# Configurar VPN Site a Site com Reconhecimento de VRF baseado em Rota no FTD Gerenciado pelo FDM

## Contents



## Introdução

Este documento descreve como configurar a VPN de site a site baseada em rota com reconhecimento de VRF em FTD gerenciado pelo FDM.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Entendimento básico de VPN
- Compreensão básica de Virtual Routing and Forwarding (VRF)
- Experiência com o FDM

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco FTDv versão 7.4.2
- Cisco FDM versão 7.4.2
- Cisco ASAv versão 9.20.3

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

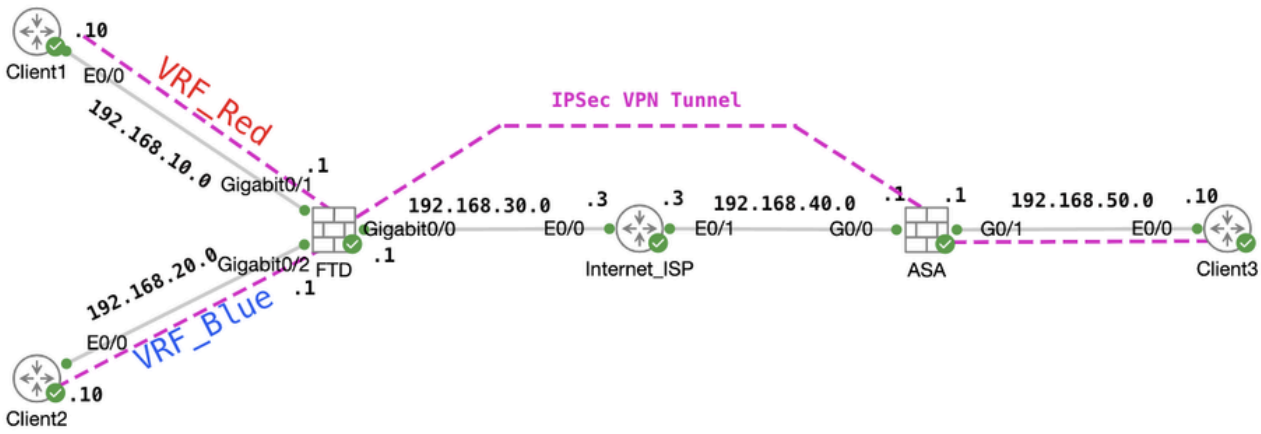
# Informações de Apoio

O Virtual Routing and Forwarding (VRF) no Firepower Device Manager (FDM) permite criar várias instâncias de roteamento isoladas em um único dispositivo Firepower Threat Defense (FTD). Cada instância do VRF opera como um roteador virtual separado com sua própria tabela de roteamento, permitindo a separação lógica do tráfego de rede e fornecendo recursos avançados de segurança e gerenciamento de tráfego.

Este documento explica como configurar VPN IPSec sensível a VRF com VTI. As redes VRF Red e VRF Blue estão atrás do FTD. Client1 na rede VRF Red e Client2 no VRF Blue se comunicariam com o Client 3 atrás do ASA através do túnel VPN IPSec.

# Configurar

## Diagrama de Rede

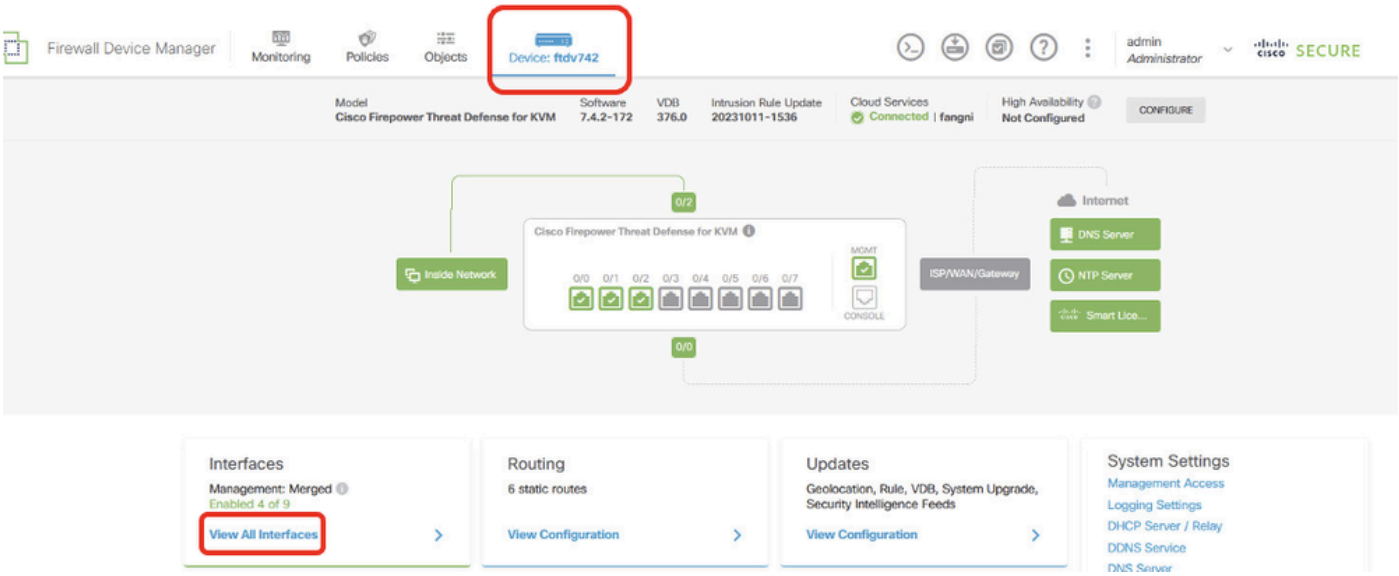



Topologia

## Configurar o FTD

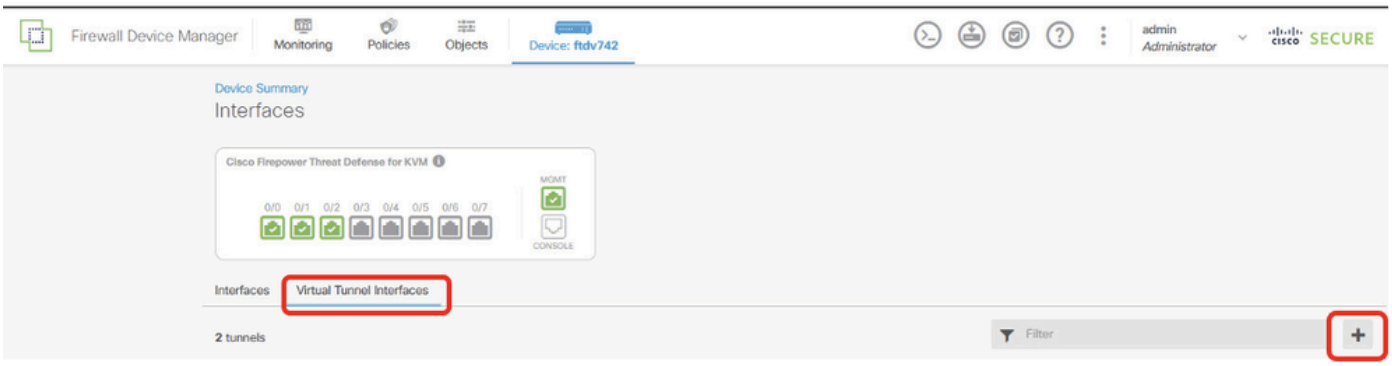
Etapa 1. É essencial garantir que a configuração preliminar da interconectividade IP entre os nós tenha sido devidamente concluída. O Cliente1 e o Cliente2 estão com o endereço IP interno do FTD como gateway.  O Client3 está com o endereço IP interno ASA como gateway.

Etapa 2. Criar interface de túnel virtual. Efetue login na GUI do FDM do FTD. Navegue até Dispositivo > Interfaces . Clique em View All Interfaces .




FTD_View_Interfaces

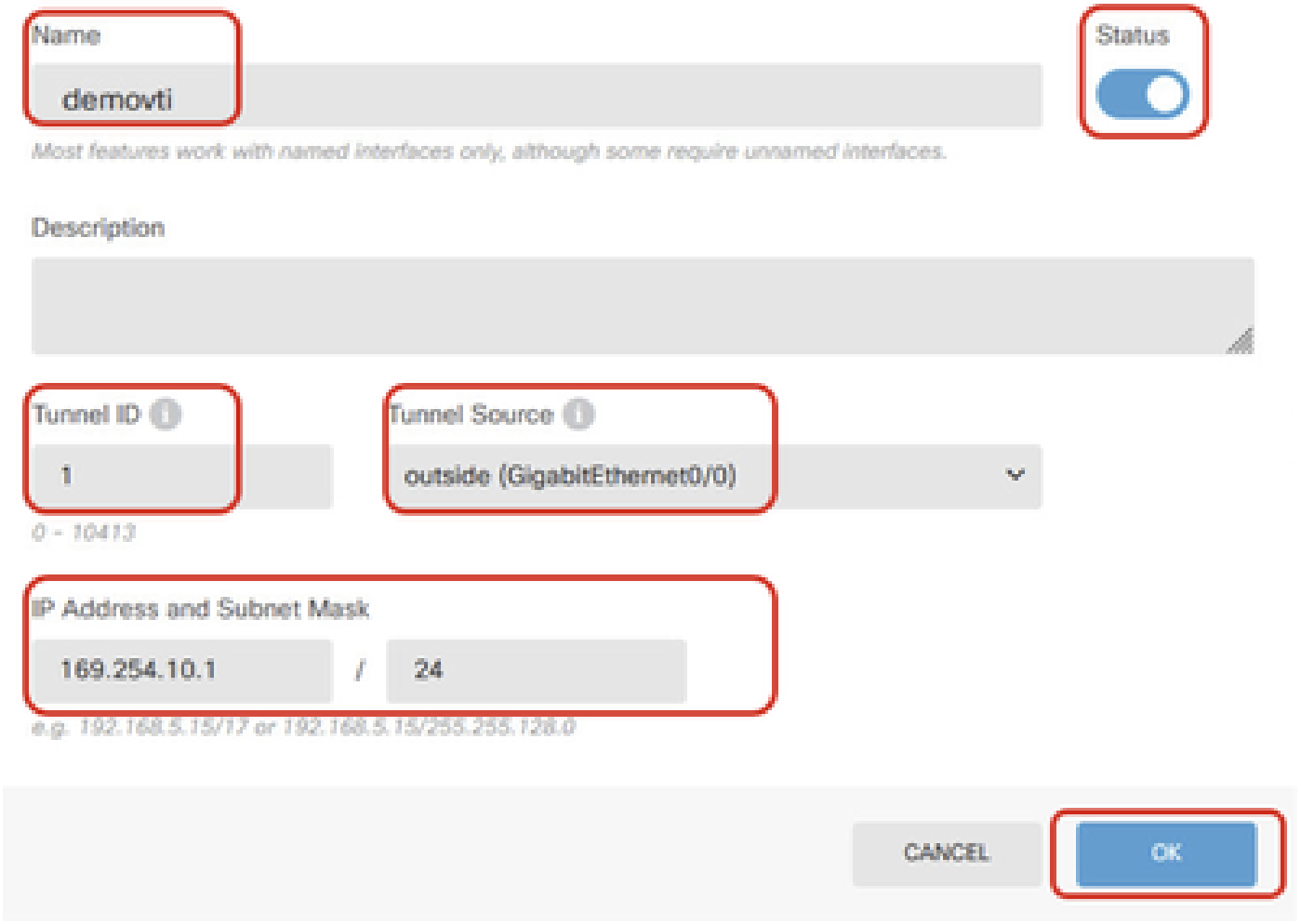
Etapa 2.1. Clique na guia Virtual Tunnel Interfaces. Clique no botão +.




