

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

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurare la VPN su accesso sicuro](#)

[Configurazione VPN ad accesso sicuro](#)

[Configurazione della VPN su Meraki MX](#)

[VPN da sito a sito](#)

[Impostazioni VPN](#)

[Peer VPN non Meraki](#)

[Configura tunnel primario](#)

[Configura tunnel secondario](#)

[Configura direzione traffico \(Tunnel Traffic Bypass\)](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Verifica controlli di integrità](#)

[Informazioni correlate](#)

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



CISCO

Meraki

Cisco Meraki MX

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

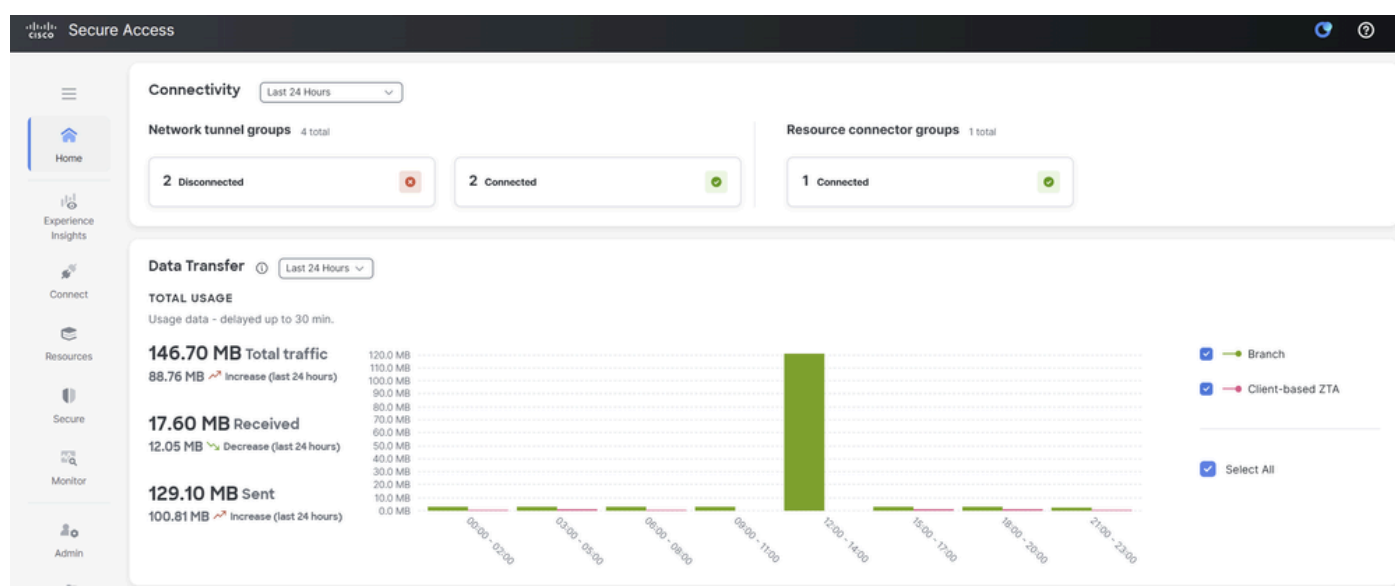
basate su Internet con l'applicazione di policy nel cloud.

- 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.

