

使用Meraki MX配置安全訪問，以實現高可用性和運行狀況監控

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[在安全訪問中配置VPN](#)

[安全訪問VPN配置](#)

[在Meraki MX上配置VPN](#)

[站點到站點VPN](#)

[VPN設定](#)

[非Meraki VPN對等點](#)

[配置主隧道](#)

[配置輔助隧道](#)

[設定流量導向（通道流量旁路）](#)

[驗證](#)

[疑難排解](#)

[驗證運行狀況檢查](#)

[相關資訊](#)

簡介

本文檔介紹如何使用Meraki MX通過運行狀況檢查配置思科安全訪問以實現高可用性。

必要條件

- [檢視具有安全存取的IPsec通道要求](#)
- 瞭解安全訪問元件
- [瞭解Meraki MX中的運行狀況檢查功能](#)

需求

- Meraki MX必須運行韌體版本19.7.1或更高版本
- 使用專用訪問時，由於Meraki的限制阻止更改運行狀況檢查IP，使得其他SPA（安全專用訪問）隧道需要NAT，因此僅支援一個隧道。在使用SIA（安全Internet訪問）時該選項不適用。
- 明確定義哪些內部子網或資源通過隧道路由到安全訪問。

採用元件

- Cisco Secure Access
- Meraki MX安全裝置 (韌體版本19.7.1或更高版本)
- Meraki 儀表板
- 安全訪問控制面板

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊



思科安全訪問是一個雲原生安全平台，可實現對私有應用 (通過私有訪問) 和網際網路目標 (通過網際網路訪問) 的安全訪問。與Meraki MX整合後，組織可以在分支機構站點和雲之間建立安全的IPsec隧道，從而確保加密流量和集中安全實施。

此整合使用靜態路由IPsec隧道。Meraki MX建立到Cisco Secure Access的主和輔助IPsec隧道，並利用其內建的上行鏈路運行狀況檢查在隧道之間執行自動故障切換。這為分支機構連線提供了可復

原的高可用性配置。

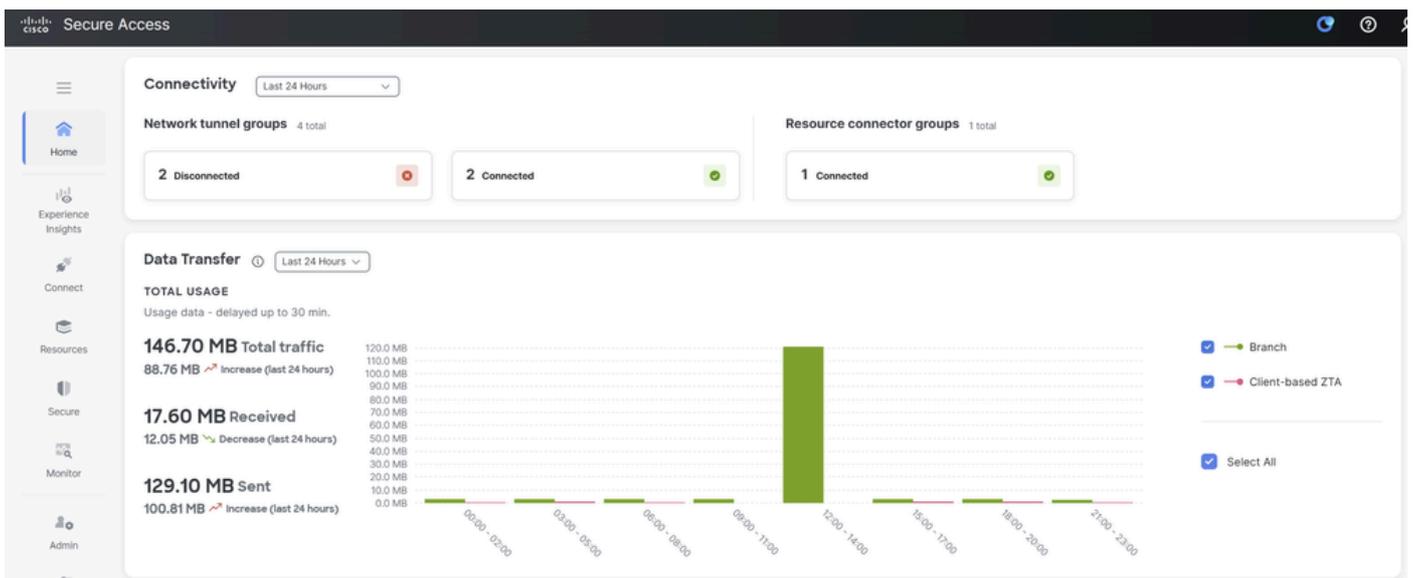
此部署的關鍵要素包括：

- Meraki MX充當思科安全訪問的非Meraki VPN對等體。
- 靜態配置主隧道和輔助隧道，使用運行狀況檢查確定可用性。
- 私有訪問支援通過SPA（安全私有訪問）安全訪問內部應用，而網際網路訪問允許流量通過雲中的策略實施訪問基於網際網路的資源。
- 由於運行狀況檢查IP靈活性中的Meraki限制，在專用訪問模式下僅支援一個隧道組。如果多個Meraki MX裝置需要連線到專用訪問的安全訪問，您必須使用BGP進行動態路由，或配置靜態隧道，同時瞭解只有一個網路隧道組可以支援運行狀況檢查和高可用性。其他隧道無需運行狀況監控或冗餘即可運行。

