

Configuração da VPN site a site no FTD Gerenciado pelo FMC

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configuração](#)

[Etapa 1. Defina a topologia de VPN.](#)

[Etapa 2. Configurar parâmetros IKE.](#)

[Etapa 3. Configurar parâmetros de IPsec.](#)

[Etapa 4. Ignorar Controle de Acesso.](#)

[Etapa 5. Crie uma Política de Controle de Acesso.](#)

[Etapa 6. Configurar isenção de NAT.](#)

[Passo 7. Configure o ASA.](#)

[Verificar](#)

[Solução de problemas e depuração](#)

[Problemas iniciais de conectividade](#)

[Problemas específicos de tráfego](#)

Introdução

Este documento descreve como configurar a VPN site a site no Firepower Threat Defense (FTD) gerenciado pelo FMC.

Pré-requisitos

Requisitos

Você deve ter conhecimento destes tópicos:

- Entendimento básico de VPN
- Experiência com o Firepower Management Center
- Experiência com a linha de comando ASA

Componentes Utilizados

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

- FTD 6.5 da Cisco
- ASA 9.10(1)32
- IKEv2

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.

Configuração

Comece com a configuração no FTD com o FirePower Management Center.

Etapa 1. Defina a topologia de VPN.

1. Navegue até **Devices > VPN > Site To Site**. Em Adicionar VPN, clique em **Dispositivo Firepower Threat Defense**, como mostrado nesta imagem.

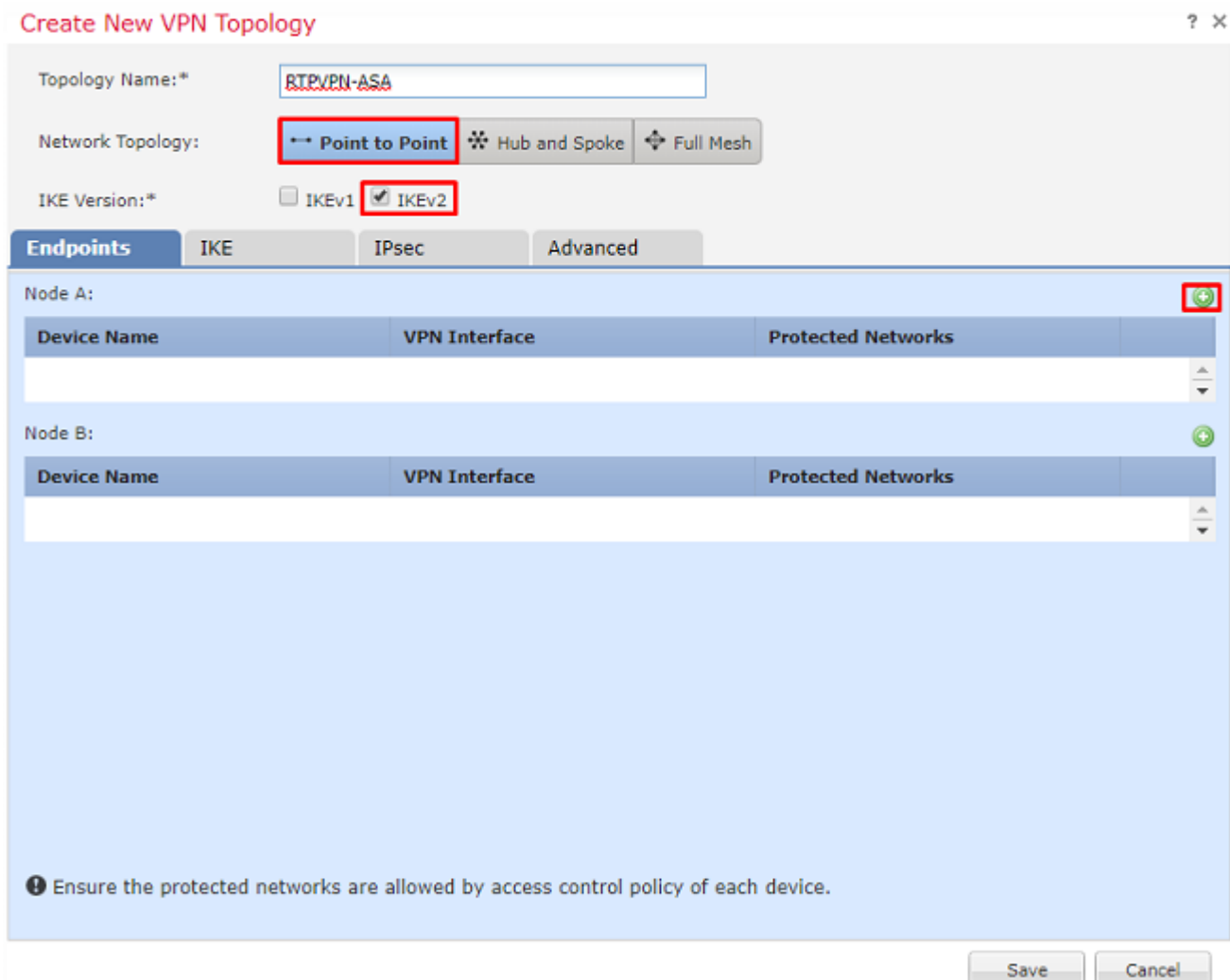


2. **Create New VPN Topology** é exibido. Dê à VPN um nome que seja facilmente identificável.

