

Configurar VPN Baseada em Rota com Rota Estática no FTD Gerenciado pelo FDM

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Etapas de Configuração no FDM](#)

[Verificar](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar um túnel VPN site a site baseado em rota estática em um FTD gerenciado pelo FDM.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão básica de como um túnel VPN funciona.
- Conhecimento prévio de navegação pelo Firepower Device Manager (FDM).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

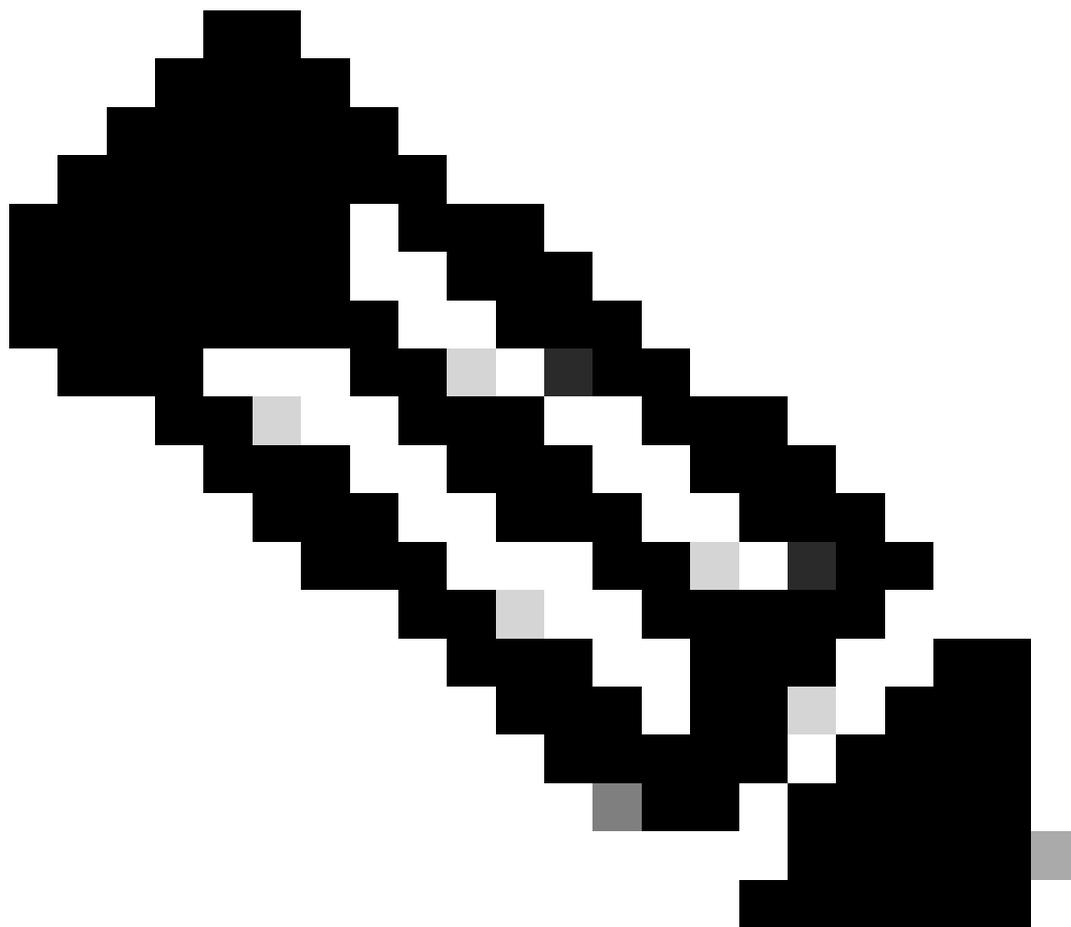
- Cisco Firepower Threat Defense (FTD) versão 7.0 gerenciado pelo Firepower Device Manager (FDM).

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

A VPN baseada em rota permite que a determinação do tráfego interessante seja criptografada ou enviada pelo túnel VPN, e usa o roteamento de tráfego em vez da política/lista de acesso como na VPN baseada em política ou em mapa de criptografia. O domínio de criptografia é definido para permitir qualquer tráfego que entre no túnel IPsec. Os seletores de tráfego local e remoto de IPsec são definidos como 0.0.0.0/0.0.0.0. Isso significa que qualquer tráfego roteado para o túnel IPsec é criptografado, independentemente da sub-rede de origem/destino.

