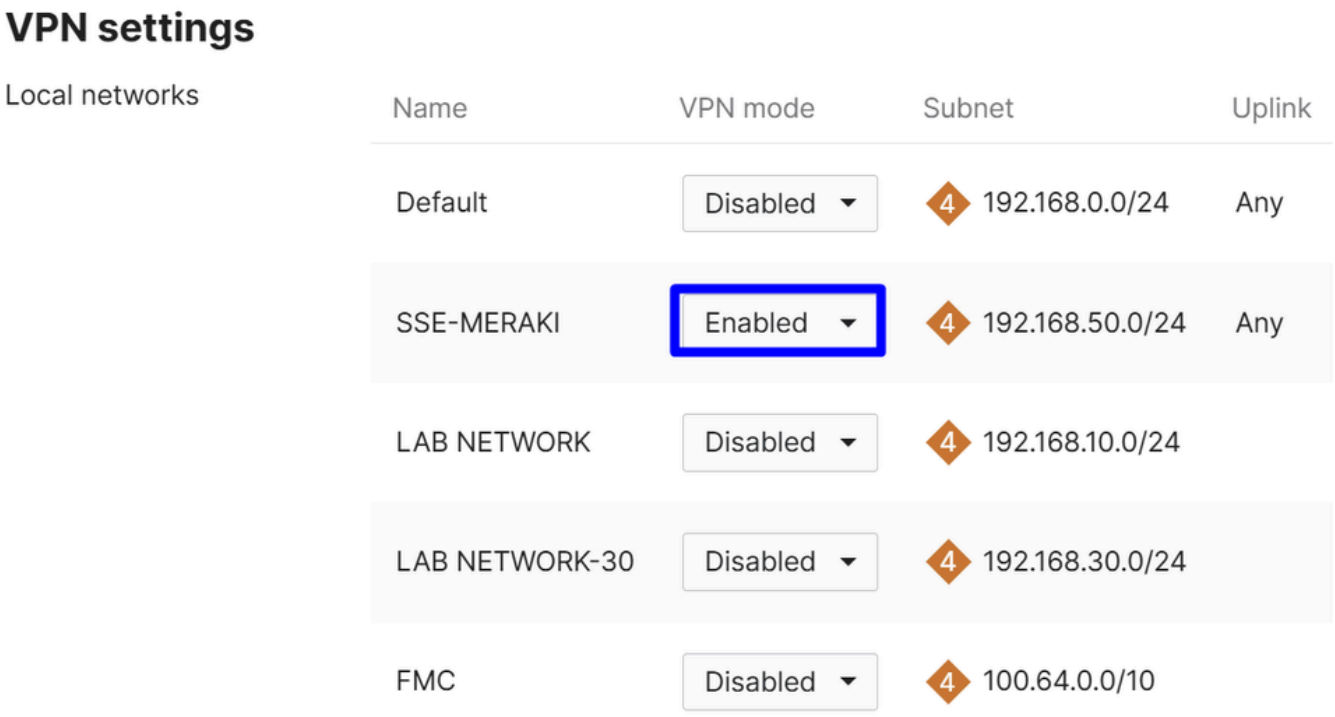
VPN de sitio a sitio

Elegir Hub.

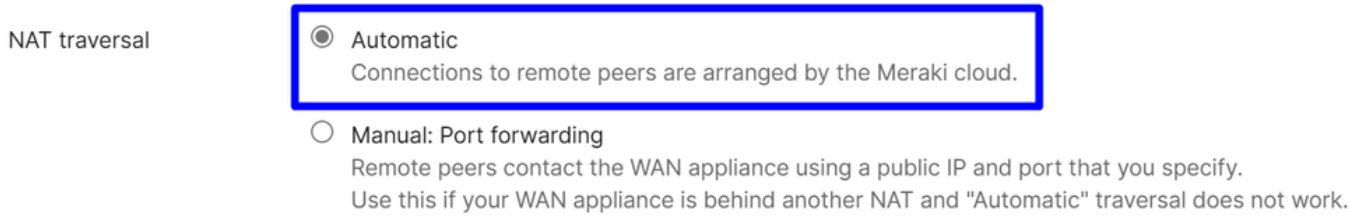


Configuración de VPN

Elija las redes que seleccionó para enviar tráfico a Secure Access:



Elegir en NAT Traversal Automático



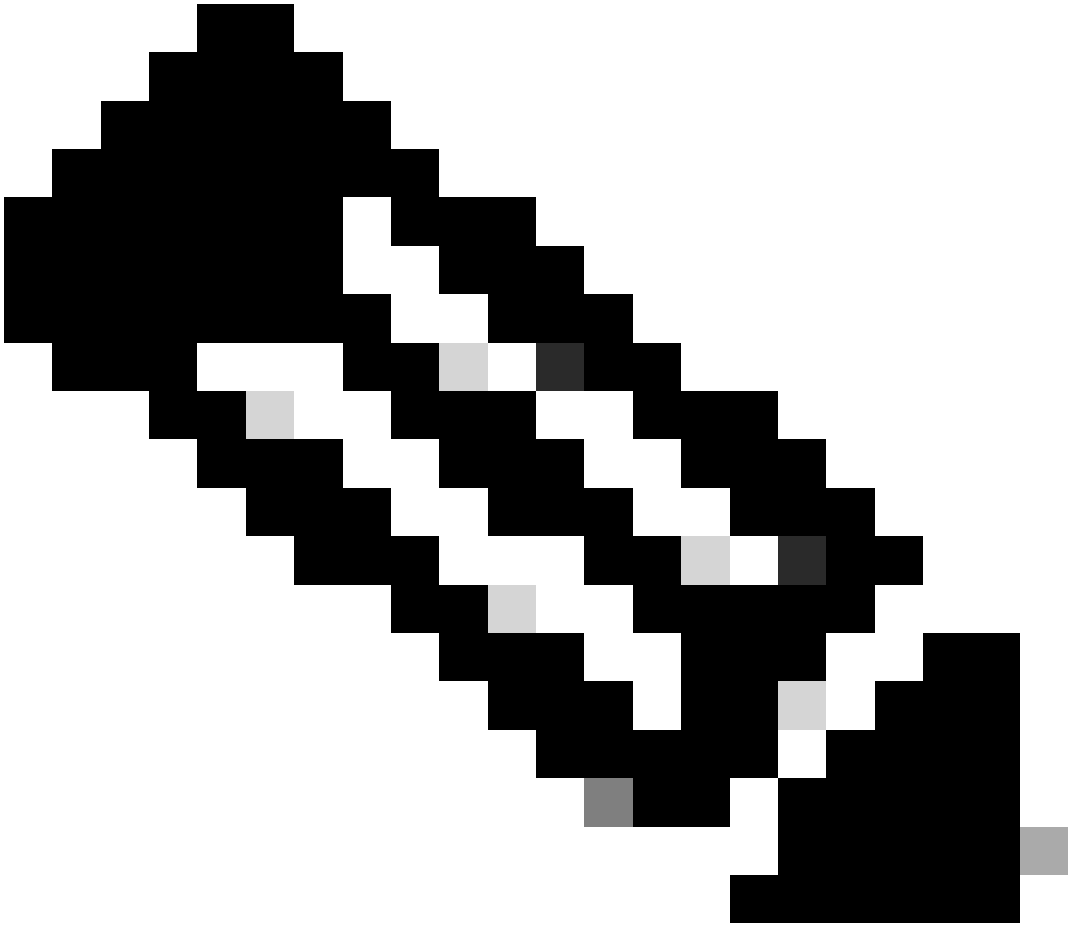
Puntos de VPN que no son Meraki

Debe configurar las comprobaciones de estado que utiliza Meraki para dirigir el tráfico a Secure Access:

