

# Configurar o túnel VPN site a site baseado em rota no FTD gerenciado pelo FMC

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Limitações e restrições](#)

[Etapas de configuração no FMC](#)

[Verificar](#)

[na GUI do FMC](#)

[Da CLI do FTD](#)

---

## Introdução

Este documento descreve como configurar um túnel VPN site a site baseado em rota estática em um Firepower Threat Defense gerenciado por um Firepower Management Center.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão básica de como um túnel VPN funciona.
- Entender como navegar pelo FMC.

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Cisco Firepower Management Center (FMC) versão 6.7.0
- Cisco Firepower Threat Defense (FTD) versão 6.7.0

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 use 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 IPsec são definidos como 0.0.0.0/0.0.0.0. Isso significa que todo o 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). Para obter a configuração da Dynamic Virtual Tunnel Interface (DVTI) no Secure Firewall, consulte este [documento](#).

## Limitações e restrições


Estas são limitações e restrições conhecidas para túneis baseados em rota no FTD:

- Suporta somente IPsec. Não há suporte para GRE.
- Suporta somente interfaces IPv4, bem como IPv4, redes protegidas ou payload de VPN (Sem suporte para IPv6).
- O roteamento estático e somente o protocolo de roteamento dinâmico BGP são suportados para interfaces VTI que classificam o tráfego para VPN (Sem suporte para outros protocolos como OSPF, RIP e assim por diante).
- Somente 100 VTIs são suportados por interface.
- Não há suporte para VTI em um Cluster FTD.
- O VTI não é suportado nestas políticas:
  - qos
  - NAT
  - Configurações de plataforma


Esses algoritmos não são mais suportados no FMC/FTD versão 6.7.0 para novos túneis VPN (o FMC suporta todas as cifras removidas para gerenciar o FTD < 6.7):

- Não há suporte para 3DES, DES e Criptografia NULL na Política IKE.
- Os grupos DH 1, 2 e 24 não têm suporte na Política IKE e na Proposta IPsec.

- Não há suporte para a Integridade MD5 na Política IKE.
- PRF MD5 não é suportado na política IKE.
- Os algoritmos de criptografia DES, 3DES, AES-GMAC, AES-GMAC-192 e AES-GMAC-256 não são suportados na Proposta IPsec.

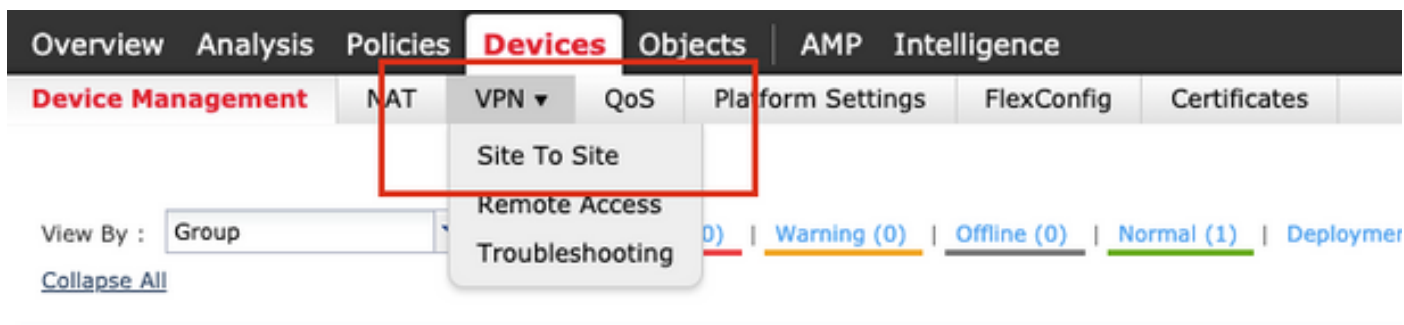
 Observação: isso é válido tanto para a rota de site para site quanto para túneis VPN baseados em políticas. A fim de atualizar um FTD antigo para 6.7 do FMC, desencadeia uma verificação de pré-validação que alerta o utilizador sobre as alterações que dizem respeito às cifras removidas que bloqueiam a atualização.

FTD 6.7 gerenciado via FMC 6.7	Configuração disponível	Túnel VPN de Site a Site
Instalação nova	Cifras fracas disponíveis, mas não podem ser usadas para configurar o dispositivo FTD 6.7.	Cifras fracas disponíveis, mas não podem ser usadas para configurar o dispositivo FTD 6.7.
Atualização: FTD configurado apenas com cifras fracas	Atualização do FMC 6.7 UI, uma verificação de pré-validação exibe um erro. A atualização está bloqueada até a reconfiguração.	Após a atualização do FTD, e suponha que o peer não tenha alterado suas configurações, o túnel será encerrado.
Atualização: FTD configurado apenas com algumas cifras fracas e algumas cifras fortes	Atualização do FMC 6.7 UI, uma verificação de pré-validação exibe um erro. A atualização está bloqueada até a reconfiguração.	Após a atualização do FTD, e suponha que o peer tenha cifras fortes, o túnel será restabelecido.
Atualização: país de classe C (não possui uma licença de criptografia forte)	Permitir DES é permitido	Permitir DES é permitido

