FDMによって管理されるFTDでのVRF対応ルートベースのサイト間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VRF対応のルートベースのサイト間VPN(VPN)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の基本的な知識
- Virtual Routing and Forwarding(VRF)の基本的な知識
- 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
- Cisco ASAvバージョン9.20.3

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。

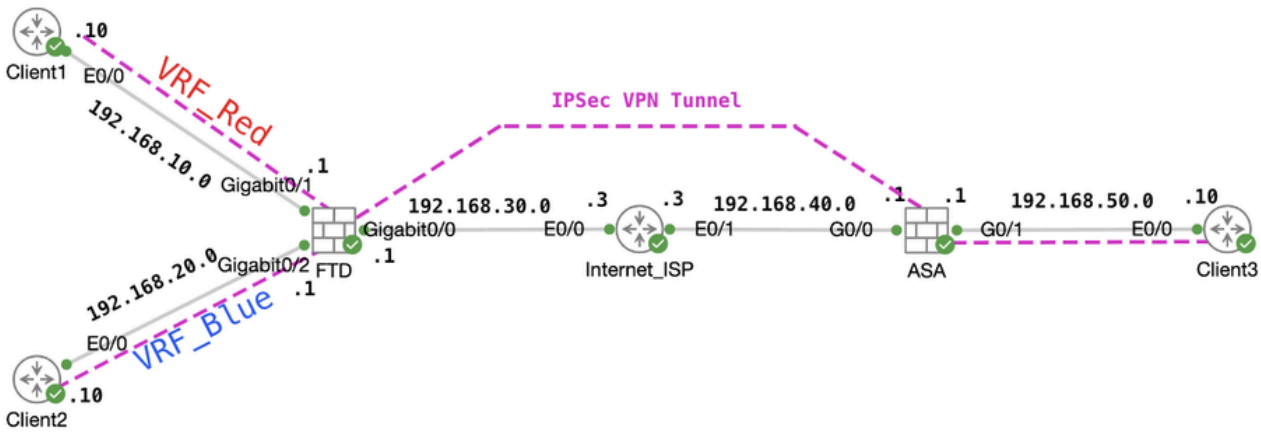
背景説明

Firepower Device Manager(FDM)のVirtual Routing and Forwarding(VRF)を使用すると、単一のFirepower Threat Defense(FTD)デバイス上に複数の隔離されたルーティングインスタンスを作成できます。各VRFインスタンスは、独自のルーティングテーブルを持つ別個の仮想ルータとして動作し、ネットワークトラフィックの論理的な分離を可能にし、拡張されたセキュリティおよびトラフィック管理機能を提供します。

このドキュメントでは、VTIを使用してVRF対応IPSec VPNを設定する方法について説明します。FTDの背後には、VRF RedネットワークとVRF Blueネットワークがあります。VRF RedネットワークのClient1とVRF BlueネットワークのClient2は、IPSec VPNトンネル経由でASAの背後にあるClient 3と通信します。

設定

ネットワーク図

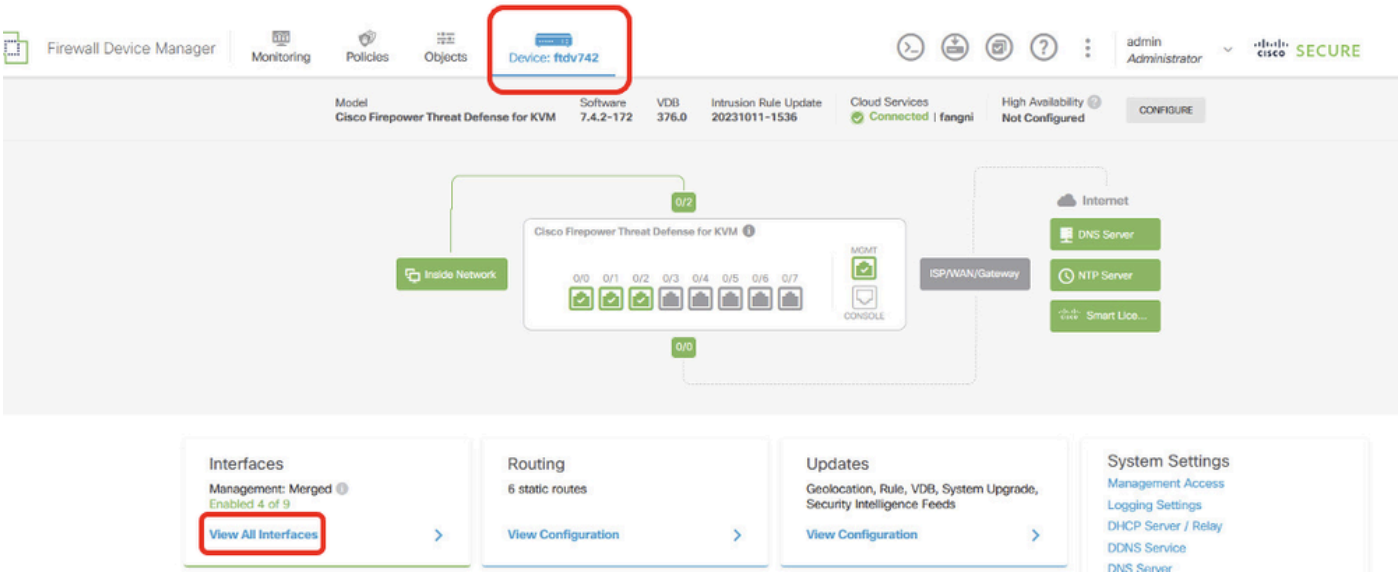


トポロジ

FTDの設定

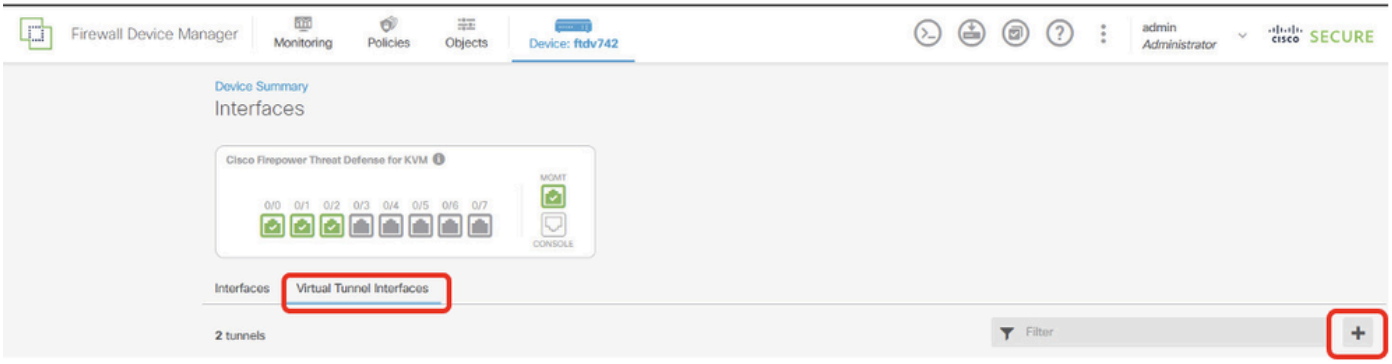
ステップ 1：ノード間のIP相互接続の事前設定が正常に完了していることを確認することが不可欠です。Client1とClient2には、ゲートウェイとしてFTDの内部IPアドレスが設定されています。Client3には、ゲートウェイとしてASA内部IPアドレスが設定されています。

ステップ 2： 仮想トンネルインターフェイスを作成します。 FTDのFDM GUIにログインします。 Device > Interfacesの順に移動します。View All Interfaces をクリックします。



FTD_View_インターフェイス

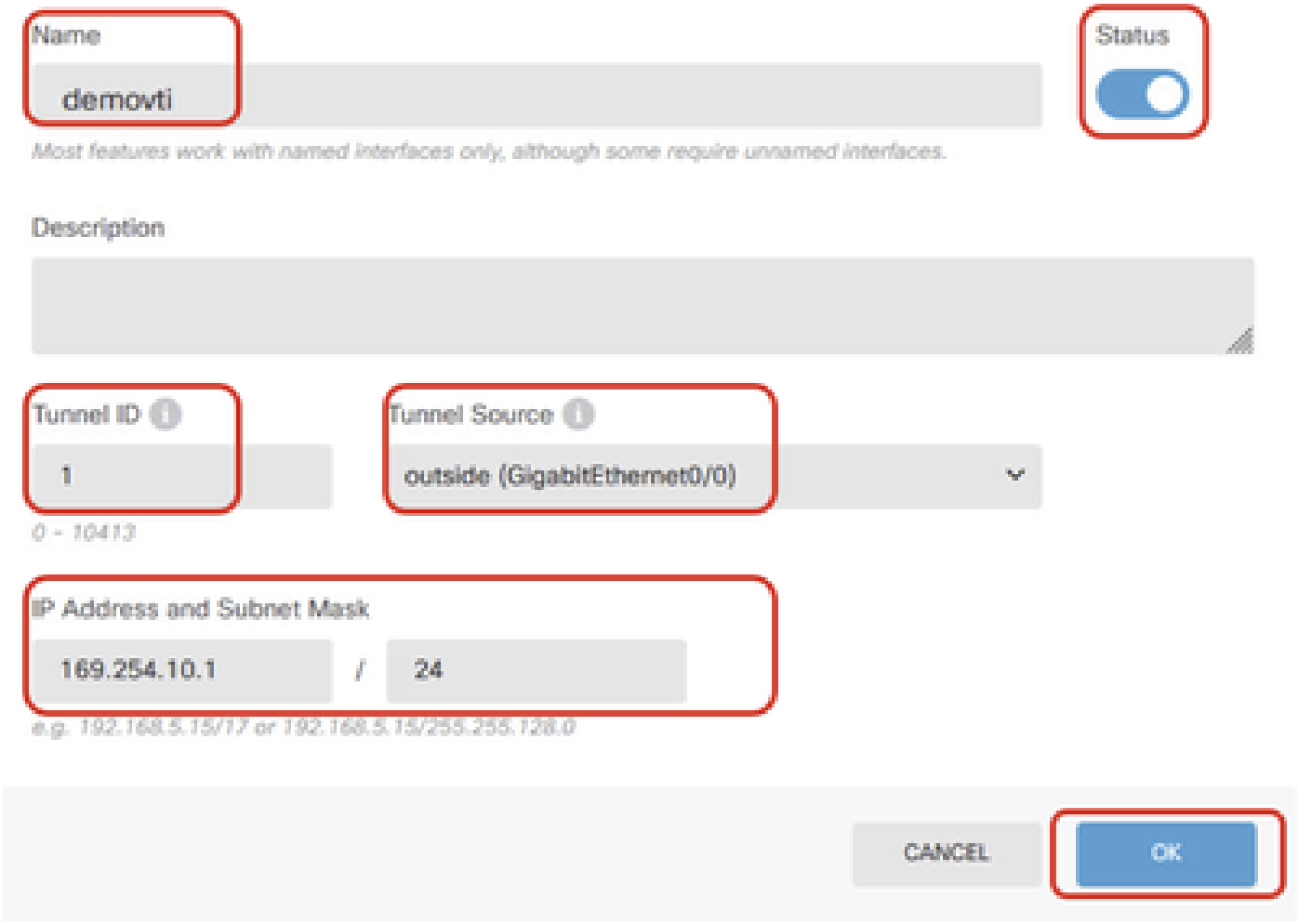
ステップ 2.1： Virtual Tunnel Interfacesタブをクリックします。+ボタンをクリックします。