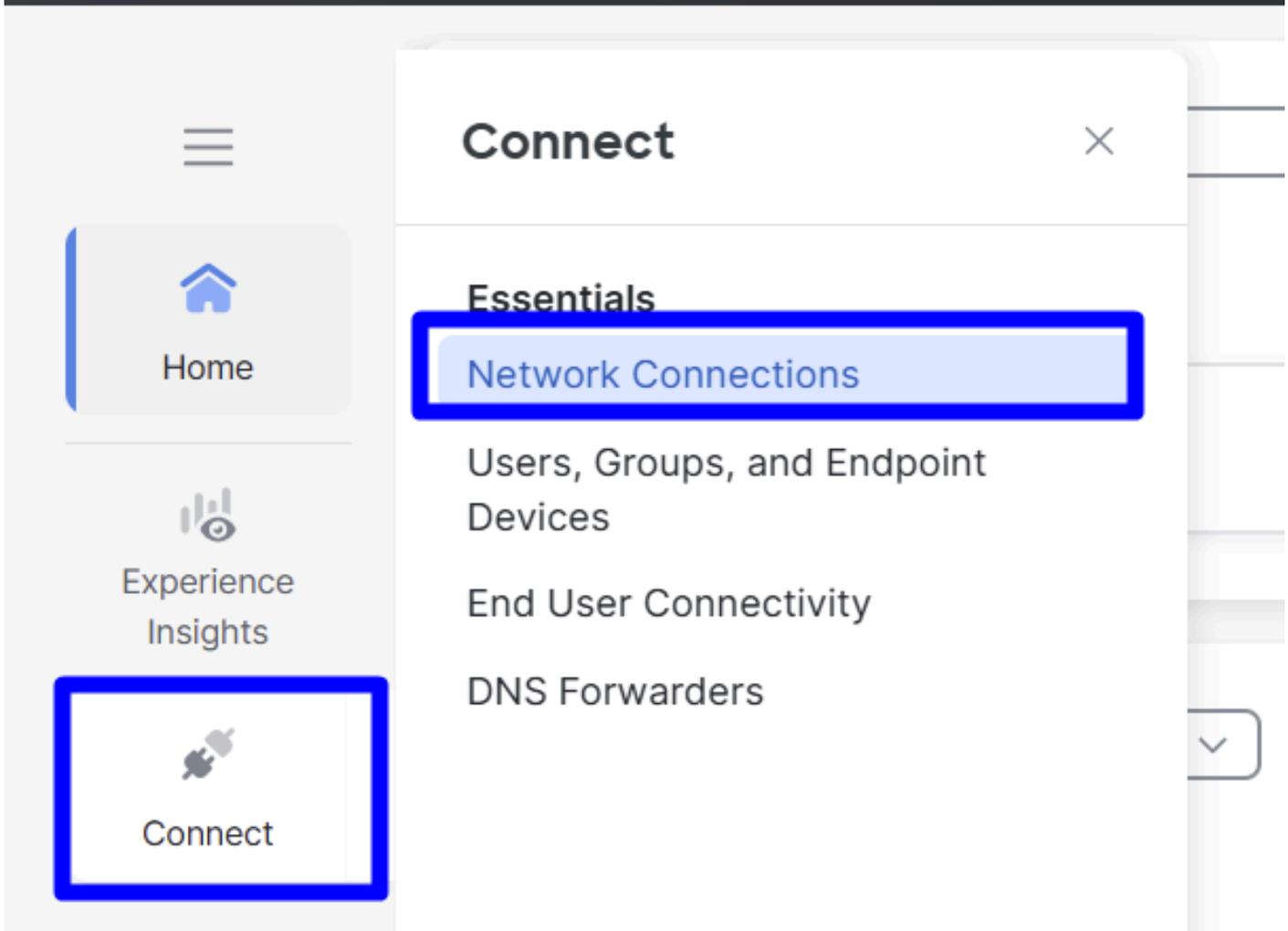
設定

在安全訪問中配置VPN

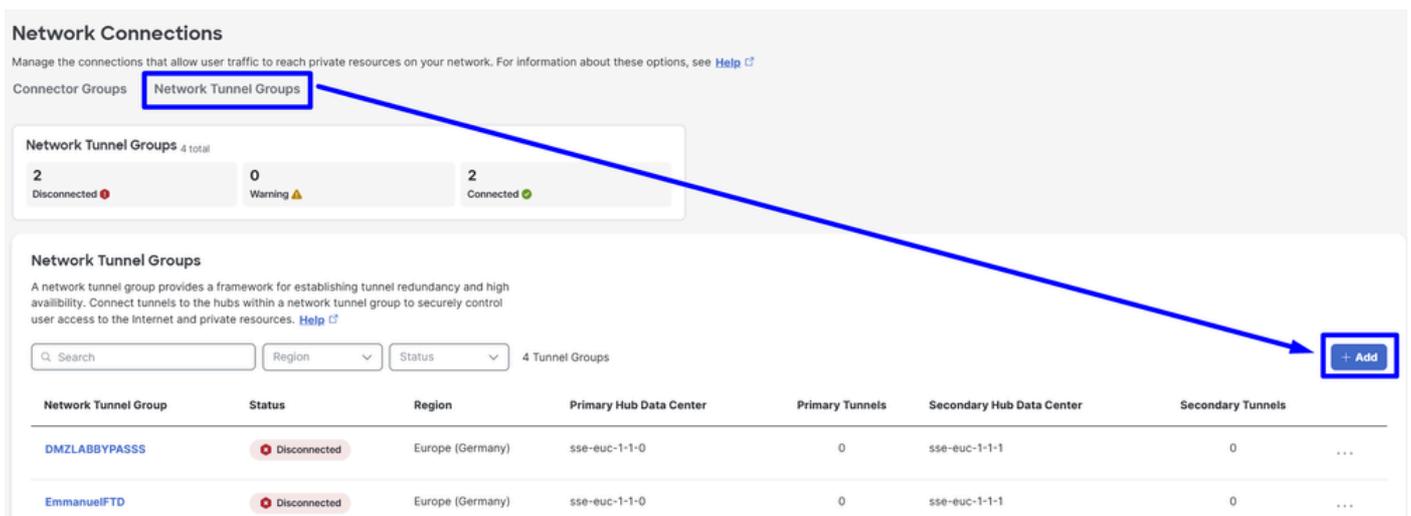
導航到[Secure Access](#)的管理面板。



- 按一下 [Connect > Network Connections](#)



