ダイナミックルーティングを使用したプライベートアクセスに対するセキュアファイアウォール脅威対策による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、ダイナミックルーティングを使用したセキュアプライベートアクセスのために、IPsec経由でFTDを使用した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

要 件

- Cisco Secure Accessの知識
- Cisco Secure Accessダッシュボード/テナント
- Secure Firewall Threat DefenseおよびFirewall Management Centerの知識
- IPSecに関する知識
- ダイナミックルーティングの知識

使用するコンポーネント

- 7.7.10コードを実行するセキュアファイアウォール
- クラウド提供のファイアウォール管理センター。設定は一般的な仮想FMCにも適用されます
- Cisco Secure Access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たものです。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。

バックグラウンド情報

Secure Accessのネットワークトンネルは、主にSecure Internet AccessとSecure Private Accessの2つの目的に使用できます。

セキュアなプライベートアクセスでは、ゼロトラストアクセス(ZTA)やVPN as a Service(VPNaaS)を活用して、ユーザを内部アプリケーションやデータセンターなどのプライベートリソースに接続できます。IPSecトンネルは、ユーザとプライベートリソース間のネットワークトラフィックを安全に暗号化することで、このアーキテクチャで重要な役割を果たします。これにより、機密データが信頼できないネットワークを通過する際も、機密データが保護された状態で維持されます。IPSecトンネルをZTAまたはVPNaaSと統合することで、組織は堅牢なセキュリティ制御と可視性を維持しながら、内部リソースへのシームレスで安全なアクセスを提供できます。

このドキュメントでは、セキュアプライベートアクセス用にIPsec経由でセキュアファイアウォール脅威対策(FTD)を使用してセキュアアクセスを設定する方法について説明します。
また、このガイドでは、BGPを使用したダイナミックルーティングの設定手順についても説明します。

このドキュメントでは、セキュアプライベートアクセスのためのIPSecトンネルの設定について説明しますが、プライベートアプリケーションにアクセスするためのZero Trust Access(ZTA)またはVPN as a Service(VPNaaS)のセットアップについては、このガイドでは取り上げていません。

設定

セキュアアクセスの設定

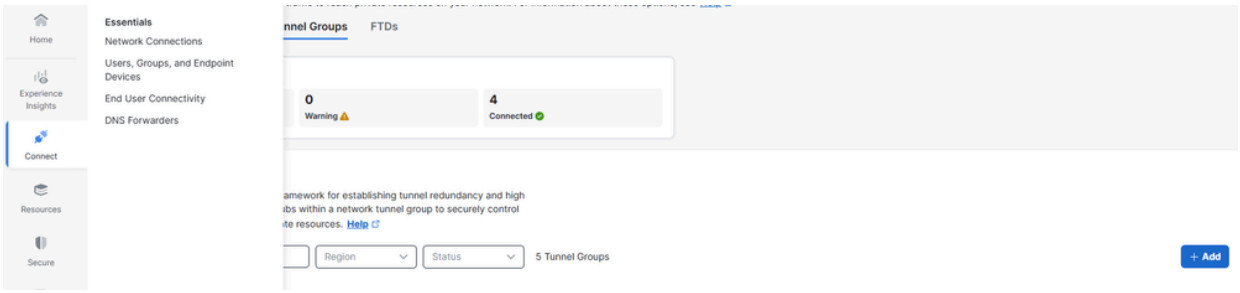
ネットワークトンネルグループの設定

1. Secure Accessの管理パネルに移動します。

CSAダッシュボード

2. ネットワークトンネルグループを追加します。

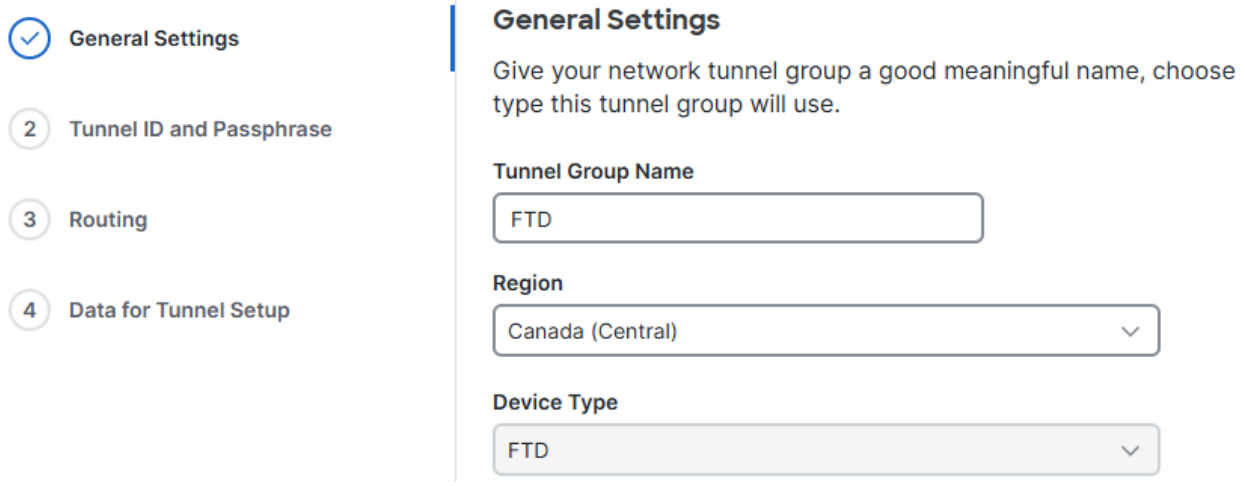
- Connect > Network Connectionsの順にクリックします。
  - Network Tunnel Groupsの下で、Addをクリックします。



NTGの確認

3. 一般設定の設定。

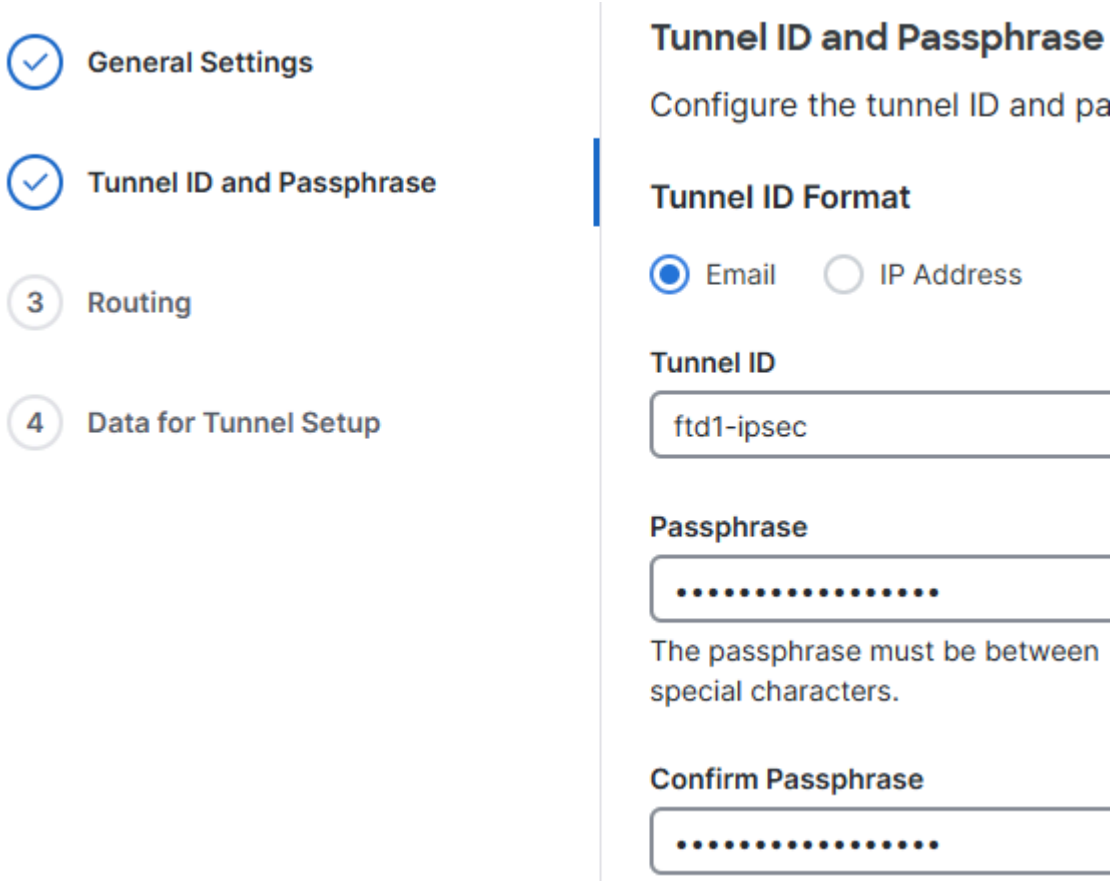
- トンネルグループ名、リージョン、およびデバイスタイプの設定
  - [Next] をクリックします。



一般設定

4. トンネル IDとパスフレーズを設定します。 このIDはFTDの設定に必要なため、重要です

- Nextをクリックします。



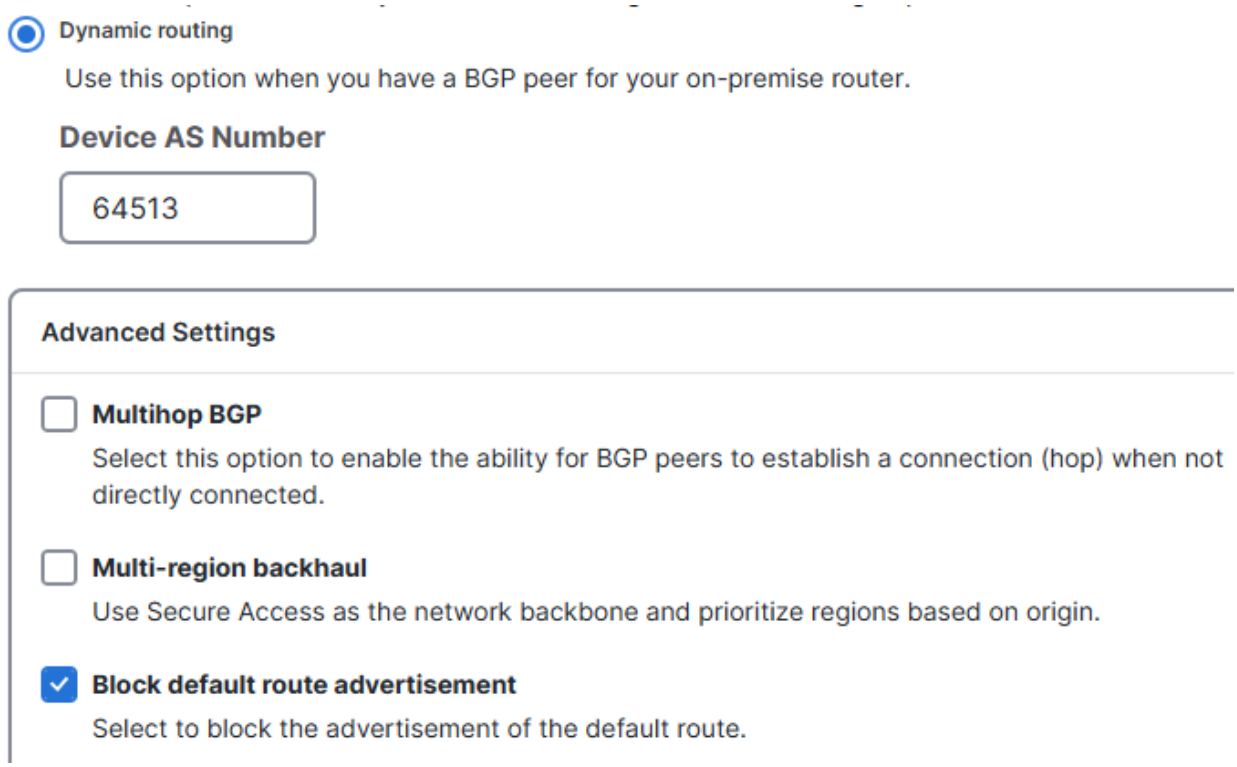
IDおよびPSK

5. ダイナミックルーティングを設定します。

セキュアアクセスルーティング

ダイナミックルーティング(BGP)

