Configure o acesso seguro com FTD seguro e ASA para acesso privado com NAT

Contents

Introdução

Este documento descreve como configurar o Grupo de Túnel de Rede de Acesso Seguro com Tradução de Endereço de Rede.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Firewall Management Center
- Defesa contra ameaças do Cisco Secure Firewall
- Acesso seguro da Cisco

- Cisco Adaptive Security Appliance
- Tradução de Endereço de Rede
- Roteamento baseado em políticas
- Capturas de pacotes no firewall

Componentes Utilizados

As informações neste documento são baseadas em:

- Cisco Firewall Management Center 7.10
- Cisco Secure Firewall Threat Defense 7.10
- Acesso seguro da Cisco
- Cisco Adaptive Security Appliance 9.22
- Roteadores Cisco

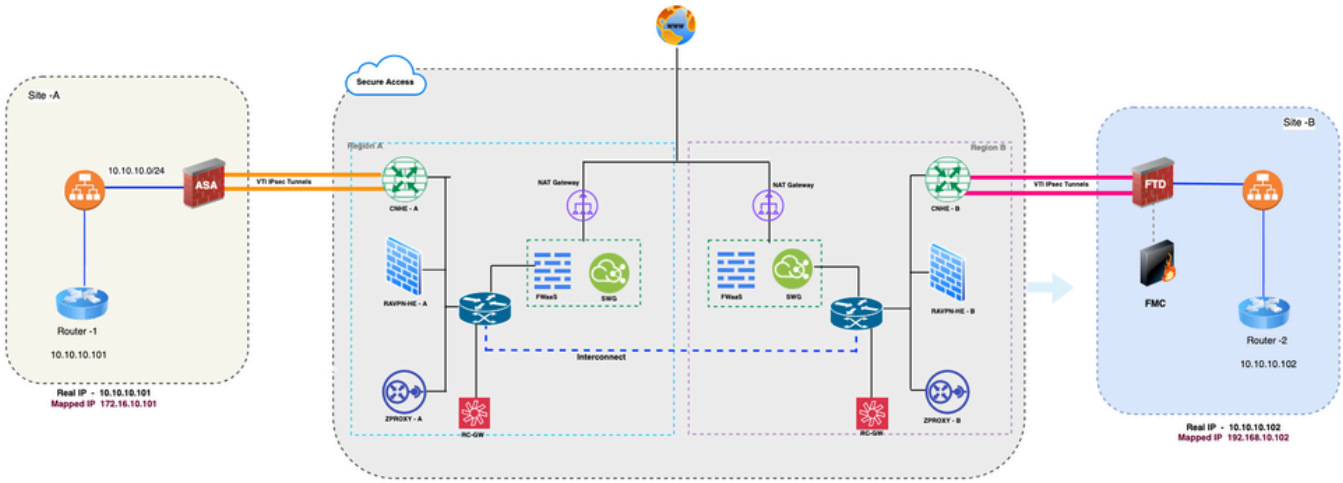
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

Informações de Apoio

O Cisco Secure Access oferece recursos de Secure Service Edge nativos da nuvem, incluindo Secure Internet Access (SIA) e Secure Private Access (SPA). Para empresas que estendem o acesso de aplicativos privados a usuários remotos sem fazer backhaul de todo o tráfego por meio de um data center, o Secure Access usa os Network Tunnel Groups (NTGs) IPsec para criar túneis criptografados entre dispositivos de rede locais — como o Cisco Firewall Threat Defense (FTD), o Adaptive Security Appliance (ASA) — e os Cisco Secure Access Cloud Points-of-Presence (PoPs).

Este documento detalha como estabelecer um túnel IPsec baseado em rota usando IKEv2 entre o Cisco FTD , ASA e o Cisco Secure Access, habilitando o Network Address Translation (NAT) no Secure Access e o Policy-Based Routing (PBR) no FTD e no ASA para orientar somente o tráfego de acesso privado no túnel.

Diagrama de Rede



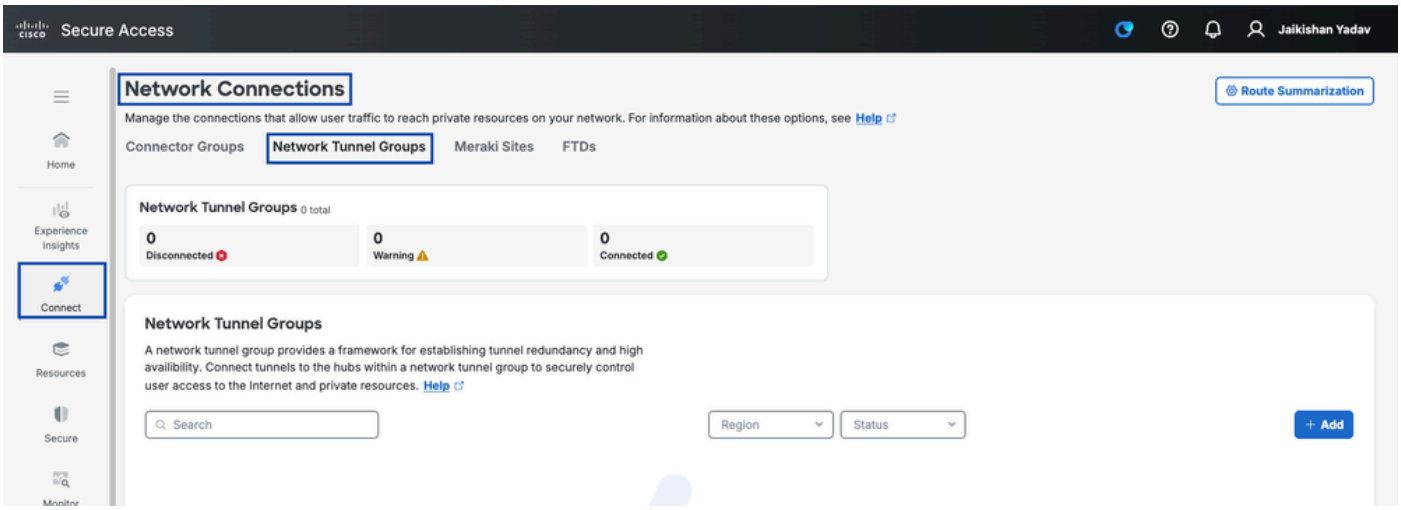
Topologia de rede

Configurar

Secure Access e Secure Firewall Thread Defense - VPN dinâmica (BGP) baseada em rota com PBR

Configurar o grupo de túneis de rede no acesso seguro

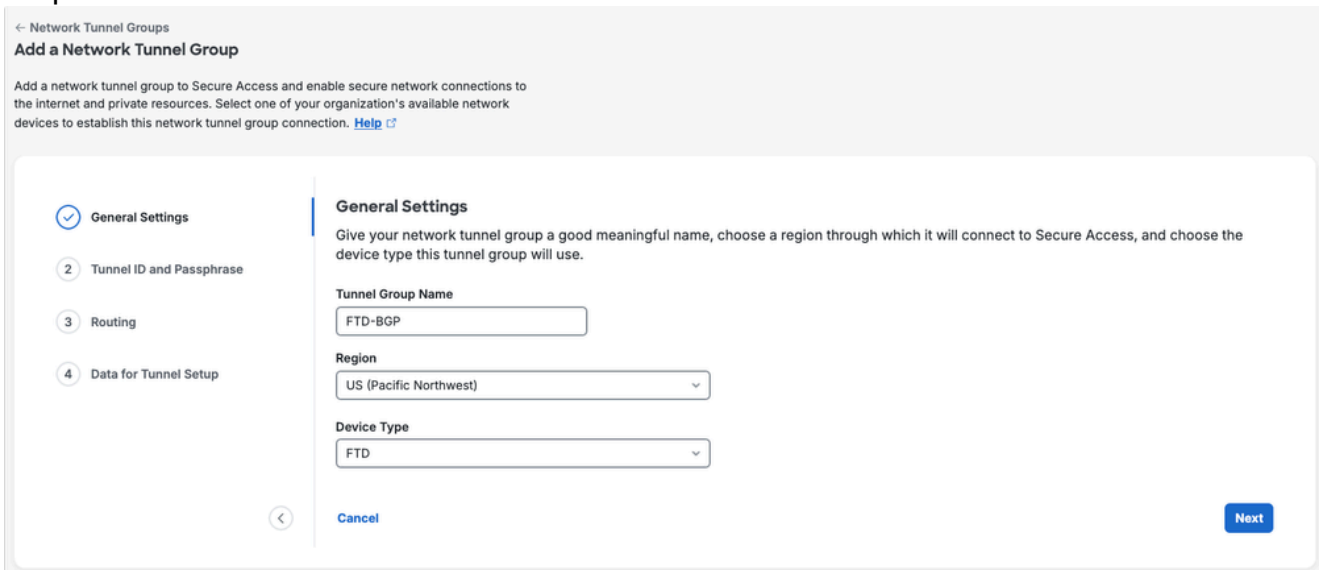
1. Faça login no painel de acesso seguro Acesso seguro
2. Navegue para Connect > Network Connections > Network Tunnel Groups e clique em +Add para configurar o Network Tunnel Group



Acesso seguro - Grupos de túnel de rede

3. Configurar Grupo de Túneis de Rede - Definições Gerais

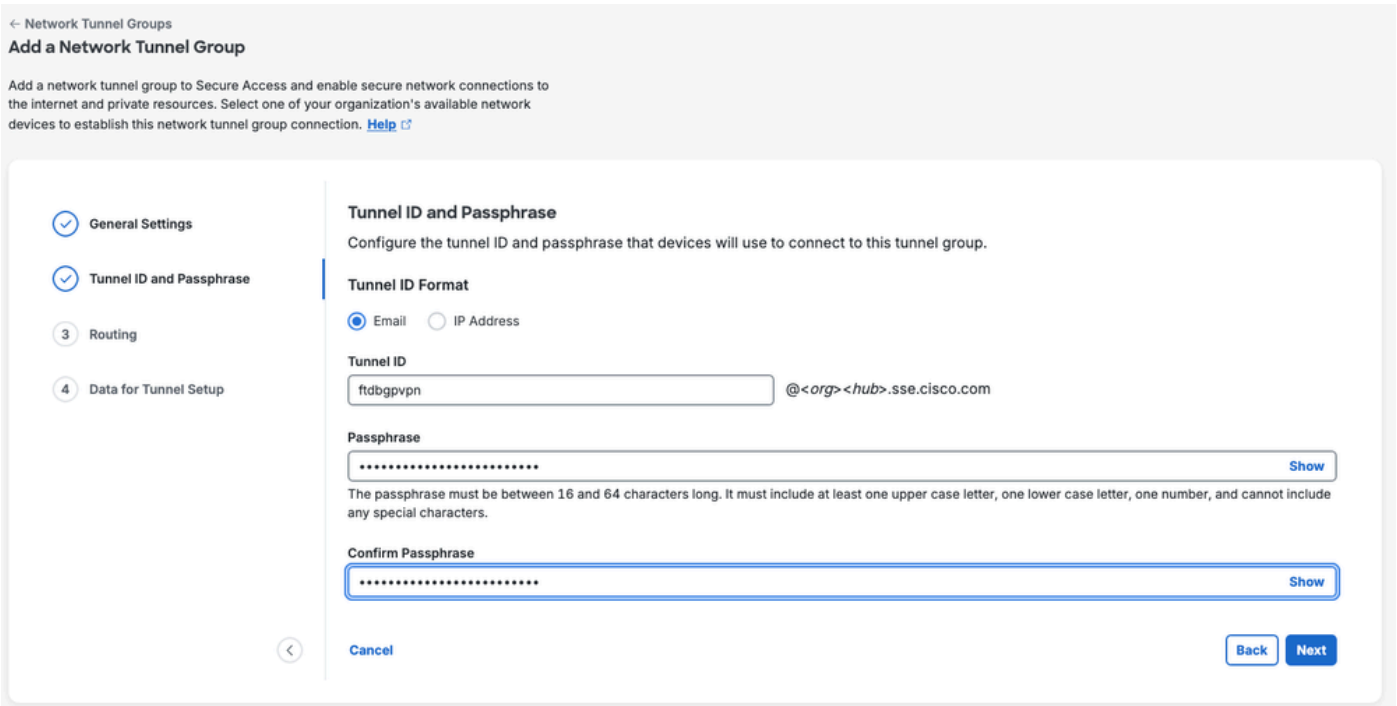
- Configure o nome do grupo de túneis, a região e o tipo de dispositivo
- Clique em Next



Acesso seguro - Configurações gerais dos grupos de túneis de rede

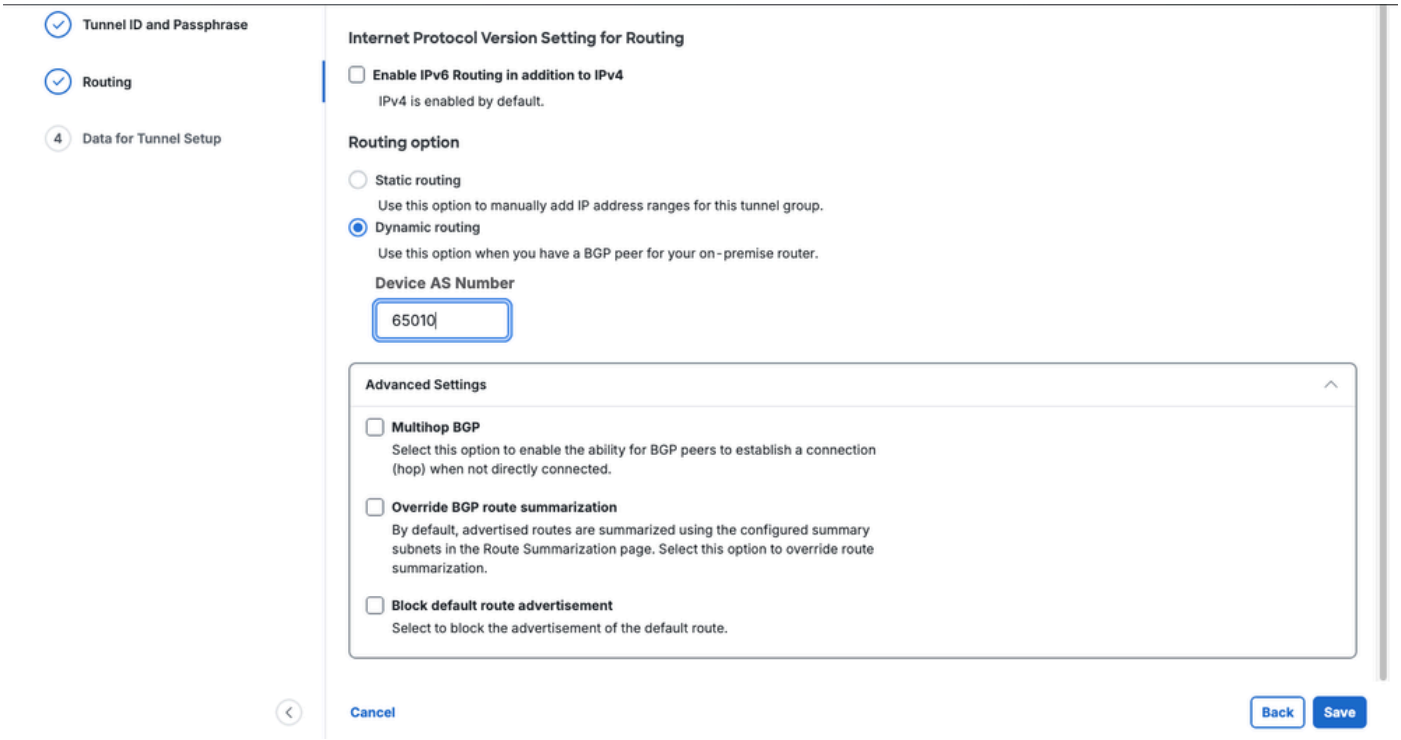
4. Configure Tunnel ID e Passphrase.