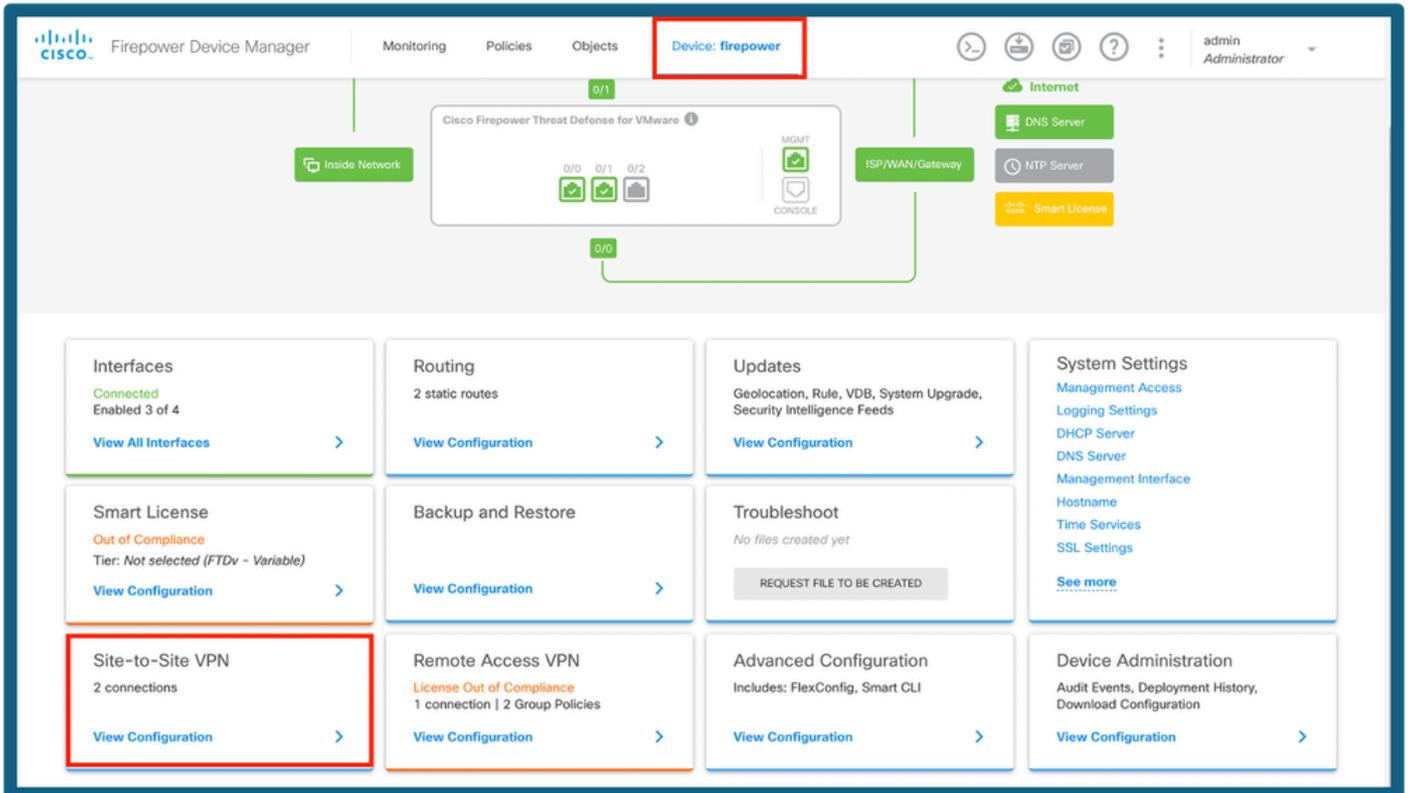
Este documento se concentra na configuração da Interface de túnel virtual estático (SVTI).



Note: Não é necessário nenhum licenciamento adicional, a VPN Baseada em Rota pode ser configurada nos Modos Licenciado e de Avaliação. Sem a conformidade com criptografia (Recursos Controlados por Exportação Habilitados), somente DES pode ser usado como um algoritmo de criptografia.

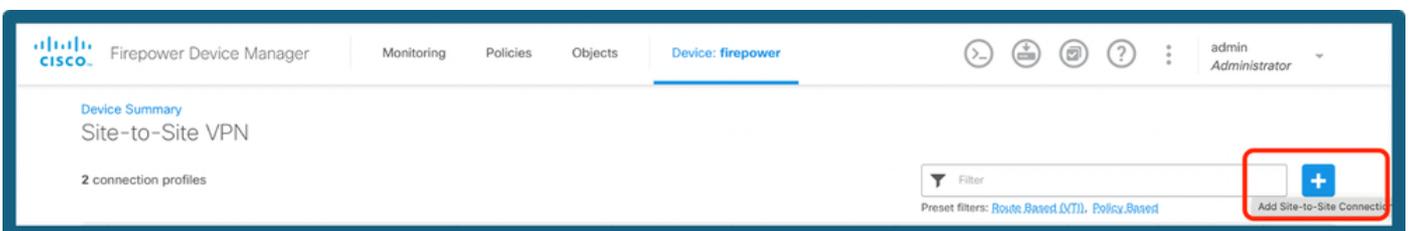
Etapas de Configuração no FDM

Etapa 1. Navegue até Device > Site To Site.



Painel do FDM

Etapa 2. Clique no ícone + para adicionar um novo site à conexão de site.



Adicionar conexão S2S

Etapa 3. Forneça um nome de topologia e selecione o tipo de VPN como baseado em rota (VTI).

Clique em Local VPN Access Interface e, em seguida, clique em Create new Virtual Tunnel Interface ou selecione um na lista existente.

Firepower Device Manager | Monitoring | Policies | Objects | Device: firepower | admin Administrator

Local Network | FIREPOWER | VPN TUNNEL | INTERNET | OUTSIDE INTERFACE | PEER ENDPOINT | Remote Network

Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name: Type: Route Based (VTI) Policy Based

Sites Configuration

LOCAL SITE: Local VPN Access Interface:

REMOTE SITE: Remote IP Address:

[Create new Virtual Tunnel Interface](#)

Adicionar interface de túnel

Etapa 4. Definir os parâmetros da Nova Interface de Túnel Virtual. Click OK.

Create Virtual Tunnel Interface

Name: Status:

Most features work with named interfaces only, although some require unnamed interfaces.

Description:

Tunnel ID: Tunnel Source:

