FDMによって管理されるFTDのスタティックルートを使用したルートベースのVPNの設定

内容

はじめに

このドキュメントでは、FDMによって管理されるFTDでスタティックルートベースのサイト間VPNトンネル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。

- VPNトンネルの動作方法に関する基本的な知識。
- Firepower Device Manager(FDM)を使用したナビゲーションに関する予備知識。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

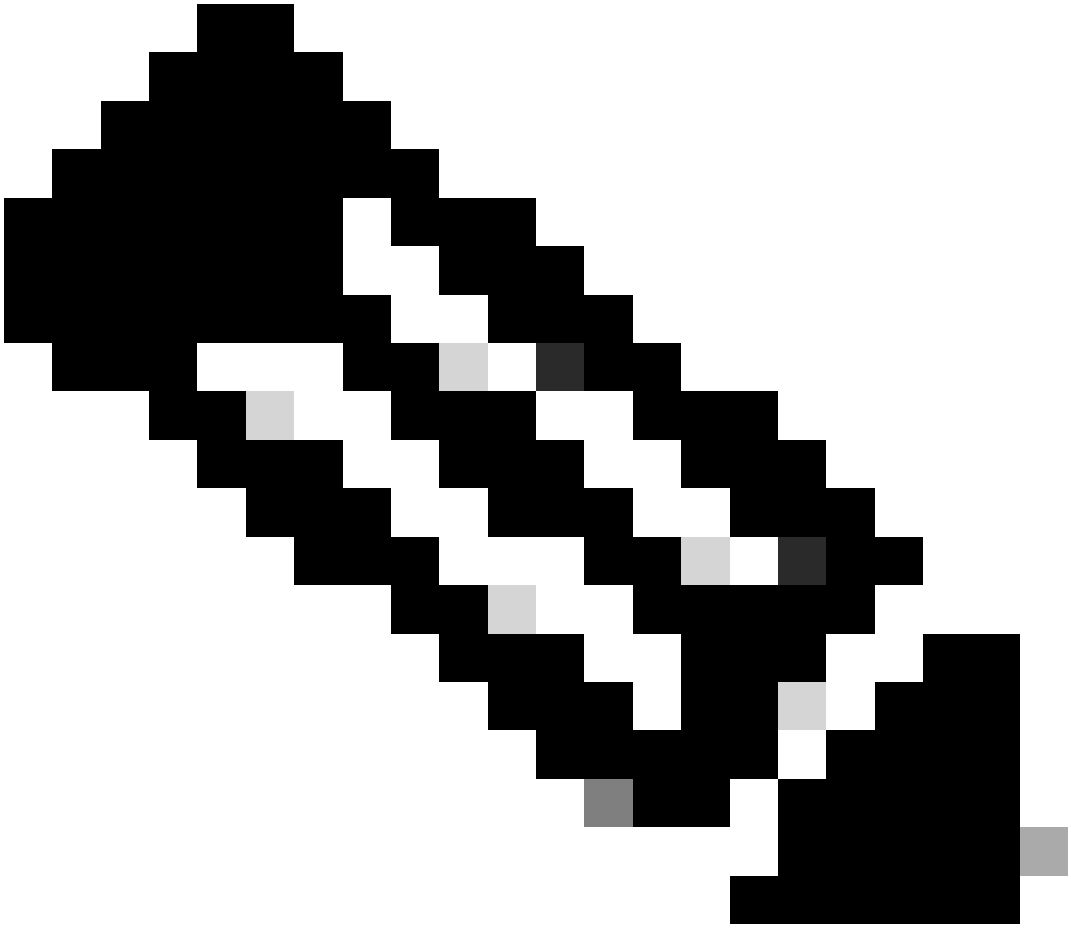
- Firepower Device Manager(FDM)で管理されるCisco Firepower Threat Defense(FTD)バージョン7.0。

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

ルートベースのVPNでは、VPNトンネルを介して暗号化または送信される対象トラフィックを判別でき、ポリシーベースまたはクリプトマップベースのVPNのように、ポリシー/アクセスリストの代わりにトラフィックルーティングを使用します。 暗号化ドメインは、IPSecトンネルに入るすべてのトラフィックを許可するように設定されます。IPsecローカルおよびリモートトラフィックセレクタは0.0.0.0/0.0.0.0に設定されます。つまり、IPSecトンネルにルーティングされるすべてのトラフィックは、送信元/宛先サブネットに関係なく暗号化されます。

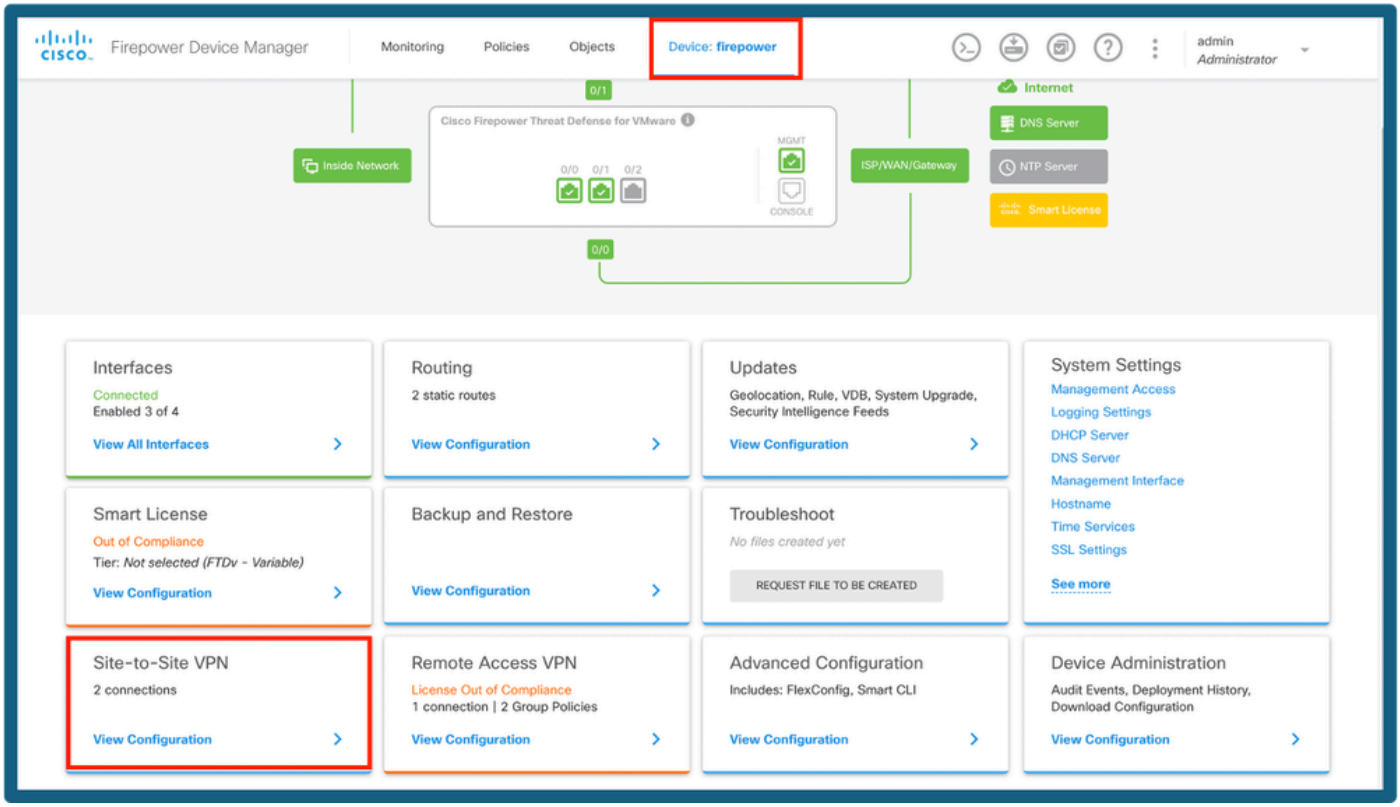
このドキュメントでは、スタティック仮想トンネルインターフェイス(SVTI)の設定を中心に説明します。



注：追加のライセンスは必要ありません。ルートベースのVPNは、ライセンスモードと評価モードで設定できます。 暗号に準拠していない場合（輸出規制機能が有効になっている場合）、暗号化アルゴリズムとして使用できるのはDESだけです。