- Configure a ID do túnel e a senha.
- Clique em Avançar



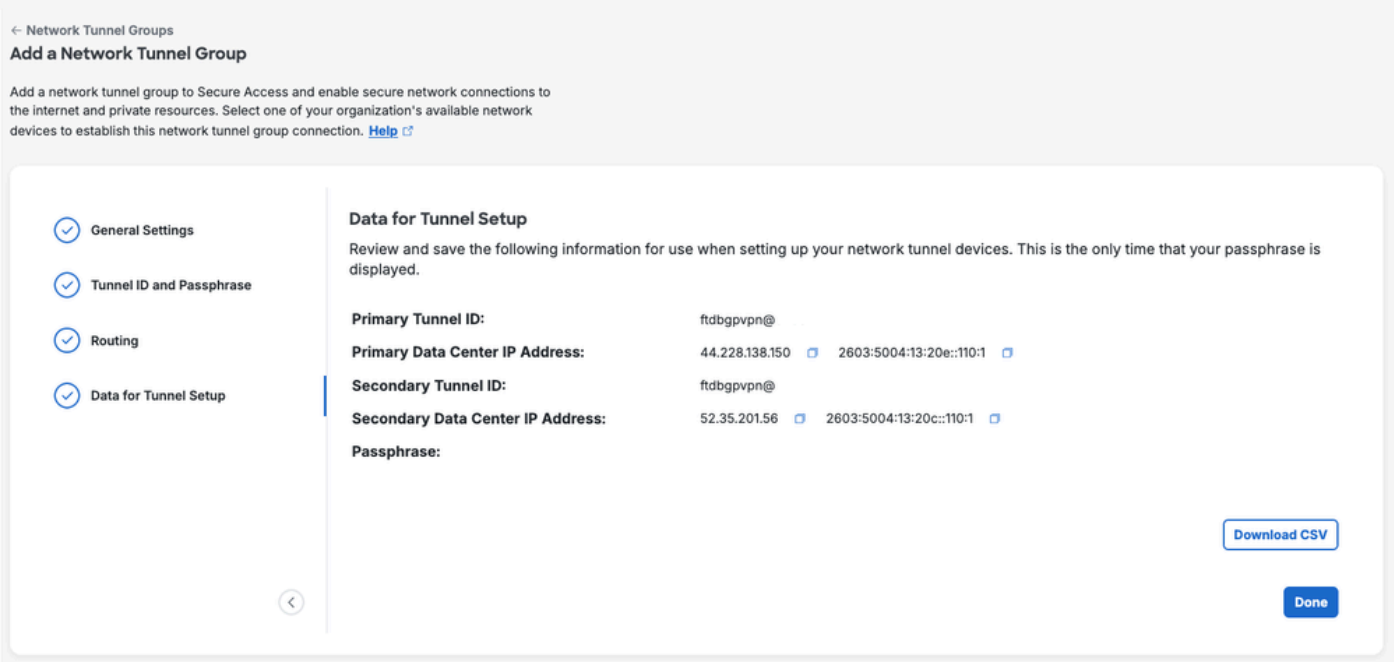
5. Configurar o Roteamento

- Configurar número AS do dispositivo
- Clique em Salvar



Acesso seguro - Roteamento de grupos de túnel de rede

6. Salvar Configuração do Grupo de Túneis de Rede



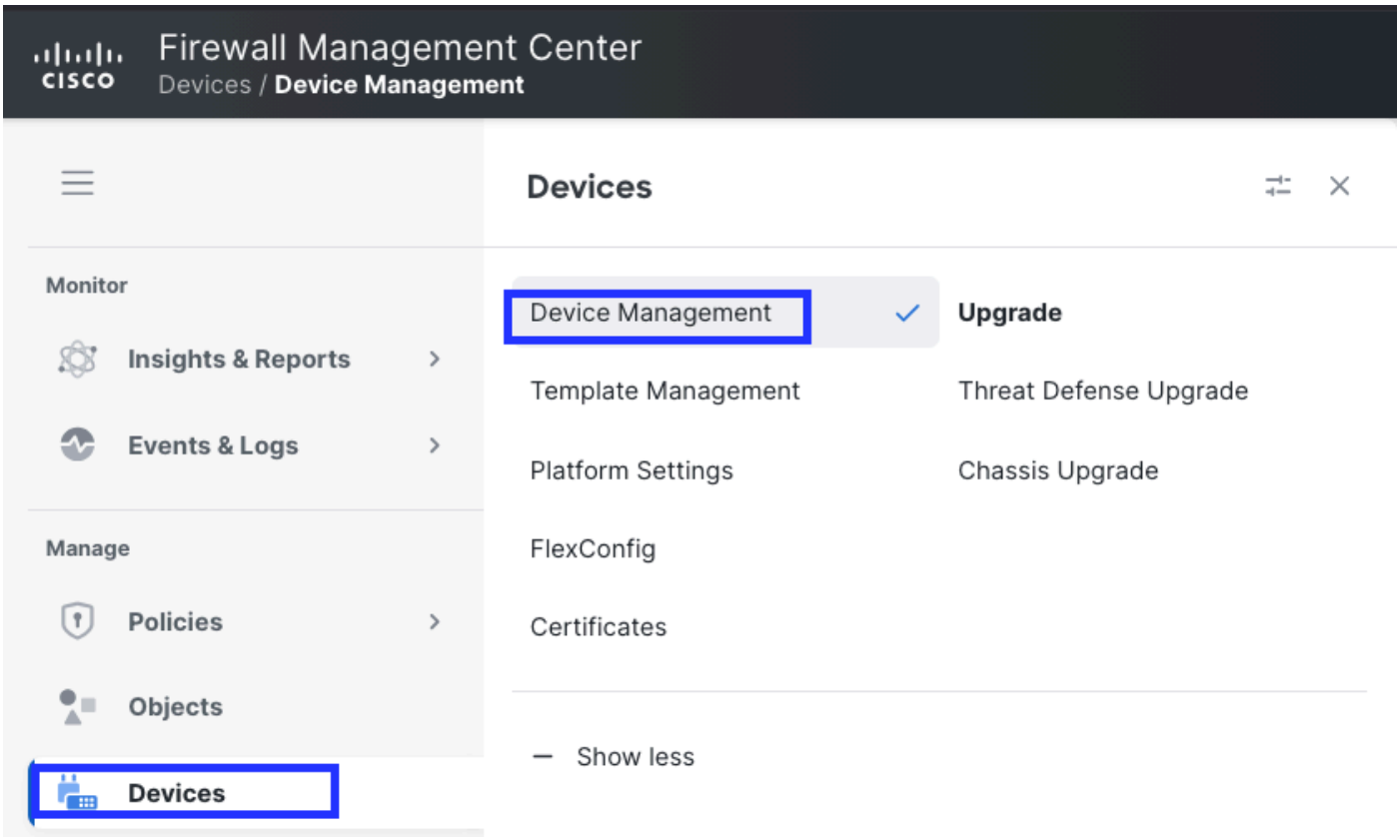
Acesso seguro - Grupos de túnel de rede

Configurar a VPN IPsec baseada em rota dinâmica no Secure Firewall Threat Defense (FTD) com PBR

1. Faça login no Centro de gerenciamento de firewall (FMC)

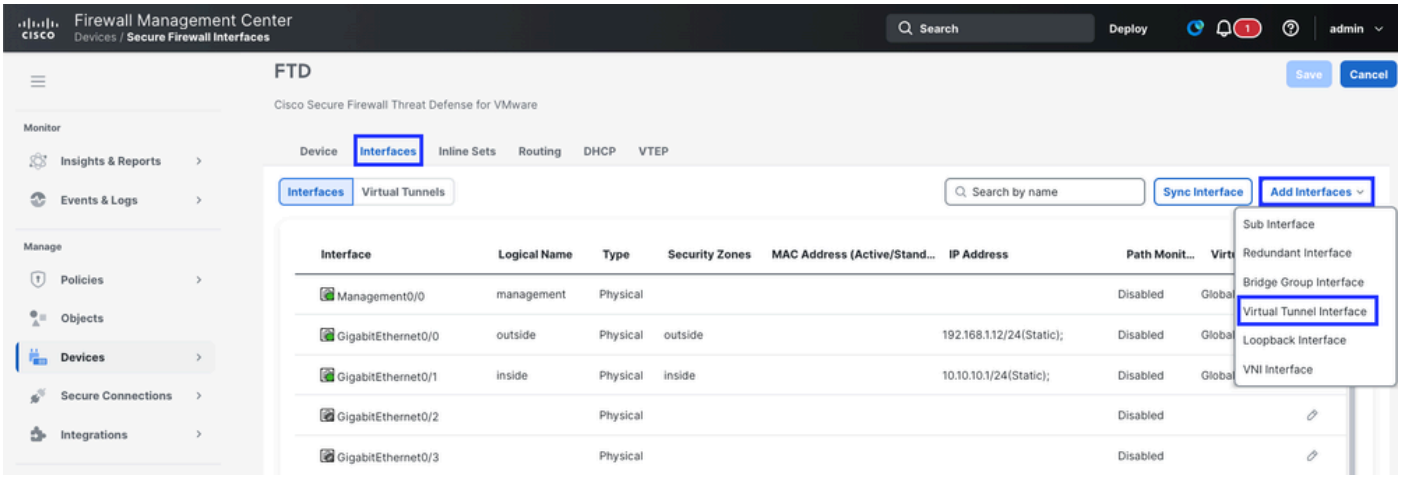
2. Configurar o Virtual Tunnel Interface VTI

- Navegue até Dispositivos > Gerenciamento de dispositivos



Gerenciamento seguro de firewall - Painel

- Clique no ícone do Lápis ao lado do dispositivo e navegue até a seção Interface
- Clique em Add interfaces e selecione Virtual Tunnel Interface



Gerenciamento seguro de firewall - Configuração de FTD VTI

- Configurar VTI

Add Virtual Tunnel Interface

General | Path Monitoring

Tunnel Type

(•) Static ( ) Dynamic

Name:*

VTI-1

[x] Enabled

Description:

Virtual Tunnel interface for Primary VTI VPN

Security Zone:

vti

Priority:

0 *(0 - 65535)*

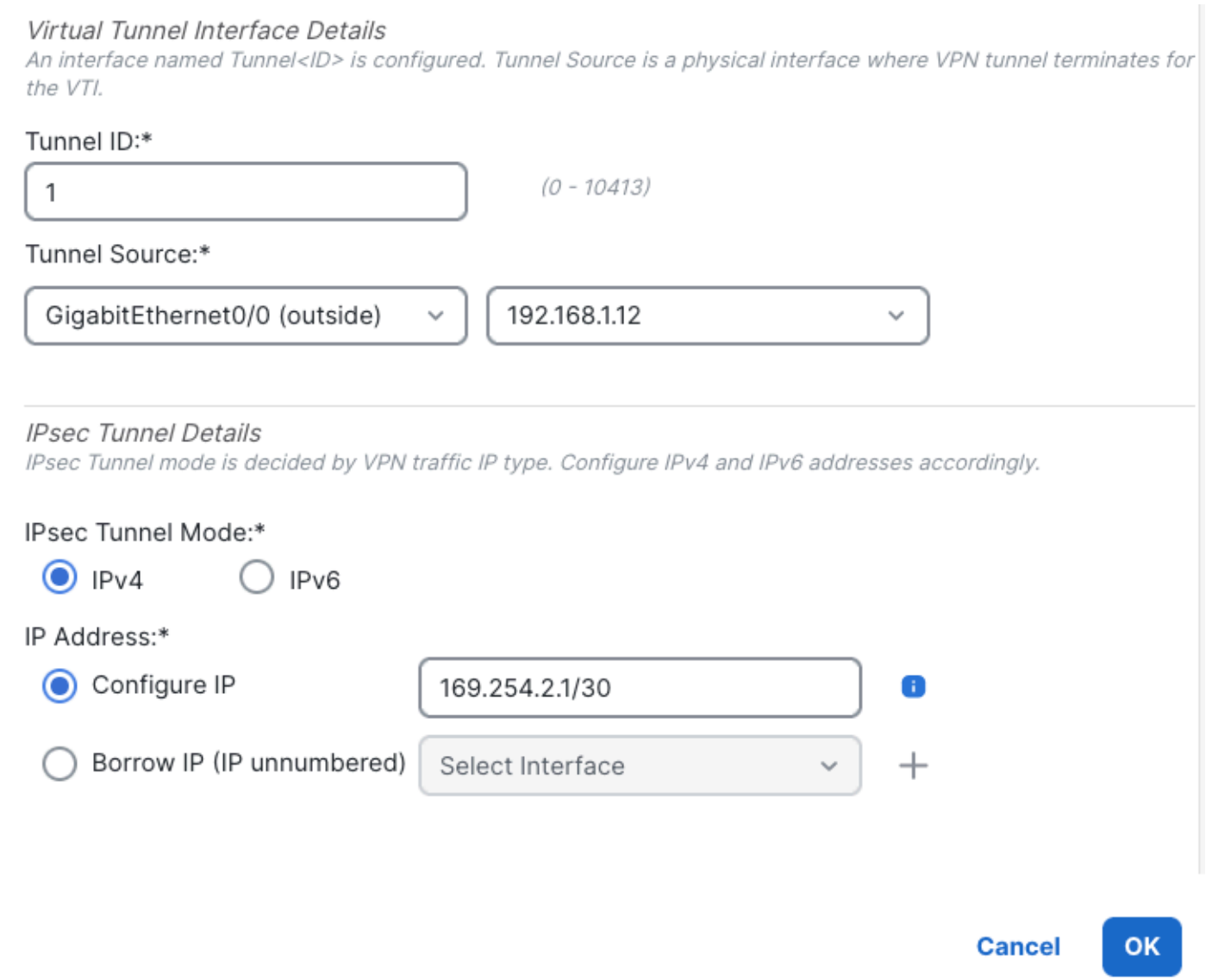
Propagate Security Group Tag: [x]

