Configurar VPN site a site dupla baseada em rota ativa com PBR no FTD gerenciado pelo FDM

Contents

Introdução

Este documento descreve como configurar a VPN site a site baseada em rota dupla ativa com PBR no FTD gerenciado pelo FDM.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Entendimento básico de VPN
- Compreensão básica do Roteamento Baseado em Políticas (PBR - Policy Based Routing)
- Entendimento básico do Contrato de nível de serviço de protocolo Internet (IP SLA)
- 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

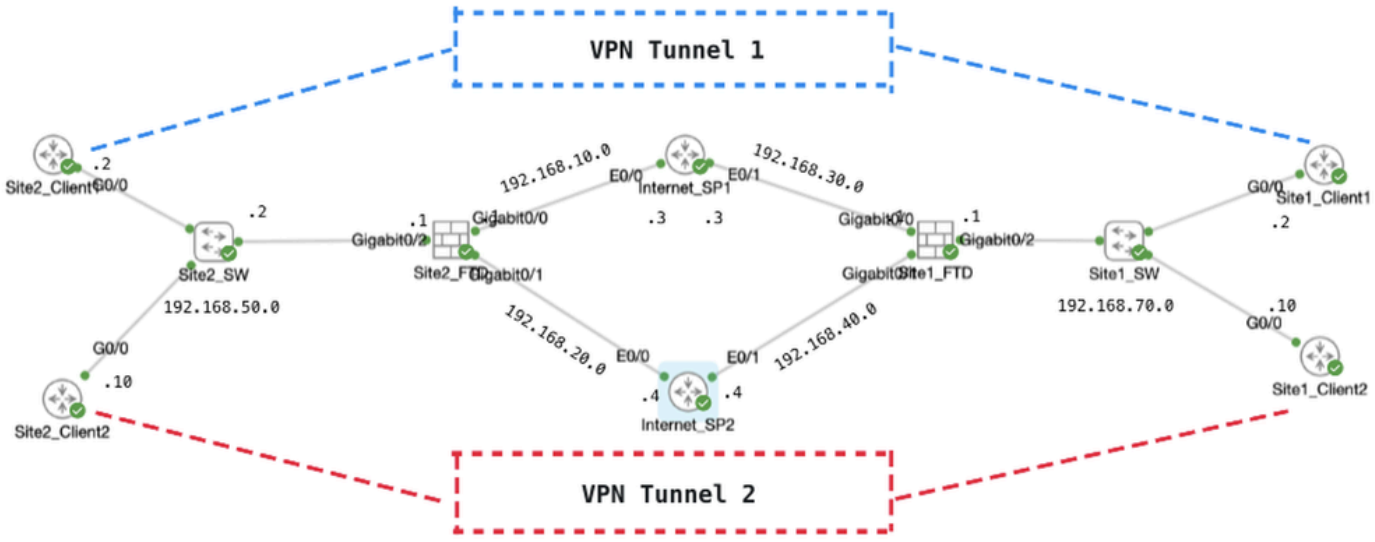
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

Informações de Apoio

Este documento explica como configurar uma VPN site a site baseada em rota dupla ativa no FTD. Neste exemplo, os FTDs no Site1 e no Site2 têm conexões ISP ativas duplas que estabelecem a VPN site a site com ambos os ISPs simultaneamente. Por padrão, o tráfego VPN atravessa o túnel 1 sobre ISP1 (linha azul). Para hosts específicos, o tráfego passa pelo túnel 2 pelo ISP2 (linha vermelha). Se o ISP1 sofrer uma interrupção, o tráfego muda para o ISP2 como backup. Por outro lado, se o ISP2 sofrer uma interrupção, o tráfego muda para o ISP1 como backup. O Roteamento Baseado em Políticas (PBR - Policy-Based Routing) e o Contrato de Nível de Serviço de Protocolo Internet (IP SLA - Internet Protocol Service Level Agreement) são utilizados neste exemplo para atender a esses requisitos.

Configurar

Diagrama de Rede



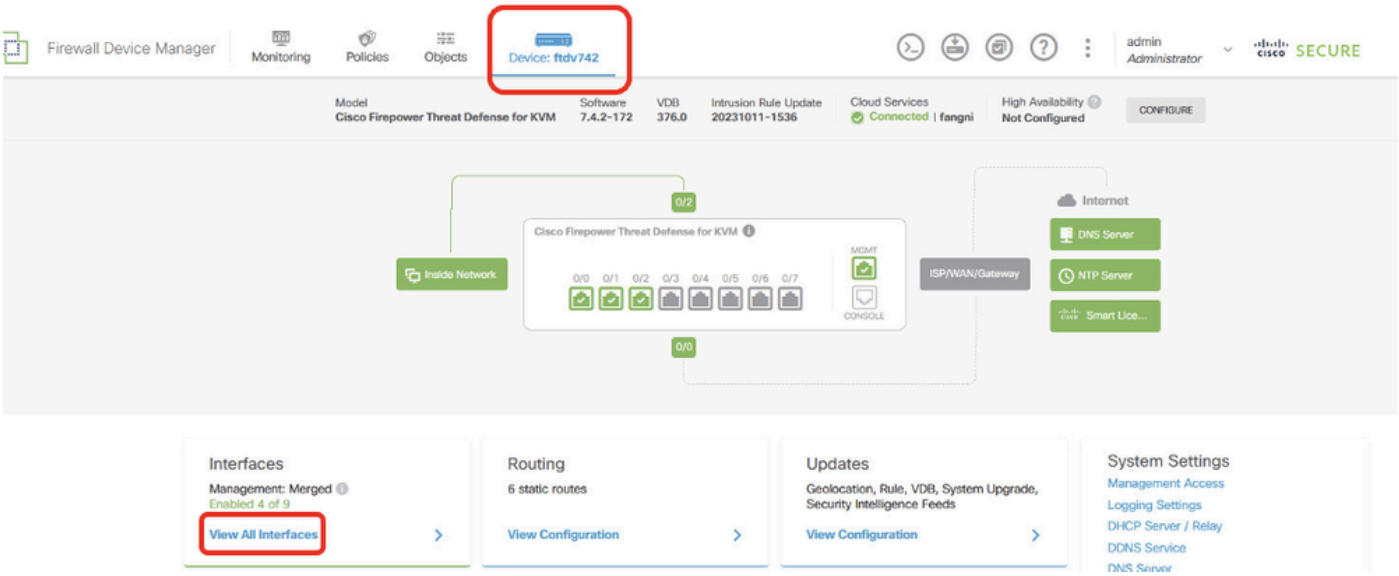
Topologia

Configurações em VPN

É essencial garantir que a configuração preliminar da interconectividade IP entre os nós tenha sido devidamente concluída. Os clientes no Site1 e no Site2 estão com o endereço IP interno FTD como gateway.

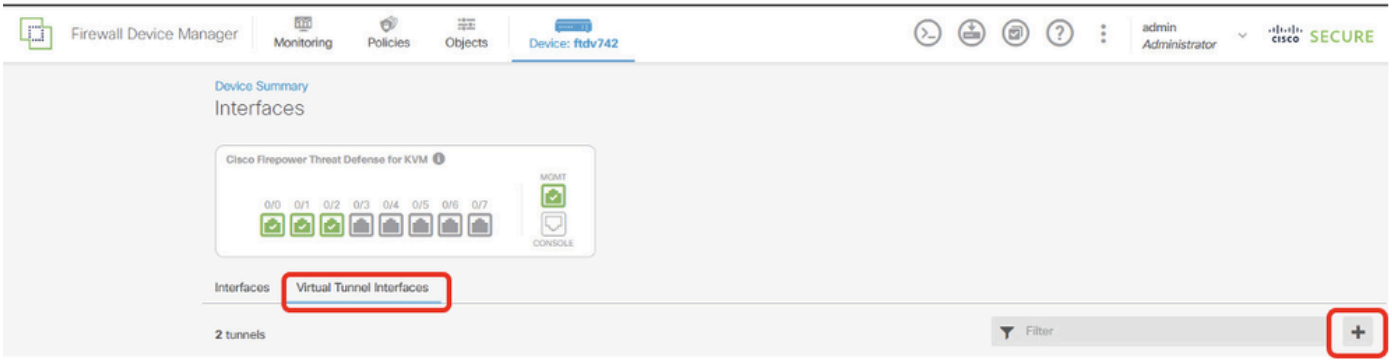
Configuração de VPN FTD do Site1

Etapa 1. Crie interfaces de túnel virtual para ISP1 e ISP2. Faça login na GUI do FDM do Site1 FTD. Navegue até Device > Interfaces. Clique em View All Interfaces.



Site1FTD_View_All_Interfaces

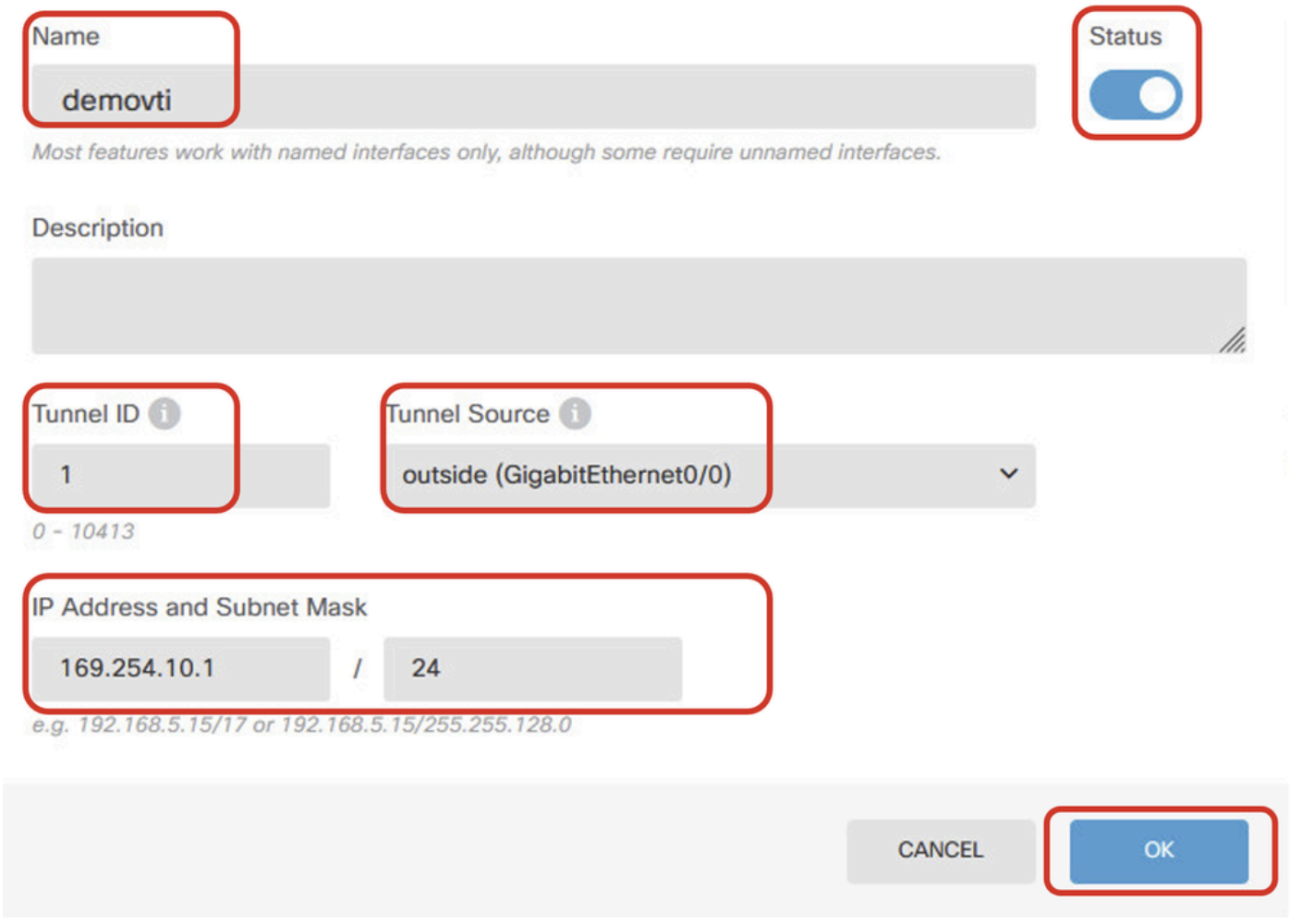
Etapa 2. Clique na guia Virtual Tunnel Interfaces e no botão +.



Site1FTD_Create_VTI

Etapa 3. Fornecer as informações necessárias dos detalhes do VTI. Clique no botão OK.

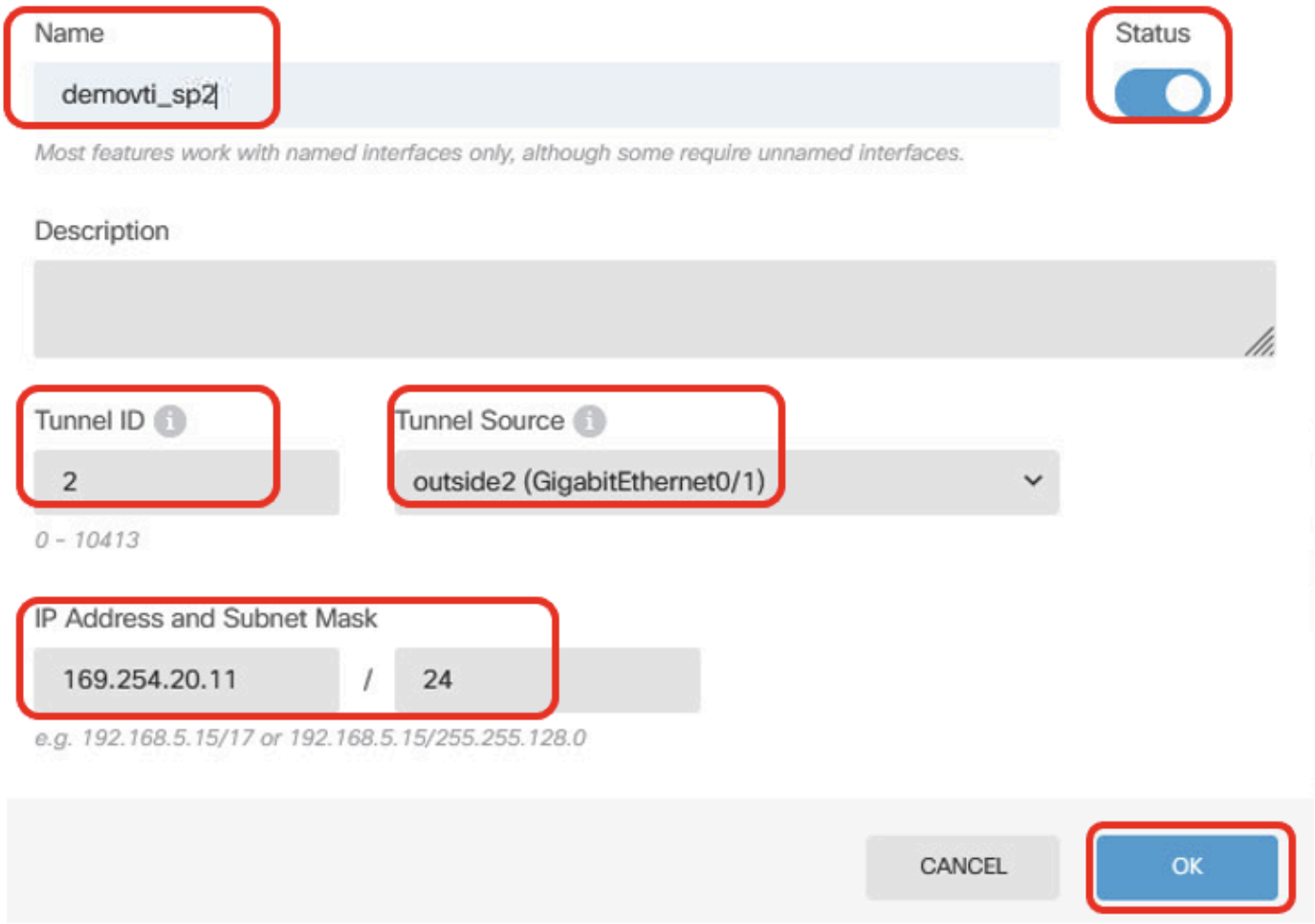
- Nome: demovti
- ID do túnel: 1
- Origem do túnel: externo (GigabitEthernet0/0)
- Endereço IP e máscara de sub-rede: 169.254.10.1/24
- Status: clique no controle deslizante para a posição Habilitado



Site1FTD_VTI_Details_Tunnel1_ISP1

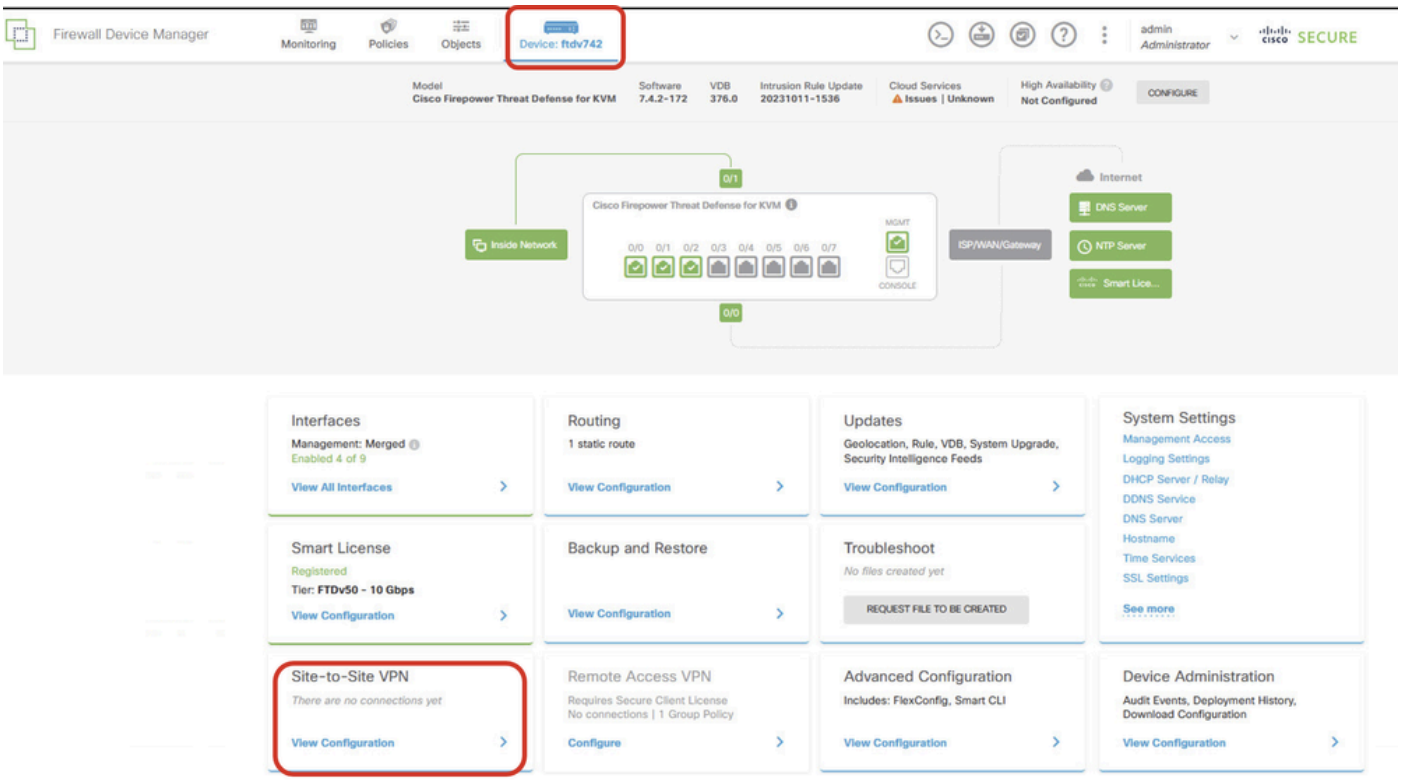
- Nome: demovti_sp2
- ID do túnel: 2

- Origem do túnel: outside2 (GigabitEthernet0/1)
- Endereço IP e máscara de sub-rede: 169.254.20.11/24
- Status: clique no controle deslizante para a posição Habilitado



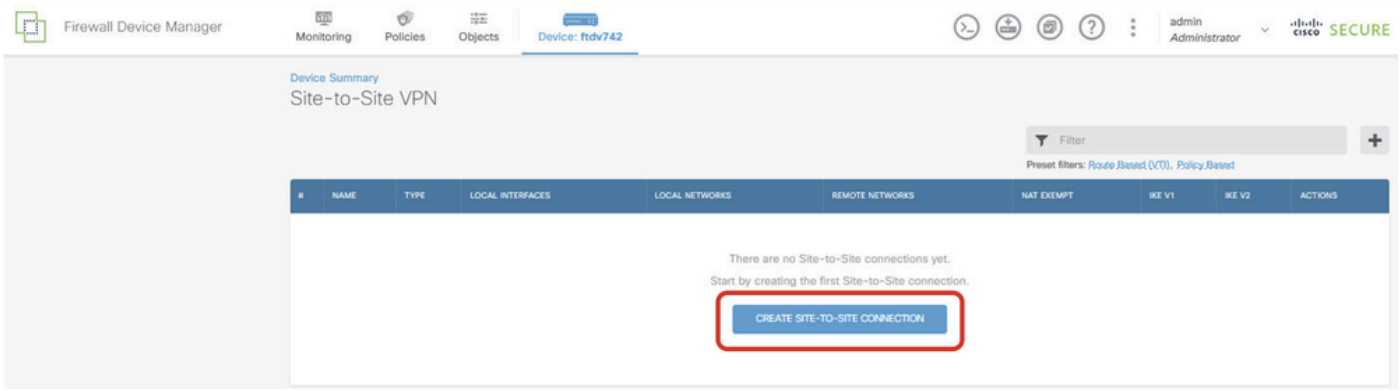
Site1FTD_VTI_Details_Tunnel2_ISP2

Etapa 4. Navegue até Device > Site-to-Site VPN. Clique no botão View Configuration.



Site1FTD_View_Site2Site_VPN

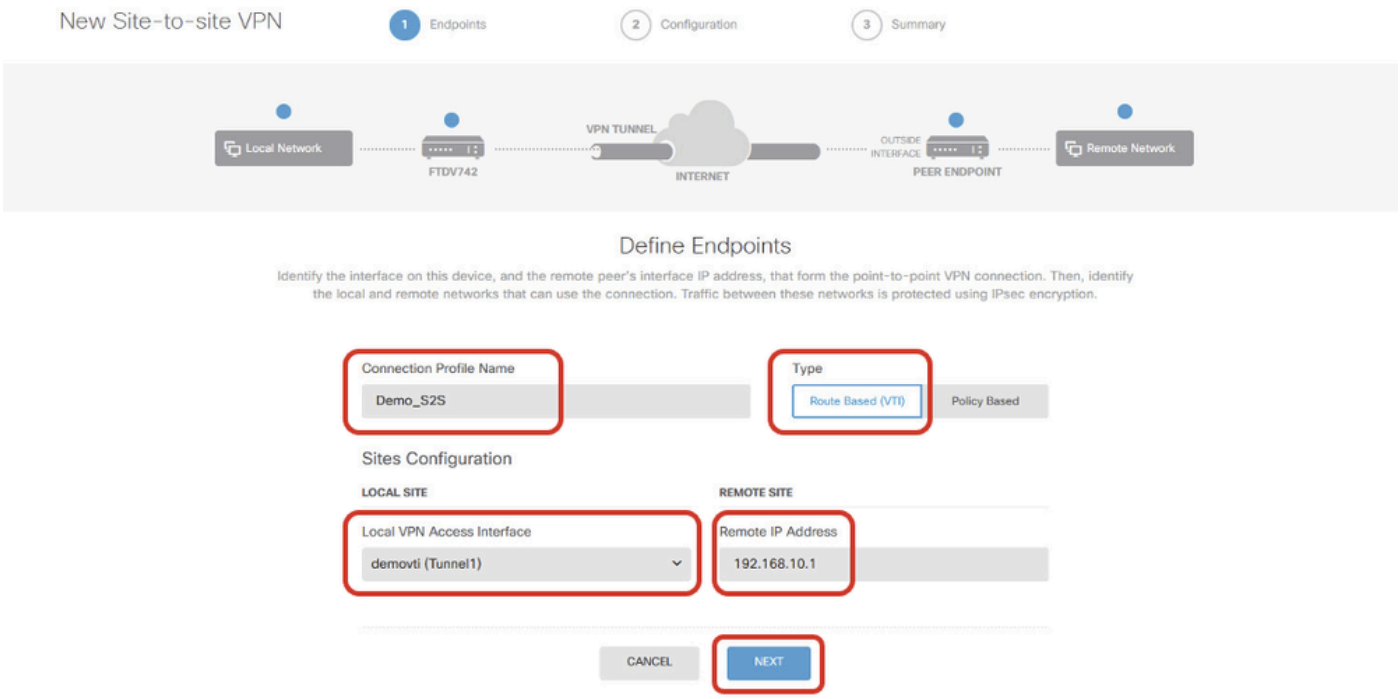
Etapa 5. Comece a criar uma nova VPN site a site através do ISP1. Clique no botão CREATE SITE-TO-SITE CONNECTION ou clique no botão +.



Site1FTD_Create_Site-to-Site_Connection

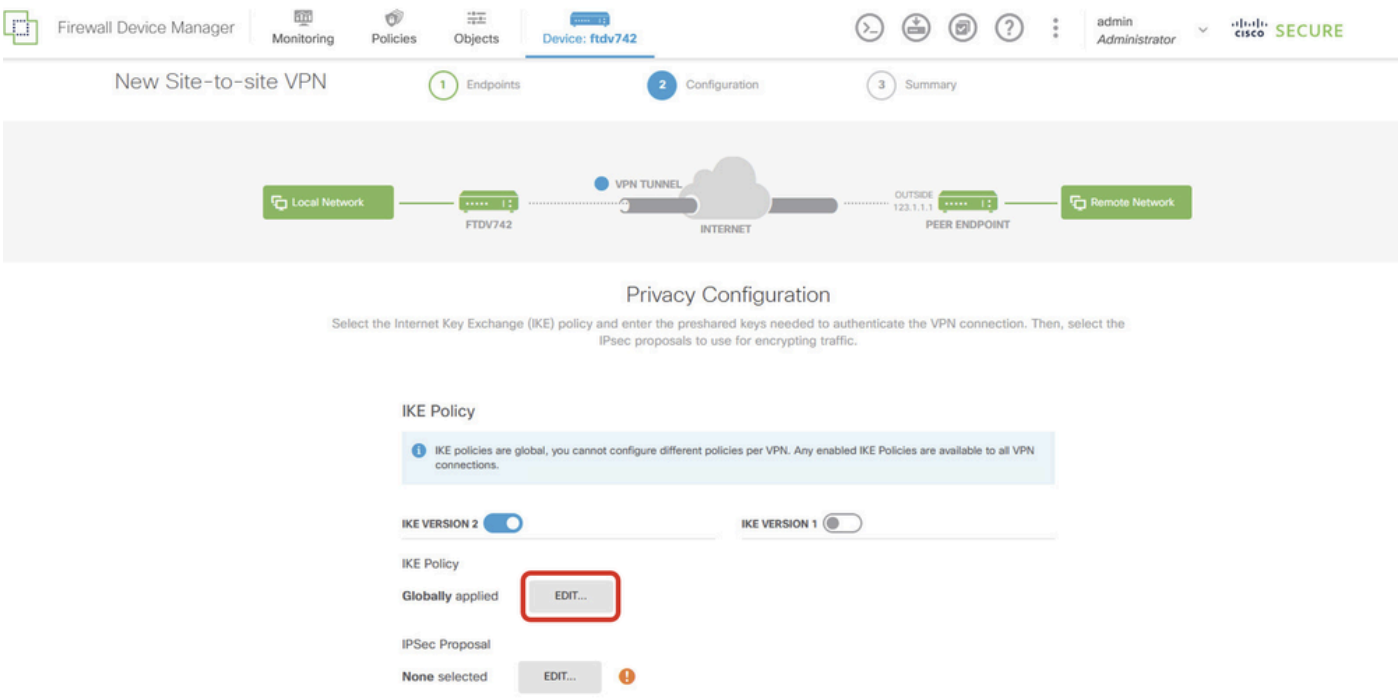
Etapa 5.1. Forneça as informações necessárias sobre Endpoints. Clique no botão AVANÇAR.

- Nome do perfil de conexão: Demo_S2S
- Digite: Baseado em Rota (VTI)
- Local VPN Access Interface: demovti (criado na Etapa 3.)
- Endereço IP remoto: 192.168.10.1 (este é o endereço IP do FTD do Site2 ISP1)



Site1FTD_ISP1_Site-to-Site_VPN_Define_Endpoints

Etapa 5.2. Navegue até Política IKE. Clique no botão EDITAR.