Topologia de rede: ponto a ponto

Versão do IKE: IKEv2

Neste exemplo, quando você seleciona endpoints, o Nó A é o FTD e o Nó B é o ASA. Clique no botão de mais verde para adicionar dispositivos à topologia, como mostrado nesta imagem.



3. Adicione o FTD como o primeiro ponto final.

Escolha a interface em que um mapa de criptografia é colocado. O endereço IP deve ser preenchido automaticamente a partir da configuração do dispositivo.

Clique no sinal de mais verde em Redes protegidas, como mostrado nesta imagem, para selecionar quais sub-redes devem ser criptografadas nesta VPN.

Add Endpoint ? x

Device:* FTD

Interface:* outside

IP Address:* 172.16.100.20

This IP is Private

Connection Type: Bidirectional

Certificate Map: [dropdown] +

Protected Networks:*

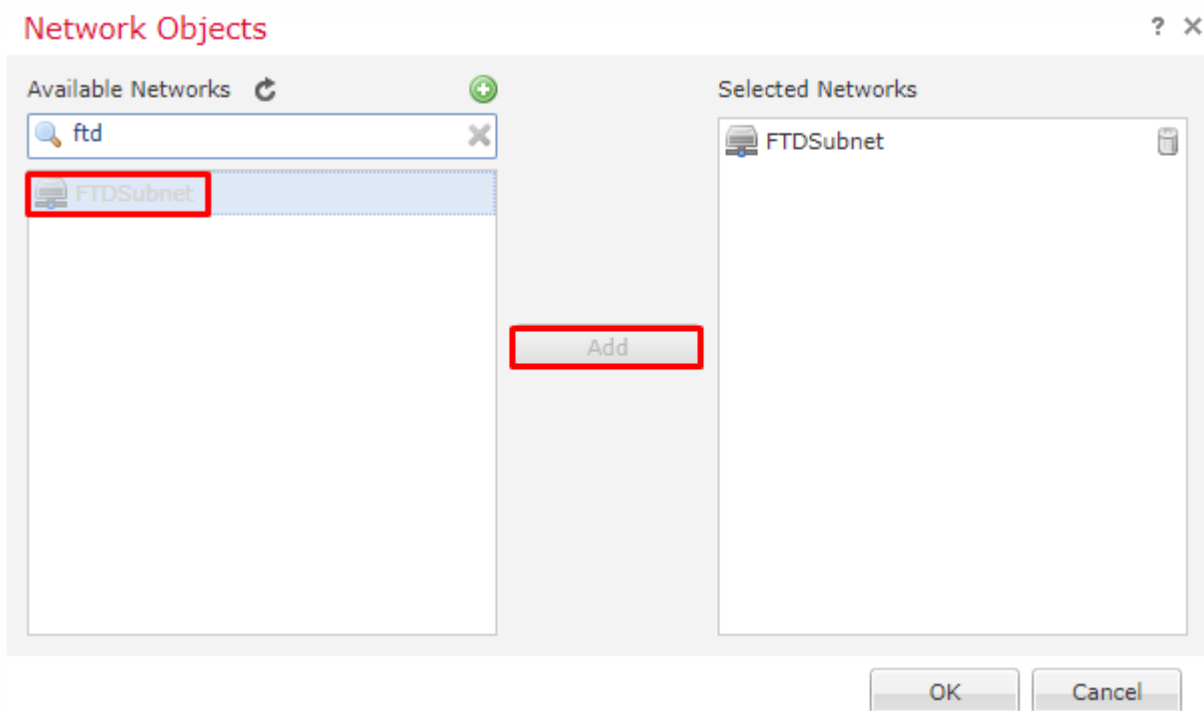
Subnet / IP Address (Network) Access List (Extended) +