FTD_Create_VTI（仮想トンネルエンドポイント）

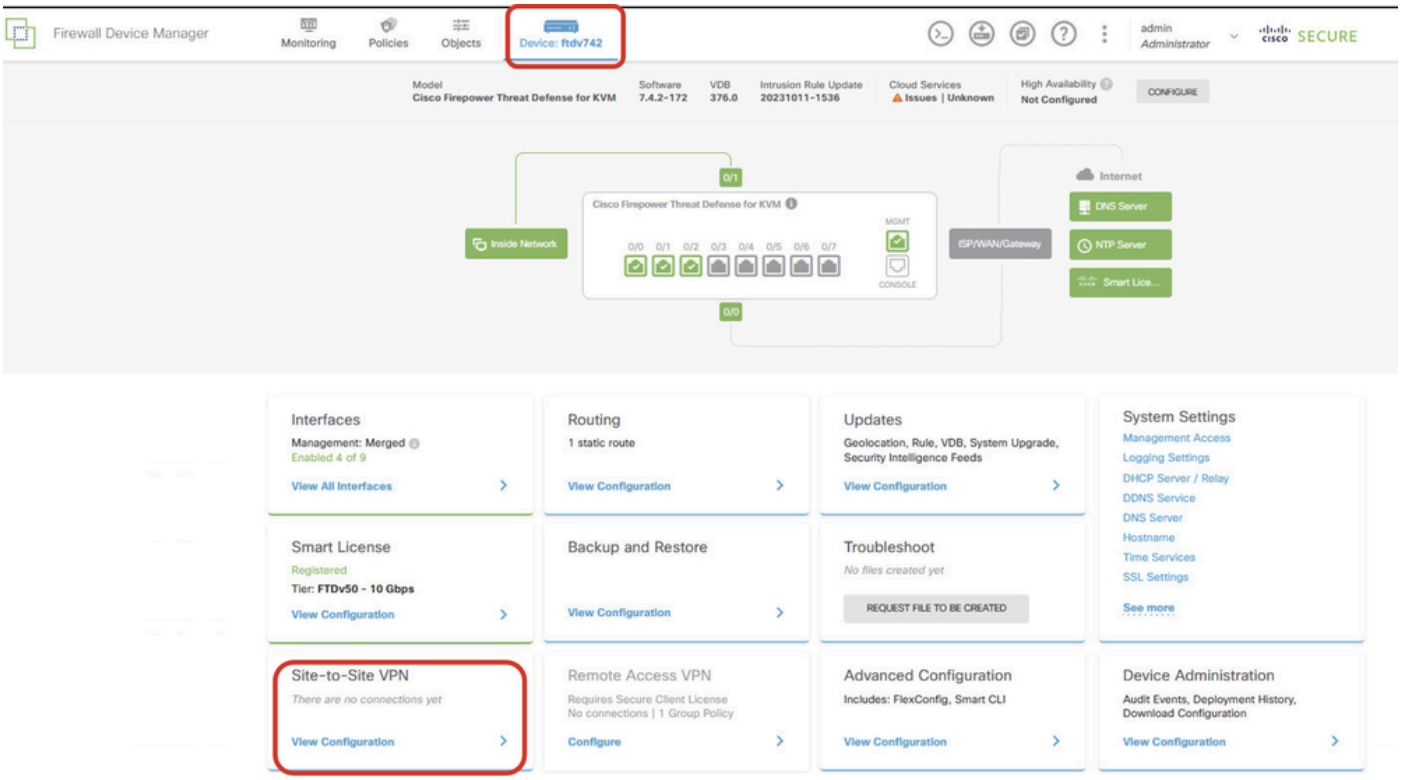
ステップ 2.2：必要な情報を提供します。OKボタンをクリックします。

- 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。



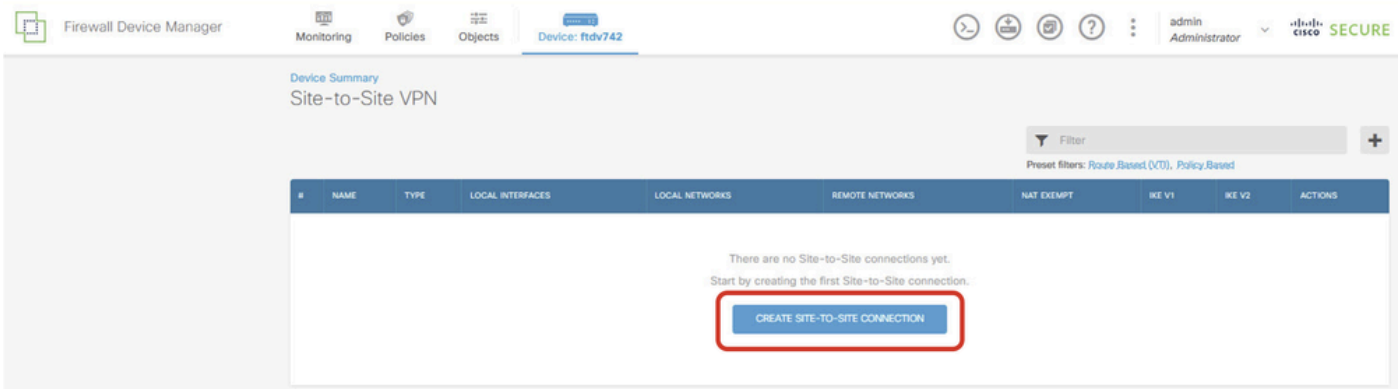
FTD_Create_VTI_Details

ステップ 3：Device > Site-to-Site VPNの順に移動します。View Configurationボタンをクリックします。



FTD_Site-to-Site_VPN_View_設定

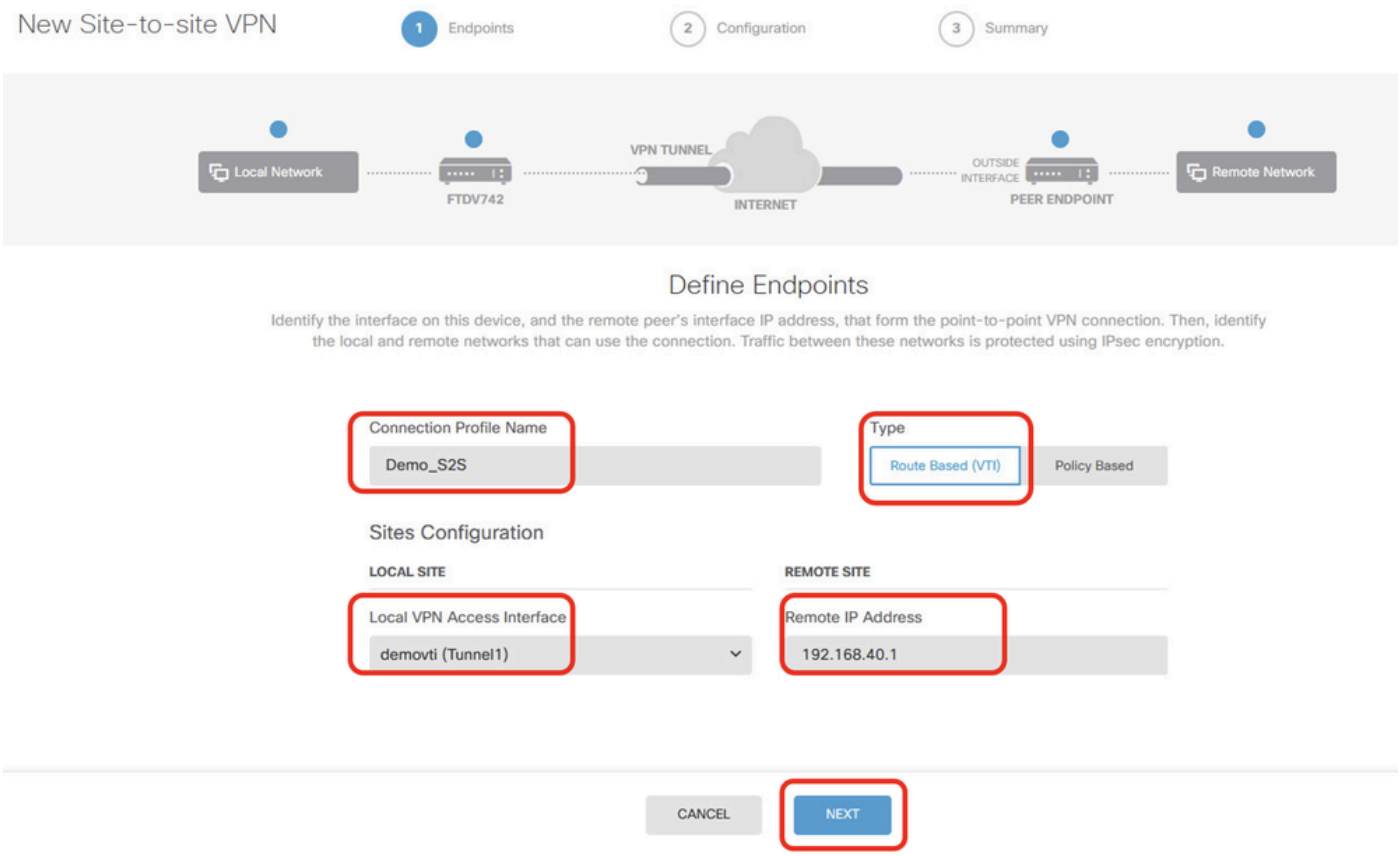
ステップ 3.1： 新しいサイト間VPNの作成を開始します。CREATE SITE-TO-SITE CONNECTIONボタンをクリックします。または、+ボタンをクリックします。



FTD_Create_Site2Site_Connection（サイト接続）

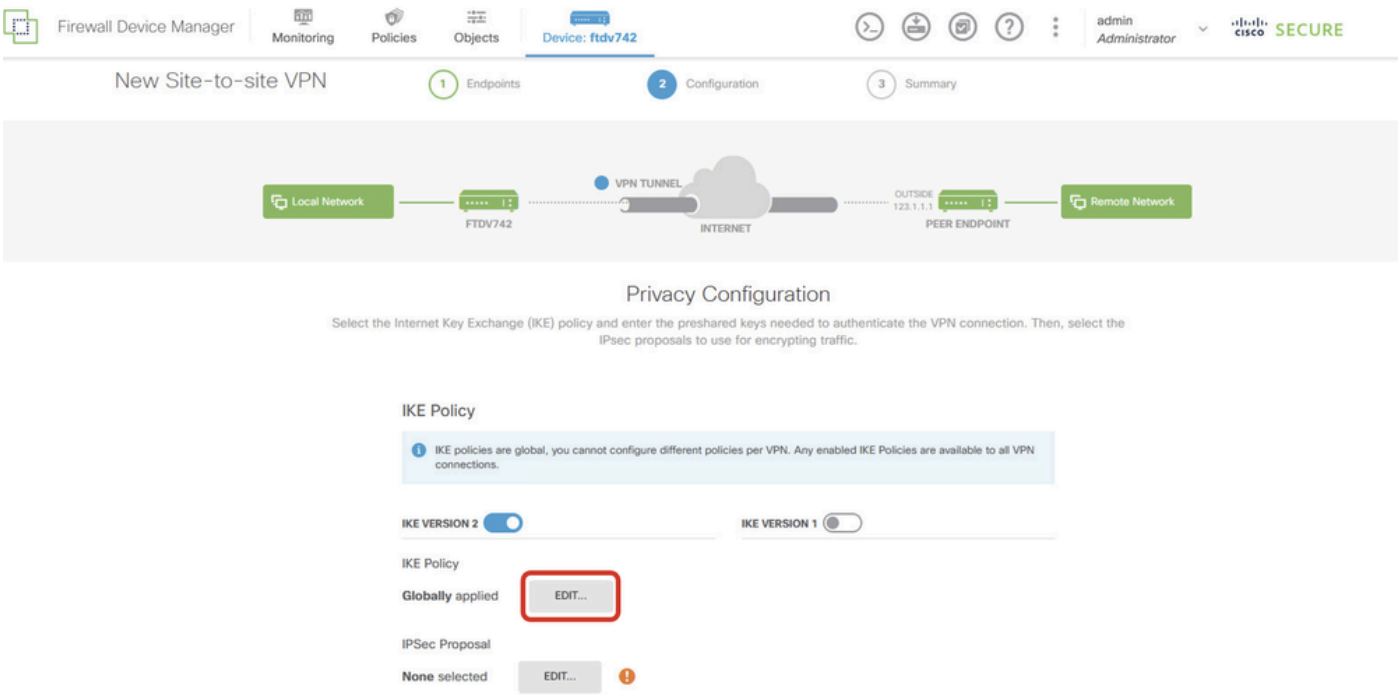
ステップ 3.2： 提供 必要な情報NEXTボタンをクリックします。

- 接続プロファイル名：Demo_S2S
- タイプ：ルートベース(VTI)
- ローカルVPNアクセスインターフェイス：demovti（ステップ2で作成）
- リモートIPアドレス：192.168.40.1（これはピアASA外部IPアドレスです）



FTD_Site-to-Site_VPN_エンドポイント

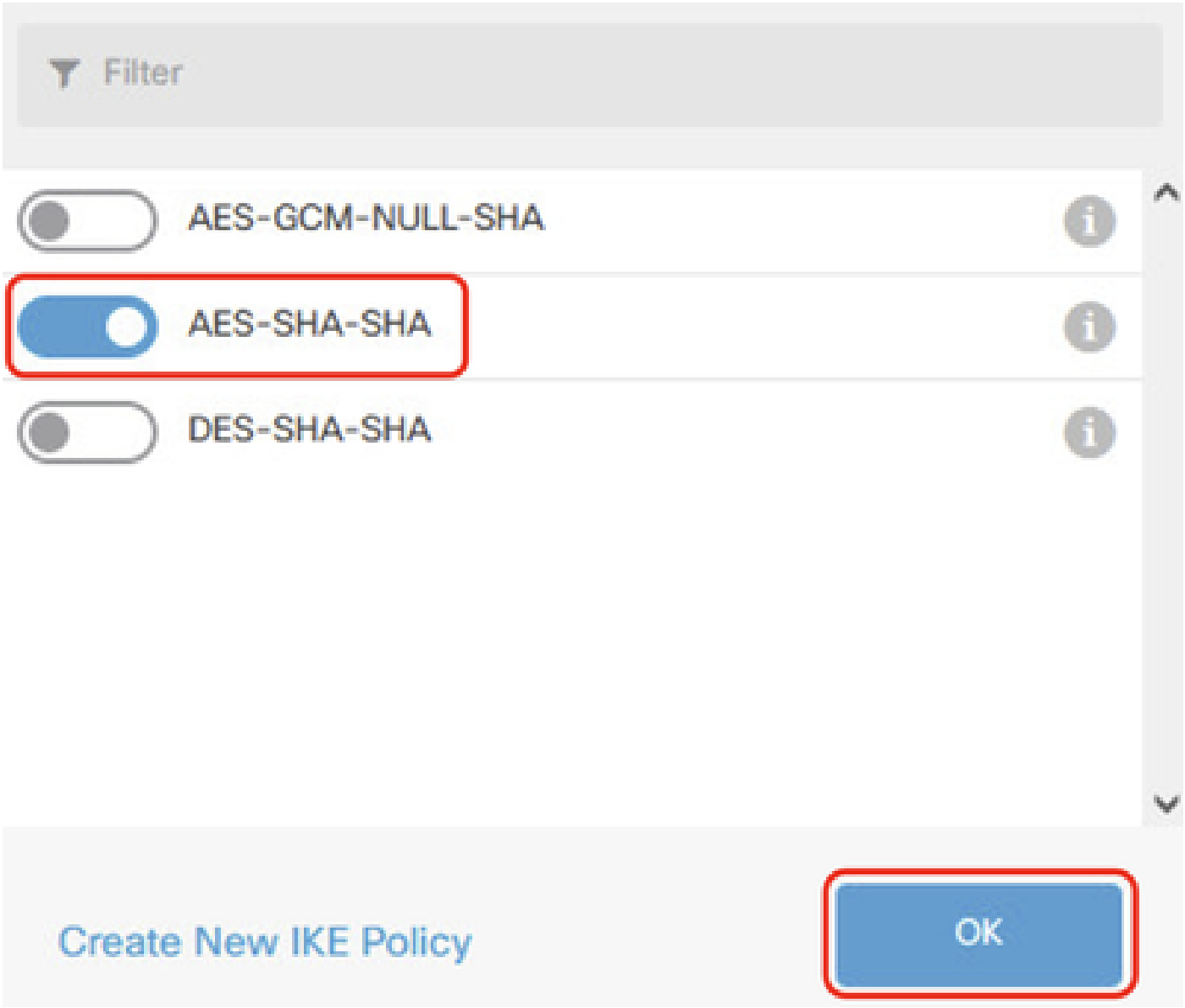
ステップ 3.3：IKE Policyに移動します。EDIT ボタンをクリックします。