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

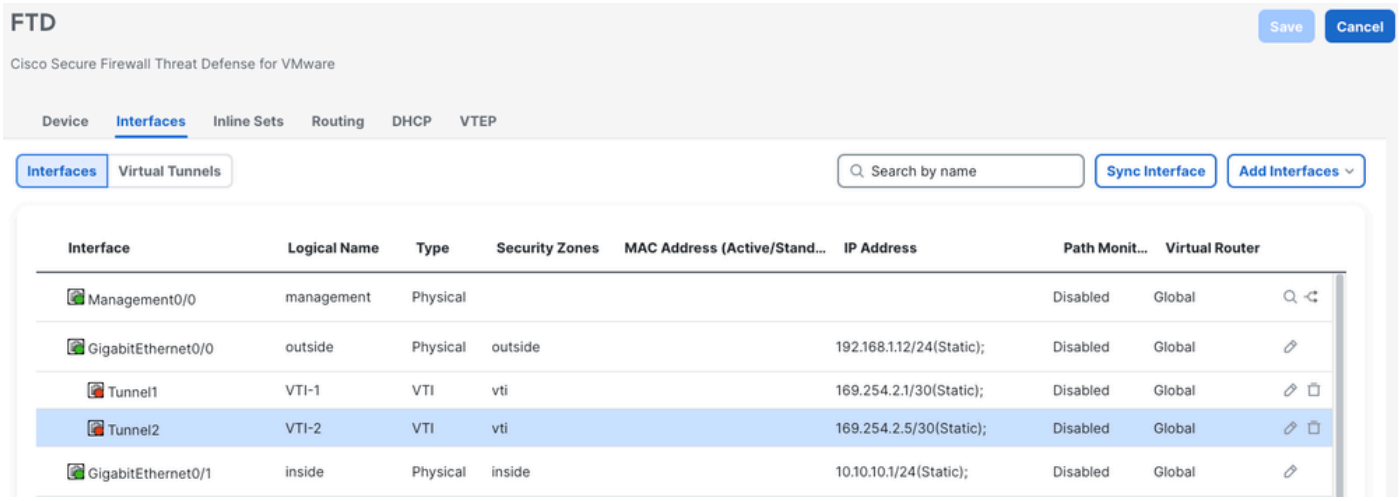
Tunnel ID:*

1 *(0 - 10413)*

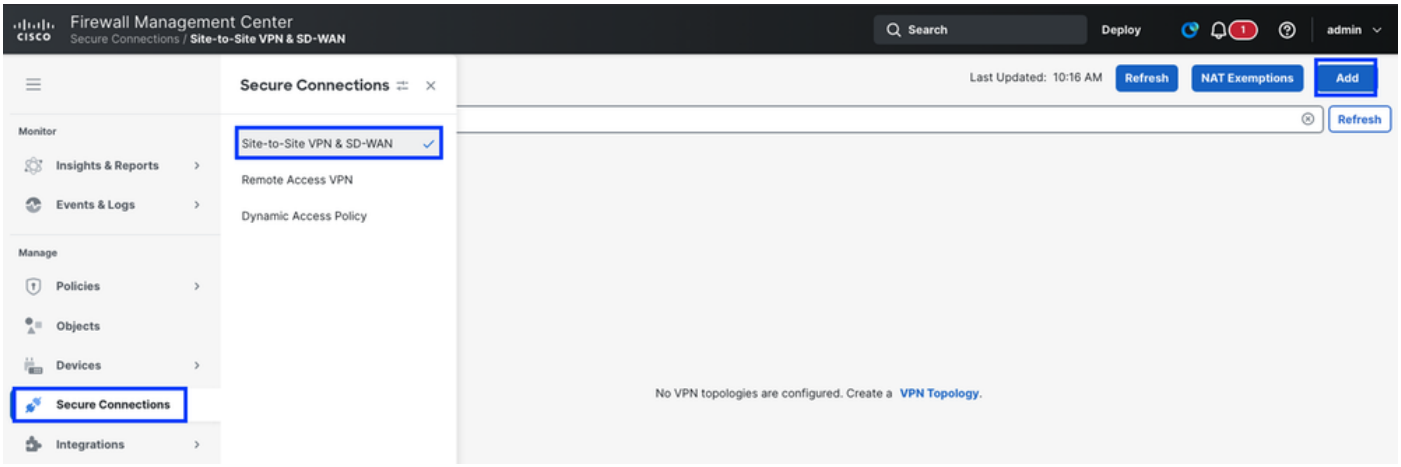


Gerenciamento seguro de firewall - Configuração de FTD VTI

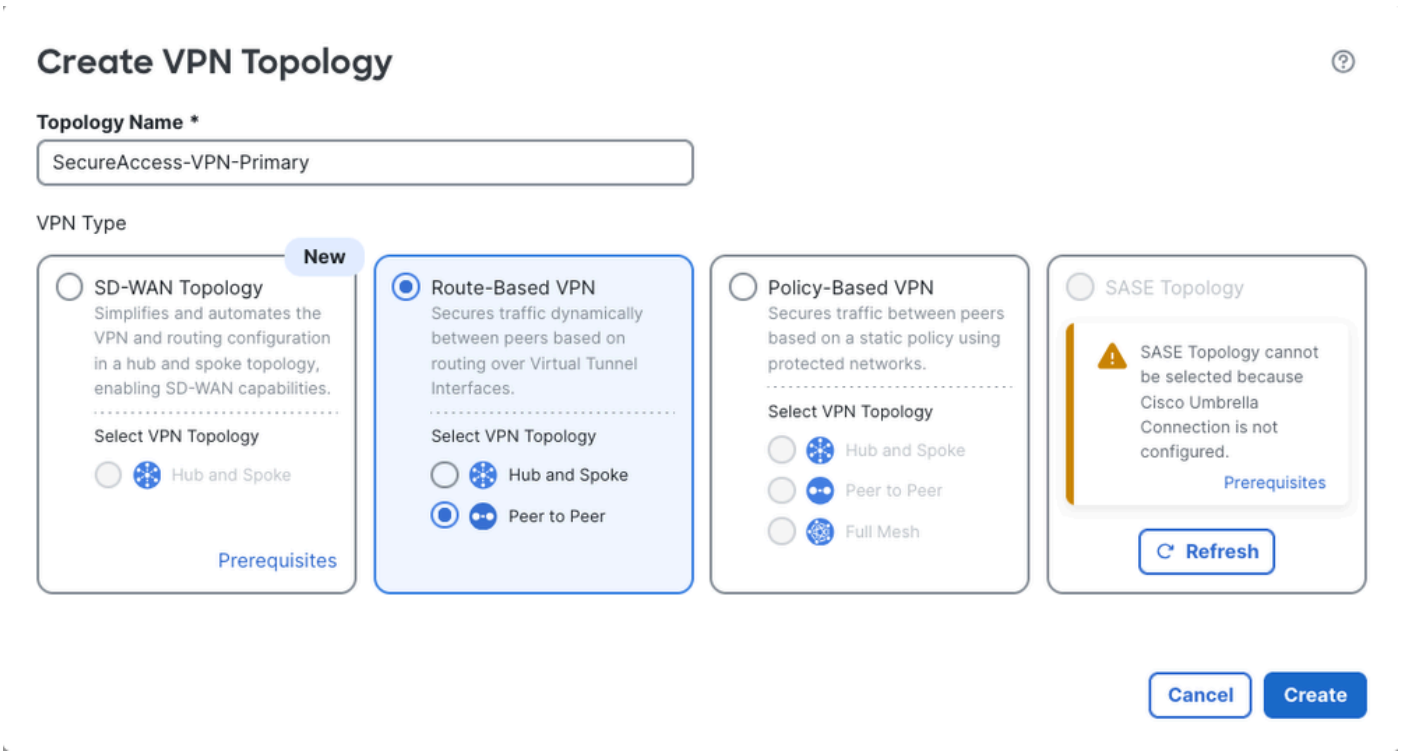
- Configurar VTI-2 também para VPN IPsec secundária com acesso seguro



3. Navegue para Conexões Seguras > VPN Site a Site e SD-WAN e clique em Adicionar para configurar a VPN



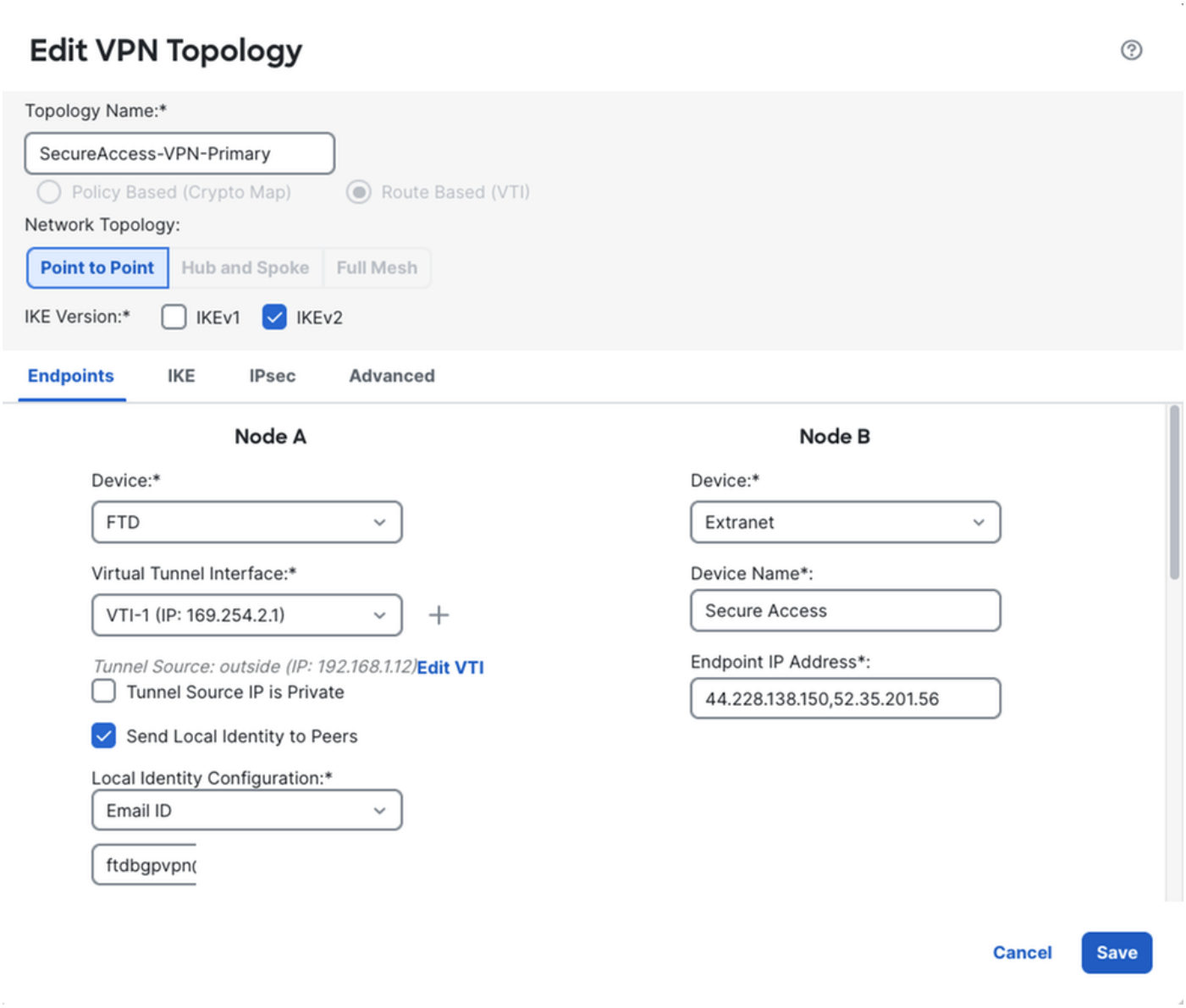
- Criar topologia de VPN



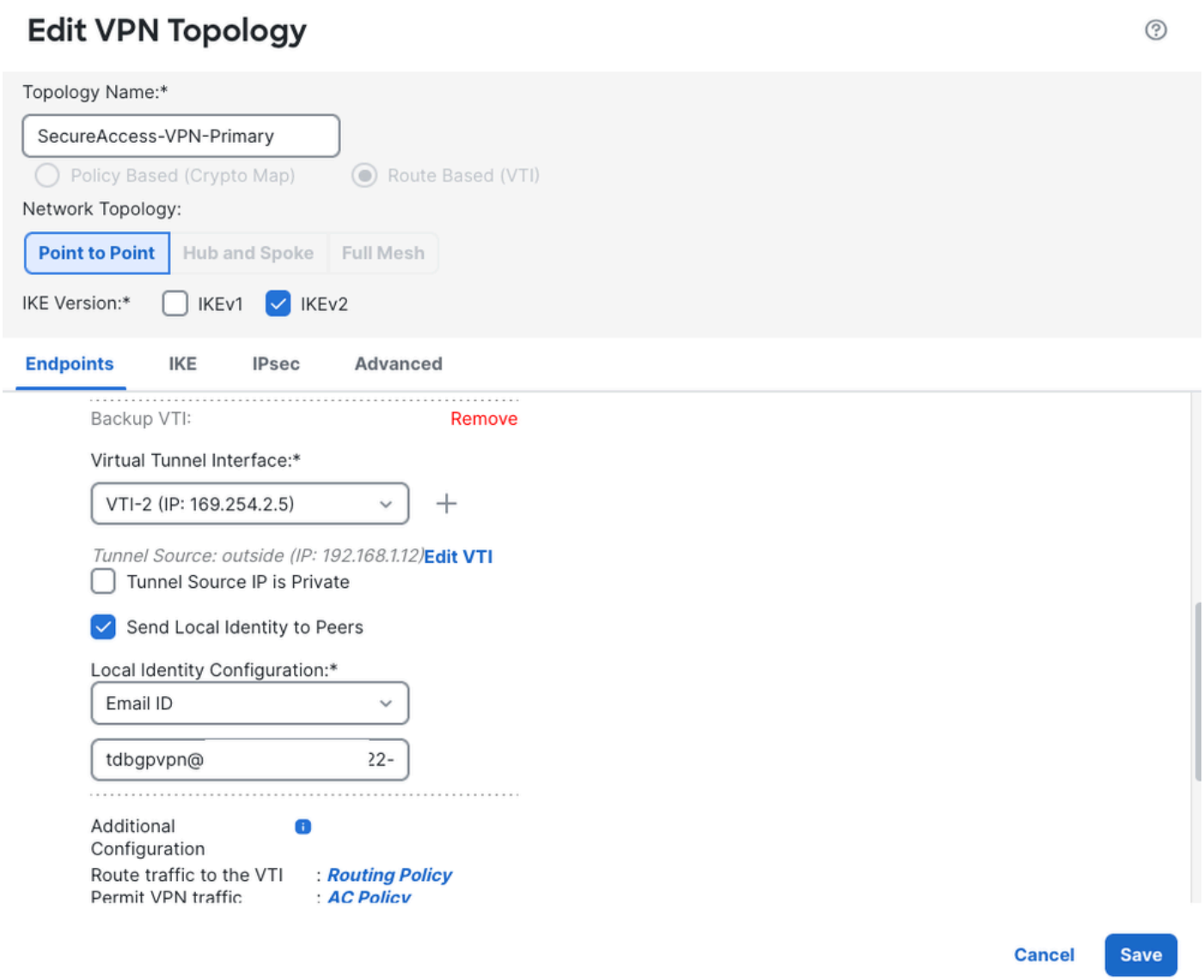
- Na etapa 6 do Configure Network Tunnel Group on Secure Access , obtenha as IDs de túnel

e os endereços IP dos data centers principal e secundário.

- Clique em Endpoints
- Em Node A, clique em Device e selecione seu dispositivo FTD
- Clique em Virtual Tunnel Interface e selecione a primeira interface VTI criada na etapa anterior
- Clique na opção Send Local Identity to Peers e selecione Email ID, insira o ID de túnel principal (em "Save Network Tunnel Group Configuration", em Configure Network Tunnel Group on Secure Access)
- Em Node B, clique em Device e selecione Extranet
- Clique no Nome do dispositivo e dê um nome a ele
- Clique em Endpoint IP Addresses (Endereços IP de endpoint) e insira os endereços IP principal e secundário de acesso seguro separados por vírgula (de "Save Network Tunnel Group Configuration" (Salvar configuração do grupo de túneis de rede) em Configure Network Tunnel Group on Secure Access)
- Clique em Adicionar VTI de backup
- Clique em Virtual Tunnel Interface e selecione a segunda interface VTI criada na etapa anterior
- Clique na opção Send Local Identity to Peers e selecione Email ID, insira o ID de túnel secundário (em "Save Network Tunnel Group Configuration", em Configure Network Tunnel Group on Secure Access)
- Clique em Salvar