- 在Network Tunnel Groups 下，按一下 + Add



- Configure Tunnel Group Name, Region 和 Device Type
- 按一下 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
MERAKE

Region
Europe (Germany)

Device Type
Meraki MX

Cancel Next

- 配置 Tunnel ID Format 和 Passphrase
- 按一下 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

- 配置網路上已配置且希望通過 Secure Access 傳輸流量的 IP 地址範圍或主機，並確保包括 Meraki 監控探測 IP 192.0.2.3/32，以允許從 Secure Access 返回流量到 Meraki MX。
- 按一下 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.

Meraki MX Probe IP

192.0.2.3/32 192.168.50.0/24

Dynamic routing

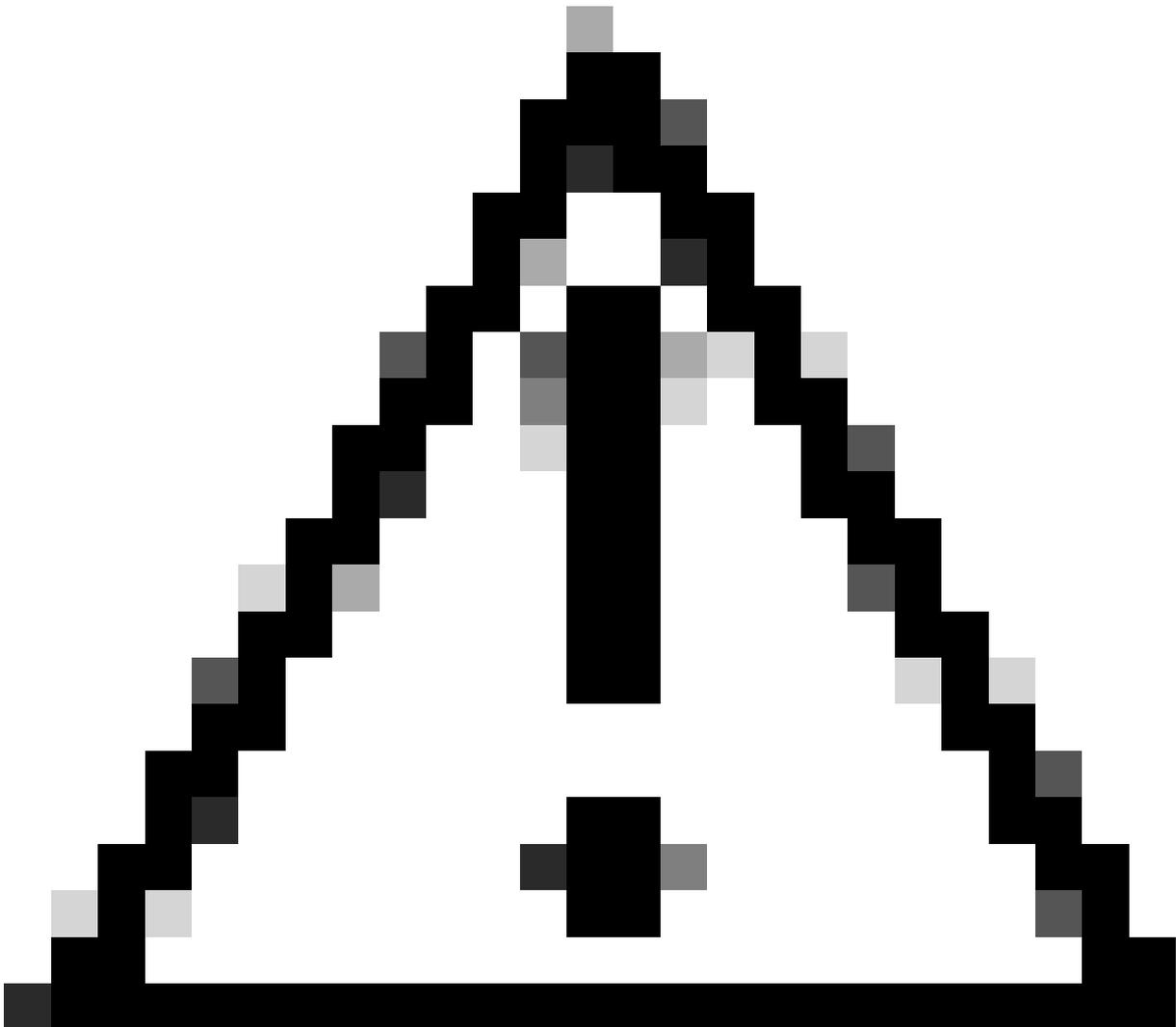
Use this option when you have a BGP peer for your on-premise router.



