Sophos XGファイアウォールを使用したセキュアアクセスの設定

内容

はじめに

このドキュメントでは、Sophos XGファイアウォールでセキュアアクセスを設定する方法について説明します。

前提条件

- ユーザプロビジョニングの設定
- ZTNA SSO認証設定
- リモートアクセスVPNセキュアアクセスの設定

要件

次の項目に関する知識があることが推奨されます。

- Sophos XGファイアウォール

- セキュアなアクセス
- Cisco Secure Client - VPN（トンネルモード）
- Cisco Secureクライアント – ZTNA
- クライアントレスZTNA

使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- Sophos XGファイアウォール
- セキュアなアクセス
- Cisco Secure Client - VPN（トンネルモード）
- Cisco Secureクライアント – ZTNA

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

SOPHOS

セキュアなアクセス – Sophos

シスコは、プライベートアプリケーション（オンプレミスとクラウドベースの両方）へのアクセスの保護とプロビジョニングを確実に行えるように、セキュアなアクセスを設計しました。また、ネットワークからインターネットへの接続も保護します。これは、複数のセキュリティ方式とレイヤの実装によって実現されます。すべての目的は、クラウド経由でアクセスする情報を保持

することです。

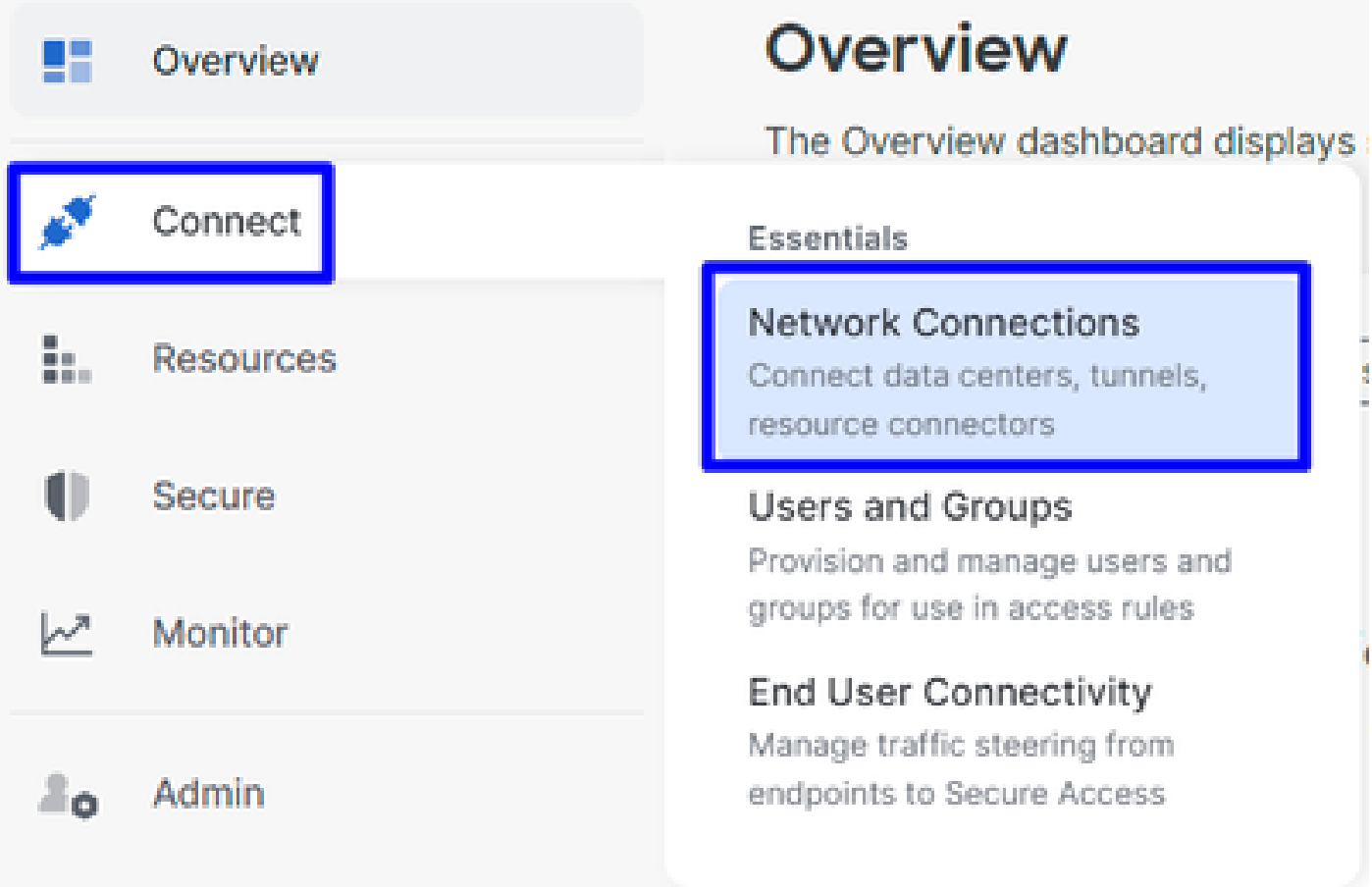
設定

セキュアアクセスでのトンネルの設定

Secure Accessの管理パネルに移動します。

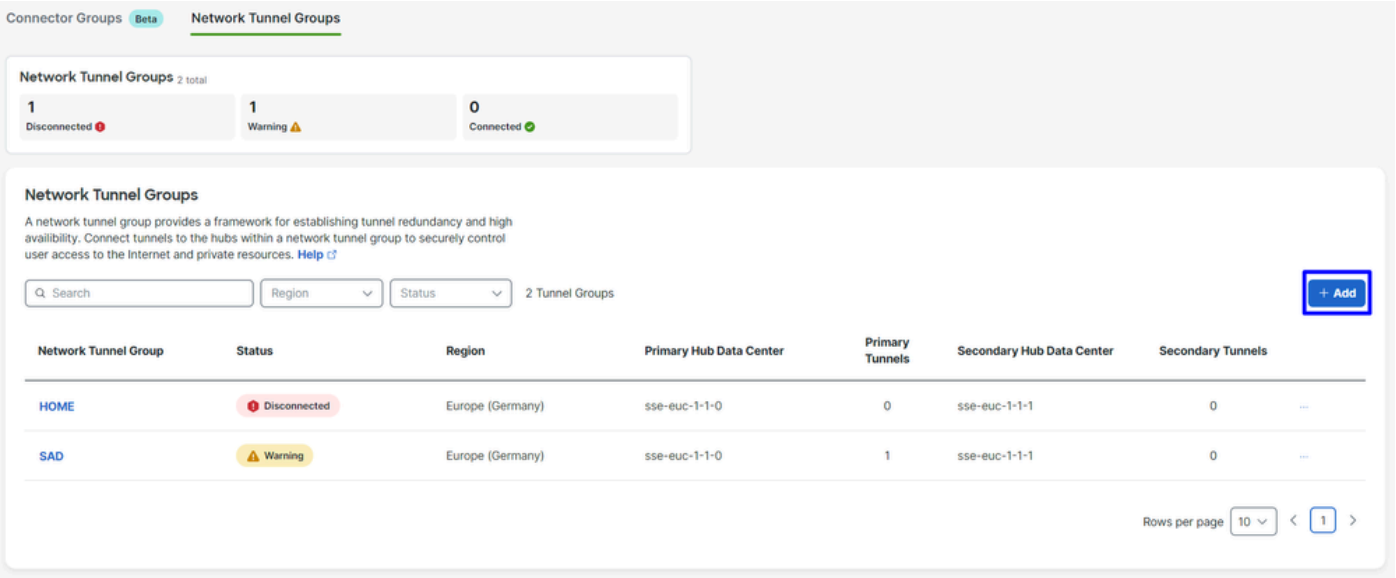
セキュアアクセス – メインページ

- クリック Connect > Network Connections.



セキュアアクセス – ネットワーク接続

- Network Tunnel Groupsの下で、+ Addをクリックします。



セキュアアクセス – ネットワークトンネルグループ

- Tunnel Group Name、Region、およびDevice Typeを設定します。
- をクリックします。 **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

SophosFirewall

Region

Europe (Germany)

