FDMによって管理されるFTDでのルートベースVPNを介したBGPの設定

内容

はじめに

このドキュメントでは、FirePower Device Manager(FDM)で管理されるFTDv上のルートベースのサイト間VPNでのBGPの設定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の基本的な知識
- FTDvでのBGPの設定
- FDMの経験

使用するコンポーネント

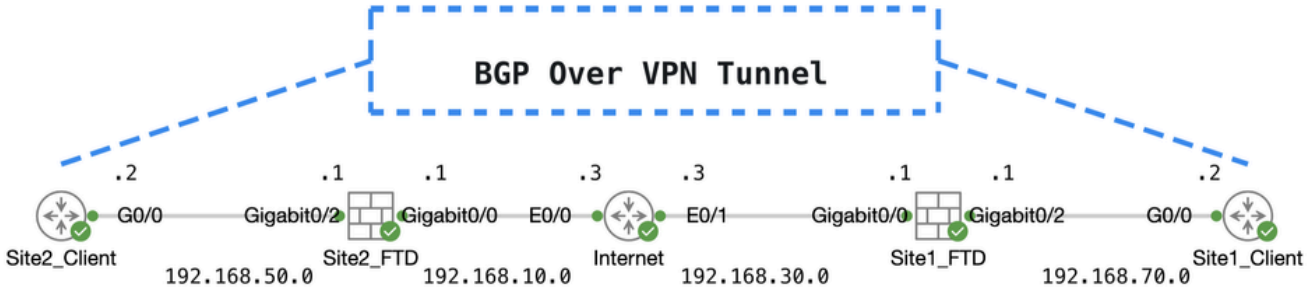
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco FTDvバージョン7.4.2
- Cisco FDMバージョン7.4.2

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。

設定

ネットワーク図



トポ

VPNでの設定

ステップ 1：ノード間のIP相互接続の準備が整い、安定していることを確認します。FDMのスマートライセンスがスマートアカウントに正常に登録されます。

ステップ 2： Site1クライアントのゲートウェイは、Site1 FTDの内部IPアドレス(192.168.70.1)で設定されます。Site2クライアントのゲートウェイは、Site2 FTDの内部IPアドレス(192.168.50.1)で設定されます。また、FDMの初期化後に両方のFTDのデフォルトルートが正しく設定されていることを確認します。

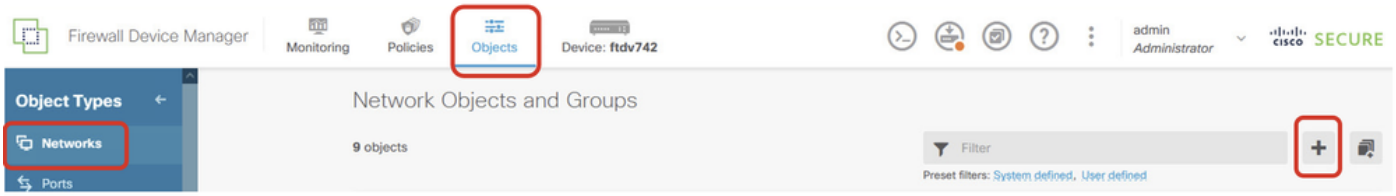
各FDMのGUIにログインします。Device > Routingに移動します。をクリックします。View Configurationデフォルトスタティックルートを確認するには、**Static Routing**タブをクリックします。

Site1_FTD_Gateway（ゲートウェイ）

サイト2_FTD_ゲートウェイ

ステップ 3：ルートベースのサイト間VPNを設定する。 この例では、最初にSite1 FTDを設定します。

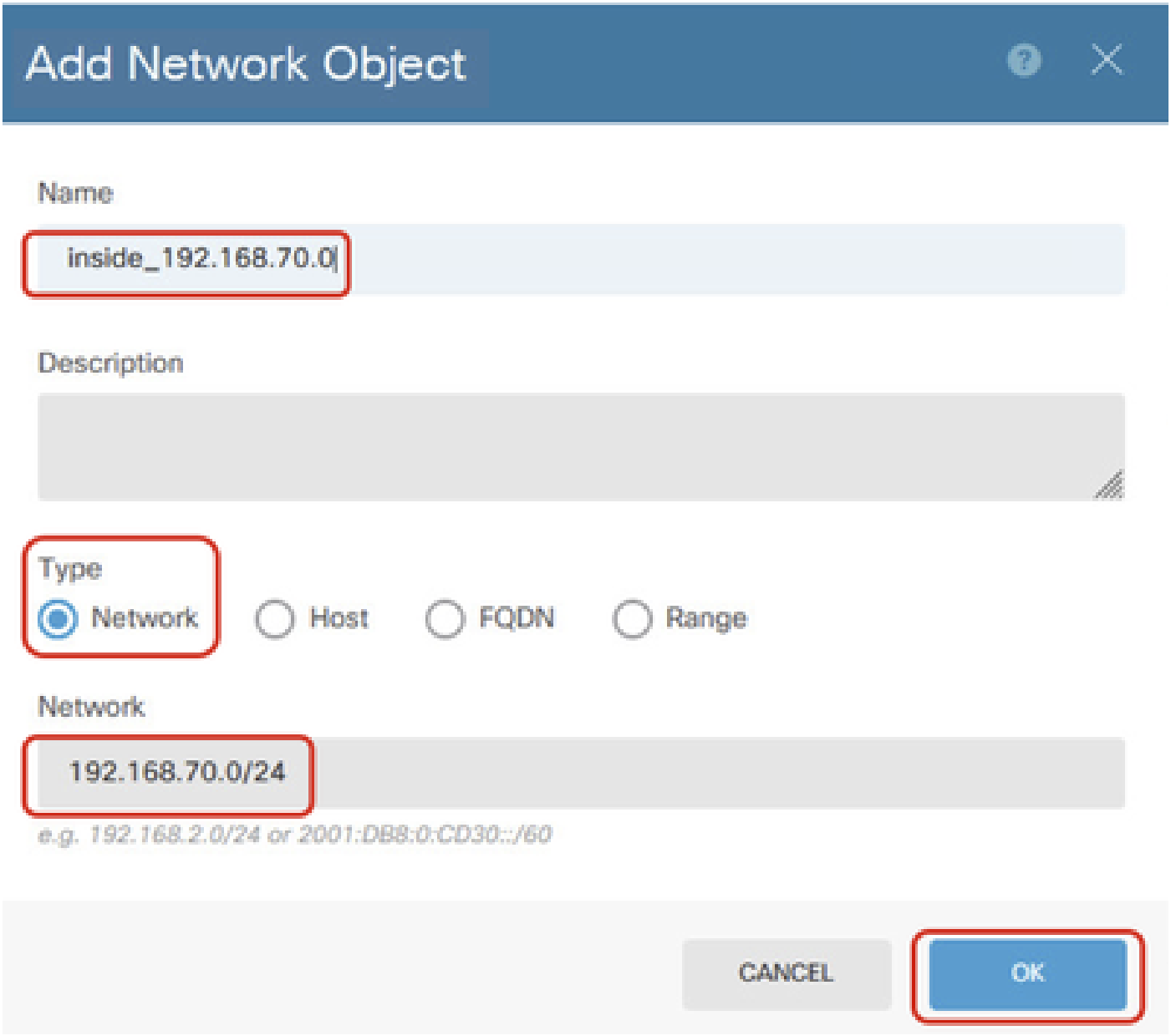
ステップ 3.1： Site1 FTDのFDM GUIにログインします。Site1 FTDの内部ネットワークの新しいネットワークオブジェクトを作成します。 **Objects > Networks**に移動し、+ボタンをクリックします。



Create_Network_オブジェクト

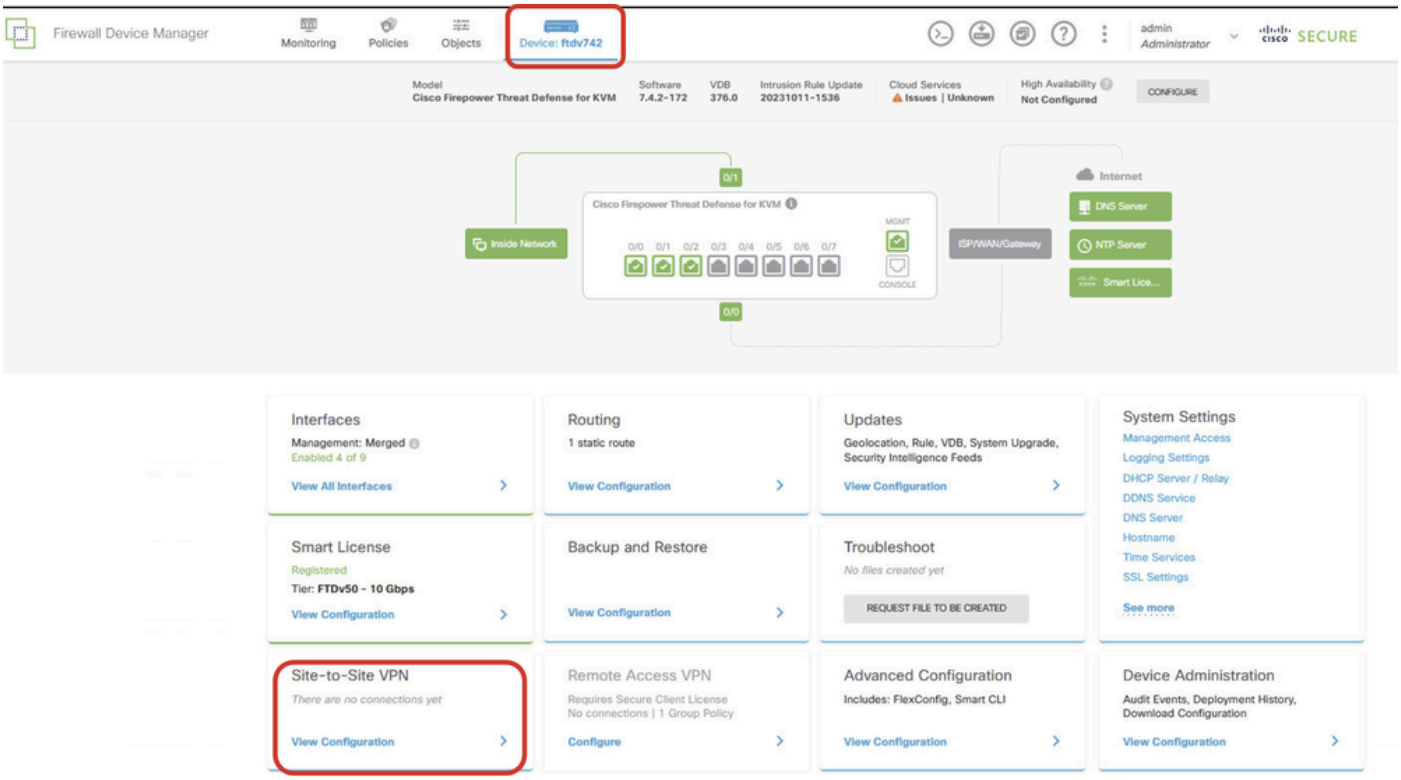
ステップ 3.2：必要な情報を提供します。そのボタンをクリックします。OK

- 名前： inside_192.168.70.0
- タイプ：ネットワーク
- ネットワーク：192.168.70.0/24



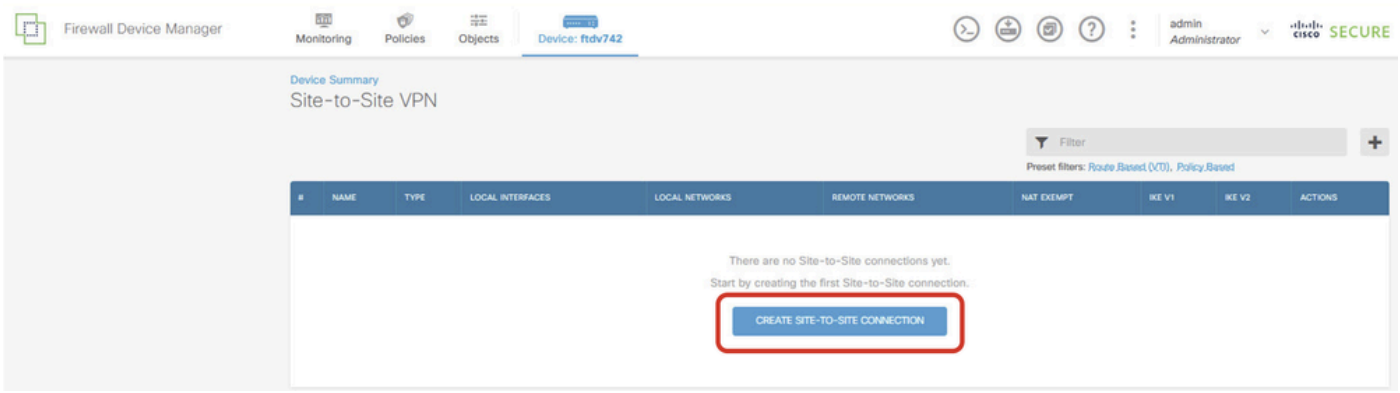
サイト1_内部_ネットワーク

ステップ 3.3：**Device > Site-to-Site VPN**に移動します。をクリックします。**View Configuration**



サイト間VPNの表示

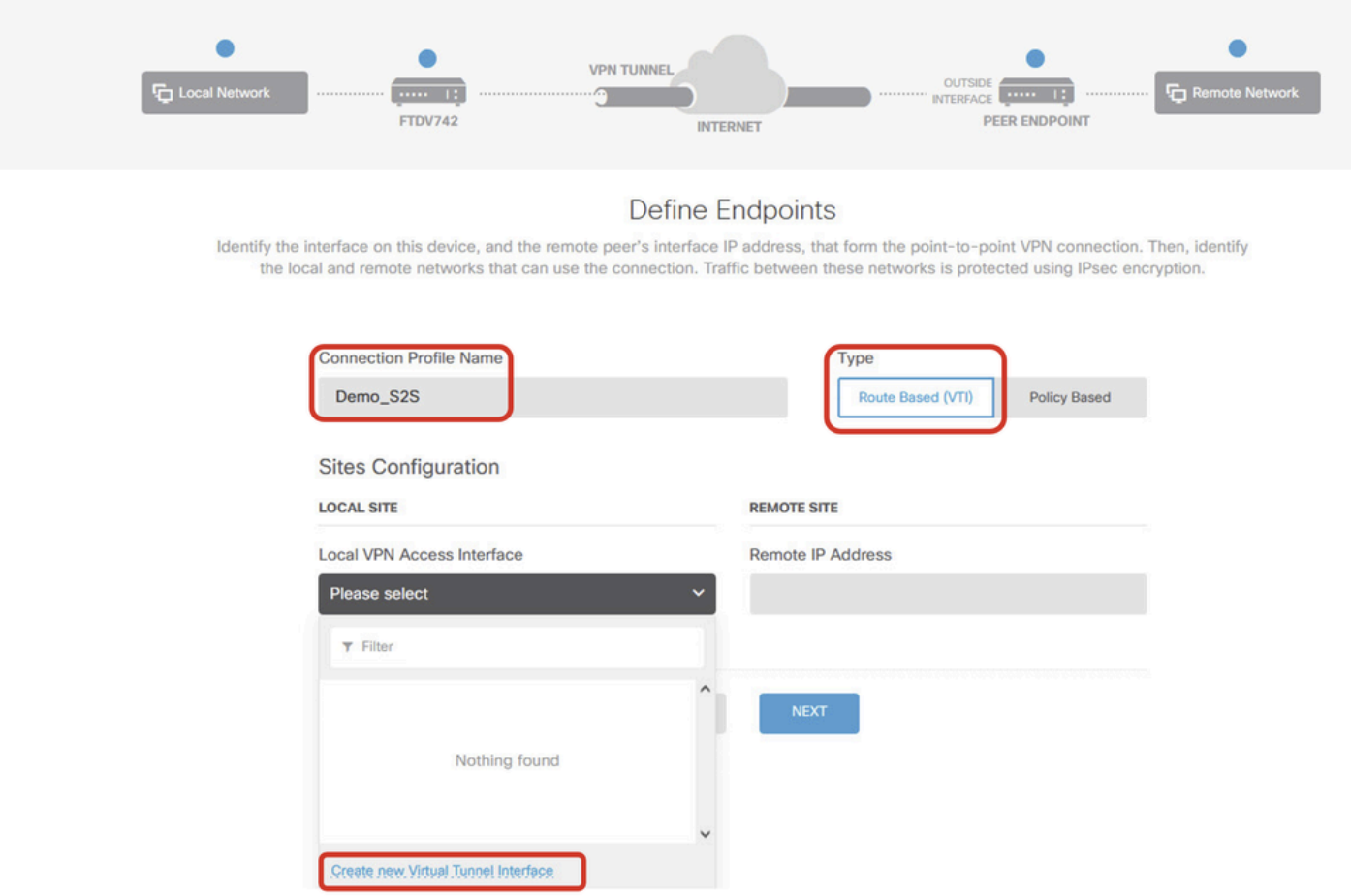
ステップ 3.4：新しいサイト間VPNの作成を開始します。をクリックします。**CREATE SITE-TO-SITE CONNECTION**