- セキュアアクセスでBGPピアを設定するときに、FTDのBGP自律システム(AS)番号を指定します。
- Routing> Dynamic routingの順にクリックします。
  - Device AS Numberをクリックして、FTDのBGP ASNを追加します。
  - Block default route advertisementチェックボックスにチェックマークを付けます
  - [Save] をクリックします。



CSA BGPの設定

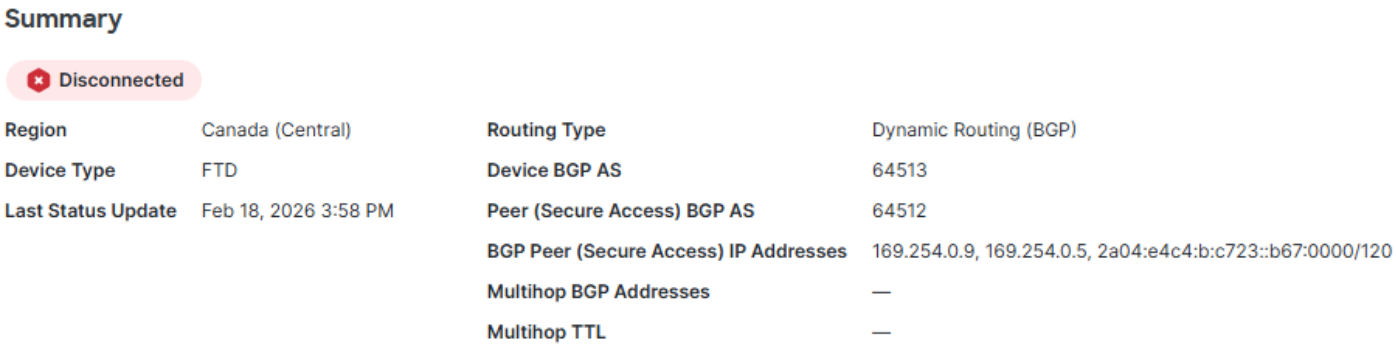
注：セキュアアクセスによってアドバタイズされたルートは、元のASパスを付加して、プライマリトンネルに1を、セカンダリトンネルに2を含めます。マルチリージョンバックホールシナリオがサポートされています。詳細については、をクリックしてください。

ネットワークトンネルグループ設定の保存

FTDの設定に必要なトンネルセットアップデータをダウンロードして保存します。

- Download CSVをクリックします。
- Doneをクリックします。

NTGデータ



BGPの設定

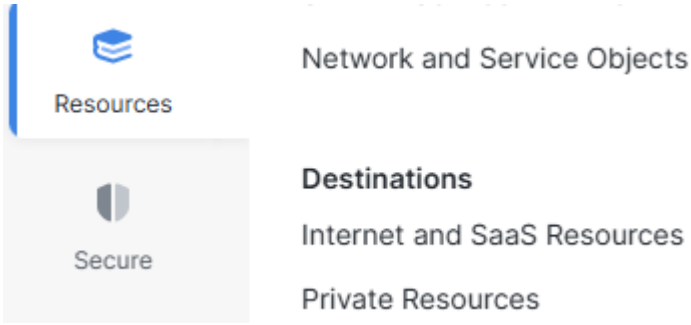
注:Network Tunnel Groupをクリックすると、BGP AS番号とBGPピアのIPアドレスが表示されます。これらは後でFTD側に設定されます。

プライベートリソースの作成

プライベートリソースは、データセンターまたはプライベートクラウド環境でホストされる内部アプリケーション、ネットワーク、またはサブネットです。これらのリソースは一般に公開されておらず、組織のインフラストラクチャの背後で保護されています。

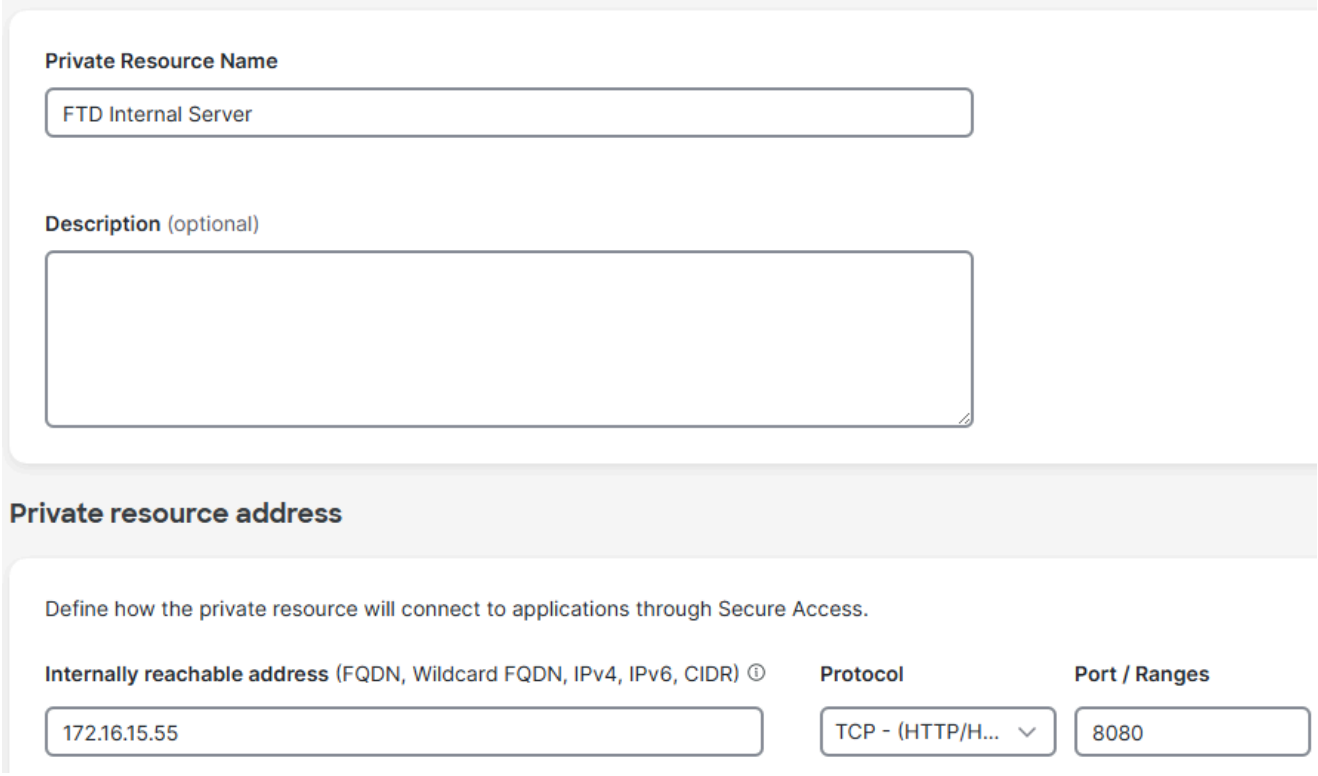
Secure Accessでプライベートリソースとして定義することにより、ゼロトラストアクセス(ZTA)やVPN as a Service(VPNaaS)などのソリューションを通じてアクセス制御を実現できます。 これにより、ユーザは、リソースをインターネットに直接公開することなく、ID、デバイスポスチャ、およびアクセスポリシーに基づいて内部システムに安全に接続できます。

Resources > **Private Resources**の順に選択し、**Add**をクリックします。



PR

- プライベートリソース名、内部到達可能アドレス、プロトコル、ポート/範囲を指定します。ポートとプロトコルを指定し、必要に応じてプライベートリソースを追加する
- 必要に応じて、接続方法（ゼロトラスト接続やVPN接続など）を選択します
- [Save] をクリックします。



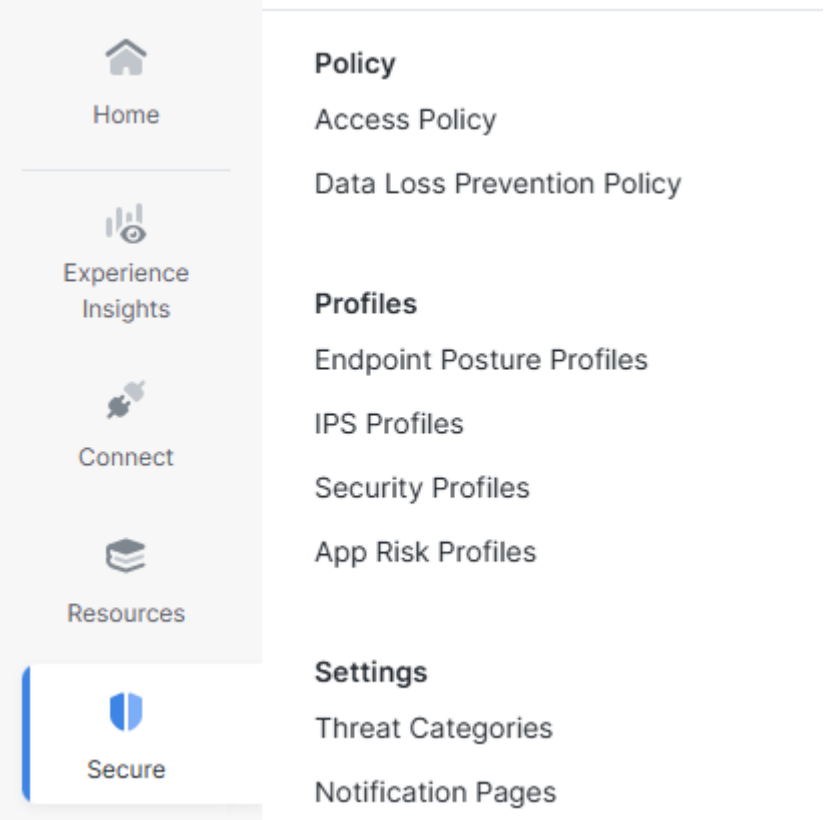
プライベートリソース

アクセスポリシールールの作成

プライベートアクセスルールは、一般にアクセスできない内部リソースおよびアプリケーションにユーザが安全に接続する方法を定義します。

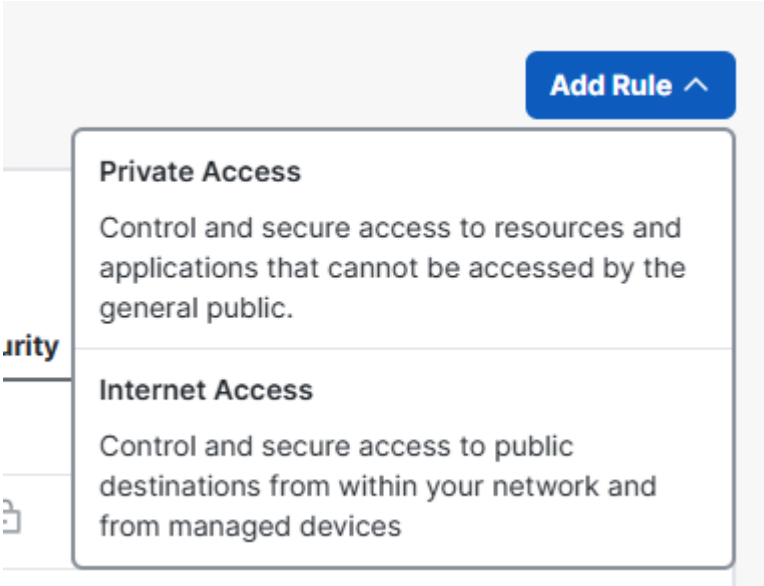
これらのルールは、ユーザID、グループメンバーシップ、デバイスのポスチャ、場所、その他のポリシー条件などの要因に基づいて、特定のプライベートリソースに誰がアクセスできるかを制御することで、セキュリティを強化します。これにより、機密性の高い内部システムを一般のパブリックアクセスから保護しながら、ZTAまたはVPNaaSを介して許可されたユーザが安全に利用できます。

