NATを使用したプライベートアクセスのための、セキュアなFTDおよびASA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、ネットワークアドレス変換(NAT)を使用してセキュアアクセスネットワークトンネルグループを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Ciscoファイアウォール管理センター

- Cisco Secure Firewall脅威対策
- シスコセキュアアクセス
- Cisco Adaptive Security Appliance
- ネットワークアドレス変換
- ポリシーベースルーティング
- ファイアウォールでのパケットキャプチャ

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。

- Ciscoファイアウォール管理センター7.10
- Cisco Secure Firewall Threat Defense 7.10
- シスコセキュアアクセス
- Cisco適応型セキュリティアプライアンス9.22
- Cisco ルータ

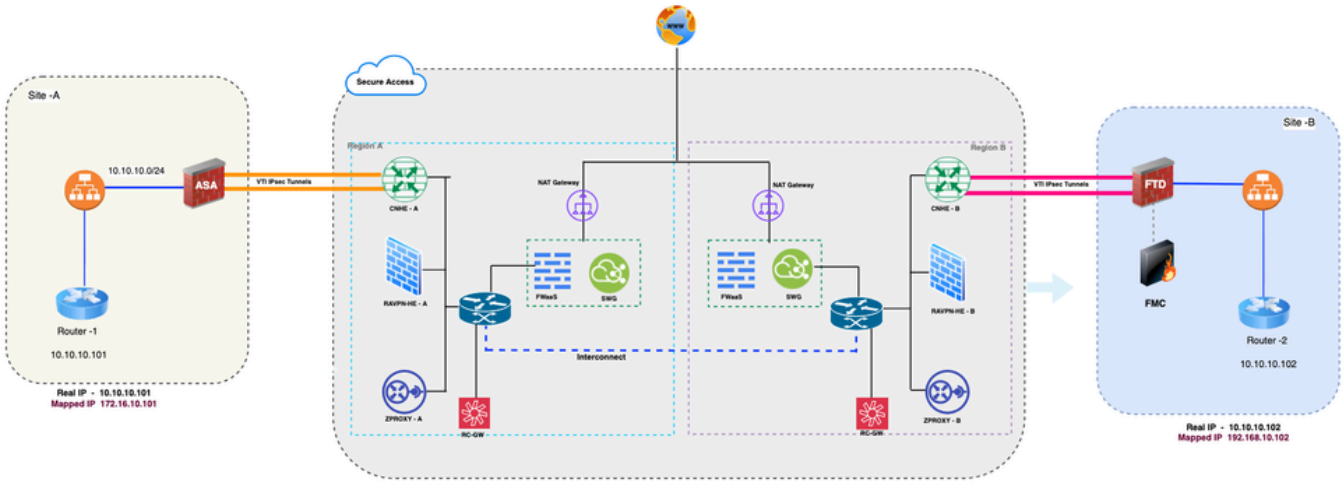
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

バックグラウンド情報

Cisco Secure Accessは、Secure Internet Access(SIA)やSecure Private Access(SPA)など、クラウドネイティブのセキュアサービスエッジ機能を提供します。 データセンターを経由するすべてのトラフィックをバックホールすることなく、リモートユーザへのプライベートアプリケーションアクセスを拡張する組織では、Secure AccessはIPsecネットワークトンネルグループ(NTG)を使用して、Cisco Firewall Threat Defense(FTD)、Adaptive Security Appliance(ASA)、Cisco Secure Access Cloud Points-of-Presence(PoP)などのオンプレミスネットワークデバイス間に暗号化トンネルを作成します。

このドキュメントでは、Cisco FTD(FTD)、ASA、およびCisco Secure Accessの間でIKEv2を使用してルートベースのIPSecトンネルを確立し、セキュアアクセス上でネットワークアドレス変換(NAT)を有効にし、FTDおよびASA上でポリシーベースルーティング(PBR)を有効にして、プライベートアクセスバウンドのトラフィックだけをトンネルに誘導する方法について説明します。

ネットワーク図



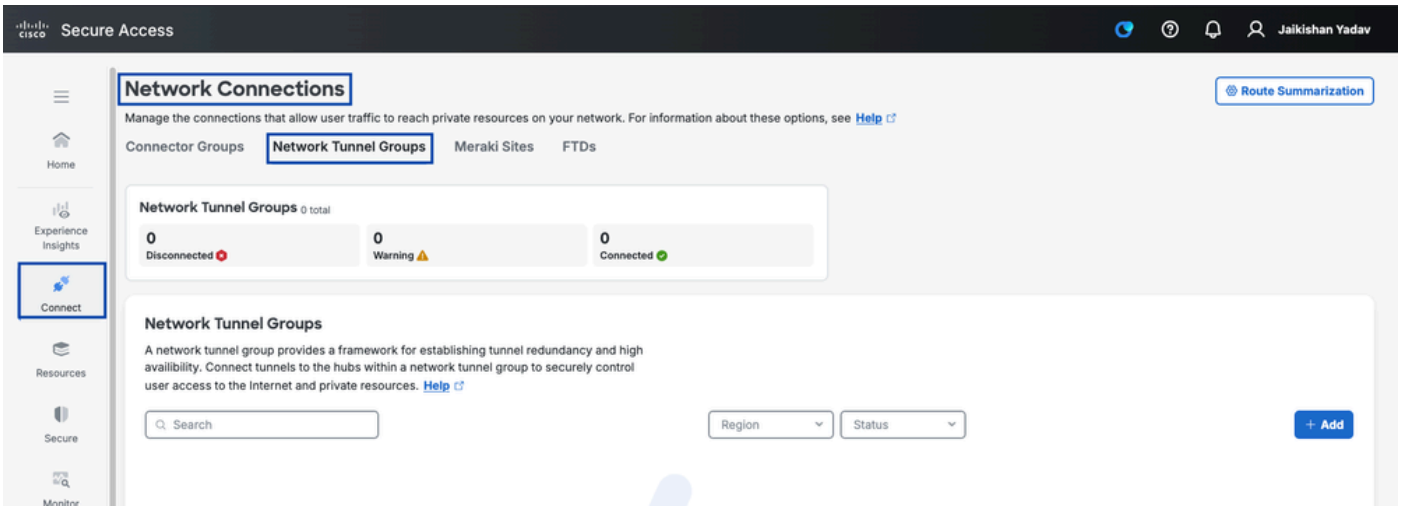
Network Topology

設定

セキュアアクセスおよびセキュアファイアウォールスレッド防御：PBRを使用したダイナミック(BGP)ルートベースVPN

セキュアアクセスでのネットワークトンネルグループの設定

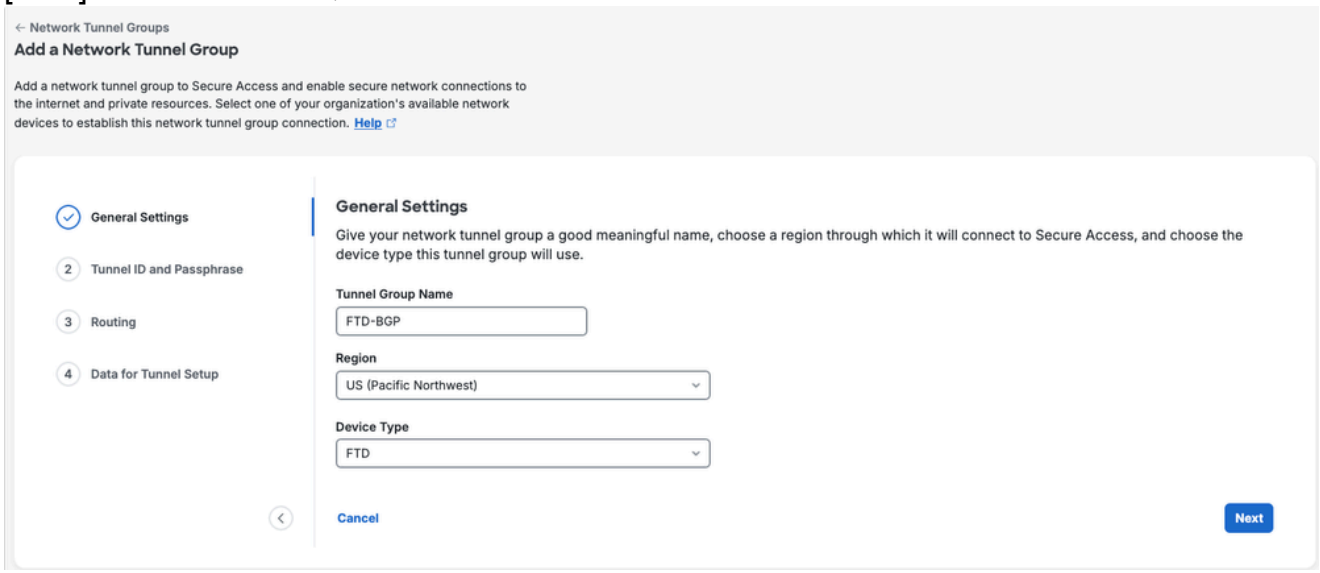
1.セキュアアクセスダッシュボードへのログインセキュアアクセス
2. Connect > Network Connections > Network Tunnel Groupsの順に移動し、+Addをクリックしてネットワークトンネルグループを設定します



セキュアアクセス – ネットワークトンネルグループ

3.ネットワークトンネルグループの構成 – 一般設定

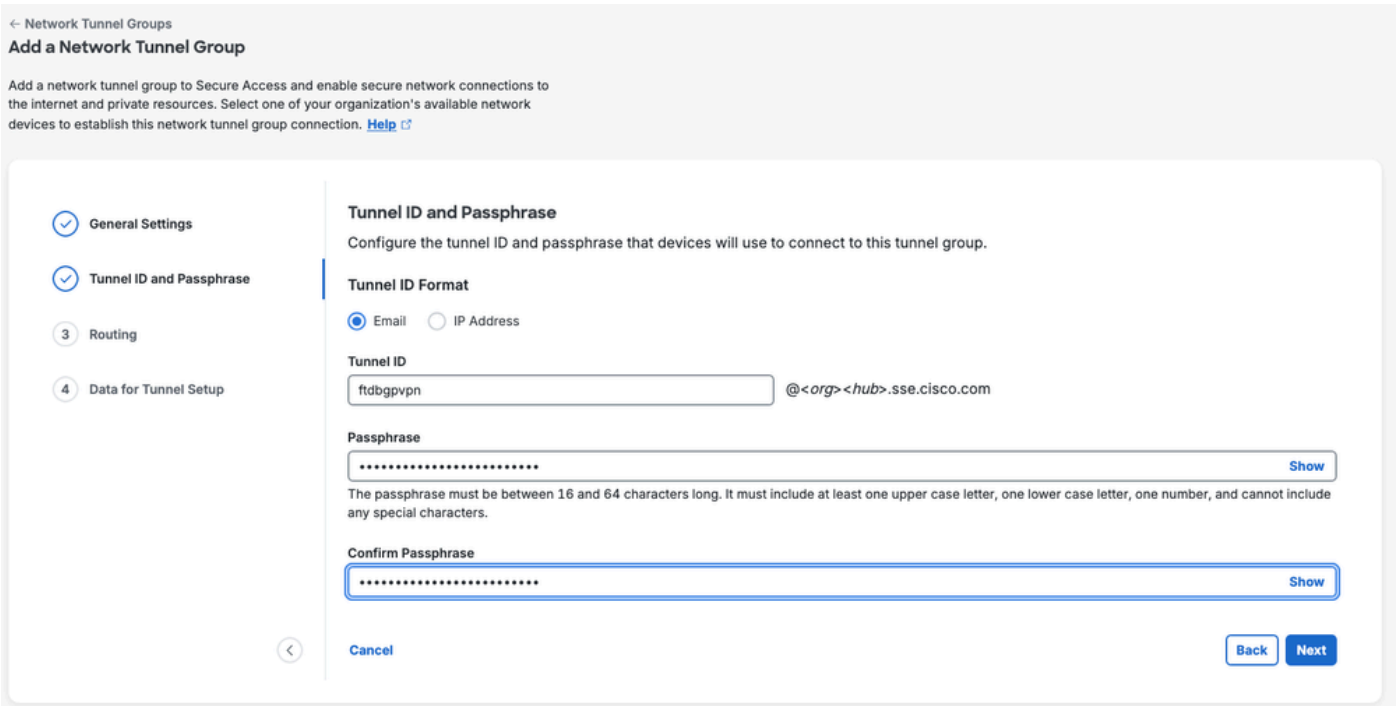
- トンネルグループの名前、リージョン、およびデバイスタイプの設定
- [Next] をクリックします。