サイト間接続の作成

ステップ 3.5：必要な情報を入力します。

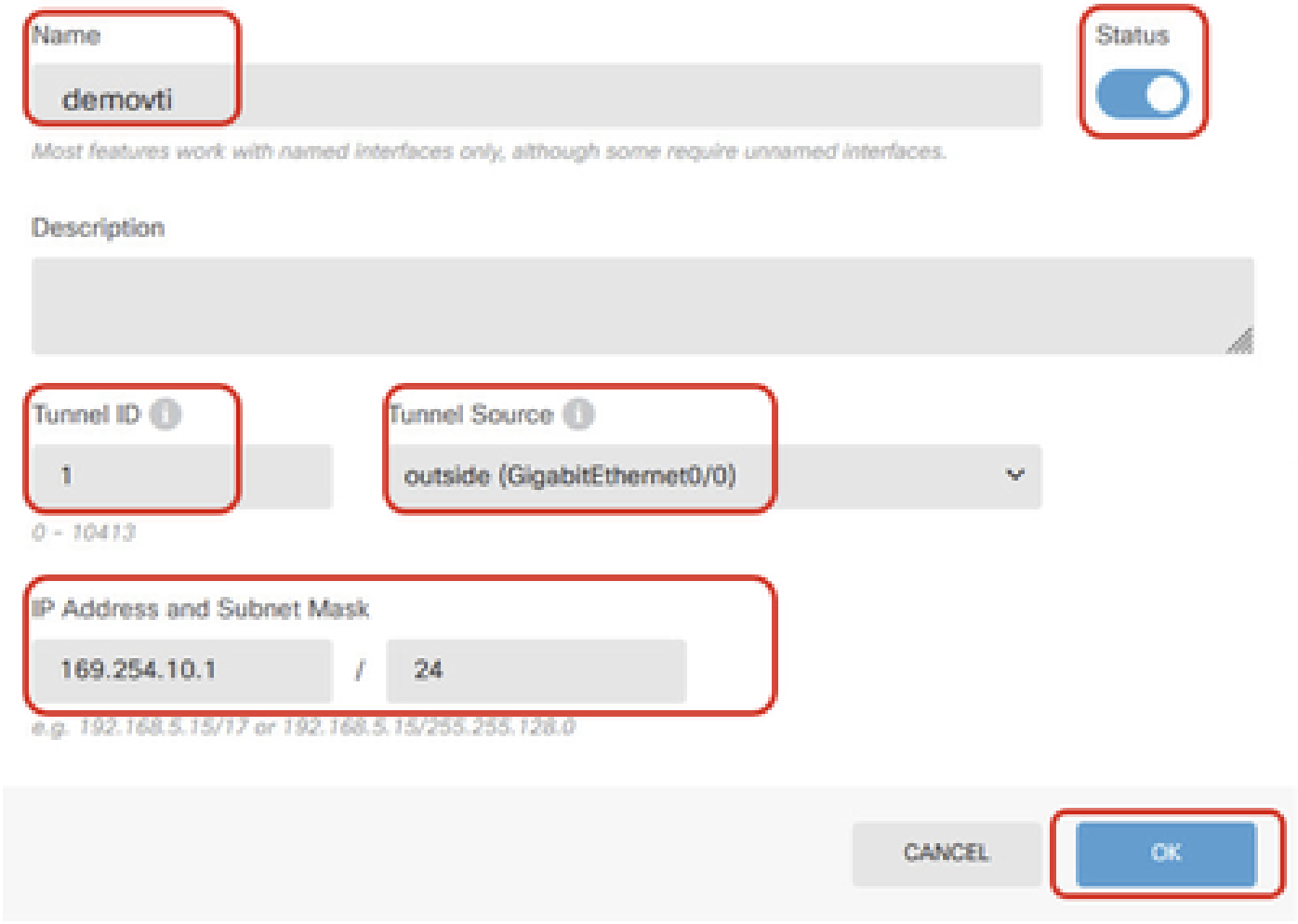
- 接続プロファイル名：Demo_S2S
- タイプ：ルートベース(VTI)
- Local VPN Access Interface：ドロップダウンリストをクリックし、次に**Create new Virtual Tunnel Interface**をクリックします。



Create_VTI_in_VPN_ウィザード

ステップ 3.6：新しいVTIを作成するために必要な情報を提供します。 [OK] ボタンをクリックします。

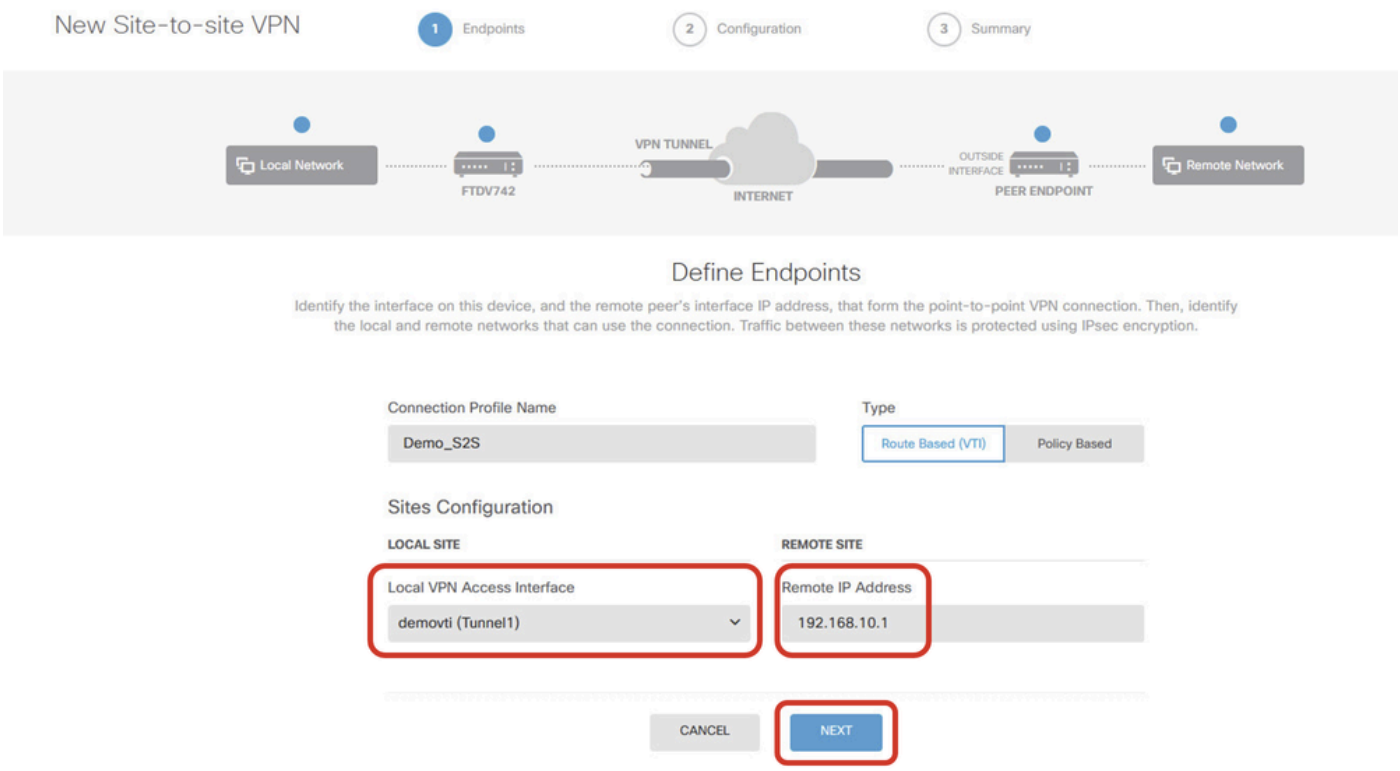
- 名前： demovti
- トンネルID:1
- トンネル送信元：外部(GigabitEthernet0/0)
- IPアドレスとサブネットマスク：169.254.10.1/24
- ステータス：スライダをクリックして有効の位置にします。



作成_VTI_詳細

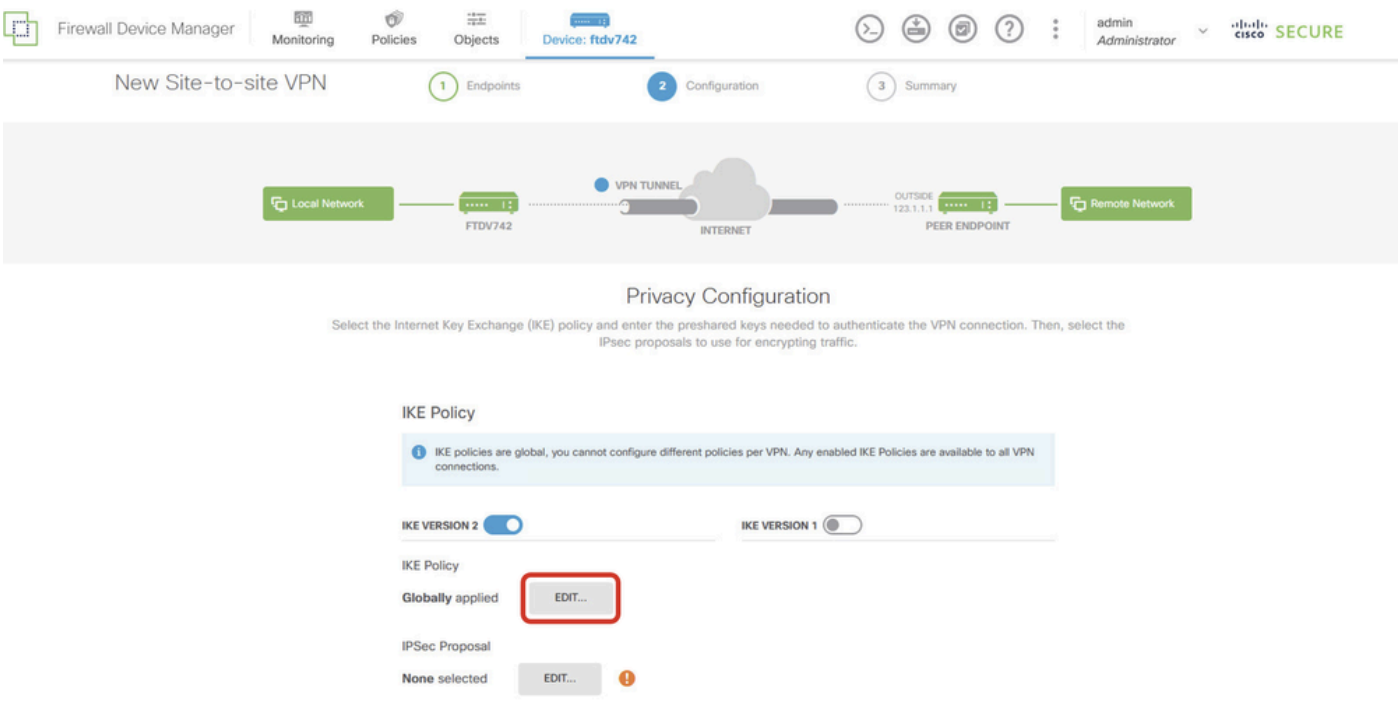
ステップ 3.7：必要な情報を引き続き入力します。 [Next] ボタンをクリックします。

- ローカルVPNアクセスインターフェイス：demovti（ステップ3.6で作成）
- リモートIPアドレス：192.168.10.1



VPN_Wizard_Endpoints_ステップ1

ステップ 3.8：IKE Policyに移動します。[Edit] ボタンをクリックします。



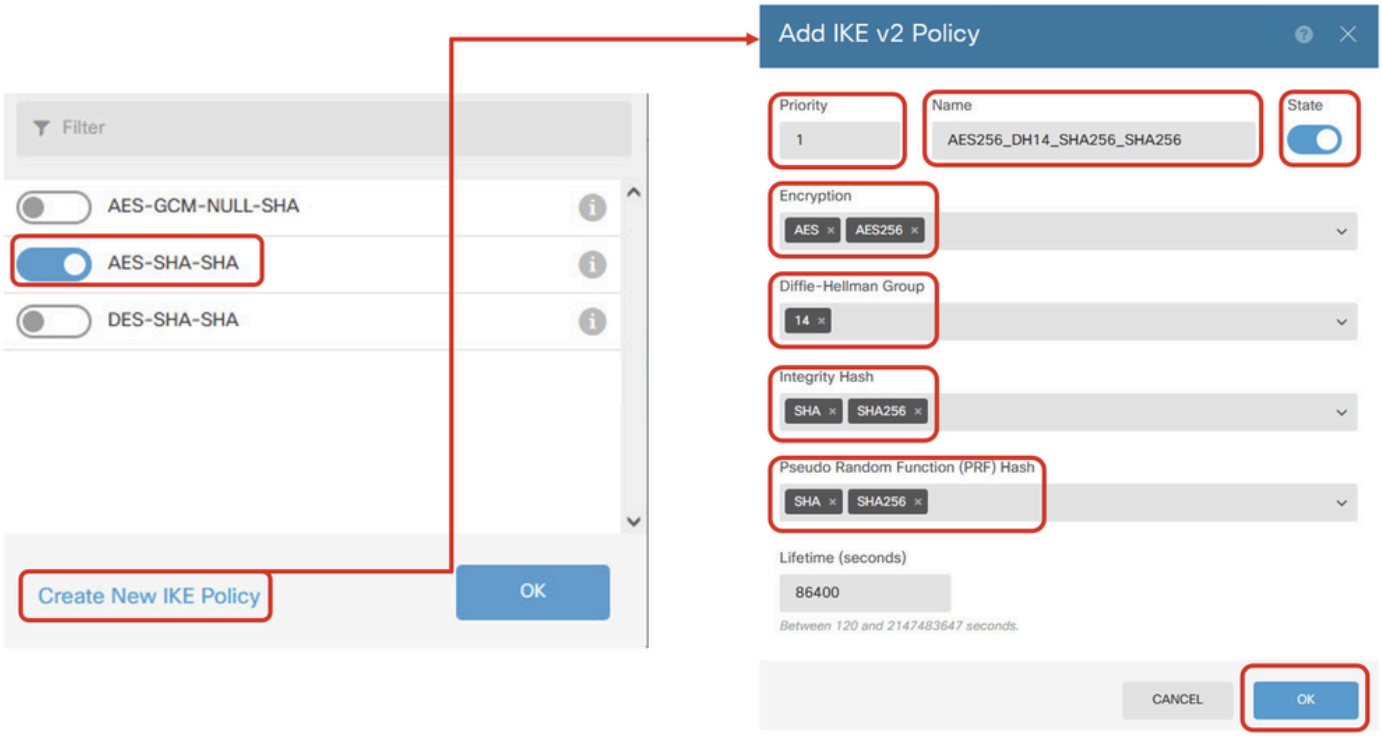
編集_IKE_ポリシー

ステップ 3.9： IKEポリシーの場合は、事前に定義されたポリシーを使用するか、Create New IKE Policyをクリックして新しいポリシーを作成します。

