Configurazione di un accesso sicuro con Meraki MX per il monitoraggio dell'alta disponibilità e dello stato

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco Secure Access con Meraki MX per l'alta disponibilità usando i controlli di integrità.

Prerequisiti

- Verifica dei requisiti del tunnel IPsec con accesso sicuro
- Informazioni sui componenti Secure Access
- Comprendere la funzionalità di verifica dello stato in Meraki MX

Requisiti

- Meraki MX deve disporre del firmware versione 19.7.1 o successive
- Quando si utilizza l'accesso privato, è supportato un solo tunnel a causa di una limitazione

Meraki che impedisce la modifica dell'IP di controllo dello stato, rendendo necessario il protocollo NAT per altri tunnel SPA (Secure Private Access). Ciò non è valido quando si utilizza SIA (Secure Internet Access).
- Definire chiaramente le subnet o le risorse interne instradate attraverso il tunnel per l'accesso protetto.

Componenti usati

- Cisco Secure Access
- Appliance di sicurezza Meraki MX (versione firmware 19.7.1 o successiva)
- Dashboard Meraki
- Dashboard di accesso protetto

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Cisco Secure Access è una piattaforma di sicurezza nativa del cloud che consente l'accesso sicuro sia alle applicazioni private (tramite Accesso privato) che alle destinazioni Internet (tramite Accesso Internet). Se integrato con Meraki MX, consente alle organizzazioni di stabilire tunnel IPsec sicuri tra i siti delle filiali e il cloud, garantendo un flusso di traffico crittografato e l'applicazione centralizzata della sicurezza.

Questa integrazione utilizza tunnel IPsec di routing statico. Meraki MX stabilisce i tunnel IPsec primari e secondari per Cisco Secure Access e sfrutta i controlli di integrità dell'uplink integrati per eseguire il failover automatico tra i tunnel. In questo modo è possibile ottenere una configurazione resiliente e ad alta disponibilità per la connettività delle filiali.

Gli elementi chiave di questa distribuzione includono:

- Meraki MX che opera come peer VPN non Meraki per Cisco Secure Access.
- Tunnel primario e secondario configurati in modo statico, con controlli di integrità che determinano la disponibilità.
- L'accesso privato supporta l'accesso sicuro alle applicazioni interne tramite SPA (Secure Private Access), mentre l'accesso Internet consente al traffico di raggiungere le risorse

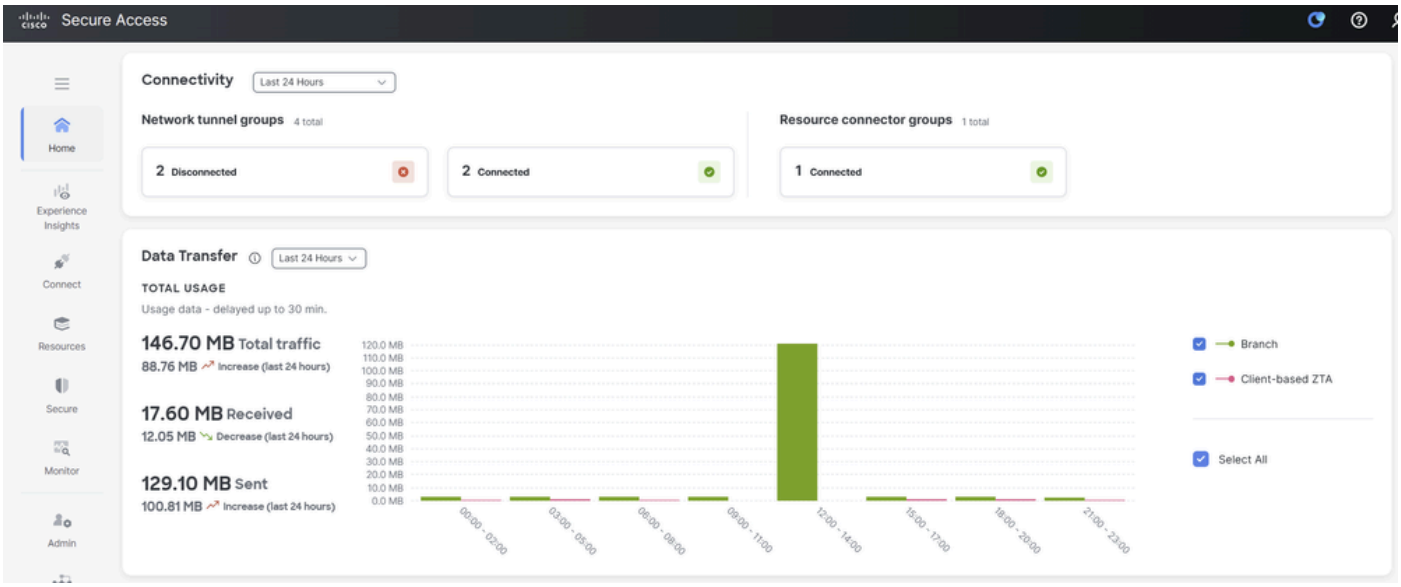
basate su Internet con l'applicazione di policy nel cloud.

- A causa dei limiti di Meraki nella flessibilità IP del controllo di integrità, in modalità di accesso privato è supportato un solo gruppo di tunnel. Se più dispositivi Meraki MX devono collegarsi a Secure Access for Private Access, è necessario usare BGP per il routing dinamico o configurare i tunnel statici. In questo modo, solo un gruppo di tunnel di rete può supportare i controlli di integrità e l'elevata disponibilità. I tunnel aggiuntivi funzionano senza monitoraggio dello stato o ridondanza.

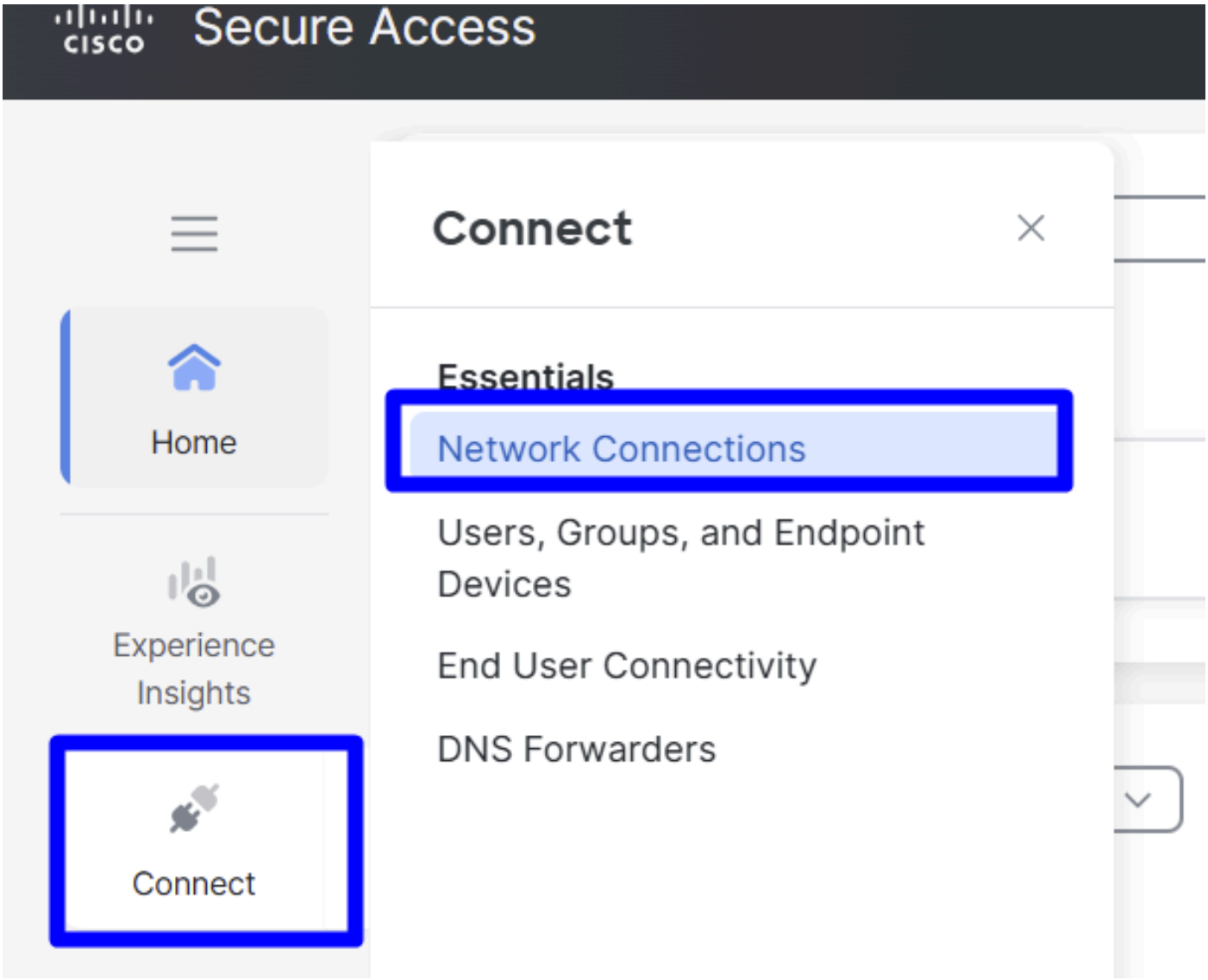
Configurazione

Configurare la VPN su accesso sicuro

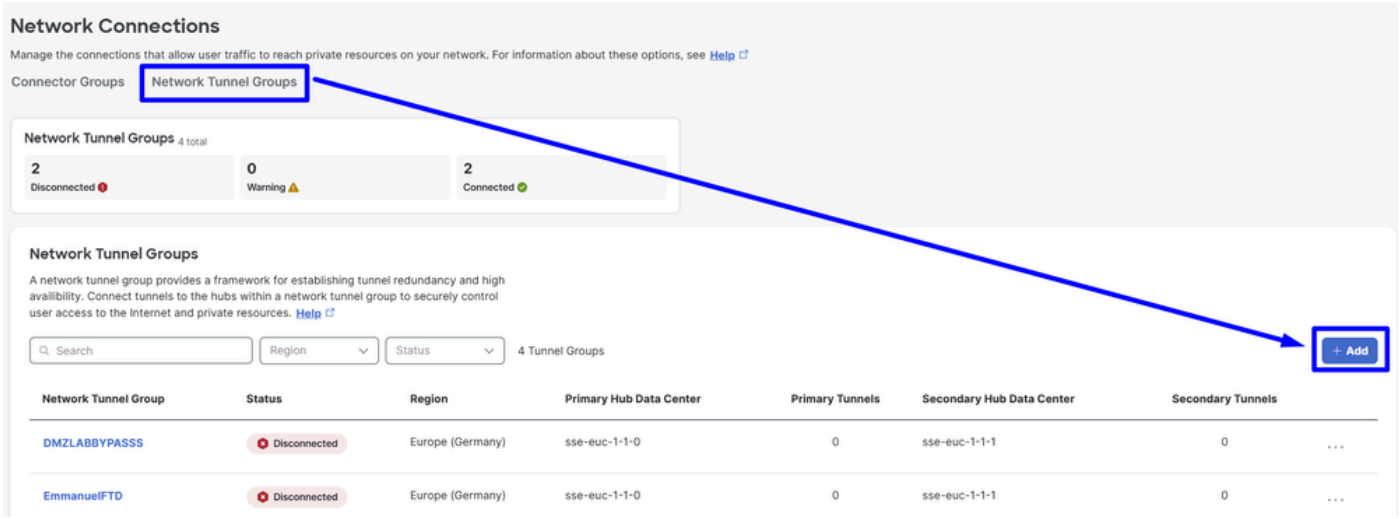
Passare al pannello di amministrazione di Accesso sicuro.



