使用Meraki MX配置安全访问，以实现高可用性和运行状况监控

目录

简介

本文档介绍如何使用Meraki MX通过运行状况检查配置思科安全访问以实现高可用性。

先决条件

- 评审具有安全访问的IPsec隧道要求
- 了解安全访问组件
- 了解Meraki MX中的运行状况检查功能

要求

- Meraki MX必须运行固件版本19.7.1或更高版本
- 使用专用访问时，由于Meraki的限制阻止更改运行状况检查IP，使得其他SPA（安全专用访问）隧道需要NAT，因此仅支持一个隧道。使用SIA（安全互联网接入）时不适用。
- 明确定义哪些内部子网或资源通过隧道路由到安全访问。

使用的组件

- 思科安全访问
- Meraki MX安全设备（固件版本19.7.1或更高版本）
- Meraki 控制面板
- 安全访问控制面板

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

思科安全访问是一个云原生安全平台，支持对私有应用（通过私有访问）和互联网目标（通过互联网访问）的安全访问。 当与Meraki MX集成时，组织可以在分支机构站点和云之间建立安全的IPsec隧道，从而确保加密流量和集中式安全实施。

此集成使用静态路由IPsec隧道。Meraki MX建立到思科安全访问的主和辅助IPsec隧道，并利用其内置的上行链路运行状况检查在隧道之间执行自动故障切换。这为分支机构连接提供了可恢复的高

可用性配置。

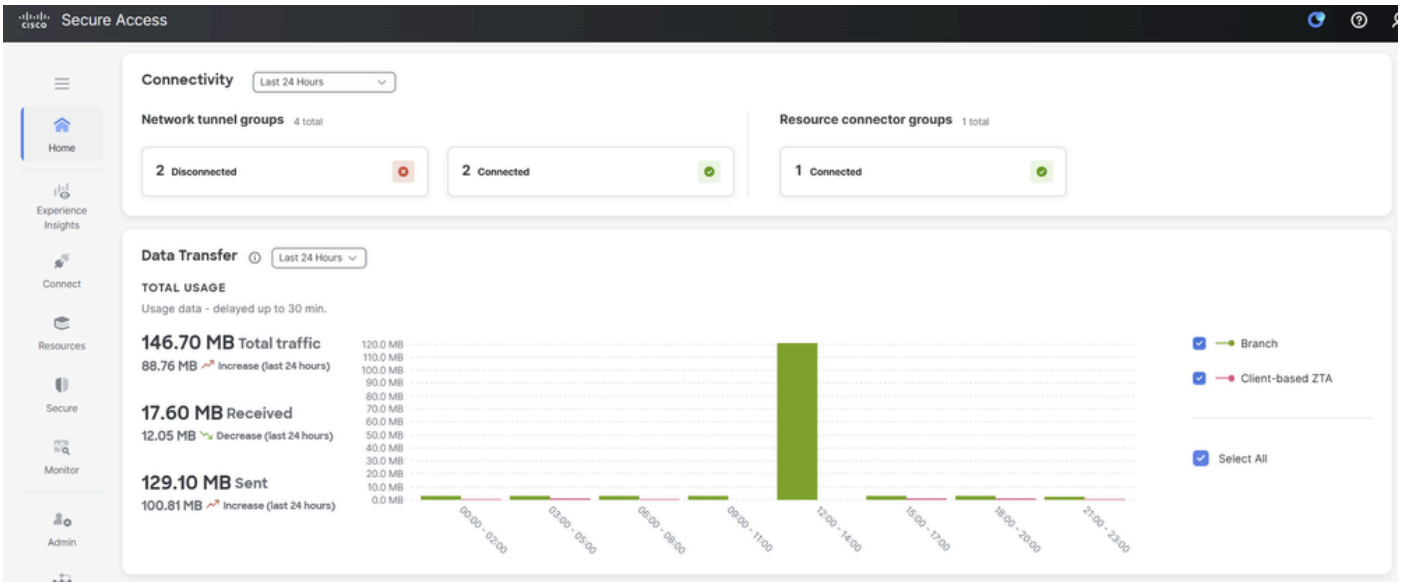
此部署的关键要素包括：

- Meraki MX充当思科安全访问的非Meraki VPN对等体。
- 静态配置主隧道和辅助隧道，使用运行状况检查确定可用性。
- 私有访问支持通过SPA（安全私有访问）安全访问内部应用，而互联网访问允许流量通过云中的策略实施访问基于互联网的资源。
- 由于Meraki在运行状况检查IP灵活性方面的限制，在专用访问模式中仅支持一个隧道组。如果多个Meraki MX设备需要连接到专用访问的安全访问，则必须使用BGP进行动态路由，或配置静态隧道，因为只有一个网络隧道组可以支持运行状况检查和高可用性。其他隧道无需运行状况监控或冗余即可运行。