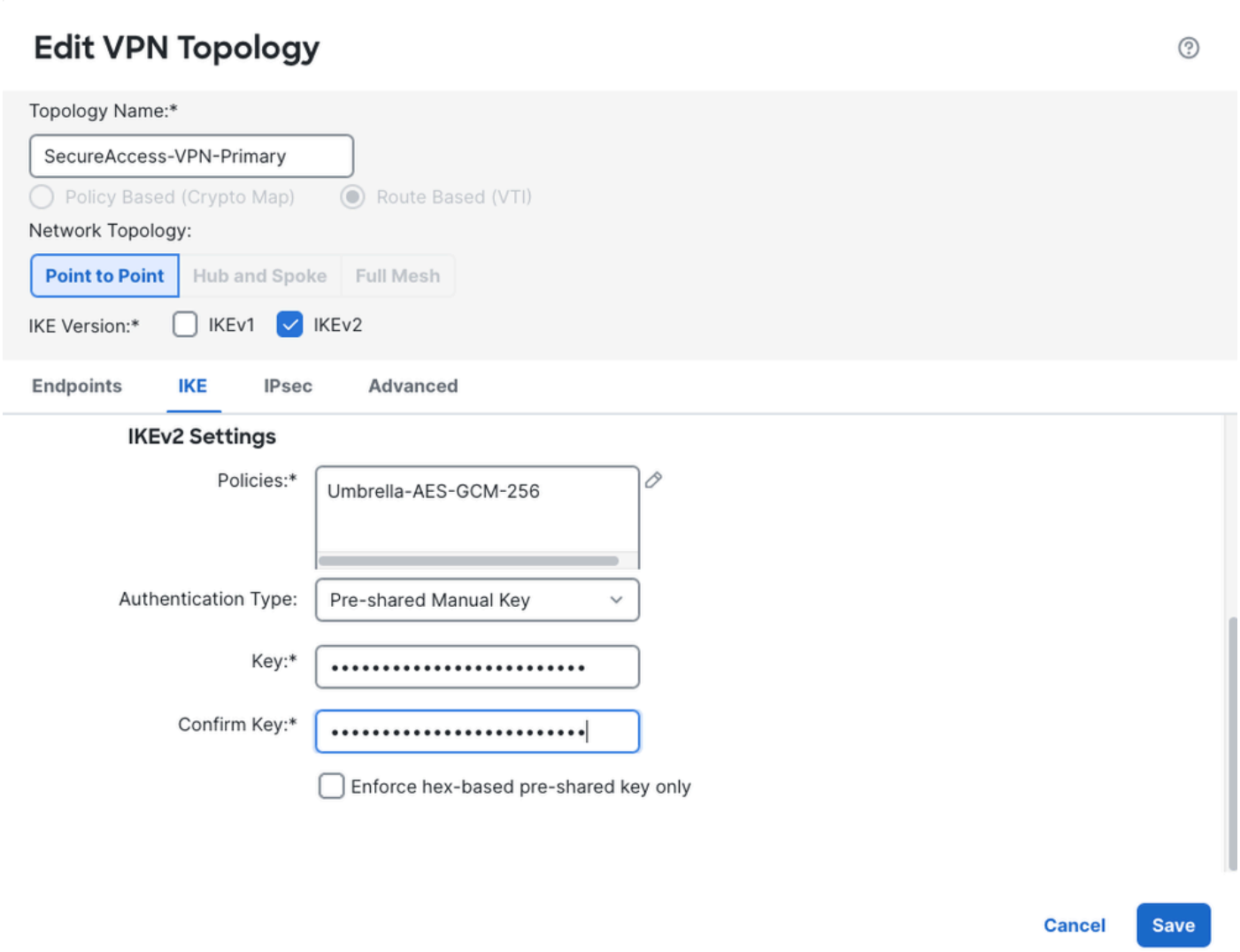


FTD Seguro - Configuração de Ponto de Extremidade VPN



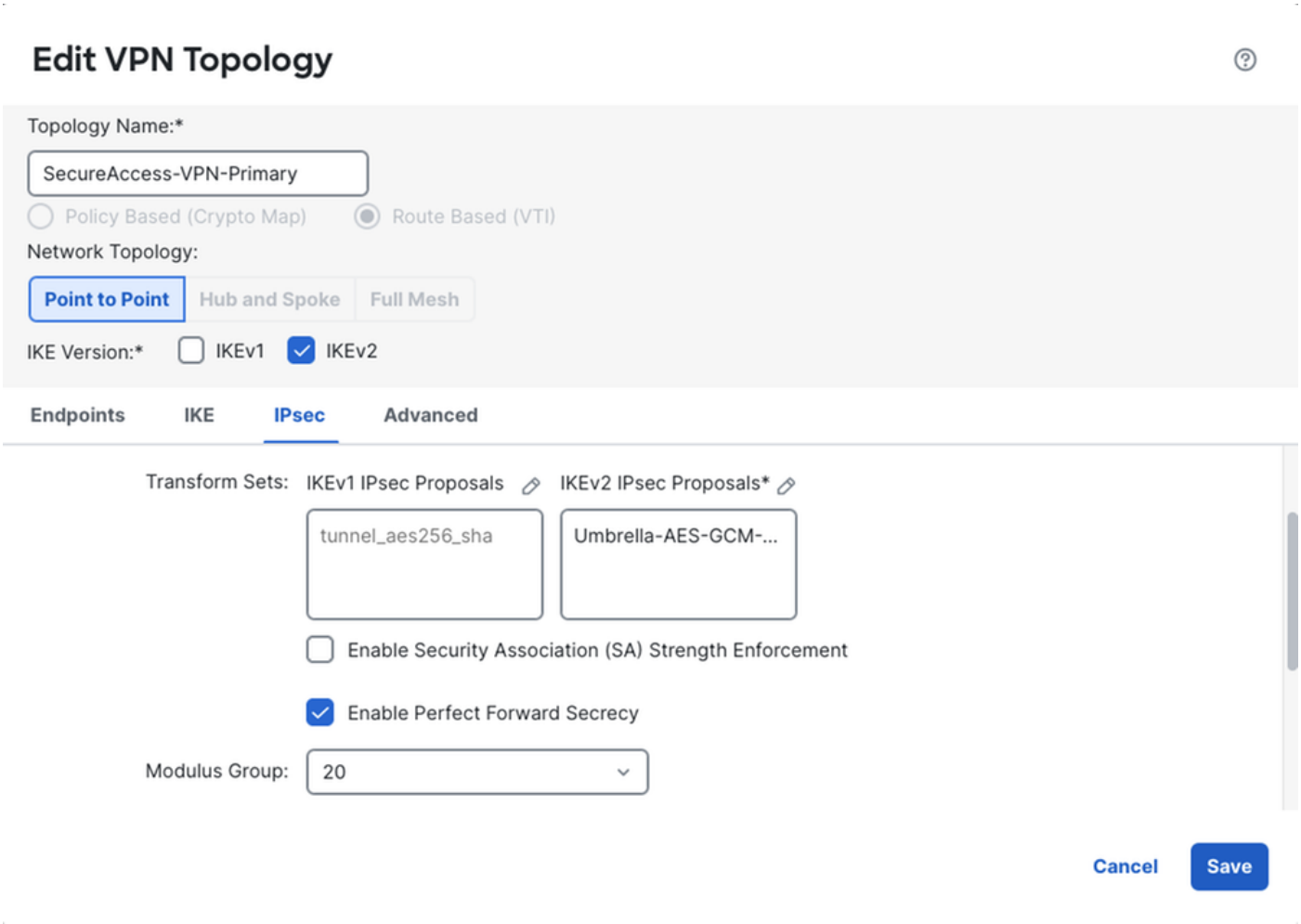
FTD Seguro - Configuração de Ponto de Extremidade VPN

- Configurar configurações de IKEv2 de acordo com parâmetros IPsec suportados
  - Selecione Policies (Regras) como Umbrella-AES-GCM-256
  - Selecione o tipo de autenticação como chave manual pré-compartilhada



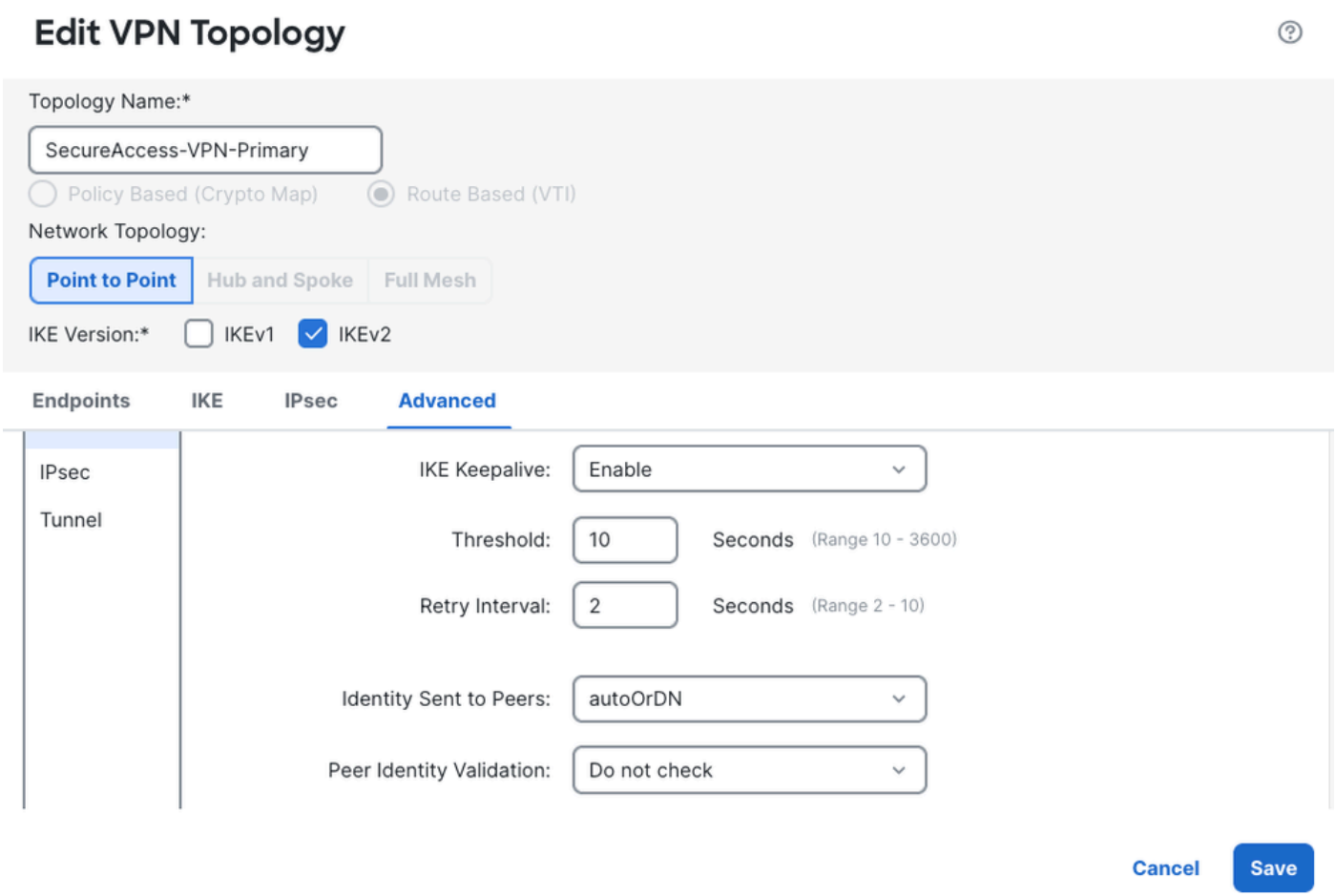
FTD Seguro - Configurações de VPN IKE

- Definir configurações de IPsec
  - Selecione Propostas IKEv2 IPsec como Umbrella-AES-GCM-256
  - Habilite o PFS como o grupo de módulos selecionado como 20



FTD Seguro - Configurações de IPsec de VPN

- Configurações avançadas
- Clique em Salvar



FTD seguro - Configurações avançadas de VPN

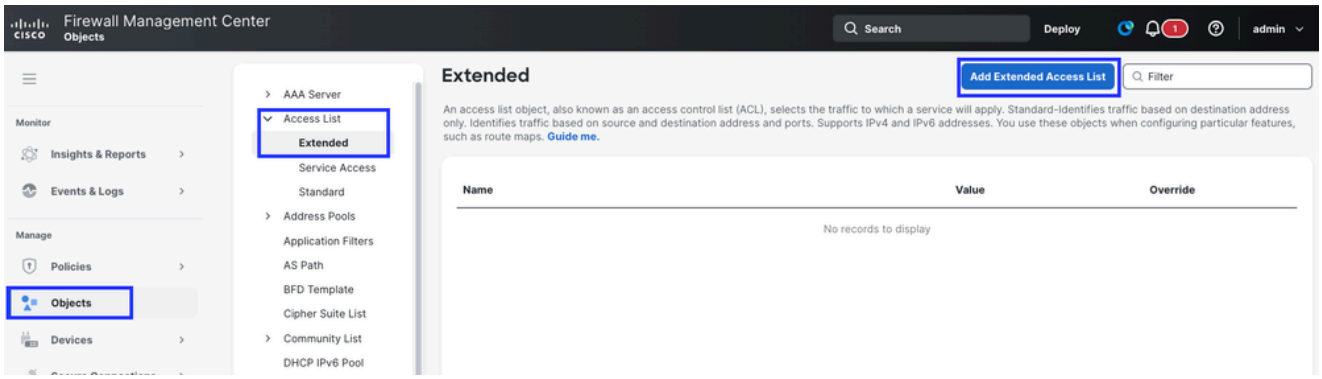
Roteamento baseado em política de FTD

No roteamento tradicional, os pacotes são roteados com base no endereço IP destino. Alterar o roteamento de tráfego específico em um sistema de roteamento baseado em destino é difícil. O Roteamento Baseado em Políticas (PBR) estende e complementa os mecanismos fornecidos pelos protocolos de roteamento, dando a você mais controle sobre o roteamento.

O PBR permite que você defina a precedência do IP. Também permite especificar um caminho para determinado tráfego, como o tráfego prioritário sobre um link de alto custo. Com o PBR, você pode definir o roteamento com base em critérios diferentes da rede de destino, como porta de origem, endereço de destino, porta de destino, protocolo, aplicativos ou uma combinação desses objetos. Para obter mais informações, consulte Roteamento Baseado em Política

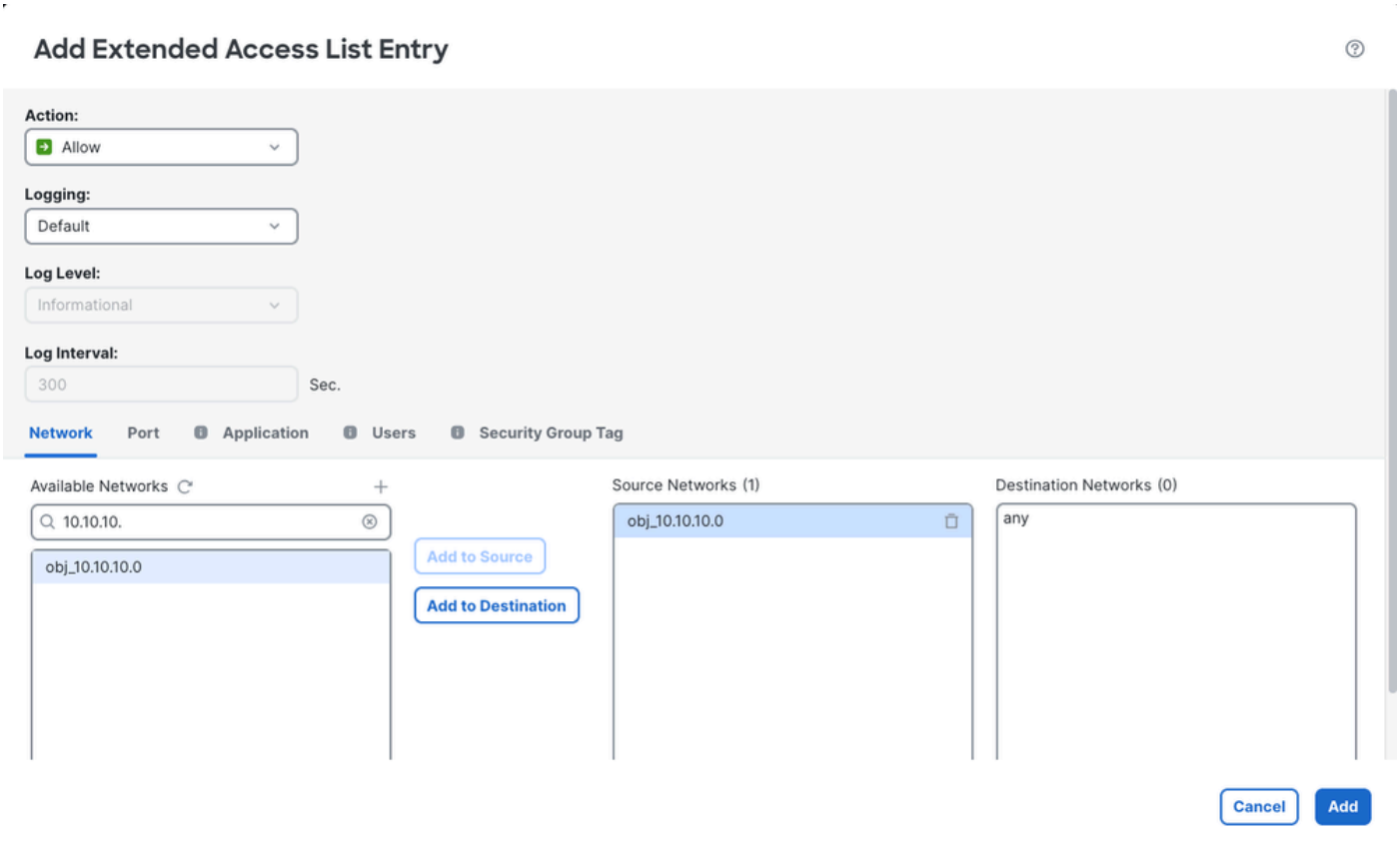
1. Configurar Lista de Acesso

- Navegue até Objetos > Lista de acesso > Estendido
- Clique em Adicionar Lista de Acesso Estendida

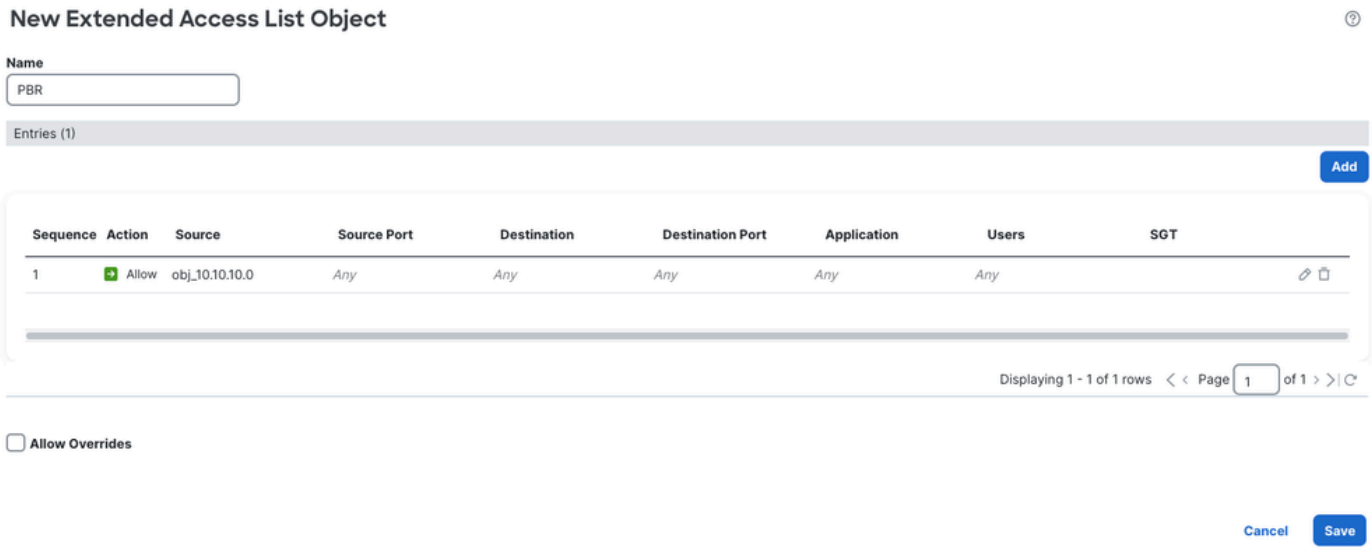


FTD seguro - Lista de acesso estendida

- Fornecer o Nome da Lista de Acesso
- Definir a ação
  - Permissão. - O tráfego definido será enviado para o túnel IPsec
  - Bloquear - o tráfego será ignorado do túnel IPsec
  - A regra será correspondida com base no número de sequência (do menor para o maior)
  - Clique em Adicionar
  - Clique em Salvar