OK Cancel

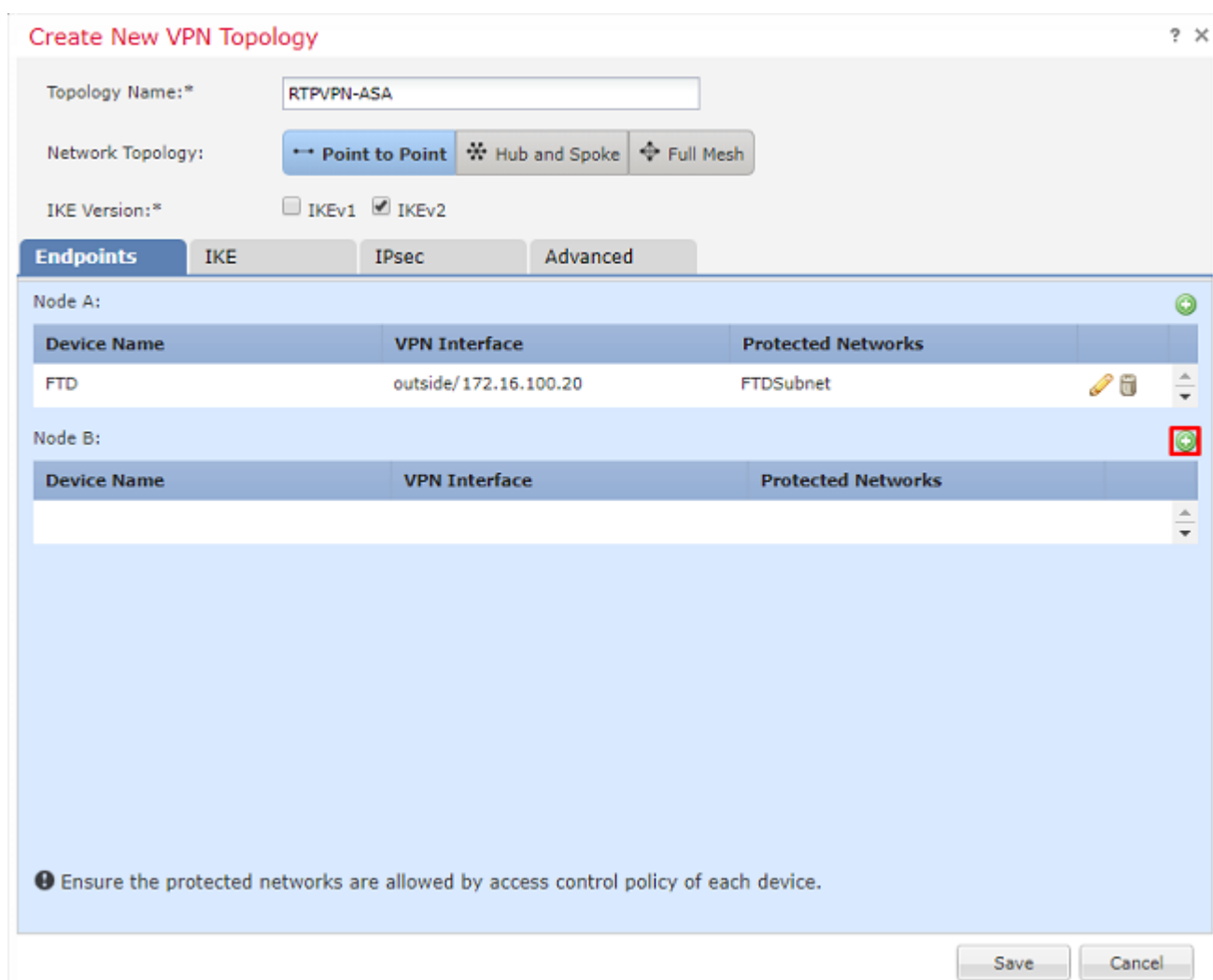
4. Clique em verde mais e um objeto de rede será criado aqui.

5. Adicione todas as sub-redes locais ao FTD que precisam ser criptografadas. Clique em **Adicionar** para movê-las para as Redes selecionadas. Agora, clique em **OK**, conforme mostrado nesta imagem.

FTDSubnet = 10.10.113.0/24



O ponto de extremidade do Nó A: (FTD) foi concluído. Clique no sinal de mais verde para Node B, conforme mostrado na imagem.



O nó B é um ASA. Os dispositivos que não são gerenciados pelo FMC são considerados Extranet.

6. Adicione um nome de dispositivo e um endereço IP. Clique no sinal de mais verde para adicionar redes protegidas, como mostrado na imagem.