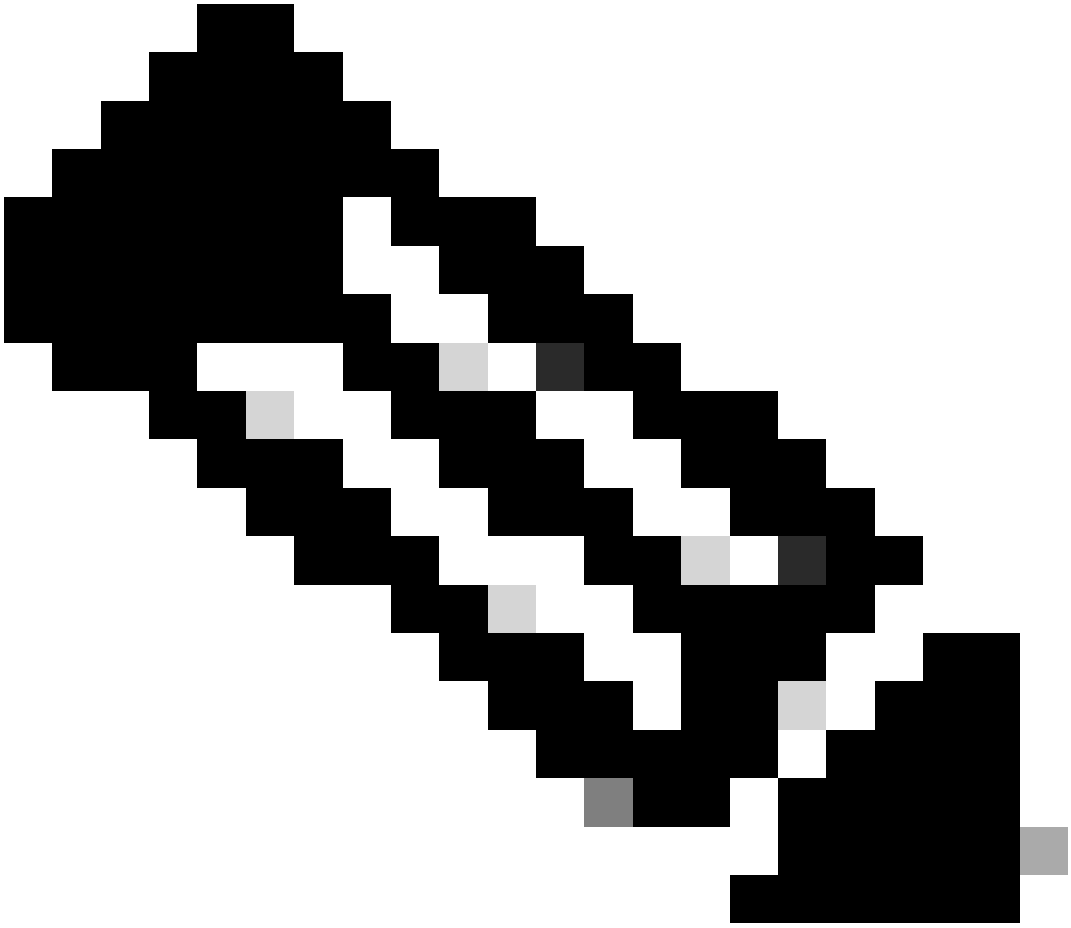
Device Type

Other

Cancel

Next

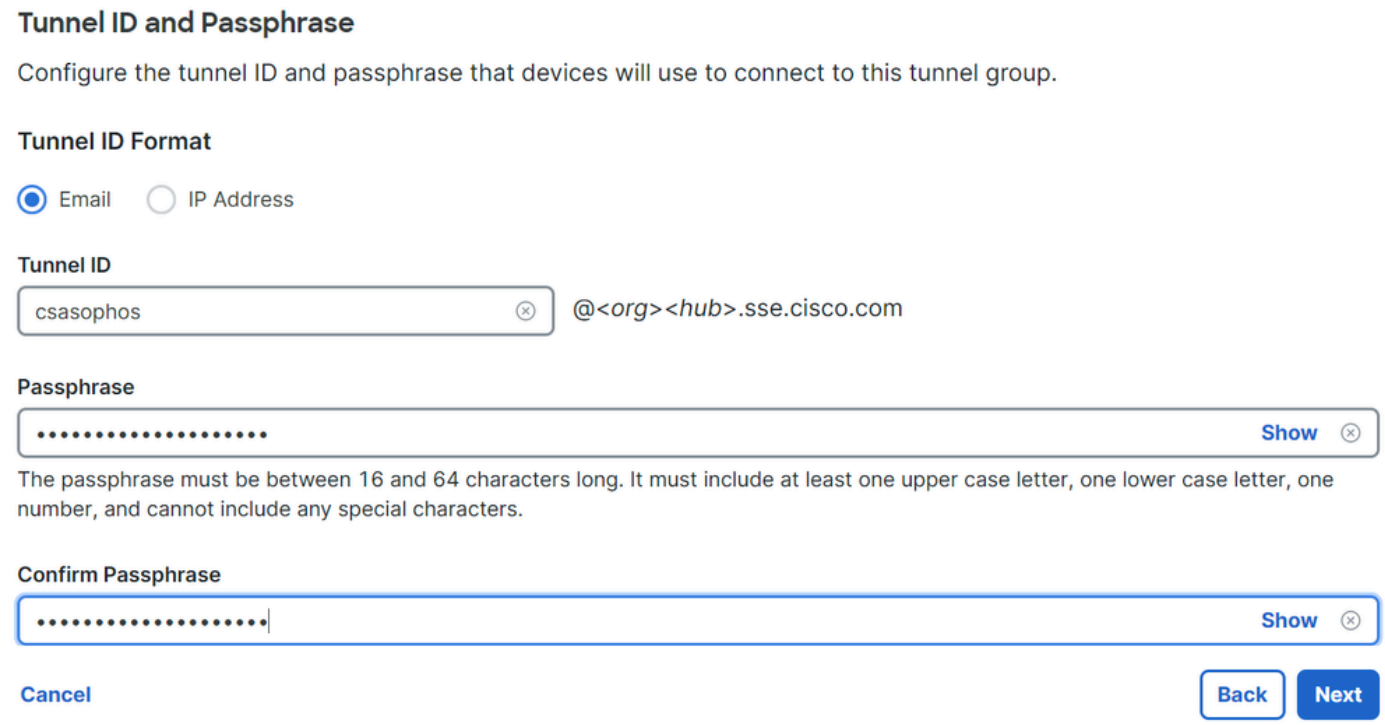
セキュアアクセス – トンネルグループ – 一般設定



注：ファイアウォールの場所に最も近い地域を選択します。

Tunnel ID Format

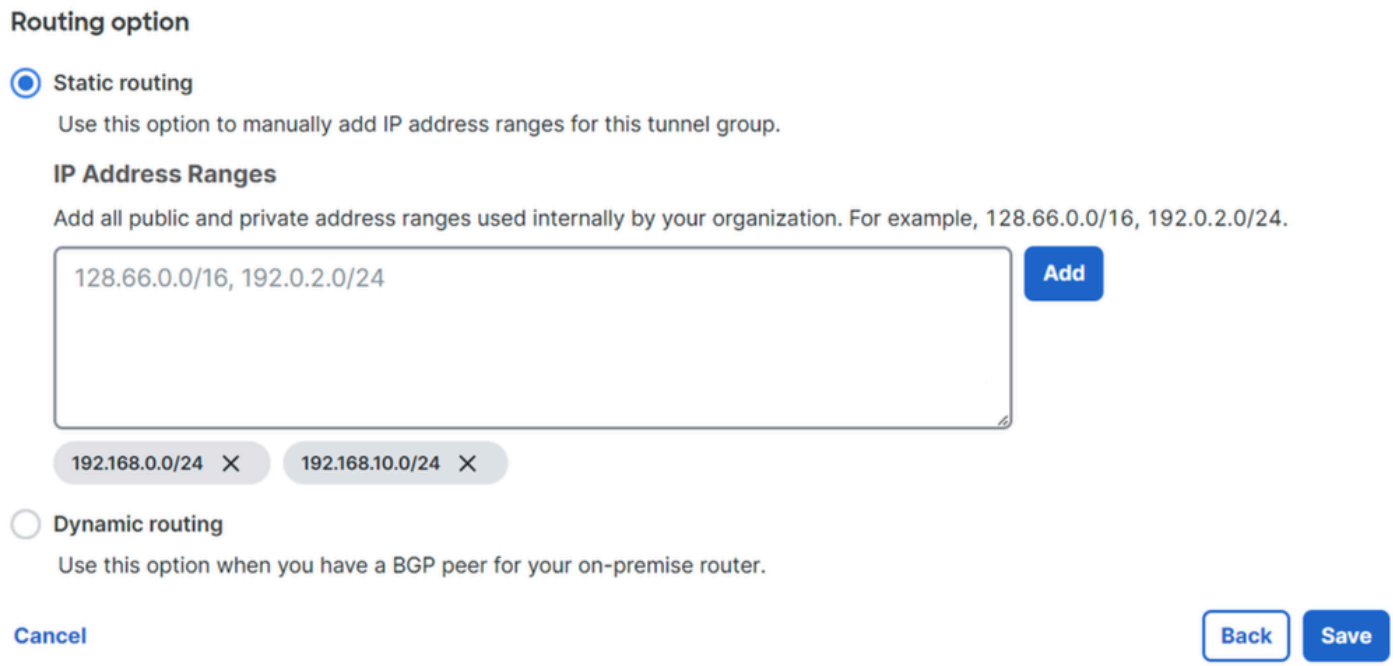
- およびPassphraseを設定します。
- をクリックします。Next



セキュアアクセス – トンネルグループ – トンネルIDおよびパスフレーズ

- ネットワークで設定した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通過させる。

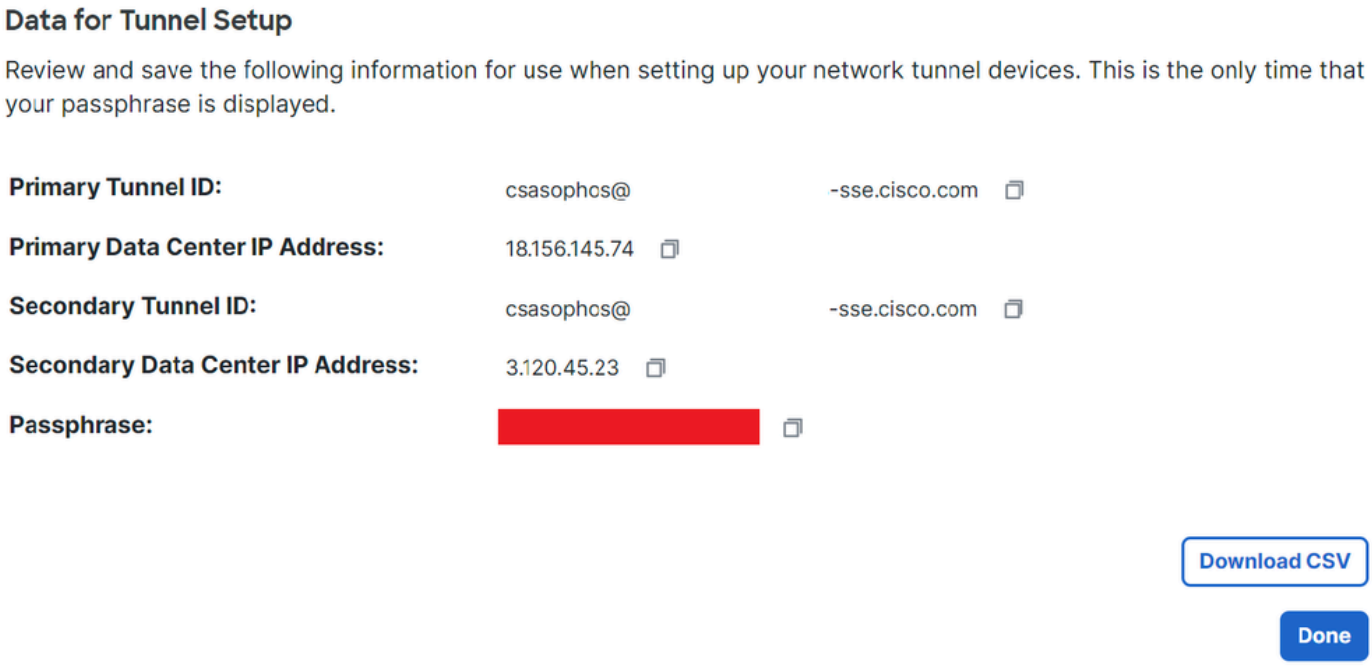
- をクリックします。 **Save**



セキュアアクセス – トンネルグループ – ルーティングオプション

トンネルに関すSave る情報をクリックして表示した後、次の手順Configure the tunnel on Sophosでその情報を保存してください。

トンネルデータ



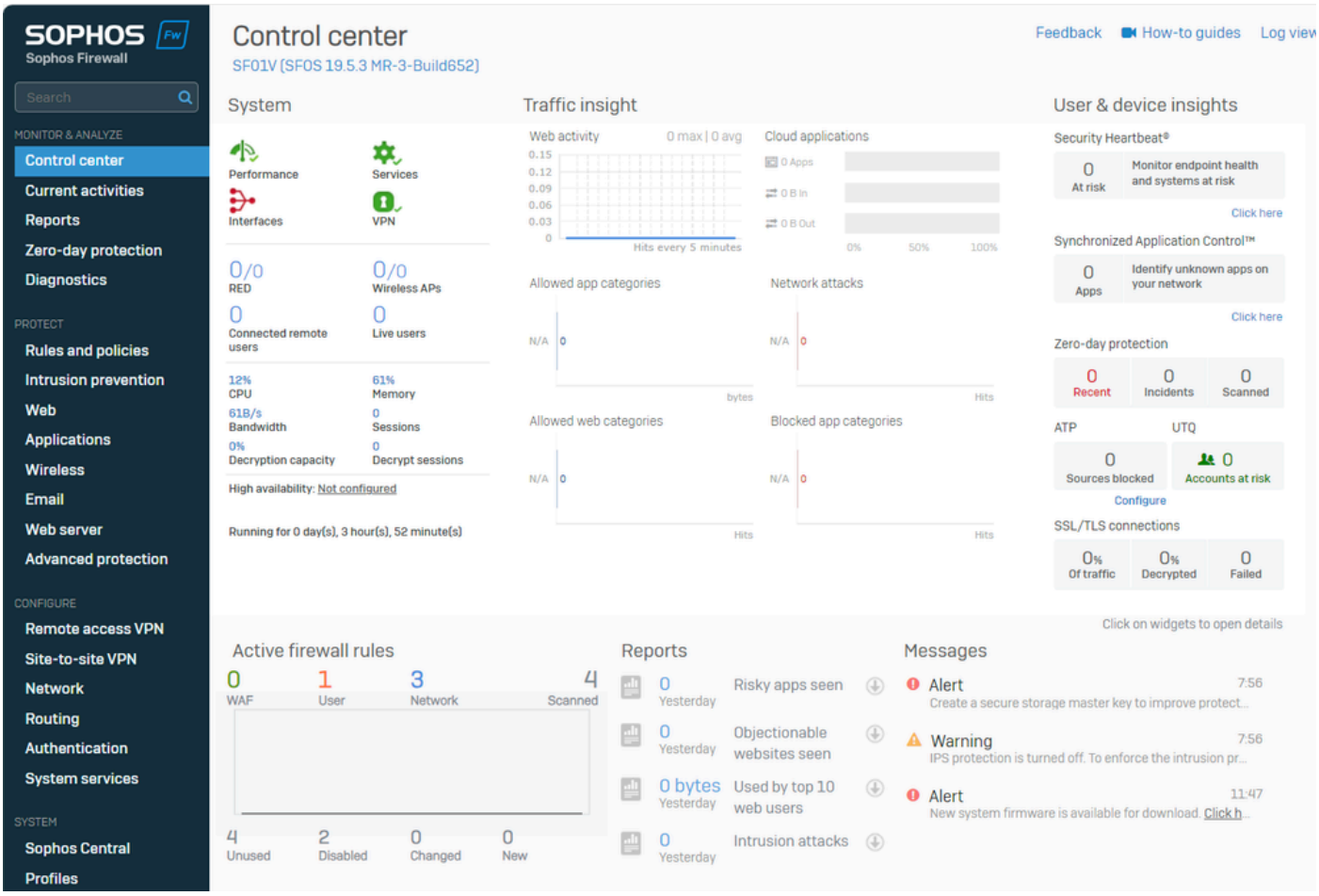
セキュアアクセス – トンネルグループ – 設定の再開

Sophosでのトンネルの設定

IPSecプロファイルの設定

IPsecプロファイルを設定するには、Sophos XGファイアウォールに移動します。

次のような結果が得られます。

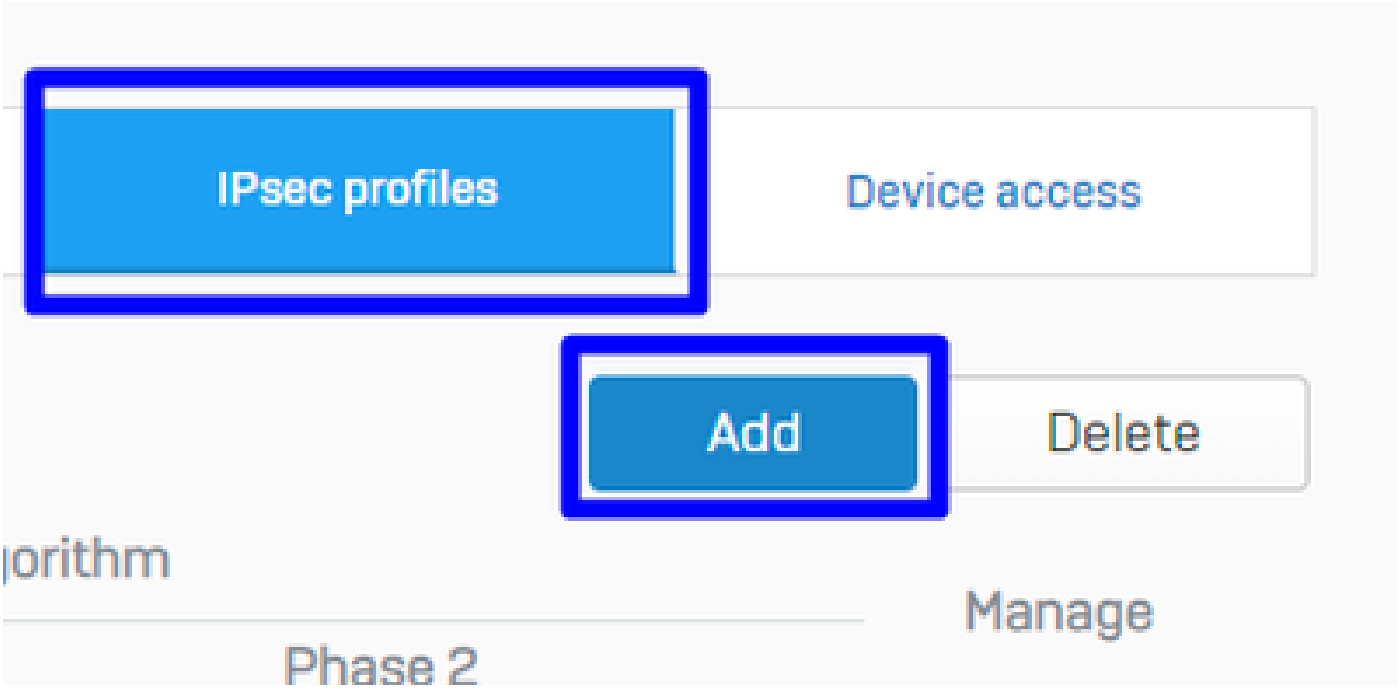


Sophos – 管理パネル

- 移動先 Profiles

IPsec Profiles

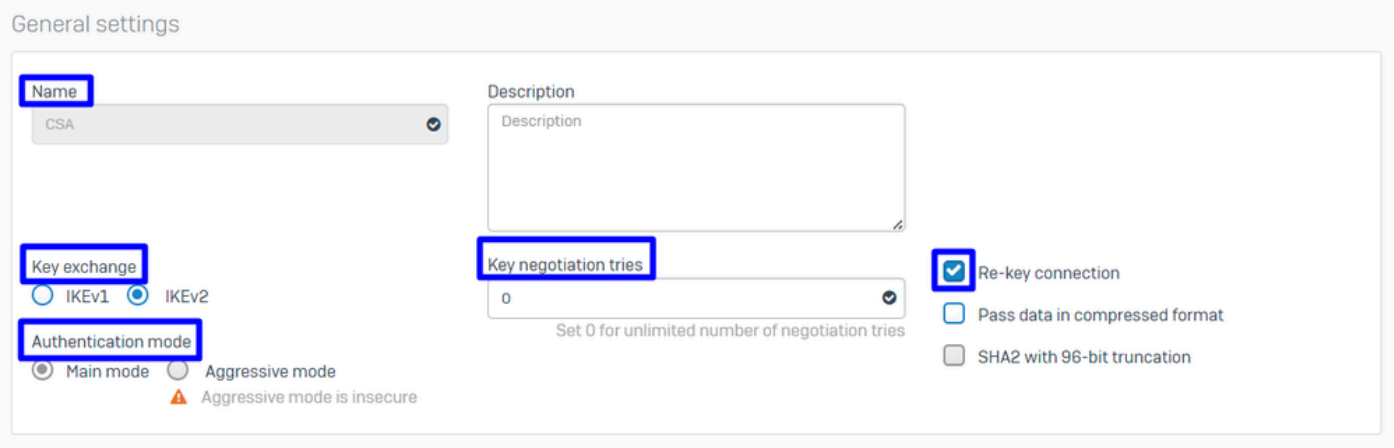
- をクリックし、その後でAdd



Sophos:IPsecプロファイル

設General Settings 定の下：

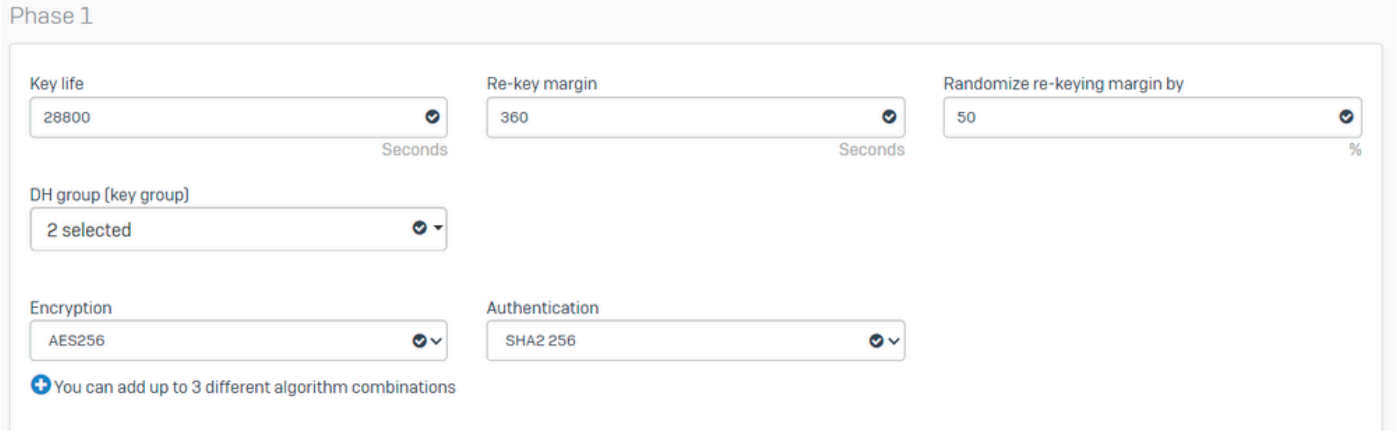
- **Name**:Cisco Secure Access Policyへの参照名
- **Key Exchange**:IKEv2
- **Authentication Mode**:Main Mode
- **Key Negotiation Tries**:0
- **Re-Key connection**：オプションをオンにします。



Sophos - IPsecプロファイル – 全般設定

設Phase 1 定の下：

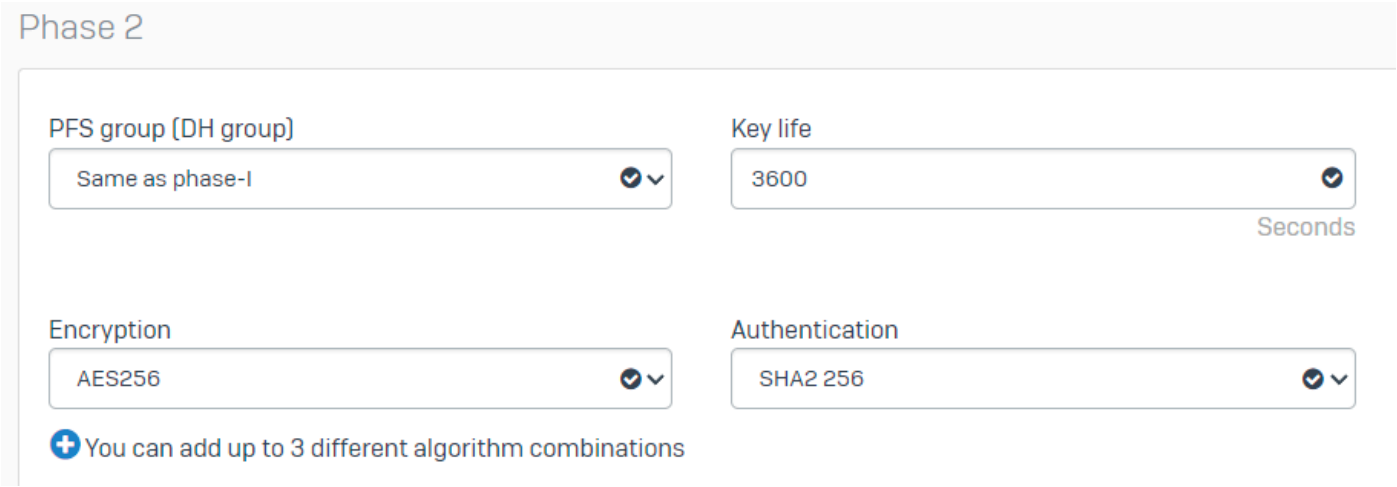
- **Key Life**:28800
- **DH group(key group)**: 19と20を選択
- **Encryption**: AES256
- **Authentication**: SHA2 256
- Re-key margin:360（デフォルト）
- **Randomize re-keying margin by**:50（デフォルト）



Sophos - IPsecプロファイル – フェーズ1

設Phase 2 定の下：

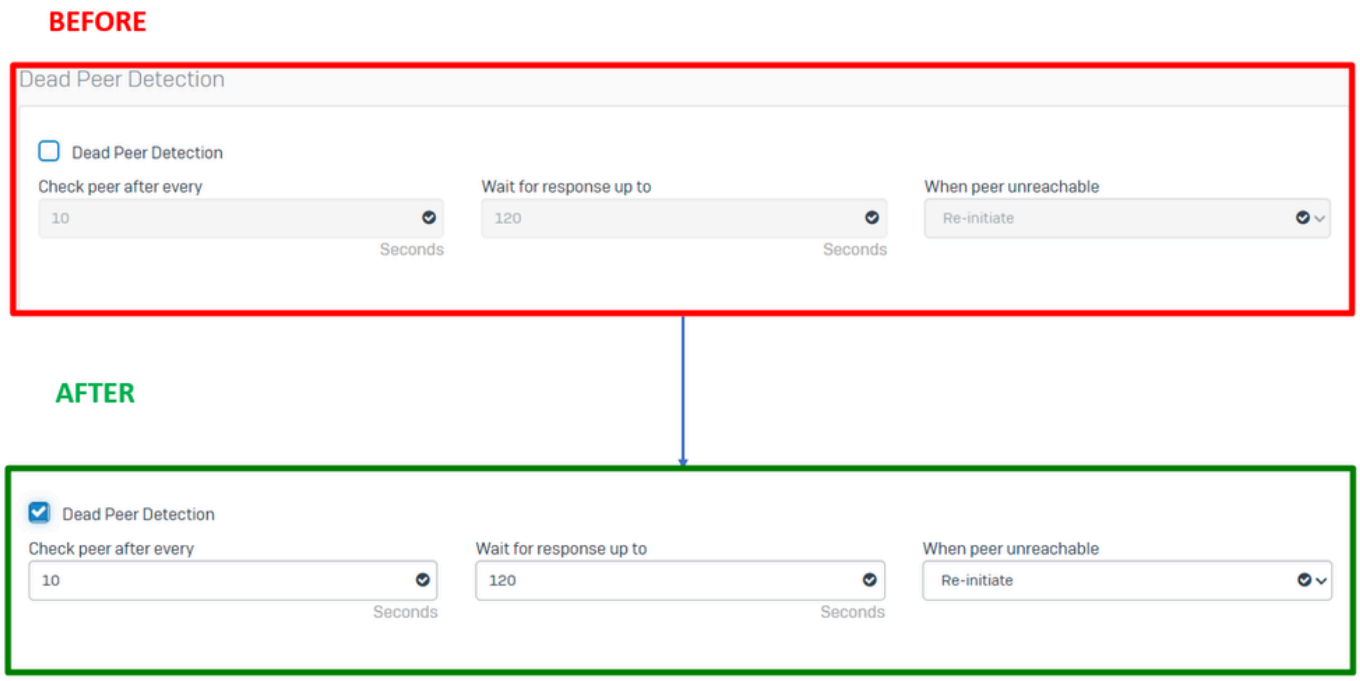
- PFS group (DH group): phase-Iと同じ
- **Key life**:3600
- **Encryption**: AES 256
- Authentication: SHA2 256



Sophos - IPsecプロファイル – フェーズ2

設 Dead Peer Detection 定の下：

- **Dead Peer Detection**：オプションをオンにします。
- **Check peer after every**:10
- **Wait for response up to**:120（デフォルト）
- **When peer unreachable**：再初期化（デフォルト）

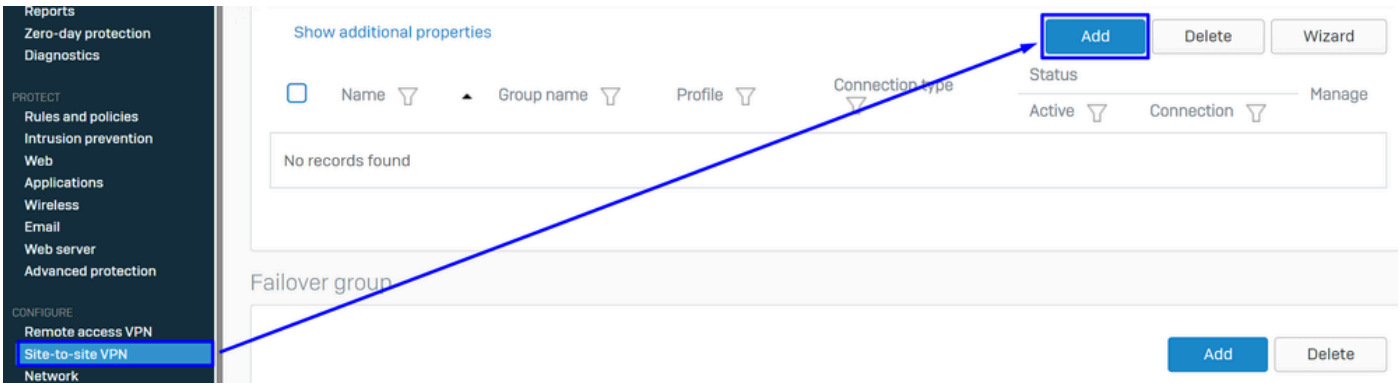


*Sophos - IPsec*プロファイル – デッドピア検出

その後、 **Save** and proceed with the next step, Configure Site-to-site VPNをクリックします。

