

# Configure o acesso seguro com o Meraki MX para alta disponibilidade e monitoramento de integridade

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configurar a VPN no acesso seguro](#)

[Configuração de VPN de acesso seguro](#)

[Configurar a VPN no Meraki MX](#)

[VPN site a site](#)

[Configurações de VPN](#)

[Pares VPN não Meraki](#)

[Configurar túnel primário](#)

[Configurar túnel secundário](#)

[Configurar o tráfego direcionado \(desvio de tráfego de túnel\)](#)

[Verificar](#)

[Troubleshooting](#)

[Verificar as Verificações de Integridade](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve como configurar o Cisco Secure Access com Meraki MX para alta disponibilidade usando verificações de integridade.

## Pré-requisitos

- [Revisar os requisitos de túnel IPsec com acesso seguro](#)
- Compreender os componentes de acesso seguro
- [Compreenda a funcionalidade de verificação de integridade no Meraki MX](#)

## Requisitos

- O Meraki MX deve estar executando a versão do firmware 19.7.1 ou posterior
- Ao usar o acesso privado, somente um túnel é suportado devido a uma limitação da Meraki

que impede a alteração do IP de verificação de integridade, tornando o NAT necessário para túneis SPA (acesso privado seguro) adicionais. Isso não se aplica ao usar o SIA (Secure Internet Access).

- Defina claramente quais sub-redes internas ou recursos são roteados pelo túnel para acesso seguro.

## Componentes Utilizados

- Acesso seguro da Cisco
- Meraki MX Security Appliance (versão do firmware 19.7.1 ou posterior)
- Painel Meraki
- Painel de acesso seguro

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

# CISCO Secure Access



CISCO

Meraki

## Cisco Meraki MX

O Cisco Secure Access é uma plataforma de segurança nativa da nuvem que permite acesso seguro a aplicativos privados (via Private Access) e destinos da Internet (via Internet Access). Quando integrado ao Meraki MX, ele permite que as empresas estabeleçam túneis IPsec seguros entre os locais da filial e a nuvem, garantindo fluxo de tráfego criptografado e aplicação de segurança centralizada.

Essa integração usa túneis IPsec de roteamento estático. O Meraki MX estabelece túneis IPsec principal e secundário para o Cisco Secure Access e aproveita suas verificações de integridade de uplink integradas para executar failover automático entre túneis. Isso fornece uma configuração resiliente e de alta disponibilidade para conectividade de filial.

Os principais elementos dessa implantação incluem:

- O Meraki MX atua como um par VPN não-Meraki para o Cisco Secure Access.
- Túneis primários e secundários configurados estaticamente, com verificações de integridade determinando a disponibilidade.
- O acesso privado dá suporte ao acesso seguro a aplicativos internos por meio do SPA (Secure Private Access), enquanto o acesso à Internet permite que o tráfego acesse

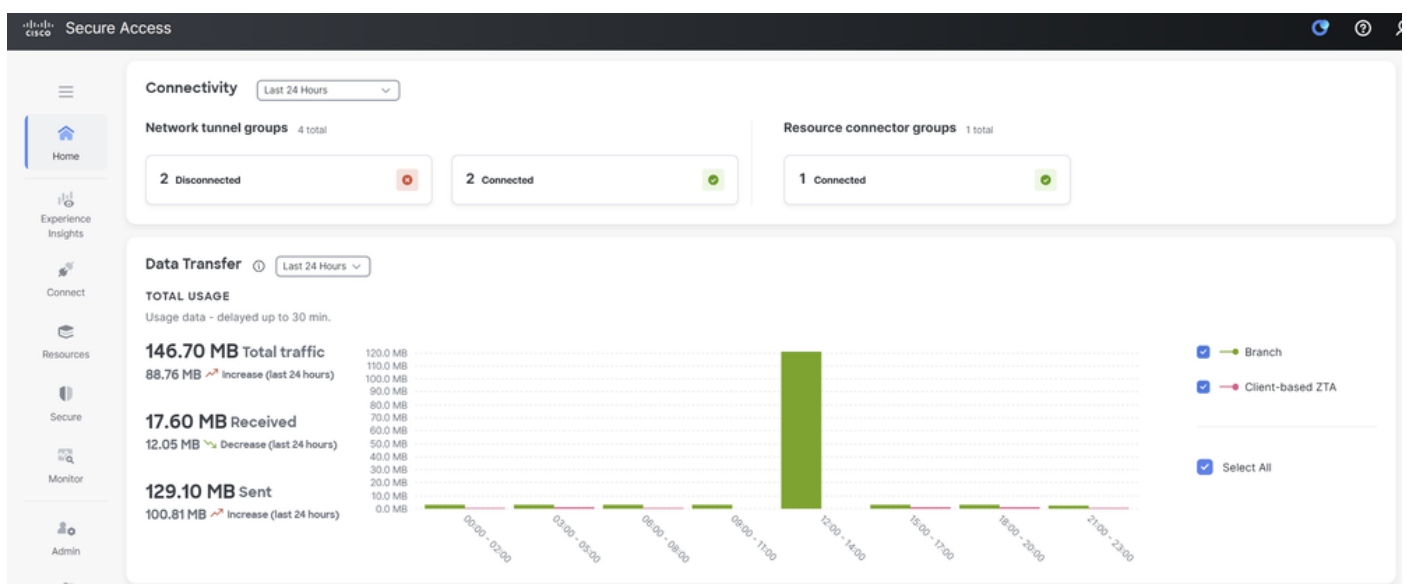
recursos baseados na Internet com aplicação de política na nuvem.

