

Configurar o túnel de site para site IPv6 IKEv2 entre ASA e FTD

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração do ASA](#)

[Configuração do FTD](#)

[Ignorar controle de acesso](#)

[Configurar isenção de NAT](#)

[Verificar](#)

[Troubleshoot](#)

[Referências](#)

Introduction

Este documento fornece um exemplo de configuração para configurar um túnel de site para site IPv6 entre um ASA (Adaptive Security Appliance) e FTD (Firepower Threat Defense) usando o protocolo IKEv2 (Internet Key Exchange versão 2). A configuração inclui conectividade de rede IPv6 de ponta a ponta com ASA e FTD como dispositivos de terminação de VPN.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento fundamental da configuração do ASA CLI
- Conhecimento fundamental dos protocolos IKEv2 e IPSEC
- Entendendo o endereçamento IPv6 e o roteamento
- Compreensão básica da configuração do FTD via FMC

Componentes Utilizados

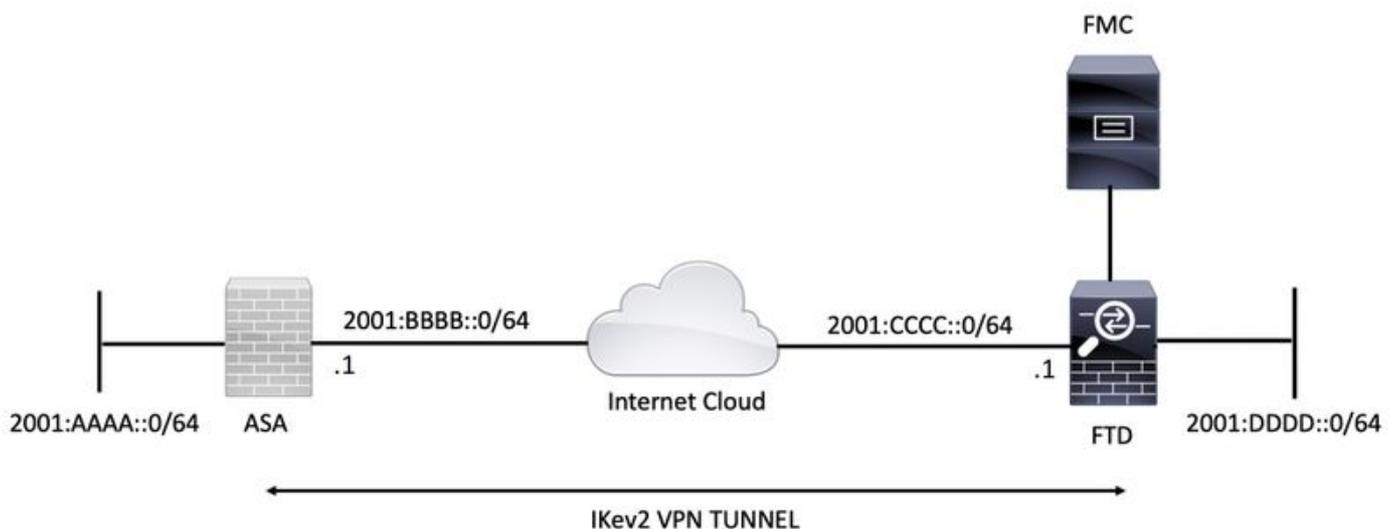
As informações neste documento são baseadas em um ambiente virtual, criado a partir de dispositivos em uma configuração de laboratório específica. All of the devices used in this document started with a cleared (default) configuration. Se sua rede estiver em produção, certifique-se de que você entendeu o impacto potencial de qualquer comando.

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

- Cisco ASAv executando 9.6.(4)12
- Cisco FTDv executando 6.5.0
- Cisco FMCv executando 6.6.0

Configurar

Diagrama de Rede



Configuração do ASA

Esta seção descreve a configuração necessária no ASA.