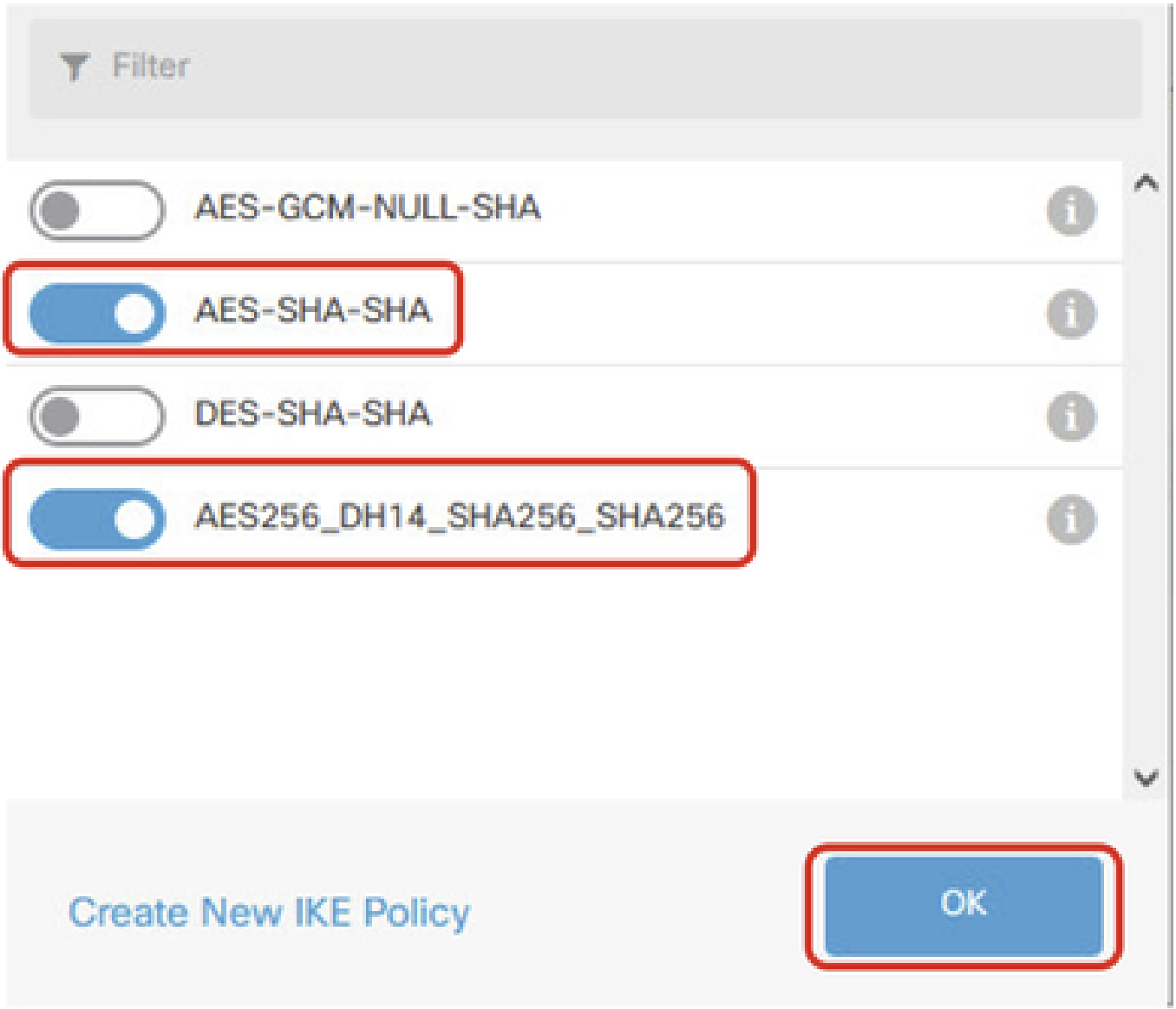
この例では、既存のIKEポリシーAES-SHA-SHAを切り替え、デモ用に新しいIKEポリシーを作成

します。OKボタンをクリックして保存します。

- 名前：AES256_DH14_SHA256_SHA256
- 暗号化：AES、AES256
- DHグループ：14
- 整合性ハッシュ：SHA、SHA256
- PRFハッシュ：SHA、SHA256
- ライフタイム：86400（デフォルト）

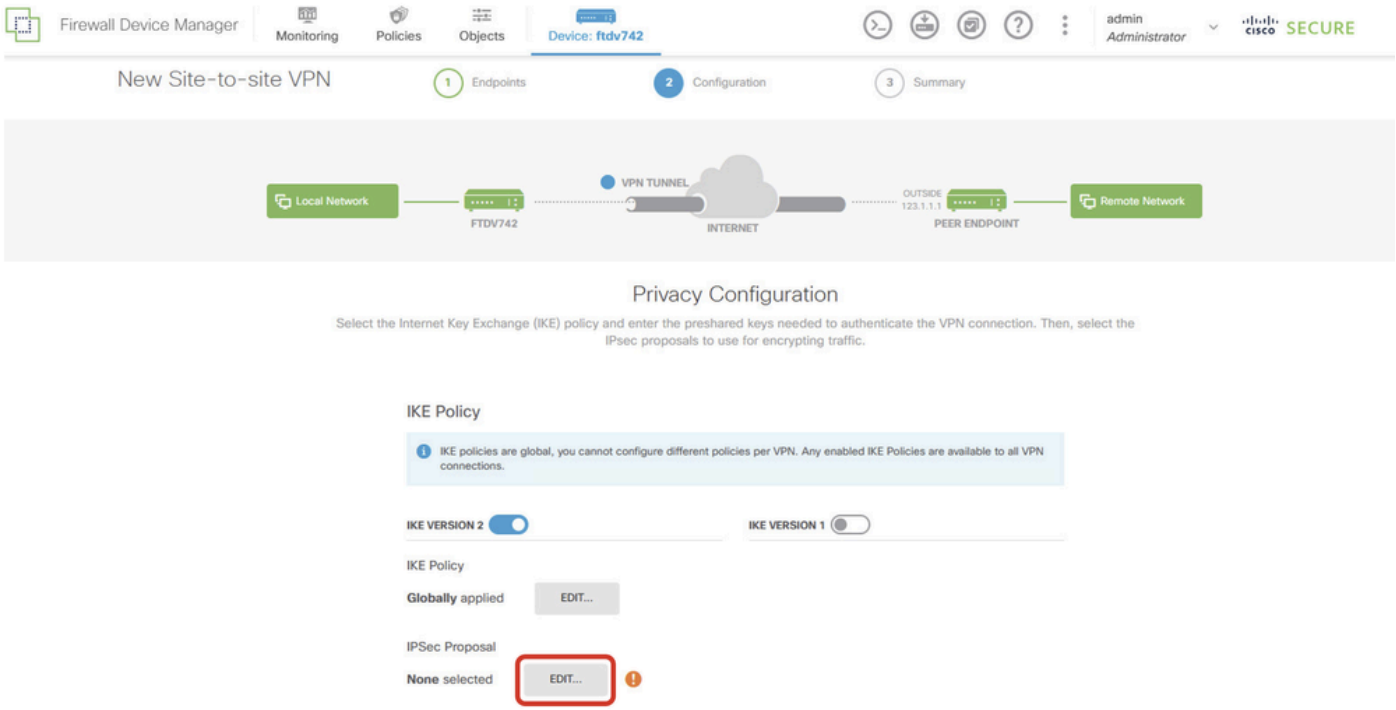


Add_New_IKE_ポリシー



Enable_New_IKE_ポリシー

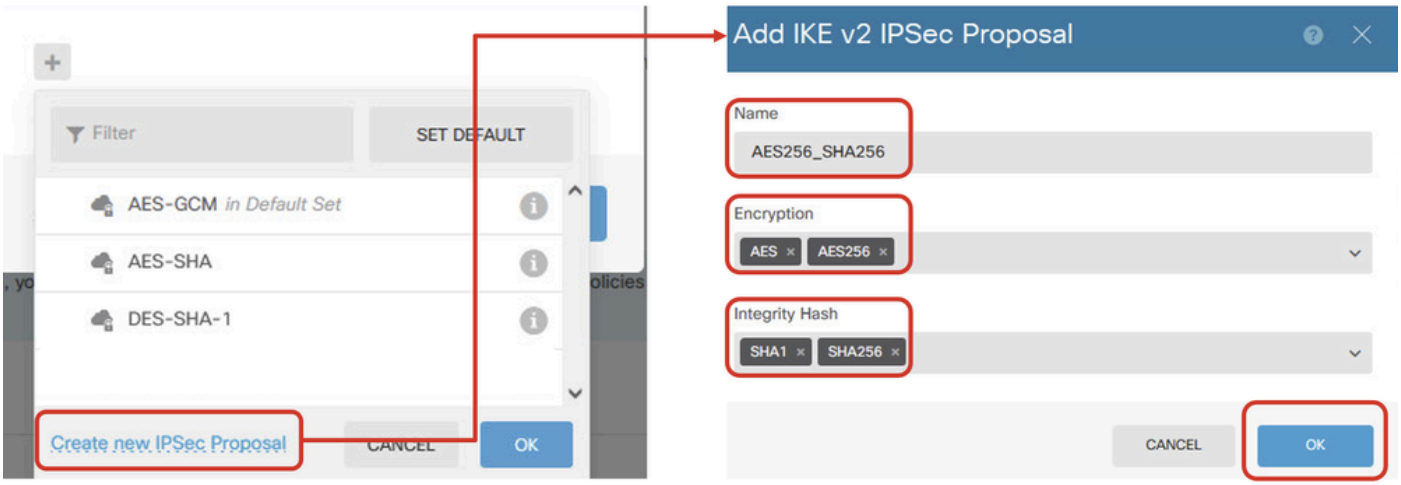
ステップ 3.10： IPSecプロポーザルに移動します。[Edit] ボタンをクリックします。



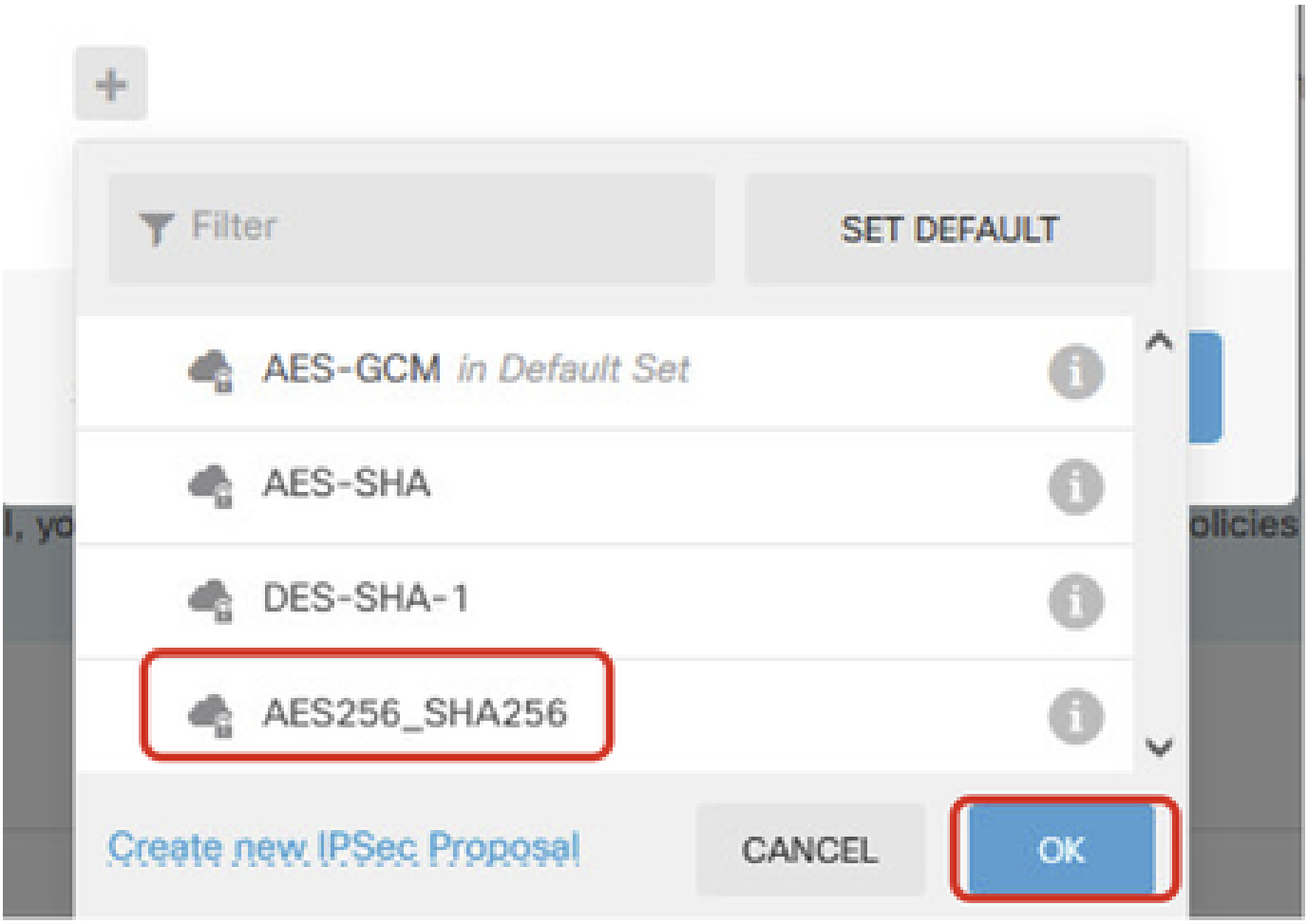
編集_IKE_プロポーザル

ステップ 3.11： IPSecプロポーザルには、事前に定義されたプロポーザルを使用するか、Create new IPSec Proposalをクリックして新しいプロポーザルを作成します。この例では、デモ用に新しいプロファイルを作成します。必要な情報を入力します。OKボタンをクリックして保存します。