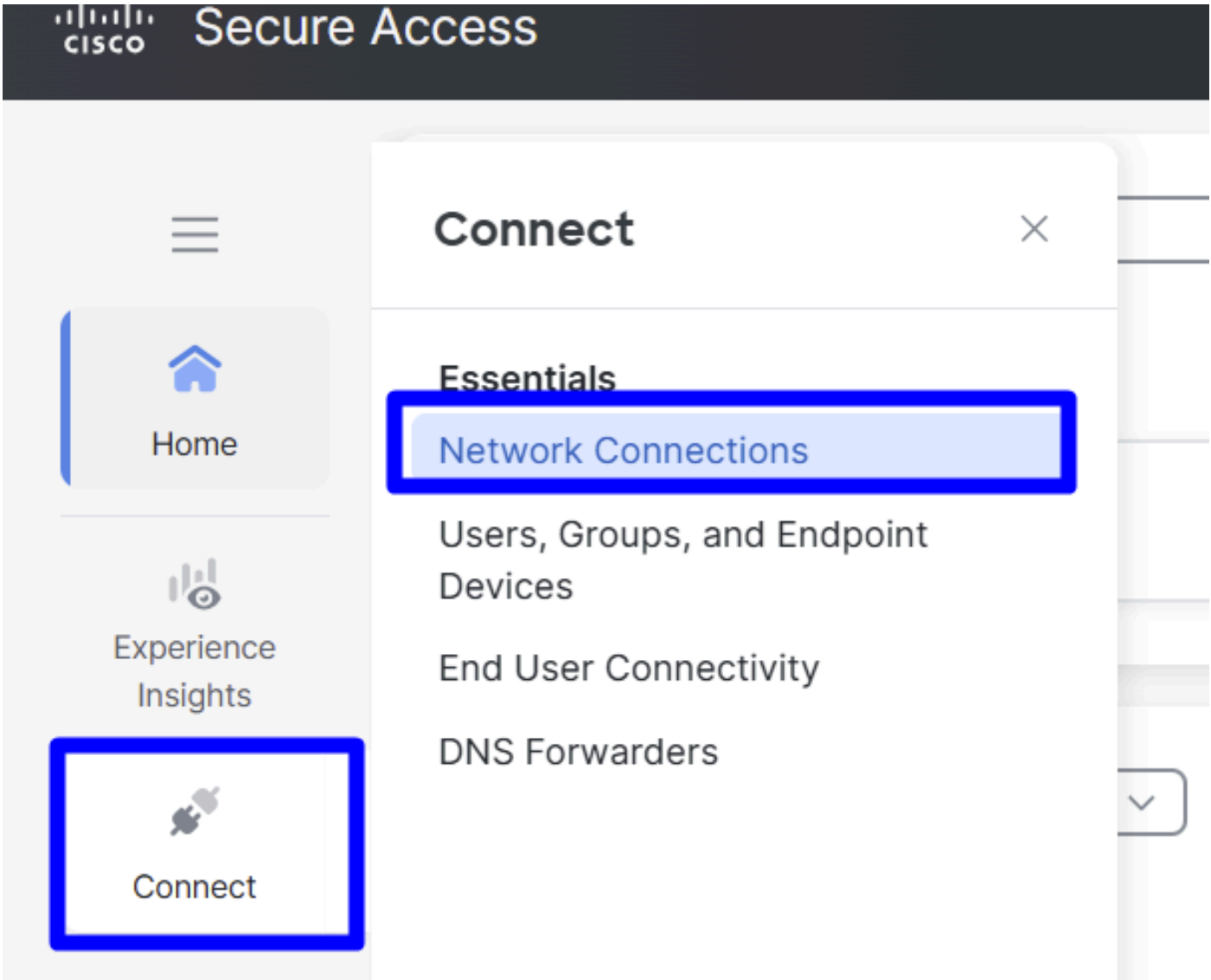
Configurazione

Configurare la VPN su accesso sicuro

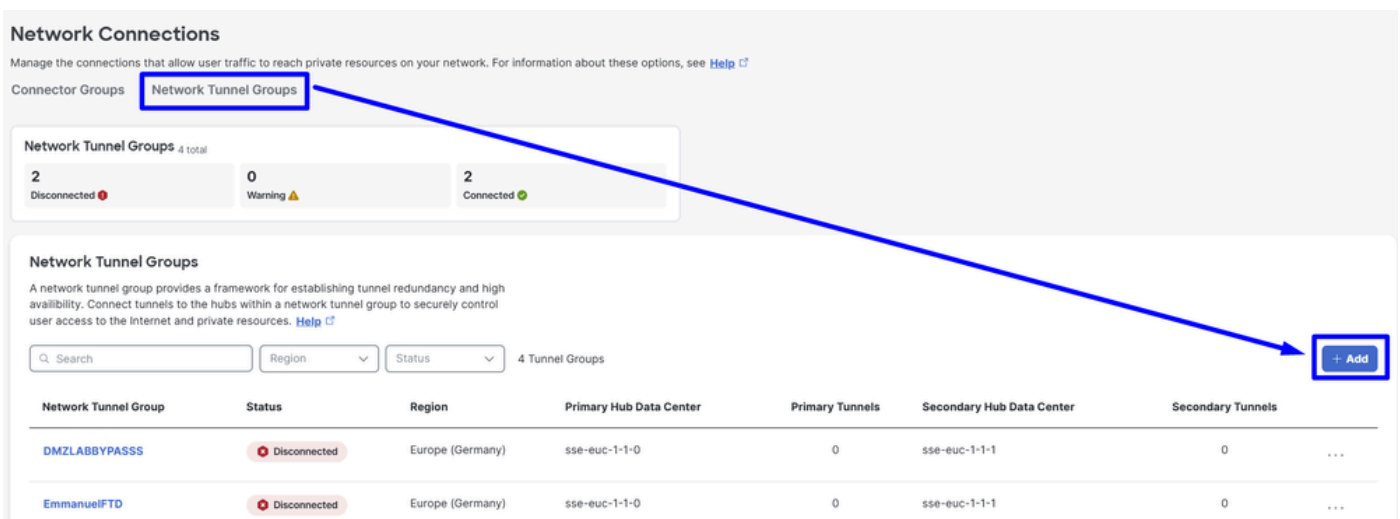
Passare al pannello di amministrazione di [Accesso sicuro](#).