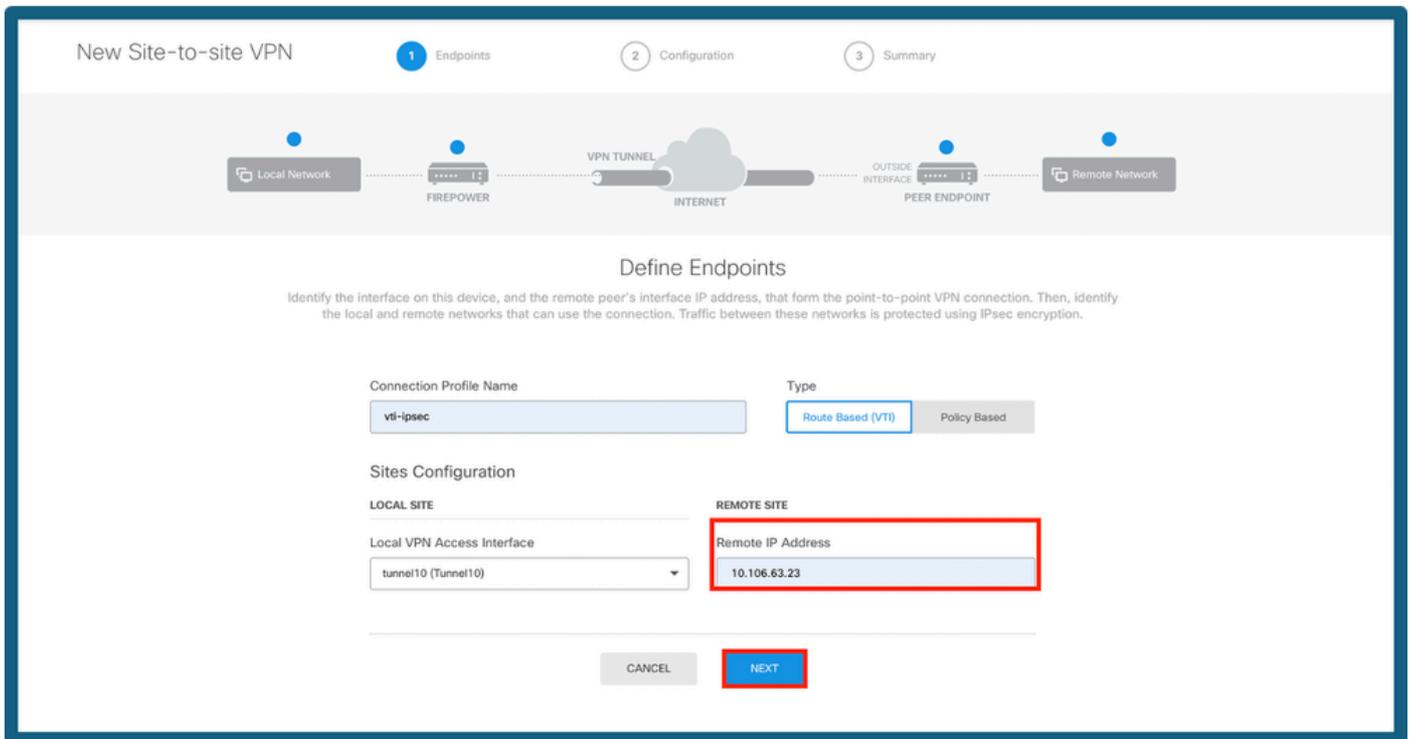
0 - 10413

IP Address and Subnet Mask: /

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

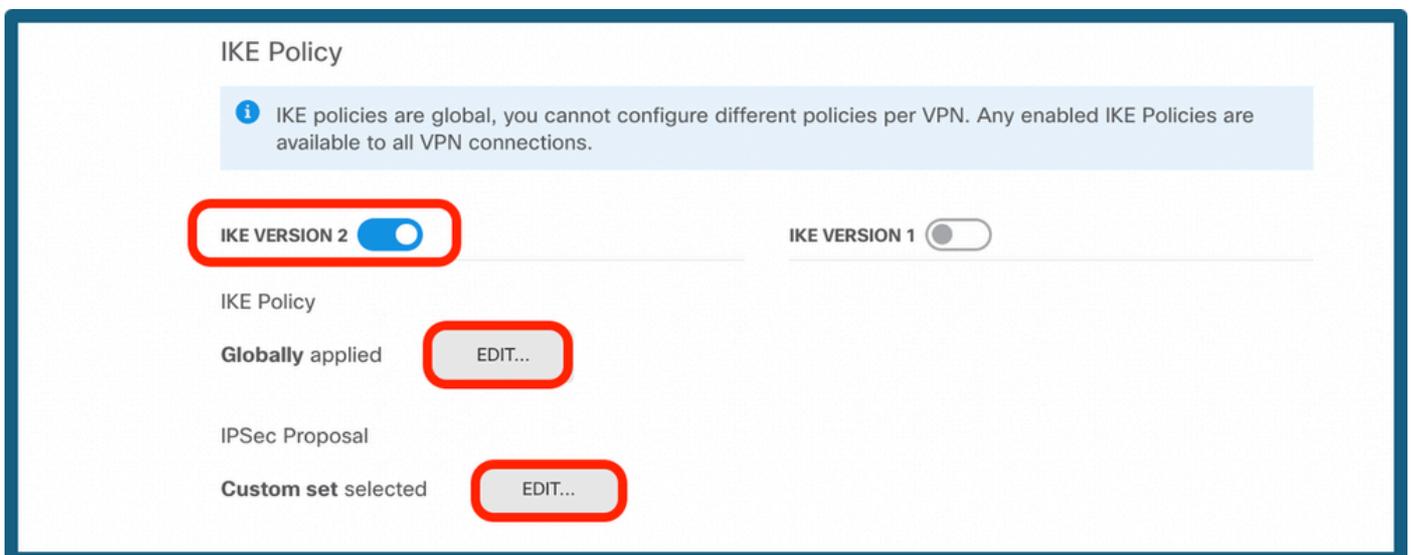
Configuração de VTI

Etapa 5. Escolha o VTI recém-criado ou um VTI que exista na Virtual Tunnel Interface. Forneça o endereço IP remoto.



Adicionar IP do Par

Etapa 6. Escolha a versão IKE e escolha o botão Edit para definir os parâmetros IKE e IPsec como mostrado na imagem.



Configurar a versão do IKE

Etapa 7a. Escolha o botão IKE Policy como mostrado na imagem e clique no botão ok ou Create New IKE Policy, se você quiser criar uma nova política.