移動先： セキュア>アクセスポリシー



ACP

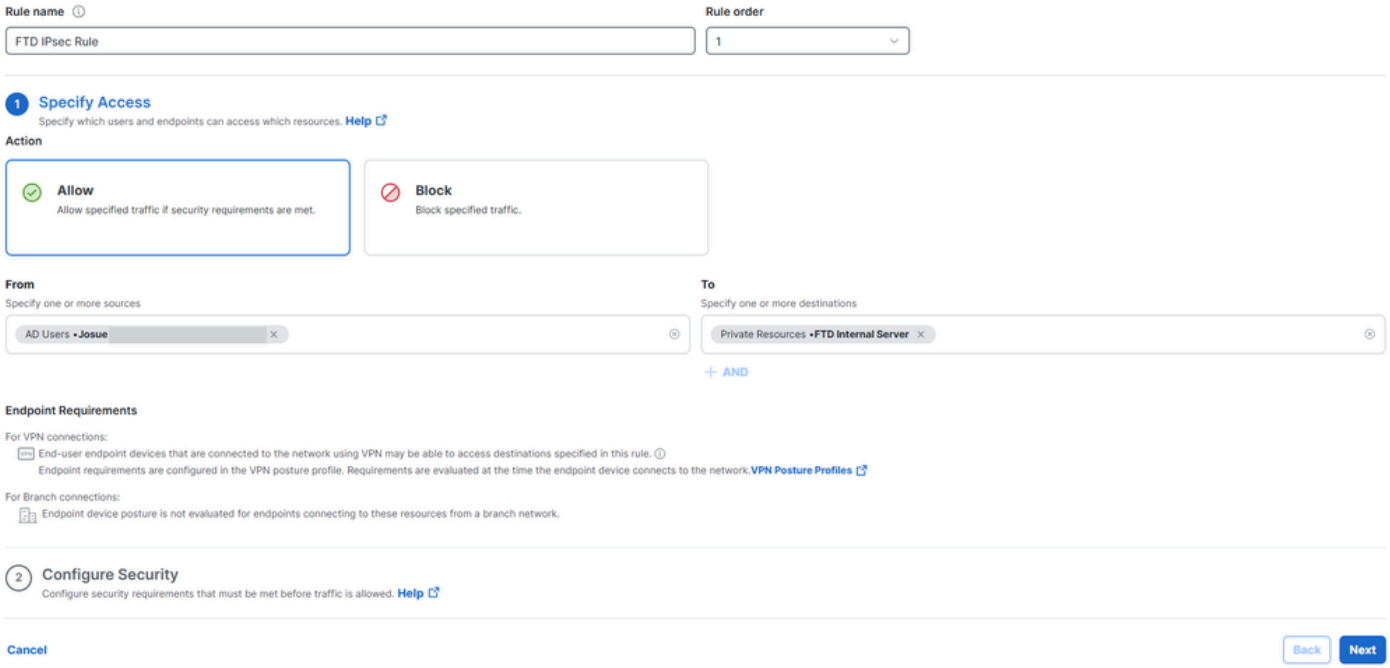
- Add Ruleをクリックします。
  - Private Accessをクリックします。



ACPの追加

- Rule Nameをクリックして、名前を指定します
- Actionをクリックし、Allowto permit this trafficを選択します。
- onFromfromをクリックして、権限を付与されるユーザを指定します
- Toをクリックし、ユーザがこのルールに基づいて持つアクセスを指定します

- Nextをクリックし、次のページでSaveをクリックします。



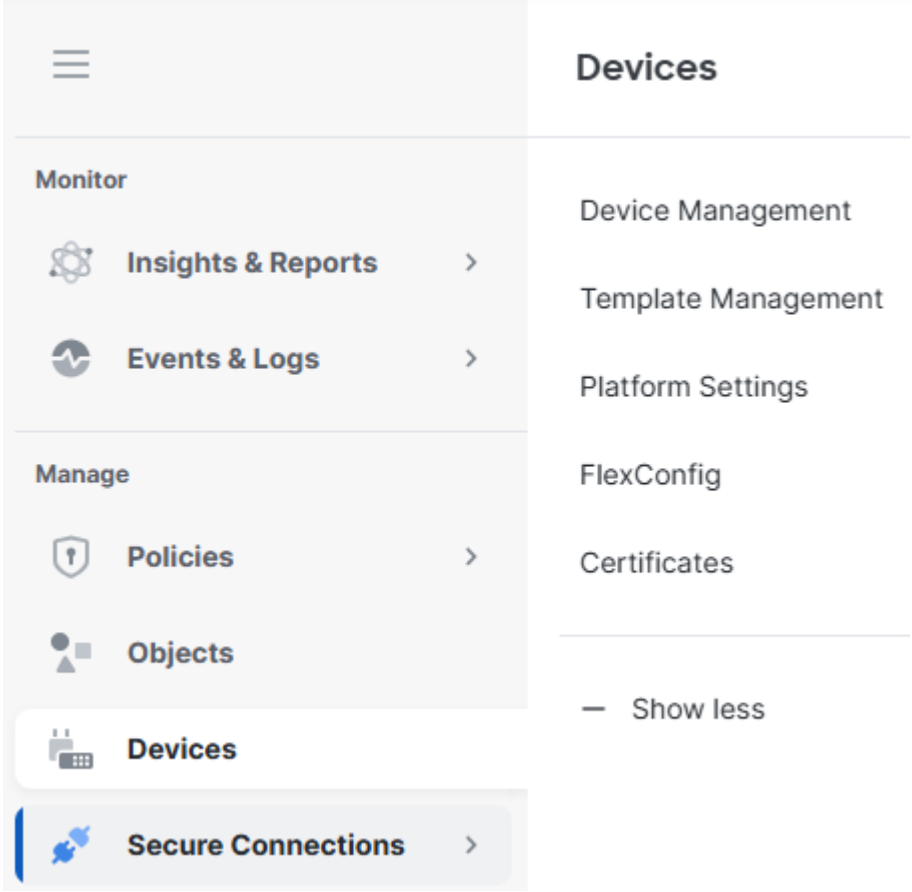
ACPの設定

セキュアファイアウォール脅威対策(FTD)の設定

仮想トンネルインターフェイスの設定

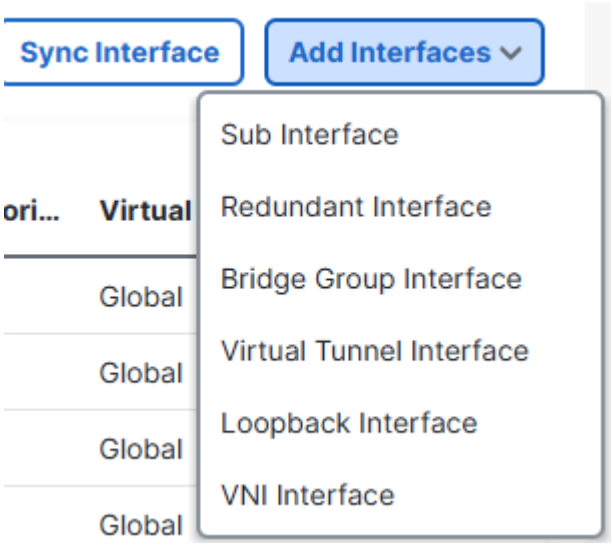
FTDの仮想トンネルインターフェイス(VTI)は、ルートベースのIPsec VPNトンネルの設定に使用される論理レイヤ3インターフェイスです。

1. Devices> Device Managementの順に移動します。



FTDデバイス

- FTDデバイスのInterfacesをクリックします。
  - Add Interfacesをクリックします。
  - Virtual Tunnel Interfaceをクリックします。
  - 2つの仮想トンネルインターフェイスの作成（1つはプライマリセキュアアクセスハブ用、もう1つはセカンダリセキュアアクセスハブ用）