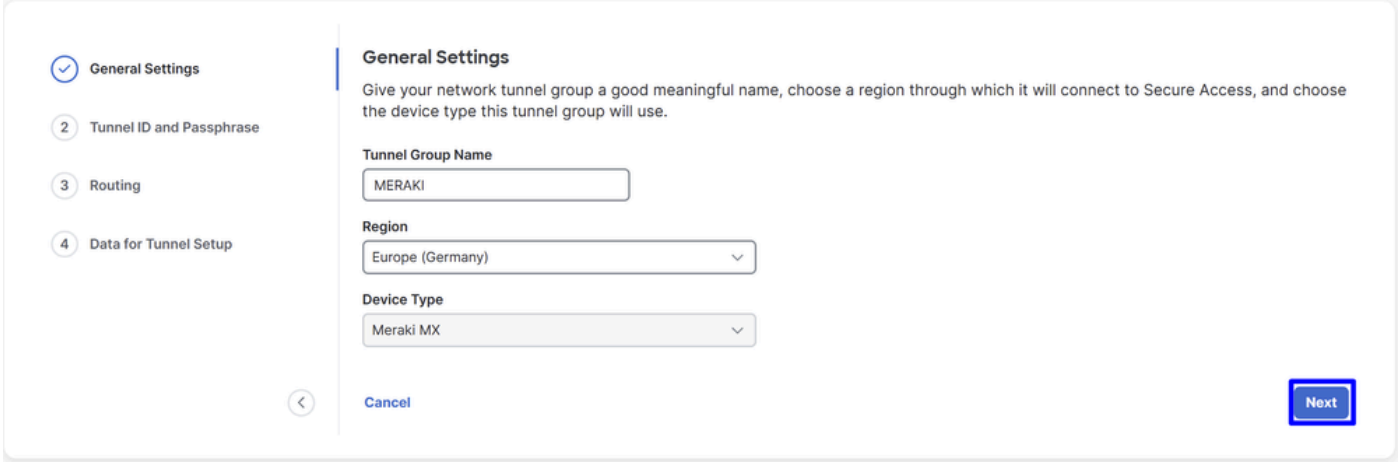
- Fare clic su Connect > Network Connections



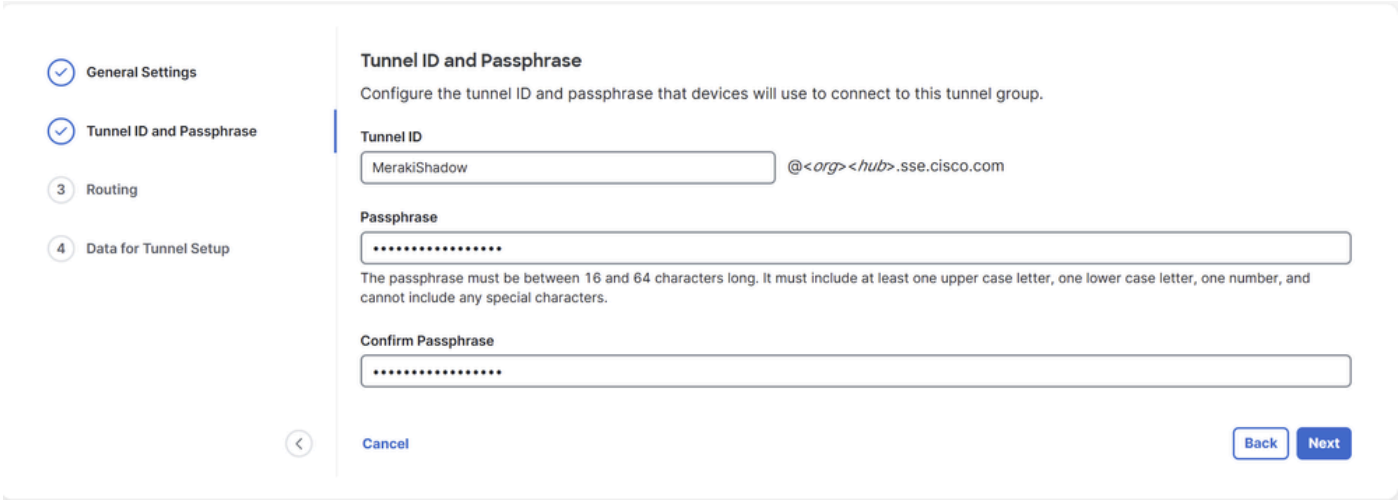
- In fareNetwork Tunnel Groupsclic su + Add



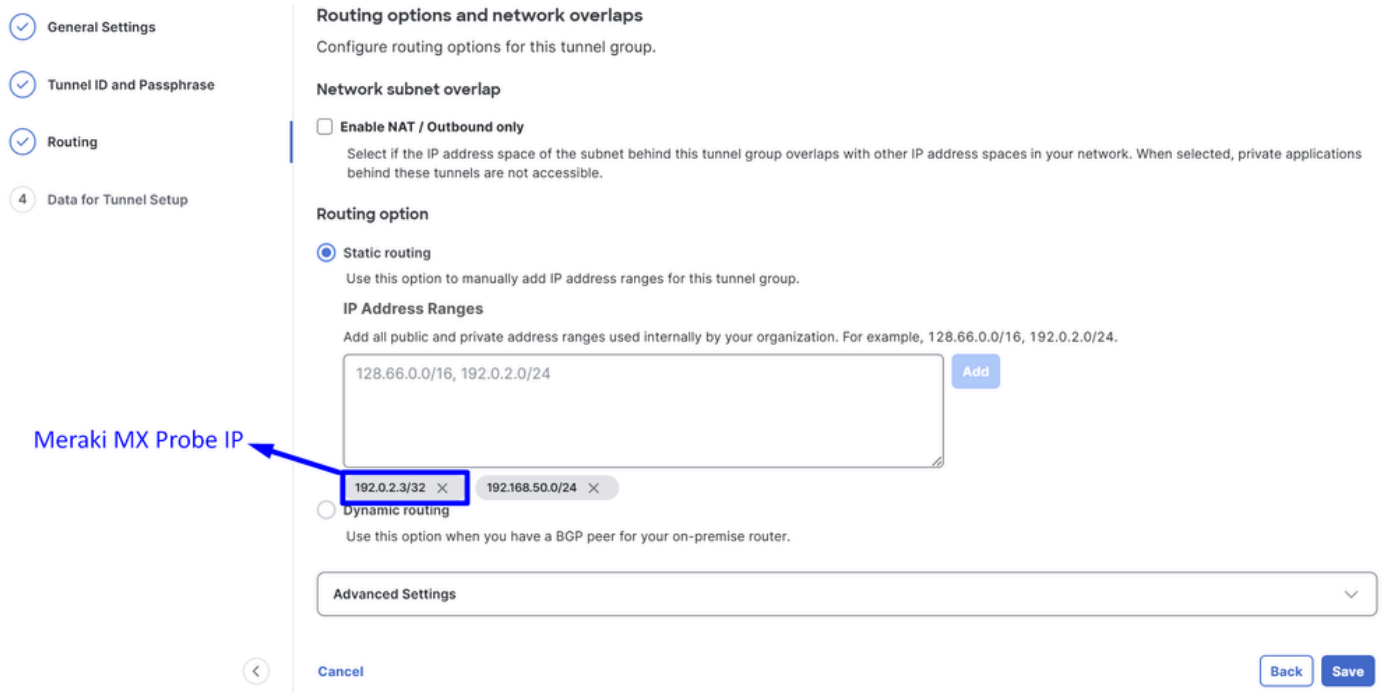
- ConfigurazioneTunnel Group Name, RegioneDevice Type
- Fare clic su **Next**

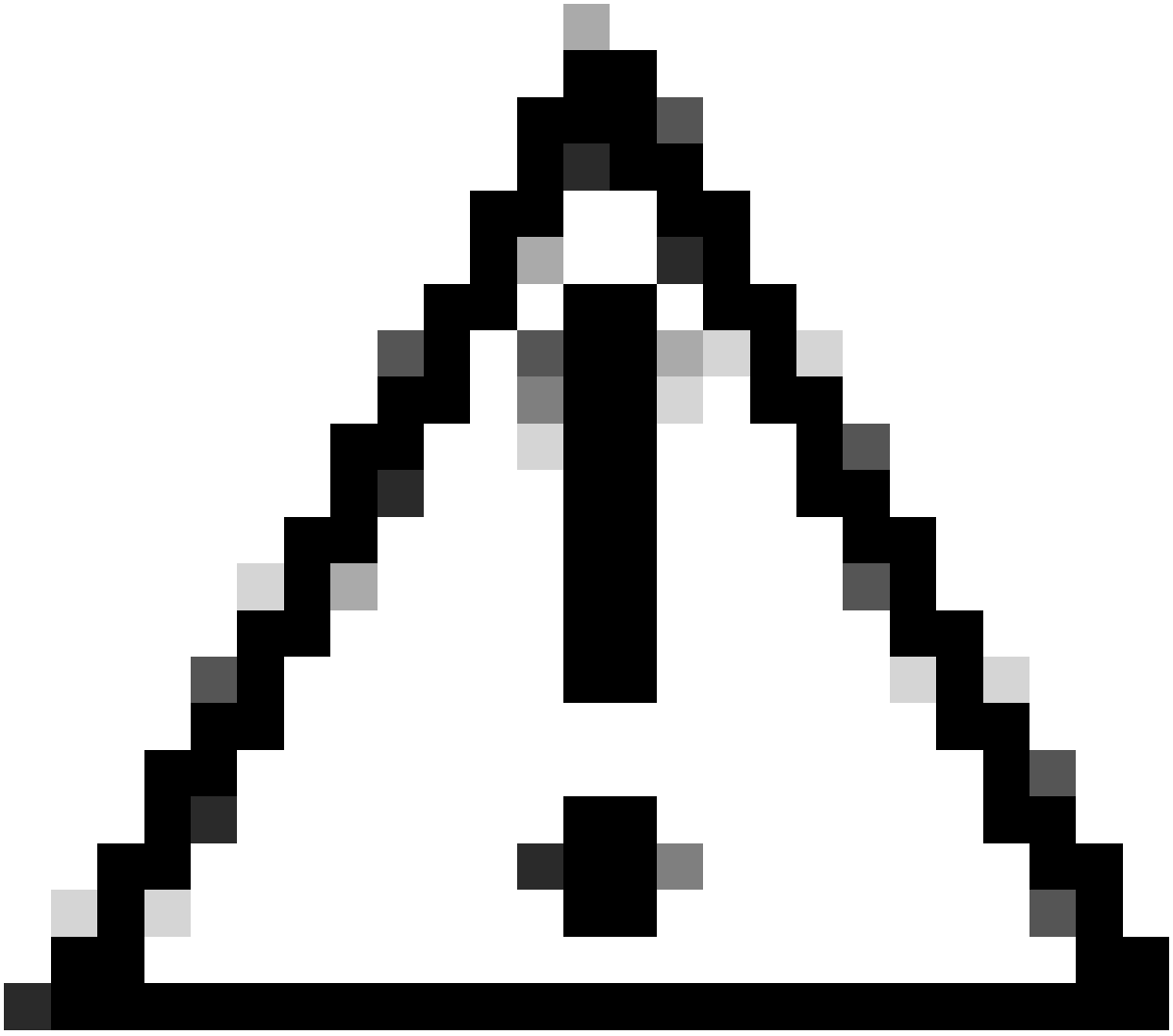


- Configurare Tunnel ID Format e Passphrase
- Fare clic su Next



- Configurare gli intervalli di indirizzi IP o gli host configurati sulla rete e che si desidera passare il traffico attraverso Secure Access, quindi accertarsi di includere l'IP della sonda di monitoraggio Meraki per 192.0.2.3/32 consentire la restituzione del traffico da Secure Access al Meraki MX.
- Fare clic su 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