- 名前：AES256_SHA256
- 暗号化：AES、AES256
- 整合性ハッシュ：SHA1、SHA256



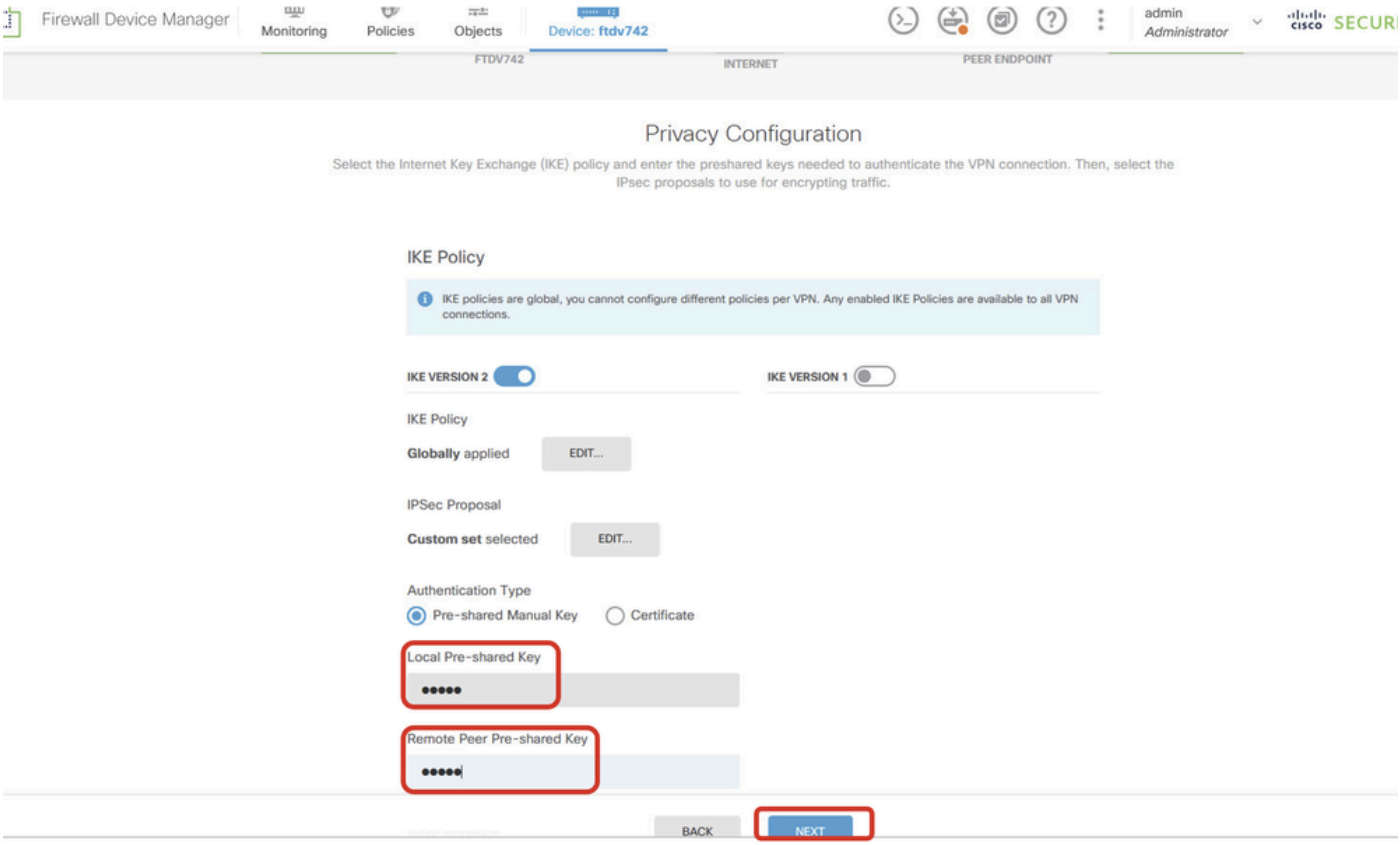
Add_New_IPSec_プロポーザル



Enable_New_IPSec_プロポーザル

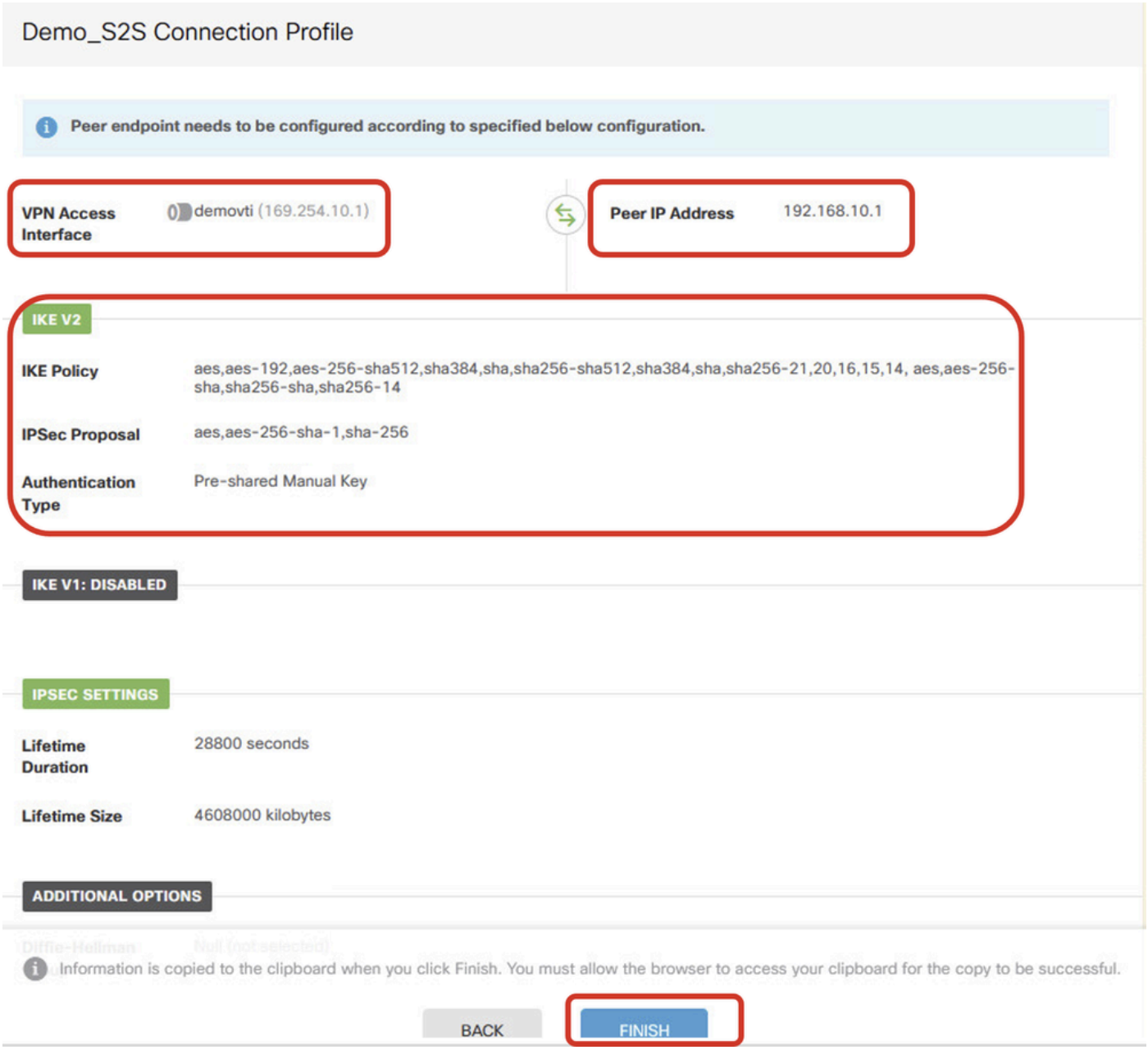
ステップ 3.12：事前共有キーを設定します。[Next] ボタンをクリックします。

この事前共有キーをメモし、後でSite2 FTDで設定します。



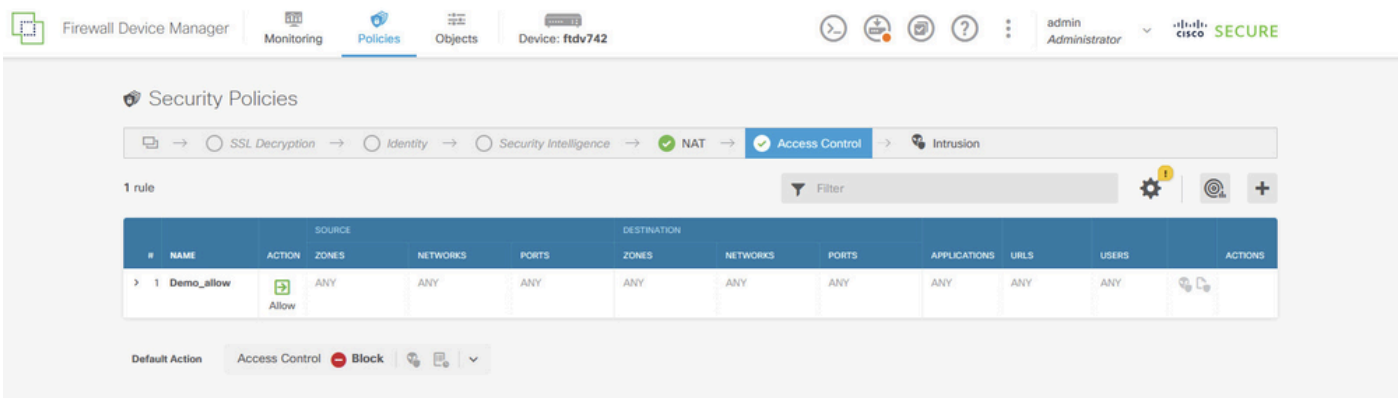
設定_事前共有キー

ステップ 3.13：VPN設定を確認します。変更が必要な場合は、BACKボタンをクリックします。問題がなければ、「FINISH」ボタンをクリックします。



VPN_Wizard_Complete

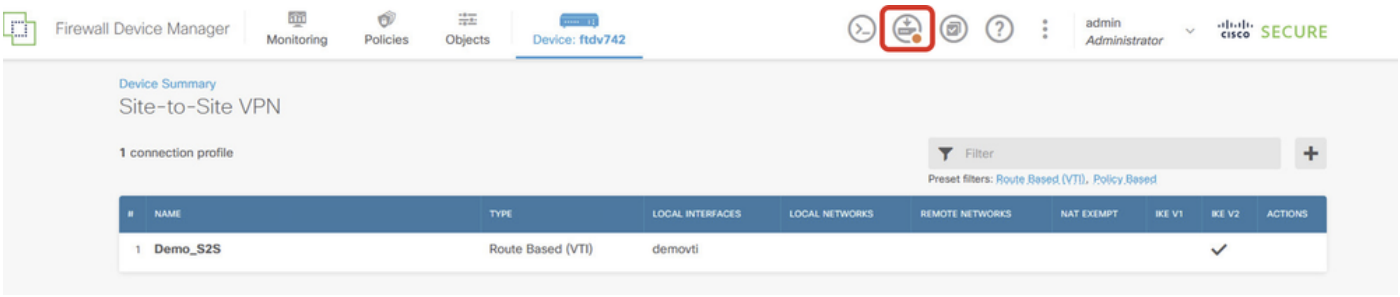
ステップ 3.14：トラフィックがFTDを通過できるようにするには、アクセスコントロールルールを作成します。この例では、デモの目的ですべてを許可します。 実際のニーズに基づいてポリシーを変更します。



アクセス制御ルールの例

ステップ3.15:（オプション）インターネットにアクセスするためにクライアントにダイナミックNATが設定されている場合は、FTDでクライアントトラフィックのNAT免除ルールを設定します。各FTDにはダイナミックNATが設定されていないため、この例では、NAT免除ルールを設定する必要はありません。