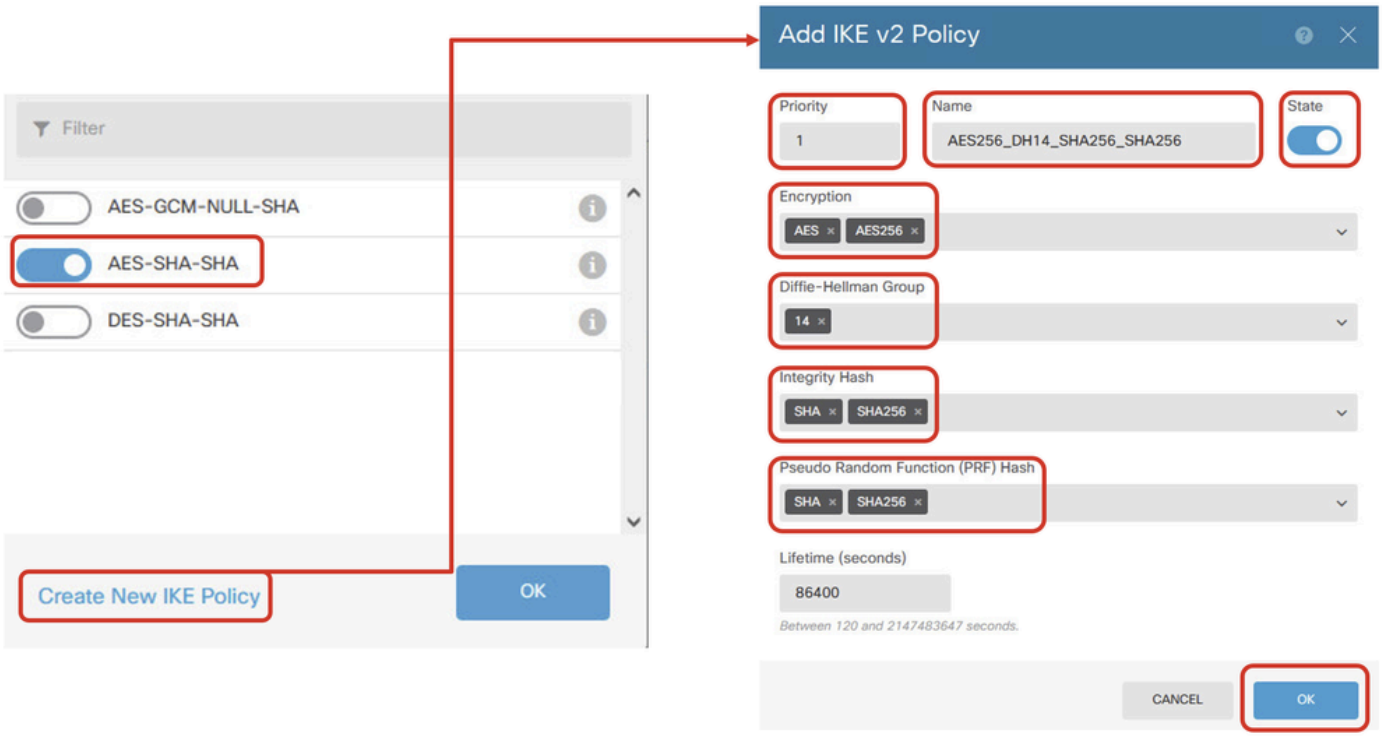


Site1FTD_Edit_IKE_Policy

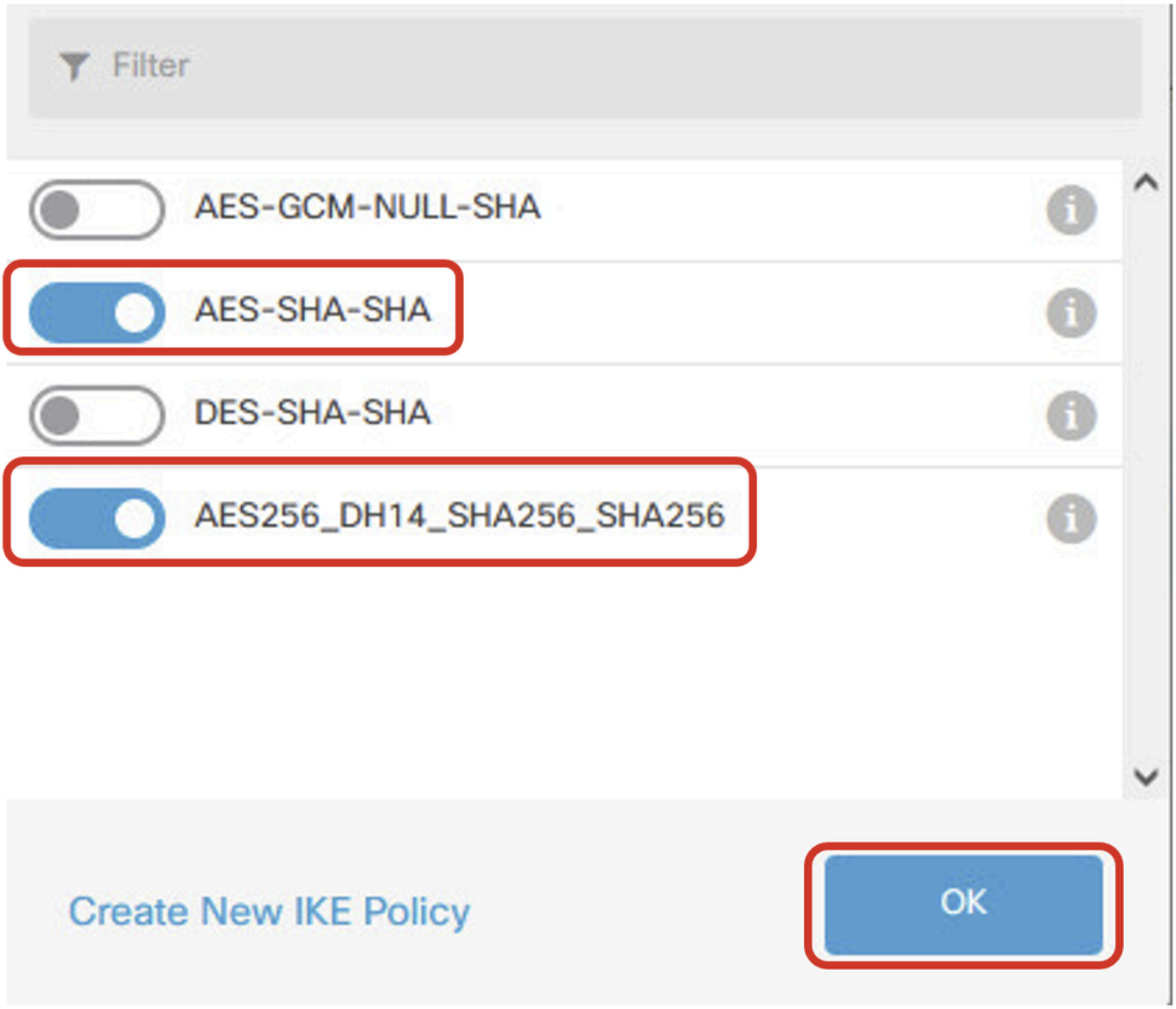
Etapa 5.3. Para a política IKE, você pode usar uma política predefinida ou pode criar uma nova clicando em Criar nova política IKE.

Neste exemplo, alterne uma política IKE existente AES-SHA-SHA e crie uma nova para fins de demonstração. Clique no botão OK para salvar.

- Nome: AES256_DH14_SHA256_SHA256
- Criptografia: AES, AES256
- Grupo DH: 14
- Hash de integridade: SHA, SHA256
- Hash PRF: SHA, SHA256
- Duração: 86400 (padrão)

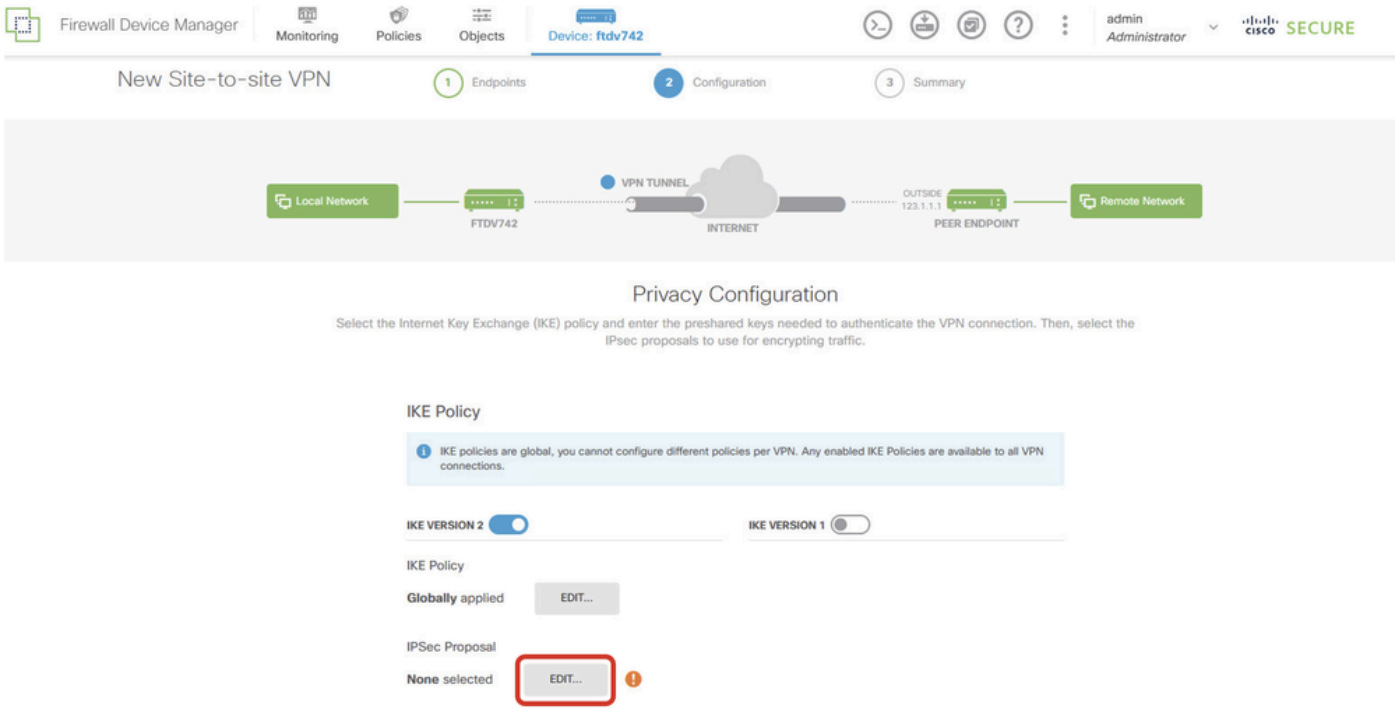


Site1FTD_Add_New_IKE_Policy



Site1FTD_Enable_New_IKE_Policy

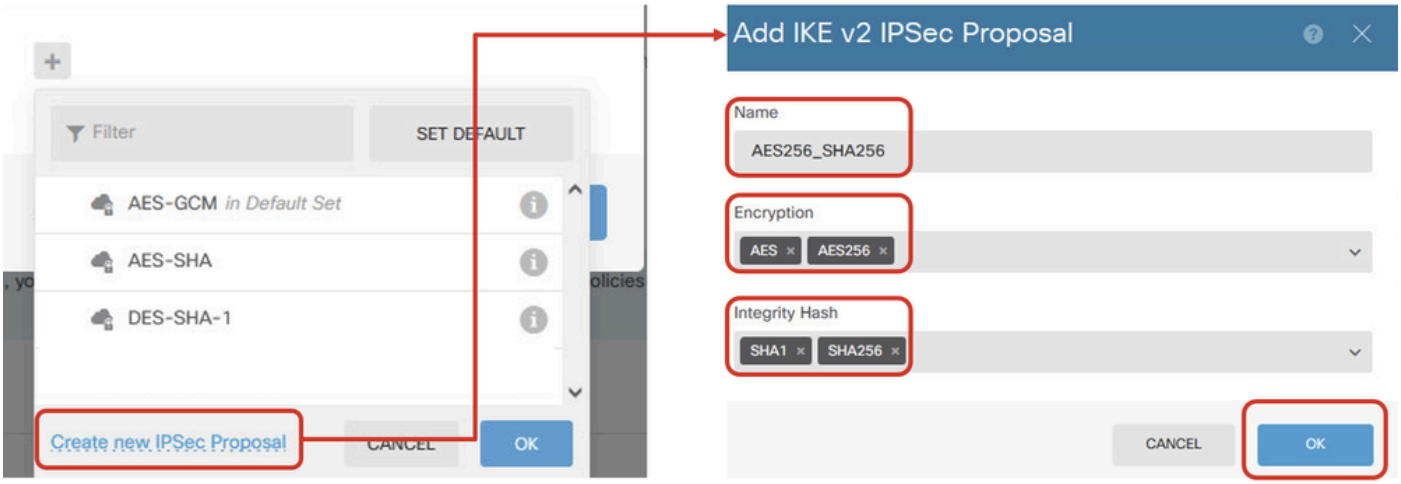
Etapa 5.4. Navegue até IPSec Proposal (Proposta IPSec). Clique no botão EDITAR.



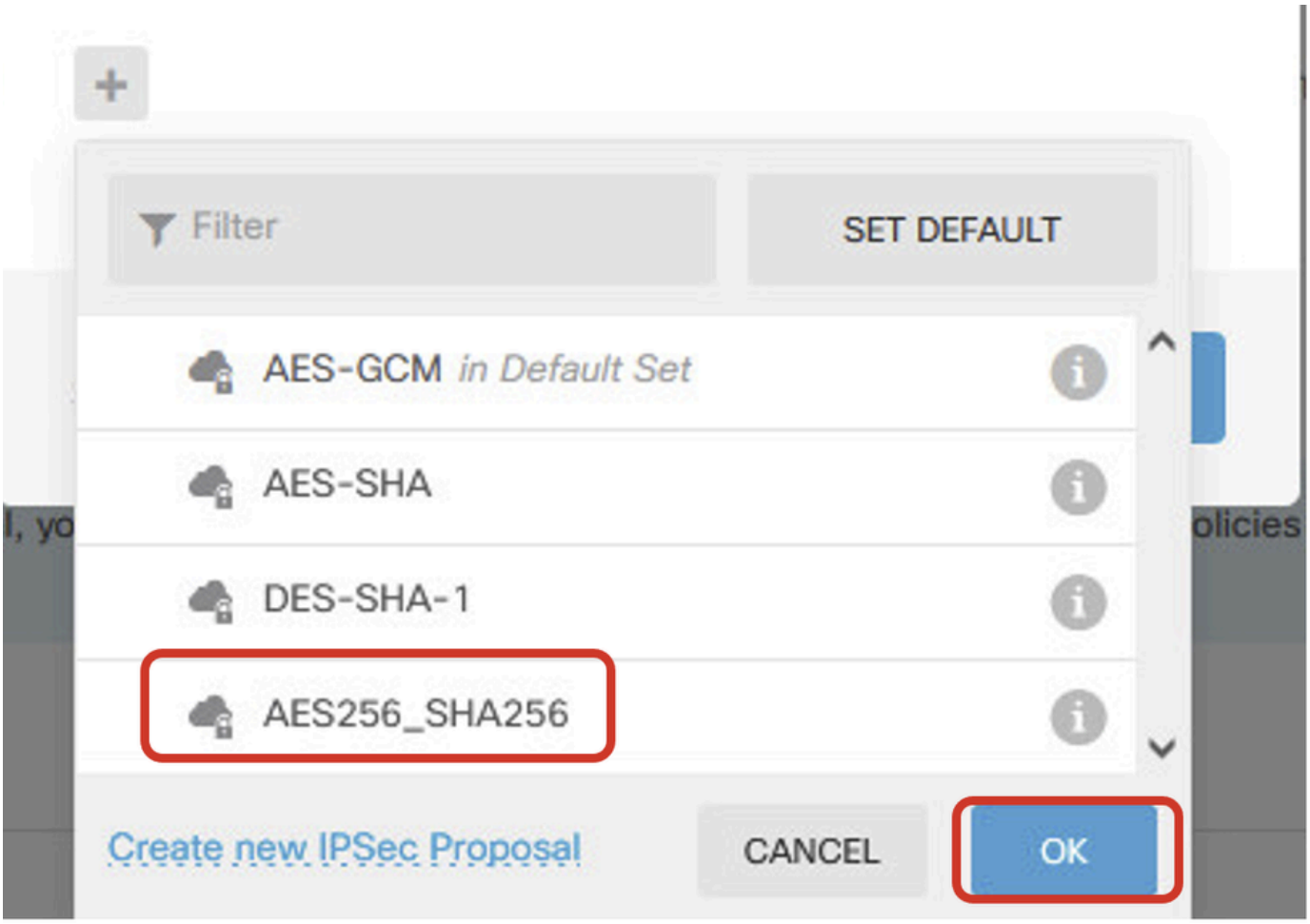
Site1FTD_Edit_IKE_Proposal

Etapa 5.5. Para uma proposta IPSec, você pode usar uma predefinida ou pode criar uma nova clicando em Criar nova proposta IPSec. Neste exemplo, crie um novo para fins de demonstração. Clique no botão OK para salvar.

- Nome: AES256_SHA256
- Criptografia: AES, AES256
- Hash de integridade: SHA1, SHA256



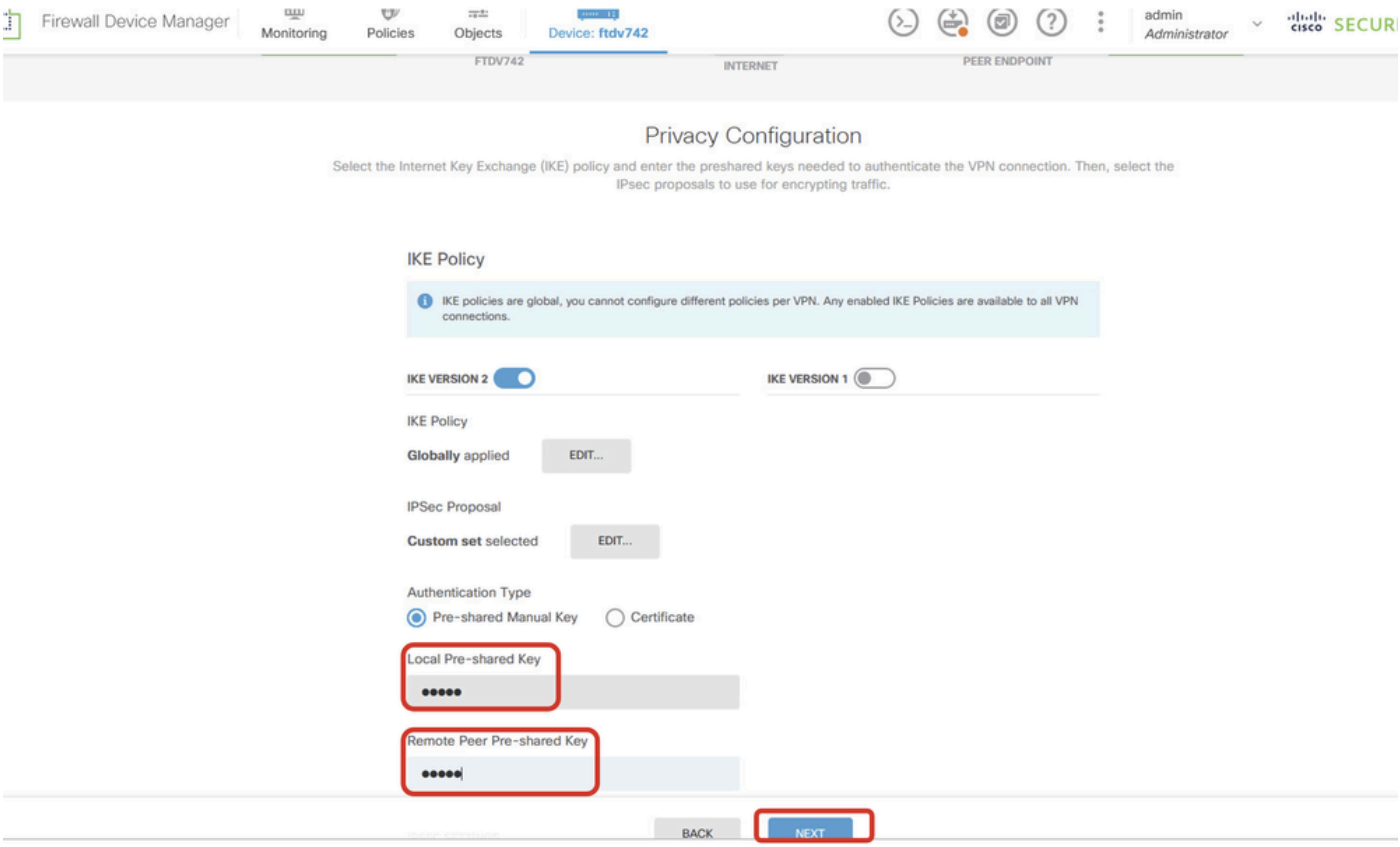
Site1FTD_Add_New_IKE_Proposal



Site1FTD_Enable_New_IKE_Proposal

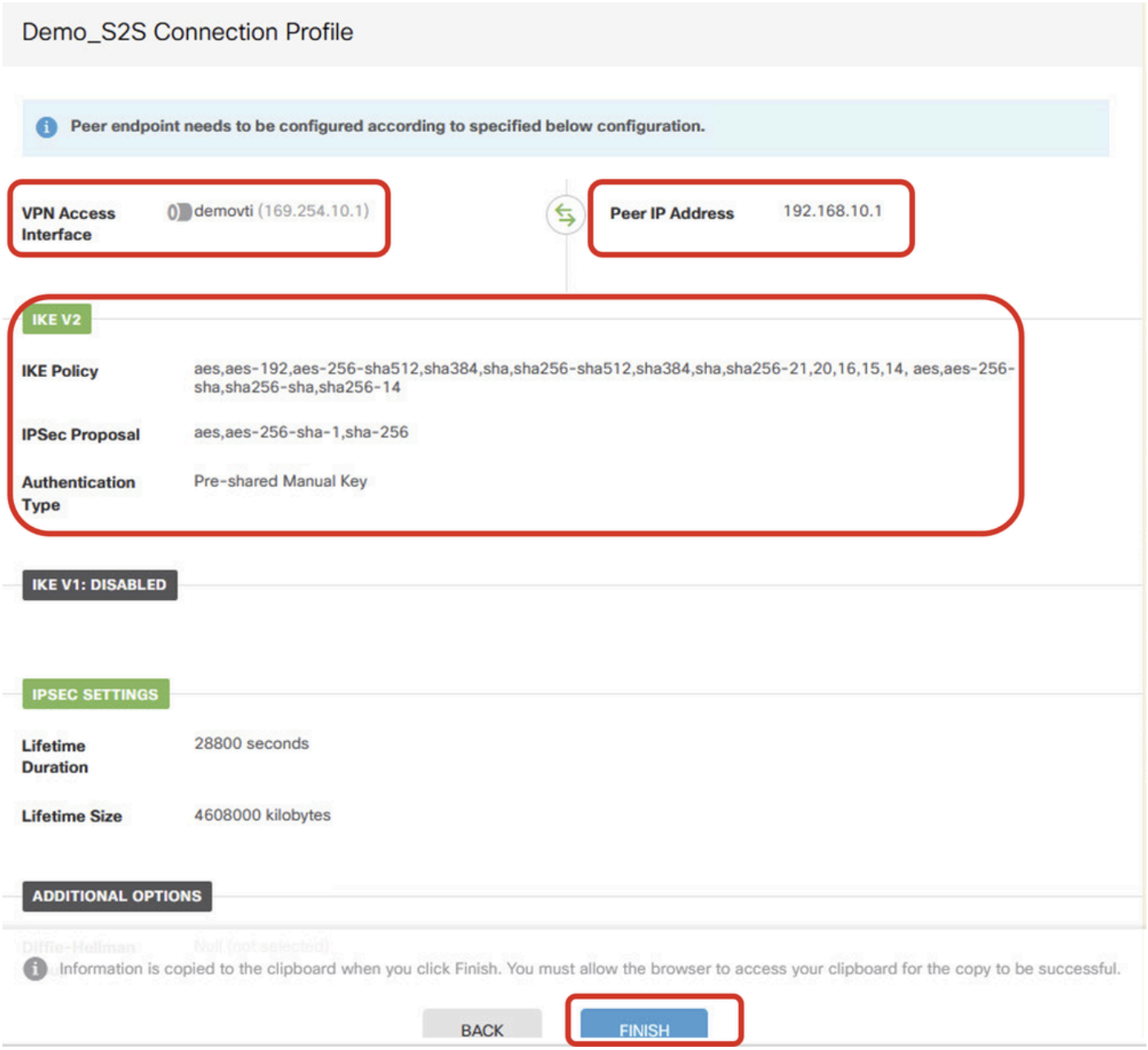
Etapa 5.6. Role a página para baixo e configure a chave pré-compartilhada. Clique no botão AVANÇAR.

Anote essa chave pré-compartilhada e configure-a posteriormente no Site2 FTD.



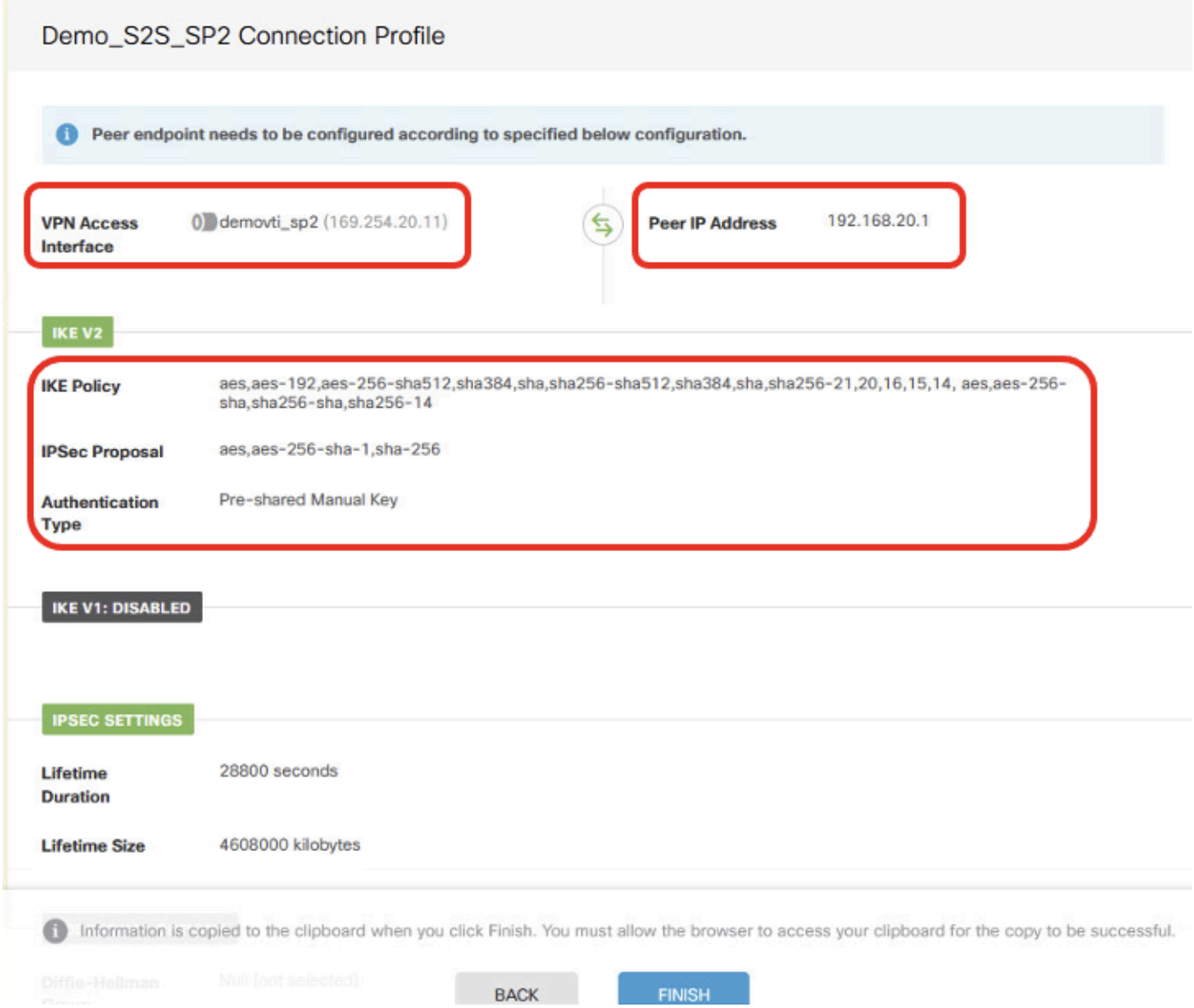
Site1FTD_Configure_Pre_Shared_Key

Etapa 5.7. Reveja a configuração da VPN. Se algo precisar ser modificado, clique no botão BACK. Se tudo estiver bem, clique no botão FINISH.



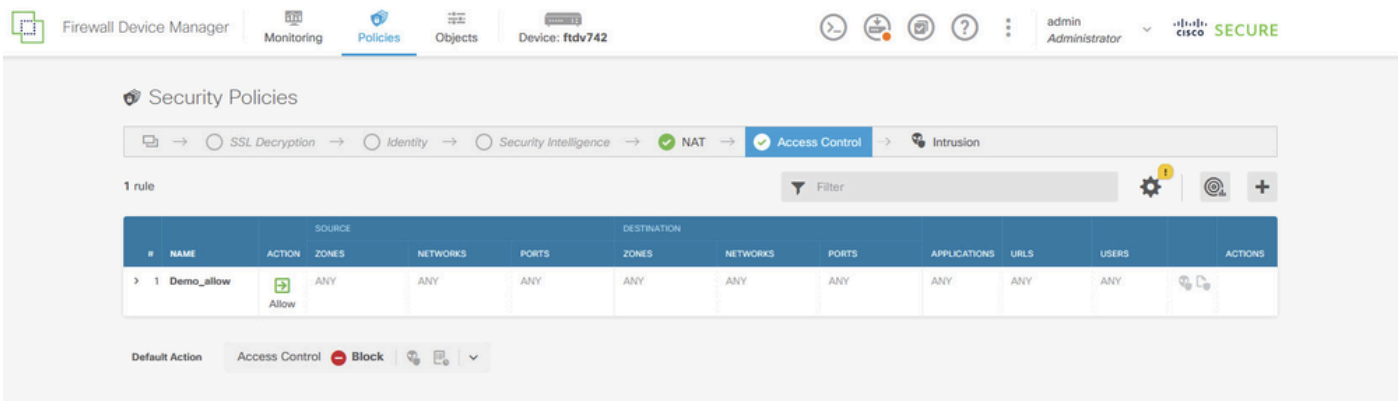
Site1FTD_ISP1_Review_VPN_Config_Summary

Etapa 6. Repita a Etapa 5. para criar uma nova VPN site a site através do ISP2.