- Devido às limitações da Meraki na flexibilidade IP da verificação de integridade, somente um grupo de túneis é suportado no modo de acesso privado. Se vários dispositivos Meraki MX precisarem se conectar ao acesso seguro para acesso privado, você deverá usar o [BGP](#) para roteamento dinâmico ou configurar túneis estáticos, entendendo que apenas um grupo de túnel de rede pode suportar verificações de integridade e alta disponibilidade. Túneis adicionais operam sem monitoramento de integridade ou redundância.

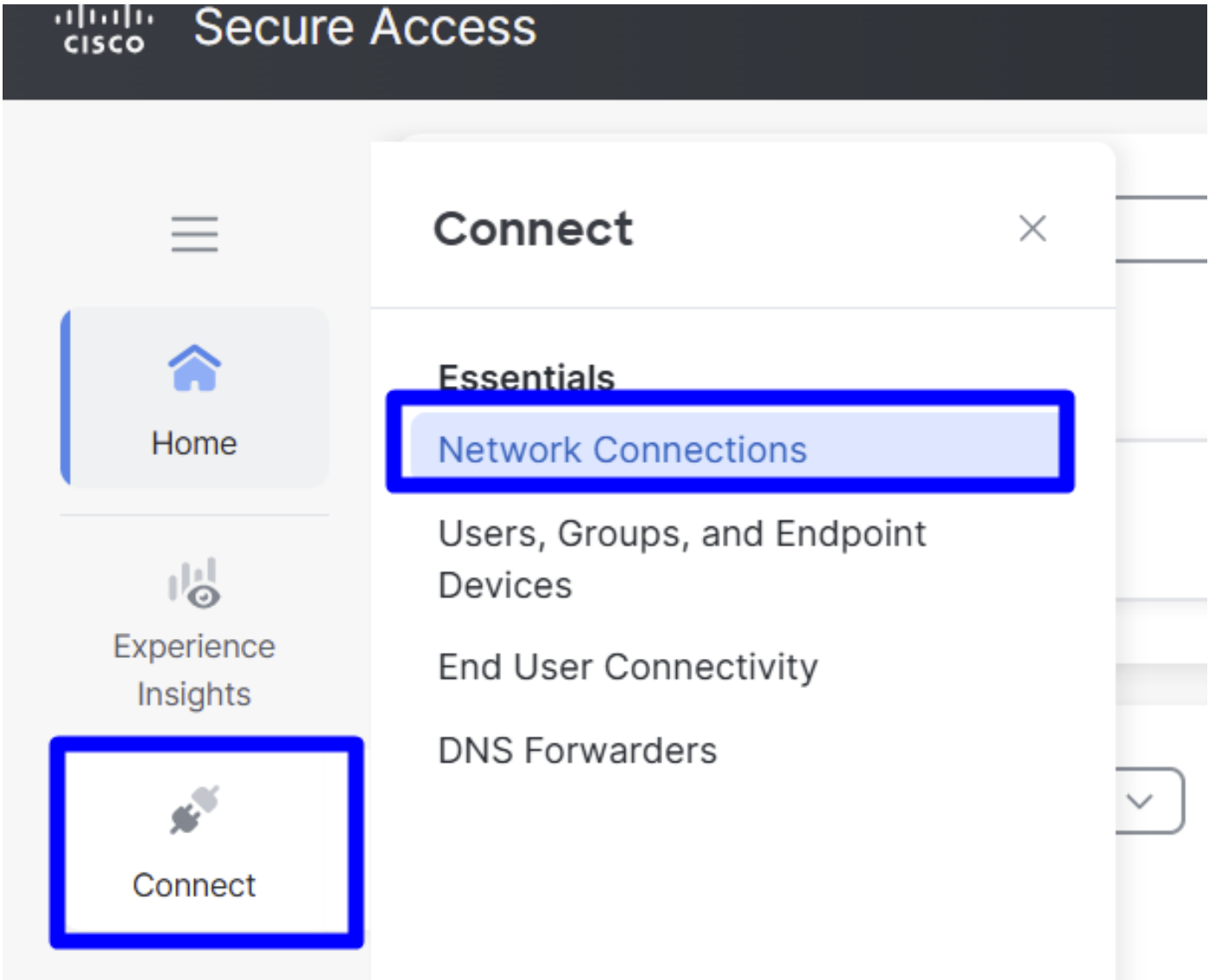
## Configurar

### Configurar a VPN no acesso seguro

Navegue até o painel de administração do [Secure Access](#).