FTD_Create_VTI

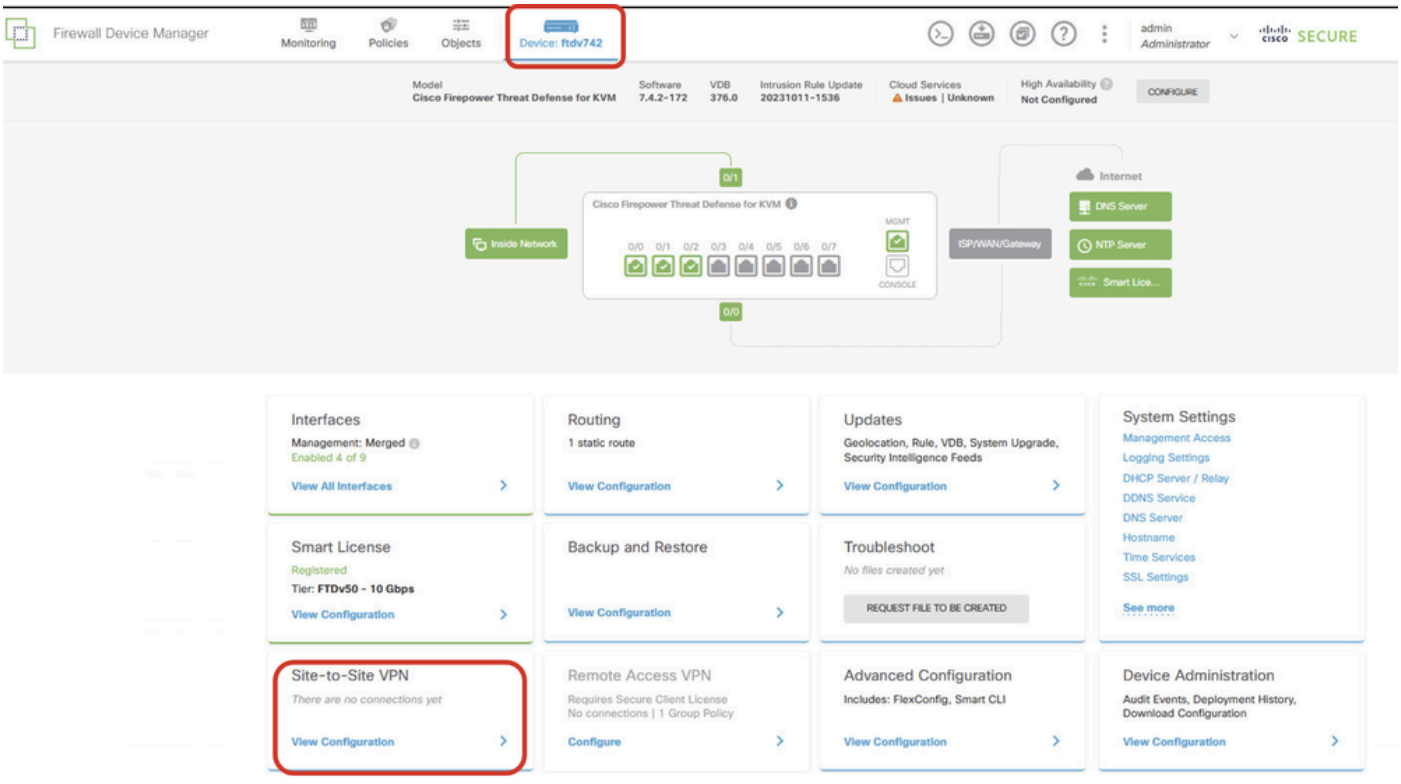
Etapa 2.2. Forneça as informações necessárias. Clique no botão OK.

- Nome: demovti
- ID do túnel: 1
- Origem do túnel: externo (GigabitEthernet0/0)
- Endereço IP e máscara de sub-rede: 169.254.10.1/24
- Status: clique no controle deslizante para a posição Habilitado



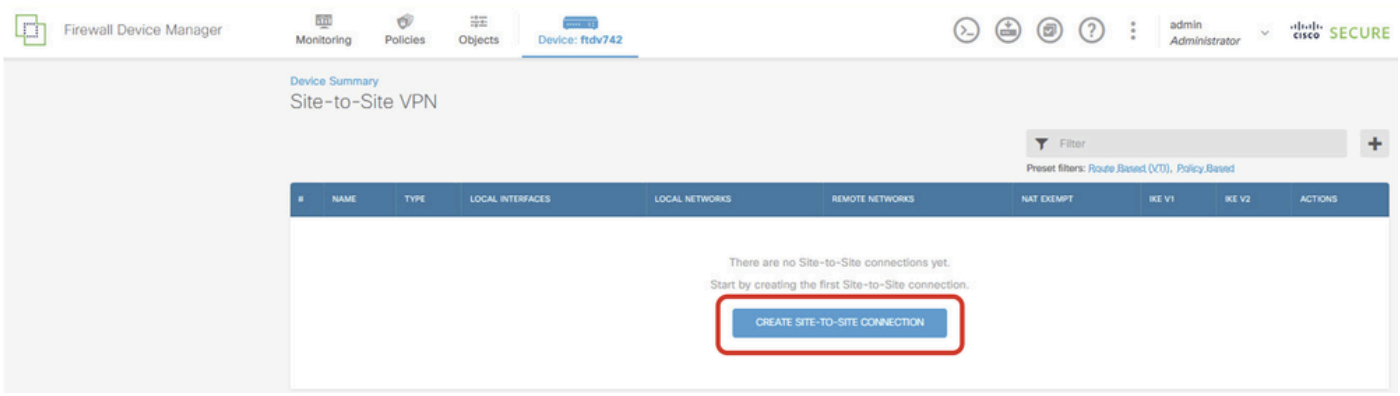

FTD_Create_VTI_Details

Etapa 3. Navegue até Device > Site-to-Site VPN . Clique no botão View Configuration.



FTD_Site-to-Site_VPN_View_Configurations

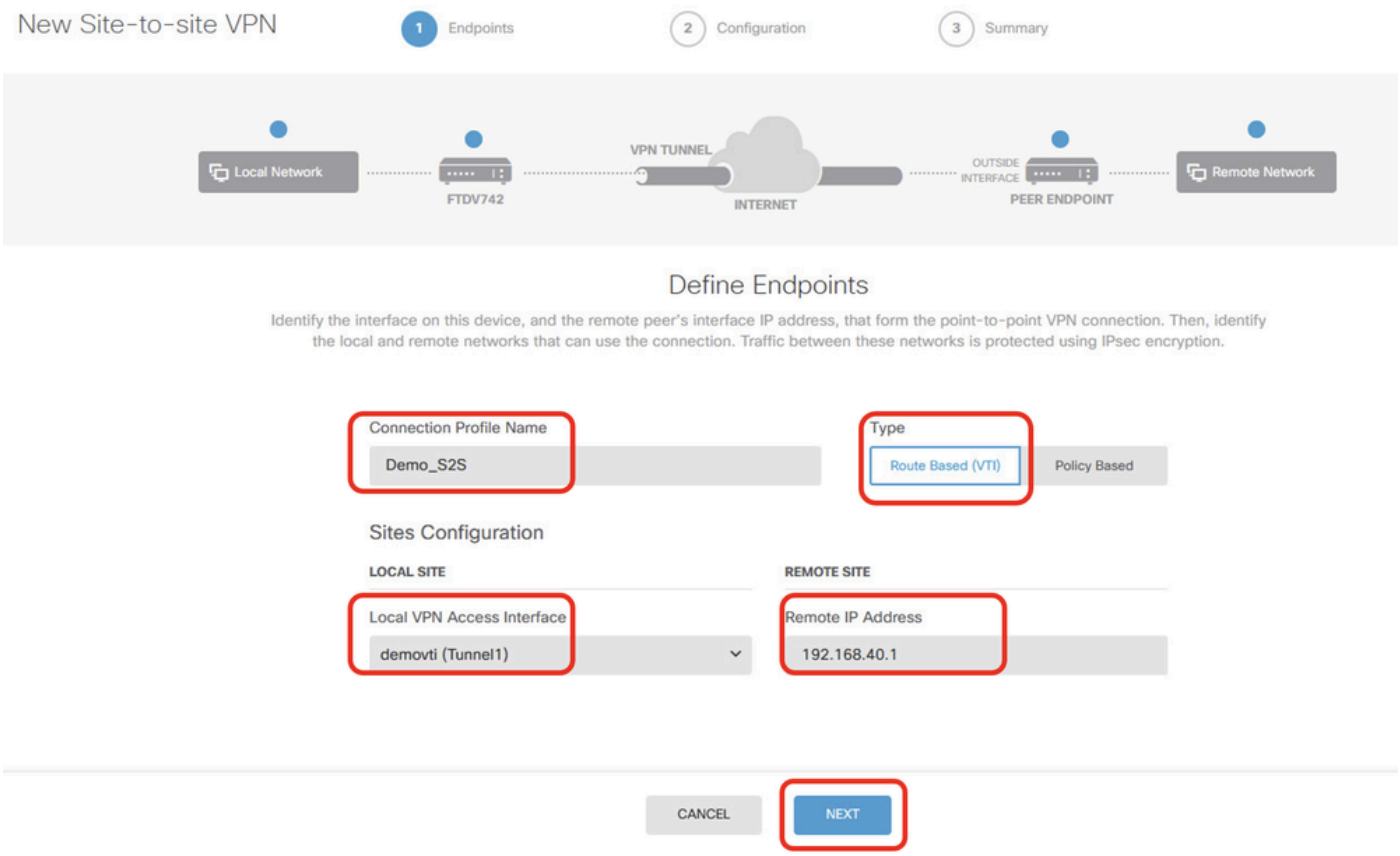
Etapa 3.1. Comece a criar uma nova VPN site a site. Clique no botão CRIAR CONEXÃO SITE A SITE. Ou clique no botão +.




FTD_Create_Site2Site_Connection

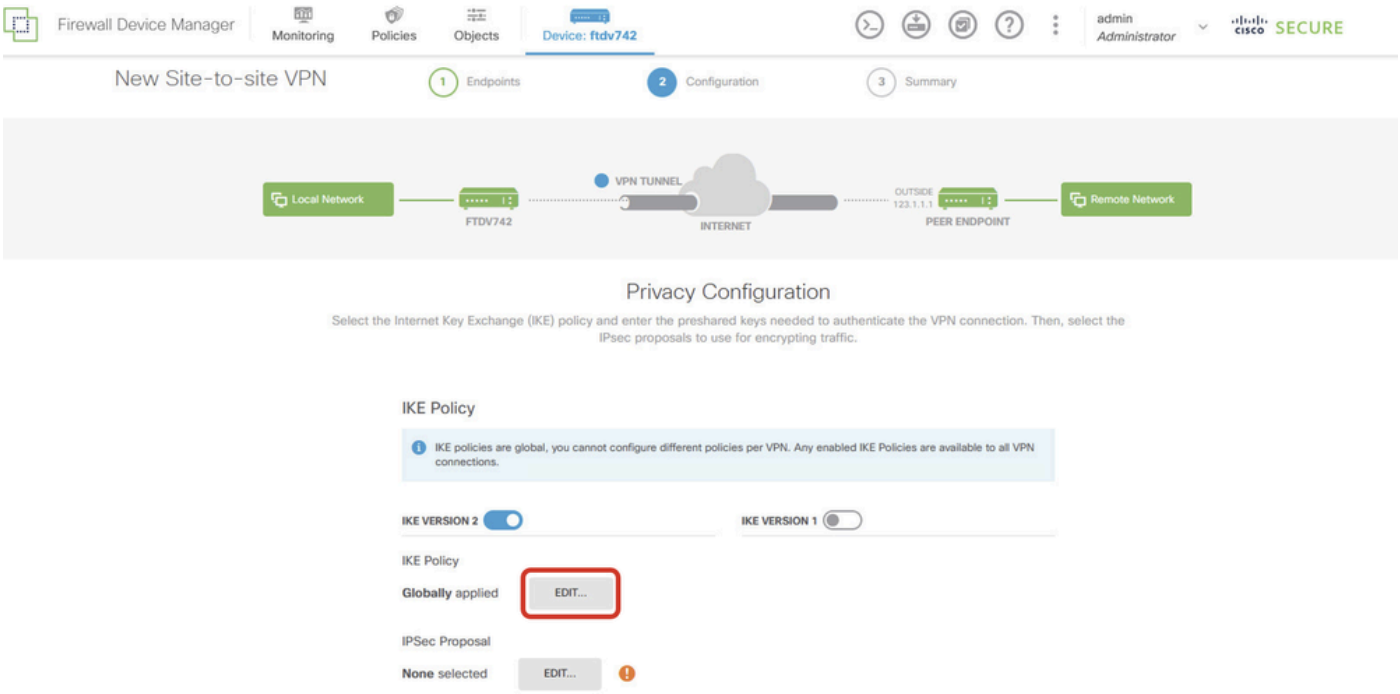
Etapa 3.2. Fornecer informações necessárias. Clique no botão AVANÇAR.