Cancel

Back

Save



注意：請務必新增監控探測IP(192.0.2.3/32);否則，您可能會遇到將流量路由到ZTNA使用的Internet、VPN池和CGNAT範圍100.64.0.0/10的Meraki裝置上的流量問題。

- 按一下顯示的Save「通道資訊」後，請儲存下一步的相關資訊。 **Configure the tunnel on Meraki MX.**

安全訪問VPN配置

在記事本中複製隧道的配置，使用此資訊完成Meraki中的配Non-Meraki VPN Peers置。

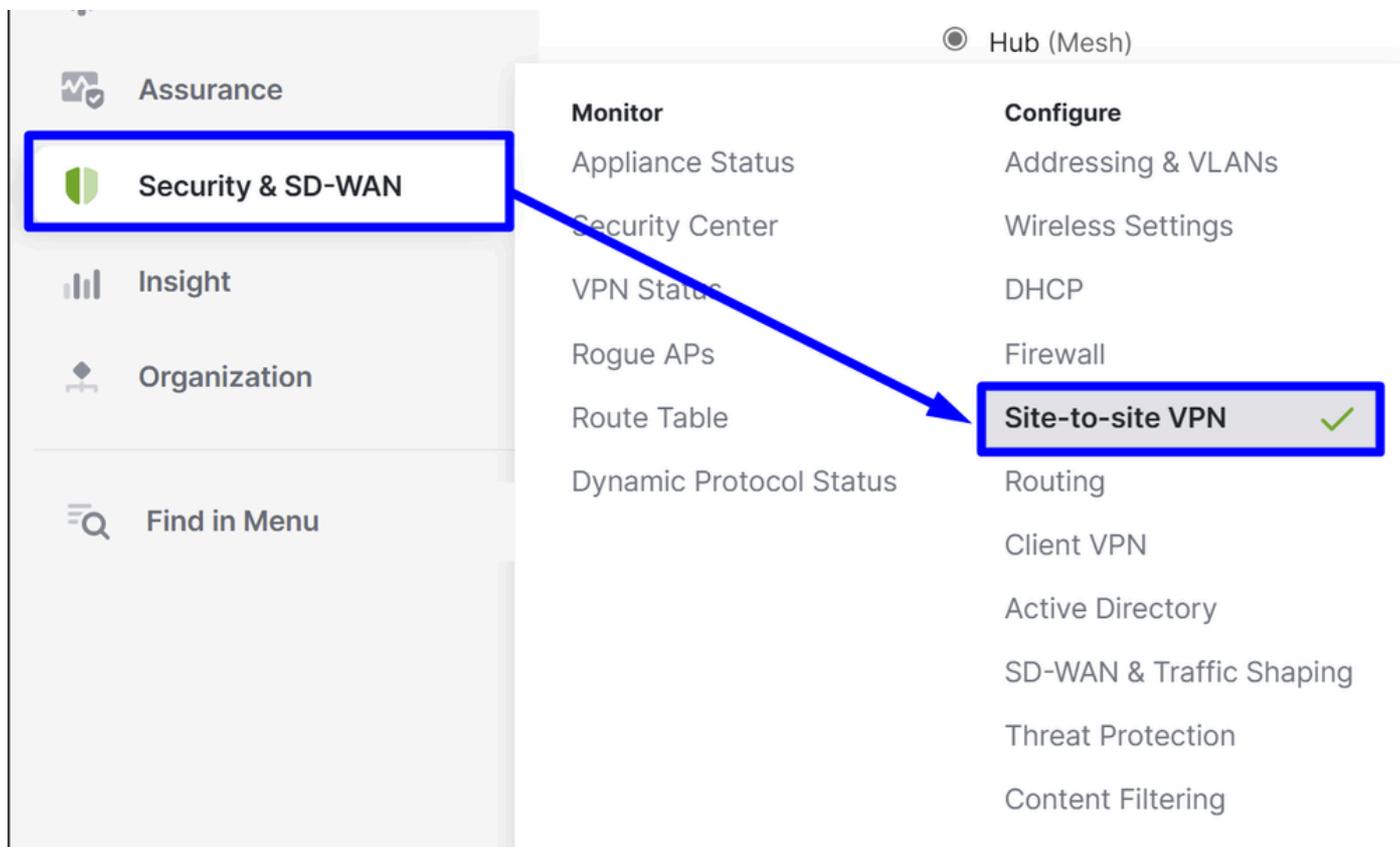
The screenshot shows the 'Data for Tunnel Setup' configuration page in the Meraki MX interface. On the left, there is a navigation menu with four items: 'General Settings', 'Tunnel ID and Passphrase', 'Routing', and 'Data for Tunnel Setup' (which is currently selected). The main content area is titled 'Data for Tunnel Setup' and contains the following information:

Data for Tunnel Setup	
Review and save the following information for use when setting up your network tunnel devices.	
Primary Tunnel ID:	MerakiShadow@ [redacted] [copy icon]
Primary Data Center IP Address:	18.156.145.74 [copy icon]
Secondary Tunnel ID:	MerakiShadow@ [redacted] [copy icon]
Secondary Data Center IP Address:	3.120.45.23 [copy icon]

At the bottom right of the page, there are two buttons: 'Download CSV' and 'Done'.

在Meraki MX上配置VPN

導航到Meraki MX並按一下Security & SD-WAN> Site-to-site VPN



站點到站點VPN

選擇 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.

VPN設定

選擇要將流量傳送到安全訪問的網路：

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	

在「NAT Traversal Automatic(自動)」中選擇

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.