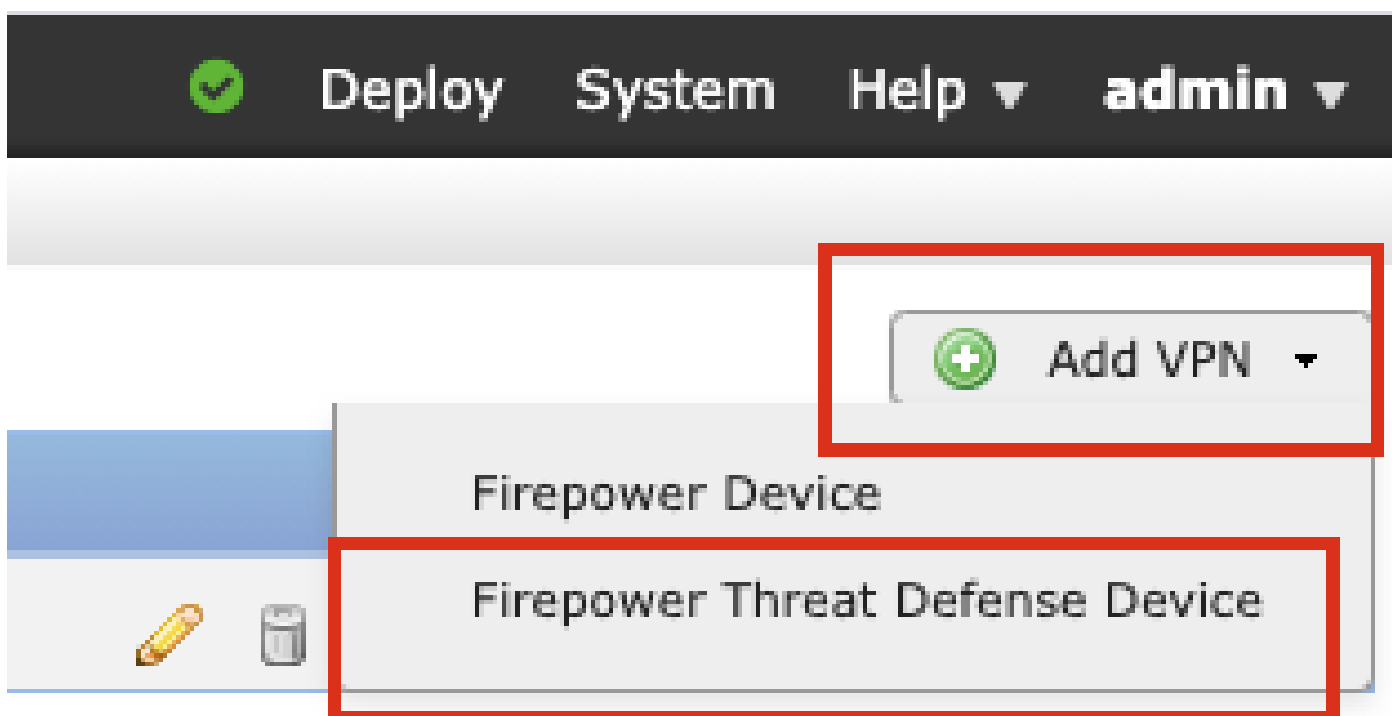
 Observação: não é necessário licenciamento adicional, a VPN baseada em rota pode ser configurada nos Modos licenciado e de avaliação. Sem a conformidade de criptografia (Export Controlled Features Enabled), somente o DES pode ser usado como algoritmo de criptografia.

## Etapas de configuração no FMC

Etapa 1. Navegue até Devices >VPN >Site To Site.



Etapa 2. Clique em Add VPN e escolha Firepower Threat Defense Device, como mostrado na imagem.



Etapa 3. Forneça um Nome da Topologia e selecione o Tipo de VPN como Baseado em Rota (VTI). Escolha a Versão IKE.

Para efeitos desta demonstração:

Nome da topologia: VTI-ASA

Versão do IKE: IKEv2

Topology Name:\* VTI-ASA

Policy Based (Crypto Map)  Route Based (VTI)

Network Topology:  Point to Point  Hub and Spoke  Full Mesh

IKE Version:\*  IKEv1  IKEv2

Etapa 4. Escolha o dispositivo no qual o túnel precisa ser configurado. Você pode optar por adicionar uma nova interface de túnel virtual (clique no ícone +), ou selecionar uma na lista que existe.

Endpoints | IKE | IPsec | Advanced

Node A

Device:\* FTD

Virtual Tunnel Interface:\* [Empty] +

Tunnel Source IP is Private [Edit VTI](#)

Connection Type:\* Bidirectional

Tunnel IP Address :  
Tunnel Source Interface :  
Tunnel Source Interface IP :

Node B

Device:\* Empty

Virtual Tunnel Interface:\* [Empty] +

Tunnel Source IP is Private [Edit VTI](#)

Connection Type:\* Bidirectional

Tunnel IP Address :  
Tunnel Source Interface :  
Tunnel Source Interface IP :

Etapa 5. Defina os parâmetros da New Virtual Tunnel Interface. Click OK.

Para efeitos desta demonstração:

Nome: VTI-ASA

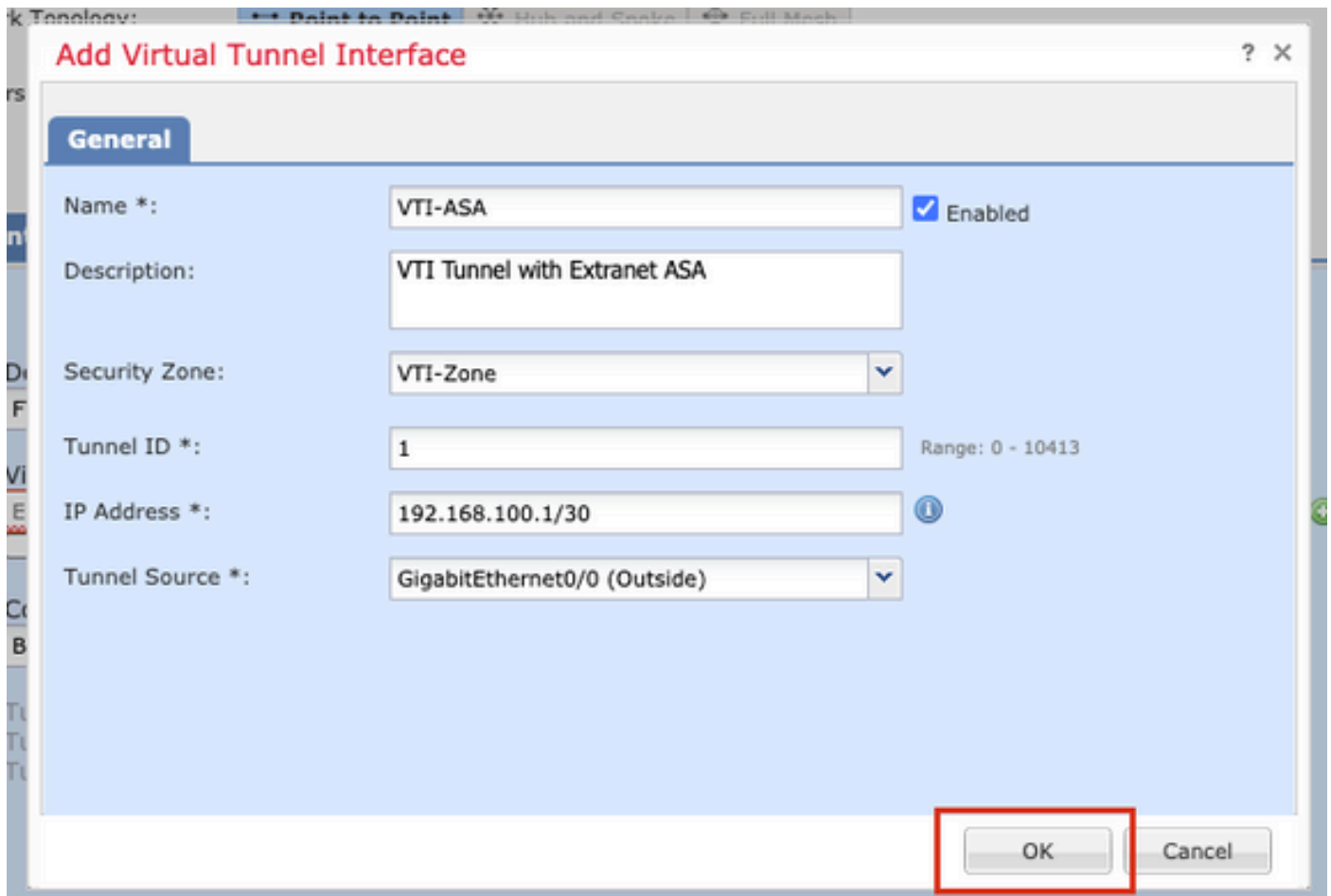
Descrição (Opcional): Túnel VTI com Extranet ASA