セキュアアクセス – ネットワークトンネルグループの一般設定

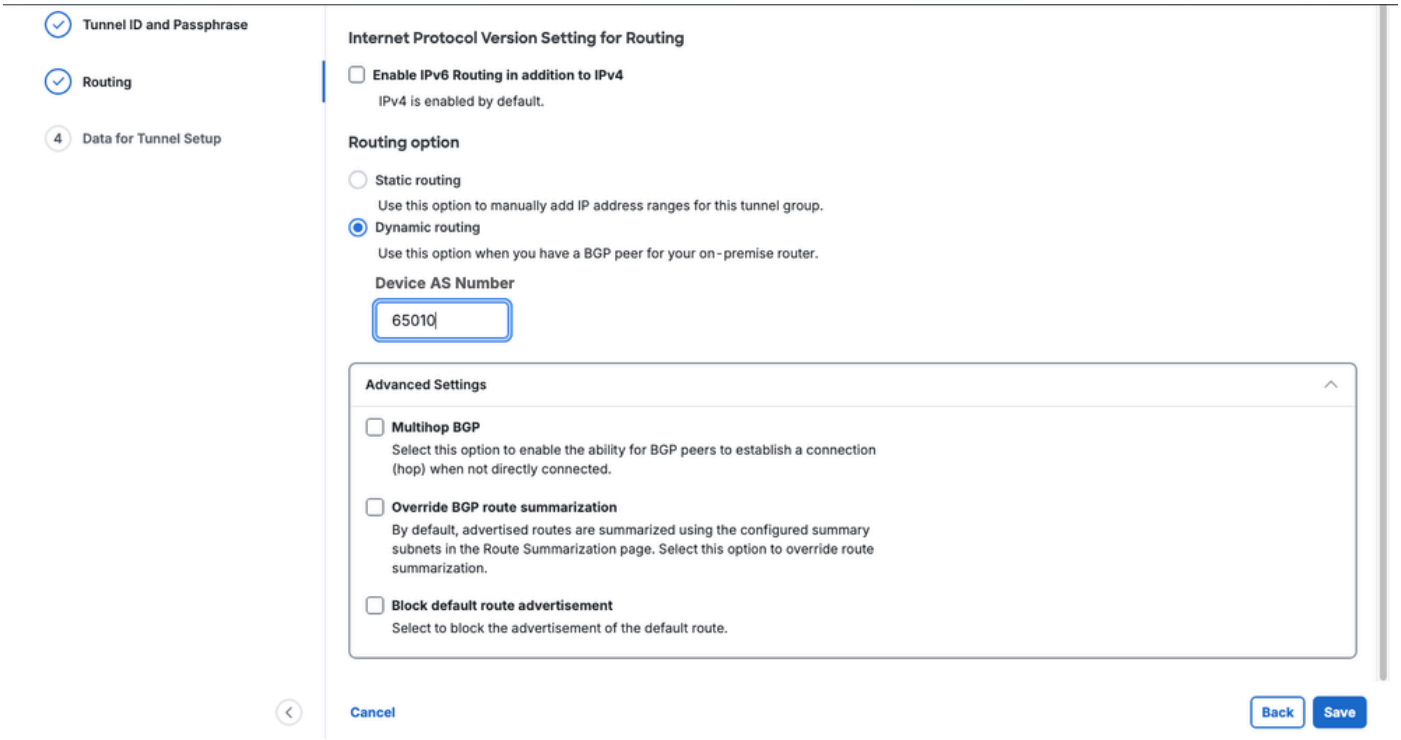
4.トンネルIDとパスフレーズを設定します。

- トンネルIDとパスフレーズを設定します。
- Nextをクリックします。



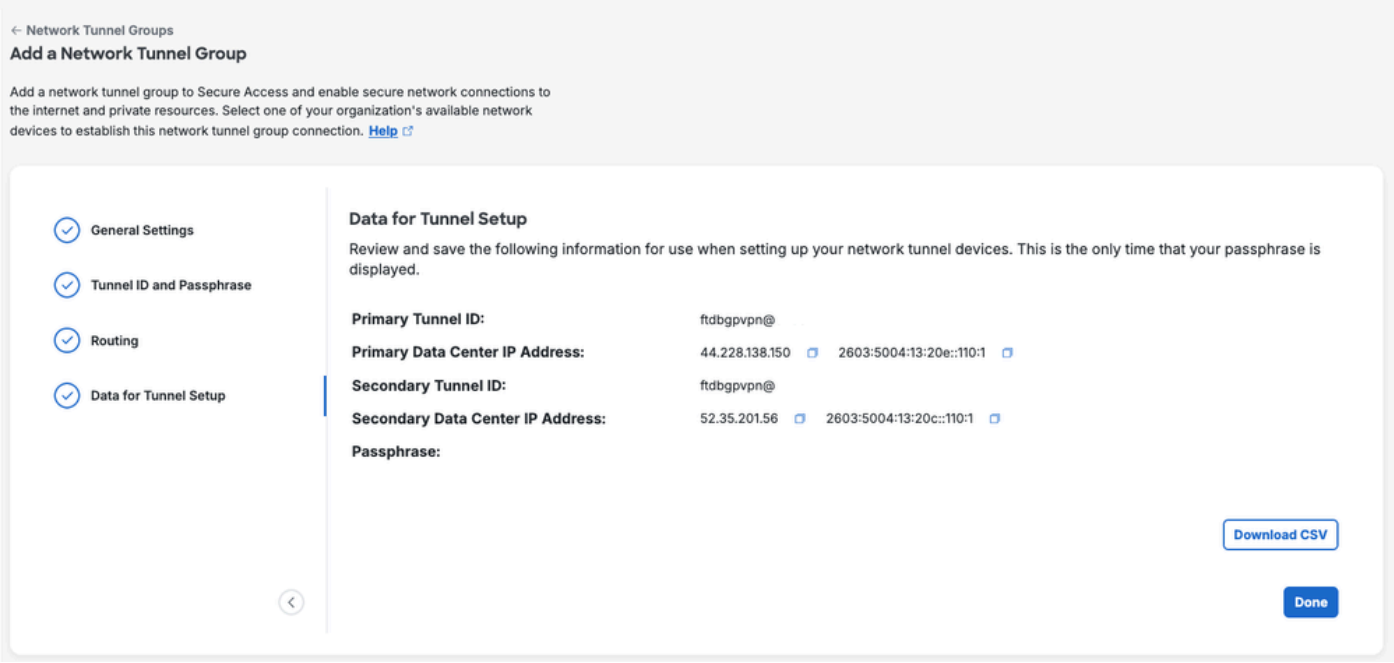
5.ルーティングの設定

- デバイスAS番号の設定
- [Save] 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ルーティング

6. ネットワークトンネルグループ設定の保存



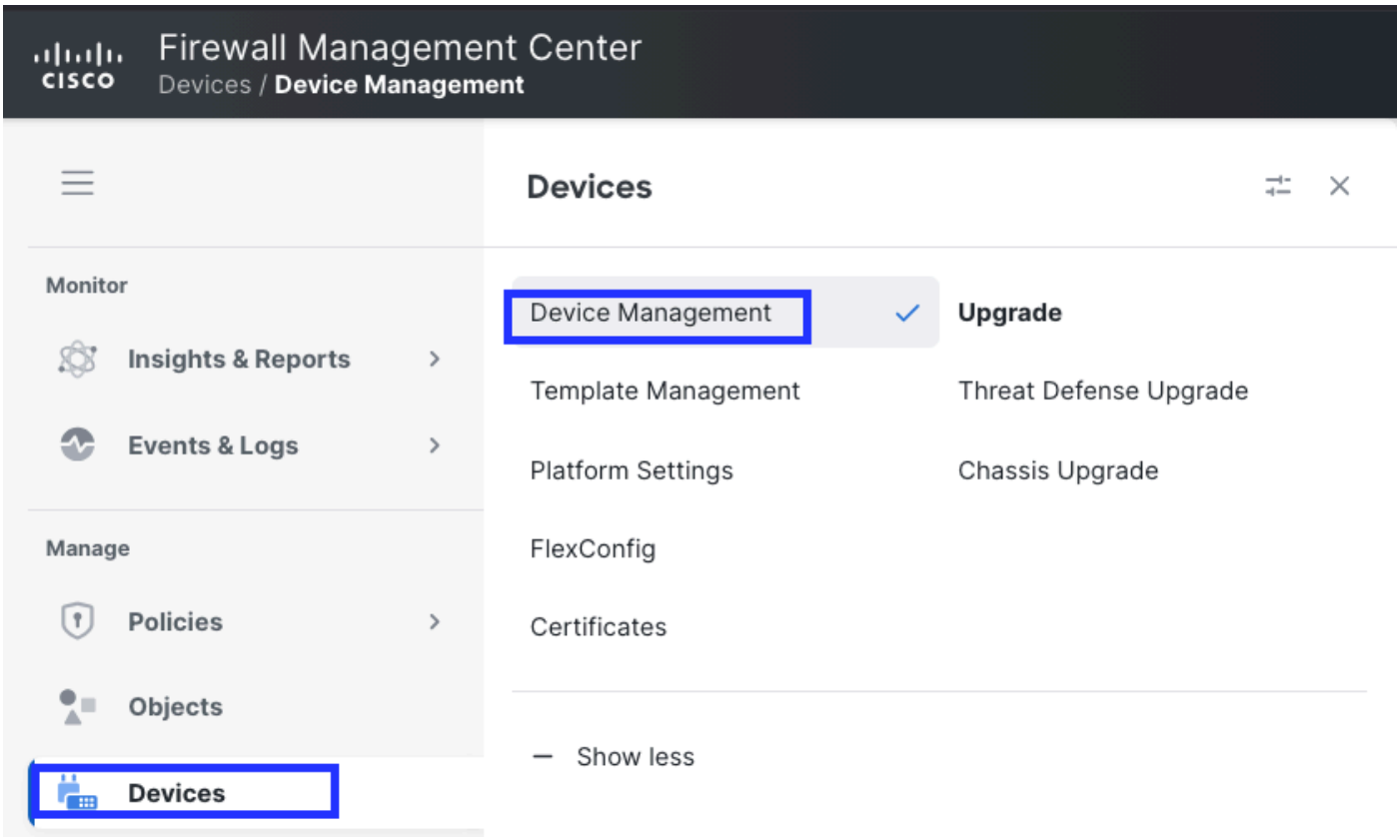
セキュアアクセス – ネットワークトンネルグループ

PBRを使用したSecure Firewall Threat Defense(FTD)でのダイナミックルートベースIPsec VPNの設定

1. ファイアウォール管理センター(FMC)へのログイン

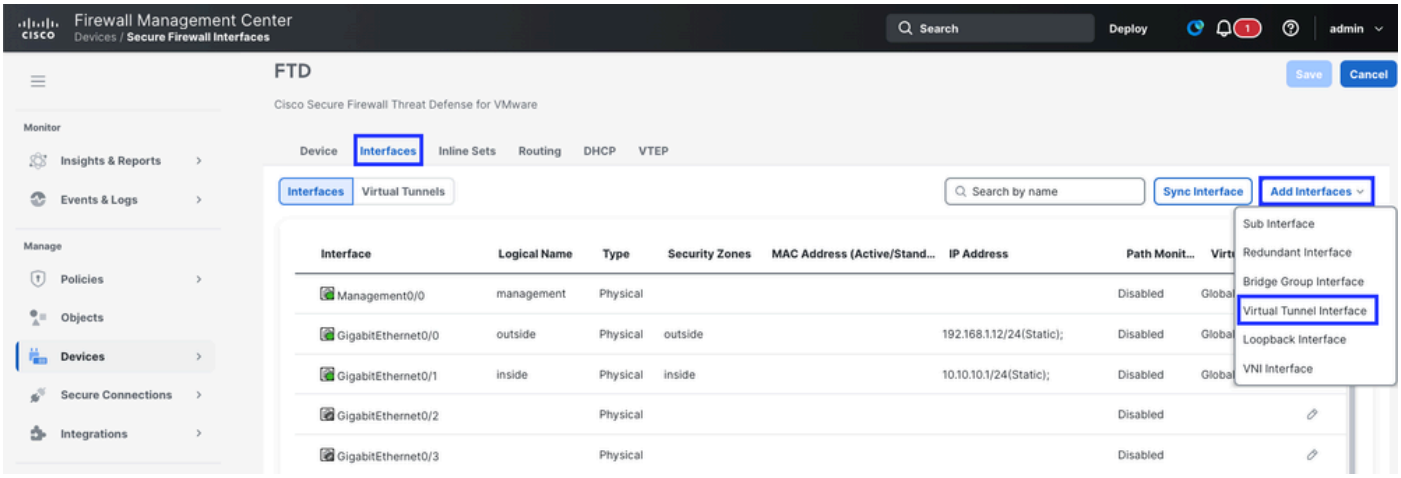
2.仮想トンネルインターフェイスVTIの設定

- Devices > Device Managementに移動します



セキュアファイアウォール管理 – ダッシュボード

- デバイスの横にある鉛筆アイコンをクリックし、インターフェイスセクションに移動します。
- Add interfacesをクリックして、Virtual Tunnel Interfaceを選択します。



セキュアファイアウォール管理：FTD VTIの設定

- VTIの設定

Add Virtual Tunnel Interface

General | Path Monitoring

Tunnel Type

(•) Static ( ) Dynamic

Name:*

VTI-1

[x] Enabled

Description:

Virtual Tunnel interface for Primary VTI VPN

Security Zone:

vti

Priority:

0 *(0 - 65535)*

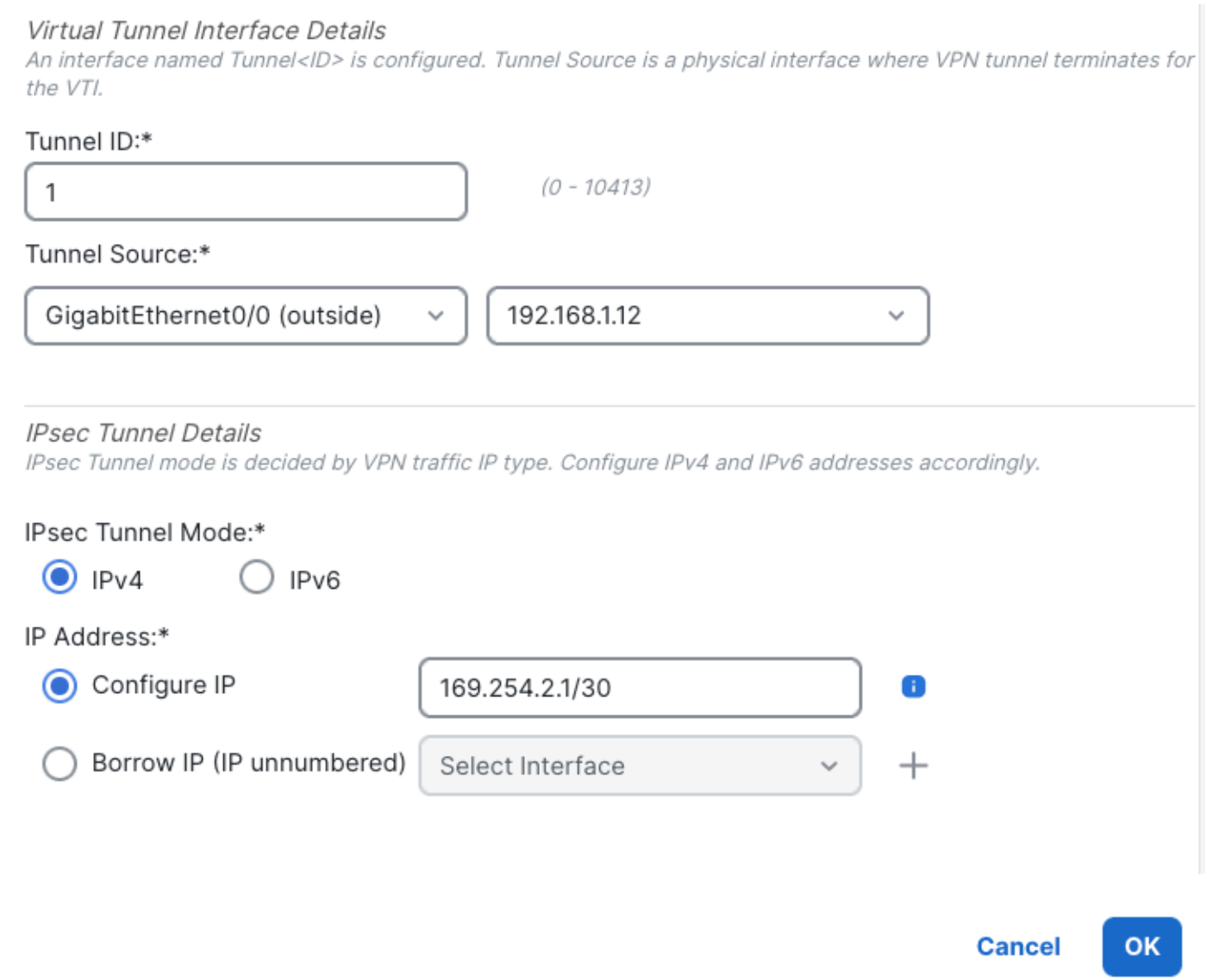
Propagate Security Group Tag: [x]