Edit Globally: IKE v2 Policy



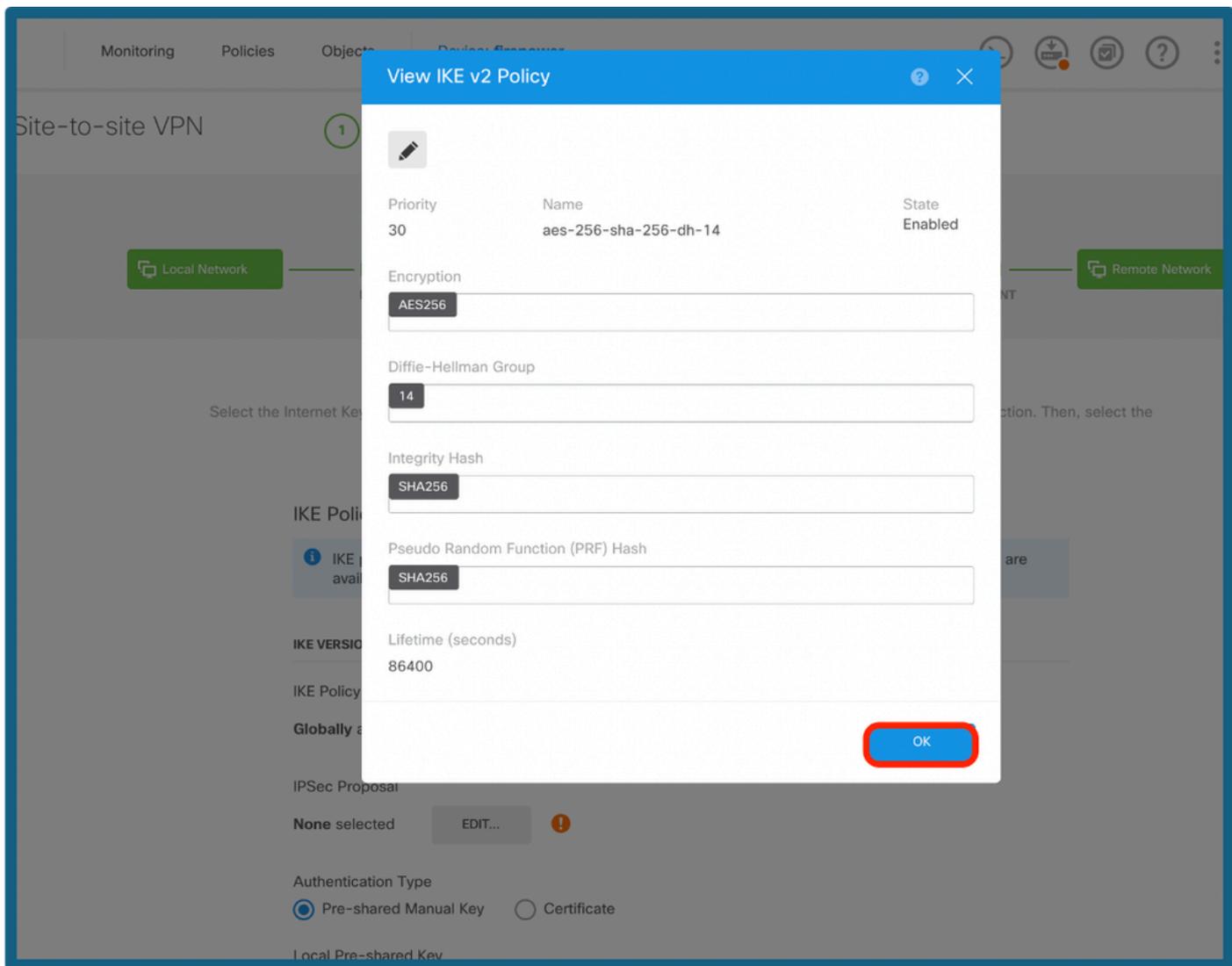
Filter

- AES-GCM-NULL-SHA 
- AES-SHA-SHA 
- DES-SHA-SHA 
- aes-256-sha-256-dh-14 
- ike2_policy 