Edit Endpoint ? x

Device:* Extranet

Device Name:* ASA

IP Address:* Static Dynamic
192.168.200.10

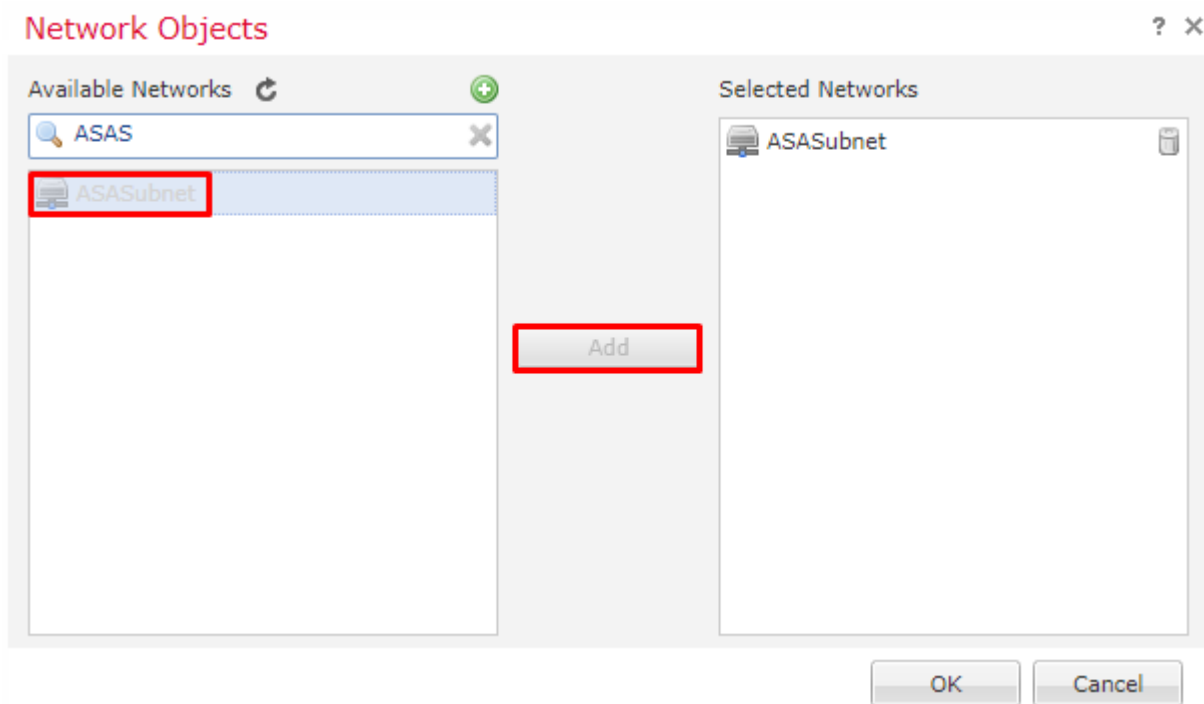
Certificate Map: [dropdown] +

Protected Networks:*
 Subnet / IP Address (Network) Access List (Extended) +

OK Cancel

7. Como mostrado nesta imagem, selecione as **sub-redes ASA** que precisam ser criptografadas e adicione-as às redes selecionadas.

ASASubnet = 10.10.110.0/24



Etapa 2. Configurar parâmetros IKE.

Agora que ambos os endpoints estão instalados, execute a configuração IKE/IPSEC.

1. Na guia **IKE**, especifique os parâmetros usados para a troca inicial de IKEv2. Clique no sinal de mais verde para criar uma nova política IKE, como mostrado na imagem.

Create New VPN Topology ? x

Topology Name:* RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:* preshared_sha_aes256_dh5_5

Authentication Type: Pre-shared Automatic Key

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

IKEv2 Settings

Policy:* AES-GCM-NULL-SHA

Authentication Type: Pre-shared Automatic Key

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

Save Cancel

2. Na nova política IKE, especifique um número de prioridade, bem como o tempo de vida da fase 1 da conexão. Este documento usa estes parâmetros para a troca inicial: Integridade (SHA256), Criptografia (AES-256), PRF (SHA256) e Grupo Diffie-Hellman (Grupo 14)

Observação: todas as políticas IKE no dispositivo são enviadas ao peer remoto, independentemente do que está na seção de política selecionada. A primeira Política IKE correspondida pelo peer remoto será selecionada para a conexão VPN. Escolha qual política é enviada primeiro usando o campo de prioridade. A prioridade 1 será enviada primeiro.

New IKEv2 Policy

? X

Name:*

Description:

Priority: (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms

- Encryption Algorithms
- PRF Algorithms
- Diffie-Hellman Group

Available Algorithms

- MD5
- SHA
- SHA512
- SHA256
- SHA384
- NULL

Add

Selected Algorithms

- SHA256

Save

Cancel

New IKEv2 Policy

? X

Name:*	<input type="text" value="ASA"/>
Description:	<input type="text"/>
Priority:	<input type="text" value="1"/> (1-65535)
Lifetime:	<input type="text" value="86400"/> seconds (120-2147483647)

Integrity Algorithms	Available Algorithms	Selected Algorithms
Encryption Algorithms	<ul style="list-style-type: none"><input type="checkbox"/> AES<input checked="" type="checkbox"/> AES-256<input type="checkbox"/> DES<input type="checkbox"/> 3DES<input type="checkbox"/> AES-192<input type="checkbox"/> AES-GCM<input type="checkbox"/> AES-GCM-192<input type="checkbox"/> AES-GCM-256<input type="checkbox"/> NULL	<ul style="list-style-type: none"><input checked="" type="checkbox"/> AES-256
PRF Algorithms	<input type="button" value="Add"/>	
Diffie-Hellman Group		

New IKEv2 Policy

? X

Name:*	<input type="text" value="ASA"/>
Description:	<input type="text"/>
Priority:	<input type="text" value="1"/> (1-65535)
Lifetime:	<input type="text" value="86400"/> seconds (120-2147483647)