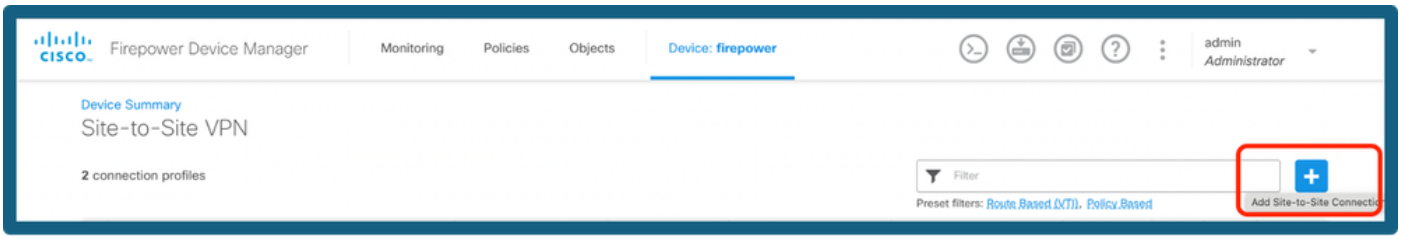
FDMでの構成手順

ステップ 1：Device > Site To Siteの順に移動します。



FDMダッシュボード

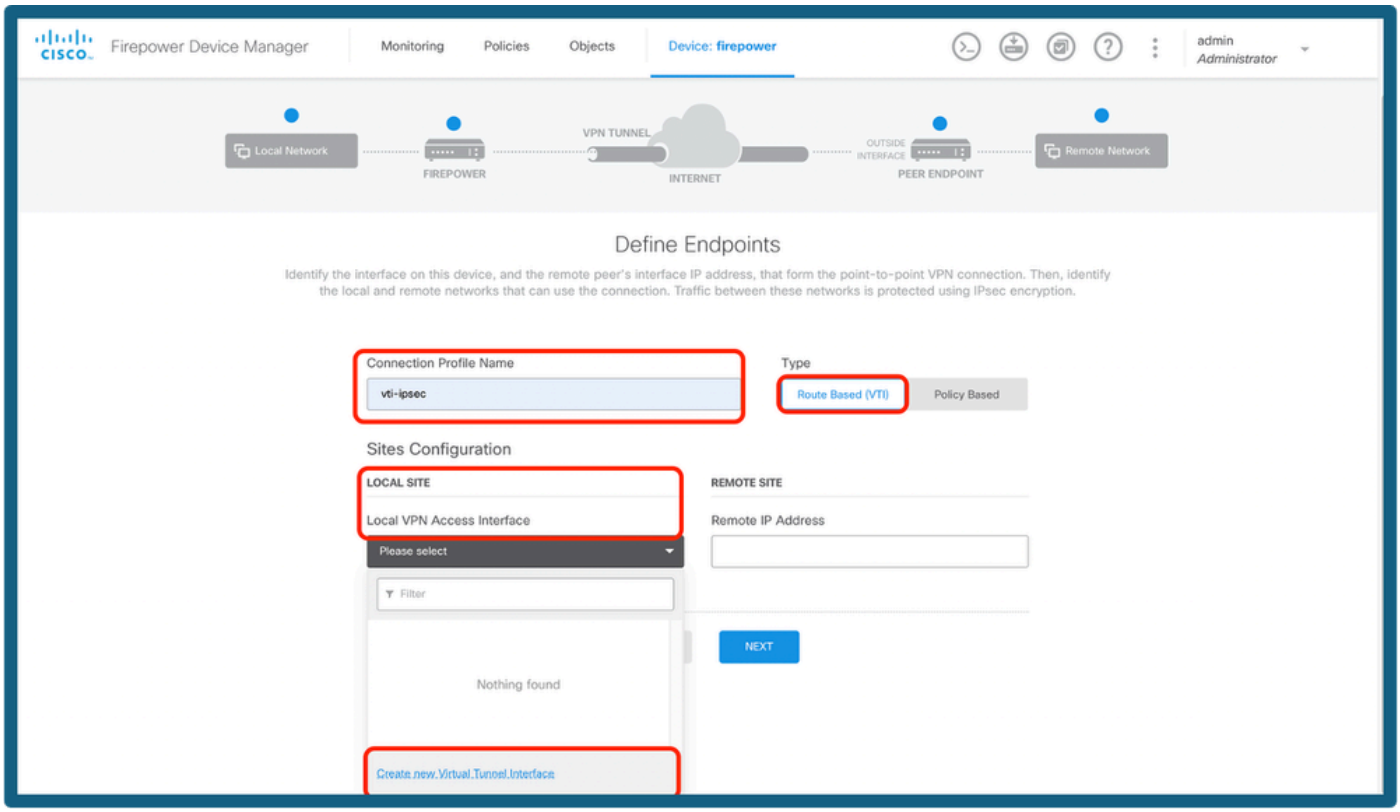
ステップ 2：+アイコンをクリックして、新しいサイト間接続を追加します。



S2S接続の追加

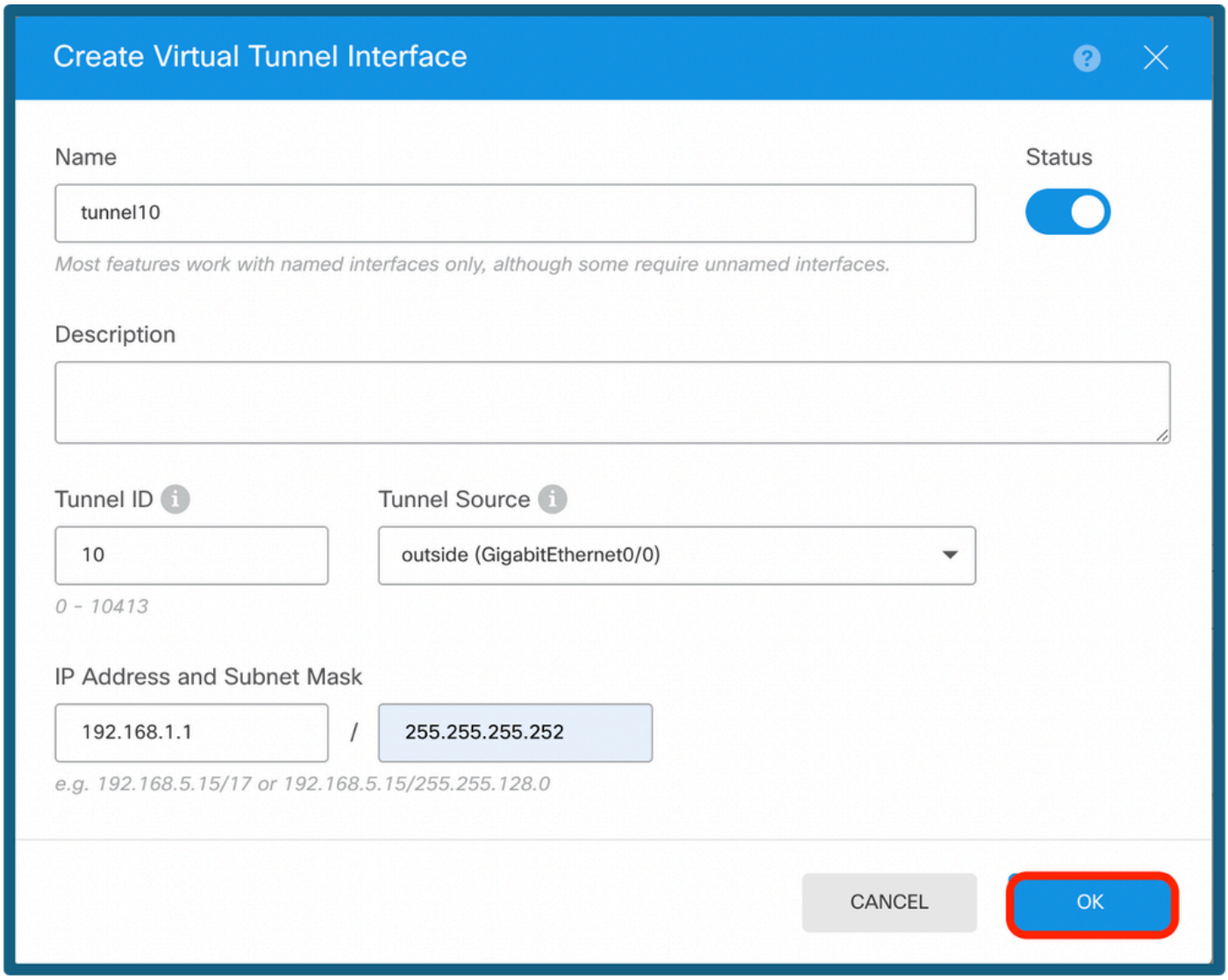
ステップ3:トポロジ名を指定し、ルートベース(VTI)としてVPNのタイプを選択します。

Local VPN Access Interfaceをクリックしてから Create new Virtual Tunnel Interfaceをクリックするか、既存のリストから1つ選択します。