サイト間VPNの設定

VPNの設定を開始するには、**Site-to-site VPN** をクリックし、 **Add**をクリックします。

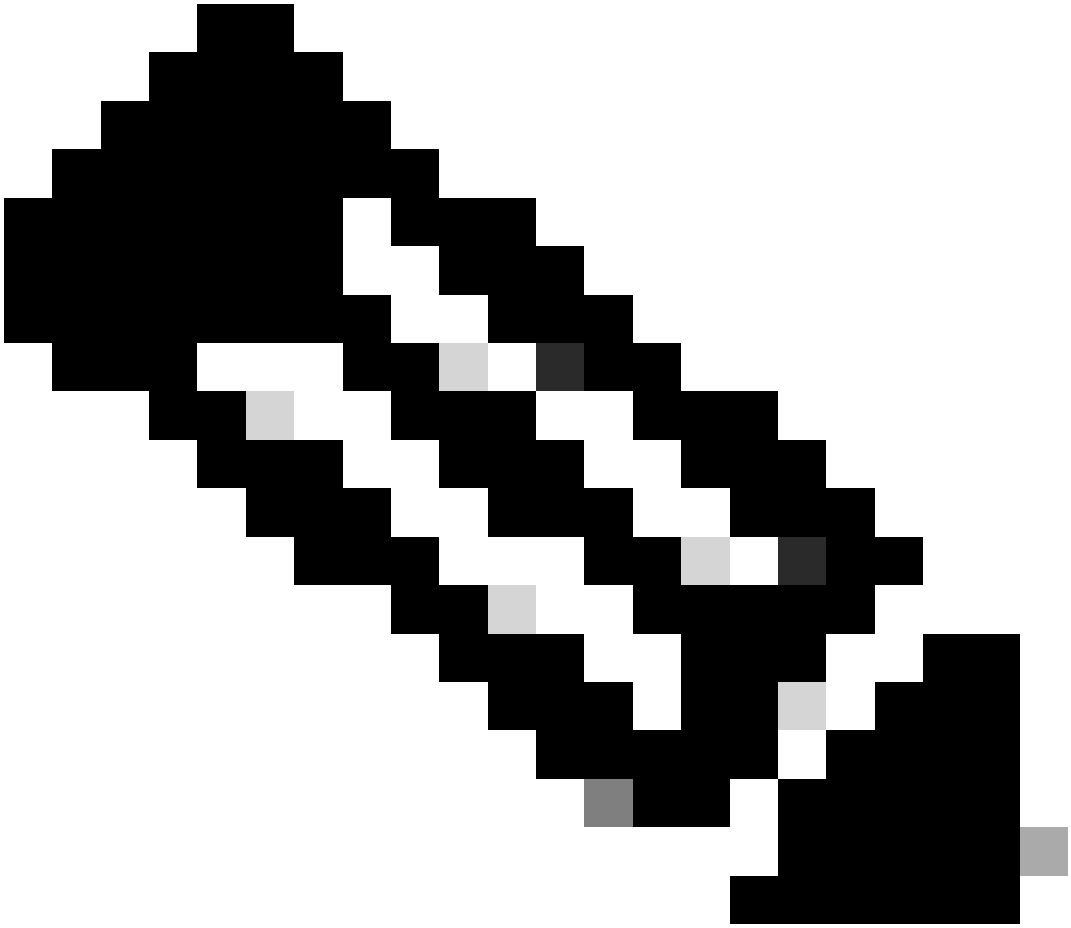


Sophos:Site-to-site VPN (サイト間*VPN*)

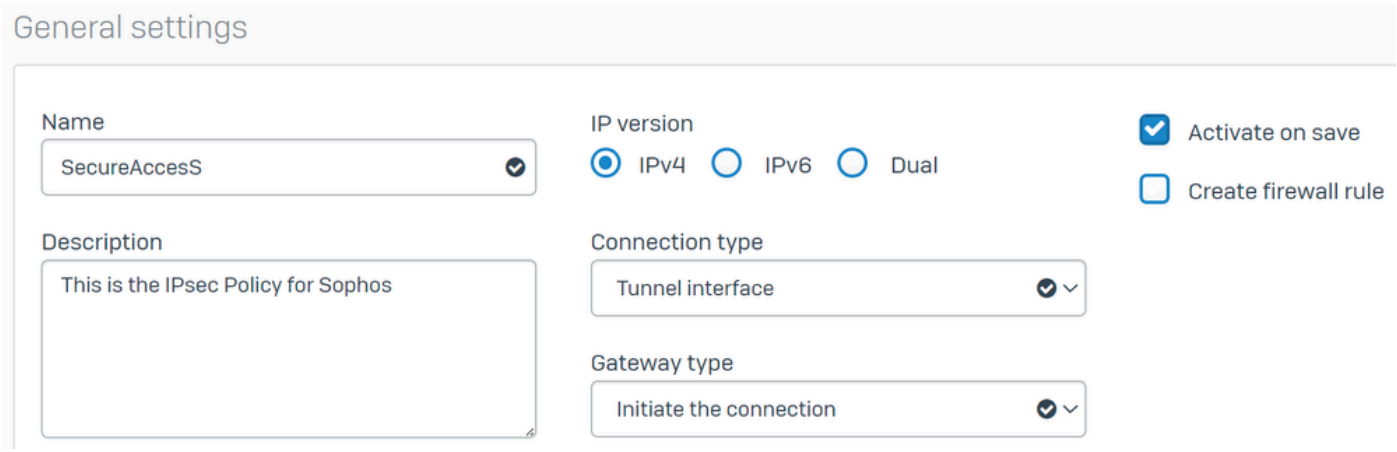
設General Settings 定の下：

- **Name**:Cisco Secure Access IPsecポリシーへの参照名
- IP version: IPv4
- Connection type：トンネルインターフェイス
- Gateway type：接続を開始します

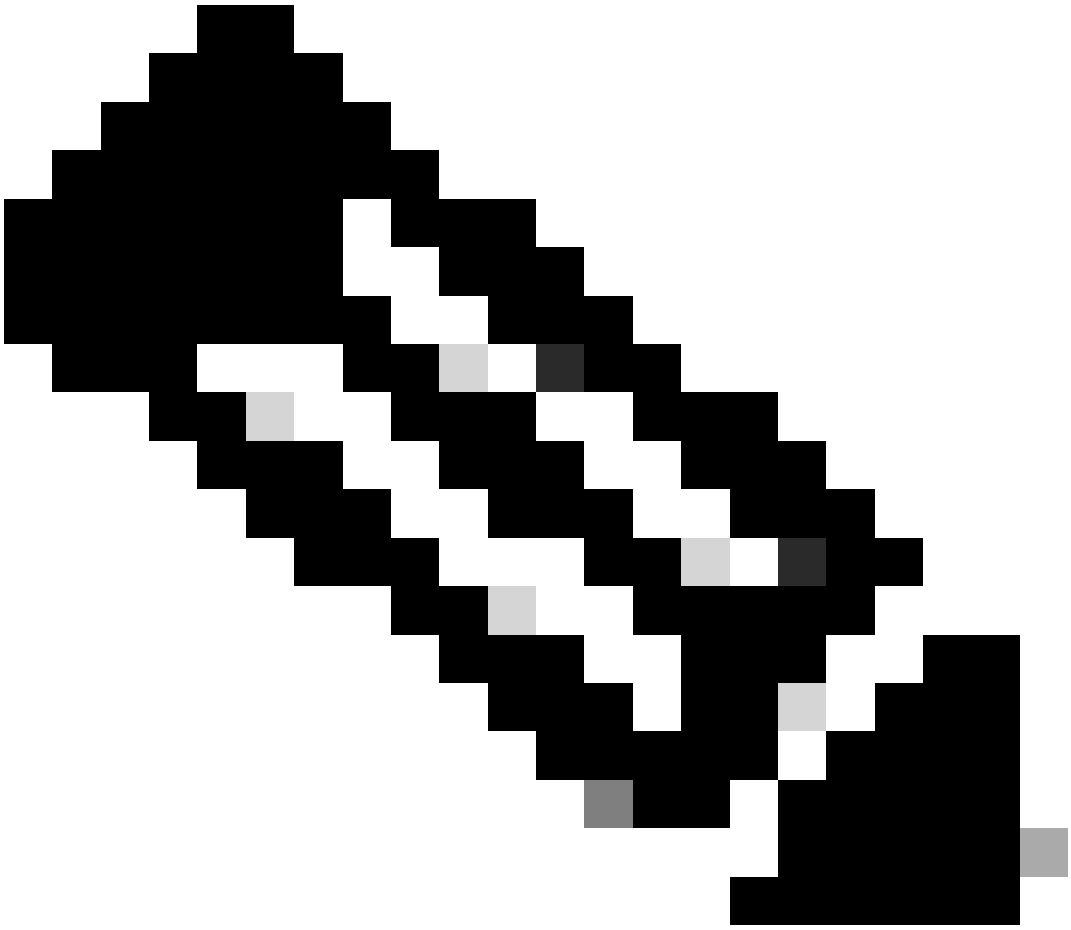
- Active on save：オプションをオンにします。



注：サイト間VPNを設定した後、このオプションによってVPNが自動的に有**Active on save** 効になります。



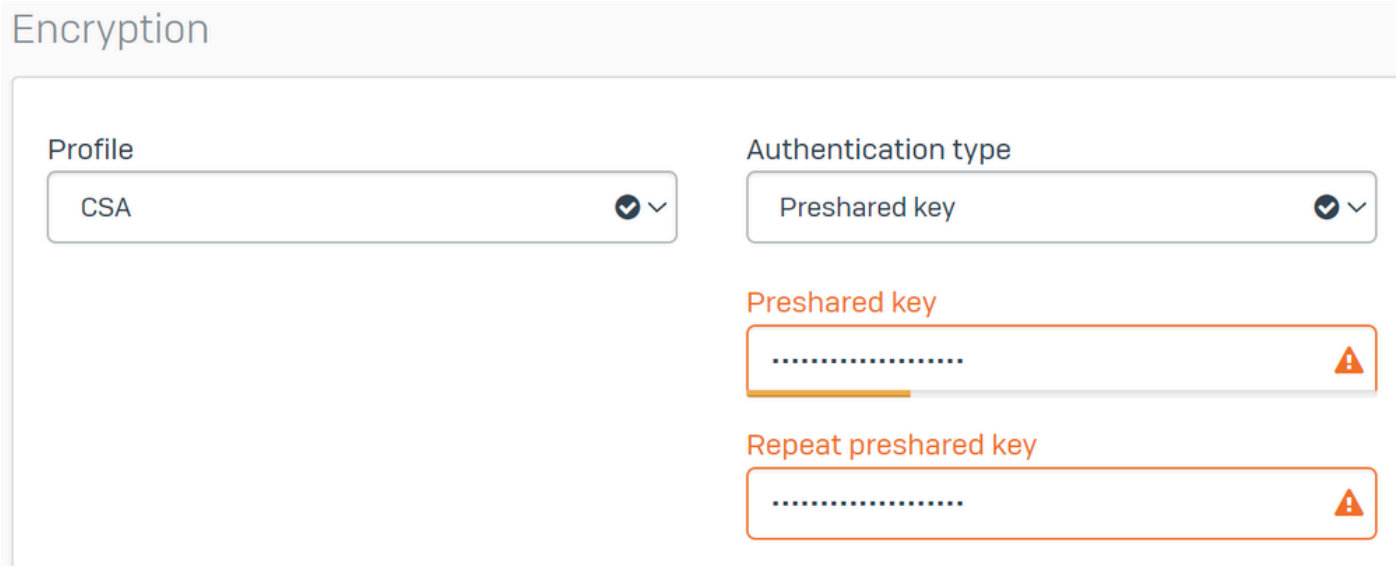
Sophos – サイト間*VPN* – 全般設定



注：オプションのトンネルインターフェイスでは、Sophos XGファイアウォール用の仮想トンネルインターフェイスがXFRMという名前で作成されます。

設Encryption 定の下：

- **Profile**：ステップで作成したプロファイル、 **Configure IPsec Profile**
- **Authentication type**:事前共有鍵
- **Preshared key**：ステップで設定するキー、 Configure the Tunnel on Secure Access
- **Repeat preshared key**: **Preshared key**

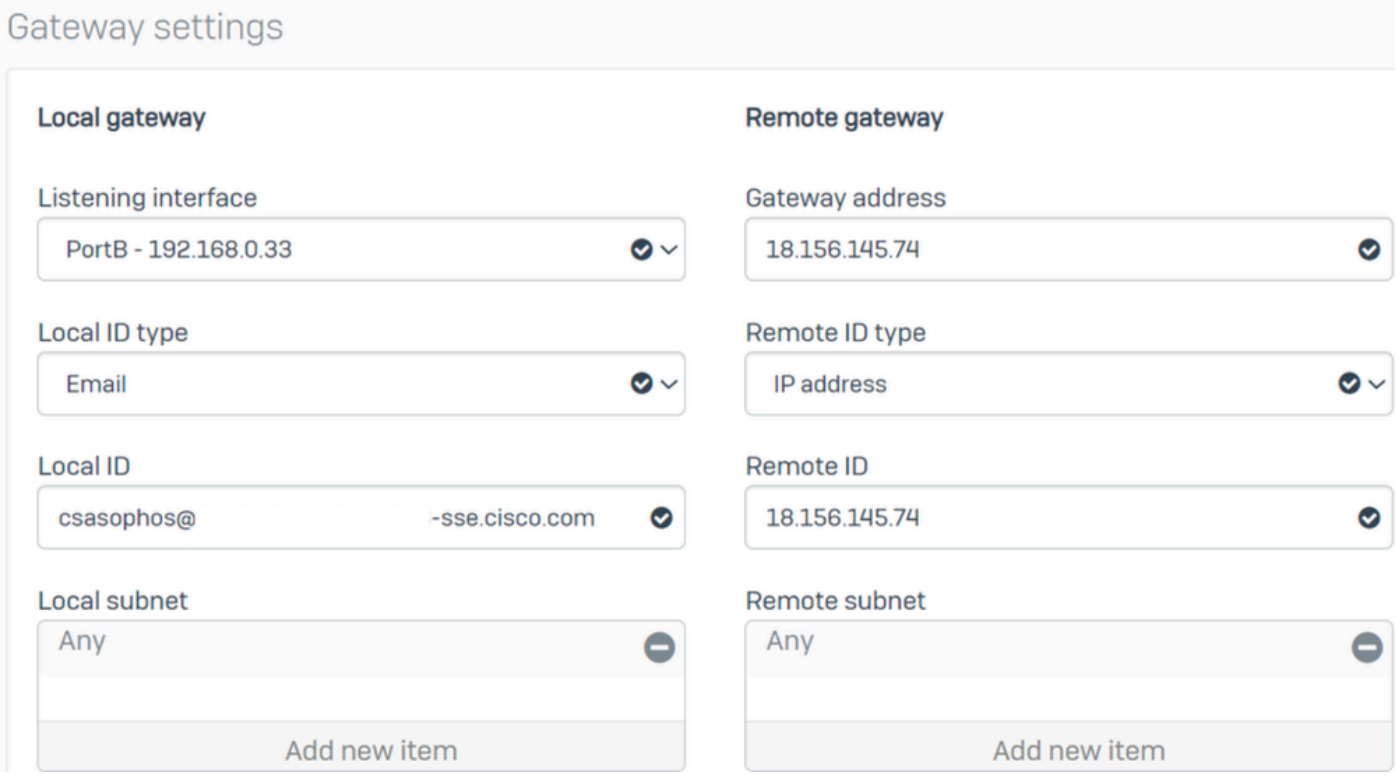


Sophos – サイト間VPN – 暗号化

設Gateway Settings 定 Local Gatewayおよび**Remote Gateway**オプションで、次の表を参照用に使用します。

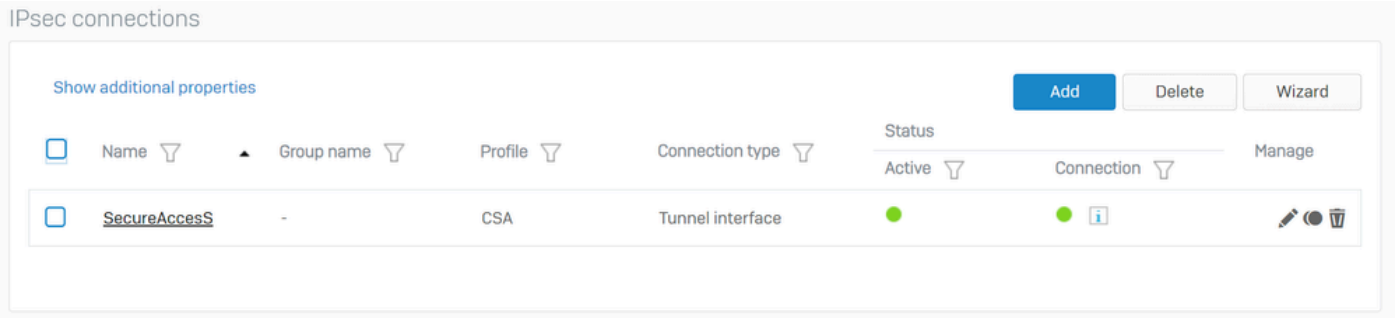
ローカル ゲートウェイ	リモートゲートウェイ
リスニングインターフェイス Wanインターネットインターフェイス	ゲートウェイ アドレス ステップの下で生成されたパブリックIPアドレス、 **Tunnel Data**
ローカルIDタイプ Email	リモートIDの種類

	IP アドレス
ローカルID 手順の下で生成された電子メール Tunnel Data	リモート ID ステップの下で生成されたパブリックIPアドレス、 Tunnel Data
ローカルサブネット [Any]	リモートサブネット [Any]