- Clique em Connect > Network Connections



- EmNetwork Tunnel Groupsclique em + Add

**Network Connections**

Manage the connections that allow user traffic to reach private resources on your network. For information about these options, see [Help](#)

Connector Groups **Network Tunnel Groups**

**Network Tunnel Groups** 4 total

2  
Disconnected

0  
Warning

2  
Connected

**Network Tunnel Groups**

A network tunnel group provides a framework for establishing tunnel redundancy and high availability. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources. [Help](#)

4 Tunnel Groups

| Network Tunnel Group | Status       | Region           | Primary Hub Data Center | Primary Tunnels | Secondary Hub Data Center | Secondary Tunnels |     |
|----------------------|--------------|------------------|-------------------------|-----------------|---------------------------|-------------------|-----|
| DMZLABYPASS          | Disconnected | Europe (Germany) | sse-euc-1-1-0           | 0               | sse-euc-1-1-1             | 0                 | ... |
| EmmanuelFTD          | Disconnected | Europe (Germany) | sse-euc-1-1-0           | 0               | sse-euc-1-1-1             | 0                 | ... |

- Configure Tunnel Group Name, Region, Device Type
- Clique em 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

Region

Device Type

[<](#) [Cancel](#) [Next](#)

- Configure o Tunnel ID Format e Passphrase
- Clique em Next

**Tunnel ID and Passphrase**

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

Tunnel ID  
 @<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](#)

- Configure os intervalos de endereços IP ou hosts configurados na rede e deseje passar o tráfego pelo Secure Access e certifique-se de incluir o IP da sonda de monitoramento Meraki 192.0.2.3/32 para permitir o tráfego de retorno do Secure Access de volta ao Meraki MX.
- Clique em 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