Site1FTD_ISP2_Review_VPN_Config_Summary

Etapa 7. 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.



Site1FTD_Allow_Access_Control_Rule_Example

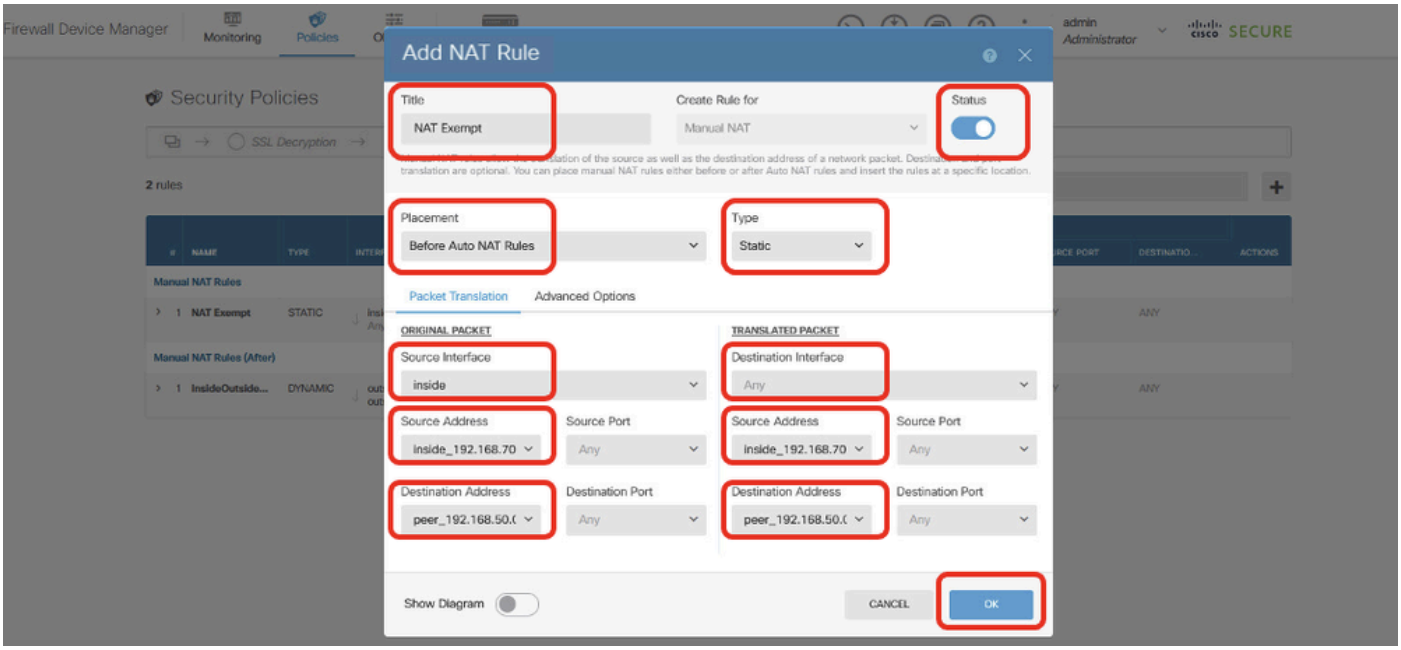
Etapa 8. (Opcional) Configure a regra de isenção de NAT para o tráfego do cliente no FTD se

houver NAT dinâmico configurado para o cliente para acessar a Internet.

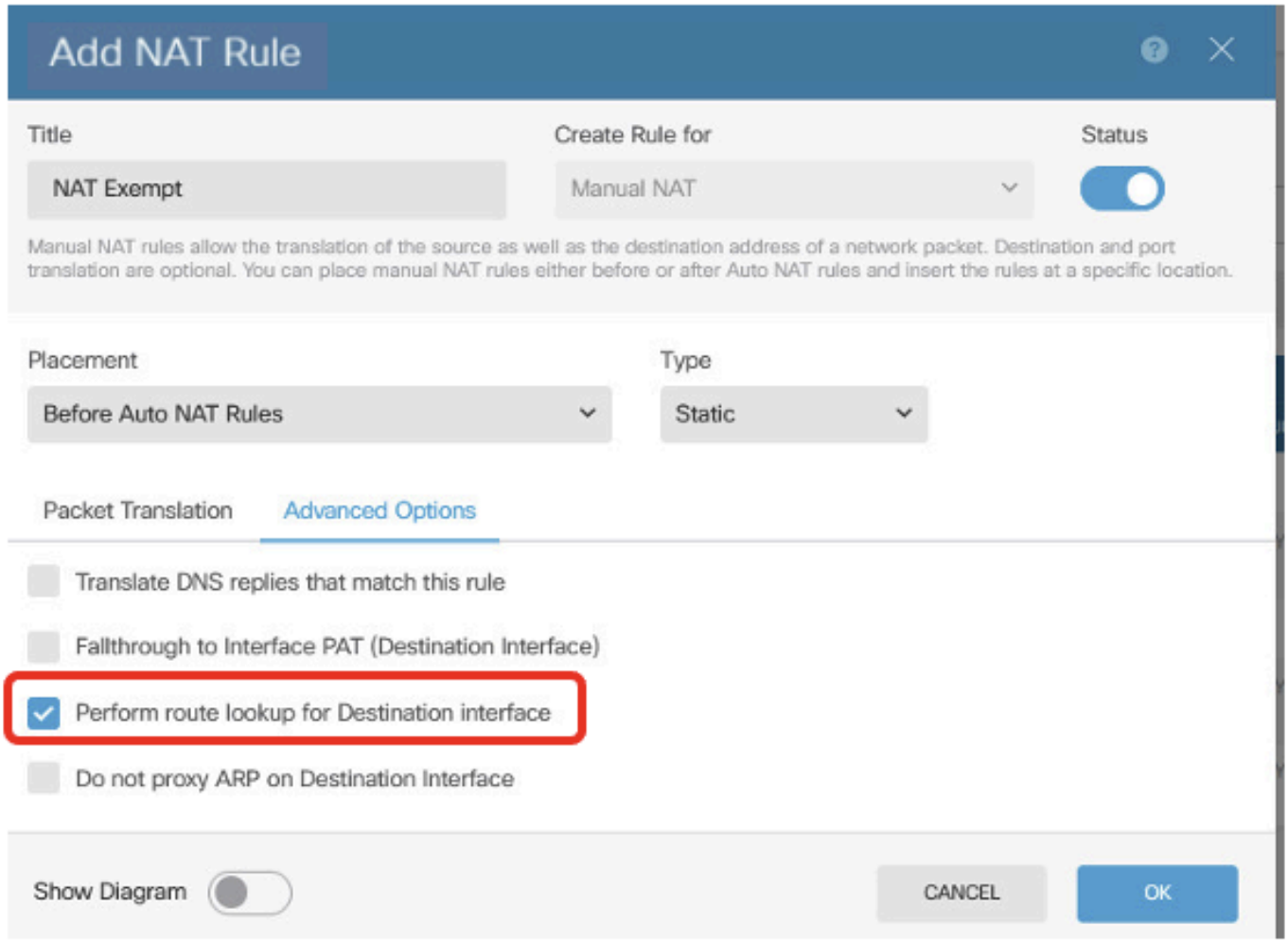
Para fins de demonstração, o NAT dinâmico é configurado para clientes para acessar a Internet neste exemplo. Portanto, a regra de isenção de NAT é necessária.

Navegue até Policies > NAT. Clique no botão +. Forneça os detalhes e clique em OK.

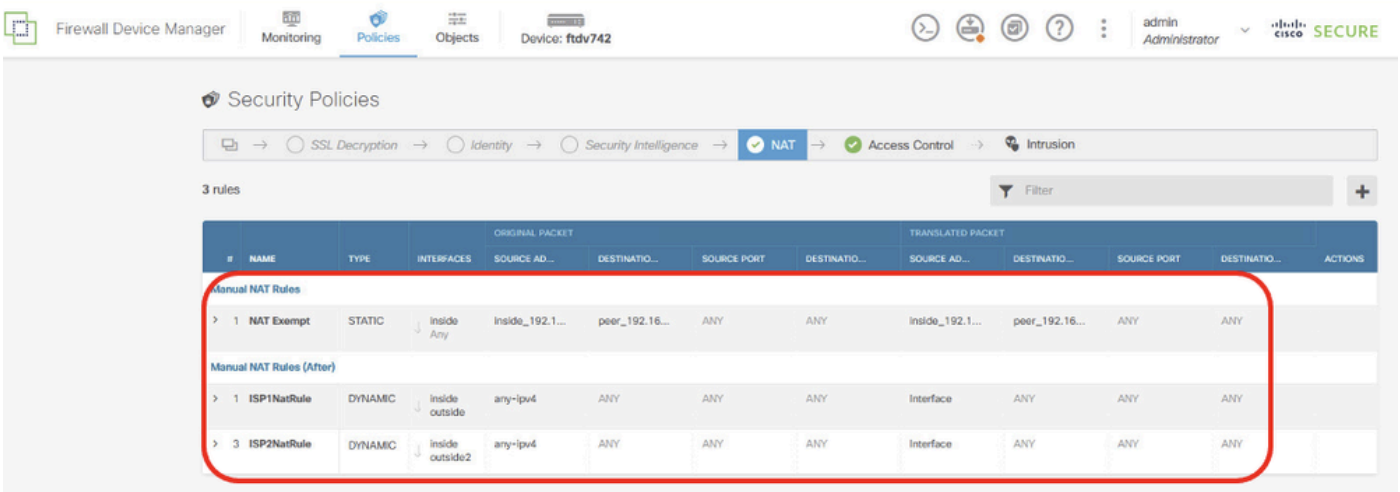
- Título: Isento de NAT
- Posicionamento: Antes das regras de NAT automático
- Digite: Estático
- Interface de origem: Interna
- Destino: qualquer um
- Endereço de origem original: 192.168.70.0/24
- Endereço de Origem Convertido: 192.168.70.0/24
- Endereço de destino original: 192.168.50.0/24
- Endereço de destino traduzido: 192.168.50.0/24
- Com pesquisa de rota ativada



Site1FTD_Nat_Exempt_Rule



Site1FTD_Nat_Exempt_Rule_2



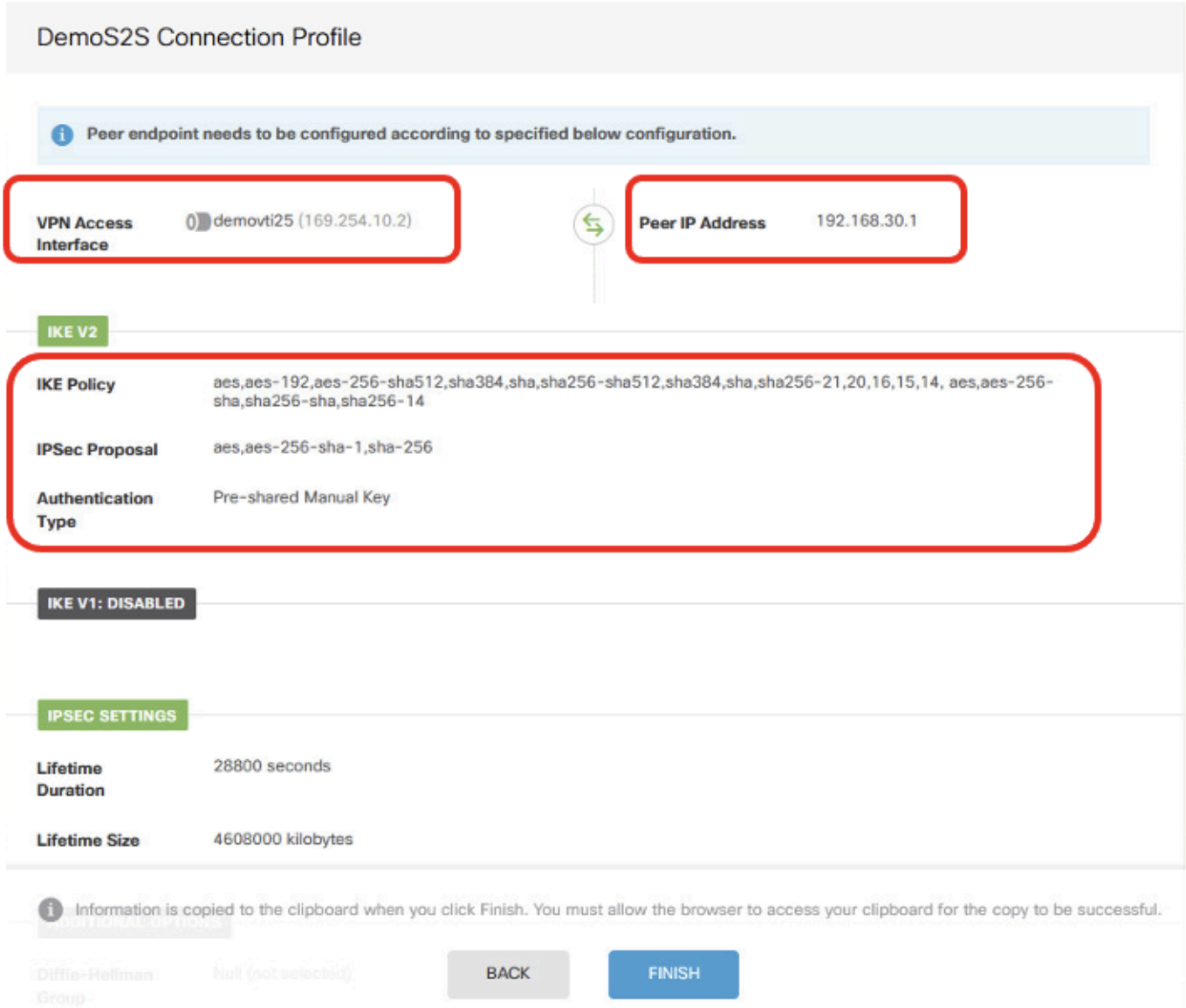
Site1FTD_Nat_Rule_Overview

Etapa 9. Implantar as alterações de configuração.

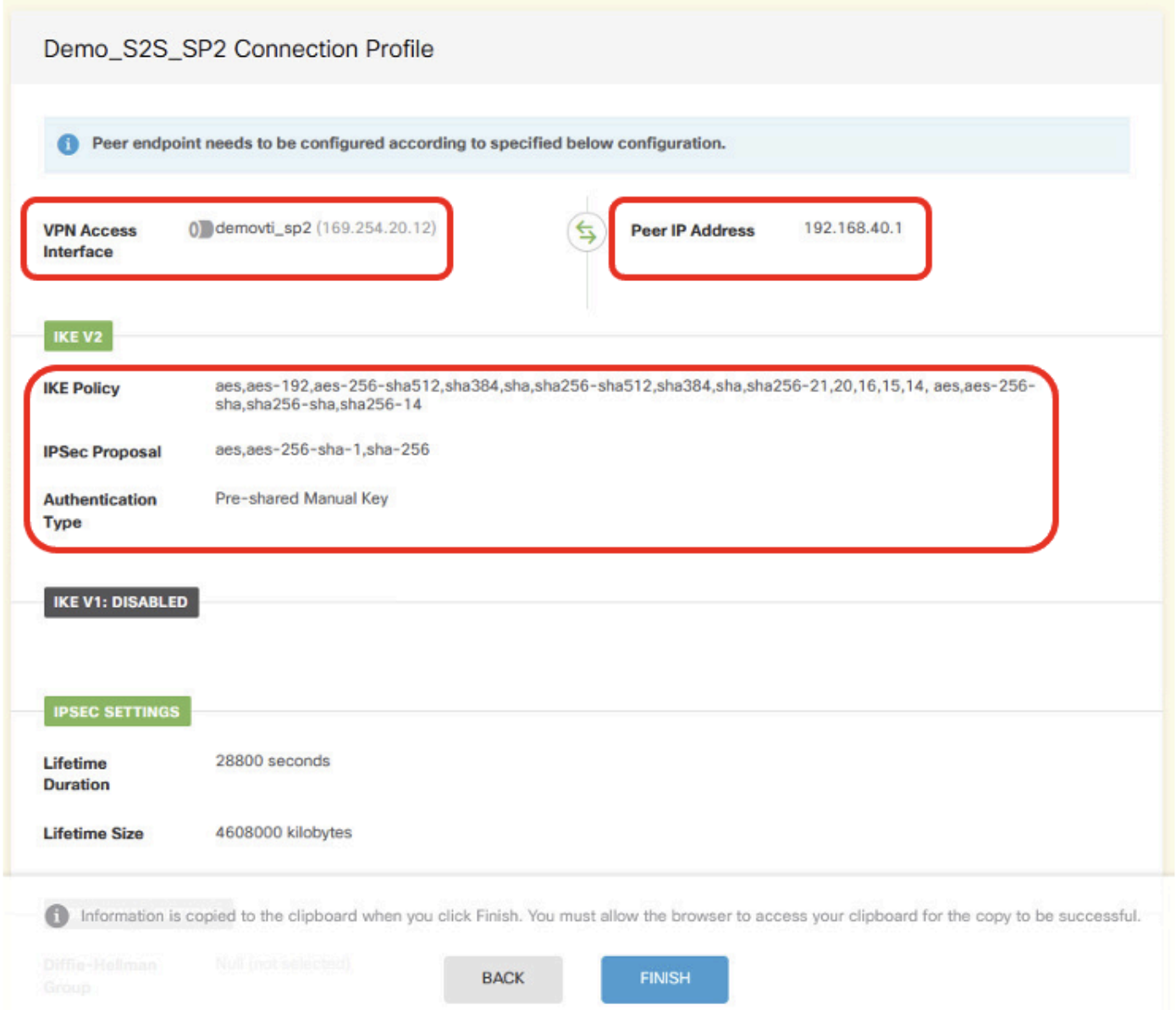
Site1FTD_Deployment_Changes

Configuração de VPN FTD do Site2

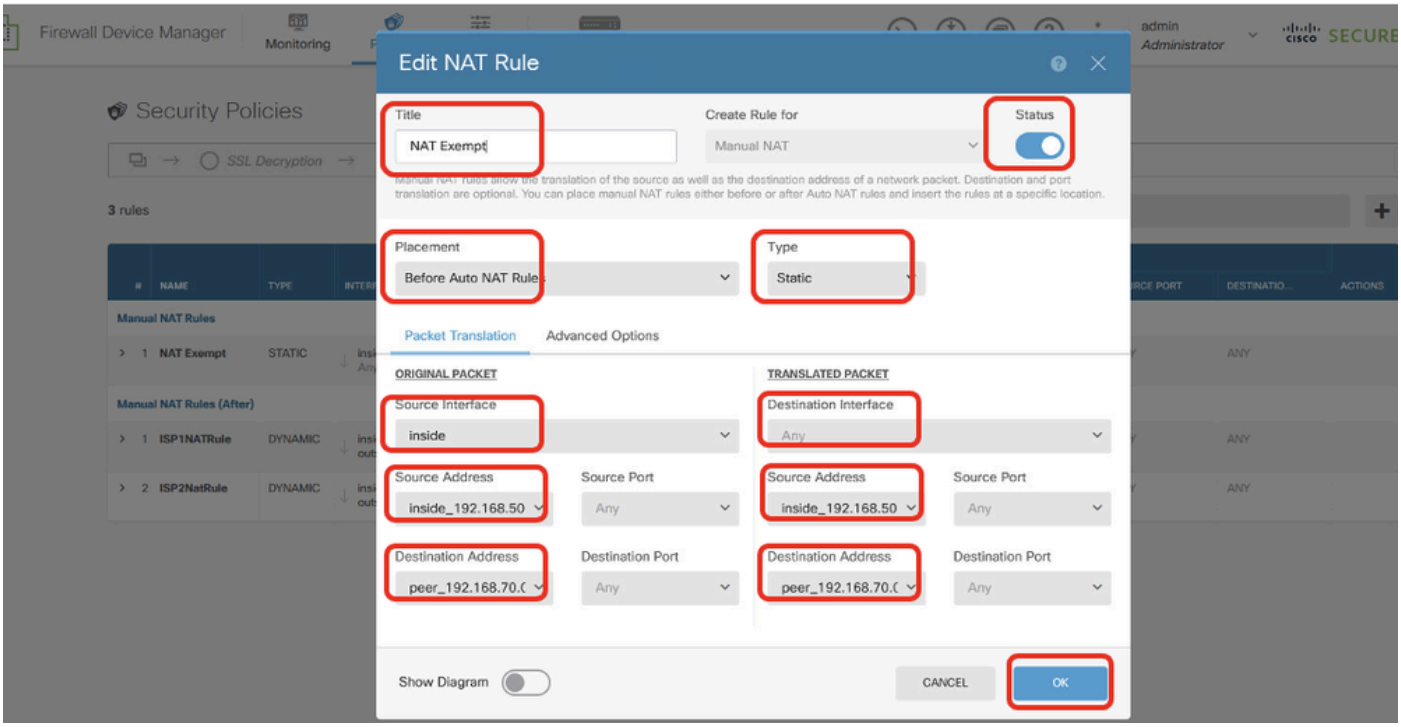
Etapa 10. Repita as Etapas 1 a 9 com os parâmetros correspondentes para o FTD do Site2.



Site2FTD_ISP1_Review_VPN_Config_Summary



Site2FTD_ISP2_Review_VPN_Config_Summary

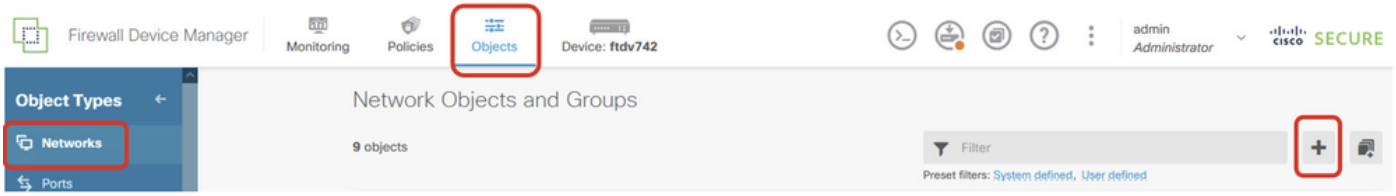


Site2FTD_Nat_Exempt_Rule

Configurações no PBR

Configuração do Site1 FTD PBR

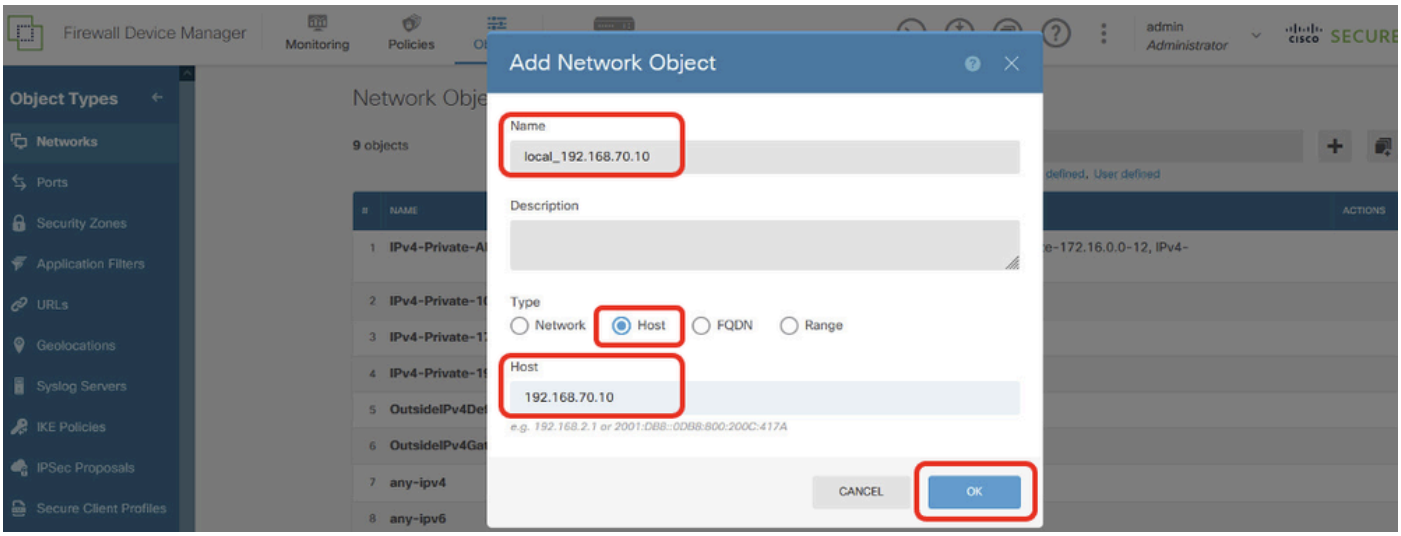
Etapa 11. Crie novos objetos de rede a serem usados pela lista de acesso do PBR para o FTD do Site1. Navegue até Objetos > Redes e clique no botão +.



Site1FTD_Create_Network_Object

Etapa 11.1. Crie o objeto do endereço IP do Site1 Client2. Forneça as informações necessárias. Clique na tecla OK.

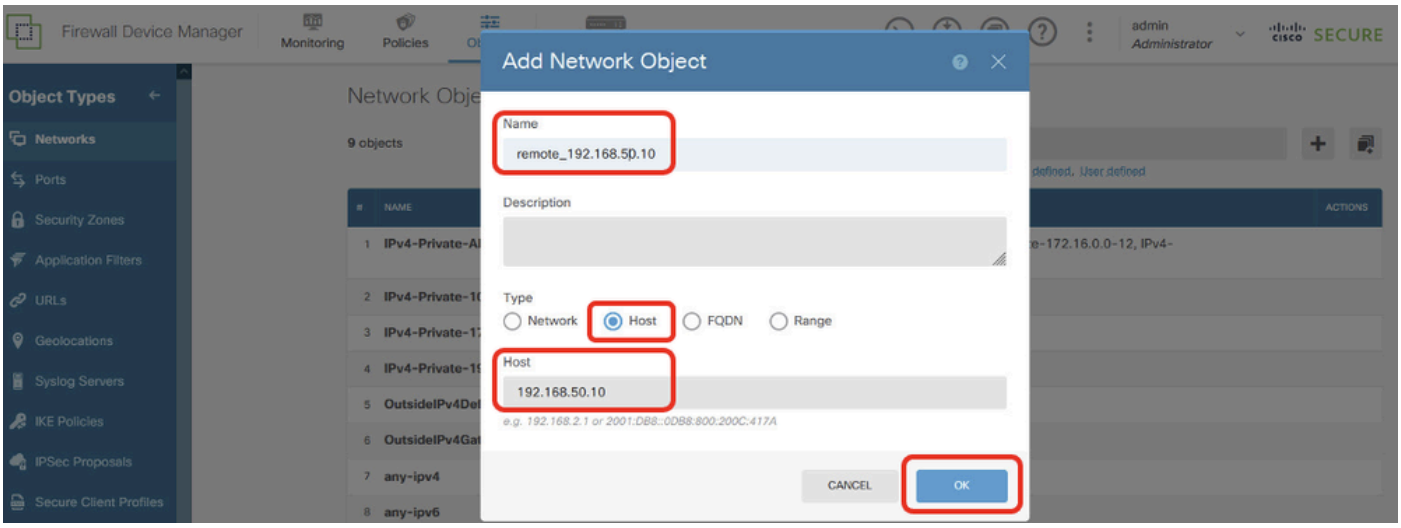
- Nome: local_192.168.70.10
- Digite: Host
- Host: 192.168.70.10



Site1FTD_Site1FTD_PBR_LocalObject

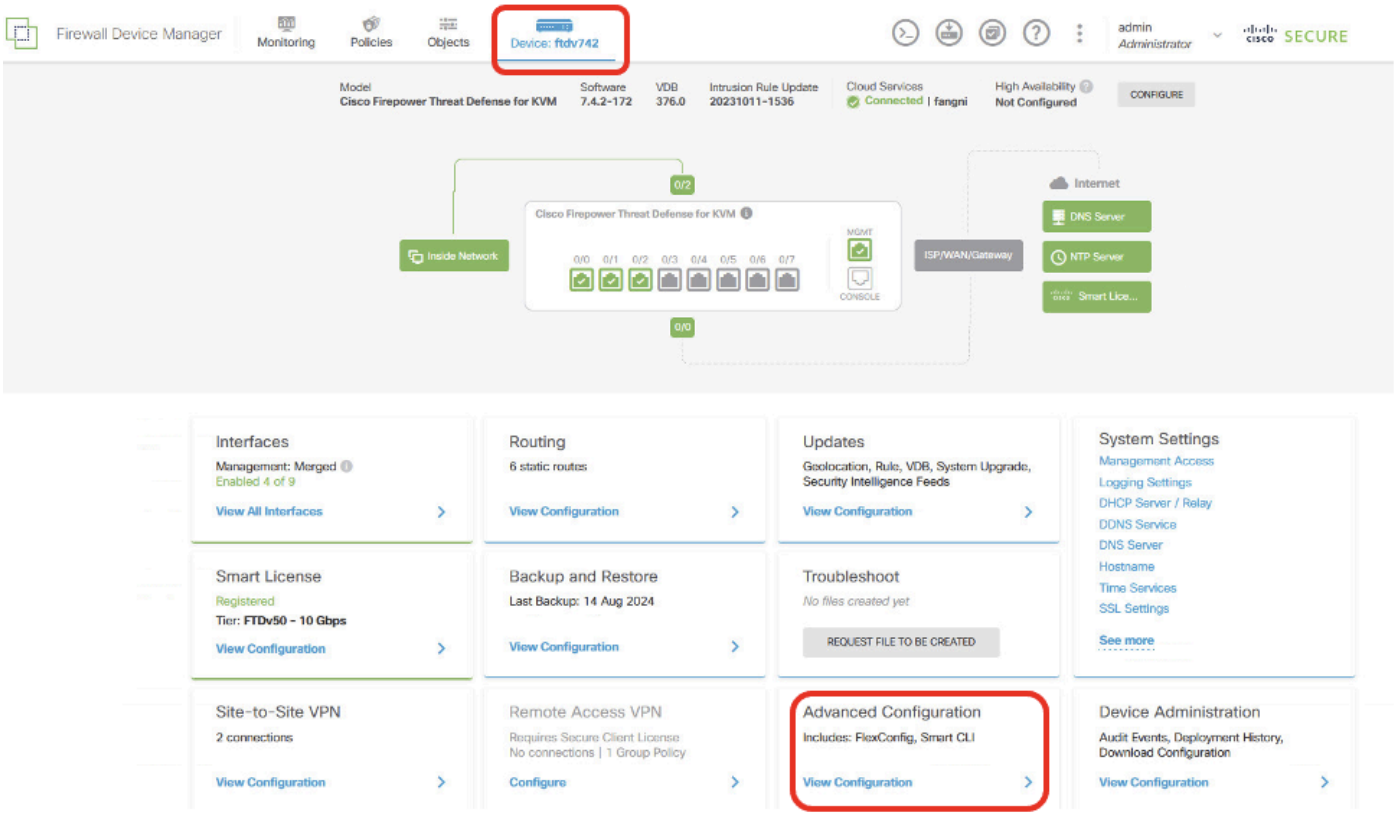
Etapa 11.2. Criar objeto do endereço IP do Site2 Client2. Forneça as informações necessárias. Clique no botão OK.