Zona de segurança: VTI-Zone

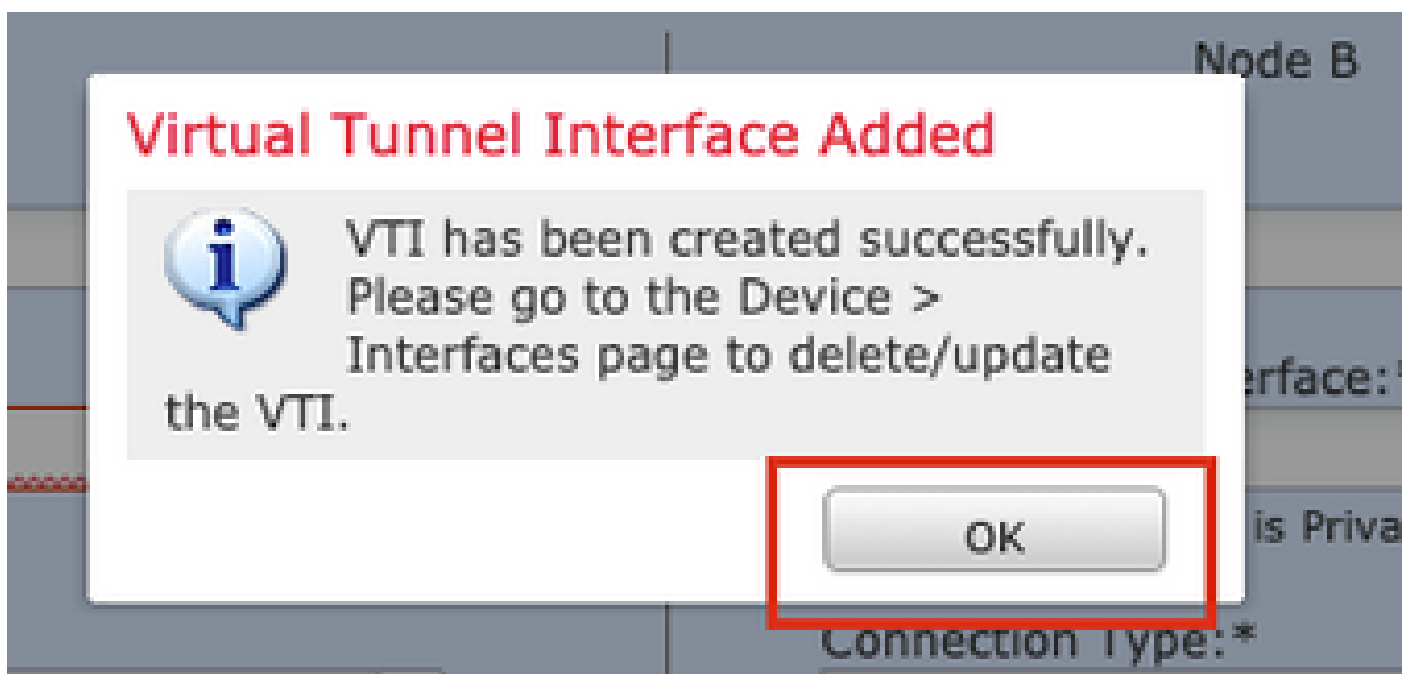
ID do túnel: 1

Endereço IP: 192.168.100.1/30

Origem do Túnel: GigabitEthernet0/0 (Externo)



Etapa 6. Clique em OK no pop-up que menciona que o novo VTI foi criado.



Passo 7. Escolha o VTI recém-criado ou um VTI que exista em Virtual Tunnel Interface. Forneça as informações para o Nó B (que é o dispositivo peer).

Para efeitos desta demonstração:

Dispositivo: Extranet

Nome do dispositivo: ASA-Peer

Endereço IP do endpoint: 10.106.67.252

**Create New VPN Topology**

Topology Name: \*

Policy Based (Crypto Map)  Route Based (VTI)

Network Topology:

IKE Version: \*  IKEv1  IKEv2

**Endpoints** | IKE | IPsec | Advanced

**Node A**

Device: \*

Virtual Tunnel Interface: \*   Tunnel Source IP is Private [Edit VTI](#)

Connection Type: \*

Tunnel IP Address : 192.168.100.1  
Tunnel Source Interface : Outside  
Tunnel Source Interface IP : 10.197.224.90

Additional Configuration ⓘ  
Route traffic to the VTI : [Routing Policy](#)  
Permit VPN traffic : [AC Policy](#)

**Node B**


Device: \*

Device Name: \*

Endpoint IP Address: \*

Etapa 8. Navegue até a guia IKE. Você pode optar por usar uma política predefinida ou clicar no botão + ao lado da guia Política e criar uma nova.

**IKEv2 Settings**

Policy:\* AES-GCM-NULL-SHA-LATEST 

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:\* 24 Characters (Range 1-127)

Etapa 9. (Opcional, se você criar uma nova Política IKEv2.) Forneça um Nome para a Política e selecione os Algoritmos a serem usados na política. Click Save.