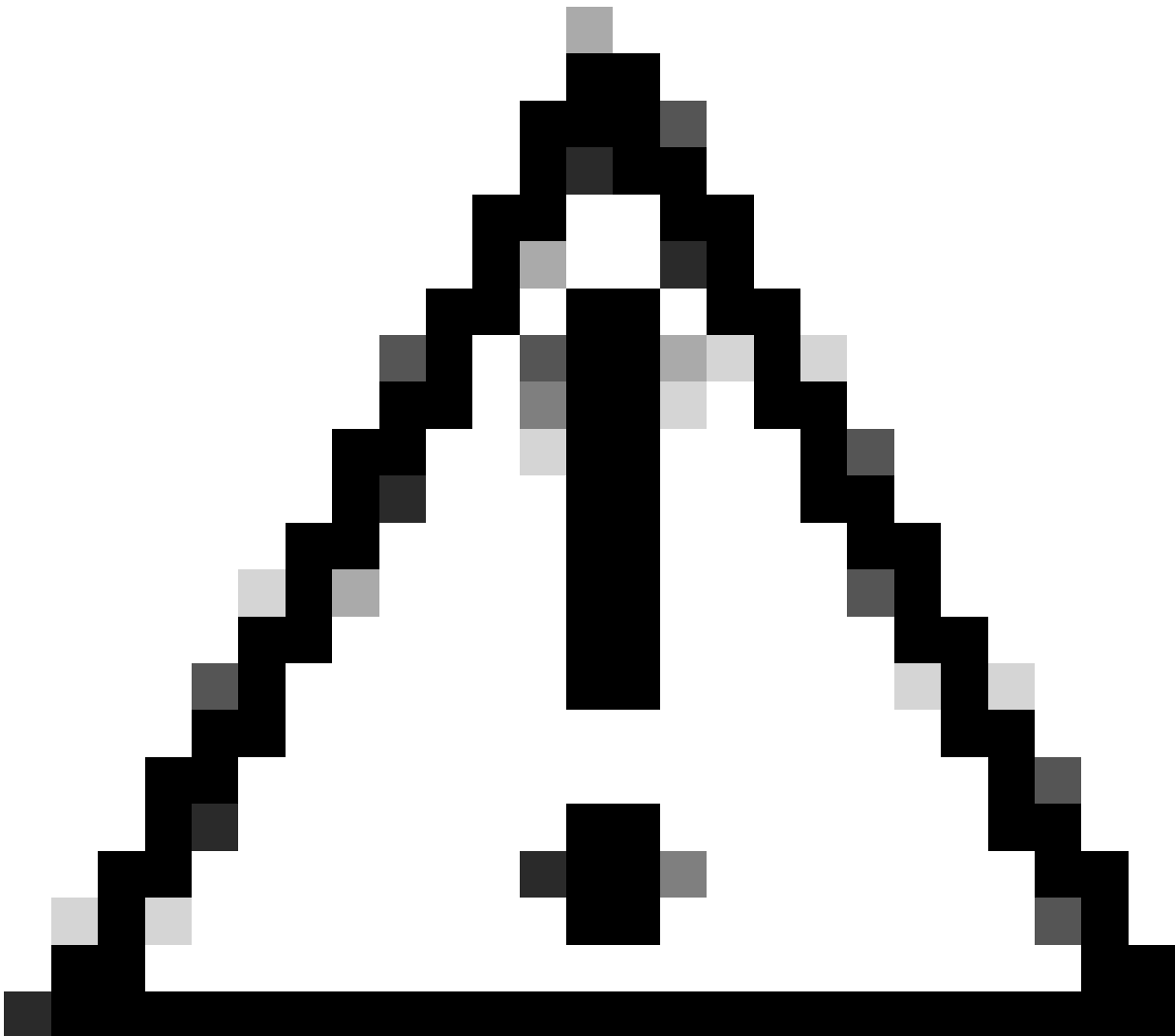


Cancel

Back

Save

Meraki MX Probe IP



Caution: Certifique-se de adicionar o IP da sonda de monitoramento (192.0.2.3/32); caso contrário, você poderá ter problemas de tráfego no dispositivo Meraki que roteia o tráfego para a Internet, Pools de VPN e CGNAT Range 100.64.0.0/10 usado pela ZTNA.

- Depois de clicar **save** nas informações sobre o túnel que são exibidas, salve essas informações para a próxima etapa, **Configure the tunnel on Meraki MX**.

## Configuração de VPN de acesso seguro

Copie a configuração dos túneis em um bloco de notas. Use essas informações para concluir a configuração no Meraki **Non-Meraki VPN Peers**.

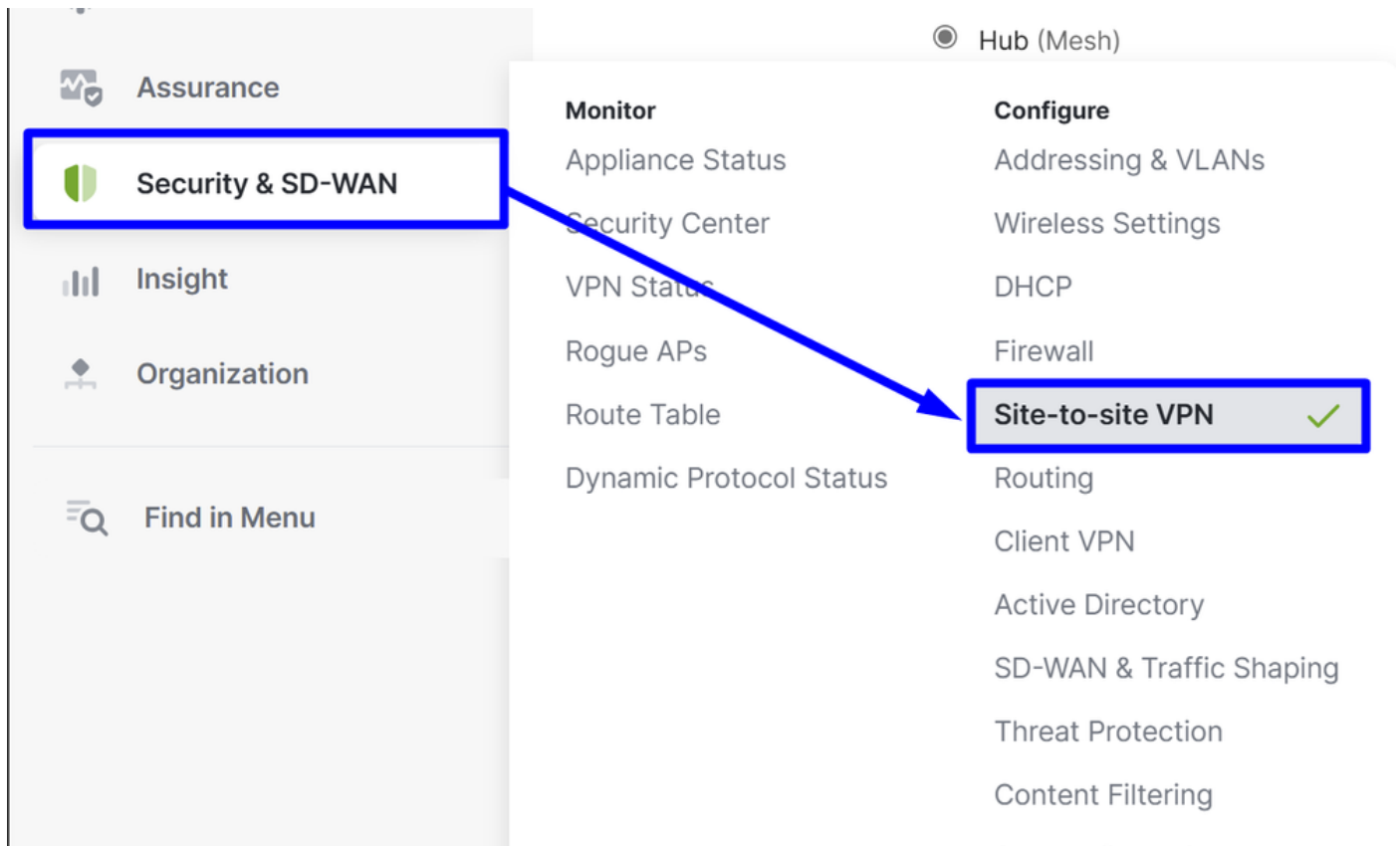
The screenshot shows the 'Data for Tunnel Setup' configuration page in the Meraki MX interface. On the left, a sidebar lists four steps: 'General Settings', 'Tunnel ID and Passphrase', 'Routing', and 'Data for Tunnel Setup' (which is currently selected). The main content area is titled 'Data for Tunnel Setup' and includes a sub-header '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 value 'MerakiShadow@' and a copy icon; 'Primary Data Center IP Address' with value '18.156.145.74' and a copy icon; 'Secondary Tunnel ID' with value 'MerakiShadow@' and a copy icon; and 'Secondary Data Center IP Address' with value '3.120.45.23' and a copy icon. At the bottom right of the main area, there are two buttons: 'Download CSV' and 'Done'.