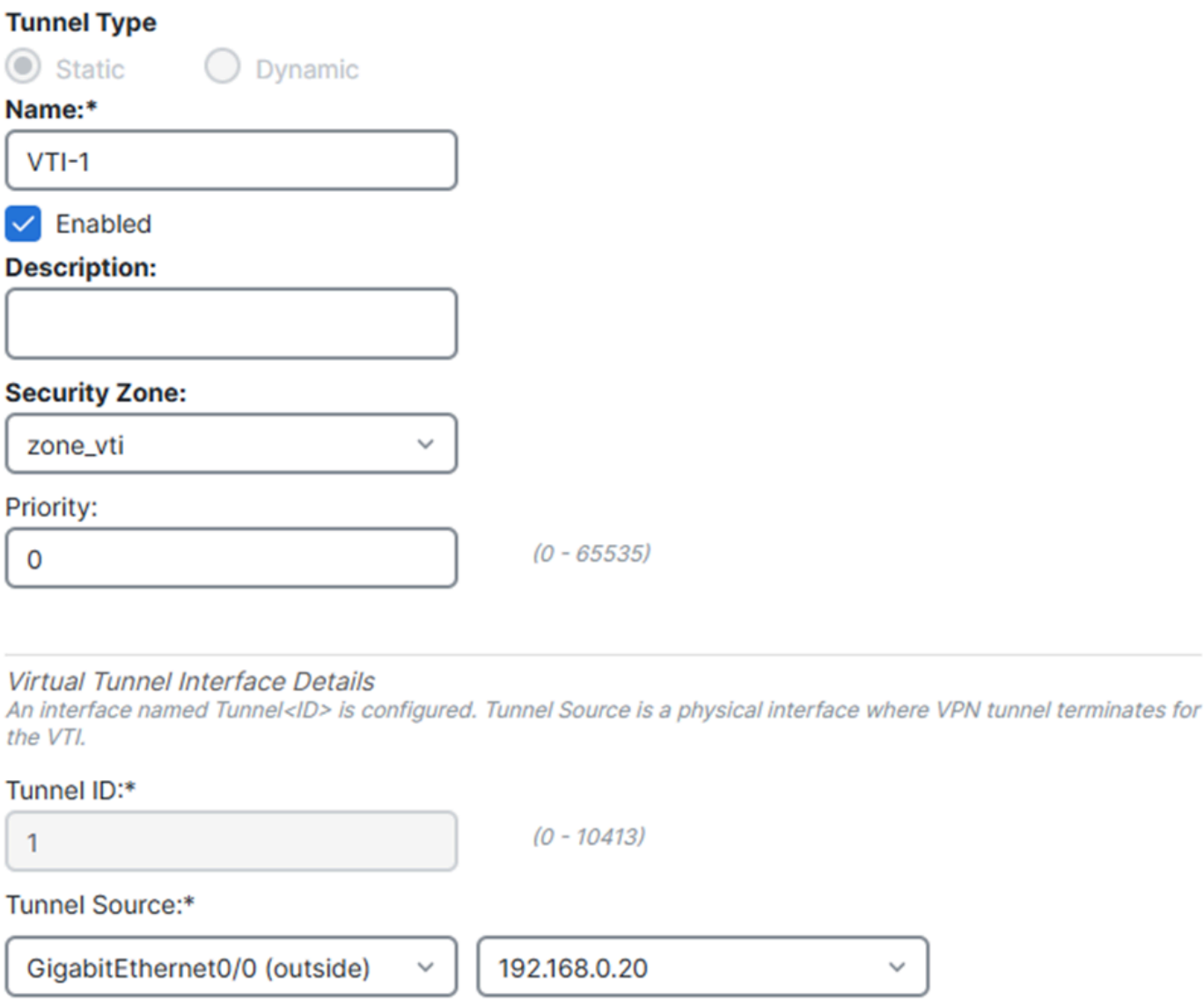


VTIの追加

仮想トンネルインターフェイス1:

- 名前を入力し、Enableをクリックします。
- セキュリティゾーンを選択または作成する
- Tunnel IDをクリックして、値を指定します。
- Tunnel Sourceをクリックし、トンネルを確立するWANインターフェイスを指定します
- IPSec Tunnel Modeをクリックし、selectIPv4
- IP Addressをクリックして、VTIのIPアドレスを設定します

OKをクリックします。

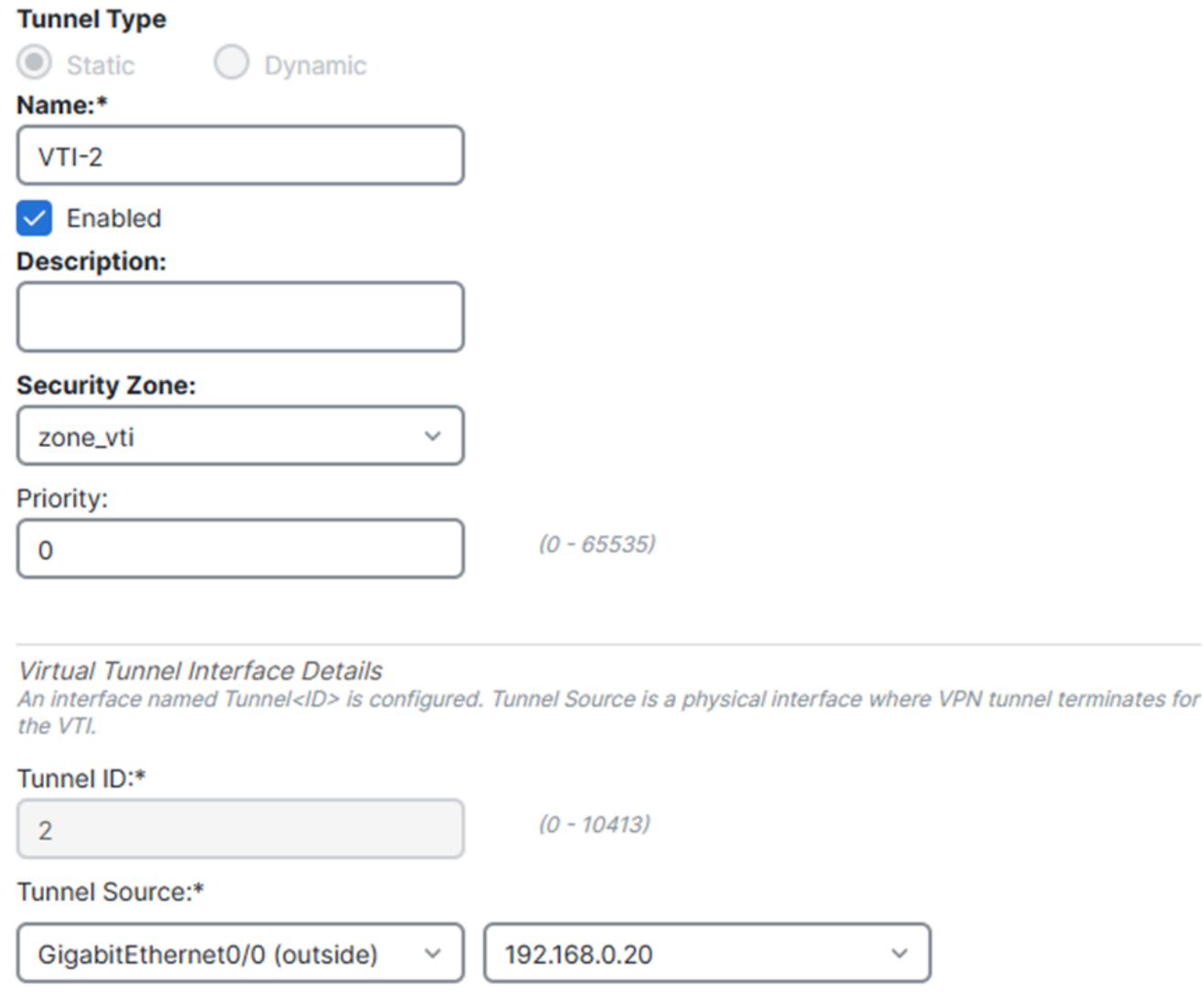


VTI1.1

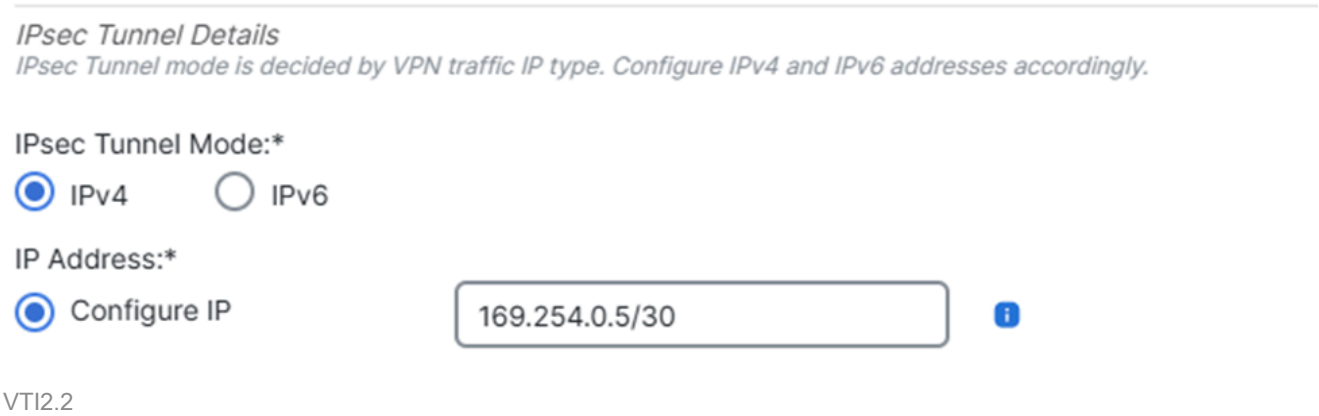
VTI1.2

仮想トンネルインターフェイス2:

- 名前を入力し、Enableをクリックします。
- セキュリティゾーンを選択または作成する
- Tunnel IDをクリックして、値を指定します
- Tunnel Sourceをクリックし、トンネルを確立するWANインターフェイスを指定します
- IPSec Tunnel Modeをクリックし、selectIPv4
- IP Addressをクリックして、VTIのIPアドレスを設定します
- OKをクリックします。