Etapa 1. Configure as interfaces do ASA.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ipv6 address 2001:bbbb::1/64
ipv6 enable
```

```
interface GigabitEthernet0/1
nameif inside
security-level 100
ipv6 address 2001:aaaa::1/64
ipv6 enable
```

Etapa 2. Defina uma rota padrão IPv6.

```
ipv6 route outside ::/0 2001:bbbb::2
```

Etapa 3. Configure a política IKEv2 e ative IKEv2 na interface externa.

```
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 14
prf sha256
lifetime seconds 86400
```

```
crypto ikev2 enable outside
```

Etapa 4. Configure o grupo de túnel.

```
tunnel-group 2001:cccc::1 type ipsec-l2l
tunnel-group 2001:cccc::1 ipsec-attributes
ikev2 remote-authentication pre-shared-key cisco123
ikev2 local-authentication pre-shared-key cisco123
```

Etapa 5. Crie os objetos e a ACL (Access Control List, lista de controle de acesso) para corresponder ao tráfego interessante.

```
object-group network local-network
network-object 2001:aaaa::/64
```

```
object-group network remote-network
network-object 2001:dddd::/64
```

```
access-list CRYPTO_ACL extended permit ip object-group local-network object-group remote-network
```

Etapa 6. Configure as regras de Conversão de Endereço de Rede (NAT - Network Address Translation) de identidade para o tráfego interessante.

```
nat (inside,outside) source static local-network local-network destination static remote-network
remote-network no-proxy-arp route-lookup
```

Passo 7. Configure a proposta de IPsec IKEv2.

```
crypto ipsec ikev2 ipsec-proposal ikev2_aes256
protocol esp encryption aes-256
protocol esp integrity sha-1
```

Etapa 8. Defina o Mapa de Criptografia e aplique-o à interface externa.

```
crypto map VPN 1 match address CRYPTO_ACL
crypto map VPN 1 set peer 2001:cccc::1
crypto map VPN 1 set ikev2 ipsec-proposal ikev2_aes256
crypto map VPN 1 set reverse-route
```