Haga clic en **Configure Health Checks**

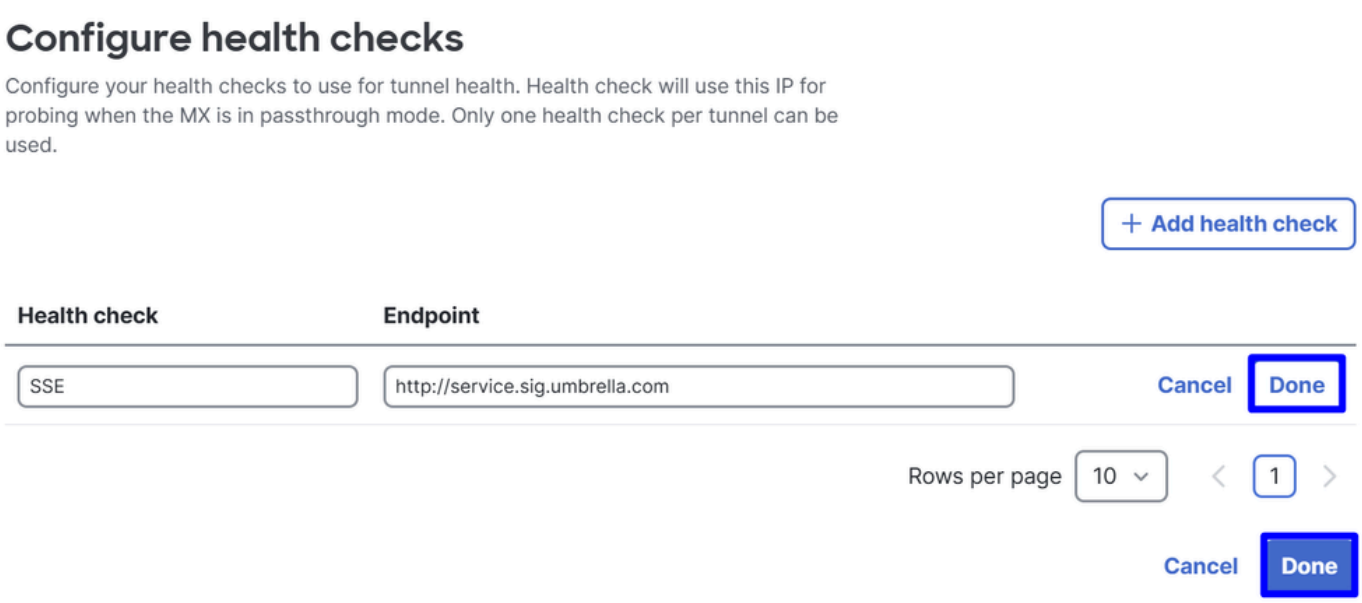
- Haga clic en **+Add health Check**

- **Health Check**: Configurar un nombre para la prueba
- **Endpoint**: Utilice el recomendado por Secure Access http://service.sig.umbrella.com



Nota: Este dominio solo responde cuando se accede a través de un túnel de sitio a sitio con Secure Access o Umbrella: los intentos de acceso desde fuera de estos túneles fallan.

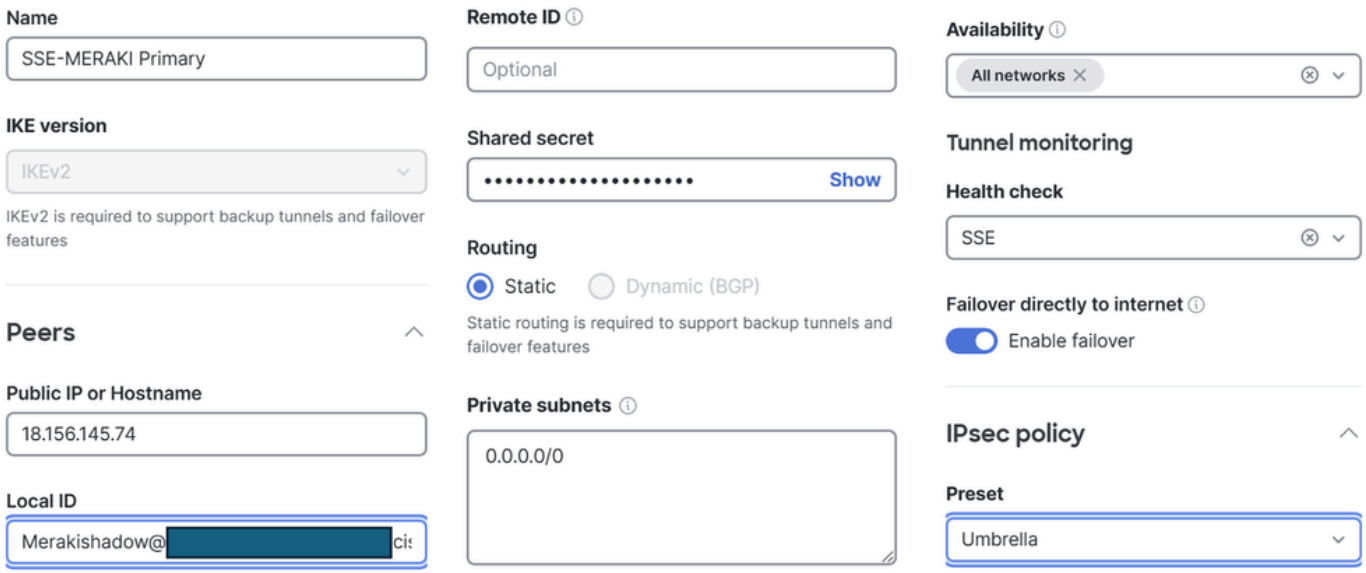
A continuación, haga clic **Done** dos veces para finalizar.



Ahora se han configurado las comprobaciones de estado y está listo para configurar el **Peer:**