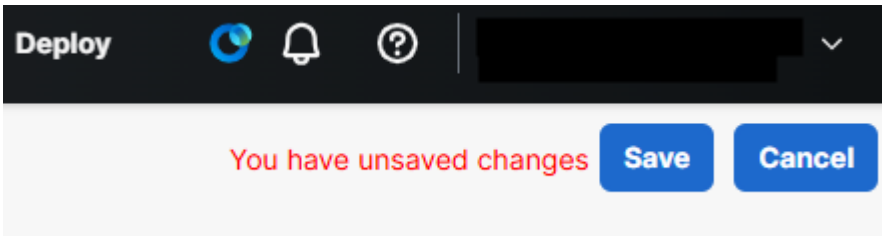


VTI2.1



VTI2.2

[Save] をクリックします。

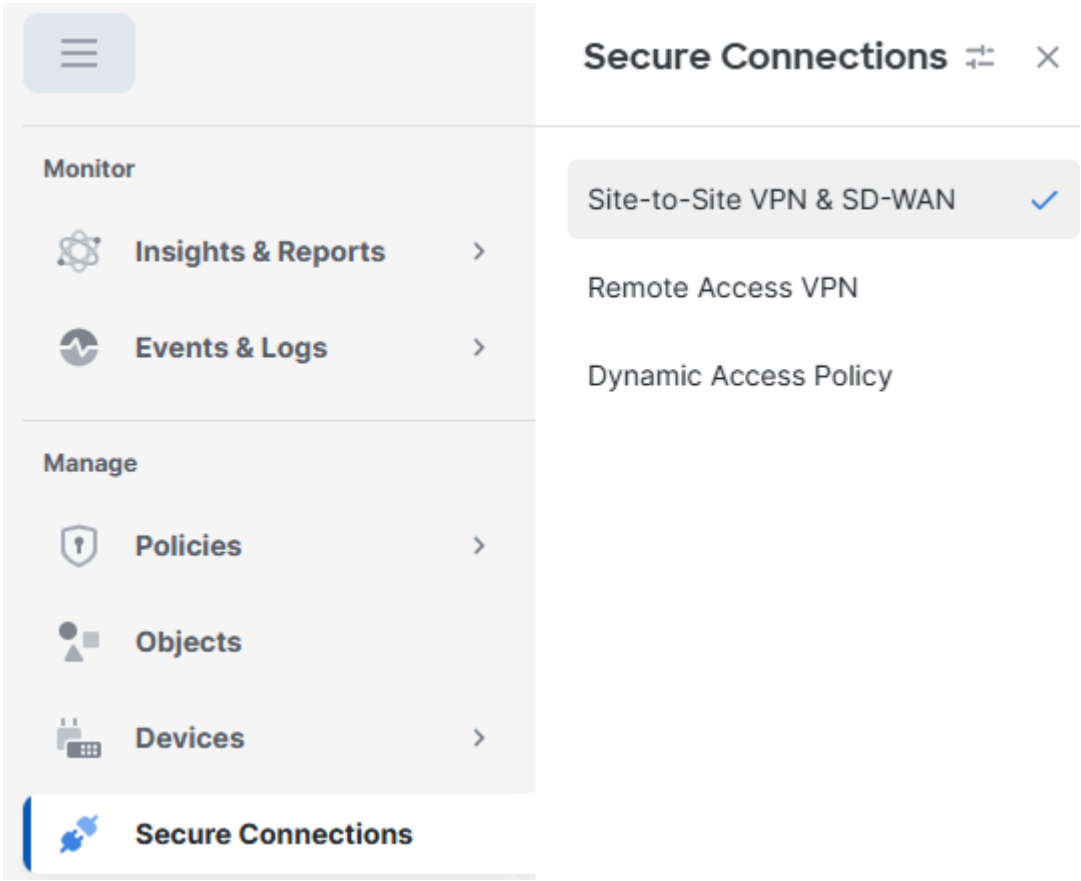


VTIの変更の保存

IPSecトンネルの設定

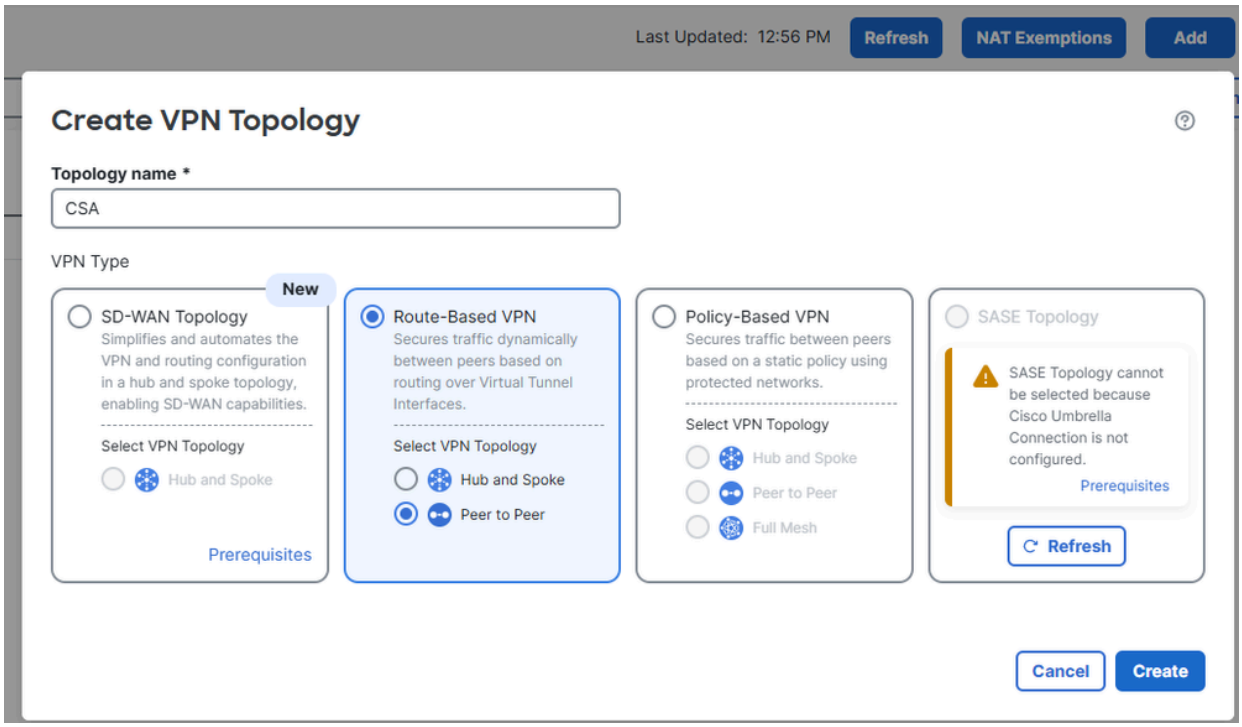
cdFMCダッシュボードに移動します。

- Secure Connectionをクリックします> サイト間VPNおよびSD-WAN



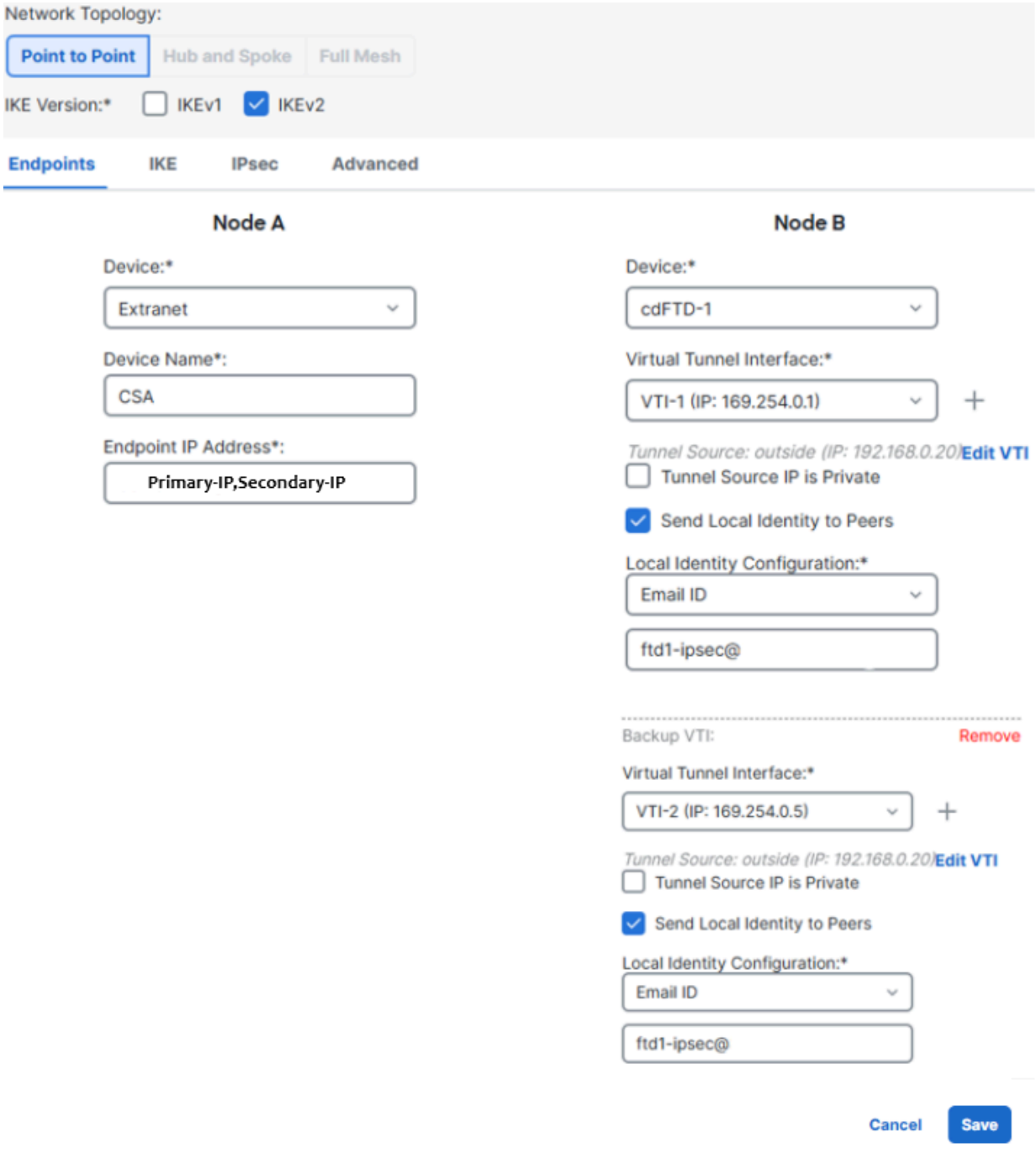
S2S

- onAddをクリックします。
  - Route-Based VPNをクリックします。
  - ピアツーピアをクリックします。



VPNの追加

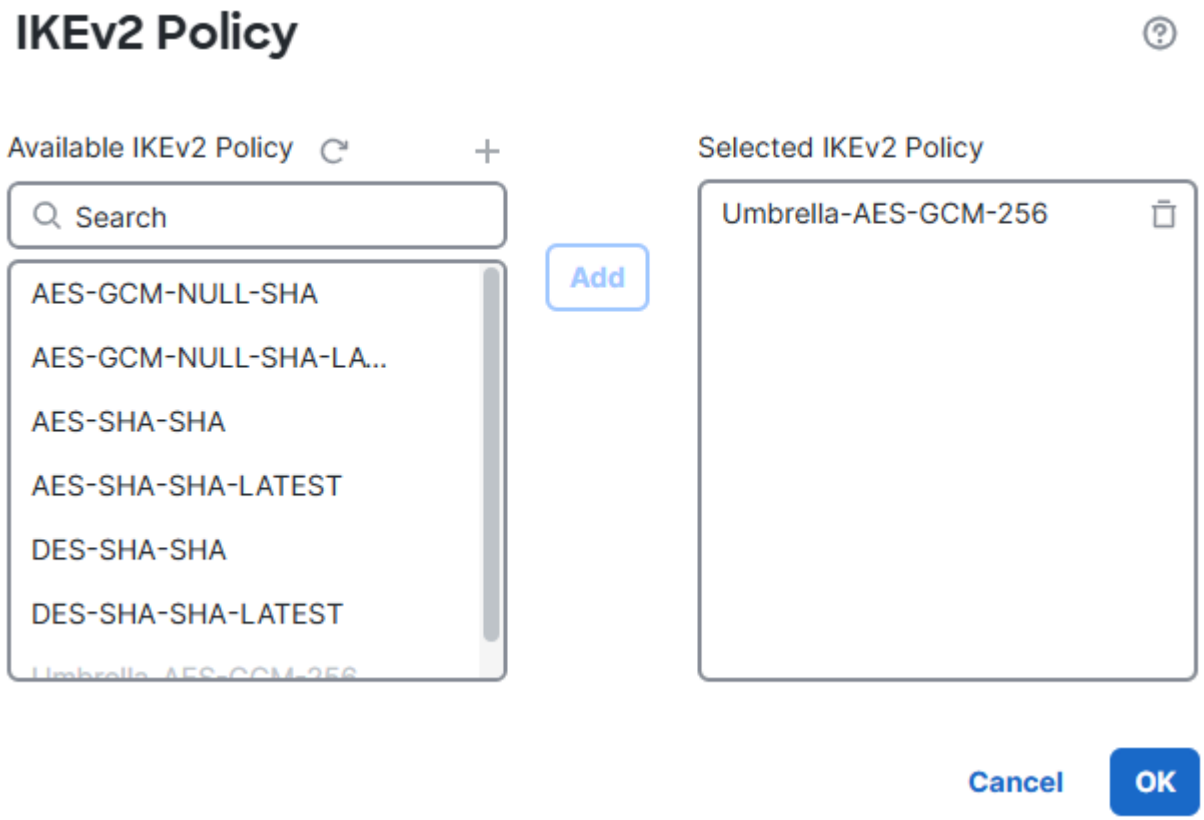
- セキュアアクセス設定のステップ5から、プライマリおよびセカンダリデータセンターのトンネルIDとIPアドレスを取得します
- onEndpointsをクリックします。
  - Node Aの下で、onDeviceをクリックして、Extranetを選択します。
  - Device Nameをクリックして、名前を指定します
  - Enpoint IP Addressesをクリックし、Secure Accessのプライマリ IPアドレスとセカンダリIPアドレスをカンマで区切って入力します（「Secure Access」の下の「Save Network Tunnel Group Configuration」から）コンフィギュレーション)
  - ノードBでデバイスをクリックし、FTDデバイスを選択します
  - Virtual Tunnel Interfaceをクリックし、前の手順で作成した最初のVTIインターフェイスを選択します
  - Send Local Identity to Peersオプションをクリックして、Email IDを選択し、（Secure Access Configurationの下の「Save Network Tunnel Group Configuration」にある）プライマリトンネルIDを入力します。
  - Add Backup VTIをクリックします。
  - Virtual Tunnel Interfaceをクリックし、前のステップで作成した2番目のVTIインターフェイスを選択します
  - Send Local Identity to Peersoptionをクリックし、Email IDを選択し、（Secure Access Configurationの下の「Save Network Tunnel Group Configuration」にある）セカンダリトンネルIDを入力します。
  - [Save] をクリックします。