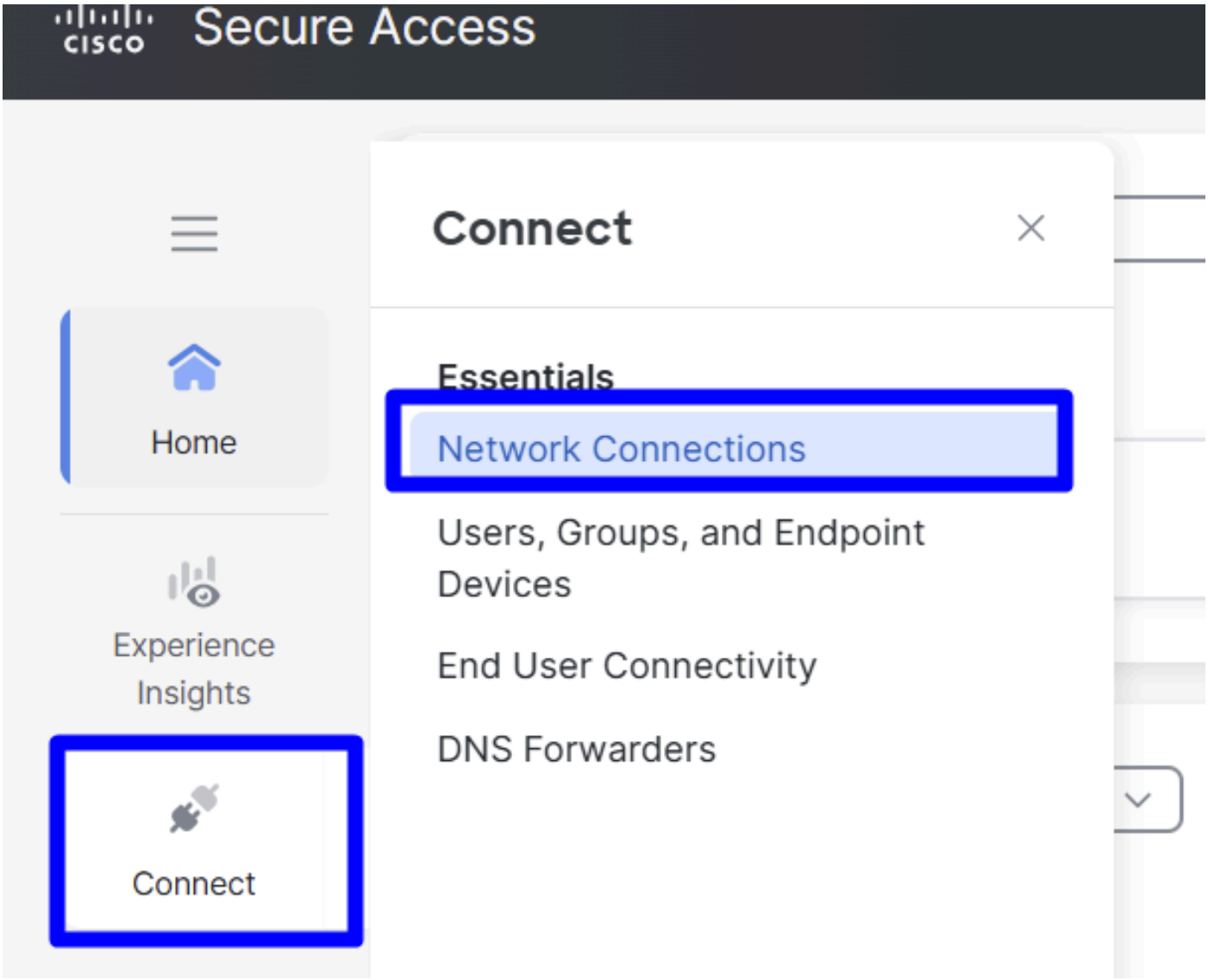
配置

在安全访问中配置VPN

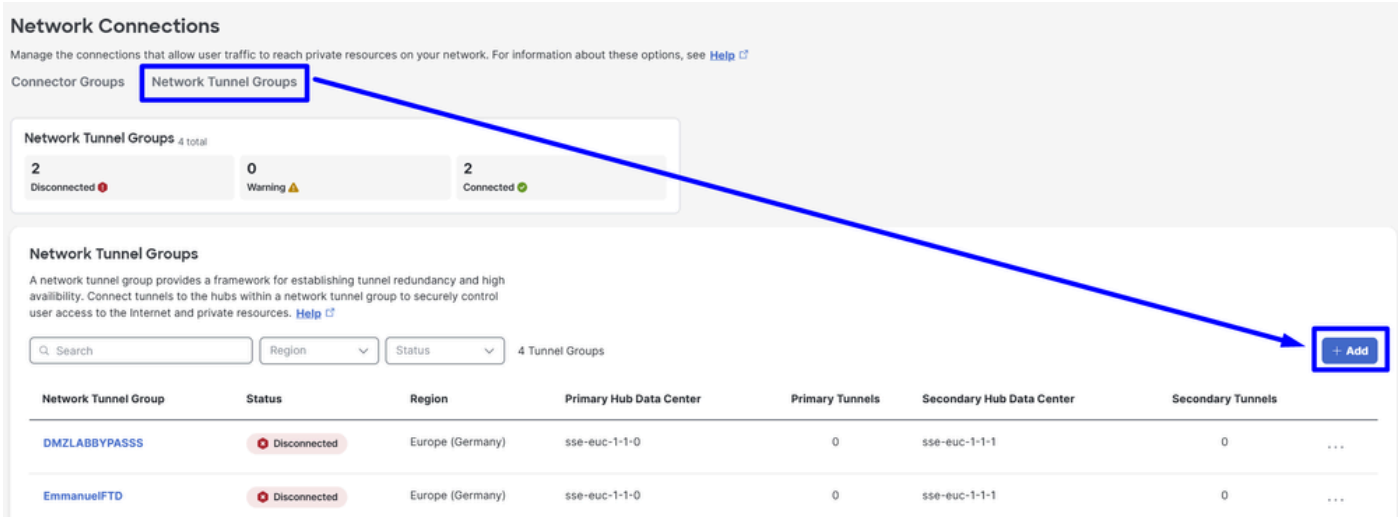
导航到Secure Access的管理面板。



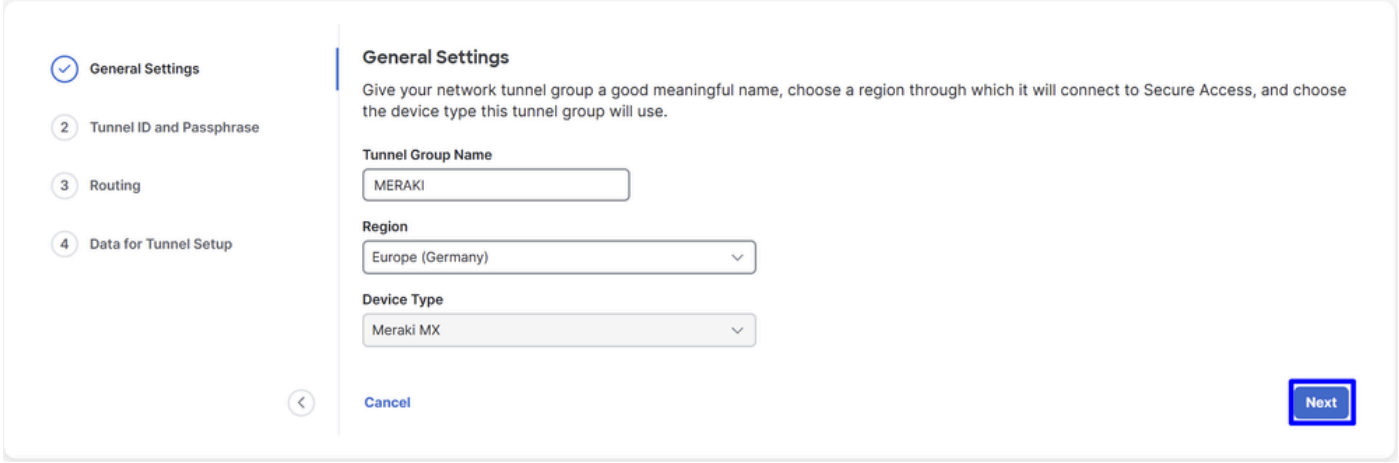
- 点击 Connect > Network Connections



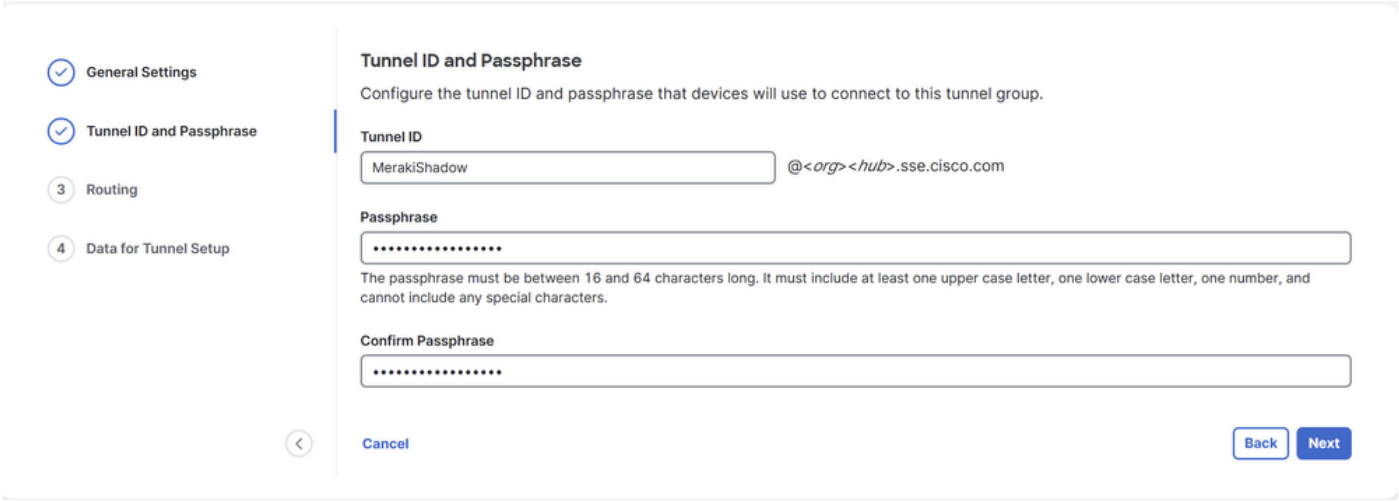
- 在Network Tunnel Groups下，单击 + Add



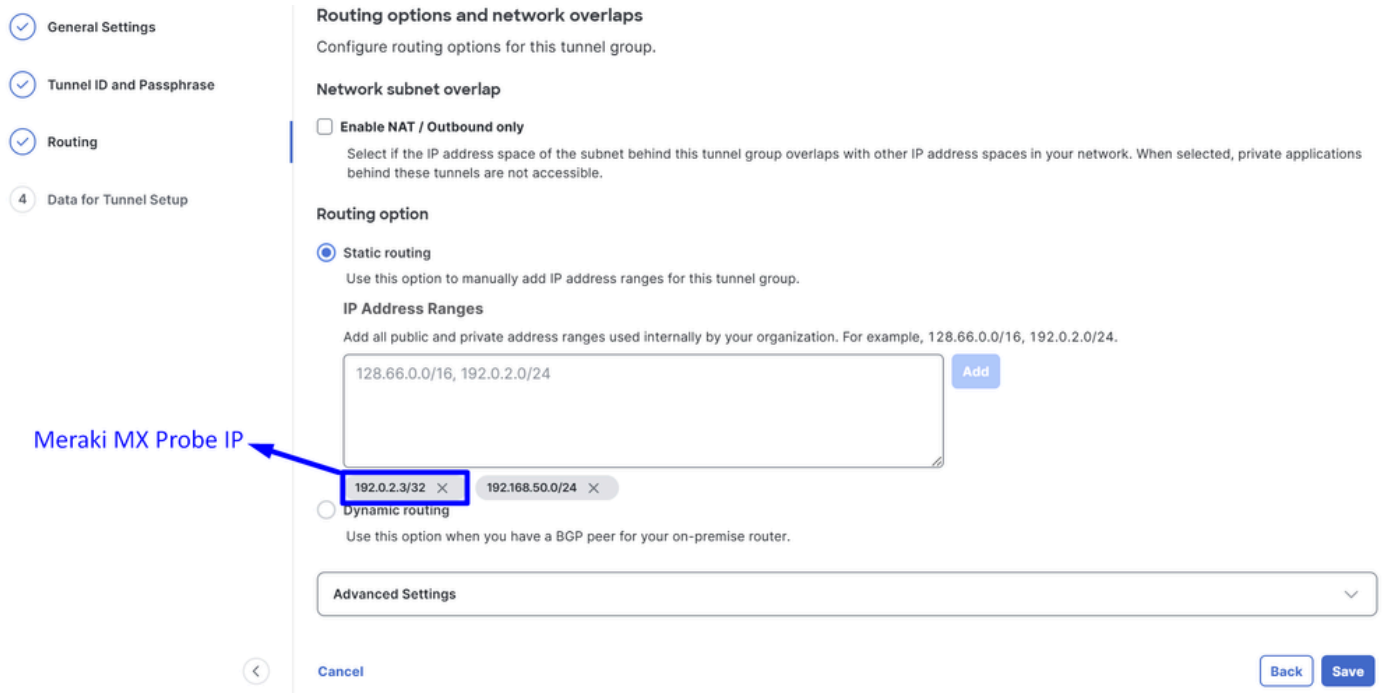
- 配置Tunnel Group Name,Region和Device Type
- 点击 **Next**

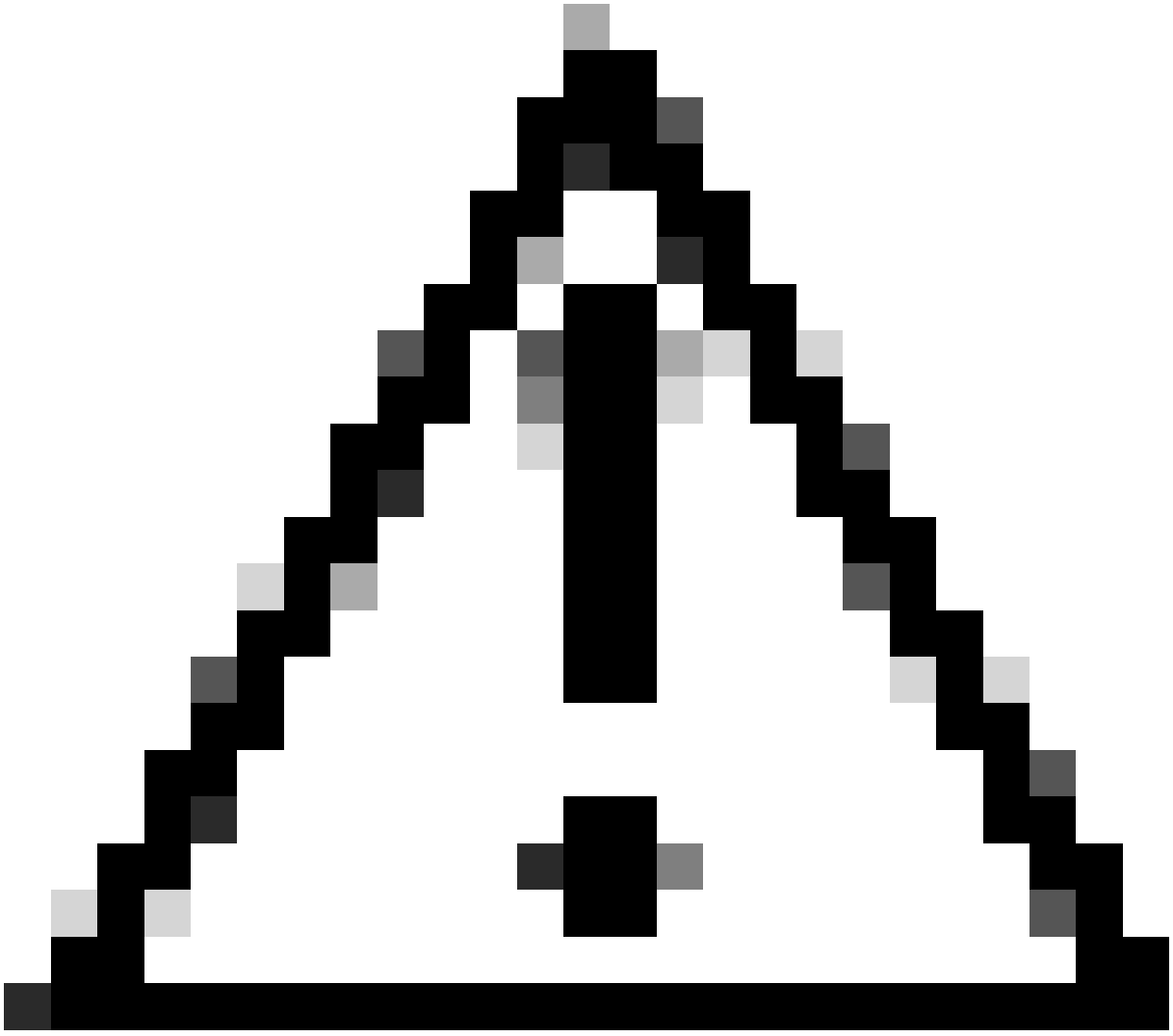


- 配置Tunnel ID Format和 Passphrase
- 点击Next



- 配置网络上已配置且希望通过安全访问传递流量的IP地址范围或主机，并确保包含Meraki监控探测IP192.0.2.3/32，以允许从安全访问返回流量返回Meraki MX。
- 点击**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