Para efeitos desta demonstração:

Nome: ASA-IKEv2-Política

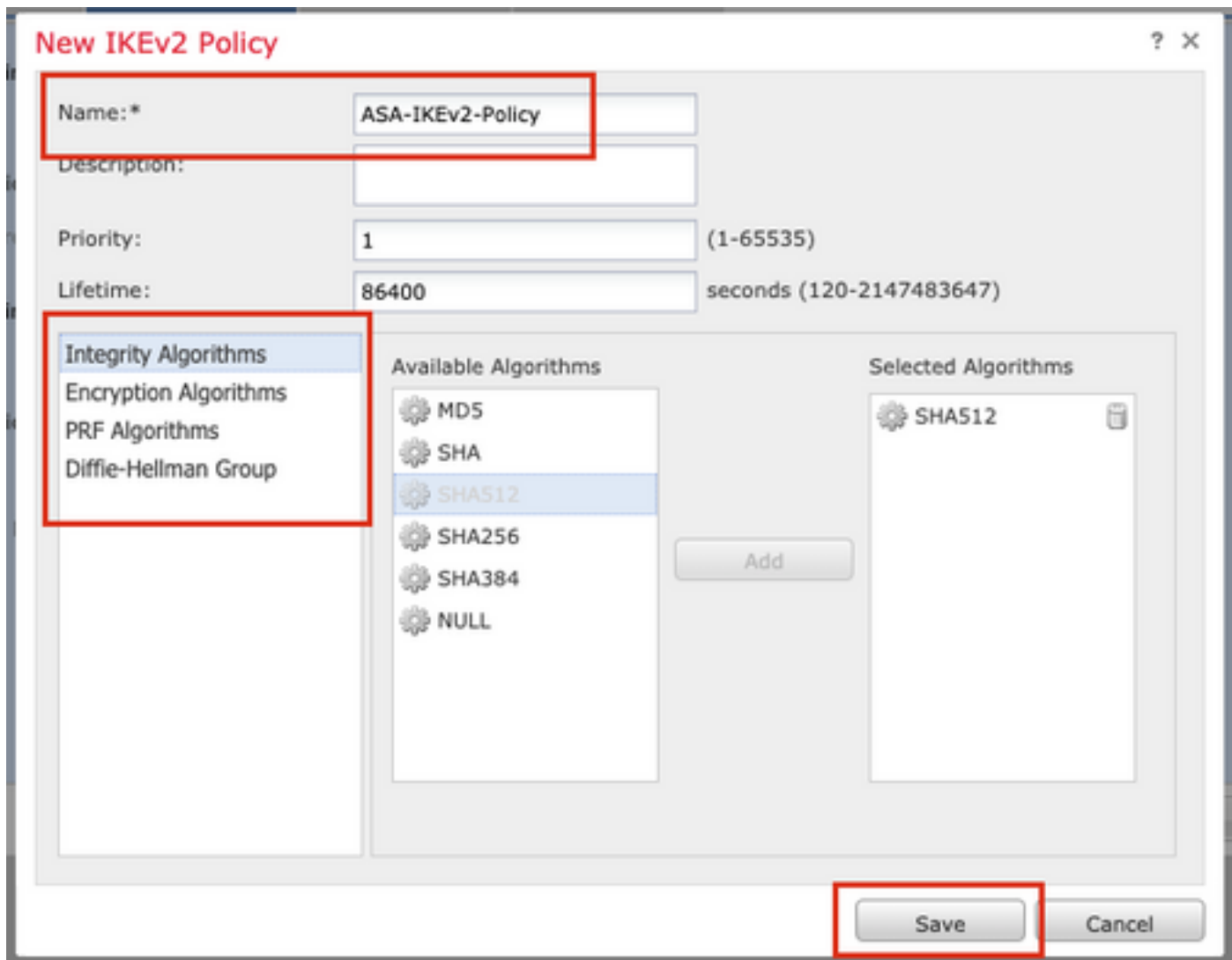
Algoritmos de integridade: SHA-512

Algoritmos de criptografia: AES-256

Algoritmos PRF: SHA-512

Grupo Diffie-Hellman: 21





Etapa 10. Escolha a política recém-criada ou a política existente. Selecione o Tipo de autenticação. Se uma chave manual pré-compartilhada for usada, forneça a chave nas caixas Key e Confirm Key .

Para efeitos desta demonstração:

Política: ASA-IKEv2-Política

Tipo de autenticação: chave manual pré-compartilhada

Tecla: cisco123

Confirmar chave: cisco123

Endpoints    **IKE**    IPsec    Advanced

**IKEv1 Settings**

Policy:\*    preshared\_sha\_aes256\_dh14\_3    [v]    [⊕]

Authentication Type:    Pre-shared Automatic Key    [v]

Pre-shared Key Length:\*    24    Characters    (Range 1-127)

---

**IKEv2 Settings**


Policy:\*    ASA-IKEv2-Policy    [v]    [⊕]

Authentication Type:    Pre-shared Manual Key    [v]

Key:\*    [.....]

Confirm Key:\*    [.....]

Enforce hex-based pre-shared key only



 Nota: Se ambos os terminais estiverem registrados no mesmo CVP, a opção de chave automática pré-compartilhada também pode ser utilizada.

Etapa 11. Navegue até a guia IPsec. Você pode optar por usar uma proposta de IPsec IKEv2 predefinida ou criar uma nova. Clique no botão Editar ao lado da guia IKEv2 IPsec Proposal.

Crypto Map Type:     Static     Dynamic

IKEv2 Mode:    Tunnel    [v]

Transform Sets:

IKEv1 IPsec Proposals     IKEv2 IPsec Proposals\* 

tunnel\_aes256\_sha    AES-GCM

Enable Security Association (SA) Strength Enforcement

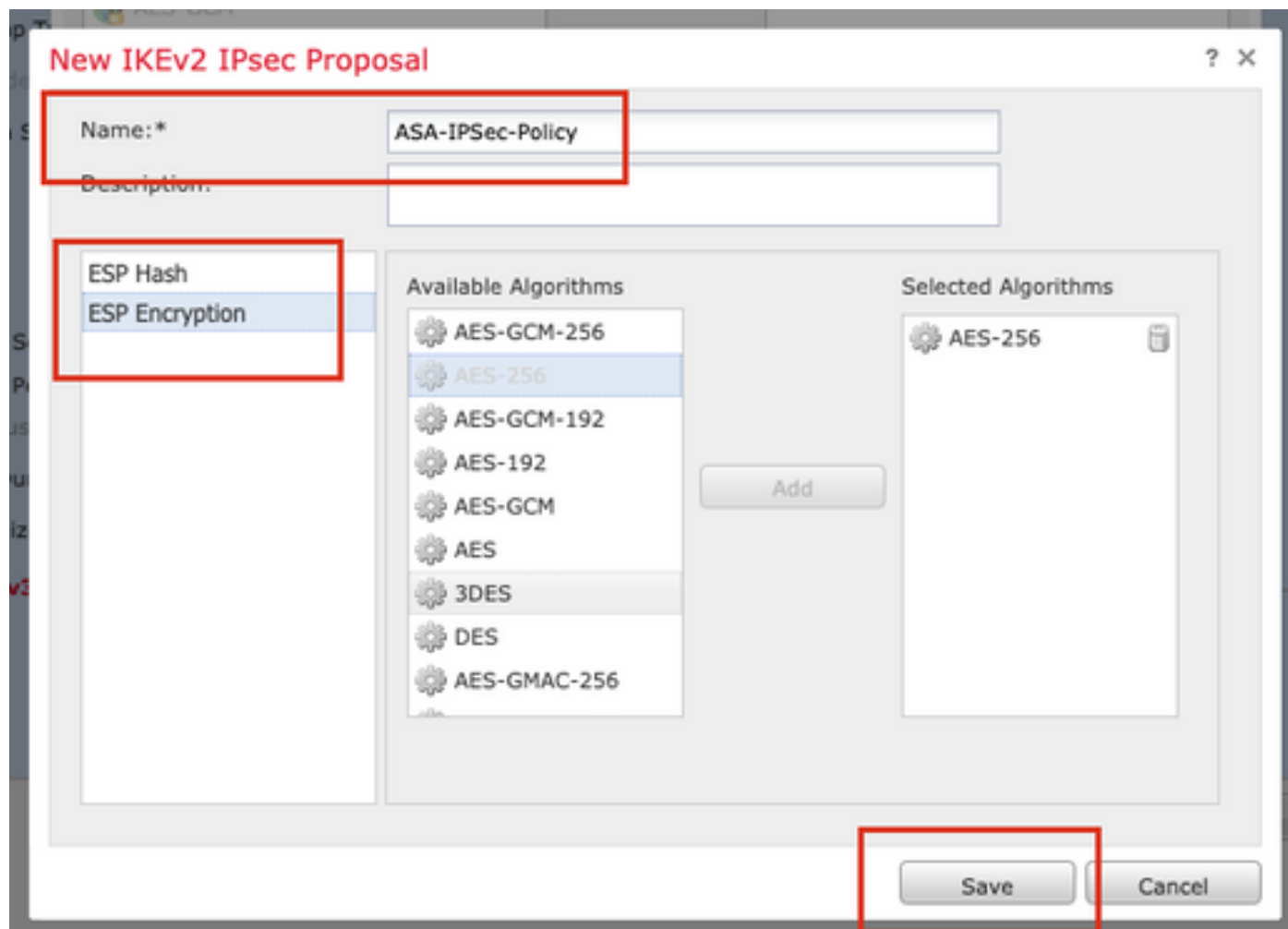
Etapa 12. (Opcional, se você criar uma nova Proposta IKEv2 IPsec.) Forneça um Nome para a Proposta e selecione os Algoritmos a serem usados na Proposta. Click Save.

Para efeitos desta demonstração:

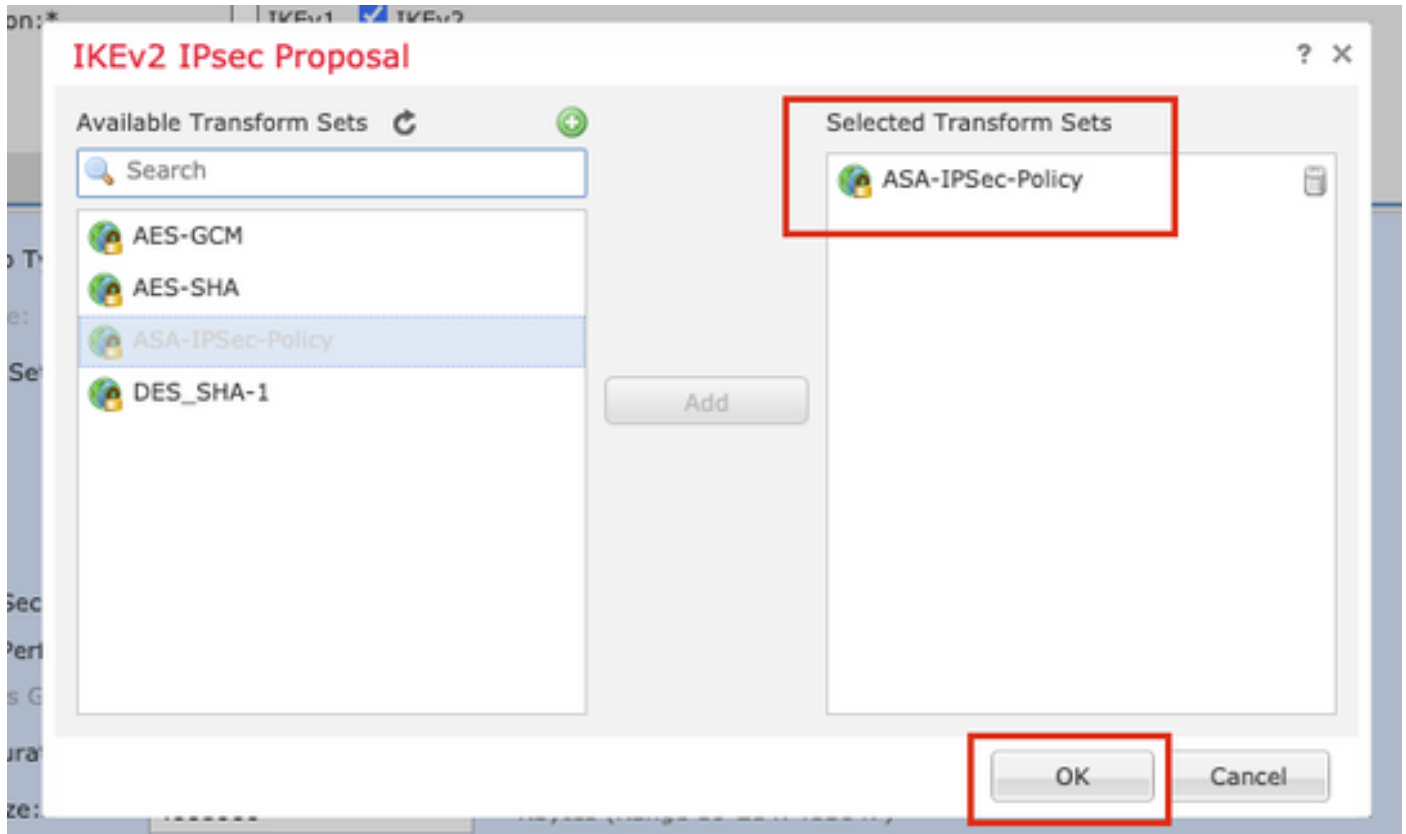
Nome: ASA-IPSec-Policy

Hash ESP: SHA-512

Criptografia ESP: AES-256



Etapa 13. Escolha a Proposta recém-criada ou a Proposta que existe na lista de propostas disponíveis. Click OK.