Create New IKE Policy

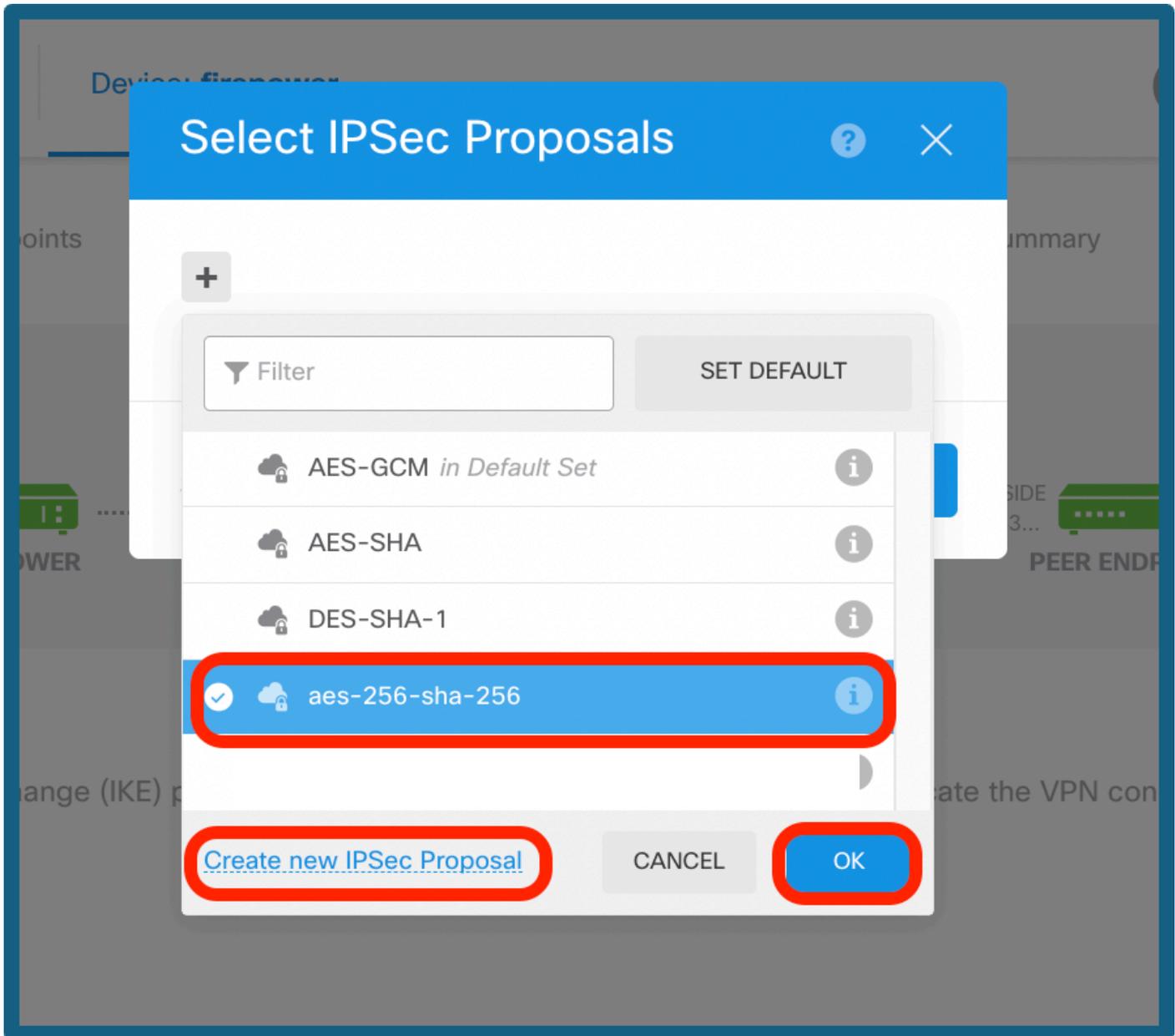
OK

Escolher Política IKE



Configuração da política IKE

Etapa 7b. Escolha o botão IPsec Policy como mostrado na imagem e clique no botão ok ou Create New IPsec Proposal, se você quiser criar uma nova proposta.



Selecionar Proposta IPsec

IKE v2 IPsec Proposal

Name
aes-256-sha-256

Encryption
AES256

Integrity Hash
SHA256

OK

Configuração da proposta de IPsec

Etapa 8a. Selecione o Tipo de autenticação. Se Pre-shared Manual Key for usado, forneça a chave pré-compartilhada Local e Remote.

Etapa 8b. (Opcional) Escolha as configurações de Perfect Forward Secrecy. Configure IPsec Lifetime Duration and Lifetime Size e clique em Next.

IKE VERSION 2 IKE VERSION 1

IKE Policy

Globally applied

IPSec Proposal

Custom set selected

Authentication Type

Pre-shared Manual Key Certificate

Local Pre-shared Key

Remote Peer Pre-shared Key

IPSEC SETTINGS

Lifetime Duration seconds
120 - 2147483647; (Default: 28800)

Lifetime Size kilobytes
10 - 2147483647; (Default: 4608000).
Leave empty for Unlimited.

Additional Options

Diffie-Hellman Group for Perfect Forward Secrecy

PSK e configuração vitalícia

Etapa 9. Revise a configuração e clique em Finish.

Summary

Review your configuration. Click Finish to save the connection, or Back to edit settings. When you click Finish, this information will be copied to the clipboard so that you can save it and use it to configure the remote endpoint.

Vti-Ipsec Connection Profile

i Peer endpoint needs to be configured according to specified below configuration.

VPN Access Interface IP tunnel10 (1.1.1.1)



Peer IP Address 10.106.63.23

IKE V2

IKE Policy aes-256-sha256-sha256-14

IPSec Proposal aes-256-sha-256

Authentication Type Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

Lifetime Duration 28800 seconds

Lifetime Size 4608000 kilobytes

ADDITIONAL OPTIONS

Diffie-Hellman Group Null (not selected)

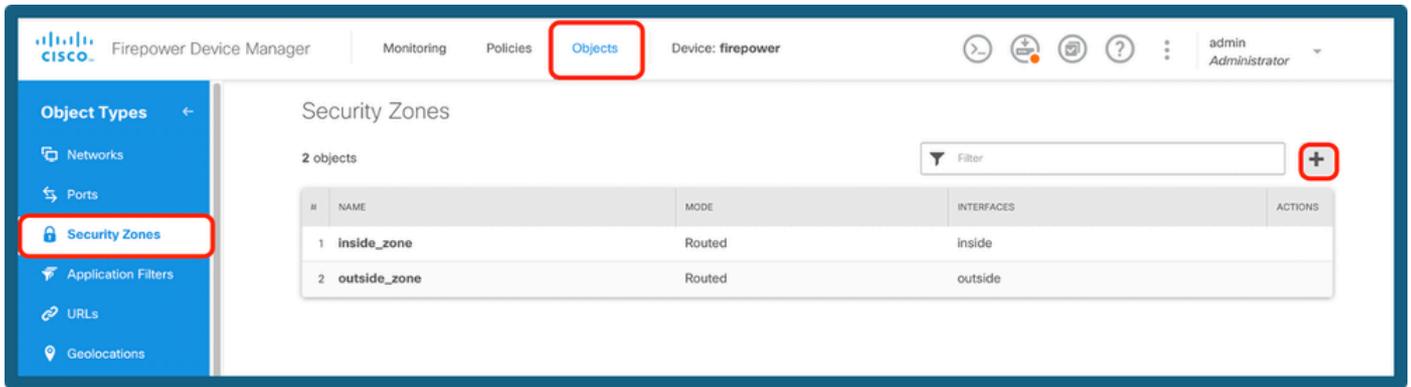
i Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