Integrity Algorithms	Available Algorithms	Selected Algorithms
Encryption Algorithms	<ul style="list-style-type: none">MD5SHASHA512SHA256SHA384	<ul style="list-style-type: none">SHA256
PRF Algorithms	<input type="button" value="Add"/>	
Diffie-Hellman Group		

New IKEv2 Policy

? X

Name:*	<input type="text" value="ASA"/>
Description:	<input type="text"/>
Priority:	<input type="text" value="1"/> (1-65535)
Lifetime:	<input type="text" value="86400"/> seconds (120-2147483647)

Integrity Algorithms	Available Groups	Selected Groups
Encryption Algorithms		
PRF Algorithms	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 5 <input checked="" type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21	<input checked="" type="checkbox"/> 14
Diffie-Hellman Group		

3. Depois que os parâmetros forem adicionados, selecione essa política e escolha o **Tipo de Autenticação**.

4. Escolha **pre-shared-key** manual. Para este documento, a PSK cisco123 é usada.

Create New VPN Topology ? x

Topology Name:* RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:* preshared_sha_aes256_dh5_5

Authentication Type: Pre-shared Automatic Key

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

IKEv2 Settings

Policy:* **ASA**

Authentication Type: **Pre-shared Manual Key**

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Save Cancel

Etapa 3. Configurar parâmetros de IPsec.

1. Em **IPsec**, clique no lápis para editar o conjunto de transformação e criar uma nova Proposta IPsec, conforme mostrado nesta imagem.

Create New VPN Topology ? X

Topology Name: RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version: IKEv1 IKEv2

Endpoints IKE **IPsec** Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets:

- IKEv1 IPsec Proposals: tunnel_aes256_sha
- IKEv2 IPsec Proposals***: AES-GCM

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group: 14

Lifetime Duration*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

— **ESPv3 Settings**

Save Cancel

2. Para criar uma nova Proposta IKEv2 IPsec, clique no sinal de mais verde e insira os parâmetros da fase 2.

Selecione **ESP Encryption > AES-GCM-256**. Quando o algoritmo GCM é usado para criptografia, um algoritmo Hash não é necessário. Com o GCM, a função de hash é integrada.

Edit IKEv2 IPsec Proposal

? X

Name:* ASA

Description:

ESP Hash

ESP Encryption

Available Algorithms

- AES-GCM-256
- AES-256
- AES-GCM-192
- AES-192
- AES-GCM
- AES
- 3DES
- DES
- AES-GMAC-25

Add

Selected Algorithms

- AES-GCM-256

Save Cancel

3. Depois que a nova proposta de IPsec tiver sido criada, adicione-a aos conjuntos de transformação selecionados.

IKEv2 IPsec Proposal

Available Transform Sets

Search

- AES-GCM
- AES-SHA
- ASA
- DES_SHA-1

Add

Selected Transform Sets

- ASA

OK Cancel

A proposta IPsec selecionada recentemente está listada nas Propostas IKEv2 IPsec.

Se necessário, o tempo de vida da fase 2 e o PFS podem ser editados aqui. Para este exemplo, o tempo de vida será definido como padrão e o PFS será desabilitado.

Create New VPN Topology ? X

Topology Name:

Network Topology: Point to Point Hub and Spoke Full Mesh

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

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

— **ESPv3 Settings**

Opcional - Conclua a opção para Ignorar Controle de Acesso ou Criar uma Política de Controle de Acesso.

Etapa 4. Ignorar Controle de Acesso.

Opcionalmente, `sysopt permit-vpn` pode ser habilitado em **Advanced > Tunnel**.

Isso elimina a possibilidade de usar a Política de controle de acesso para inspecionar o tráfego proveniente dos usuários. Os filtros VPN ou as ACLs disponíveis para download ainda podem ser usados para filtrar o tráfego do usuário. Este é um comando global e será aplicado a todas as VPNs se esta caixa de seleção estiver habilitada.

Create New VPN Topology ? x

Topology Name: RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version: IKEv1 IKEv2

Endpoints IKE IPsec **Advanced**

IKE
IPsec
Tunnel

NAT Settings

Keepalive Messages Traversal
Interval: 20 Seconds (Range 10 - 3600)

Access Control for VPN Traffic

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Certificate Map Settings

Use the certificate map configured in the Endpoints to determine the tunnel

Use the certificate OU field to determine the tunnel

Use the IKE identity to determine the tunnel

Use the peer IP address to determine the tunnel

Save Cancel

Se **sysopt permit-vpn** não estiver habilitado, uma política de controle de acesso deverá ser criada para permitir o tráfego de VPN através do dispositivo FTD. Se **sysopt permit-vpn** estiver habilitado, ignore a criação de uma política de controle de acesso.

Etapa 5. Crie uma Política de Controle de Acesso.

Em Access Control Policies (Políticas de controle de acesso), navegue até **Policies (Políticas) > Access Control (Controle de acesso) > Access Control (Controle de acesso)** e selecione a Policy (Política) que se destina ao dispositivo FTD. Para adicionar uma regra, clique em **Add Rule**, como mostrado na imagem aqui.