- Nome do perfil de conexão: Demo_S2S
- Digite: Baseado em Rota (VTI)
- Local VPN Access Interface: demovti (criada na Etapa 2)
- Endereço IP remoto: 192.168.40.1 (esse é o endereço IP externo do ASA do peer)




FTD_Site-to-Site_VPN_Endpoints

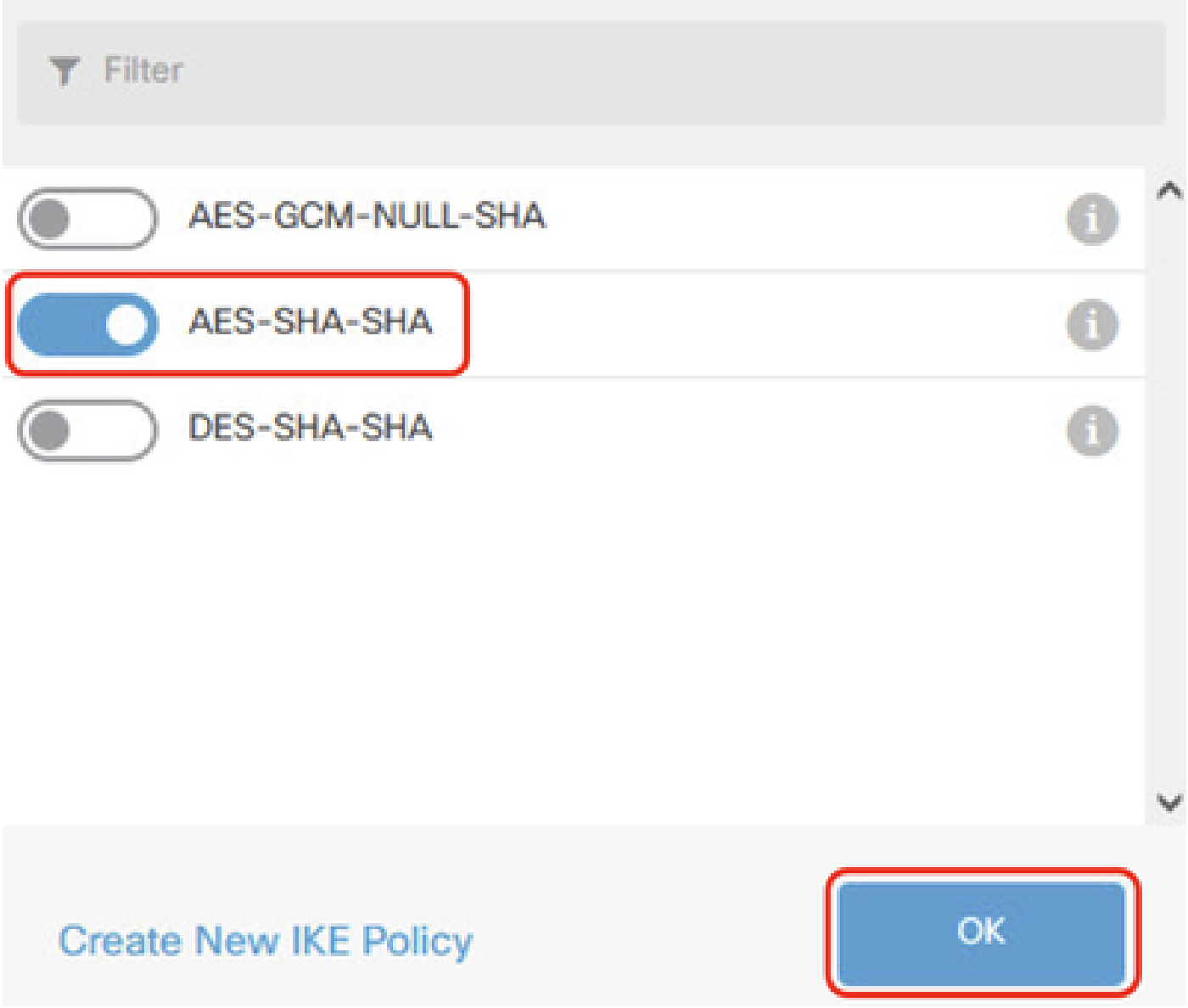
Etapa 3.3. Navegue até Política IKE. Clique no botão EDITAR.




FTD_Edit_IKE_Policy

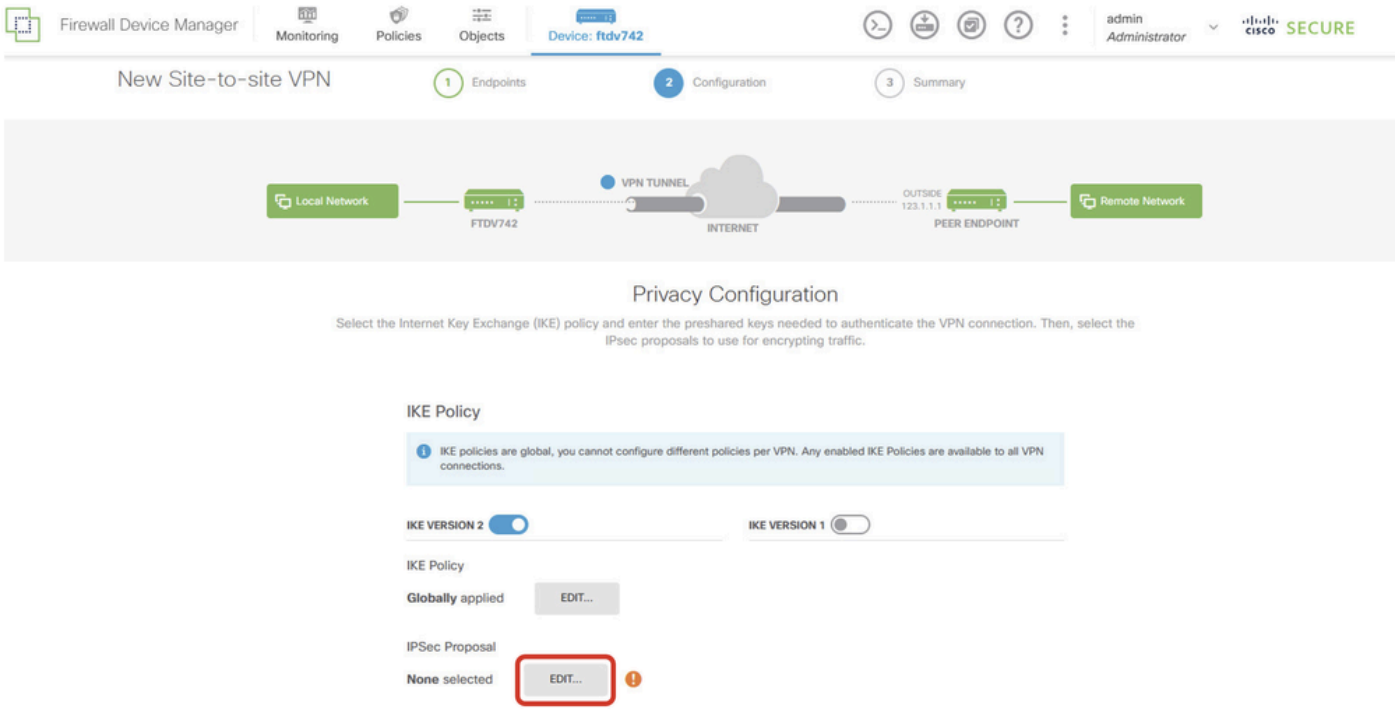
Etapa 3.4. Para a política IKE, você pode usar o predefinido ou pode criar um novo clicando em  Criar nova política IKE  .

Neste exemplo, alterne um nome de política IKE existente AES-SHA-SHA . Clique no botão OK para salvar.




FTD_Enable_IKE_Policy

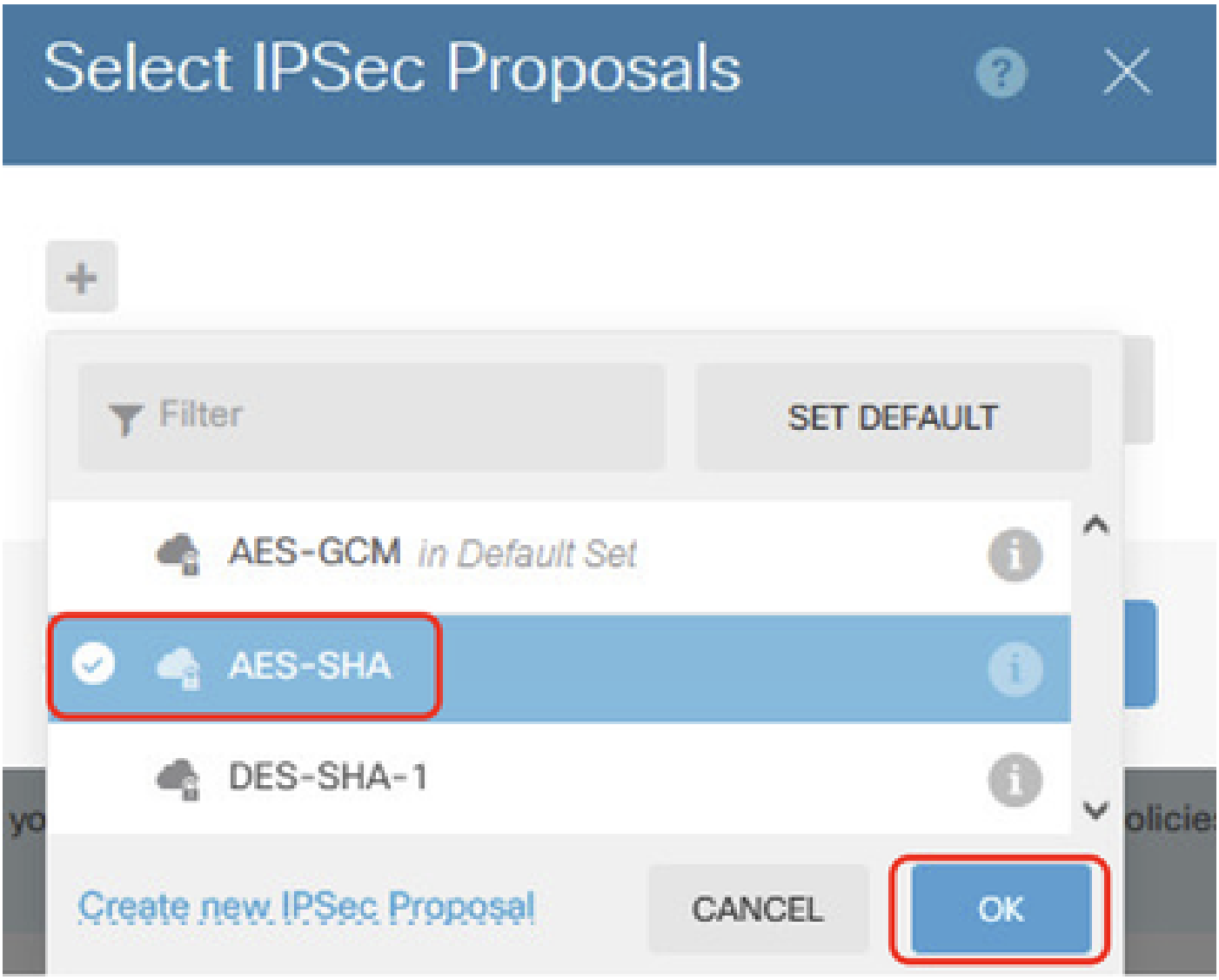
Etapa 3.5. Navegue até IPSec Proposal (Proposta IPSec). Clique no botão EDITAR.




FTD_Edit_IPSec_Proposal

Etapa 3.6. Para uma proposta IPSec, você pode usar uma predefinida ou pode criar uma nova clicando em Criar nova proposta IPSec .