BACK

FINISH

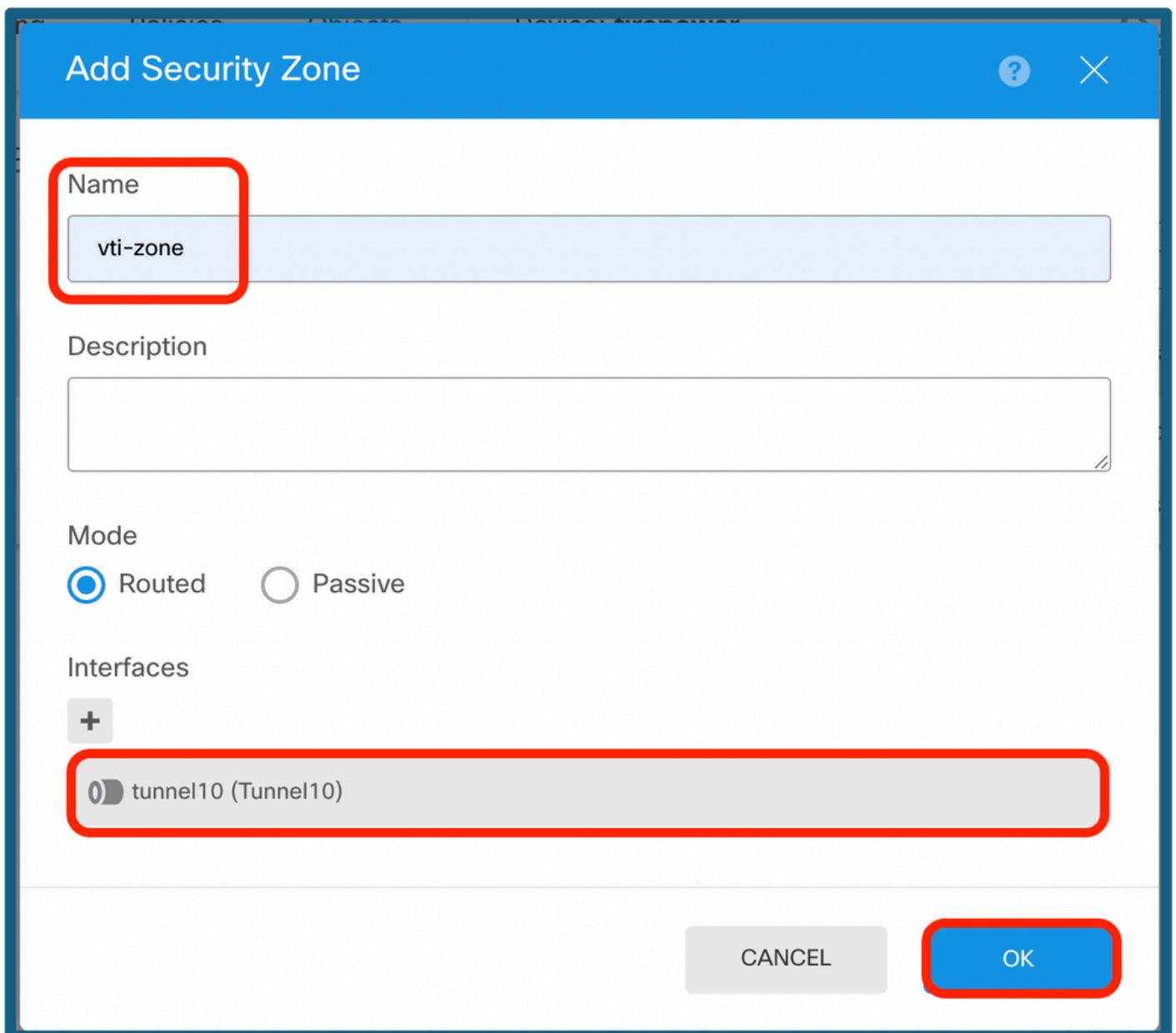
Resumo da configuração

Etapa 10a. Navegue até Objetos > Zonas de segurança e clique no ícone +.



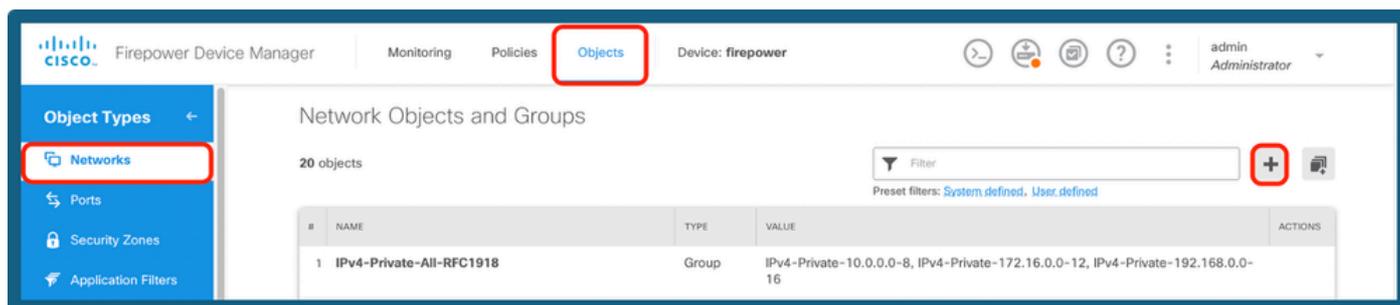
Adicionar uma zona de segurança

Etapa 10b. Crie uma região e selecione a interface VTI como mostrado abaixo.