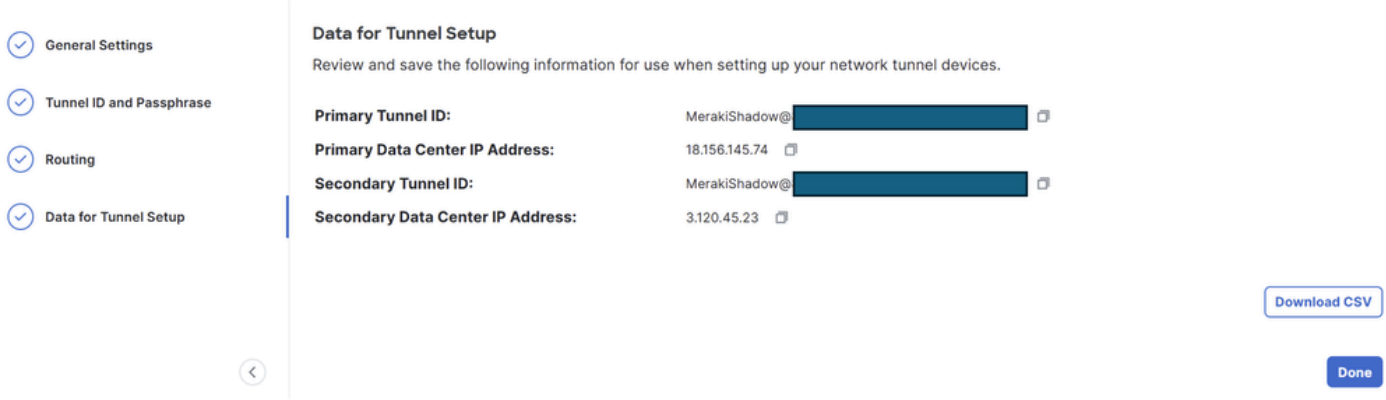


Attenzione: Accertarsi di aggiungere la sonda di monitoraggio IP (192.0.2.3/32); in caso contrario, si potrebbero verificare problemi di traffico sul dispositivo Meraki che indirizzano il traffico a Internet, ai pool VPN e all'intervallo CGNAT 100.64.0.0/10 usato da ZTNA.

- Dopo aver fatto clic sulle informazioni relative al **Save** tunnel che vengono visualizzate, salvarle per il passaggio successivo, **Configure the tunnel on Meraki MX.**

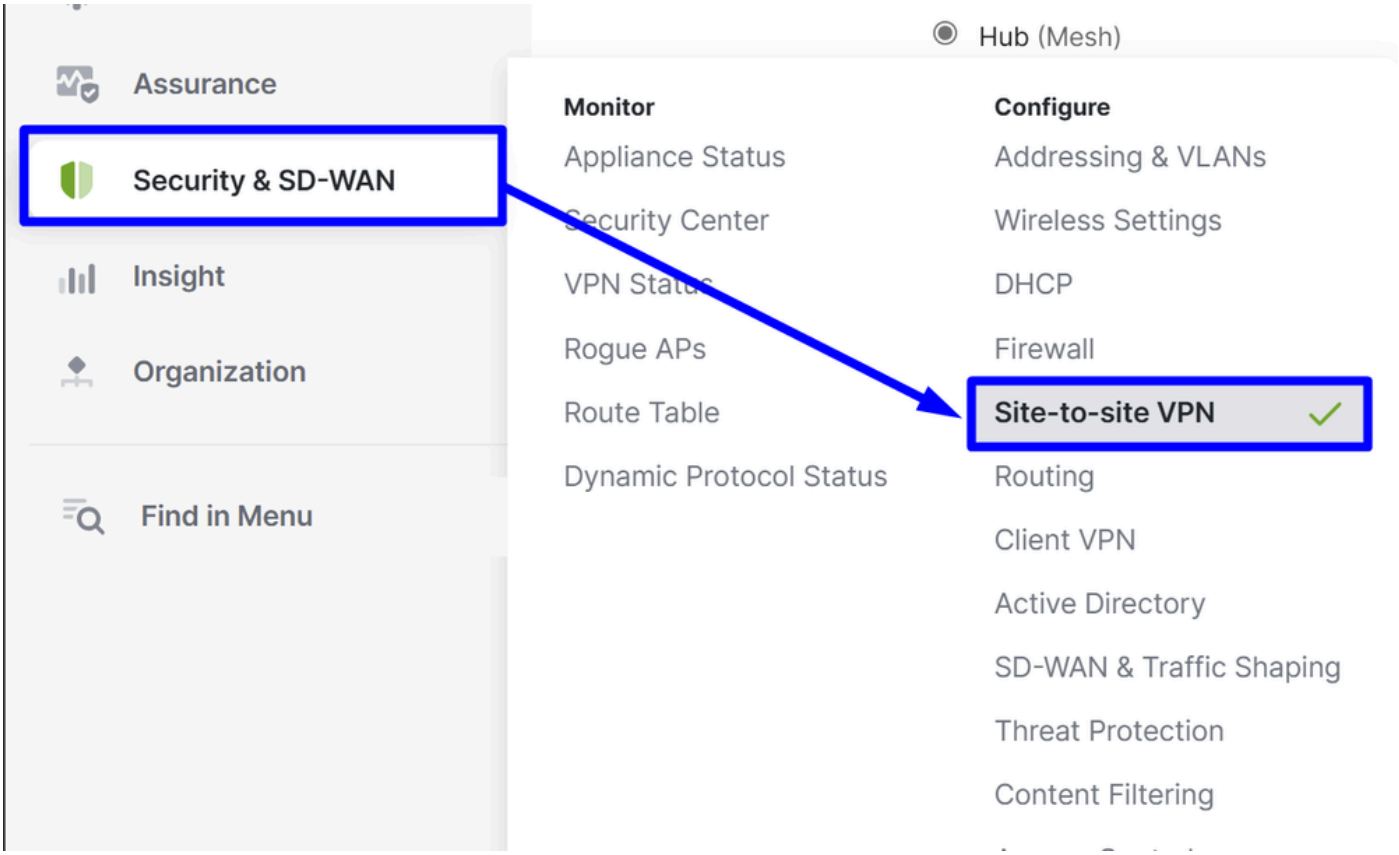
Configurazione VPN ad accesso sicuro

Copiare la configurazione dei tunnel in un blocco note. Utilizzare queste informazioni per completare la configurazione in Meraki **Non-Meraki VPN Peers**.



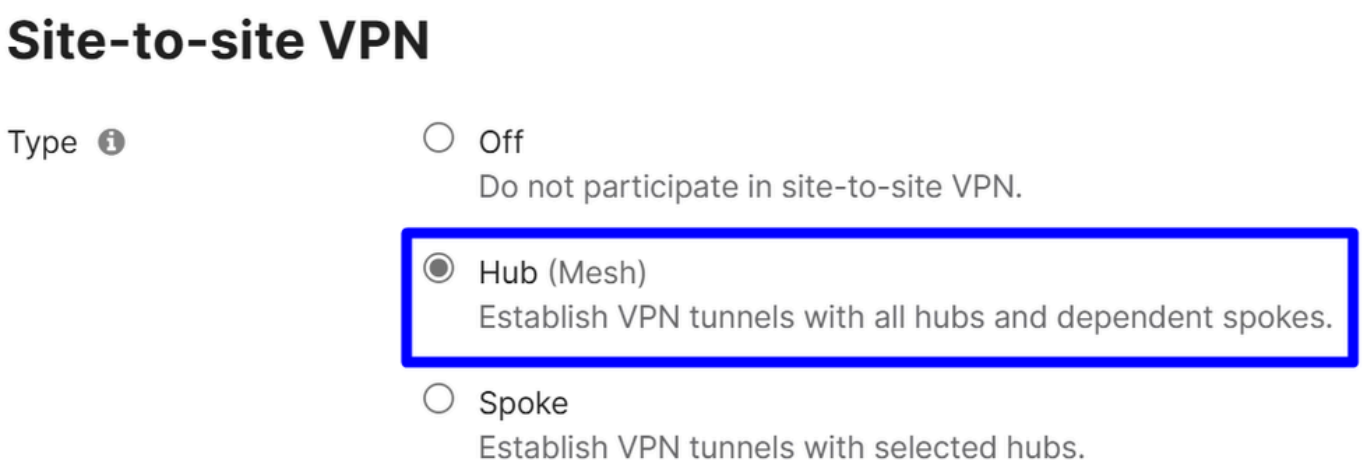
Configurazione della VPN su Meraki MX

Accedere a Meraki MX e fare clic su **Security & SD-WAN** > Site-to-site VPN



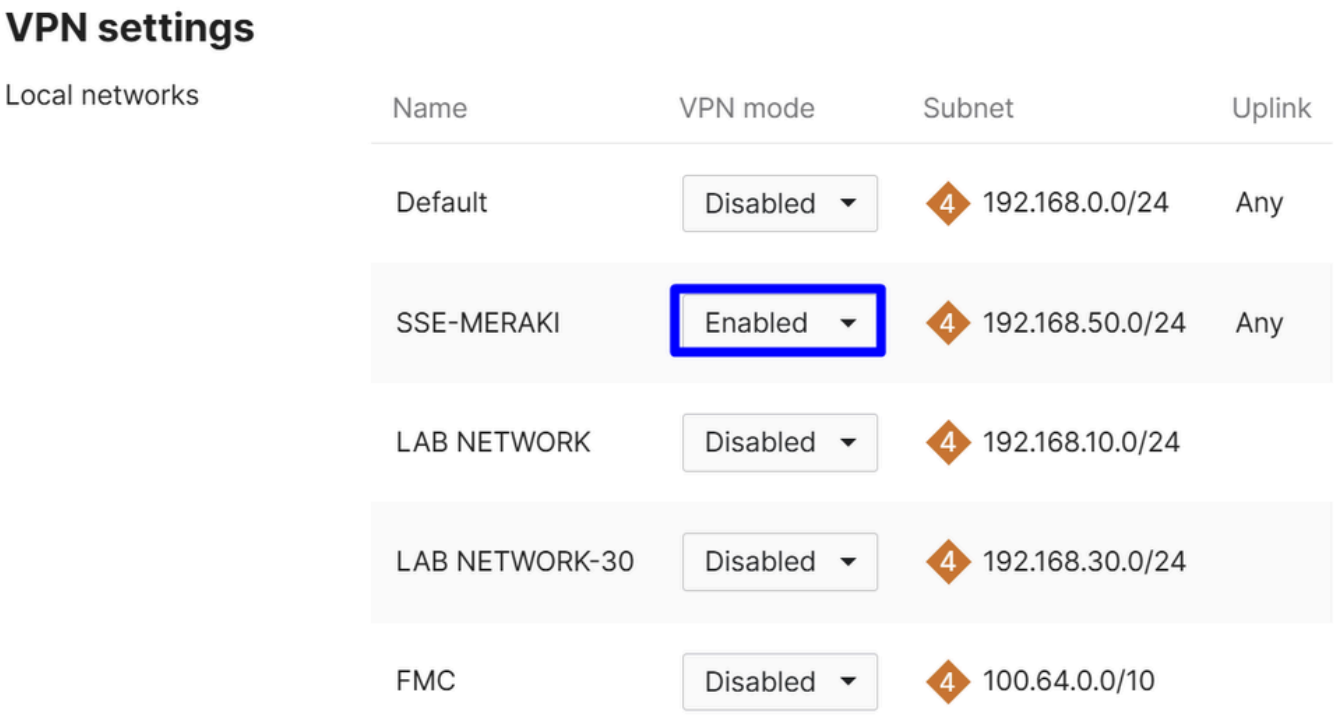
VPN da sito a sito

Scegli Hub.