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

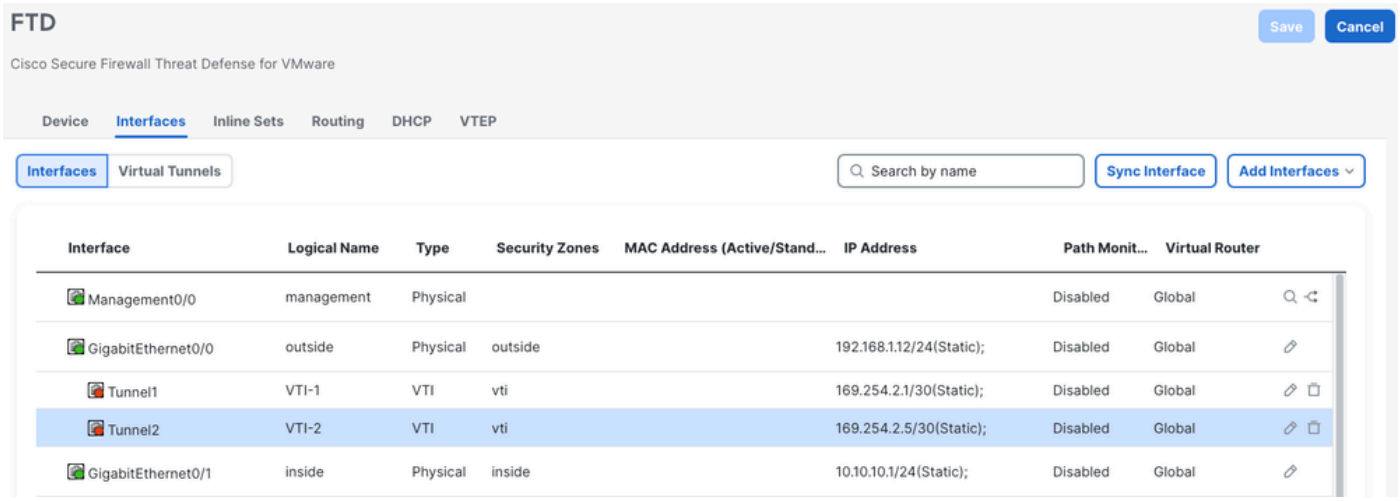
Tunnel ID:*

1 *(0 - 10413)*

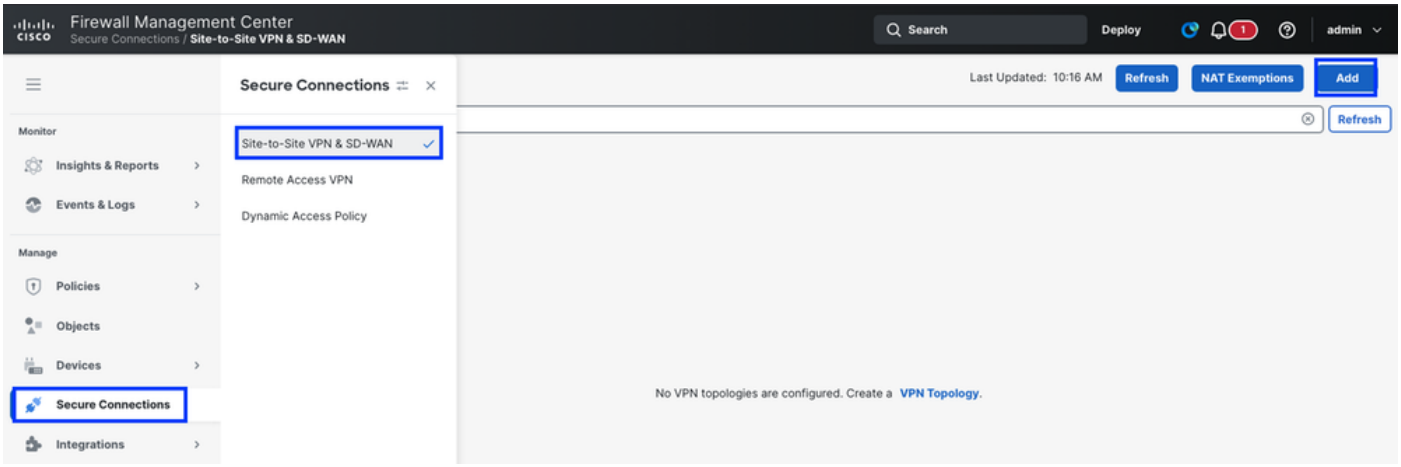


セキュアファイアウォール管理：FTD VTIの設定

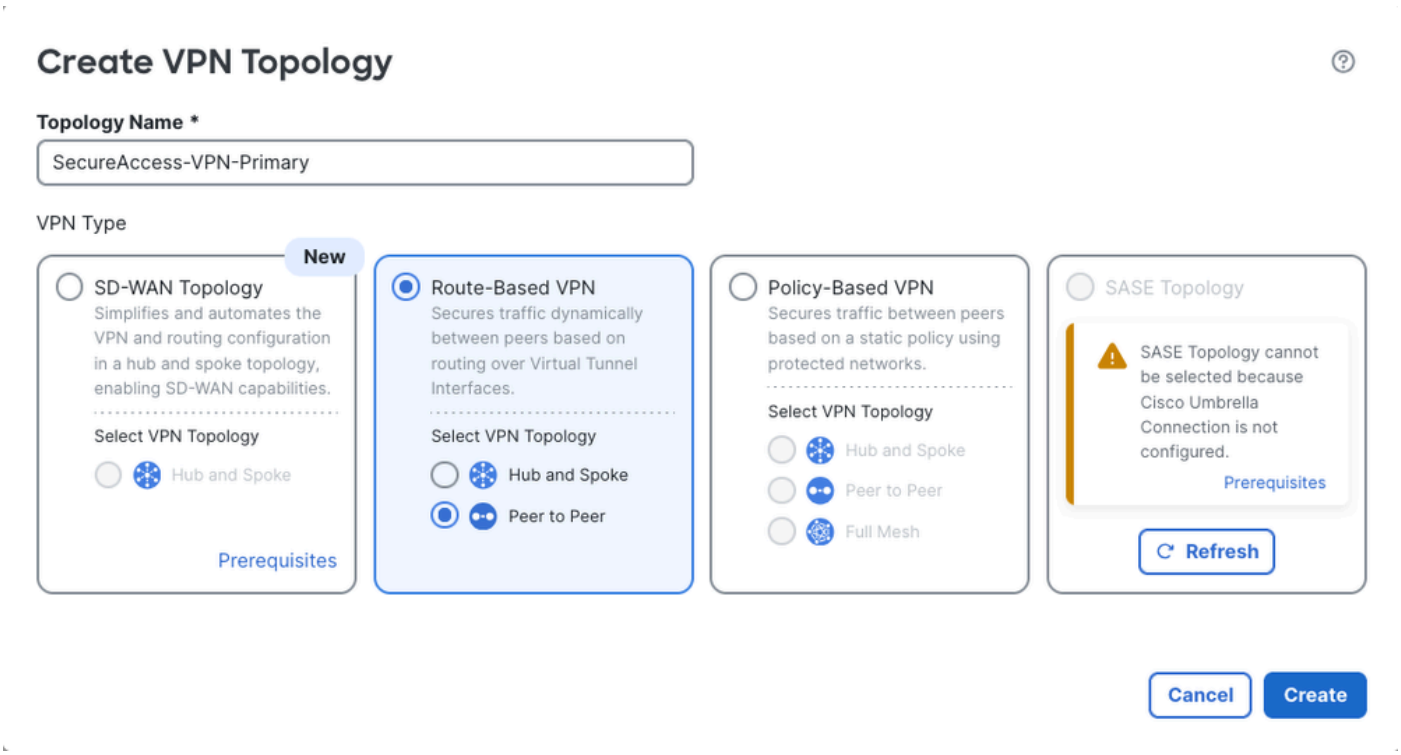
- セキュアアクセスを使用したセカンダリIPsec VPNに対してもVTI-2を設定します。



3. Secure Connections > Site-to-Site VPN & SD-WANの順に移動し、Addをクリックして VPNを設定します

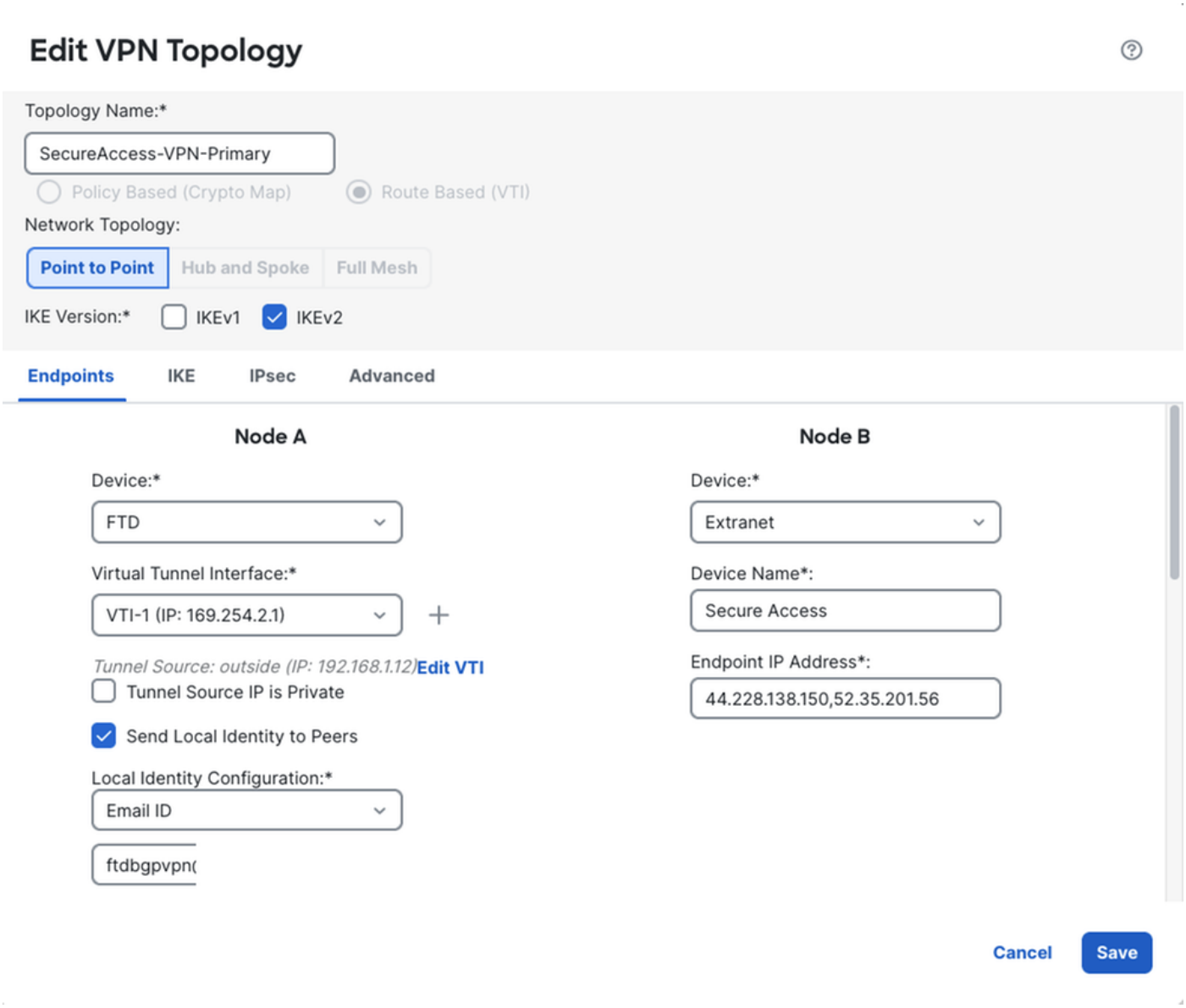


- VPNトポロジの作成

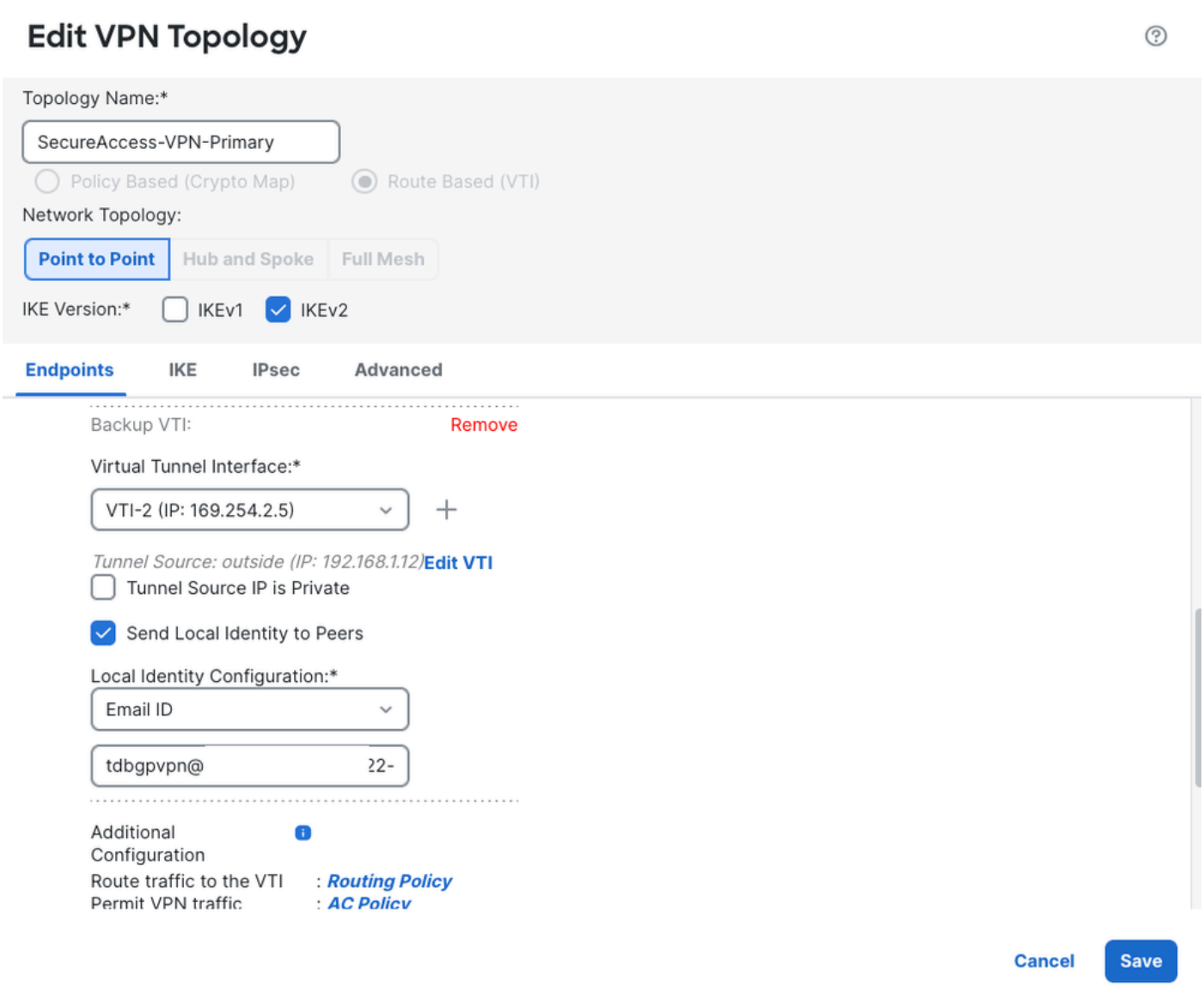


- 「セキュアアクセスでのネットワークトンネルグループの設定」のステップ6で、プライマ

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。
- エンドポイントをクリック
- ノードAでDevice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、プライマリトンネルIDを入力します（Secure AccessのConfigure Network Tunnel Groupの下の「Save Network Tunnel Group Configuration」のセクションを参照）。
- ノードBでDeviceをクリックし、Extranetを選択します
- Device Nameをクリックして、名前を付けます
- Endpoint 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Configure Network Tunnel Groupの下のSave Network Tunnel Group Configurationから）
- Add Backup VTIをクリックします。
- Virtual Tunnel Interfaceをクリックし、前の手順で作成した2番目のVTIインターフェイスを選択します
- Send Local Identity to Peersオプションをクリックして、Email IDを選択し、セカンダリトンネルIDを入力します（「Configure Network Tunnel Group on Secure Access」の「Save Network Tunnel Group Configuration」の下）
- [Save] をクリックします。