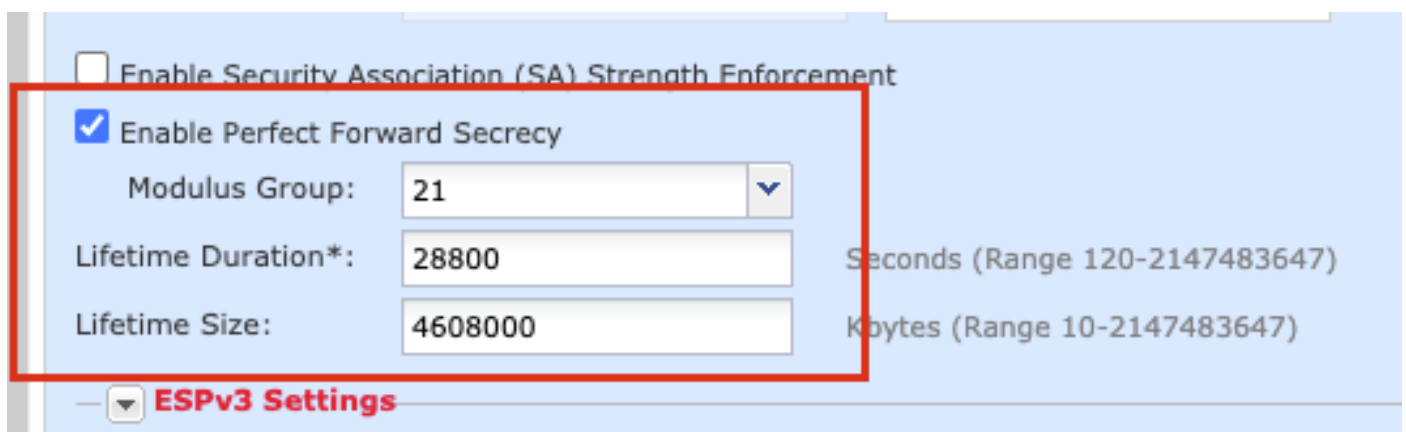
Etapa 14. (Opcional) Escolha as configurações de Perfect Forward Secrecy. Configure a Duração e o Tamanho da Vida Útil do IPsec.

Para efeitos desta demonstração:

Segredo de encaminhamento perfeito: Grupo de módulos 21

Duração da Vida Útil: 28800 (Padrão)

Tamanho do Tempo de Vida: 4608000 (Padrão)



Etapa 15. Verifique as configurações definidas. Clique em Salvar, conforme mostrado nesta imagem.

Topology Name:\*

Policy Based (Crypto Map)  Route Based (VTI)

Network Topology:

IKE Version:\*  IKEv1  IKEv2

---

Endpoints | IKE | **IPsec** | Advanced

Crypto Map Type:  Static  Dynamic

IKEv2 Mode:

Transform Sets:

IKEv1 IPsec Proposals	IKEv2 IPsec Proposals*
tunnel_aes256_sha	ASA-IPsec-Policy

Enable Security Association (SA) Strength Enforcement

Enable Perfect Forward Secrecy


Modulus Group:

Lifetime Duration\*:  Seconds (Range 120-2147483647)

Lifetime Size:  Kbytes (Range 10-2147483647)

— **ESPv3 Settings** —

Etapa 16. Configure a Política de Controle de Acesso. Navegue até Políticas > Access Control > Access Control. Edite a Política aplicada ao FTD.

 Observação: sysopt connection permit-vpn não funciona com túneis VPN Baseados em Rota. As regras de controle de acesso precisam ser configuradas para zonas IN-> OUT e OUT -> IN.

Forneça as Zonas de origem e as Zonas de destino na guia Zonas .

Forneça as redes de origem, redes de destino na guia Redes . Clique em Add.

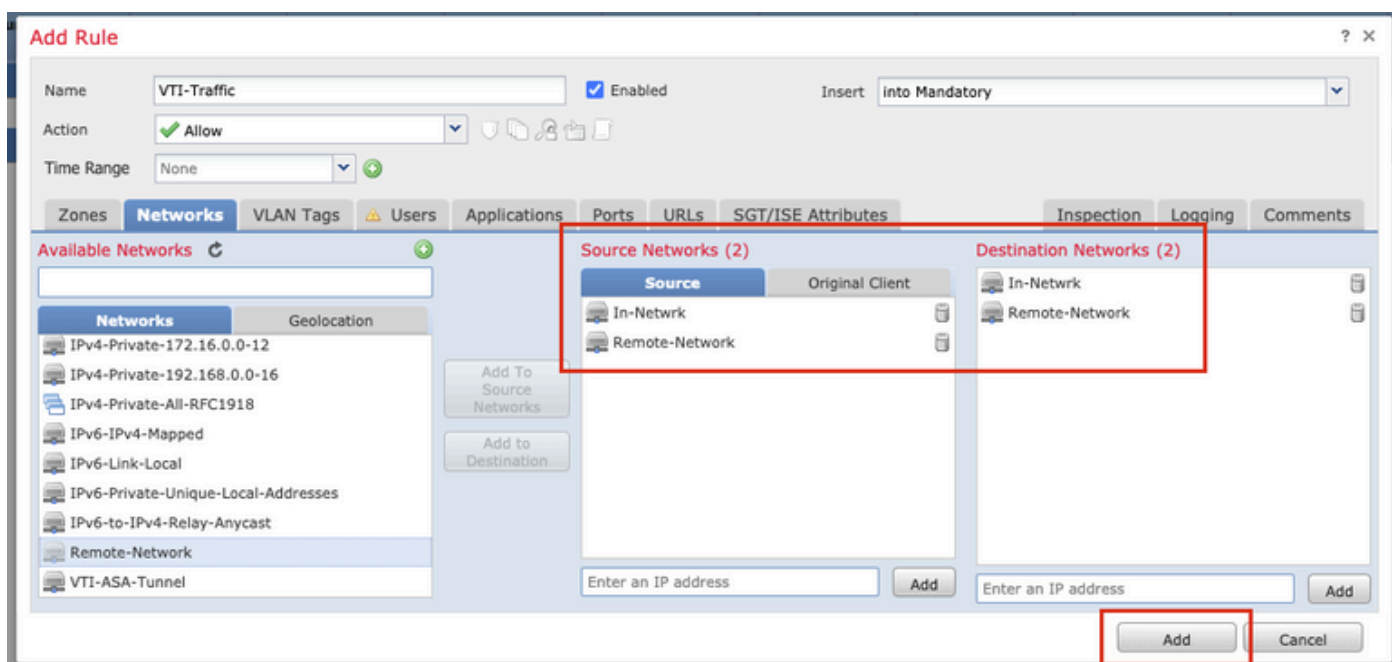
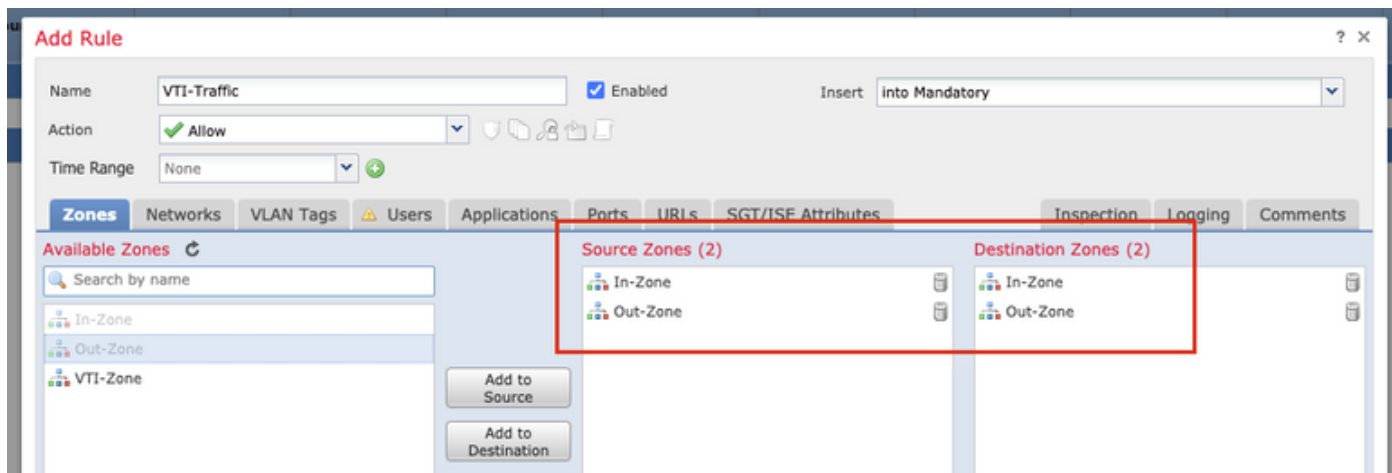
Para efeitos desta demonstração:

Zonas de origem: na zona e fora da zona

Zonas de destino: Out-Zone e In-Zone

Redes de origem: rede interna e remota

Redes de destino: rede remota e na rede



Etapa 17. Adicione o roteamento sobre o túnel VTI. Navegue até Devices > Device Management. Edite o dispositivo no qual o túnel VTI está configurado.

Navegue até Static Route na guia Routing. Clique em Add Route.

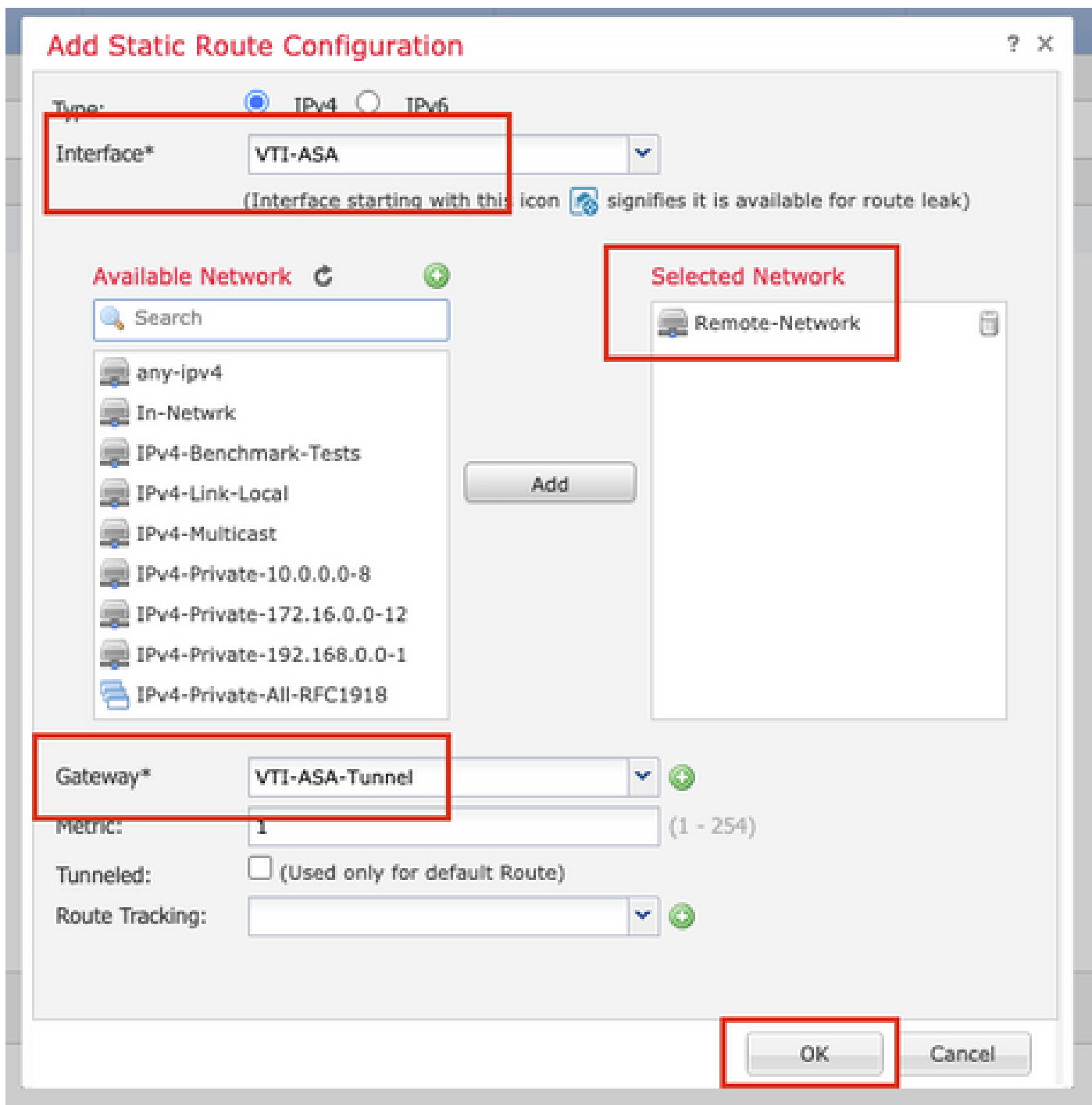
Forneça a interface, escolha a rede, forneça o gateway. Click OK.

Para efeitos desta demonstração:

Interface: VTI-ASA

Rede: Rede Remota

Gateway: túnel VTI-ASA



Etapa 18. Navegue até Implantar > Implantação. Escolha o FTD no qual a configuração precisa ser implantada e clique em Implantar.

