

Meraki MXでセキュアなアクセスを設定し、ハイ アベイラビリティとヘルスマモニタリングを実現

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[セキュアアクセスでのVPNの設定](#)

[セキュアアクセスVPNの設定](#)

[Meraki MXでのVPNの設定](#)

[サイト間VPN](#)

[VPNの設定](#)

[Meraki以外のVPNピア](#)

[プライマリトンネルの設定](#)

[セカンダリトンネルの設定](#)

[トラフィックステアリングの設定 \(トンネルトラフィックバイパス\)](#)

[確認](#)

[トラブルシュート](#)

[ヘルスチェックの確認](#)

[関連情報](#)

はじめに

このドキュメントでは、ヘルスチェックを使用してCisco Secure Access with Meraki MXをハイアベイラビリティに設定する方法について説明します。

前提条件

- [セキュアアクセスを使用したIPSecトンネル要件の確認](#)
- セキュアアクセスコンポーネントの理解
- [Meraki MXのヘルスチェック機能について](#)

要件

- Meraki MXはファームウェアバージョン19.1.6以降を実行している必要があります。
- プライベートアクセスを使用する場合、ヘルスチェックIPの変更を妨げるMerakiの制限により、1つのトンネルのみがサポートされ、追加のSPA (セキュアプライベートアクセス) トンネルにNATが必要になります。これは、SIA (セキュアインターネットアクセス) を使用

している場合は適用されません。

- どの内部サブネットまたはリソースがトンネル経由でセキュアアクセスにルーティングされるかを明確に定義します。

使用するコンポーネント

- シスコセキュアアクセス
- Meraki MXセキュリティアプライアンス (ファームウェアバージョン19.1.6以降)
- Meraki ダッシュボード
- セキュアアクセスダッシュボード

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明



Cisco Secure Accessは、プライベートアプリケーション（プライベートアクセス経由）とインターネット接続先（インターネットアクセス経由）の両方へのセキュアなアクセスを可能にする、クラウドネイティブのセキュリティプラットフォームです。Meraki MXと統合すると、組織はブランチサイトとクラウドの間にセキュアなIPsecトンネルを確立し、暗号化されたトラフィックフローと一元化されたセキュリティを確実に適用できるようになります。

この統合では、スタティックルーティングIPsecトンネルを使用します。Meraki MXは、Cisco Secure AccessへのプライマリおよびセカンダリIPsecトンネルを確立し、トンネル間の自動フェールオーバーを実行するために組み込みのアップリンクヘルスチェックを活用します。これにより、復元力のあるハイアベイラビリティ設定がブランチ接続に提供されます。