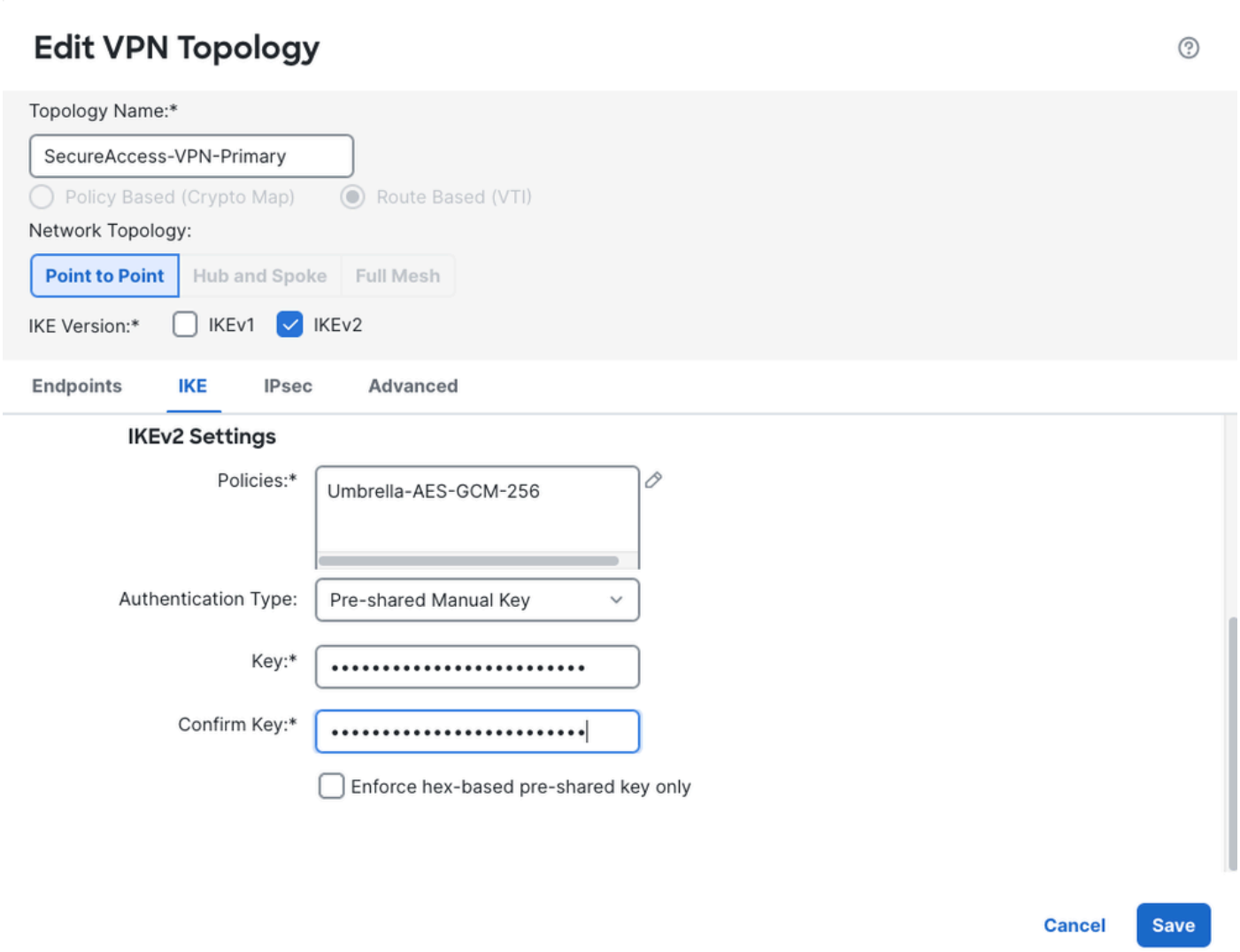


セキュアFTD:VPNエンドポイントの設定



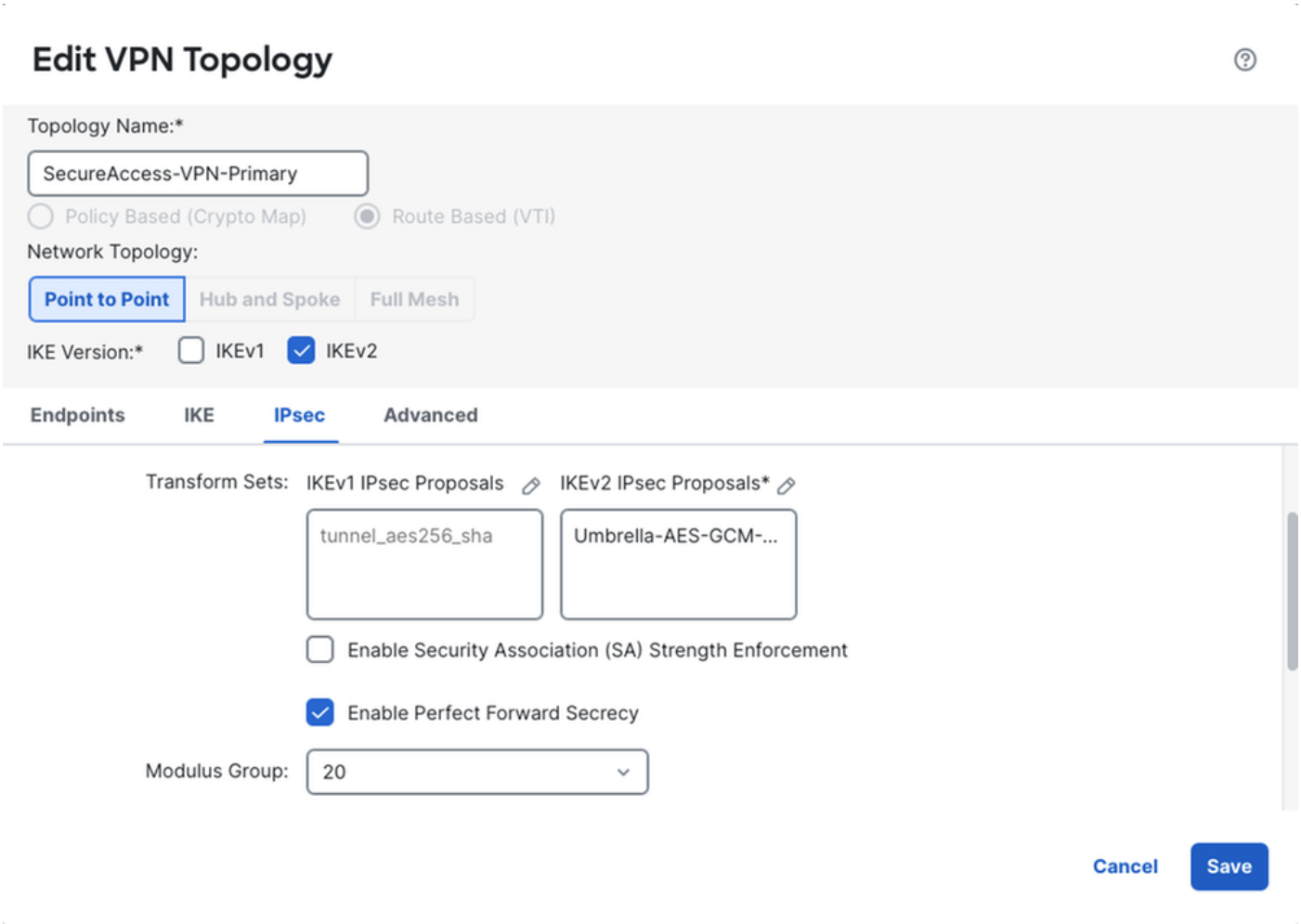
セキュアFTD:VPNエンドポイントの設定

- サポートされているIPsecパラメータに従ったIKEv2設定
  - ポリシーとしてUmbrella-AES-GCM-256を選択します。
  - 認証タイプとしてPre-Shared Manual Keyを選択します。



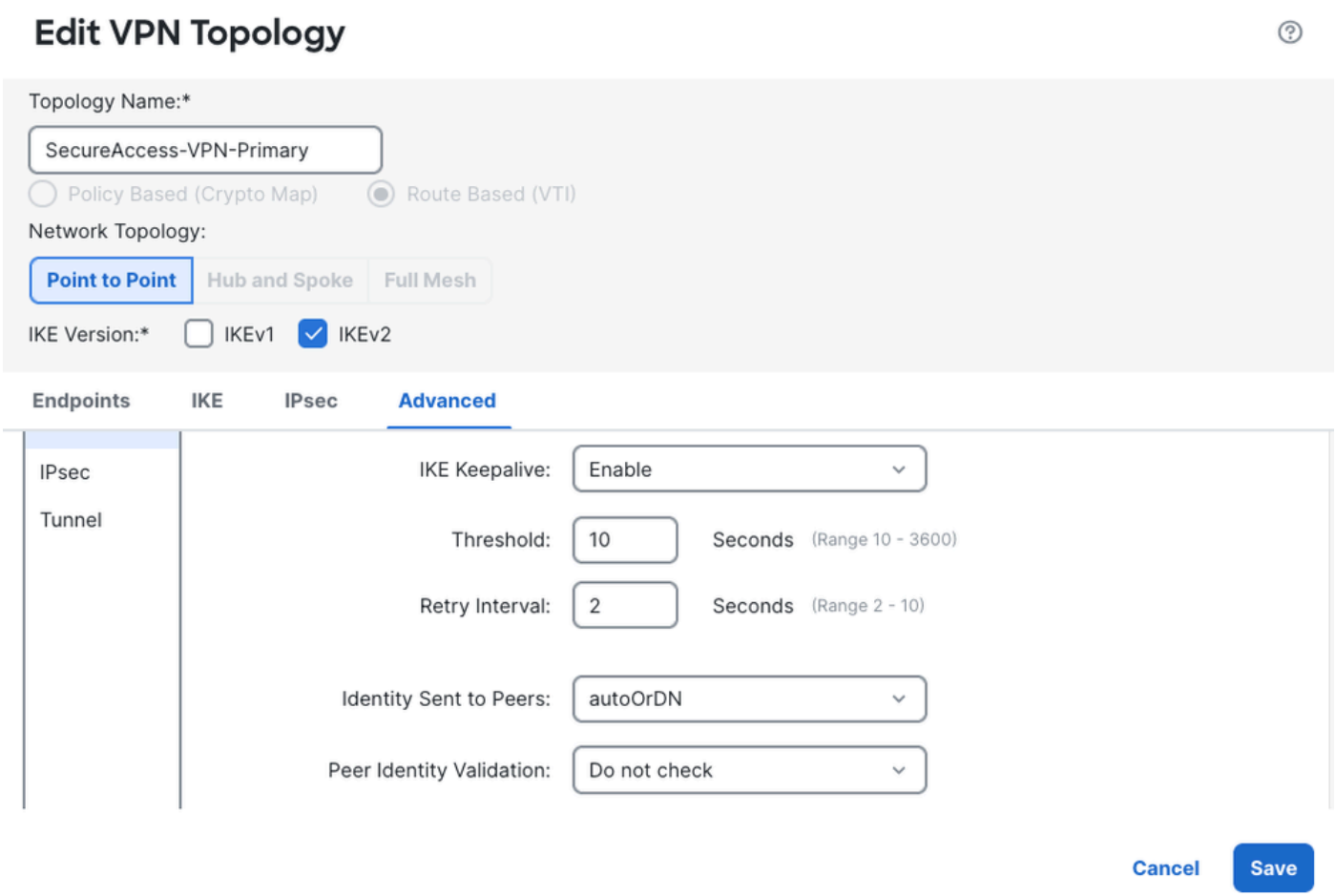
セキュアFTD:VPN IKEの設定

- IPSecの設定
  - IKEv2 IPsec Proposals as Umbrella-AES-GCM-256を選択します
  - select Modulus GroupとしてPFSを20に有効化



セキュアFTD:VPN IPsecの設定

- 高度な設定
- [Save] をクリックします。



セキュアFTD:VPNの詳細設定

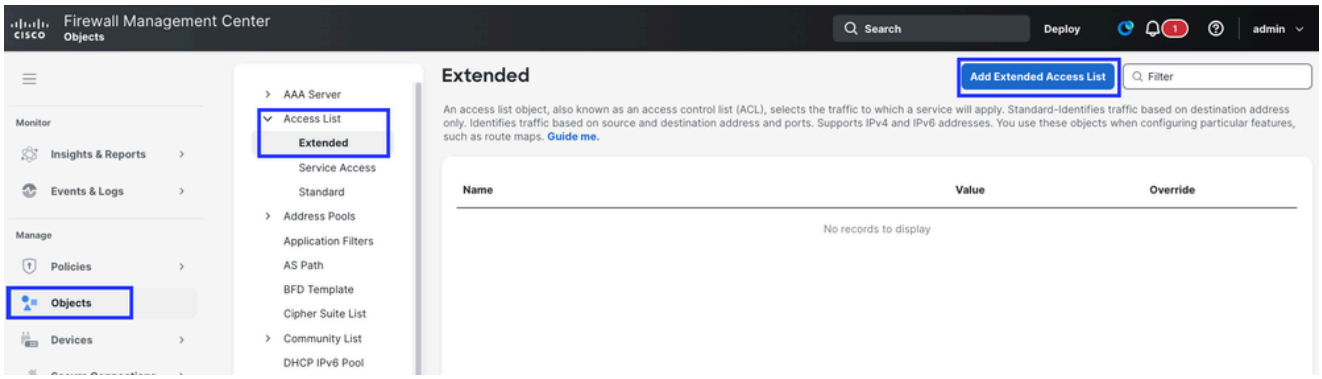
FTDポリシーベースルーティング

従来のルーティングでは、パケットは宛先IPアドレスに基づいてルーティングされます。宛先ベースのルーティングシステムで特定のトラフィックのルーティングを変更することは困難です。ポリシーベースルーティング(PBR)は、ルーティングプロトコルによって提供されるメカニズムを拡張および補完し、ルーティングをより詳細に制御できるようにします。

PBRでは、IP優先順位を設定できます。また、高コストリンク上のプライオリティトラフィックなど、特定のトラフィックのパスを指定することもできます。PBRを使用すると、送信元ポート、宛先アドレス、宛先ポート、プロトコル、アプリケーション、またはこれらのオブジェクトの組み合わせなど、宛先ネットワーク以外の基準に基づいてルーティングを定義できます。詳細については、『ポリシーベースルーティング(PBR)』を参照してください。

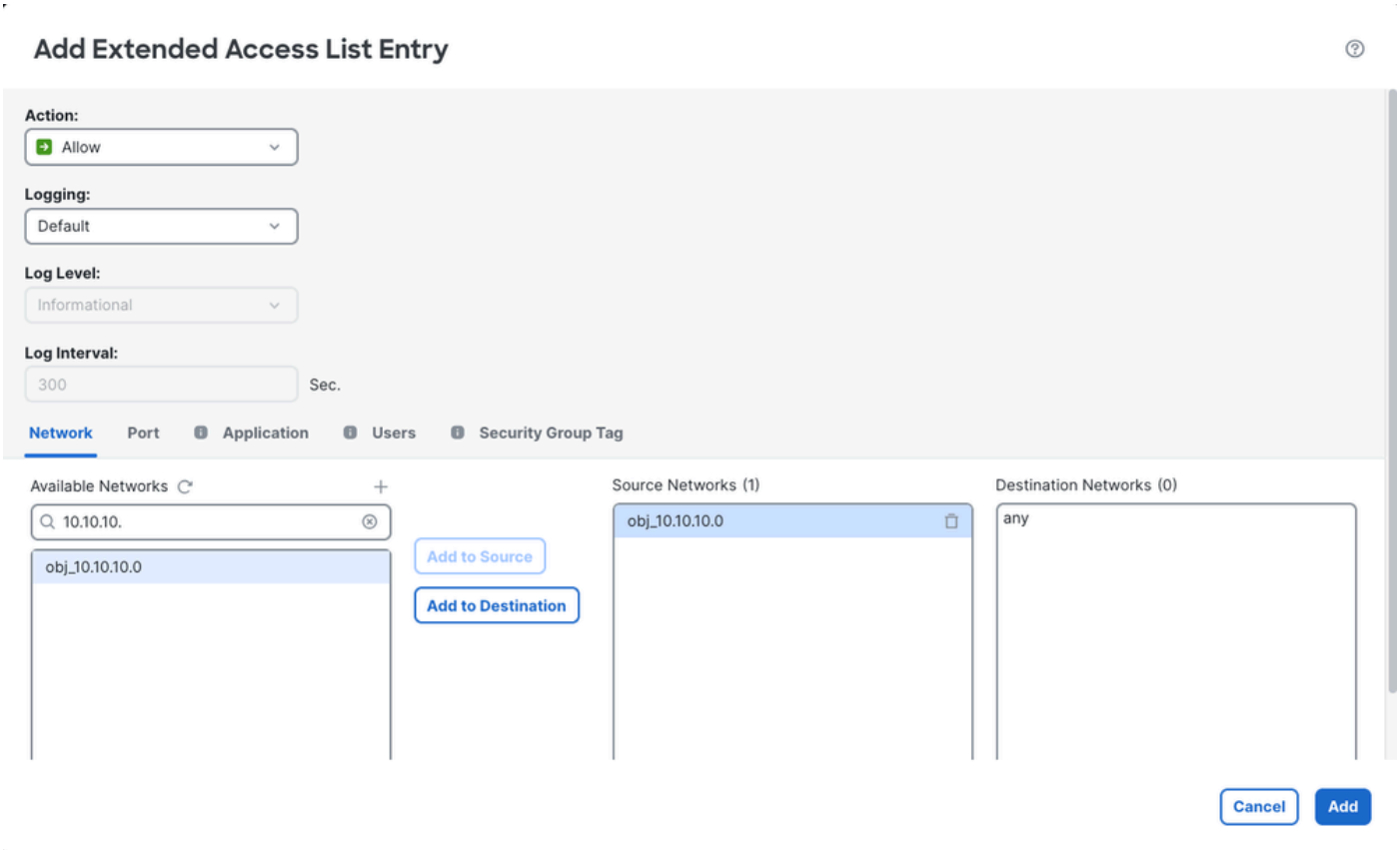
1. アクセスリストの設定

- Objects > Access List > Extendedの順に移動します。
- Add Extended Access Listをクリックします。

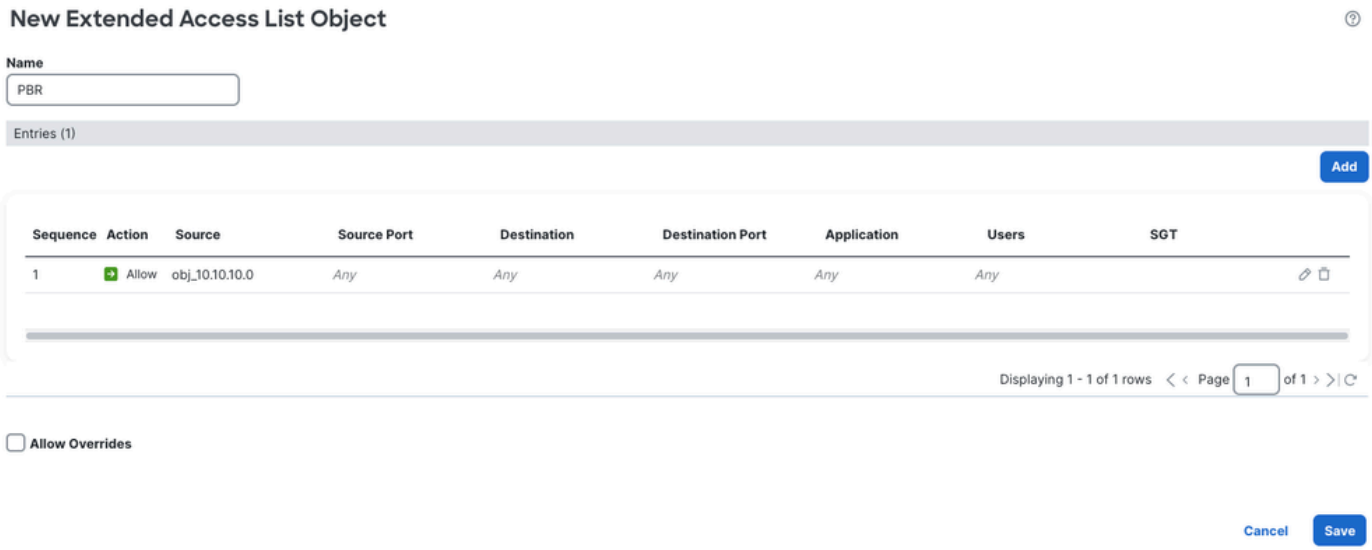


セキュアFTD：拡張アクセスリスト

- アクセスリスト名の指定
- アクションの定義
  - allow です。 – 定義されたトラフィックはIPSecトンネルに送信されます
  - ブロック：トラフィックはIPSecトンネルからバイパスされる
  - ルールはシーケンス番号に基づいて照合される（下位から上位）
  - Addをクリックします。
  - [Save] をクリックします。



