# 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モニタリングを実現

## 内容



## 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。

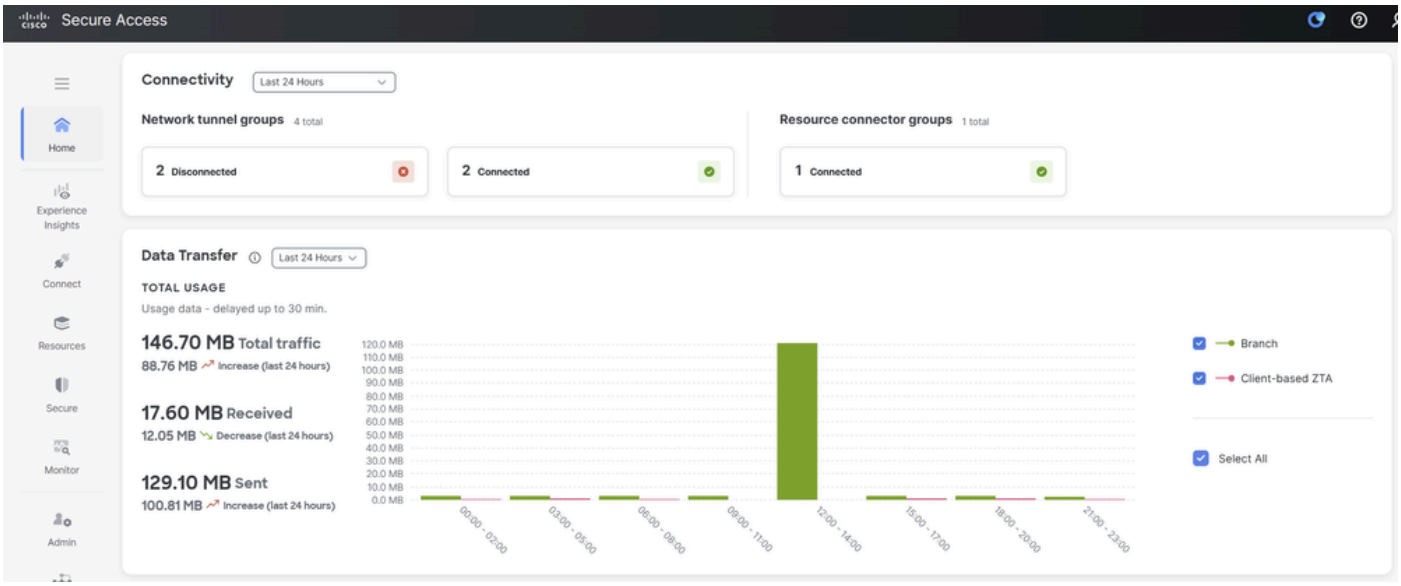
この導入の主な要素は次のとおりです。

- 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。

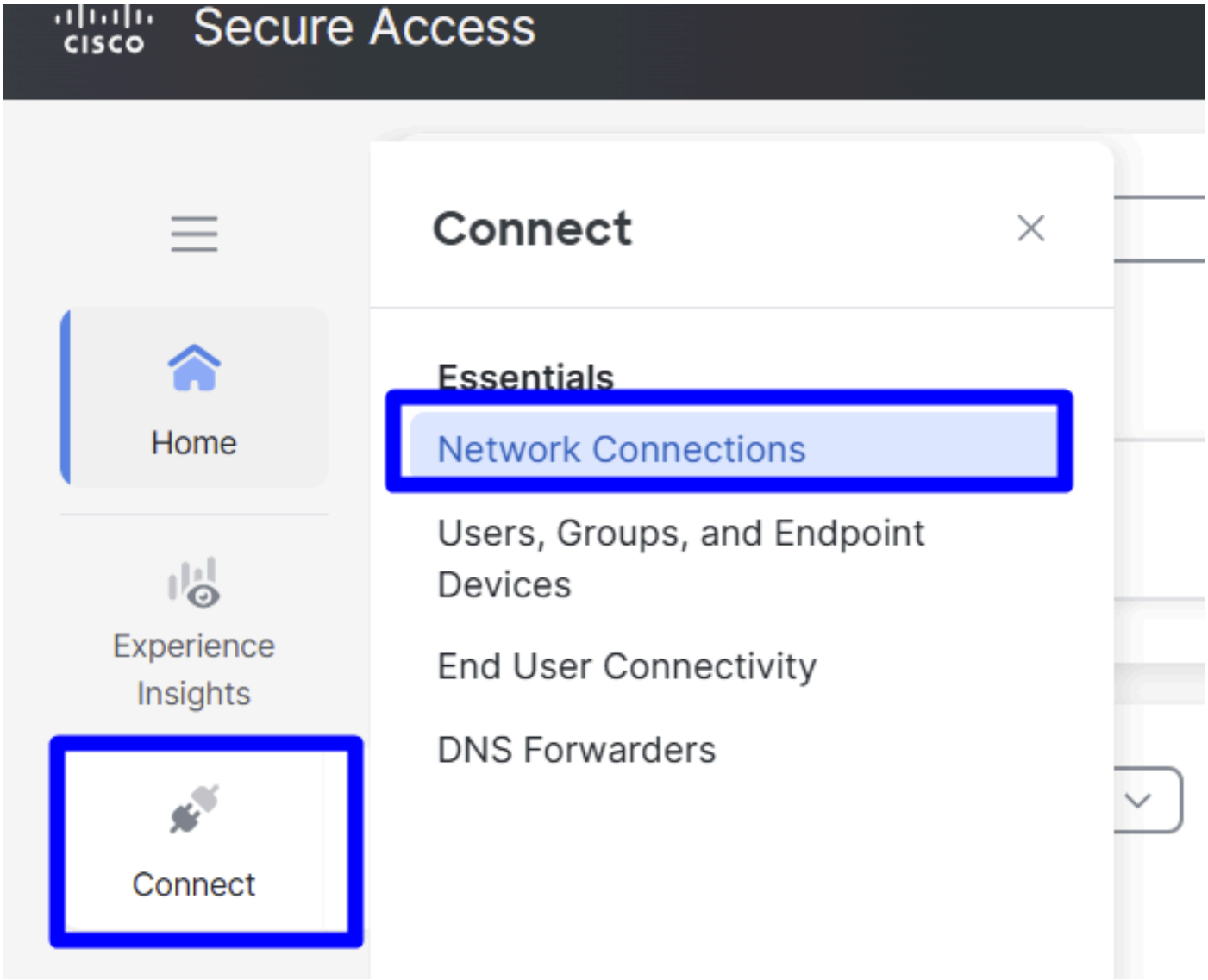
# 設定

# セキュアアクセスでのVPNの設定

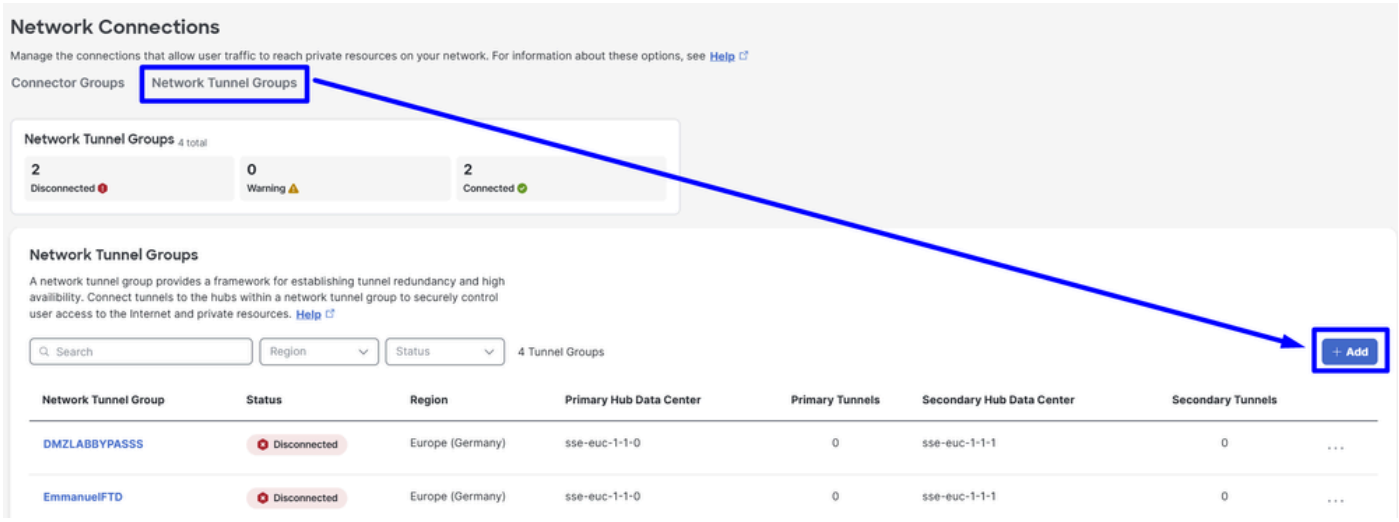
Secure Accessの管理パネルに移動します。



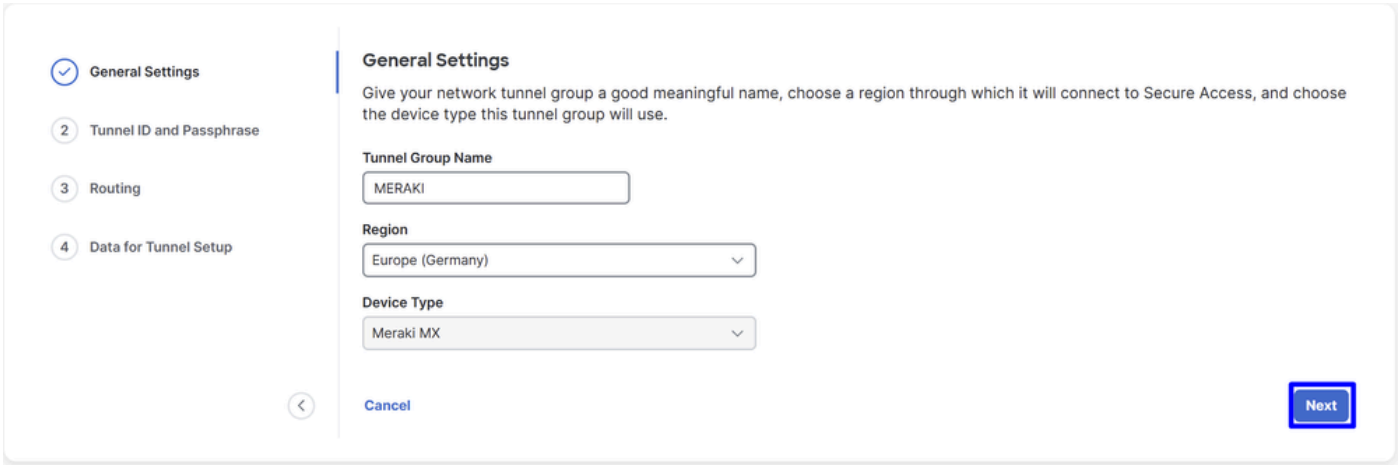