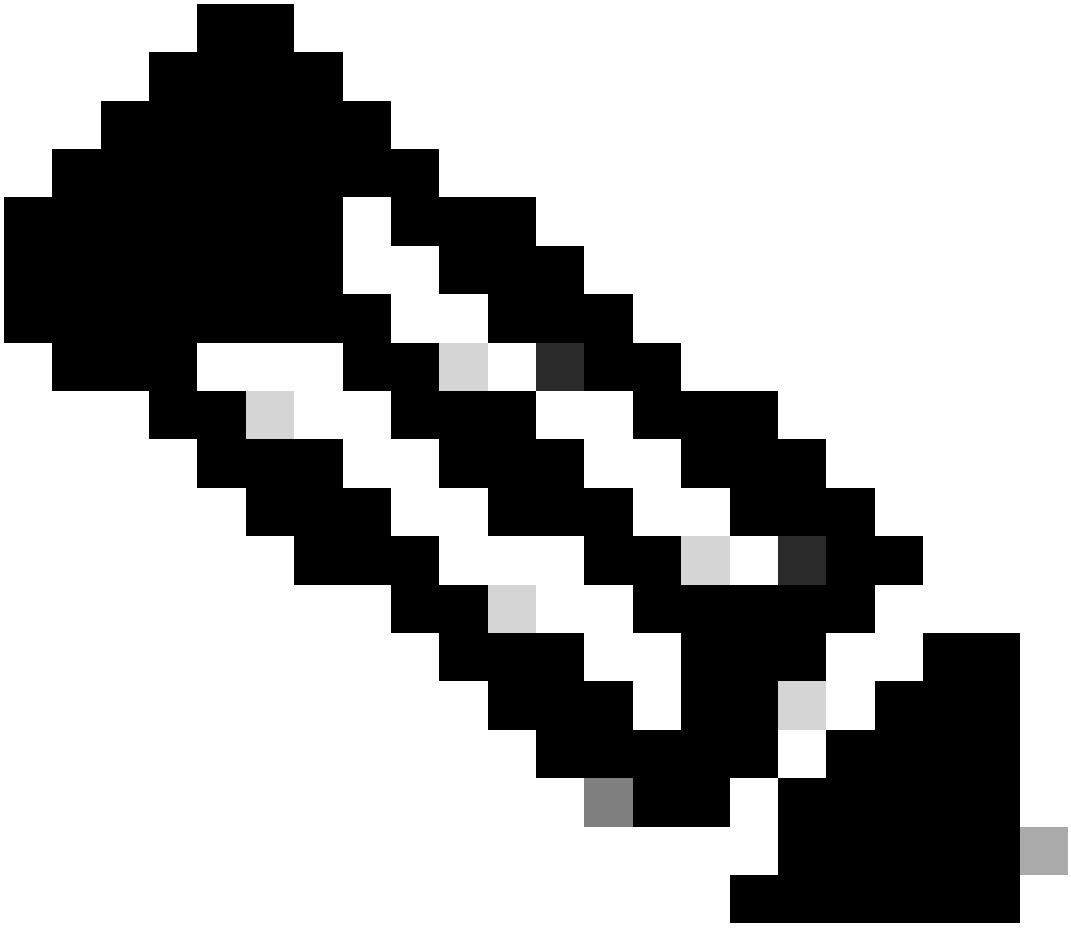


Sophos – サイト間*VPN* – ゲートウェイ設定

その後、**Save**をクリックすると、トンネルが作成されたことが分かります。

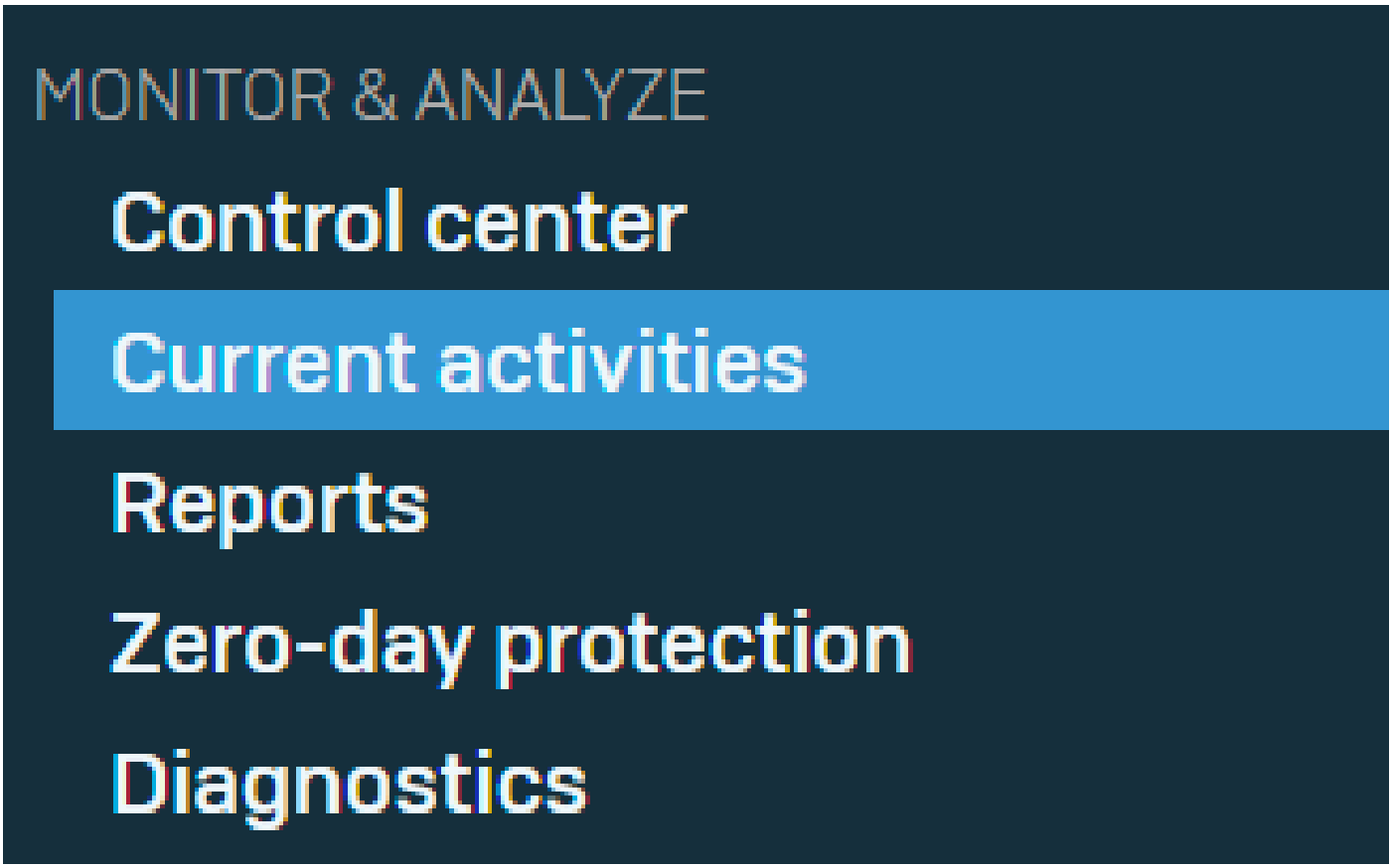


Sophos – サイト間*VPN - IPsec*接続

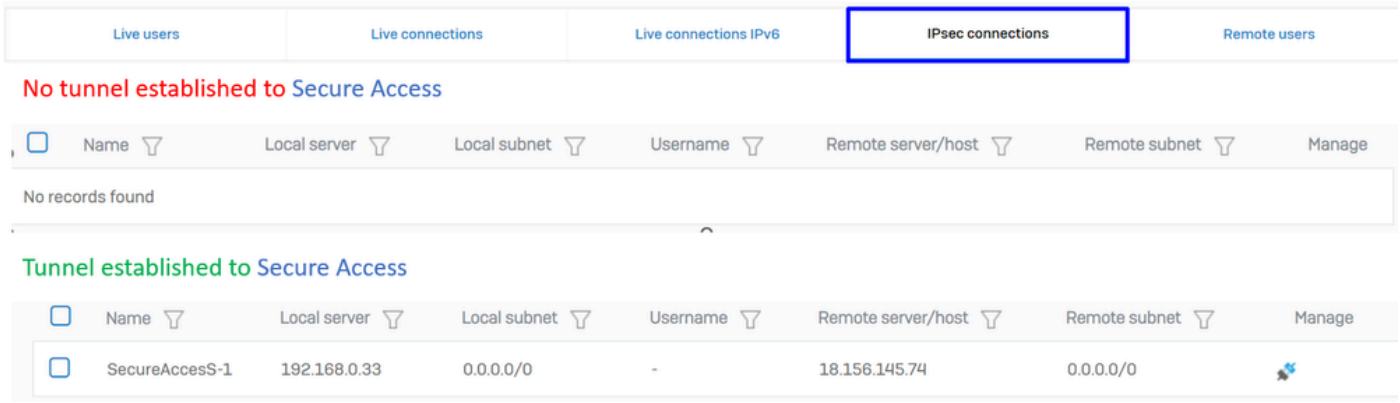


注：最後のイメージでトンネルが正しく有効化されているかどうかを確認するには、**Connection** ステータスを確認します。ステータスが緑の場合、トンネルは接続されています（緑ではない場合）。トンネルは接続されていません。

トンネルが確立されているかどうかを確認するには、 **Current Activities > IPsec Connections**に移動します。



Sophos – 監視と分析 – IPsec



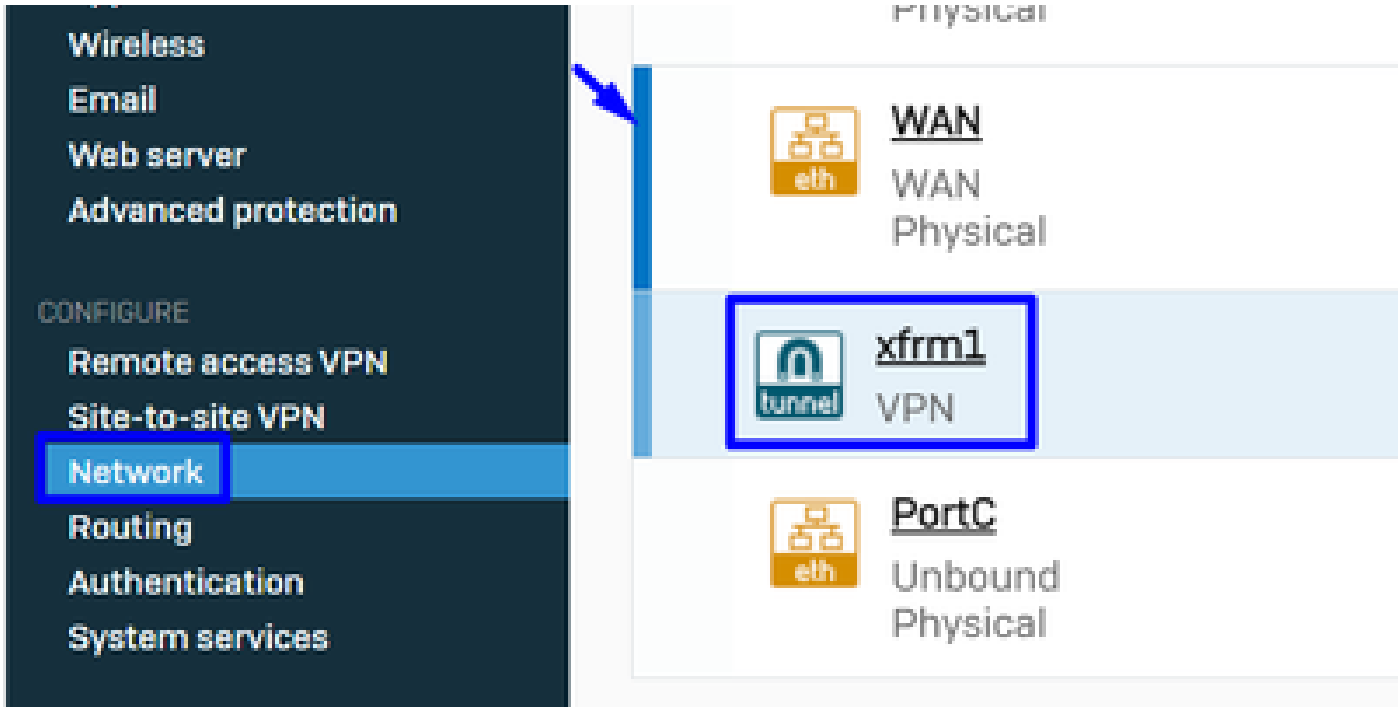
Sophos – 監視と分析 – 前後のIPSec

その後、手順 Configure Tunnel Interface Gatewayに進みます。

トンネルインターフェイスの設定

Network に移動し、VPN上で設定されているWANインターフェイスを確認して、仮想トンネルインターフェイスを名前xfrmで編集します。

- インターフェイス**xfrm** をクリックします。



Sophos – ネットワーク – トンネルインターフェイス

- ネットワーク内でルーティング不可能なIPを使用してインターフェイスを設定します。たとえば、ルーティング不可能な空間のIPである169.254.x.x/30を使用できます。この例では、169.254.0.1/30を使用します

Sophos – ネットワーク – トンネルインターフェイス – 設定

ゲートウェイの設定

仮想インターフェイス(xfrm)のゲートウェイを設定するには、

- 移動先 Routing > Gateways
- クリック Add

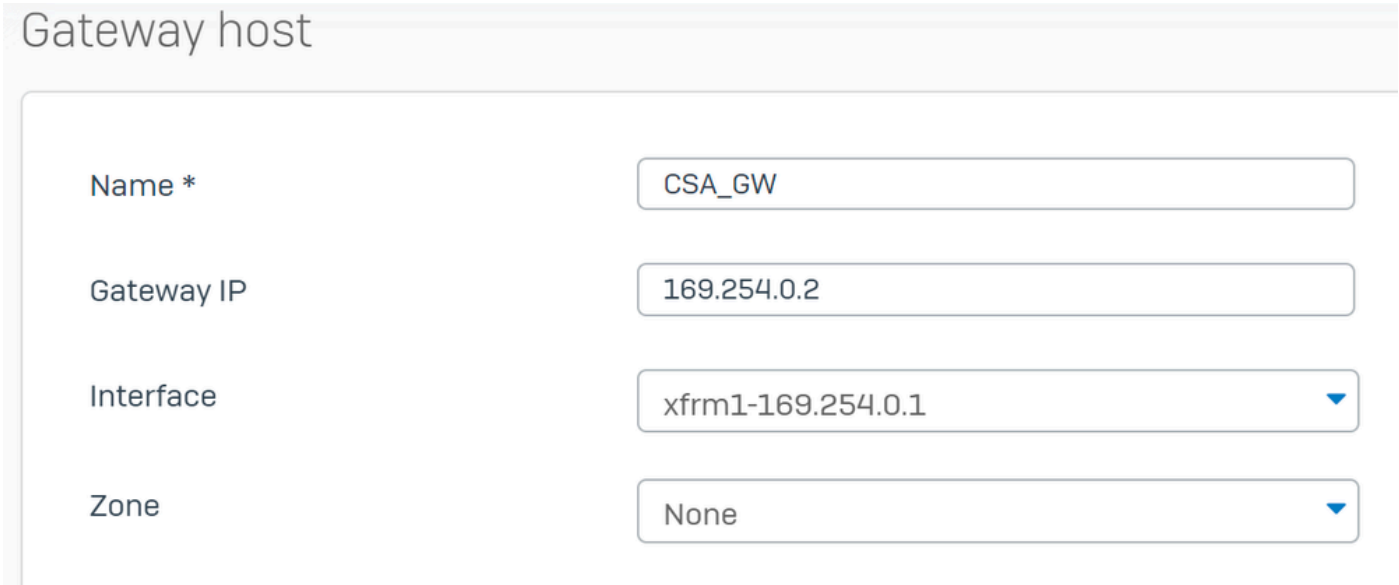
Sophos – ルーティング – ゲートウェイ

設Gateway host 定の下：

- **Name**:VPN用に作成された仮想インターフェイスを参照する名前
- **Gateway IP**：この例では169.254.0.2が、このステップですでに割り当てたネットワーク169.254.0.1/30のIPです。