O tráfego deve ser permitido da rede interna para a rede externa e da rede externa para a rede interna. Crie uma regra para executar ambas ou crie duas regras para mantê-las separadas. Neste exemplo, uma regra é criada para fazer ambos.

Editing Rule - VPN_Traffic

Name: VPN_Traffic Enabled Move

Action: Allow

Zones: Networks | VLAN Tags | Users | Applications | Ports | URLs | SGT/ISE Attributes | Inspection | Logging | Comments

Available Networks: subnet

Source Networks (2): ASASubnet, FTDSubnet

Destination Networks (2): ASASubnet, FTDSubnet

Buttons: Add To Source Networks, Add to Destination, Save, Cancel

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VL...	Us...	Ap...	So...	De...	URLs	So...	De...	A...	Actions
1	VPN_Traffic	Inside Outside	Inside Outside	ASASubnet FTDSubnet	ASASubnet FTDSubnet	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow

Etapa 6. Configurar isenção de NAT.

Configure uma instrução de Isenção de NAT para o tráfego VPN. A isenção de NAT deve estar em vigor para evitar que o tráfego VPN acesse outra instrução de NAT e converta incorretamente o tráfego VPN.

1. Navegue até **Devices > NAT**, selecione a política de NAT que se destina ao FTD. Crie uma nova regra ao clicar no botão **Adicionar regra**.