- クリック Connect > Network Connections



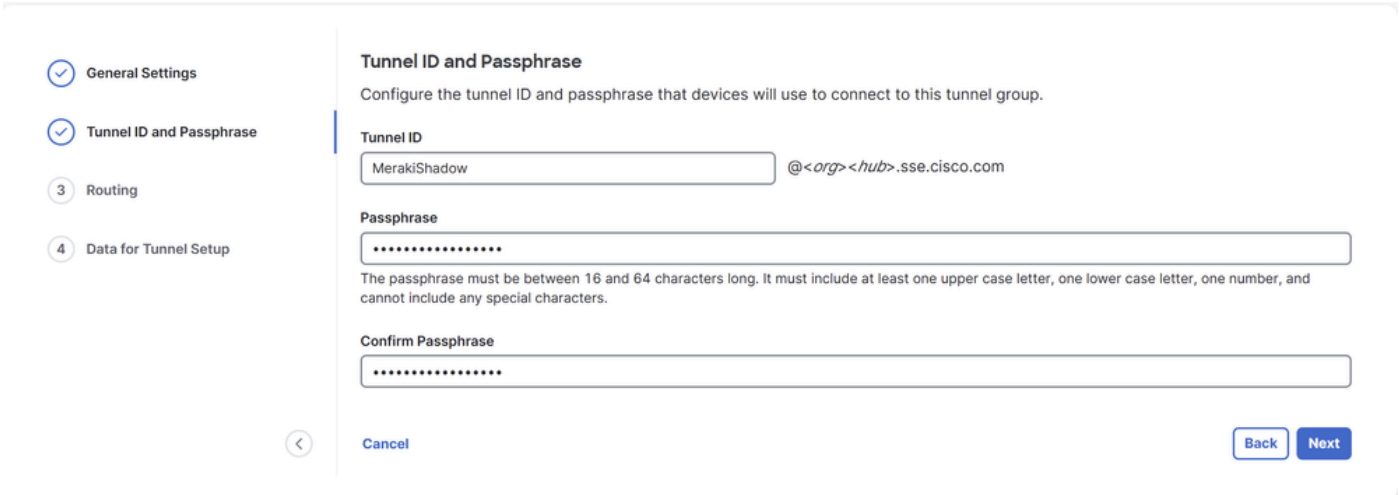

- 「Network Tunnel Groups」で、 + Add




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

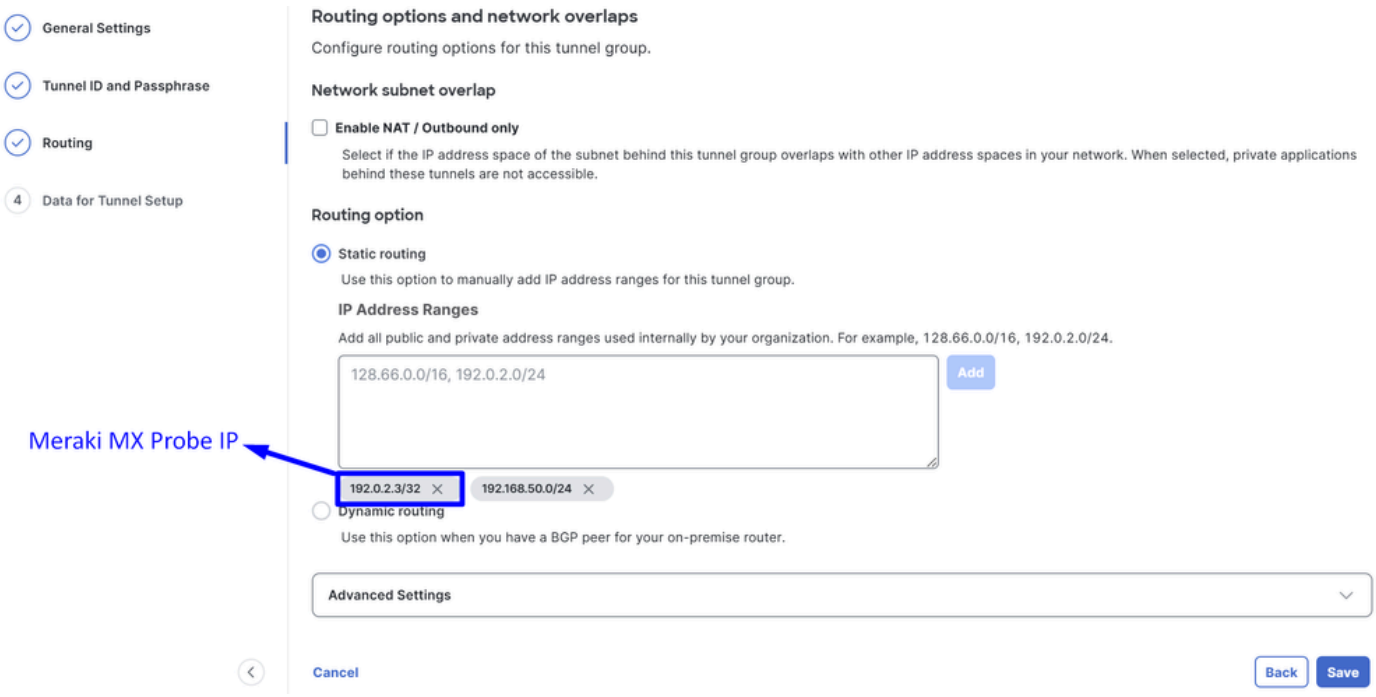


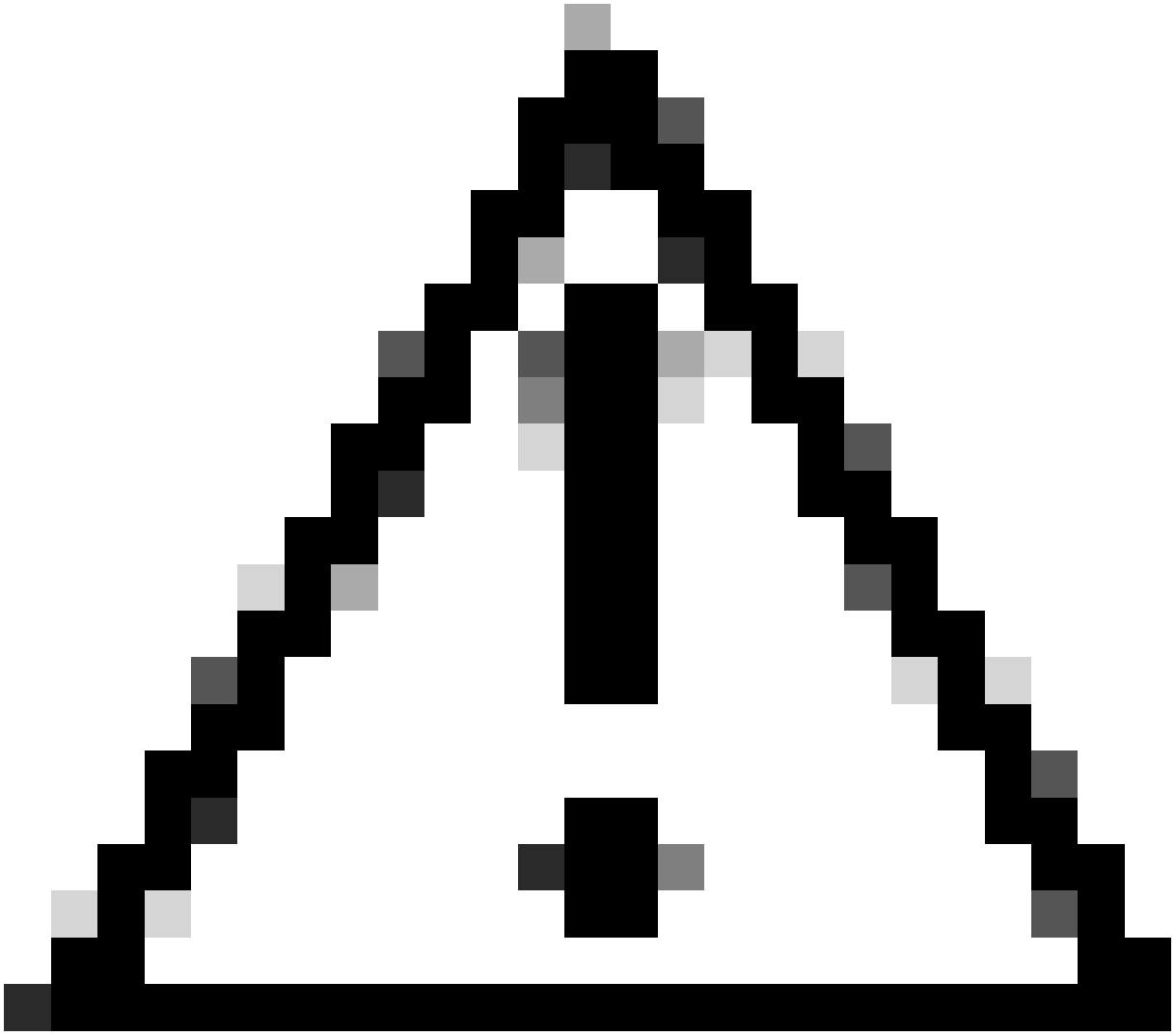

- Tunnel ID Formatコマンドと Passphrase
- [保存（ Next




- 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
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