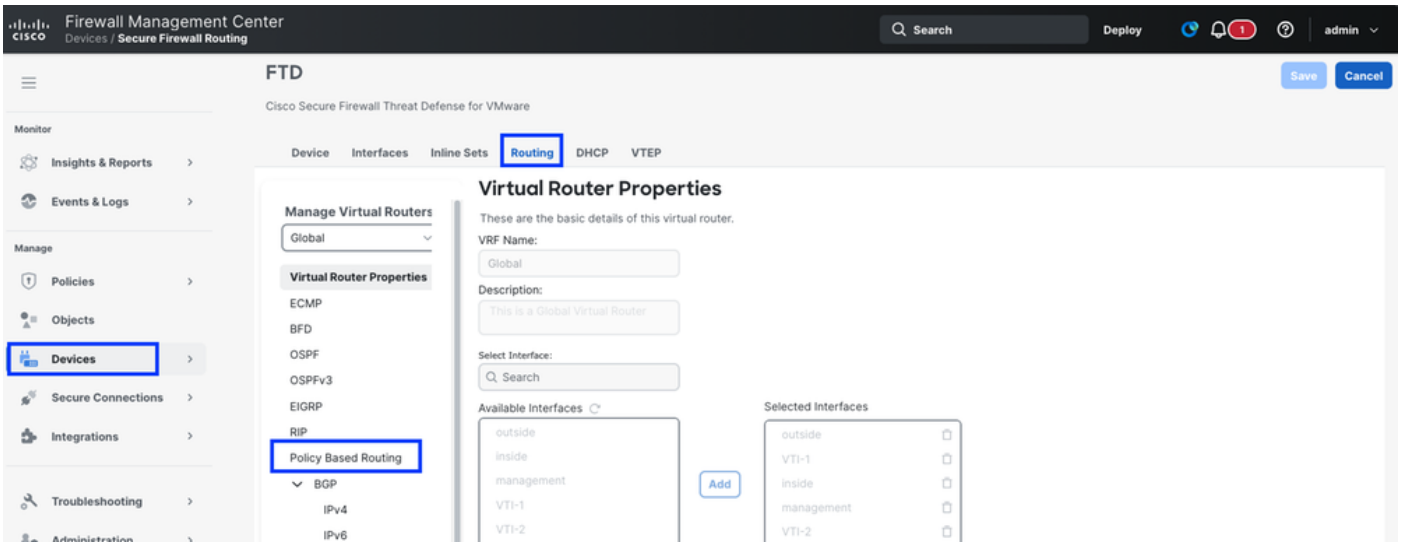
セキュアFTD：拡張アクセスリスト



セキュアFTD：拡張アクセスリスト

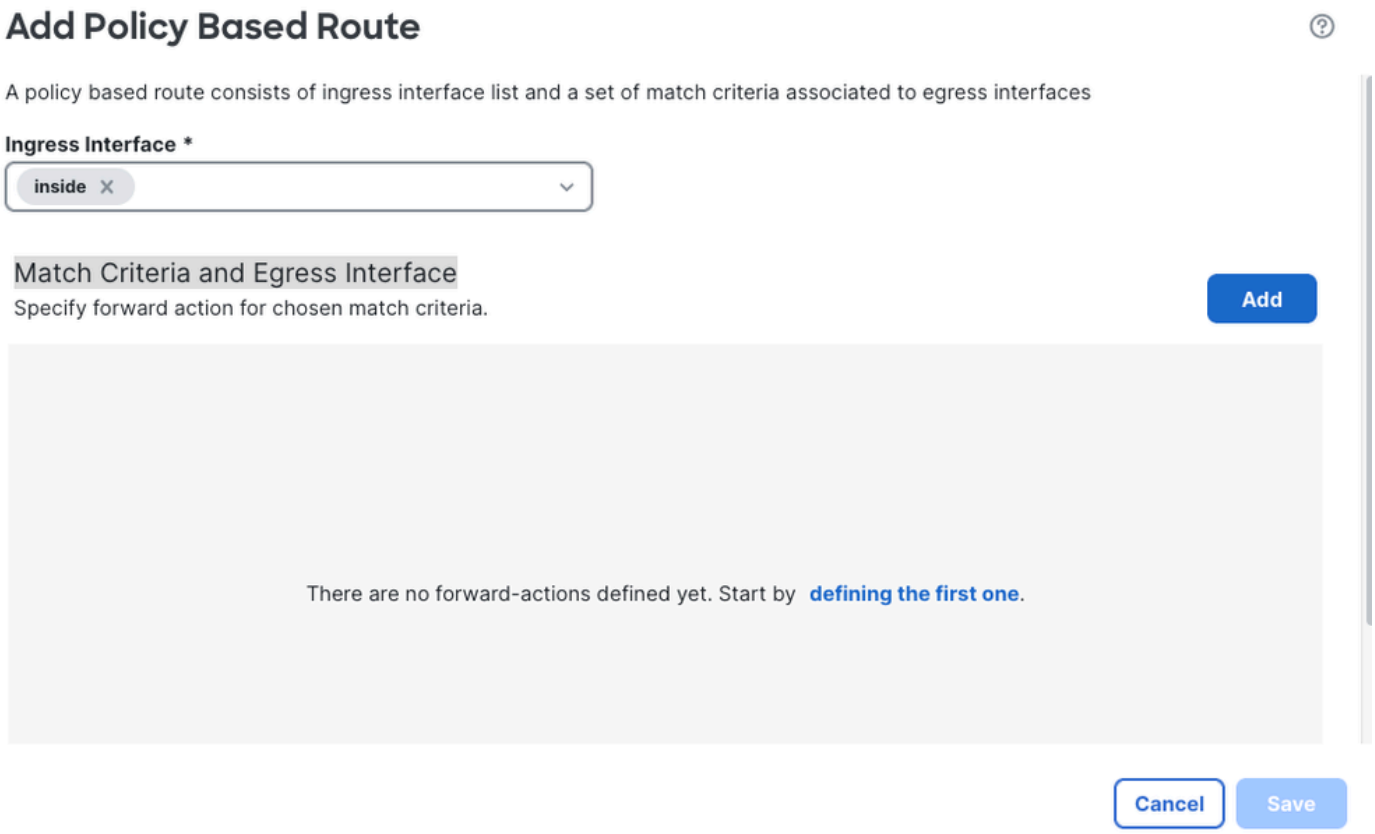
2. ポリシーベースルーティングの設定

- Devices > Device Management > FTD > Routingの順に移動します。



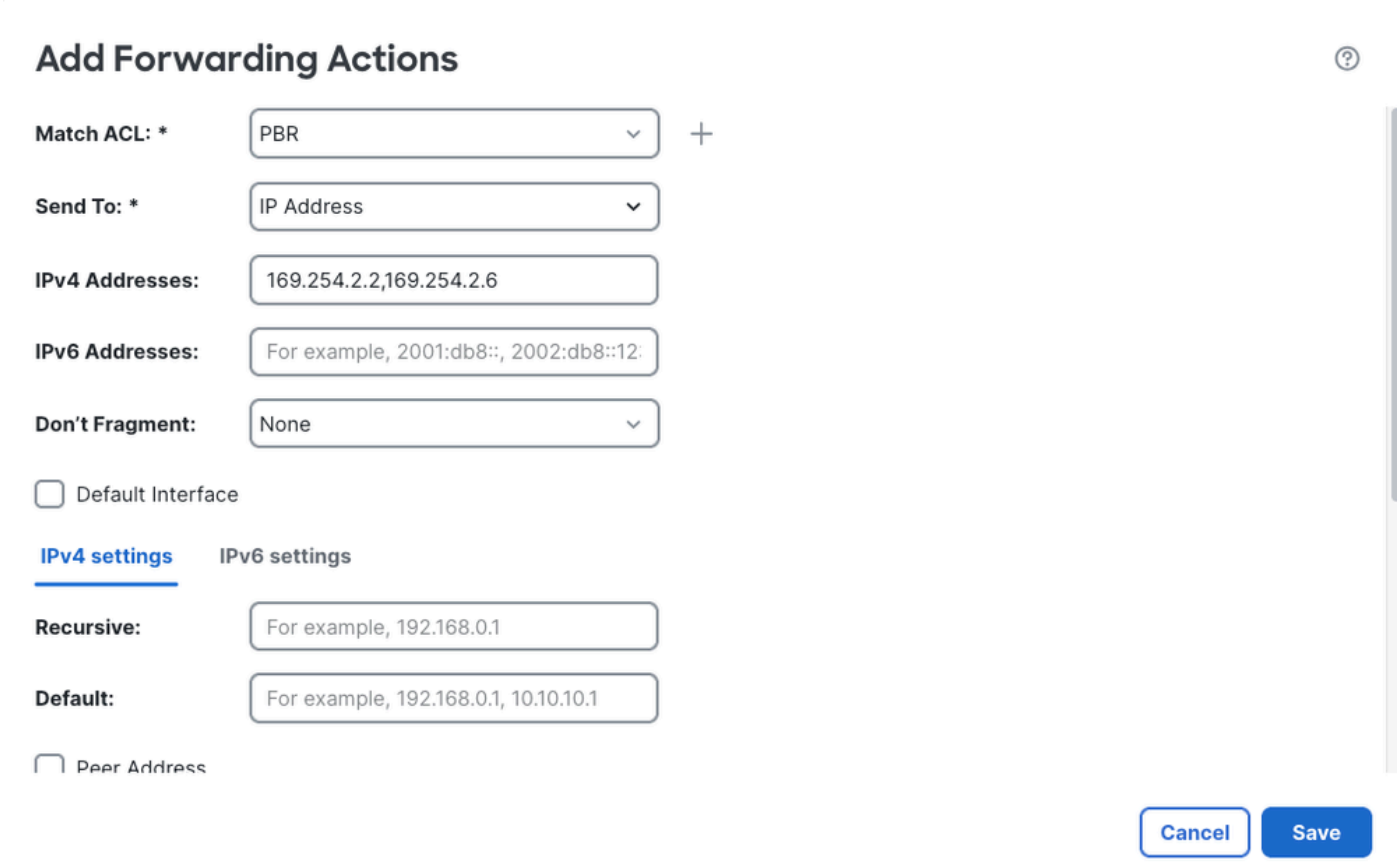
セキュアなFTD：ポリシーベースルーティング

- Addをクリックします。
- Ingress Interfaceの選択：アクセスリストで定義したサブネットの入力インターフェイス

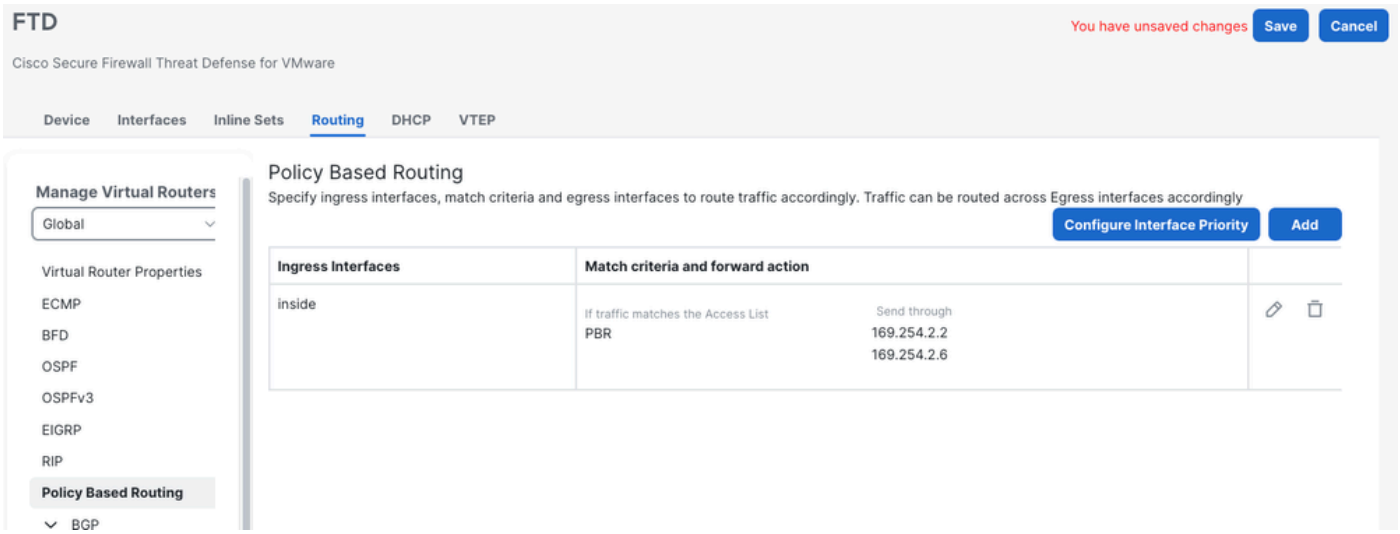


セキュアなFTD：ポリシーベースルーティング

- 一致基準と出力インターフェイスの定義
  - Addをクリックします。
  - Match ACLを選択します。
  - IPアドレスとしてSend toを選択します。
  - ネクストホップIPアドレスを追加します。- VTIインターフェイスのIPアドレスはです。169.254.2.130および169.254.2.5/30.したがって、VTI-1とVTI-2のネクストホップIPアドレスは169.254.2.2であり、それぞれ169.254.2.6
  - [Save] をクリックします。