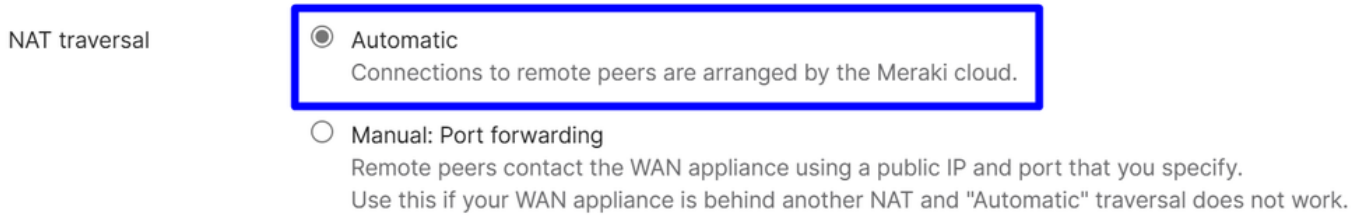


Impostazioni VPN

Scegliere le reti selezionate per l'invio del traffico ad Accesso sicuro:



Scegli in**NAT Traversal**automatico



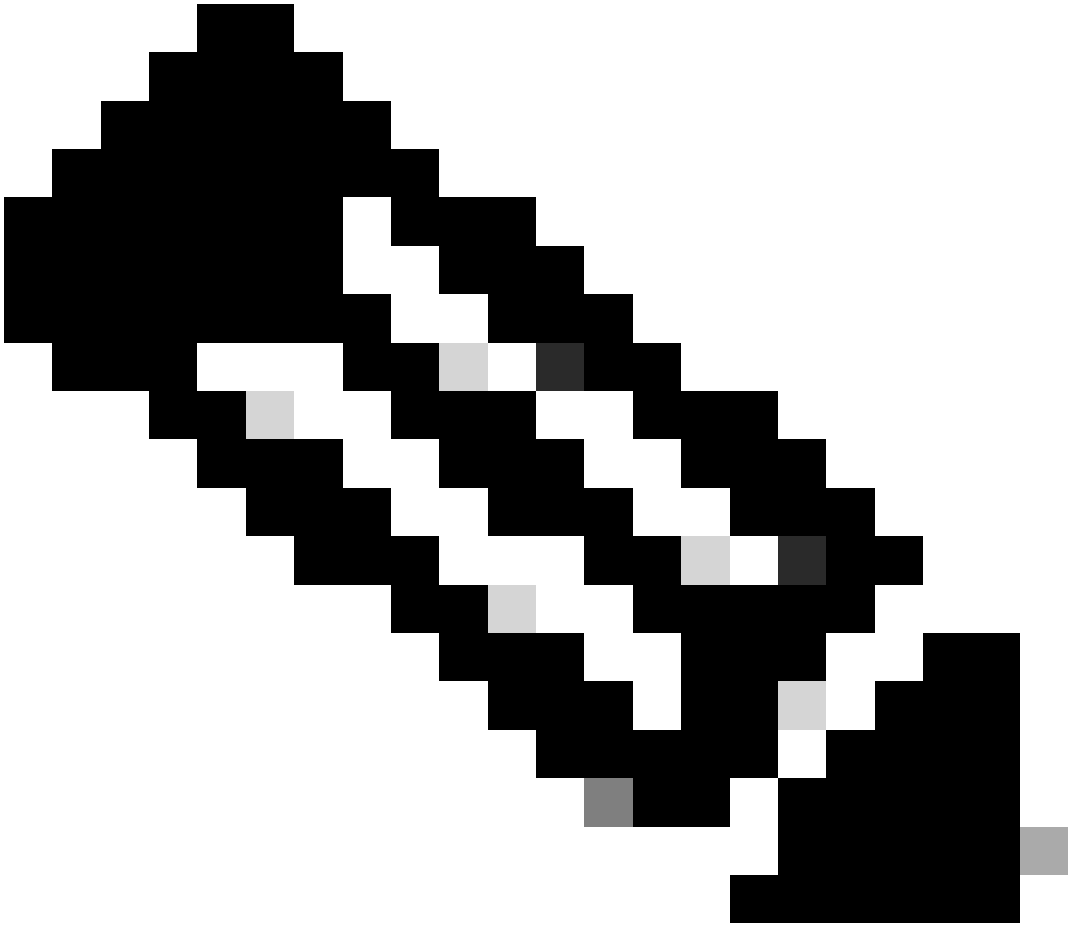
Peer VPN non Meraki

È necessario configurare i controlli di integrità utilizzati da Meraki per instradare il traffico verso Secure Access:

Fare clic su **Configure Health Checks**

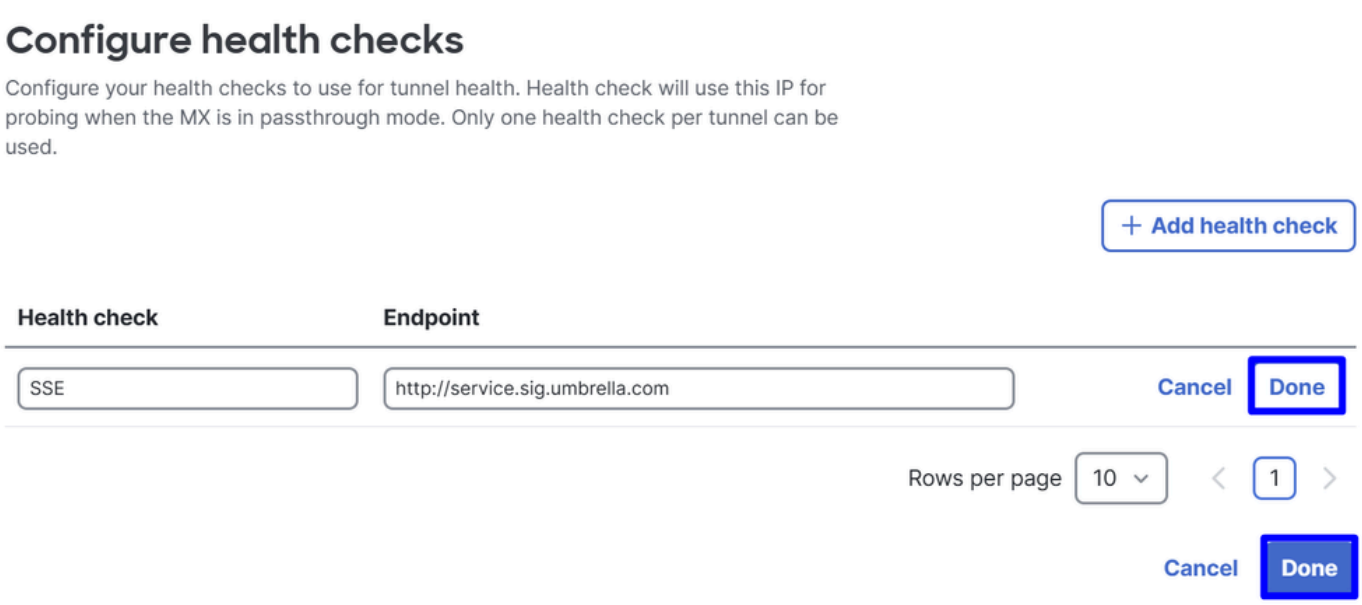
- Fare clic su **+Add health Check**

- **Health Check**: Configurare un nome per il test
- **Endpoint**: Utilizzare quello consigliato da Secure Access http://service.sig.umbrella.com



Nota: Questo dominio risponde solo quando vi si accede tramite un tunnel da sito a sito con Secure Access o Umbrella: i tentativi di accesso dall'esterno di questi tunnel non riescono.

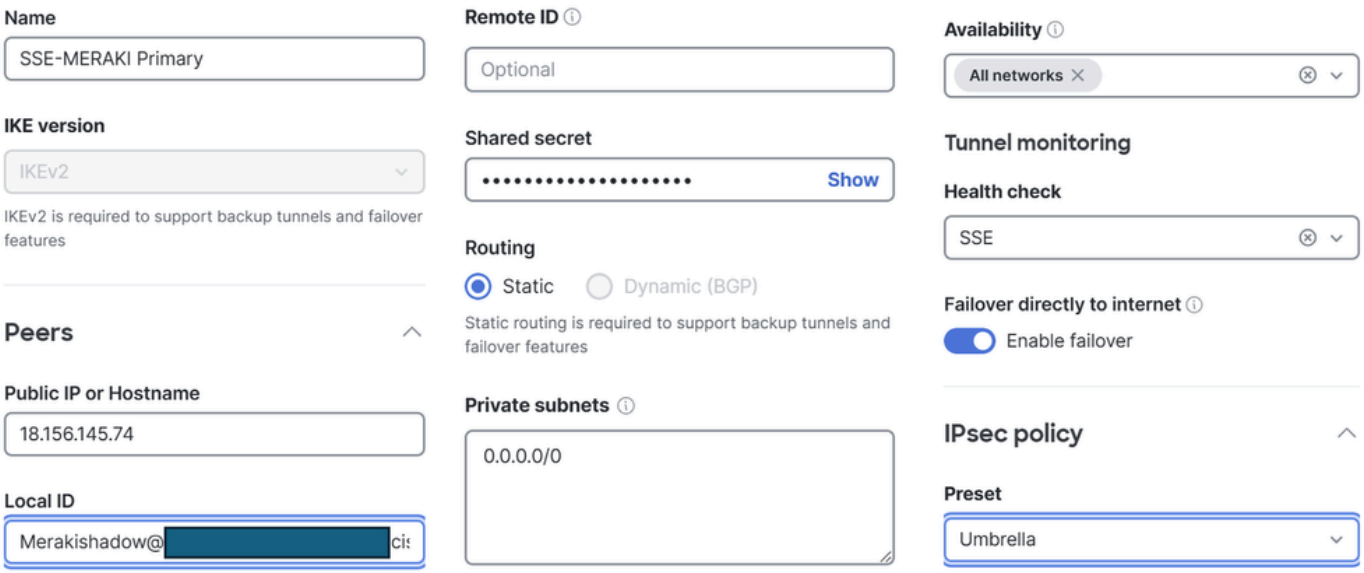
Quindi fare clic **Done** due volte per finalizzare.