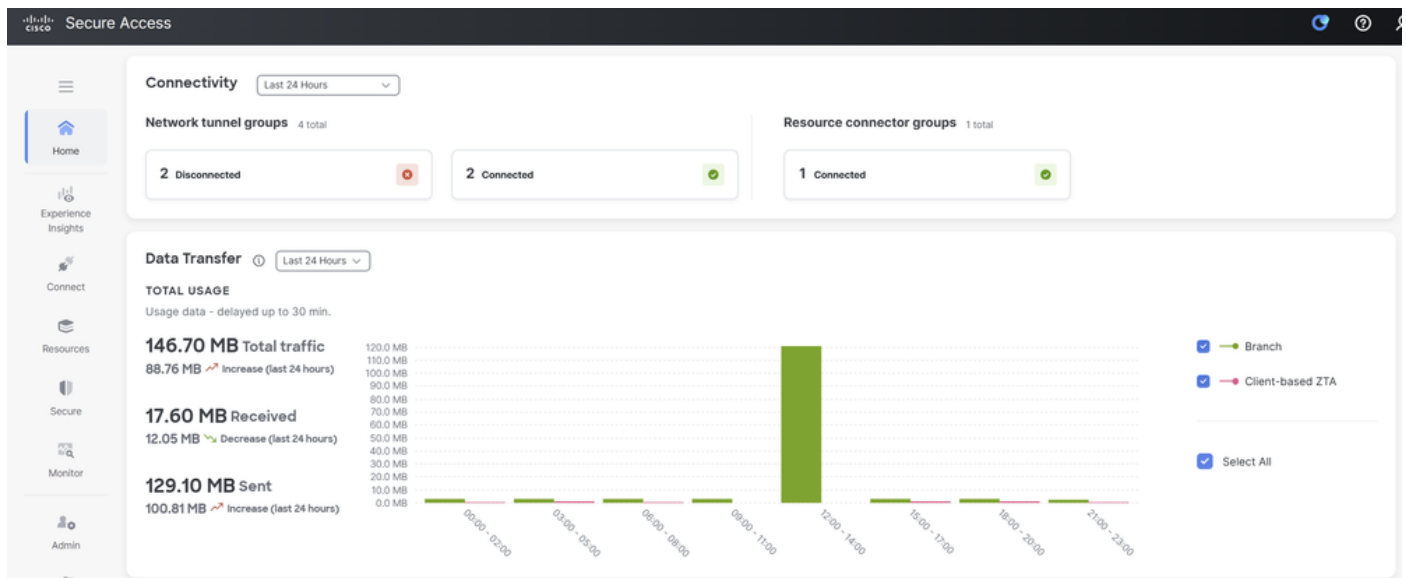
この導入の主な要素は次のとおりです。

- Cisco Secure Accessに対する非Meraki VPNピアとして機能するMeraki MX
- アベイラビリティを決定するヘルスチェックを使用して静的に設定されたプライマリおよびセカンダリトンネル
- プライベートアクセスは、SPA（セキュアプライベートアクセス）を介した内部アプリケーションへのセキュアなアクセスをサポートします。インターネットアクセスは、クラウドでポリシーを適用することで、トラフィックがインターネットベースのリソースに到達できるようにします。
- ヘルスチェックIPの柔軟性に関するMerakiの制限により、プライベートアクセスモードでは1つのトンネルグループのみがサポートされます。複数のMeraki MXデバイスをプライベートアクセスのセキュアアクセスに接続する必要がある場合は、[BGP](#)を使用してダイナミックルーティングを行うか、またはスタティックトンネルを設定する必要があります。これにより、1つのネットワークトンネルグループのみがヘルスチェックとハイアベイラビリティをサポートできることがわかります。追加のトンネルは、ヘルスマモニタリングや冗長性なしで動作します。

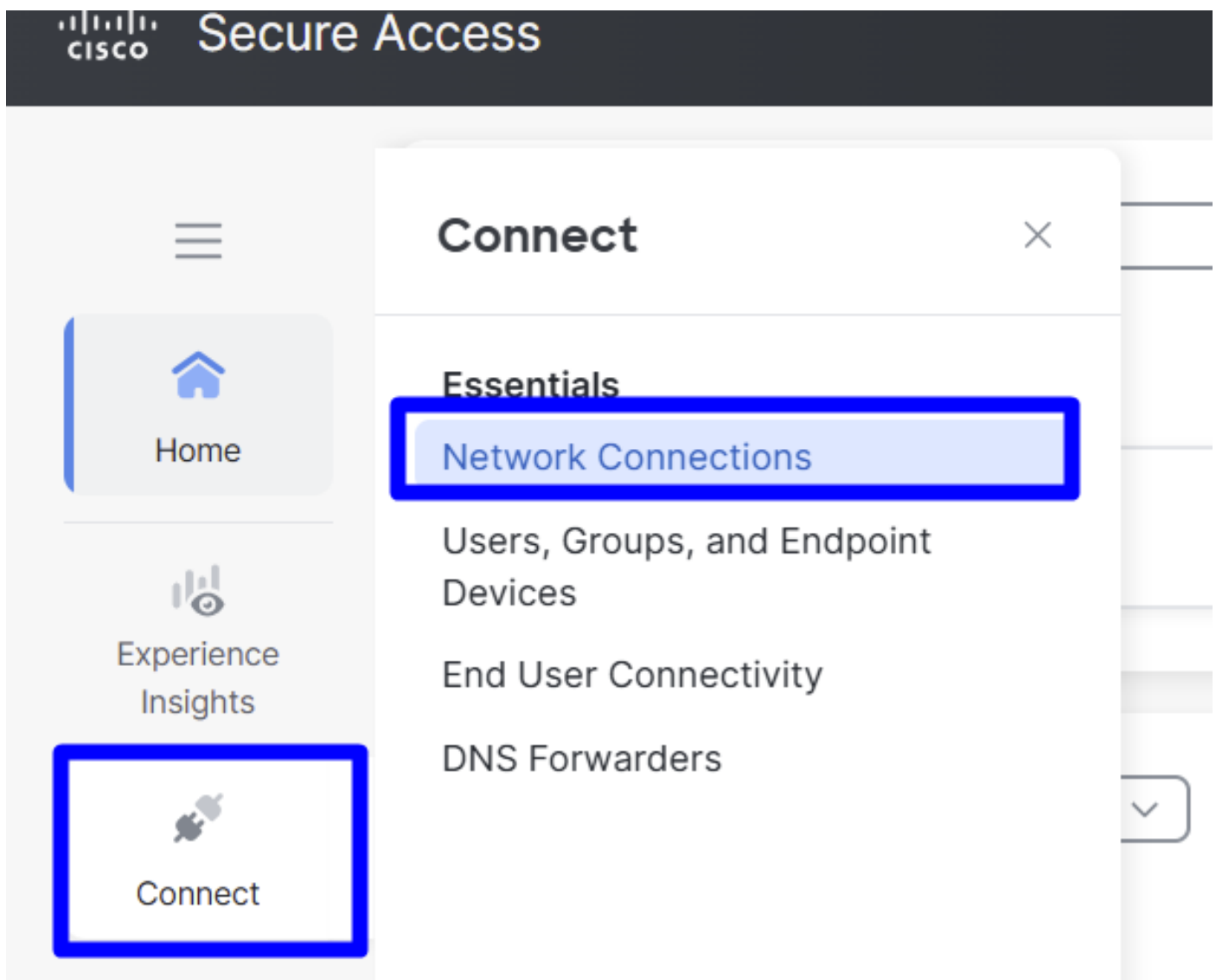
設定

セキュアアクセスでのVPNの設定

[Secure Access](#)の管理パネルに移動します。



- クリック Connect > Network Connections



- 「Network Tunnel Groups」で、 + 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
DMZLABYPASSS	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