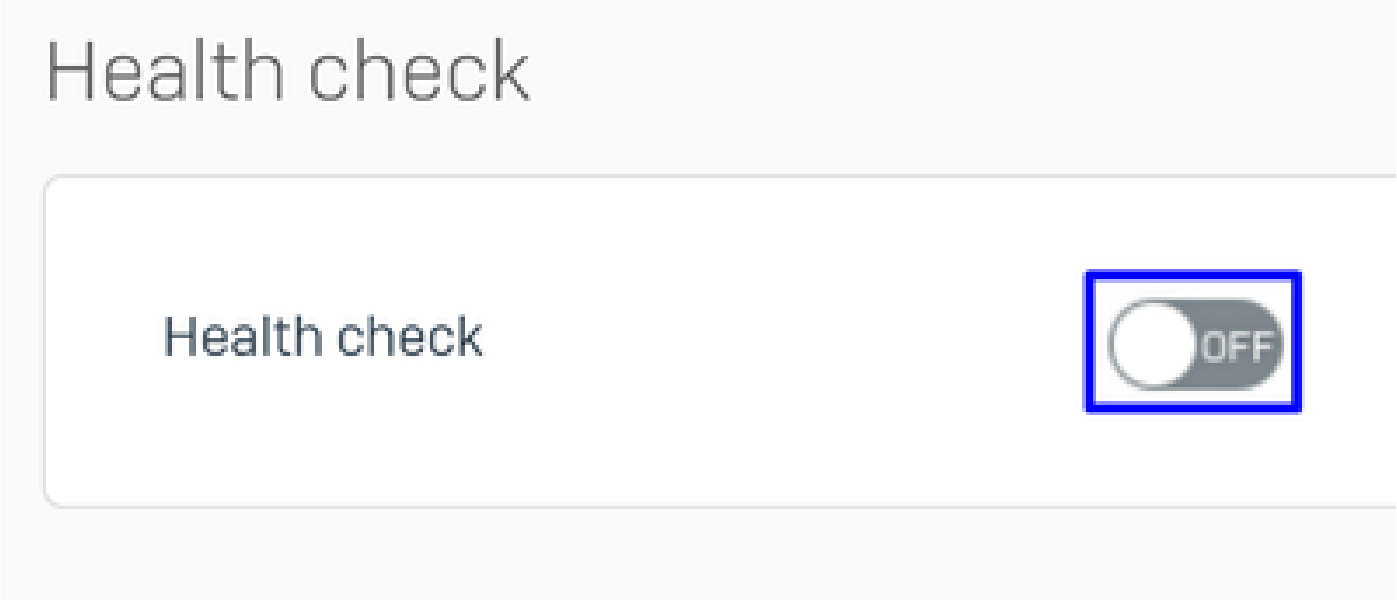
Configure Tunnel Interface

- Interface:VPN仮想インターフェイス
- **Zone**：なし（デフォルト）



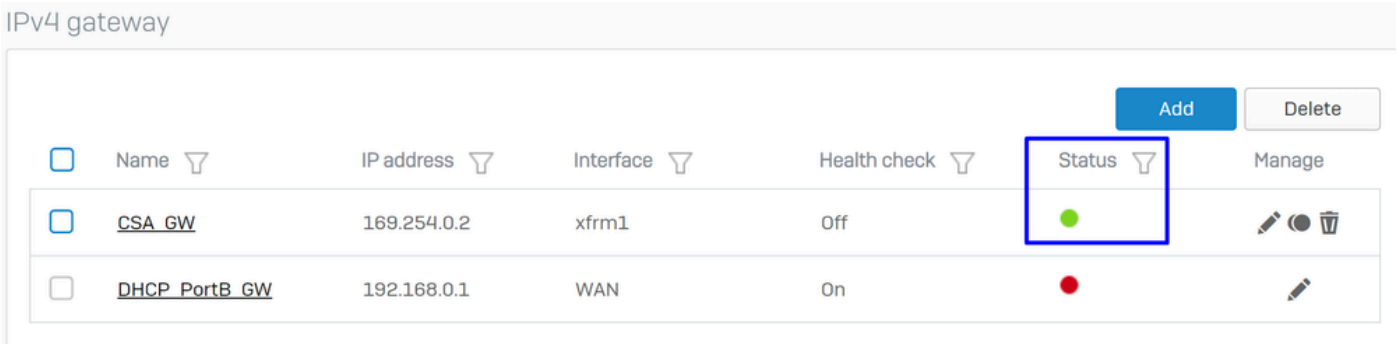
Sophos – ルーティング – ゲートウェイ – ゲートウェイホスト

- チェックを無**Health check** 効にする
- クリック **Save**



Sophos – ルーティング – ゲートウェイ – ヘルスチェック

設定を保存すると、ゲートウェイのステータスを確認できます。



Sophos – ルーティング – ゲートウェイ – ステータス

SD-WANルートの設定

設定プロセスを完了するには、トラフィックをセキュアアクセスに転送できるルートを作成する必要があります。

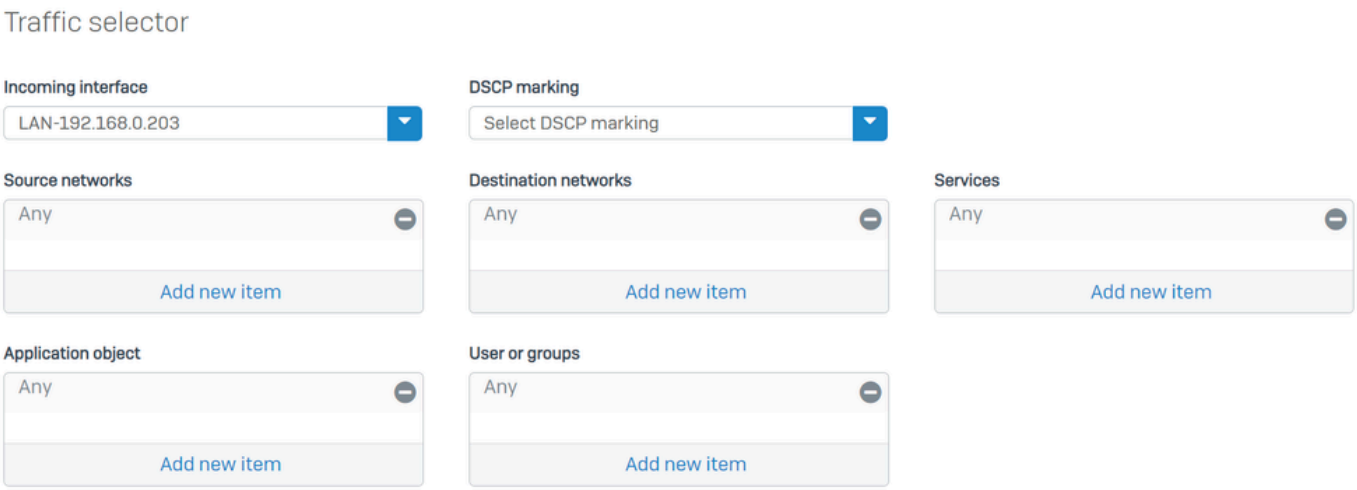
移動先 **Routing > SD-WAN routes.**

- クリック **Add**

Sophos:SD-Wanルート

設**Traffic Selector** 定の下：

- Incoming interface：トラフィックを送信するインターフェイス、またはRA-VPN、ZTNA、またはクライアントレスZTNAからアクセスするユーザを選択します。
- DSCP marking：この例では何も行いません
- **Source networks**：トンネル経由でルーティングするアドレスを選択します
- **Destination networks**：任意の宛先、または宛先を指定できます。
- **Services**：サービスを指定できます。
- **Application object**：オブジェクトが構成されている場合のアプリケーション
- User or groups：特定のユーザグループを追加して、トラフィックをセキュアアクセスにルーティングする場合

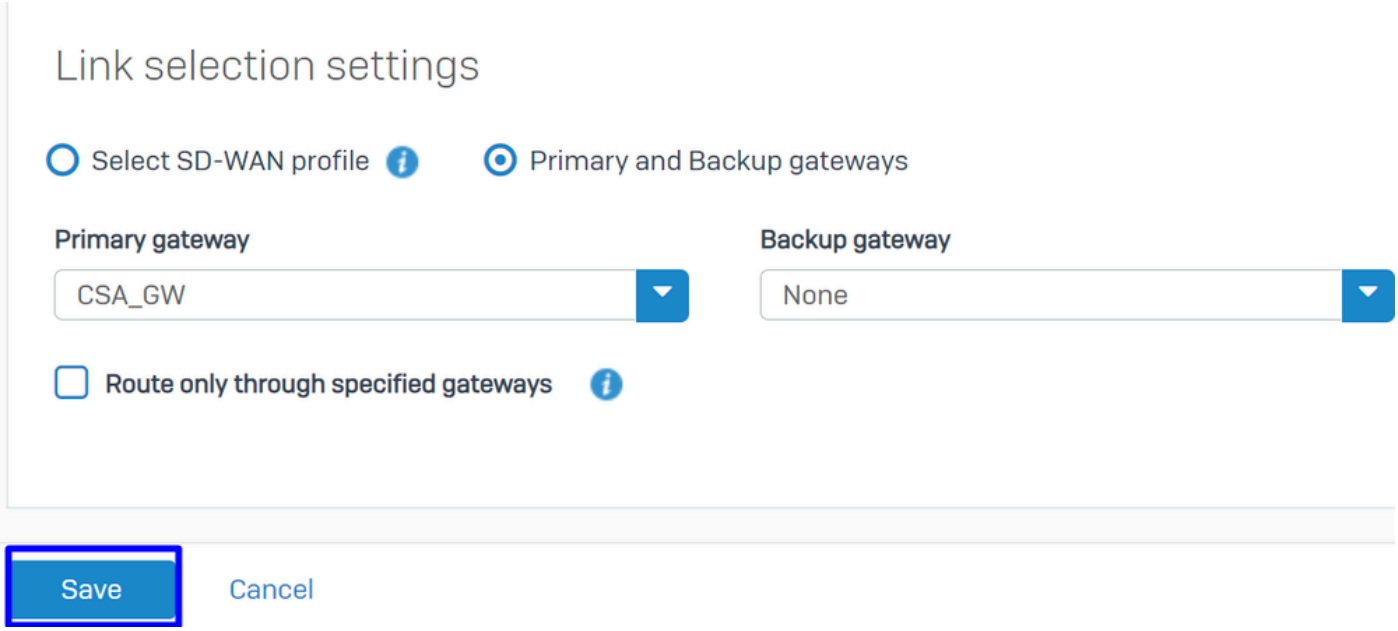


Sophos - SD-Wanルート – トラフィックセレクタ

ゲートウェイの設**Link selection settings** 定：

- Primary and Backup gateways：オプションをオンにします。

- **Primary gateway**：手順で設定したゲートウェイを選択します。 Configure the Gateways
- クリック **Save**



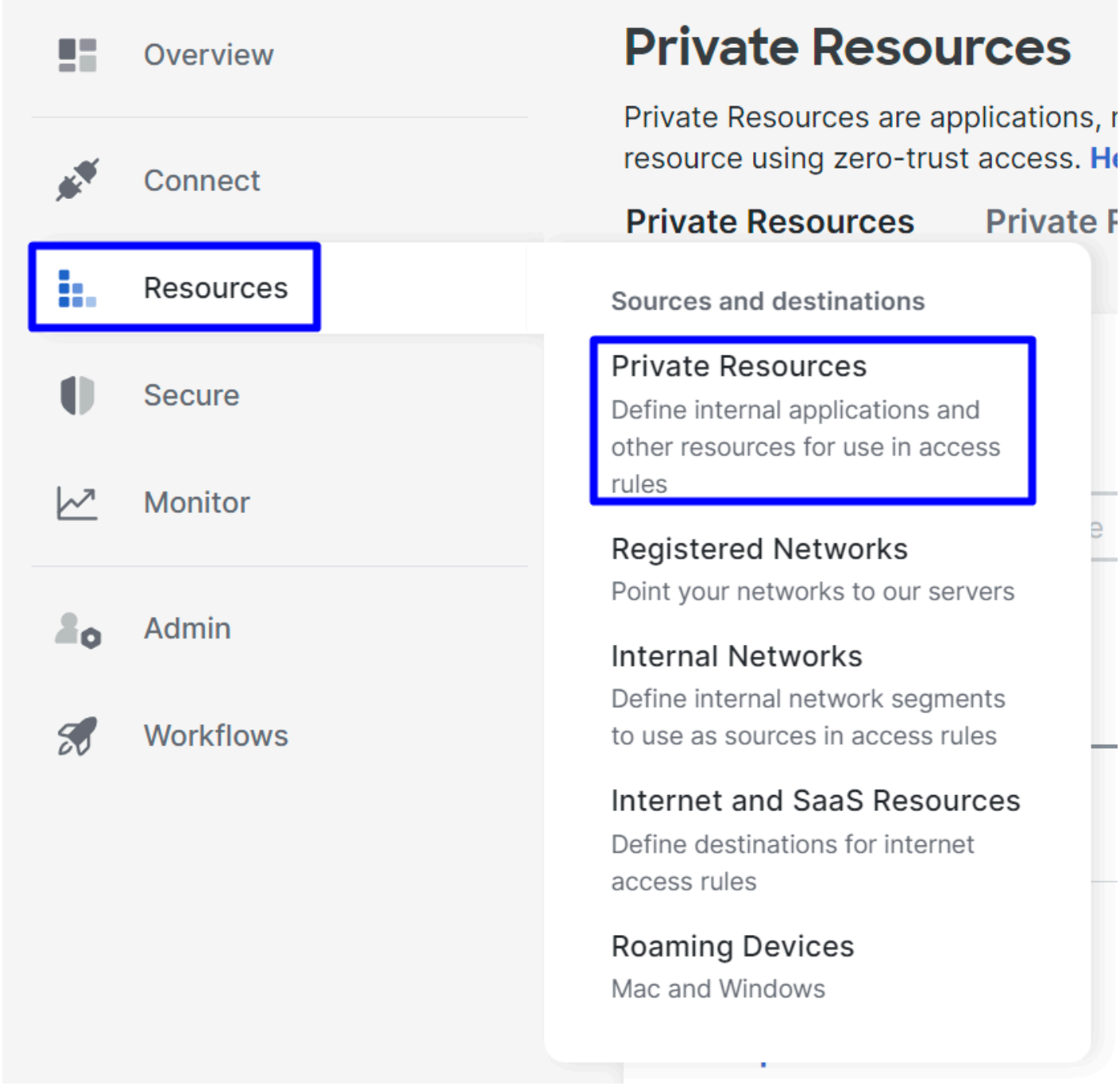
*Sophos - SD-Wan*ルート – トラフィックセレクタ – プライマリおよびバックアップゲートウェイ

Sophos XGファイアウォールの設定を完了したら、次の手順に進みます。 **Configure Private App.**

プライベートアプリの構成

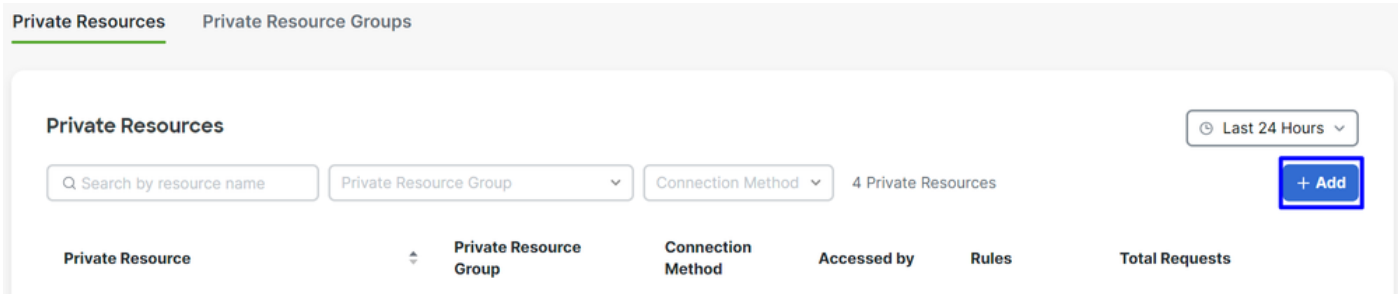
プライベートアプリケーションアクセスを設定するには、管理ポータルにログインします。

- 移動先 **Resources** > **Private Resources**



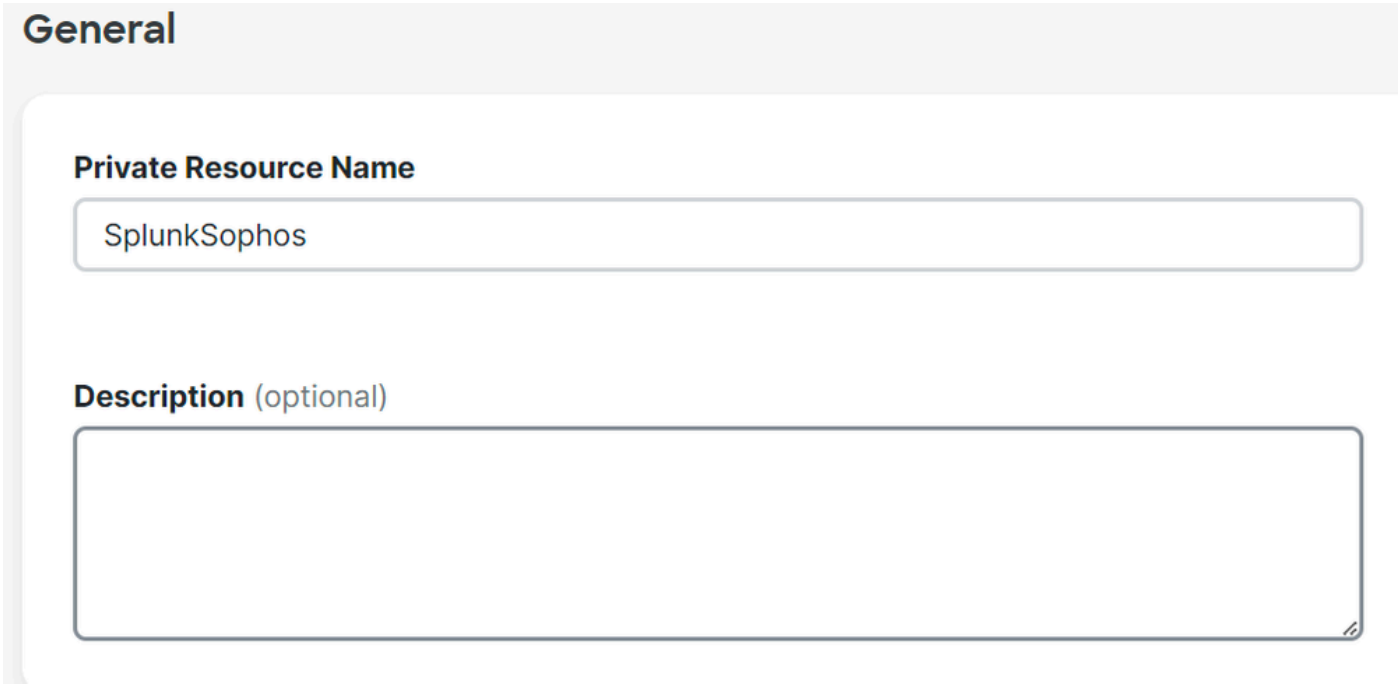
セキュアアクセス – プライベートリソース

- クリック + Add



セキュアアクセス – プライベートリソース2

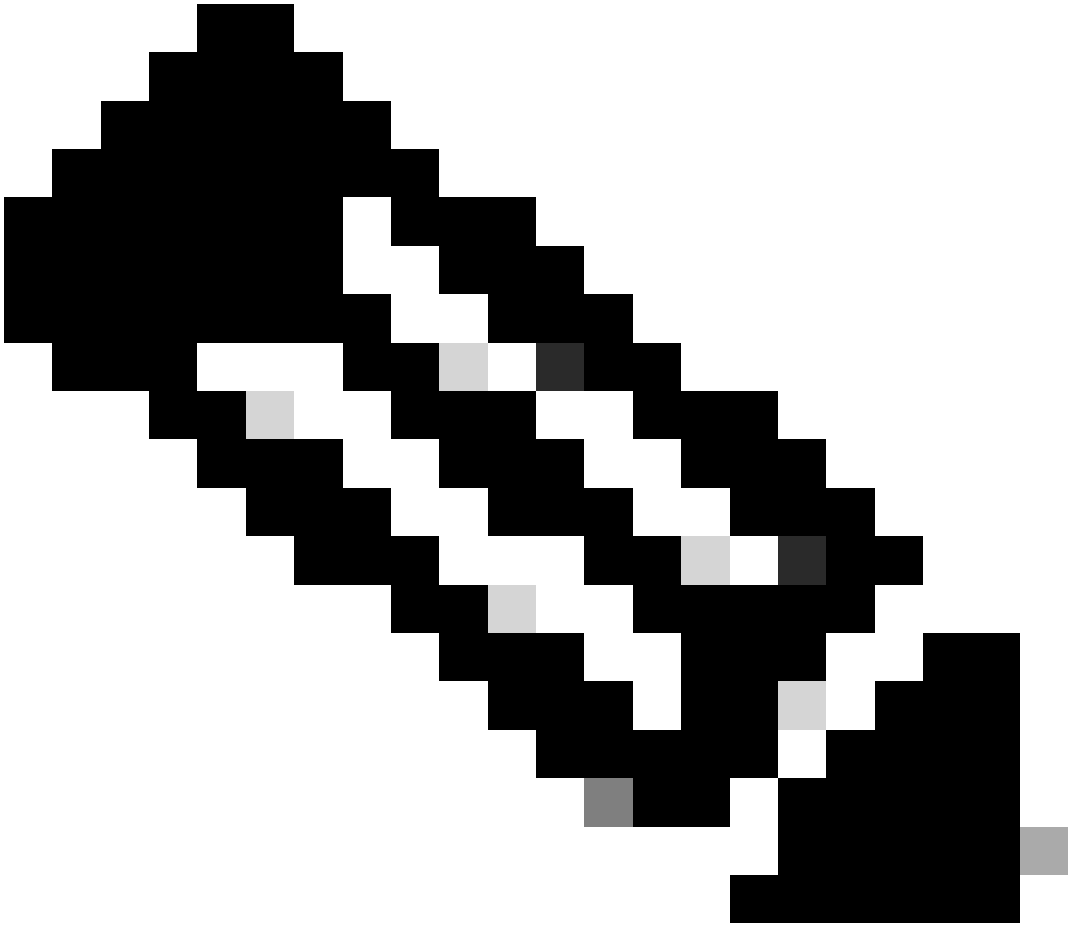
- 「設General 定」の **Private Resource Name**



セキュアアクセス – プライベートリソース – 全般

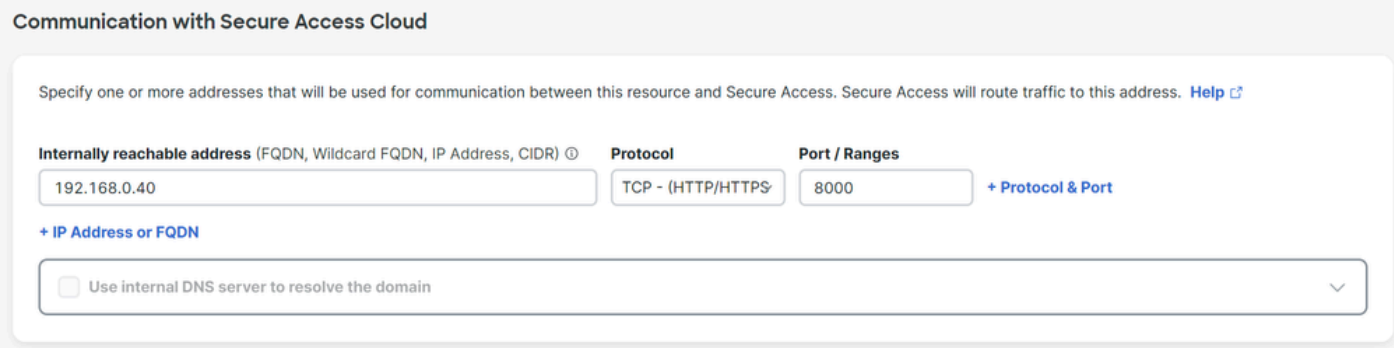
設Communication with Secure Access Cloud 定の下：