```
crypto map VPN interface outside
```

Configuração do FTD

Esta seção fornece instruções para configurar um FTD usando o FMC.

Definir a topologia da VPN

Etapa 1. Navegue até **Dispositivos > VPN > Site a Site**.

Selecionar 'Adicione VPN' e escolha 'Firepower Threat Defense Device', como mostrado nesta imagem.

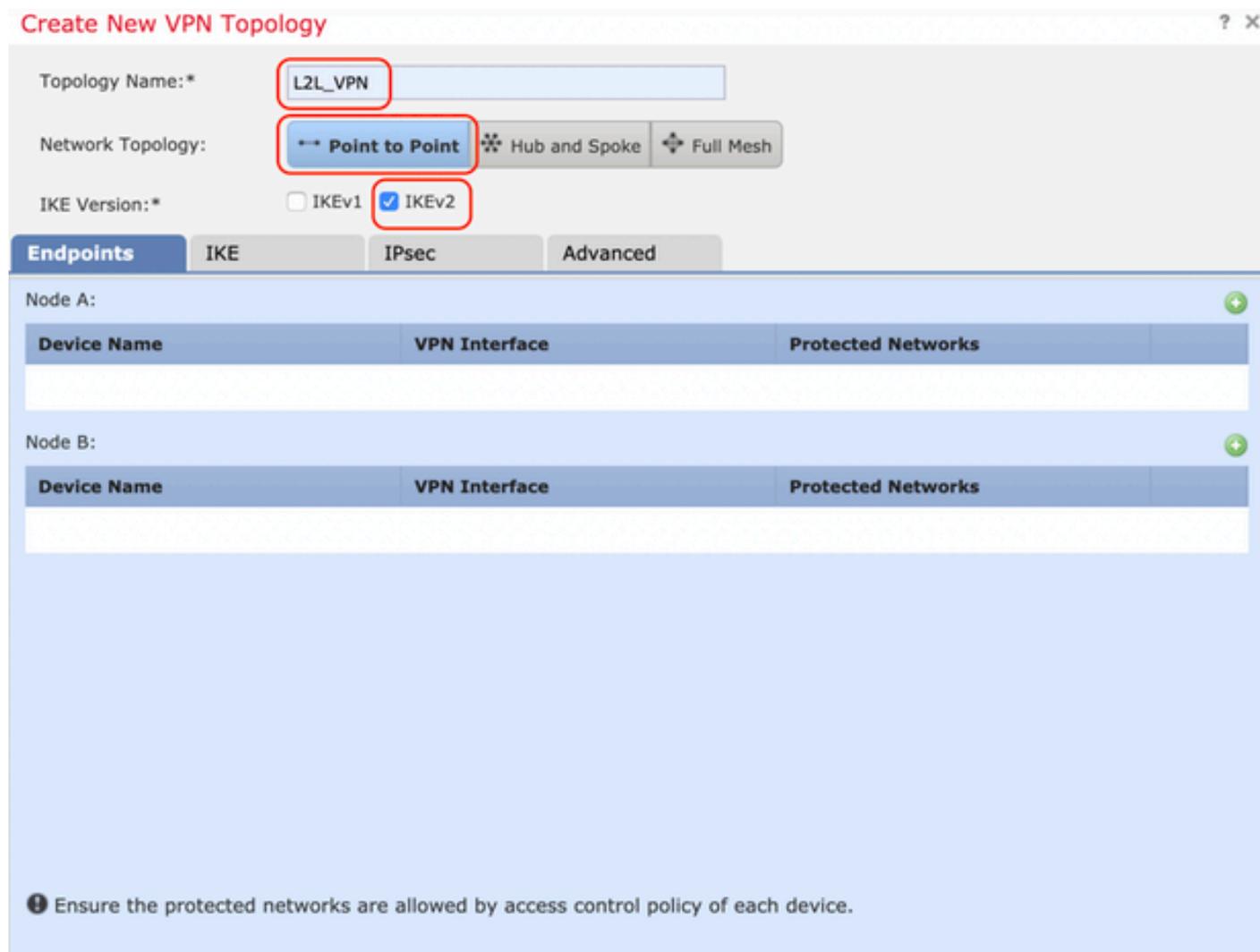


Etapa 2. A caixa 'Create New VPN Topology' (Criar nova topologia de VPN) é exibida. Dê ao VPN um nome facilmente identificável.

Topologia de rede: Ponto a ponto

Versão IKE: IKEv2

Neste exemplo, ao selecionar endpoints, o nó A é o FTD. O nó B é o ASA. Clique no botão verde mais para adicionar dispositivos à topologia.



Etapa 3. Adicione o FTD como o primeiro endpoint.

Escolha a interface onde o mapa de criptografia é aplicado. O endereço IP deve ser preenchido automaticamente a partir da configuração do dispositivo.

Clique no ícone de mais verde em Redes protegidas para selecionar sub-redes criptografadas por meio desse túnel VPN. Neste exemplo, o objeto de rede 'Proxy local' no FMC compreende a sub-rede IPv6 '2001:DDDD::/64'.

Edit Endpoint



Device:*

FTDv

Interface:*

OUTSIDE

IP Address:*

2001:CCCC::1

This IP is Private

Connection Type:

Bidirectional

Certificate Map:

Protected Networks:*

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

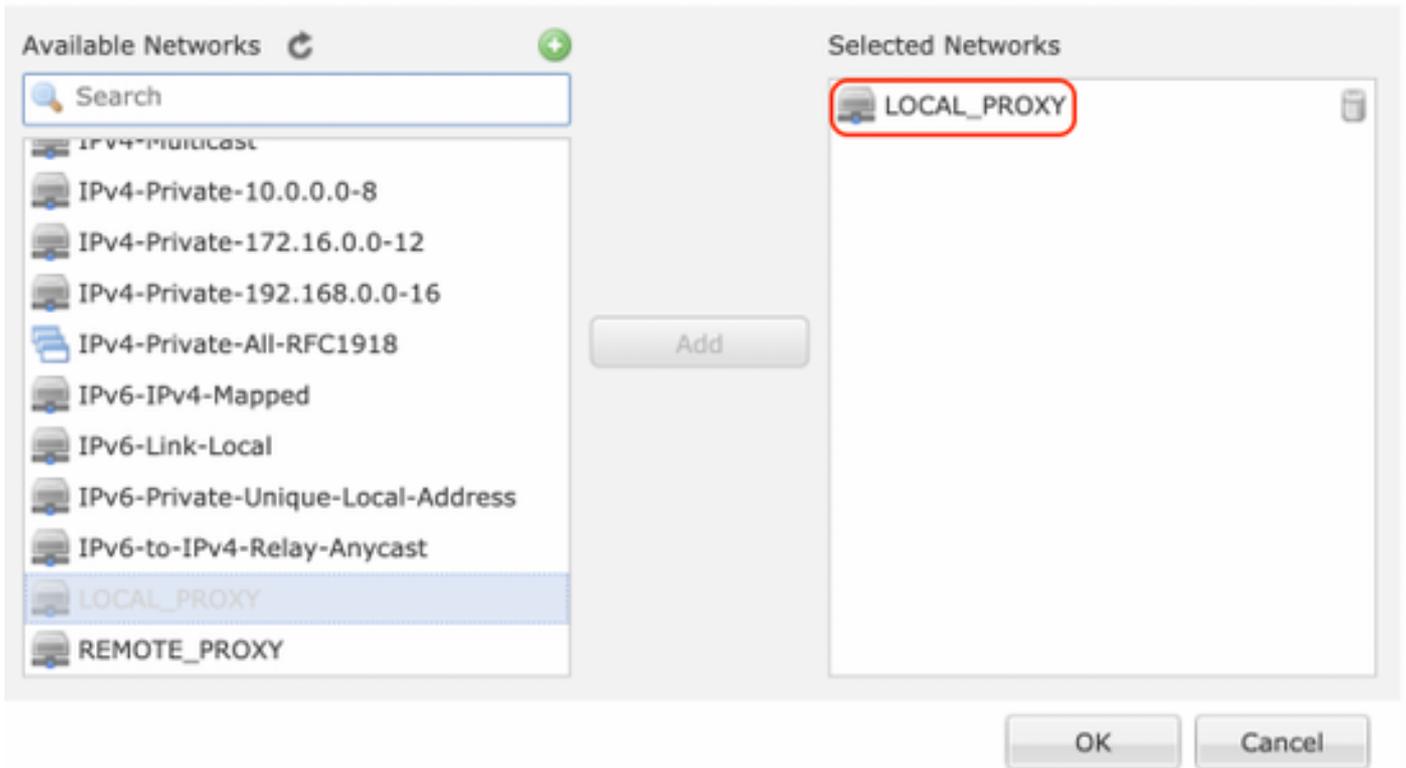


LOCAL_PROXY

OK

Cancel

Network Objects



Com a etapa acima, a configuração do ponto final FTD está concluída.

Etapa 4. Clique no ícone de mais verde para o Nó B, que é um ASA no exemplo de configuração. Os dispositivos que não são gerenciados pelo FMC são considerados extranet. Adicione um nome de dispositivo e um endereço IP.

Etapa 5. Selecione o ícone de mais verde para adicionar redes protegidas.

Edit Endpoint ? X

Device:* Extranet

Device Name:* ASA

IP Address:* Static Dynamic
2001:BBBB::1

Certificate Map: +

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

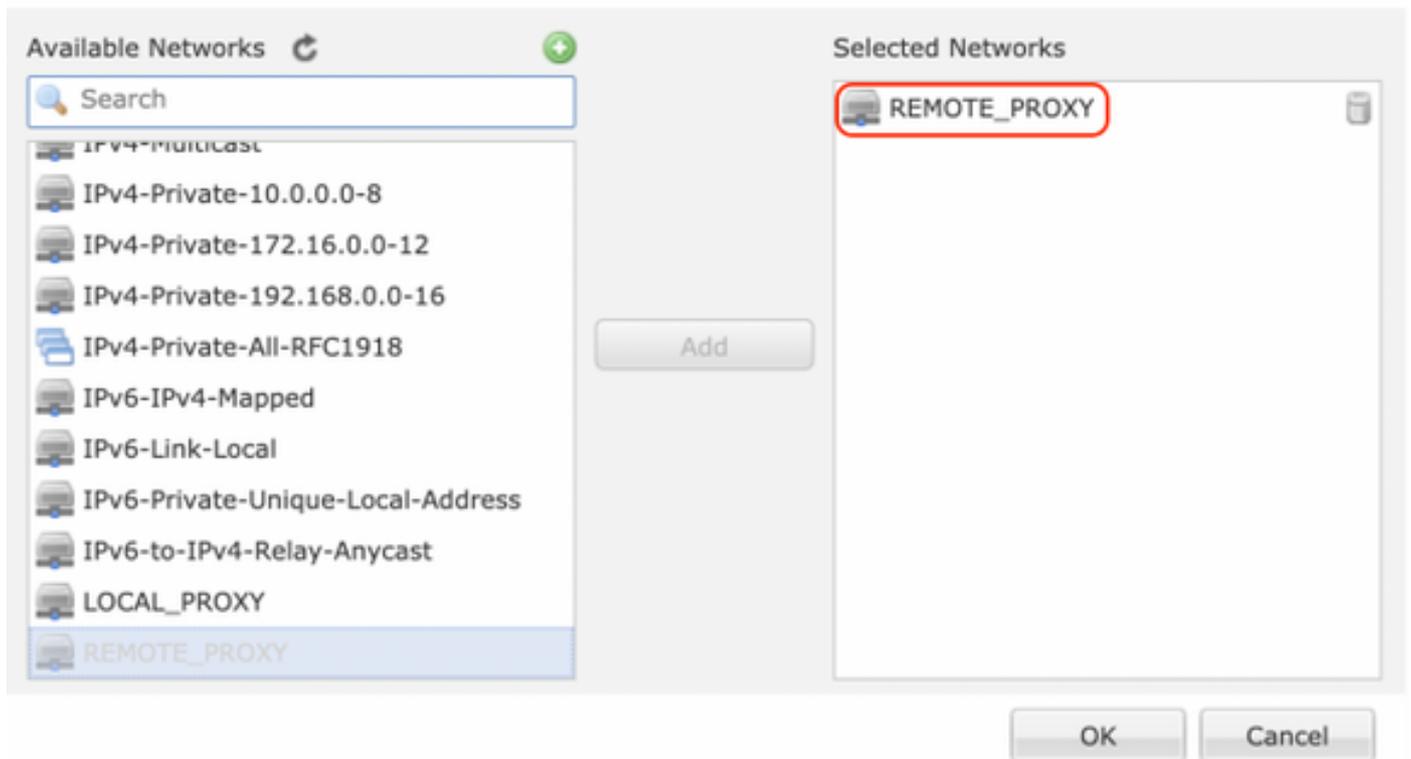
REMOTE_PROXY

OK Cancel

Etapa 6. Selecione as sub-redes ASA que precisam ser criptografadas e adicione-as às redes selecionadas.

'Remote Proxy' é a sub-rede ASA '2001:AAAA::/64' neste exemplo.