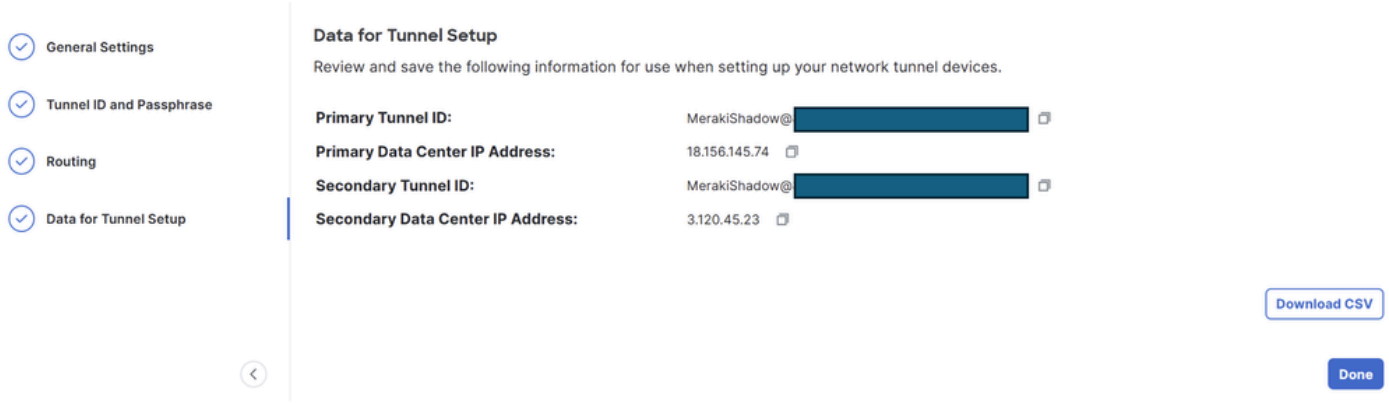


警告：请务必添加监控探头IP(192.0.2.3/32);否则，您可能会遇到将流量路由到Internet、VPN池和ZTNA使用的CGNAT范围100.64.0.0/10的Meraki设备上的流量问题。

- 单击显示的Save“通道信息”后，请保存下一步的信息。 **Configure the tunnel on Meraki MX.**

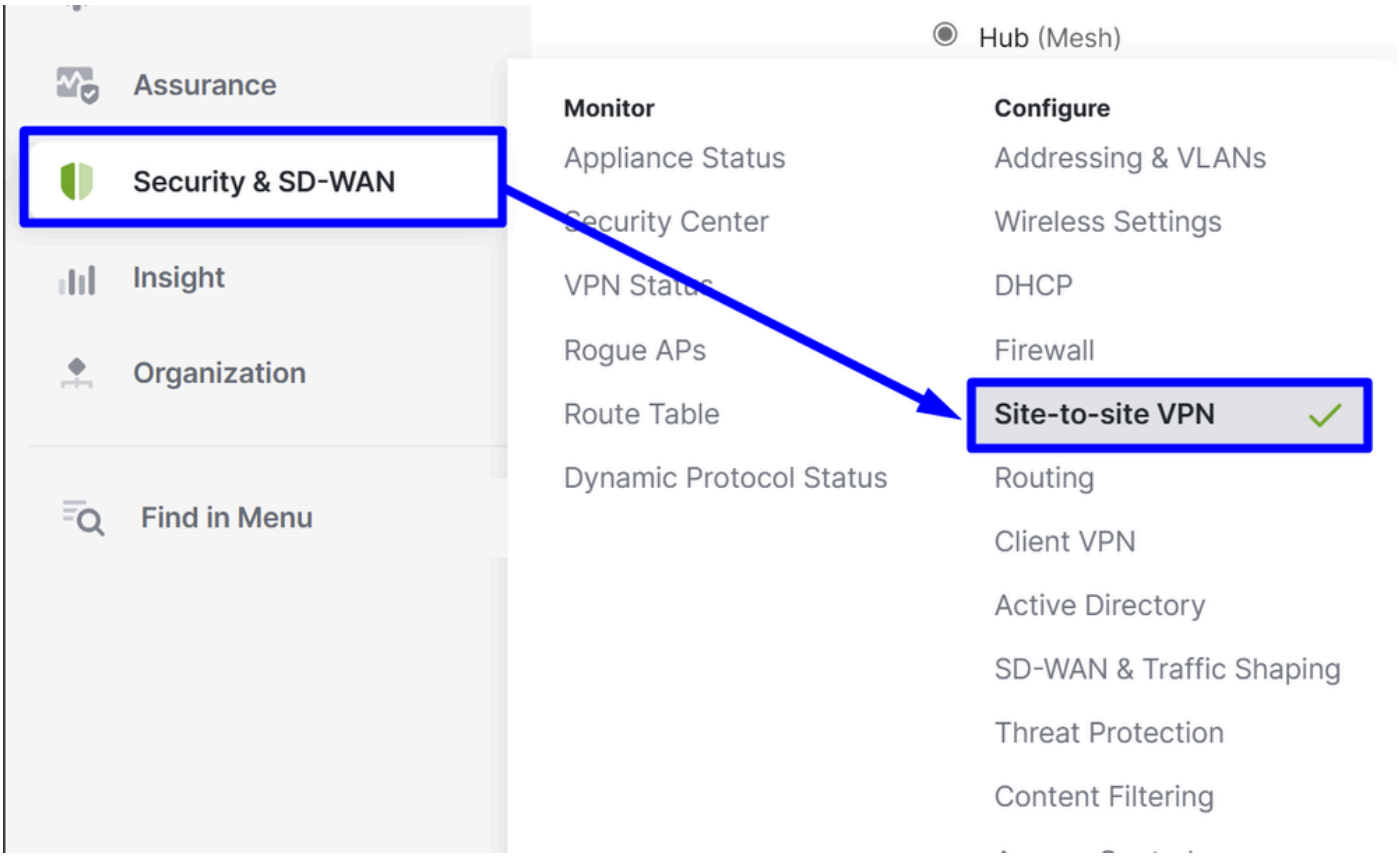
安全访问VPN配置

在记事本中复制隧道的配置，使用此信息完成Meraki中的配**Non-Meraki VPN Peers**置。



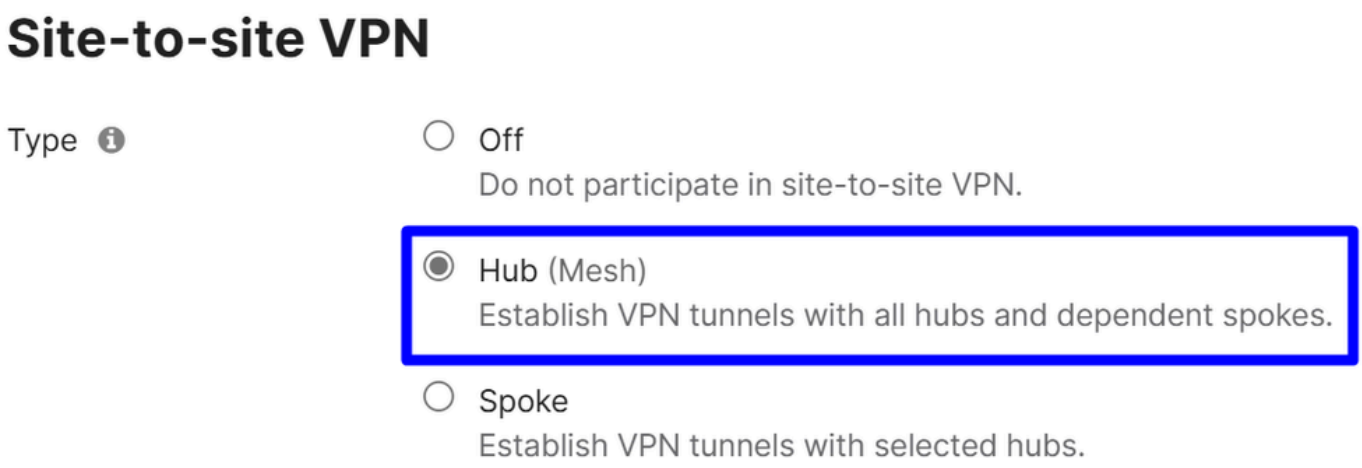
在Meraki MX上配置VPN

导航到您的Meraki MX并点击**Security & SD-WAN>** Site-to-site VPN



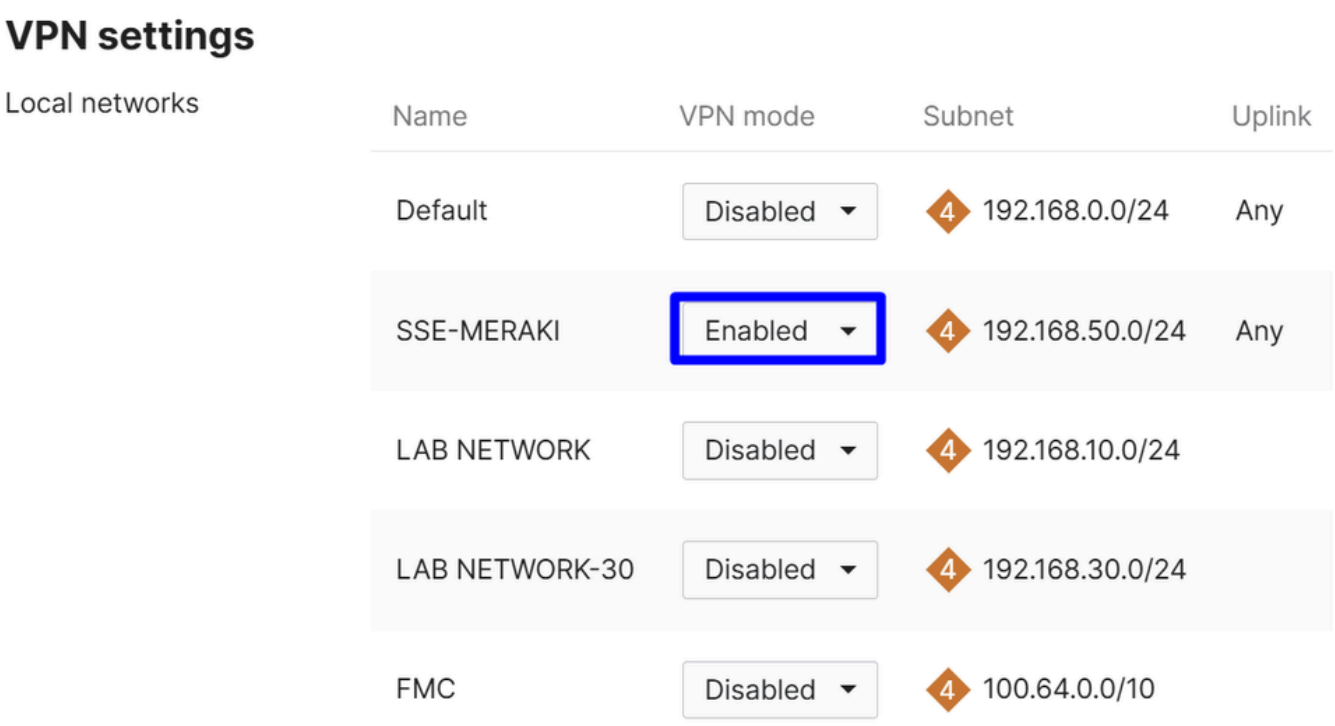
站点到站点 VPN

选择 Hub.