FTD_Edit_IKE_Policy（ポリシーの編集）

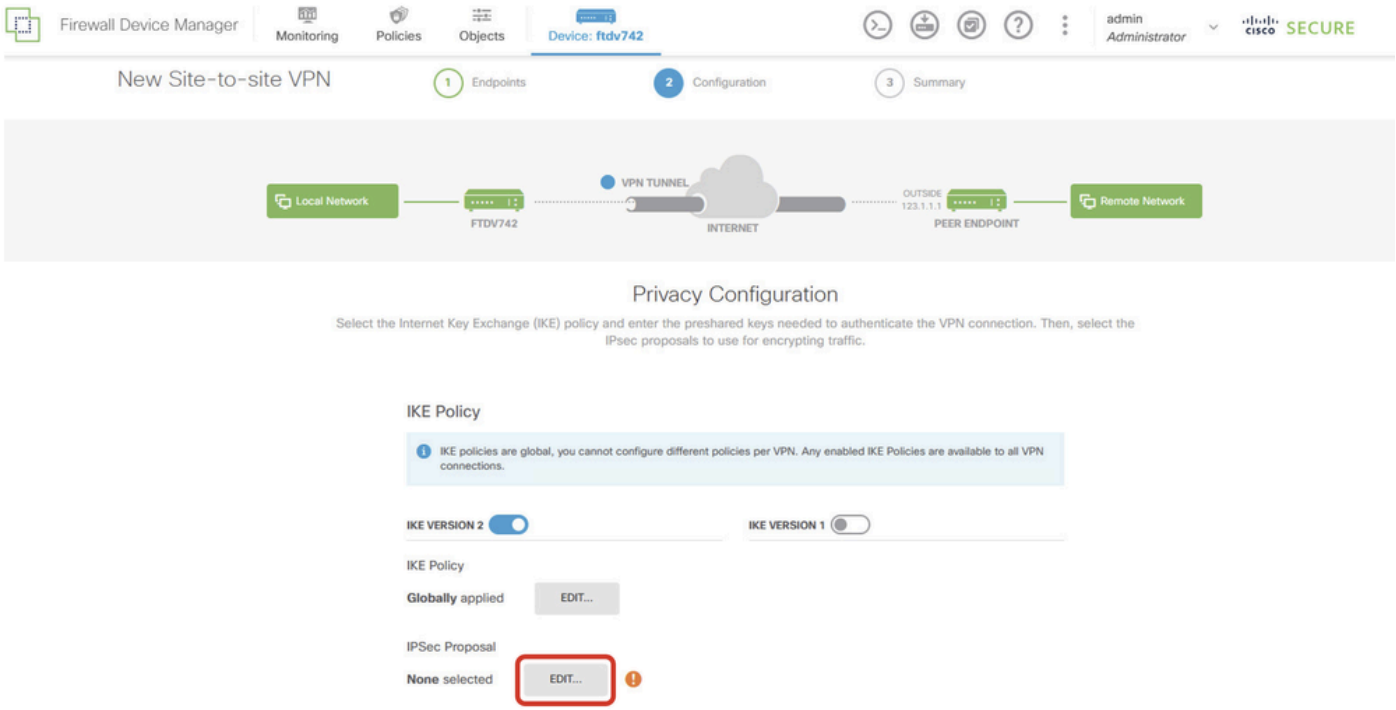
ステップ 3.4： IKEポリシーの場合は、事前に定義したポリシーを使用するか、 新しいIKEポリシーの作成 .

この例では、既存のIKEポリシー名をAES-SHA-SHA に切り替えます。OK ボタンをクリックして保存します。



FTD_Enable_IKE_ポリシー

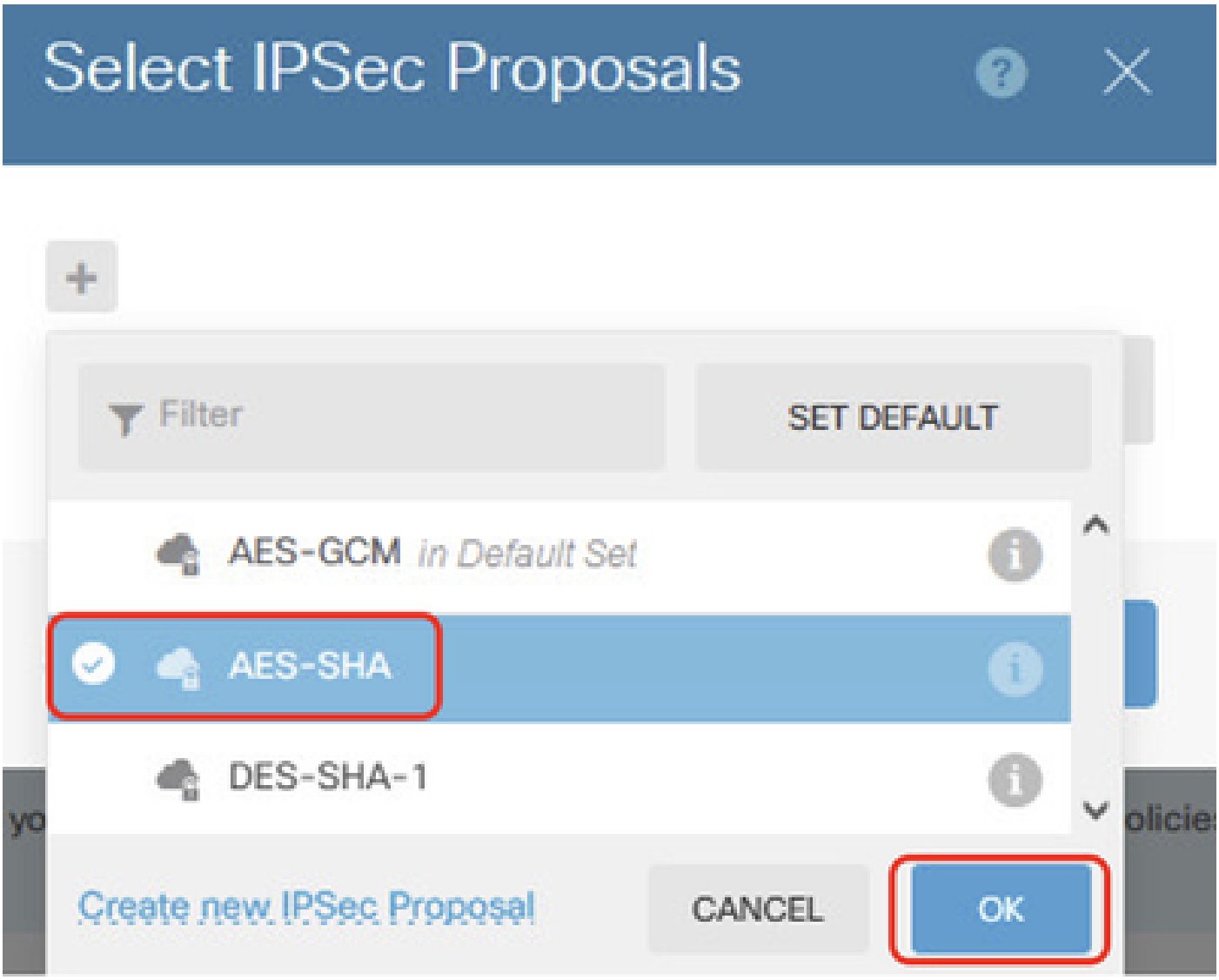
ステップ 3.5： IPSec Proposalに移動します。EDIT ボタンをクリックします。



FTD_Edit_IPSec_Proposal（提案）

ステップ 3.6： IPSecプロポーザルの場合は、事前に定義されたパスワードを使用するか、Create new IPSec Proposal をクリックして新しいパスワードを作成できます。

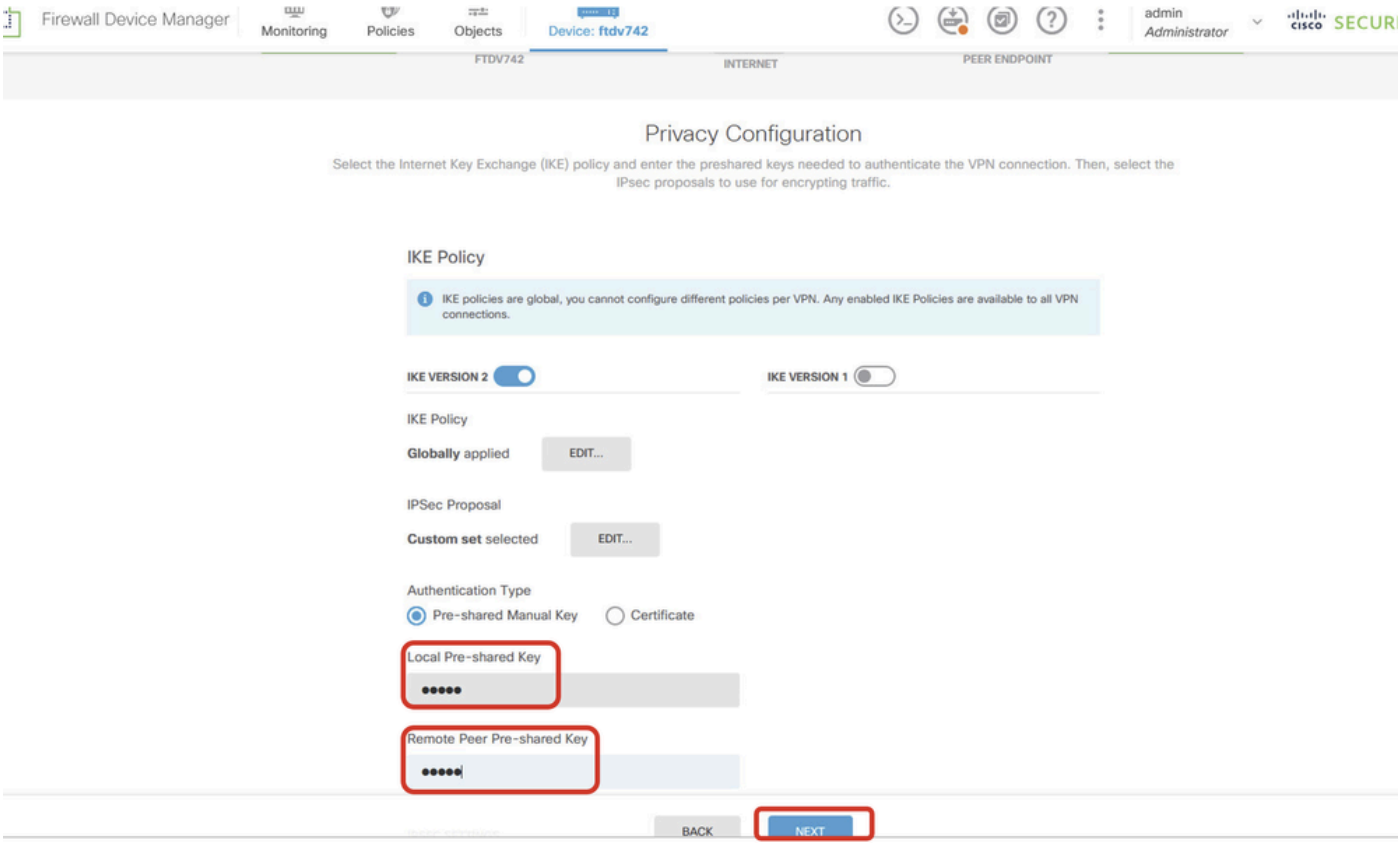
次の例では、既存のIPSecプロポーザル名をAES-SHAに切り替えます。[保存（ OK ボタンをクリックします。