- **Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR)**：アクセスするリソースを選択します



注：内部で到達可能なアドレスはステップ **Configure the Tunnel on Secure Access**で割り当てられていることに注意してください。

- **Protocol**：そのリソースにアクセスするために使用するプロトコルを選択します
- Port / Ranges ：アプリにアクセスするために有効にする必要があるポートを選択します

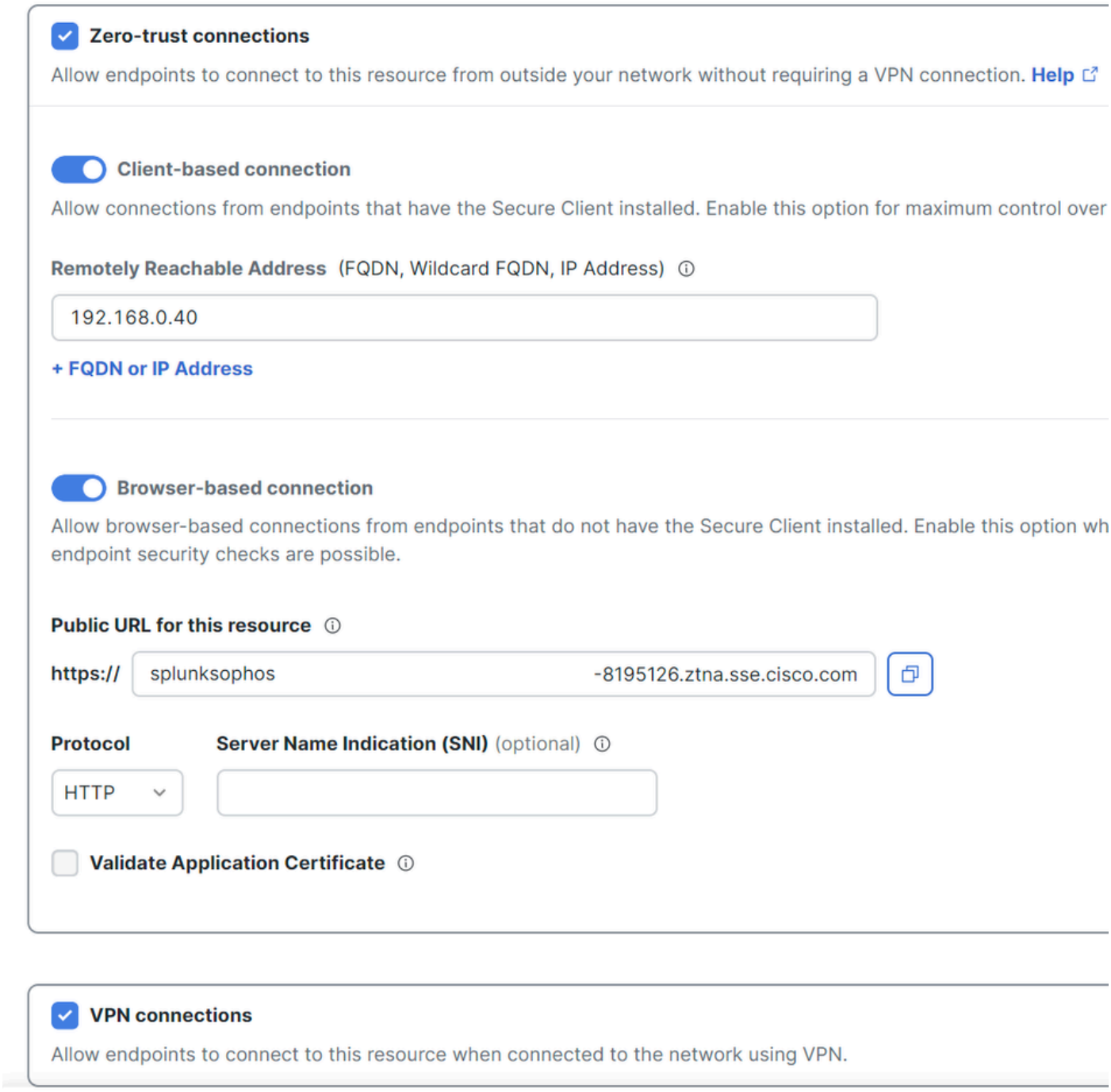


セキュアアクセス – プライベートリソース – セキュアアクセスクラウドを使用した通信

では **Endpoint Connection Methods**、セキュアアクセスを介してプライベートリソースにアクセスするために可能なすべての方法を設定し、環境で使用する方法を選択します。

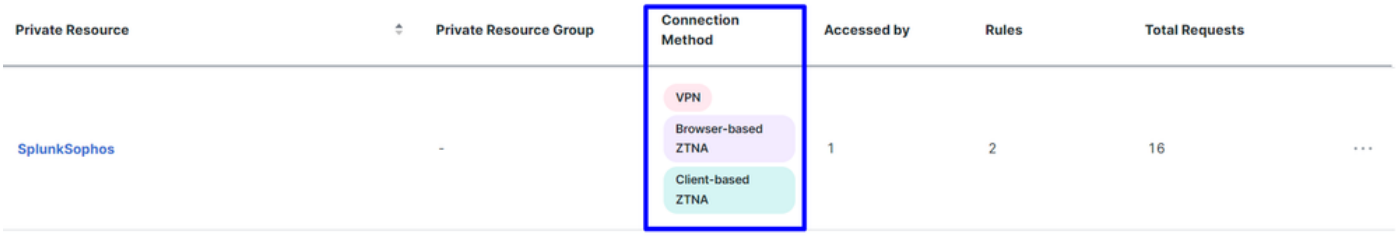
- **Zero-trust connections**:ZTNAアクセスを有効にするには、このチェックボックスをオンにします。
  - **Client-based connection**：ボタンを有効にしてクライアントベースZTNAを許可します。
    - **Remotely Reachable Address**：プライベートアプリのIPを設定します
  - **Browser-based connection**：ボタンを有効にしてブラウザベースのZTNAを許可します。
    - Public URL for this resource：ドメインztna.sse.cisco.comとともに使用する名前を追加します。
      - Protocol：ブラウザ経由でアクセスするプロトコルとしてHTTPまたはHTTPSを選択します。
- **VPN connections**:RA-VPNアクセスを有効にするには、このチェックボックスをオンにします。

- クリック **Save**



セキュアアクセス – プライベートリソース – セキュアアクセスクラウドを使用した通信2

設定が完了すると、次のような結果になります。

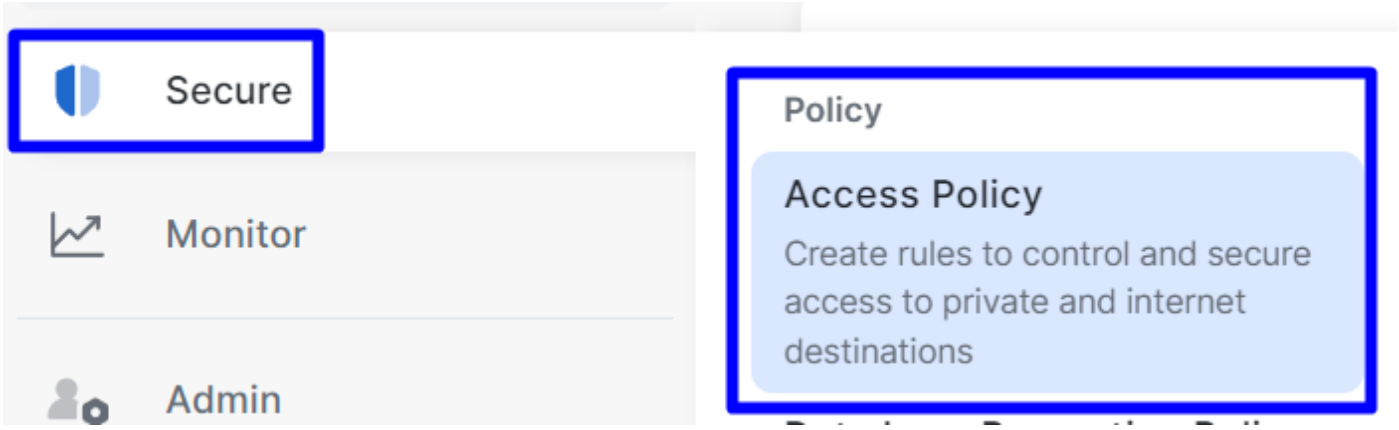


セキュアアクセス – プライベートリソースの設定

ここで、ステップ **Configure the Access Policy**に進むことができます。

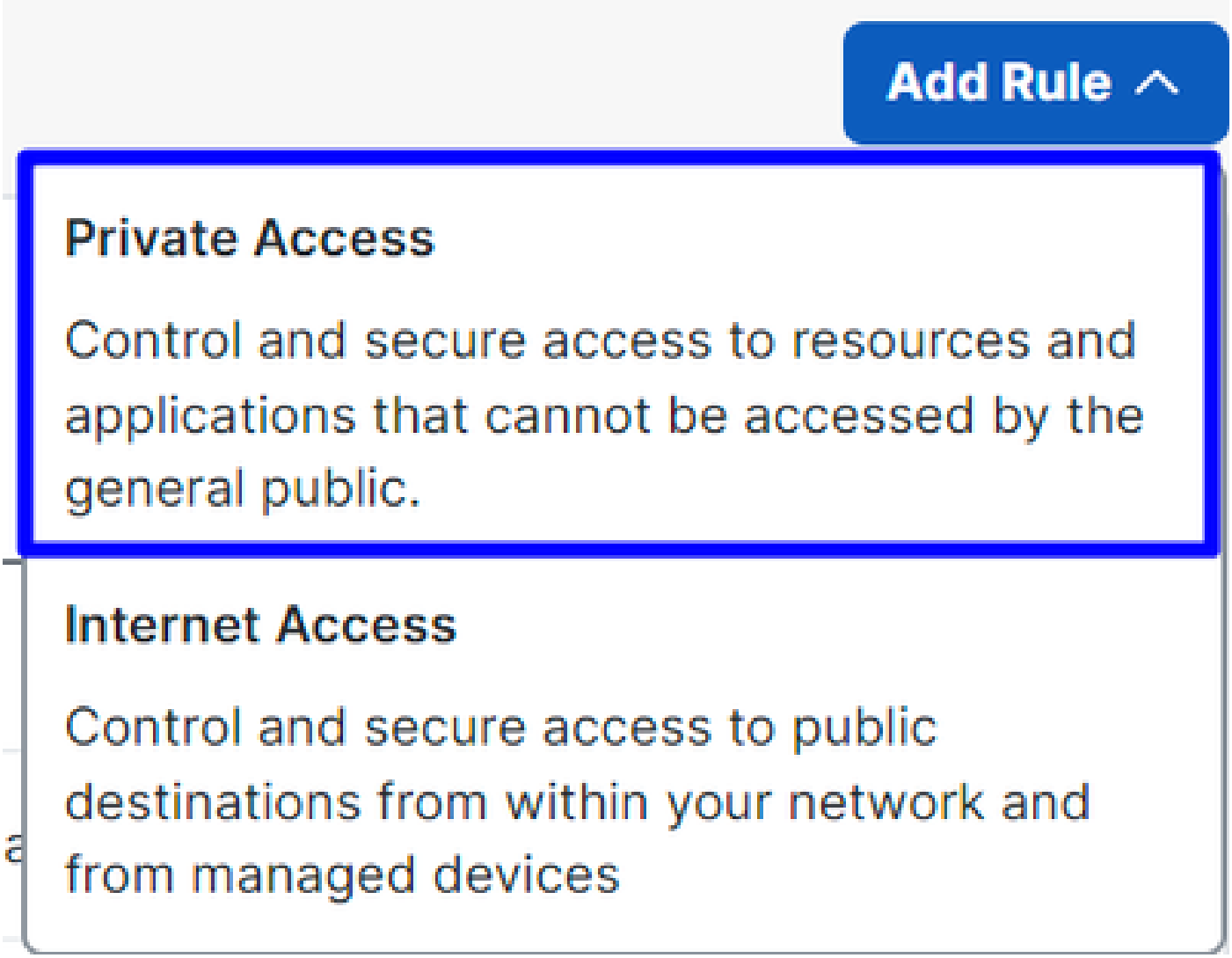
アクセスポリシーの設定

アクセスポリシーを設定するには、Secure > Access Policyに移動します。



セキュアアクセス：アクセスポリシー

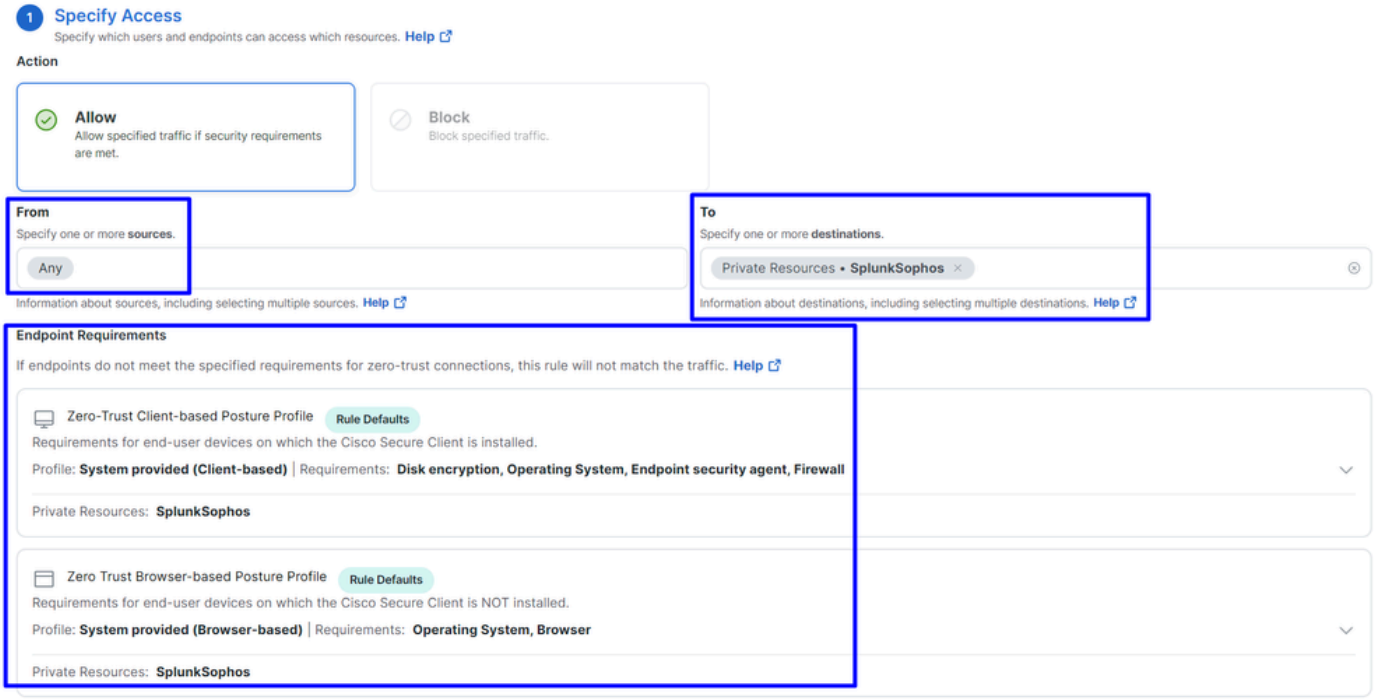
- クリック **Add Rule** > **Private Access**



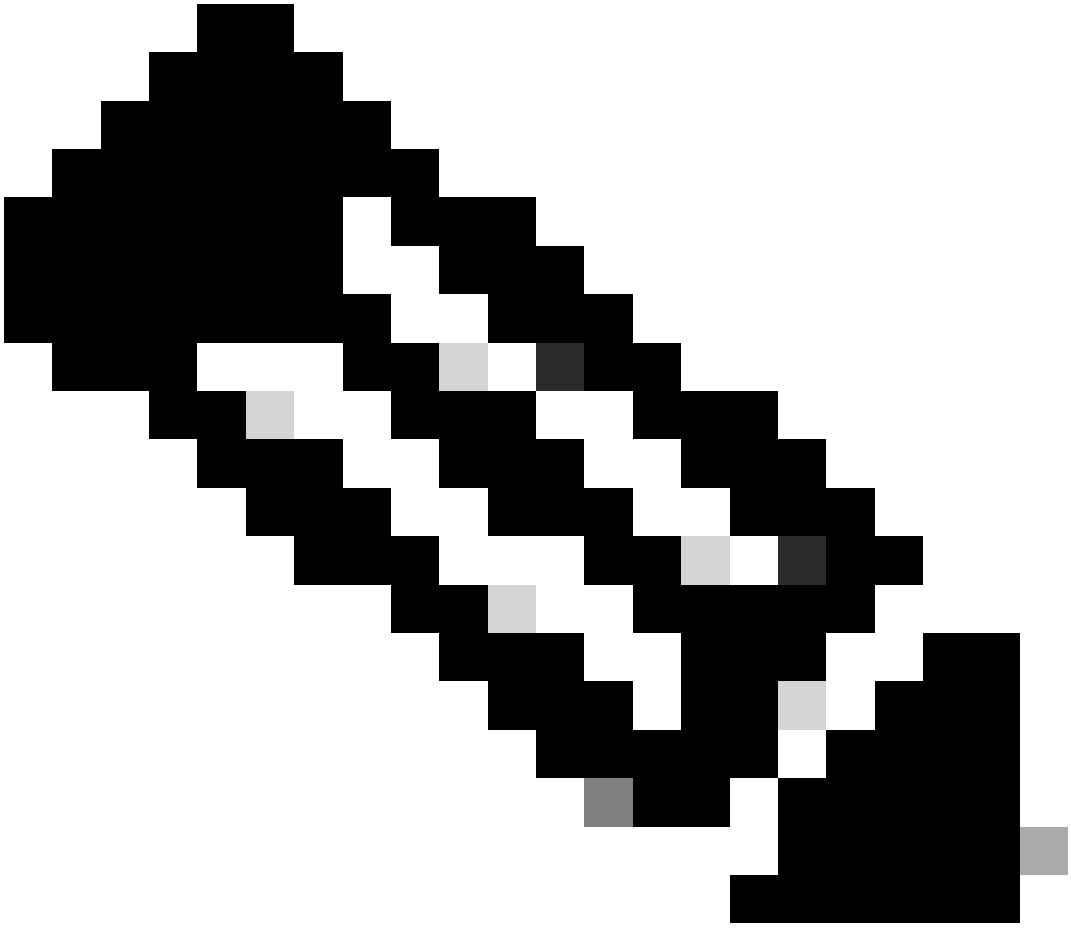
セキュアアクセス – アクセスポリシー – プライベートアクセス

次のオプションを設定して、複数の認証方式によるアクセスを提供します。

- 1. Specify Access
    - Action:プライベート ネットワーク間で
        - **Rule name**：アクセスルールの名前を指定します
        - **From**：アクセス権を付与するユーザ
        - **To**：アクセスを許可したいアプリケーション
        - Endpoint Requirements:（デフォルト）
- クリック **Next**