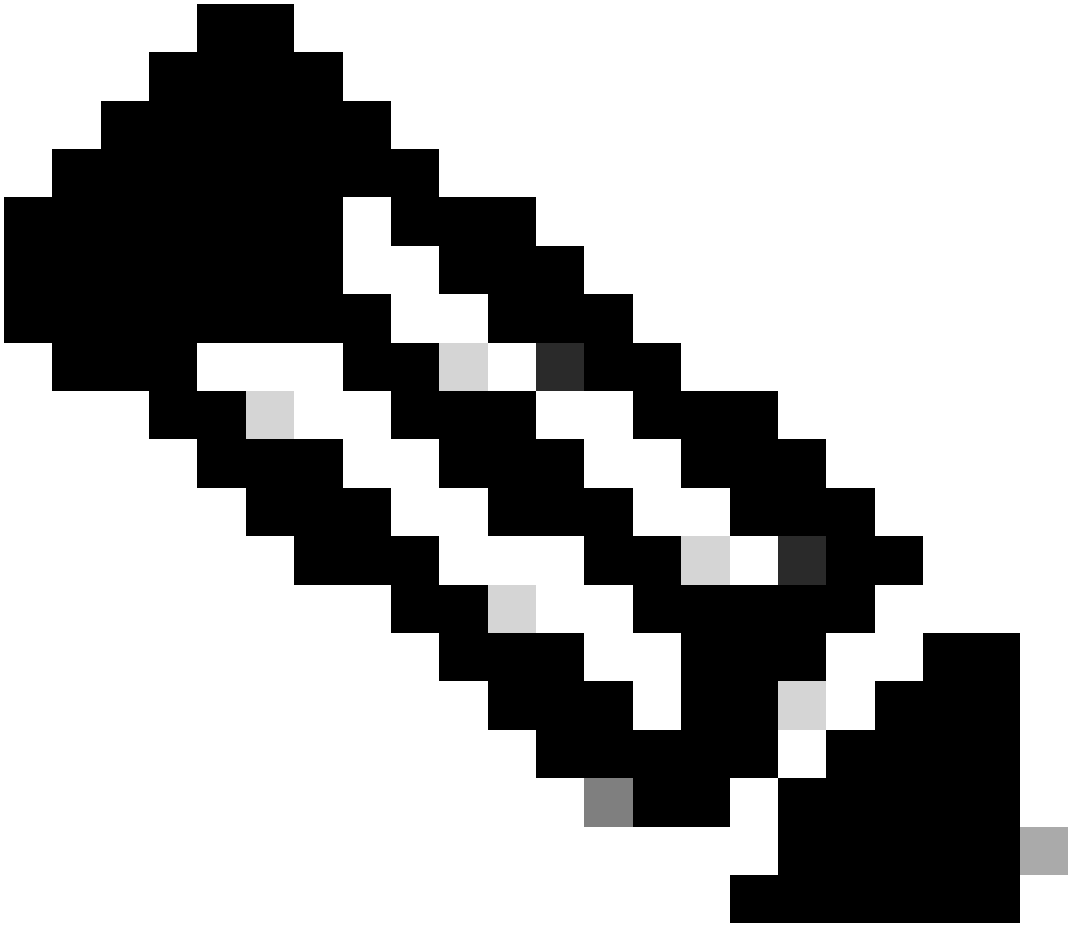
Configuración del túnel principal

- Haga clic en+Add a peer



- Agregar par VPN
  - Nombre: Configure un nombre para la VPN para Secure Access
  - Versión de IKE: Elija IKEv2
- Pares
  - IP pública o nombre de host: Configure los **Primary Datacenter IP** datos proporcionados por Secure Access en el paso Secure Access VPN Configurations
  - ID local: Configure los **Primary Tunnel ID** datos proporcionados por Secure Access en el paso Secure Access VPN Configurations
  - ID remoto: N/A
  - Secreto compartido: configure los **Passphrase** datos proporcionados por Secure Access

en el paso Configuraciones VPN de Secure Access
    - Ruteo: Elegir estática
    - Subredes privadas: si tiene pensado configurar tanto el acceso a Internet como el acceso privado, utilice **0.0.0.0/0** como destino. Si está configurando solamente el acceso privado para ese túnel VPN, especifique el **Remote Access VPN IP Pool** y el rango CGNAT **100.64.0.0/10** como redes de destino
    - Disponibilidad: si solo dispone de un dispositivo Meraki, puede seleccionar **All Networks.** Si tiene varios dispositivos, asegúrese de seleccionar solo la red Meraki específica en la que va a configurar el túnel.
- Monitoreo de Túnel
    - Comprobación de estado: Utilice la comprobación de estado configurada anteriormente para supervisar la disponibilidad del túnel
    - Conmutación por fallo directamente a Internet: si activa esta opción y tanto el túnel 1 como el 2 no superan sus comprobaciones de estado, el tráfico se redirige a la interfaz WAN para evitar la pérdida de acceso a Internet.



Funcionalidad de comprobación de estado: si se está supervisando el túnel 1 y su

---

comprobación de estado falla, el tráfico pasa automáticamente por error al túnel 2. Si el túnel 2 también falla y la**Failover directly to Internet**opción está activada, el tráfico se enruta a través de la interfaz WAN del dispositivo Meraki.

- directiva IPsec
  - Preajuste: Elegir **Umbrella**

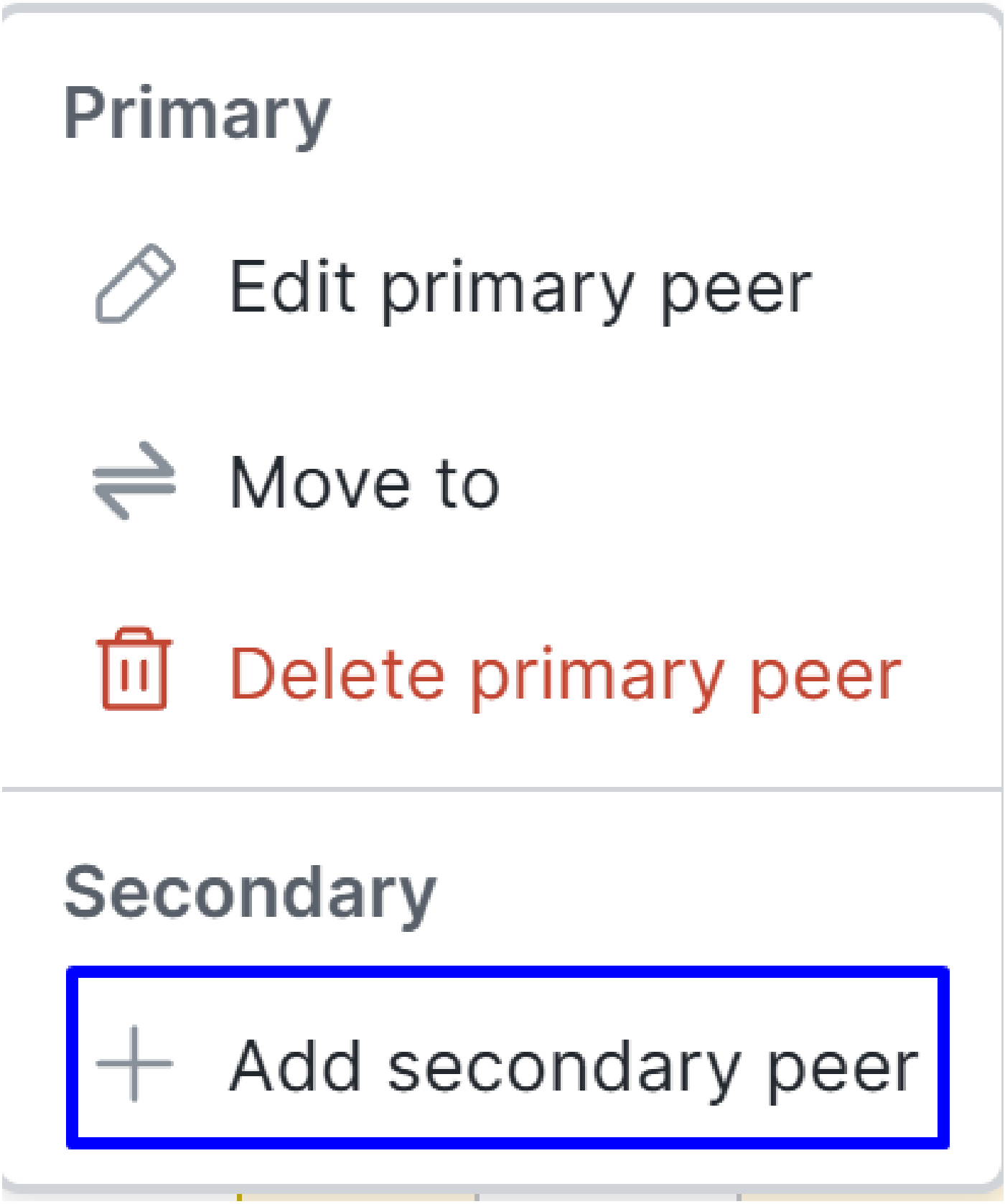
A continuación, haga clic en **Save**.