FTD VTIの設定

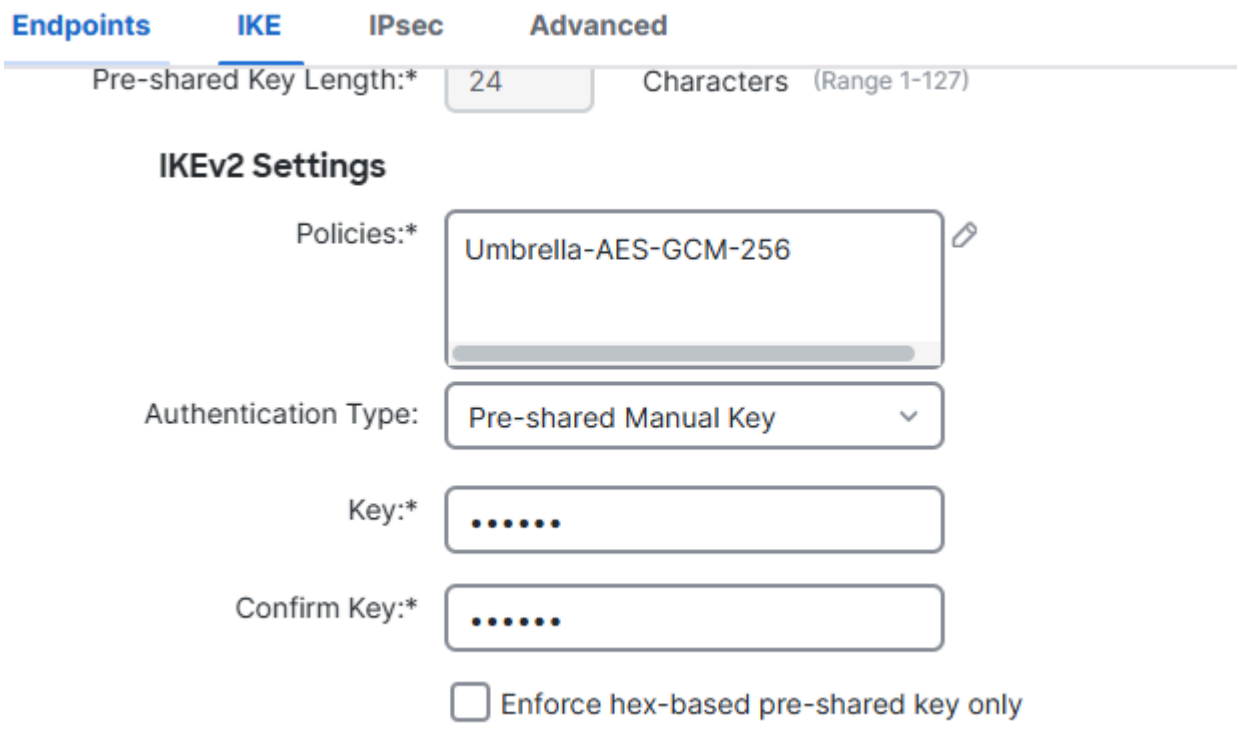
- IKEをクリックします
  - **IKEv2 Settings** > **Policies**の順にクリックします。
  - Umbrella-AES-GCM-256オプションを選択します

OKをクリックします。



IKEv2ポリシー

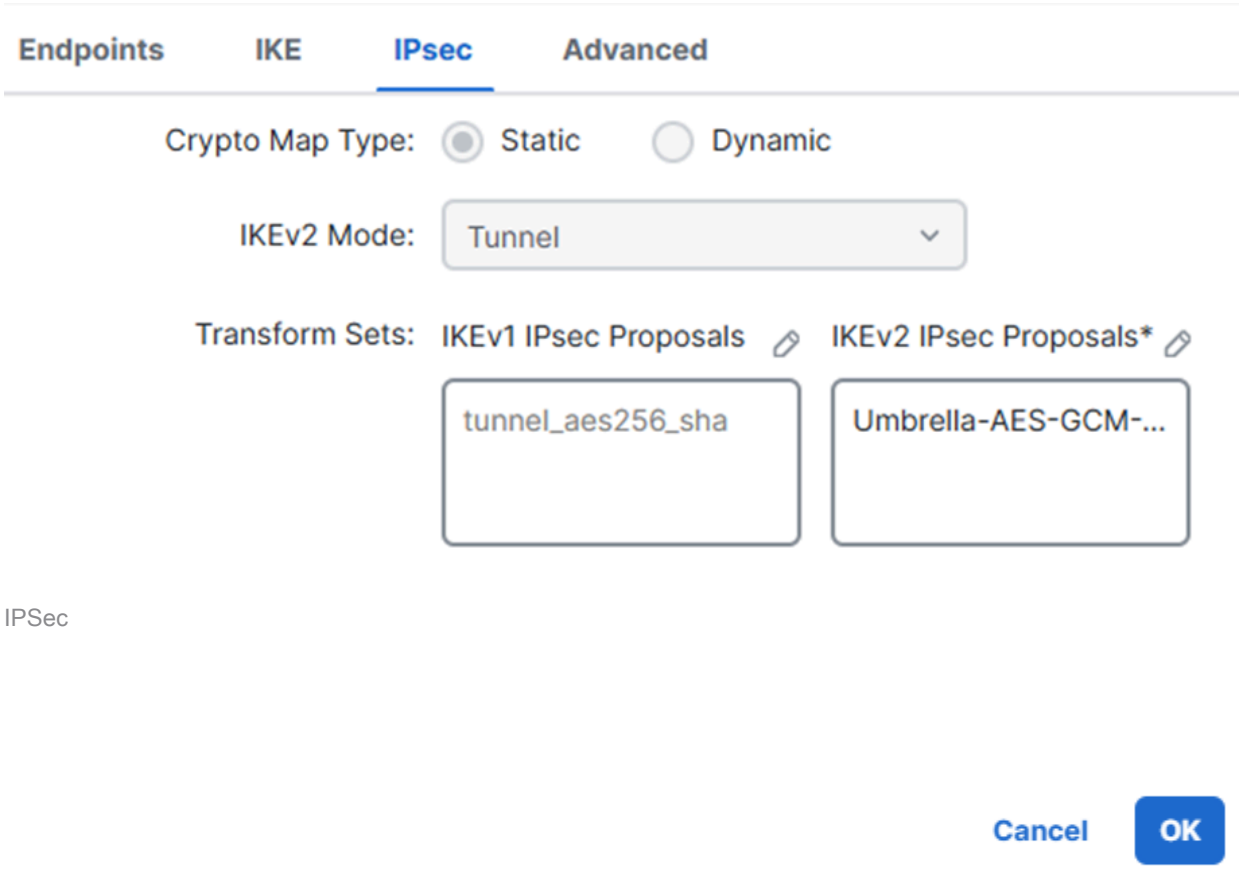
- Authentication Typeをクリックして Pre Shared Manual Keyを選択し、Secure Access（パスフレーズ）で設定したPSKを入力します



IKE

- IPSEC

- IKEv2 Proposals
- Umbrella-AES-GCM-256を選択します。
- OKをクリックします。



IPSec

IKEv2プロポーザルの保存

FTDルーティングの設定

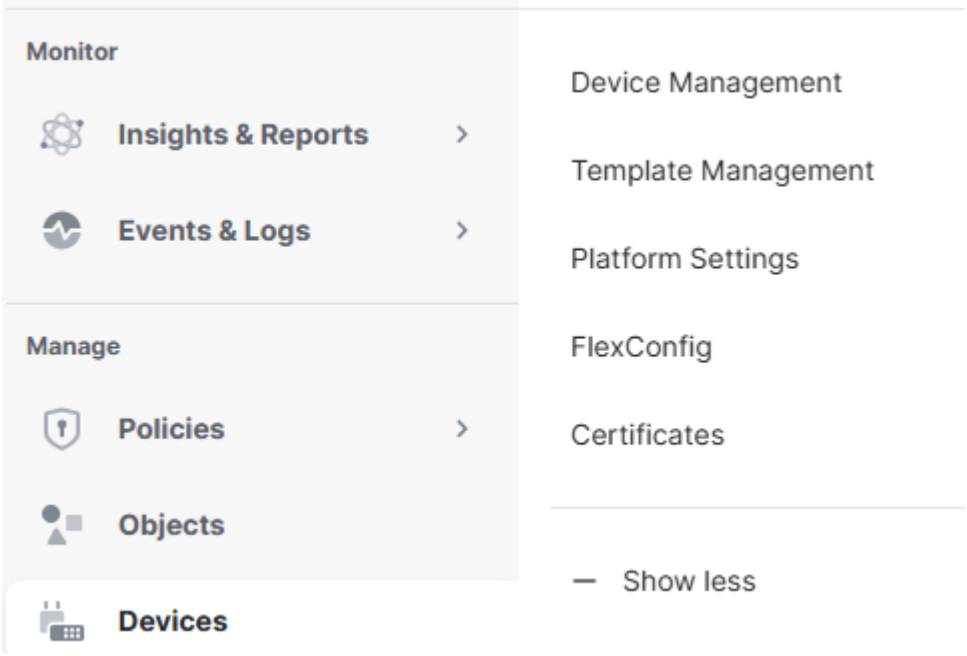
ダイナミックルーティング(BGP)

ボーダーゲートウェイプロトコル(BGP)は、自律システム(AS)間のルーティング情報の交換を自動化するダイナミックルーティングプロトコルです。 スタティックルートに依存するのではなく、属性とポリシーに基づいてデータトラフィックに使用できるベストパスを決定する。