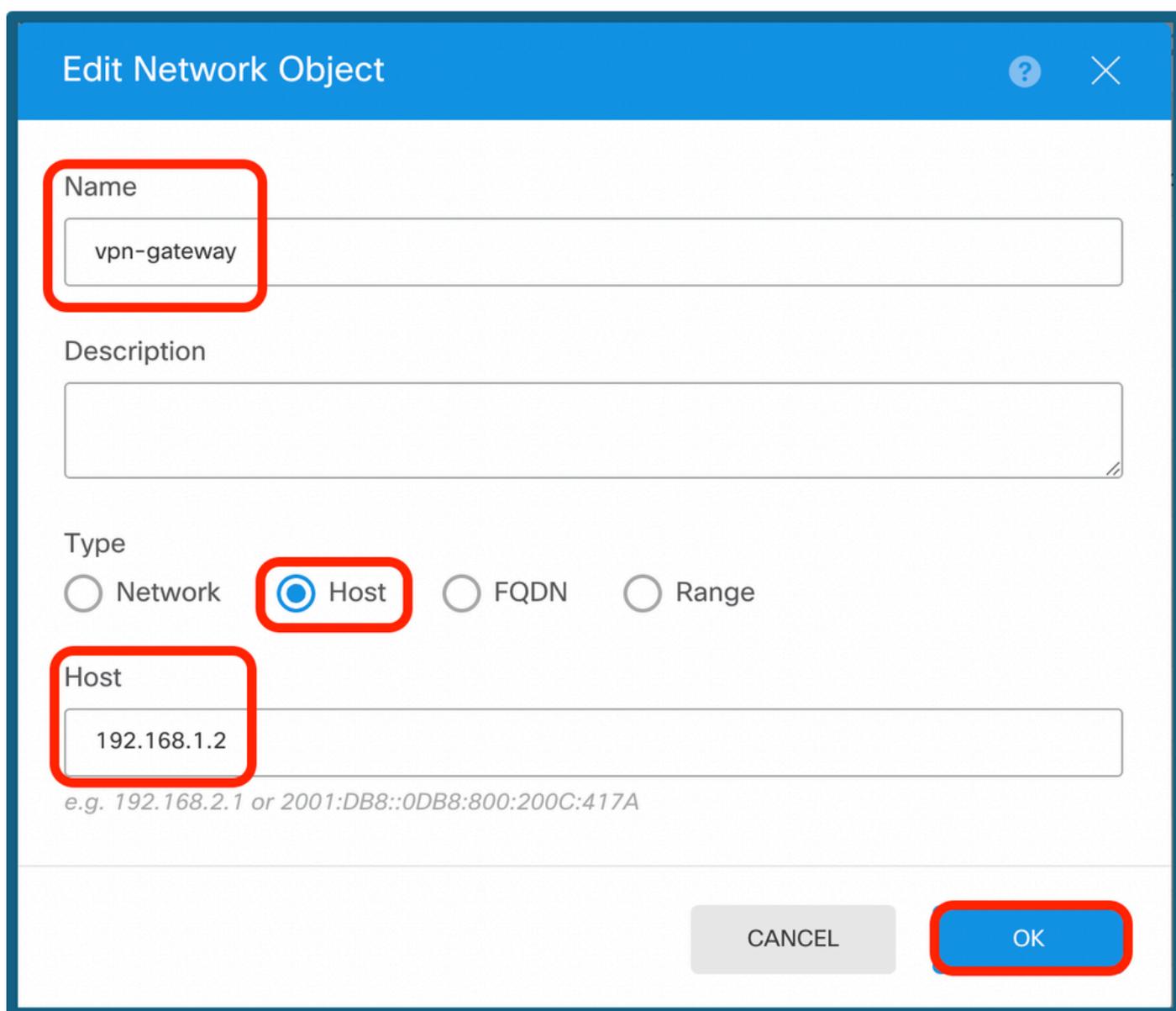
Configuração da zona de segurança

Etapa 11a. Navegue até Objetos > Redes, clique no ícone +.



Adicionar objetos de rede

Etapa 11b. Adicione um objeto de host e crie um gateway com o ip de túnel da extremidade do peer.



Configurar o gateway VPN

Etapa 11c. Adicione a sub-rede remota e a sub-rede local.