セキュアなFTD：ポリシーベースルーティング

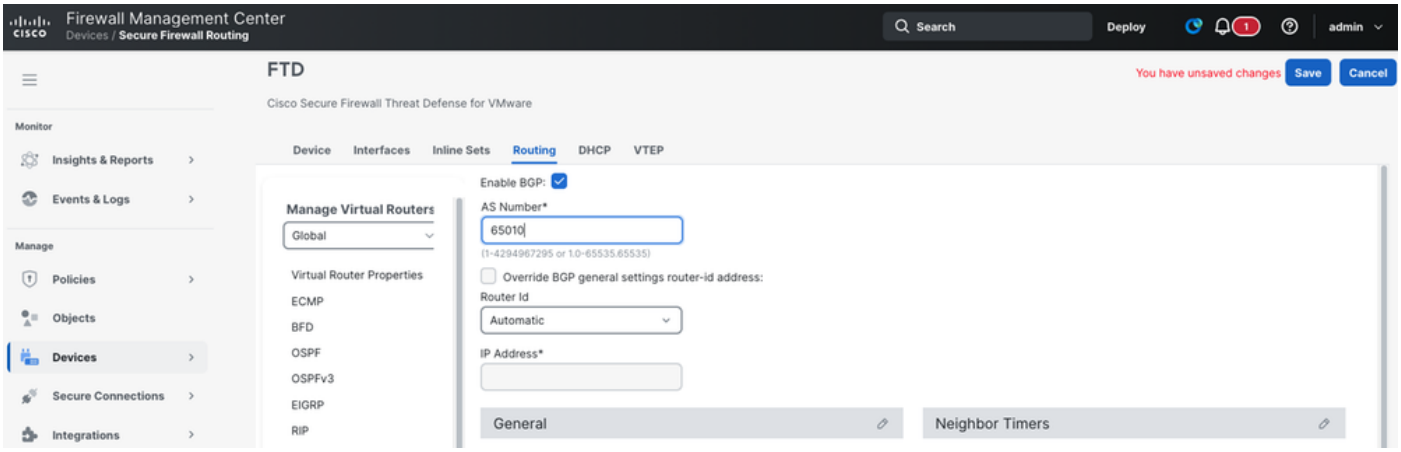


セキュアなFTD：ポリシーベースルーティング

FTDでのBGPの設定

1. BGPの有効化

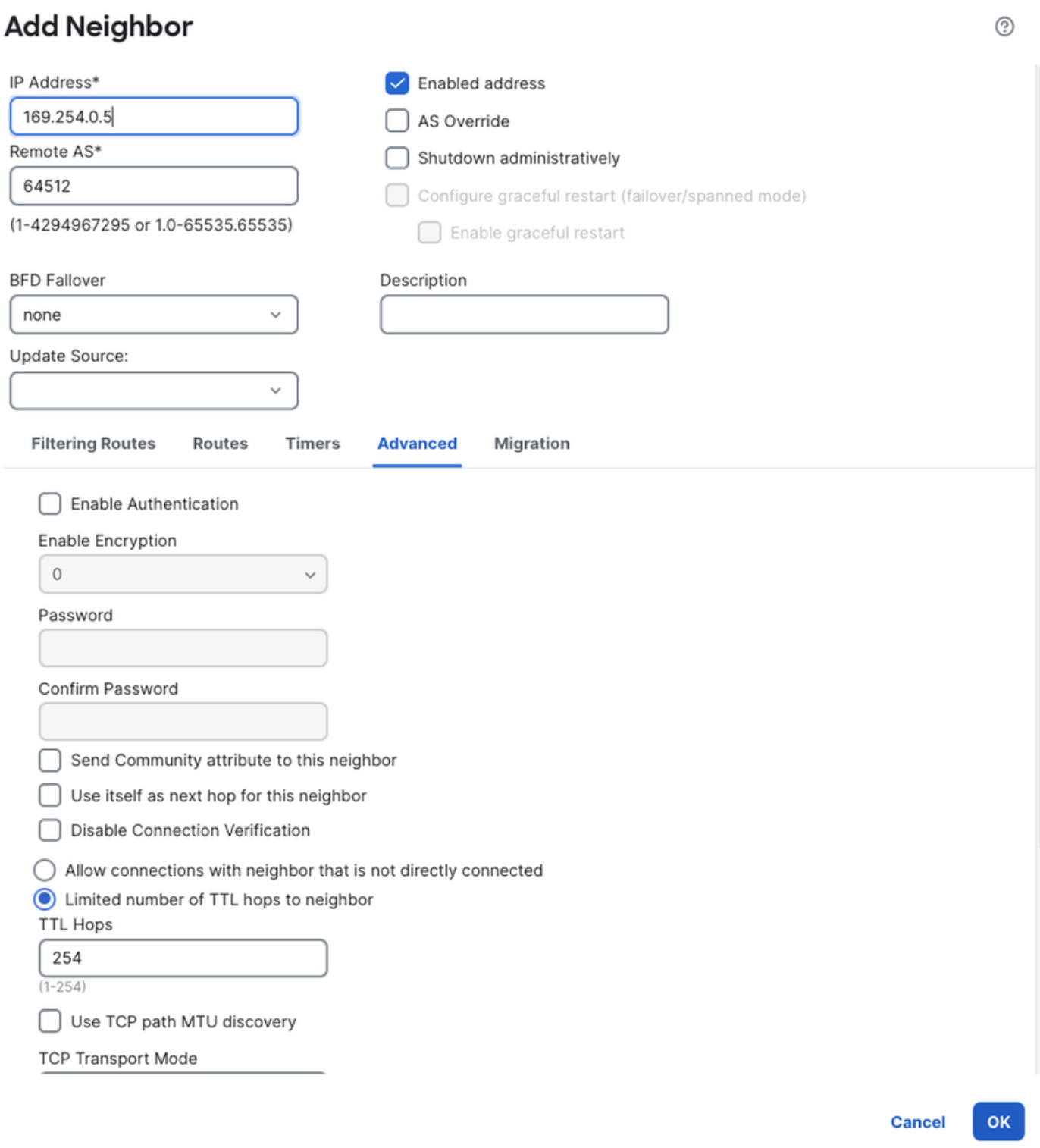
- Devices > Device Management > FTD > Routing > General Settings > BGPの順に移動します。
- BGPを有効にし、AS番号（FTDローカルAS番号）を追加します。
- [Save] をクリックします。



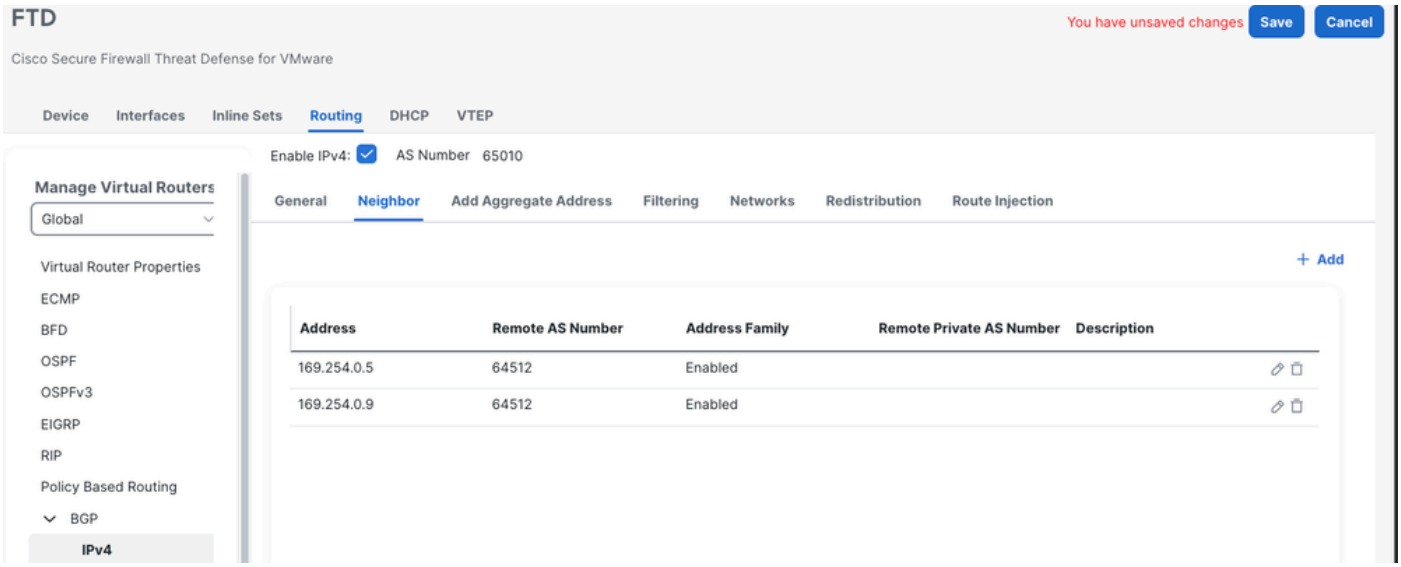
セキュアFTD:BGPルーティング

- BGP > IPv4の順に移動します。

2. BGP ネイバーを追加します。セキュアアクセスBGPピアは169.254.0.5およびです。169.254.0.9



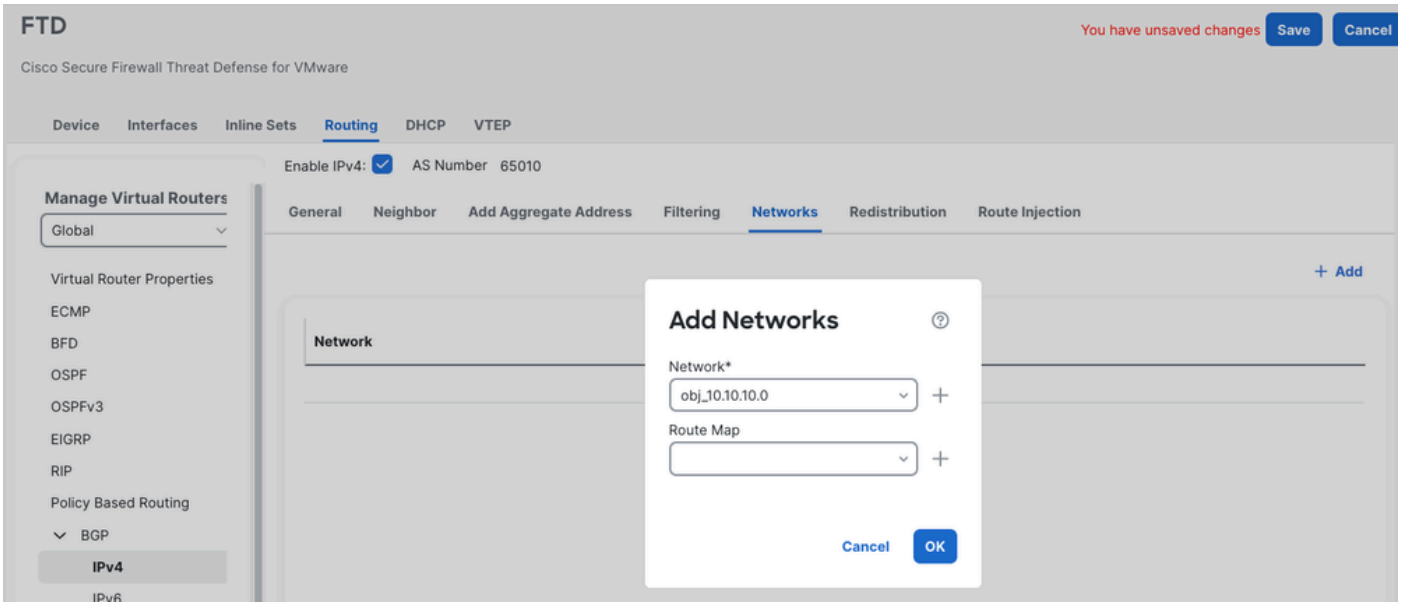
セキュアFTD:BGPルーティング



セキュアFTD:BGPルーティング

3. ネットワークを追加する – アクセスを保護するためにアドバタイズする必要があるネットワーク

- [OK] をクリックします。

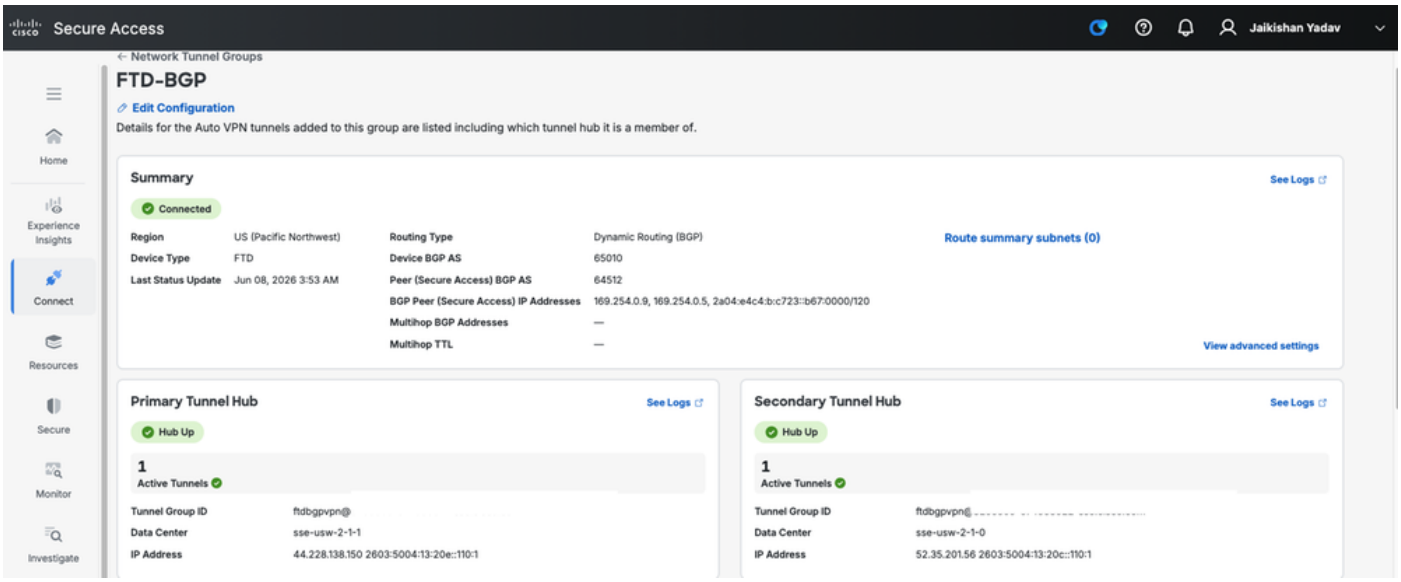


セキュアFTD:BGPルーティング

- 変更を保存して展開する

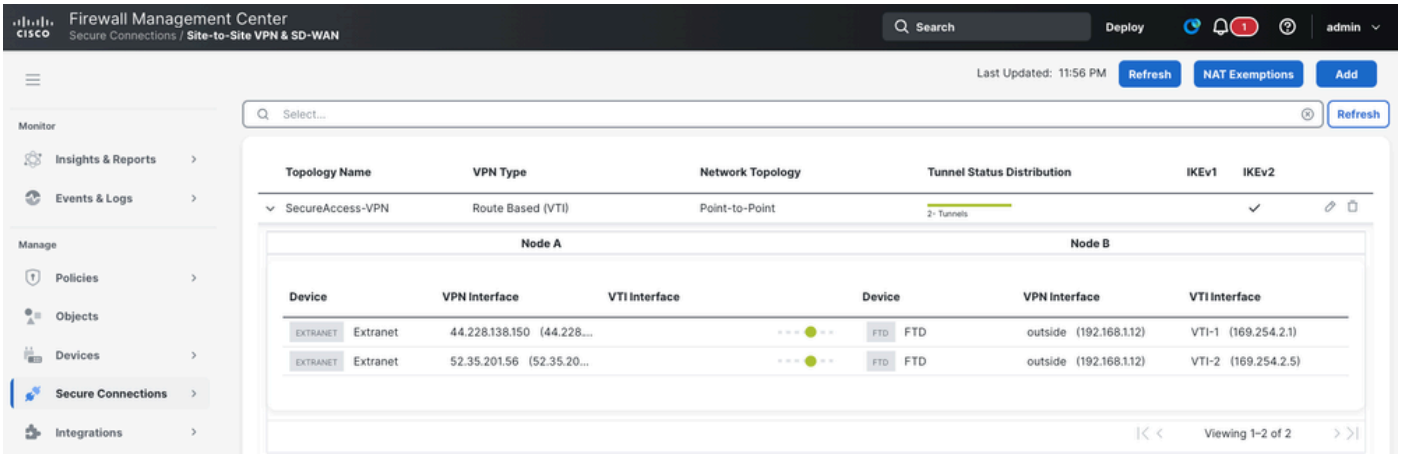
トンネルステータスの確認

セキュアアクセス



セキュアFTD:IPsecトンネルステータス

FMC上



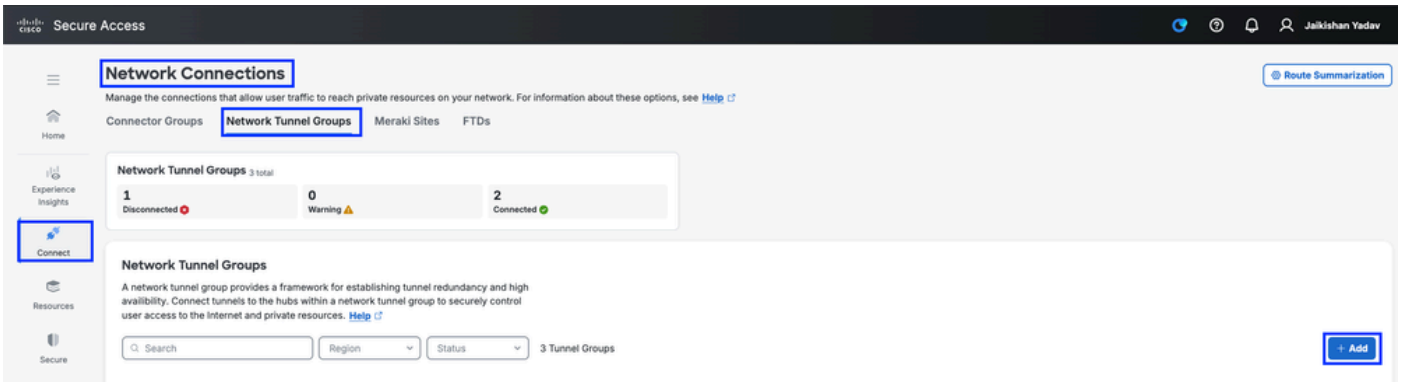
セキュアFMC:IPSecトンネルステータス

PBRを使用した適応型セキュリティアプライアンス(ASA)でのスタティックルートベースIPsec VPNの設定

セキュアアクセスでのVPN設定

1.セキュアアクセスダッシュボードへのログイン[セキュアアクセス]
2. Connect > Network Connections > Network Tunnel Groupsの順に移動し、+Addをクリックして