BGPは、ルートを動的に学習および更新することで、拡張性を向上させ、パス選択を最適化し、リンクまたはネットワークの変更時に自動フェールオーバーを提供します。

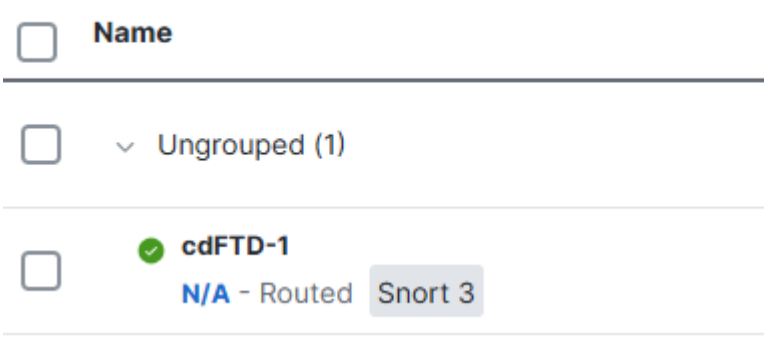
cdFMCダッシュボードに移動します。

- Devices> Device Managementの順にクリックします。



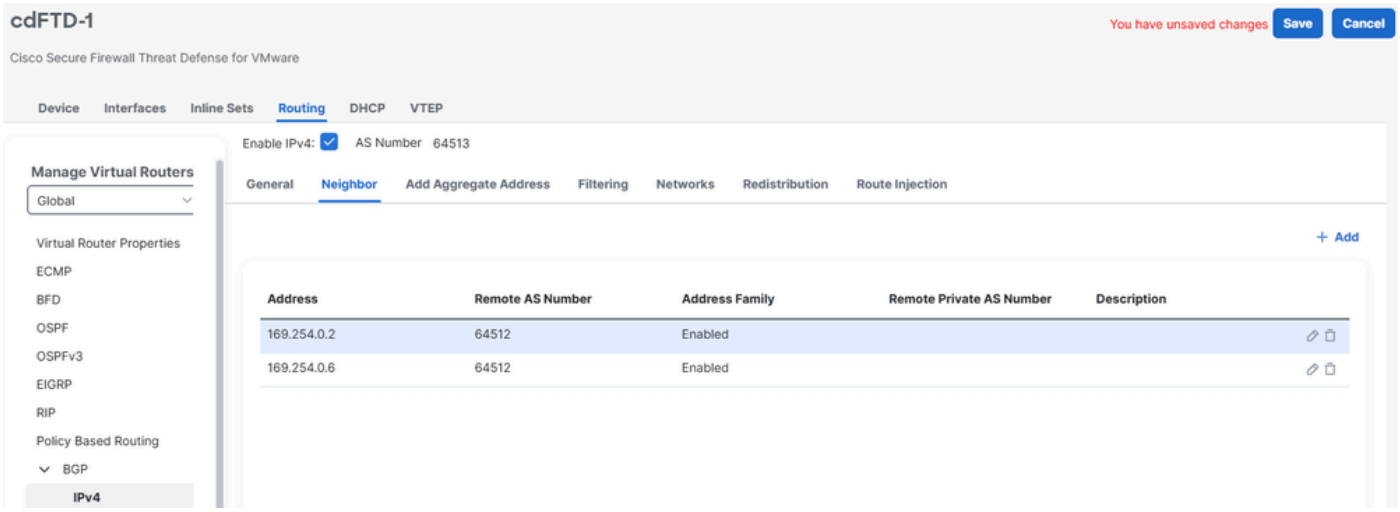
デバイス

- FTDをクリック



FTDデバイス

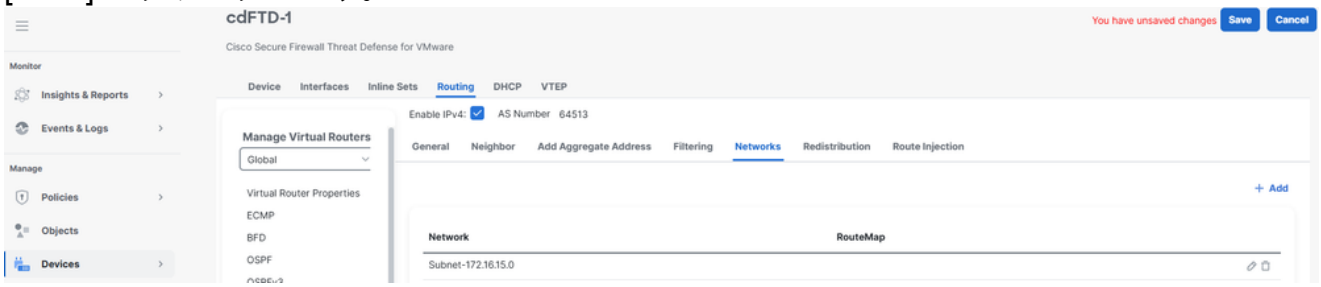
  - Routing > BGP > IPv4 > Enable IPv4の順にクリックします
  - Neighborをクリックして、セキュアアクセスのためのBGP自律システム(AS)番号を、ネイバーのIPアドレスとともに指定します
    このプロセスに関連するすべての設定の詳細が記載されている「セキュアアクセスの設定」の下の注を参照してください。
  - onSaveをクリックします



BGPネイバー

注:2025年11月以降、新しく作成されたすべてのセキュアアクセス組織は、デフォルトでネットワークトンネルグループのBGPピアリングにパブリックASN 32644を使用します。2025年11月より前に設立された既存の組織は、以前はSecure Access BGPピア用に予約されていたプライベートASN 64512を引き続き使用します。

- Networksをクリックし、アドバタイズするネットワークをSecure Accessに追加します
- [Save] をクリックします。



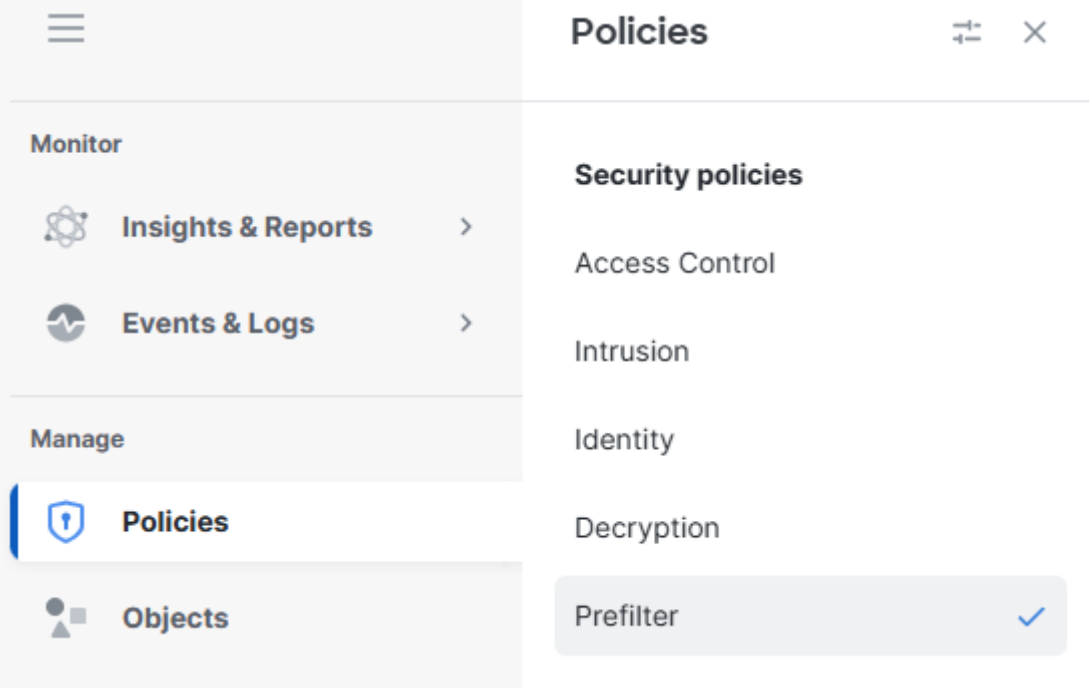
ネットワークの追加

アクセスポリシーの設定

Cisco Firepower Threat Defense(FTD)でトラフィックを許可し、プライベートリソースへのアクセスを有効にするには、トラフィックが最初にプレフィルタリングと呼ばれるアクセスコントロールの初期段階を通過する必要があります。

プレフィルタリングは、より深い検査が行われる前に処理され、シンプルで高速になるように設計されています。基本的な外部ヘッダー基準（送信元と宛先のIPアドレスとポートなど）を使用してトラフィックを評価し、トラフィックを迅速に許可、ブロック、またはバイパスします。この段階でトラフィックを許可すると、ディープパケットインスペクションや侵入ポリシーなど、よりリソースを大量に消費するインスペクションを省略できるため、セキュリティ制御を維持しながらパフォーマンスを向上させることができます。

Policies> Prefilterの順に移動します。



プレフィルタ

- アクセスポリシーで使用されているプレフィルタポリシーの編集をクリックします。

プレフィルタをクリックします。

- Add Tunnel Ruleをクリックします。
  - VPNaaSネットワークやZTAサブネットからプライベートリソースへのトラフィックを追加し、許可します。
  - onSaveをクリックします

ルールの保存

この時点で、FTDの設定が完了して確認されたら、展開を続行できます。導入後、IPsecトンネルとBGPネイバーセッションの両方が正常に起動し、接続とダイナミックルーティングが期待どおりに動作していることを確認します。

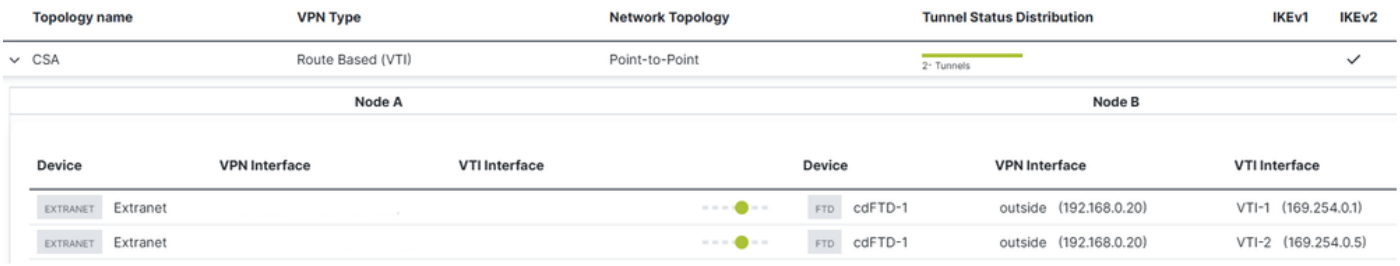
確認

FTDでの確認

FTDのトンネルステータス

トンネルの現在のステータス(アップ状態またはダウン状態を含む)を表示できます。これにより、IPSecトンネルが適切に確立されていることを確認できます。

- Secure Connectionsをクリックします。
- Site-to-Site VPN & SD-WANをクリックします。
- トポロジ名をクリックします。