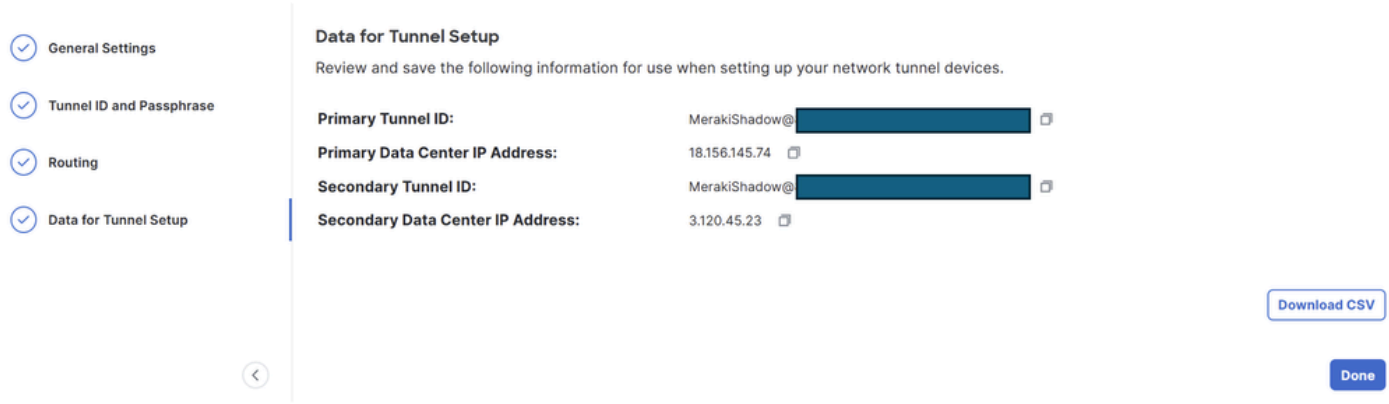


注意：必ずモニタリングプローブIP(192.0.2.3/32)を追加してください。そうしないと、Merakiデバイスで、トラフィックをインターネット、VPNプール、およびZTNAで使用されるCGNAT範囲100.64.0.0/10にルーティングする際に、トラフィックの問題が発生する可能性があります。

- 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.**

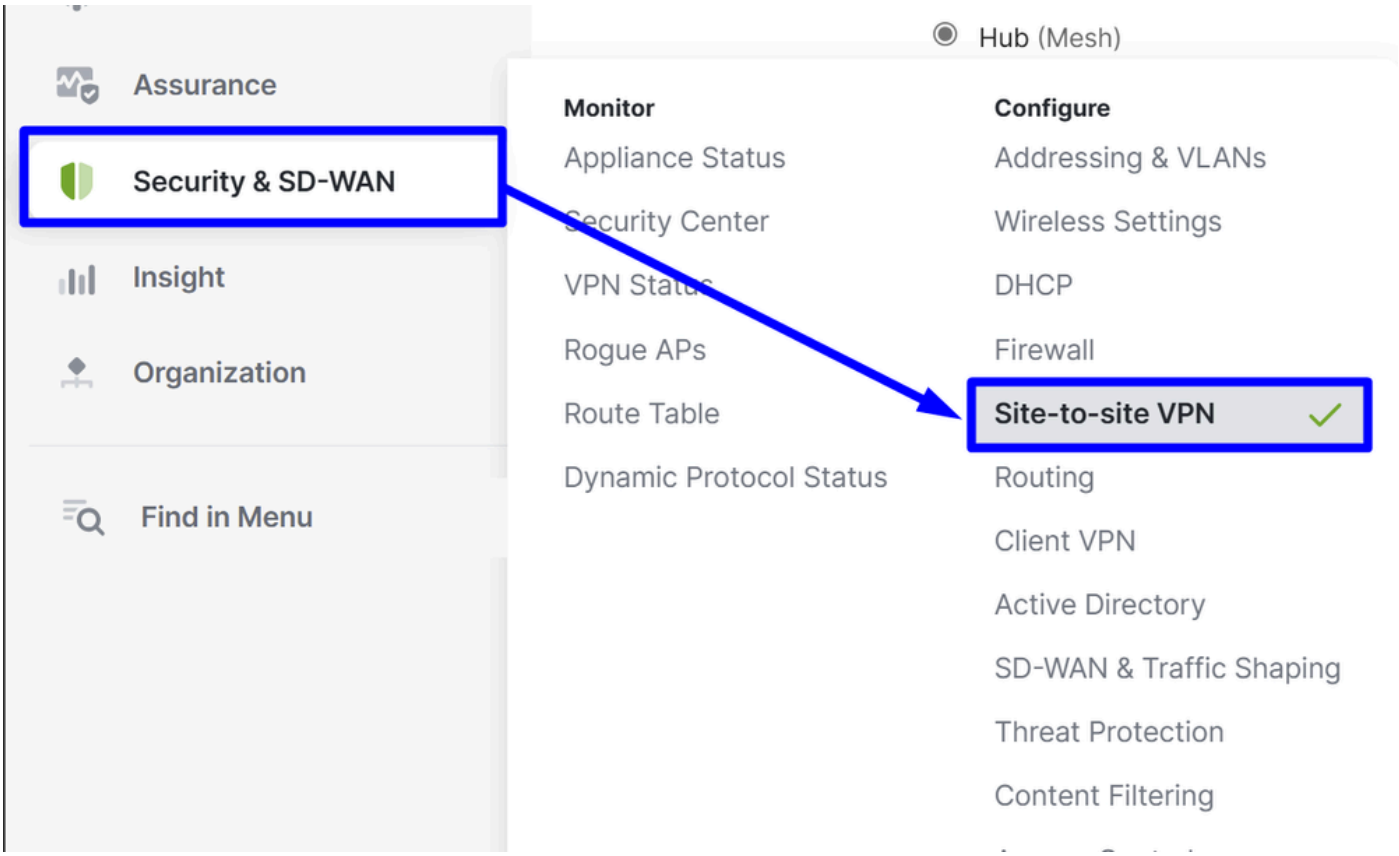
## セキュアアクセスVPNの設定

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。



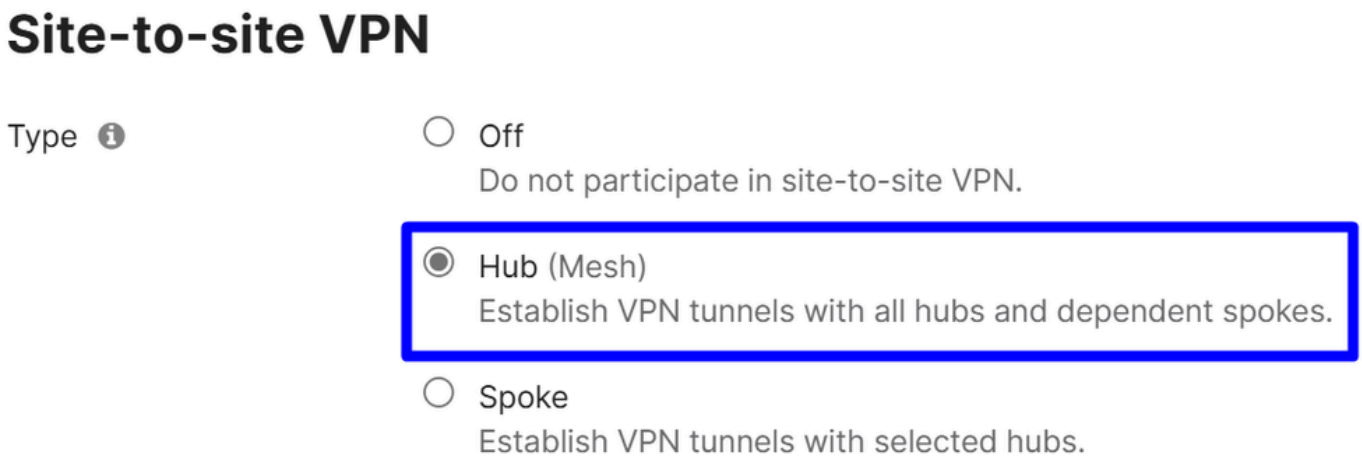

# Meraki MXでのVPNの設定

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



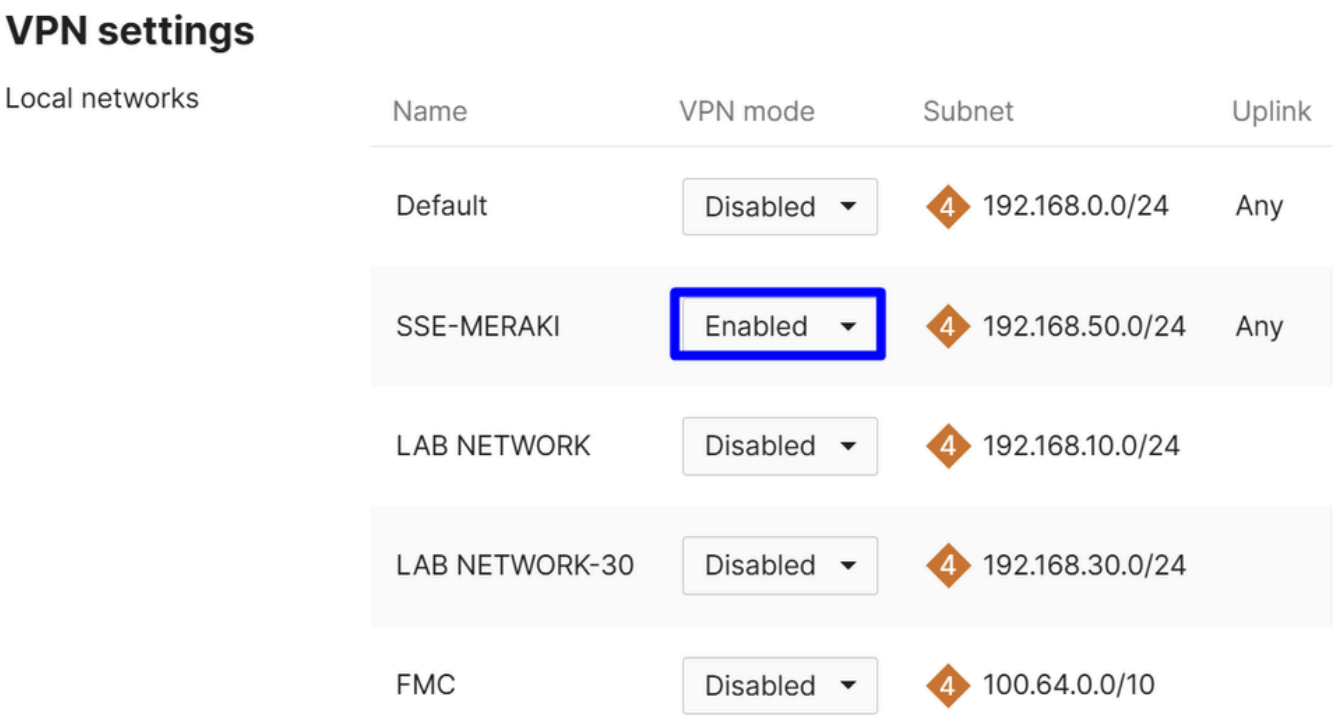

## サイト間 VPN

選択 Hub.