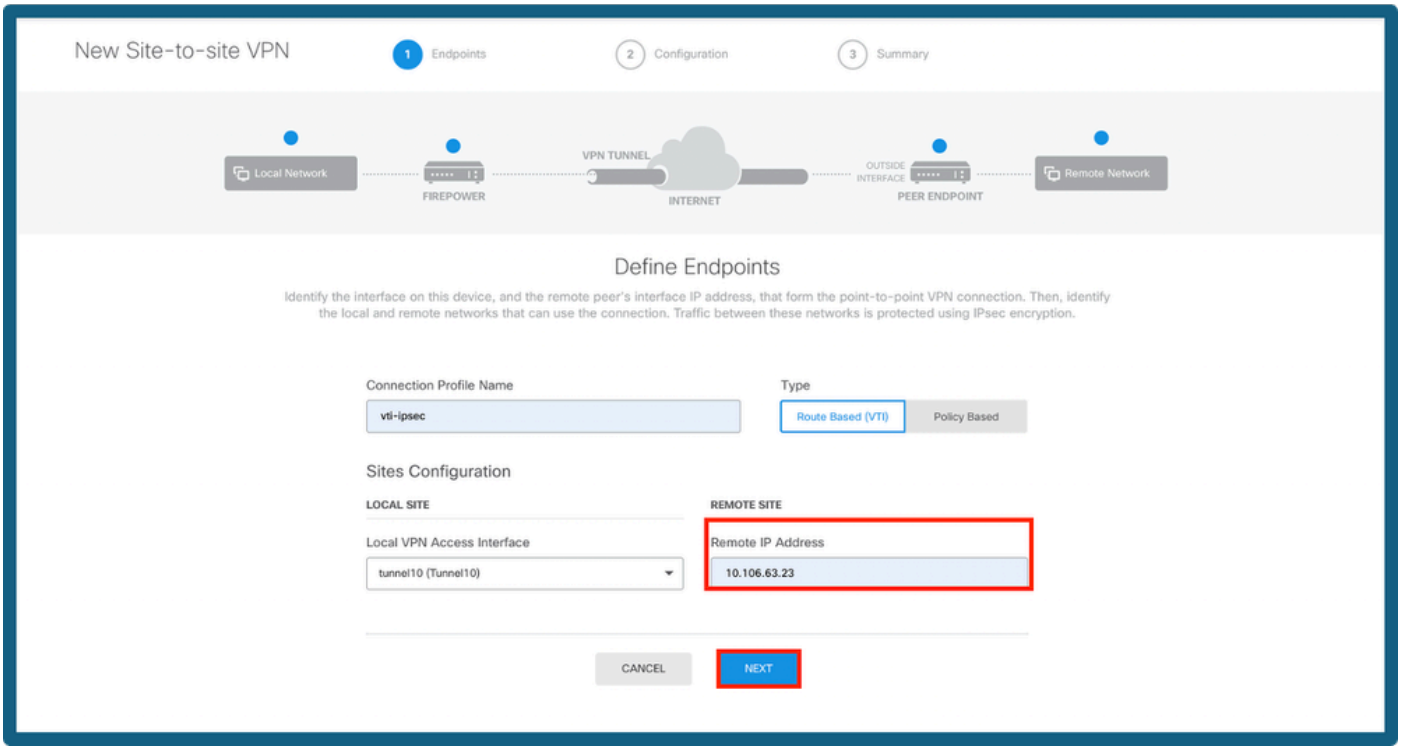
トンネルインターフェイスの追加

ステップ 4：新しい仮想トンネルインターフェイスのパラメータを定義します。[OK] をクリックします。



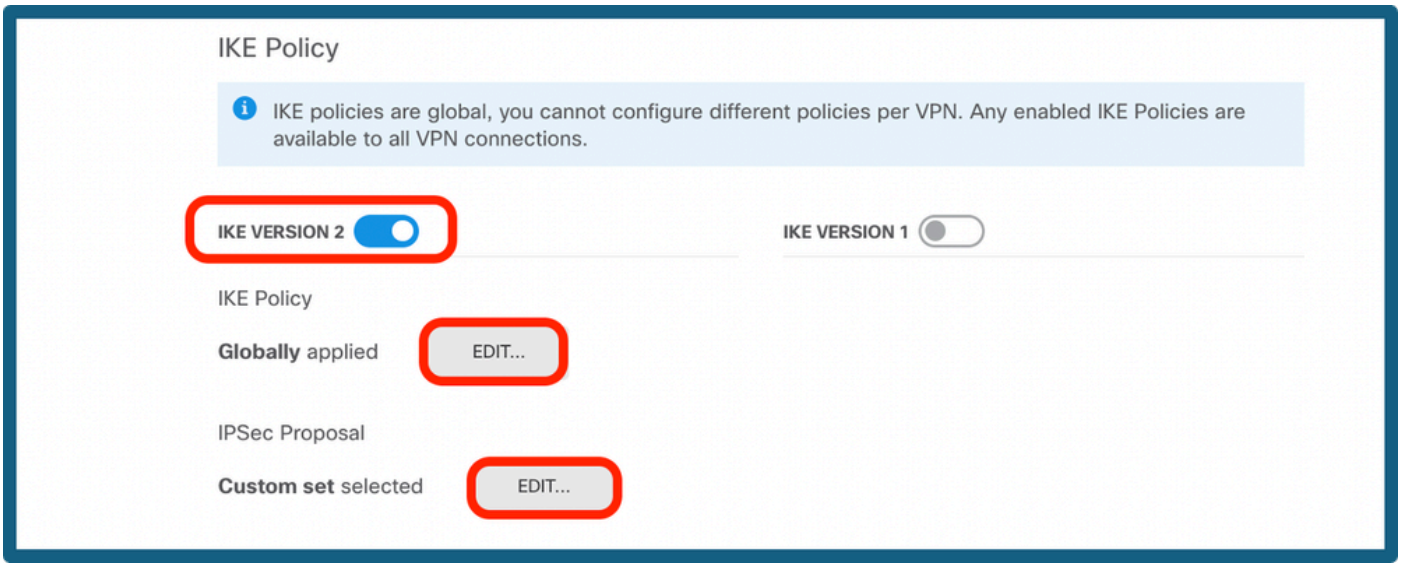
VTIの設定

ステップ 5：新しく作成したVTIか、Virtual Tunnel Interfaceの下に存在するVTIを選択します。リモートIPアドレスを指定します。



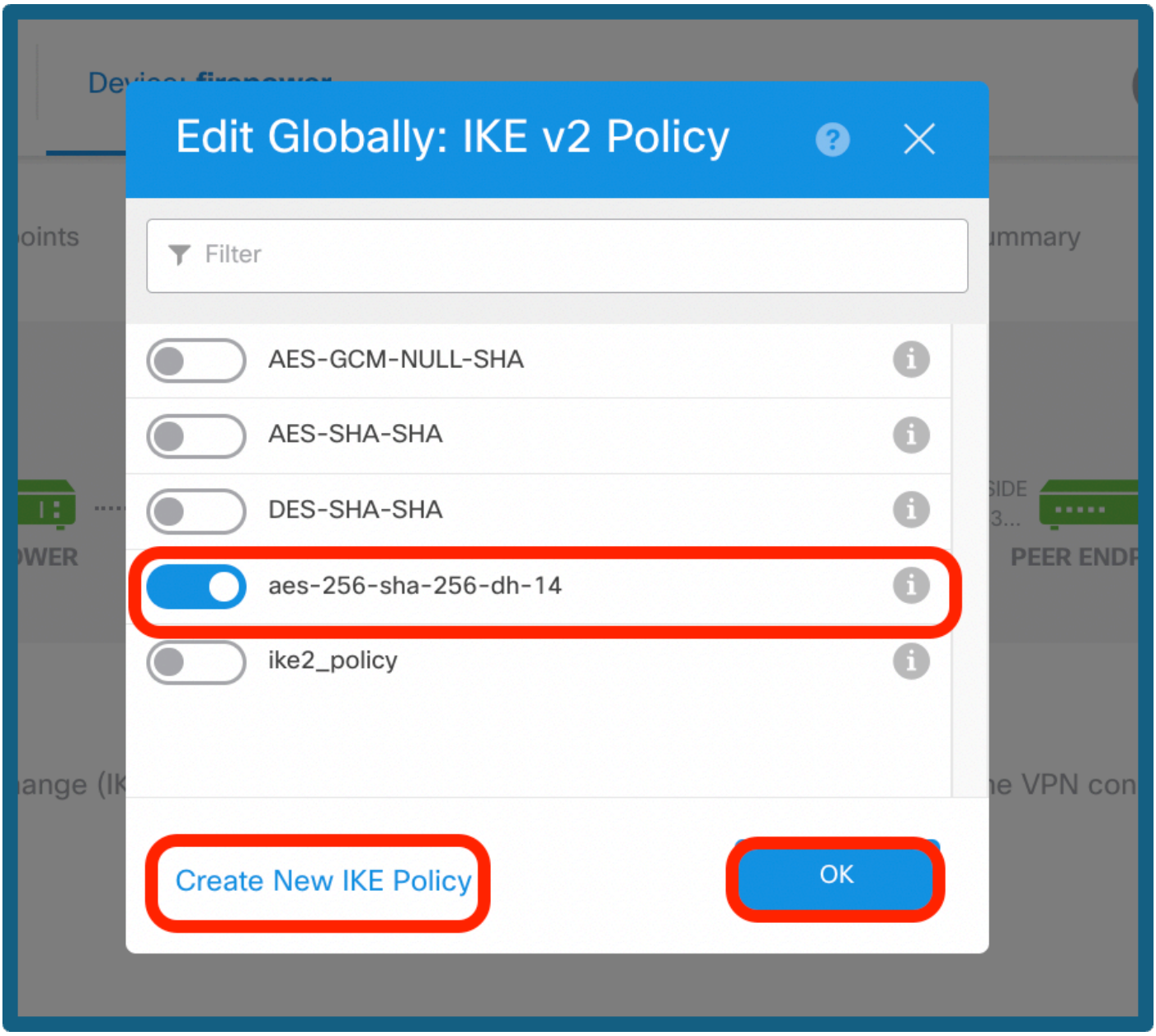
ピアIPの追加

手順 6：IKE Versionを選択し、Editボタンを選択して、図に示すようにIKEおよびIPSecパラメータを設定します。

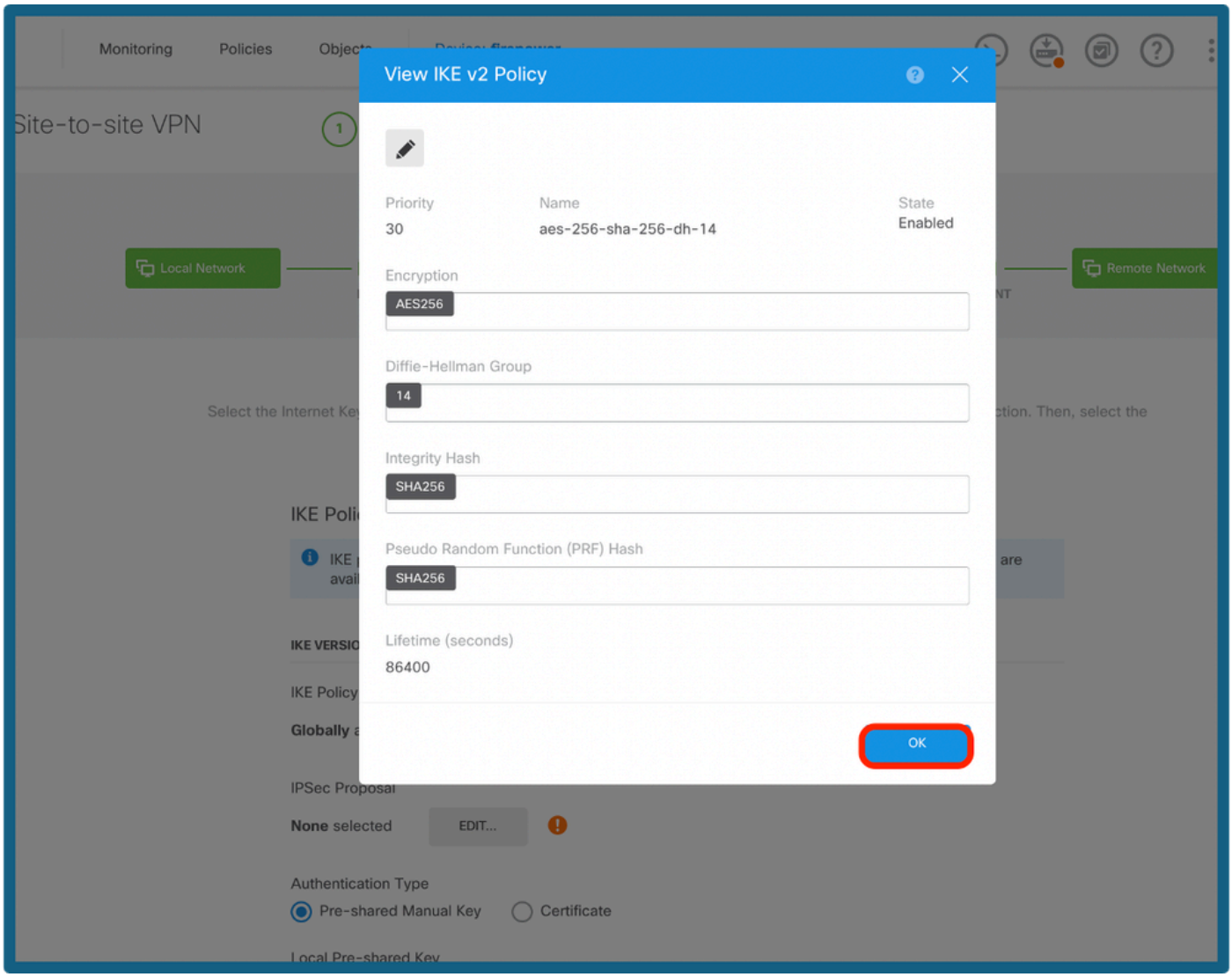


IKEバージョンの設定

ステップ7a:図に示すようにIKE Policyボタンを選択し、新しいポリシーを作成する場合はokボタンまたはCreate New IKE Policyをクリックします。