- Tunnel Group Name、Regionの設定
- [保存 (Next

1 General Settings

2 Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup

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](#)

- Tunnel ID Formatコマンドと Passphrase
- [保存 (Next

1 General Settings

2 Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup

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](#)

- ネットワークに設定したIPアドレス範囲またはホストを設定し、トラフィックをセキュアアクセス経由で送信し、セキュアアクセスからMeraki MXへのリターントラフィックを許可するMeraki監視プローブIP 192.0.2.3/32を含めることを確認します。

• [保存 (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



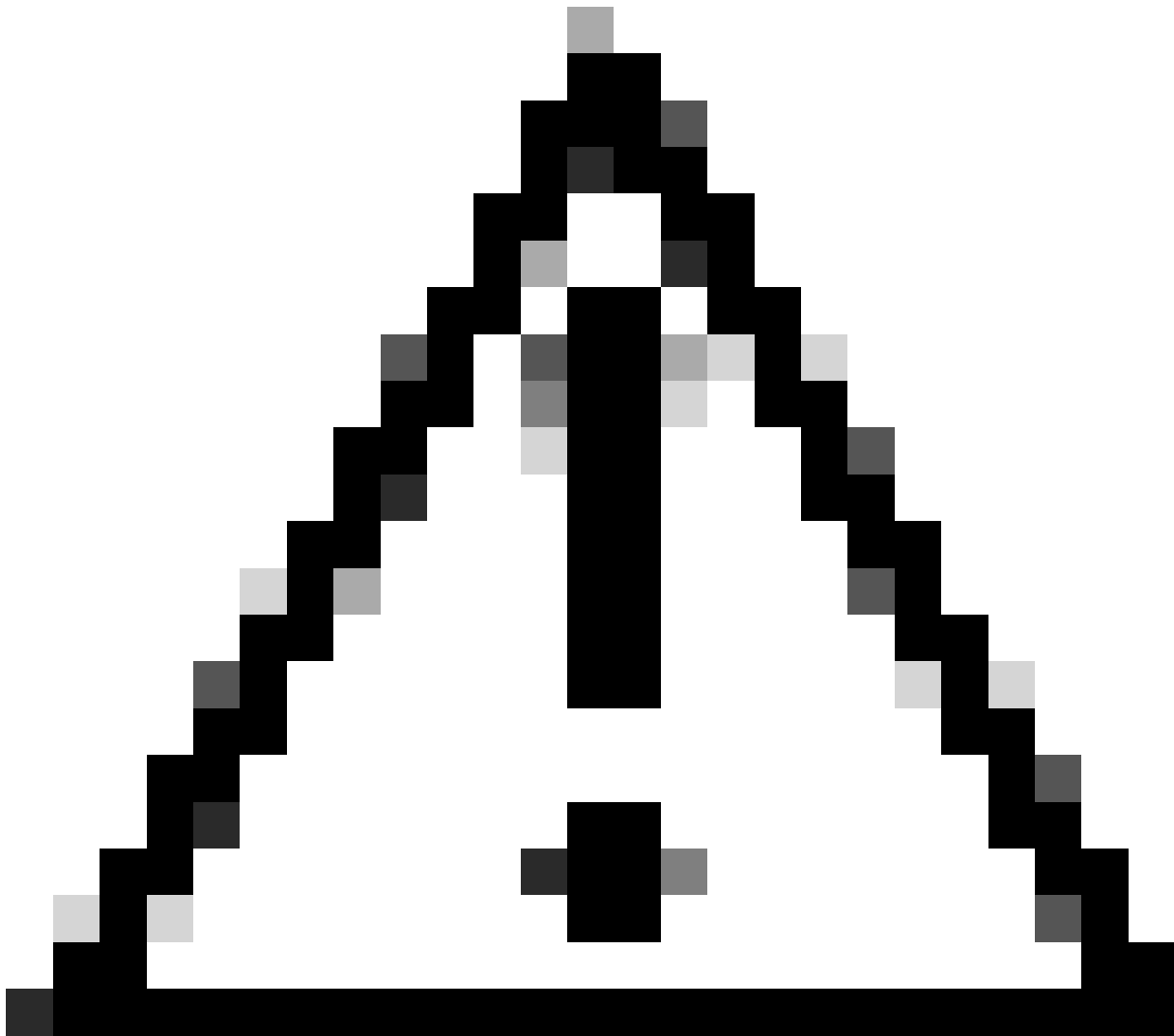
Cancel

Back

Save

Meraki MX Probe IP





注意：必ずモニタリングプロープIP(192.0.2.3/32)を追加してください。そうしないと、Merakiデバイスで、トラフィックをインターネット、VPNプール、およびZTNAで使用されるCGNAT範囲100.64.0.0/10にルーティングする際に、トラフィックの問題が発生する可能性があります。

-
- トンネルに関する情報が表示されるSaveをクリックした後、次の手順のためにその情報を保存してください。 **Configure the tunnel on Meraki MX.**

セキュアアクセスVPNの設定

トンネルの設定をメモ帳にコピーします。この情報を使用して、Meraki Non-Meraki VPN Peersの設定を完了します。

✓ General Settings

✓ Tunnel ID and Passphrase

✓ Routing

✓ Data for Tunnel Setup

Data for Tunnel Setup

Review and save the following information for use when setting up your network tunnel devices.