Configuración del túnel secundario

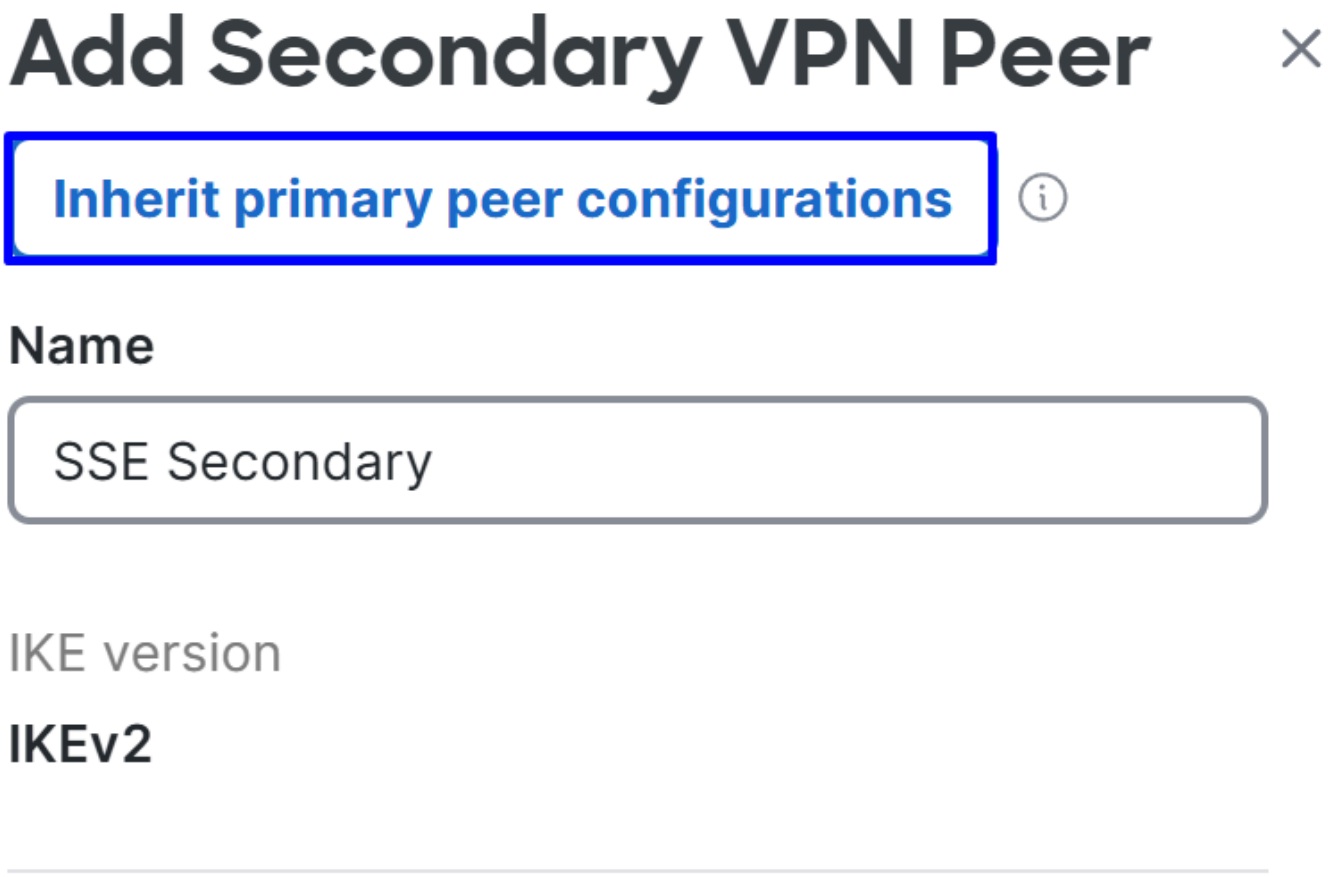
Para configurar el túnel secundario, haga clic en el menú de opciones del túnel principal:

- Haga clic en los tres puntos

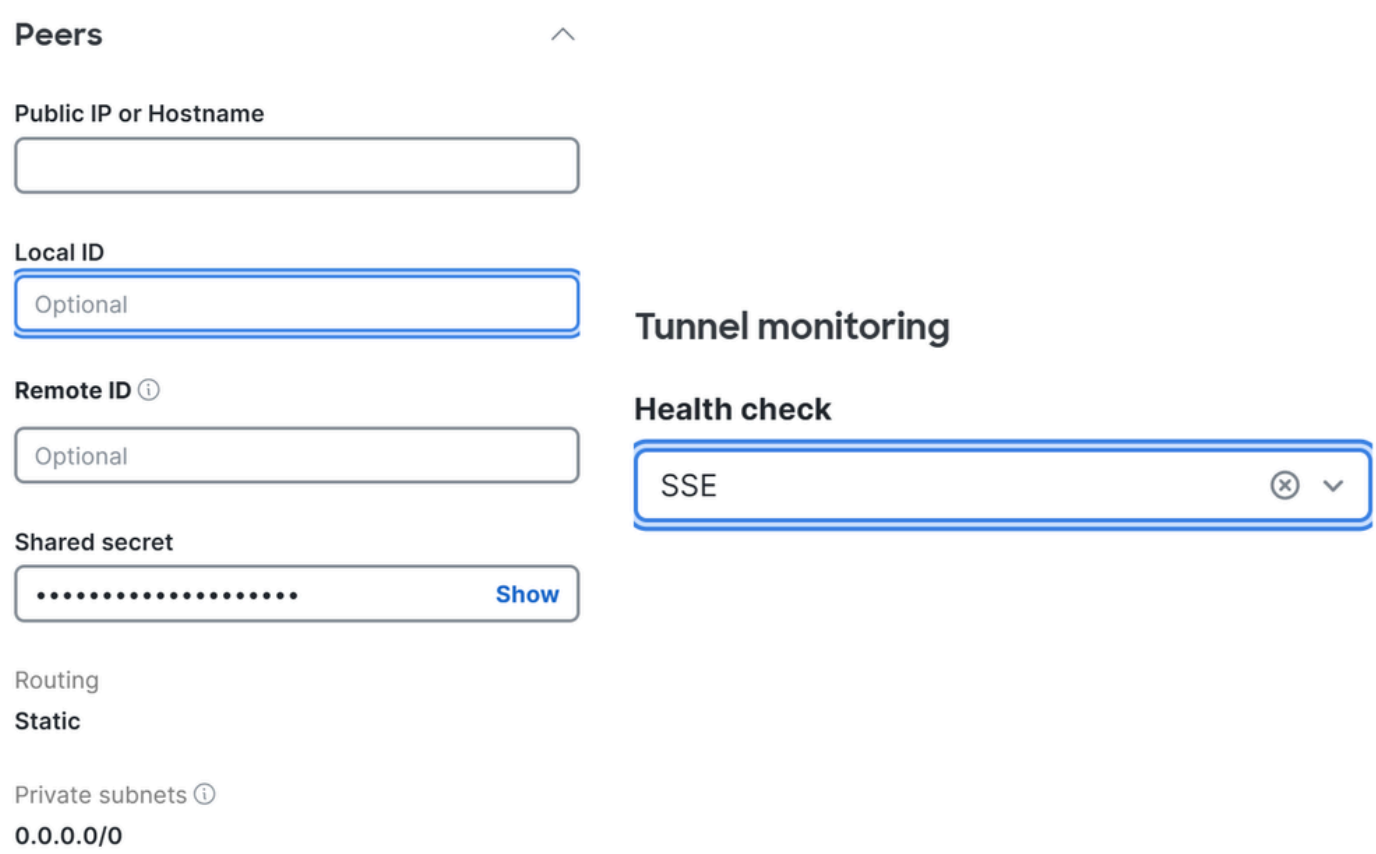
- Haga clic en **+ Add Secondary peer**



- Haga clic enInherit primary peer configurations

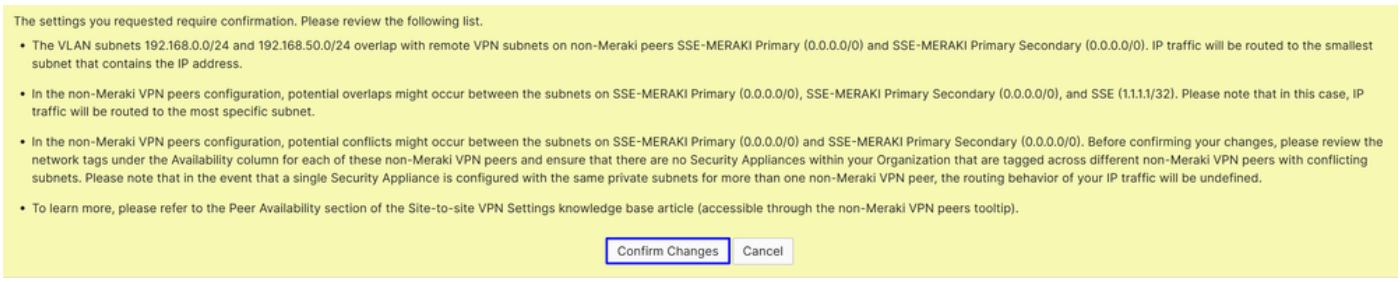


A continuación, observará que algunos campos se rellenan automáticamente. Revíselos, realice los cambios necesarios y complete el resto manualmente:



- Pares
  - IP pública o nombre de host: Configure los **Secondary Datacenter IP** datos proporcionados por Secure Access en el paso Secure Access VPN Configurations
  - ID local: Configure los **Secondary Tunnel ID** datos proporcionados por Secure Access en el paso Secure Access VPN Configurations
  - ID remoto: N/A
  - Secreto compartido: configure los **Passphrase** datos proporcionados por Secure Access en el paso Configuraciones VPN de Secure Access
- Monitoreo de Túnel
  - Comprobación de estado: Utilice la comprobación de estado configurada anteriormente para supervisar la disponibilidad del túnel

A continuación, puede hacer clic en **Save**, y aparecerá la siguiente alerta:

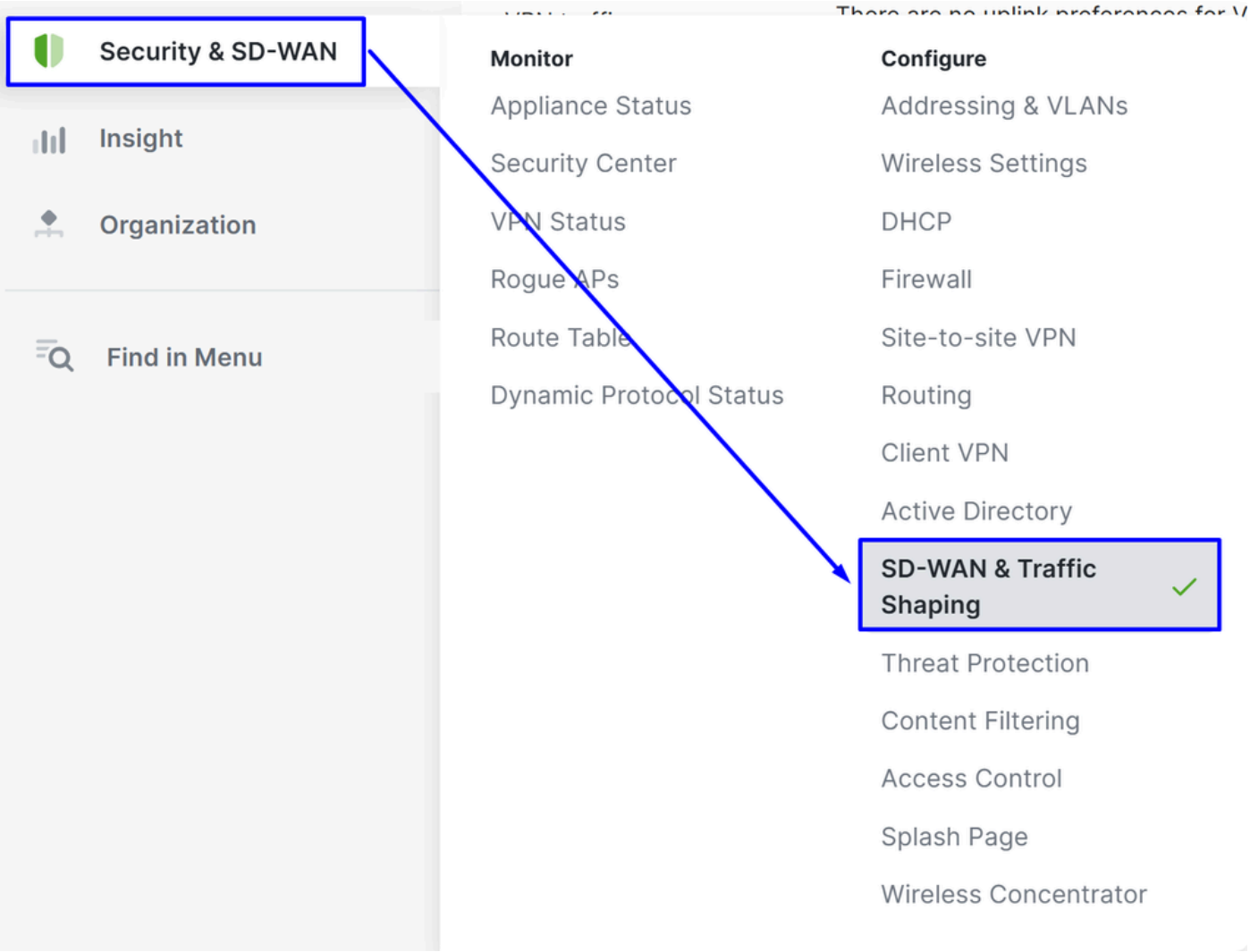


No se preocupe y haga clic **Confirm Changes**.