Network Objects



Configurar parâmetros IKE

Etapa 1. Na guia IKE, especifique os parâmetros a serem usados para a troca inicial de IKEv2. Clique no ícone de mais verde para criar uma nova política IKE.

Edit VPN Topology



Topology Name:* L2L_VPN

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:* preshared_sha_aes256_dh14_3

Authentication Type: Pre-shared Automatic Key

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

IKEv2 Settings

Policy:* Ikev2_Policy

Authentication Type: Pre-shared Manual Key

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Save Cancel

Etapa 2. Na nova política IKE, especifique um número de prioridade, bem como a duração da fase 1 da conexão. Este guia usa estes parâmetros para a troca inicial:

Integridade (SHA256),
Criptografia (AES-256),
PRF (SHA256) e
Diffie-Hellman Group (Grupo 14).

Todas as políticas de IKE no dispositivo serão enviadas para o peer remoto, independentemente do que está na seção de política selecionada. A primeira correspondência de peer remoto será selecionada para a conexão VPN.

[Opcional] Escolha qual política será enviada primeiro usando o campo de prioridade. A prioridade 1 é enviada primeiro.

Edit IKEv2 Policy

Name:*

Ikev2_Policy

Description:

Priority:

(1-65535)

Lifetime:

86400

seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

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

Selected Algorithms

SHA256

Add

Save

Cancel

Edit IKEv2 Policy



Name:*

Description:

Priority: (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

- AES
- AES-256
- DES
- 3DES
- AES-192
- AES-GCM
- AES-GCM-192
- AES-GCM-256
- NULL

Add

Selected Algorithms

- AES-256 

Save

Cancel

Edit IKEv2 Policy



Name:*

Ikev2_Policy

Description:

Priority:

(1-65535)

Lifetime:

86400

seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

- MDS
- SHA
- SHA512
- SHA256
- SHA384

Selected Algorithms

SHA256

Add

Save

Cancel

Edit IKEv2 Policy



Name:*

Description:

Priority:

Lifetime: seconds (120-2147483647)

Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group

Available Groups

- 1
- 2
- 5
- 14
- 15
- 16
- 19
- 20
- 21

Add

Selected Groups

- 14

Save Cancel