- Fare clic su Connect > Network Connections



- In fareNetwork Tunnel Groups clic su + Add



- Configurazione Tunnel Group Name, Region e Device Type
- Fare clic su Next

General Settings

Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.

Tunnel Group Name
MERAKEI

Region
Europe (Germany)

Device Type
Meraki MX

Cancel Next

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

Tunnel ID and Passphrase

Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.

Tunnel ID
MerakiShadow @<org><hub>.sse.cisco.com

Passphrase
.....

The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

Confirm Passphrase
.....

Cancel Back 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

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

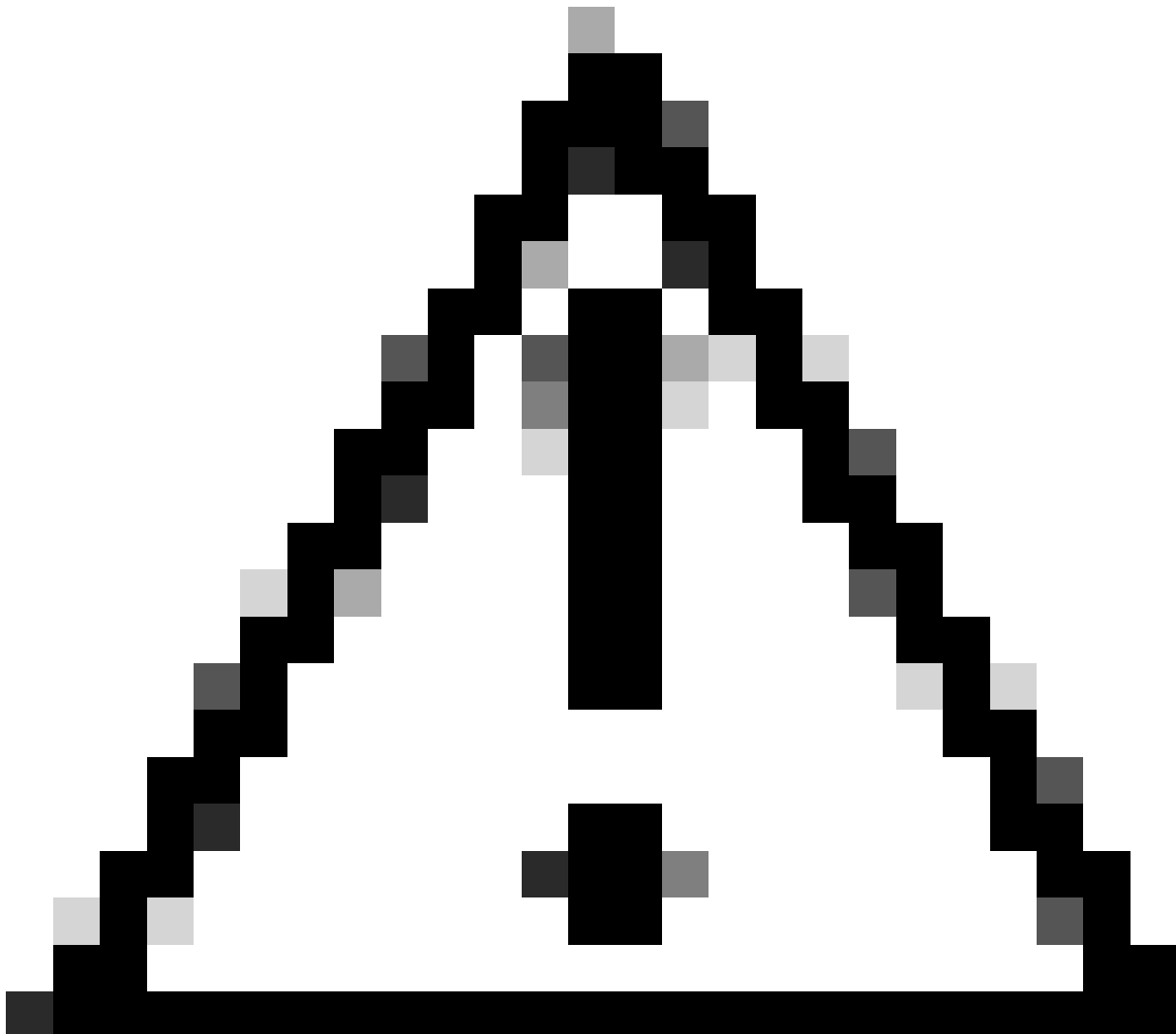


Cancel

Back

Save

Meraki MX Probe IP



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

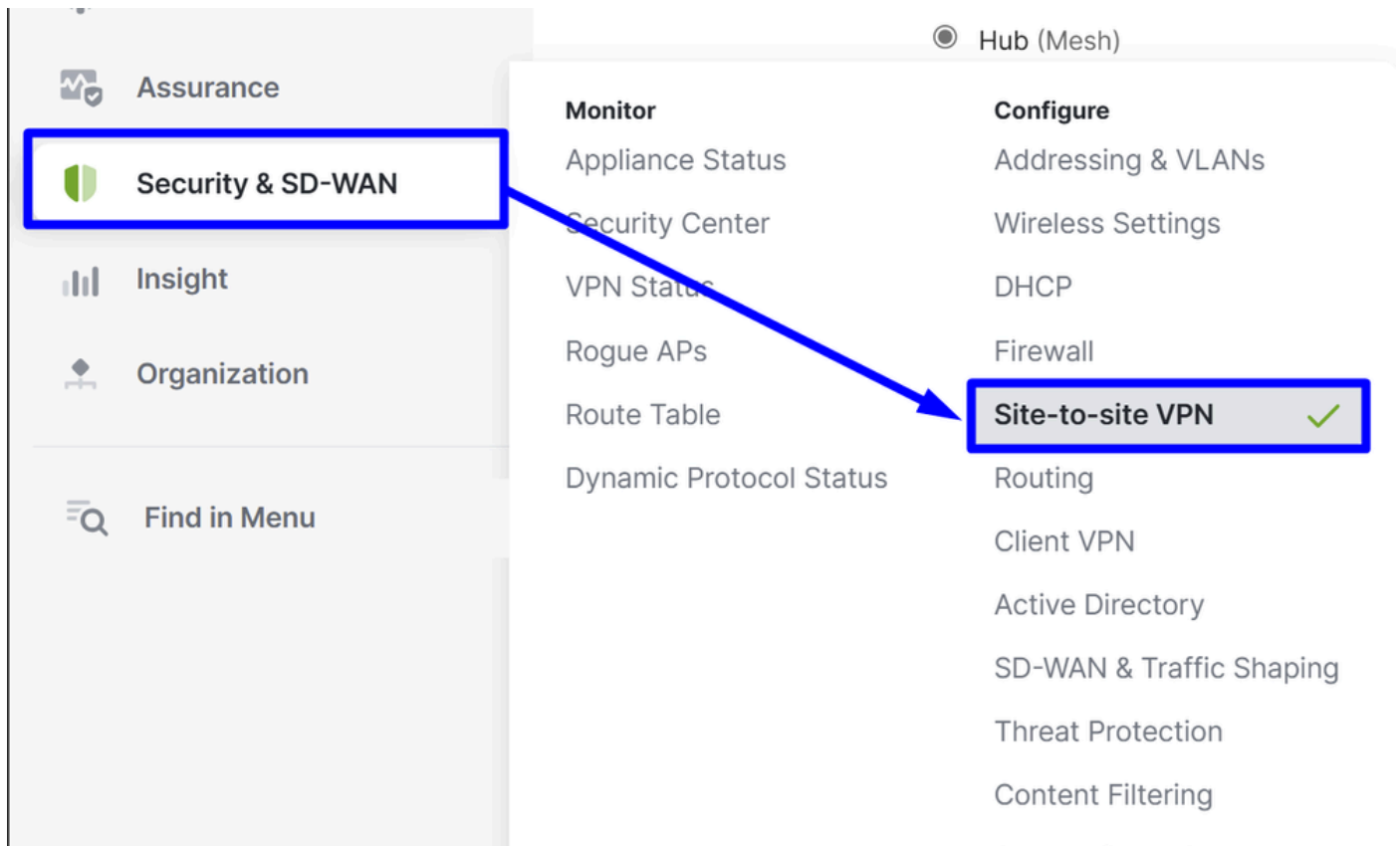
Copiare la configurazione dei tunnel in un blocco note. Utilizzare queste informazioni per completare la configurazione in Meraki **Non-Meraki VPN Peers**.