Configuração enviada por push para a CLI do FTD após implantação bem-sucedida:

```
<#root>
```

```
crypto ikev2 policy 1
```

```
encryption aes-256  
integrity sha512  
group 21  
prf sha512  
lifetime seconds 86400
```

```
crypto ikev2 enable Outside

crypto ipsec ikev2 ipsec-proposal CSM_IP_1

  protocol esp encryption aes-256
  protocol esp integrity sha-512

crypto ipsec profile FMC_IPSEC_PROFILE_1

  set ikev2 ipsec-proposal CSM_IP_1
  set pfs group21

group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
  vpn-idle-timeout 30
  vpn-idle-timeout alert-interval 1
  vpn-session-timeout none
  vpn-session-timeout alert-interval 1
  vpn-filter none
  vpn-tunnel-protocol ikev1 ikev2

tunnel-group 10.106.67.252 type ipsec-l2l
tunnel-group 10.106.67.252 general-attributes
  default-group-policy .DefaultS2SGroupPolicy
tunnel-group 10.106.67.252 ipsec-attributes
  ikev2 remote-authentication pre-shared-key *****
  ikev2 local-authentication pre-shared-key *****

interface Tunnel1

  description VTI Tunnel with Extranet ASA
  nameif VTI-ASA

  ip address 192.168.100.1 255.255.255.252
  tunnel source interface Outside
  tunnel destination 10.106.67.252
  tunnel mode ipsec ipv4

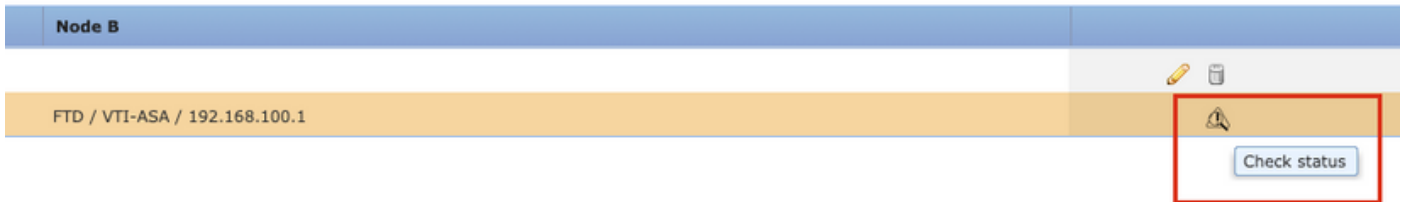
  tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

## Verificar

na GUI do FMC

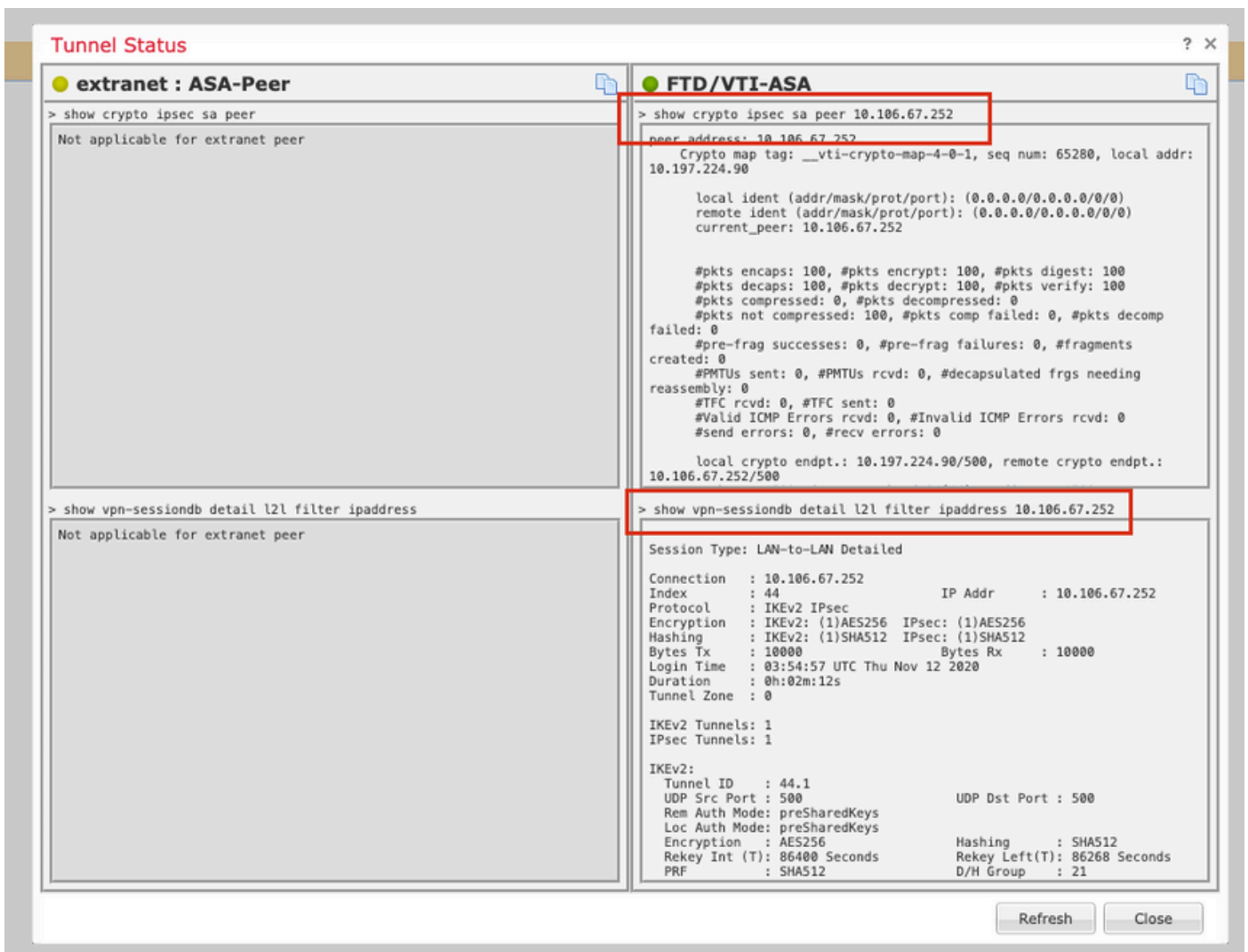
Clique na opção Check Status para monitorar o status ao vivo do túnel VPN a partir da própria GUI





Isso inclui estes comandos extraídos da CLI do FTD:

- show crypto ipsec sa peer <Peer IP Address>
- show vpn-sessiondb detail l2l filter ipaddress <Peer IP Address>



Da CLI do FTD

Esses comandos podem ser usados na CLI do FTD para visualizar a configuração e o status dos túneis VPN.

```
show running-config crypto
show running-config nat
```

```
show running-config route
show crypto ikev1 sa detailed
show crypto ikev2 sa detailed
show crypto ipsec sa detailed
show vpn-sessiondb detail 121
```

## 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.