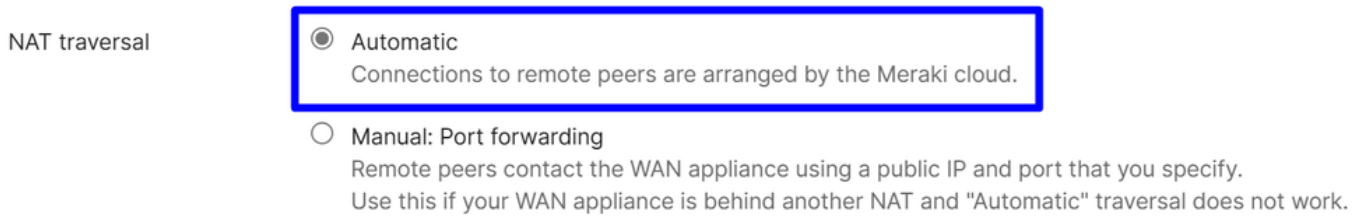


VPN设置

选择您选择要将流量发送到安全访问的网络：



在自动中选择NAT Traversal。



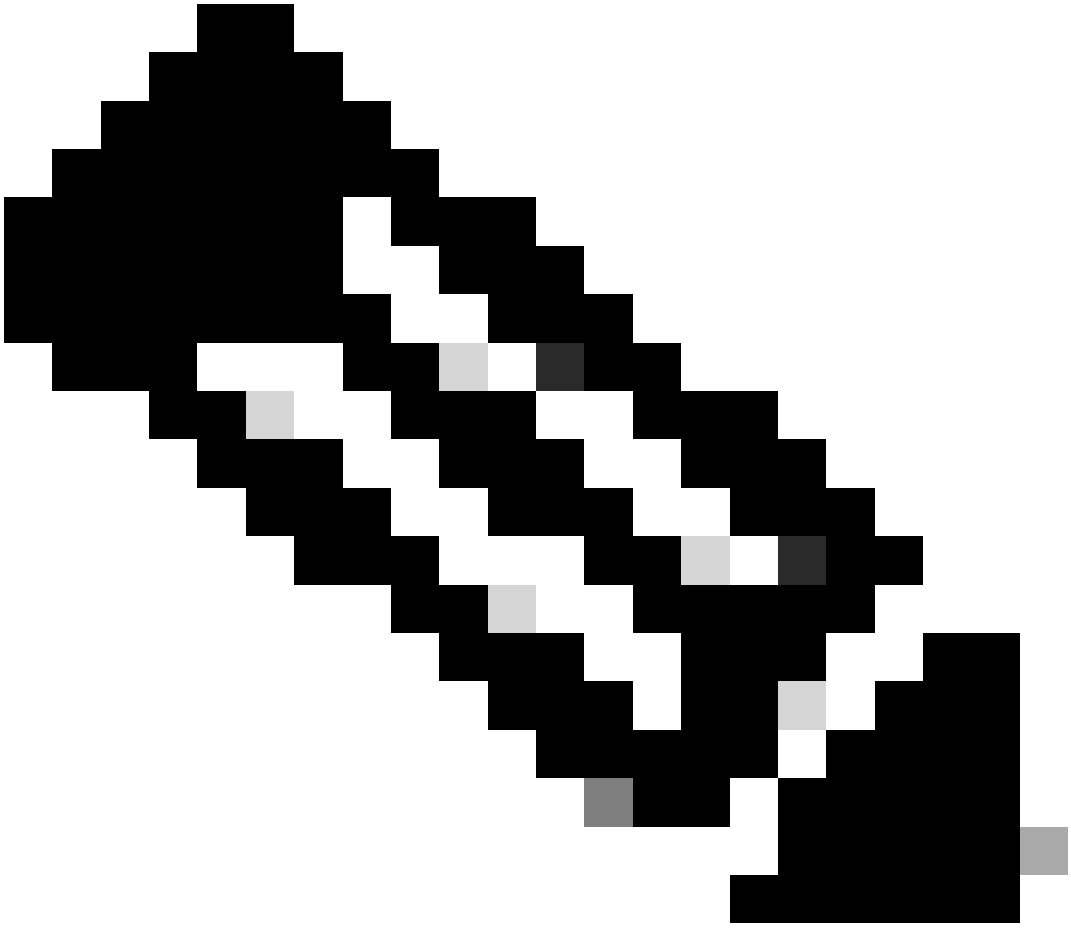
非Meraki VPN对等点

您需要配置Meraki用于将流量路由到安全访问的运行状况检查：

点击 **Configure Health Checks**

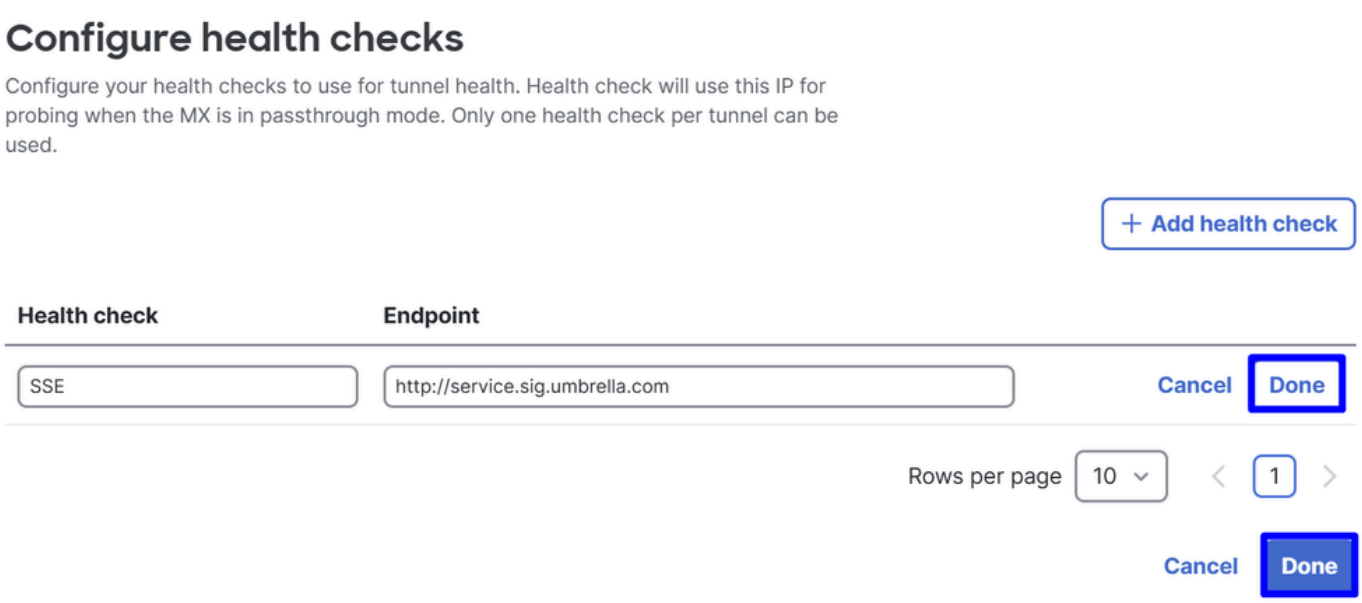
- 点击 **+Add health Check**

- **Health Check**:配置测试的名称
- **Endpoint**:使用Secure Access推荐的方法 http://service.sig.umbrella.com