Etapa 3. Depois de adicionar os parâmetros, selecione a política configurada acima e escolha o tipo de autenticação.

Selecione a opção Pre-shared Manual Key. Para este guia, a chave pré-compartilhada 'cisco123' é usada.

Edit VPN Topology



Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:*

Authentication Type:

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

IKEv2 Settings

Policy:*

Authentication Type:

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Configurar parâmetros IPSEC

Etapa 1. Vá até a guia IPsec e crie uma nova proposta de IPsec clicando no ícone do lápis para editar o conjunto de transformações.

Edit VPN Topology



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* 

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

Etapa 2. Crie uma nova proposta de IPsec IKEv2 selecionando o ícone de adição verde e inserindo os parâmetros da fase 2 conforme mostrado abaixo:

Hash ESP: SHA-1

Criptografia ESP: AES-256

Edit IKEv2 IPsec Proposal



Name:*

Ikev2__IPSec_Proposal

Description:

ESP Hash

ESP Encryption

Available Algorithms

- SHA-512
- SHA-384
- SHA-256
- SHA-1
- MD5
- NULL

Selected Algorithms

SHA-1

Add

Save

Cancel

Edit IKEv2 IPsec Proposal



Name:*

Description:

ESP Hash

ESP Encryption

Available Algorithms

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

Add

Selected Algorithms

- AES-256**

Save **Cancel**

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

IKEv2 IPsec Proposal



Available Transform Sets

- AES-GCM
- AES-SHA
- DES_SHA-1
- Ikev2__IPSec_Proposal**

Add

Selected Transform Sets

- Ikev2__IPSec_Proposal**

OK **Cancel**

Etapa 4. A proposta de IPsec recentemente selecionada agora está listada nas propostas de IPsec IKEv2.

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

Edit VPN Topology ? X

Topology Name:* L2L_VPN

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 IKEv2 IPsec Proposals*

tunnel_aes256_sha Ikev2_IPSec_Proposal

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group: [Dropdown]

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

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

ESPv3 Settings

Save Cancel