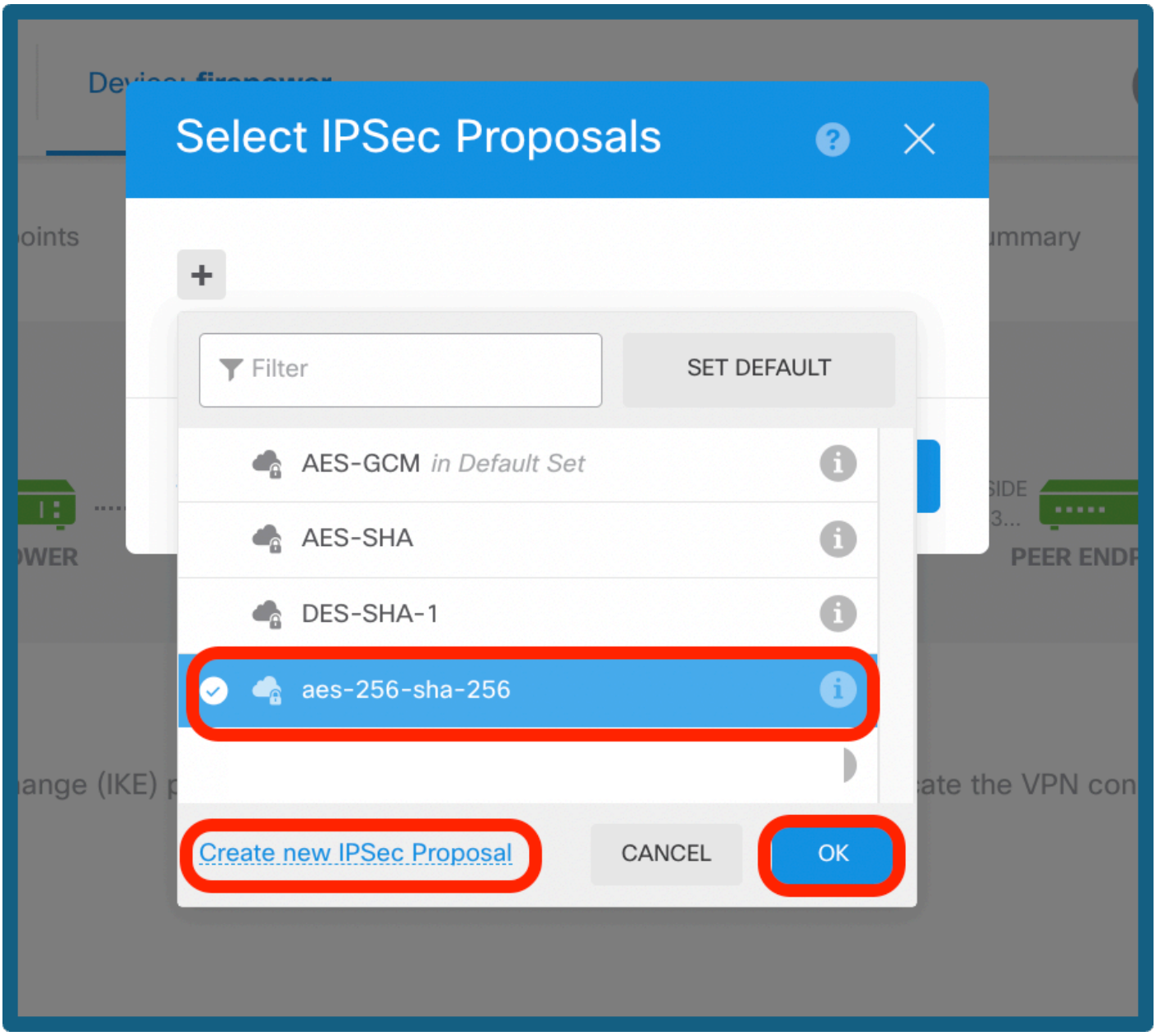

Edit Globally: IKE v2 Policy
Filter
AES-GCM-NULL-SHA
AES-SHA-SHA
DES-SHA-SHA
aes-256-sha-256-dh-14
ike2_policy
Create New IKE Policy
OK

IKEポリシーの選択

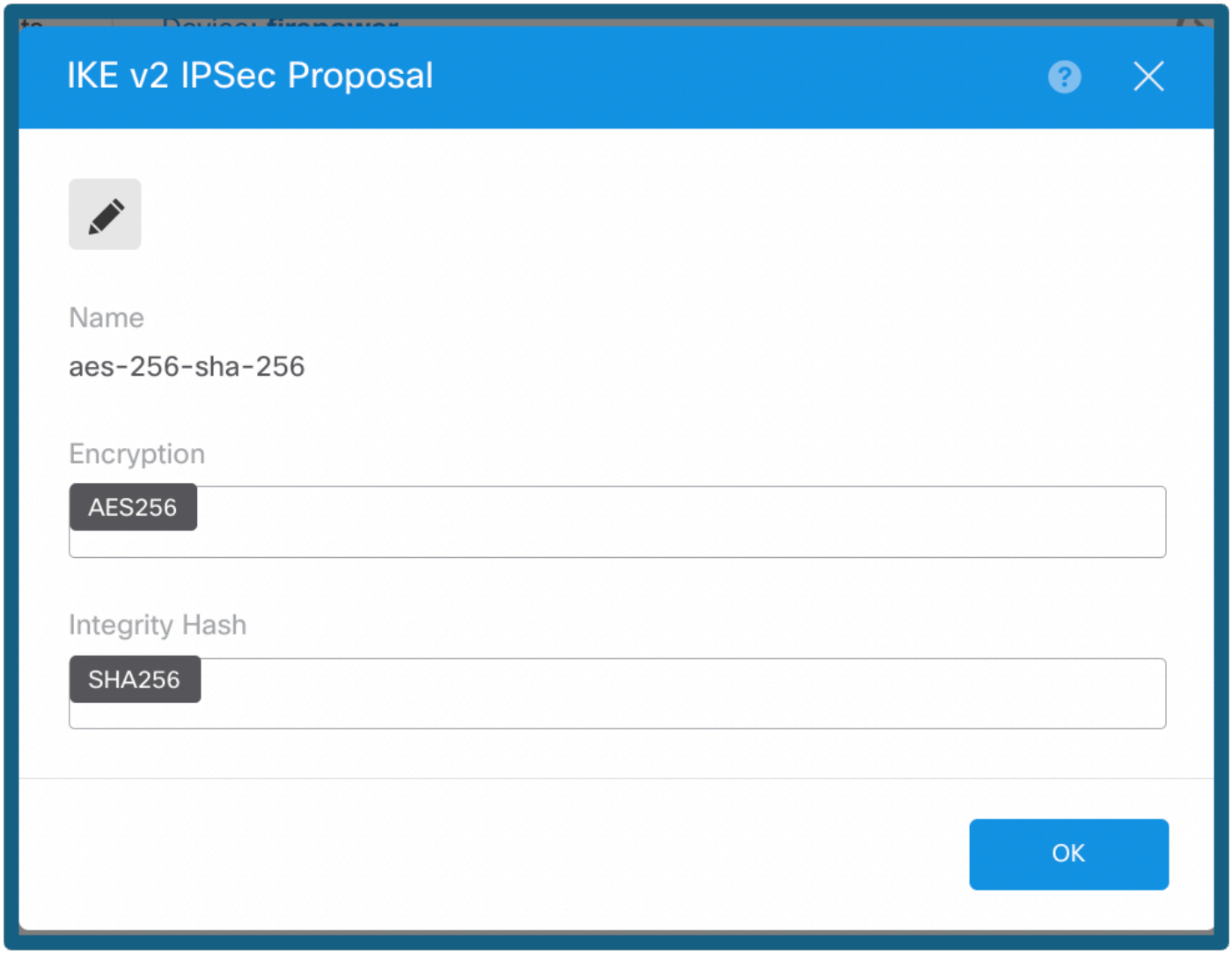


IKEポリシーの設定

ステップ7b:図に示すようにIPSec Policyボタンを選択し、新しいプロポーザルを作成する場合はokボタンまたはCreate New IPSsec Proposalをクリックします。