FTD_Enable_IPSec_Proposal（提案）

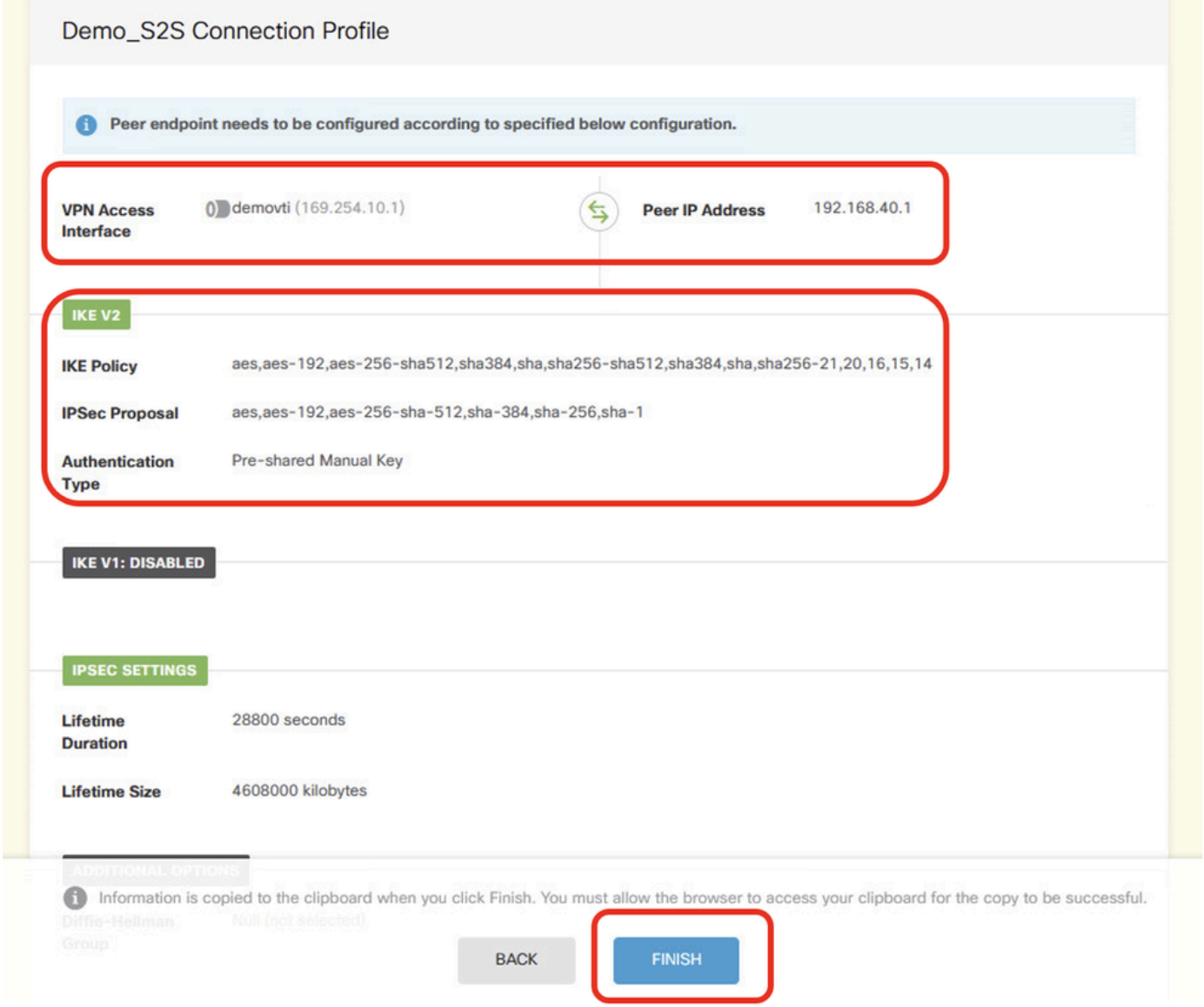
ステップ 3.7： ページを下にスクロールし、事前共有キーを設定します。NEXTボタンをクリックします。

この事前共有キーをメモし、後でASAで設定してください。



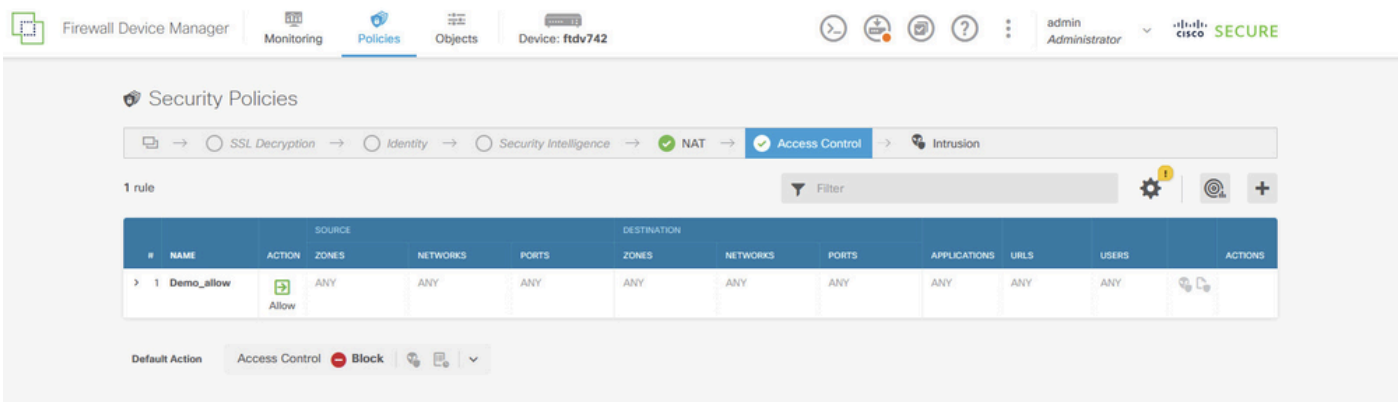
FTD_Configure_Pre_Shared_Keyを設定します。

ステップ 3.8： VPN設定を確認します。変更が必要な場合は、BACK (戻る) 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。



FTD_Review_VPN_設定

ステップ 3.9： アクセスコントロールルールを作成して、トラフィックがFTDを通過できるようにします。この例では、デモ用にすべて許可します。実際のニーズに基づいてポリシーを変更してください。

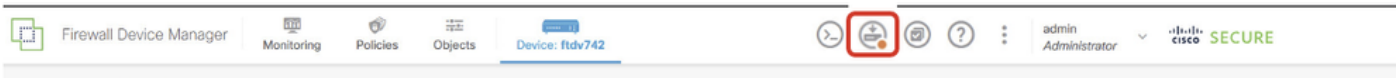


FTD_ACP_例

ステップ3.10:（オプション）クライアントがインターネットにアクセスできるようにダイナミッ

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。この例では、FTDにダイナミックNATが設定されていないため、NAT免除ルールを設定する必要はありません。

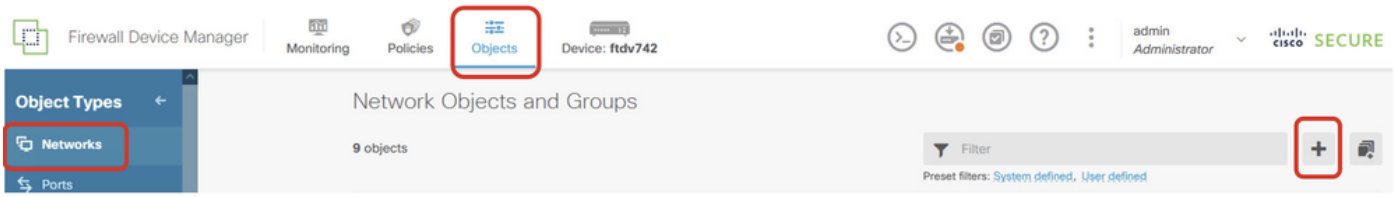
ステップ 3.11： 設定変更を導入します。



FTD_Deployment_Changes

ステップ 4：仮想ルータを設定します。

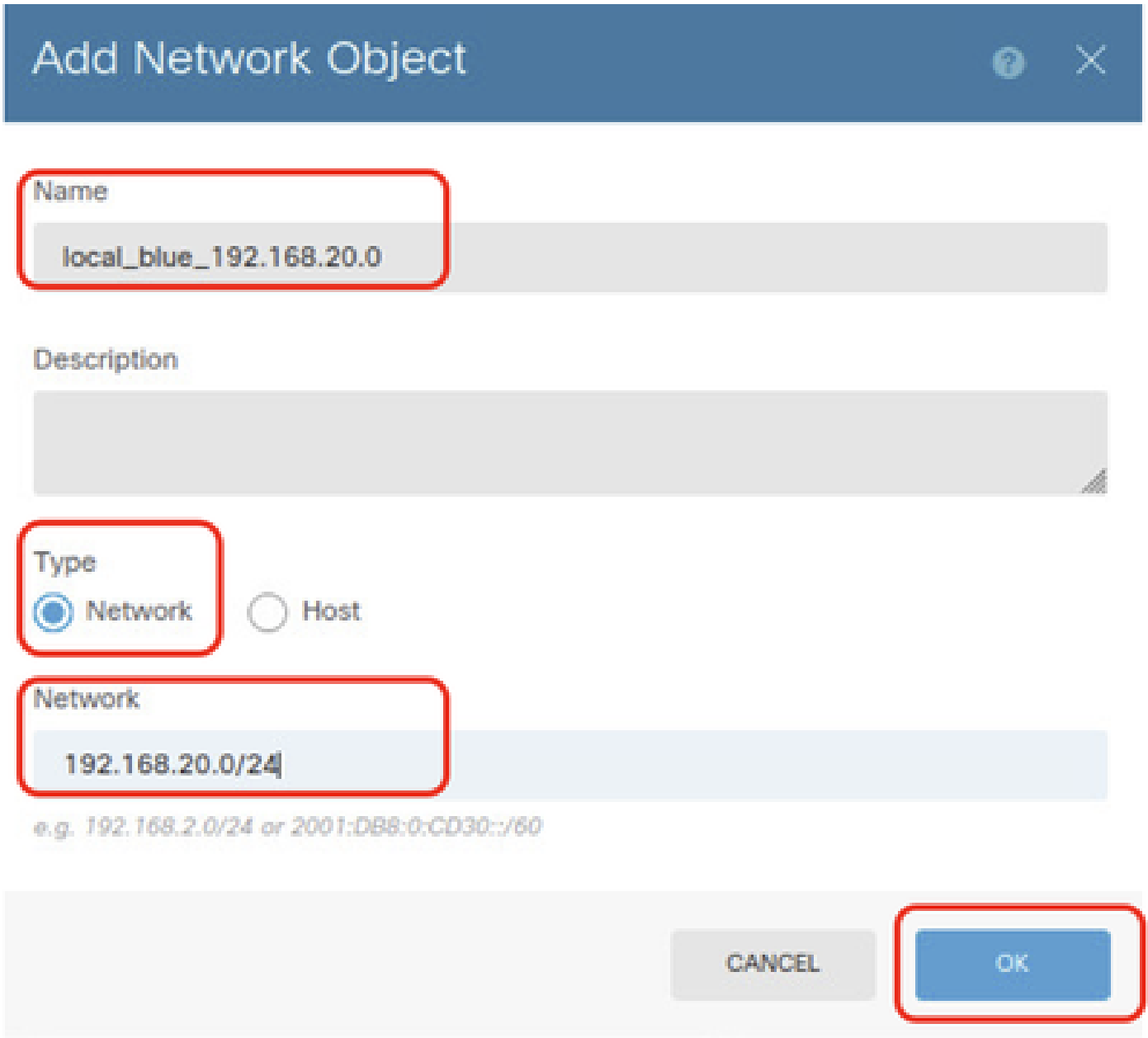
ステップ 4.1：スタティックルートのネットワークオブジェクトを作成します。 Objects > Networks の順に移動し、+ボタンをクリックします。