注意：仅当通过具有Secure Access或Umbrella的站点到站点隧道访问时，此域才会响应：从这些隧道外部进行的访问尝试失败。

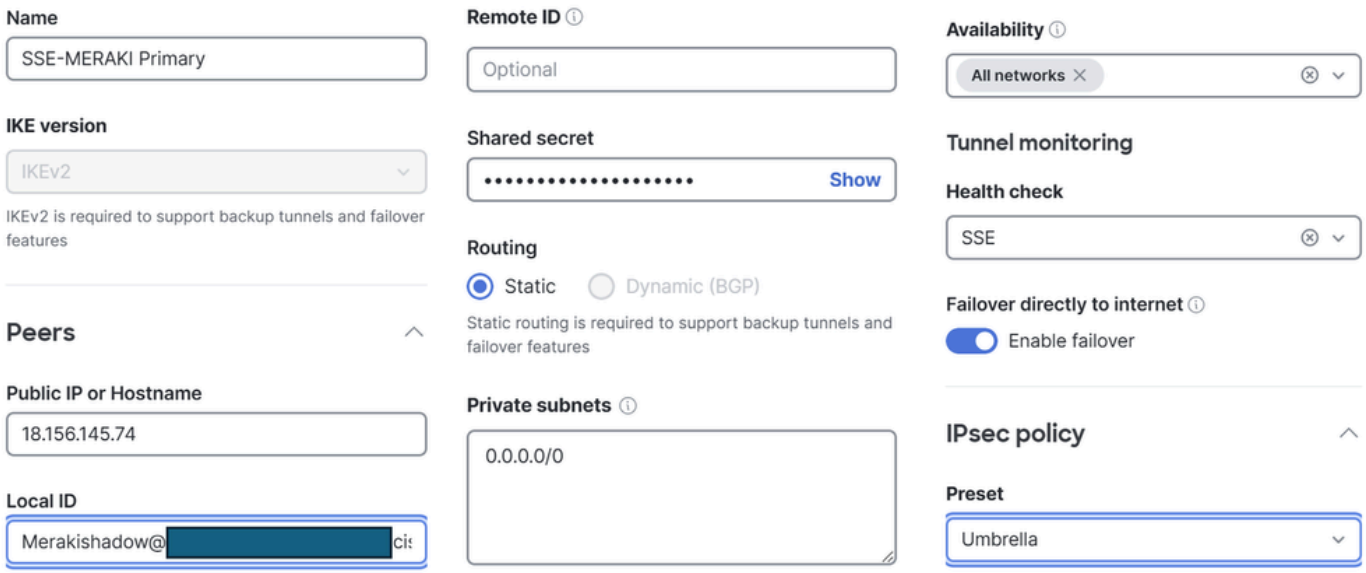
然后点击**Done**两次以最终确定。



现在，您的运行状况检查已配置好，并且您已准备好配置 **Peer:**

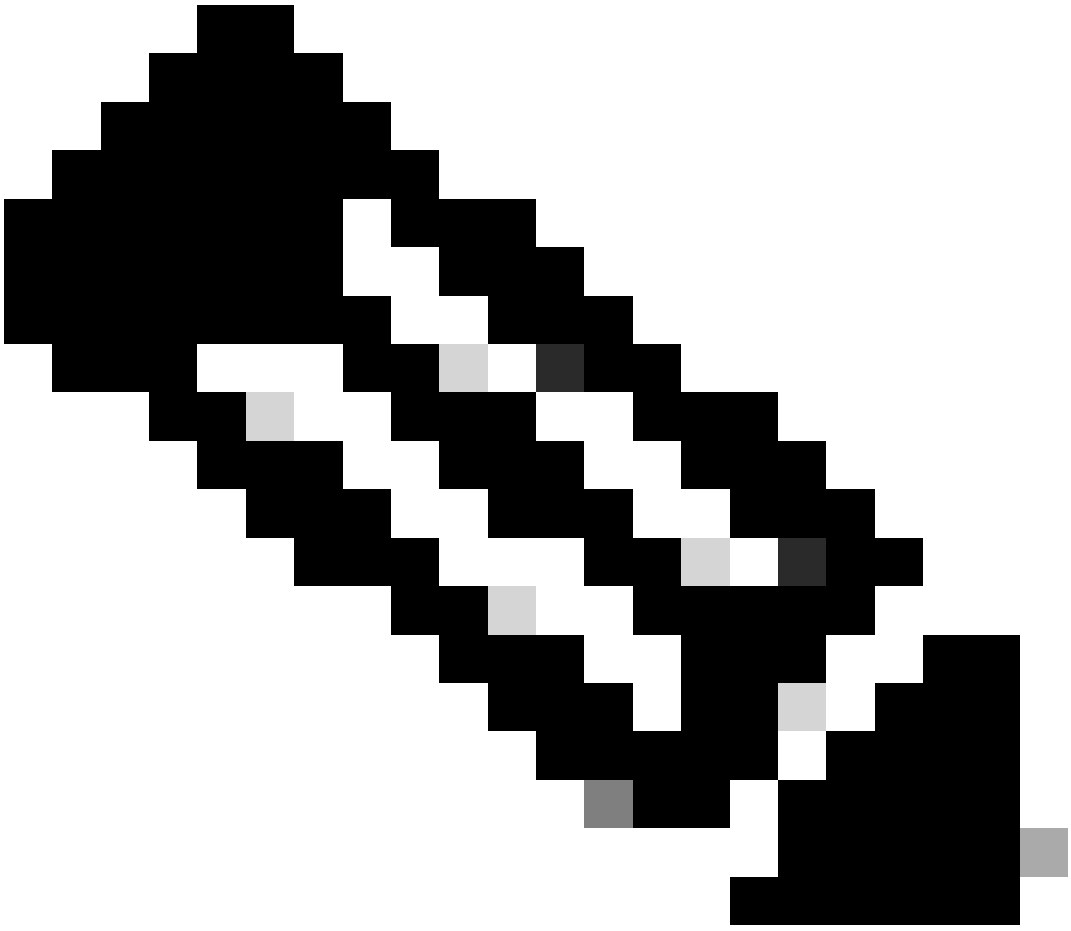
配置主隧道

- 点击+Add a peer



- 添加VPN对等项
  - 名称：为VPN配置安全访问名称
  - IKE版本:选择IKEv2
- 对等体
  - 公共IP或主机名:在Secure Access VPN Configurations步骤中配置**Primary Datacenter IP**Secure Access给定的
  - 本地ID:在Secure Access VPN Configurations步骤中配置**Primary Tunnel ID**Secure Access给定的
  - 远程ID:不适用
  - 共享密码：在Secure Access VPN Configurations步**Passphrase**中，配置由Secure

Access提供的
    - 路由:选择静态
    - 专用子网：如果您计划同时配置Internet接入和专用接入，**0.0.0.0/0**请使用作为目标。如果仅配置该VPN隧道的专用接入，请将和**Remote Access VPN IP Pool**CGNAT范围指定**100.64.0.0/10**为目标网络
    - 可用性：如果您只有一个Meraki设备，则可以选**All Networks**择。如果有多个设备，请确保仅选择要在其中配置隧道的特定Meraki网络。
- 隧道监控
    - 运行状况检查：使用之前配置的运行状况检查监控隧道可用性
    - 直接故障切换到Internet：如果启用此选项，并且隧道1和隧道2的运行状况检查均失败，流量将重定向到WAN接口以防止无法访问Internet。



运行状况检查功能：如果正在监控隧道1且其运行状况检查失败，则流量会自动故障转移到隧道2。如果隧道2也发生故障，并且启用了选Failover directly to Internet项，则流量通过Meraki设备的WAN接口路由。