- Nome: remote_192.168.50.10
- Digite: Host
- Host: 192.168.50.10



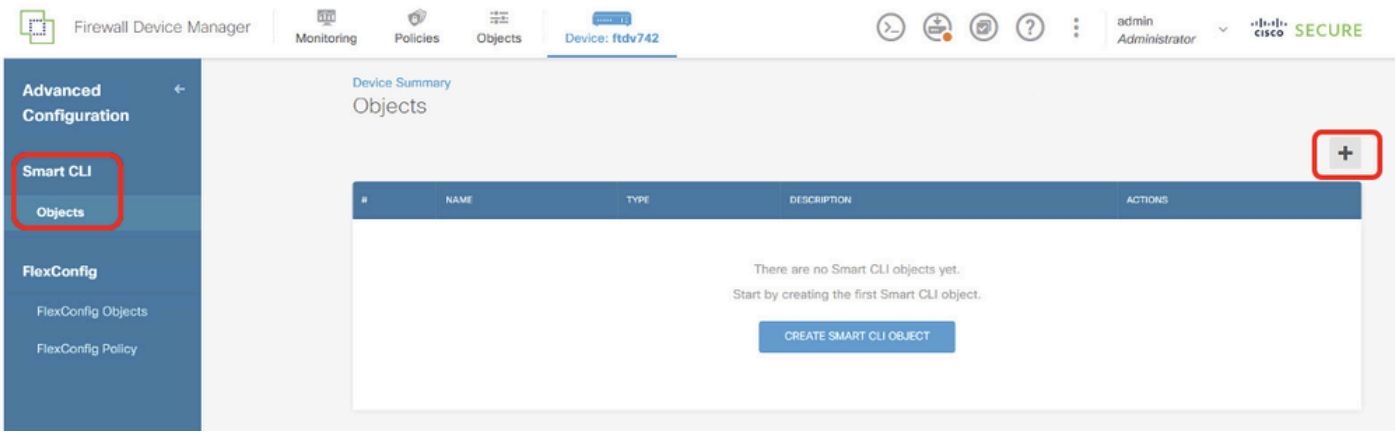
Site1FTD_PBR_RemoteObject

Etapa 12. Criar uma lista de acesso estendida para o PBR. Navegue até Device > Advanced Configuration. Clique em View Configuration.



Site1FTD_View_Advanced_Configuration

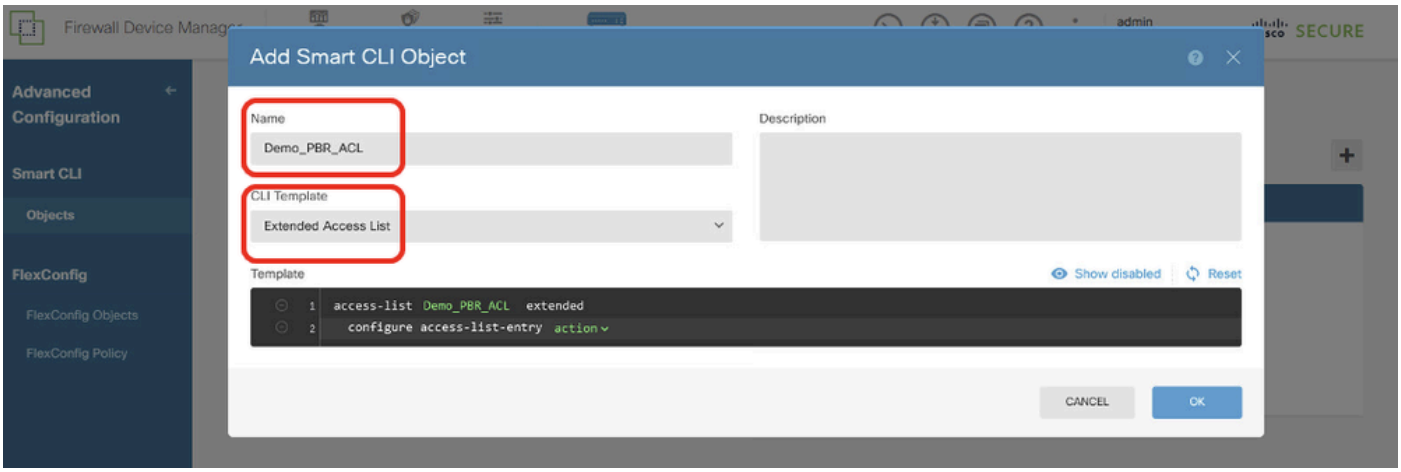
Etapa 12.1. Navegue até Smart CLI > Objects. Clique no botão +.



Site1FTD_Add_SmartCLI_Object

Etapa 12.2. Digite um nome para o objeto e escolha o Modelo CLI.

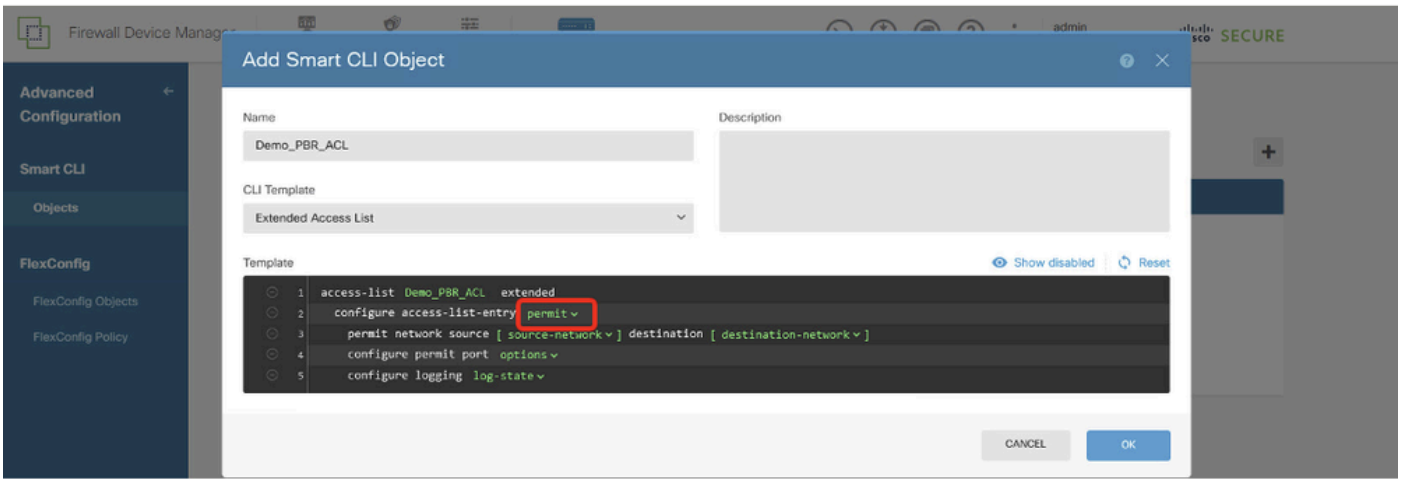
- Nome: Demo_PBR_ACL
- Modelo CLI: Lista de acesso estendida



Site1FTD_Create_PBR_ACL_1

Etapa 12.3. Navegue até Template e configure. Clique no botão OK para salvar.

Na linha 2, clique em action. Escolha Permitir.

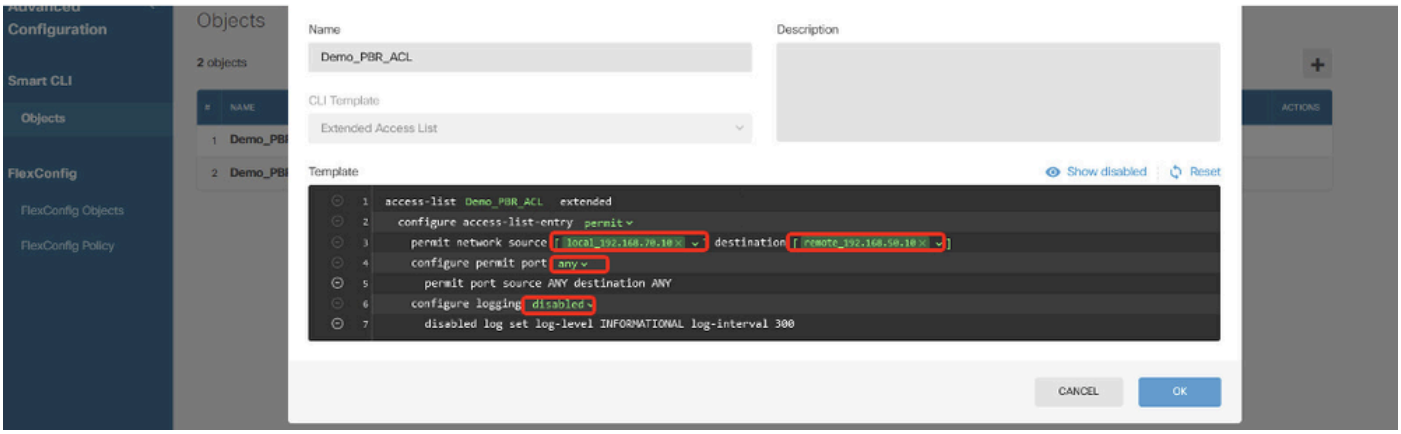


Site1FTD_Create_PBR_ACL_2

Na linha 3, clique em source-network. Escolha local_192.168.70.10. Clique em rede de destino. Escolha remote_192.168.50.10.

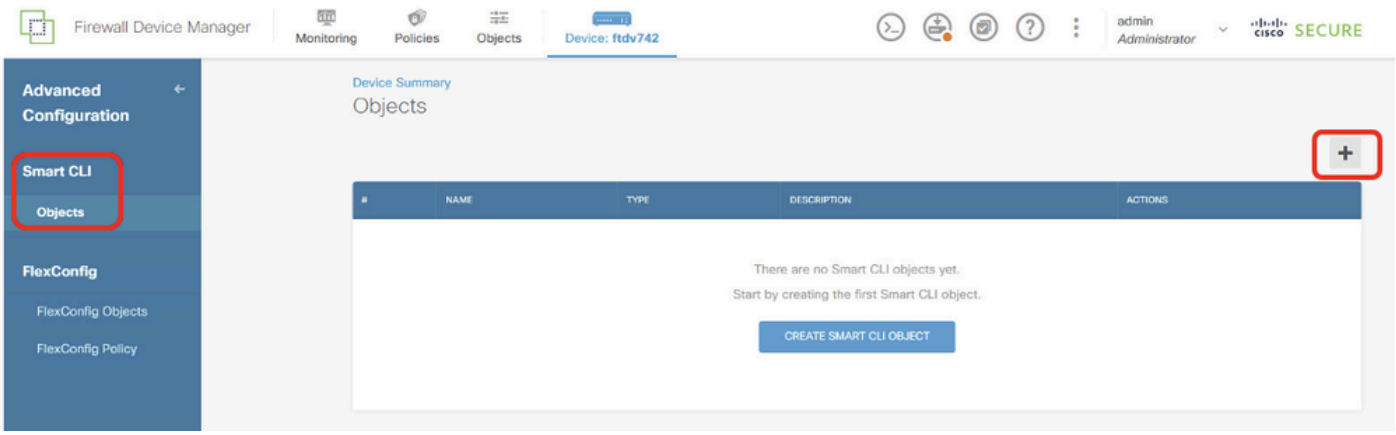
Na linha 4, clique em options e escolha any.

Na linha 6, clique em log-state e selecione disabled.



Site1FTD_Create_PBR_ACL_3

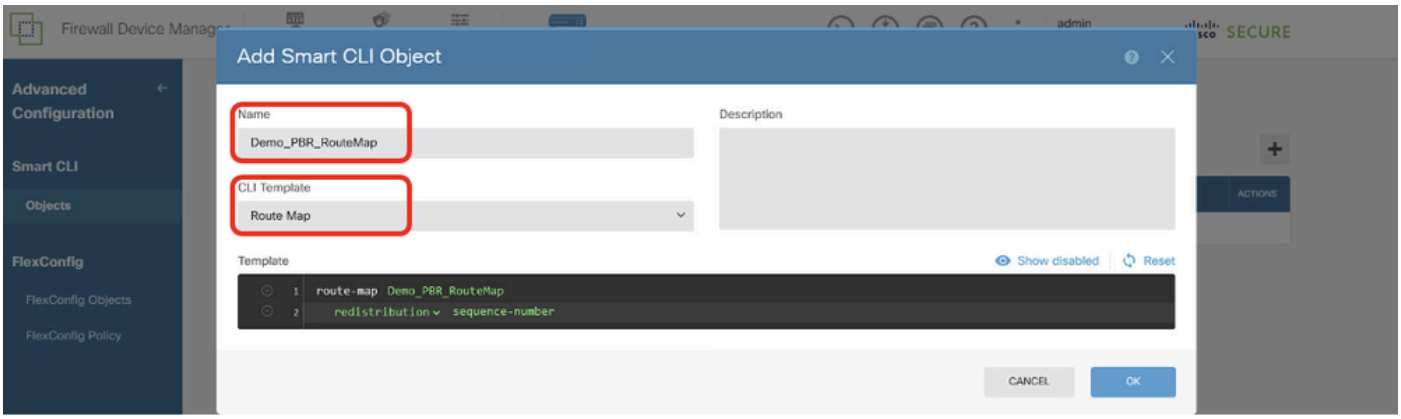
Etapa 13. Crie um mapa de rotas para o PBR. Navegue até Device > Advanced Configuration > Smart CLI > Objects. Clique no botão +.



Site1FTD_Add_SmartCLI_Object

Etapa 13.1. Digite um nome para o objeto e escolha o Modelo CLI.

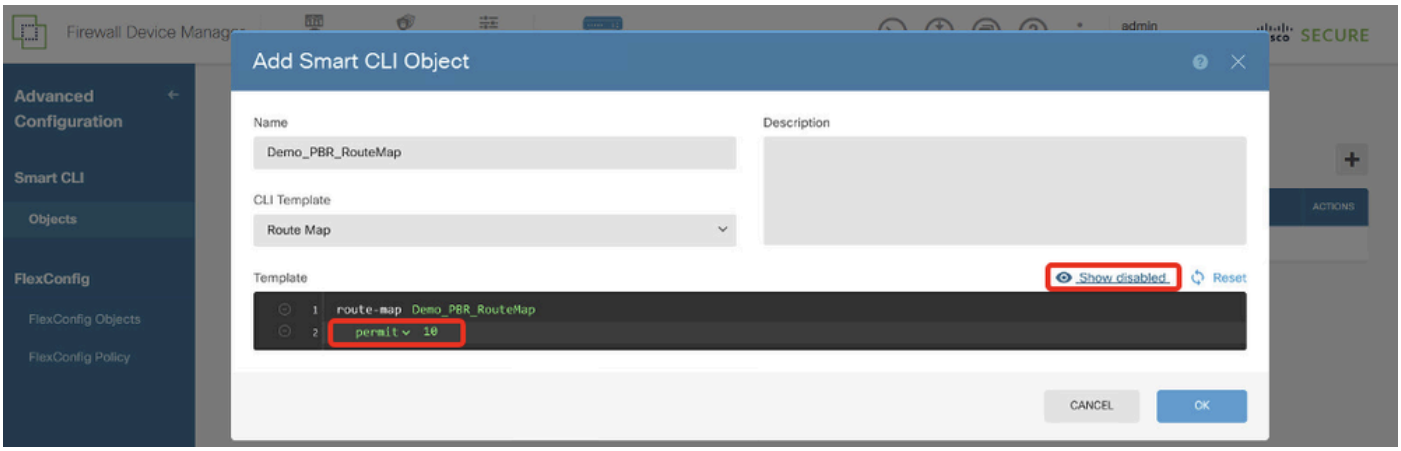
- Nome: Demo_PBR_RouteMap
- Modelo CLI: Mapa de Rotas



Site1FTD_Create_PBR_RouteMap_1

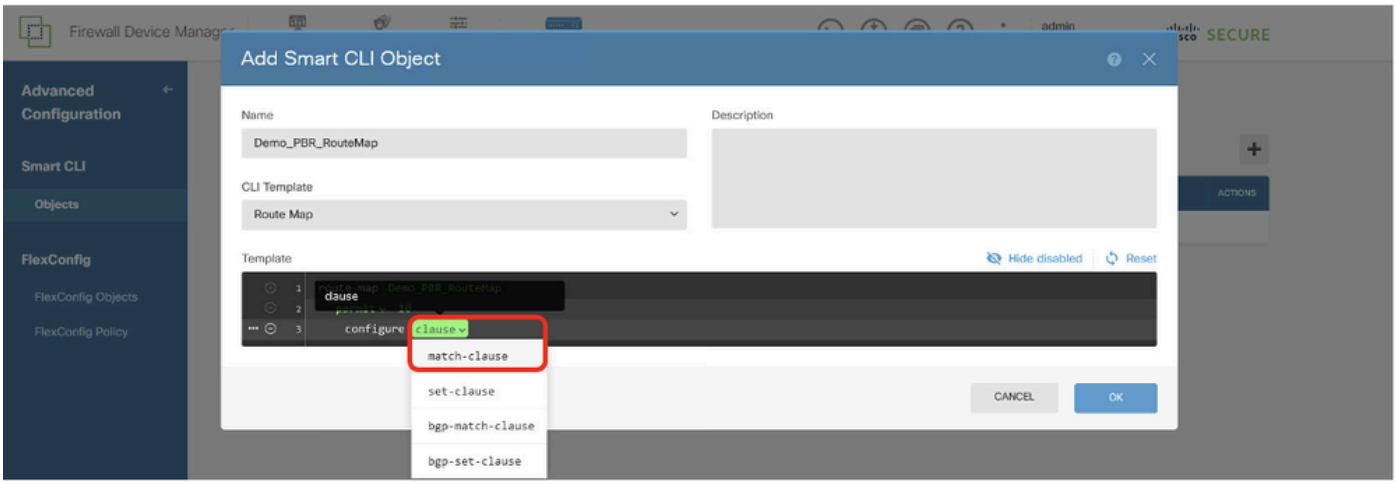
Etapa 13.2. Navegue até Template e configure. Clique no botão OK para salvar.

Na linha 2, clique em redistribution. Escolha Permitir. Clique em sequence-number, manual input 10. Clique em Mostrar desativado.



Site1FTD_Create_PBR_RouteMap_2

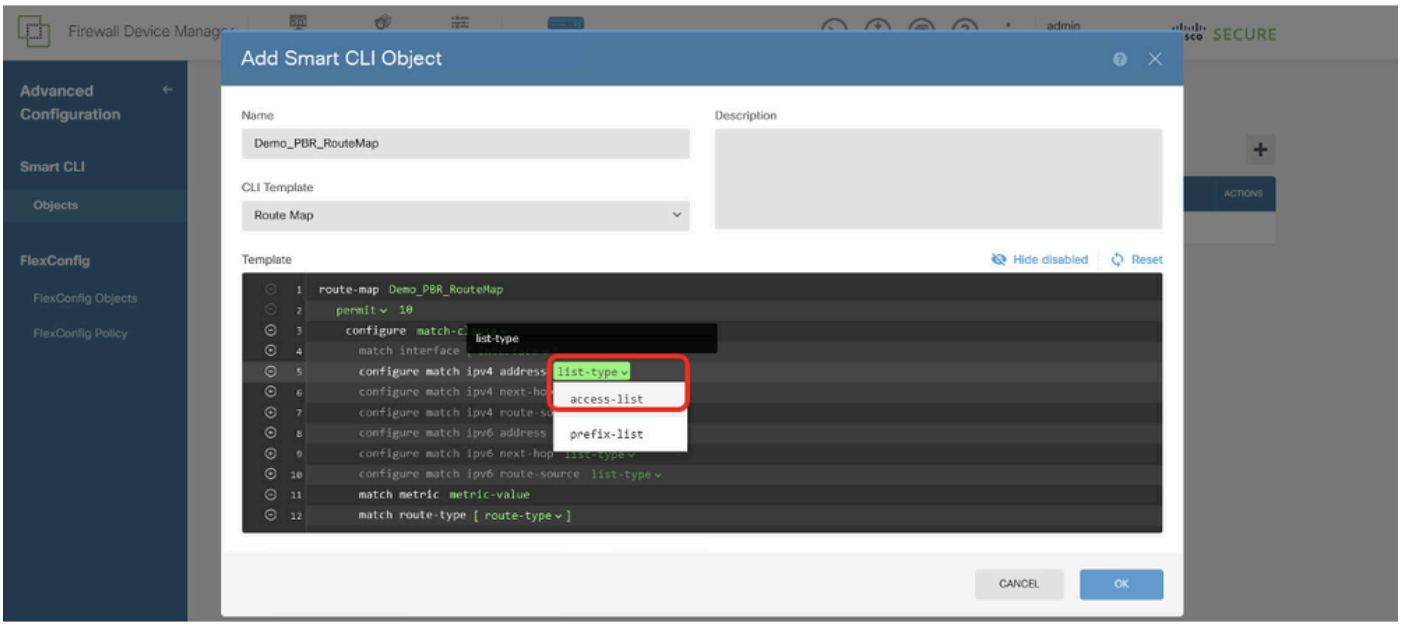
Linha 3, clique em + para ativar a linha. Clique em cláusula. Escolha match-clause.



Site1FTD_Create_PBR_RouteMap_3

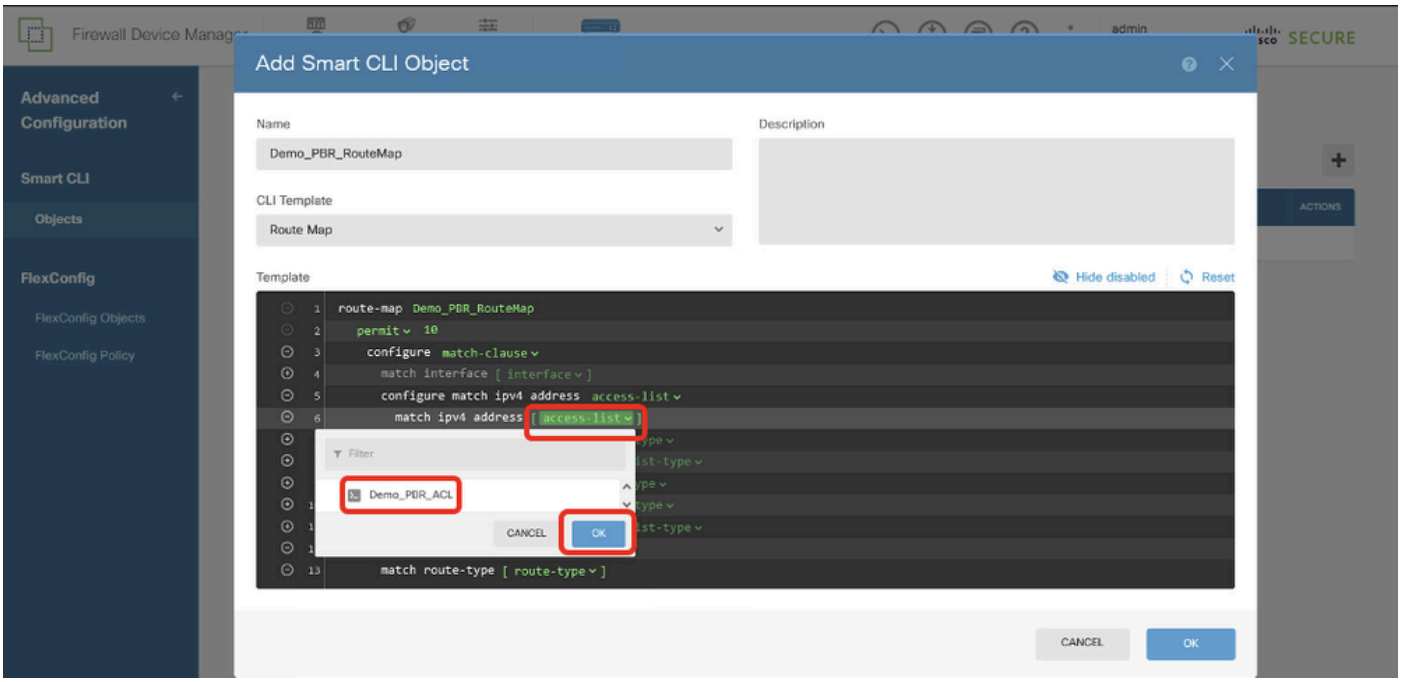
Linha 4, clique em - para desativar a linha.

Linha 5, clique em + para ativar a linha. Clique em tipo de lista. Escolha access-list.



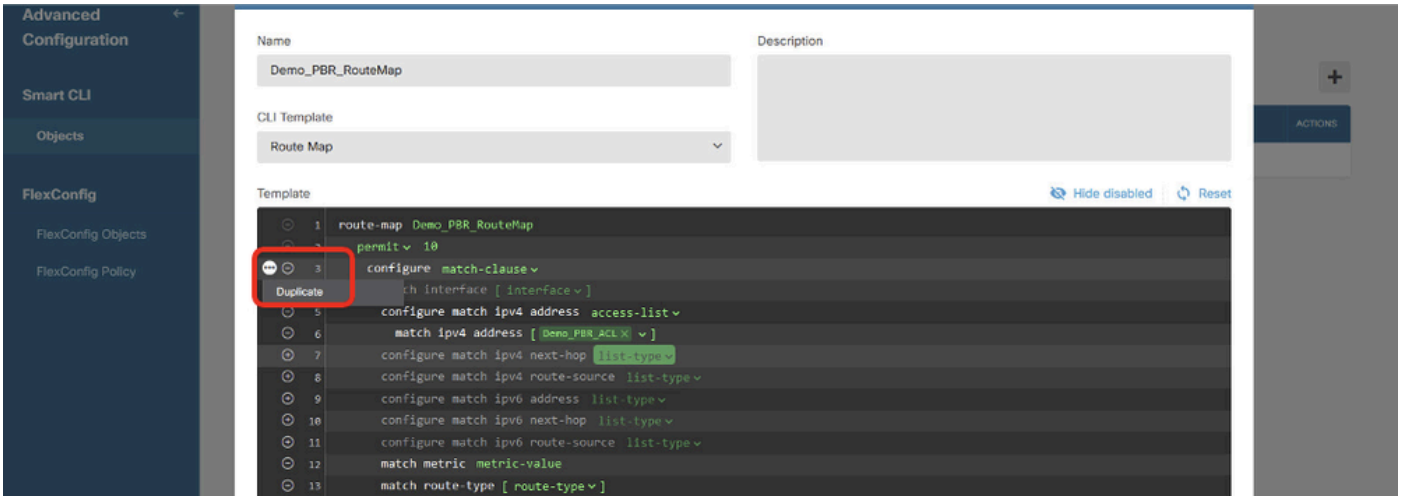
Site1FTD_Create_PBR_RouteMap_4

Na linha 6, clique em access-list. Escolha o nome da ACL criado na Etapa 12. Neste exemplo, é Demo_PBR_ACL.



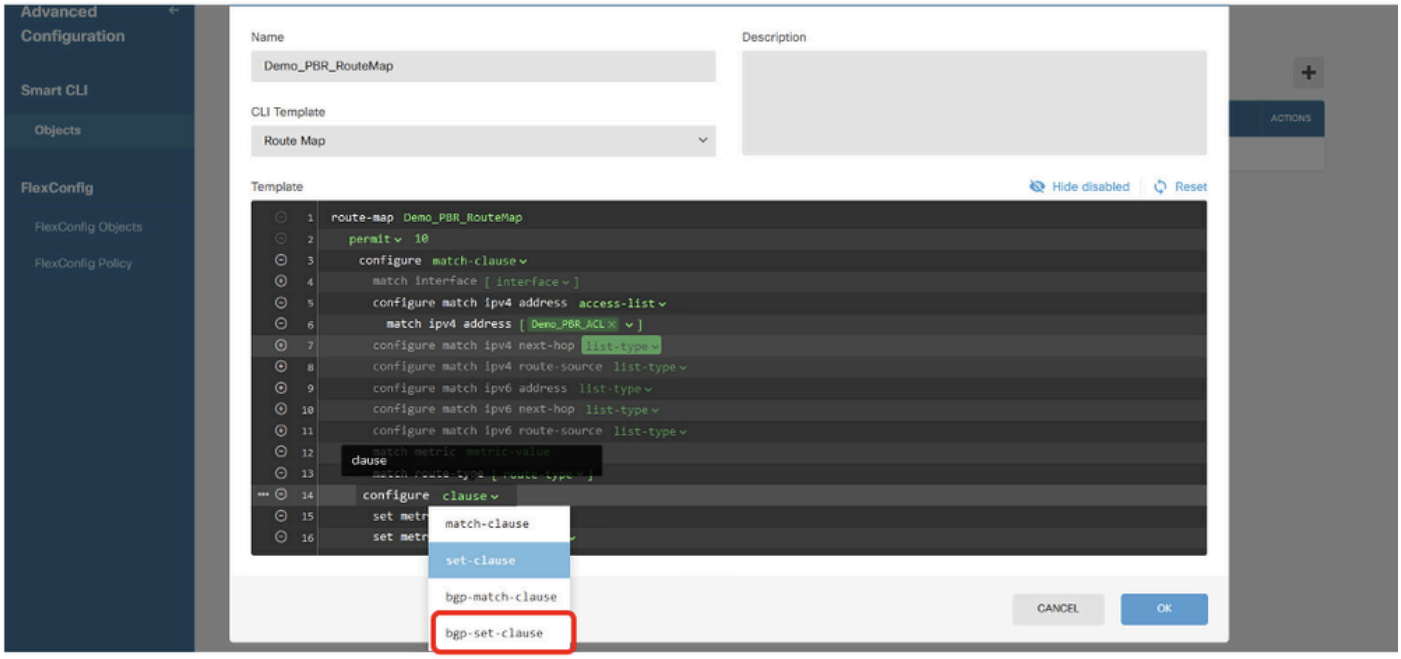
Site1FTD_Create_PBR_RouteMap_5

Volte para a Linha 3. Clique nas opções ... e escolha Duplicar.