Ora i controlli di integrità sono configurati e si è pronti per configurare **Peer:**

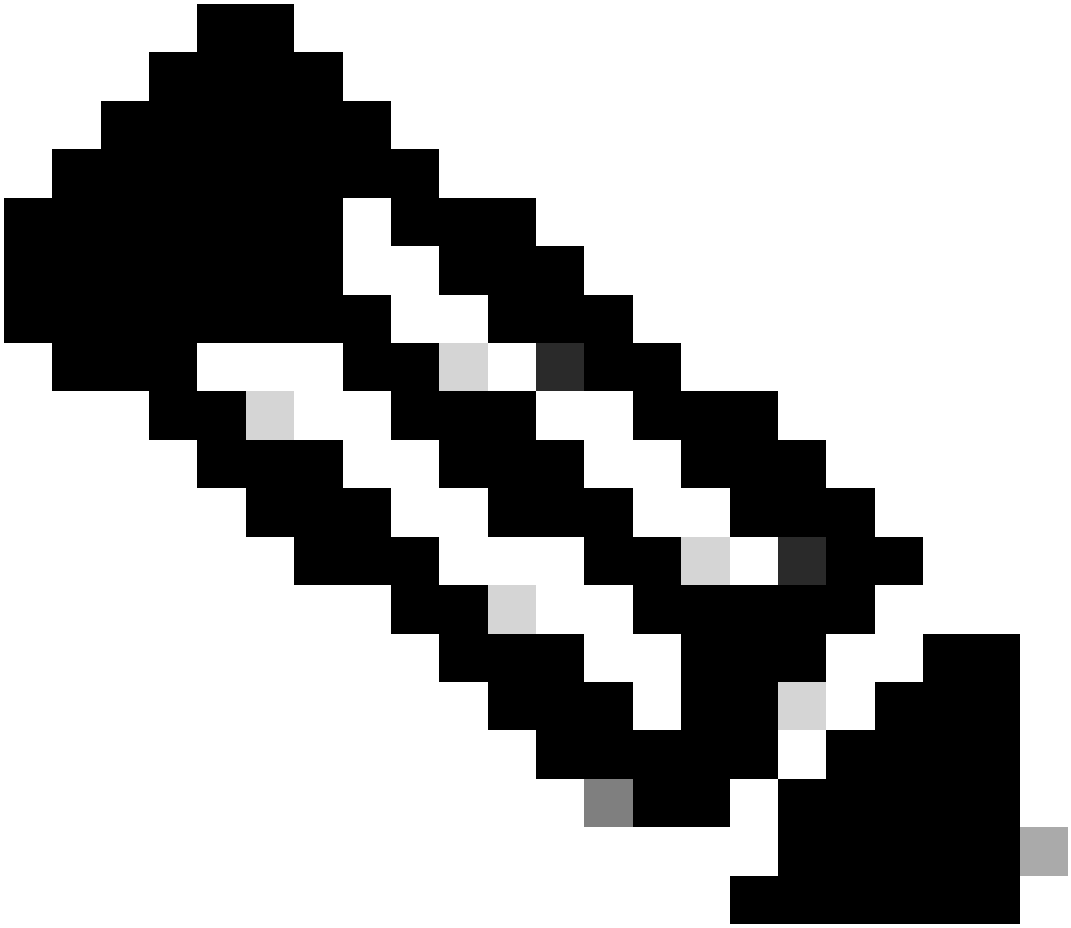
Configura tunnel primario

- Fare clic su+Add a peer



- Aggiungi peer VPN
  - Nome: Configurare un nome per la VPN per l'accesso protetto
  - Versione IKE: Scegli IKEv2
- Peer
  - IP pubblico o nome host: Configurare i **Primary Datacenter IP** dati forniti da Secure Access nel passaggio Configurazioni VPN per l'accesso sicuro
  - ID locale: Configurare i **Primary Tunnel ID** dati forniti da Secure Access nel passaggio Configurazioni VPN per l'accesso sicuro
  - ID remoto: N/D
  - Segreto condiviso: configurare il segreto **Passphrase** fornito da Secure Access nel passo

Configurazioni VPN ad accesso sicuro
    - Instradamento: Scegli statico
    - Subnet private: se si prevede di configurare sia l'accesso a Internet che l'accesso privato, utilizzare **0.0.0.0/0** come destinazione. Se si sta configurando solo l'accesso privato per il tunnel VPN, specificare l'intervallo CGNAT **Remote Access VPN IP Pool** e l'intervallo CGNAT **100.64.0.0/10** come reti di destinazione
    - Disponibilità: se si dispone di un solo dispositivo Meraki, è possibile selezionare **All Networks**. Se si hanno più dispositivi, assicurarsi di selezionare solo la rete Meraki specifica su cui si sta configurando il tunnel.
- Monitoraggio tunnel
    - Controllo dello stato: Usa il controllo dello stato configurato in precedenza per monitorare la disponibilità del tunnel
    - Failover diretto su Internet:se si abilita questa opzione e i controlli di integrità del tunnel 1 e del tunnel 2 hanno esito negativo, il traffico viene reindirizzato all'interfaccia WAN per impedire la perdita dell'accesso a Internet.



Failover directly to InternetFunzionalità di verifica dello stato:se il tunnel 1 viene monitorato e il

---

controllo dello stato ha esito negativo, il traffico viene automaticamente indirizzato al tunnel 2. Se anche il tunnel 2 ha esito negativo e l'opzione è abilitata, il traffico viene indirizzato tramite l'interfaccia WAN del dispositivo Meraki.

- criterio IPSec
  - Preimpostato: Scegli **Umbrella**

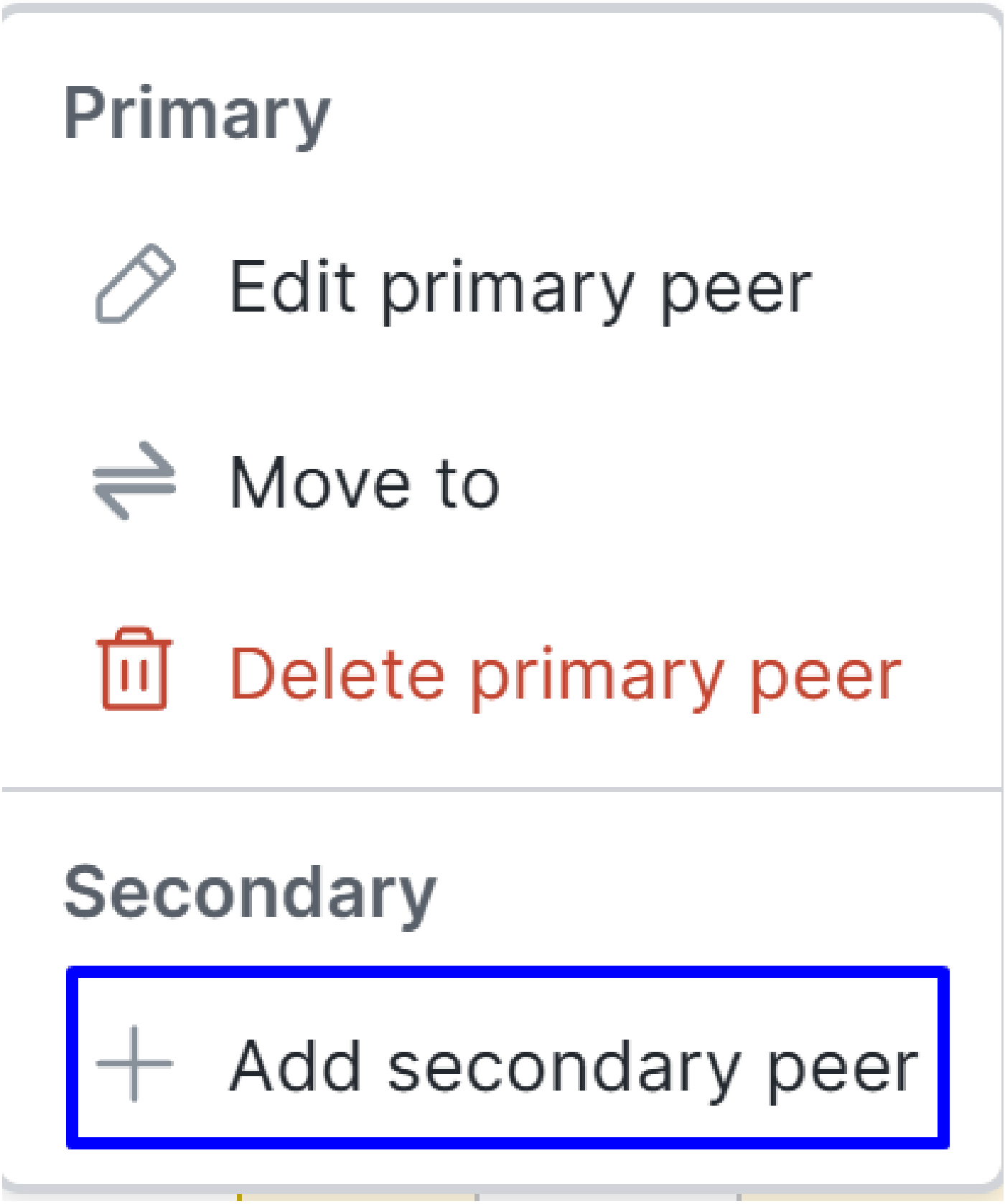
Quindi fate clic su **Save**.

Configura tunnel secondario

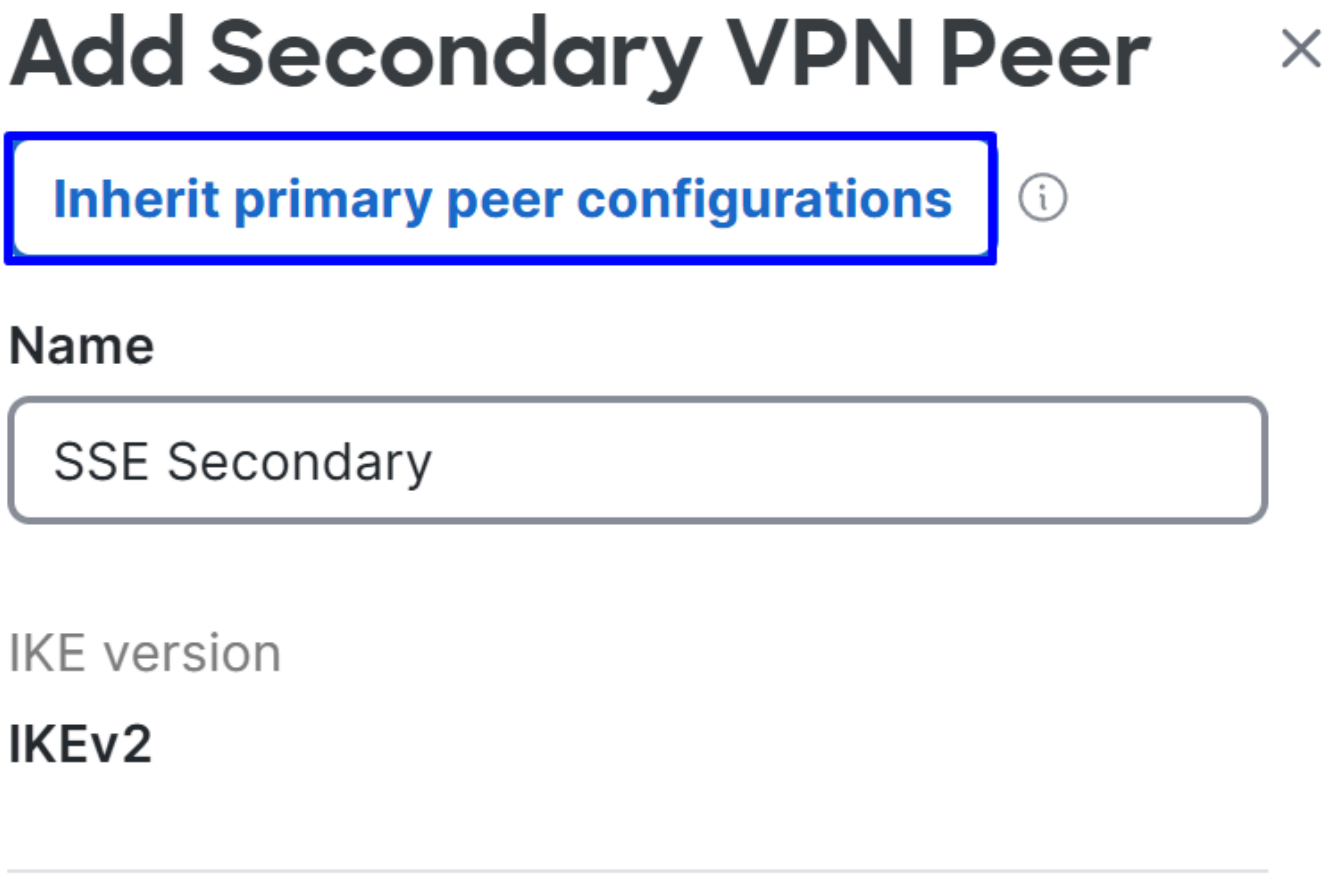
Per configurare il tunnel secondario, fare clic sul menu opzioni del tunnel primario:

- Fare clic sui tre punti

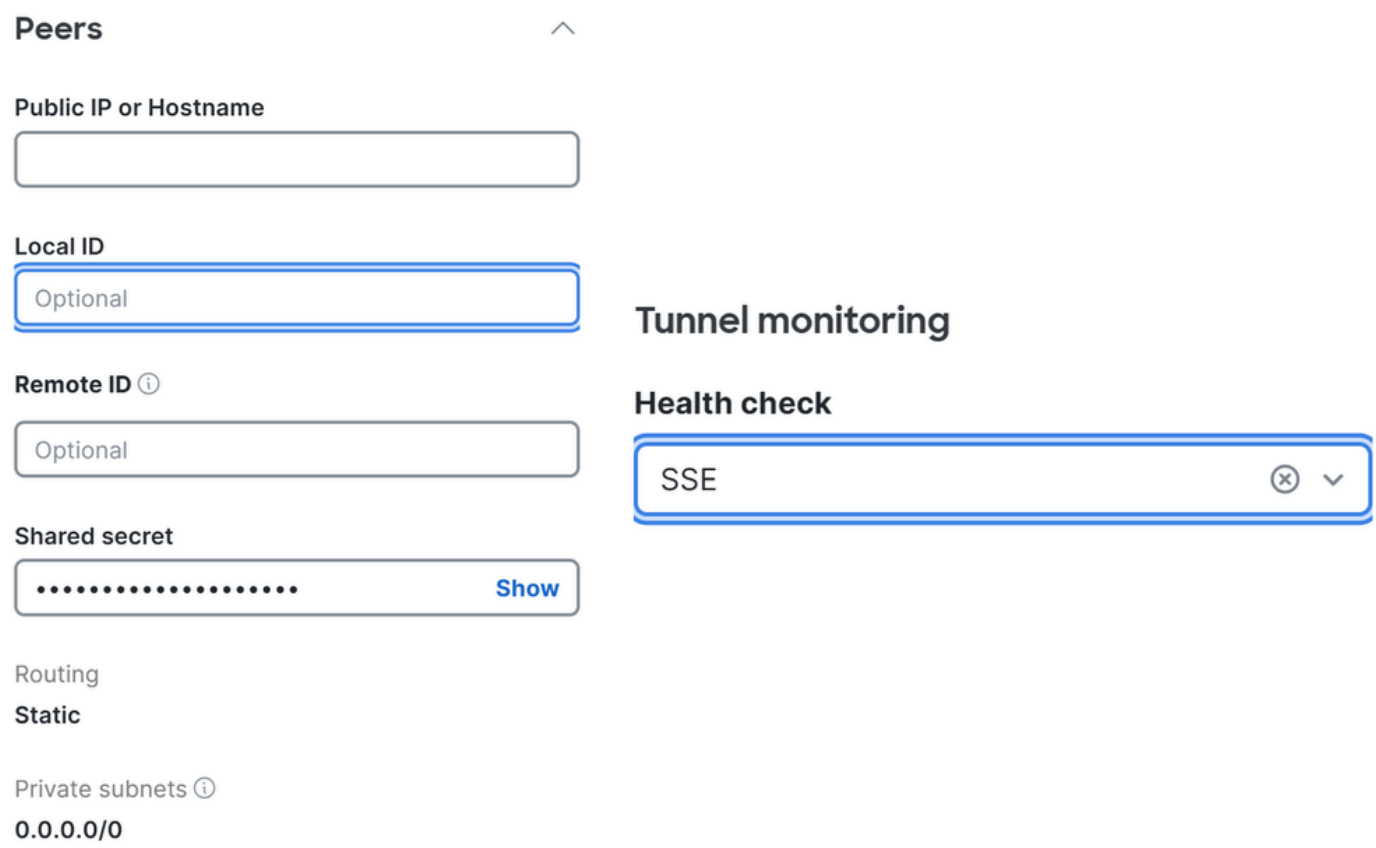
- Fare clic su + Add Secondary peer



- Fare clic suInherit primary peer configurations

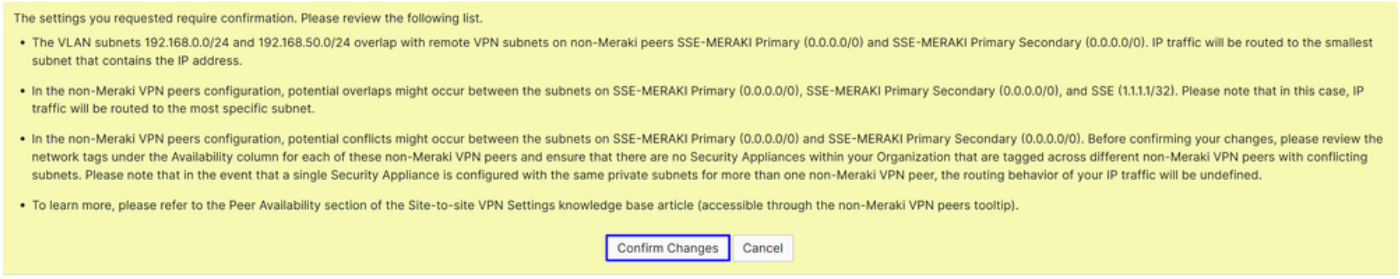


Si noterà che alcuni campi vengono compilati automaticamente. Esaminatele, apportate le modifiche necessarie e completate il resto manualmente:



- Peer
  - IP pubblico o nome host: Configurare i **Secondary Datacenter IP** dati forniti da Secure Access nel passaggio Configurazioni VPN per l'accesso sicuro
  - ID locale: Configurare i **Secondary Tunnel ID** dati forniti da Secure Access nel passaggio Configurazioni VPN per l'accesso sicuro
  - ID remoto: N/D
  - Segreto condiviso: configurare il segreto **Passphrase** fornito da Secure Access nel passo Configurazioni VPN ad accesso sicuro
- Monitoraggio tunnel
  - Controllo dello stato: Usa il controllo dello stato configurato in precedenza per monitorare la disponibilità del tunnel

Quindi fare clic su **Save**e viene visualizzato l'avviso successivo:

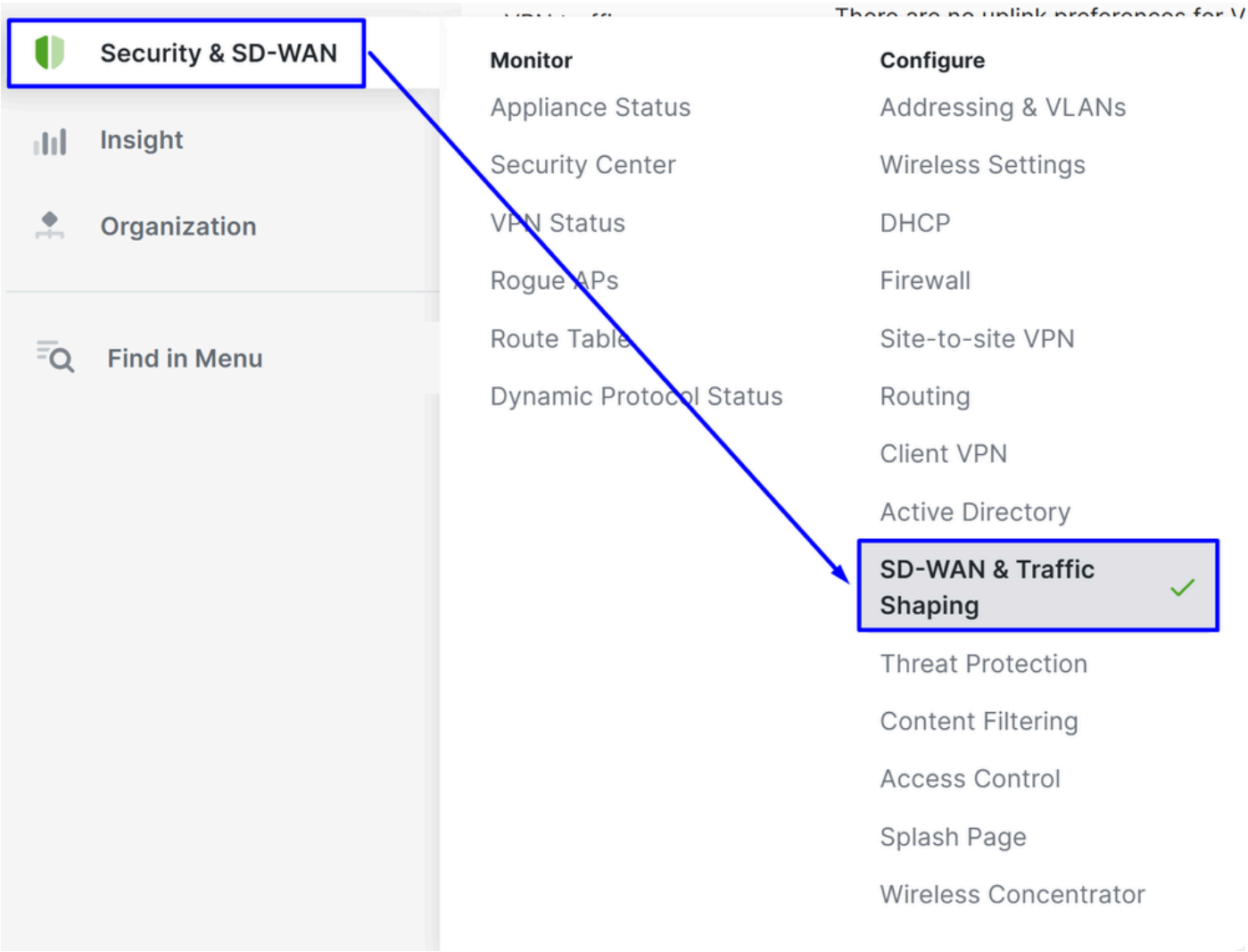


Non preoccupatevi e fate clic **Confirm Changes**.