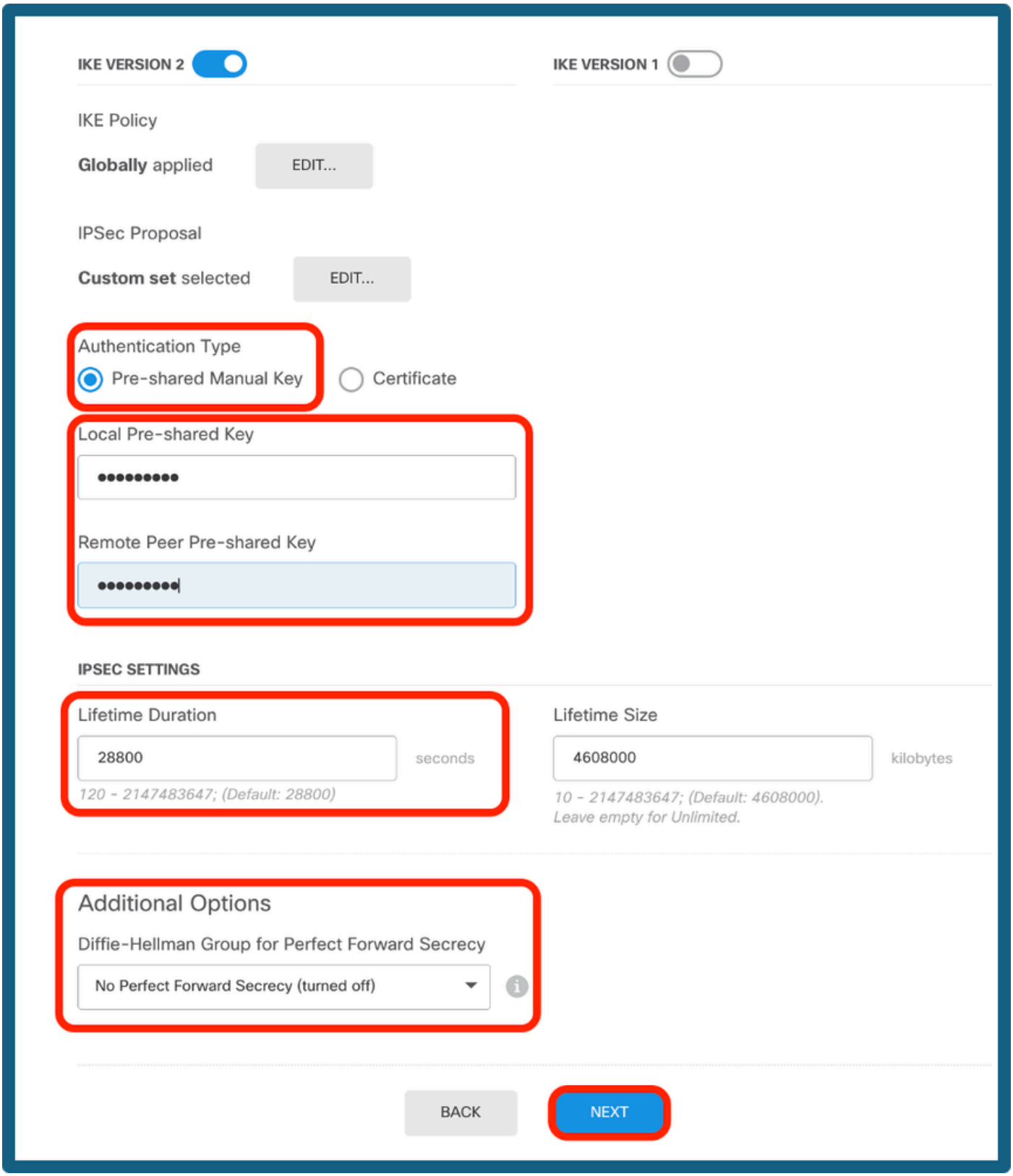
IPSecプロポーザルの選択



IPSecプロポーザルの設定

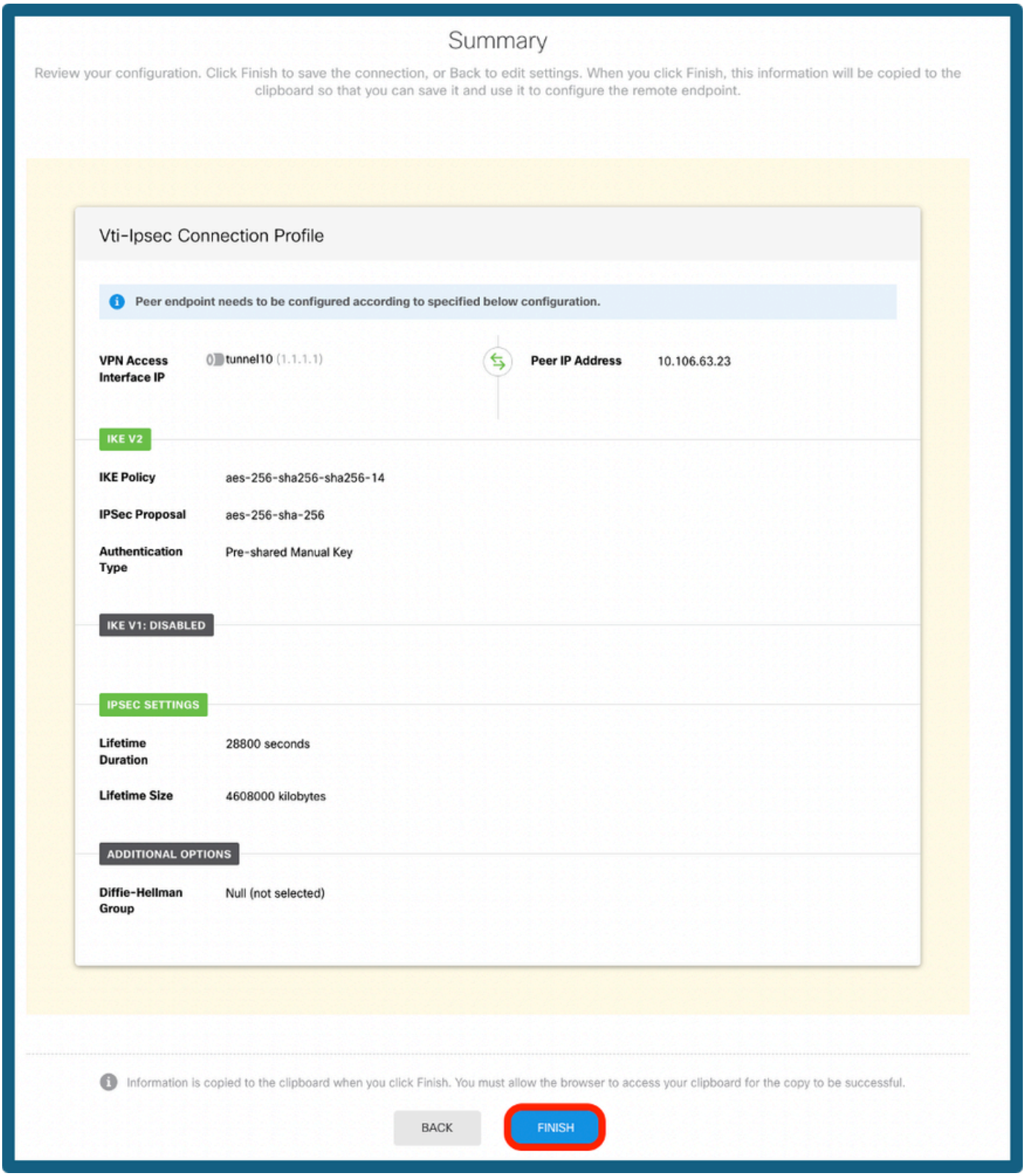
ステップ8a:Authentication Typeを選択します。事前共有手動キーを使用する場合は、ローカルおよびリモート事前共有キーを指定します。

ステップ8b:（オプション）Perfect Forward Secrecy設定を選択します。IPsec Lifetime DurationとLifetime Sizeを設定し、nextをクリックします。