Site1FTD_Create_PBR_RouteMap_6

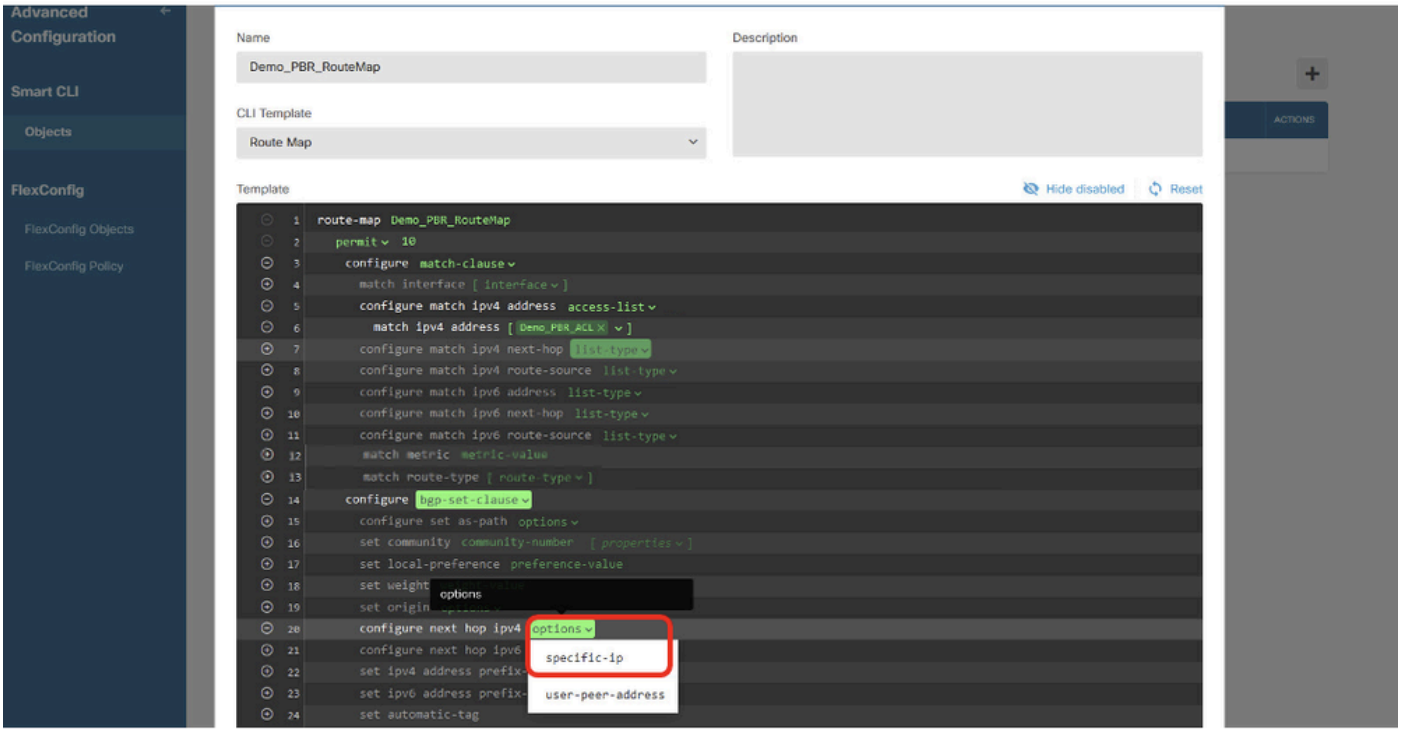
Na linha 14, clique em clause e escolha bgp-set-clause.



Site1FTD_Create_PBR_RouteMap_7

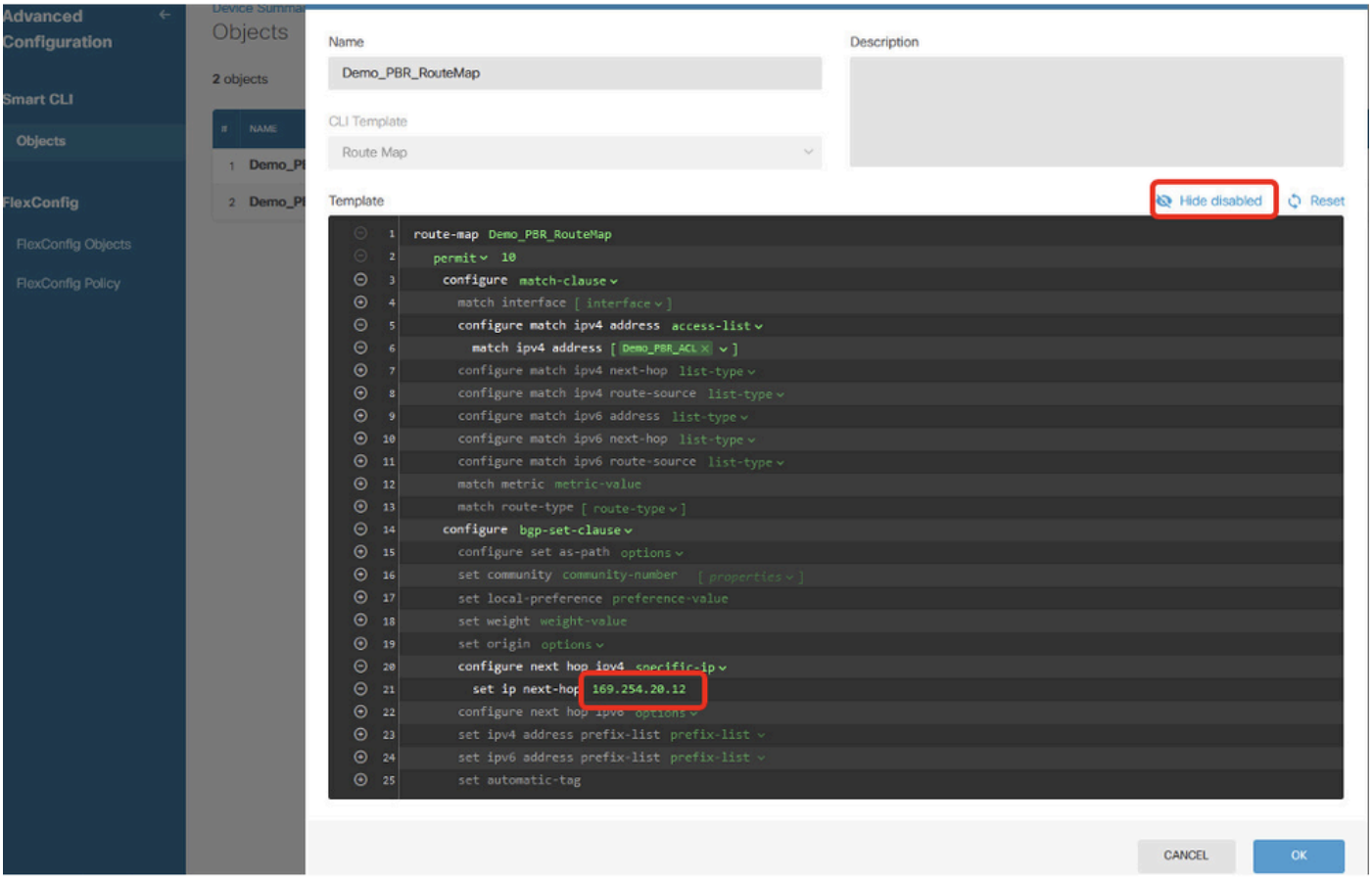
Nas Linhas 12, 13, 15, 16, 17, 18, 19, 21, 22, 23, 24, clique no botão - para desabilitar.

Na linha 20, clique em options e escolha specific-ip.



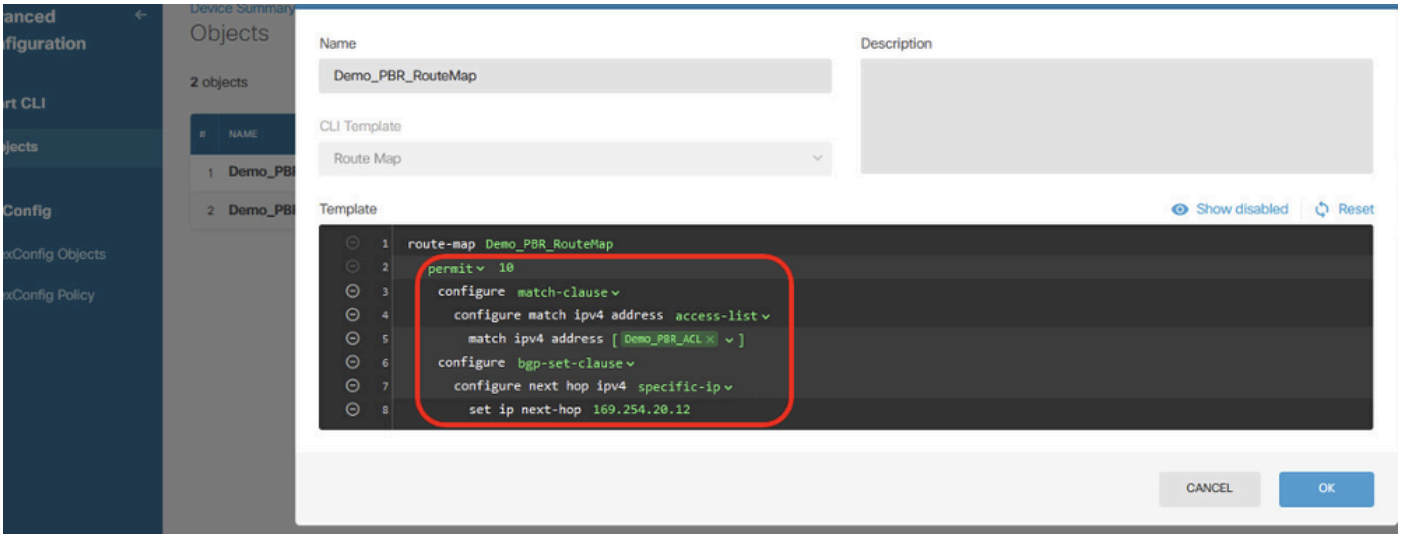
Site1FTD_Create_PBR_RouteMap_8

Na linha 21, clique em ip-address. Endereço IP do próximo salto de entrada manual. Neste exemplo, é o endereço IP de peer Site2 FTD VTI tunnel2 (169.254.20.12). Clique em Hide disabled.



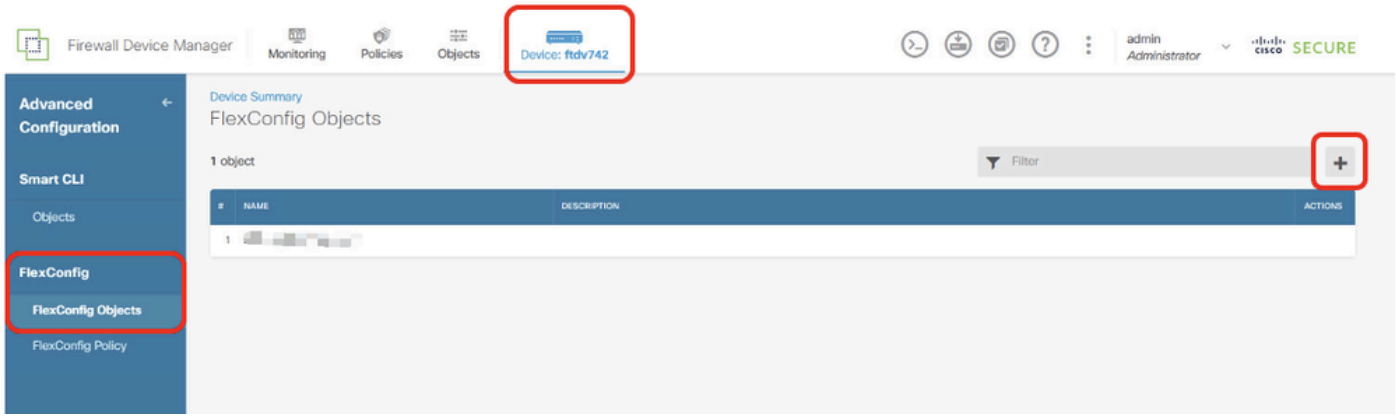
Site1FTD_Create_PBR_RouteMap_9

Reveja a configuração do mapa de rotas.



Site1FTD_Create_PBR_RouteMap_10

Etapa 14. Criar objeto FlexConfig para PBR. Navegue até Device > Advanced Configuration > FlexConfig Objects e clique no botão +.



Site1FTD_Create_PBR_FlexObj_1

Etapa 14.1. Digite um nome para o objeto. Neste exemplo, Demo_PBR_FlexObj. No editor Template e Negate Template, insira as linhas de comando.

- Modelo:

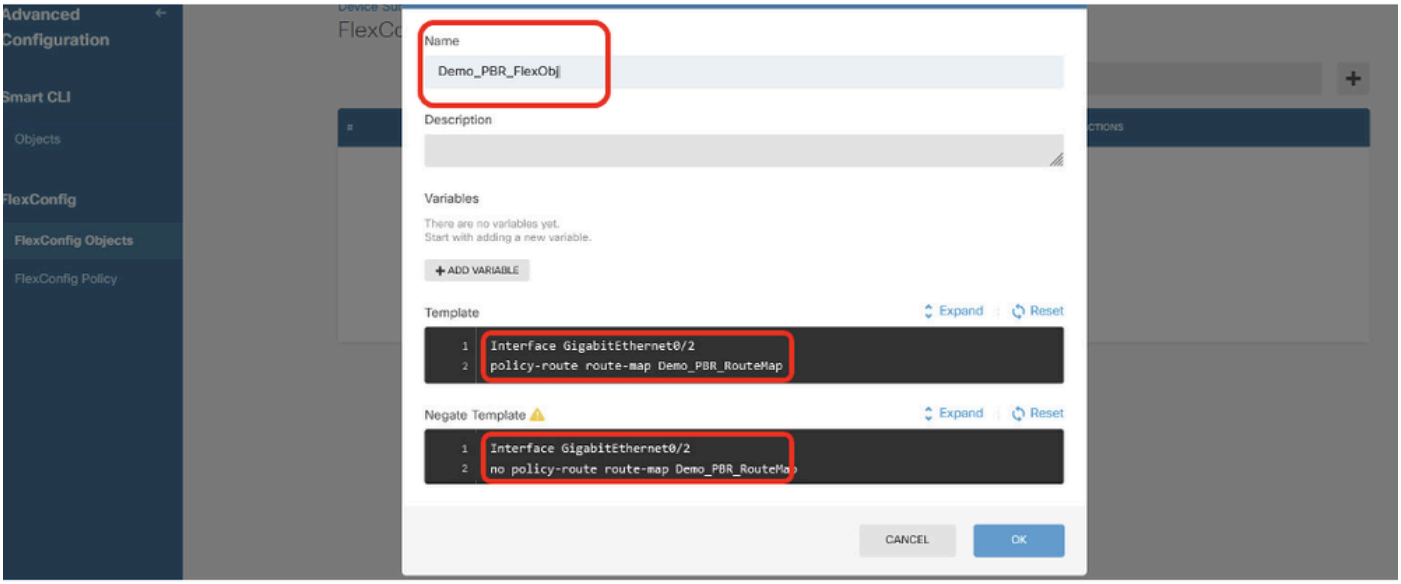
interface GigabitEthernet0/2

policy-route route-map Demo_PBR_RouteMap_Site2

- Negar Modelo:

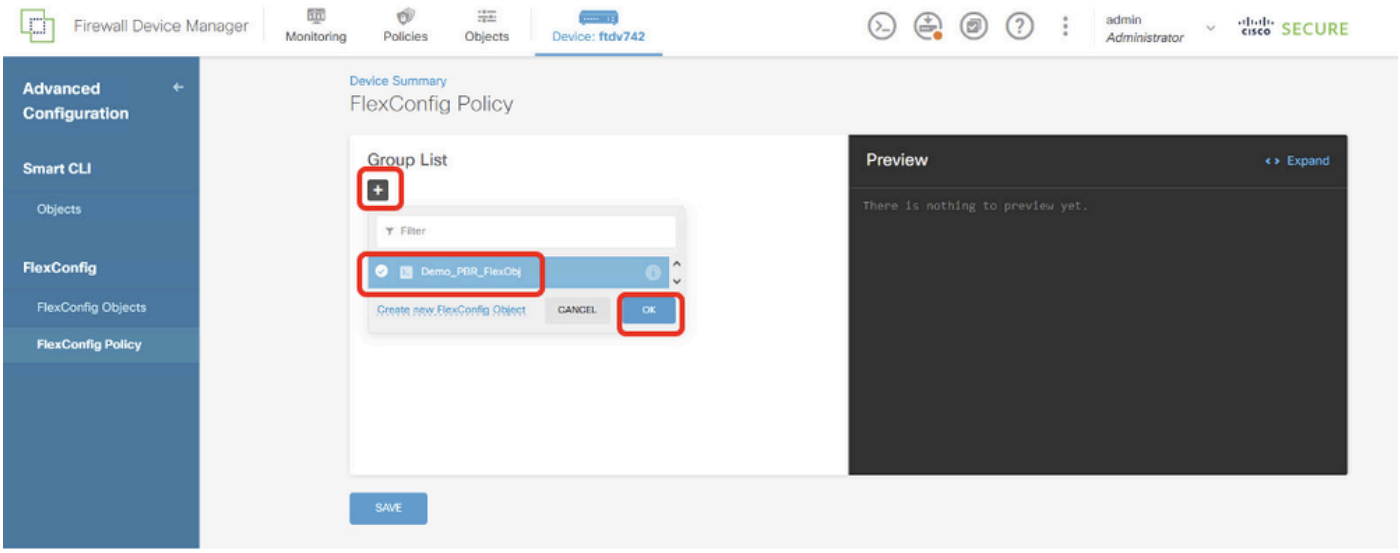
interface GigabitEthernet0/2

no policy-route route-map Demo_PBR_RouteMap_Site2



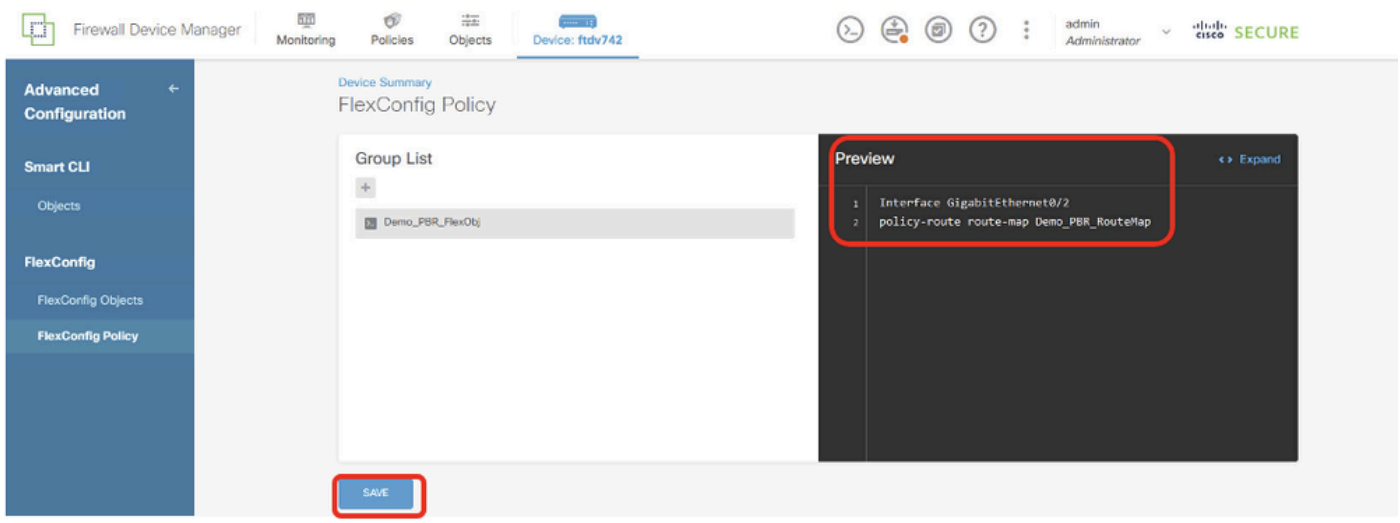
Site1FTD_Create_PBR_FlexObj_2

Etapa 15. Criar política FlexConfig para PBR. Navegue até Dispositivo > Configuração avançada > Política FlexConfig. Clique no botão +. Escolha o nome do Objeto FlexConfig criado na Etapa 14. Clique no botão OK.



Site1FTD_Create_PBR_FlexPolicy_1

Etapa 15.1. Verifique o comando na janela Preview. Se estiver bom, clique em Salvar.



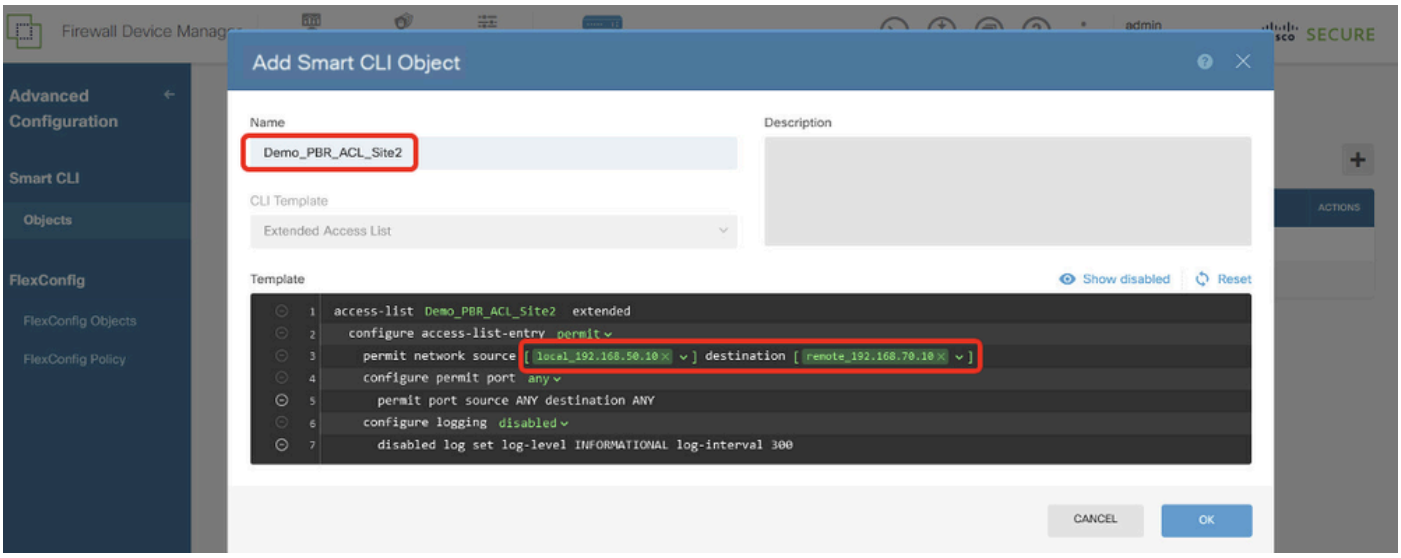
Site1FTD_Create_PBR_FlexPolicy_2

Etapa 16. Implantar as alterações de configuração.

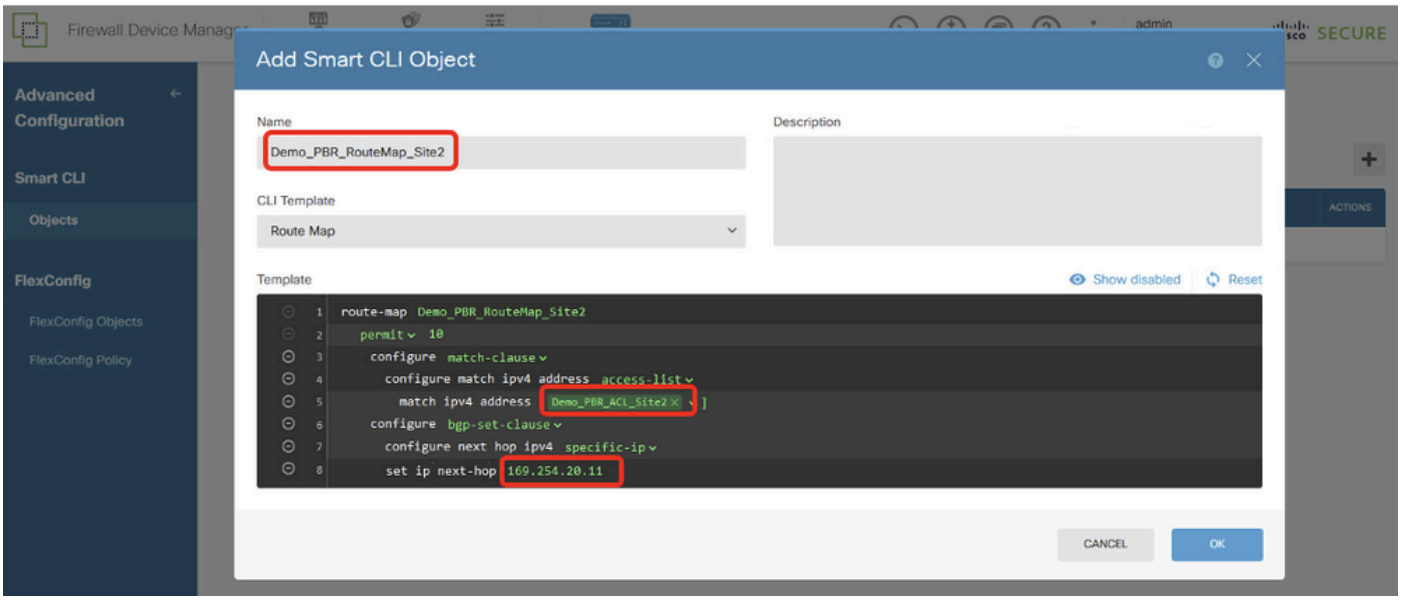
Site1FTD_Deployment_Changes

Configuração do Site2 FTD PBR

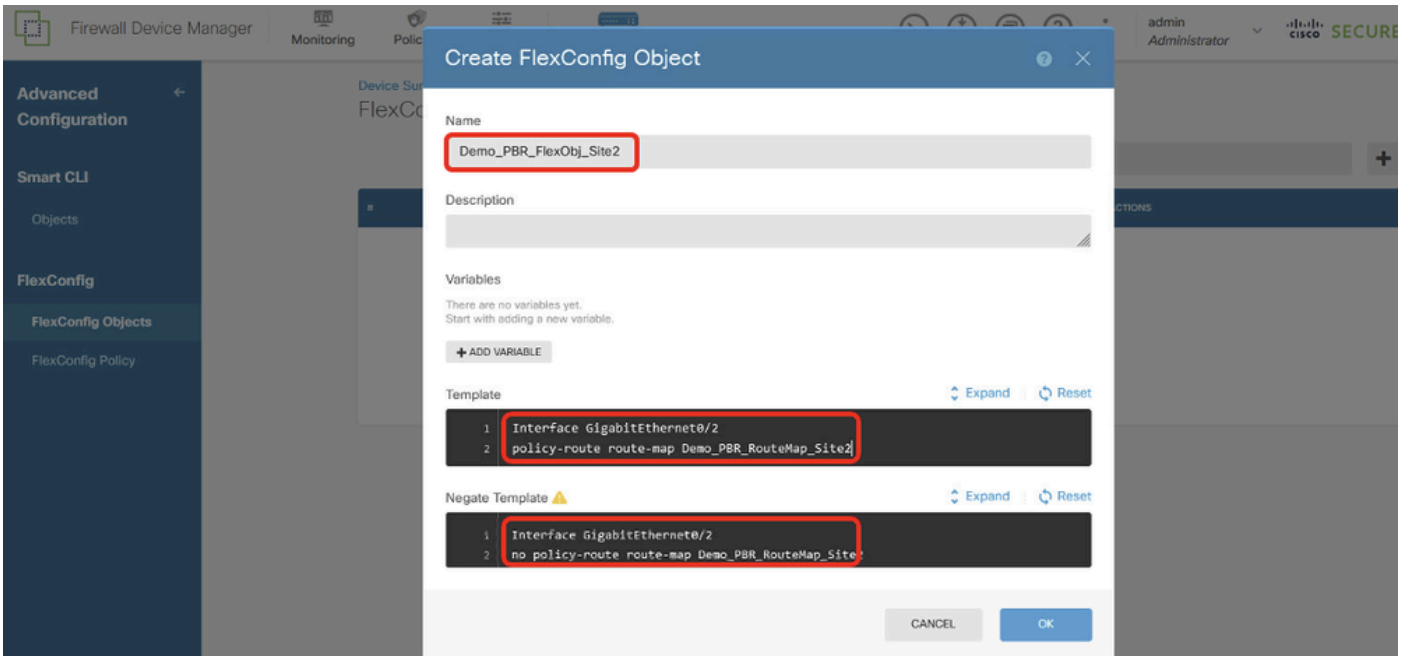
Etapa 17. Repita as Etapas 11 a 16 para criar o PBR com os parâmetros correspondentes para o FTD do Site2.