Primary Tunnel ID:

MerakiShadow@

Primary Data Center IP Address:

18.156.145.74

Secondary Tunnel ID:

MerakiShadow@

Secondary Data Center IP Address:

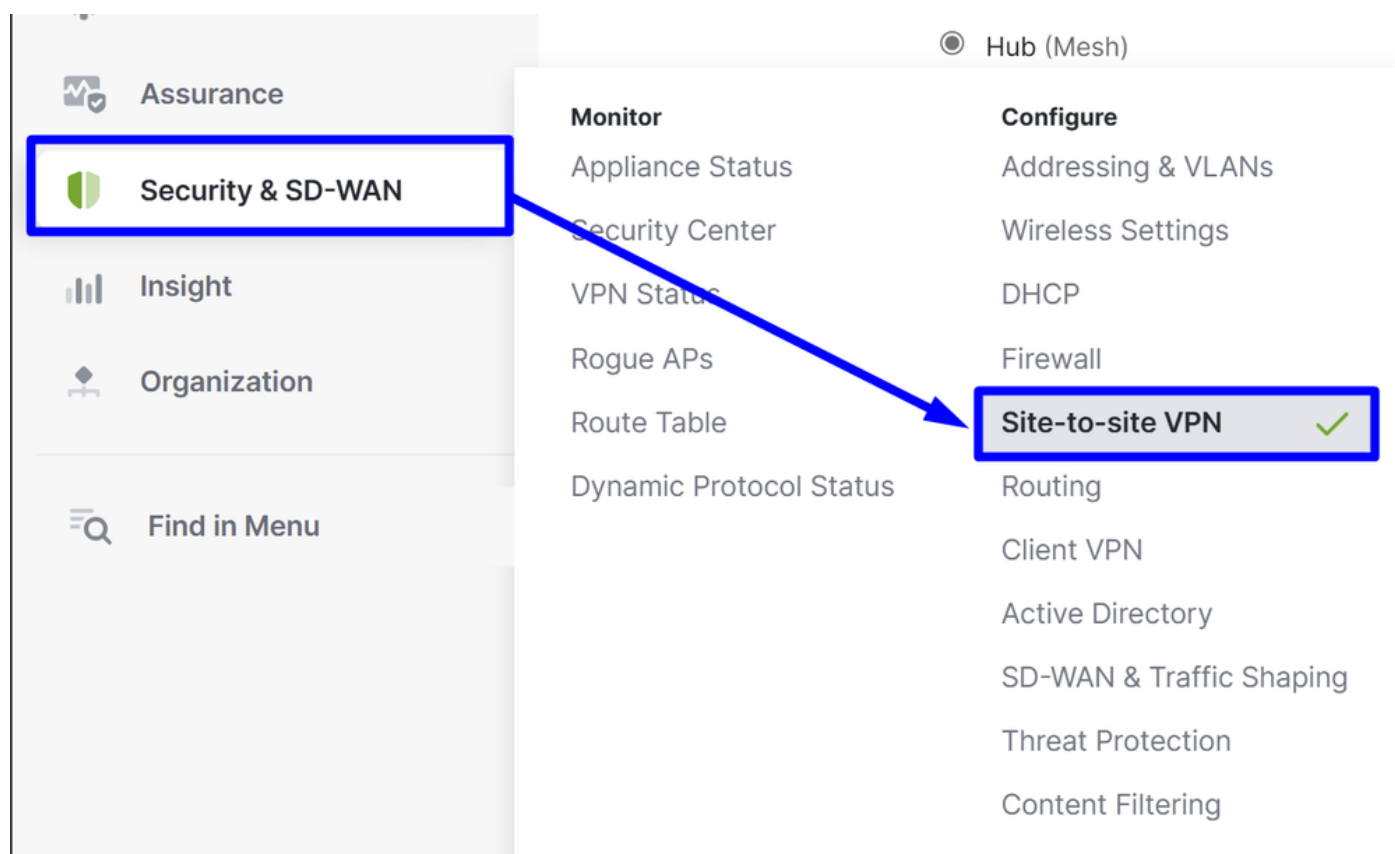
3.120.45.23

Download CSV

Done

Meraki MXでのVPNの設定

Meraki MXに移動して、Security & SD-WANをクリックします。 Site-to-site VPN



サイト間 VPN

選択 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の設定

トラフィックをセキュアアクセスに送信するために選択したネットワークを選択します。

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	

NAT Traversalで選択

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.