- IPSec 策略

- 预设：选择 **Umbrella**

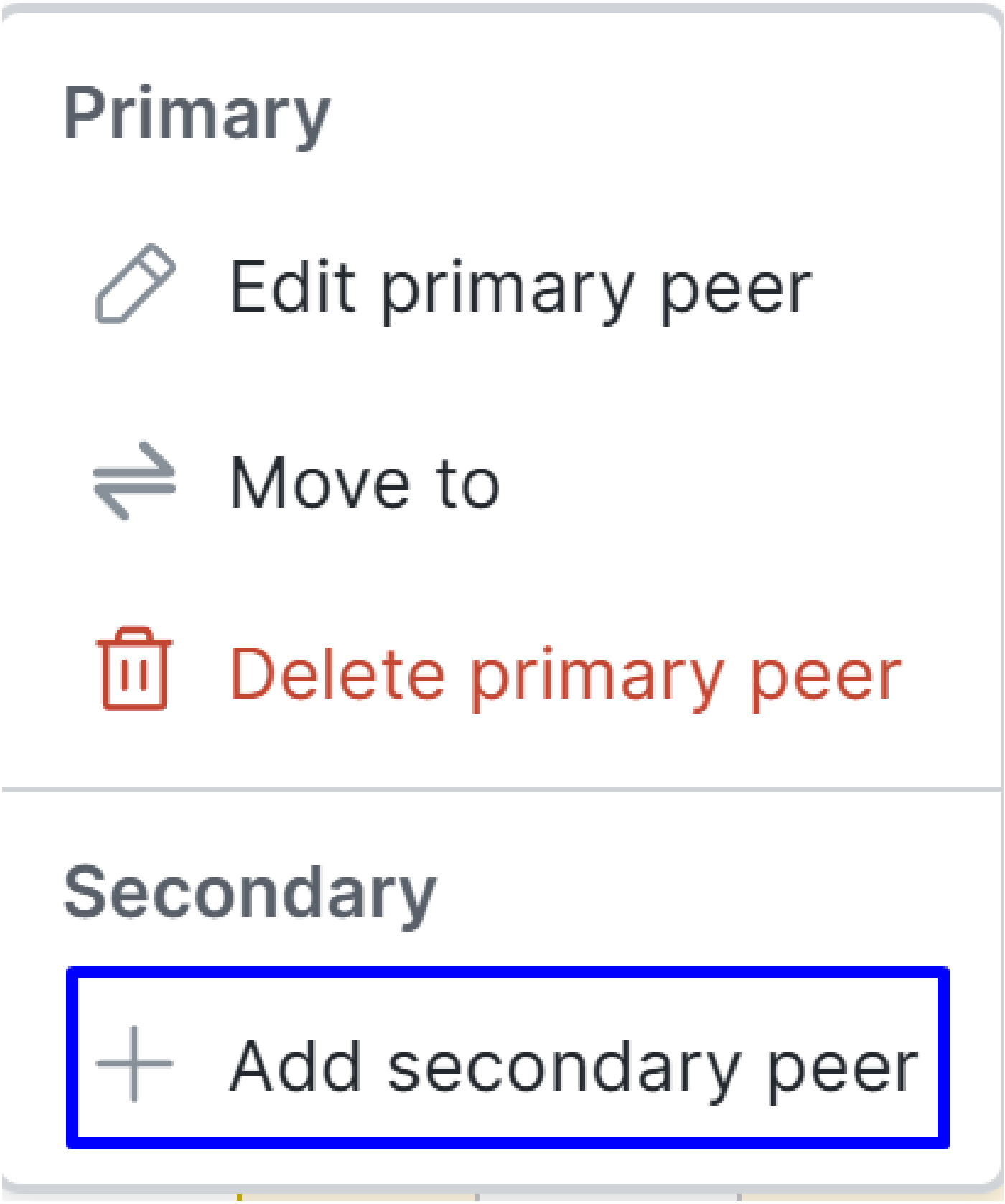
？？然后单击.**Save**

配置辅助隧道

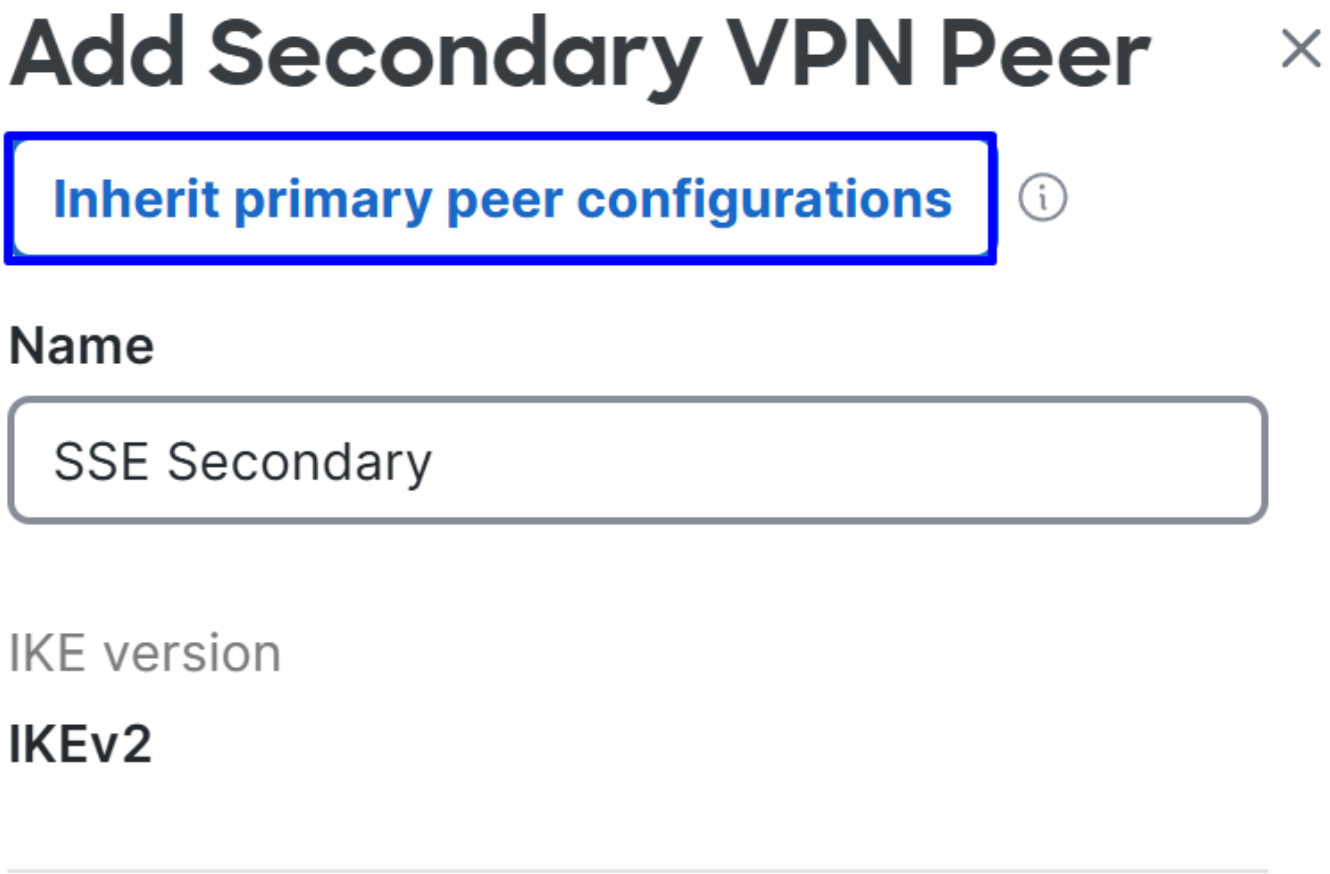
要配置辅助隧道，请点击主隧道的选项菜单：

- 单击三个点

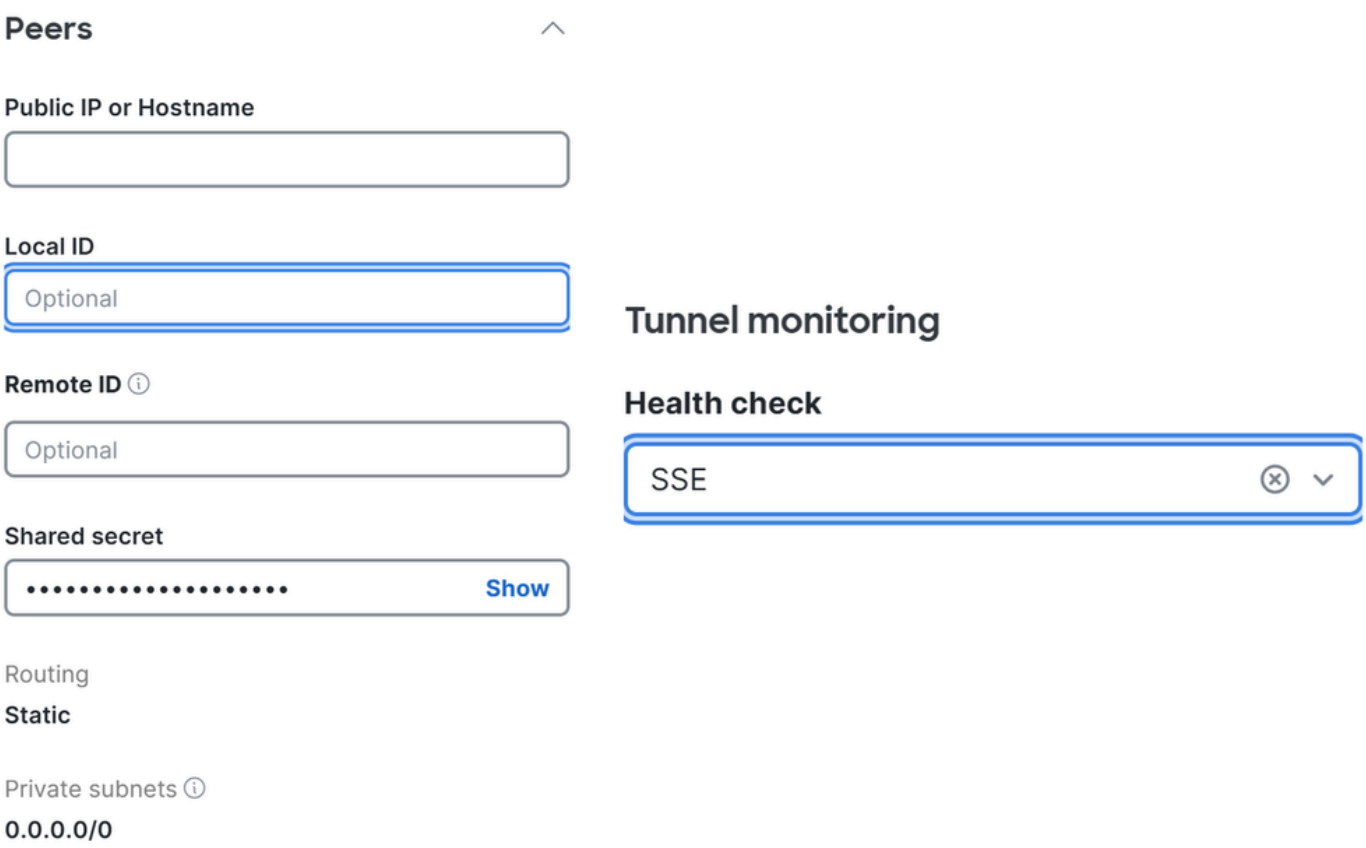
- 点击 + Add Secondary peer



- 点击Inherit primary peer configurations

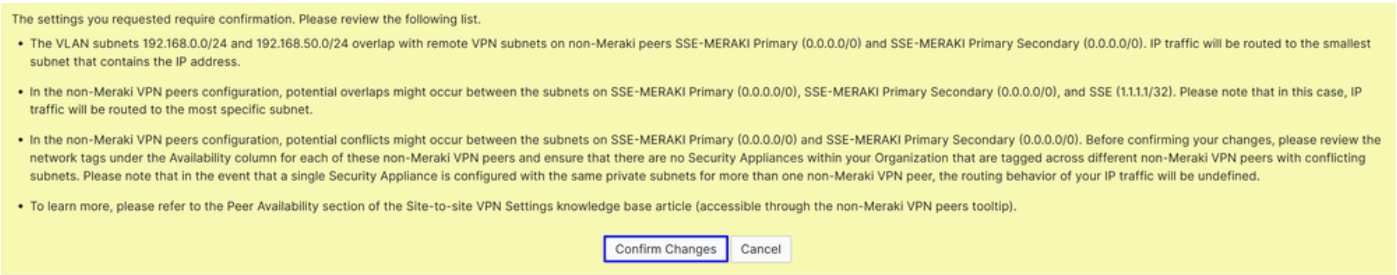


您会发现有些字段是自动填写的。检查它们，进行必要的更改，然后手动完成其余操作：



- 对等体
  - 公共IP或主机名:在Secure Access VPN Configurations步骤中配置**Secondary Datacenter IP**Secure Access给定的
  - 本地ID:在Secure Access VPN Configurations步骤中配置**Secondary Tunnel ID**Secure Access给定的
  - 远程ID:不适用
  - 共享密码：在Secure Access VPN Configurations步**Passphrase**中，配置由Secure Access提供的
- 隧道监控
  - 运行状况检查：使用之前配置的运行状况检查监控隧道可用性

然后，您可以点击，**Save**系统将显示下一个警报：

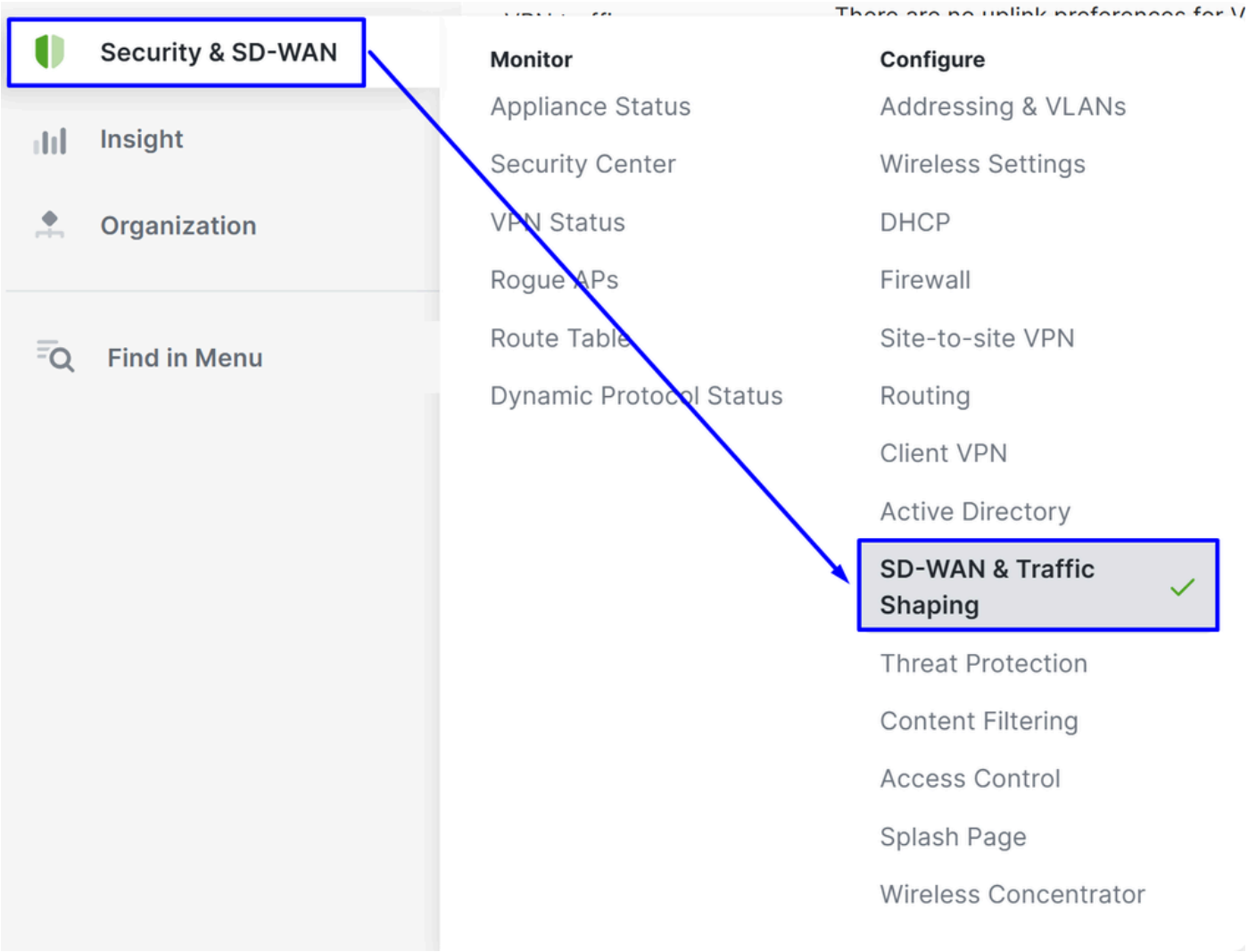


不必担心点击 **Confirm Changes**.