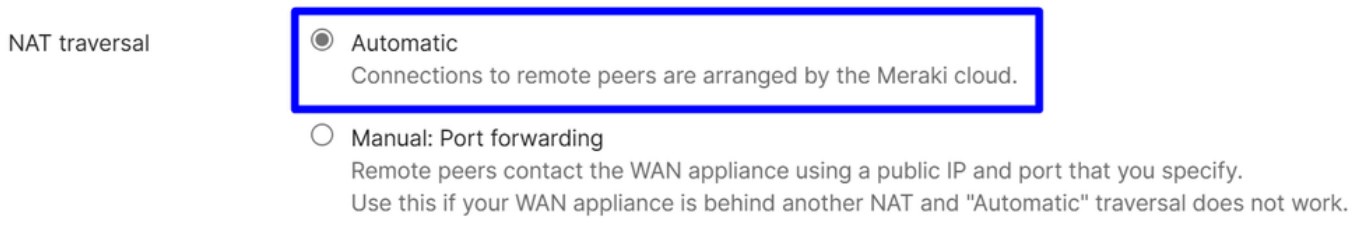



VPNの設定

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。




NAT Traversalで選択




Meraki以外のVPNピア

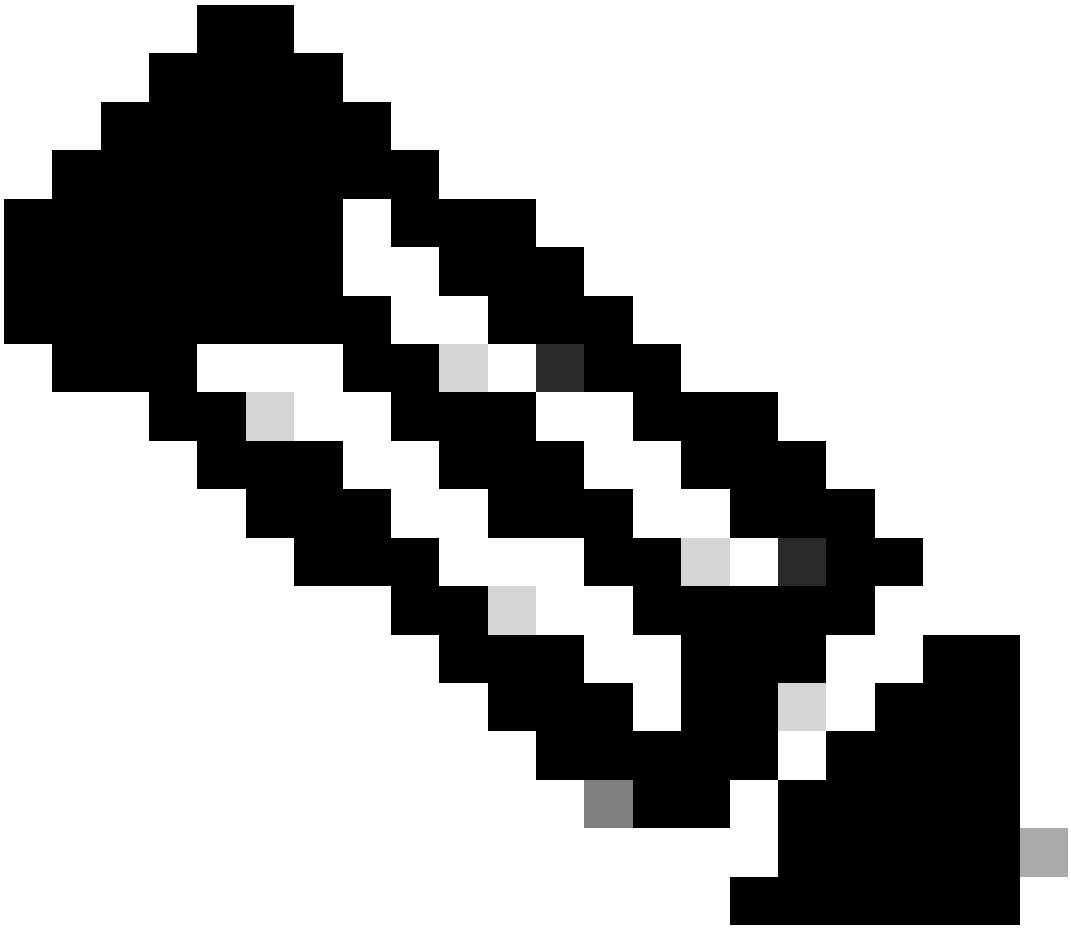
セキュアアクセスへのトラフィックをルーティングするためにMerakiが使用するヘルスチェックを設定する必要があります。