Configuración de la Dirección de Tráfico (Omisión de Tráfico de Túnel)

Esta función permite omitir el tráfico específico del túnel mediante la definición de dominios o direcciones IP en la configuración de omisión de SD-WAN:

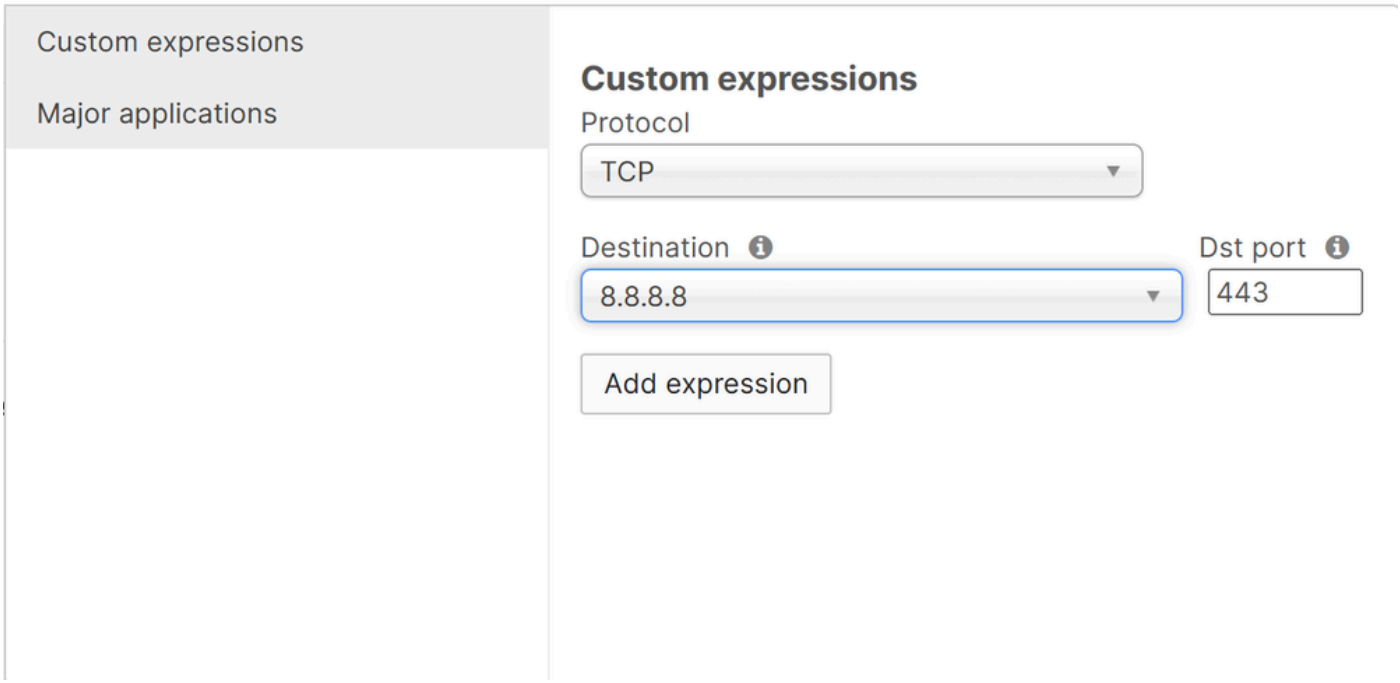
- Vaya a **Security & SD-WAN** > SD-WAN & Traffic Shaping



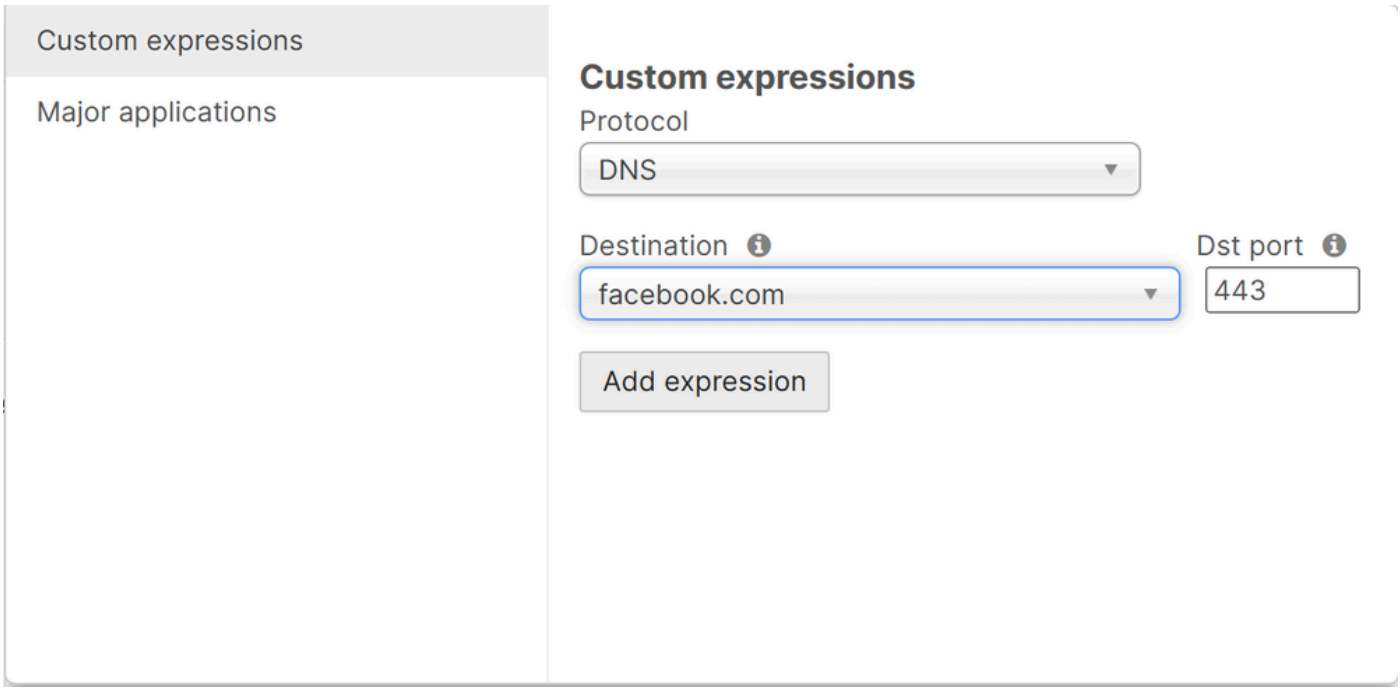
- Desplácese hacia abajo hasta la **Local Internet Breakout** sección y haga clic en **Add+**

A continuación, cree el desvío basado en **Custom Expressions** o **Major Applications**:

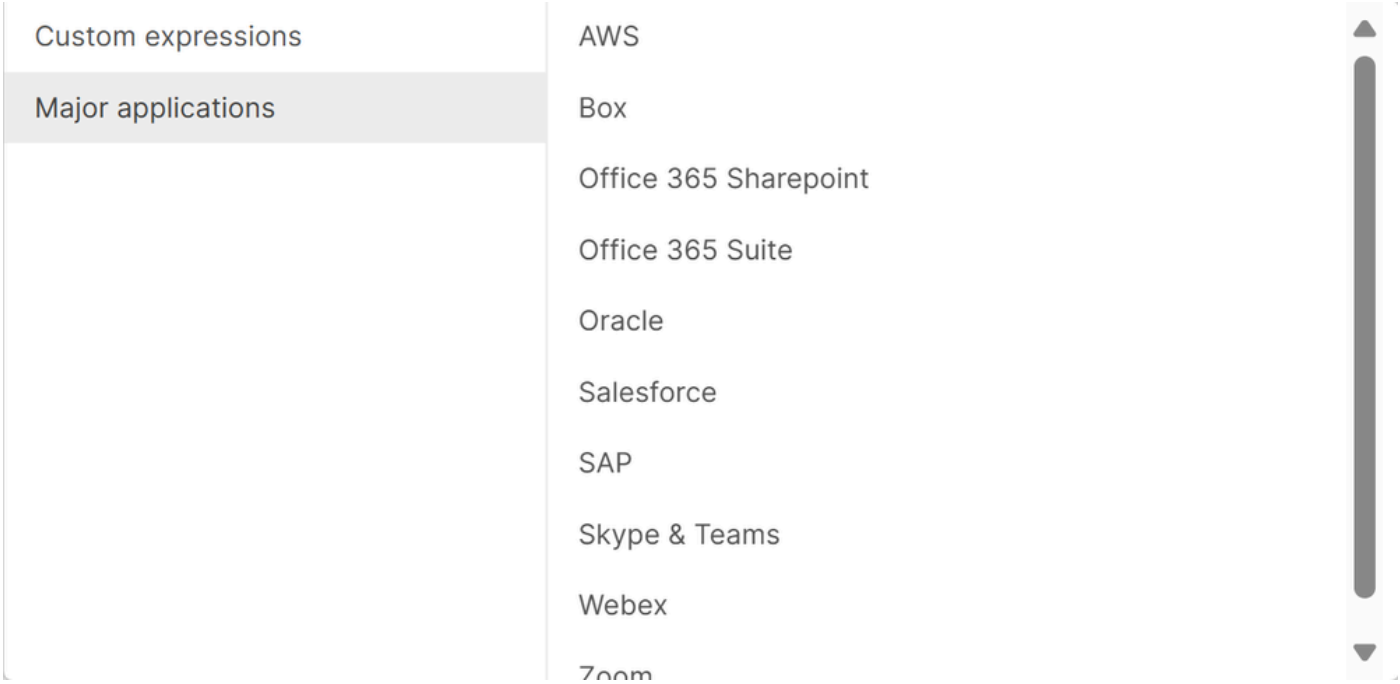
Custom Expressions - Protocol



Custom Expressions - DNS



Major Applications

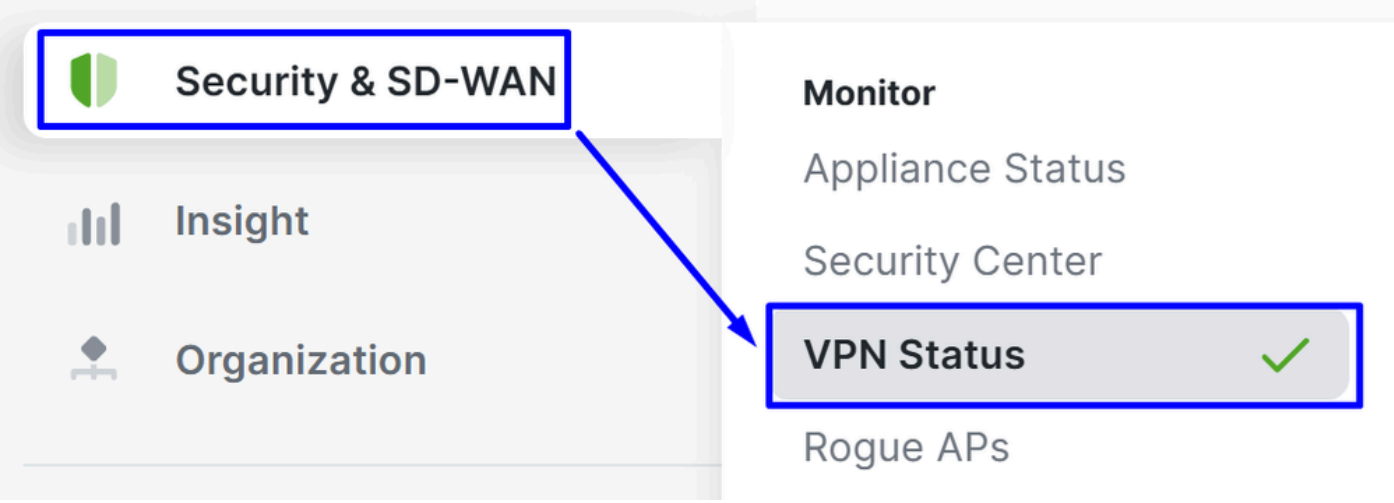


Para obtener más información, visite: [Configuración de reglas de exclusión de VPN (IP/Port/DNS/APP)]

Verificación

Para comprobar si los túneles están activos, verifique el estado en:

- Haga clic en Security & SD-WAN > **VPN Status** en el panel de Meraki.



- Haga clic en 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 los estados de VPN primario y secundario se muestran en verde, significa que los túneles están activos y activos.

Meraki VPN Status Codes

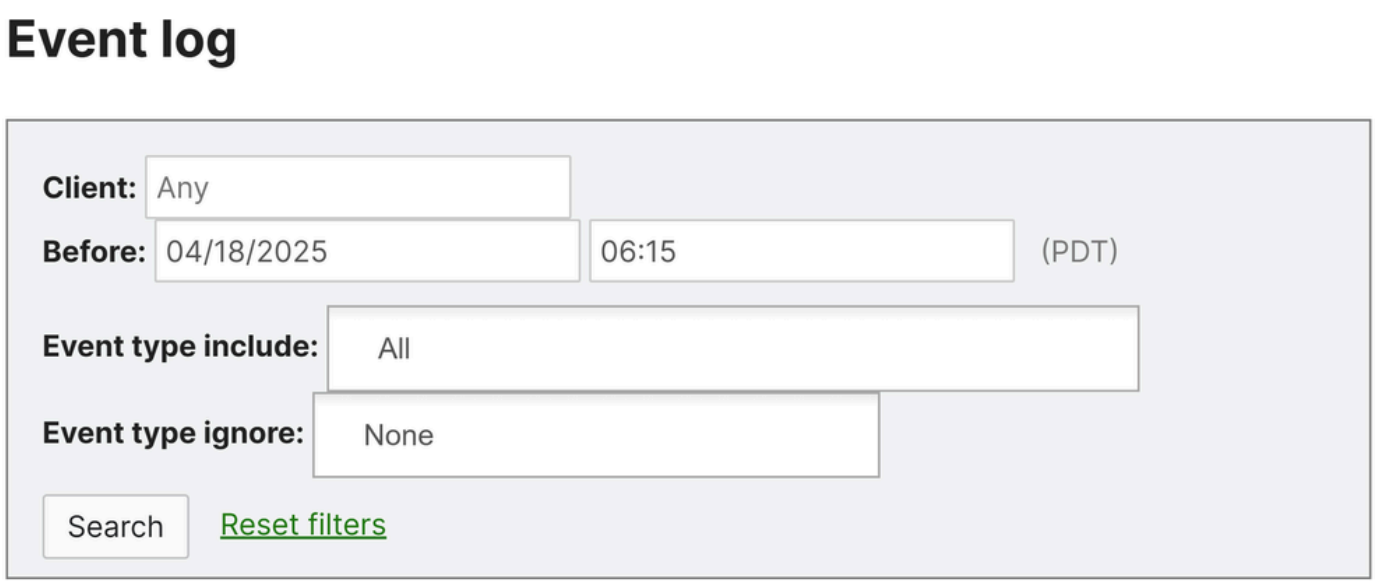
Status Indicator	Color	Meaning
Primary/Secondary Up	Green	Phase 1 and phase 2 are up
Partial Connectivity	Amber	Phase 1 is up but phase 2 is down
Tunnel Down	Red	Phase 1 and phase 2 are both down