配置流量引导（隧道流量旁路）

此功能允许您通过在SD-WAN旁路配置中定义域或IP地址来旁路来自隧道的特定流量：

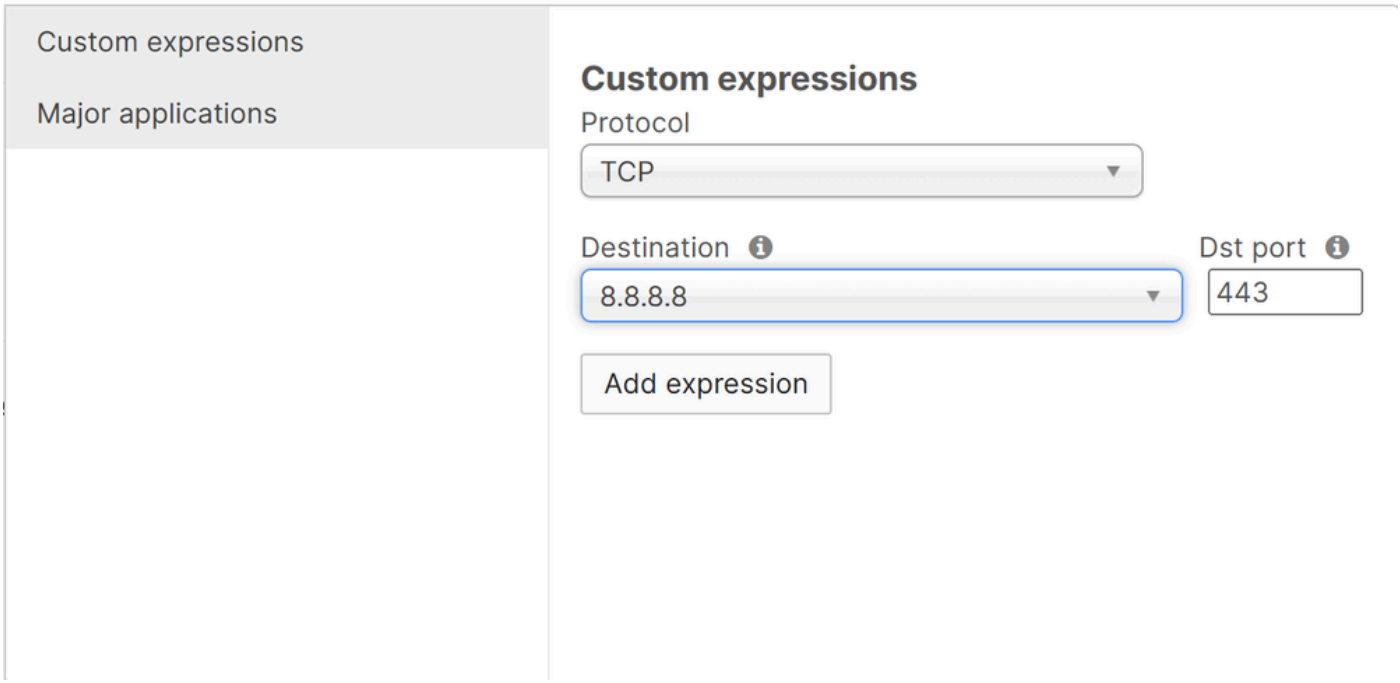
- 导航到**Security & SD-WAN>** SD-WAN & Traffic Shaping



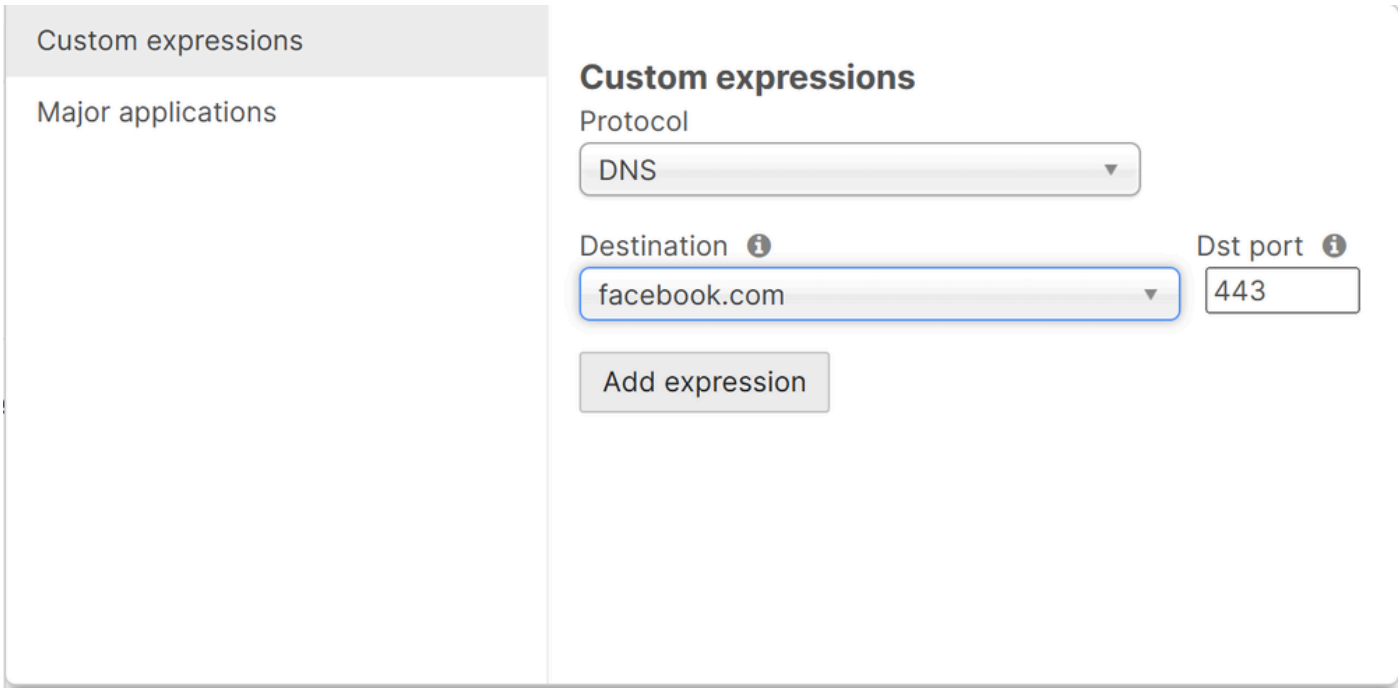
- 向下滚动到部**Local Internet Breakout**分，然后单击 **Add+**

然后根据或创建旁**Custom Expressions**路**Major Applications**由：

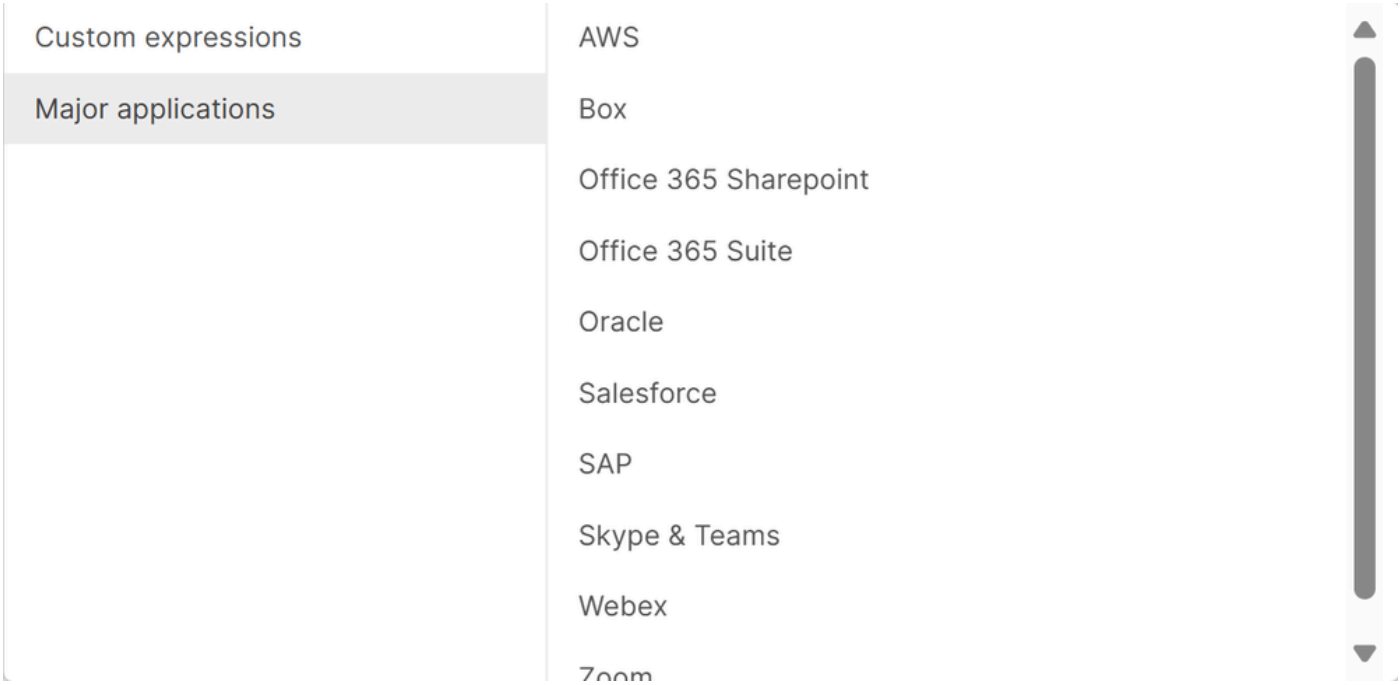
Custom Expressions - Protocol



Custom Expressions - DNS



Major Applications

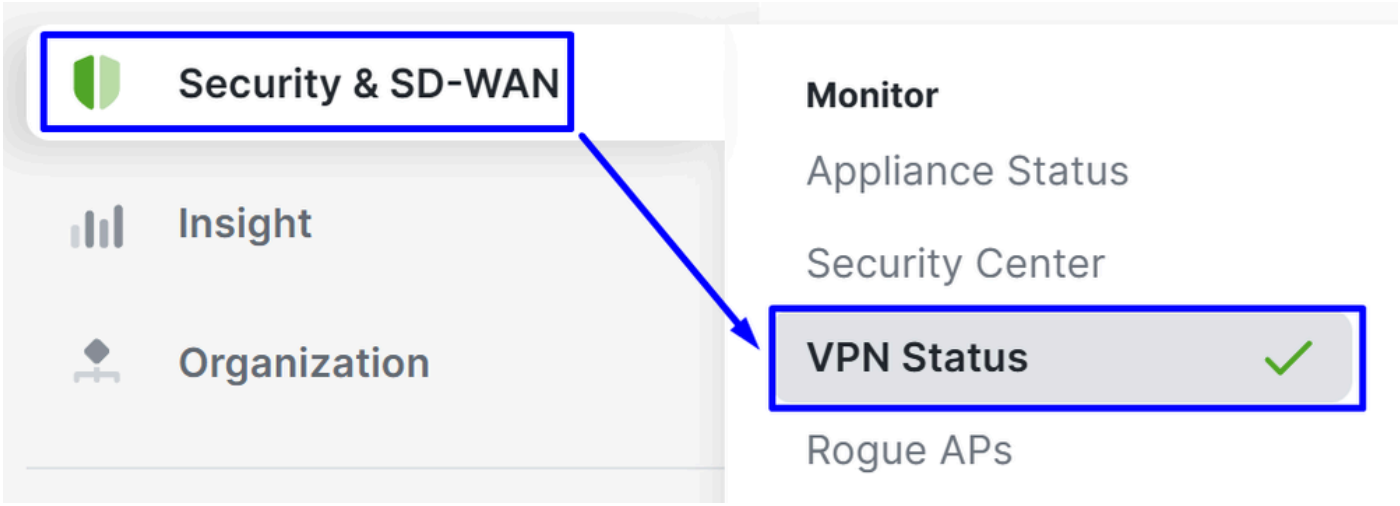


有关详细信息，请访问[：配置VPN排除规则（IP/端口/DNS/APP）]