FTD_Create_NetObjects

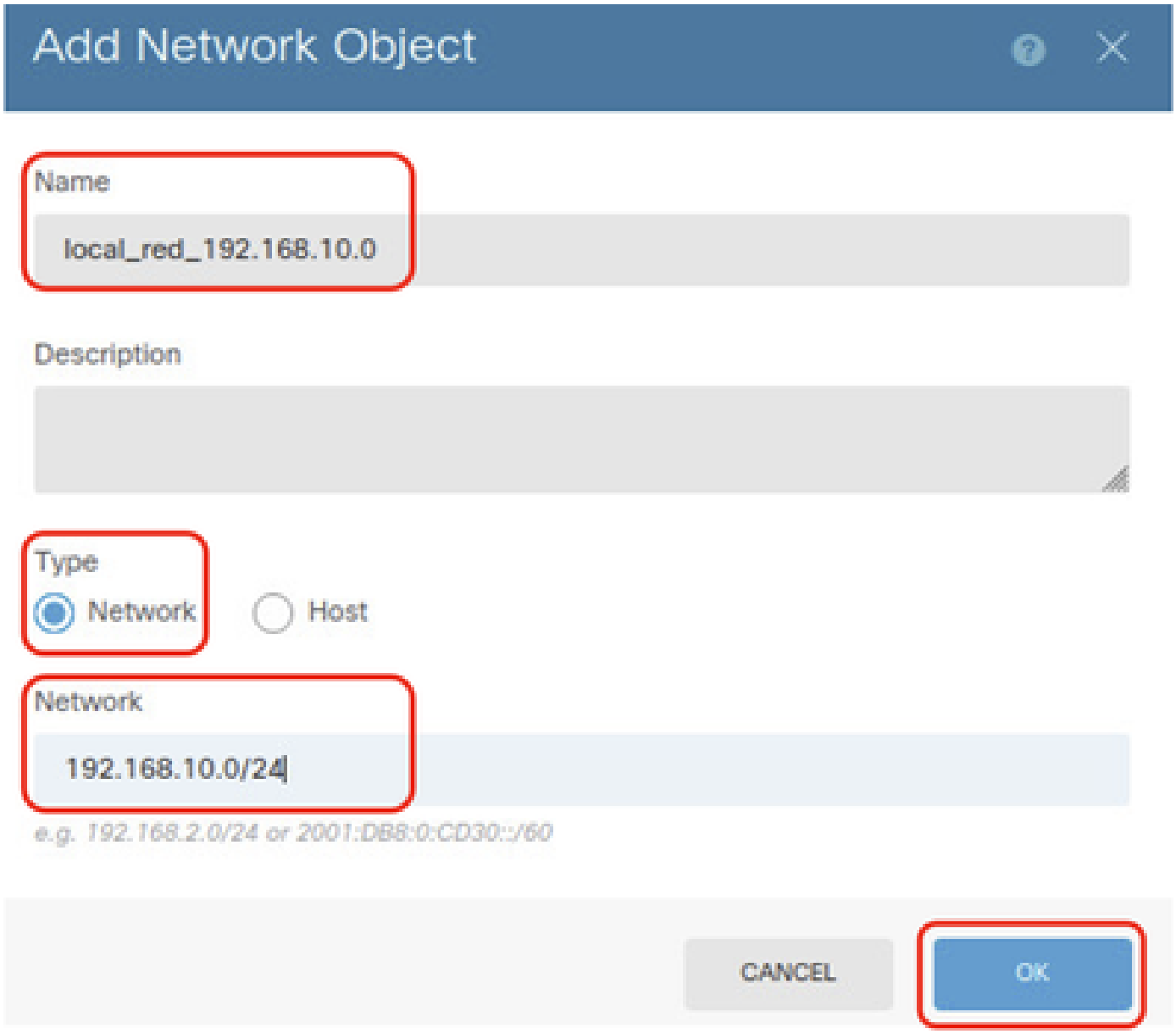
ステップ 4.2：各ネットワークオブジェクトに必要な情報を提供します。OKボタンをクリックします。