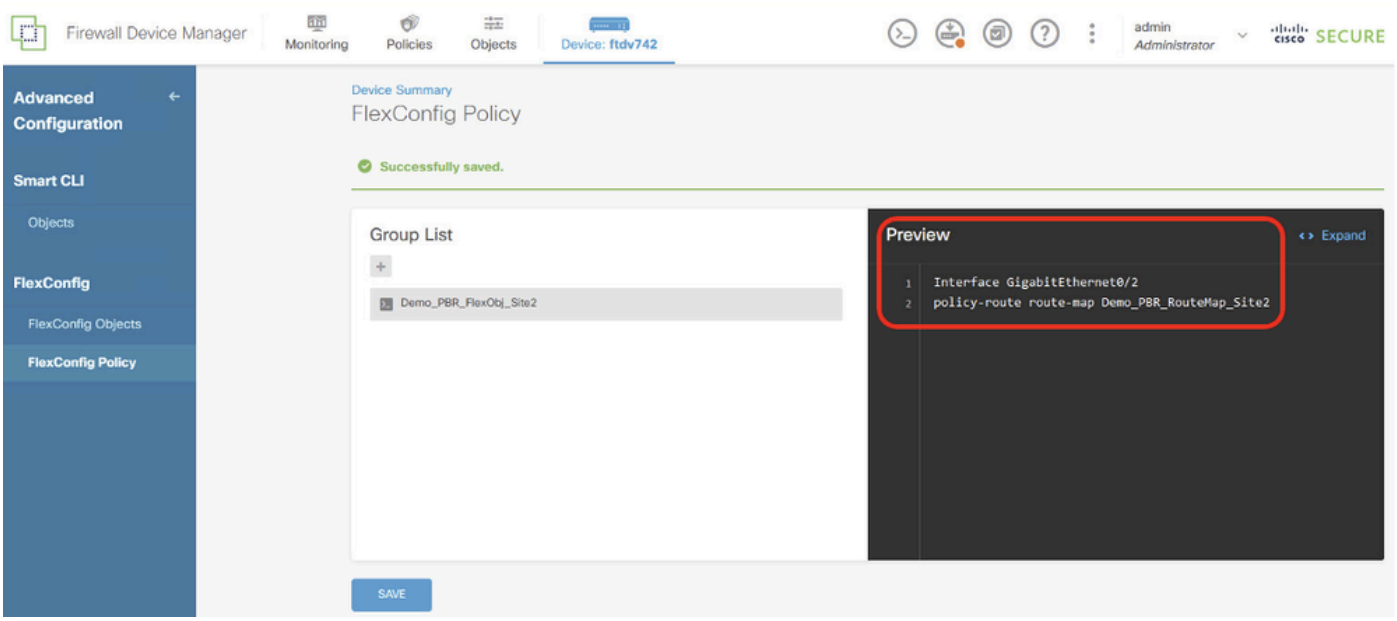
Site2FTD_Create_PBR_ACL



Site2FTD_Create_PBR_RouteMap



Site2FTD_Create_PBR_FlexObj

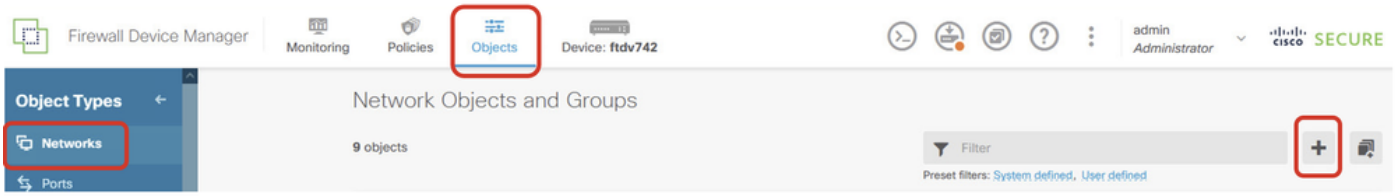


Site2FTD_Create_PBR_FlexPolicy

Configurações no monitor de SLA

Configuração do Monitor de SLA de FTD do Site1

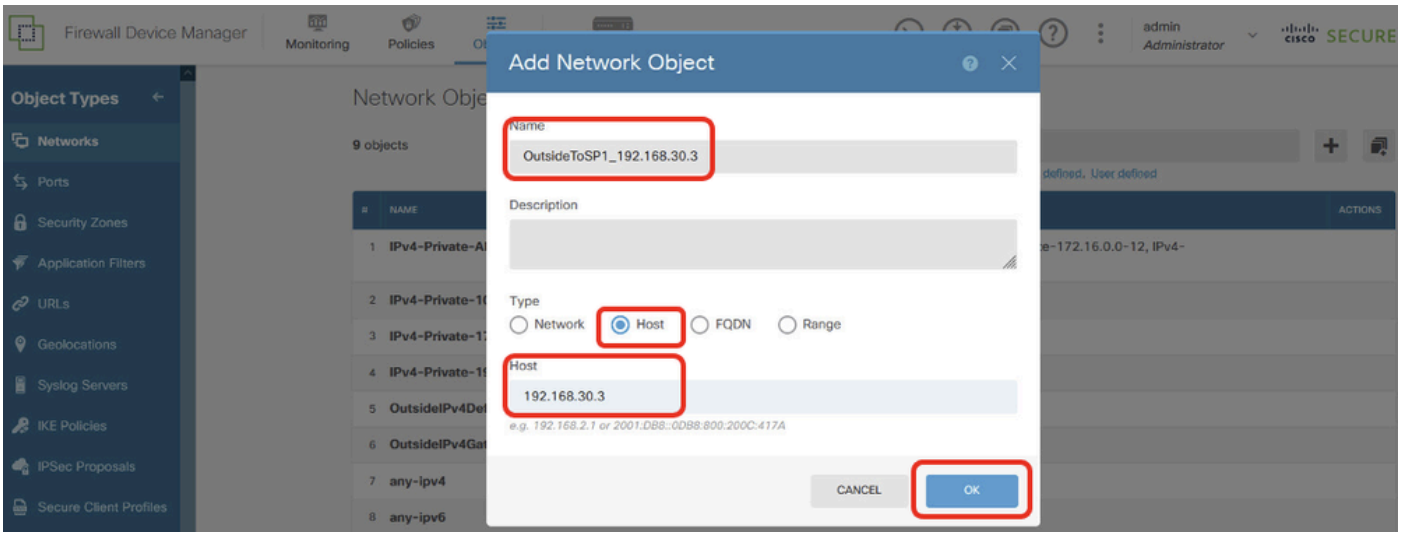
Etapa 18. Crie novos objetos de rede a serem usados pelos Monitores de SLA para Site1 FTD. Navegue até Objetos > Redes, clique no botão +.



Site1FTD_Create_Network_Object

Etapa 18.1. Criar objeto para o endereço IP do gateway ISP1. Forneça as informações necessárias. Clique no botão OK.

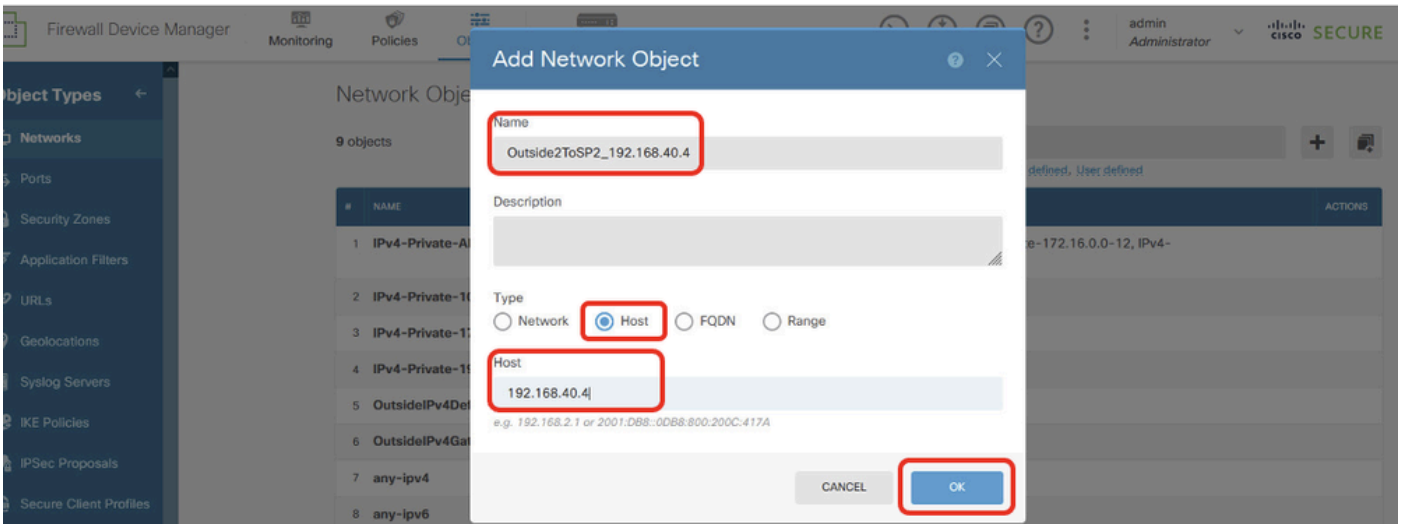
- Nome: OutsideToSP1_192.168.30.3
- Digite: Host
- Host: 192.168.30.3



Site1FTD_Create_SLAMonitor_NetObj_ISP1

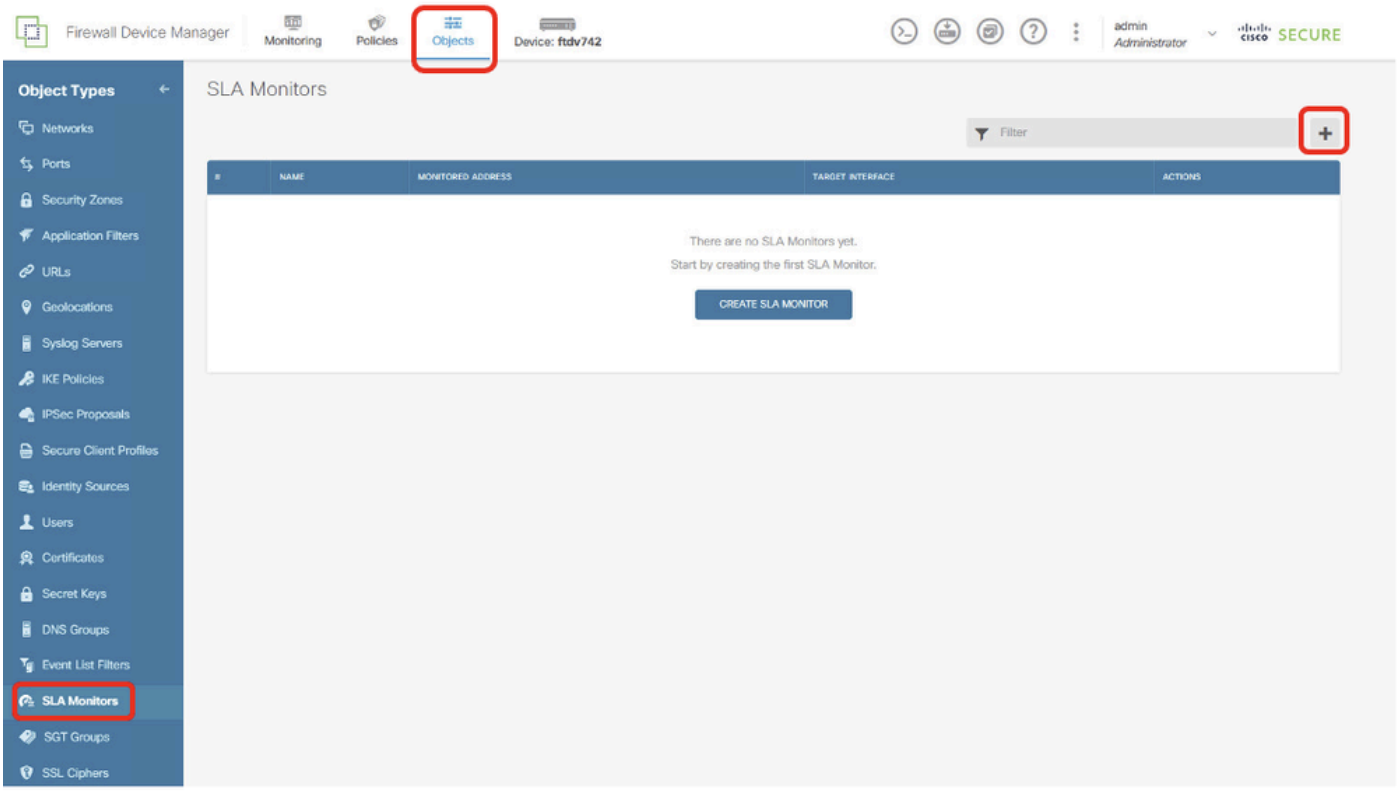
Etapa 18.2. Criar objeto para o endereço IP do gateway do ISP2. Forneça as informações necessárias. Clique no botão OK.

- Nome: Outside2ToSP2_192.168.40.4
- Digite: Host
- Host: 192.168.40.4



Site1FTD_Create_SLAMonitor_NetObj_ISP2

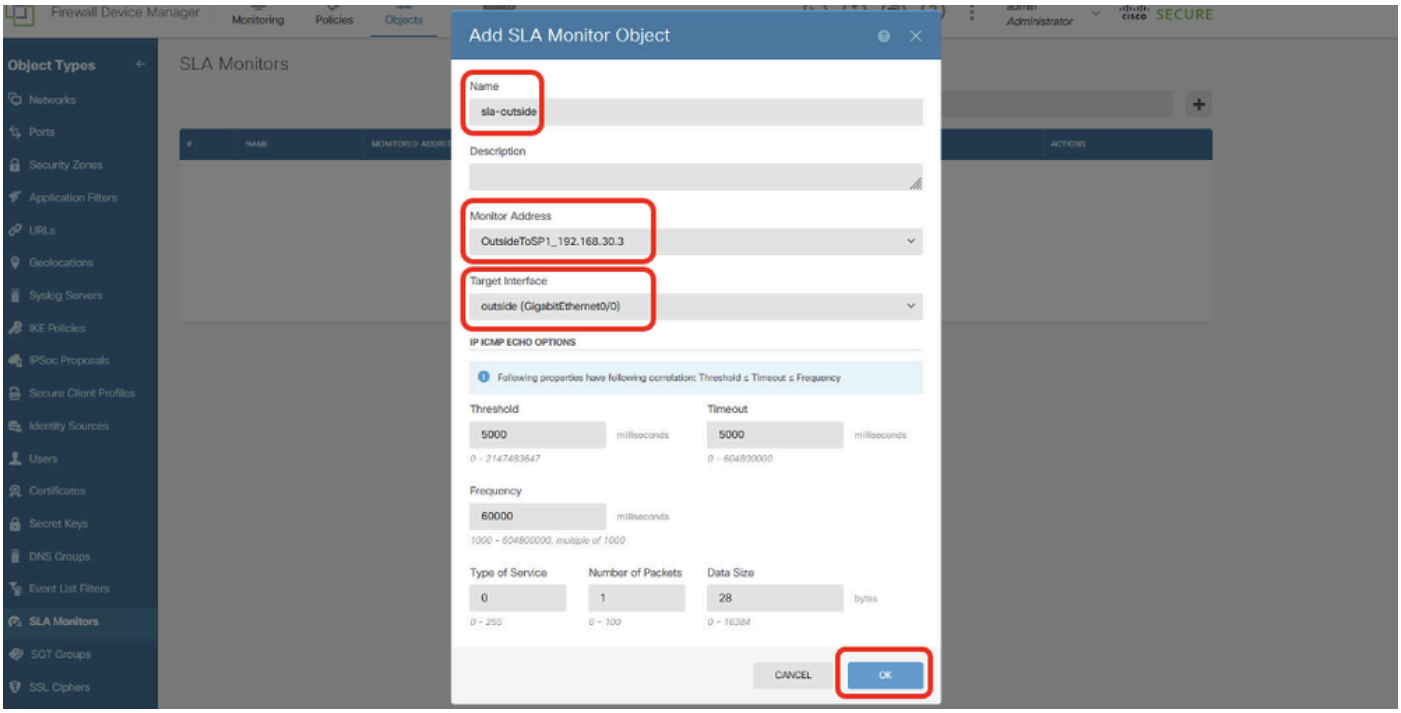
Etapa 19. Criar monitor de SLA. Navegue até Objetos > Tipos de objeto > Monitores SLA. Clique no botão + para criar um novo monitor de SLA.



Site1FTD_Create_SLAMonitor

Etapa 19.1. Na janela Add SLA Monitor Object, forneça as informações necessárias para o gateway ISP1. Clique no botão OK para salvar.

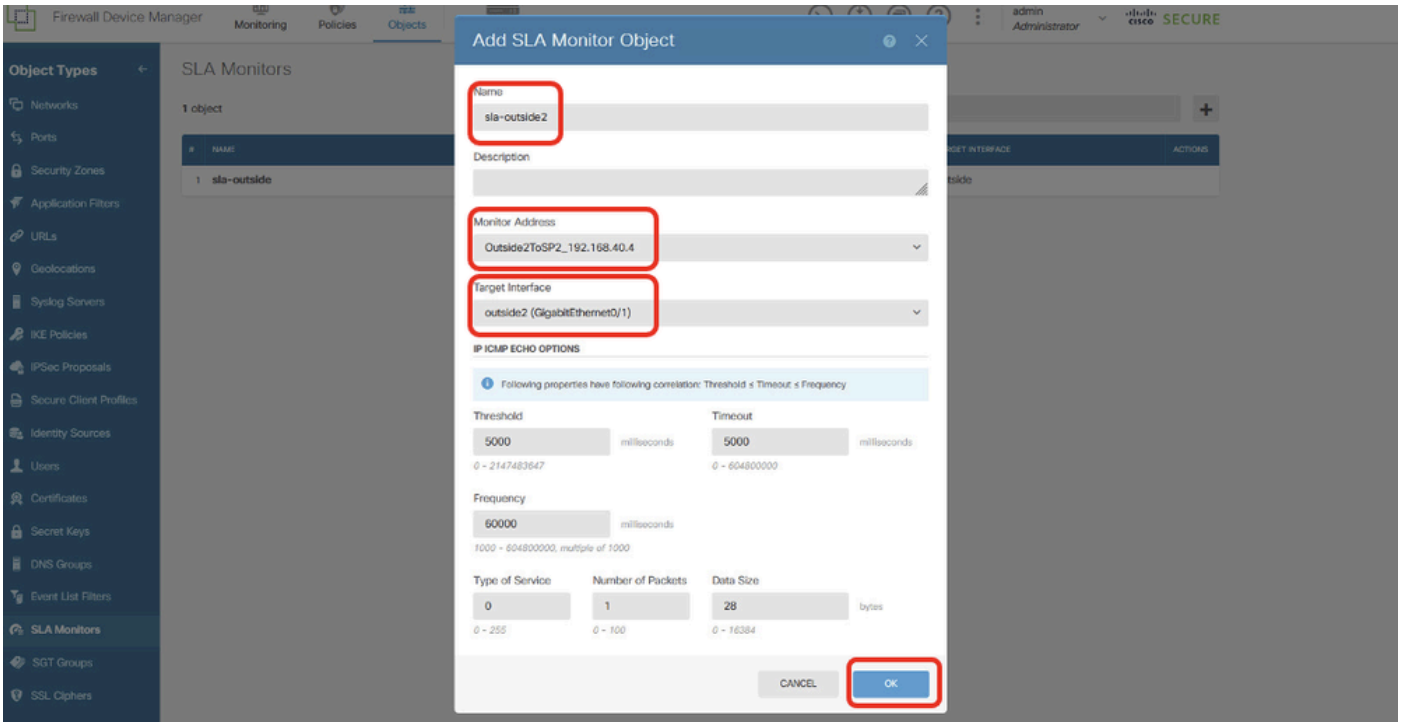
- Nome: sla-outside
- Endereço do monitor: OutsideToSP1_192.168.30.3
- Interface de destino: externo(GigabitEthernet0/0)
- OPÇÕES DE ECO IP ICMP: padrão



Site1FTD_Create_SLAMonitor_NetObj_ISP1_Details

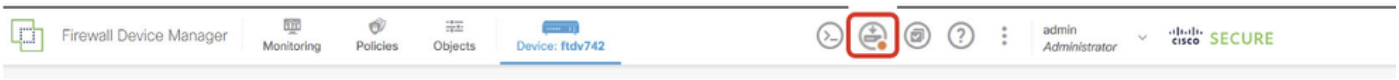
Etapa 19.2. Continue clicando no botão + para criar um novo monitor de SLA para o gateway ISP2. Na janela Add SLA Monitor Object, forneça as informações necessárias para o gateway ISP2. Clique no botão OK para salvar.

- Nome: sla-outside2
- Endereço do monitor: Outside2ToSP2_192.168.40.4
- Interface de destino: outside2(GigabitEthernet0/1)
- OPÇÕES DE ECO IP ICMP: padrão



Site1FTD_Create_SLAMonitor_NetObj_ISP2_Details

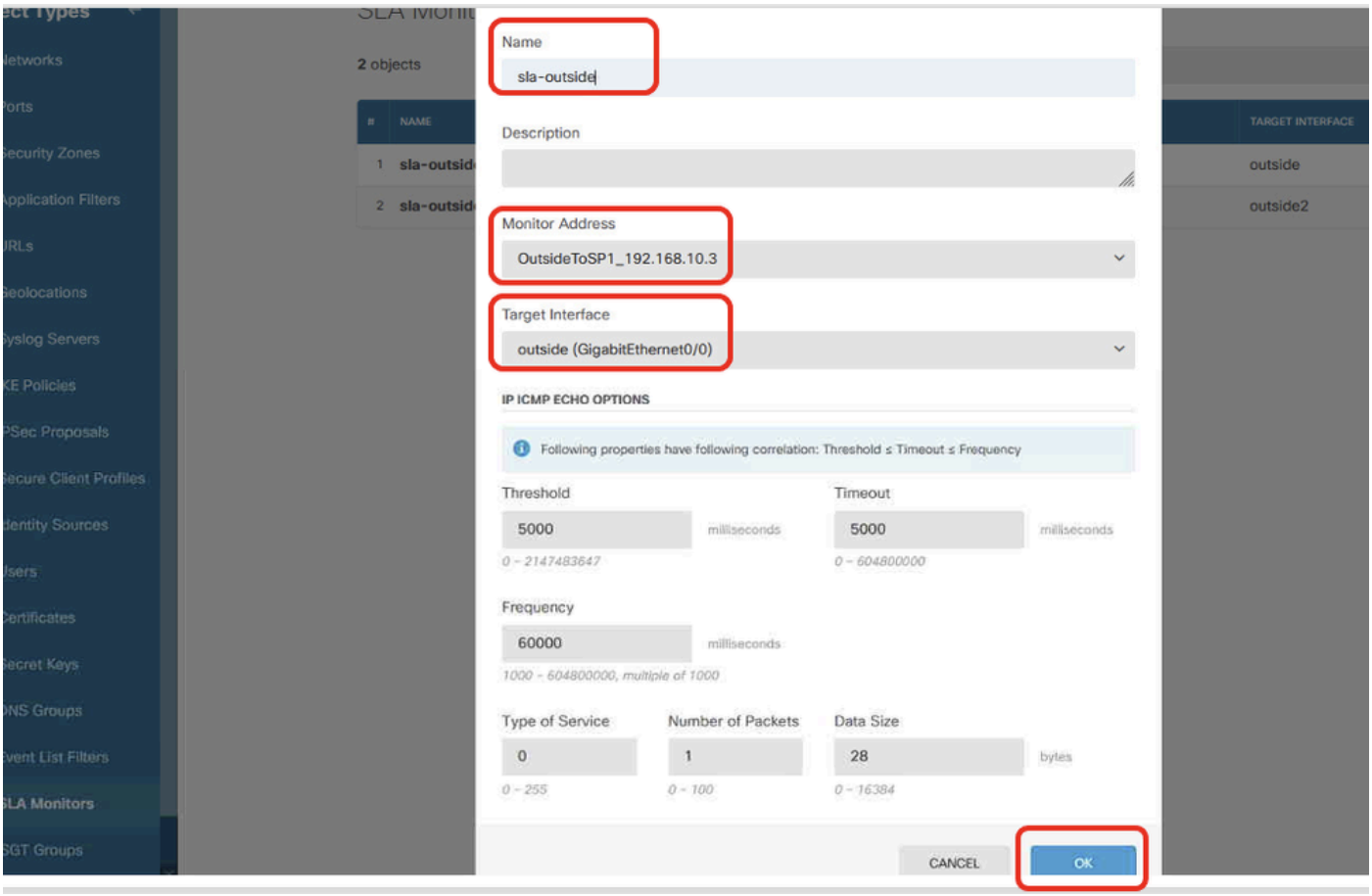
Etapa 20. Implantar as alterações de configuração.



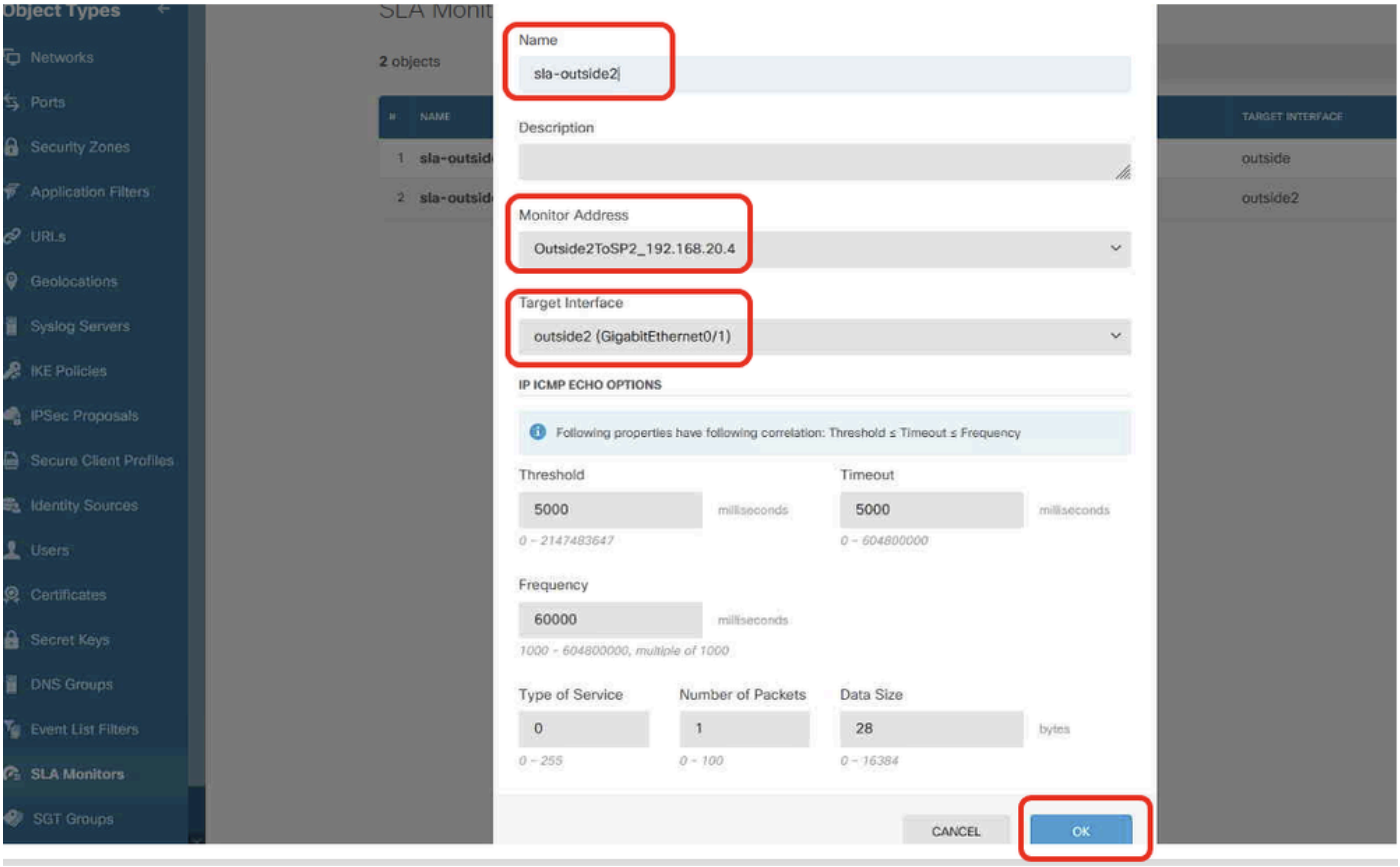
Site1FTD_Deployment_Changes

Configuração do Monitor de SLA de FTD do Site2

Etapa 21. Repita a Etapa 18. à Etapa 20. crie o Monitor do SLA com os parâmetros correspondentes no FTD do Site2.