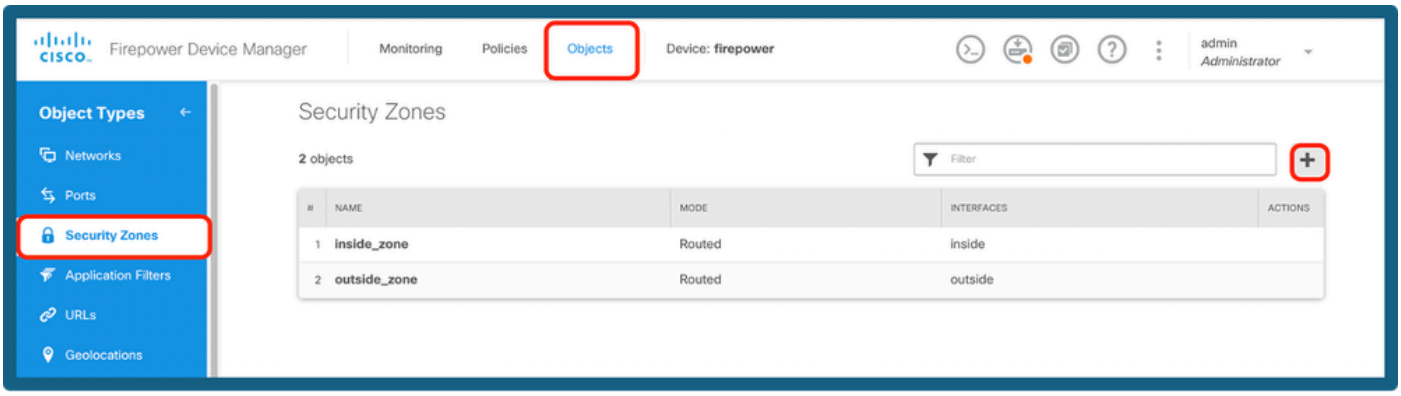
PSKおよびライフタイム設定

ステップ 9：設定を確認し、Finishをクリックします。



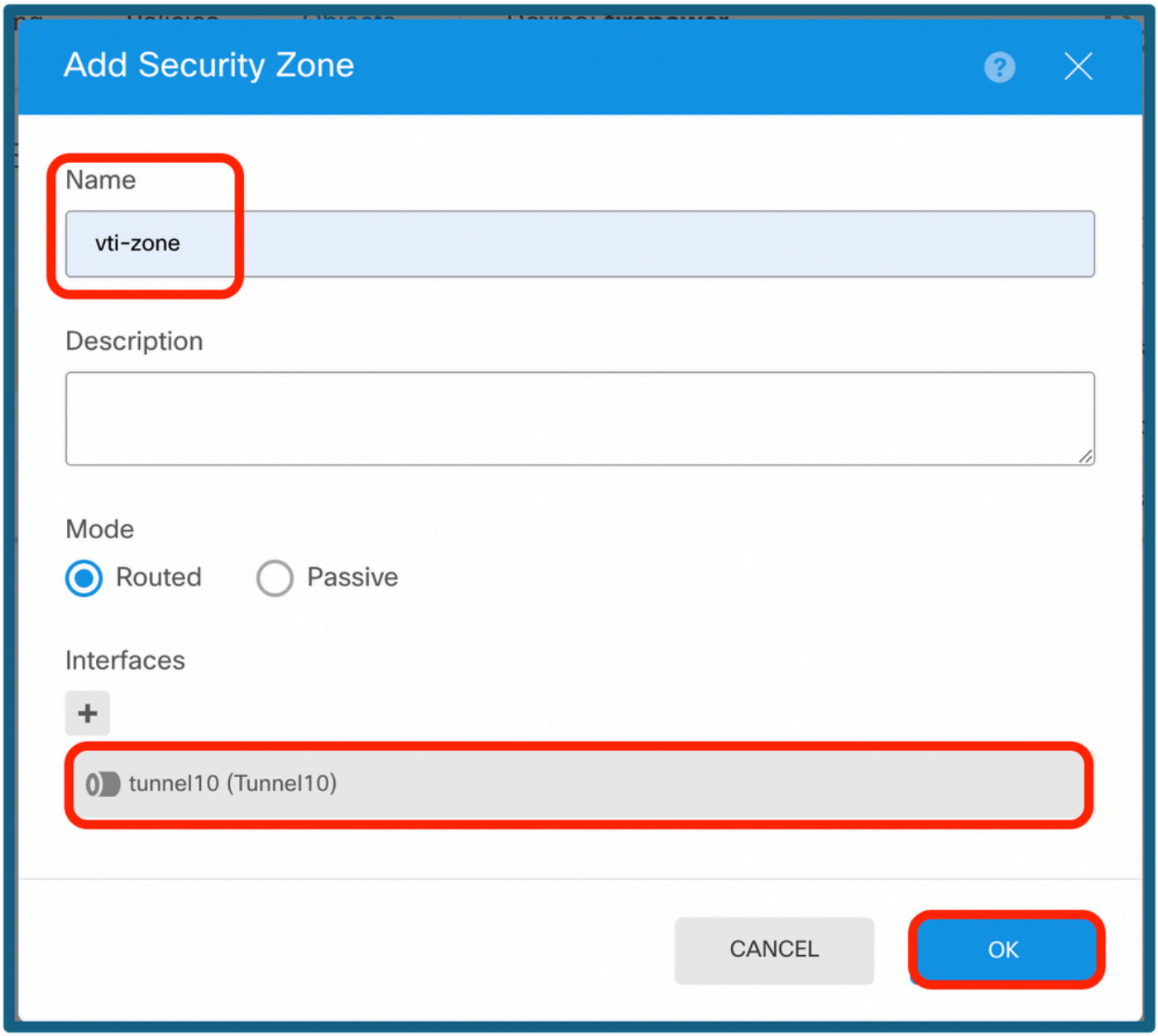
設定の概要

ステップ10a:Objects > Security Zonesの順に移動し、+アイコンをクリックします。



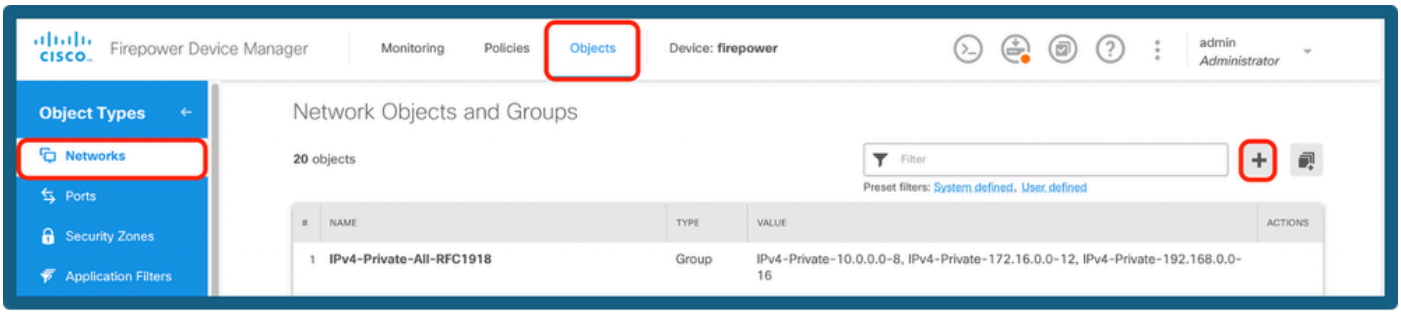
セキュリティゾーンの追加

ステップ10b:ゾーンを作成し、次に示すようにVTIインターフェイスを選択します。



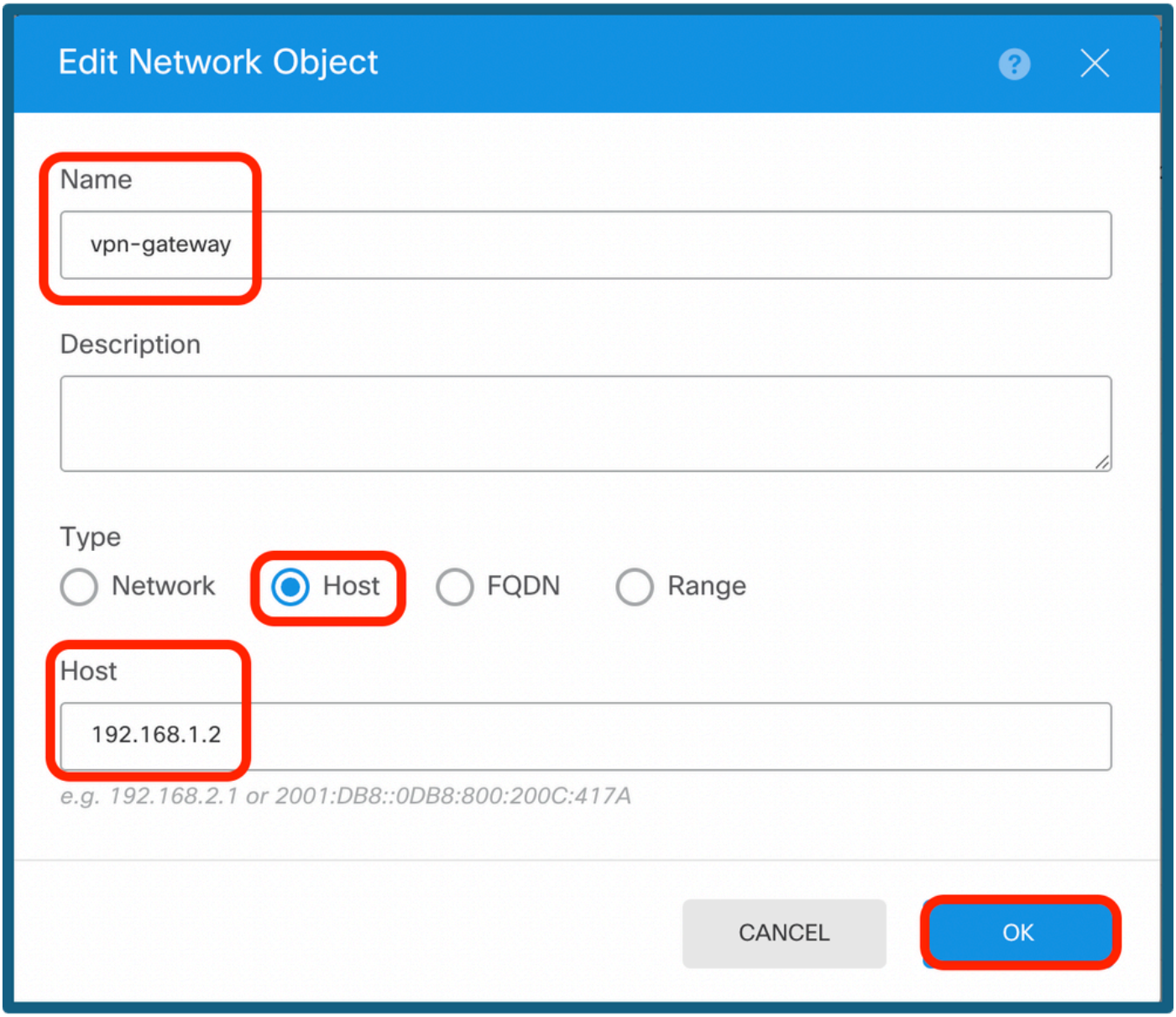
セキュリティゾーンの構成

ステップ11a:Objects > Networksの順に移動し、+アイコンをクリックします。



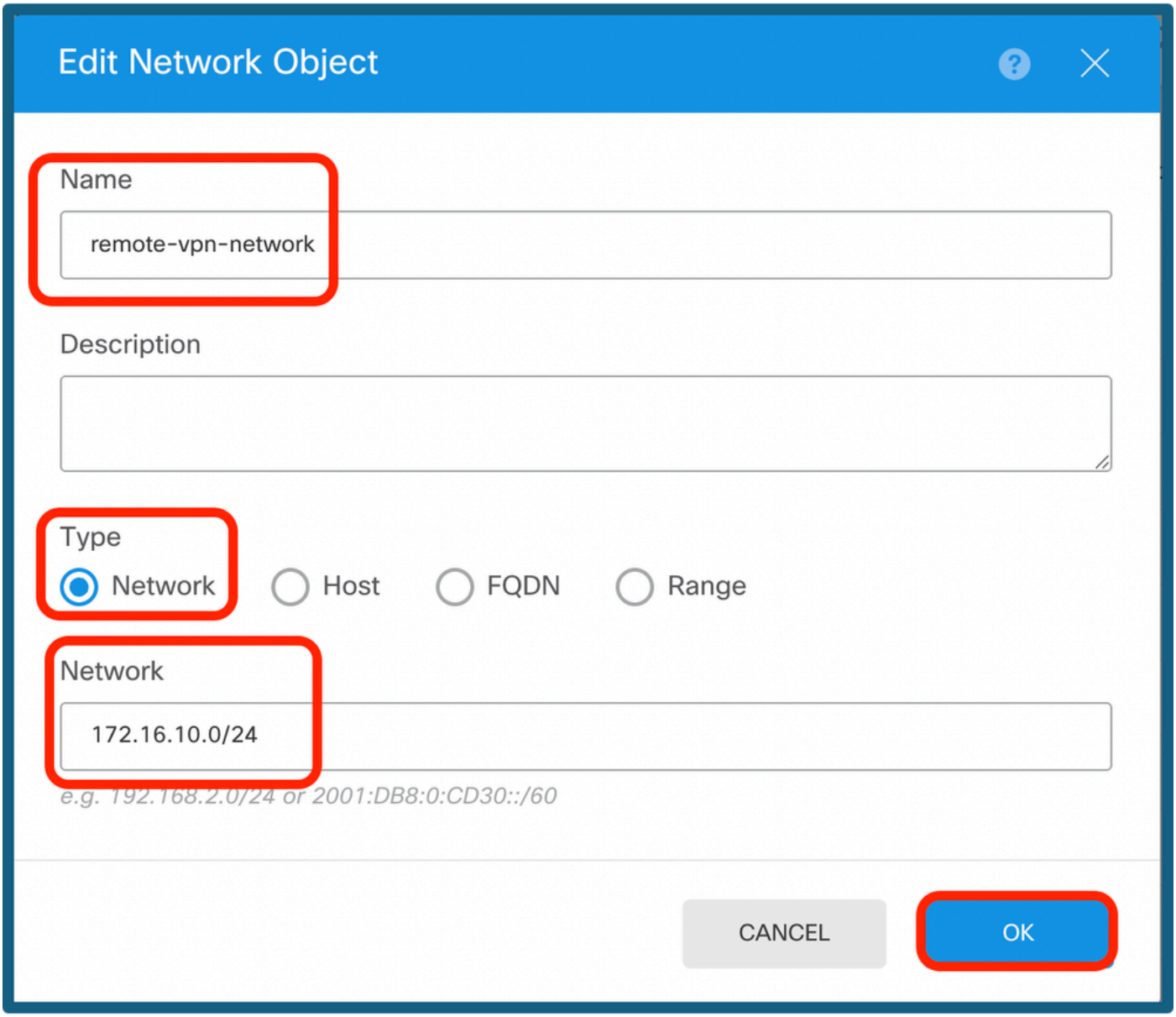
ネットワーク オブジェクトの追加

ステップ11b:hostオブジェクトを追加し、ピアエンドのトンネルIPを持つゲートウェイを作成します。