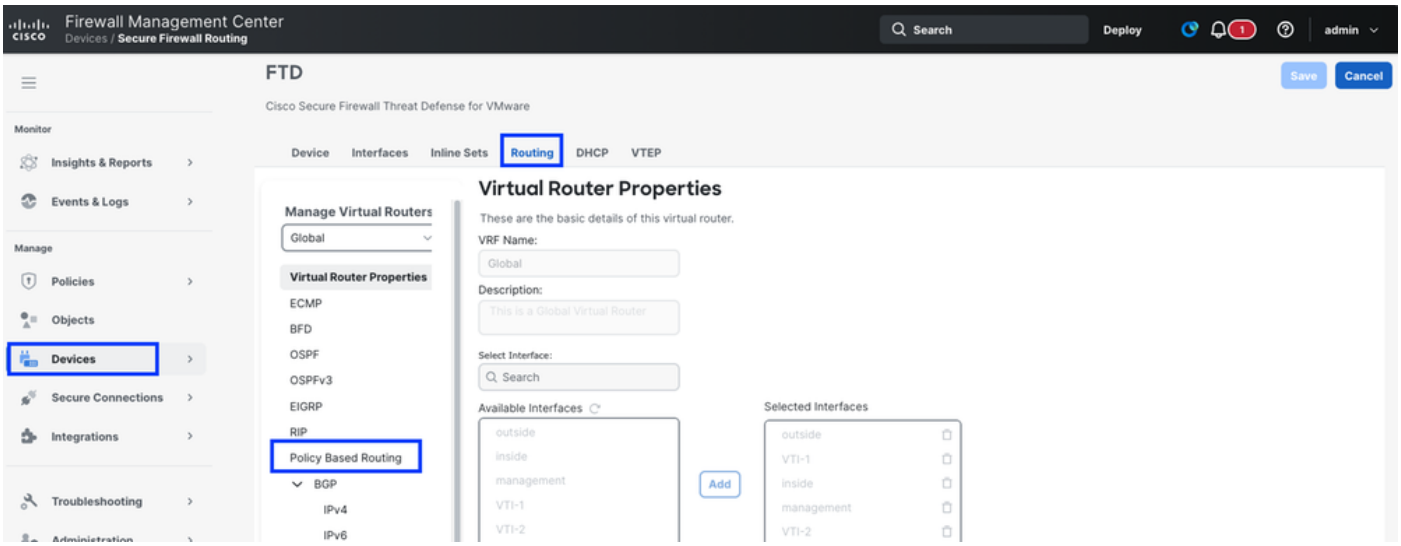
FTD seguro - Lista de acesso estendida



FTD seguro - Lista de acesso estendida

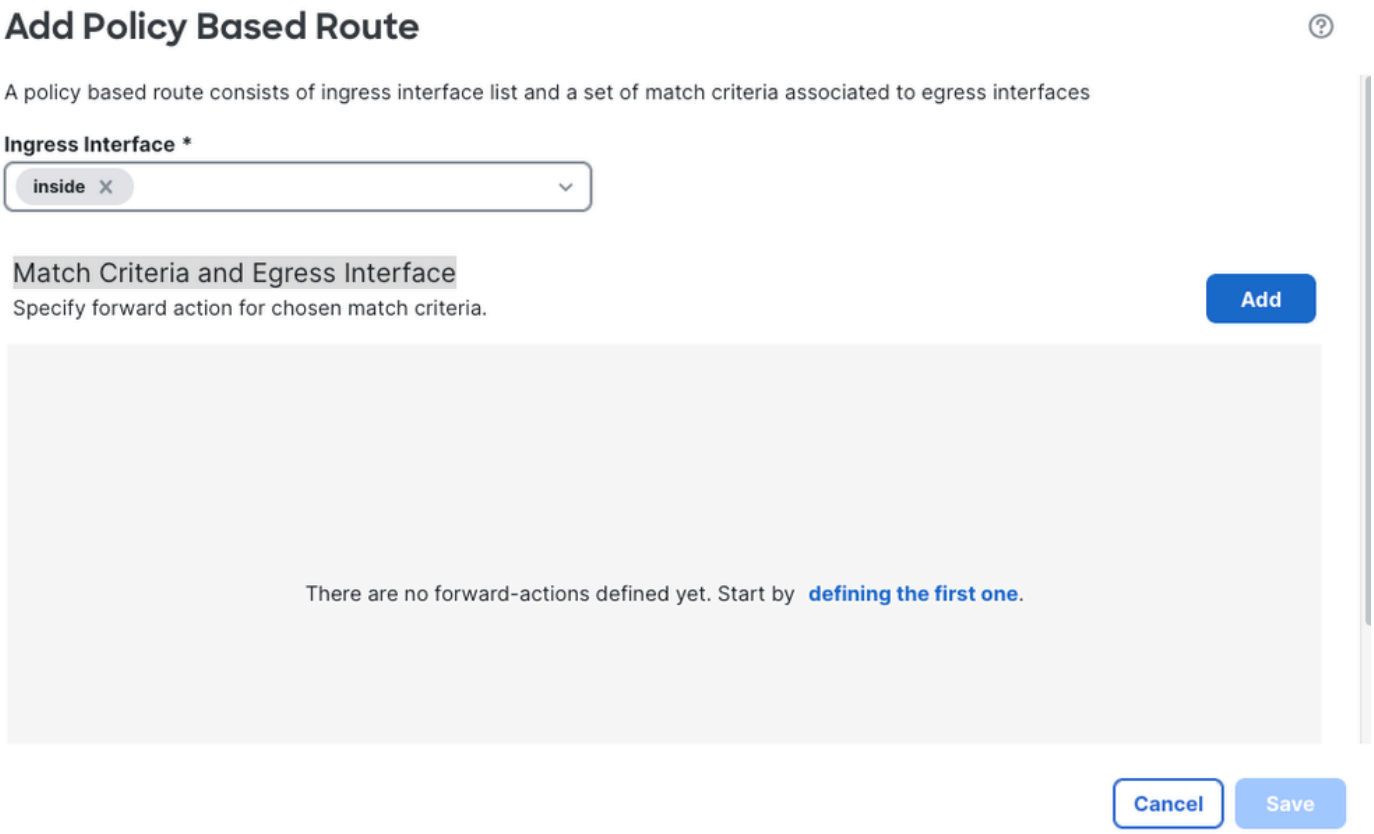
2. Configurar o Roteamento Baseado em Políticas

- Navegue até Devices > Device Management > FTD > Routing



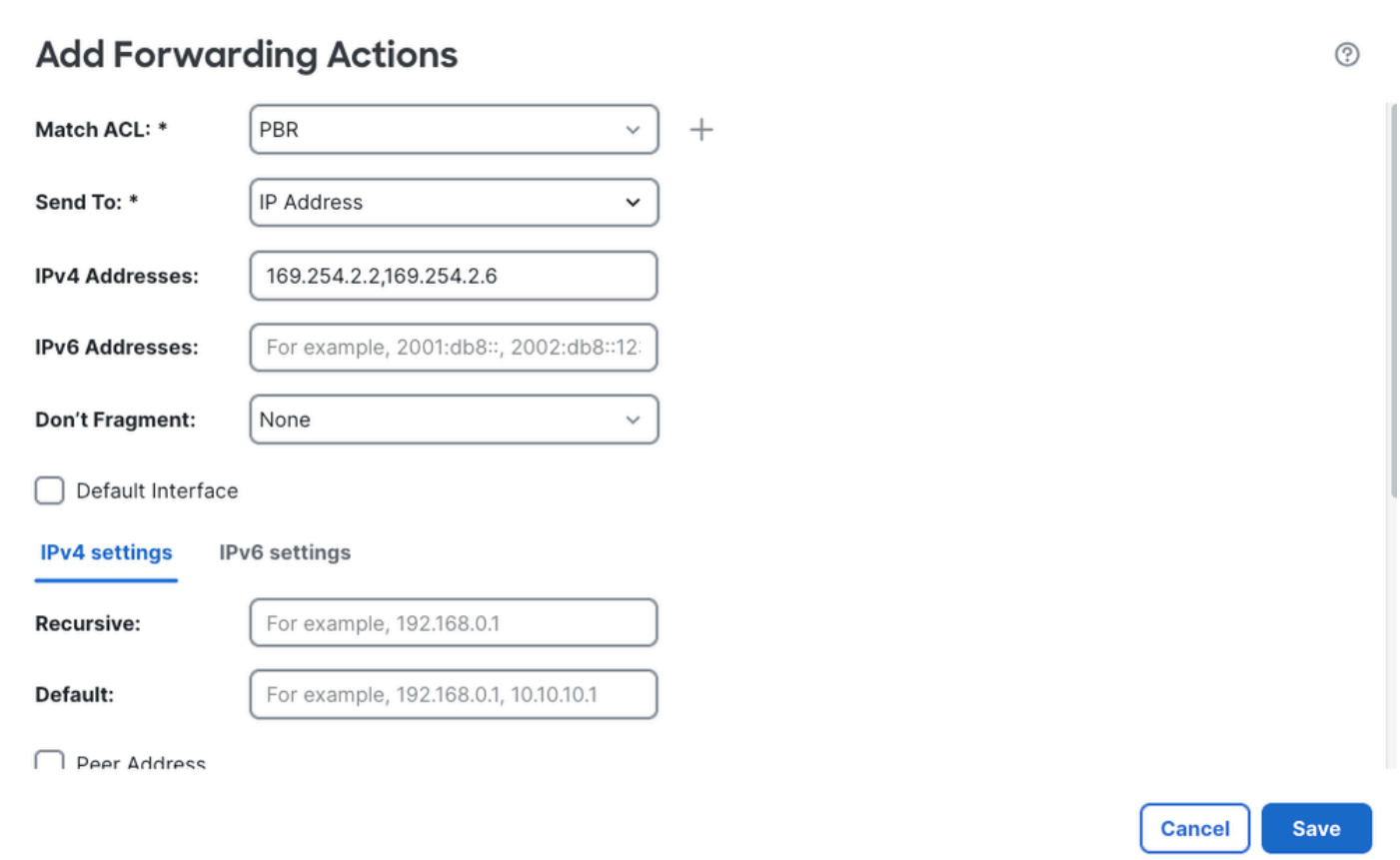
FTD seguro - Roteamento baseado em políticas

- Clique em Adicionar
- Selecione Ingress Interface - Ingress interface para a sub-rede definida na Lista de Acesso

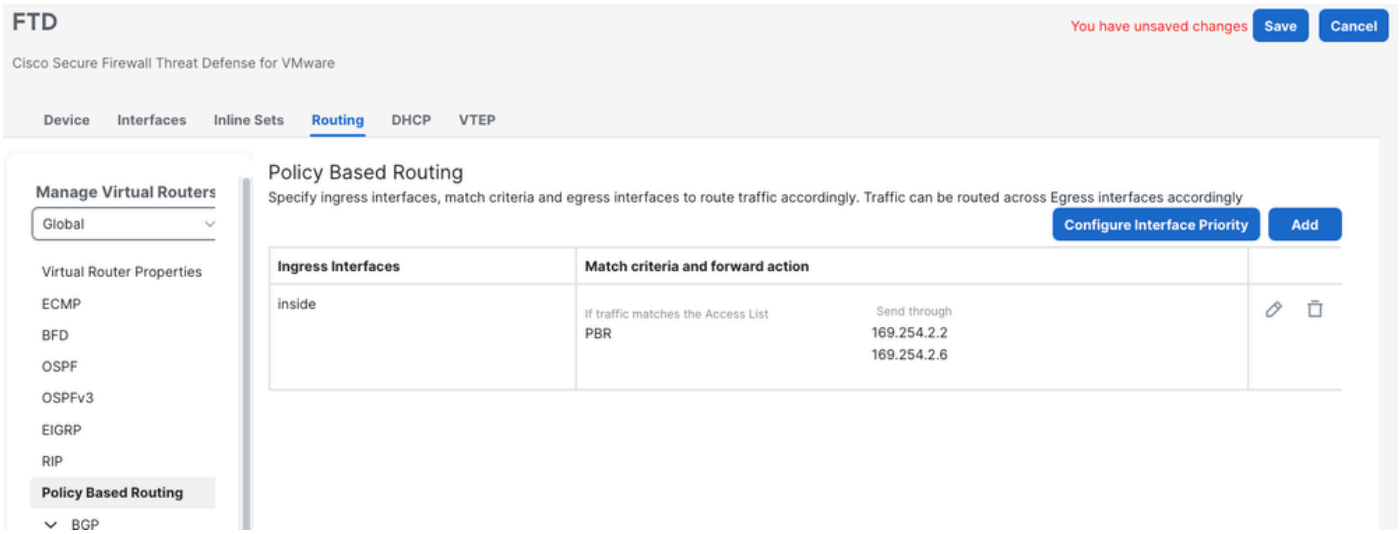


FTD seguro - Roteamento baseado em políticas

- Definir Critérios de Correspondência e Interface de Saída
  - Clique em Adicionar
  - Selecione a ACL Match
  - Selecione Enviar para como endereço IP
  - Adicione o endereço IP do próximo salto. - Os endereços IP da interface VTIs são. 169 254 2 130 e. 169.254.2.5/30. Assim, os endereços IP do próximo salto para VTI -1 e VTI-2 seriam 169.254.2.2 e. 169.254.2.6, respectivamente
  - Clique em Salvar