| Data for Tunnel Setup                                                                          |                                    |
|------------------------------------------------------------------------------------------------|------------------------------------|
| Review and save the following information for use when setting up your network tunnel devices. |                                    |
| Primary Tunnel ID:                                                                             | MerakiShadow@ <input type="text"/> |
| Primary Data Center IP Address:                                                                | 18.156.145.74 <input type="text"/> |
| Secondary Tunnel ID:                                                                           | MerakiShadow@ <input type="text"/> |
| Secondary Data Center IP Address:                                                              | 3.120.45.23 <input type="text"/>   |

[Download CSV](#) [Done](#)

## Configurar a VPN no Meraki MX

Acesse o Meraki MX e clique em **Security & SD-WAN > Site-to-site VPN**



## VPN site a site

Escolha **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.

## Configurações de VPN

Escolha as redes que você selecionou para enviar tráfego para o Secure Access:

## 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   |        |

### Escolher em NAT Traversal Automático

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.

## Pares VPN não Meraki

Você precisa configurar as verificações de integridade que a Meraki usa para rotear o tráfego para o acesso seguro:

Clique em **Configure Health Checks**

- Clique em **+Add health Check**

| Health check                                                                                                                     | Endpoint                             |                                             |
|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|---------------------------------------------|
| <input type="text"/>                                                                                                             | <input type="text" value="http://"/> | <a href="#">Cancel</a> <a href="#">Done</a> |
| <div> Health check name can't be blank.</div> |                                      |                                             |

- **Health Check:** Configurar um nome para o teste
- **Endpoint:** Use o recomendado pelo Secure Access <http://service.sig.umbrella.com>



Note: Este domínio responde apenas quando acessado por meio de um túnel de site a site com Acesso seguro ou Umbrella: as tentativas de acesso de fora desses túneis falham.

---

Em seguida, clique duas vezes **Done** para finalizar.

## 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"/> | <a href="#">Cancel</a> <a href="#">Done</a> |

Rows per page  [<](#) [1](#) [>](#)

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

Agora, suas verificações de integridade estão configuradas e você está pronto para configurar  
O Peer:

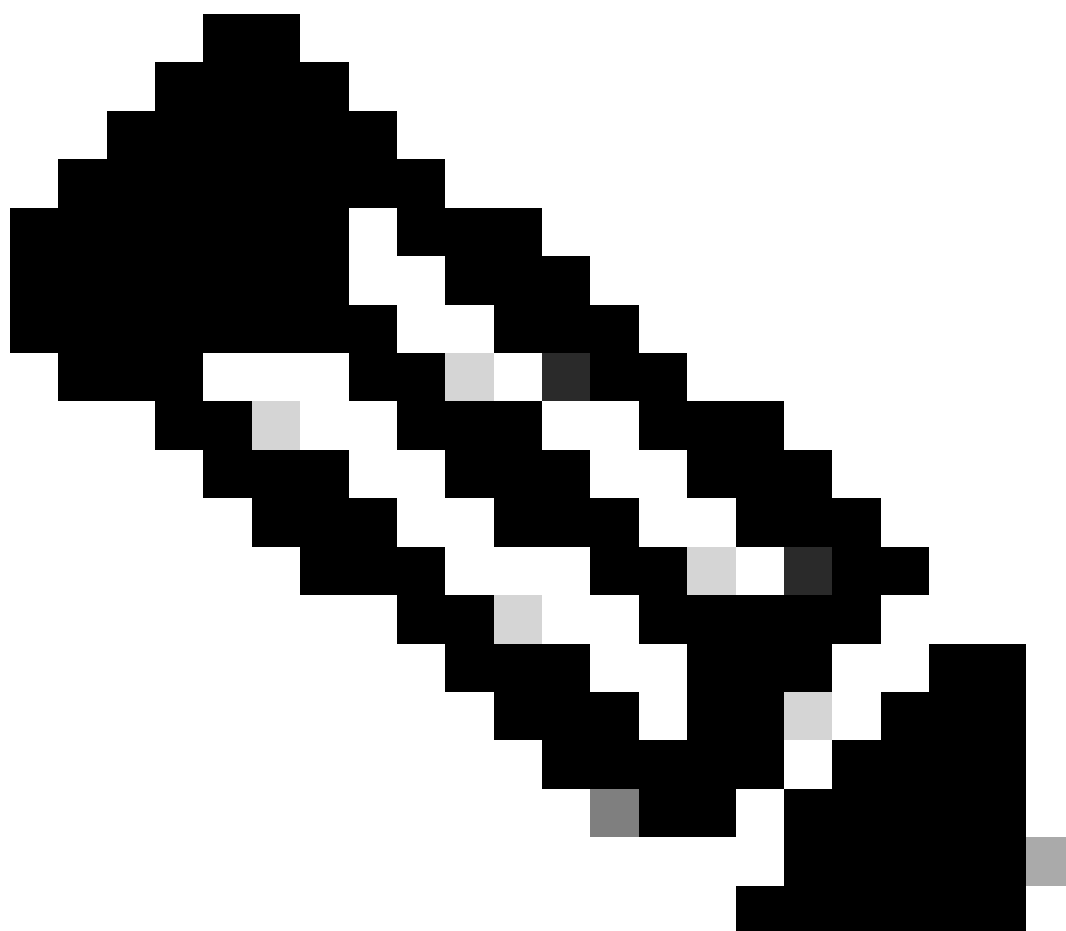
### Configurar túnel primário

- Clique em [+Add a peer](#)

|                                                                                                                                              |                                                                                                                                                                                            |                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <b>Name</b><br><input type="text" value="SSE-MERAKI Primary"/>                                                                               | <b>Remote ID</b> ⓘ<br><input type="text" value="Optional"/>                                                                                                                                | <b>Availability</b> ⓘ<br><input type="text" value="All networks"/>                            |
| <b>IKE version</b><br><input type="text" value="IKEv2"/><br><small>IKEv2 is required to support backup tunnels and failover features</small> | <b>Shared secret</b><br><input type="text" value="....."/> <a href="#">Show</a>                                                                                                            | <b>Tunnel monitoring</b><br><b>Health check</b><br><input type="text" value="SSE"/>           |
| <b>Peers</b> ^                                                                                                                               | <b>Routing</b><br><input checked="" type="radio"/> Static <input type="radio"/> Dynamic (BGP)<br><small>Static routing is required to support backup tunnels and failover features</small> | <b>Failover directly to internet</b> ⓘ<br><input checked="" type="checkbox"/> Enable failover |
| <b>Public IP or Hostname</b><br><input type="text" value="18.156.145.74"/>                                                                   | <b>Private subnets</b> ⓘ<br><input type="text" value="0.0.0.0/0"/>                                                                                                                         | <b>IPsec policy</b> ^                                                                         |
| <b>Local ID</b><br><input type="text" value="Merakishadow@ci:"/>                                                                             |                                                                                                                                                                                            | <b>Preset</b><br><input type="text" value="Umbrella"/>                                        |

- Adicionar Par VPN
  - Nome: Configurar um nome para a VPN para Acesso Seguro
  - Versão do IKE: Escolher IKEv2
- Pares
  - IP público ou nome de host: Configure o **Primary Datacenter IP** fornecido pelo Secure Access na etapa [Secure Access VPN Configurations](#)
  - ID local: Configure o **Primary Tunnel ID** fornecido pelo Secure Access na etapa [Secure Access VPN Configurations](#)
  - ID remota: N/A

- Segredo compartilhado: Configure o **Passphrase** fornecido pelo Secure Access na etapa [Configurações de VPN do Secure Access](#)
  - Roteamento: Escolher Estático
  - Sub-redes privadas: se você planeja configurar o Acesso à Internet e o Acesso privado, use 0.0.0.0/0 como o destino. Se você estiver configurando somente o acesso privado para esse túnel VPN, especifique o **Remote Access VPN IP Pool** e o intervalo CGNAT 100.64.0.0/10 como redes de destino
  - Disponibilidade: se você tiver apenas um dispositivo Meraki, poderá selecionar **All Networks**. Se você tiver vários dispositivos, certifique-se de selecionar apenas a rede Meraki específica na qual você está configurando o túnel.
  - Monitoramento de túnel
    - Verificação de integridade: Usar a verificação de integridade configurada anteriormente para monitorar a disponibilidade do túnel
    - Failover diretamente para a Internet: Se você habilitar essa opção e o Túnel 1 e o Túnel 2 não passarem nas verificações de integridade, o tráfego será redirecionado para a interface WAN para evitar a perda de acesso à Internet.
- 



Funcionalidade de verificação de integridade: Se o túnel 1 estiver sendo monitorado e sua verificação de integridade falhar, o tráfego automaticamente fará o failover para o túnel 2. Se o túnel 2 também falhar, e a opção **Failover directly to Internet** estiver habilitada, o tráfego será roteado através da interface WAN do dispositivo Meraki.