Configura direzione traffico (Tunnel Traffic Bypass)

Questa funzione consente di ignorare il traffico specifico dal tunnel definendo i domini o gli indirizzi IP nella configurazione SD-WAN Bypass:

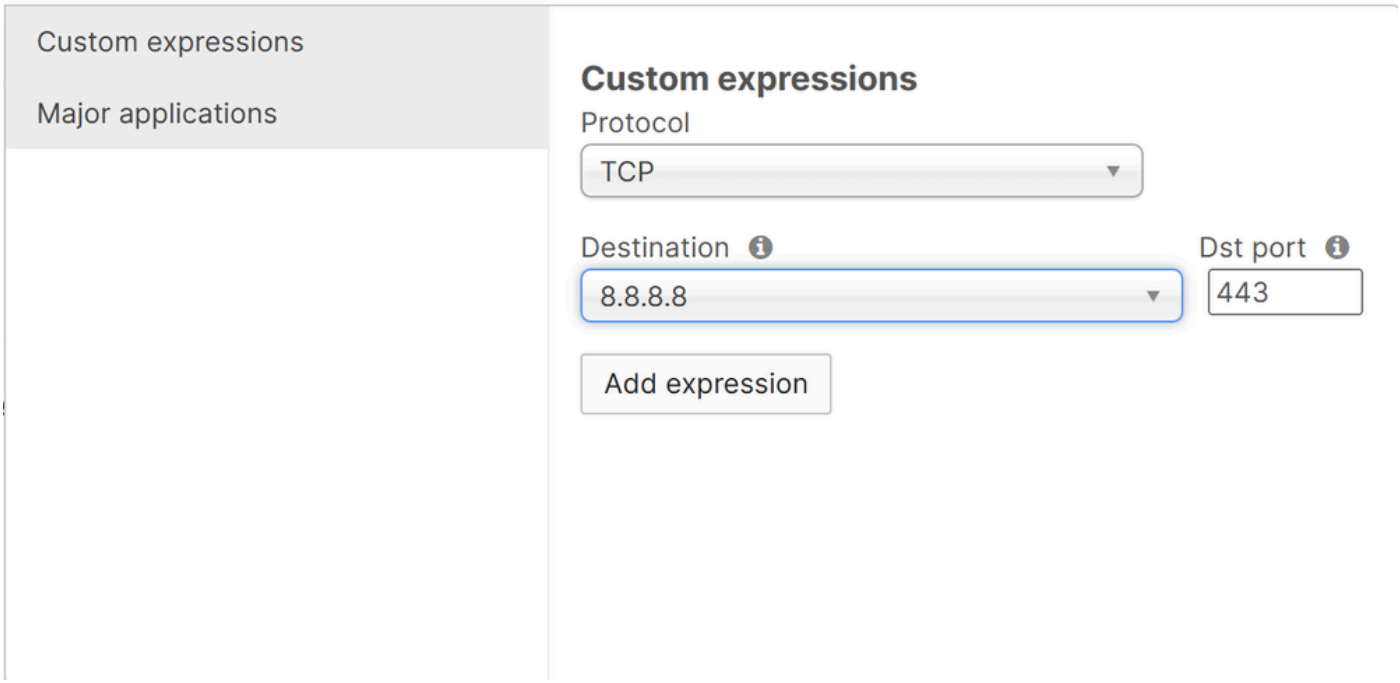
- Passare a **Security & SD-WAN** > SD-WAN & Traffic Shaping



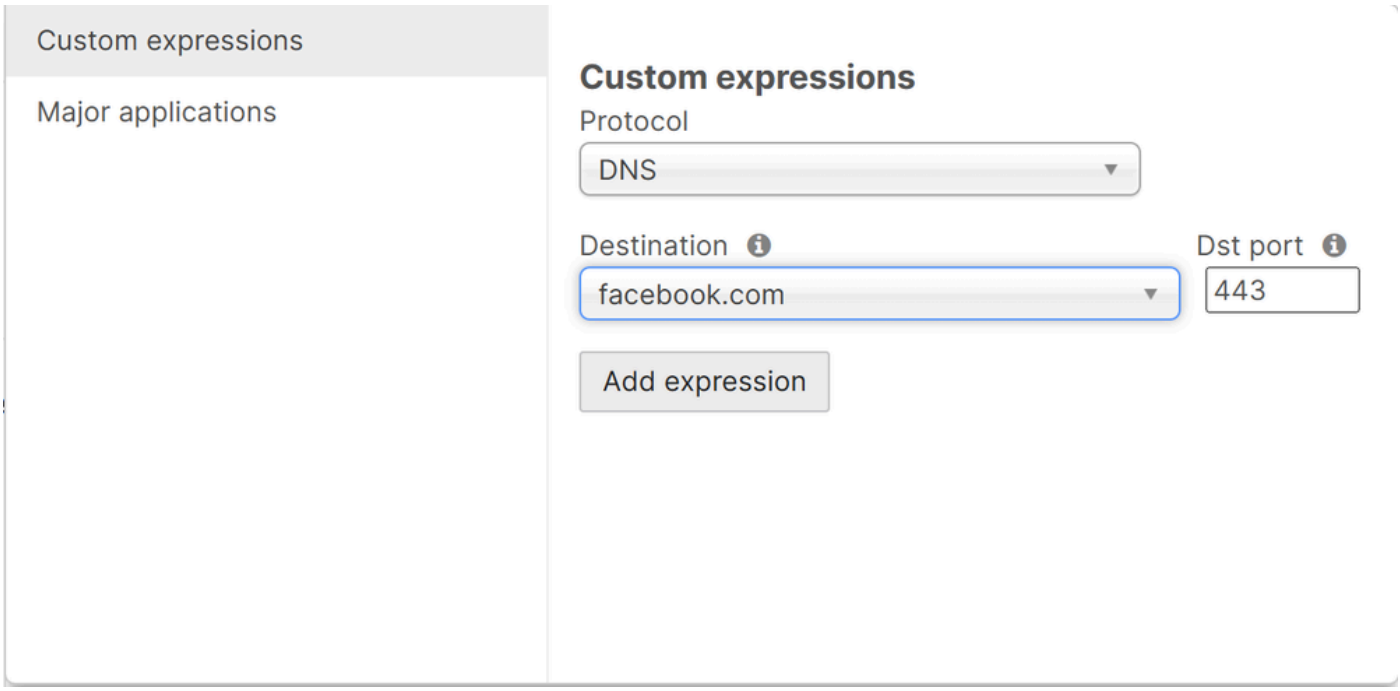
- Scorrere fino alla **Local Internet Breakout** sezione e fare clic su **Add+**

Creare quindi il bypass in base a **Custom Expressions** o **Major Applications**:

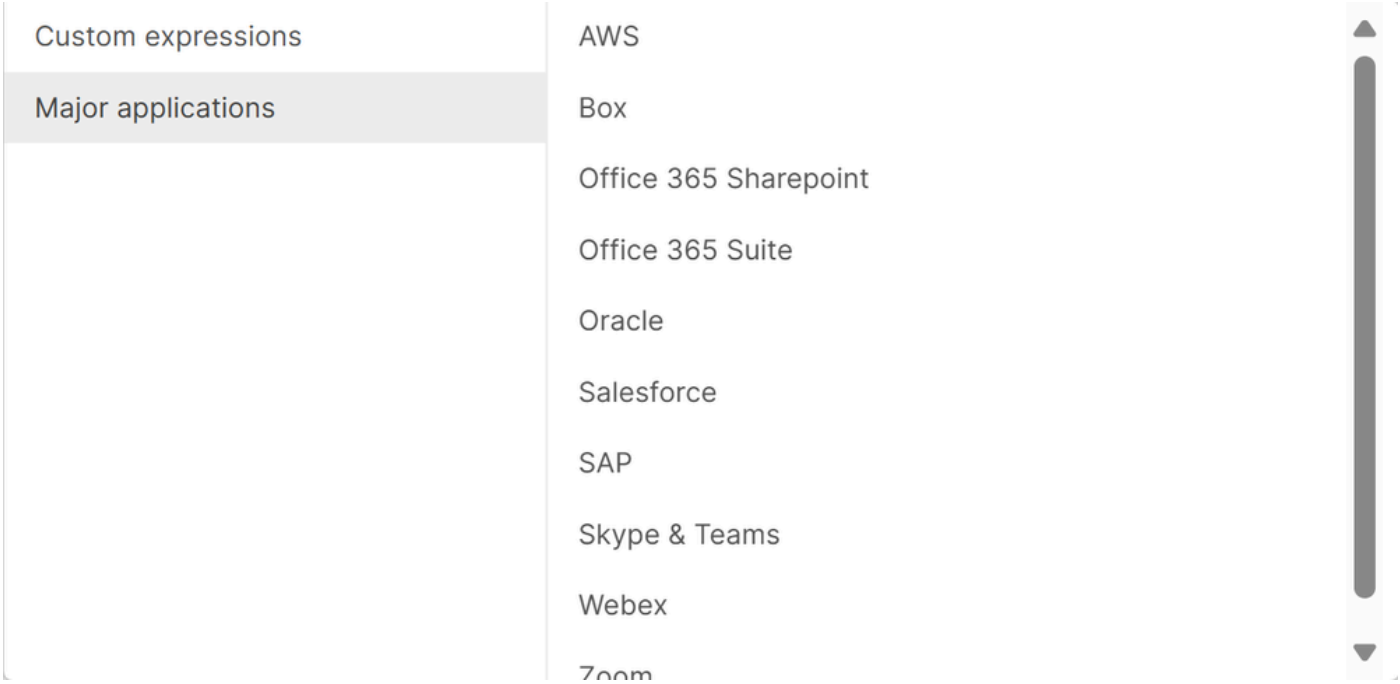
Custom Expressions - Protocol



Custom Expressions - DNS



Major Applications

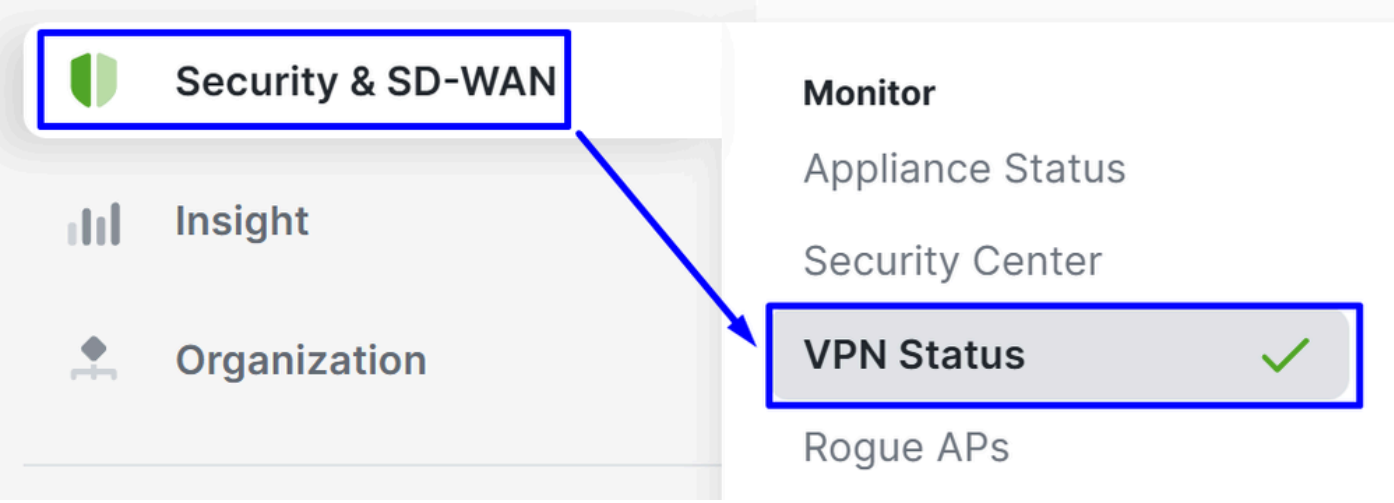


Per ulteriori informazioni, visitare: [Configurazione delle regole di esclusione VPN (IP/Porta/DNS/APP)]

Verifica

Per verificare se i tunnel sono attivi, verificare lo stato in:

- Fare clic suSecurity & SD-WAN**> VPN Status** sul dashboard Meraki.