验证

要检查隧道是否启用，请验证中的状态：

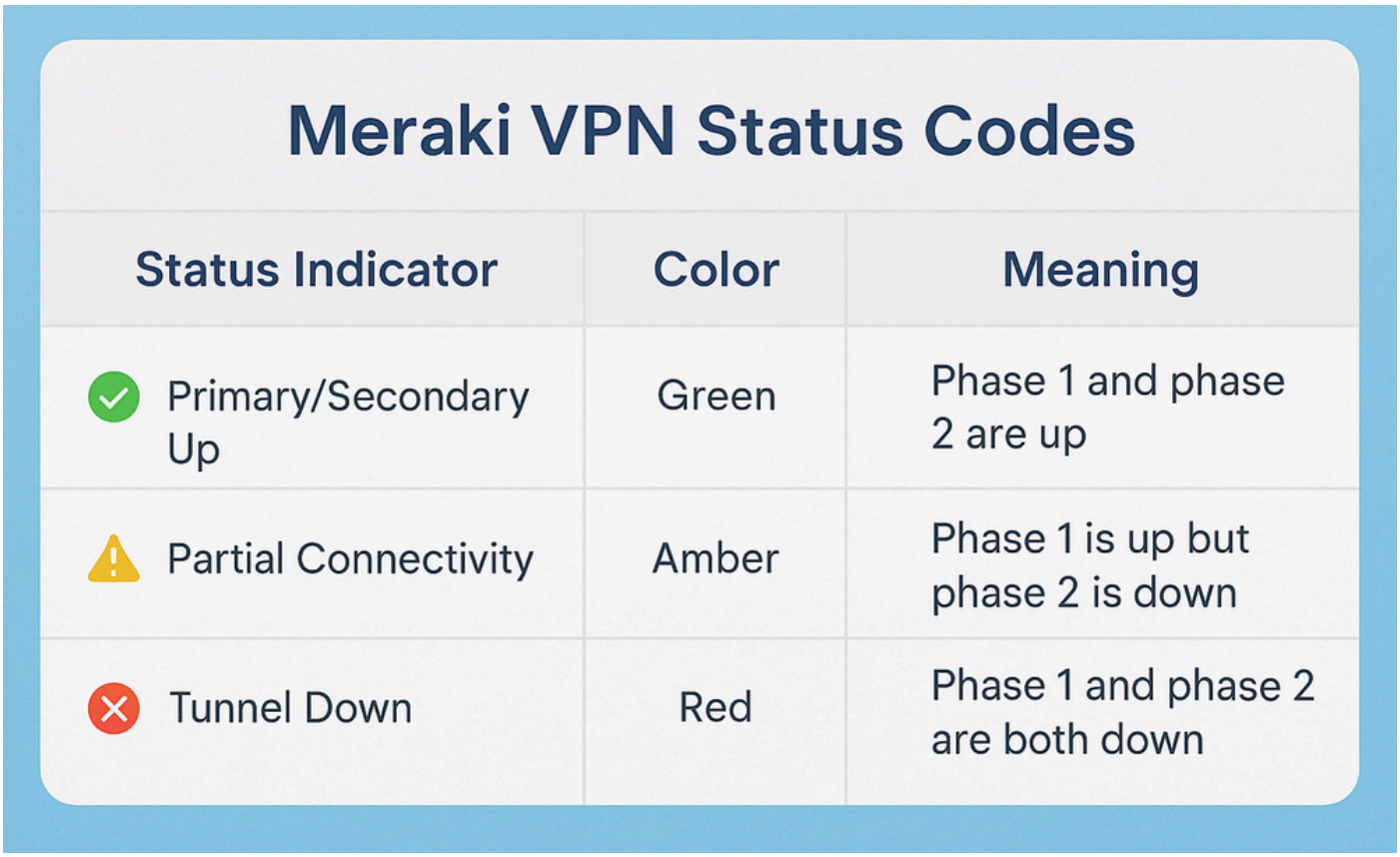
- Security & SD-WAN 在Meraki控**VPN Status**制面板上点击>。



- 点击 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				

如果主要VPN和辅助VPN状态均显示为绿色，则意味着隧道已启用且处于活动状态。



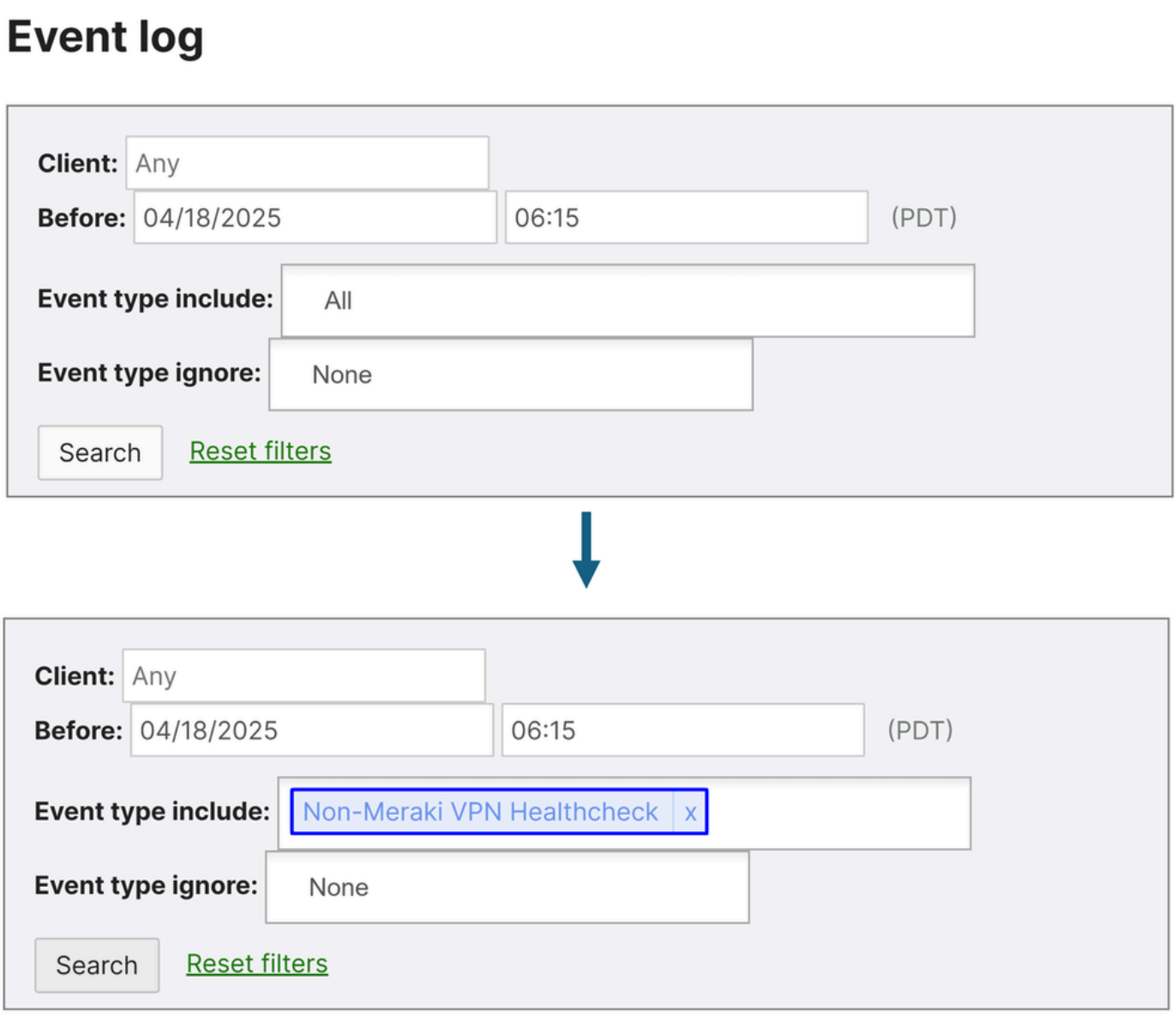
故障排除

验证运行状况检查

要验证VPN的Meraki运行状况检查是否正常工作，请导航至：

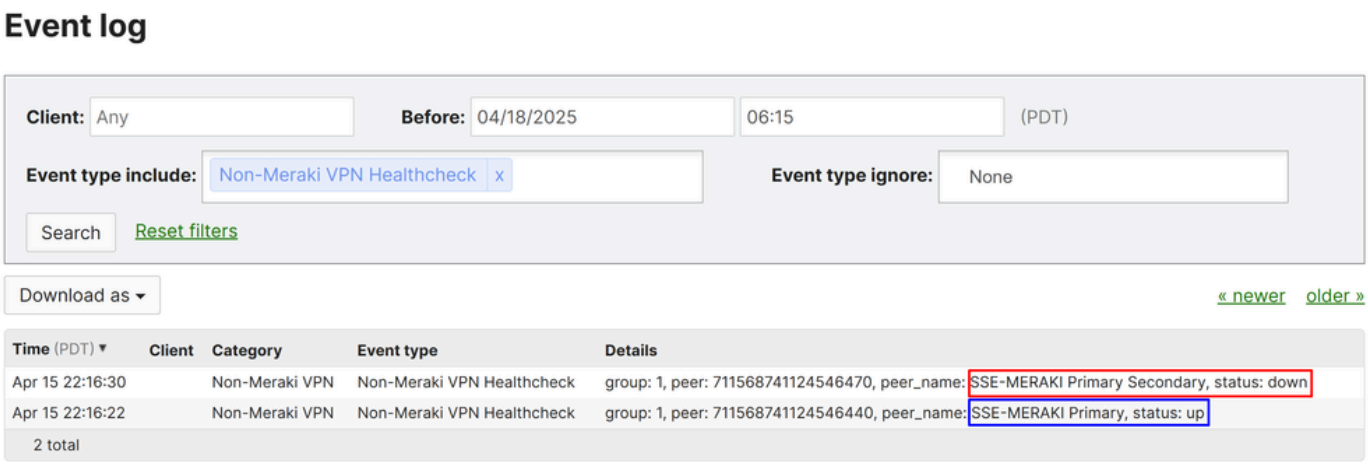
- 点击 **Assurance>** Event Log

在**Event Type Include**下，选择 Non-Meraki VPN Healthcheck



当Cisco安全访问的主要隧道处于活动状态时，会丢弃通过辅助隧道到达的数据包，以保持一致的路由路径。

辅助隧道保持备用，并且仅当主隧道上发生故障时（从Meraki端或在安全访问内，由运行状况检查机制确定）才使用。



- 主隧道运行状况检查显示状态：打开，表示它当前正在传递并主动转发流量。
- 辅助隧道运行状况检查显示状态：关闭，不是因为隧道不可用，而是因为主设备运行正常且正在使用。这是预期行为，因为流量仅允许通过隧道1，从而导致辅助隧道的运行状况检查失败。

相关信息

- 思科技术支持和下载
- 思科安全访问帮助中心
- 思科安全访问Meraki BGP配置指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。