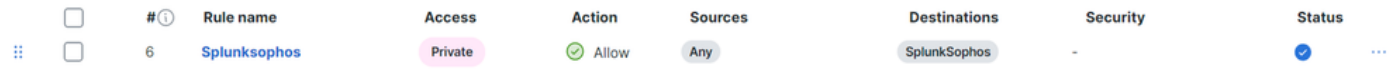
セキュアアクセス – アクセスポリシー – アクセスの指定



注：必要に応じて手順 **2. Configure Security** を実行しますが、この場合、 **Intrusion Prevention (IPS)**も **Tenant Control Profile**も有効にしていません。

Save

- をクリックすると、次の情報が表示されます。



セキュアアクセス：アクセスポリシーの設定

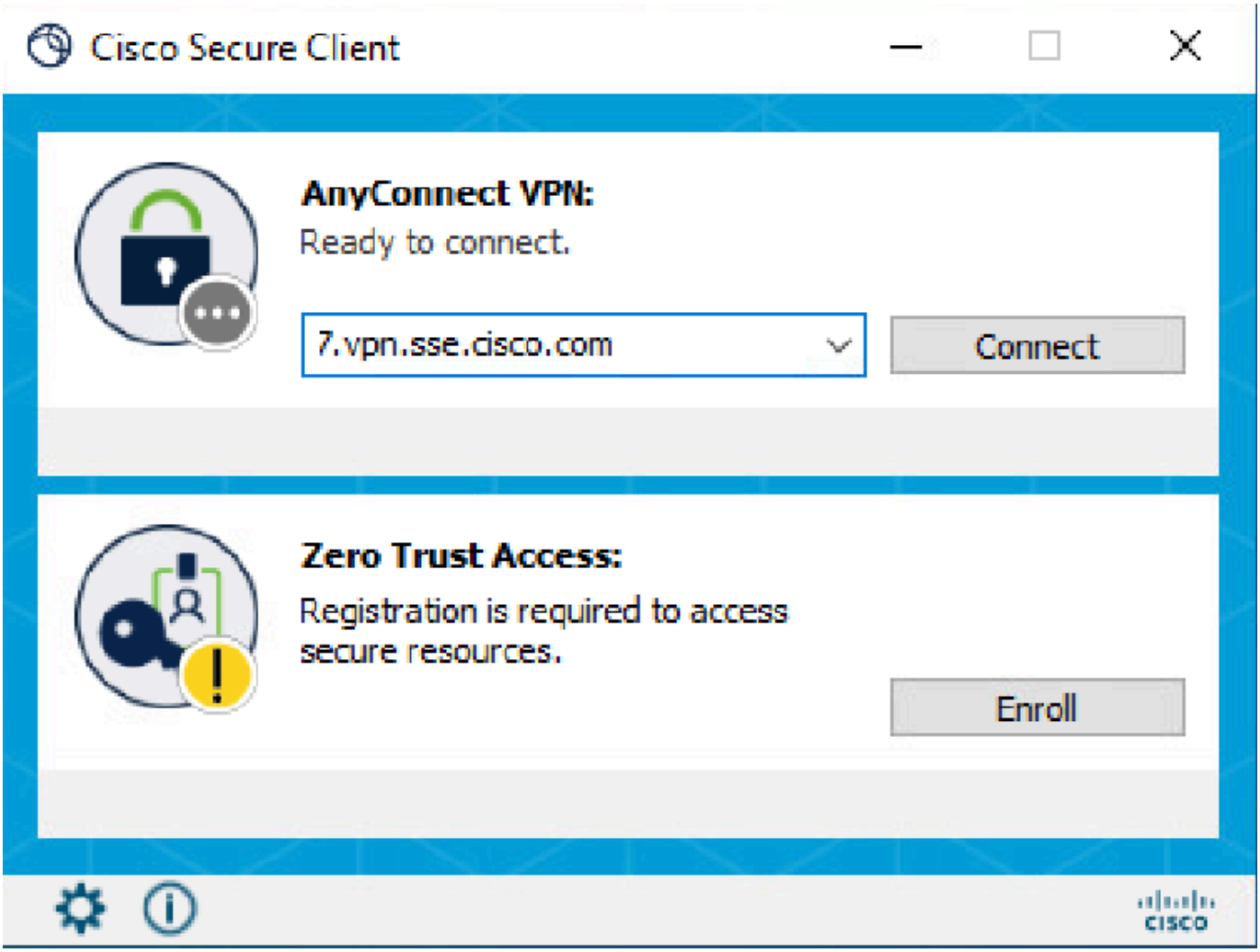
その後、Verifyステップに進むことができます。

確認

アクセスを確認するには、ソフトウェアダウンロード – Cisco Secure Clientからダウンロードできる Cisco Secure Clientのエージェントをインストールしている必要があります。