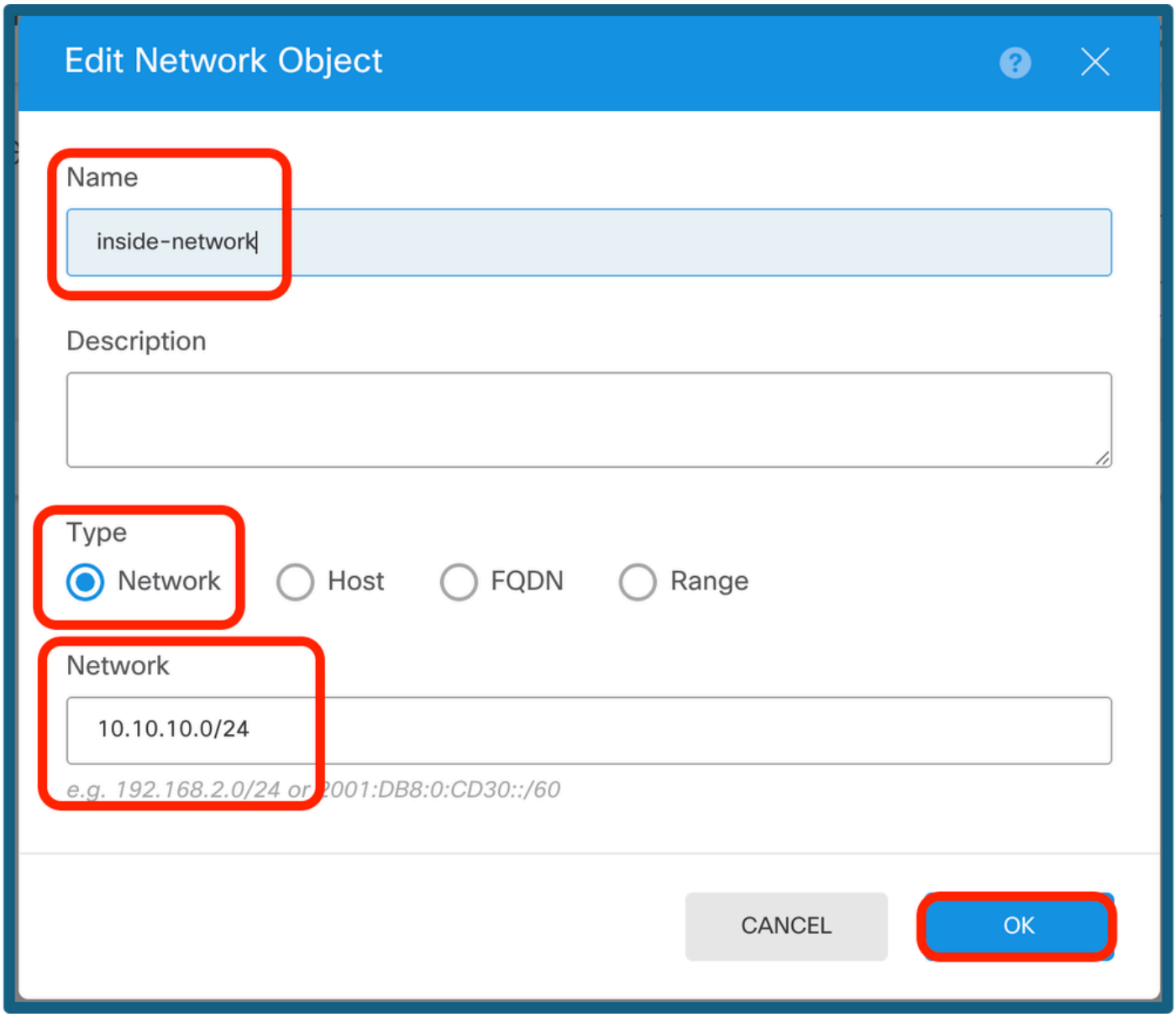


VPNゲートウェイの設定

ステップ11c:リモートサブネットとローカルサブネットを追加します。

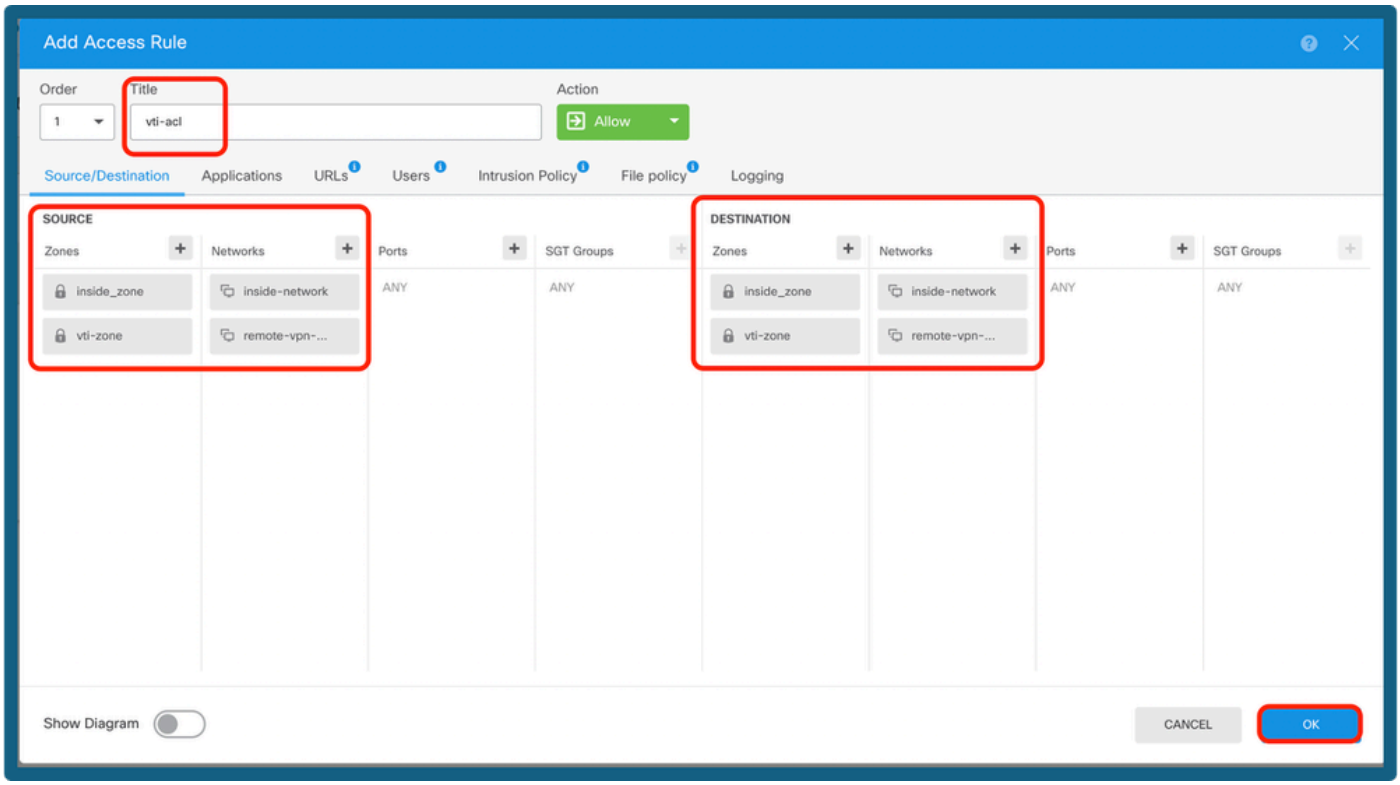


リモートIP設定



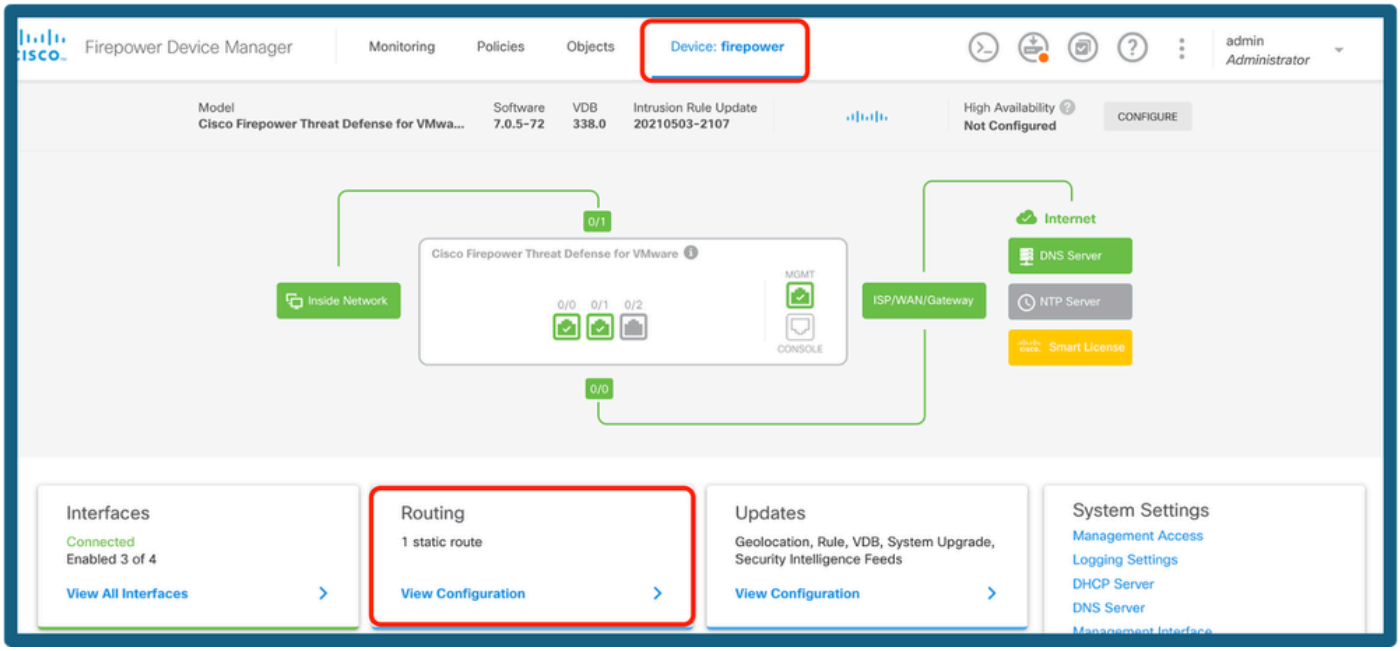
ローカルIP設定

ステップ 12Device > Policiesに移動し、アクセスコントロールポリシーを設定します。



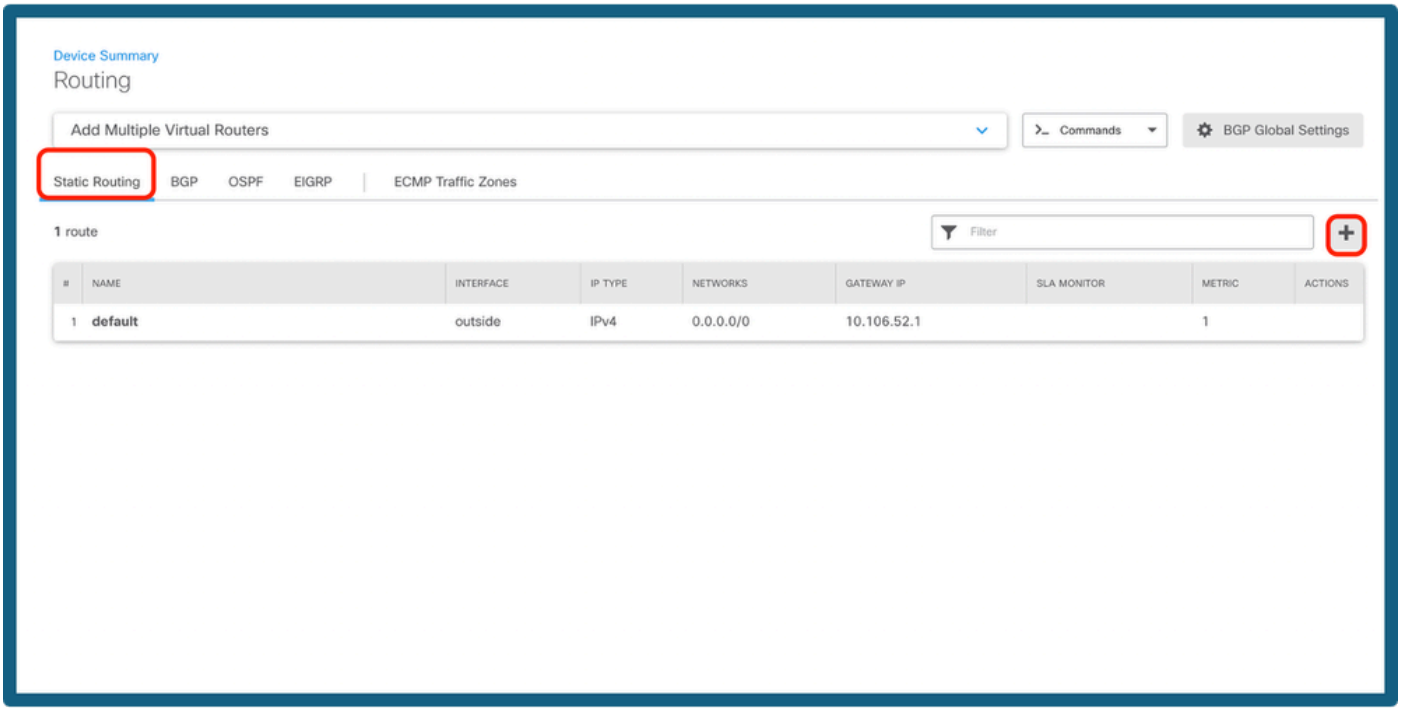
アクセスコントロールポリシーの追加

ステップ13a:VTIトンネルを介したルーティングを追加します。Device > Routingの順に移動します。



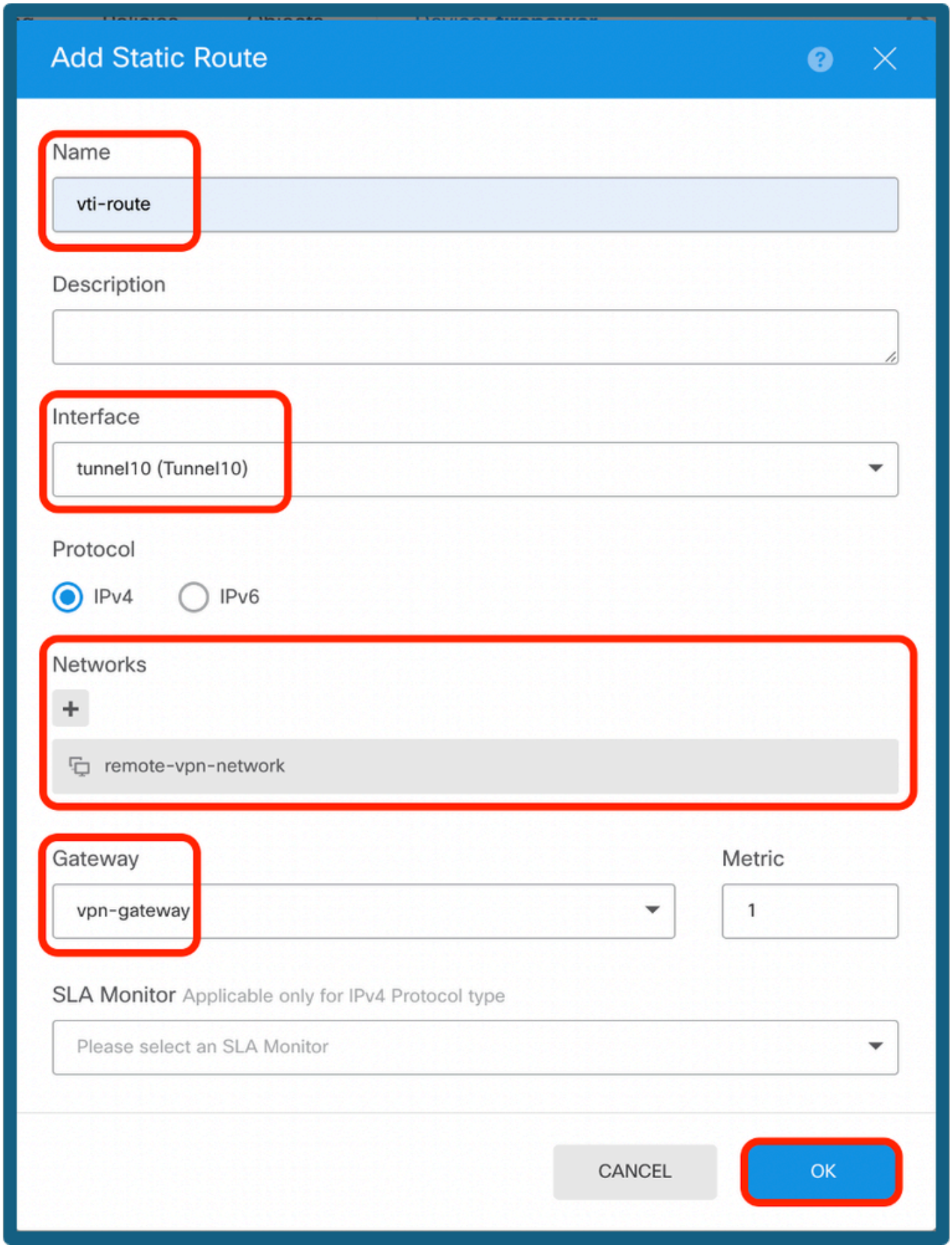
工順の選択

ステップ13b:Routingタブの下にあるStatic Routeに移動します。+アイコンをクリックします。