非Meraki VPN對等點

您需要配置Meraki用於將流量路由到安全訪問的運行狀況檢查：

按一下 **Configure Health Checks**

- 按一下 **+Add health Check**

Health check

Endpoint

http://

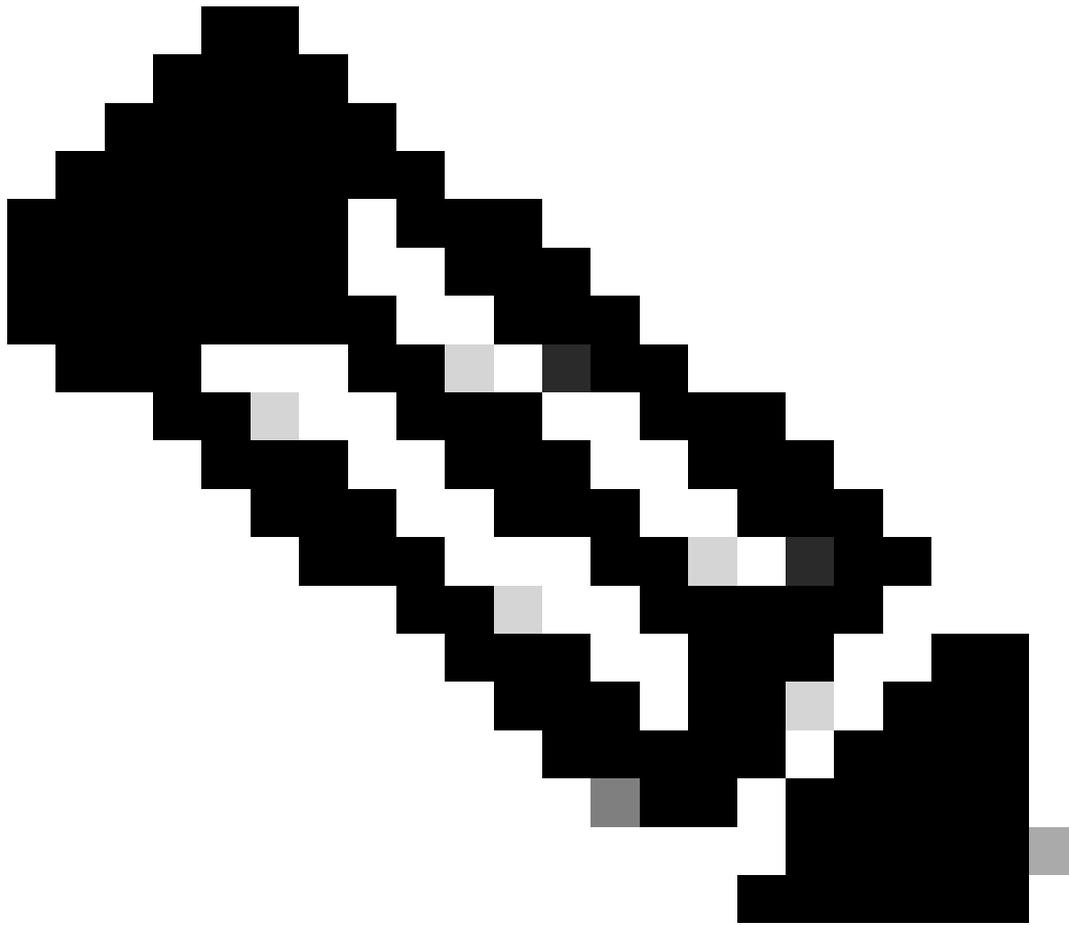
Cancel

Done



Health check name
can't be blank.

- **Health Check:**配置測試的名稱
- **Endpoint:**使用安全訪問推薦的方法 <http://service.sig.umbrella.com>



附註：僅當通過具有Secure Access或Umbrella的站點到站點隧道訪問時，此域才會響應：從這些隧道外部進行的訪問嘗試失敗。

然後單Done擊兩次以完成。

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"/>	Cancel Done

Rows per page < >

Cancel **Done**

現在，您的運行狀況檢查已配置，並且您準備配置 Peer:

配置主隧道

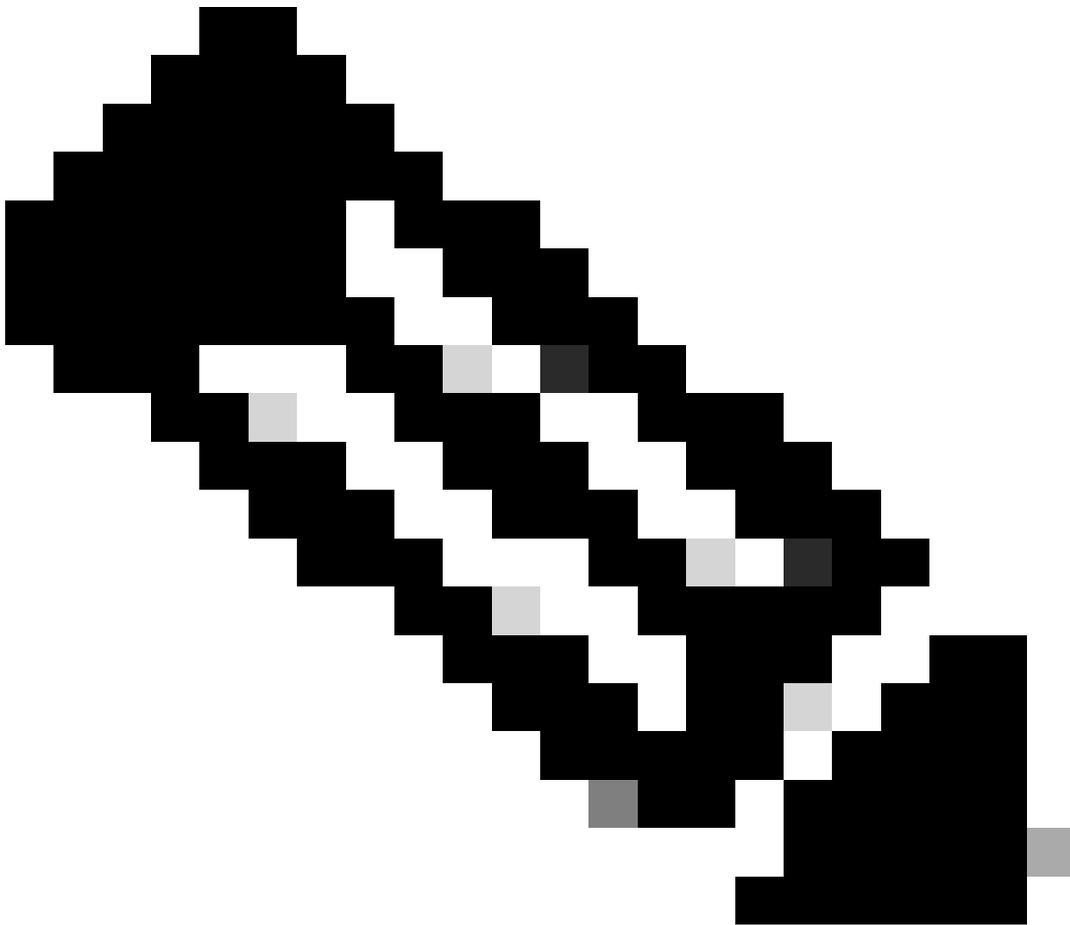
- 按一下 +Add a peer

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

- 新增VPN對等點
 - 名稱:為VPN配置安全訪問名稱
 - IKE版本:選擇IKEv2
- 同儕節點
 - 公共IP或主機名:Primary Datacenter IP在[Secure Access VPN Configurations](#)步驟中配置由安全訪問提供的
 - 本地ID:Primary Tunnel ID在[Secure Access VPN Configurations](#)步驟中配置由安全訪問提供的
 - 遠端ID:不適用
 - 共用密碼:在[Secure Access VPN Configurations](#)Passphrase步驟中配置由安全訪問提供的

金鑰

- 路由:選擇靜態
 - 專用子網：如果計畫同時配置Internet接入和專用接入，請使用0.0.0.0/0作為目標。如果只為該VPN隧道配置專用接入，請將和Remote Access VPN IP PoolCGNAT範圍指定為100.64.0.0/10目標網路
 - 可用性：如果您只有一個Meraki裝置，則可以選All Networks擇。如果有多個裝置，請確保僅選擇要在其中配置隧道的特定Meraki網路。
- 通道監控
 - 運行狀況檢查：使用先前配置的運行狀況檢查來監控通道可用性
 - 直接故障轉移到Internet：如果啟用此選項，並且隧道1和隧道2的運行狀況檢查均失敗，則流量將重定向到WAN介面以防止丟失網際網路訪問。
-



運行狀況檢查功能：如果隧道1受到監控且其運行狀況檢查失敗，則流量會自動故障轉移到隧道2。如果隧道2也發生故障，並且啟用該選Failover directly to Internet，則流量通過Meraki裝置的WAN介面進行路由。

- 預設：選擇 Umbrella

然後單Save擊。

配置輔助隧道

要配置輔助隧道，請按一下主隧道的選項選單：

- 按一下三個點

#	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 >

- 按一下 + Add Secondary peer

Primary



Edit primary peer



Move to



Delete primary peer

Secondary



Add secondary peer

- 按一下 `Inherit primary peer configurations`

Add Secondary VPN Peer



Inherit primary peer configurations



Name

SSE Secondary

IKE version

IKEv2

您會注意到有些欄位是自動填寫的。檢查它們，進行任何必要的更改，然後手動完成其餘操作：

Peers ^

Public IP or Hostname

Local ID

Remote ID i

Shared secret

 Show

Routing

Static

Private subnets i

0.0.0.0/0

Tunnel monitoring

Health check

 ⊗ ▾

- 同儕節點

- 公共IP或主機名:Secondary Datacenter IP在[Secure Access VPN Configurations](#)步驟中配置由安全訪問提供的
- 本地ID:Secondary Tunnel ID在[Secure Access VPN Configurations](#)步驟中配置由安全訪問提供的
- 遠端ID:不適用
- 共用密碼：在[Secure Access VPN Configurations](#)Passphrase步驟中配置由安全訪問提供的金鑰

- 通道監控

- 運行狀況檢查：使用先前配置的運行狀況檢查來監控通道可用性

然後，您可以點選Save下一個警報：

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).