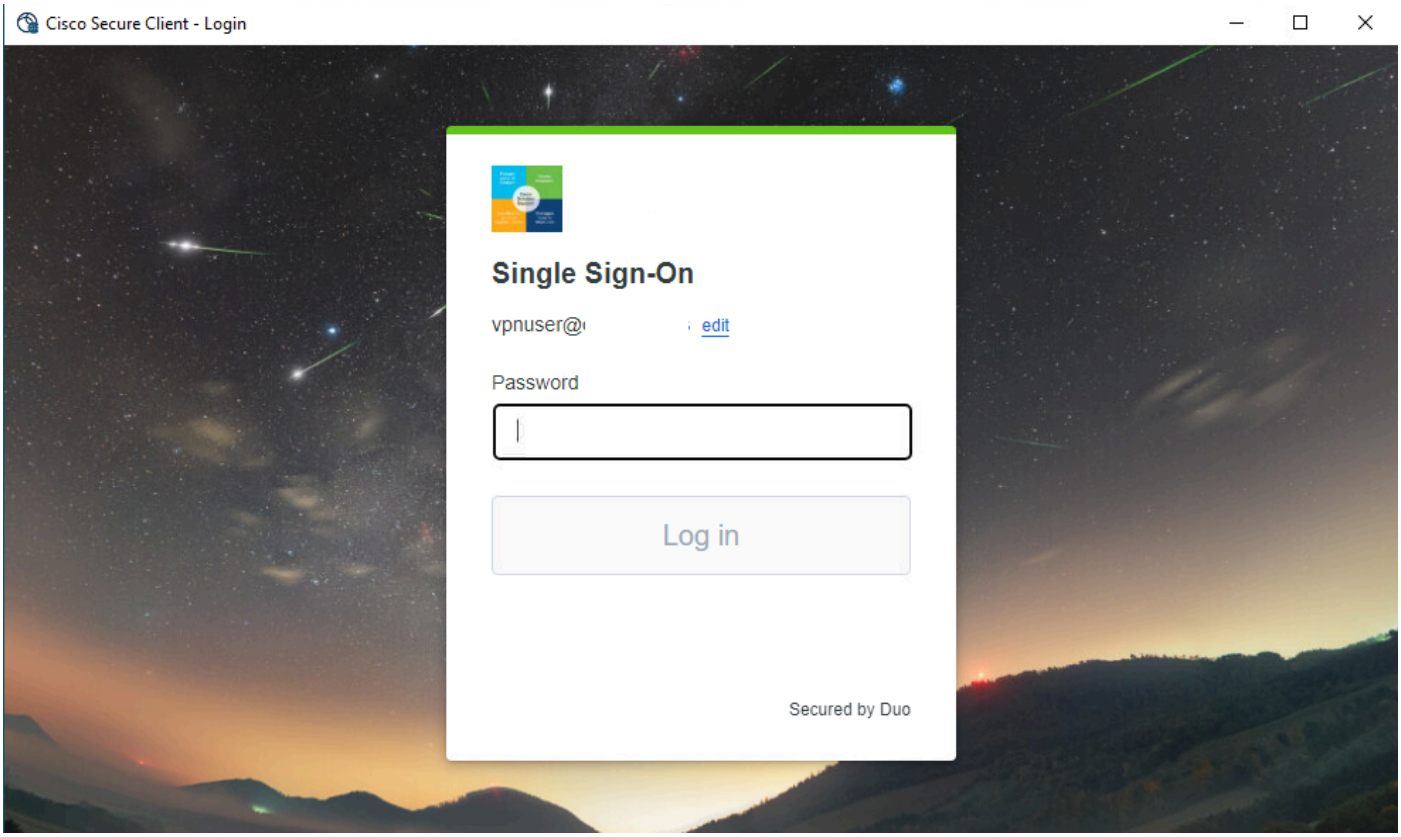
RA-VPN（オプション）

Cisco Secure Client Agent-VPNからログインします。



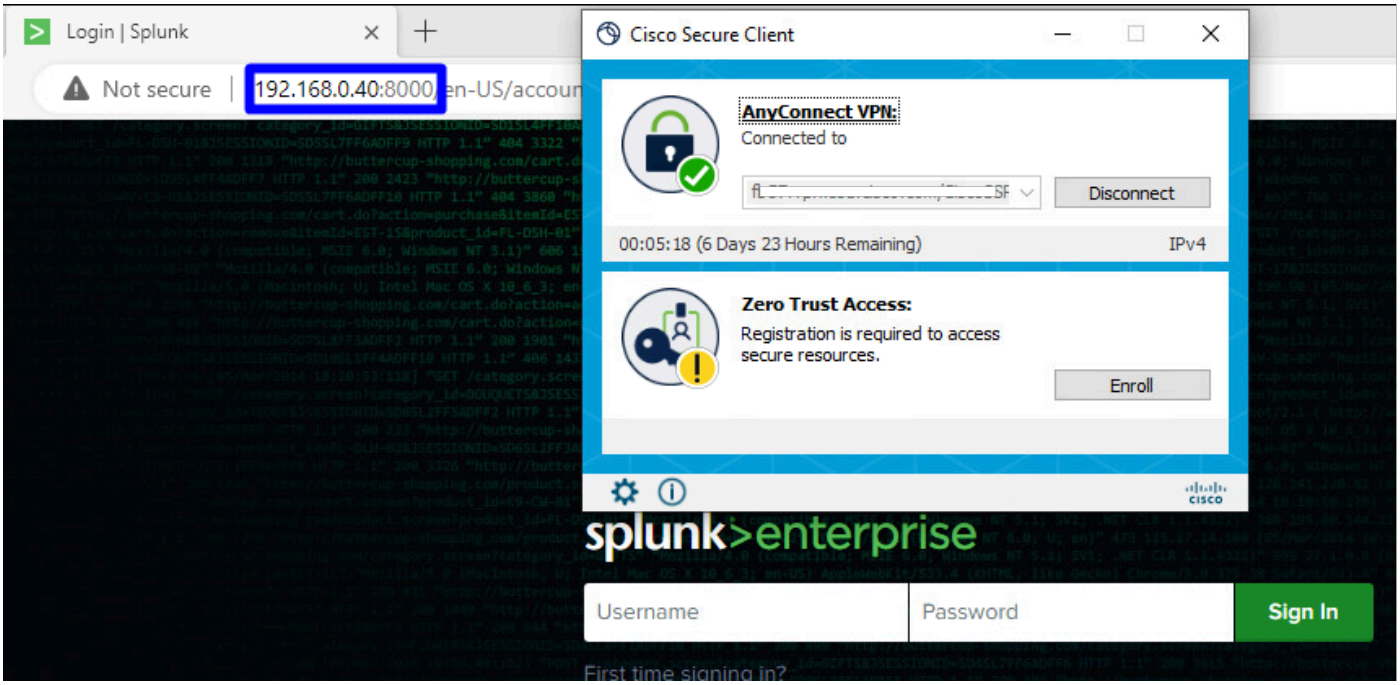
セキュアクライアント – *VPN*

- SSOプロバイダーを介した認証



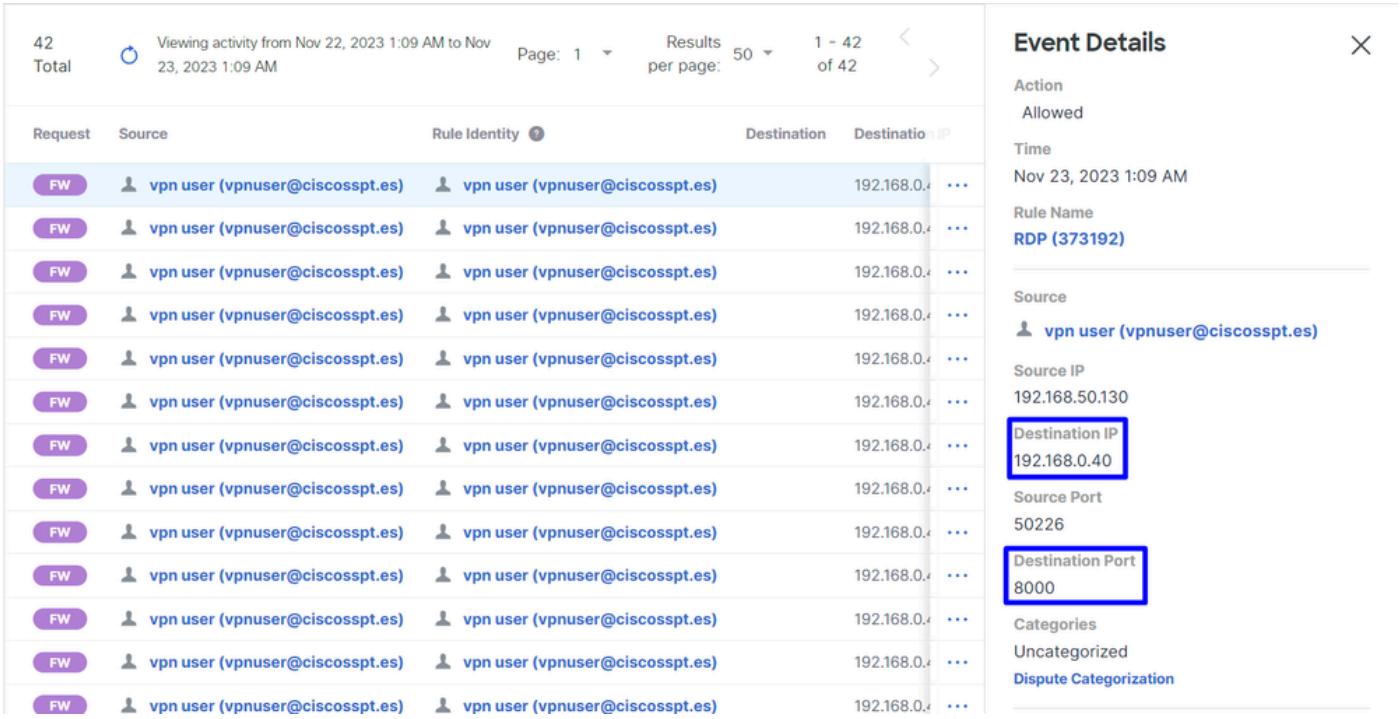
セキュアアクセス – *VPN - SSO*

- 認証を受けた後、リソースにアクセスします。



セキュアアクセス – *VPN* – 認証

次のとおりに移動します。Monitor > Activity Search

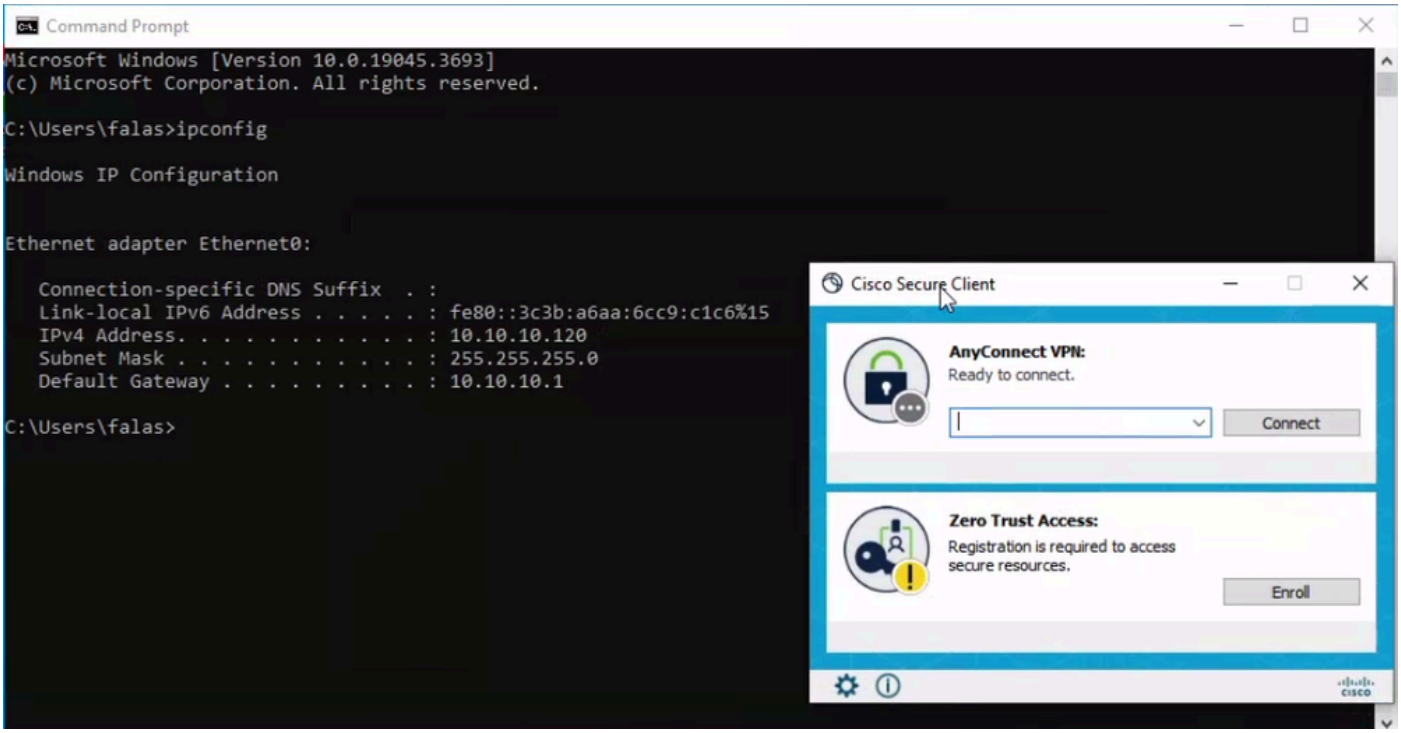


セキュアアクセス – アクティビティ検索 – *RA-VPN*

ユーザがRA-VPNを介して認証を受けたことを確認できます。

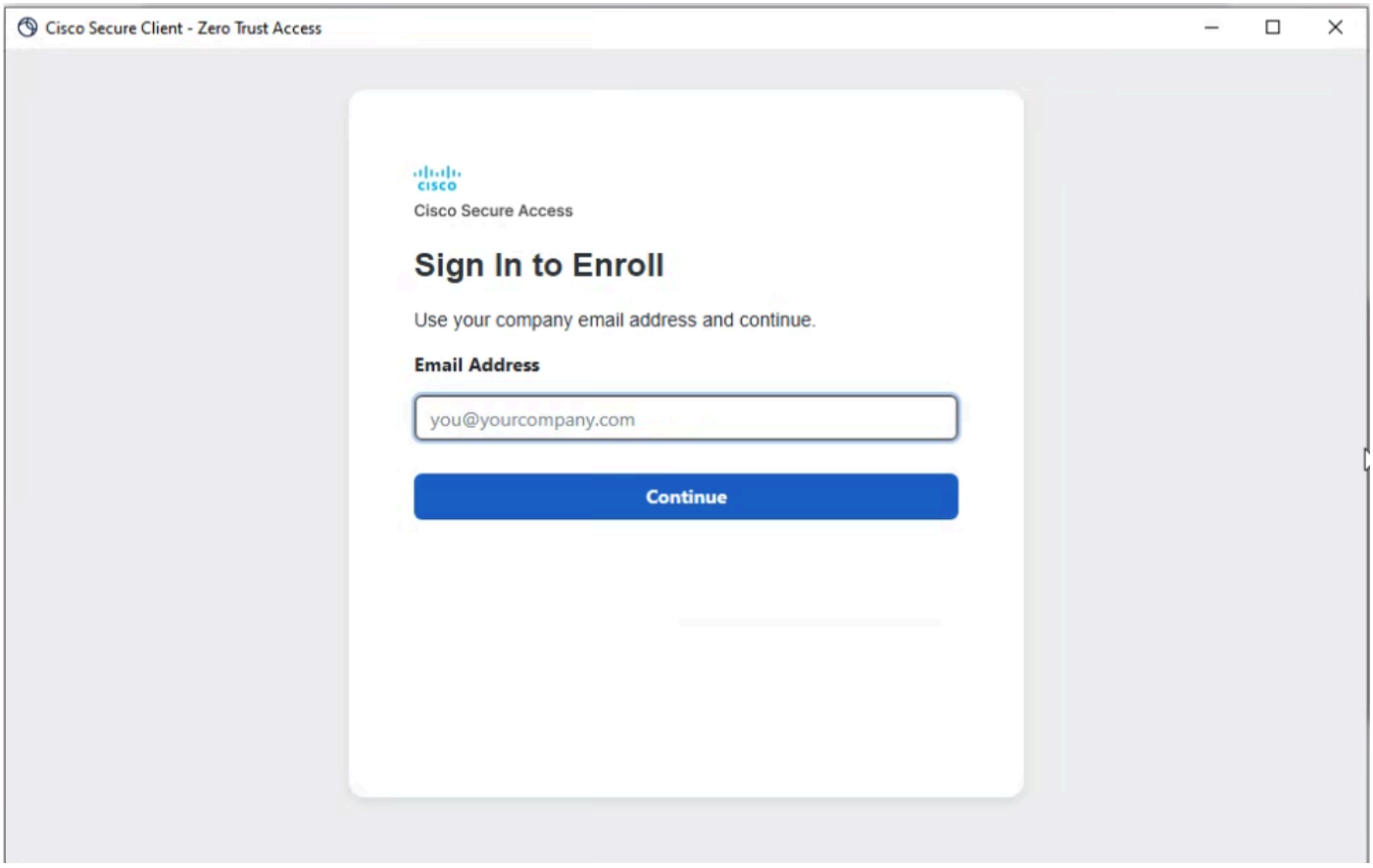
クライアントベースのZTNA

Cisco Secure Client Agent(ZTNA)からログインします。



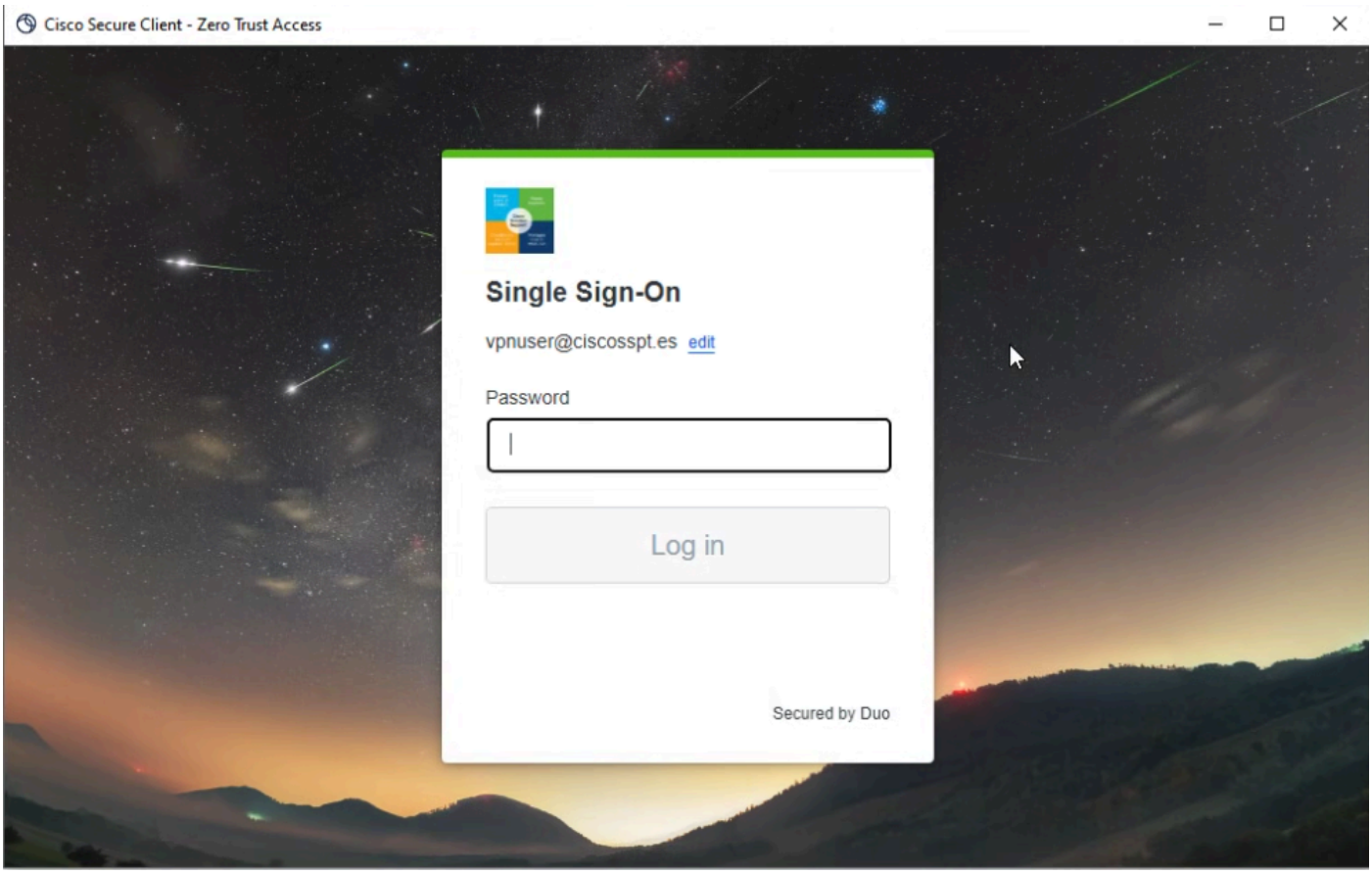
セキュアクライアント – *ZTNA*

- ユーザ名で登録します。



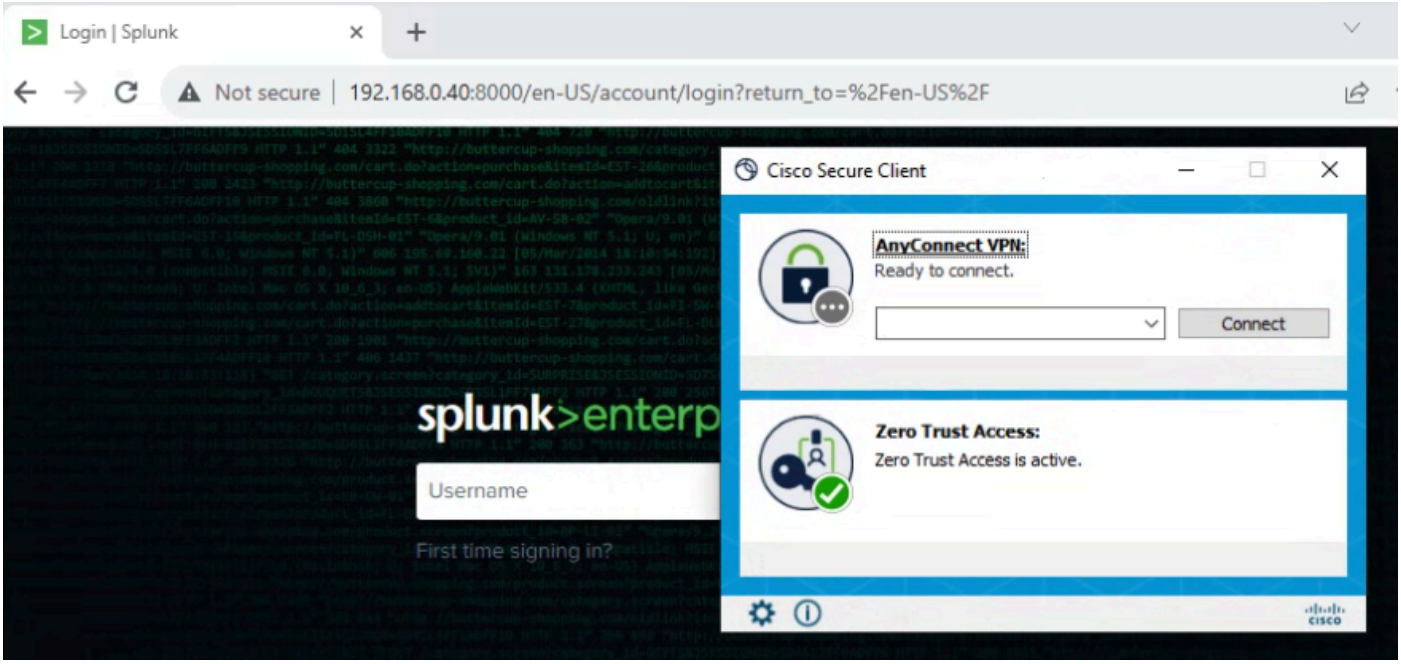
セキュアクライアント – *ZTNA* – 登録

- SSOプロバイダーでの認証



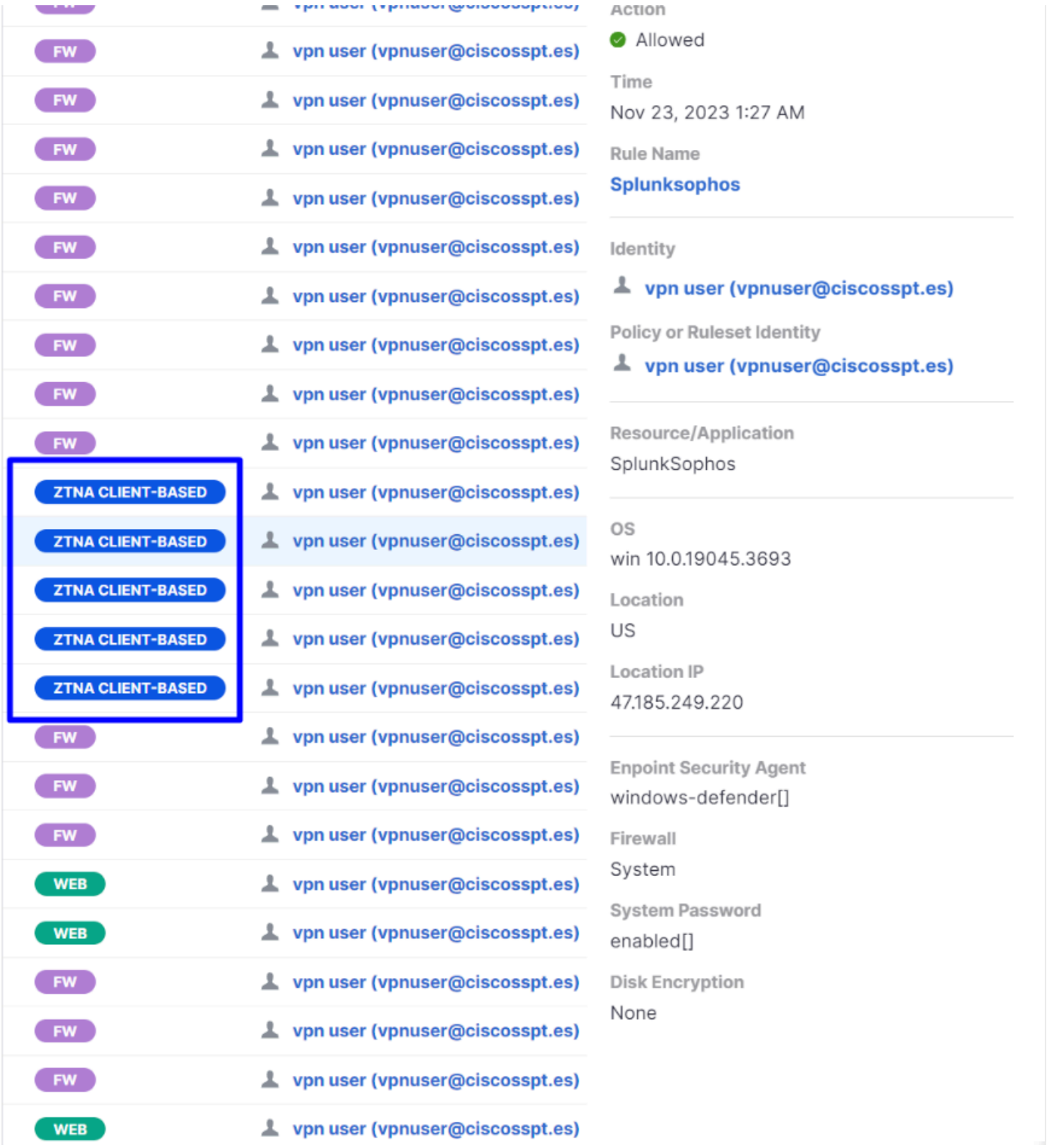
セキュアクライアント – *ZTNA - SSO*ログイン

- 認証を受けた後、リソースにアクセスします。



セキュアアクセス – *ZTNA* – ログ

次のとおりに移動します。Monitor > Activity Search

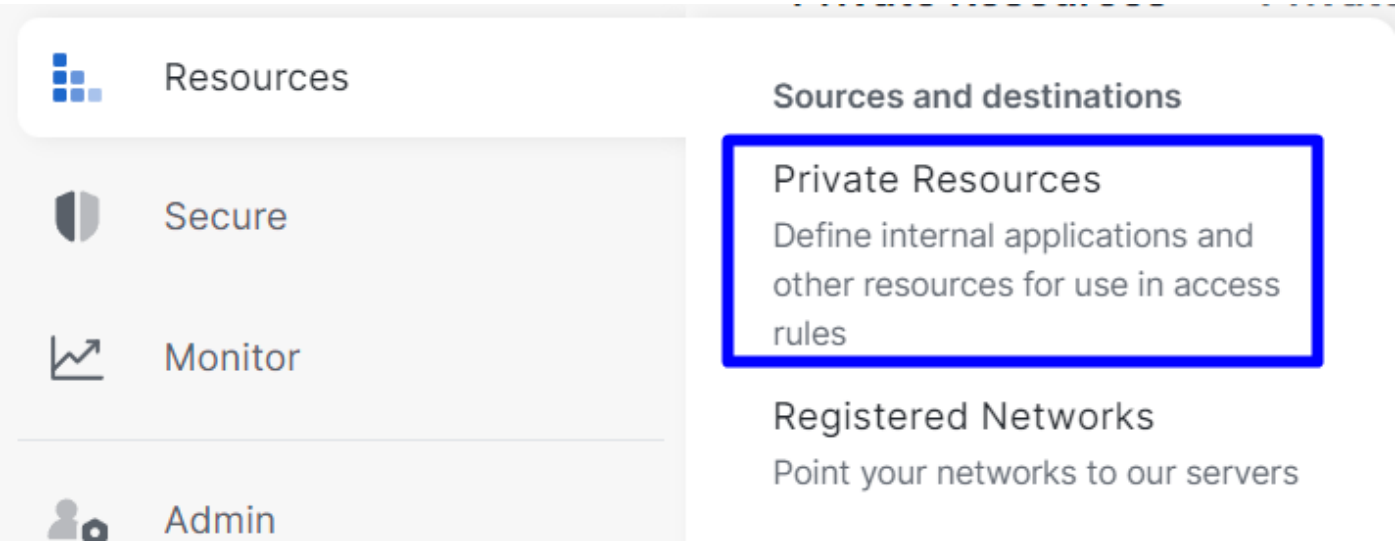


セキュアアクセス – アクティビティ検索 – *ZTNA*クライアントベース

ユーザがクライアントベースのZTNAを介して認証を許可されたことを確認できます。

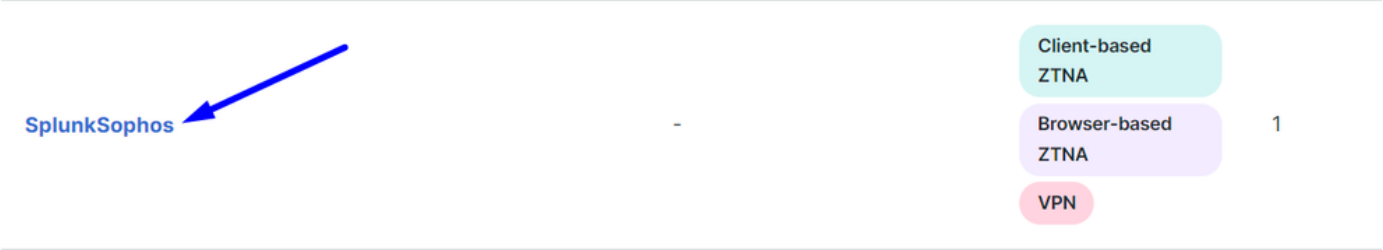
ブラウザベースのZTNA

URLを取得するには、**Resources** > **Private Resources**に移動する必要があります。



セキュアアクセス – プライベートリソース

- ポリシーをクリックします。



セキュアアクセス – プライベートリソース – *SplunkSophos*

- 下にスクロール

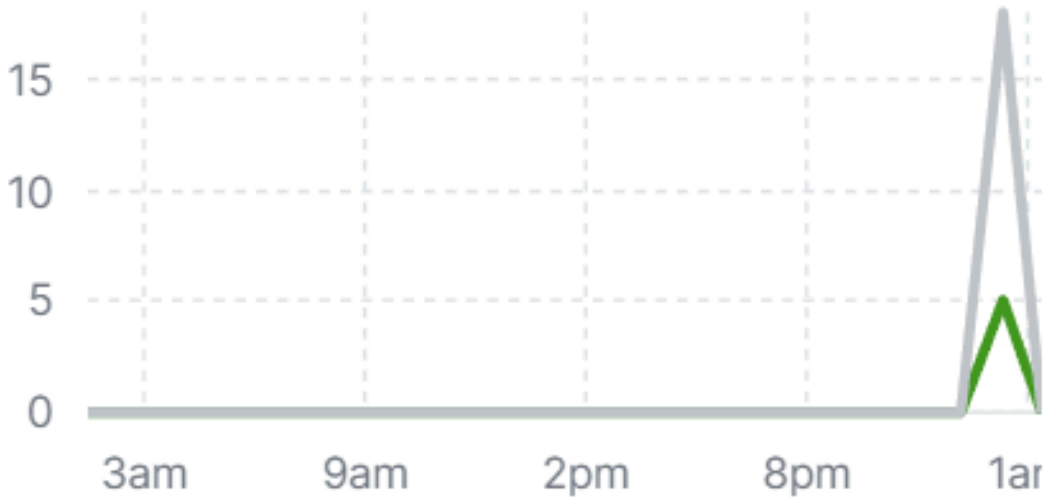
SplunkSophos

Client-based ZTNA Browser-based ZTNA

VPN

Total Requests

23 44% from previous 24 hours



TOTAL REQUESTS BY STATUS

Status	
Success	5
Blocked	18

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。