Edit Network Object ? ×

Name
remote-vpn-network

Description

Type
 Network Host FQDN Range

Network
172.16.10.0/24
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL OK

Configuração de IP remoto

Edit Network Object ? ×

Name
inside-network

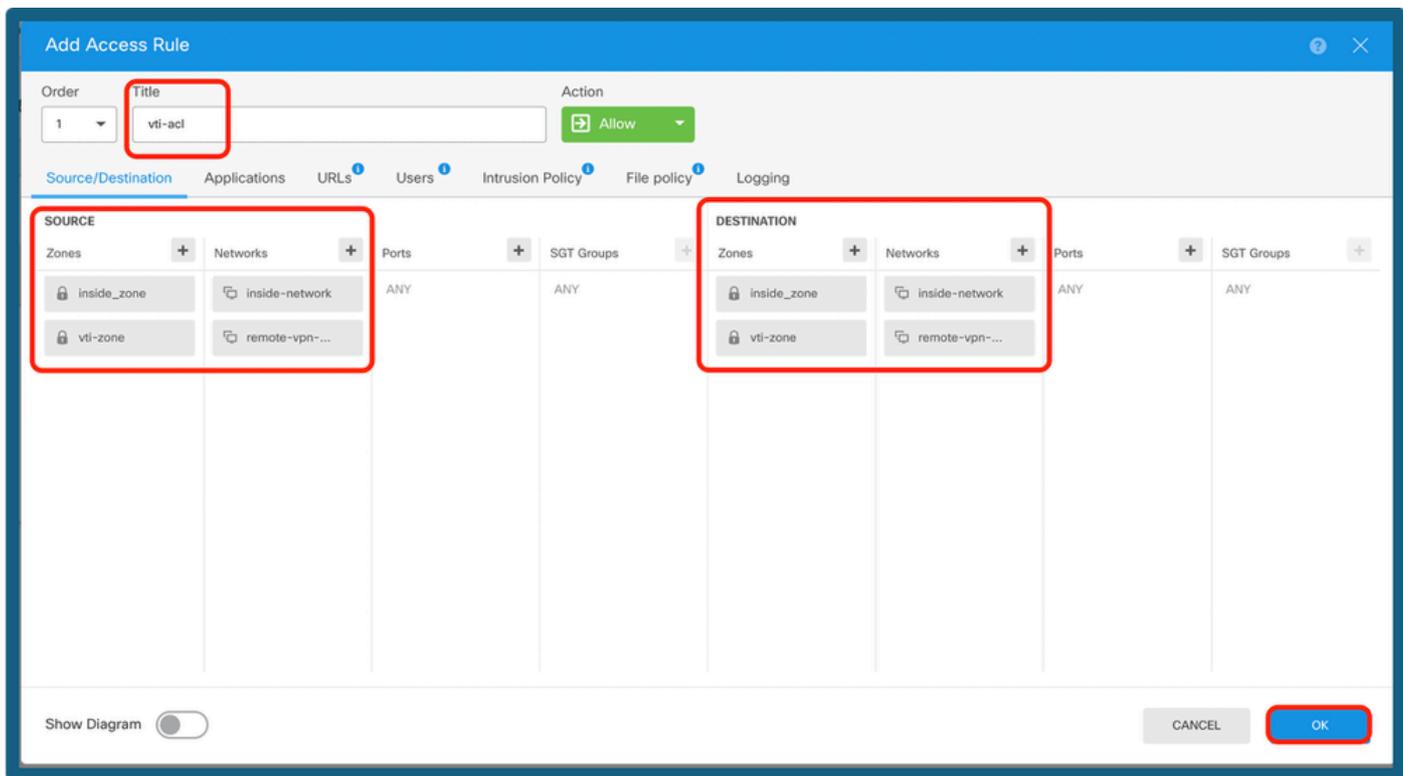
Description

Type
 Network Host FQDN Range

Network
10.10.10.0/24
e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

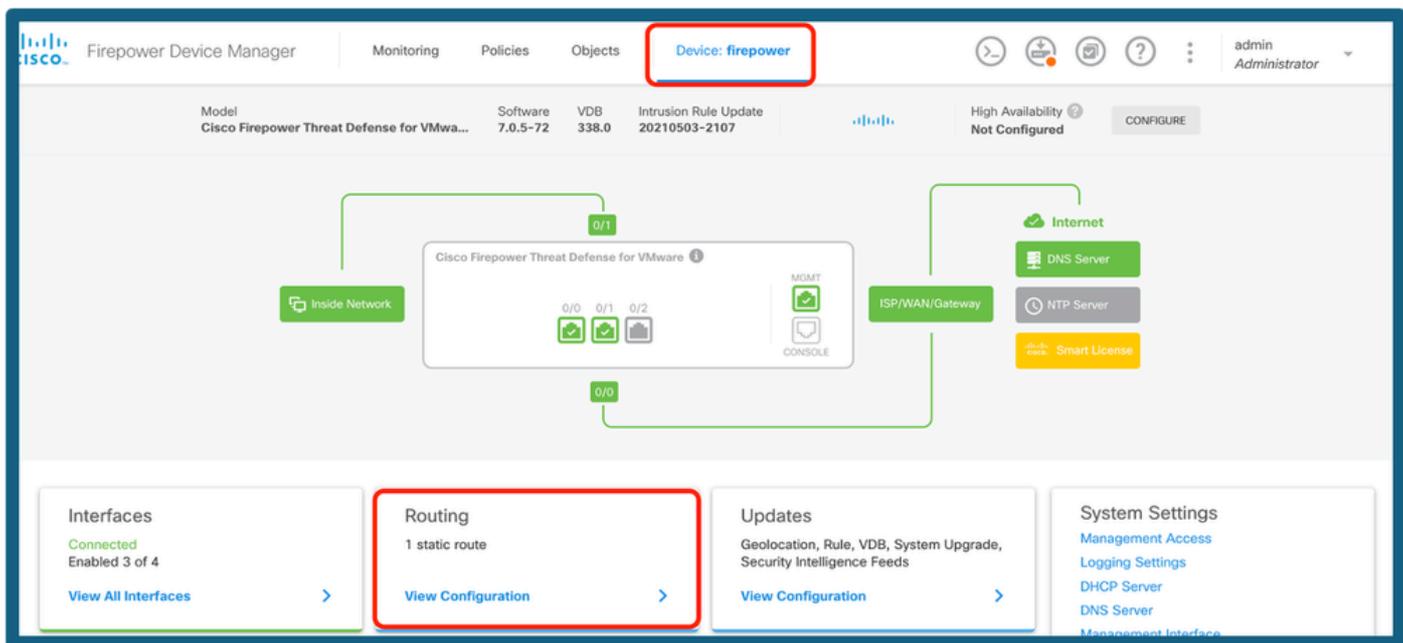
Configuração de IP local

Etapa 12. Navegue até Device > Policies e configure a Access Control Policy.



Adicionar Política de Controle de Acesso

Etapa 13a. Adicione o roteamento sobre o túnel VTI. Navegue até Device > Routing.



Selecionar Roteamento

Etapa 13b. Navegue até Static Route na guia Routing. Clique no ícone +.

Device Summary
Routing

Add Multiple Virtual Routers ▾ Commands ▾ BGP Global Settings

Static Routing | BGP | OSPF | EIGRP | ECMP Traffic Zones

1 route Filter +

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	default	outside	IPv4	0.0.0.0/0	10.106.52.1		1	

Adicionar rota

Etapa 13c. Forneça a interface, escolha a rede, forneça o gateway. Click OK.

Add Static Route

Name
vti-route

Description

Interface
tunnel10 (Tunnel10)

Protocol
 IPv4 IPv6

Networks
+
remote-vpn-network

Gateway
vpn-gateway

Metric
1

SLA Monitor Applicable only for IPv4 Protocol type
Please select an SLA Monitor

CANCEL OK

Configurar a rota estática

Etapa 14. Navegue até Implantar. Revise as alterações e clique em Implantar agora.

Pending Changes

✓ **Last Deployment Completed Successfully**
26 Jun 2025 05:27 PM. [See Deployment History](#)

Deployed Version (26 Jun 2025 05:27 PM)	Pending Version
+ Static Route Added: vti-route	
-	metricValue: 1
-	ipType: IPv4
-	name: vti-route
iface:	
-	tunnel10
gateway:	
-	vpn-gateway
networks:	
-	remote-vpn-network
+ Access Rule Added: vti-acl	
-	logFiles: false
-	eventLogAction: LOG_NONE
-	ruleId: 268435458
-	name: vti-acl
sourceZones:	
-	vti-zone
-	inside_zone
destinationZones:	
-	vti-zone
-	inside_zone
sourceNetworks:	
-	remote-vpn-network
-	inside-network
destinationNetworks:	

MORE ACTIONS ▼ CANCEL **DEPLOY NOW** ▼

Implantar a configuração

Verificar

Quando a implantação estiver concluída, você poderá verificar o status do túnel na CLI usando os comandos:

1. show crypto ikev2 sa
2. show crypto ipsec sa <peer-ip>

```
> show crypto ikev2 sa
```

```
IKEv2 SAs:
```

```
Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Remote Status Role
3294213359 10.106.52.222/500 10.106.63.23/500 READY INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/141 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: 0x26a14554/0xd5db88bc
```

```
> show crypto ipsec sa
```

```
interface: tunnel10
```

```
Crypto map tag: __vti-crypto-map-5-0-10, seq num: 65280, local addr: 10.106.52.222
```

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 10.106.63.23
```

comandos show

Informações Relacionadas

Para obter mais informações sobre VPNs Site a Site no FTD gerenciado pelo FDM, você pode encontrar o guia de configuração completo aqui:

[FTD Gerenciado pelo Guia de Configuração do FDM](#)

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.