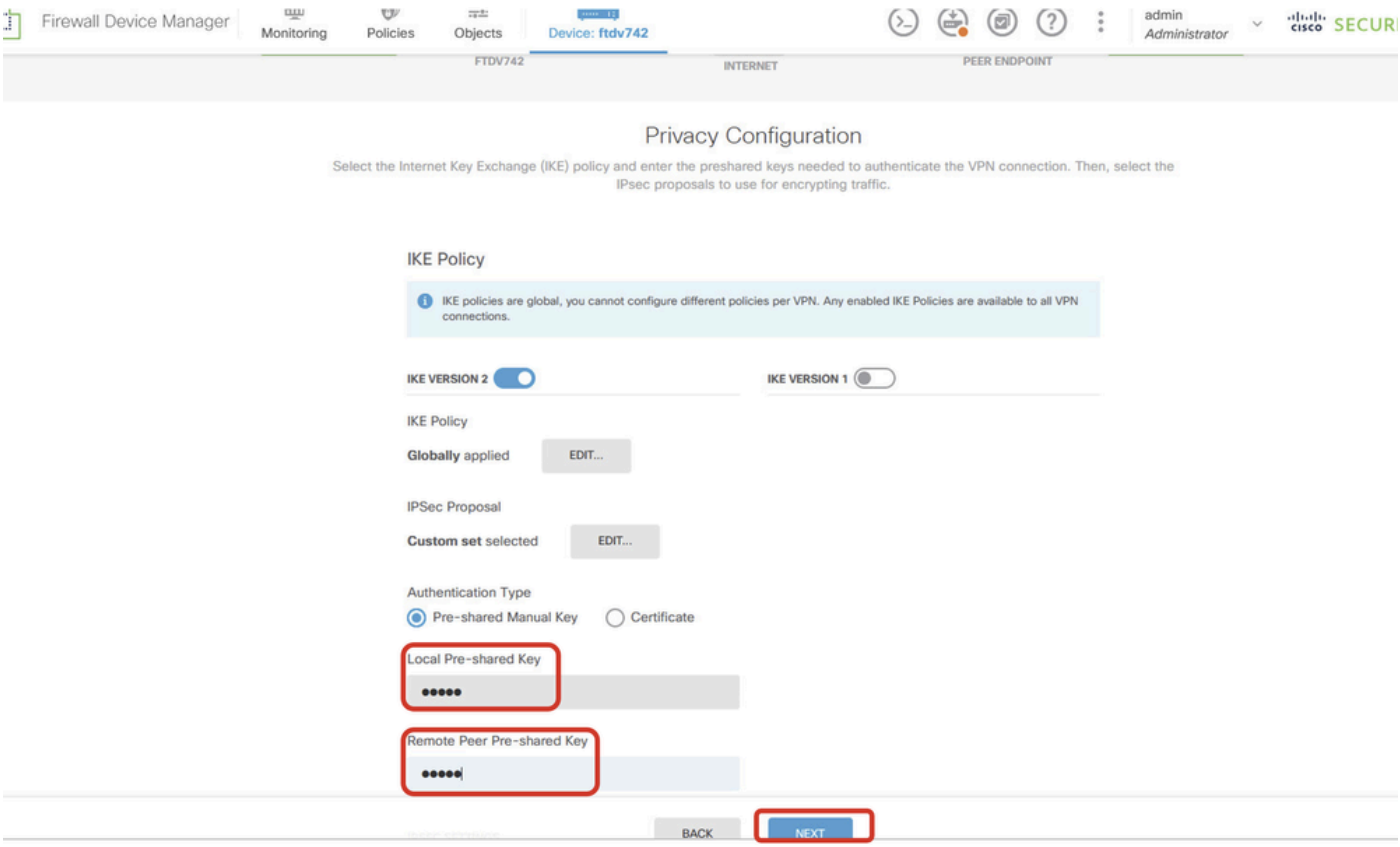
Neste exemplo, alterne um nome de Proposta IPSec existente AES-SHA . Clique em OK para salvar.




FTD_Enable_IPSec_Proposal

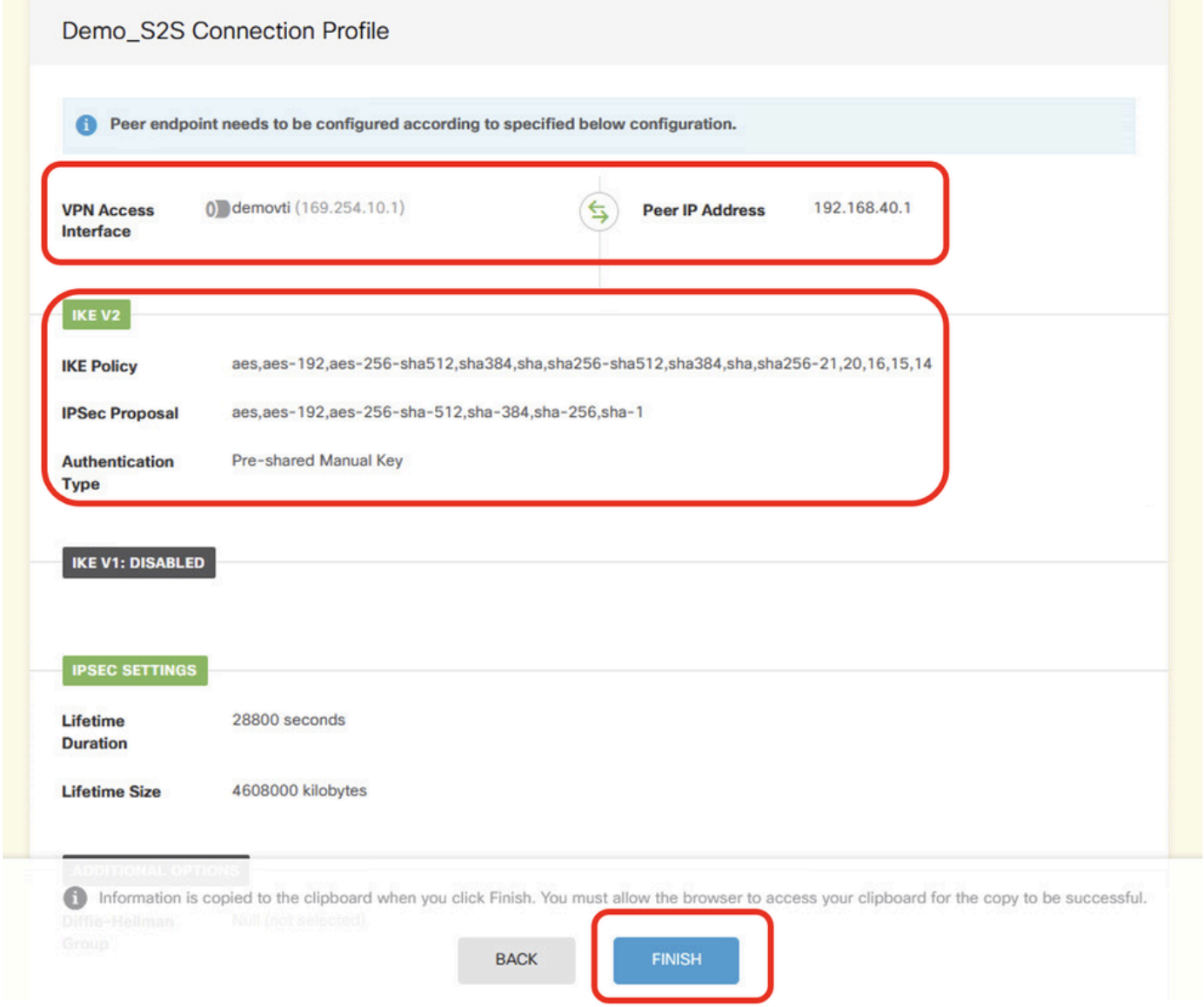
Etapa 3.7. Role a página para baixo e configure a chave pré-compartilhada. Clique no botão AVANÇAR.

Anote essa chave pré-compartilhada e configure-a mais tarde no ASA.



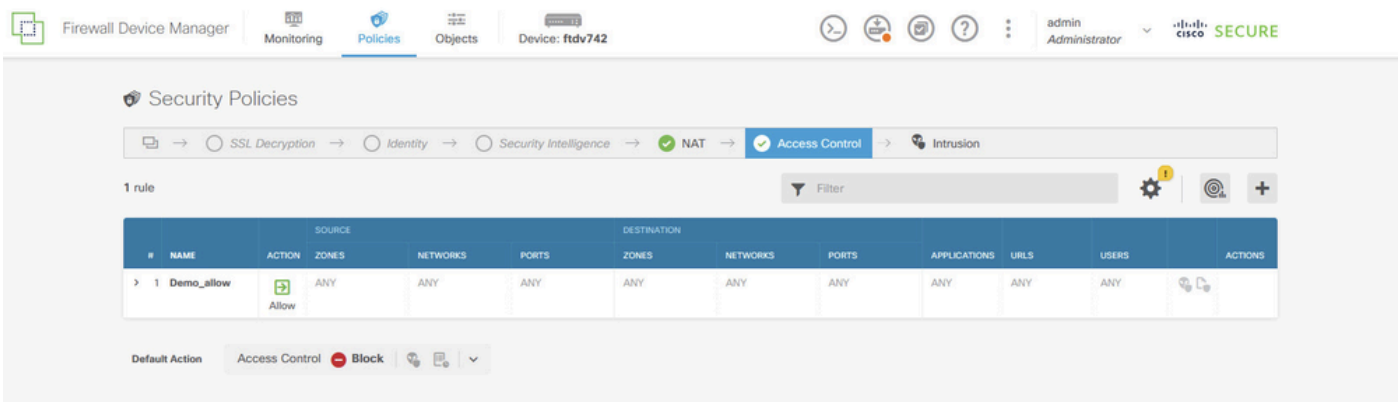

FTD_Configure_Pre_Shared_Key

Etapa 3.8. Rever a configuração da VPN. Se algo precisar ser modificado, clique no botão VOLTAR. Se tudo estiver bem, clique no botão FINISH.




FTD_Review_VPN_Configuration

Etapa 3.9. Crie uma regra de Controle de Acesso para permitir que o tráfego passe pelo FTD. Neste exemplo, permita todos para demonstração. Modifique sua política com base em suas necessidades reais.

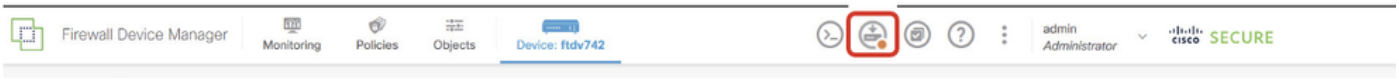



FTD_ACP_Example

Etapa 3.10. (Opcional) Configure a regra de isenção de NAT para o tráfego do cliente no FTD se

houver um NAT dinâmico configurado para o cliente acessar a Internet. Neste exemplo, não há necessidade de configurar uma regra de isenção de NAT porque não há NAT dinâmico configurado em FTD.

Etapa 3.11. Implantar as alterações de configuração.




FTD_Deployment_Changes

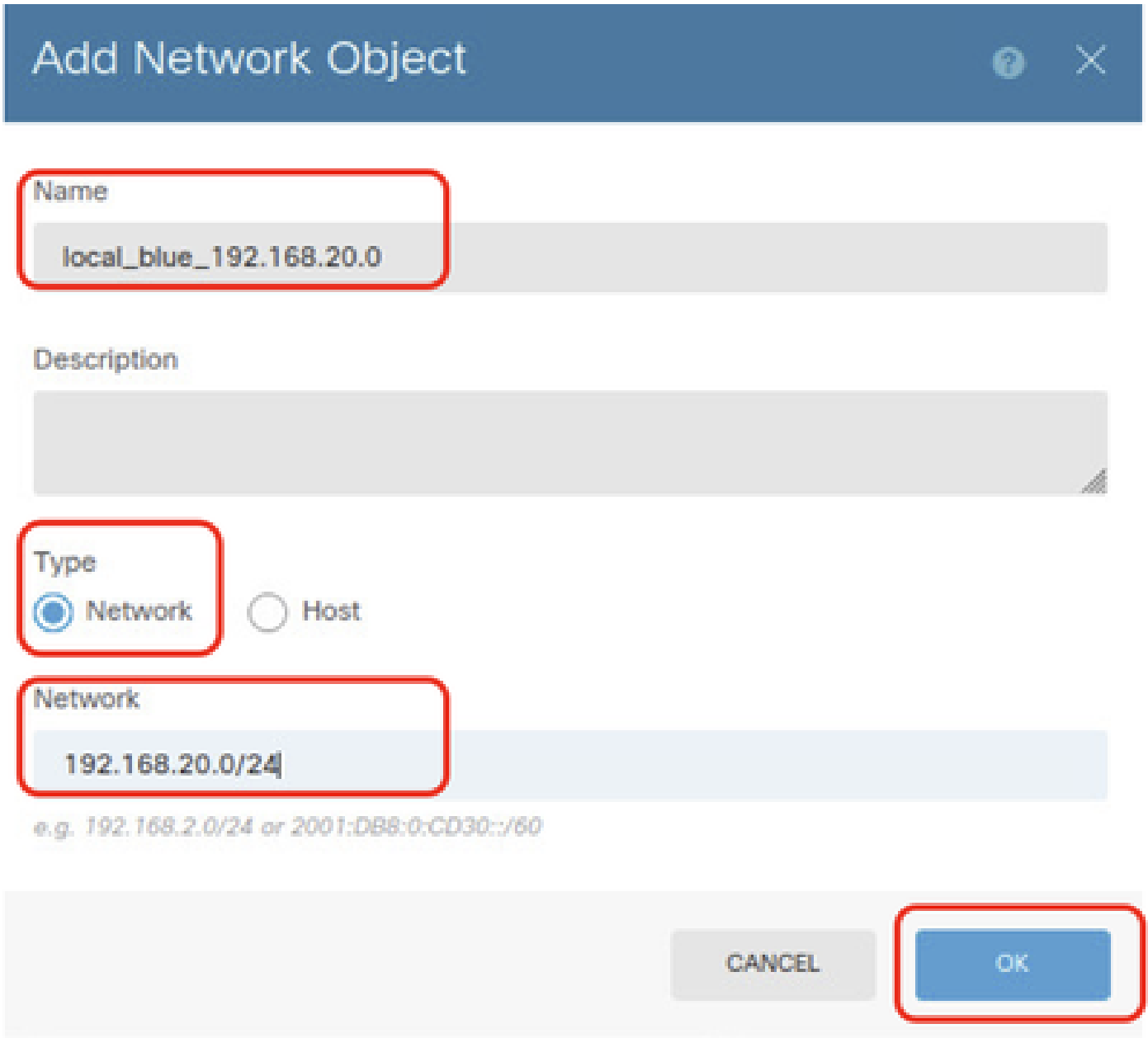
Etapa 4. Configurar roteadores virtuais.