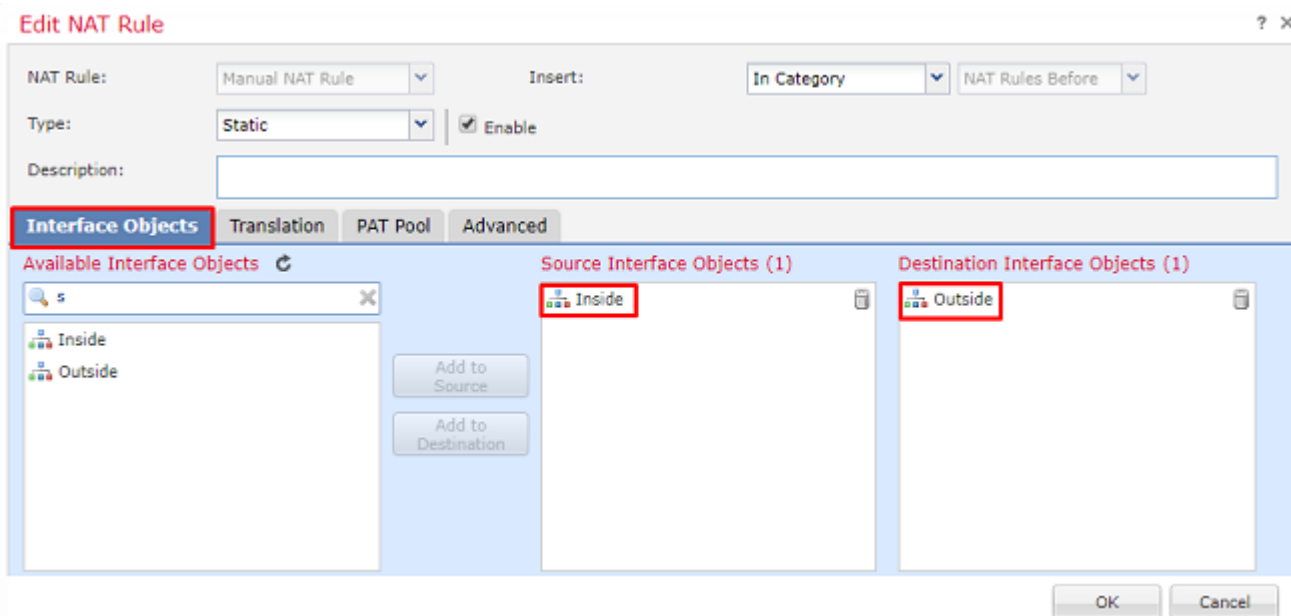
VirtualFTDNAT

Rules

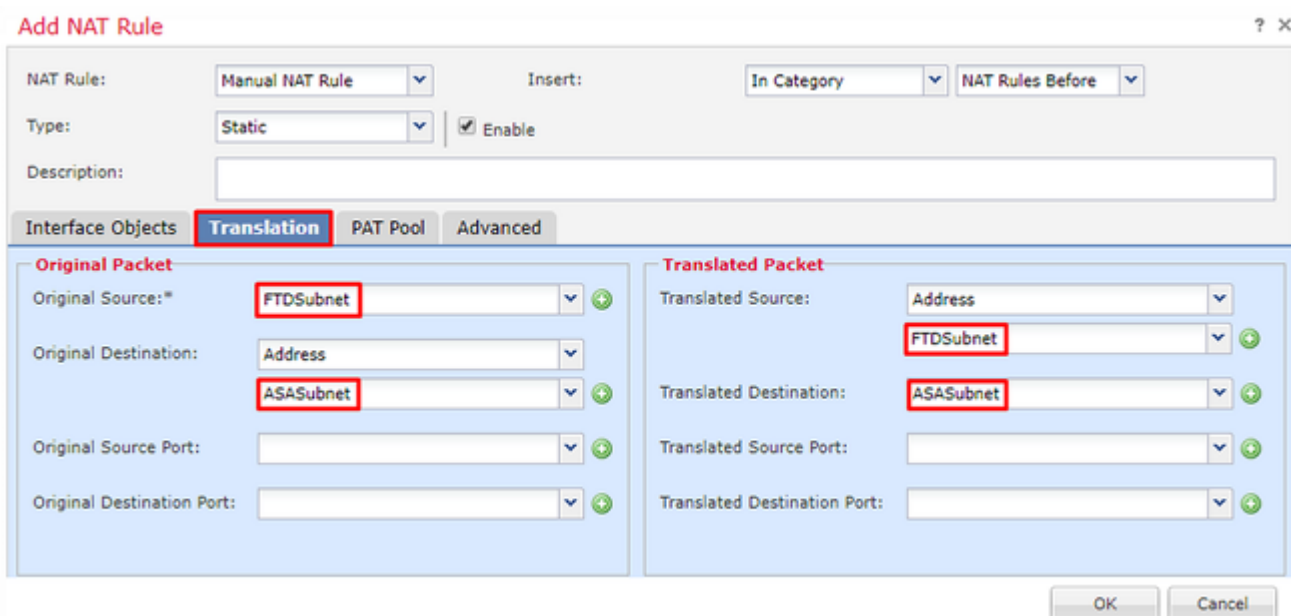
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
NAT Rules Before											
Auto NAT Rules											

Buttons: Add Rule

2. Crie uma nova Regra de NAT Manual Estático. Faça referência às interfaces interna e externa.



3. Na guia **Tradução** e selecione as sub-redes de origem e destino. Como esta é uma regra de isenção de NAT, torne a origem/destino original e a origem/destino convertida iguais, como mostrado nesta imagem:



4. Por fim, vá até a guia **Advanced** e habilite no-proxy-arp e route-lookup.

Add NAT Rule ? X

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Fallthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Unidirectional

5. Salve essa regra e examine os resultados finais na lista NAT.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

VirtualFTDNAT Show Warnings Save Cancel

Enter Description Policy Assignments

Rules Filter by Device Add Rule

#	Direction	Type	Source Interface...	Destination Interface...	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
▼ NAT Rules Before											
1	↔	Static	Inside	Outside	FTDSubnet	ASASubnet		FTDSubnet	ASASubnet		Dns:fail route-lx no-prop
▼ Auto NAT Rules											
#	↔	Dynamic	Inside	Outside	any-obj			Interface			Dns:fail
▼ NAT Rules After											

6. Quando a configuração estiver concluída, salve e implante a configuração no FTD.

Passo 7. Configure o ASA.

1. Ative o IKEv2 na interface externa do ASA:

```
Crypto ikev2 enable outside
```

2. Crie a Política IKEv2 que define os mesmos parâmetros configurados no FTD:

```
Crypto ikev2 policy 1
Encryption aes-256
Integrity sha256
Group 14
Prf sha256
```

```
Lifetime seconds 86400
```

3. Crie uma política de grupo que permita o protocolo ikev2:

```
Group-policy FTD_GP internal
Group-policy FTD_GP attributes
Vpn-tunnel-protocol ikev2
```

4. Crie um grupo de túneis para o endereço IP público do FTD do peer. Consulte a política de grupo e especifique a chave pré-compartilhada:

```
Tunnel-group 172.16.100.20 type ipsec-l2l
Tunnel-group 172.16.100.20 general-attributes
Default-group-policy FTD_GP
Tunnel-group 172.16.100.20 ipsec-attributes
ikev2 local-authentication pre-shared-key cisco123
ikev2 remote-authentication pre-shared-key cisco123
```

5. Crie uma lista de acesso que defina o tráfego a ser criptografado: (FTDSubnet 10.10.113.0/24) (ASASubnet 10.10.110.0/24)

```
Object network FTDSUBNET
Subnet 10.10.113.0 255.255.255.0
Object network ASASUBNET
Subnet 10.10.110.0 255.255.255.0
Access-list ASAtoFTD extended permit ip object ASASUBNET object FTDSUBNET
```

6. Crie uma proposta ikev2 ipsec referenciando os algoritmos especificados no FTD:

```
Crypto ipsec ikev2 ipsec-proposal FTD
Protocol esp encryption aes-gcm-256
```

7. Crie uma entrada de mapa de criptografia que vincule a configuração:

```
Crypto map outside_map 10 set peer 172.16.100.20
Crypto map outside_map 10 match address ASAtoFTD
Crypto map outside_map 10 set ikev2 ipsec-proposal FTD
Crypto map outside_map 10 interface outside
```

8. Crie uma declaração de isenção de NAT que evitará que o tráfego de VPN seja NAT pelo firewall:

```
Nat (inside,outside) 1 source static ASASubnet ASASubnet destination static FTDSubnet FTDSubnet no-p
```

Verificar

Observação: no momento, não há como revisar o status do túnel VPN do FMC. Há uma solicitação de aprimoramento para esse recurso [CSCvh7603](#).