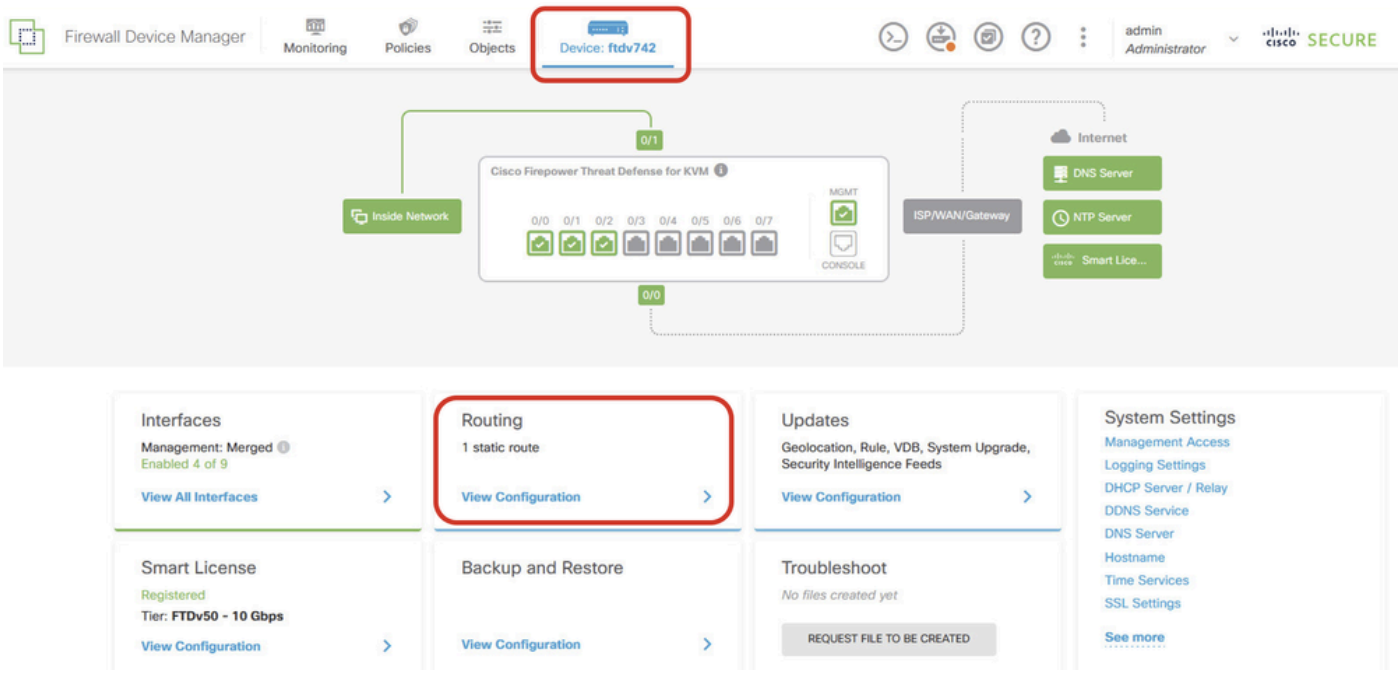
ステップ 3.16：設定変更を導入します。



導入VPNの設定

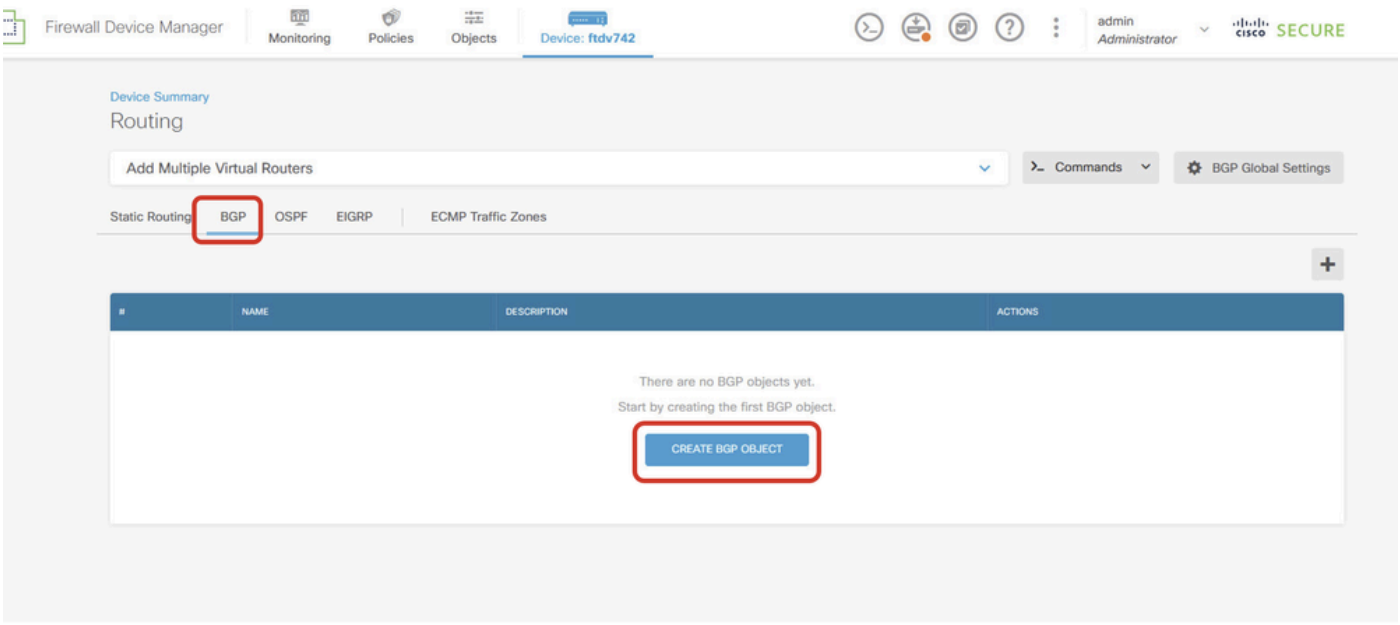
BGPでの設定

ステップ 4： Device > Routingの順に移動します。View Configurationをクリックします。



View_Routing_設定

ステップ 5：BGPタブをクリックし、次にCREATE BGP OBJECTをクリックします。



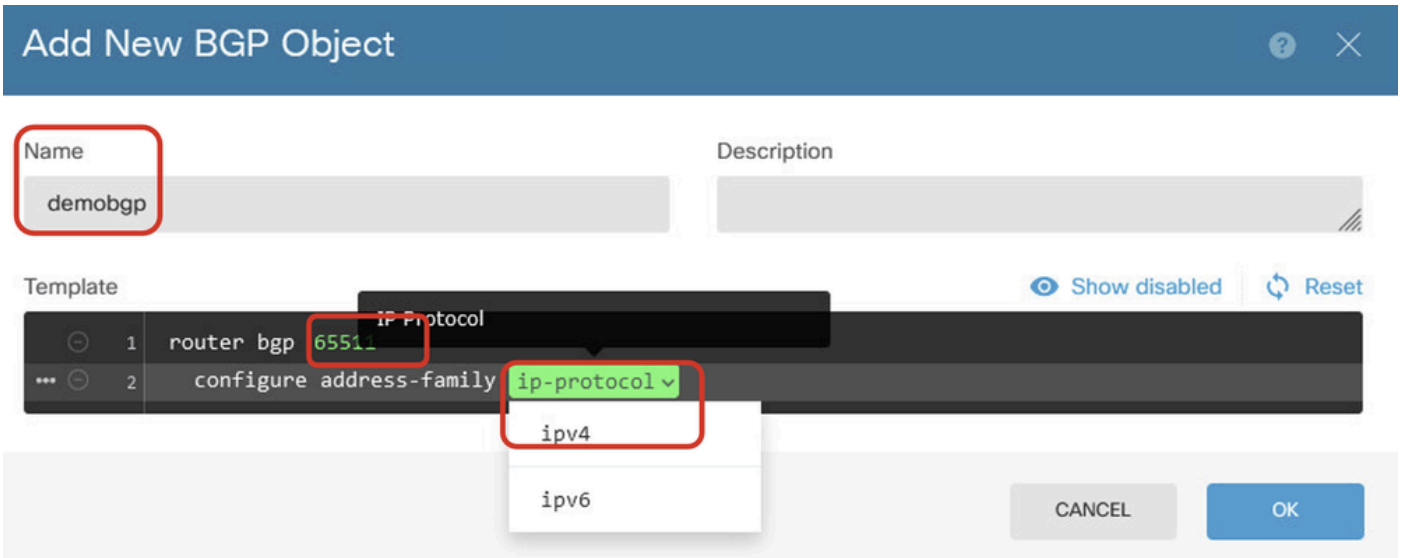
Create_BGP_オブジェクト

手順 6：オブジェクトの名前を指定します。 Templateに移動して設定します。OKボタンをクリックして保存します。

名前： demobgp

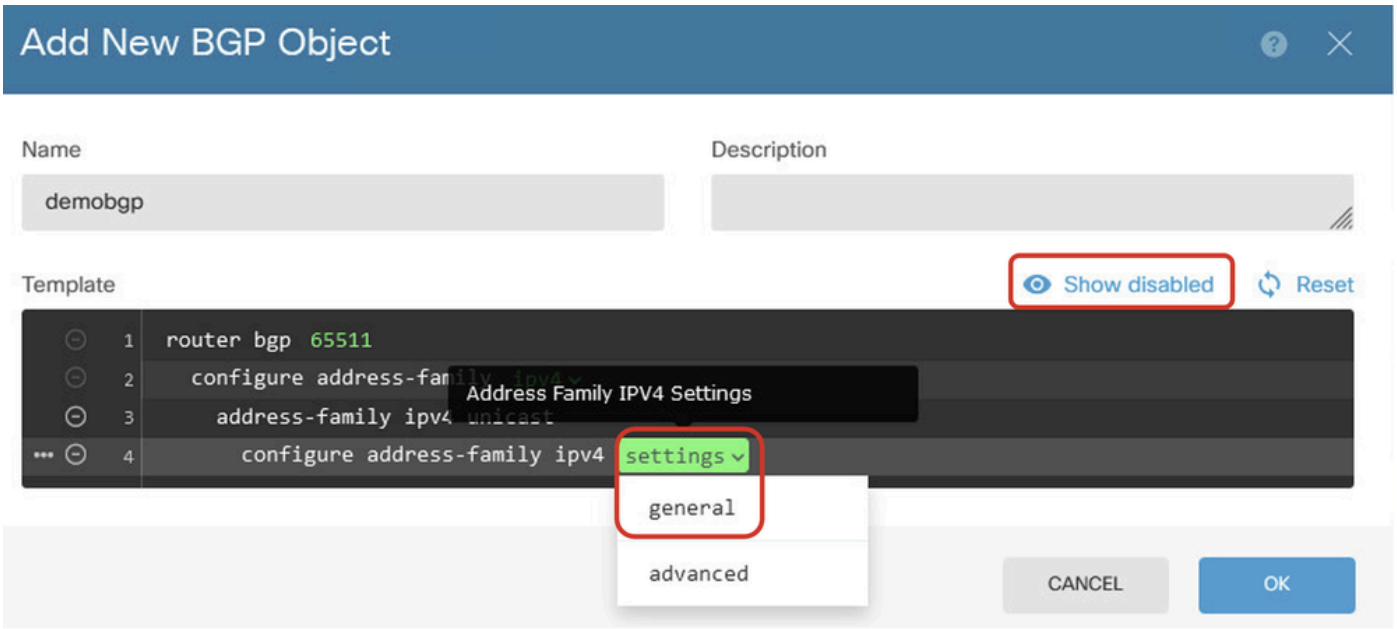
回線1:AS番号を設定します。as-numberをクリックします。ローカルAS番号を手動で入力します。この例では、Site1 FTDのAS番号は65511です。

2行目：IPプロトコルを設定します。ip-protocolをクリックします。ipv4を選択します。



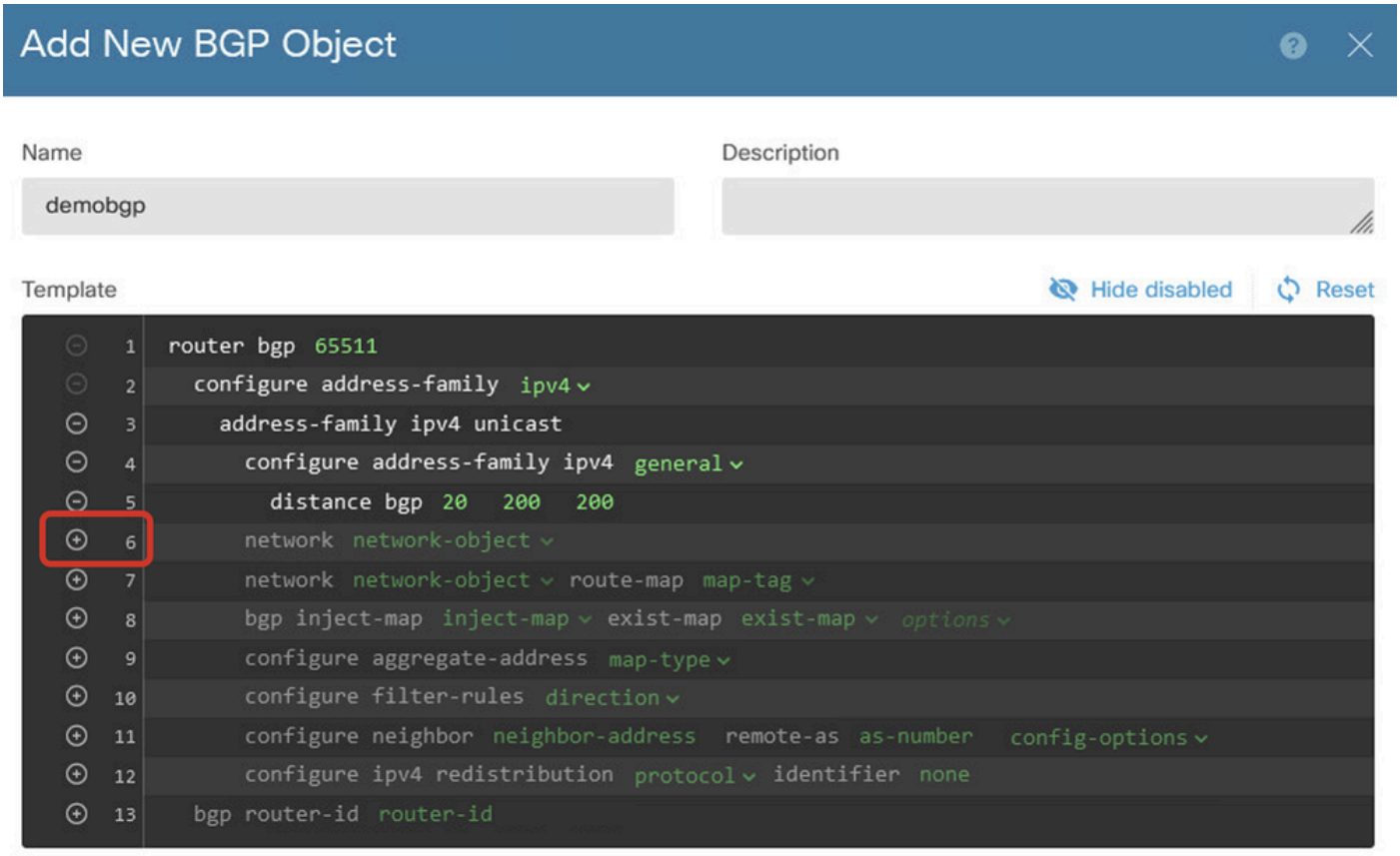
作成BGPオブジェクトASNumber_プロトコル

4行目：さらに設定します。settingsをクリックし、generalを選択して、Show disabledをクリックします。

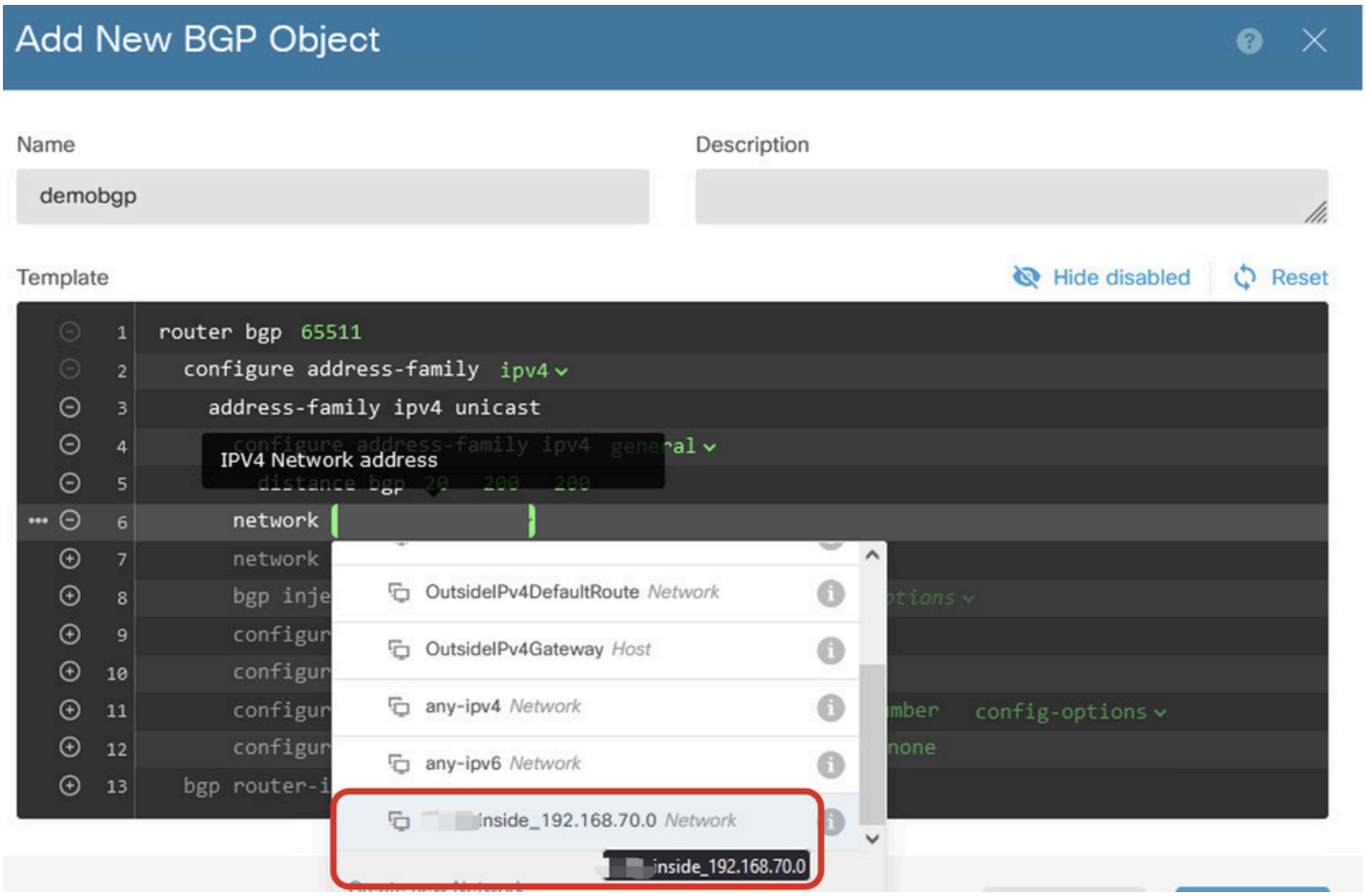


作成BGPオブジェクトのアドレス設定

回線6:+アイコンをクリックして、回線でのBGPネットワークの設定を有効にします。network-objectをクリックします。既存の使用可能なオブジェクトを表示し、選択することができます。この例では、オブジェクト名inside_192.168.70.0（ステップ3.2で作成）を選択します。