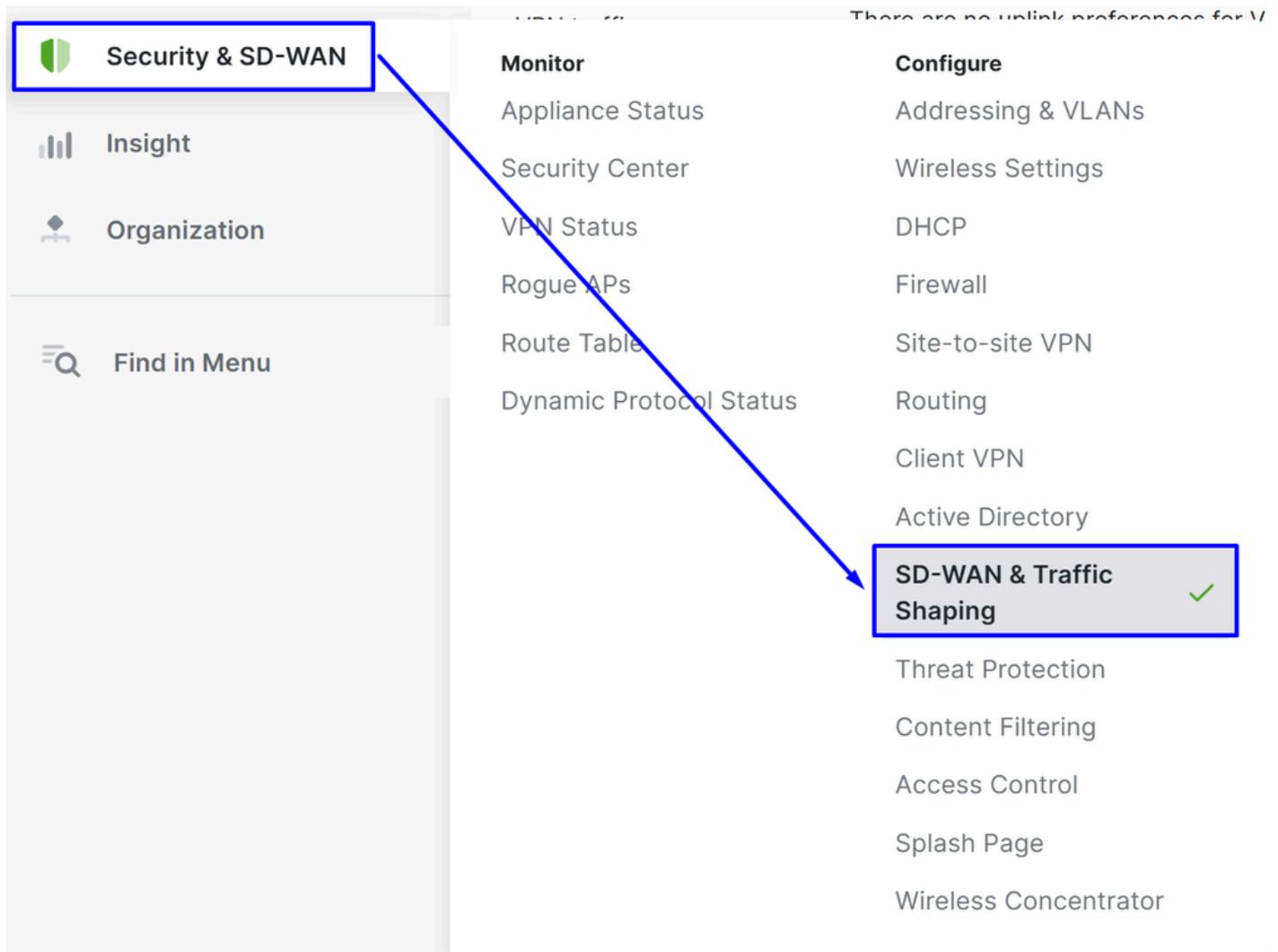
Confirm Changes Cancel

不用擔心按一下 **Confirm Changes**.