- 名前： local_blue_192.168.20.0
- タイプ：ネットワーク
- ネットワーク：192.168.20.0/24



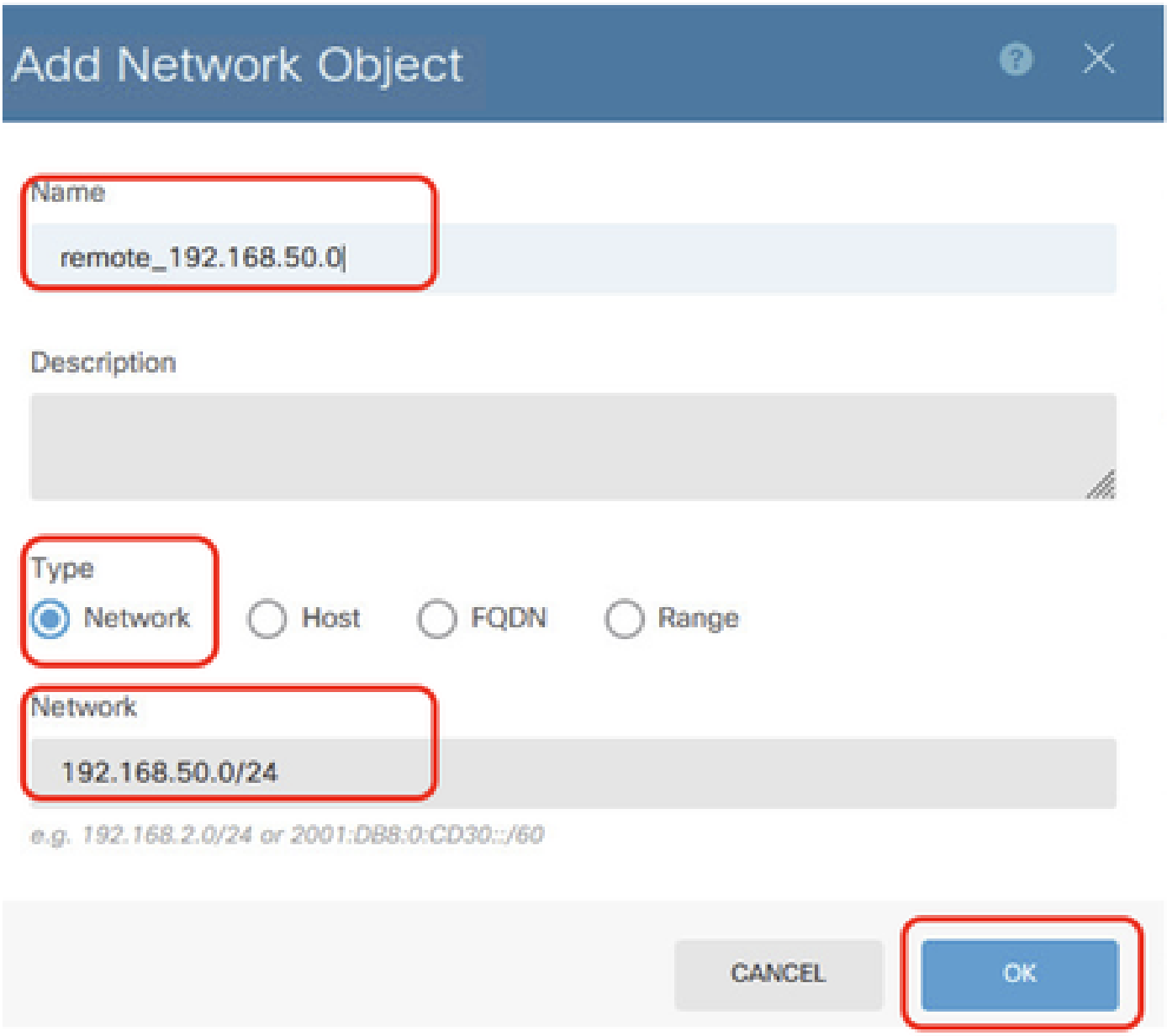
FTD_VRF_Blue_Network

- 名前： local_red_192.168.10.0
- タイプ：ネットワーク
- ネットワーク：192.168.10.0/24



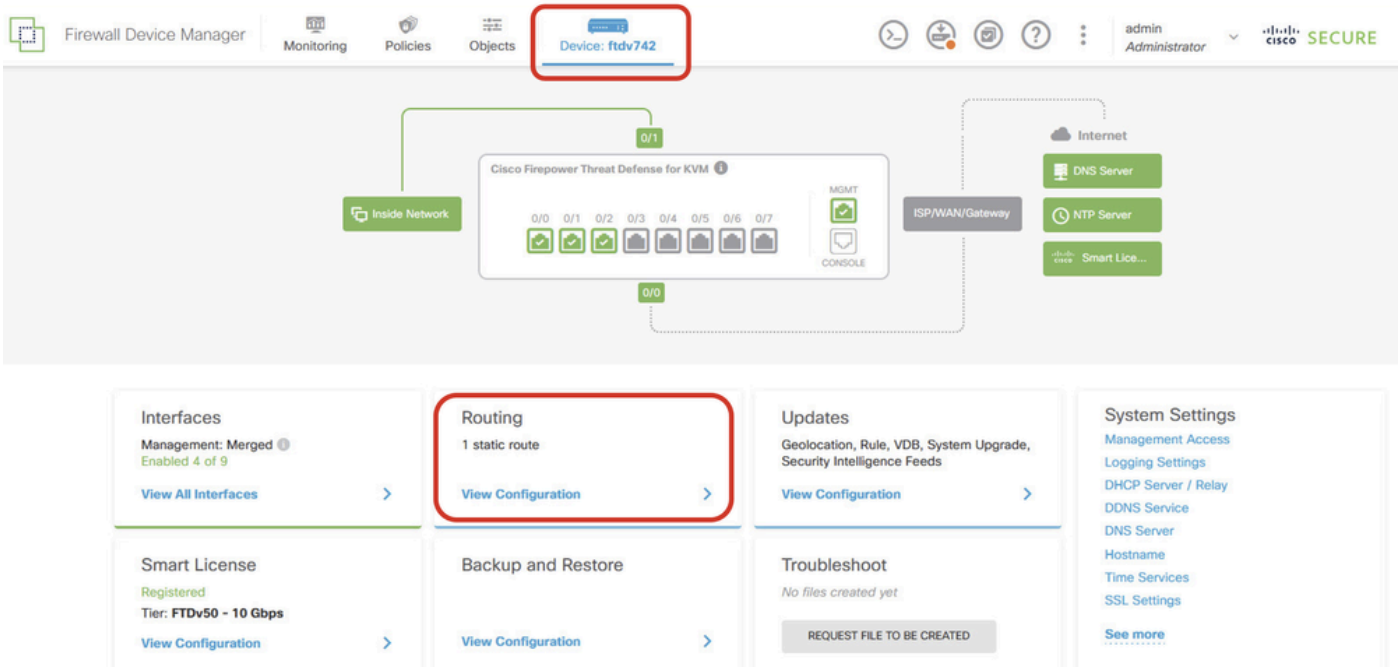
FTD_VRF_Red_ネットワーク

- 名前： remote_192.168.50.0
- タイプ：ネットワーク
- ネットワーク：192.168.50.0/24



FTD_Remote_Network

ステップ 4.3：最初の仮想ルータを作成します。Device > Routing の順に移動します。View Configuration をクリックします。



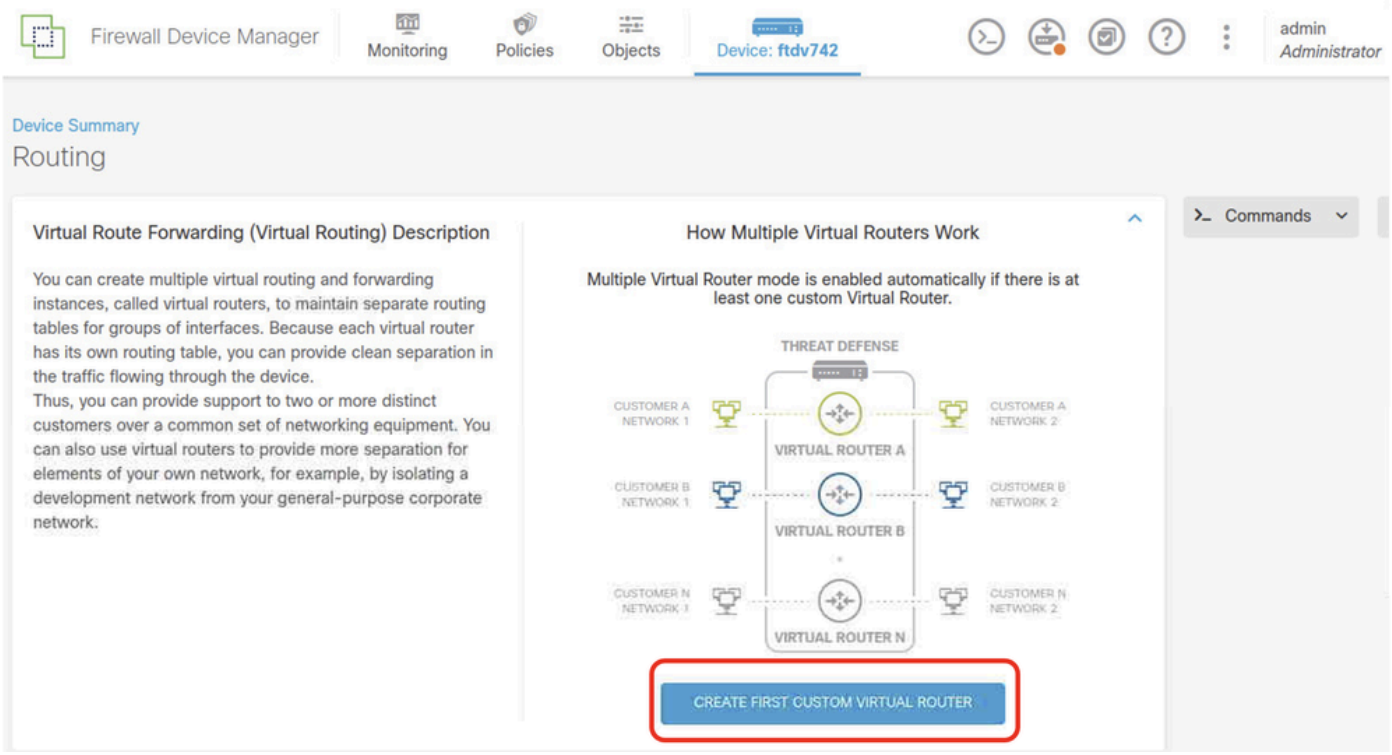
FTD_View_Routing_設定

ステップ 4.4：Add Multiple Virtual Routers をクリックします。

注意： Outsideインタフェースを経由する静的ルートは、FDMの初期化中にすでに構成されています。もしなければ、手動で設定してください。

FTD_Add_First_Virtual_Router1

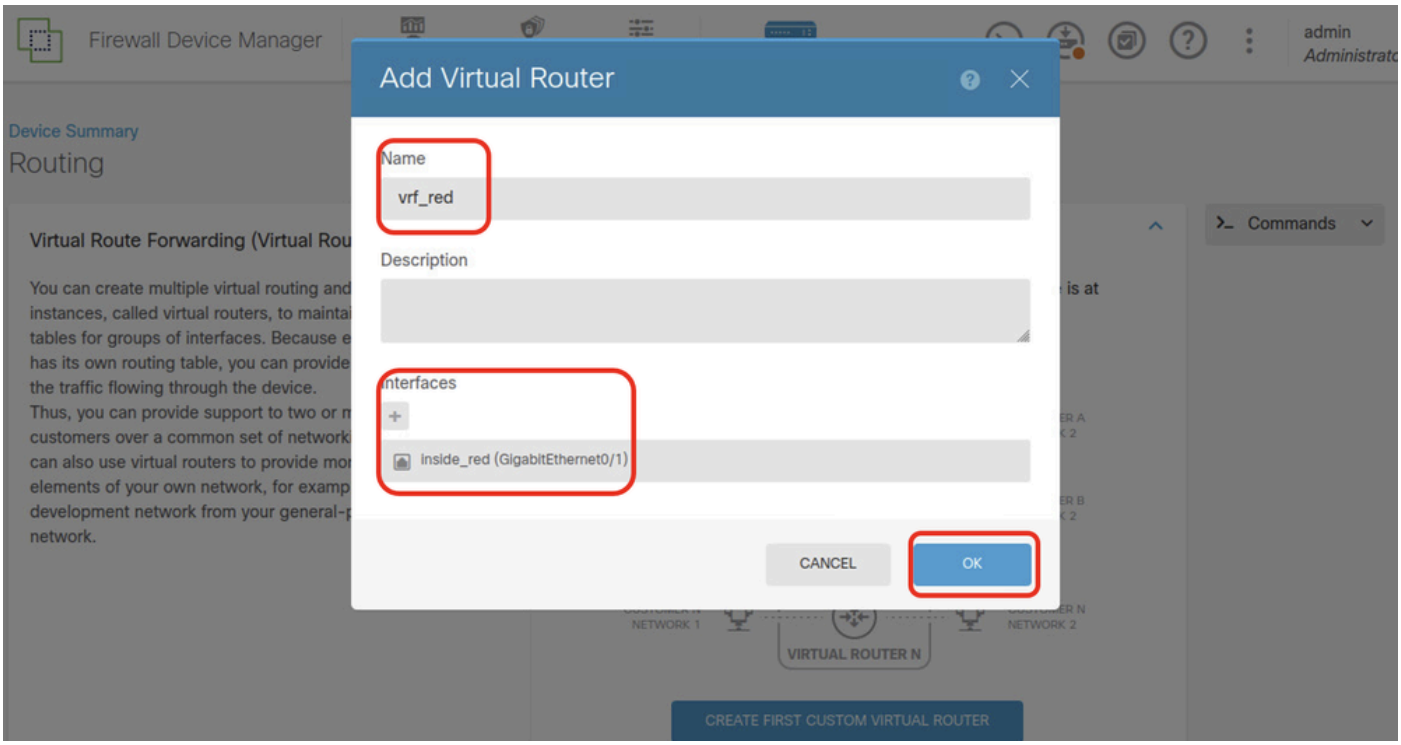
ステップ 4.5： CREATE FIRST CUSTOM VIRTUAL ROUTER をクリックします。



FTD_Add_First_Virtual_Router2

ステップ 4.6：最初の仮想ルータに関する必要な情報を提供します。OK ボタンをクリックします。最初の仮想ルータを作成した後、vrf名Globalが自動的に表示されます。

- 名前：vrf_red
- インターフェイス：inside_red(GigabitEthernet0/1)



FTD_Add_First_Virtual_Router3

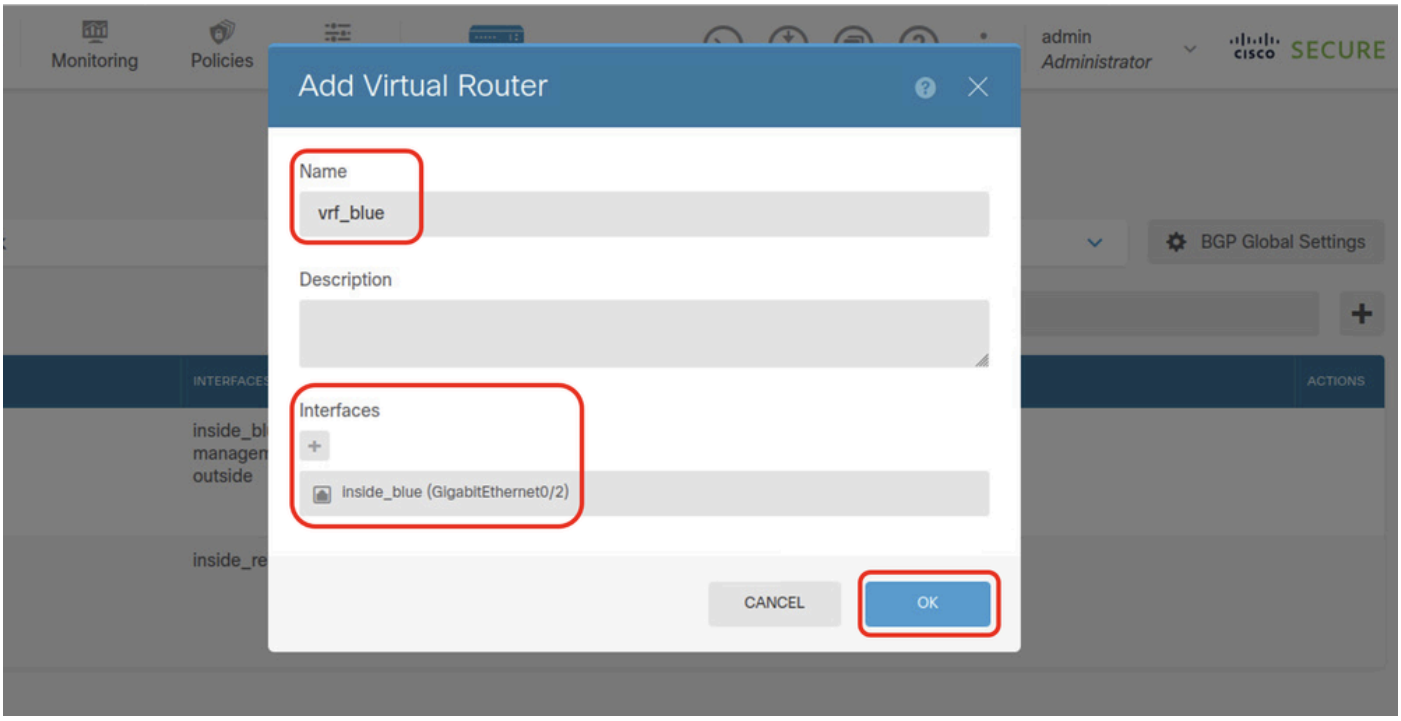
ステップ 4.7：2番目の仮想ルータを作成します。 Device > Routing の順に移動します。View

Configuration をクリックします。+ボタンをクリックします。

FTD_Add_Second_Virtual_ルータ

ステップ 4.8： 2番目の仮想ルータに関する必要な情報を提供します。OK ボタンをクリックします

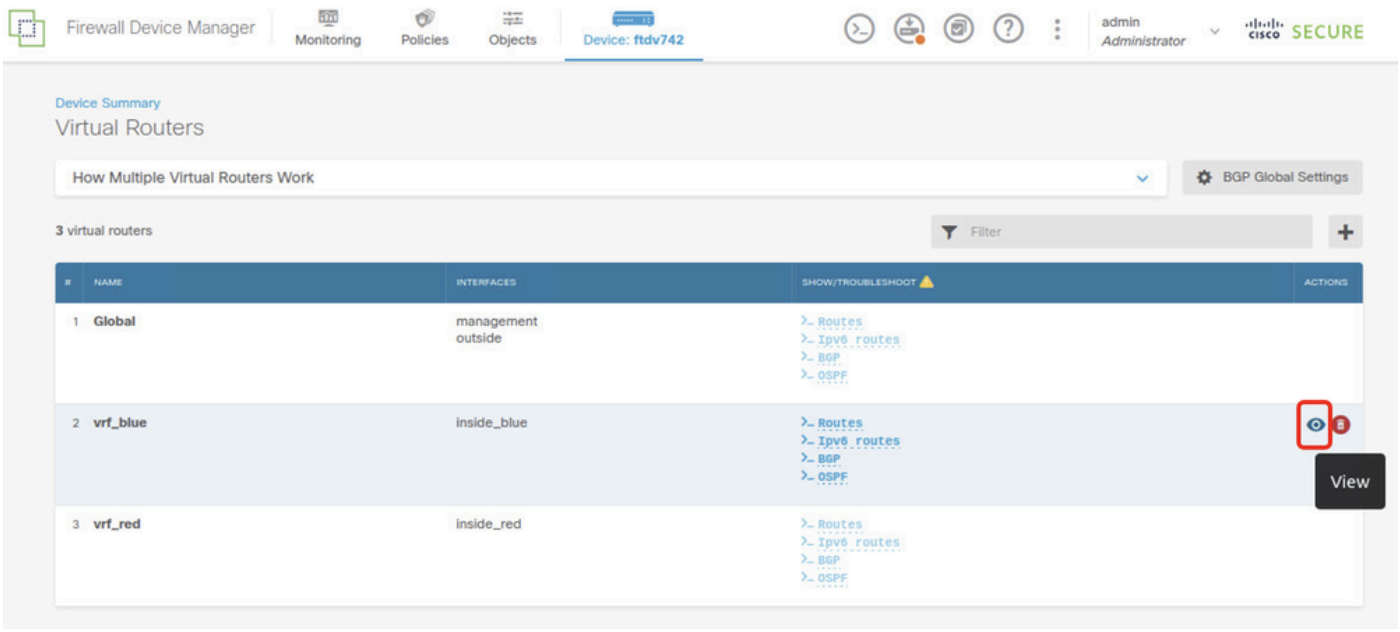
- 名前：vrf_blue
- インターフェイス：inside_blue(GigabitEthernet0/2)



FTD_Add_Second_Virtual_Router2に追加します。

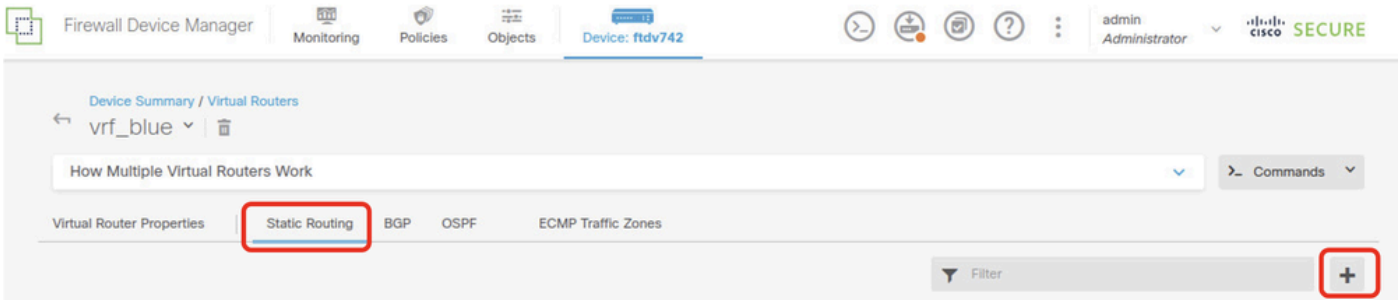
ステップ 5：vrf_blueからGlobalへのルートリークを作成します。 このルートにより、192.168.20.0/24ネットワーク上のエンドポイントは、サイト間VPNトンネルを通過する接続を開始できます。この例では、リモートエンドポイントが192.168.50.0/24ネットワークを保護しています。

Device > Routing の順に移動します。View Configuration をクリックし、View アイコンをクリックします 仮想ルータvrf_blueのActionセル