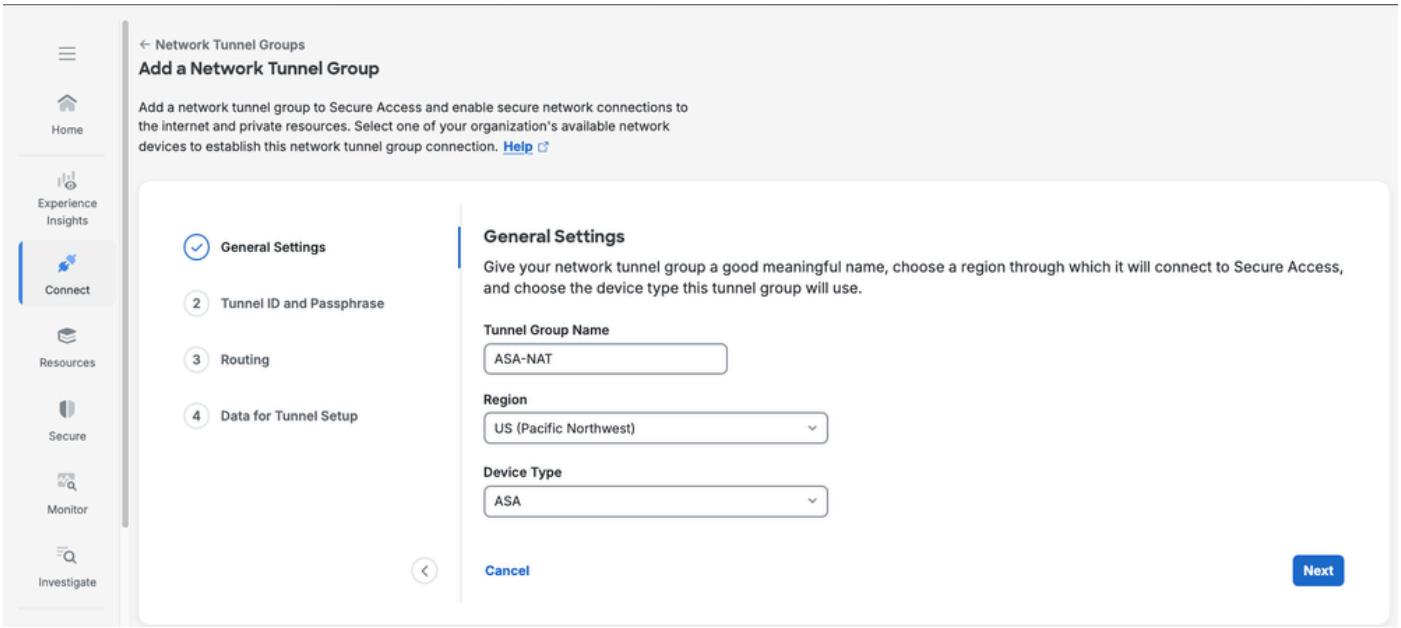
ネットワークトンネルグループを設定します



セキュアアクセス – ネットワークトンネルグループ

3.ネットワークトンネルグループの構成 – 一般設定

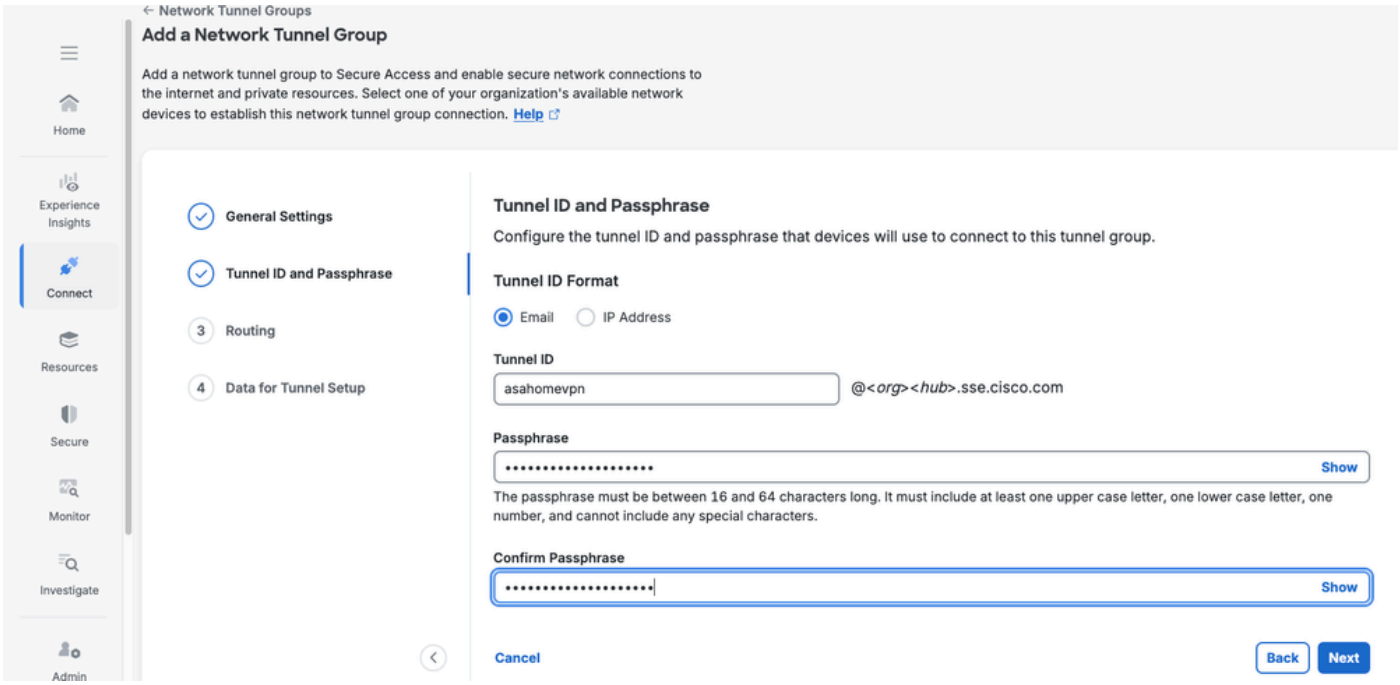
- トンネルグループの名前、リージョン、およびデバイスタイプの設定
- [Next] をクリックします。



セキュアアクセス – ネットワークトンネルグループの一般設定

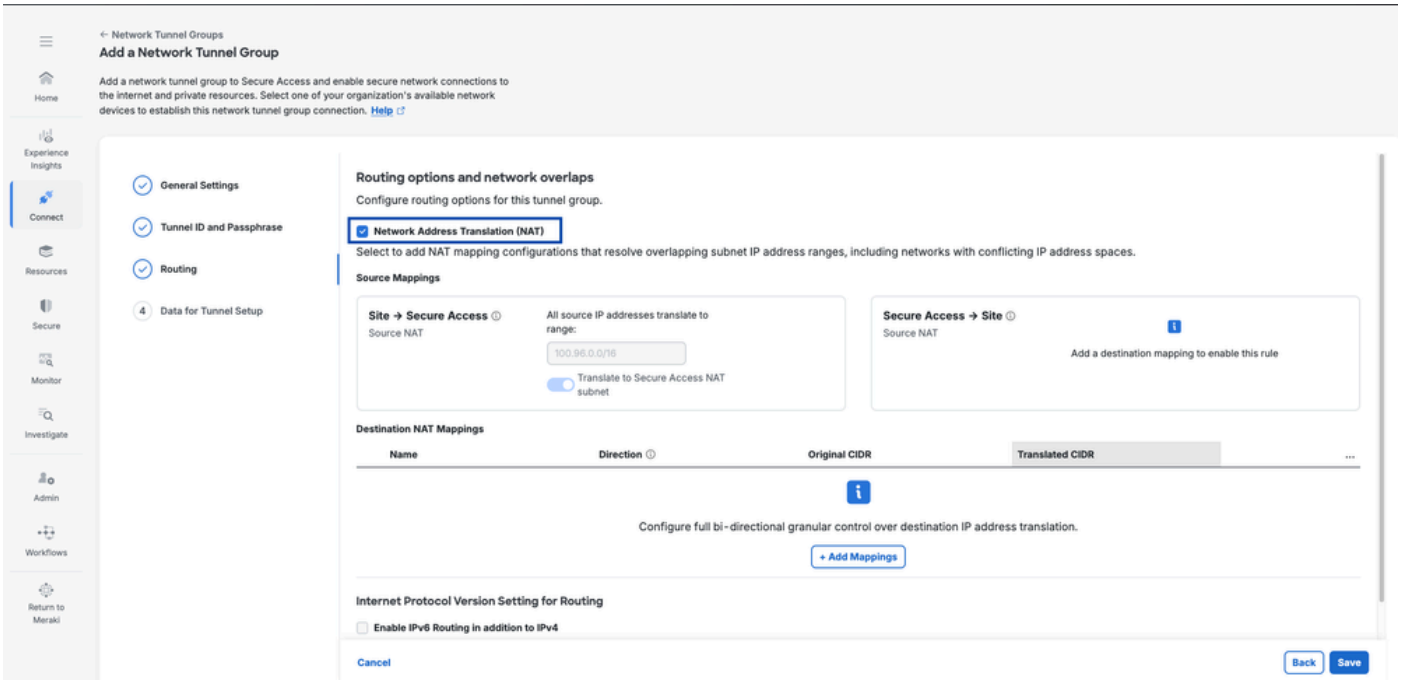
4.トンネルIDとパスフレーズを設定します。

- トンネルIDとパスフレーズを設定します。
- Next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

5. ネットワークアドレス変換(NAT)の有効化

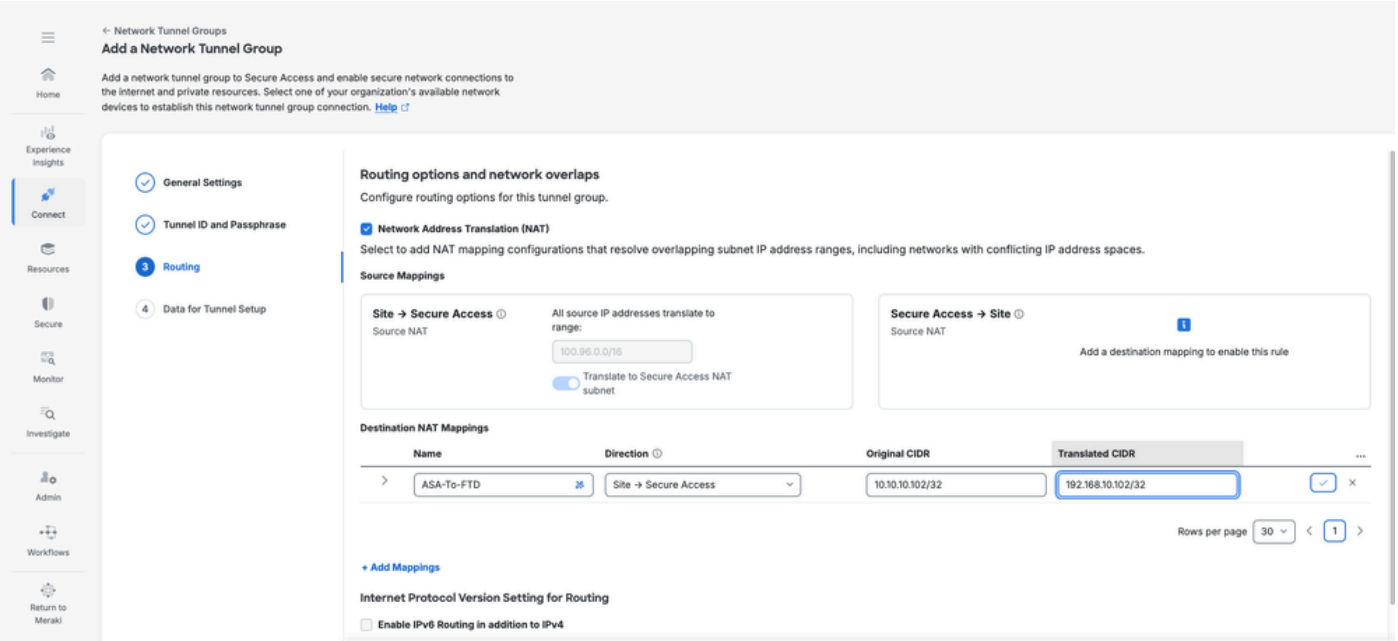


セキュアアクセス – ネットワークトンネルグループのNAT設定

6. 宛先NATマッピングの追加

フロー1：ルータ1からルータ2（アクセスを保護するサイト）

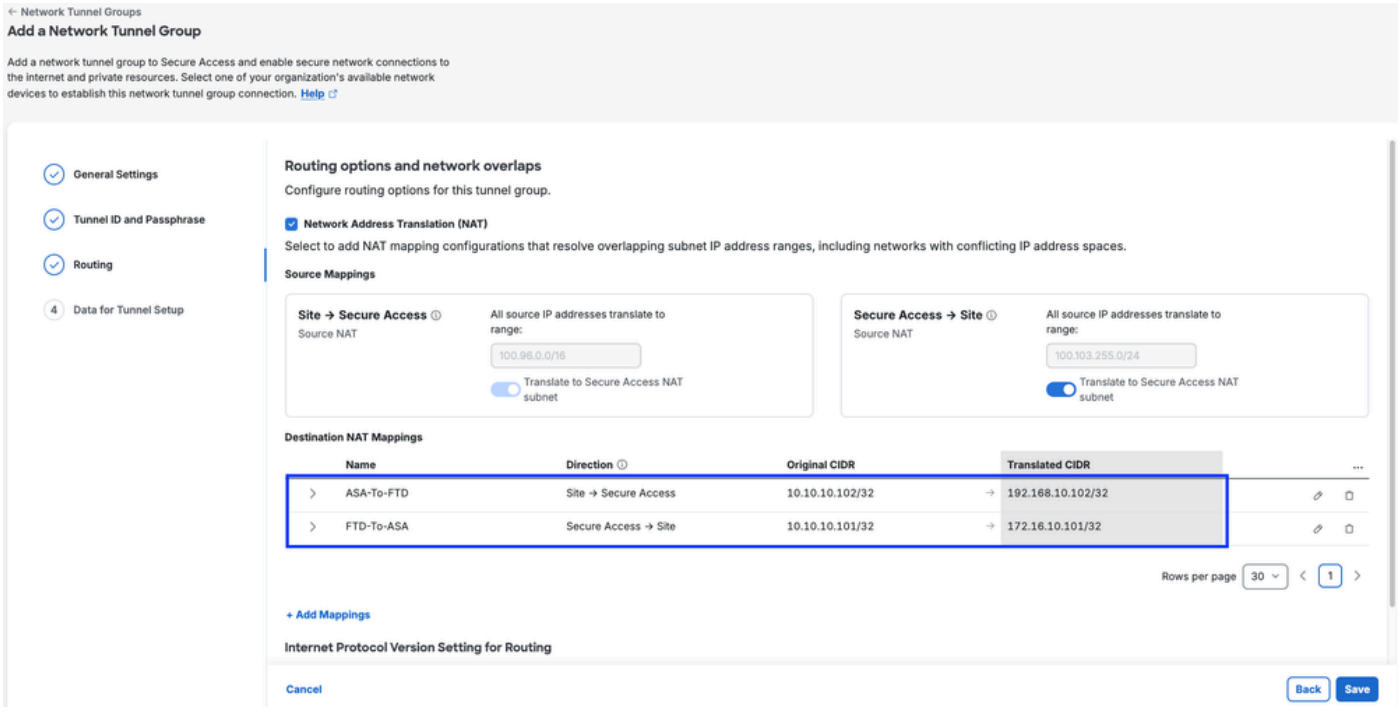
フロー2 – ルータ2からルータ1（サイトへのセキュアなアクセス）



セキュアアクセス – ネットワークトンネルグループのNAT設定

注意:NATが有効な場合、BGPは使用できません（BGPが有効な場合）。また、カスタマーエッジデバイスでもスタティックVPNを設定します

ヒント：常に、変換されたIP（宛先IP）に対してpingを実行することを忘れないでください。
変換後のIPは変換後のCIDRに配置され、実際のIPは元のCIDRに配置されます。