The screenshot shows the 'Data for Tunnel Setup' configuration page in the Meraki MX interface. On the left, a sidebar contains four menu items: 'General Settings', 'Tunnel ID and Passphrase', 'Routing', and 'Data for Tunnel Setup' (which is currently selected and highlighted with a blue bar). 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: 'Primary Tunnel ID' with the value 'MerakiShadow@' followed by a redacted field; 'Primary Data Center IP Address' with the value '18.156.145.74'; 'Secondary Tunnel ID' with the value 'MerakiShadow@' followed by a redacted field; and 'Secondary Data Center IP Address' with the value '3.120.45.23'. Each field has a small square icon to its right. At the bottom right of the page, there are two buttons: 'Download CSV' and 'Done'.

Data for Tunnel Setup	
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

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.

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.

Impostazioni VPN

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

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	

Scegli in NAT Traversal automatico

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.

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**

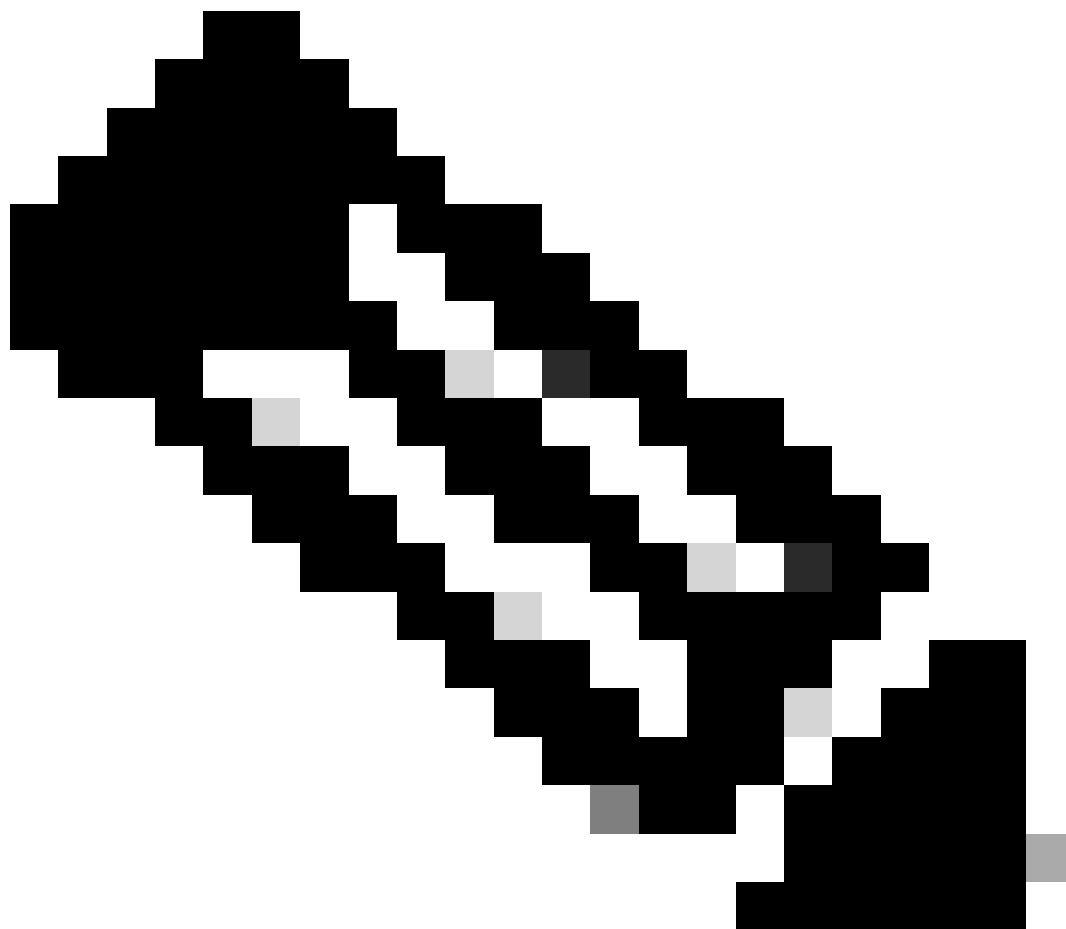
- Fare clic su **+Add health Check**

Health check

Endpoint

	http://	Cancel Done
 Health check name can't be blank.		

- 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.

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	
SSE	http://service.sig.umbrella.com	Cancel Done

Rows per page < >

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

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

Configura tunnel primario

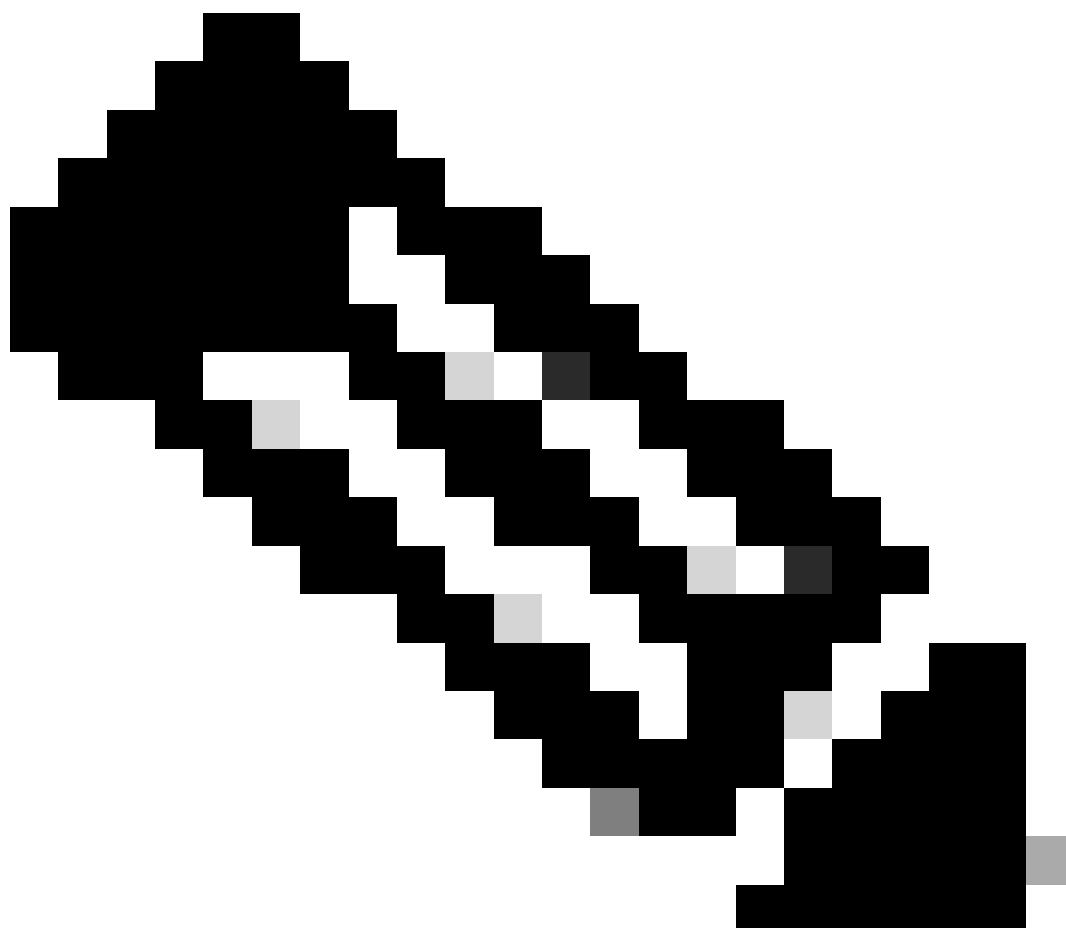
- Fare clic su [+Add a peer](#)