クリック **Configure Health Checks**

- クリック **+Add health Check**


- **Health Check**：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

---

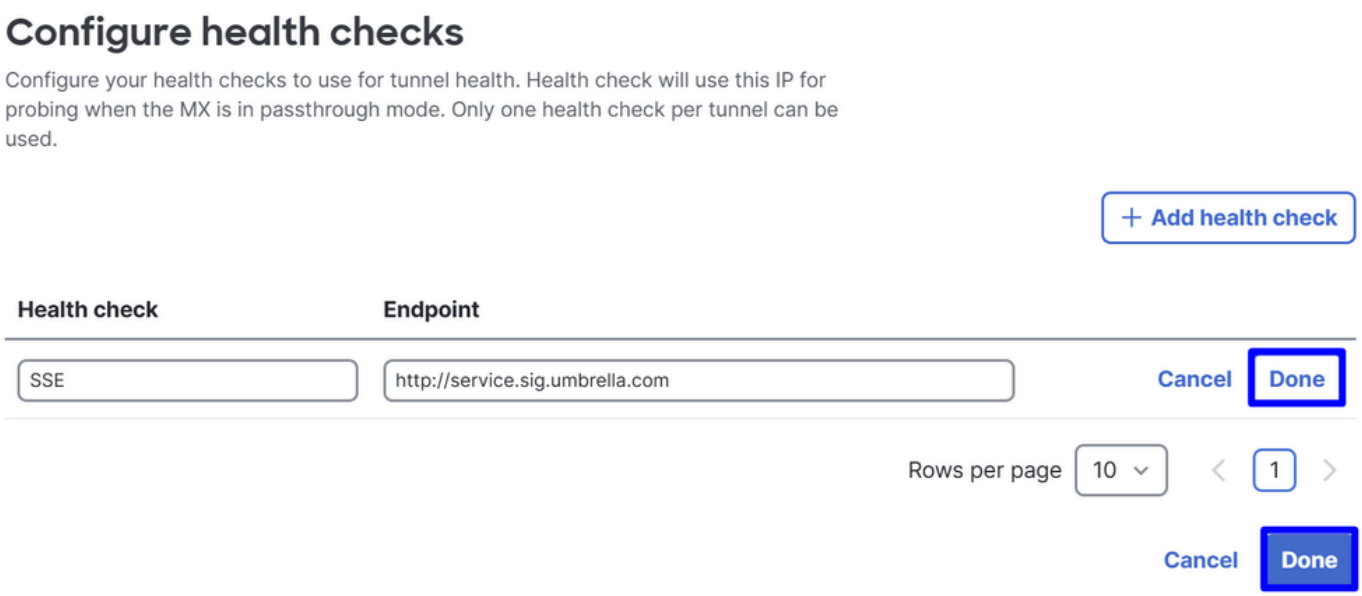


注：このドメインは、セキュアアクセスまたはUmbrellaを使用したサイト間トンネル経

---

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。

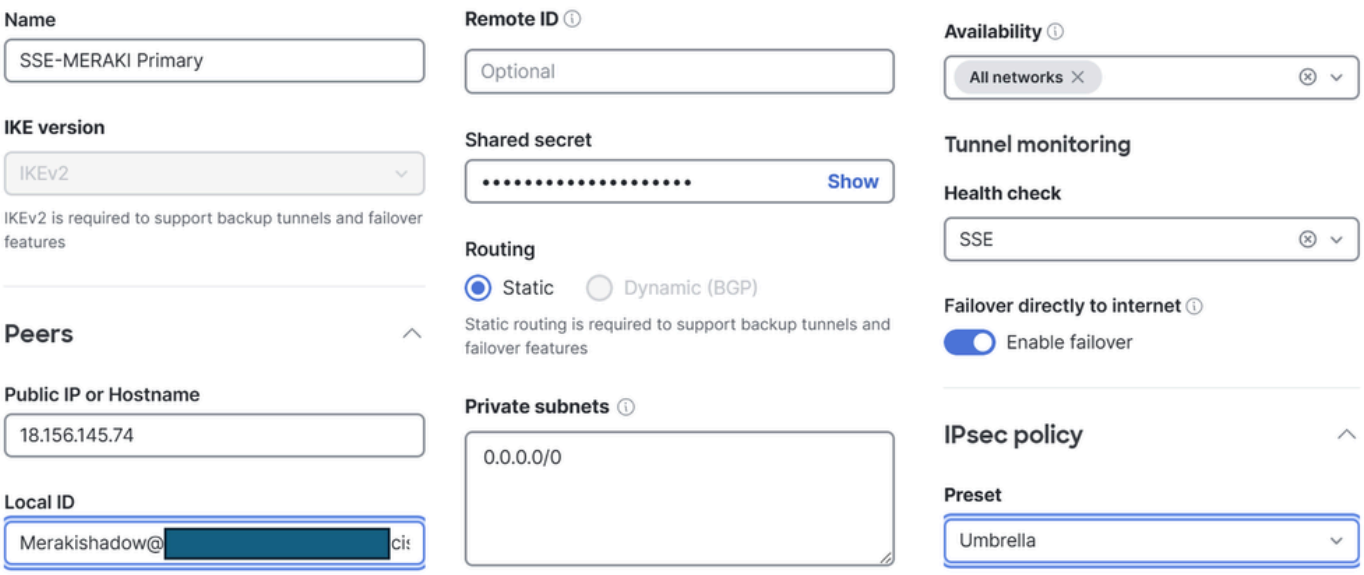
次に、「**Done**」を2回クリックして完了します。




これでヘルスチェックが設定され、 **Peer:**

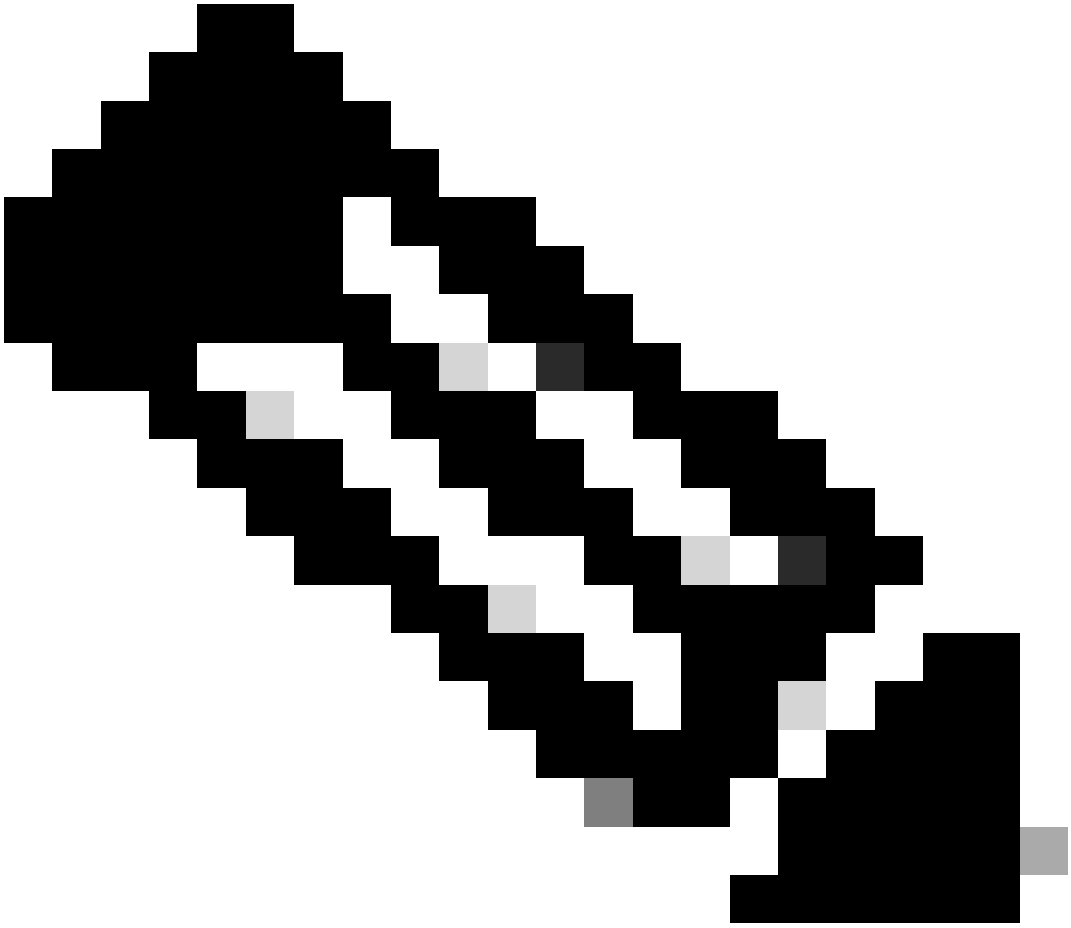
プライマリトンネルの設定

- クリック+Add a peer




- 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**

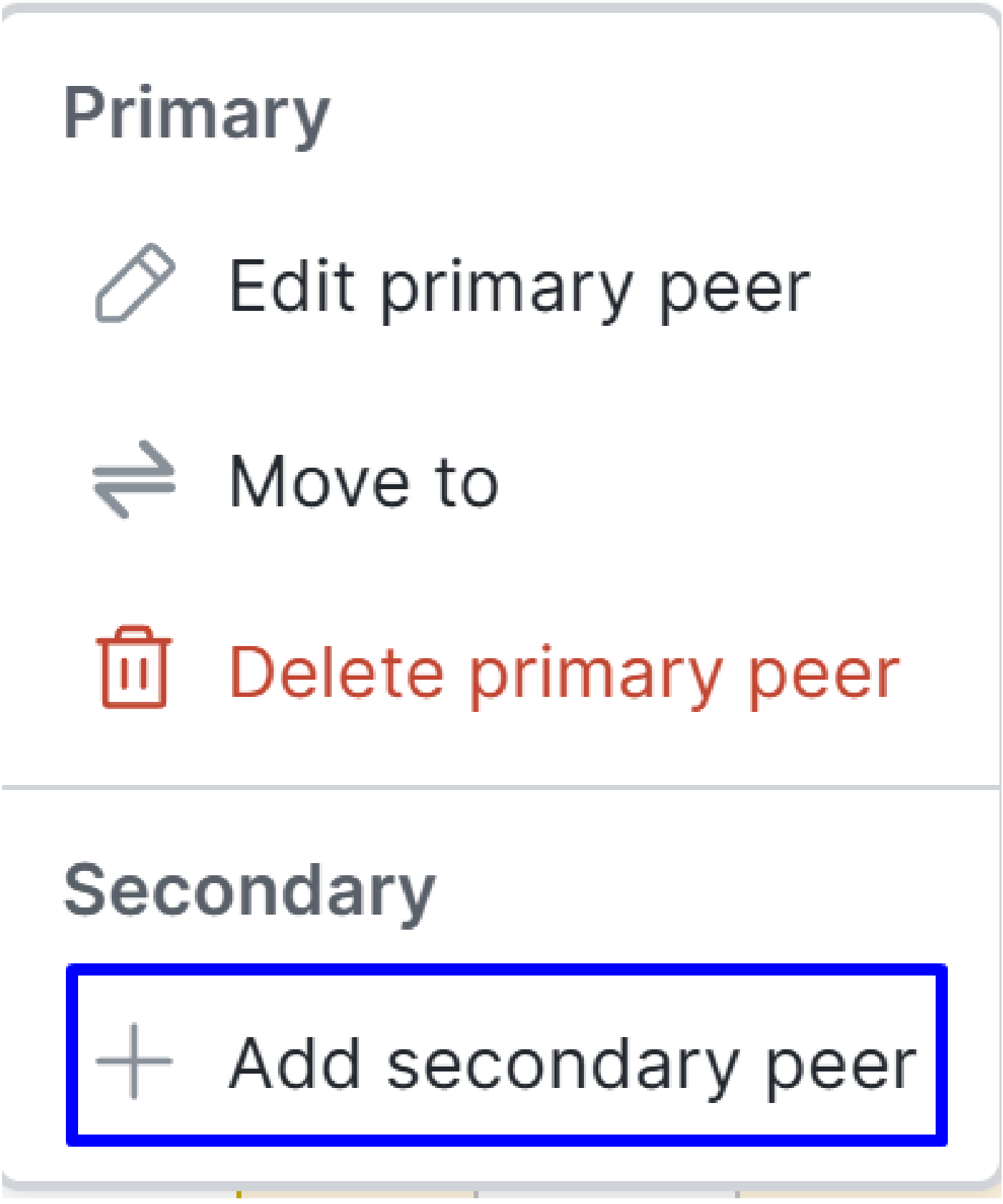
次に、**Save**をクリックします。

セカンダリトンネルの設定

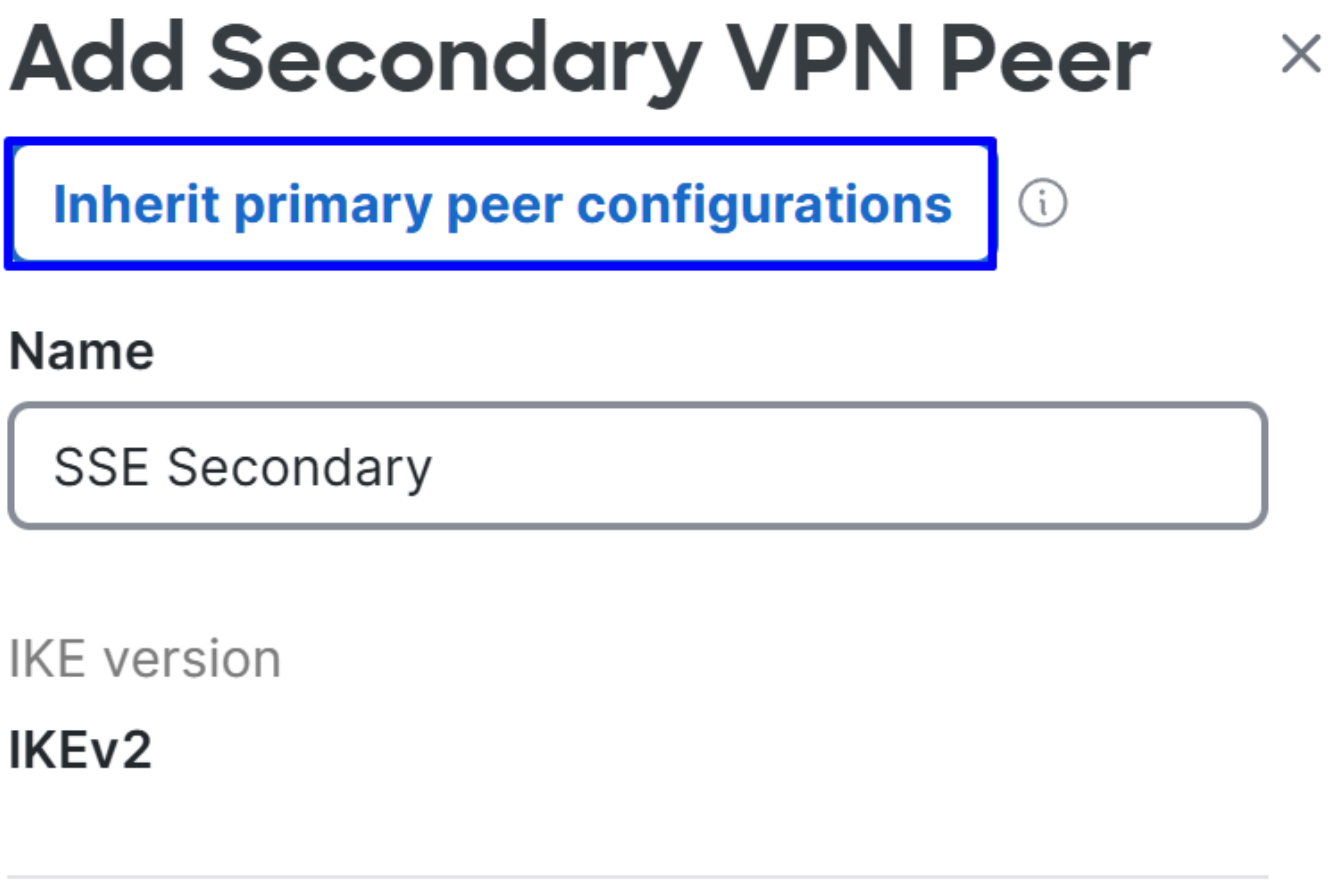
セカンダリトンネルを設定するには、プライマリトンネルのオプションメニューをクリックします。