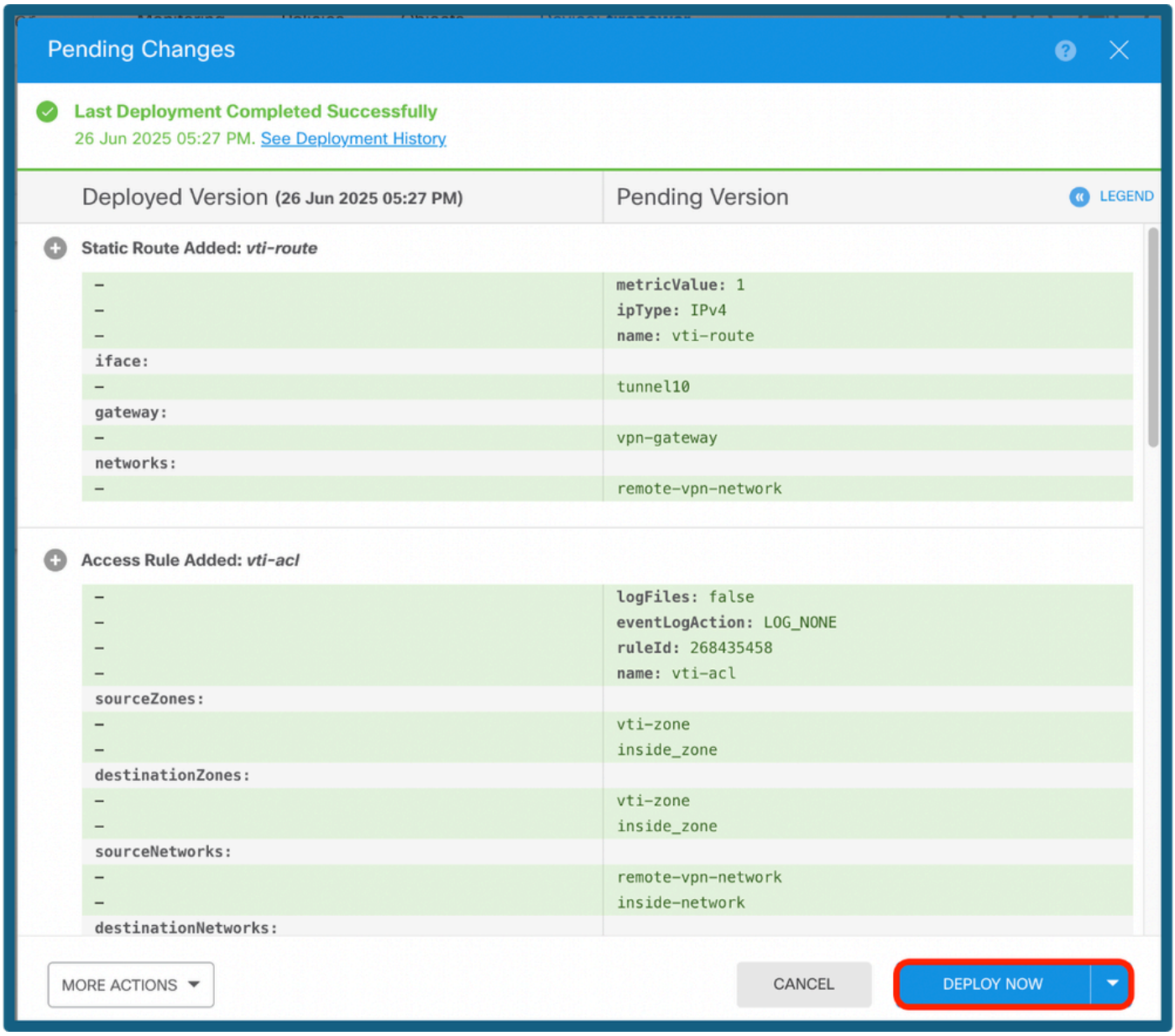
ルートの追加

ステップ13c:Interfaceを指定し、Networkを選択してGatewayを指定します。[OK] をクリックします。



スタティックルートの設定

ステップ 14：Deployに移動します。変更内容を確認し、Deploy Nowをクリックします。

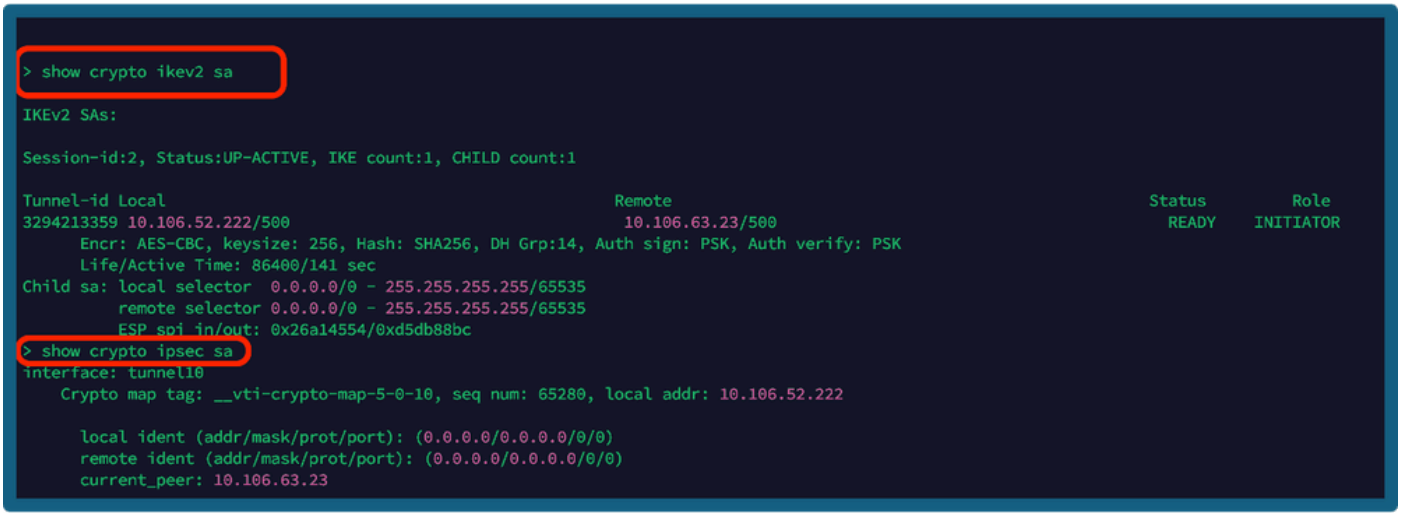


構成の展開

確認

導入が完了したら、次のコマンドを使用してCLIでトンネルステータスを確認できます。

1. show crypto ikev2 sa
2. show crypto ipsec sa <ピアIP>



show コマンド

関連情報

FDMによって管理されるFTDのサイト間VPNの詳細については、次のサイトで完全な構成ガイドを参照してください。

FDMで管理されるFTDの構成ガイド

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。