- política de IPsec
  - Predefinição: Escolha **Umbrella**

Depois, clique em **.Save**

Configurar túnel secundário

Para configurar o túnel secundário, clique no menu de opções do túnel principal:

- Clique nos três pontos

| #   | 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 | 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 >

- Clique em **+ Add Secondary peer**

## Primary



Edit primary peer



Move to



Delete primary peer

---

## Secondary



Add secondary peer

- Clique em `emInherit` primary peer configurations

# Add Secondary VPN Peer



**Inherit primary peer configurations**



**Name**

SSE Secondary

IKE version

**IKEv2**

---

Em seguida, observe que alguns campos são preenchidos automaticamente. Revise-os, faça as alterações necessárias e conclua o restante manualmente:

## 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

 ⓘ ▾

### • Pares

- IP público ou nome de host: Configure o **Secondary Datacenter IP** fornecido pelo Secure Access na etapa [Secure Access VPN Configurations](#)
- ID local: Configure o **Secondary Tunnel ID** fornecido pelo Secure Access na etapa [Secure Access VPN Configurations](#)
- ID remota: N/A
- Segredo compartilhado: Configure o **Passphrase** fornecido pelo Secure Access na etapa [Configurações de VPN do Secure Access](#)

### • Monitoramento de túnel

- Verificação de integridade: Usar a verificação de integridade configurada anteriormente para monitorar a disponibilidade do túnel

Depois disso, você poderá clicar em **save** e o próximo alerta será exibido:

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](#)

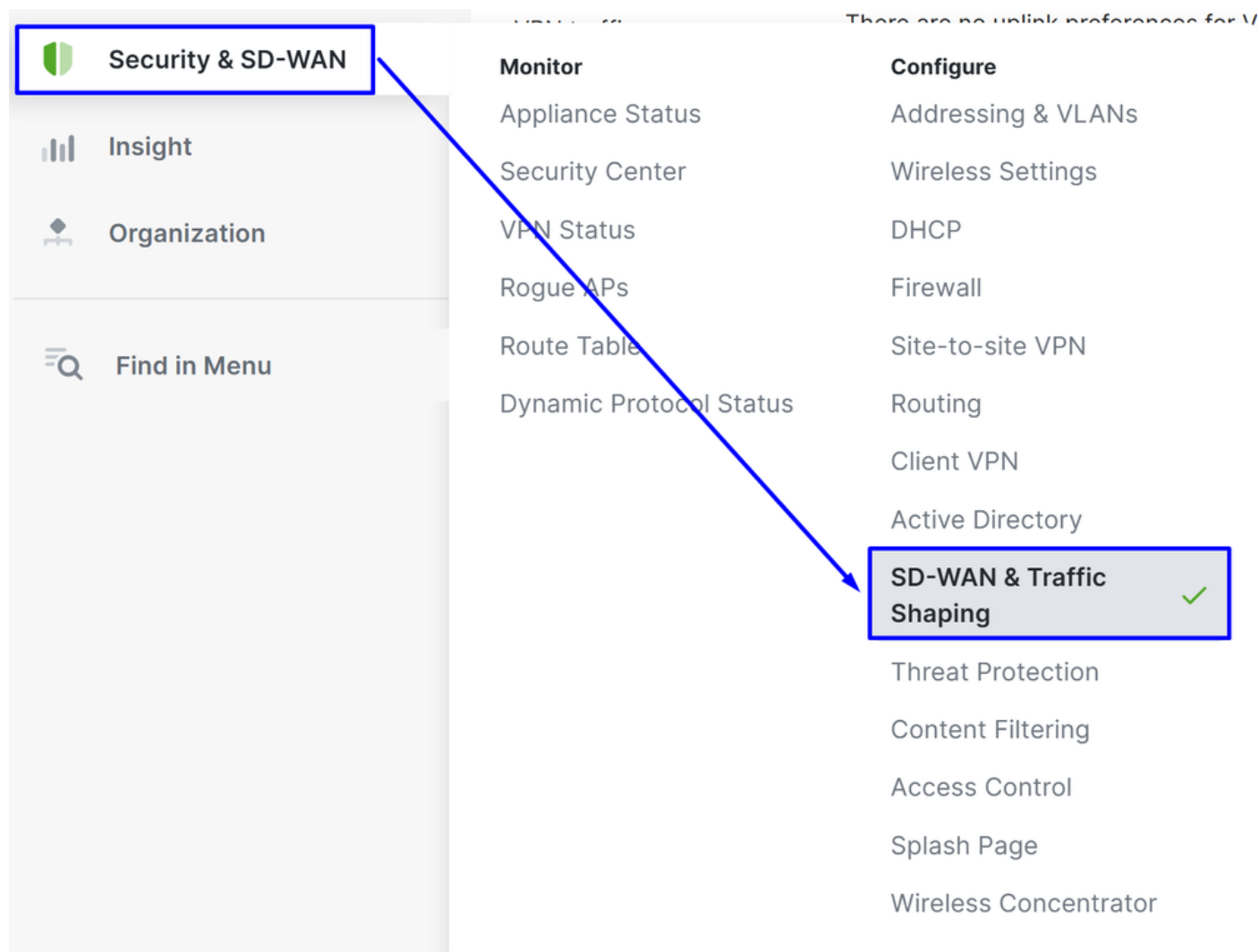
[Cancel](#)

Não se preocupe e clique **Confirm Changes**.