セキュアアクセス – ネットワークトンネルグループのNAT設定

クリック 保存します。

ヒント:「サイトA」から「サイトB」に送信されるトラフィックの場合、CNHE-1の観点から見た方向は「サイト – >セキュアアクセス」です。
「サイトB」から「サイトA」に送信されるトラフィックの場合、CNHE-1の観点から見ると、方向は「SecureAccess -> Site」です。

ASAでのVPNの設定

1. ASA CLIにログインし、イネーブルモードに入り、インターネットへの基本的なIP接続を確認します

ASA# sh ip
システムIPアドレス：
インターフェイス名IPアドレスサブネットマスク方式
GigabitEthernet0/0 outside 192.168.1.40 255.255.255.0マニュアル
10.10.10.1 255.255.255.0マニュアル内のGigabitEthernet0/1

現在のIPアドレス：
インターフェイス名IPアドレスサブネットマスク方式
GigabitEthernet0/0 outside 192.168.1.40 255.255.255.0マニュアル

10.10.10.1 255.255.255.0マニュアル内のGigabitEthernet0/1

ASA# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/28/30 ms
ASA番号

2. IKEv2ポリシーを設定し、外部インターフェイスでIKEv2を有効にします

クリプトikev2ポリシー10
暗号化aes-gcm-256
整合性　　NULL
group 19
ライフタイム秒数86400
crypto ikev2 enable outside

3. IPSecプロポーザルの設定

crypto ipsec ikev2 ipsec-proposal Ipsec-Proposal-primary
protocol esp encryption aes-gcm-256

4. IPsecプロファイルの設定

crypto ipsec profile csa-profile-primary（暗号化IPSecプロファイルのCSAプロファイルのプライマリ）
set ikev2 ipsec-proposal Ipsec-Proposal-primary
set ikev2 local-identity email-id <primary tunnel-id>

5. グループポリシーを設定し、attributeでIKEv2プロトコルを有効にします。

group-policy csa-policy-primary internalコマンド
group-policy csa-policy-primary属性
vpn-tunnel-protocol ikev2

6. トンネルグループを設定します。

tunnel-group 44.228.138.150 type ipsec-l2l
tunnel-group 44.228.138.150一般属性

デフォルト：グループポリシーcsa-policy-primary
tunnel-group 44.228.138.150 ipsec属性
ikev2 remote-authentication pre-shared-key <事前共有キー>
ikev2 local-authentication pre-shared-key <事前共有キー>

7. 仮想トンネルインターフェイス(VTI)の設定

- Nameifは任意の場合に使用できます
- VTIに割り当てられたIPアドレスがASAの他のインターフェイスと重複しないようにしてください
- Tunnel sourcemustbe：ファイアウォールのOutsideインターフェイス。
- トンネルの宛先は、データセンターのIPアドレスである必要があります

interface Tunnel1
nameif VTI-1
ip address 169.254.2.1 255.255.255.252
トンネル送信元インターフェイス外部
トンネルの宛先44.228.138.150
トンネルモードipsec ipv4
トンネル保護ipsecプロファイルcsa-profile-primary

8. マッピングされたIPアドレスまたはサブネットへのトラフィックがVTIインターフェイス内でルーティングされるようにルーティングを設定します。ネクストホップは、VTIの範囲内のIPを使用する必要があります。

route VTI-1 0.0.0.0 0.0.0.0 169.254.2.2 5.(インターネットベースの場合、RAVPNプールまたはCGNATトラフィック

または

ルートVTI-1 172.16.10.101 255.255.255.255 169.254.2.2 5

ポリシーベースルーティング

1. アクセスリスト

access-list PBR extended permit ip 10.10.10.0 255.255.255.0 any

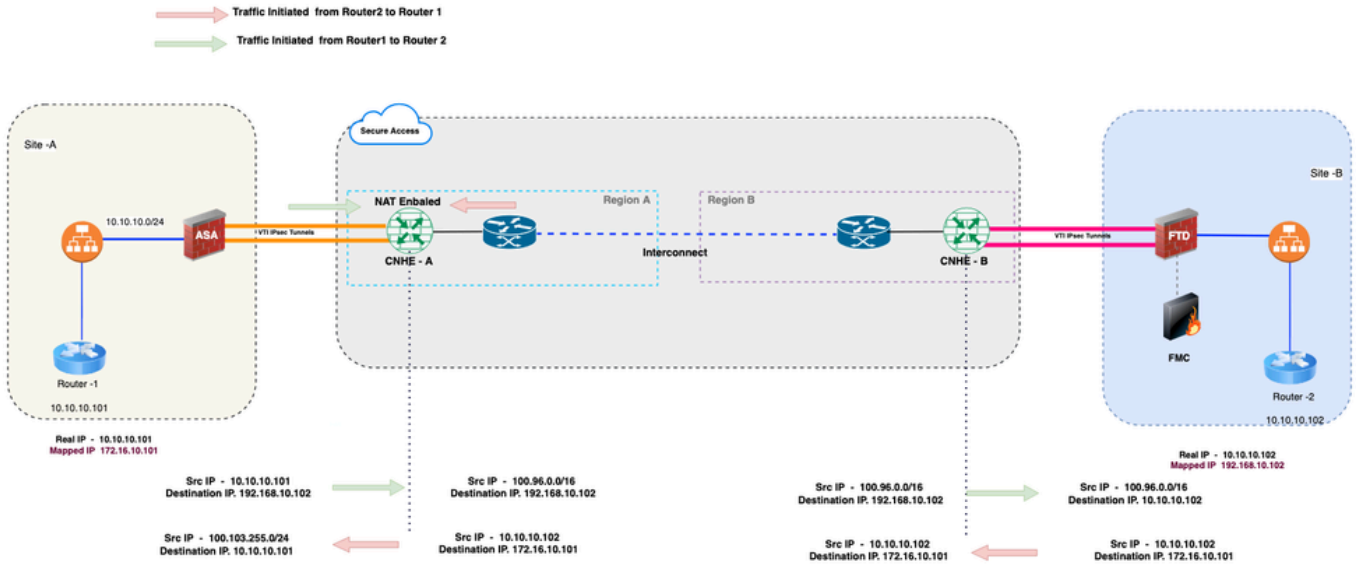
2. ルートマップ

route-map RM-CSA permit 10
IPアドレスPBRの照合
set ip next-hop 169.254.2.2 169.254.2.6

3. 入力インターフェイスでルートマップを適用します。

interface GigabitEthernet0/1
nameif内部
セキュリティレベル100
ip address 10.10.10.1 255.255.255.0
policy-route route-map RM-CSA（使用可能な場合）

確認



ルータインターフェイスおよびGW到達可能性ステータス

```
Router1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       192.168.1.101   YES NVRAM  down                  down
GigabitEthernet2       10.10.10.101    YES NVRAM  up                    up
GigabitEthernet3       unassigned      YES NVRAM  administratively down down
GigabitEthernet9       unassigned      YES unset  administratively down down
Router1#ping  10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

テスト1- Router2 —> Router1。-ping テスト

```
Router1#ping 192.168.10.102
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.102, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 207/211/223 ms
Router1#
```

ASAでのパケットキャプチャ（ローカルFW）

```
ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA#
ASA#
ASA# ter pag 20
ASA# sh cap capin

10 packets captured

   1: 10:56:45.024244       10.10.10.101 > 192.168.10.102 icmp: echo request
   2: 10:56:45.231143       192.168.10.102 > 10.10.10.101 icmp: echo reply
   3: 10:56:45.232470       10.10.10.101 > 192.168.10.102 icmp: echo request
   4: 10:56:45.441856       192.168.10.102 > 10.10.10.101 icmp: echo reply
   5: 10:56:45.443122       10.10.10.101 > 192.168.10.102 icmp: echo request
   6: 10:56:45.652477       192.168.10.102 > 10.10.10.101 icmp: echo reply
   7: 10:56:45.653423       10.10.10.101 > 192.168.10.102 icmp: echo request
   8: 10:56:45.875397       192.168.10.102 > 10.10.10.101 icmp: echo reply
   9: 10:56:45.876450       10.10.10.101 > 192.168.10.102 icmp: echo request
  10: 10:56:46.082301       192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

   1: 10:56:45.024458       10.10.10.101 > 192.168.10.102 icmp: echo request
   2: 10:56:45.230914       192.168.10.102 > 10.10.10.101 icmp: echo reply
   3: 10:56:45.232516       10.10.10.101 > 192.168.10.102 icmp: echo request
   4: 10:56:45.441795       192.168.10.102 > 10.10.10.101 icmp: echo reply
   5: 10:56:45.443153       10.10.10.101 > 192.168.10.102 icmp: echo request
   6: 10:56:45.652432       192.168.10.102 > 10.10.10.101 icmp: echo reply
   7: 10:56:45.653454       10.10.10.101 > 192.168.10.102 icmp: echo request
   8: 10:56:45.875351       192.168.10.102 > 10.10.10.101 icmp: echo reply
   9: 10:56:45.876480       10.10.10.101 > 192.168.10.102 icmp: echo request
  10: 10:56:46.082240       192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
```

FTD（リモートFW）でのパケットキャプチャ

```
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd# sh cap vti

10 packets captured

   1: 16:06:41.122292       100.96.2.0 > 10.10.10.102 icmp: echo request
   2: 16:06:41.124856       10.10.10.102 > 100.96.2.0 icmp: echo reply
   3: 16:06:41.329557       100.96.2.0 > 10.10.10.102 icmp: echo request
   4: 16:06:41.330442       10.10.10.102 > 100.96.2.0 icmp: echo reply
   5: 16:06:41.546327       100.96.2.0 > 10.10.10.102 icmp: echo request
   6: 16:06:41.547106       10.10.10.102 > 100.96.2.0 icmp: echo reply
   7: 16:06:41.752036       100.96.2.0 > 10.10.10.102 icmp: echo request
   8: 16:06:41.752814       10.10.10.102 > 100.96.2.0 icmp: echo reply
   9: 16:06:41.967891       100.96.2.0 > 10.10.10.102 icmp: echo request
  10: 16:06:41.968501       10.10.10.102 > 100.96.2.0 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

   1: 16:06:41.123299       100.96.2.0 > 10.10.10.102 icmp: echo request
   2: 16:06:41.124825       10.10.10.102 > 100.96.2.0 icmp: echo reply
   3: 16:06:41.330000       100.96.2.0 > 10.10.10.102 icmp: echo request
   4: 16:06:41.330396       10.10.10.102 > 100.96.2.0 icmp: echo reply
   5: 16:06:41.546800       100.96.2.0 > 10.10.10.102 icmp: echo request
   6: 16:06:41.547090       10.10.10.102 > 100.96.2.0 icmp: echo reply
   7: 16:06:41.752448       100.96.2.0 > 10.10.10.102 icmp: echo request
   8: 16:06:41.752783       10.10.10.102 > 100.96.2.0 icmp: echo reply
   9: 16:06:41.968242       100.96.2.0 > 10.10.10.102 icmp: echo request
  10: 16:06:41.968486       10.10.10.102 > 100.96.2.0 icmp: echo reply
10 packets shown
```

テスト2. – ルータ2 —>ルータ1 pingテスト

```
Router2#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       unassigned      YES NVRAM  administratively down down
GigabitEthernet2       10.10.10.102    YES NVRAM  up                    up
GigabitEthernet3       unassigned      YES NVRAM  administratively down down
Router2#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

FTDパケットキャプチャ（ローカルFW）

```
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd#
ftd#
ftd#
ftd# sh cap vti

10 packets captured

   1: 16:11:45.622450       10.10.10.102 > 172.16.10.101 icmp: echo request
   2: 16:11:45.823825       172.16.10.101 > 10.10.10.102 icmp: echo reply
   3: 16:11:45.825762       10.10.10.102 > 172.16.10.101 icmp: echo request
   4: 16:11:46.045667       172.16.10.101 > 10.10.10.102 icmp: echo reply
   5: 16:11:46.046857       10.10.10.102 > 172.16.10.101 icmp: echo request
   6: 16:11:46.252321       172.16.10.101 > 10.10.10.102 icmp: echo reply
   7: 16:11:46.253572       10.10.10.102 > 172.16.10.101 icmp: echo request
   8: 16:11:46.453803       172.16.10.101 > 10.10.10.102 icmp: echo reply
   9: 16:11:46.454764       10.10.10.102 > 172.16.10.101 icmp: echo request
  10: 16:11:46.664119       172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

   1: 16:11:45.622083       10.10.10.102 > 172.16.10.101 icmp: echo request
   2: 16:11:45.823886       172.16.10.101 > 10.10.10.102 icmp: echo reply
   3: 16:11:45.825442       10.10.10.102 > 172.16.10.101 icmp: echo request
   4: 16:11:46.045697       172.16.10.101 > 10.10.10.102 icmp: echo reply
   5: 16:11:46.046582       10.10.10.102 > 172.16.10.101 icmp: echo request
   6: 16:11:46.252352       172.16.10.101 > 10.10.10.102 icmp: echo reply
   7: 16:11:46.253313       10.10.10.102 > 172.16.10.101 icmp: echo request
   8: 16:11:46.453849       172.16.10.101 > 10.10.10.102 icmp: echo reply
   9: 16:11:46.454596       10.10.10.102 > 172.16.10.101 icmp: echo request
  10: 16:11:46.664150       172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
```

ASAパケットキャプチャ（リモートFW）

```
ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA# sh cap capin

10 packets captured

   1: 11:08:30.288391       100.103.255.195 > 10.10.10.101 icmp: echo request
   2: 11:08:30.289123       10.10.10.101 > 100.103.255.195 icmp: echo reply
   3: 11:08:30.504566       100.103.255.195 > 10.10.10.101 icmp: echo request
   4: 11:08:30.504963       10.10.10.101 > 100.103.255.195 icmp: echo reply
   5: 11:08:30.710992       100.103.255.195 > 10.10.10.101 icmp: echo request
   6: 11:08:30.711404       10.10.10.101 > 100.103.255.195 icmp: echo reply
   7: 11:08:30.917112       100.103.255.195 > 10.10.10.101 icmp: echo request
   8: 11:08:30.917402       10.10.10.101 > 100.103.255.195 icmp: echo reply
   9: 11:08:31.128243       100.103.255.195 > 10.10.10.101 icmp: echo request
  10: 11:08:31.128640       10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

   1: 11:08:30.287964       100.103.255.195 > 10.10.10.101 icmp: echo request
   2: 11:08:30.289322       10.10.10.101 > 100.103.255.195 icmp: echo reply
   3: 11:08:30.504505       100.103.255.195 > 10.10.10.101 icmp: echo request
   4: 11:08:30.505009       10.10.10.101 > 100.103.255.195 icmp: echo reply
   5: 11:08:30.710961       100.103.255.195 > 10.10.10.101 icmp: echo request
   6: 11:08:30.711434       10.10.10.101 > 100.103.255.195 icmp: echo reply
   7: 11:08:30.917066       100.103.255.195 > 10.10.10.101 icmp: echo request
   8: 11:08:30.917417       10.10.10.101 > 100.103.255.195 icmp: echo reply
   9: 11:08:31.128197       100.103.255.195 > 10.10.10.101 icmp: echo request
  10: 11:08:31.128685       10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
```

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。