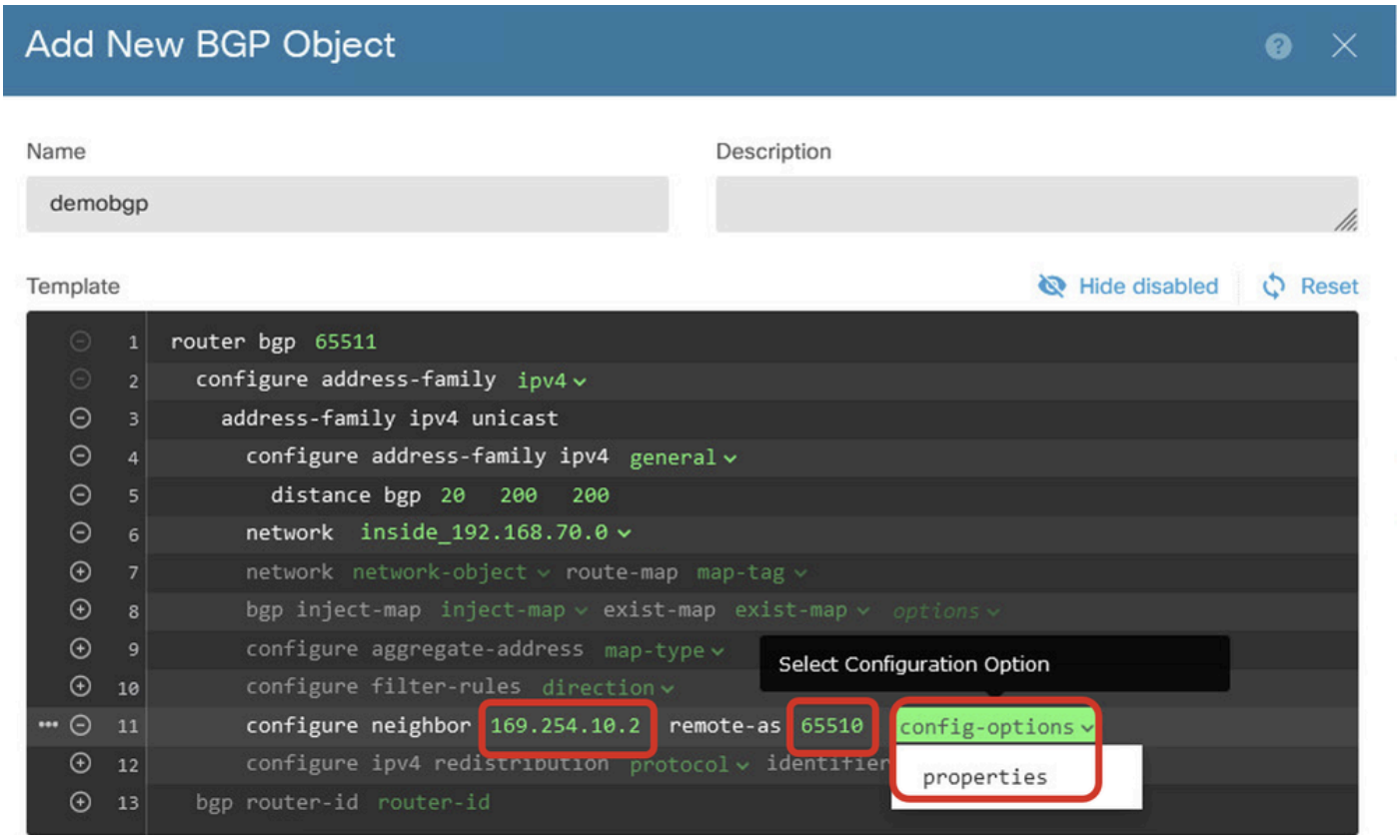


作成BGPオブジェクト追加ネットワーク



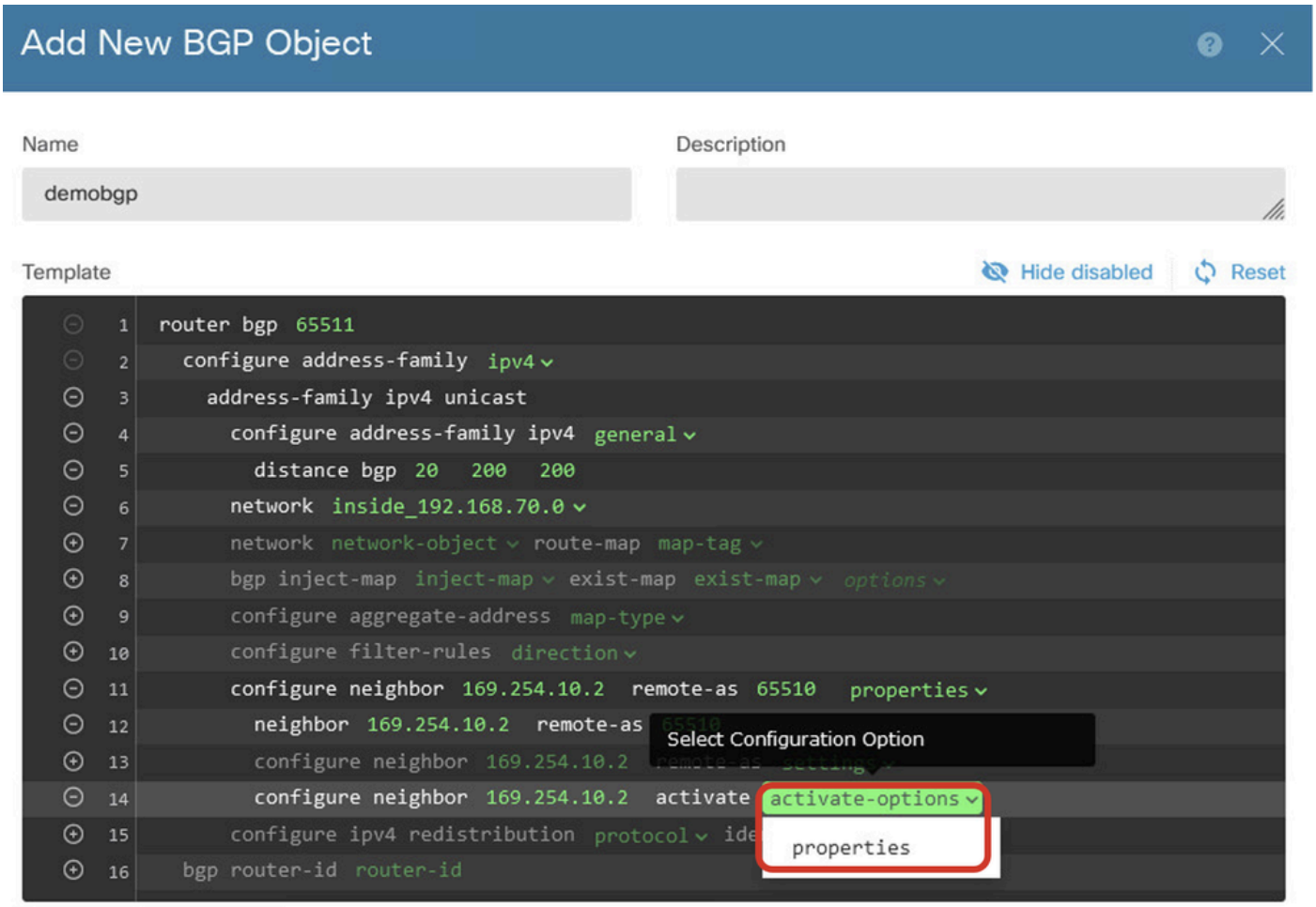
作成BGPオブジェクト追加ネットワーク2

回線11:+アイコンをクリックして、回線でBGPネイバー関連情報を設定できるようにします。neighbor-addressをクリックし、ピアのBGPネイバーアドレスを手動で入力します。この例では、169.254.10.2（Site2 FTDのVTI IPアドレス）です。as-numberをクリックし、ピアのAS番号を手動で入力します。この例では、65510はSite2 FTD用です。config-optionsをクリックして、propertiesを選択します。



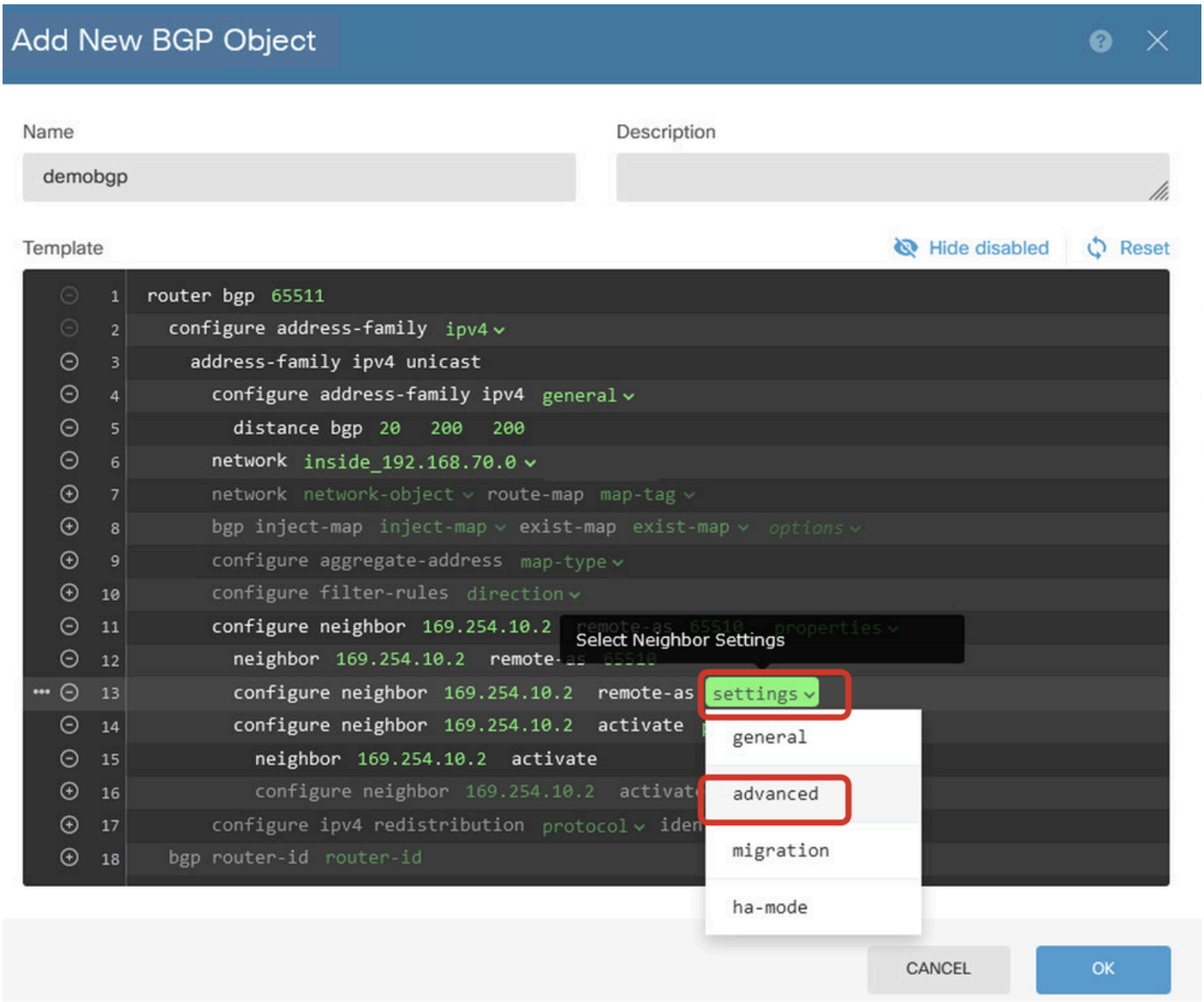
Create_BGP_Object_NeighborSetting（設定）

回線14:+アイコンをクリックして、回線でネイバーの一部のプロパティを設定できるようにします。activate-optionsをクリックして、propertiesを選択します。