設定流量導向（通道流量旁路）

此功能允許您通過在SD-WAN旁路配置中定義域或IP地址來旁路來自隧道的特定流量：

- 導航至Security & SD-WAN > SD-WAN & Traffic Shaping



- 向下滾動到部Local Internet Breakout分，然後按一下 Add+

Local internet breakout

VPN exclusion rules

Add +

然後根據或以下條件建立Custom Expressions旁路Major Applications路：

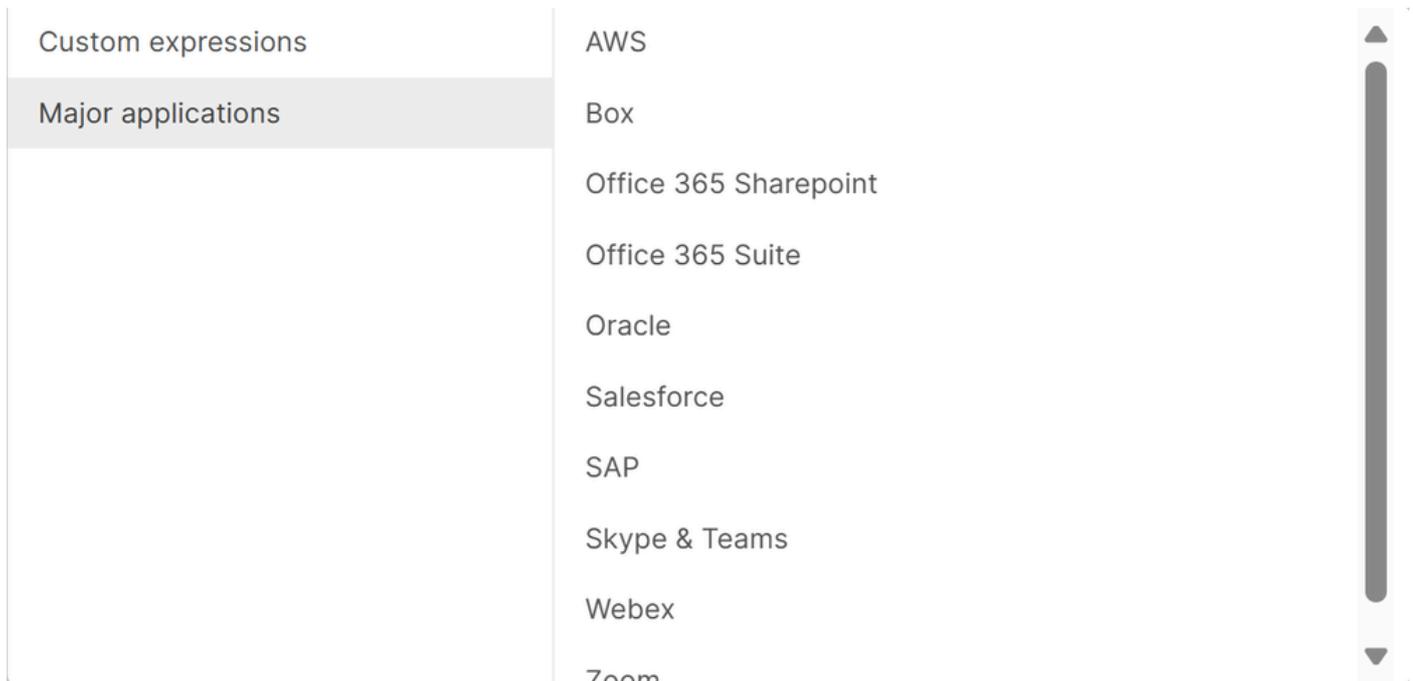
Custom Expressions - Protocol

Custom expressions	<h3>Custom expressions</h3> <p>Protocol</p> <p>TCP</p> <p>Destination ⓘ</p> <p>8.8.8.8</p> <p>Dst port ⓘ</p> <p>443</p> <p>Add expression</p>
Major applications	

Custom Expressions - DNS

Custom expressions	<h3>Custom expressions</h3> <p>Protocol</p> <p>DNS</p> <p>Destination ⓘ</p> <p>facebook.com</p> <p>Dst port ⓘ</p> <p>443</p> <p>Add expression</p>
Major applications	

Major Applications

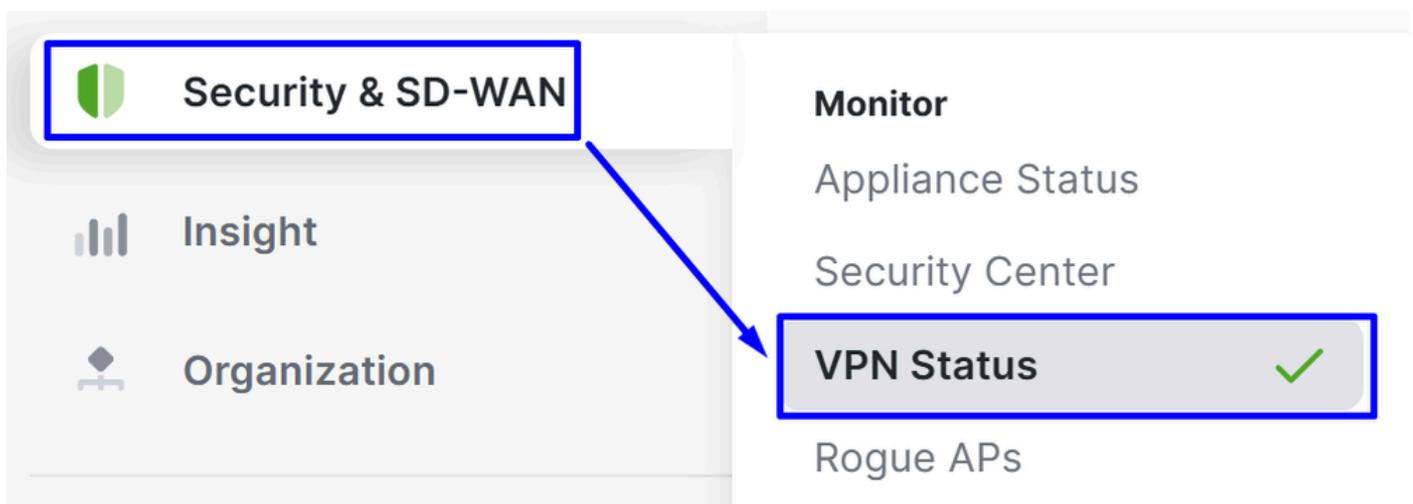


有關詳細資訊，請訪問：[配置VPN排除規則 \(IP/埠/DNS/APP \)](#)

驗證

要檢查通道是否啟用，請驗證中的狀態：

- 在Meraki儀表板VPN Status上按一下Security & SD-WAN>。



- 按一下 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VPN和輔助VPN狀態均顯示為綠色，則表示隧道處於啟用和活動狀態。

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

疑難排解

驗證運行狀況檢查

要驗證針對VPN的Meraki運行狀況檢查是否正常工作，請導航至：

- 按一下 Assurance > Event Log

Event log

Client:

Before: (PDT)

Event type include:

Event type ignore:

[Reset filters](#)

在Event Type Include下，選擇 Non-Meraki VPN Healthcheck

Event log

Client:

Before: (PDT)

Event type include:

Event type ignore:

[Reset filters](#)



Client:

Before: (PDT)

Event type include:

Event type ignore:

[Reset filters](#)

當通往Cisco Secure Access的主要隧道處於活動狀態時，通過輔助隧道到達的資料包將被丟棄，以保持一致的路由路徑。

輔助隧道保持待機狀態，並且僅當主隧道發生故障時（從Meraki端或在安全訪問內，由運行狀況檢查機制確定）才使用。

Event log

Client: Before: (PDT)

Event type include: Event type ignore:

[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

- 主隧道運行狀況檢查顯示狀態：up，表示它當前正在傳遞並主動轉發流量。
- 輔助隧道運行狀況檢查顯示狀態：關閉，不是因為通道不可用，而是因為主裝置運行正常且正在使用。這是預期行為，因為流量僅允許通過隧道1，從而導致輔助隧道的運行狀況檢查失敗。

相關資訊

- [思科技術支援與下載](#)
- [Cisco Secure Access幫助中心](#)
- [Cisco Secure Access Meraki BGP配置指南](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。