FTD_View_VRF_Blue

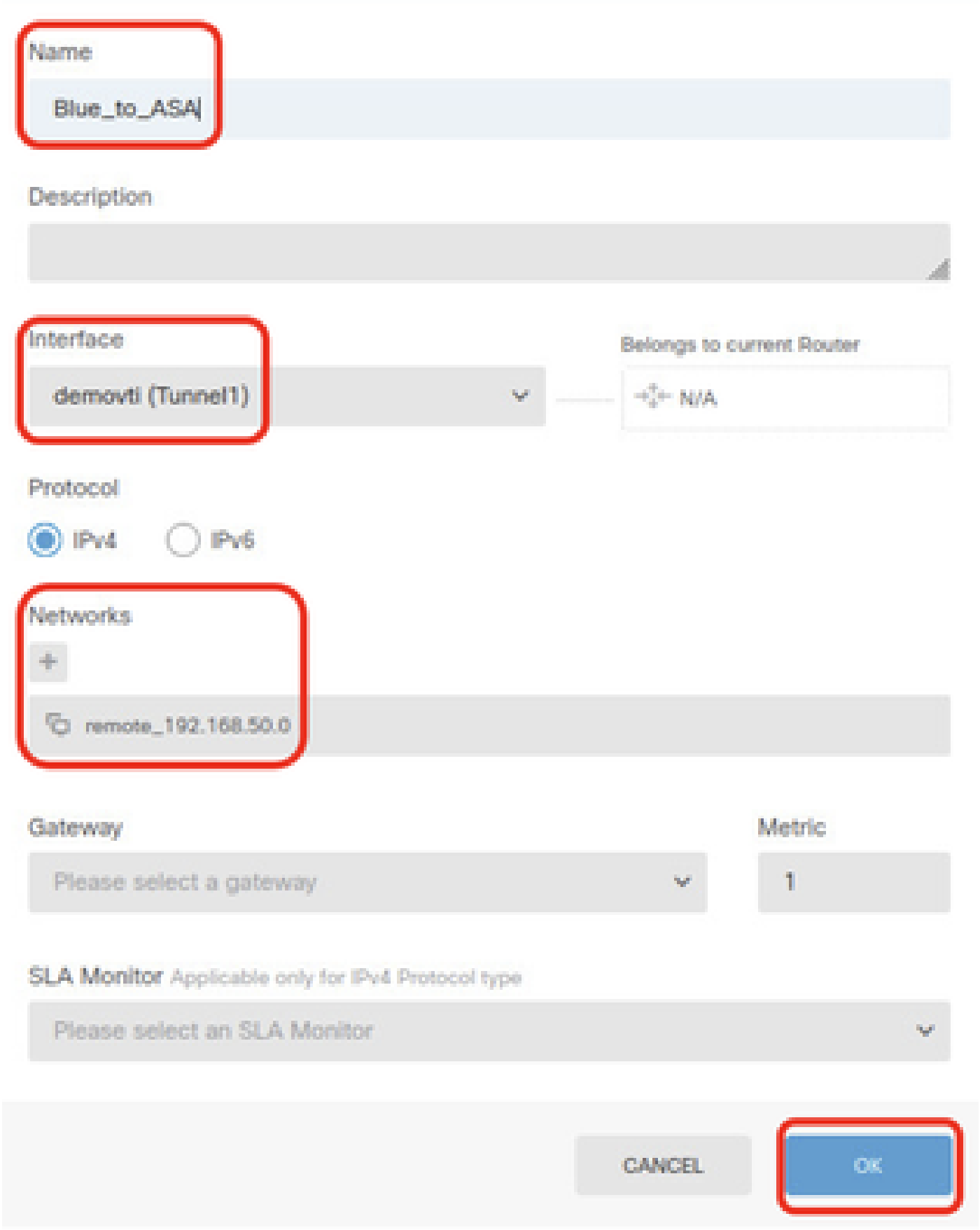
ステップ 5.1：Static Routing タブをクリックします。+ボタンをクリックします。



FTD_Create_Static_Route_VRF_青

ステップ 5.2： 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：Blue_to_ASA
- インターフェイス：demovti(Tunnel1)
- ネットワーク：remote_192.168.50.0
- ゲートウェイ：この項目は空白のままにします。

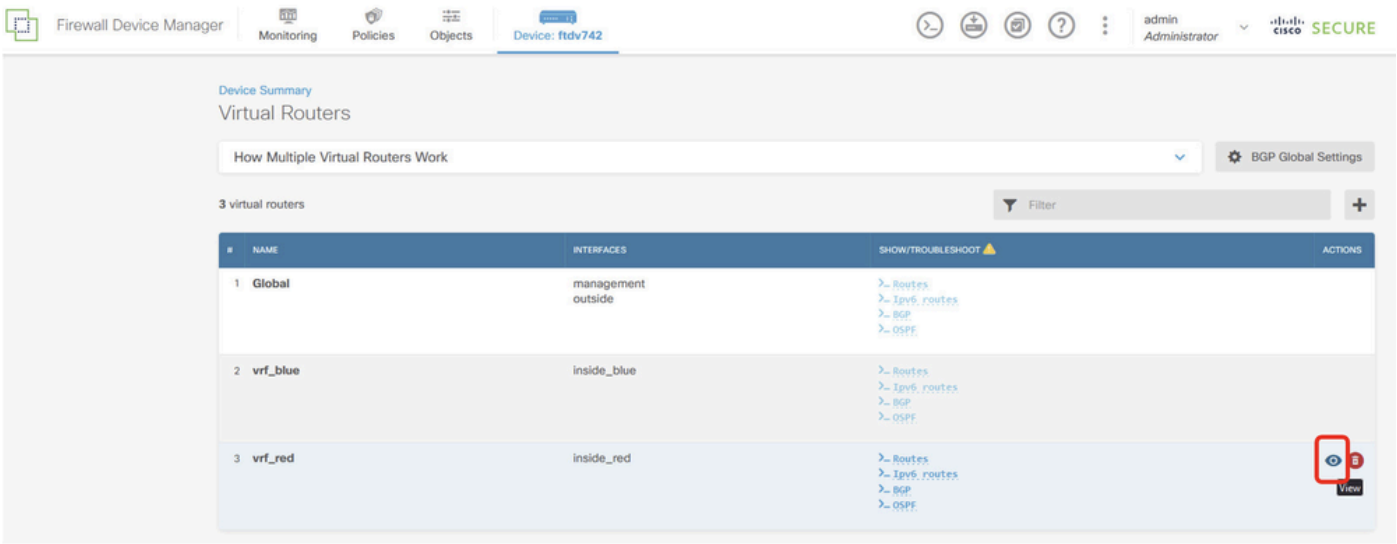


FTD_Create_Static_Route_VRF_Blue_Details

手順 6： vrf_redからGlobalへのルートリークを作成します。 このルートにより、192.168.10.0/24ネットワーク上のエンドポイントは、サイト間VPNトンネルを通過する接続を開

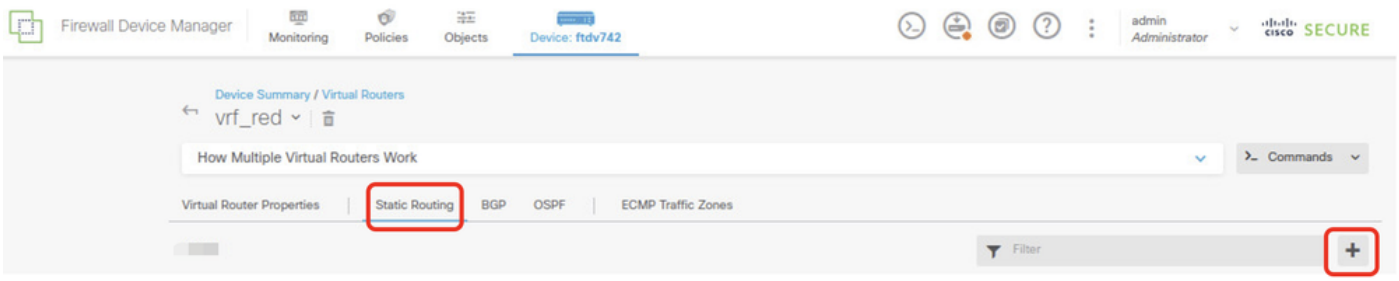
始できます。この例では、リモートエンドポイントが192.168.50.0/24ネットワークを保護しています。

Device > Routing の順に移動します。View Configuration をクリックし、View アイコンをクリックします 仮想ルータvrf_redのActionセル内。



FTD_View_VRF_Red

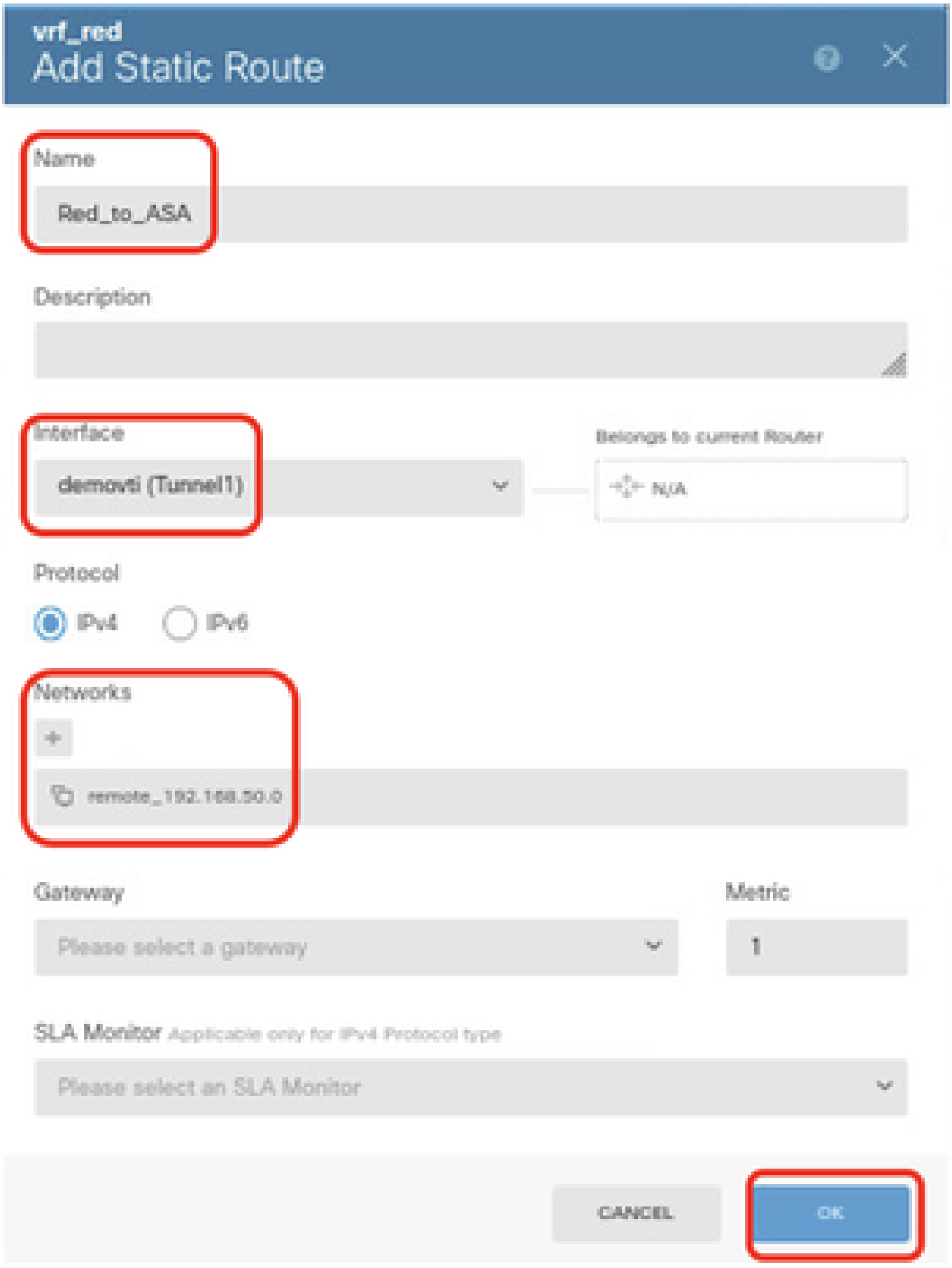
ステップ 6.1： Static Routing タブをクリックします。+ボタンをクリックします。



FTD_Create_Static_Route_VRF_赤

ステップ 6.2： 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：Red_to_ASA
- インターフェイス：demovti(Tunnel1)
- ネットワーク：remote_192.168.50.0
- ゲートウェイ：この項目は空白のままにします。

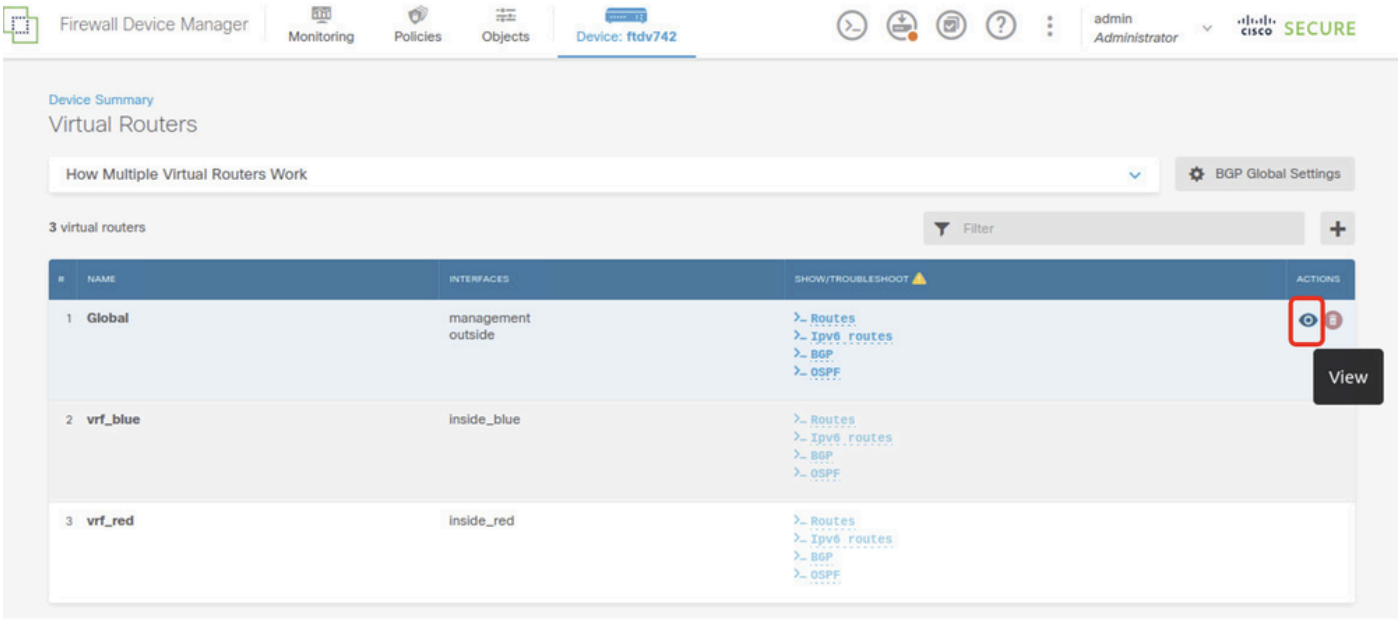


FTD_Create_Static_Route_VRF_Red_Details

手順 7：グローバルルータから仮想ルータへのルートリークを作成する。このルートにより、サイト間VPNのリモートエンドによって保護されているエンドポイントは、vrf_red仮想ルータ内の