Troubleshoot

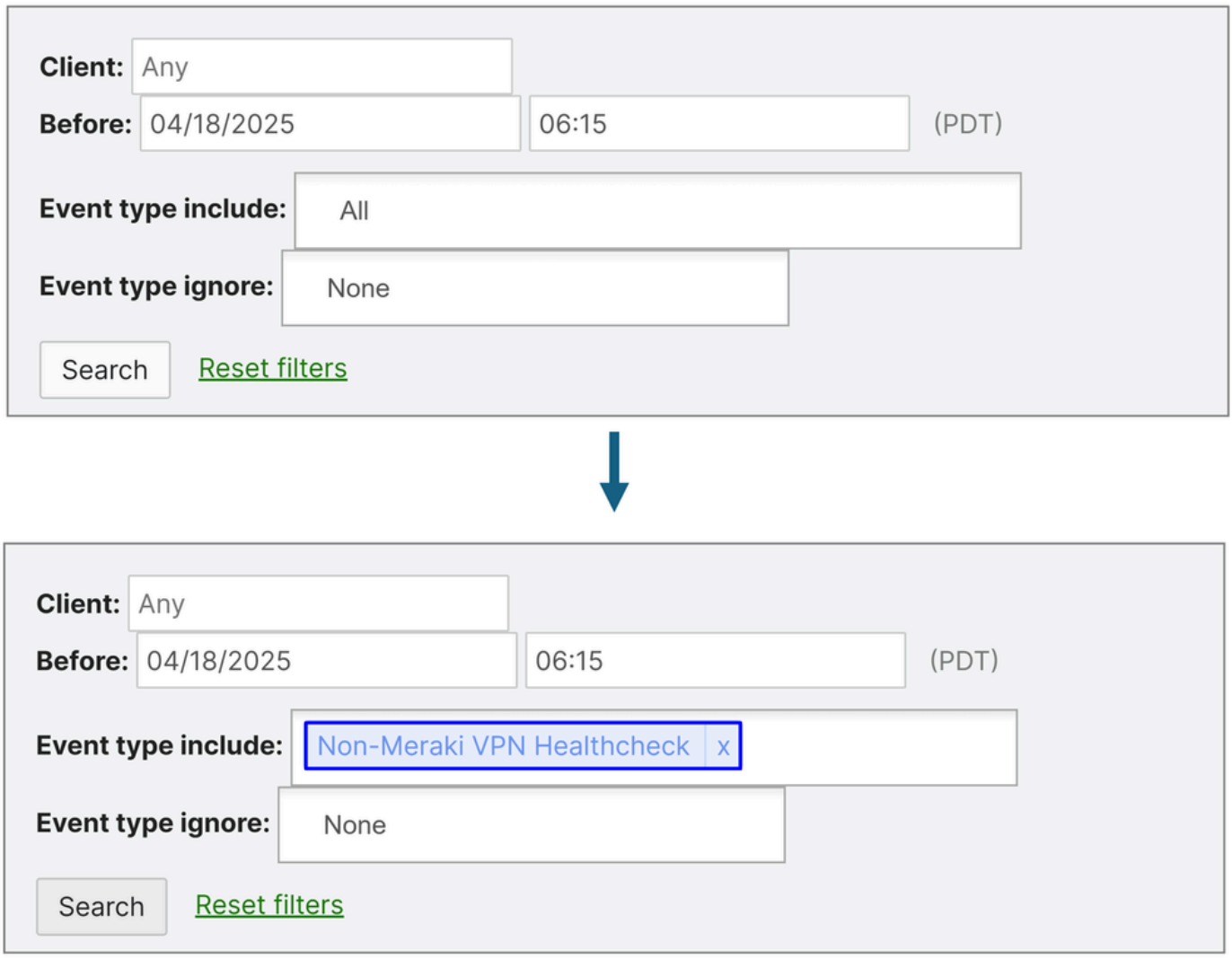
Verificar comprobaciones de estado

Para comprobar si las comprobaciones de estado de Meraki de la VPN funcionan correctamente, vaya a:

- Haga clic en **Assurance** > Event Log

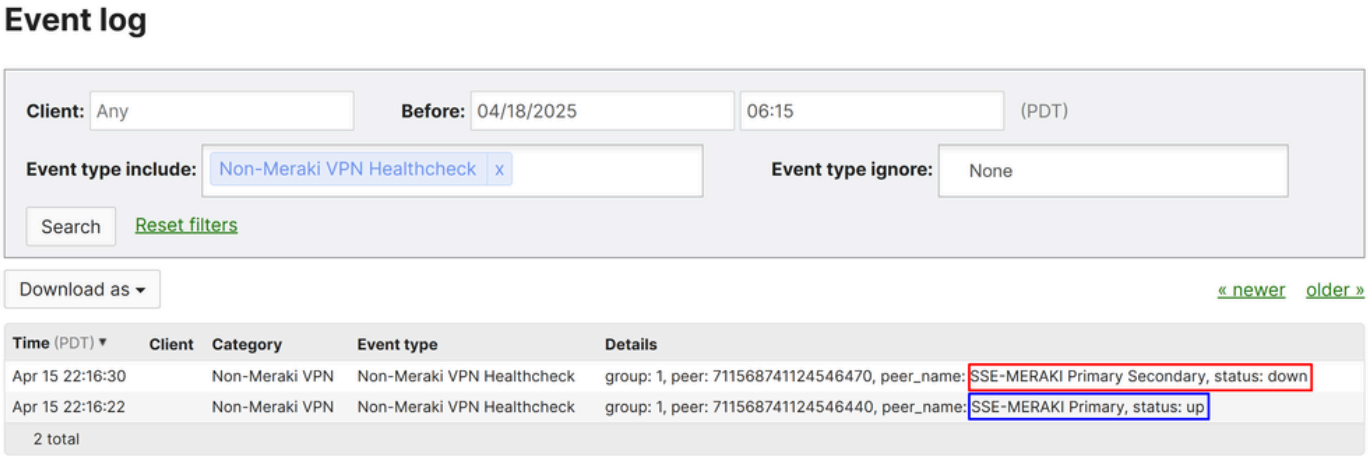


En **Event Type Include**, elija Non-Meraki VPN Healthcheck



Cuando el túnel principal a Cisco Secure Access está activo, los paquetes que llegan a través del túnel secundario se descartan para mantener un trayecto de ruteo consistente.

El túnel secundario permanece en modo de espera y solo se utiliza si se produce un fallo en el túnel principal, ya sea desde el lado de Meraki o dentro de Secure Access, según lo determinado por el mecanismo de comprobación de estado.



- La comprobación de estado del túnel principal muestra el estado: activo, lo que significa que actualmente está transmitiendo y reenviando tráfico activamente.
- La comprobación de estado del túnel secundario muestra el estado: down, no porque el túnel no esté disponible, sino porque el primario se encuentra en buen estado y se está utilizando activamente. Se espera este comportamiento, ya que sólo se permite que el tráfico pase a través del túnel 1, lo que provoca un error en la comprobación de estado del túnel secundario.

Información Relacionada

- Soporte técnico y descargas de Cisco
- Centro de ayuda de Cisco Secure Access
- Guía de configuración de Cisco Secure Access Meraki BGP

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).