- Fare clic su 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				

Se lo stato della VPN primaria e secondaria è visualizzato in verde, i tunnel sono attivi e attivi.

Meraki VPN Status Codes

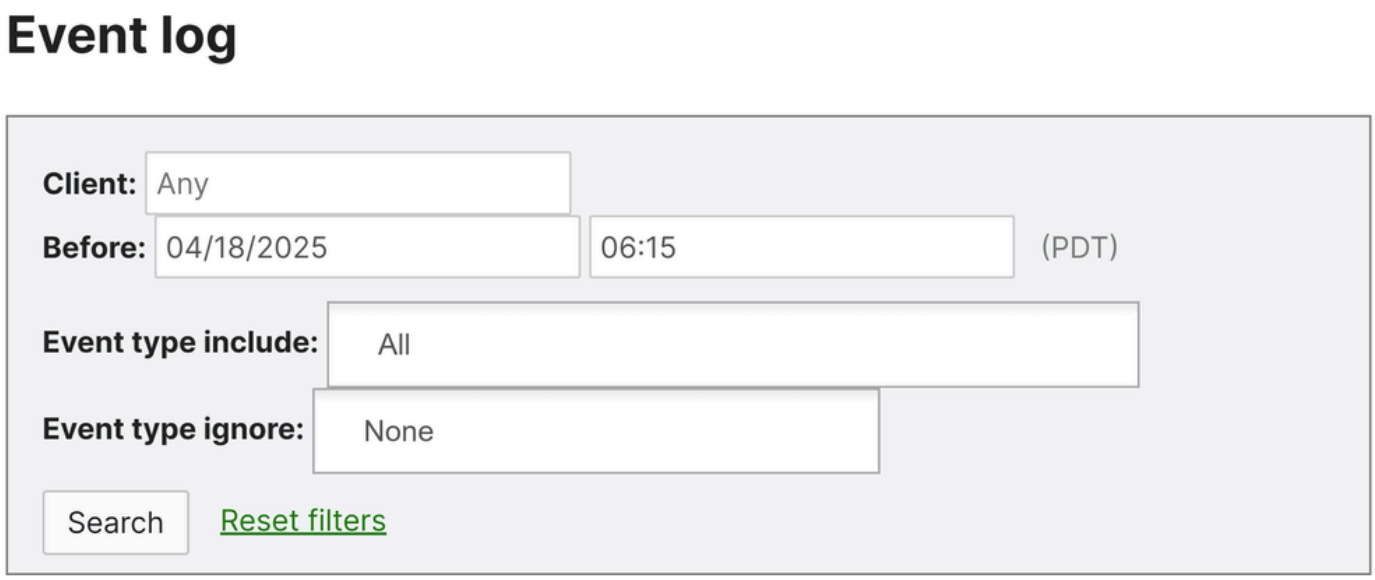
Status Indicator	Color	Meaning
Primary/Secondary Up	Green	Phase 1 and phase 2 are up
Partial Connectivity	Amber	Phase 1 is up but phase 2 is down
Tunnel Down	Red	Phase 1 and phase 2 are both down

Risoluzione dei problemi

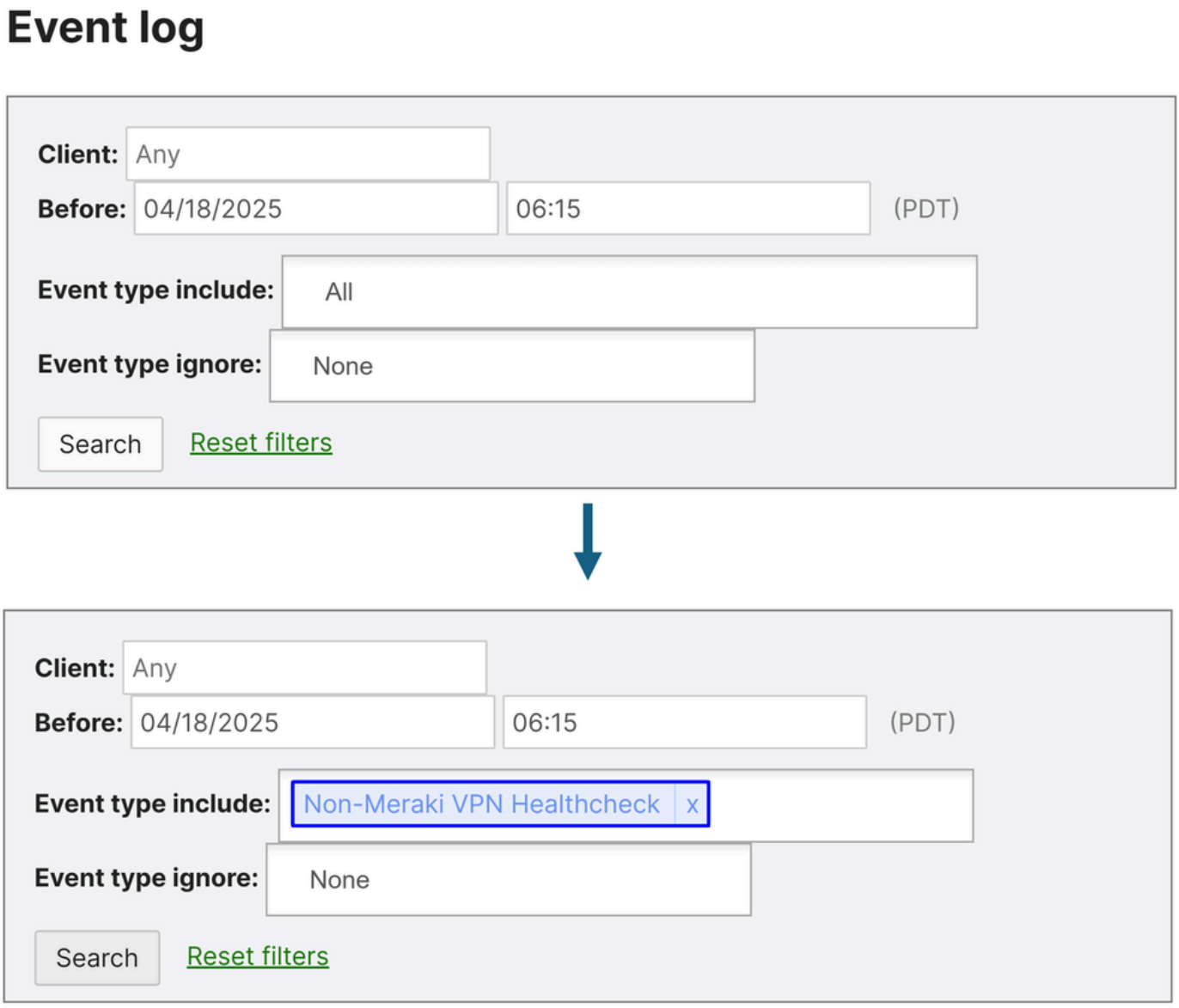
Verifica controlli di integrità

Per verificare il corretto funzionamento dei controlli di integrità Meraki per la VPN, passare a:

- Fate clic su > (On **Assurance**) Event Log

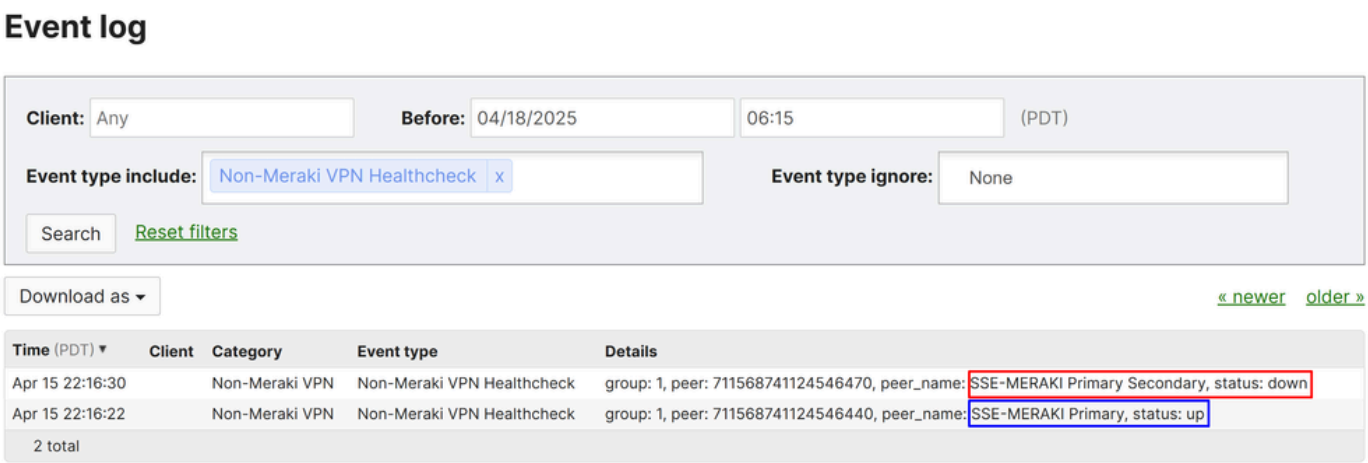


In, **Event Type Include**scegliere Non-Meraki VPN Healthcheck



Quando il tunnel primario per Cisco Secure Access è attivo, i pacchetti in arrivo attraverso il tunnel secondario vengono scartati per mantenere un percorso di routing coerente.

Il tunnel secondario rimane in standby e viene utilizzato solo se si verifica un guasto sul tunnel primario, dal lato Meraki o in Secure Access, come determinato dal meccanismo di controllo dello stato.



- Il controllo di integrità del tunnel primario mostra lo stato: , ovvero sta passando e inoltrando attivamente il traffico.
- Il controllo di integrità del tunnel secondario mostra lo stato: inattivo, non perché il tunnel non sia disponibile, ma perché il sistema primario è integro e in uso. Questo comportamento è previsto, in quanto il traffico può passare solo attraverso il tunnel 1 e il controllo dello stato del tunnel secondario ha esito negativo.

Informazioni correlate

- Supporto tecnico Cisco e download
- Cisco Secure Access Help Center
- Guida alla configurazione di Cisco Secure Access Meraki BGP

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).