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

- 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.
-



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

#	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 >

- Fare clic su **+** Add Secondary peer

Primary



Edit primary peer



Move to



Delete primary peer

Secondary



Add secondary peer

- Fare clic su `Inherit` primary peer configurations

Add Secondary VPN Peer



Inherit primary peer configurations



Name

SSE Secondary

IKE version

IKEv2

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

Peers



Public IP or Hostname

Local ID

Remote ID ⓘ

Shared secret

 [Show](#)

Tunnel monitoring

Health check

 ⓘ ▼

Routing

Static

Private subnets ⓘ

0.0.0.0/0

- 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** viene visualizzato l'avviso successivo:

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](#)

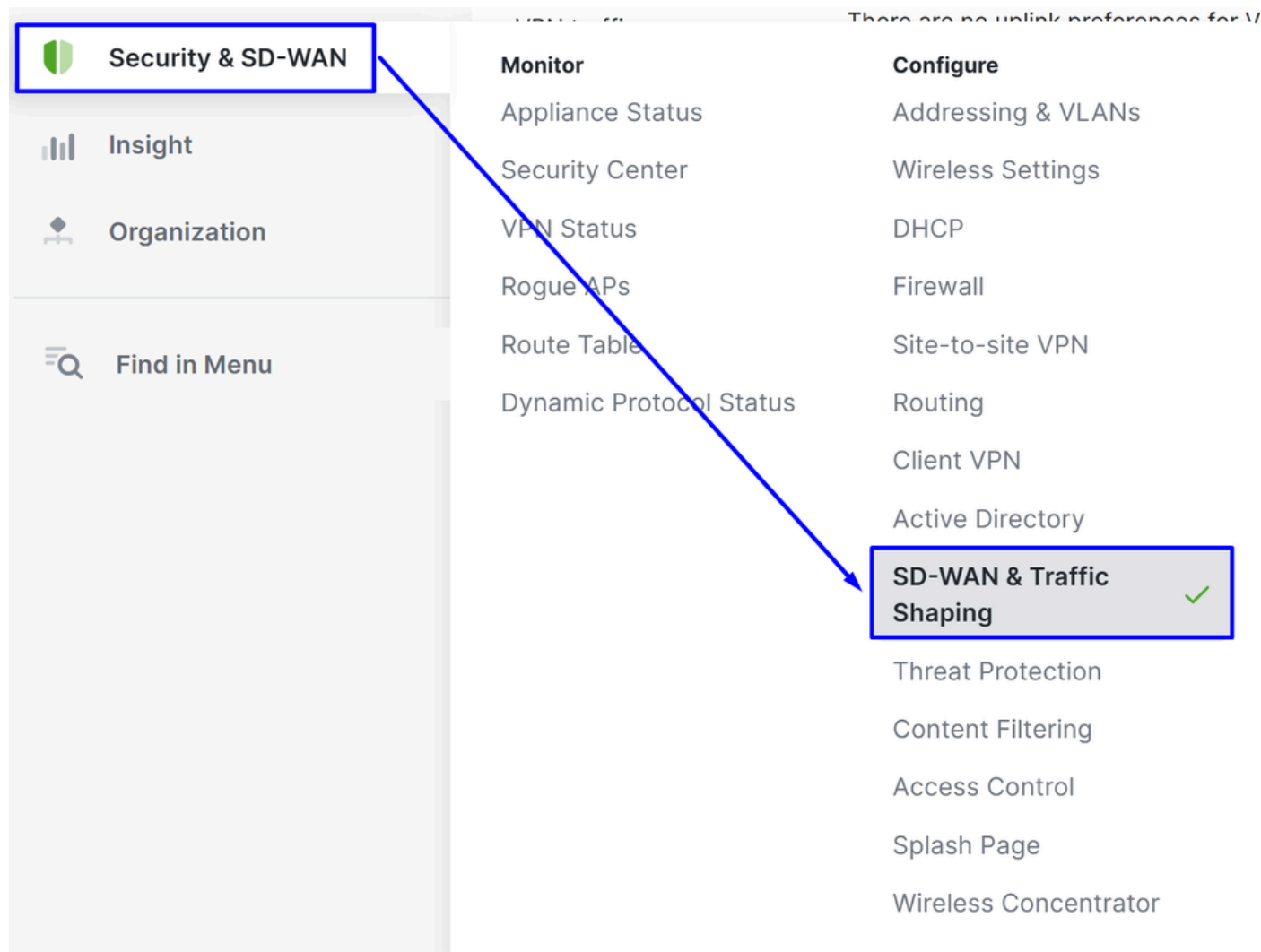
[Cancel](#)