Etapa 4.1. Crie objetos de rede para a rota estática. Navegue até Objetos > Redes , clique no botão +.


FTD_Create_NetObjects

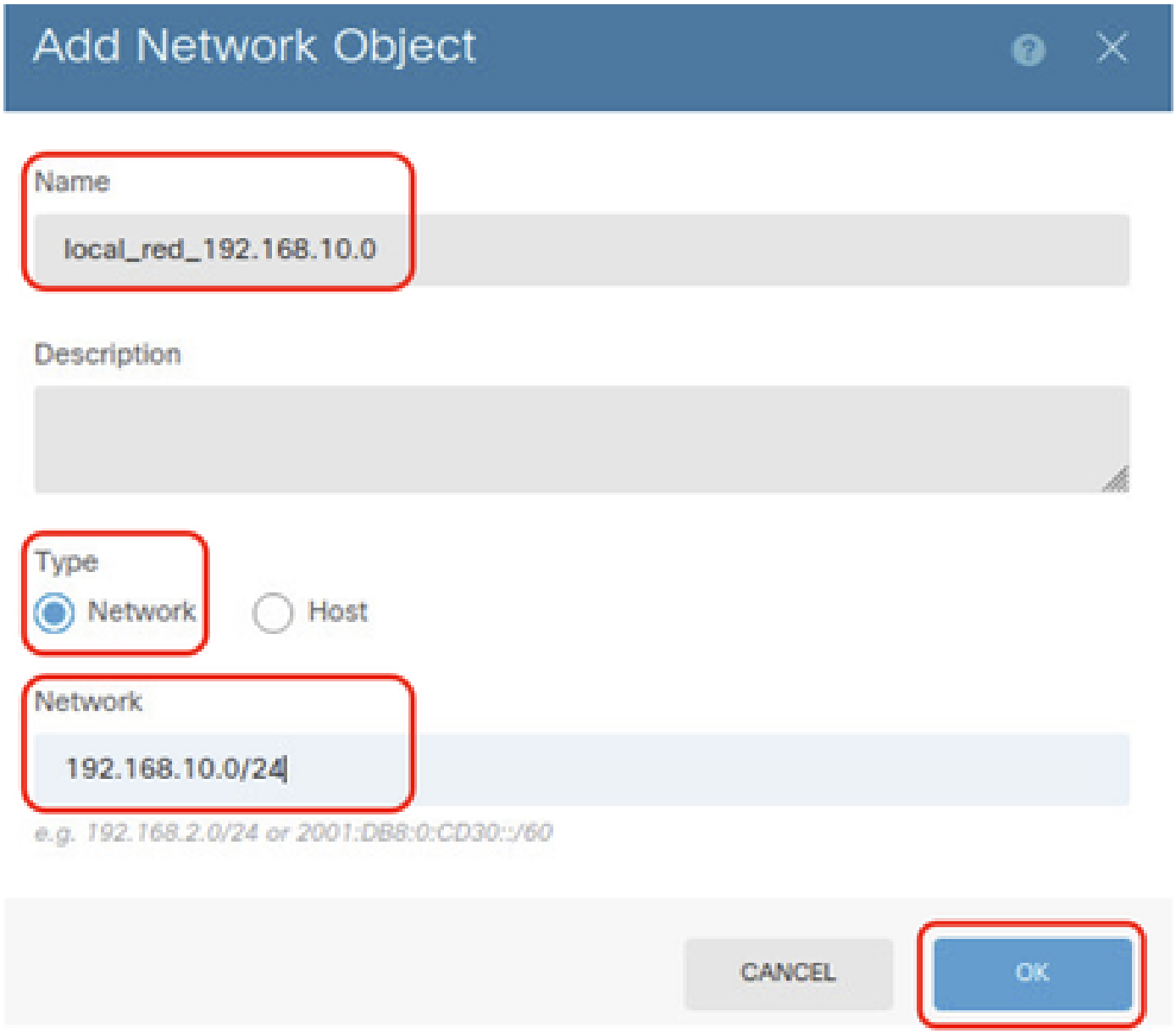
Etapa 4.2. Forneça as informações necessárias de cada objeto de rede. Clique no botão OK.

- Nome: local_blue_192.168.20.0
- Digite: Rede
- Rede: 192.168.20.0/24



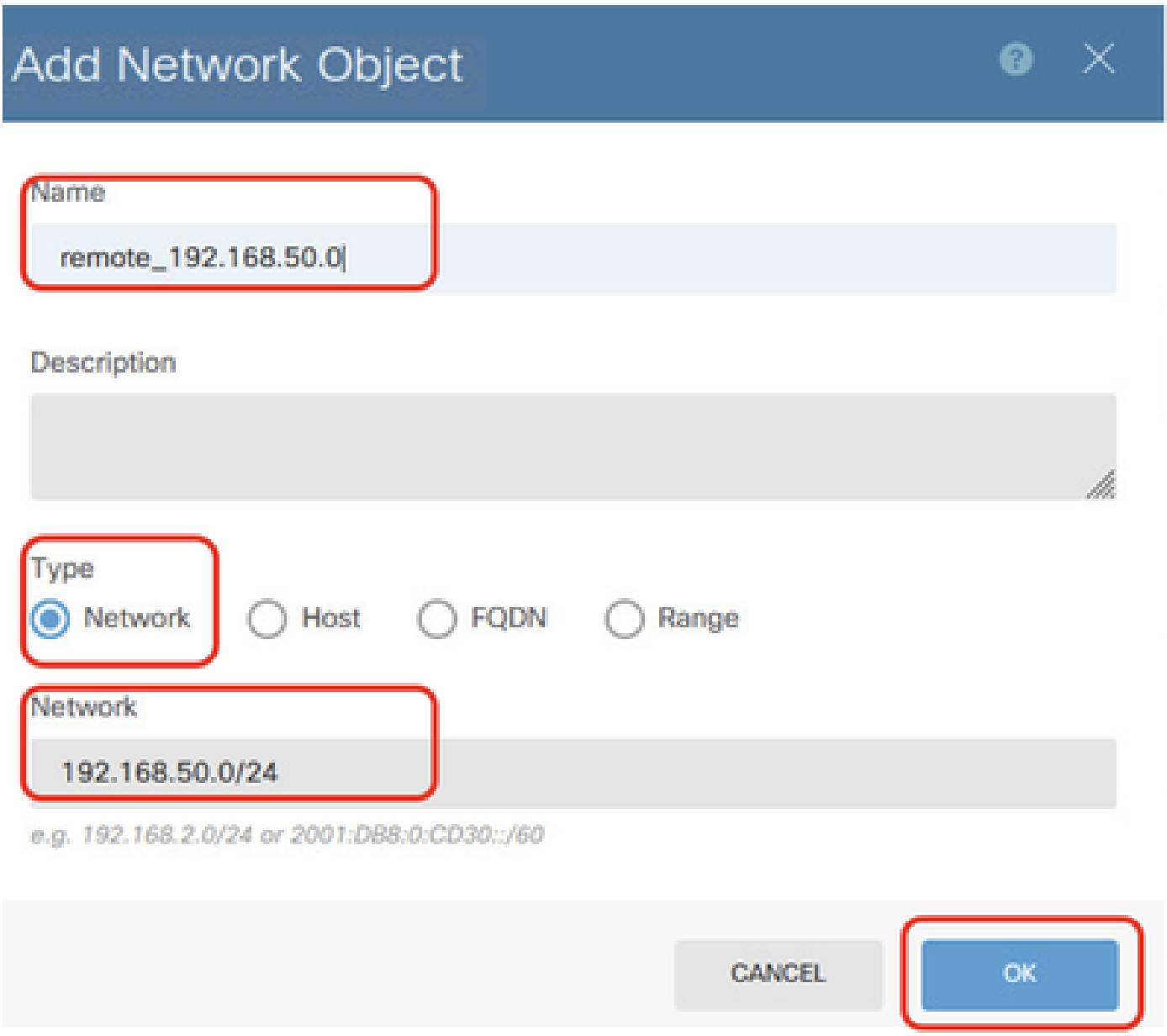

FTD_VRF_Blue_Network

- Nome: local_red_192.168.10.0
- Digite: Rede
- Rede: 192.168.10.0/24



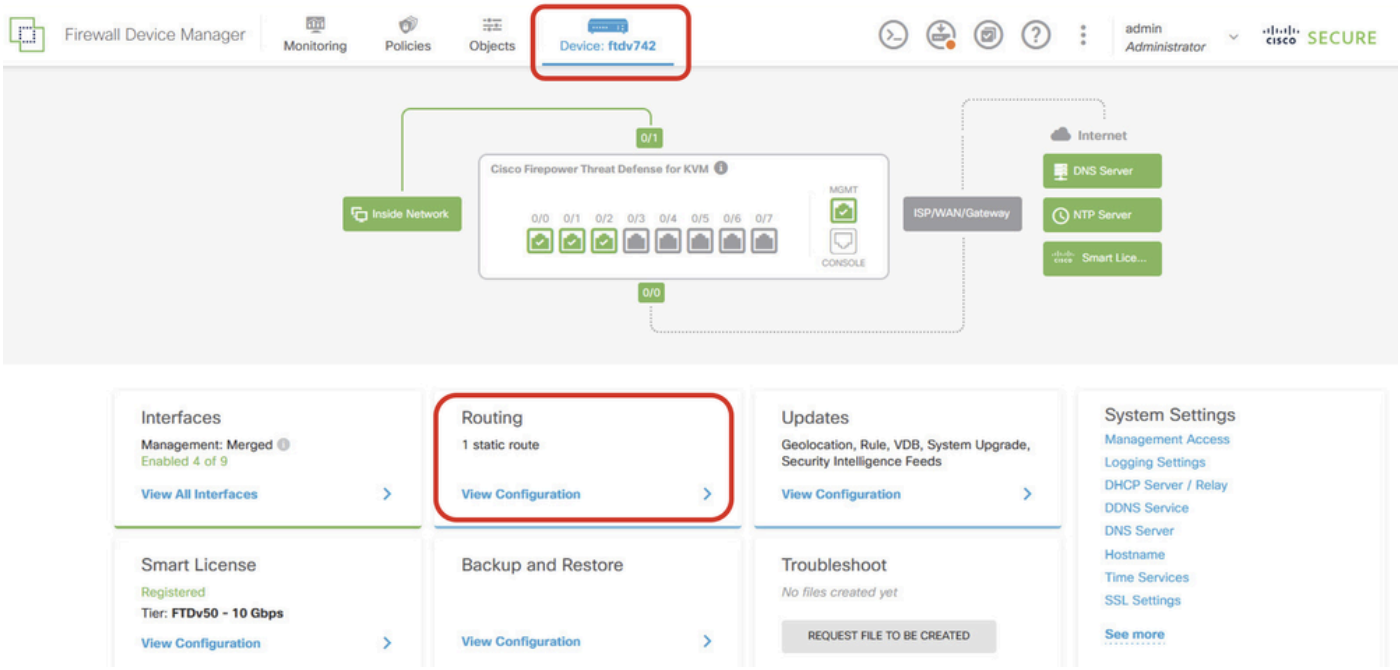

FTD_VRF_Red_Network

- Nome: remote_192.168.50.0
- Digite: Rede
- Rede: 192.168.50.0/24




FTD_Remote_Network

Etapa 4.3. Crie o primeiro roteador virtual. Navegue até Device > Routing . Clique em View Configuration .