Site2FTD_Create_SLAMonitor_NetObj_ISP1_Details

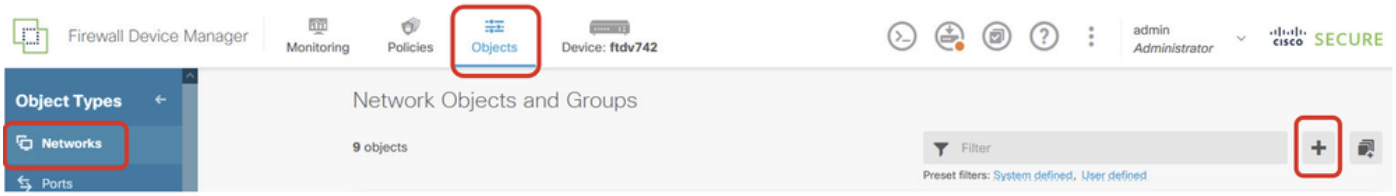


Site2FTD_Create_SLAMonitor_NetObj_ISP2_Details

Configurações em rota estática

Configuração de Rota Estática FTD do Site1

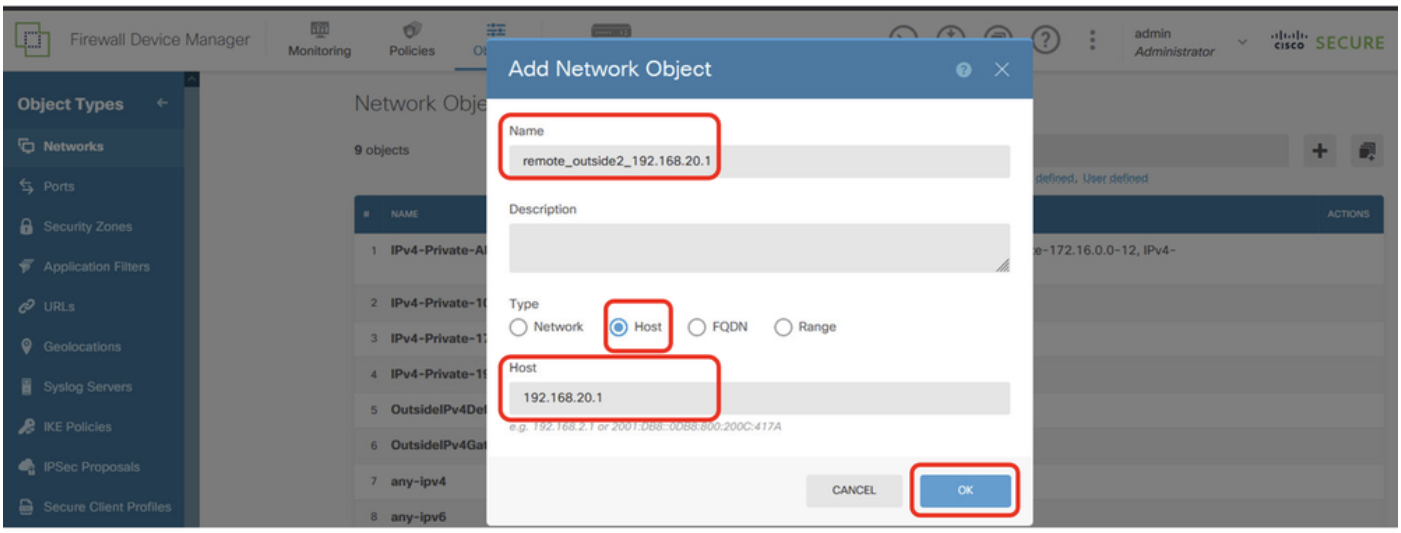
Etapa 22. Crie novos objetos de rede a serem usados pela rota estática para Site1 FTD. Navegue até Objetos > Redes, clique no botão +.



Site1FTD_Create_Obj

Etapa 22.1. Crie um objeto para o endereço IP externo2 do FTD do Site2 par. Forneça as informações necessárias. Clique no botão OK.

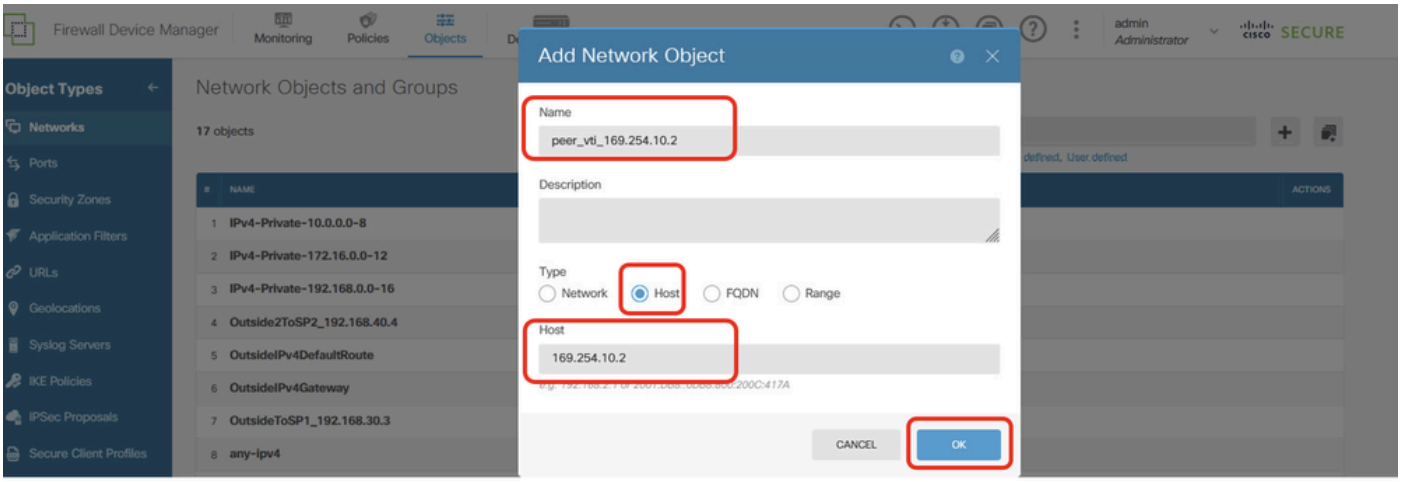
- Nome: remote_outside2_192.168.20.1
- Digite: HOST
- Rede: 192.168.20.1



Site1FTD_Create_NetObj_StaticRoute_1

Etapa 22.2. Criar objeto para o endereço IP do Túnel VTI1 do FTD do Site2 par. Fornecer as informações necessárias. Clique no botão OK.

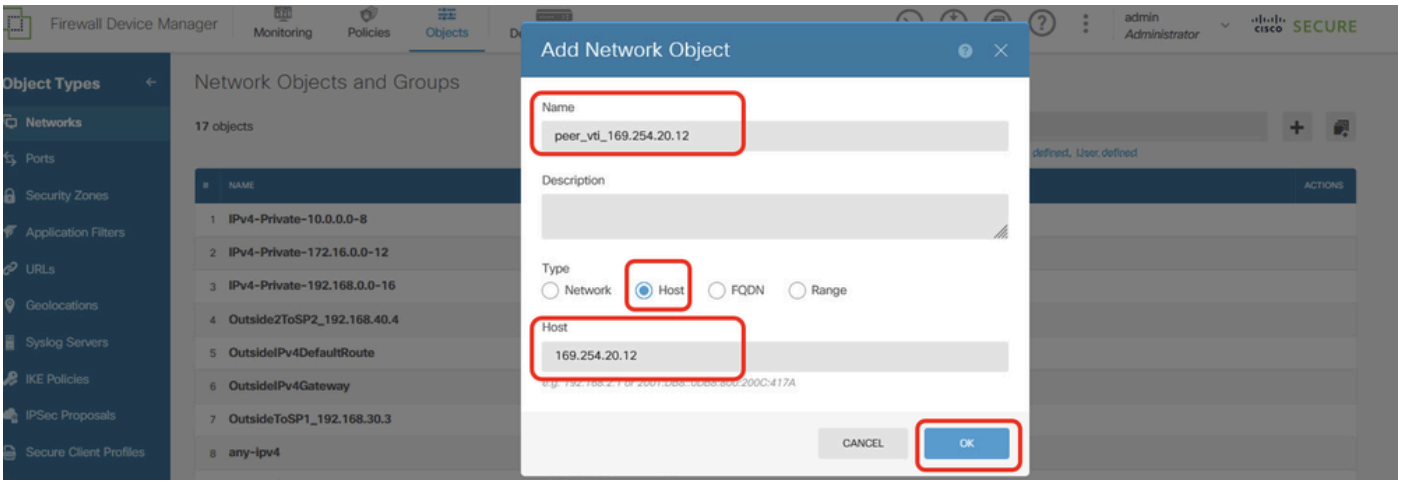
- Nome: peer_vti_169.254.10.2
- Digite: HOST
- Rede:169.254.10.2



Site1FTD_Create_NetObj_StaticRoute_2

Etapa 22.3. Criar objeto para o endereço IP do Túnel VTI2 do FTD do Site2 par. Fornecer as informações necessárias. Clique no botão OK.

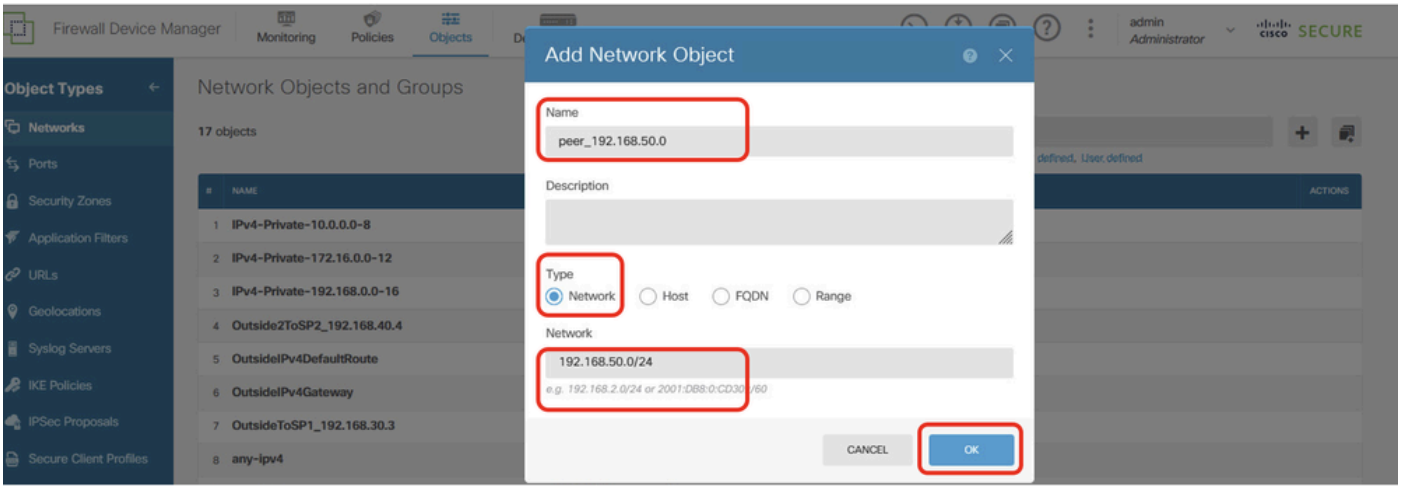
- Nome: peer_vti_169.254.20.12
- Digite: HOST
- Rede:169.254.20.12



Site1FTD_Create_NetObj_StaticRoute_3

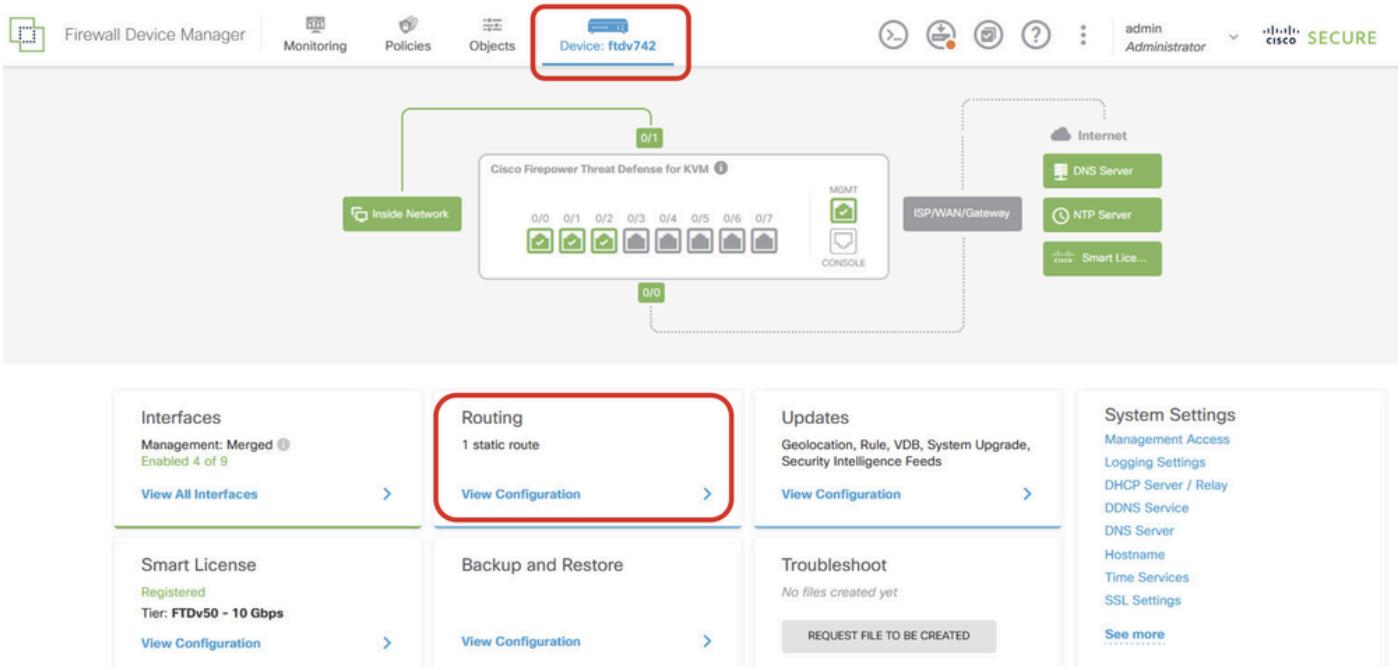
Etapa 22.4. Criar objeto para a rede interna do FTD do Site2 par. Forneça as informações necessárias. Clique no botão OK.

- Nome: peer_192.168.50.0
- Digite: REDE
- Rede:192.168.50.0/24

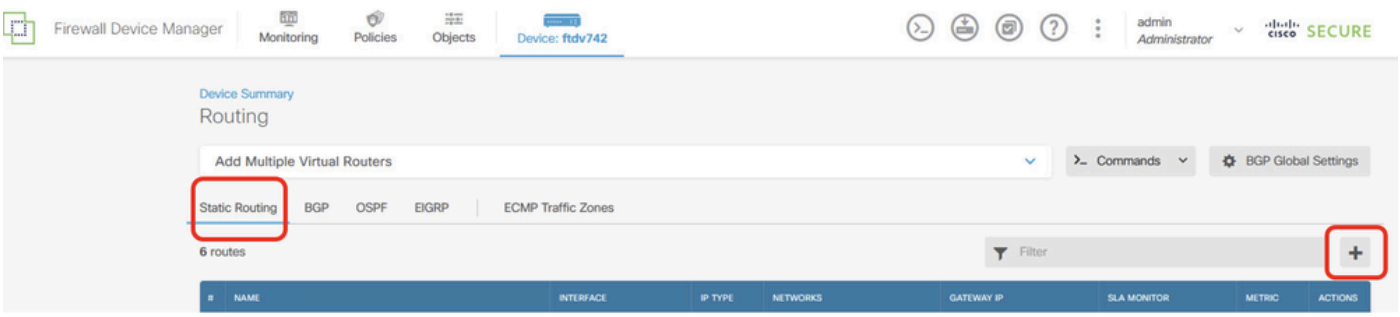


Site1FTD_Create_NetObj_StaticRoute_4

Etapa 23. Navegue até Device > Routing. Clique em View Configuration. Clique na guia Static Routing. Clique no botão + para adicionar uma nova rota estática.



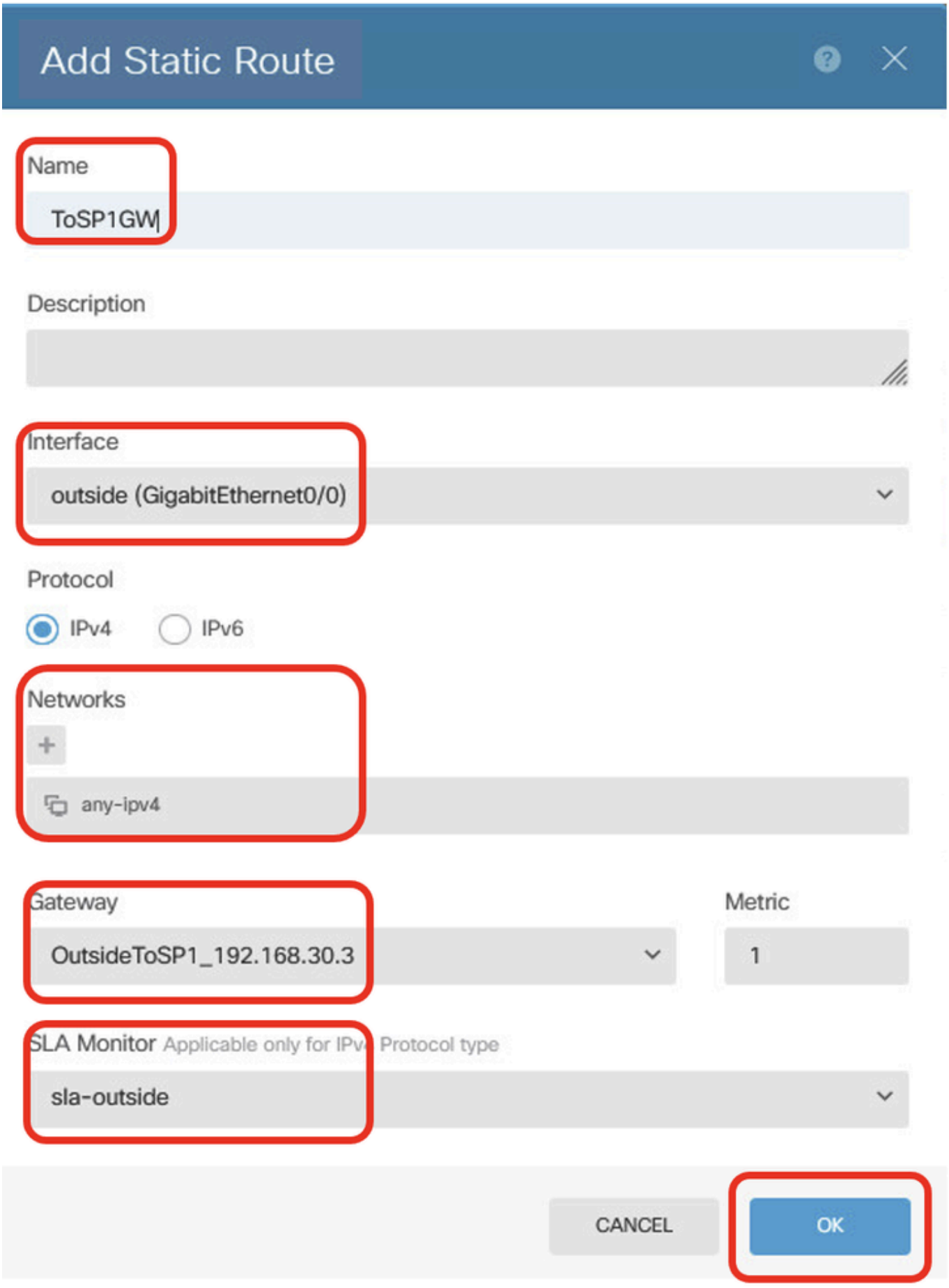
Site1FTD_View_Route_Configuration



Site1FTD_Add_Static_Route

Etapa 23.1. Criar uma rota padrão usando o gateway ISP1 com monitoramento SLA. Se o gateway do ISP1 sofrer uma interrupção, o tráfego alterna para a rota padrão de backup via ISP2. Depois que o ISP1 for recuperado, o tráfego voltará a usar o ISP1. Forneça as informações necessárias. Clique no botão OK para salvar.

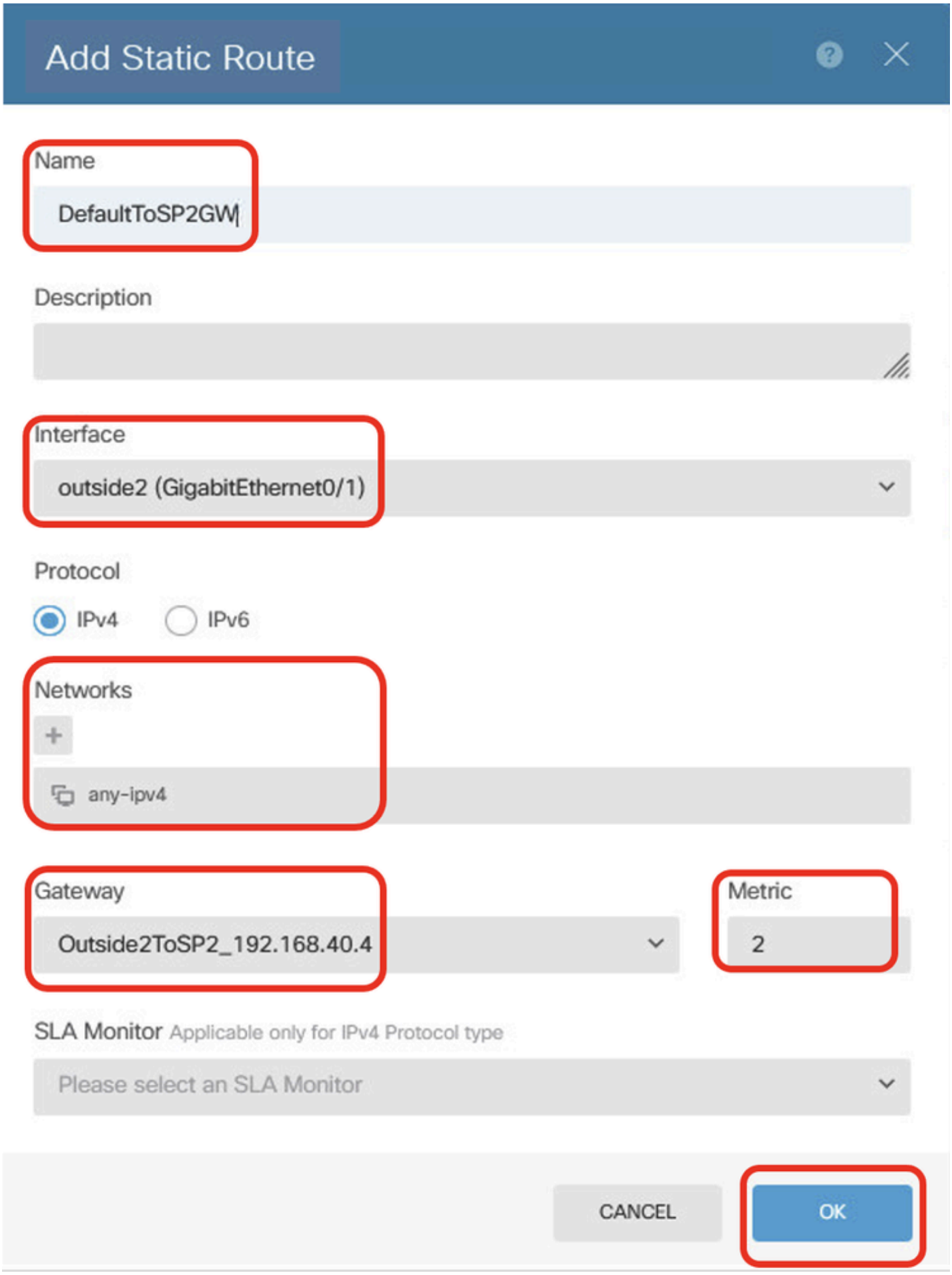
- Nome: ToSP1GW
- Interface: externo(GigabitEthernet0/0)
- Protocolo: IPv4
- Redes: any-ipv4
- Gateway: OutsideToSP1_192.168.30.3
- Métrico: 1
- Monitor do SLA: sla-outside



Site1FTD_Create_StaticRoute_1

Etapa 23.2. Criar uma rota padrão de backup através do gateway gateway ISP2. A métrica deve ser maior que 1. Neste exemplo, a métrica é 2. Forneça as informações necessárias. Clique no botão OK para salvar.

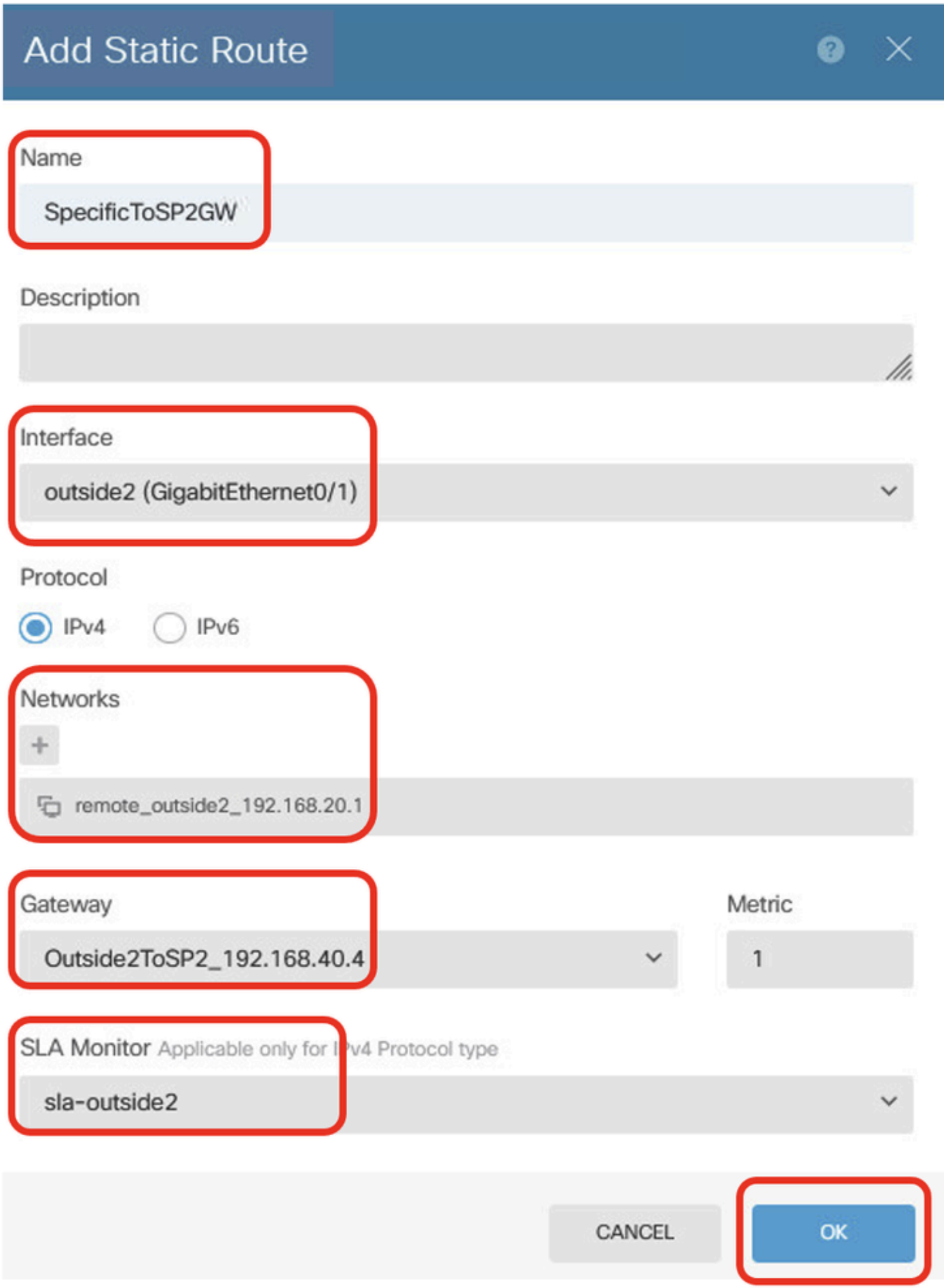
- Nome: PadrãoParaSP2GW
- Interface: outside2(GigabitEthernet0/1)
- Protocolo: IPv4
- Redes: any-ipv4
- Gateway: Outside2ToSP2_192.168.40.4
- Métrico: 2



Site1FTD_Create_StaticRoute_2

Etapa 23.3. Criar uma rota estática para o tráfego de destino para o endereço IP externo2 do FTD do Site2 par via gateway do ISP2, com monitoramento do SLA, usado para estabelecer a VPN com o 2 externo do FTD do Site2. Fornecer as informações necessárias. Clique no botão OK para salvar.