## Configurar o tráfego direcionado (desvio de tráfego de túnel)

Esse recurso permite que você ignore o tráfego específico do túnel, definindo domínios ou endereços IP na configuração de desvio de SD-WAN:

- Navegue até **Security & SD-WAN** > SD-WAN & Traffic Shaping



- Role para baixo até a **Local Internet Breakout** seção e clique em Add+

# Local internet breakout

VPN exclusion rules

Add +

Em seguida, crie o desvio com base em Custom Expressions OU Major Applications:

Custom Expressions - Protocol

|                    |                           |                |
|--------------------|---------------------------|----------------|
| Custom expressions | <b>Custom expressions</b> |                |
| Major applications | Protocol                  |                |
|                    | <div>TCP</div>            |                |
|                    | Destination ⓘ             | Dst port ⓘ     |
|                    | <div>8.8.8.8</div>        | <div>443</div> |
|                    | <div>Add expression</div> |                |

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

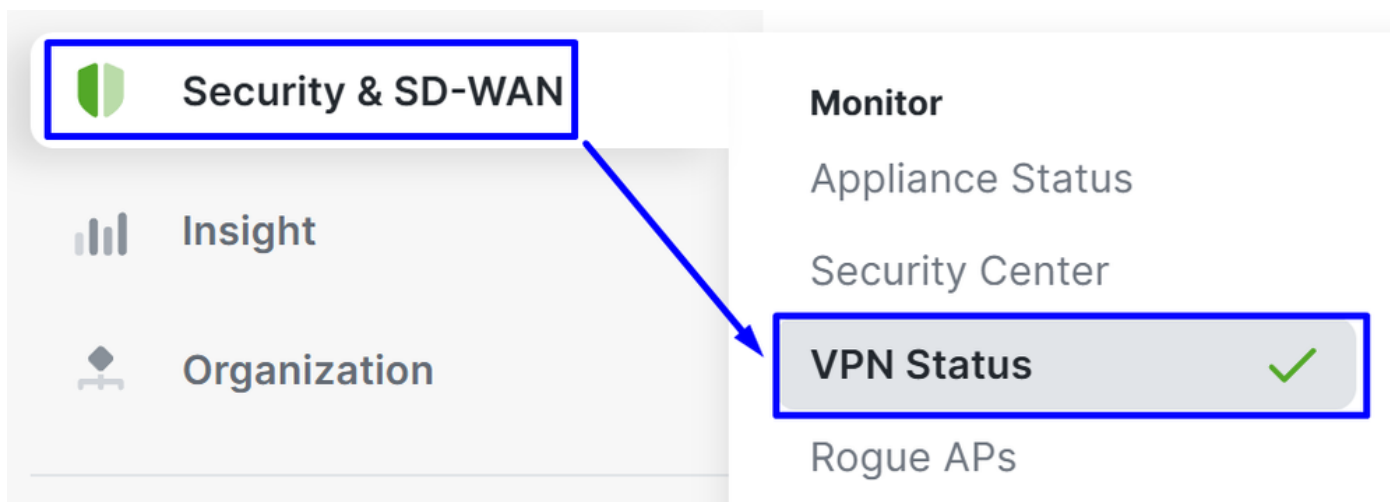
Zoom

Para obter mais informações, visite: [Configurando regras de exclusão de VPN \(IP/Porta/DNS/APP\)](#)

## Verificar

Para verificar se os túneis estão ativos, verifique o status em:

- Clique em **Security & SD-WAN > VPN Status** no painel da Meraki.



- Clique em 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 os status de VPN primário e secundário forem mostrados em verde, significa que os túneis estão ativos.

## 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 |

# Troubleshooting

## Verificar as Verificações de Integridade

Para verificar se as verificações de integridade da Meraki para a VPN estão funcionando corretamente, navegue para:

- Clique **Assurance** em > Event Log

## Event log

**Client:**

**Before:**   (PDT)

**Event type include:**

**Event type ignore:**

[Reset filters](#)

Em **Event Type Include**, escolha 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 o túnel principal para o Cisco Secure Access está ativo, os pacotes que chegam pelo túnel secundário são descartados para manter um caminho de roteamento consistente.

O túnel secundário permanece em espera e é usado somente se ocorrer uma falha no túnel principal, seja do lado da Meraki ou do Secure Access, conforme determinado pelo mecanismo de verificação de integridade.

## 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         |                |                |                            |                                                                                           |

- A verificação de integridade do túnel primário mostra o status: ativo, o que significa que ele está atualmente transmitindo e encaminhando ativamente o tráfego.
- A verificação de integridade do túnel secundário mostra o status: inoperante, não porque o túnel não está disponível, mas porque o primário está íntegro e em uso ativo. Esse comportamento é esperado, pois o tráfego só tem permissão para passar pelo túnel 1, fazendo com que a verificação de integridade do túnel secundário falhe.

## Informações Relacionadas

- [Suporte técnico e downloads da Cisco](#)
- [Central de ajuda do Cisco Secure Access](#)
- [Guia de configuração do Cisco Secure Access Meraki BGP](#)

### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.