FTD seguro - Roteamento baseado em políticas

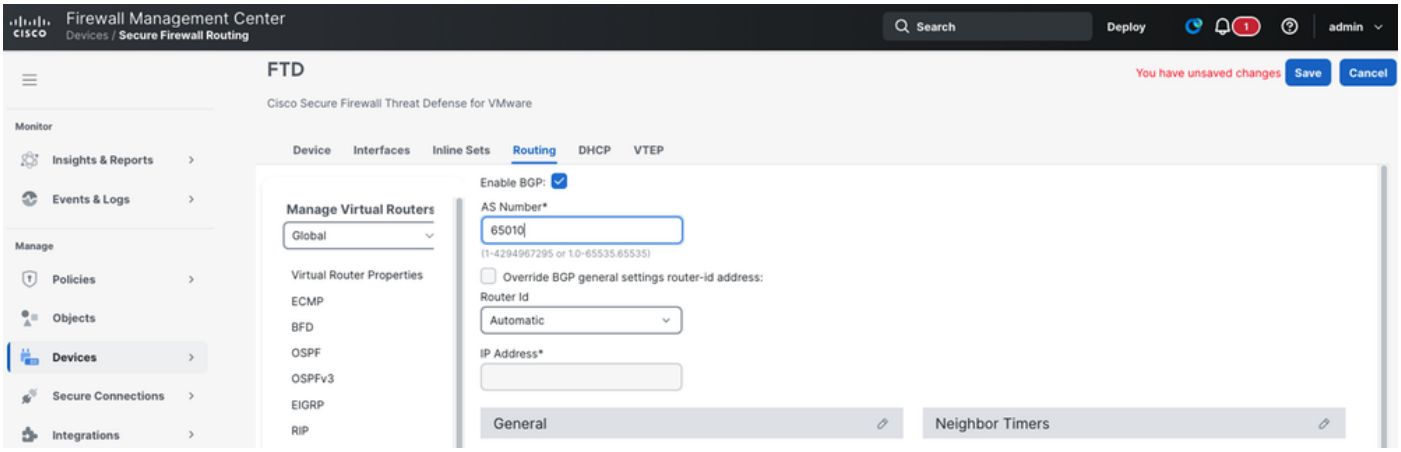


FTD seguro - Roteamento baseado em políticas

Configurar o BGP no FTD

1. Habilitar BGP

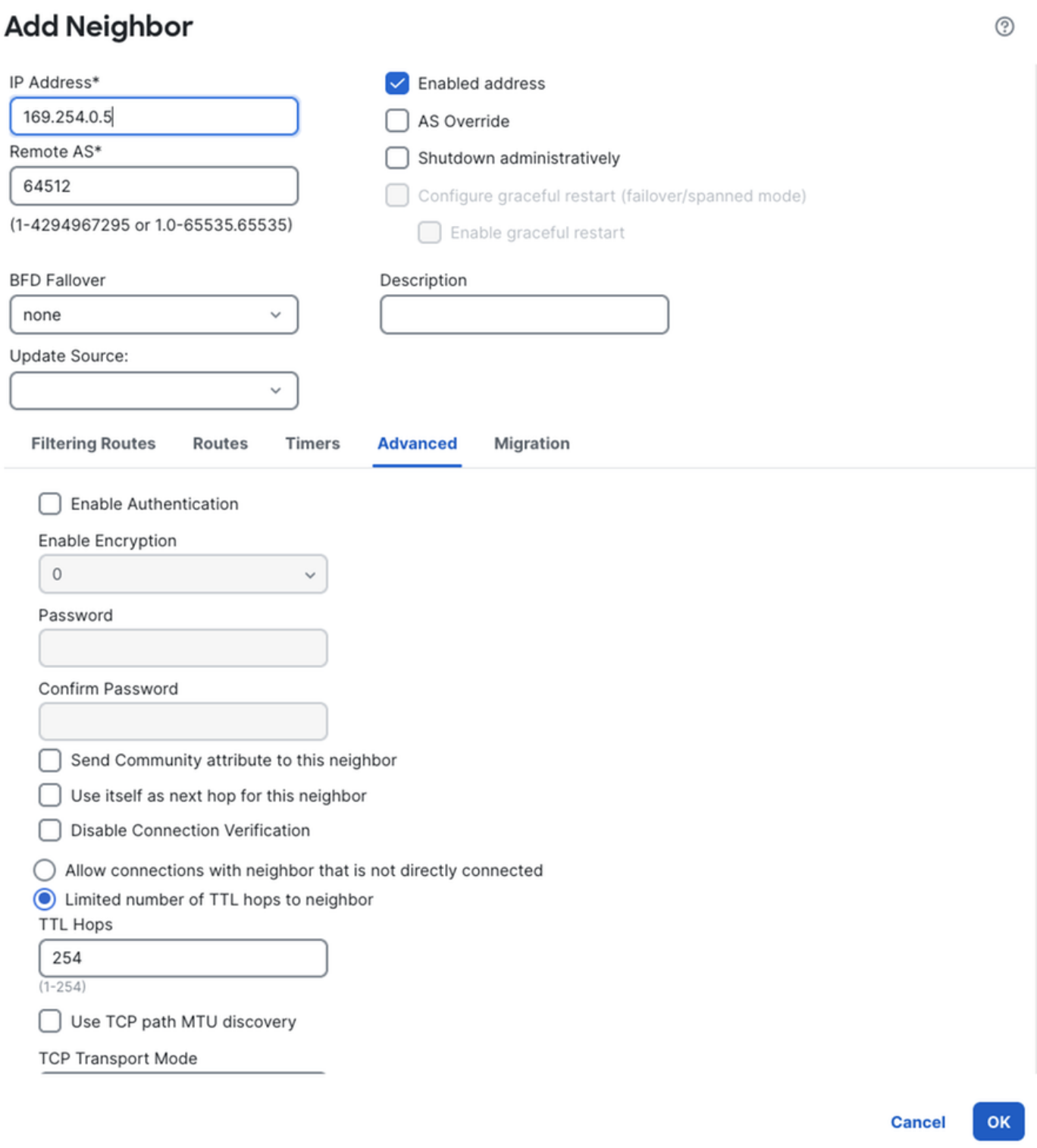
- Navegue até Devices > Device Management > FTD > Routing > General Settings > BGP
- Ative o BGP e adicione o número AS (número AS local do FTD)
- Clique em Salvar

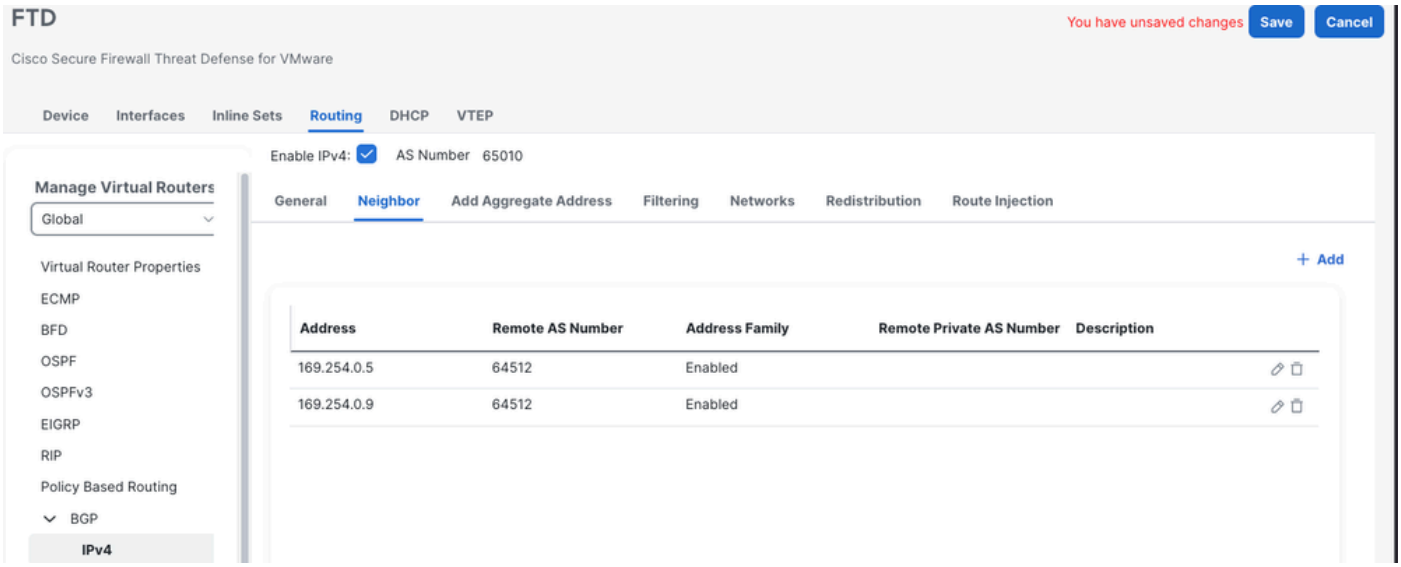


FTD seguro - Roteamento BGP

- Navegue até BGP > IPv4

2. Adicionar Vizinho de BGP- Os peers de BGP de Acesso Seguro são 169.254.0.5 e. 169.254.0.9

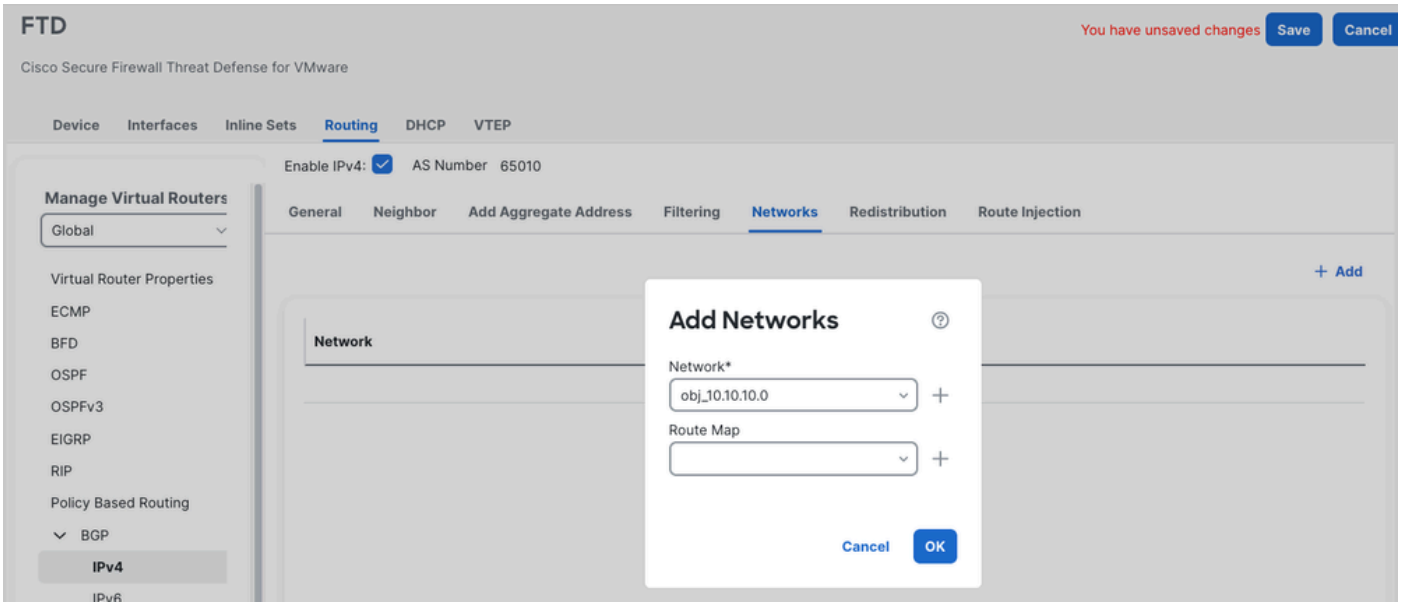

Add Neighbor
IP Address*
169.254.0.5
Remote AS*
64512
(1-4294967295 or 1.0-65535.65535)
Enabled address
AS Override
Shutdown administratively
Configure graceful restart (failover/spanned mode)
Enable graceful restart
BFD Fallover
none
Description
Update Source:
Filtering Routes
Routes
Timers
Advanced
Migration
Enable Authentication
Enable Encryption
0
Password
Confirm Password
Send Community attribute to this neighbor
Use itself as next hop for this neighbor
Disable Connection Verification
Allow connections with neighbor that is not directly connected
Limited number of TTL hops to neighbor
TTL Hops
254
(1-254)
Use TCP path MTU discovery
TCP Transport Mode
Cancel
OK



FTD seguro - Roteamento BGP

3. Adicione as redes - Redes que precisam ser anunciadas para acesso seguro

- Clique em OK.

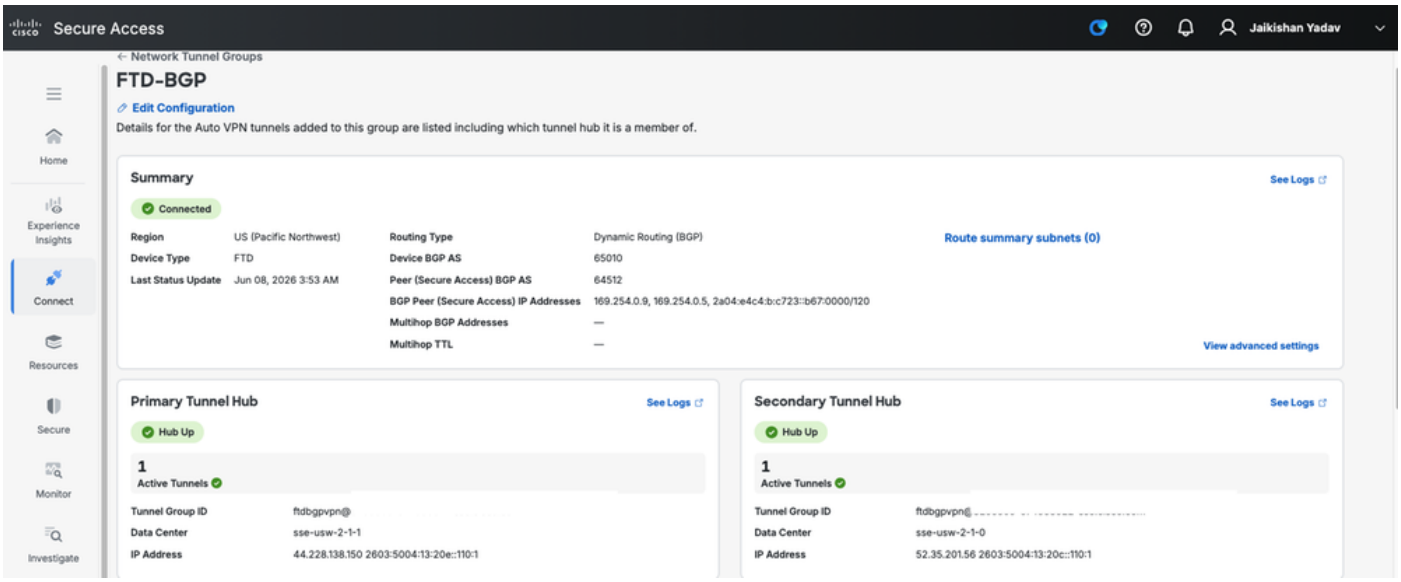


FTD seguro - Roteamento BGP

- Salvar e implantar as alterações

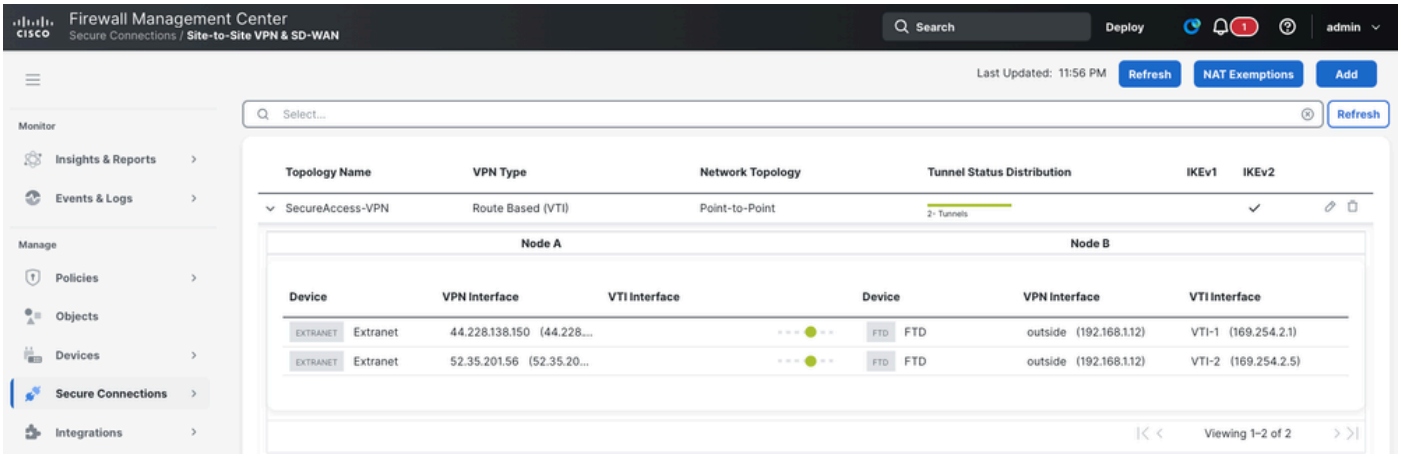
Verificar o status do túnel

No acesso seguro



FTD seguro - Status do túnel IPsec

No CVP



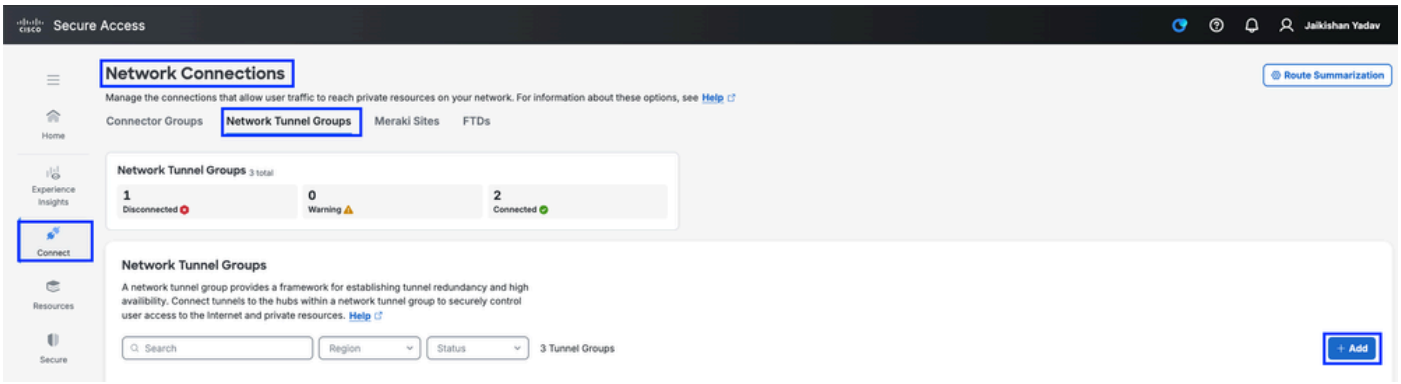
FMC Seguro - Status do Túnel IPsec

Configurar a VPN IPsec baseada em rota estática no Adaptive Security Appliance (ASA) com PBR