- 3つのドットをクリックします。

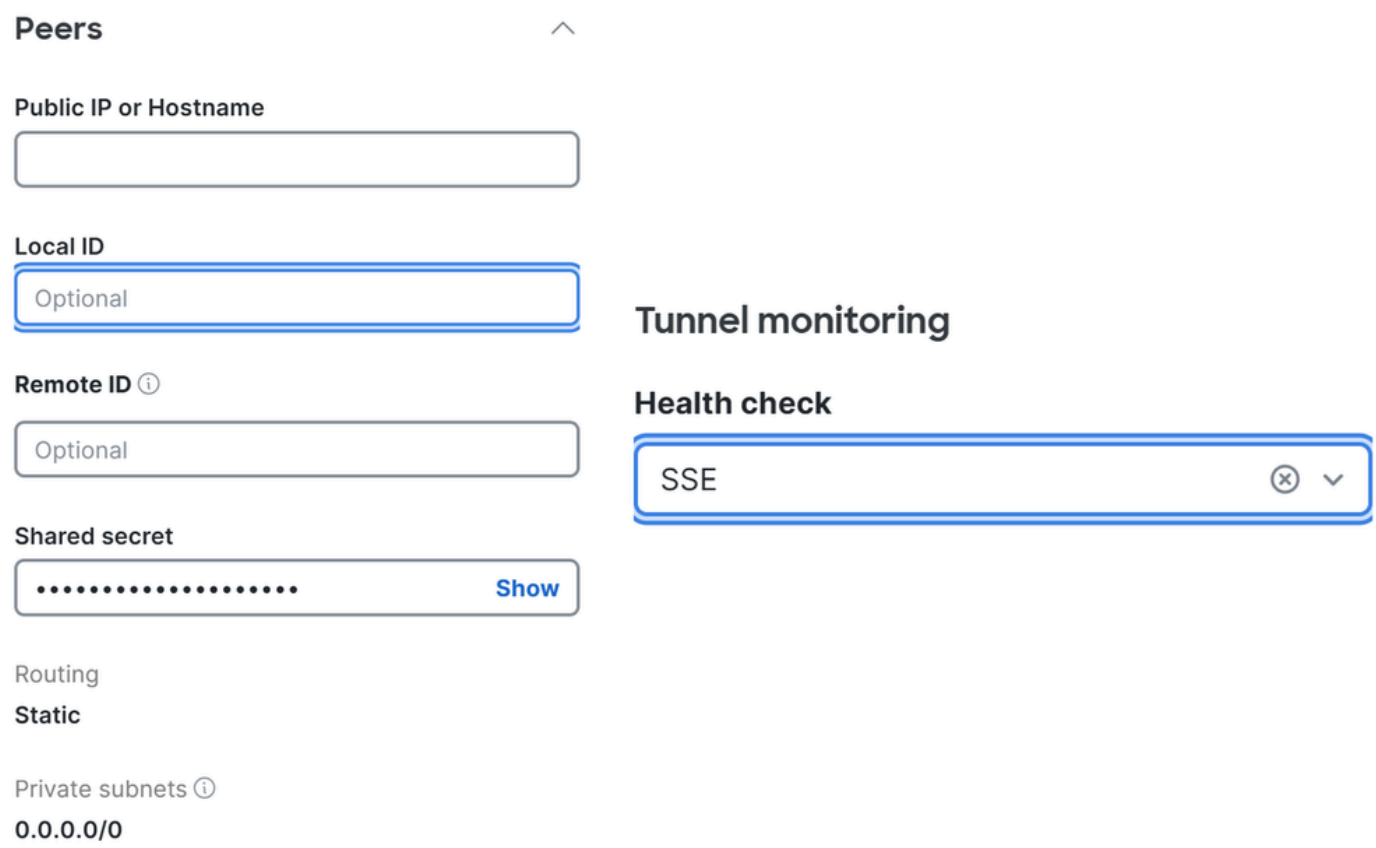

- クリック + Add Secondary peer



- クリックInherit primary peer configurations

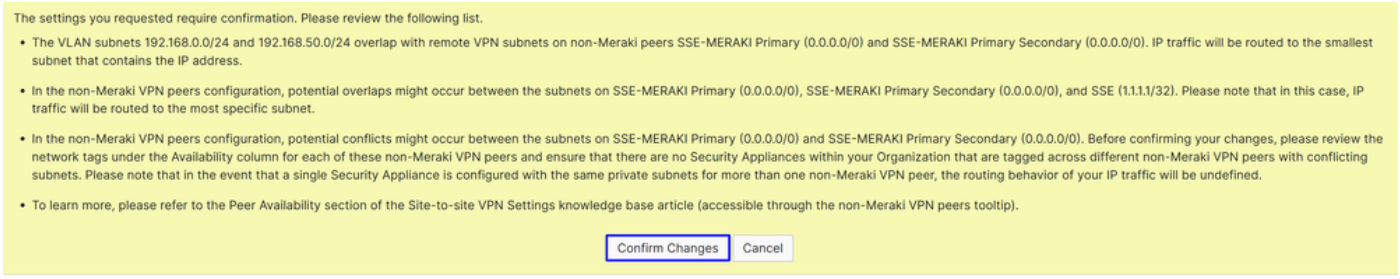



その後、一部のフィールドが自動的に入力されます。これらを確認し、必要な変更を行い、残りを手動で完了します。




- 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。

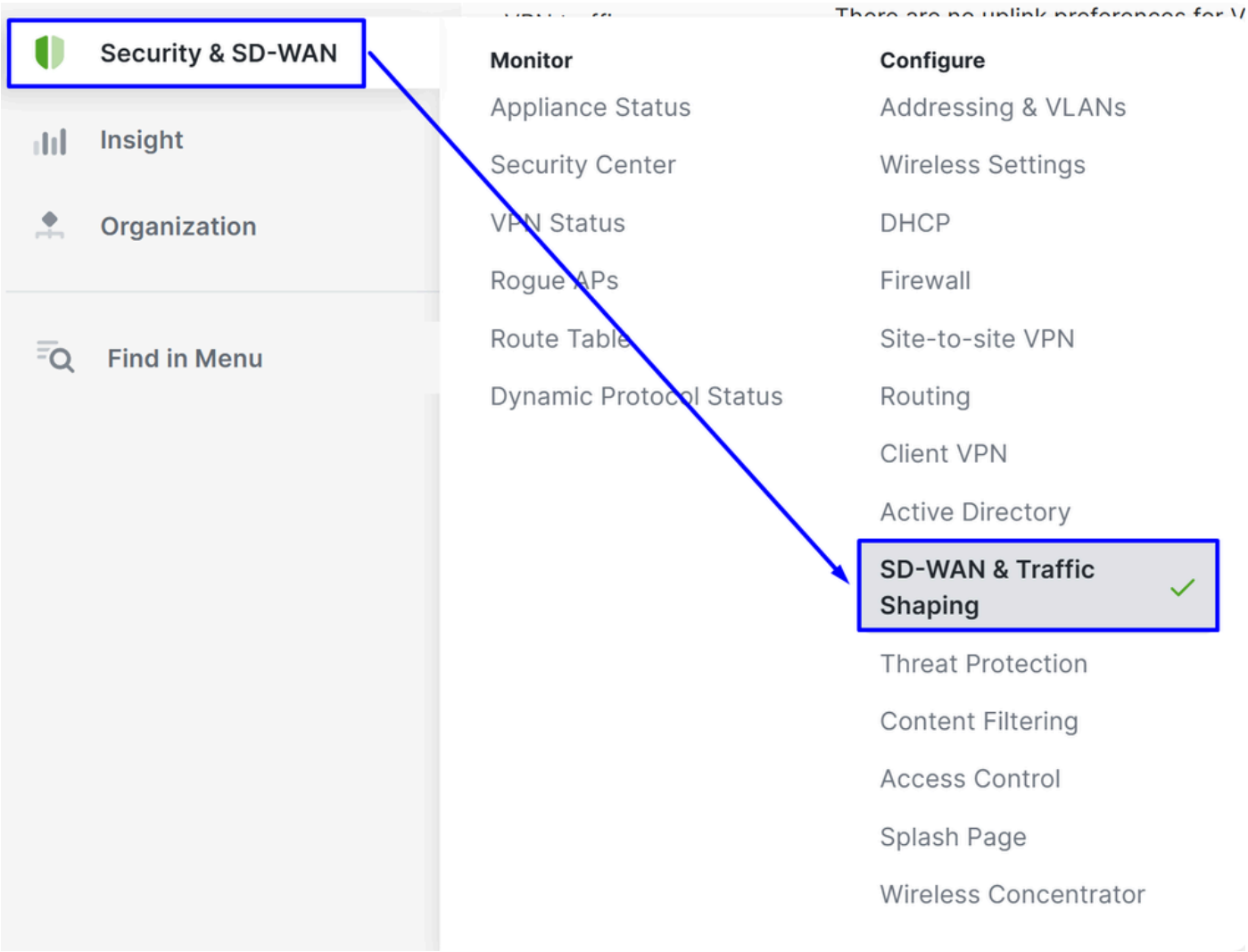



クリックするだけで問題ありません **Confirm Changes**.