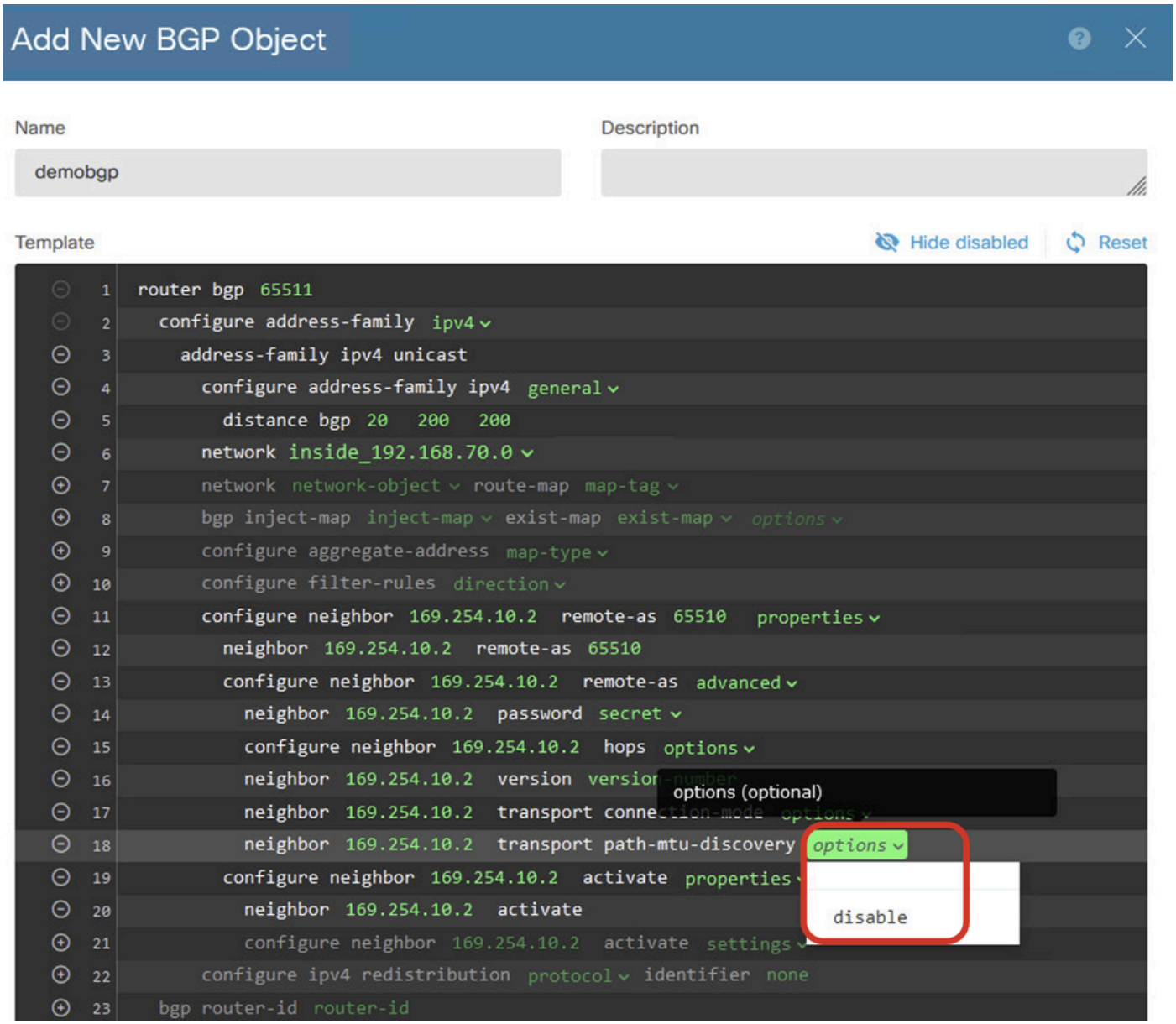
Create_BGP_Object_NeighborSetting_プロパティ

品目13:+アイコンをクリックして、品目に高度なオプションを表示できるようにします。settingsをクリックして、advancedを選択します。



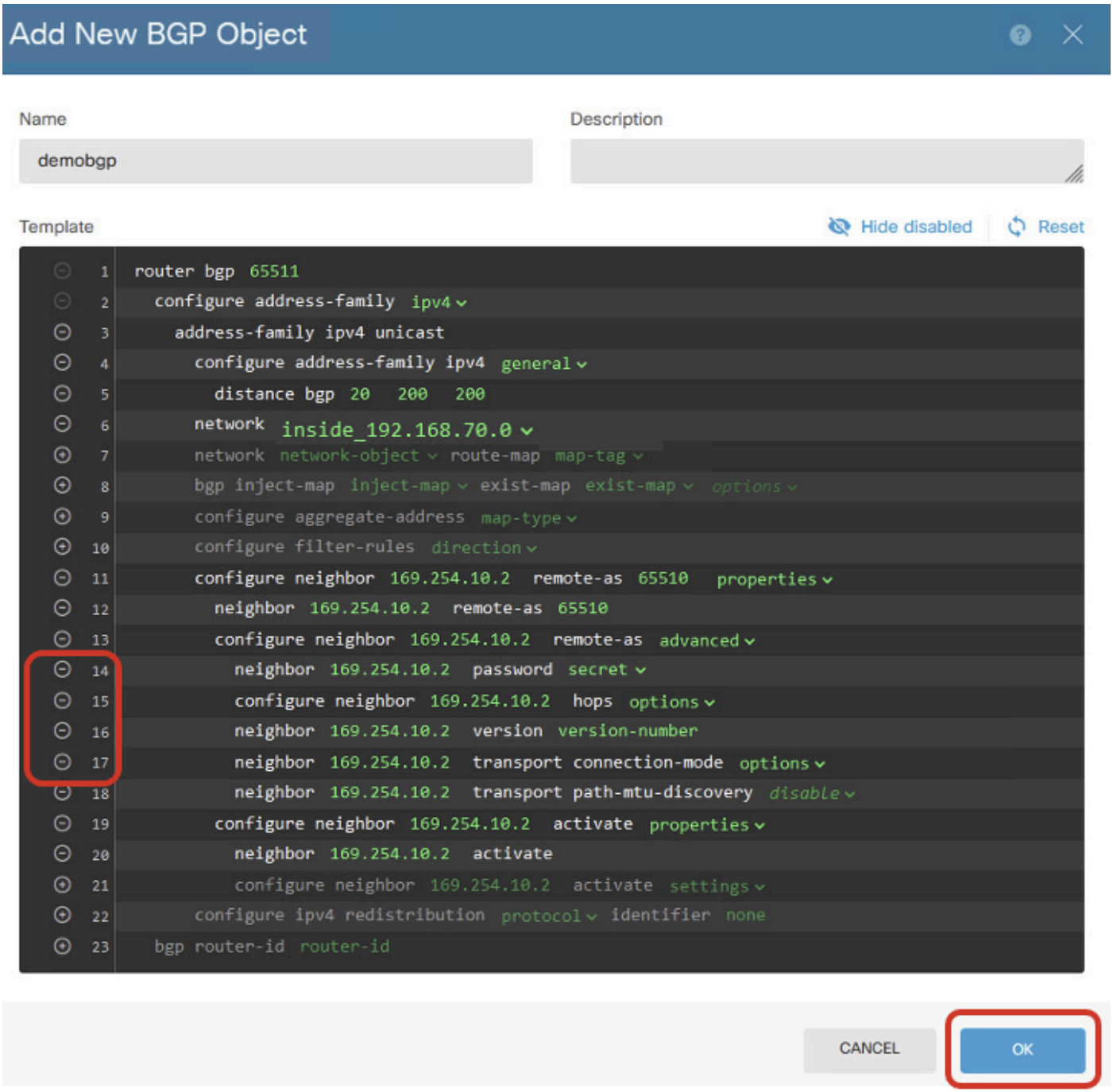
Create_BGP_Object_NeighborSetting_Properties_Advanced（高度な設定）

品目18:optionsをクリックし、disableを選択して、パスMTUディスカバリを無効にします。



Create_BGP_Object_NeighborSetting_Properties_Advanced_PMDプロパティ

回線14、15、16、17:-ボタンをクリックして、回線を無効にします。次に、OKボタンをクリックしてBGPオブジェクトを保存します。



Create_BGP_Object_DisableLines (オプション)

次に、この例のBGP設定の概要を示します。実際のニーズに基づいて、その他のBGP設定を行うことができます。

Name

demobgp

Description

Template

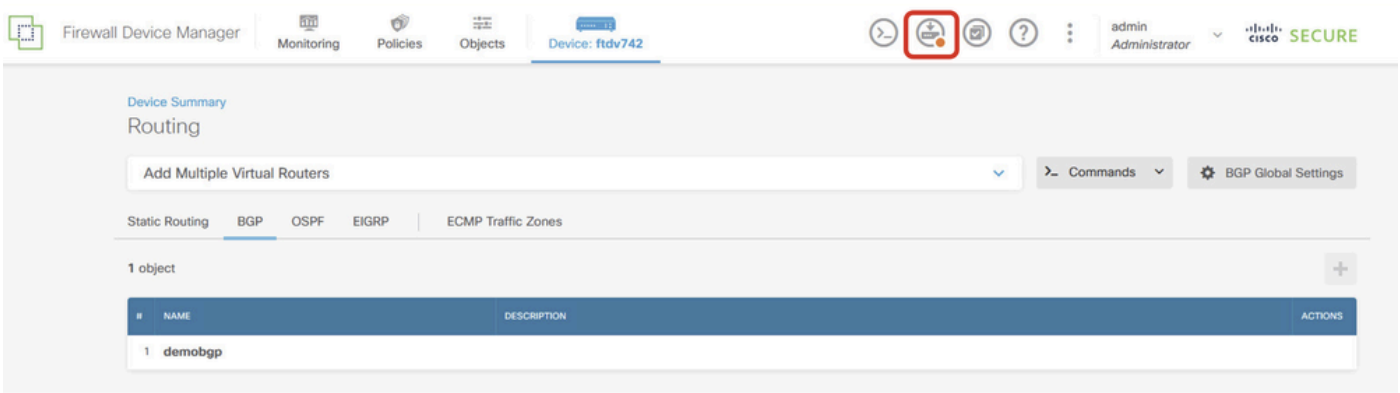
Hide disabled Reset

```
router bgp 65511
  configure address-family ipv4
    address-family ipv4 unicast
      configure address-family ipv4 general
        distance bgp 20 200 200
      network inside_192.168.70.0
      network network-object route-map map-tag
      bgp inject-map inject-map exist-map exist-map options
      configure aggregate-address map-type
      configure filter-rules direction
      configure neighbor 169.254.10.2 remote-as 65510 properties
        neighbor 169.254.10.2 remote-as 65510
        configure neighbor 169.254.10.2 remote-as advanced
          neighbor 169.254.10.2 password secret
          configure neighbor 169.254.10.2 hops options
          neighbor 169.254.10.2 version version-number
          neighbor 169.254.10.2 transport connection-mode options
          neighbor 169.254.10.2 transport path-mtu-discovery disable
        configure neighbor 169.254.10.2 activate properties
          neighbor 169.254.10.2 activate
          configure neighbor 169.254.10.2 activate settings
      configure ipv4 redistribution protocol identifier none
  bgp router-id router-id
```

CANCEL OK

Create_BGP_Object_Final_の概要

手順 7：BGP設定の変更を導入します。



Deploy_BGP_設定

ステップ 8：これで、Site1 FTDの設定が完了しました。

Site2 FTD VPNおよびBGPを設定するには、Site2 FTDの対応するパラメータを使用して、ステップ3 ~ 7を繰り返します。

CLIでのSite1 FTDとSite2 FTDの設定の概要

サイト1 FTD	サイト2 FTD
NGFWバージョン7.4.2 interface GigabitEthernet0/0 nameif外部 ctsマニュアル propagate sgt preserve-untag（sgtの保存/タグ解除を伝播） policy static sgt disabled trusted（信頼できるポリシースタティックsgt無効） セキュリティレベル0 ip address 192.168.30.1 255.255.255.0 interface GigabitEthernet0/2 nameif内部 セキュリティレベル0 ip address 192.168.70.1 255.255.255.0 interface Tunnel1 nameif demovti ip address 169.254.10.1 255.255.255.0 トンネル送信元インターフェイスOutside tunnel destination 192.168.10.1 トンネルモードipsec ipv4 tunnel protection ipsec profile ipsec_profile|e4084d322d オブジェクトネットワークOutsideIPv4ゲートウェイ ホスト192.168.30.3 オブジェクトネットワークinside_192.168.70.0 サブネット192.168.70.0 255.255.255.0 access-group NGFW_ONBOX_ACLグローバル access-list NGFW_ONBOX_ACL remark rule-id 268435457：アクセスポリシー：NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL高度な信頼オブジェクトグループ |acSvcg-268435457 ifc inside any ifc outside any rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id	NGFWバージョン7.4.2 interface GigabitEthernet0/0 nameif外部 ctsマニュアル propagate sgt preserve-untag（sgtの保存/タグ解除を伝播） policy static sgt disabled trusted（信頼できるポリシースタティックsgt無効） セキュリティレベル0 ip address 192.168.10.1 255.255.255.0 interface GigabitEthernet0/2 nameif内部 セキュリティレベル0 ip address 192.168.50.1 255.255.255.0 interface Tunnel1 nameif demovti25 ip address 169.254.10.2 255.255.255.0 トンネル送信元インターフェイスOutside tunnel destination 192.168.30.1 トンネルモードipsec ipv4 tunnel protection ipsec profile ipsec_profile|e4084d322d オブジェクトネットワークOutsideIPv4ゲートウェイ ホスト192.168.10.3 オブジェクトネットワークinside_192.168.50.0 サブネット192.168.50.0 255.255.255.0 access-group NGFW_ONBOX_ACLグローバル access-list NGFW_ONBOX_ACL remark rule-id 268435457：アクセスポリシー：NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435457: L5 RULE: Inside_Outside_Rule access-list NGFW_ONBOX_ACL高度な信頼オブジェクトグループ |acSvcg-268435457 ifc inside any ifc outside any rule-id 268435457 event-log both access-list NGFW_ONBOX_ACL remark rule-id 268435458：アクセスポリシー：NGFW_Access_Policy

268435458：アクセスポリシー：NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 268435458:L5 RULE:Demo_allow access-list NGFW_ONBOX_ACL advanced permit object-groupコマンドを発行して、 |acSvcg-268435458 any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1：アクセスポリシー：NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule access-list NGFW_ONBOX_ACL advanced deny ip any any rule-id 1 router bgp 65511 bgp log-neighbor-changes bgp router-id vrf auto-assign（VRF自動割り当て） address-family ipv4 unicast neighbor 169.254.10.2 remote-as 65510 ネイバー169.254.10.2 transport path-mtu-discovery disable neighbor 169.254.10.2 activate network 192.168.70.0 no auto-summary no synchronization exit-address-family 外部ルート0.0.0.0 0.0.0.0 192.168.30.3 1 crypto ipsec ikev2 ipsec-proposal AES256_SHA256 プロトコルesp暗号化aes-256 aes プロトコルesp整合性sha-256 sha-1 crypto ipsec profile ipsec_profile|e4084d322d set ikev2 ipsec-proposal AES256_SHA256 set security-association lifetime kilobytes4608000 set security-association lifetime seconds 28800（セキュリティアソシエーションのライフタイムを秒数で設定） crypto ipsec security-association pmtu-aging infinite クリプトikev2ポリシー1 暗号化aes-256 aes 整合性sha256 sha group 14 prf sha256 sha lifetime seconds 86400（ライフタイム秒数） crypto ikev2 policy 20	access-list NGFW_ONBOX_ACL remark rule-id 268435458:L5 RULE:Demo_allow access-list NGFW_ONBOX_ACL advanced permit object-groupコマンドを発行して、 |acSvcg-268435458 any rule-id 268435458 event-log both access-list NGFW_ONBOX_ACL remark rule-id 1：アクセスポリシー：NGFW_Access_Policy access-list NGFW_ONBOX_ACL remark rule-id 1: L5 RULE: DefaultActionRule access-list NGFW_ONBOX_ACL advanced deny ip any any rule-id 1 router bgp 65510 bgp log-neighbor-changes bgp router-id vrf auto-assign（VRF自動割り当て） address-family ipv4 unicast neighbor 169.254.10.1 remote-as 65511 ネイバー169.254.10.1 transport path-mtu-discovery disable neighbor 169.254.10.1 activate network 192.168.50.0 no auto-summary no synchronization exit-address-family 外部ルート0.0.0.0 0.0.0.0 192.168.10.3 1 crypto ipsec ikev2 ipsec-proposal AES256_SHA256 プロトコルesp暗号化aes-256 aes プロトコルesp整合性sha-256 sha-1 crypto ipsec profile ipsec_profile|e4084d322d set ikev2 ipsec-proposal AES256_SHA256 set security-association lifetime kilobytes4608000 set security-association lifetime seconds 28800（セキュリティアソシエーションのライフタイムを秒数で設定） crypto ipsec security-association pmtu-aging infinite クリプトikev2ポリシー1 暗号化aes-256 aes 整合性sha256 sha group 14 prf sha256 sha lifetime seconds 86400（ライフタイム秒数） crypto ikev2 policy 20