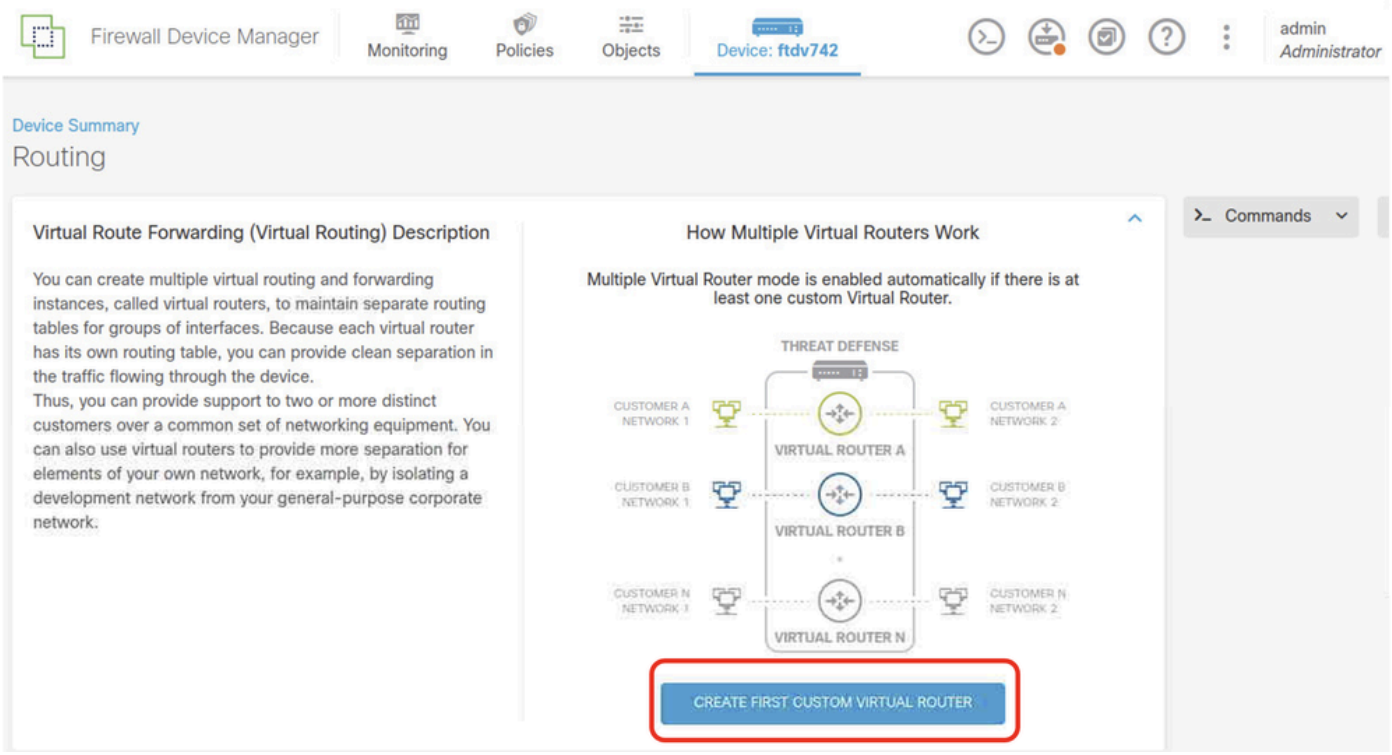

FTD_View_Routing_Configuration

Etapa 4.4. Clique em Add Multiple Virtual Routers .

Note: uma rota estática através da interface externa já foi configurada durante a inicialização do FDM. Se você não tiver, configure-o manualmente.


FTD_Add_First_Virtual_Router1

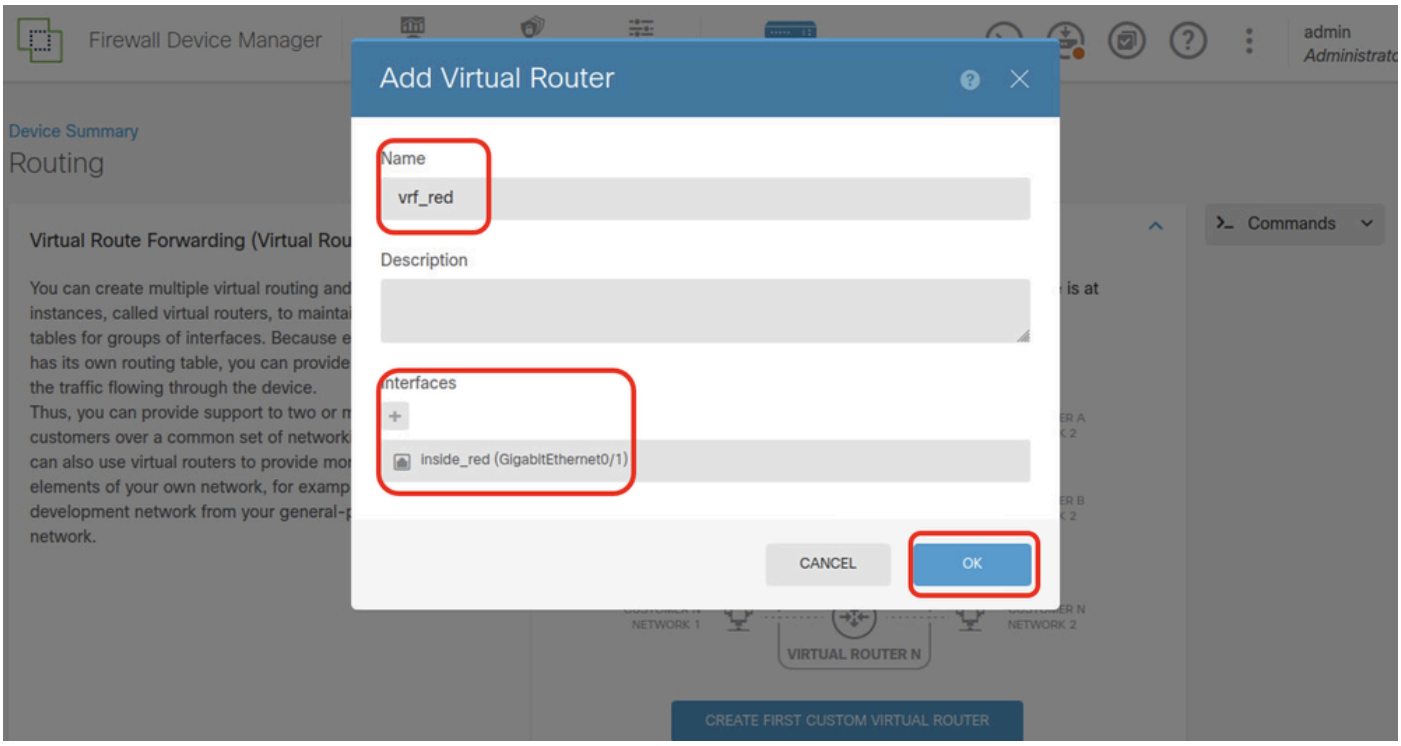
Etapa 4.5. Clique em CRIAR PRIMEIRO ROTEADOR VIRTUAL PERSONALIZADO .




FTD_Add_First_Virtual_Router2

Etapa 4.6. Forneça as informações necessárias sobre o primeiro roteador virtual. Clique no botão OK. Após a primeira criação do roteador virtual, um nome vrf Global seria mostrado automaticamente.

- Nome: vrf_red
- Interfaces: inside_red (GigabitEthernet0/1)



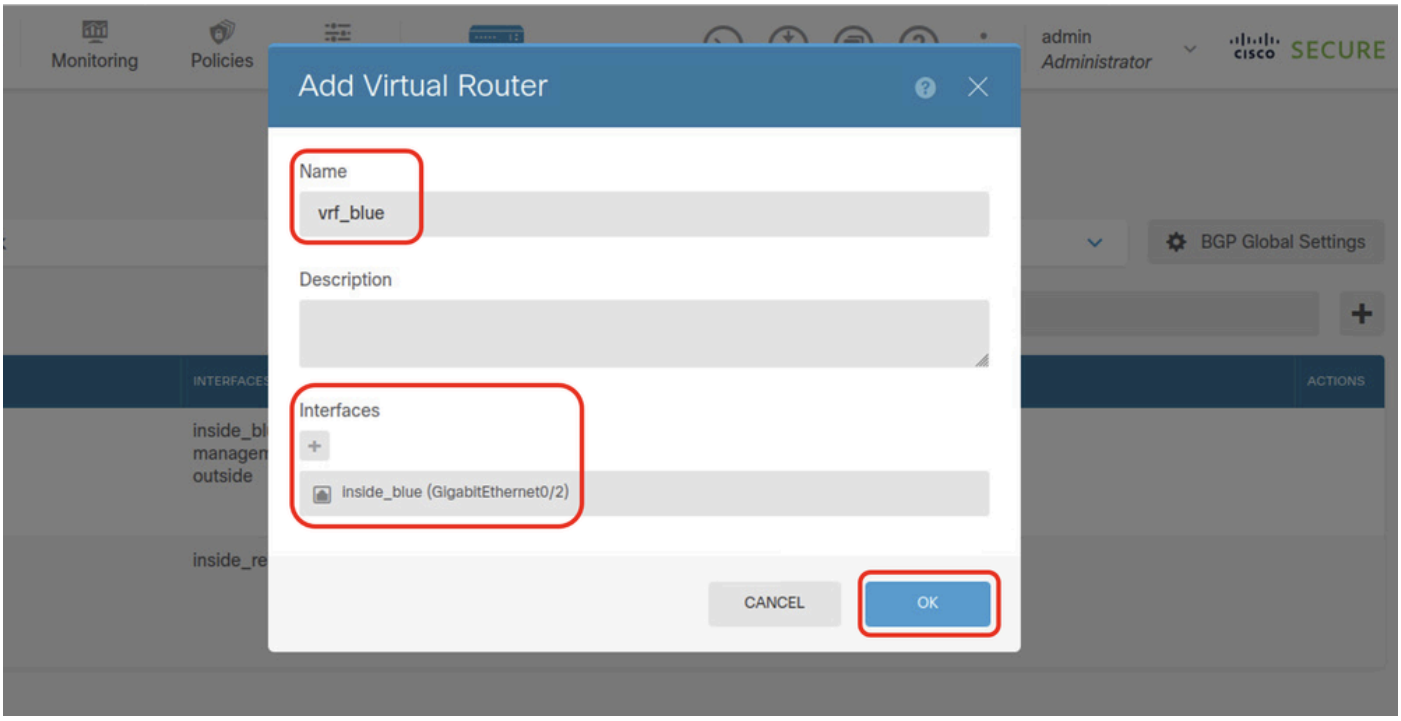

FTD_Add_First_Virtual_Router3

Etapa 4.7. Crie o segundo roteador virtual. Navegue até Device > Routing . Clique em View Configuration . Clique no botão +.


FTD_Add_Second_Virtual_Router

Etapa 4.8. Fornecer as informações necessárias do segundo roteador virtual. Clique no botão OK

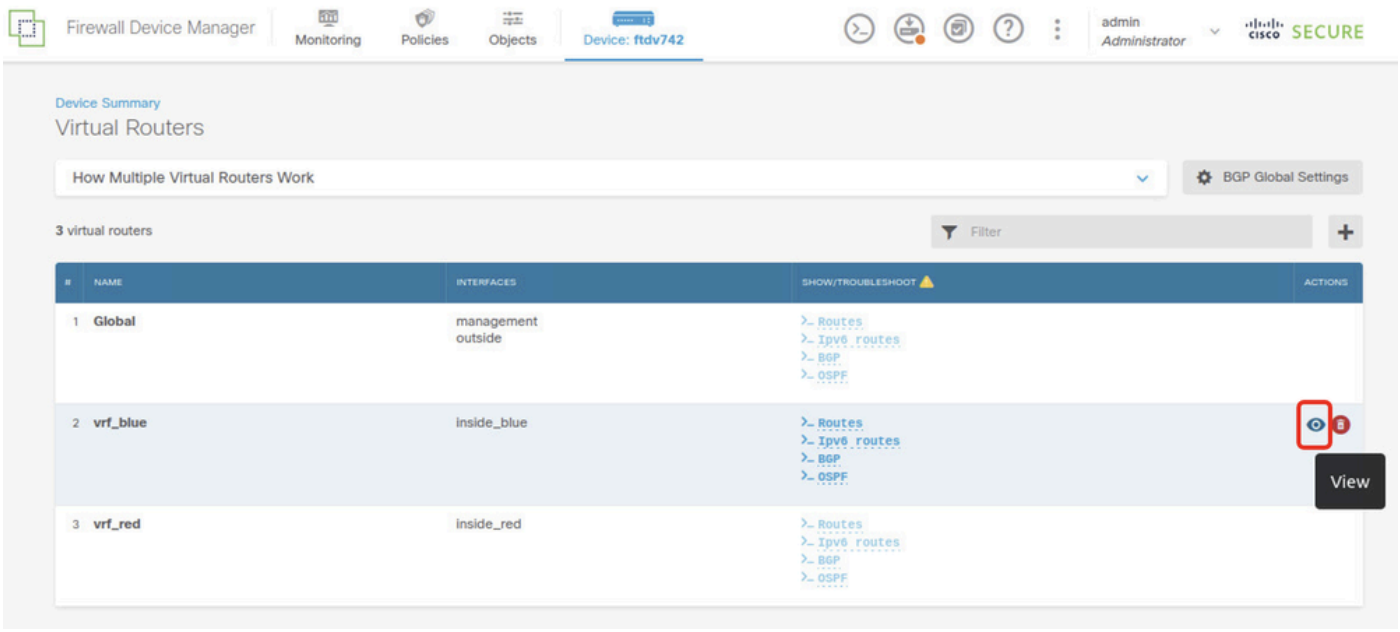
- Nome: vrf_blue
- Interfaces: inside_blue (GigabitEthernet0/2)