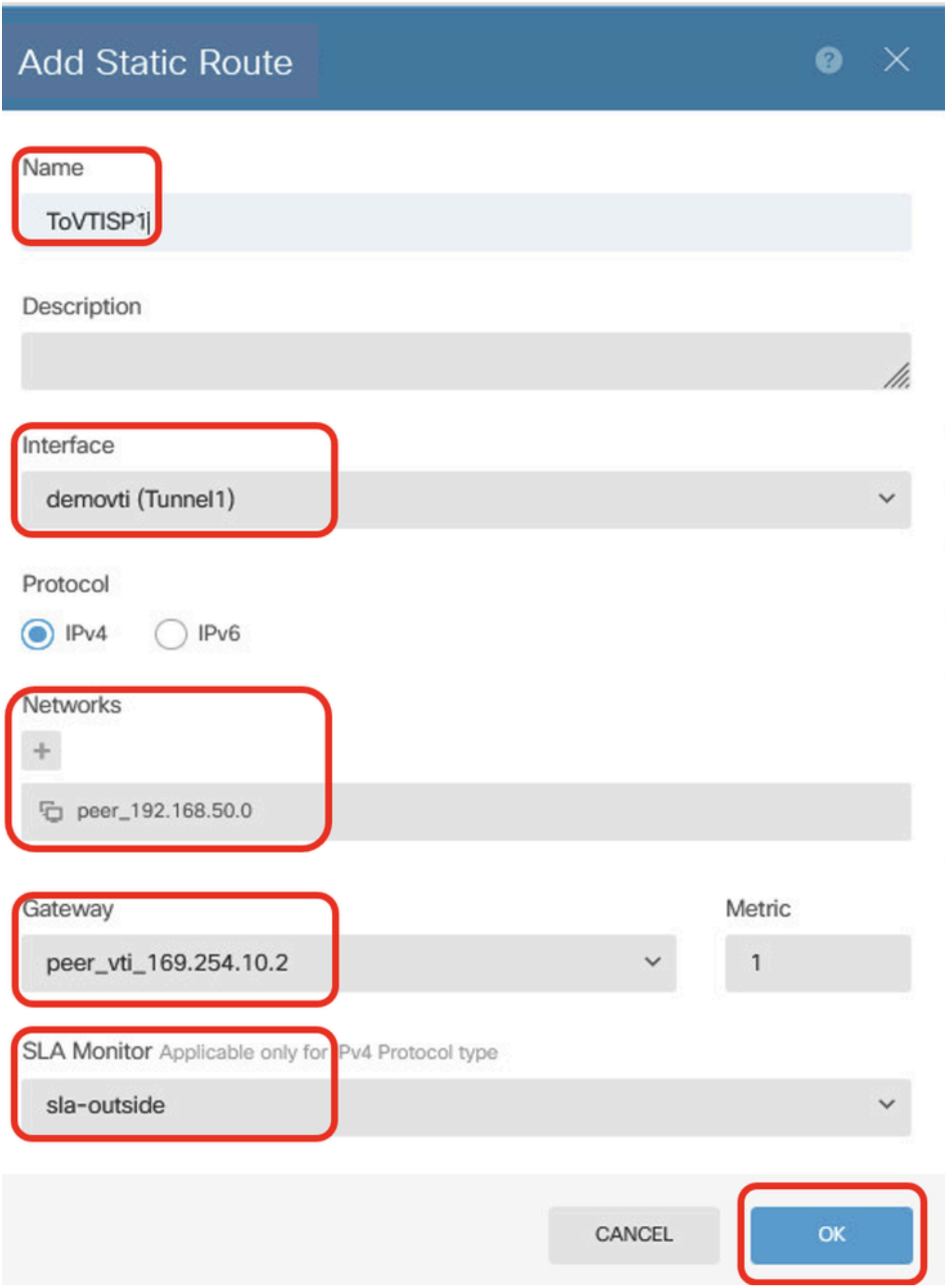
- Nome: EspecíficoParaSP2GW
- Interface: outside2(GigabitEthernet0/1)
- Protocolo: IPv4
- Redes: remote_outside2_192.168.20.1
- Gateway: Outside2ToSP2_192.168.40.4
- Métrico: 1
- Monitor do SLA: sla-outside2



Site1FTD_Create_StaticRoute_3

Etapa 23.4. Crie uma rota estática para o tráfego de destino para a rede interna do FTD do Site2 do peer através do Túnel VTI 1 do Site2 do peer como o gateway, com o monitoramento do SLA para criptografar o tráfego do cliente através do Túnel 1. Se o gateway do ISP1 experimentar uma interrupção, o tráfego de VPN alterna para o Túnel VTI 2 do ISP2. Depois que o ISP1 recuperar, o tráfego reverte para o Túnel VTI 1 do ISP1. Forneça as informações necessárias. Clique no botão OK para salvar.

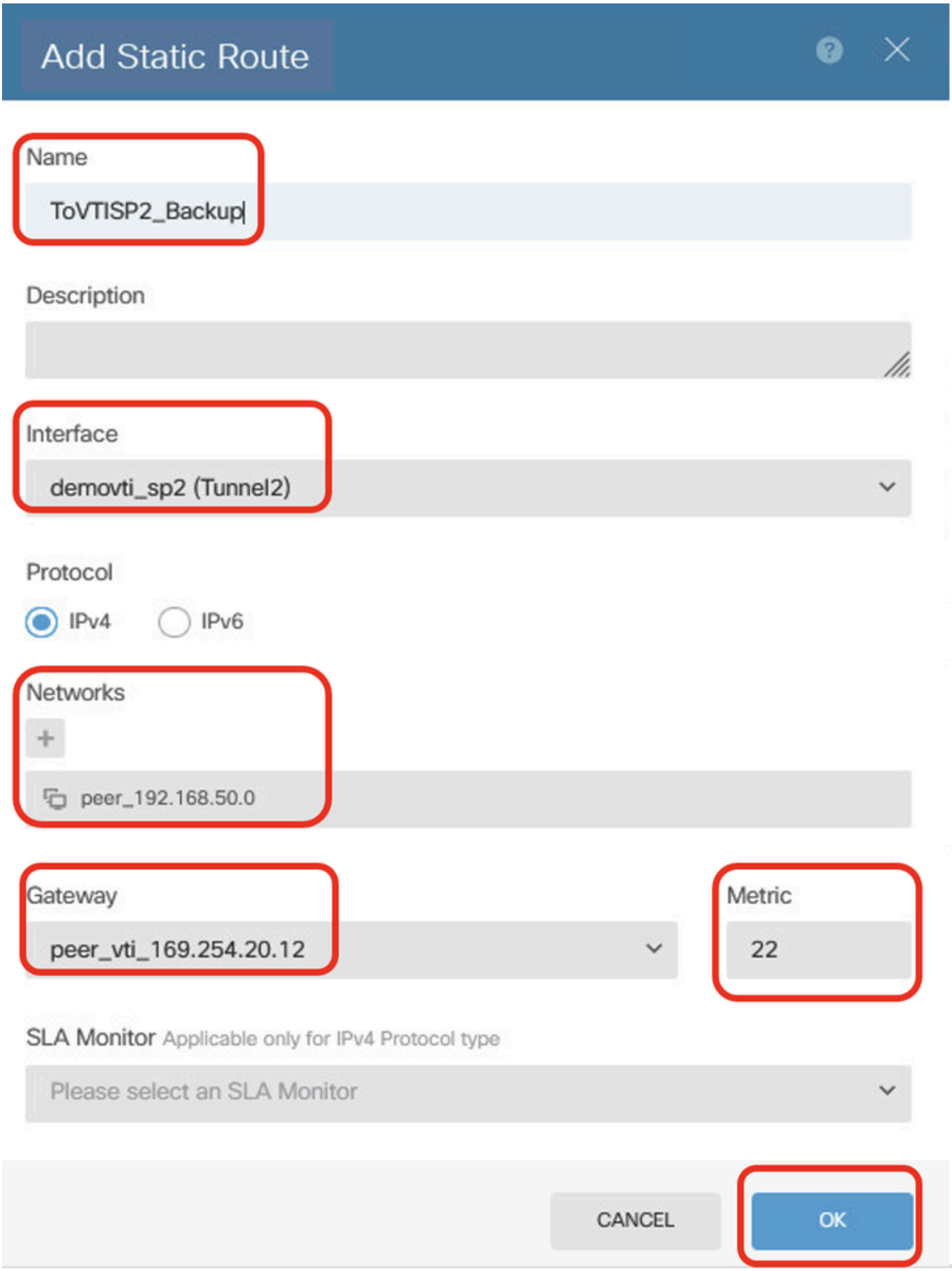
- Nome: ToVTISP1
- Interface: demovti(Tunnel1)
- Protocolo: IPv4
- Redes: peer_192.168.50.0
- Gateway: peer_vti_169.254.10.2
- Métrico: 1
- Monitor do SLA: sla-outside



Site1FTD_Create_StaticRoute_4

Etapa 23.5. Crie uma rota estática de backup para o tráfego de destino para a rede interna do FTD do Site2 par por meio do Túnel VTI 2 par do FTD do Site2 como o gateway, usado para criptografar o tráfego do cliente por meio do Túnel 2. Defina a métrica para um valor superior a 1. Neste exemplo, a métrica é 22. Forneça as informações necessárias. Clique no botão OK para salvar.

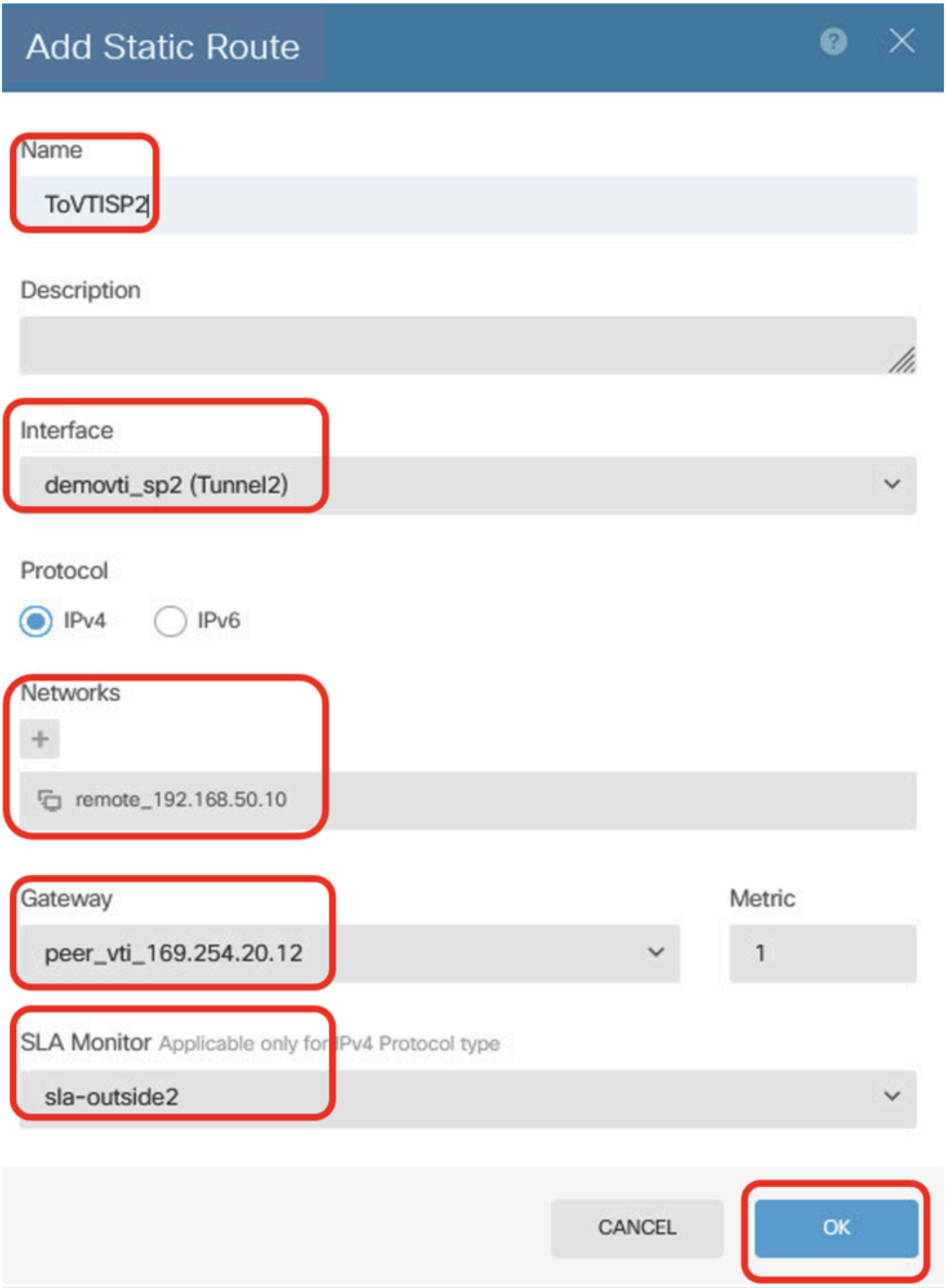
- Nome: ToVTISP2_Backup
- Interface: demovti_sp2(Tunnel2)
- Protocolo: IPv4
- Redes: peer_192.168.50.0
- Gateway: peer_vti_169.254.20.12
- Métrico: 22



Site1FTD_Create_StaticRoute_5

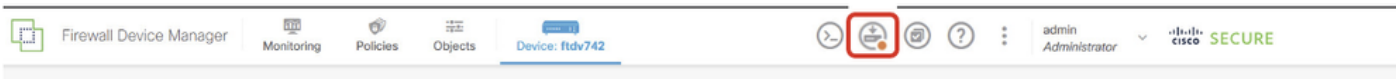
Etapa 23.6. Criar uma rota estática para o tráfego PBR. Tráfego de destino para o Site2 Client2 por meio do par VTI Tunnel 2 do Site2 FTD como gateway, com monitoramento de SLA. Forneça as informações necessárias. Clique no botão OK para salvar.

- Nome: ToVTISP2
- Interface: demovti_sp2(Tunnel2)
- Protocolo: IPv4
- Redes: remote_192.168.50.10
- Gateway: peer_vti_169.254.20.12
- Métrico: 1
- Monitor do SLA: sla-outside2



Site1FTD_Create_StaticRoute_6

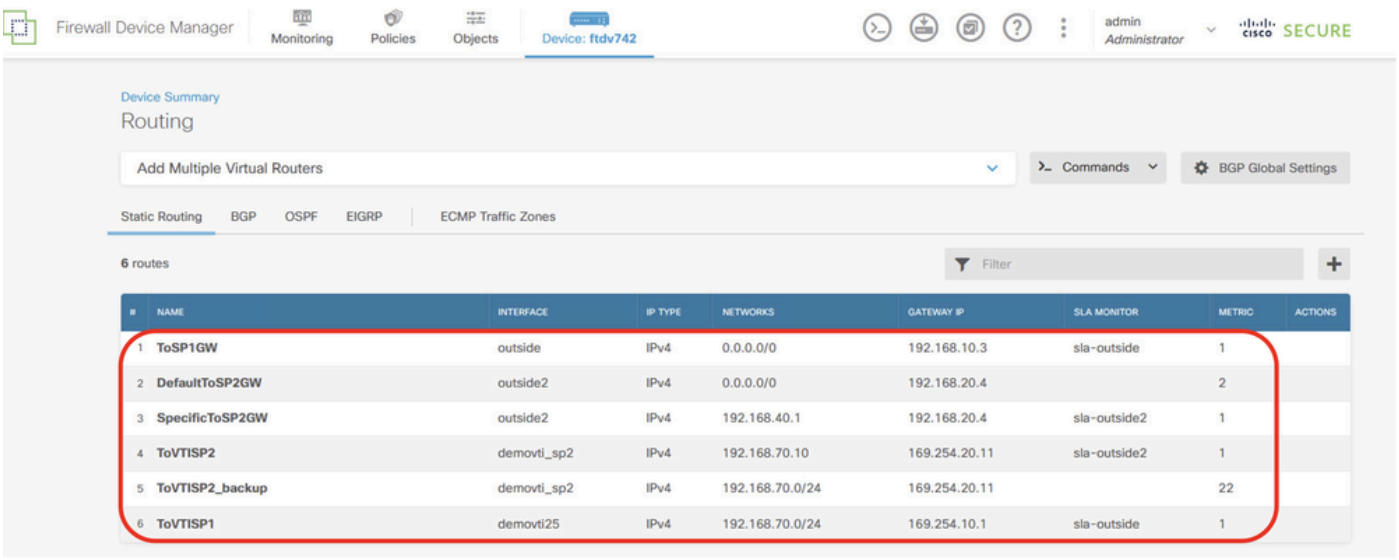
Etapa 24. Implantar as alterações de configuração.



Site1FTD_Deployment_Changes

Configuração de Rota Estática FTD do Site2

Etapa 25. Repita as Etapas 22 a 24 para criar uma rota estática com os parâmetros correspondentes para o FTD do Site2.



Site2FTD_Create_StaticRoute

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente. Navegue para a CLI do FTD do Site1 e do FTD do Site2 através do console ou do SSH.

O ISP1 e o ISP2 funcionam bem

VPN

```
//Site1 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:156, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1072332533 192.168.30.1/500                               192.168.10.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/44895 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: 0xec031247/0xc2f3f549

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1045734377 192.168.40.1/500                               192.168.20.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/77860 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: 0x47bfa607/0x82e8781d
```

```
// Site2 FTD:

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:44, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
499259237 192.168.10.1/500                               192.168.30.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/44985 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: 0xc2f3f549/0xec031247

IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
477599833 192.168.20.1/500                               192.168.40.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/77950 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: 0x82e8781d/0x47bfa607
```

Rota

```
// Site1 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
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S        192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
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
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
S        192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside




// Site2 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 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti25
L        169.254.10.2 255.255.255.255 is directly connected, demovti25
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
S        192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

Monitor de SLA

```
// Site1 FTD:
```

```
ftdv742# show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 188426425
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.40.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 855903900
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.30.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:


ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.173 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30    RTTMin: 30    RTTMax: 30
NumOfRTT: 1    RTTSum: 30    RTTSum2: 900
```

```
Entry number: 855903900
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1748
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 30
Latest operation start time: 13:44:05.178 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 30    RTTMin: 30    RTTMax: 30
NumOfRTT: 1    RTTSum: 30    RTTSum2: 900
```

// Site2 FTD:

```
ftdv742#  show sla monitor configuration
SA Agent, Infrastructure Engine-II
Entry number: 550063734
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.20.4
Interface: outside2
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

Entry number: 609724264
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.10.3
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
```

```
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

ftdv742# show sla monitor operational-state
Entry number: 550063734
Modification time: 09:05:52.864 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.916 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100

Entry number: 609724264
Modification time: 09:05:52.856 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1718
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 190
Latest operation start time: 13:42:52.921 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 190    RTTMin: 190    RTTMax: 190
NumOfRTT: 1    RTTSum: 190    RTTSum2: 36100
```

Teste de ping

Cenário 1. Site1 Client1 faça ping no Site2 Client1.

Antes do ping, verifique os contadores de show crypto ipsec sa | inc interface:|encap|decap no Site1 FTD.

Neste exemplo, Tunnel1 mostra 1497 pacotes para encapsulamento e 1498 pacotes para desencapsulamento.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
```

```
      #pkts encaps: 1497, #pkts encrypt: 1497, #pkts digest: 1497
      #pkts decaps: 1498, #pkts decrypt: 1498, #pkts verify: 1498
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
      #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 faça ping no Site2 Client1 com êxito.

```
Site1_Client1#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 = 10/97/227 ms
```

Verifique os contadores de show crypto ipsec sa | inc interface:|encap|decap no Site1 FTD após ping com êxito.

Neste exemplo, o Túnel 1 mostra 1502 pacotes para encapsulamento e 1503 pacotes para desencapsulamento, com ambos os contadores aumentando em 5 pacotes, correspondendo às 5 solicitações de eco de ping. Isso indica que os pings do Cliente1 do Site1 para o Cliente1 do Site2 são roteados via Túnel 1 do ISP1. O Túnel 2 não mostra nenhum aumento nos contadores de encapsulamento ou desencapsulamento, confirmando que não está sendo usado para esse tráfego.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1502, #pkts encrypt: 1502, #pkts digest: 1502
      #pkts decaps: 1503, #pkts decrypt: 1503, #pkts verify: 1503
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 16, #pkts encrypt: 16, #pkts digest: 16
      #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Cenário 2. Site1 Client2 faça ping no Site2 Client2.

Antes do ping, verifique os contadores de show crypto ipsec sa | inc interface:|encap|decap no Site1 FTD.

Neste exemplo, Tunnel2 mostra 21 pacotes para encapsulamento e 20 pacotes para desencapsulamento.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
      #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
      #pkts decaps: 20, #pkts decrypt: 20, #pkts verify: 20
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client2 faça ping no Site2 Client2 com êxito.

```
Site1_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 = 4/39/87 ms
```

Verifique os contadores de show crypto ipsec sa | inc interface:|encap|decap no Site1 FTD após ping com êxito.

Neste exemplo, o Túnel 2 mostra 26 pacotes para encapsulamento e 25 pacotes para desencapsulamento, com ambos os contadores aumentando em 5 pacotes, correspondendo às 5 solicitações de eco de ping. Isso indica que os pings do Site1 Client2 para o Site2 Client2 são roteados via Túnel 2 do ISP2. O Túnel 1 não mostra aumento nos contadores de encapsulamento ou desencapsulamento, confirmando que não está sendo usado para esse tráfego.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 1520, #pkts encrypt: 1520, #pkts digest: 1520
      #pkts decaps: 1521, #pkts decrypt: 1521, #pkts verify: 1521
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
interface: demovti_sp2
      #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
      #pkts decaps: 25, #pkts decrypt: 25, #pkts verify: 25
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

O ISP1 sofre uma interrupção enquanto o ISP2 funciona bem

Neste exemplo, desligue manualmente a interface E0/1 no ISP1 para simular o ISP1 que está passando por uma interrupção.

```
Internet_SP1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet_SP1(config)#
Internet_SP1(config)#interface E0/1
Internet_SP1(config-if)#shutdown
Internet_SP1(config-if)#exit
Internet_SP1(config)#
```

VPN

O Tunnel1 foi desativado. Apenas Tunnel2 está ativo com IKEV2 SA.

```
// Site1 FTD:

ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.10.1, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside    IP address: 192.168.30.1
    Destination IP address: 192.168.10.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d


ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:148, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                                 Remote
1045734377 192.168.40.1/500                                      192.168.20.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/80266 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: 0x47bfa607/0x82e8781d




// Site2 FTD:

ftdv742# show interface tunnel 1
Interface Tunnel1 "demovti25", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.10.2, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside    IP address: 192.168.10.1
    Destination IP address: 192.168.30.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d
ftdv742#

ftdv742# show crypto ikev2 sa
```

```
IKEv2 SAs:

Session-id:36, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                           Remote
477599833 192.168.20.1/500                                192.168.40.1/500                    G
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/80382 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: 0x82e8781d/0x47bfa607
```

Rota

Na tabela de roteamento, as rotas de backup entram em vigor.

```
// Site1 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 192.168.40.4 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [2/0] via 192.168.40.4, outside2
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.11 255.255.255.255 is directly connected, demovti_sp2
S        192.168.20.1 255.255.255.255 [1/0] via 192.168.40.4, outside2
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
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [22/0] via 169.254.20.12, demovti_sp2
S        192.168.50.10 255.255.255.255 [1/0] via 169.254.20.12, demovti_sp2
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside



// Site2 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 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.20.0 255.255.255.0 is directly connected, demovti_sp2
L        169.254.20.12 255.255.255.255 is directly connected, demovti_sp2
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [22/0] via 169.254.20.11, demovti_sp2
S        192.168.70.10 255.255.255.255 [1/0] via 169.254.20.11, demovti_sp2
```

Monitor de SLA

No FTD do Site1, o monitor do SLA mostra o número de entrada 855903900 o tempo limite (o endereço de destino é 192.168.30.3) para o ISP1.

```
// Site1 FTD:

ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.131 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 100
Latest operation start time: 14:22:05.132 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 100    RTTMin: 100    RTTMax: 100
NumOfRTT: 1    RTTSum: 100    RTTSum2: 10000

Entry number: 855903900
Modification time: 08:37:05.132 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1786
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:22:05.134 UTC Thu Aug 15 2024
Latest operation return code: Timeout
```

```
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0

ftdv742# show track
Track 1
  Response Time Reporter 855903900 reachability
  Reachability is Down
  7 changes, last change 00:11:03
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
Track 2
  Response Time Reporter 188426425 reachability
  Reachability is Up
  4 changes, last change 13:15:11
  Latest operation return code: OK
  Latest RTT (millisecs) 140
  Tracked by:
    STATIC-IP-ROUTING 0
```

Teste de ping

Antes do ping, verifique os contadores de show crypto ipsec sa | inc interface:|encap|decap no Site1 FTD.

Neste exemplo, Tunnel2 mostra 36 pacotes para encapsulamento e 35 pacotes para desencapsulamento.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
      #pkts encaps: 36, #pkts encrypt: 36, #pkts digest: 36
      #pkts decaps: 35, #pkts decrypt: 35, #pkts verify: 35
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 faça ping no Site2 Client1 com êxito.

```
Site1_Client1#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 = 22/133/253 ms
```

Site1 Client2 faça ping no Site2 Client2 com êxito.

```
Site1_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 = 34/56/87 ms
```

Verifique os contadores de show crypto ipsec sa | inc interface:|encap|decap no Site1 FTD após ping com êxito.

Neste exemplo, o Túnel 2 mostra 46 pacotes para encapsulamento e 45 pacotes para desencapsulamento, com ambos os contadores aumentando em 10 pacotes, correspondendo às 10 solicitações de eco de ping. Isso indica que os pacotes de ping são roteados via Túnel 2 do ISP2.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti_sp2
      #pkts encaps: 46, #pkts encrypt: 46, #pkts digest: 46
      #pkts decaps: 45, #pkts decrypt: 45, #pkts verify: 45
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

O ISP2 sofre uma interrupção enquanto o ISP1 funciona bem

Neste exemplo, desligue manualmente a interface E0/1 no ISP2 para simular o ISP2 que está passando por uma interrupção.

```
Internet_SP2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet_SP2(config)#
Internet_SP2(config)#int e0/1
Internet_SP2(config-if)#shutdown
Internet_SP2(config-if)#^Z
Internet_SP2#
```

VPN

O Tunnel2 foi desativado. Apenas Tunnel1 está ativo com IKEV2 SA.

```
// Site1 FTD:

ftdv742# show interface tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.20.11, subnet mask 255.255.255.0
```

```
  Tunnel Interface Information:
    Source interface: outside2    IP address: 192.168.40.1
    Destination IP address: 192.168.20.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:159, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1375077093 192.168.30.1/500                               192.168.10.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/349 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: 0x40f407b4/0x26598bcc




// Site2 FTD:

ftdv742# show int tunnel 2
Interface Tunnel2 "demovti_sp2", is down, line protocol is down
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
    IP address 169.254.20.12, subnet mask 255.255.255.0
  Tunnel Interface Information:
    Source interface: outside2    IP address: 192.168.20.1
    Destination IP address: 192.168.40.1
    IPsec MTU Overhead : 0
    Mode: ipsec ipv4    IPsec profile: ipsec_profile|e4084d322d

ftdv742# show crypto ikev2 sa

IKEv2 SAs:

Session-id:165, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                          Remote
1025640731 192.168.10.1/500                               192.168.30.1/500
      Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/379 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: 0x26598bcc/0x40f407b4
```

Rota

Na tabela de roteamento, a rota relacionada ao ISP2 desapareceu para o tráfego PBR.

```
// Site1 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
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
C        192.168.40.0 255.255.255.0 is directly connected, outside2
L        192.168.40.1 255.255.255.255 is directly connected, outside2
S        192.168.50.0 255.255.255.0 [1/0] via 169.254.10.2, demovti
C        192.168.70.0 255.255.255.0 is directly connected, inside
L        192.168.70.1 255.255.255.255 is directly connected, inside



// Site2 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 192.168.10.3 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 192.168.10.3, outside
C        169.254.10.0 255.255.255.0 is directly connected, demovti25
L        169.254.10.2 255.255.255.255 is directly connected, demovti25
C        192.168.10.0 255.255.255.0 is directly connected, outside
L        192.168.10.1 255.255.255.255 is directly connected, outside
C        192.168.20.0 255.255.255.0 is directly connected, outside2
L        192.168.20.1 255.255.255.255 is directly connected, outside2
S        192.168.40.1 255.255.255.255 [1/0] via 192.168.20.4, outside2
C        192.168.50.0 255.255.255.0 is directly connected, inside
L        192.168.50.1 255.255.255.255 is directly connected, inside
S        192.168.70.0 255.255.255.0 [1/0] via 169.254.10.1, demovti25
```

Monitor de SLA

No FTD do Site1, o monitor do SLA mostra o número de entrada 188426425 o tempo limite (o endereço de destino é 192.168.40.4) para o ISP2.

```
// Site1 FTD:
```

```
ftdv742# show sla monitor operational-state
Entry number: 188426425
Modification time: 08:37:05.133 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 14:52:05.174 UTC Thu Aug 15 2024
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0    RTTMin: 0    RTTMax: 0
NumOfRTT: 0    RTTSum: 0    RTTSum2: 0

Entry number: 855903900
Modification time: 08:37:05.135 UTC Wed Aug 14 2024
Number of Octets Used by this Entry: 2056
Number of operations attempted: 1816
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 10
Latest operation start time: 14:52:05.177 UTC Thu Aug 15 2024
Latest operation return code: OK
RTT Values:
RTTAvg: 10    RTTMin: 10    RTTMax: 10
NumOfRTT: 1    RTTSum: 10    RTTSum2: 100


ftdv742#  show track
Track 1
  Response Time Reporter 855903900 reachability
  Reachability is Up
  8 changes, last change 00:14:37
  Latest operation return code: OK
  Latest RTT (millisecs) 60
  Tracked by:
    STATIC-IP-ROUTING 0
Track 2
  Response Time Reporter 188426425 reachability
  Reachability is Down
  5 changes, last change 00:09:30
  Latest operation return code: Timeout
  Tracked by:
    STATIC-IP-ROUTING 0
```

Teste de ping

Antes do ping, verifique os contadores de show crypto ipsec sa | inc interface:|encap|decap no Site1 FTD.

Neste exemplo, o Túnel 1 mostra 74 pacotes para encapsulamento e 73 pacotes para desencapsulamento.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 74, #pkts encrypt: 74, #pkts digest: 74
      #pkts decaps: 73, #pkts decrypt: 73, #pkts verify: 73
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

Site1 Client1 faça ping no Site2 Client1 com êxito.

```
Site1_Client1#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 = 30/158/255 ms
```

Site1 Client2 faça ping no Site2 Client2 com êxito.

```
Site1_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 = 6/58/143 ms
```

Verifique os contadores de show crypto ipsec sa | inc interface:|encap|decap no Site1 FTD após ping com êxito.

Neste exemplo, o Túnel 1 mostra 84 pacotes para encapsulamento e 83 pacotes para desencapsulamento, com ambos os contadores aumentando em 10 pacotes, correspondendo às 10 solicitações de eco de ping. Isso indica que os pacotes de ping são roteados através do túnel 1 do ISP1.

```
// Site1 FTD:

ftdv742# show crypto ipsec sa | inc interface:|encap|decap
interface: demovti
      #pkts encaps: 84, #pkts encrypt: 84, #pkts digest: 84
```

```
      #pkts decaps: 83, #pkts decrypt: 83, #pkts verify: 83
      #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 PBR.

```
debug policy-route
```

Você pode usar esses comandos de depuração para solucionar problemas da seção Monitor do SLA.

```
ftdv742# debug sla monitor ?
  error  Output IP SLA Monitor Error Messages
  trace  Output IP SLA Monitor Trace Messages
```

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.