暗号化aes-256 aes-192 aes 整合性sha512 sha384 sha256 sha グループ21 20 16 15 14 prf sha512 sha384 sha256 sha lifetime seconds 86400（ライフタイム秒数） crypto ikev2 enable outside グループポリシー |s2sGP|192.168.10.1内部 グループポリシー |s2sGP|192.168.10.1属性 VPNトンネルプロトコルIKEV2 tunnel-group 192.168.10.1タイプipsec-l2l tunnel-group 192.168.10.1一般属性 デフォルトグループポリシー |s2sGP|192.168.10.1 tunnel-group 192.168.10.1 ipsec属性 ikev2リモート認証事前共有キー***** ikev2ローカル認証事前共有キー*****	暗号化aes-256 aes-192 aes 整合性sha512 sha384 sha256 sha グループ21 20 16 15 14 prf sha512 sha384 sha256 sha lifetime seconds 86400（ライフタイム秒数） crypto ikev2 enable outside グループポリシー |s2sGP|192.168.30.1内部 グループポリシー |s2sGP|192.168.30.1属性 VPNトンネルプロトコルIKEV2 tunnel-group 192.168.30.1タイプipsec-l2l tunnel-group 192.168.30.1一般属性 デフォルトグループポリシー |s2sGP|192.168.30.1 tunnel-group 192.168.30.1 ipsec属性 ikev2リモート認証事前共有キー***** ikev2ローカル認証事前共有キー*****

確認

ここでは、設定が正常に機能しているかどうかを確認します。

ステップ 1：コンソールまたはSSHを使用して各FTDのCLIに移動し、show crypto ikev2 saコマンドとshow crypto ipsec saコマンドを使用してフェーズ1とフェーズ2のVPNステータスを確認します。

サイト1 FTD	サイト2 FTD
ftdv742# show crypto ikev2 sa IKEv2 SA: セッションID:134、ステータス：アクティブ、IKEカウント：1、子カウント：1 Tunnel-idローカルリモートfvrf/ivrfステータスの役割 563984431 192.168.30.1/500 192.168.10.1/500グローバル/グローバル対応レスポンダ 暗号化：AES-CBC、キーサイズ：256、ハッシュ：SHA256、DHグループ：14、認証記号：PSK、認証検証：PSK	ftdv742# show crypto ikev2 sa IKEv2 SA: セッションID:13、ステータス：アクティブ、IKEカウント：1、子カウント：1 Tunnel-idローカルリモートfvrf/ivrfステータスの役割 339797985 192.168.10.1/500 192.168.30.1/500グローバル/グローバル準備イニシエータ 暗号化：AES-CBC、キーサイズ：256、ハッシュ：SHA256、DHグループ：14、認証記号：PSK、認証検証：PSK 寿命/アクティブ時間：86400/74099秒 子sa：ローカルセレクタ0.0.0.0/0 ~ 255.255.255.255/65535

寿命/アクティブ時間：86400/5145秒 子sa：ローカルセレクタ0.0.0.0/0 ~ 255.255.255.255/65535 リモートセレクタ0.0.0.0/0 ~ 255.255.255.255/65535 ESP spi in/out:0xf0c4239d/0xb7b5b38b	リモートセレクタ0.0.0.0/0 ~ 255.255.255.255/65535 ESP spi in/out:0xb7b5b38b/0xf0c4239d
ftdv742# show crypto ipsec sa インタフェース： demovti 暗号マップタグ：__vti-crypto-map-Tunnel1-0-1、シーケンス番号：65280、ローカルアドレス：192.168.30.1 Protected vrf(ivrf)：グローバル ローカルid (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) リモートid (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) current_peer:192.168.10.1 #pktsカプセル化：5720、#pkts暗号化：5720、#pktsダイジェスト：5720 #pktsデキャップ：5717、#pkts復号化：5717、#pkts検証：5717 圧縮#pkts: 0、圧縮解除#pkts: 0 #pkts圧縮なし： 5720、#pkts圧縮に失敗： 0、#pkts圧縮解除に失敗： 0 #pre-frag成功： 0、#pre-frag失敗： 0、作成#fragments: 0 送信#PMTUs: 0、#PMTUs rcvd: 0、再構成が必要な#decapsulatedフラグ： 0 #TFC rcvd: 0、送信#TFC: 0 #Valid ICMPエラー：0、#Invalid ICMPエラー：0 #sendエラー： 0、#recvエラー： 0 ローカル暗号化エンドポイント：192.168.30.1/500、リモート暗号化エンドポイント：192.168.10.1/500 パスmtu 1500、ipsecオーバーヘッド78(44)、メディアmtu 1500 残りpmtu時間（秒）:0、DFポリシー：copy-df ICMPエラー検証：無効、TFCパケット：無効	ftdv742# show crypto ipsec sa インタフェース： demovti25 暗号マップタグ：__vti-crypto-map-Tunnel1-0-1、シーケンス番号：65280、ローカルアドレス：192.168.10.1 Protected vrf(ivrf)：グローバル ローカルid (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) リモートid (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) current_peer:192.168.30.1 #pktsカプセル化：5721、#pkts暗号化：5721、#pktsダイジェスト：5721 #pktsデキャップ：5721、#pkts復号化：5721、#pkts検証：5721 圧縮#pkts: 0、圧縮解除#pkts: 0 #pkts圧縮なし： 5721、#pkts圧縮に失敗： 0、#pkts圧縮解除に失敗： 0 #pre-frag成功： 0、#pre-frag失敗： 0、作成#fragments: 0 送信#PMTUs: 0、#PMTUs rcvd: 0、再構成が必要な#decapsulatedフラグ： 0 #TFC rcvd: 0、送信#TFC: 0 #Valid ICMPエラー：0、#Invalid ICMPエラー：0 #sendエラー： 0、#recvエラー： 0 ローカル暗号化エンドポイント：192.168.10.1/500、リモート暗号化エンドポイント：192.168.30.1/500 パスmtu 1500、ipsecオーバーヘッド78(44)、メディアmtu 1500 残りpmtu時間（秒）:0、DFポリシー：copy-df ICMPエラー検証：無効、TFCパケット：無効

現在のアウトバウンドspi:B7B5B38B 現在の着信spi:F0C4239D inbound esp sas: spi: 0xF0C4239D (4039386013) SAの状態：アクティブ transform:esp-aes-256 esp-sha-256-hmac、圧縮なし 使用中の設定={L2L、トンネル、IKEv2、VTI、} スロット：0、conn_id:266、暗号マップ：__vti-crypto-map-Tunnel1-0-1 saタイミング：残りのキーの有効期間（kB/秒）：(4285389/3722) IVサイズ：16バイト リプレイ検出のサポート：Y アンチリプレイビットマップ： 0xFFFFFFFF 0xFFFFFFFF outbound esp sas： spi: 0xB7B5B38B (3082138507) SAの状態：アクティブ transform:esp-aes-256 esp-sha-256-hmac、圧縮なし 使用中の設定={L2L、トンネル、IKEv2、VTI、} スロット：0、conn_id:266、暗号マップ：__vti-crypto-map-Tunnel1-0-1 saタイミング：残りのキーの有効期間（kB/秒）：(4147149/3722) IVサイズ：16バイト リプレイ検出のサポート：Y アンチリプレイビットマップ： 0x00000000 0x00000001	現在のアウトバウンドspi:F0C4239D 現在の着信spi:B7B5B38B inbound esp sas: spi: 0xB7B5B38B (3082138507) SAの状態：アクティブ transform:esp-aes-256 esp-sha-256-hmac、圧縮なし 使用中の設定={L2L、トンネル、IKEv2、VTI、} スロット：0、conn_id:160、暗号マップ：__vti-crypto-map-Tunnel1-0-1 saタイミング：残りのキーの有効期間（kB/秒）：(3962829/3626) IVサイズ：16バイト リプレイ検出のサポート：Y アンチリプレイビットマップ： 0xFFFFFFFF 0xFFFFFFFF outbound esp sas： spi: 0xF0C4239D (4039386013) SAの状態：アクティブ transform:esp-aes-256 esp-sha-256-hmac、圧縮なし 使用中の設定={L2L、トンネル、IKEv2、VTI、} スロット：0、conn_id:160、暗号マップ：__vti-crypto-map-Tunnel1-0-1 saタイミング：残りのキーの有効期間（kB/秒）：(4101069/3626) IVサイズ：16バイト リプレイ検出のサポート：Y アンチリプレイビットマップ： 0x00000000 0x00000001

ステップ 2： show bgp neighborsコマンドとshow route bgpコマンドを使用してBGPステータスを確認するため、コンソールまたはSSH経由で各FTDのCLIに移動します。

サイト1 FTD	サイト2 FTD
ftdv742# show bgp neighbors BGPネイバーは169.254.10.2、vrf single_vf、リモートAS 65510、外部リンク BGPバージョン4、リモートルータID 192.168.50.1 BGP状態= Established, up for 1d20h 最終読み取り00:00:25、最終書き込み00:00:45、保留時間は180、キープアライブ間隔	ftdv742# show bgp neighbors BGPネイバーは169.254.10.1、vrf single_vf、リモートAS 65511、外部リンク BGPバージョン4、リモートルータID 192.168.70.1 BGP状態= Established, up for 1d20h 最終読み取り00:00:11、最終書き込み00:00:52、保留時間は180、キープアライブ間隔

は60秒 ネイバーセッション： 1アクティブ、マルチセッション対応ではない（無効） ネイバー機能： ルートリフレッシュ：アドバタイズおよび受信（新規） 4オクテットのASN機能：アドバタイズおよび受信 アドレスファミリIPv4ユニキャスト：アドバタイズおよび受信 マルチセッション機能： メッセージ統計： InQの深さは0 OutQの深さは0 送信済み受信 開始日：1 1 通知： 0 0 アップデート：2 2 キープアライブ：2423 2427 ルートリフレッシュ： 0 0 合計：2426 2430 アドバタイズメント実行間隔のデフォルトの最小時間は30秒です アドレスファミリ：IPv4ユニキャスト セッション：169.254.10.2 BGPテーブルバージョン3、ネイバーバージョン3/0 出力キューサイズ：0 Index 1 アップデートグループメンバー1名 送信済み受信 プレフィックスアクティビティ：---- ---- 現在のプレフィクス：1 1（80バイトを消費） プレフィクス合計：1 1 暗黙的な取り消し： 0 0 明示的な撤回： 0 0 最適パスとして使用：n/a 1 マルチパスとして使用：なし0 アウトバウンド受信 ローカルポリシーで拒否されたプレフィックス： -------- ------- このピアからの最適パス：1なし	は60秒 ネイバーセッション： 1アクティブ、マルチセッション対応ではない（無効） ネイバー機能： ルートリフレッシュ：アドバタイズおよび受信（新規） 4オクテットのASN機能：アドバタイズおよび受信 アドレスファミリIPv4ユニキャスト：アドバタイズおよび受信 マルチセッション機能： メッセージ統計： InQの深さは0 OutQの深さは0 送信済み受信 開始日：1 1 通知： 0 0 アップデート：2 2 キープアライブ：2424 2421 ルートリフレッシュ： 0 0 合計： 2427 2424 アドバタイズメント実行間隔のデフォルトの最小時間は30秒です アドレスファミリ：IPv4ユニキャスト セッション：169.254.10.1 BGPテーブルバージョン9、ネイバーバージョン9/0 出力キューサイズ：0 Index 4 アップデートグループメンバーx 4 送信済み受信 プレフィックスアクティビティ：---- ---- 現在のプレフィクス：1 1（80バイトを消費） プレフィクス合計：1 1 暗黙的な取り消し： 0 0 明示的な撤回： 0 0 最適パスとして使用：n/a 1 マルチパスとして使用：なし0 アウトバウンド受信 ローカルポリシーで拒否されたプレフィックス： -------- ------- このピアからの最適パス：1なし

合計：１０ 送信されたアップデート内のNLRIの数：最大1、最小0 アドレストラッキングが有効になっている場合、RIBには169.254.10.2へのルートがあります 確立された接続1、ドロップ0 前回のリセットは行わない Transport(tcp) path-mtu-discoveryがディセーブルになっている グレースフルリスタートが無効	合計：１０ 送信されたアップデート内のNLRIの数：最大1、最小0 アドレストラッキングが有効になっている場合、RIBには169.254.10.1へのルートがあります 接続は4を確立、ドロップ3 セッション1のインターフェイスフラップによる最後の1d21hリセット Transport(tcp) path-mtu-discoveryがディセーブルになっている グレースフルリスタートが無効
ftdv742# show route bgp コード：L – ローカル、C – 接続、S – スタティック、R - RIP、M – モバイル、B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF外部タイプ1、E2 - OSPF外部タイプ2、V - VPN i - IS-IS、su - IS-ISの概要、L1 - IS-ISレベル1、L2 - IS-ISレベル2 ia:IS-ISエリア間、*：候補デフォルト、U：ユーザごとのスタティックルート o:ODR、P：定期的にダウンロードされるスタティックルート、+：複製ルート SI：スタティックInterVRF、BI:BGP InterVRF Gateway of last resort is 192.168.30.3 to network 0.0.0.0 B 192.168.50.0 255.255.255.0 [20/0]経由169.254.10.2、1d20h	ftdv742# show route bgp コード：L – ローカル、C – 接続、S – スタティック、R - RIP、M – モバイル、B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF外部タイプ1、E2 - OSPF外部タイプ2、V - VPN i - IS-IS、su - IS-ISの概要、L1 - IS-ISレベル1、L2 - IS-ISレベル2 ia:IS-ISエリア間、*：候補デフォルト、U：ユーザごとのスタティックルート o:ODR、P：定期的にダウンロードされるスタティックルート、+：複製ルート SI：スタティックInterVRF、BI:BGP InterVRF Gateway of last resort is 192.168.10.3 to network 0.0.0.0 B 192.168.70.0 255.255.255.0 [20/0]経由169.254.10.1、1d20h

ステップ 3：Site1 ClientとSite2 Clientが互いにpingを正常に実行します。

Site1クライアント：

```
Site1_Client#ping 192.168.50.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 31/56/90 ms
```

サイト2クライアント：

```
Site2_Client#ping 192.168.70.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.70.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/39/71 ms
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

これらのdebugコマンドを使用して、VPNセクションのトラブルシューティングを行うことができます。

```
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
debug vti 255
```

これらのdebugコマンドを使用して、BGPセクションのトラブルシューティングを行うことができます。

```
ftdv742# debug ip bgp ?

A.B.C.D    BGP neighbor address
all All    address families
events     BGP events
import     BGP path import across topologies, VRFs or AFs in BGP Inbound information
ipv4       Address family
ipv6       Address family
keepalives BGP keepalives
out        BGP Outbound information
range      BGP dynamic range
rib-filter Next hop route watch filter events
updates    BGP updates
vpnv4      Address family
vpnv6      Address family
vrf        VRF scope
<cr>
```

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。