FTD_Add_Second_Virtual_Router2

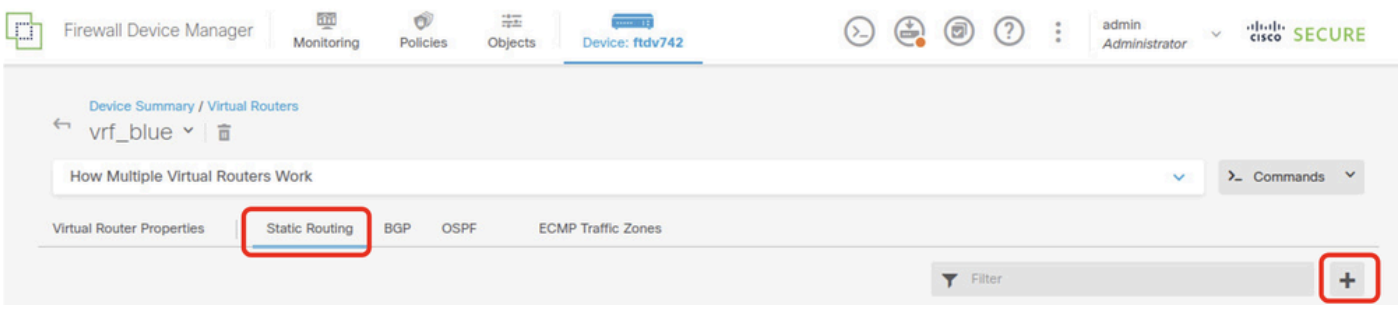
Etapa 5. Criar vazamento de rota de vrf_blue para Global. Essa rota permite que os pontos de extremidade na rede 192.168.20.0/24 iniciem conexões que atravessariam o túnel VPN site a site. Para este exemplo, o endpoint remoto está protegendo a rede 192.168.50.0/24.

Navegue até Device > Routing . Clique em View Configuration . clique no ícone View na célula Ação do roteador virtual vrf_blue.




FTD_View_VRF_Blue

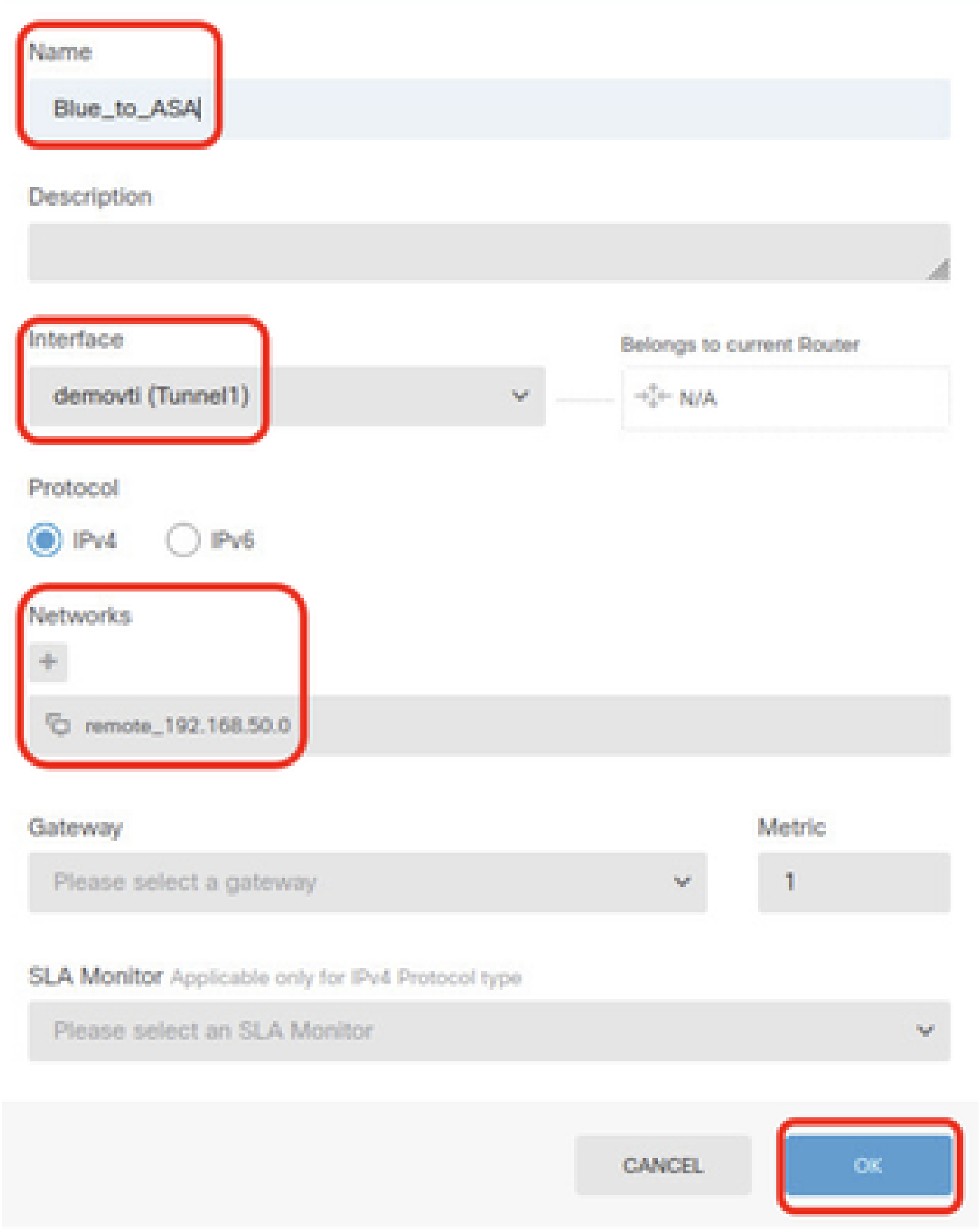
Etapa 5.1. Clique na guia Static Routing. Clique no botão +.




FTD_Create_Static_Route_VRF_Blue

Etapa 5.2. Forneça as informações necessárias. Clique no botão OK.

- Nome: Blue_to_ASA
- Interface: demovti (Tunnel1)
- Redes: remote_192.168.50.0
- Gateway: Deixe este item em branco.

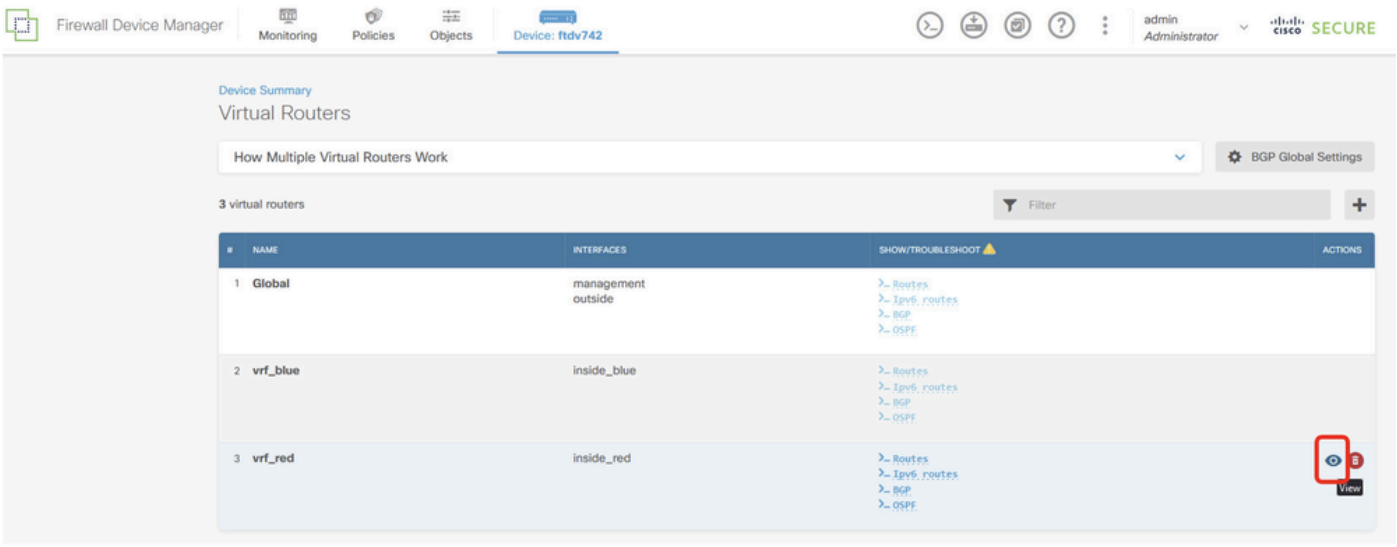



FTD_Create_Static_Route_VRF_Blue_Details

Etapa 6. Criar vazamento de rota de vrf_red para Global. Essa rota permite que os pontos finais na rede 192.168.10.0/24 iniciem conexões que atravessariam o túnel VPN site a site. Para este

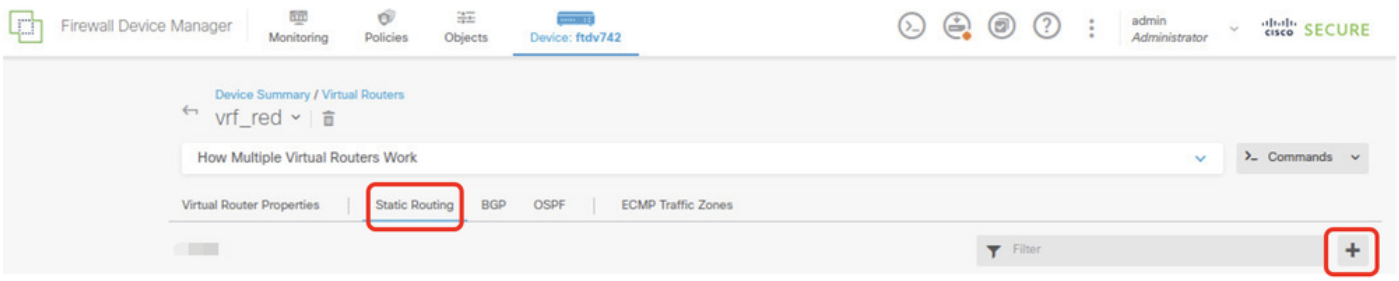
exemplo, o endpoint remoto está protegendo a rede 192.168.50.0/24.

Navegue até Device > Routing . Clique em View Configuration . clique no ícone View na célula Ação do roteador virtual vrf_red.