Configuração de VPN no acesso seguro

1. Faça login no painel de acesso seguro Acesso seguro
2. Navegue para Connect > Network Connections > Network Tunnel Groups e clique em +Add

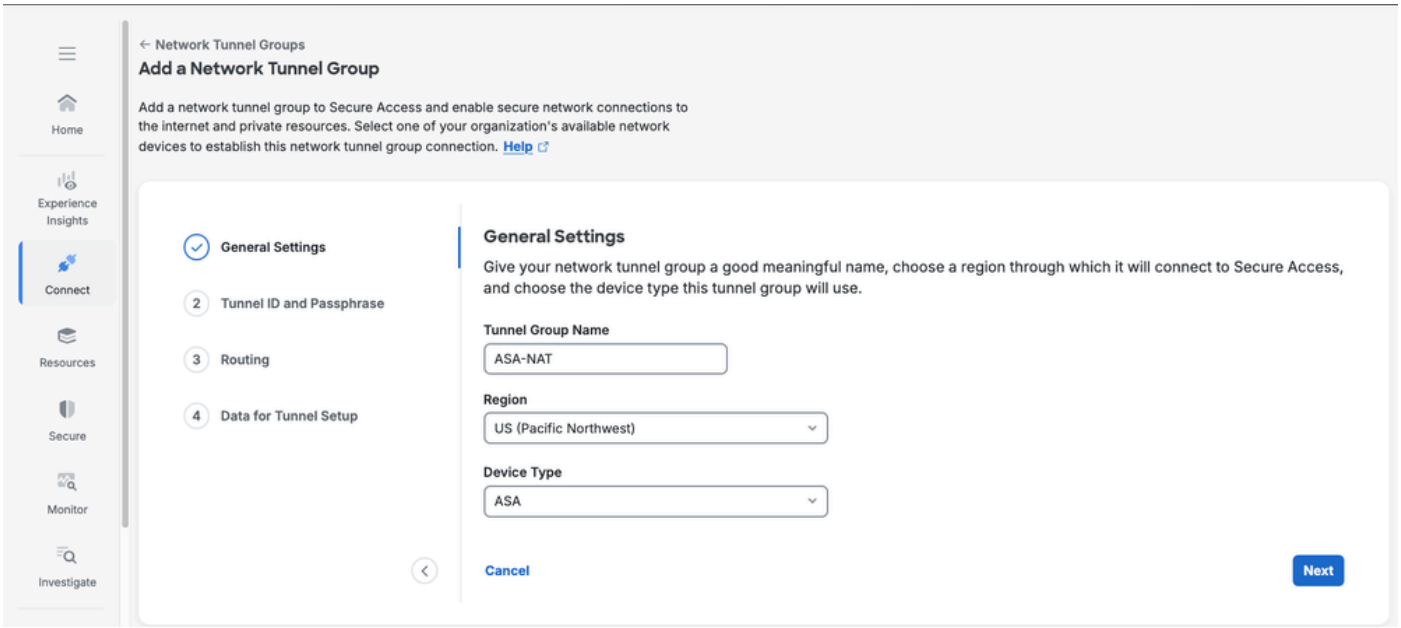
para configurar o Network Tunnel Group



Acesso seguro - Grupos de túnel de rede

3. Configurar Grupo de Túneis de Rede - Definições Gerais

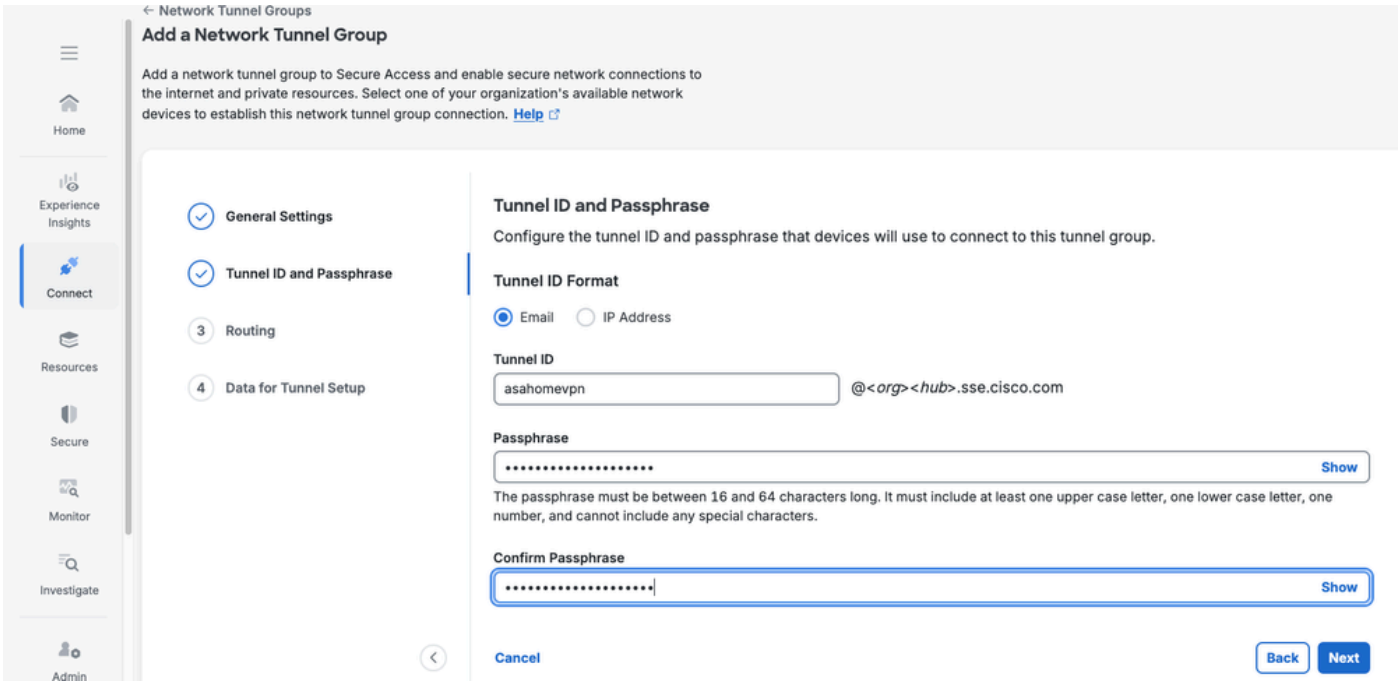
- Configure o nome do grupo de túneis, a região e o tipo de dispositivo
- Clique em Next



Acesso seguro - Configurações gerais dos grupos de túneis de rede

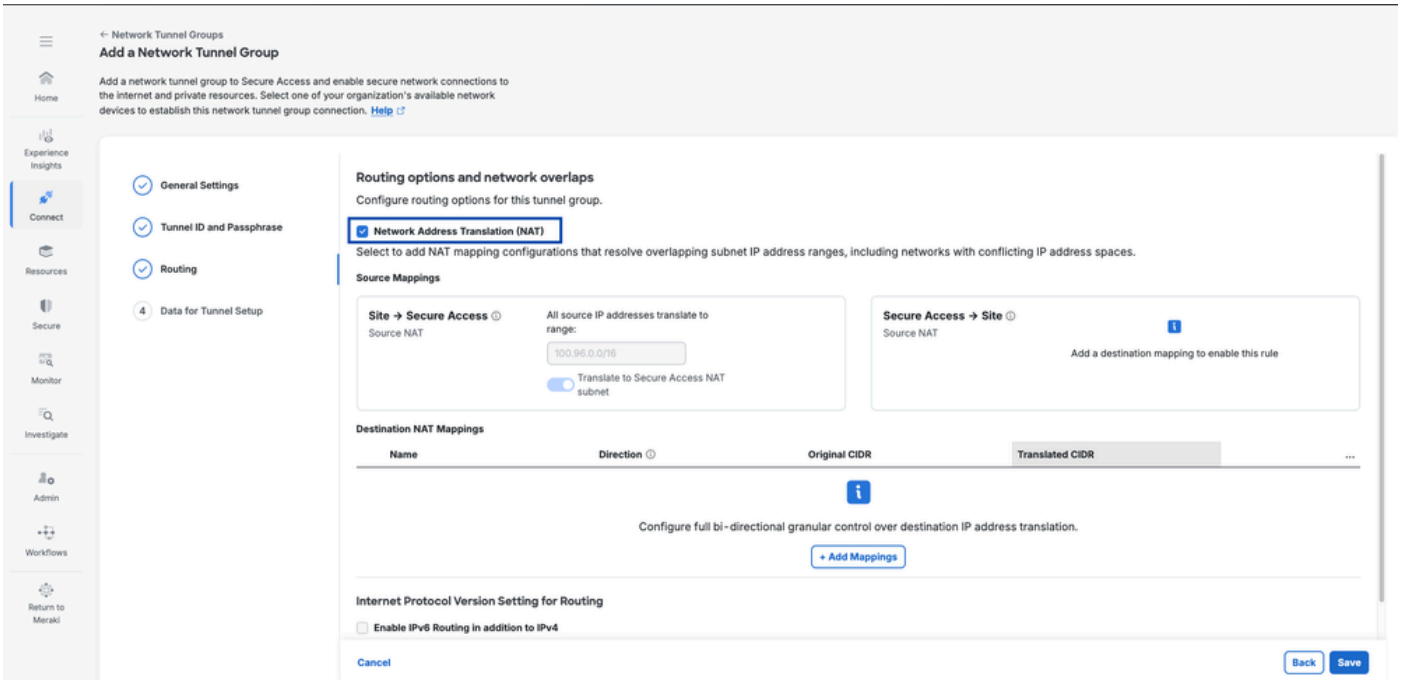
4. Configure Tunnel ID e Passphrase.

- Configure a ID do túnel e a senha.
- Clique em Avançar



Acesso seguro - Grupos de túnel de rede

5. Habilitar a Conversão de Endereço de Rede (NAT)

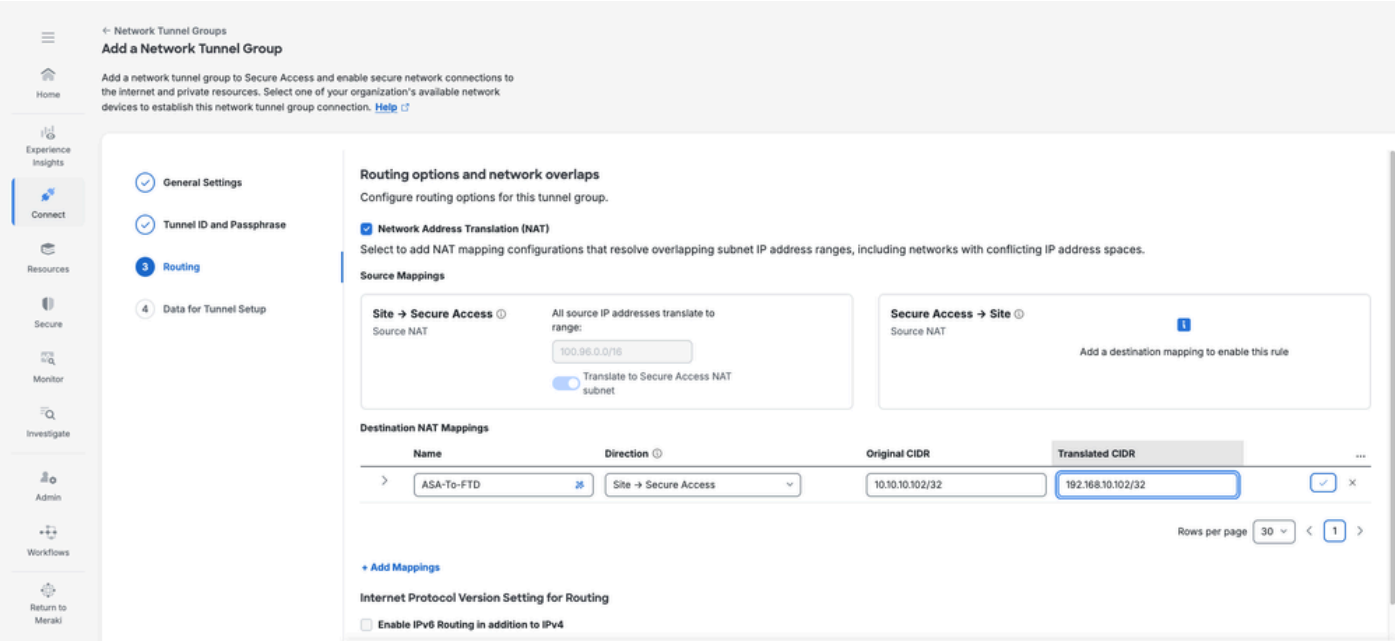


Acesso seguro - Configurações de NAT de grupos de túneis de rede

6. Adicionar mapeamento NAT de destino

Fluxo 1 - Roteador 1 para Roteador 2 (local para acesso seguro)

Fluxo 2 - Roteador 2 para Roteador 1 (Acesso seguro ao local)



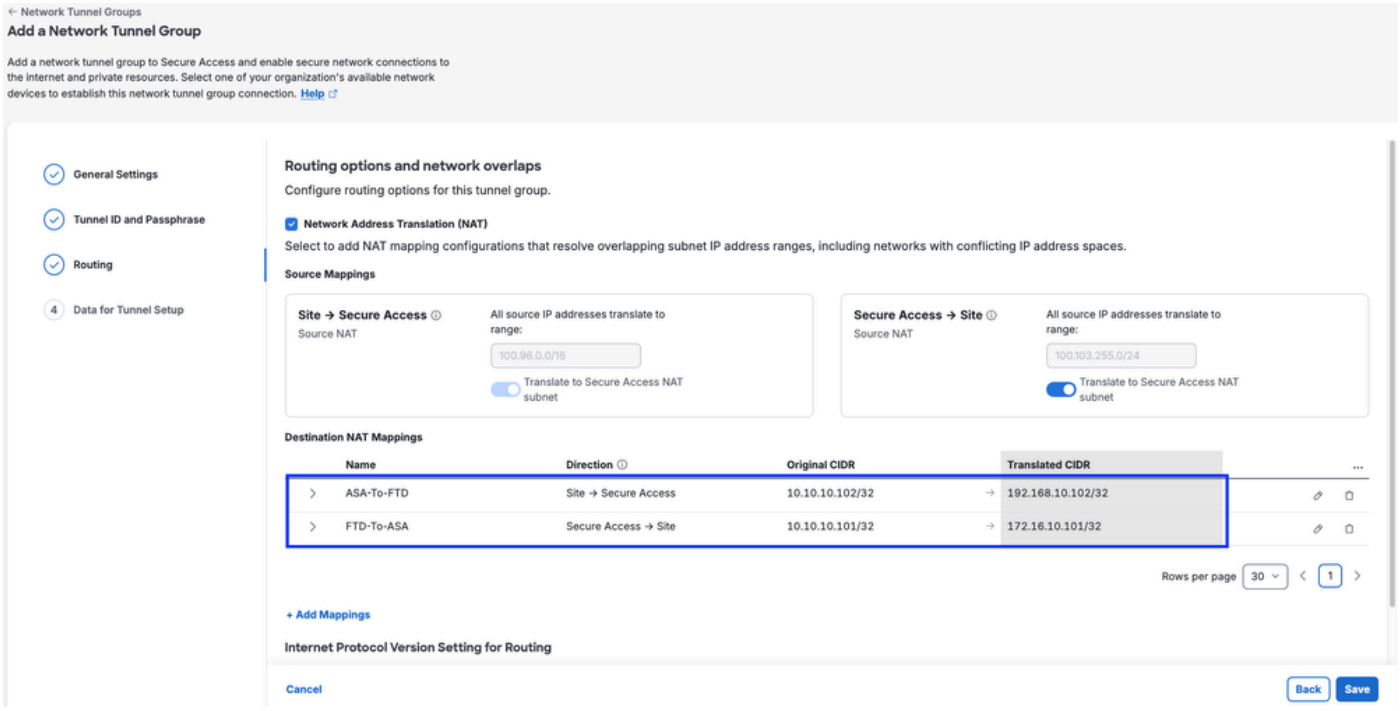
Acesso seguro - Configurações de NAT de grupos de túneis de rede

---

Caution: Quando o NAT está habilitado, o BGP não é possível . Além disso, configure também a VPN estática nos dispositivos da borda do cliente

---

Tip: Lembre-se sempre de fazer ping em um IP convertido .
O IP traduzido vai para o CIDR traduzido e o IP real vai para o CIDR original.