Meraki以外のVPNピア

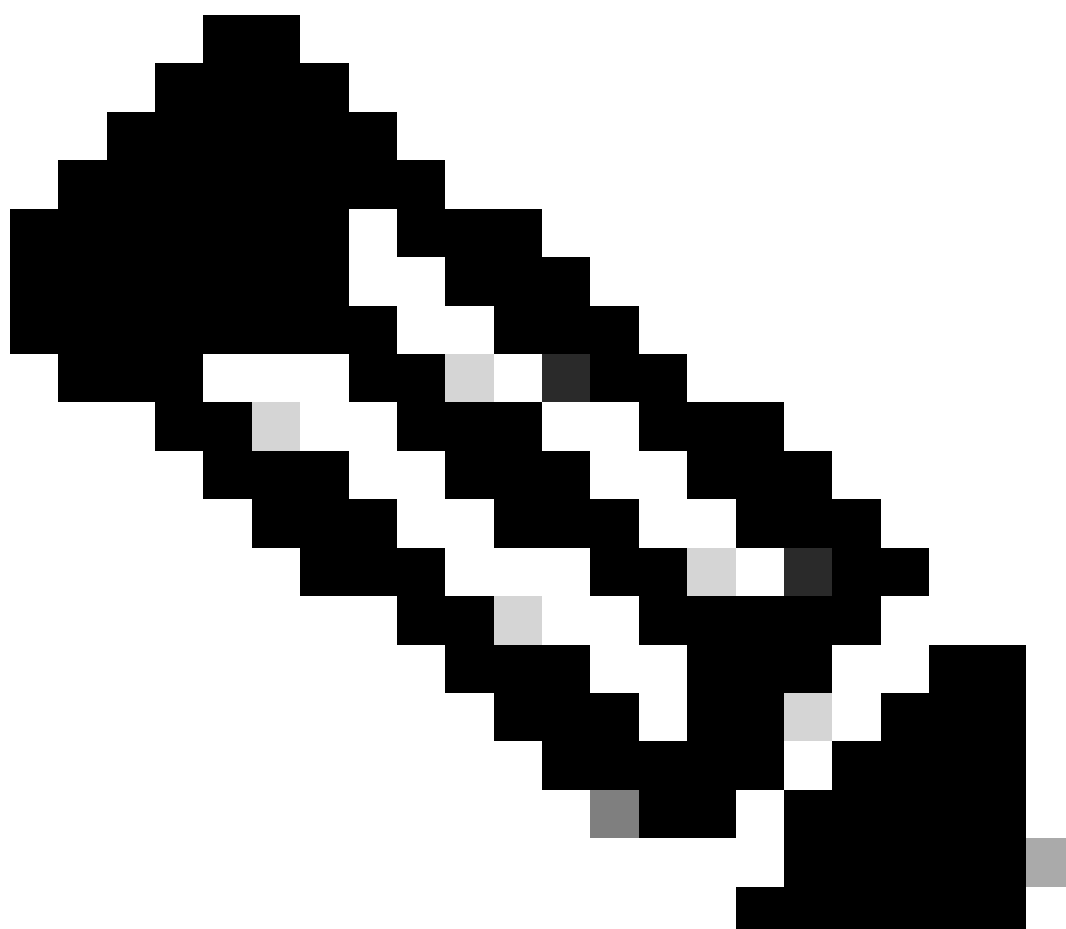
セキュアアクセスへのトラフィックをルーティングするためにMerakiが使用するヘルスチェックを設定する必要があります。

クリック Configure Health Checks

- クリック +Add health Check

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

- Health Check：テストの名前を設定します
- Endpoint:Secure Accessが推奨するものを使用してください。 <http://service.sig.umbrella.com>



注：このドメインは、セキュアアクセスまたはUmbrellaを使用したサイト間トンネル経

由でアクセスされた場合にのみ応答します。これらのトンネル外部からのアクセス試行は失敗します。

次に、「Done」を2回クリックして完了します。

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 10 < 1 >

Cancel Done

これでヘルスチェックが設定され、Peer:

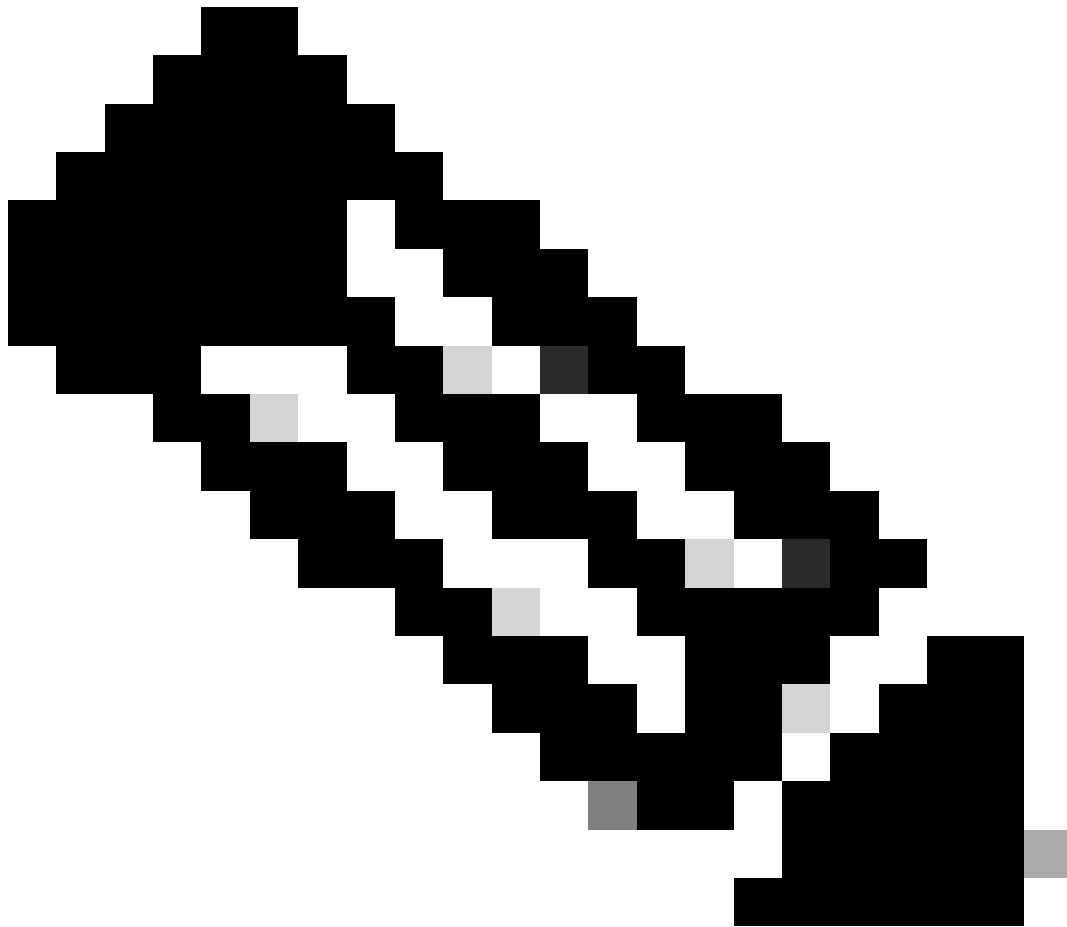
プライマリトンネルの設定

- クリック +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@.....ci:		Preset Umbrella

- VPNピアの追加
 - Name : アクセスを保護するためのVPNの名前を設定します。
 - IKE version:IKEv2を選択します
- ピア

- パブリックIPまたはホスト名：セキュアアクセスVPN設定の手順で、セキュアアクセスで指定された[Primary Datacenter IPを設定します。](#)
- ローカルID：ステップ「[セキュアアクセスVPNの設定](#)」のセキュアアクセスで指定されたPrimary Tunnel IDを設定します。
- リモートID：該当なし
- 共有秘密：手順「[セキュアアクセスVPNの設定](#)」のセキュアアクセスで指定された「[Passphrase](#)」を設定します
- ルーティング：スタティックを選択
- プライベートサブネット：インターネットアクセスとプライベートアクセスの両方を設定する場合は、宛先として0.0.0.0/0を使用します。そのVPNトンネルに対してプライベートアクセスのみを設定する場合は、宛先ネットワークとしてRemote Access VPN IP PoolとCGNAT範囲100.64.0.0/10を指定します
- 可用性:Merakiデバイスが1台のみの場合は、All Networksを選択できます。複数のデバイスがある場合は、トンネルを設定する特定のMerakiネットワークのみを選択してください。
- トンネルモニタリング
 - ヘルスチェック：以前に設定したヘルスチェックを使用して、トンネルの可用性を監視します
 - インターネットへの直接フェールオーバー：このオプションをイネーブルにして、Tunnel 1とTunnel 2の両方のヘルスチェックに失敗した場合、インターネットアクセスの喪失を防ぐためにトラフィックがWANインターフェイスにリダイレクトされます。



ヘルスチェック機能:Tunnel 1が監視されていて、そのヘルスチェックが失敗した場合、トラフィックは自動的にTunnel 2にフェールオーバーします。Tunnel 2でも障害が発生し、Failover directly to Internet オプションが有効になっている場合、トラフィックはMerakiデバイスのWANインターフェイス経由でルーティングされます。

-
- IPSec ポリシー
 - プリセット：選択 Umbrella

次に、Saveをクリックします。

セカンダリトンネルの設定

セカンダリトンネルを設定するには、プライマリトンネルのオプションメニューをクリックします。

- 3つのドットをクリックします。

#	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 >

- クリック + Add Secondary peer

Primary



Edit primary peer



Move to



Delete primary peer

Secondary



Add secondary peer

- クリック Inherit primary peer configurations

Add Secondary VPN Peer



Inherit primary peer configurations



Name

SSE Secondary

IKE version

IKEv2

その後、一部のフィールドが自動的に入力されます。これらを確認し、必要な変更を行い、残りを手動で完了します。

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

• ピア

- パブリックIPまたはホスト名：セキュアアクセスVPN設定の手順で、セキュアアクセスで指定された[Secondary Datacenter IPを設定します。](#)
- ローカルID：ステップ「[セキュアアクセスVPNの設定](#)」のセキュアアクセスで指定されたSecondary Tunnel IDを設定します。
- リモートID：該当なし
- 共有秘密：手順「[セキュアアクセスVPNの設定](#)」のセキュアアクセスで指定された「[Passphrase](#)」を設定します