FTD_View_VRF_Red

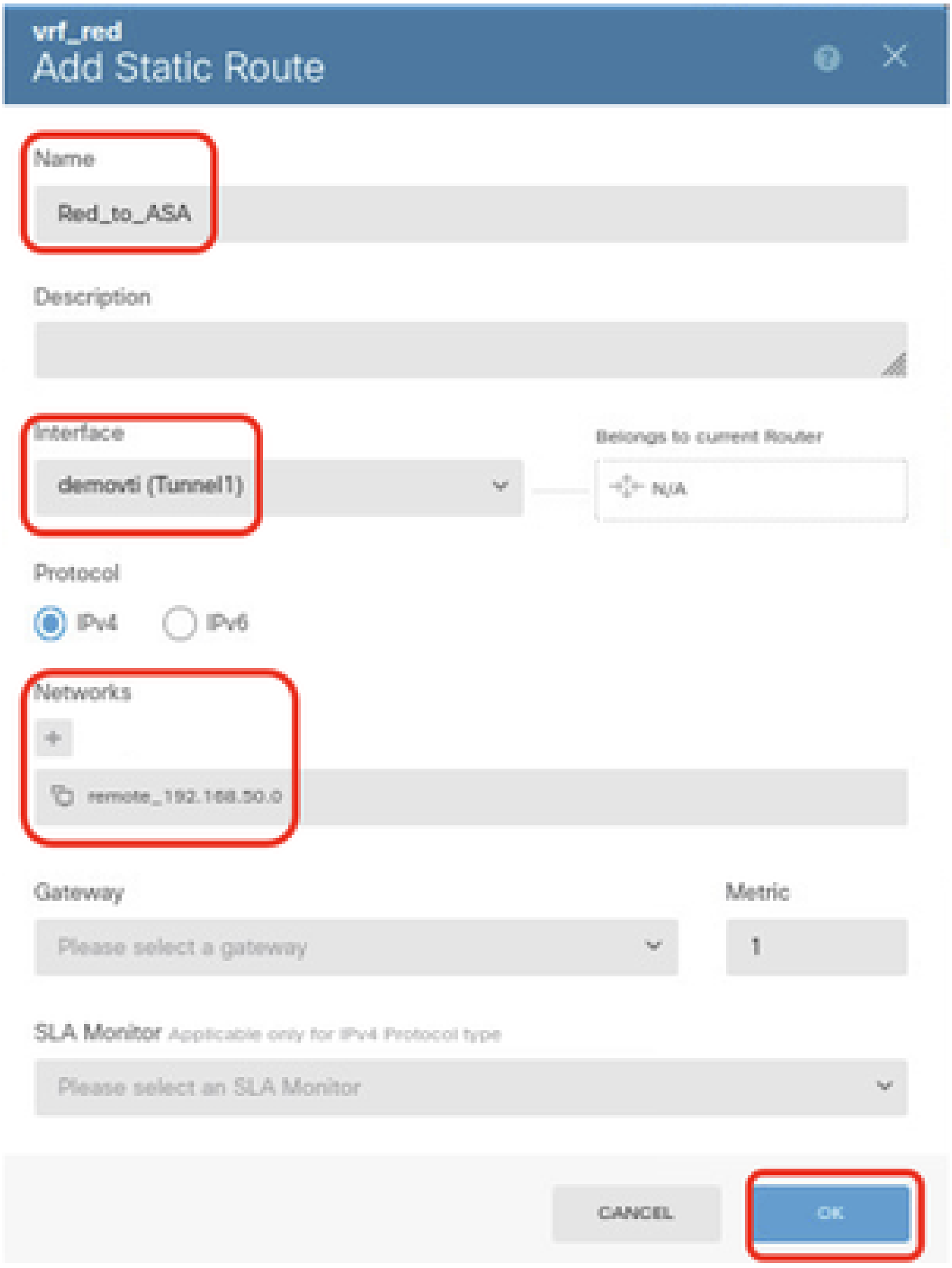
Etapa 6.1. Clique na guia Static Routing. Clique no botão +.




FTD_Create_Static_Route_VRF_Red

Etapa 6.2. Forneça as informações necessárias. Clique no botão OK.

- Nome: Vermelho_para_ASA
- Interface: demovti (Tunnel1)
- Redes: remote_192.168.50.0
- Gateway: Deixe este item em branco.

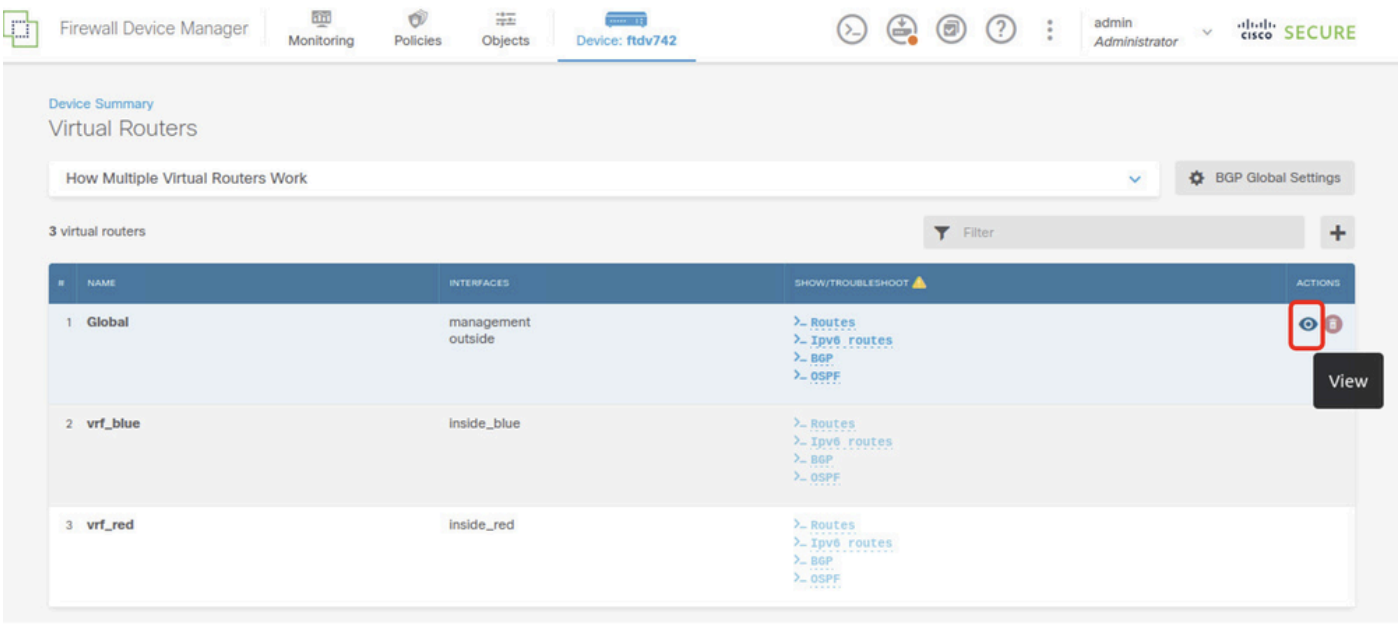



FTD_Create_Static_Route_VRF_Red_Details

Etapa 7. Criar vazamento de rota de roteadores globais para virtuais. As rotas permitem que os pontos finais protegidos pela extremidade remota da VPN site a site acessem a rede

192.168.10.0/24 no roteador virtual vrf_red e a rede 192.168.20.0/24 no roteador virtual vrf_blue.

Navegue até Device > Routing . Clique em View Configuration . clique no ícone View na célula Action do roteador virtual Global.



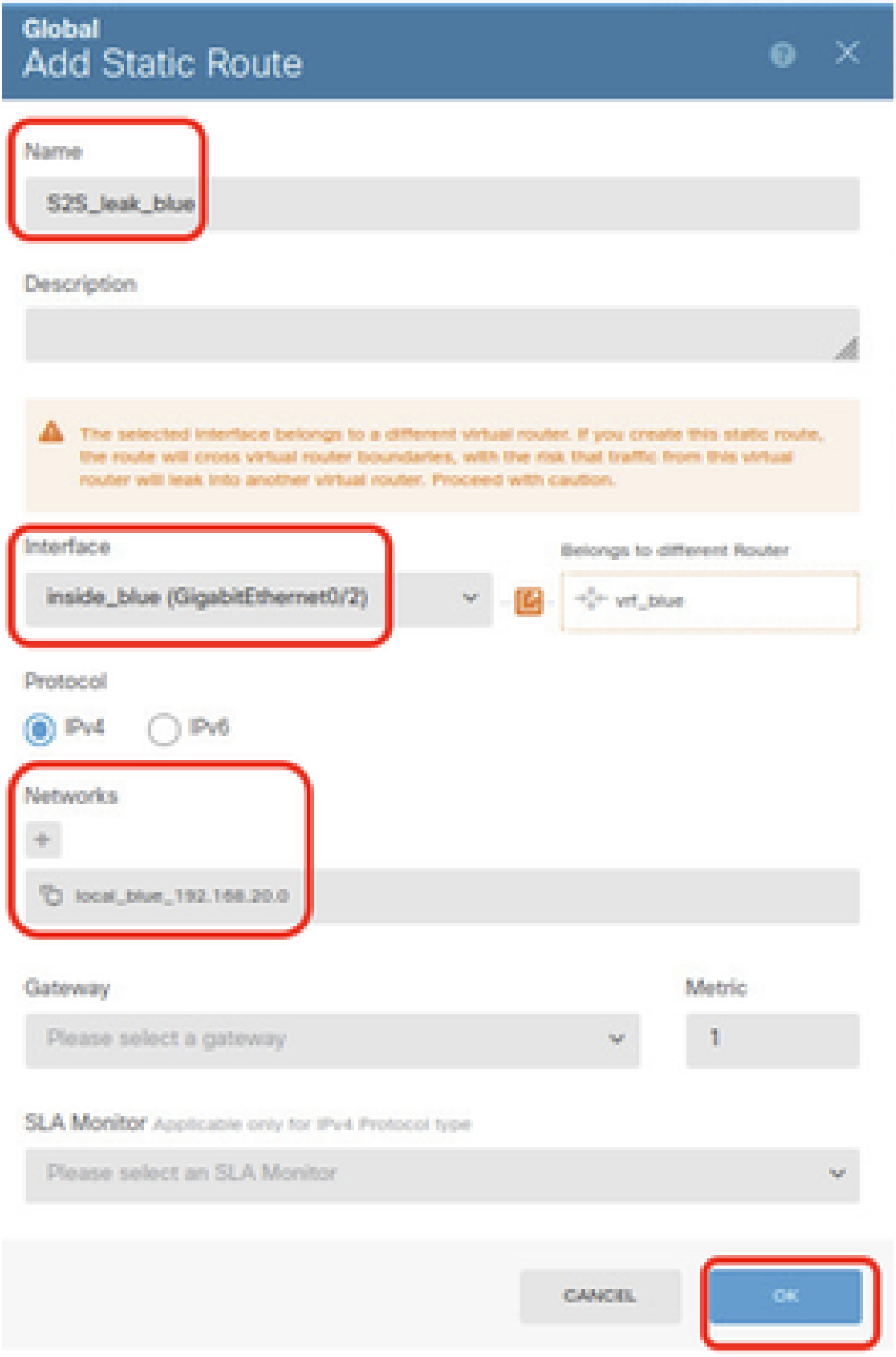

FTD_View_VRF_Global

Etapa 7.1. Clique na guia Static Routing. Clique no botão +.


FTD_Create_Static_Route_VRF_Global

Etapa 7.2. Forneça as informações necessárias. Clique no botão OK.

- Nome: S2S_leak_blue
- Interface: inside_blue (GigabitEthernet0/2)
- Redes: local_blue_192.168.20.0
- Gateway: Deixe este item em branco.


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
```

Etapa 10. Crie uma proposta ipsec IKEv2 que defina os mesmos parâmetros configurados no FTD.

```
<#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
```

Etapa 11. Criar um perfil IPSec, fazendo referência proposta de IPSec criada na Etapa 10.

```
<#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
```

Etapa 12. Criar uma política de grupo permitindo o protocolo IKEv2.

```
<#root>

group-policy

demo_gp_192.168.30.1

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

Etapa 13. Crie um grupo de túneis para o endereço IP externo FTD do peer, fazendo referência à

política de grupo criada na Etapa 12 e configurando a mesma chave pré-compartilhada com FTD(criado na Etapa 3.7).

<#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 *****
```

Etapa 14. Ativar o IKEv2 na interface externa.

```
crypto ikev2 enable outside
```

Etapa 15. Criar túnel virtual.

<#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**

Etapa 16. Criar uma rota estática.

```
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
```

# Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Etapa 1. Navegue até o CLI do FTD e do ASA através do console ou do SSH para verificar o status da VPN da fase 1 e da fase 2 através dos comandos show crypto ikev2 sa e show crypto ipsec sa .

DTF:

```
> 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
```

## Etapa 2. Verificar a rota de VRF e Global no FTD.

```
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
```

Etapa 3. Verificar o teste de ping.

Antes do ping, verifique os contadores de show crypto ipsec sa | inc interface:|encap|decap no FTD.

Neste exemplo, Tunnel1 mostra 30 pacotes para encapsulamento e desencapsulamento.

```
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#
```

Cliente1 efetuou ping no Cliente3 com êxito.

```
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 efetua ping de Client3 com êxito.

```
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
```

Verifique os contadores de  show crypto ipsec sa | inc interface:|encap|decap  no FTD após o ping com êxito.

Neste exemplo, Tunnel1 mostra 40 pacotes para encapsulamento e desencapsulamento após um ping bem-sucedido. Além disso, ambos os contadores aumentaram em 10 pacotes, correspondendo às 10 solicitações de eco de ping, indicando que o tráfego de ping passou com êxito pelo túnel IPSec.

```
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
```

# Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

Você pode usar esses comandos de depuração para solucionar problemas da seção VPN.

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

Você pode usar esses comandos de depuração para solucionar problemas da seção de rota.

```
debug ip routing
```

# Referência

Guia de configuração do gerenciador de dispositivos do Cisco Secure Firewall, versão 7.4

Guia de configuração de CLI de VPN do Cisco Secure Firewall ASA, 9.20

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.