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+**

Local internet breakout

VPN exclusion rules

Add +

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

Custom Expressions - Protocol

Custom expressions	Custom expressions	
Major applications	Protocol	
	TCP	
	Destination ⓘ	Dst port ⓘ
	8.8.8.8	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

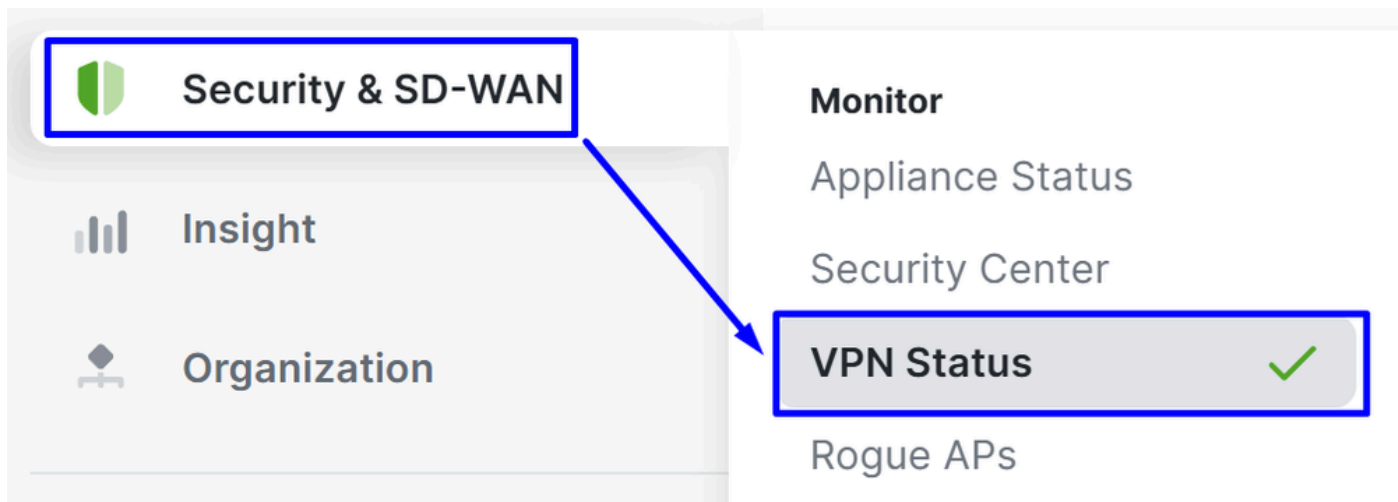
Zoom

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 su **Security & 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

Event log

Client:

Before: (PDT)

Event type include:

Event type ignore:

[Reset filters](#)

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

Event log

Client:

Any

Before:

04/18/2025

06:15

(PDT)

Event type include:

All

Event type ignore:

None

Search

[Reset filters](#)



Client:

Any

Before:

04/18/2025

06:15

(PDT)

Event type include:

Non-Meraki VPN Healthcheck x

Event type ignore:

None

Search

[Reset filters](#)

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.

Event log

Client:

Any

Before:

04/18/2025

06:15

(PDT)

Event type include:

Non-Meraki VPN Healthcheck x

Event type ignore:

None

Search

[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				

- 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).