192.168.10.0/24ネットワークおよびvrf_blue仮想ルータ内の192.168.20.0/24ネットワークにアクセスできます。

Device > Routing の順に移動します。View Configuration をクリックします。グローバル仮想ルータのActionセルにあるView アイコンをクリックします。



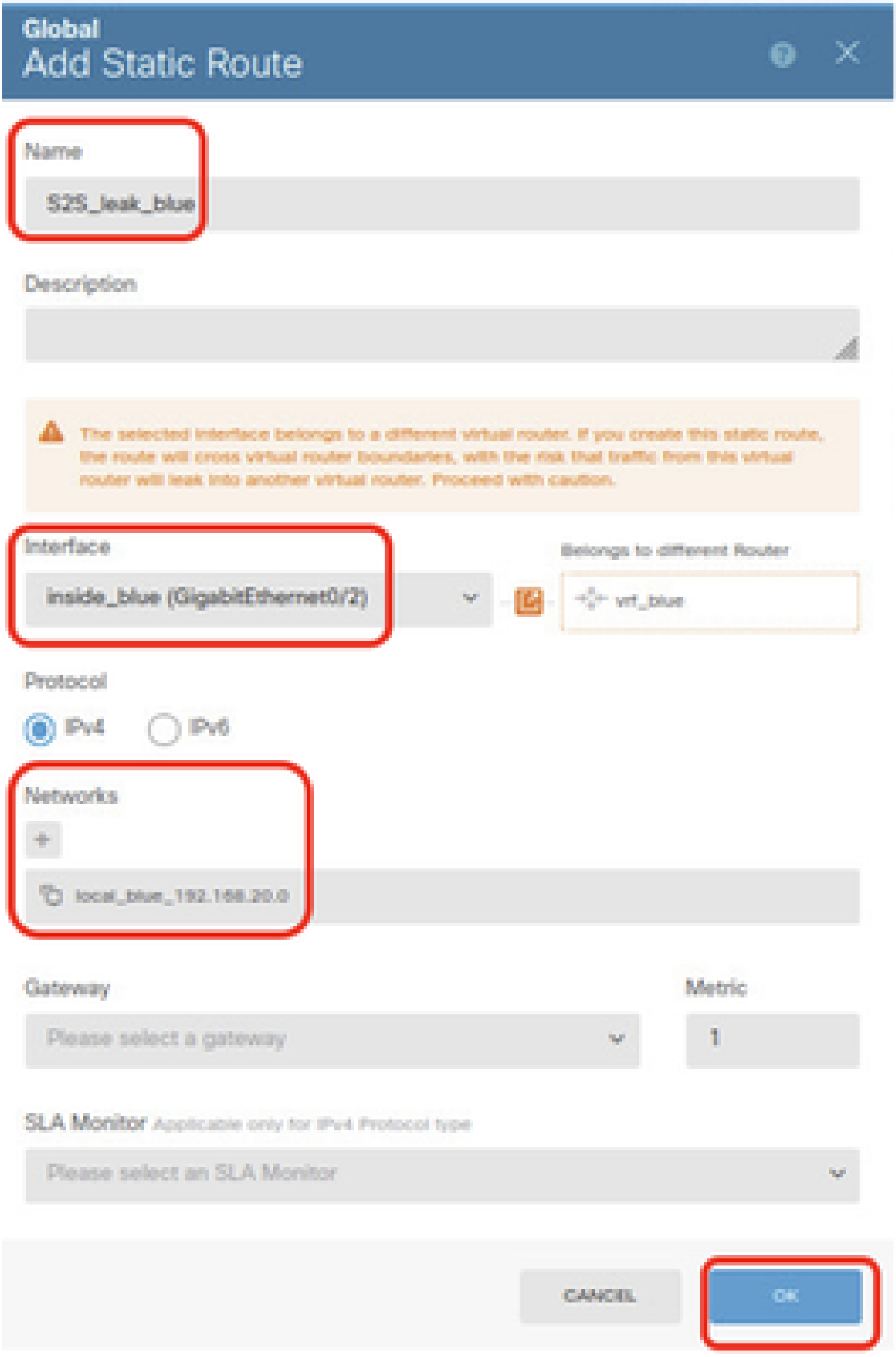
FTD_View_VRF_グローバル

ステップ 7.1： Static Routing タブをクリックします。+ボタンをクリックします。

FTD_Create_Static_Route_VRF_グローバル

ステップ 7.2： 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： S2S_leak_blue
- インターフェイス：inside_blue(GigabitEthernet0/2)
- ネットワーク：local_blue_192.168.20.0
- ゲートウェイ：この項目は空白のままにします。


Global
Add Static Route
Name
S2S_leak_blue
Description
The selected interface belongs to a different virtual router. If you create this static route, the route will cross virtual router boundaries, with the risk that traffic from this virtual router will leak into another virtual router. Proceed with caution.
Interface
inside_blue (GigabitEthernet0/2)
Belongs to different Router
vrf_blue
Protocol
IPv4
IPv6
Networks
local_blue_192.168.20.0
Gateway
Please select a gateway
Metric
1
SLA Monitor Applicable only for IPv4 Protocol type
Please select an SLA Monitor
CANCEL
OK

```
 encryption aes-256 aes-192 aes
 integrity sha512 sha384 sha256 sha
 group 21 20 16 15 14
 prf sha512 sha384 sha256 sha
 lifetime seconds 86400
```

ステップ 10： FTDで設定されているものと同じパラメータを定義するIKEv2 ipsec-proposalを作成します。

<#root>

```
crypto ipsec ikev2 ipsec-proposal
```

AES-SHA

```
 protocol esp encryption aes-256 aes-192 aes
 protocol esp integrity sha-512 sha-384 sha-256 sha-1
```

ステップ 11新しい ipsecプロファイル、参照 ipsec-proposalはステップ10で作成します。

<#root>

```
crypto ipsec profile
```

demo_ipsec_profile

```
 set ikev2 ipsec-proposal
```

AES-SHA

```
 set security-association lifetime kilobytes 4608000
 set security-association lifetime seconds 28800
```

ステップ 12 IKEv2プロトコルを許可するグループポリシーを作成します。

<#root>

```
group-policy
```

demo_gp_192.168.30.1

```
 internal
group-policy demo_gp_192.168.30.1 attributes
 vpn-tunnel-protocol ikev2
```

ステップ 13 ステップ12で作成したグループポリシーを参照して、ピアFTDのOutside IPアドレス

のトンネルグループを作成します。 ftdで同じ事前共有鍵を設定します（ステップ3.7で作成）。

<#root>

```
tunnel-group 192.168.30.1 type ipsec-l2l
tunnel-group 192.168.30.1 general-attributes
 default-group-policy
```

demo_gp_192.168.30.1

```
tunnel-group 192.168.30.1 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

ステップ 14： 外部インターフェイスでIKEv2を有効にします。

```
crypto ikev2 enable outside
```

ステップ 15：仮想トンネルを作成します。

<#root>

```
interface Tunnel1
 nameif demovti_asa
 ip address 169.254.10.2 255.255.255.0
 tunnel source interface outside
 tunnel destination 192.168.30.1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile
```

demo_ipsec_profile

ステップ 16：スタティックルートを作成します。

```
route demovti_asa 192.168.10.0 255.255.255.0 169.254.10.1 1
route demovti_asa 192.168.20.0 255.255.255.0 169.254.10.1 1
route outside 0.0.0.0 0.0.0.0 192.168.40.3 1
```

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FTDとASA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。

FTD：

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ftdv742#
ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                           Remote
 32157565 192.168.30.1/500                                192.168.40.1/500                        G
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/67986 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x4cf55637/0xa493cc83

ftdv742# show crypto ipsec sa
interface: demovti
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.30.1

      Protected vrf (ivrf): Global
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer: 192.168.40.1


      #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
      #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 30, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.30.1/500, remote crypto endpt.: 192.168.40.1/500
      path mtu 1500, ipsec overhead 94(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: A493CC83
      current inbound spi : 4CF55637

    inbound esp sas:
      spi: 0x4CF55637 (1291146807)
         SA State: active
         transform: esp-aes-256 esp-sha-512-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4055040/16867)
```

```
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
    outbound esp sas:
      spi: 0xA493CC83 (2761149571)
        SA State: active
        transform: esp-aes-256 esp-sha-512-hmac no compression
        in use settings ={L2L, Tunnel, IKEv2, VTI, }
        slot: 0, conn_id: 13, crypto-map: __vti-crypto-map-Tunnel1-0-1
        sa timing: remaining key lifetime (kB/sec): (4285440/16867)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

ASA :

```
ASA9203# show crypto ikev2 sa

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                           Remote
 26025779 192.168.40.1/500                                192.168.30.1/500                        G
      Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/68112 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xa493cc83/0x4cf55637
ASA9203#
ASA9203# show cry
ASA9203# show crypto ipsec sa
interface: demovti_asa
    Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.40.1

      Protected vrf (ivrf): Global
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer: 192.168.30.1


      #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
      #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 30, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.40.1/500, remote crypto endpt.: 192.168.30.1/500
      path mtu 1500, ipsec overhead 94(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 4CF55637
```

```
      current inbound spi : A493CC83

    inbound esp sas:
      spi: 0xA493CC83 (2761149571)
         SA State: active
         transform: esp-aes-256 esp-sha-512-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4101120/16804)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0x4CF55637 (1291146807)
         SA State: active
         transform: esp-aes-256 esp-sha-512-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, VTI, }
         slot: 0, conn_id: 4, crypto-map: __vti-crypto-map-Tunnel1-0-1
         sa timing: remaining key lifetime (kB/sec): (4055040/16804)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

ステップ 2：FTDでVRFとグローバルのルートを確認します。

```
ftdv742# show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, 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 external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 192.168.30.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.30.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti
L        169.254.10.1 255.255.255.255 is directly connected, demovti
SI       192.168.10.0 255.255.255.0 [1/0] is directly connected, inside_red
SI       192.168.20.0 255.255.255.0 [1/0] is directly connected, inside_blue
C        192.168.30.0 255.255.255.0 is directly connected, outside
L        192.168.30.1 255.255.255.255 is directly connected, outside


ftdv742# show route vrf vrf_blue


Routing Table: vrf_blue
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, 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 external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set

C        192.168.20.0 255.255.255.0 is directly connected, inside_blue
L        192.168.20.1 255.255.255.255 is directly connected, inside_blue
SI       192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti


ftdv742# show route vrf vrf_red


Routing Table: vrf_red
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, 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 external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set

C        192.168.10.0 255.255.255.0 is directly connected, inside_red
L        192.168.10.1 255.255.255.255 is directly connected, inside_red
SI       192.168.50.0 255.255.255.0 [1/0] is directly connected, demovti
```

ステップ 3：pingテストを確認します。

pingを実行する前に、FTDでshow crypto ipsec sa | inc interface:|encap|decapのカウンタを確認します。

この例では、Tunnel1でカプセル化とカプセル化解除の両方について30個のパケットが示されています。

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 30, #pkts encrypt: 30, #pkts digest: 30
      #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
ftdv742#
```

Client1 ping Client3が正常に実行されました。

```
Client1#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/299/620 ms
```

Client2 ping Client3が正常に実行されました。

```
Client2#ping 192.168.50.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 11/297/576 ms
```

次のカウンタを確認します。 show crypto ipsec sa | inc interface:|encap|decap FTDで確認します。

この例では、pingが成功した後、Tunnel1はカプセル化とカプセル化解除の両方について40個のパケットを示しています。さらに、どちらのカウンタも10パケット増加し、10個のpingエコー要求に一致しています。これは、pingトラフィックがIPSecトンネルを正常に通過したことを示しています。

```
ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 40, #pkts encrypt: 40, #pkts digest: 40
      #pkts decaps: 40, #pkts decrypt: 40, #pkts verify: 40
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

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、ルート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 ip routing
```

参考

Cisco Secure Firewall Device Managerコンフィギュレーションガイド、バージョン7.4

Cisco Secure Firewall ASA VPN CLIコンフィギュレーションガイド9.20

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。