Tente iniciar o tráfego pelo túnel VPN. Com acesso à linha de comando do ASA ou FTD, isso pode ser feito com o comando packet tracer. Ao usar o comando packet-tracer para ativar o túnel VPN, ele deve ser executado duas vezes para verificar se o túnel é ativado. A primeira vez que o comando é emitido, o túnel VPN está inoperante, de modo que o comando packet-tracer falhará com DROP de criptografia de VPN. Não use o endereço IP interno do firewall como o endereço IP origem no packet-tracer, pois isso sempre falhará.

```
firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10
```

```
Phase: 10
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:
```

```
firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10
```

```
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.100.1 using egress ifc outside
```

```
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (Inside,outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet no-proxy-a
Additional Information:
NAT divert to egress interface outside
Untranslate 10.10.110.10/0 to 10.10.110.10/0
```

```
Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip ifc Inside object-group FMC_INLINE_src_rule_268436483 ifc out
access-list CSM_FW_ACL_ remark rule-id 268436483: ACCESS POLICY: FTD-Access-Control-Policy - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268436483: L7 RULE: VPN_Traffic
```

```
object-group network FMC_INLINE_src_rule_268436483
description: Auto Generated by FMC from src of UnifiedNGFWRule# 1 (FTD-Access-Control-Policy/mandatory)
network-object object ASASubnet
network-object object FTDSubnet
object-group network FMC_INLINE_dst_rule_268436483
description: Auto Generated by FMC from dst of UnifiedNGFWRule# 1 (FTD-Access-Control-Policy/mandatory)
network-object object ASASubnet
network-object object FTDSubnet
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached
```

```
Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (Inside,outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet no-proxy-a
Additional Information:
Static translate 10.10.113.10/0 to 10.10.113.10/0
```

```
Phase: 10
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
```

```
Result:
input-interface: Inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Para monitorar o status do túnel, navegue até o CLI do FTD ou do ASA.

A partir do CLI do FTD, verifique a fase 1 e a fase 2 com este comando:

Show crypto ikev2 sa

```
<#root>
```

```
> show crypto ikev2 sa
```

```
IKEv2 SAs:
```

```
Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Remote
9528731 172.16.100.20/500 192.168.200.10/500
```

```
READY
```

```
INITIATOR
```

```
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/118 sec
```

```
Child sa: local selector
```

```
10.10.113.0/0 - 10.10.113.255/65535
```

```
remote selector
```

```
10.10.110.0/0 - 10.10.110.255/65535
```

```
ESP spi in/out:
```

```
0x66be357d/0xb74c8753
```

Solução de problemas e depuração

Problemas iniciais de conectividade

Ao construir uma VPN, há dois lados negociando o túnel. Portanto, é melhor obter ambos os lados da conversação quando você solucionar qualquer tipo de falha de túnel. Um guia detalhado sobre como depurar túneis IKEv2 pode ser encontrado aqui: [Como depurar VPNs IKEv2](#)

A causa mais comum de falhas de túnel é um problema de conectividade. A melhor maneira de determinar isso é fazer capturas de pacotes no dispositivo. Use este comando para capturar pacotes no dispositivo:

```
Capture capout interface outside match ip host 172.16.100.20 host 192.168.200.10
```

Quando a captura estiver em vigor, tente enviar o tráfego pela VPN e verifique o tráfego bidirecional na captura de pacotes.

Revise a captura de pacotes com este comando:

show cap capout

```
firepower# show cap capout
```

```
4 packets captured
```

```
1: 11:51:12.059628      172.16.100.20.500 > 192.168.200.10.500:  udp 690
2: 11:51:12.065243      192.168.200.10.500 > 172.16.100.20.500:  udp 619
3: 11:51:12.066692      172.16.100.20.500 > 192.168.200.10.500:  udp 288
4: 11:51:12.069835      192.168.200.10.500 > 172.16.100.20.500:  udp 240
```

Problemas específicos de tráfego

Os problemas comuns de tráfego que você enfrenta são:

- Problemas de roteamento por trás do FTD – a rede interna não consegue rotear os pacotes de volta para os endereços IP e clientes VPN atribuídos.
- Listas de controle de acesso bloqueando o tráfego.
- A Tradução de Endereço de Rede não está sendo ignorada para tráfego VPN.

Para obter mais informações sobre VPNs no FTD gerenciado pelo FMC, você pode encontrar o guia de configuração completo aqui: [FTD gerenciado pelo FMC](#)

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.