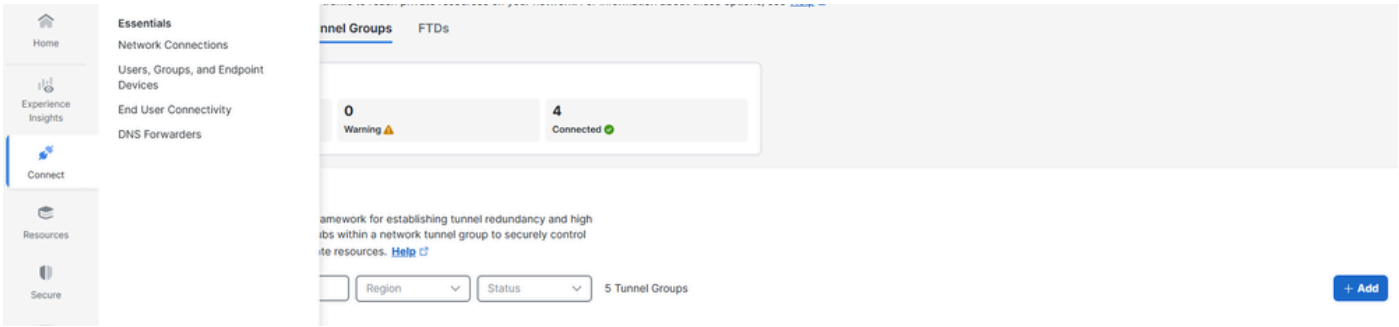


FTDトンネルステータス

セキュアアクセスのトンネルステータス

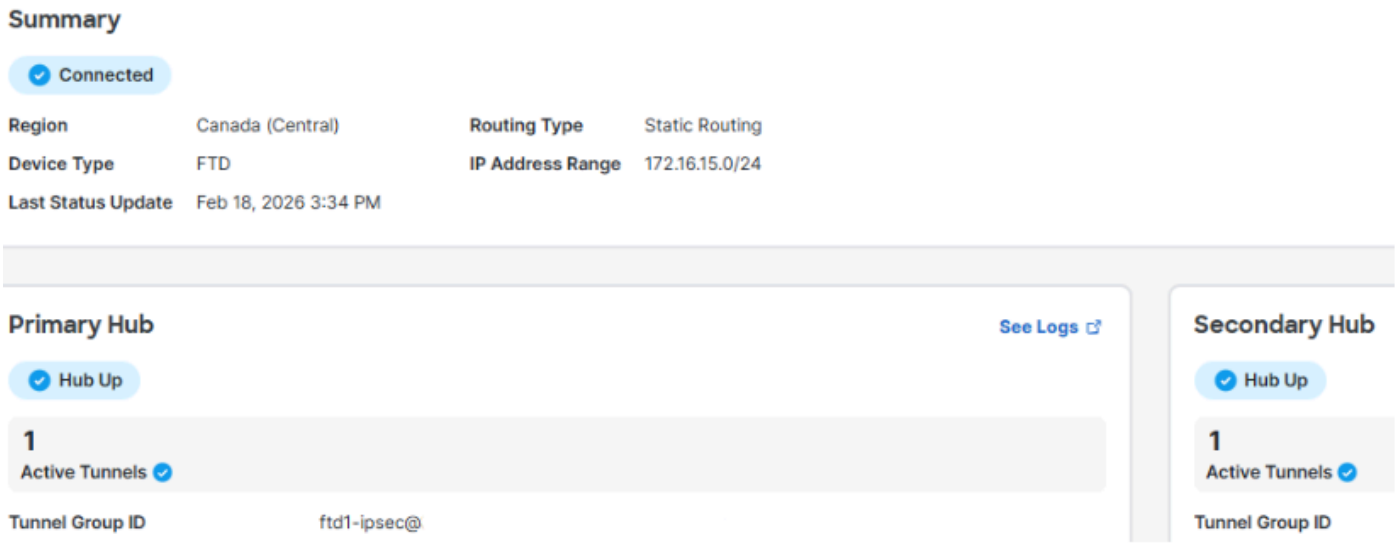
トンネルの現在のステータスを表示できます。ステータスには、接続解除、警告、または接続の有無が含まれます。これにより、IPSecトンネルが適切に確立されていることを確認できます。

- Connect > Network Connectionsの順にクリックします
- Network Tunnel Groupsをクリックします。



NTGの確認

- Network Tunnel Groupをクリックします

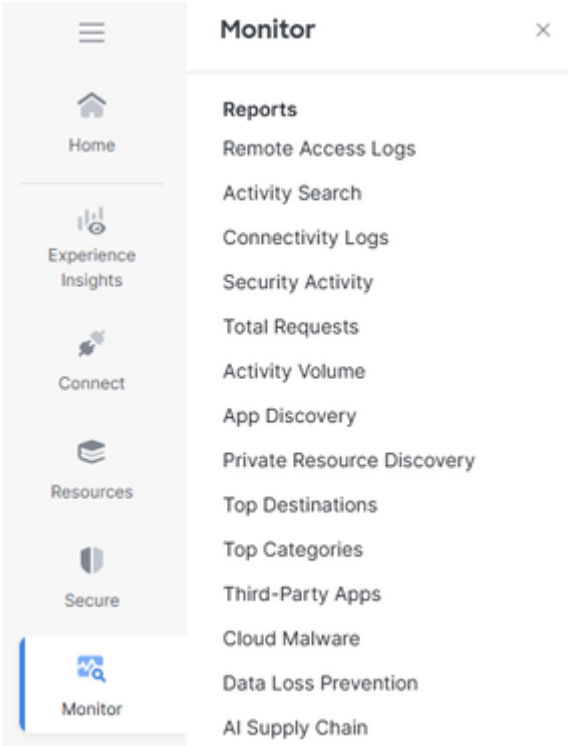


CSAトンネルステータス

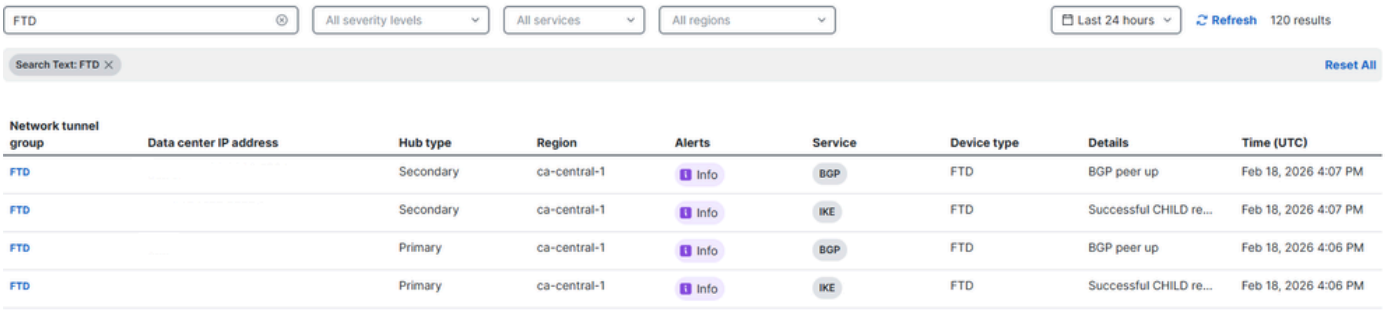
セキュアアクセスのイベント

トンネルとBGPのイベントを表示して、IPSecトンネルのステータスがアップ状態で安定しているかどうか、およびBGPセッションが確立されているかどうかを確認できます。

Monitor > Network Connectivityの順にクリックします。

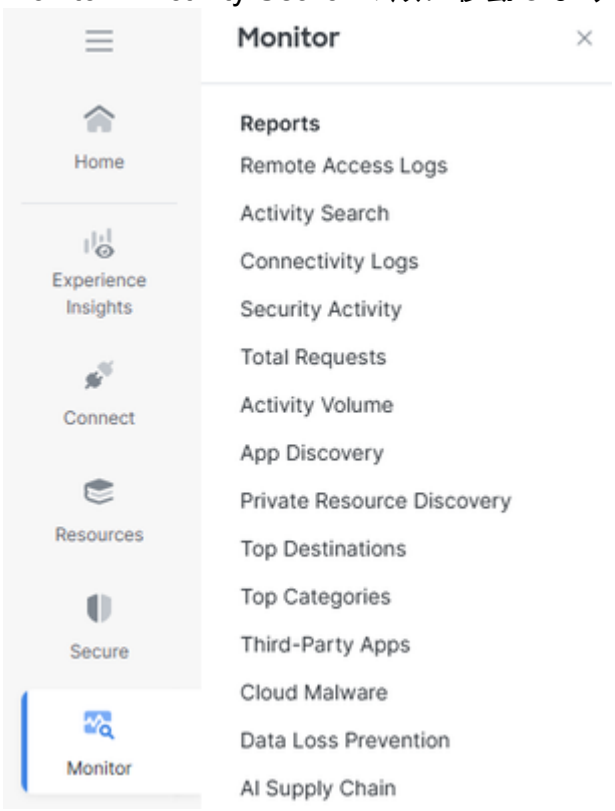


接続ログの監視



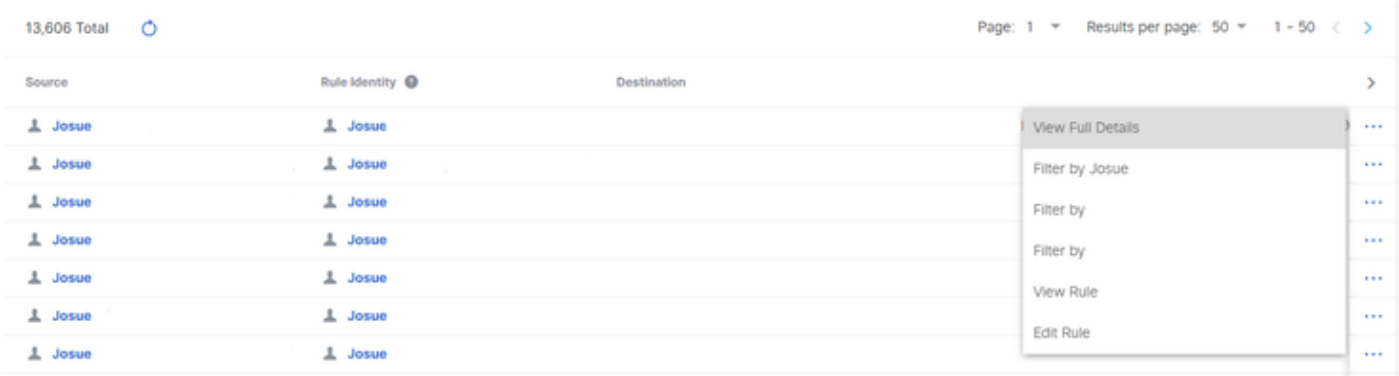
NTGログ

Monitor > Activity Searchの順に移動します。

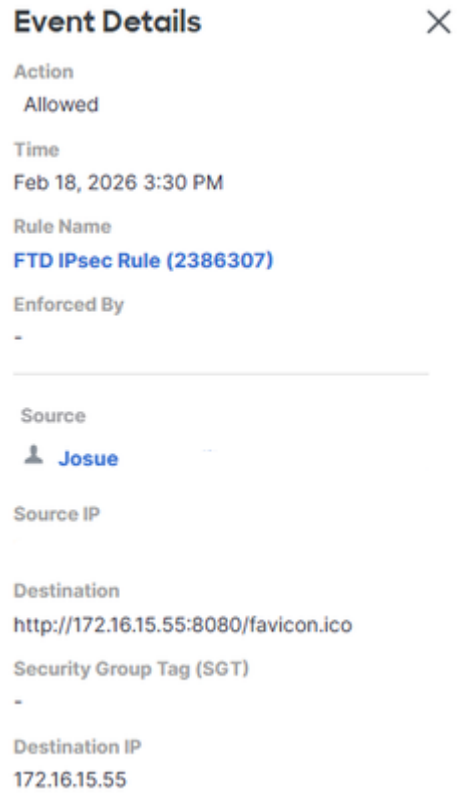


接続ログの監視

関連するイベントで、View Full Detailsをクリックします。



詳細



アクティビティ検索

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 Firewall Management Centerデバイス設定ガイド、7.7

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。