## 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。

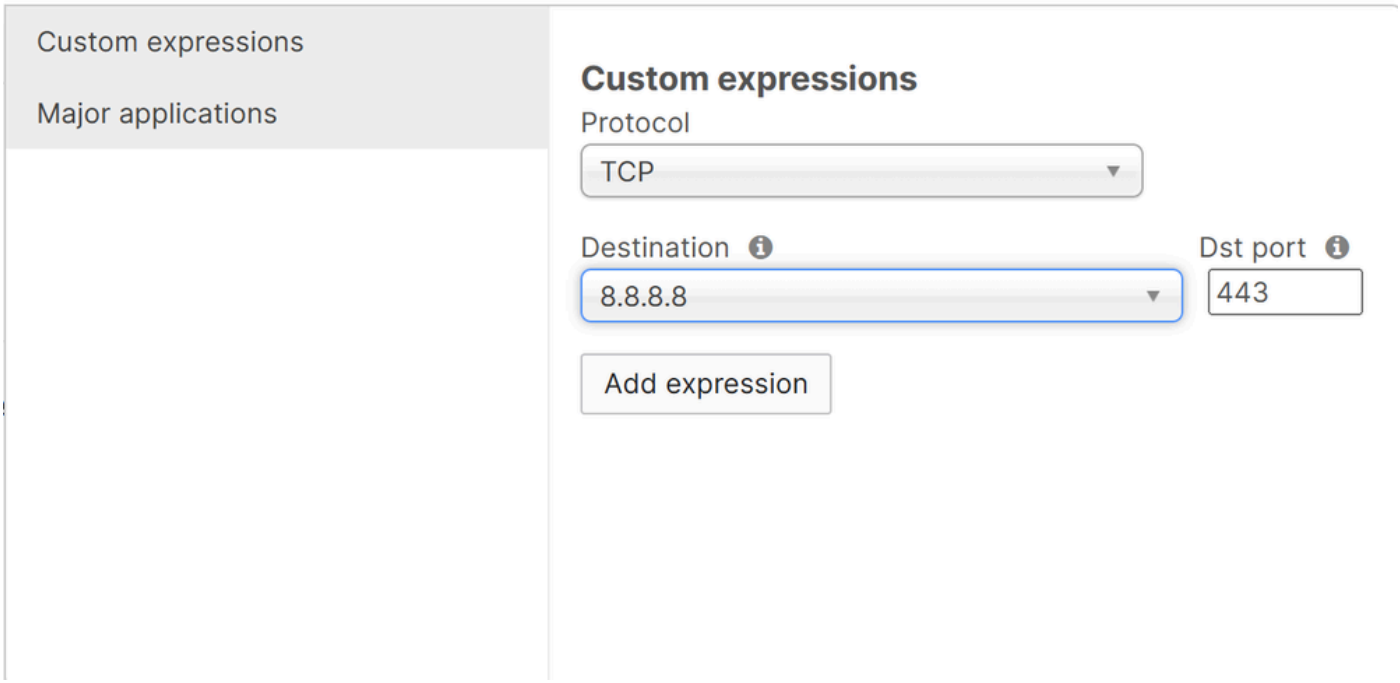
- **Security & SD-WANに移動します。** SD-WAN & Traffic Shaping