Acesso seguro - Configurações de NAT de grupos de túneis de rede

Clique em Save

Tip: Para o tráfego que vai do 'Site A' para o 'Site B', do ponto de vista CNHE-1 a direção é 'Site-> SecureAccess'

Para o tráfego que vai do 'site B' para o 'site A', do ponto de vista CNHE-1 a direção é 'SecureAccess -> Site'

Configuração de VPN no ASA

1. Faça login no CLI do ASA, entre no modo de ativação e verifique a conectividade IP básica para a Internet

ASA#sh ip
Endereços IP do sistema:
Nome da interface Endereço IP Máscara de sub-rede Método
GigabitEthernet0/0 fora de 192.168.1.40 255.255.255.0 manual
Manual de GigabitEthernet0/1 dentro de 10.10.10.1 255.255.255.0

Endereços IP atuais:
Nome da interface Endereço IP Máscara de sub-rede Método
GigabitEthernet0/0 fora de 192.168.1.40 255.255.255.0 manual

Manual de GigabitEthernet0/1 dentro de 10.10.10.1 255.255.255.0

ASA#ping 8.8.8.8
Digite a seqüência de escape para cancelar.
Enviando Echos ICMP de 5.100 bytes para 8.8.8.8, o tempo limite é de 2 segundos:
!!!!!
A taxa de sucesso é de 100% (5/5), round-trip min/avg/max = 20/28/30 ms
Nº ASA

2. Configure a política IKEv2 e habilite o IKEv2 na interface externa

crypto ikev2 policy 10
encryption aes-gcm-256
integridade nulo
grupo 19
segundos de vida útil 86400
crypto ikev2 enable outside

3. Configurar proposta de IPSec

crypto ipsec ikev2 ipsec-proposal Ipsec-Proposal-primary
protocol esp encryption aes-gcm-256

4. Configurar o perfil IPsec

crypto ipsec profile csa-profile-primary
set ikev2 ipsec-proposal Ipsec-Proposal-primary
set ikev2 local-identity email-id <primary tunnel-id>

5. Configure a Diretiva de Grupo e habilite o protocolo IKEv2 no atributo.

group-policy csa-policy-primary internal
group-policy csa-policy-primary attributes
VPN-tunnel-protocol ikev2

6. Configure o grupo de túneis.

tunnel-group 44.228.138.150 type ipsec-l2l
tunnel-group 44.228.138.150 general-attributes
default-group-policy csa-policy-primary

tunnel-group 44.228.138.150 ipsec-attributes
ikev2 remote-authentication pre-shared-key <pre-shared-key>
ikev2 local-authentication pre-shared-key <pre-shared-key>

7. Configurar a Interface de Túnel Virtual (VTI)

- Nomese você pode escolher
- O endereço IP atribuído ao VTInão deve sobrepor-se a qualquer outra interface no ASA
- A origem do túnel deve ser a interface externa do firewall
- O destino do túnel deve ser o endereço IP do data center

interface Tunnel1
nameif VTI-1
ip address 169.254.2.1 255.255.255.252
tunnel source interface outside
tunnel destination 44.228.138.150
tunnel mode ipsec ipv4
tunnel protection ipsec profile csa-profile-primary

8. Configure o roteamento de forma que o tráfego para o endereço IP ou sub-rede mapeada seja roteado dentro da interface VTI. O próximo salto precisa ser feito pelo IP dentro do intervalo de VTI.

route VTI-1 0.0.0.0 0.0.0.0 169.254.2.2 5. (para tráfego baseado em Internet, pool RAVPN ou CGNAT)

or

route VTI-1 172.16.10.101 255.255.255.255 169.254.2.2 5

Roteamento baseado em políticas

1. Lista de acesso

access-list PBR extended permit ip 10.10.10.0 255.255.255.0 any

2. Mapa de rotas

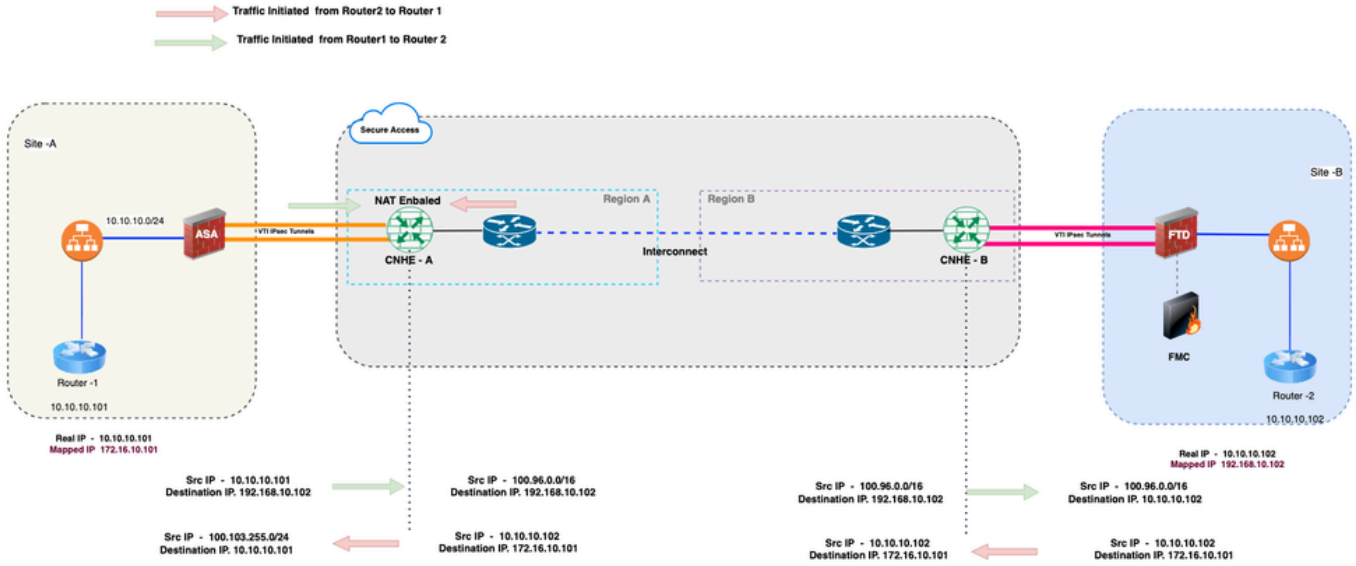
route-map RM-CSA permit 10
match ip address PBR

set ip next-hop 169 254 2 2 169 254 2 6

3. Aplicar o mapa de rotas na interface de entrada

interface GigabitEthernet0/1
nameif inside
nível de segurança 100
endereço ip 10.10.10.1 255.255.255.0
policy-route route-map RM-CSA

Verificar



Interface do roteador e status de acessibilidade do GW

```
Router1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       192.168.1.101   YES NVRAM  down                  down
GigabitEthernet2       10.10.10.101    YES NVRAM  up                    up
GigabitEthernet3       unassigned      YES NVRAM  administratively down down
GigabitEthernet9       unassigned      YES unset  administratively down down
Router1#ping  10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Teste 1- Roteador2 —> Roteador1. - Teste de ping

```
Router1#ping 192.168.10.102
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.102, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 207/211/223 ms
Router1#
```

Captura de pacotes no ASA (FW local)

```
ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA#
ASA#
ASA# ter pag 20
ASA# sh cap capin

10 packets captured

   1: 10:56:45.024244       10.10.10.101 > 192.168.10.102 icmp: echo request
   2: 10:56:45.231143       192.168.10.102 > 10.10.10.101 icmp: echo reply
   3: 10:56:45.232470       10.10.10.101 > 192.168.10.102 icmp: echo request
   4: 10:56:45.441856       192.168.10.102 > 10.10.10.101 icmp: echo reply
   5: 10:56:45.443122       10.10.10.101 > 192.168.10.102 icmp: echo request
   6: 10:56:45.652477       192.168.10.102 > 10.10.10.101 icmp: echo reply
   7: 10:56:45.653423       10.10.10.101 > 192.168.10.102 icmp: echo request
   8: 10:56:45.875397       192.168.10.102 > 10.10.10.101 icmp: echo reply
   9: 10:56:45.876450       10.10.10.101 > 192.168.10.102 icmp: echo request
  10: 10:56:46.082301       192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

   1: 10:56:45.024458       10.10.10.101 > 192.168.10.102 icmp: echo request
   2: 10:56:45.230914       192.168.10.102 > 10.10.10.101 icmp: echo reply
   3: 10:56:45.232516       10.10.10.101 > 192.168.10.102 icmp: echo request
   4: 10:56:45.441795       192.168.10.102 > 10.10.10.101 icmp: echo reply
   5: 10:56:45.443153       10.10.10.101 > 192.168.10.102 icmp: echo request
   6: 10:56:45.652432       192.168.10.102 > 10.10.10.101 icmp: echo reply
   7: 10:56:45.653454       10.10.10.101 > 192.168.10.102 icmp: echo request
   8: 10:56:45.875351       192.168.10.102 > 10.10.10.101 icmp: echo reply
   9: 10:56:45.876480       10.10.10.101 > 192.168.10.102 icmp: echo request
  10: 10:56:46.082240       192.168.10.102 > 10.10.10.101 icmp: echo reply
10 packets shown
```

Captura de pacotes no FTD (FW remoto)

```
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd# sh cap vti

10 packets captured

   1: 16:06:41.122292       100.96.2.0 > 10.10.10.102 icmp: echo request
   2: 16:06:41.124856       10.10.10.102 > 100.96.2.0 icmp: echo reply
   3: 16:06:41.329557       100.96.2.0 > 10.10.10.102 icmp: echo request
   4: 16:06:41.330442       10.10.10.102 > 100.96.2.0 icmp: echo reply
   5: 16:06:41.546327       100.96.2.0 > 10.10.10.102 icmp: echo request
   6: 16:06:41.547106       10.10.10.102 > 100.96.2.0 icmp: echo reply
   7: 16:06:41.752036       100.96.2.0 > 10.10.10.102 icmp: echo request
   8: 16:06:41.752814       10.10.10.102 > 100.96.2.0 icmp: echo reply
   9: 16:06:41.967891       100.96.2.0 > 10.10.10.102 icmp: echo request
  10: 16:06:41.968501       10.10.10.102 > 100.96.2.0 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

   1: 16:06:41.123299       100.96.2.0 > 10.10.10.102 icmp: echo request
   2: 16:06:41.124825       10.10.10.102 > 100.96.2.0 icmp: echo reply
   3: 16:06:41.330000       100.96.2.0 > 10.10.10.102 icmp: echo request
   4: 16:06:41.330396       10.10.10.102 > 100.96.2.0 icmp: echo reply
   5: 16:06:41.546800       100.96.2.0 > 10.10.10.102 icmp: echo request
   6: 16:06:41.547090       10.10.10.102 > 100.96.2.0 icmp: echo reply
   7: 16:06:41.752448       100.96.2.0 > 10.10.10.102 icmp: echo request
   8: 16:06:41.752783       10.10.10.102 > 100.96.2.0 icmp: echo reply
   9: 16:06:41.968242       100.96.2.0 > 10.10.10.102 icmp: echo request
  10: 16:06:41.968486       10.10.10.102 > 100.96.2.0 icmp: echo reply
10 packets shown
```

Ensaio 2. - Roteador 2 —> Teste de ping do roteador 1

```
Router2#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       unassigned      YES NVRAM  administratively down down
GigabitEthernet2       10.10.10.102    YES NVRAM  up                    up
GigabitEthernet3       unassigned      YES NVRAM  administratively down down
Router2#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Captura de pacote FTD (FW local)

```
ftd# sh capture
capture vti type raw-data trace interface VTI-1 include-decrypted [Capturing - 1300 bytes]
  match icmp any any
capture capin type raw-data interface inside [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ftd#
ftd#
ftd#
ftd# sh cap vti

10 packets captured

   1: 16:11:45.622450       10.10.10.102 > 172.16.10.101 icmp: echo request
   2: 16:11:45.823825       172.16.10.101 > 10.10.10.102 icmp: echo reply
   3: 16:11:45.825762       10.10.10.102 > 172.16.10.101 icmp: echo request
   4: 16:11:46.045667       172.16.10.101 > 10.10.10.102 icmp: echo reply
   5: 16:11:46.046857       10.10.10.102 > 172.16.10.101 icmp: echo request
   6: 16:11:46.252321       172.16.10.101 > 10.10.10.102 icmp: echo reply
   7: 16:11:46.253572       10.10.10.102 > 172.16.10.101 icmp: echo request
   8: 16:11:46.453803       172.16.10.101 > 10.10.10.102 icmp: echo reply
   9: 16:11:46.454764       10.10.10.102 > 172.16.10.101 icmp: echo request
  10: 16:11:46.664119       172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
ftd# sh cap capin

10 packets captured

   1: 16:11:45.622083       10.10.10.102 > 172.16.10.101 icmp: echo request
   2: 16:11:45.823886       172.16.10.101 > 10.10.10.102 icmp: echo reply
   3: 16:11:45.825442       10.10.10.102 > 172.16.10.101 icmp: echo request
   4: 16:11:46.045697       172.16.10.101 > 10.10.10.102 icmp: echo reply
   5: 16:11:46.046582       10.10.10.102 > 172.16.10.101 icmp: echo request
   6: 16:11:46.252352       172.16.10.101 > 10.10.10.102 icmp: echo reply
   7: 16:11:46.253313       10.10.10.102 > 172.16.10.101 icmp: echo request
   8: 16:11:46.453849       172.16.10.101 > 10.10.10.102 icmp: echo reply
   9: 16:11:46.454596       10.10.10.102 > 172.16.10.101 icmp: echo request
  10: 16:11:46.664150       172.16.10.101 > 10.10.10.102 icmp: echo reply
10 packets shown
```

Captura de pacote ASA (FW remoto)

```
ASA# sh capture
capture capin type raw-data trace interface inside [Capturing - 1300 bytes]
  match icmp any any
capture tunnel type raw-data trace interface vti-1 [Capturing - 1300 bytes]
  match icmp any any
capture asp type asp-drop all [Capturing - 0 bytes]
  match icmp any any
ASA# sh cap capin

10 packets captured

   1: 11:08:30.288391       100.103.255.195 > 10.10.10.101 icmp: echo request
   2: 11:08:30.289123       10.10.10.101 > 100.103.255.195 icmp: echo reply
   3: 11:08:30.504566       100.103.255.195 > 10.10.10.101 icmp: echo request
   4: 11:08:30.504963       10.10.10.101 > 100.103.255.195 icmp: echo reply
   5: 11:08:30.710992       100.103.255.195 > 10.10.10.101 icmp: echo request
   6: 11:08:30.711404       10.10.10.101 > 100.103.255.195 icmp: echo reply
   7: 11:08:30.917112       100.103.255.195 > 10.10.10.101 icmp: echo request
   8: 11:08:30.917402       10.10.10.101 > 100.103.255.195 icmp: echo reply
   9: 11:08:31.128243       100.103.255.195 > 10.10.10.101 icmp: echo request
  10: 11:08:31.128640       10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
ASA# sh cap tunnel

10 packets captured

   1: 11:08:30.287964       100.103.255.195 > 10.10.10.101 icmp: echo request
   2: 11:08:30.289322       10.10.10.101 > 100.103.255.195 icmp: echo reply
   3: 11:08:30.504505       100.103.255.195 > 10.10.10.101 icmp: echo request
   4: 11:08:30.505009       10.10.10.101 > 100.103.255.195 icmp: echo reply
   5: 11:08:30.710961       100.103.255.195 > 10.10.10.101 icmp: echo request
   6: 11:08:30.711434       10.10.10.101 > 100.103.255.195 icmp: echo reply
   7: 11:08:30.917066       100.103.255.195 > 10.10.10.101 icmp: echo request
   8: 11:08:30.917417       10.10.10.101 > 100.103.255.195 icmp: echo reply
   9: 11:08:31.128197       100.103.255.195 > 10.10.10.101 icmp: echo request
  10: 11:08:31.128685       10.10.10.101 > 100.103.255.195 icmp: echo reply
10 packets shown
```

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.