• トンネルモニタリング

- ヘルスチェック：以前に設定したヘルスチェックを使用して、トンネルの可用性を監視します

その後、Saveをクリックすると、次のアラートが表示されます。

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).

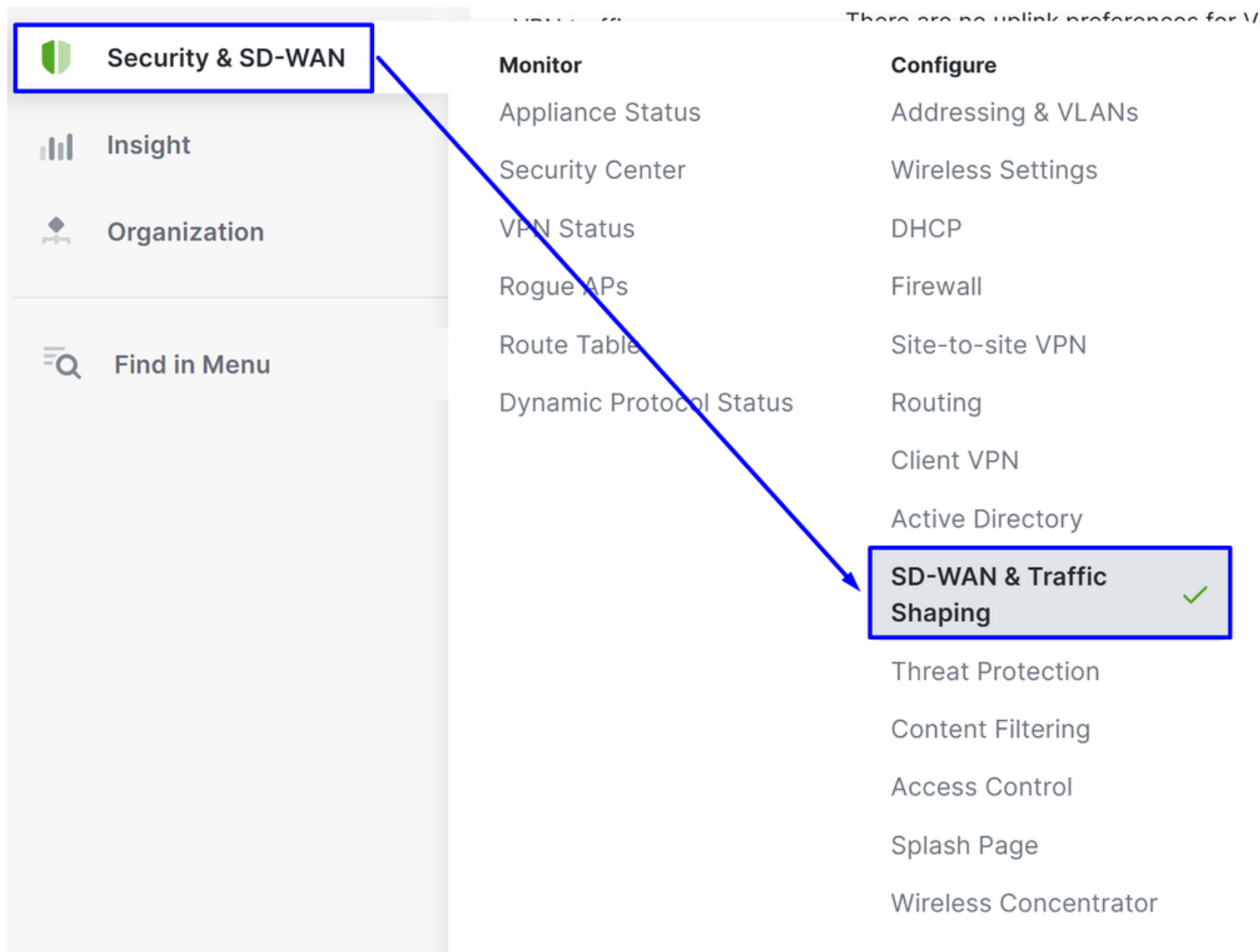
[Confirm Changes](#)[Cancel](#)

クリックするだけで問題ありません **Confirm Changes**.