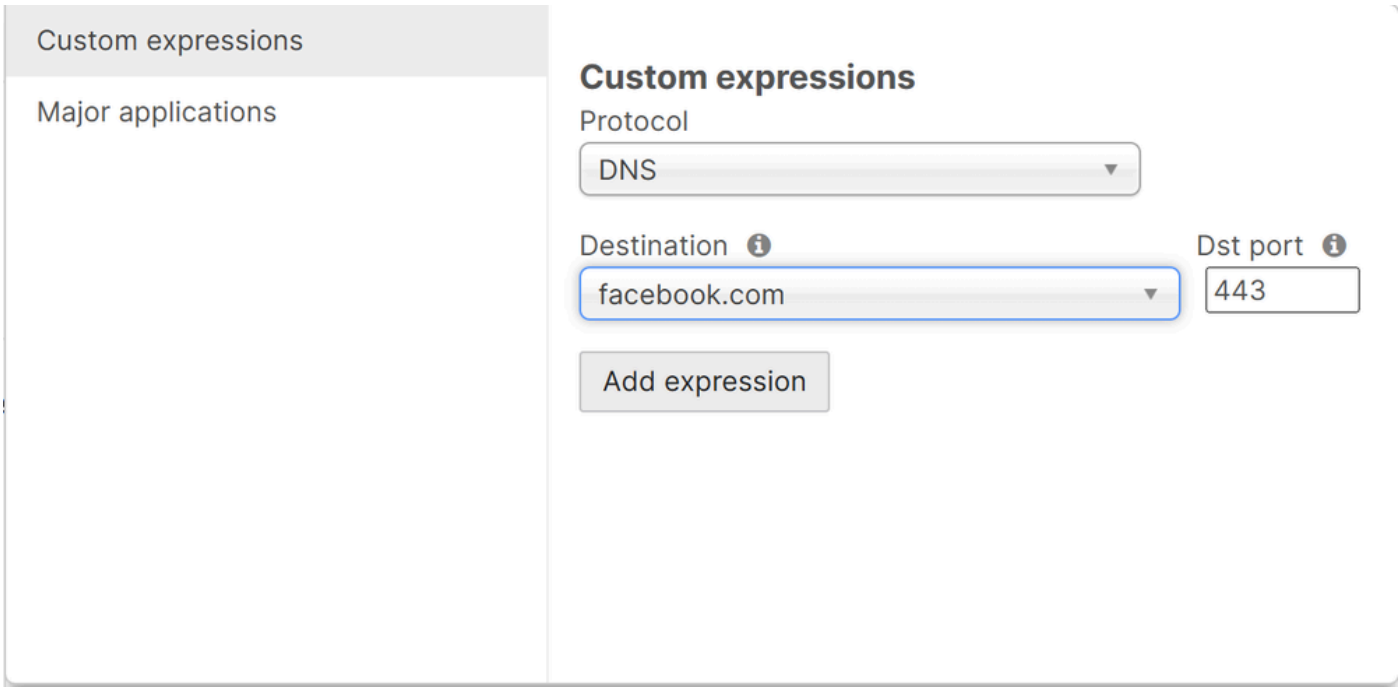

- 「**Local Internet Breakout**」セクションまでスクロールダウンして、 **Add+**


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

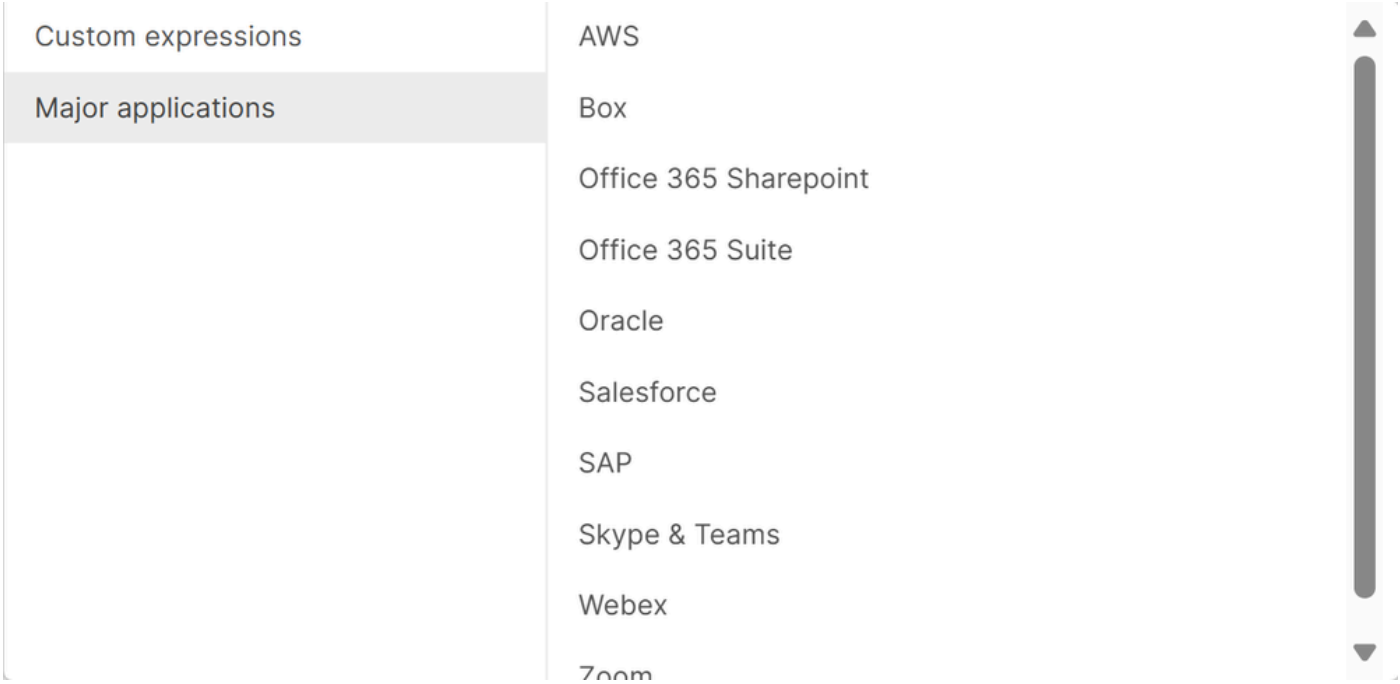
**Custom Expressions - Protocol**




**Custom Expressions - DNS**




**Major Applications**

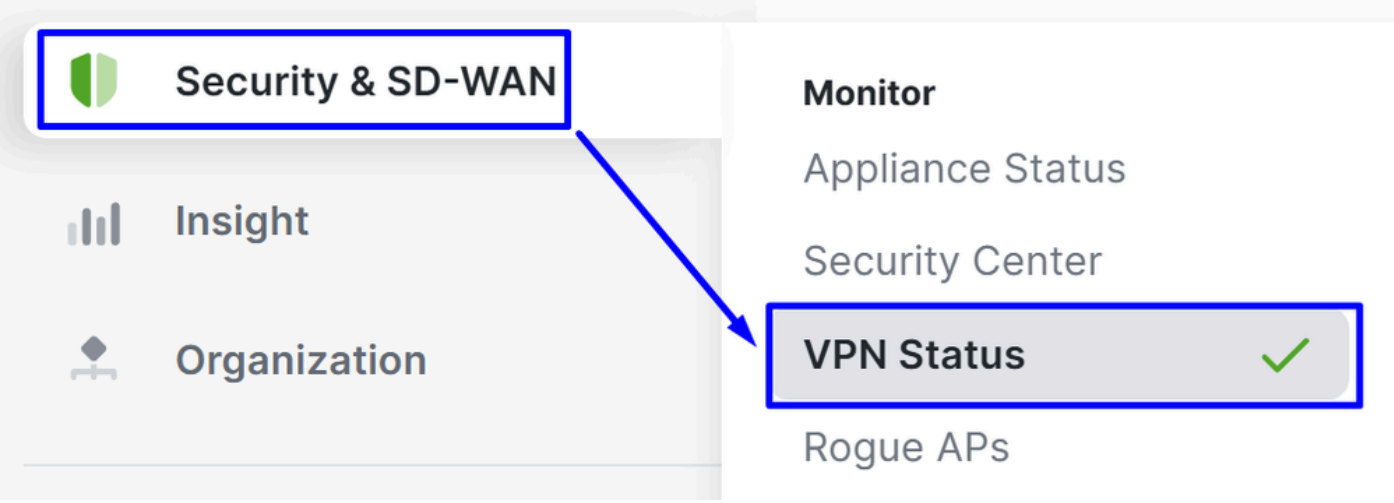



詳細については、「VPN除外ルールの設定（IP/ポート/DNS/アプリケーション）」を参照してください。

## 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

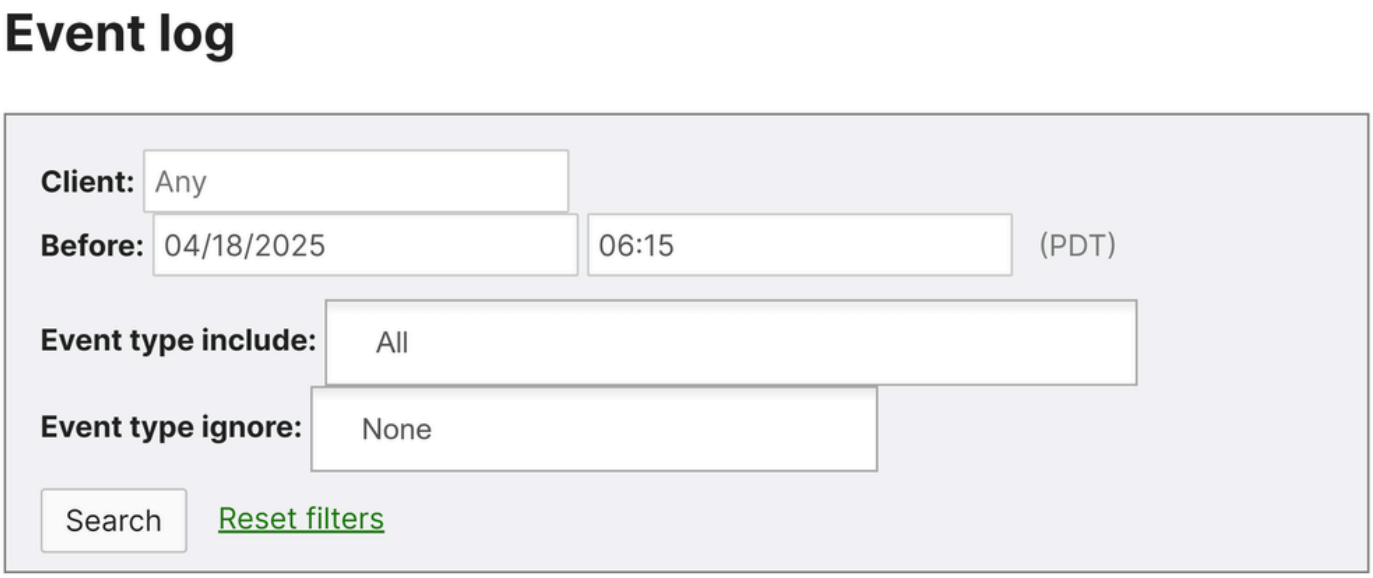
| Status Indicator | Color | Meaning |
|---|---|---|
| Primary/Secondary Up | Green | Phase 1 and phase 2 are up |
| Partial Connectivity | Amber | Phase 1 is up but phase 2 is down |
| Tunnel Down | Red | Phase 1 and phase 2 are both down |

# トラブルシュート

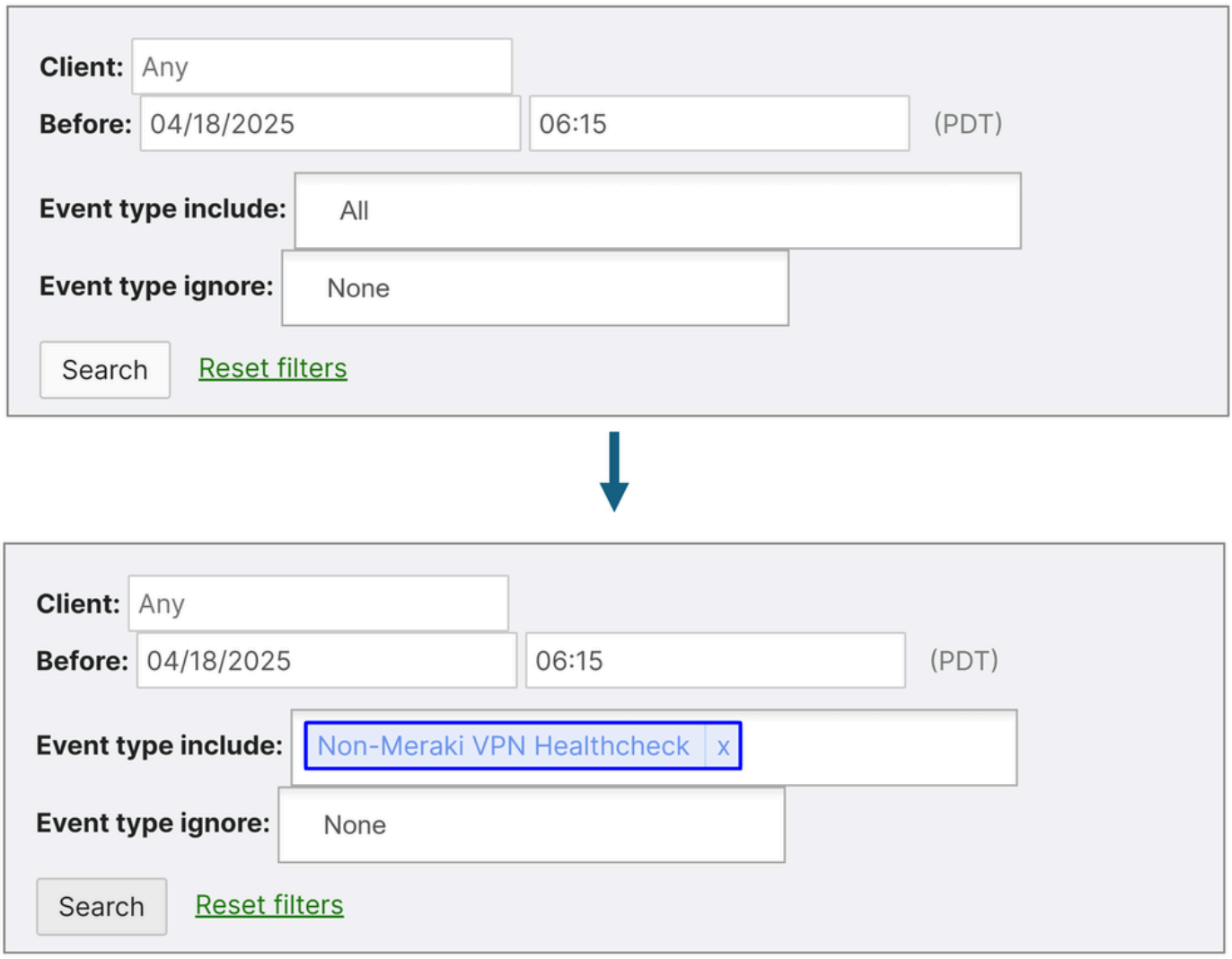
## ヘルスチェックの確認

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

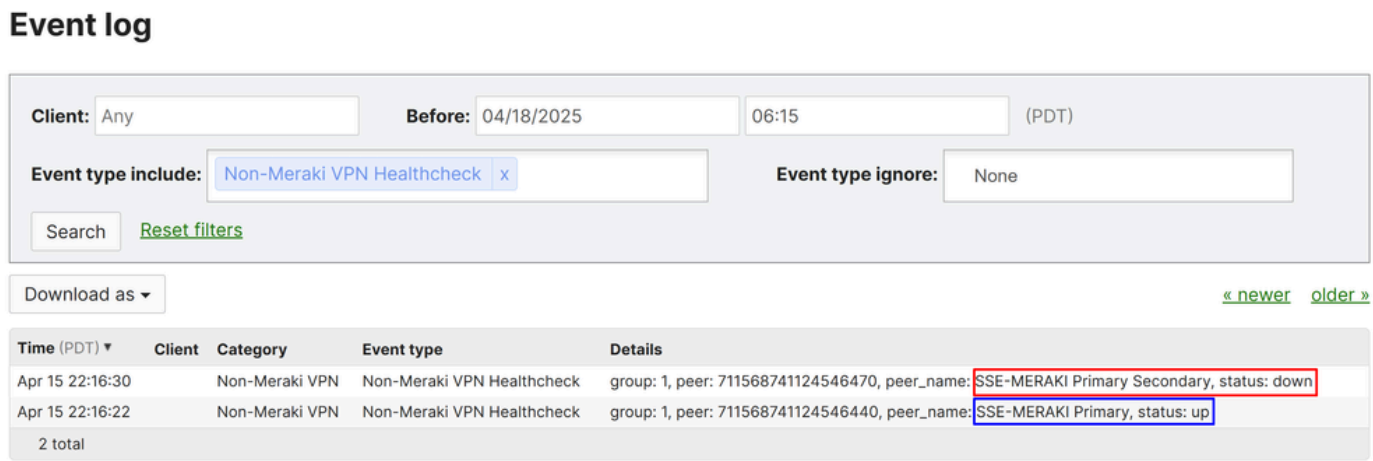



**Event Type Include**で、次のいずれかを選択します。 Non-Meraki VPN Healthcheck




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。



- 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。