トラフィックステアリングの設定 (トンネルトラフィックバイパス)

この機能では、SD-WANバイパス設定でドメインまたはIPアドレスを定義することで、トンネルからの特定のトラフィックをバイパスできます。

- Security & SD-WANに移動します。 SD-WAN & Traffic Shaping



- 「Local Internet Breakout」 セクションまでスクロールダウンして、 Add+

Local internet breakout

VPN exclusion rules

Add +

次に、Custom ExpressionsまたはMajor Applicationsに基づいてバイパスを作成します。

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

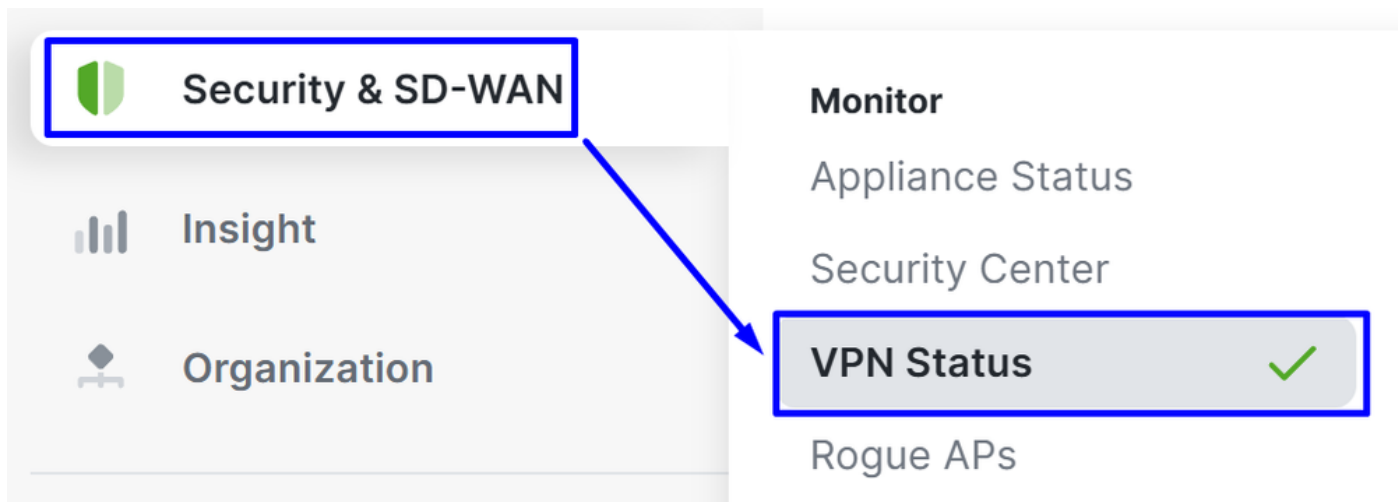
Zoom

詳細については、「[VPN除外ルールの設定 \(IP/ポート/DNS/アプリケーション\)](#)」を参照してください。

確認

トンネルがアップしているかどうかを確認するには、次の場所でステータスを確認します。

- MerakiダッシュボードでSecurity & SD-WAN > VPN Statusをクリックします。



- クリック 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				

プライマリとセカンダリの両方のVPNステータスが緑色で表示されている場合は、トンネルがアップ状態でアクティブであることを意味します。

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

トラブルシュート

ヘルスチェックの確認

VPNのMerakiヘルスチェックが正しく機能しているかどうかを確認するには、次の場所に移動します。

- をクリックします [Assurance](#)。 [Event Log](#)

Event log

Client:

Before: (PDT)

Event type include:

Event type ignore:

[Reset filters](#)

Event Type Includeで、次のいずれかを選択します。 [Non-Meraki VPN Healthcheck](#)

Event log

Client: Any

Before: 04/18/202506:15(PDT)

Event type include: All

Event type ignore: None

SearchReset filters



Client: Any

Before: 04/18/202506:15(PDT)

Event type include: Non-Meraki VPN Healthcheck x

Event type ignore: None

SearchReset filters

Cisco Secure Accessへのプライマリトンネルがアクティブな場合、セカンダリトンネルを経由して到達するパケットは、一貫したルーティングパスを維持するためにドロップされます。

セカンダリトンネルはスタンバイ状態のままであり、ヘルスチェックメカニズムによって決定されたとおり、Meraki側から、またはセキュアアクセス内のいずれかでプライマリトンネルで障害が発生した場合にのみ使用されます。

Event log

Client: AnyBefore: 04/18/202506:15(PDT)

Event type include: Non-Meraki VPN Healthcheck xEvent type ignore: None

SearchReset filters

Download as ▾

« newerolder »

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				

- プライマリトンネルのヘルスチェックでは、ステータスがupと表示されます。これは、トラフィックが現在通過しており、アクティブに転送されていることを意味します。
- セカンダリトンネルのヘルスチェックでは、ステータスが「down」と表示されます。これは、トンネルが使用不可能だからではなく、プライマリが正常でアクティブに使用されているためです。トラフィックがTunnel 1を通過することだけが許可され、セカンダリトンネルのヘルスチェックが失敗するため、この動作が期待されます。

関連情報

- [シスコのテクニカルサポートとダウンロード](#)
- [Cisco Secure Accessヘルプセンター](#)
- [Cisco Secure Access Meraki BGPコンフィギュレーションガイド](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。