Você deve configurar as etapas abaixo para ignorar o controle de acesso ou criar regras de política de controle de acesso para permitir sub-redes VPN através do FTD.

Ignorar controle de acesso

Se `sysopt permit-vpn` não estiver habilitada, uma política de controle de acesso deve ser criada para permitir o tráfego VPN através do dispositivo FTD. Se o `sysopt permit-vpn` estiver ativado, ignore a criação de uma política de controle de acesso. Este exemplo de configuração usa a opção "Ignorar controle de acesso".

O parâmetro `sysopt permit-vpn` pode ser ativado em `Advanced > Tunnel`.

Caution: Essa opção remove a possibilidade de usar a Política de controle de acesso para inspecionar o tráfego proveniente dos usuários. Os filtros de VPN ou ACLs que podem ser baixadas ainda podem ser usados para filtrar o tráfego do usuário. Este é um comando global e se aplica a todas as VPNs se essa caixa de seleção estiver habilitada.

Edit VPN Topology



Topology Name:*

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: 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

Configurar isenção de NAT

Configure uma declaração de isenção de NAT para o tráfego VPN. A isenção de NAT deve estar em vigor para impedir que o tráfego VPN corresponda a outra instrução NAT e converta incorretamente o tráfego VPN.

Etapa 1. Navegue até **Dispositivos > NAT** e crie uma nova política clicando em **Nova política > NAT de defesa contra ameaças**.



New Policy



Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

FTDv

Selected Devices

FTDv

Etapa 2. Clique em **Adicionar regra**.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

NAT_Exempt Show Warnings Show Cancel

Policy Assignments (1)

Filter by Device

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

Etapa 3. Crie uma nova regra NAT manual estática.

Consulte as interfaces interna e externa para a regra NAT. A especificação das interfaces na guia Objetos de Interface impede que essas regras afetem o tráfego de outras interfaces.

Navegue até a guia Tradução e selecione as sub-redes de origem e de destino. Como essa é uma regra de isenção de NAT, certifique-se de que a origem/destino original e a origem/destino traduzidos sejam iguais.

Add NAT Rule



NAT Rule: Insert:

Type: Enable

Description:

Interface Objects: **Translation** PAT Pool Advanced

Original Packet

Original Source:* +

Original Destination: +

Original Source Port: +

Original Destination Port: +

Translated Packet

Translated Source: +

Translated Destination: +

Translated Source Port: +

Translated Destination Port: +

Clique na guia Avançado e ative **no-proxy-arp** e **route-lookup**.

Add NAT Rule



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

Salve essa regra e confirme a instrução NAT final na lista NAT.

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

Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates Show Warnings Save Cancel

NAT_Exempt
Enter Description Policy Assignments (1)

Rules Filter by Device Add Rule

#	Direction	Type	Original Packet			Translated Packet			Options
			Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	
1		Static	LAN	WAN	LOCAL_PROXY	REMOTE_PROXY	LOCAL_PROXY	REMOTE_PROXY	Dns: false route-lookup no-proxy-arp

Etapa 4. Quando a configuração estiver concluída, salve e implante a configuração no FTD.



Verificar

Inicie o tráfego interessante da máquina LAN ou você pode executar o comando packet-tracer abaixo no ASA.

```
packet-tracer input inside icmp 2001:aaaa::23 128 0 2001:dddd::33 detail
```

Nota: Aqui Type = 128 e Code=0 representam ICMPv6 "Echo Request".

A seção abaixo descreve os comandos que você pode executar na CLI do ASA ou FTD LINA para verificar o status do túnel IKEv2.

Este é um exemplo de uma saída do ASA:

```
ciscoasa# show crypto ikev2 sa
```

IKEv2 SAs:

```
Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local                               Remote
          Status                               Role
6638313 2001:bbbb::1/500                       2001:cccc::1/500
          READY    INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/224 sec
Child sa: local selector 2001:aaaa::/0 - 2001:aaaa::ffff:ffff:ffff:ffff/65535
          remote selector 2001:dddd::/0 - 2001:dddd::ffff:ffff:ffff:ffff/65535
          ESP spi in/out: 0xa0fd3fe6/0xd95ecdb8
```

```
ciscoasa# show crypto ipsec sa detail
```

```
interface: outside
```

```
  Crypto map tag: VPN, seq num: 1, local addr: 2001:bbbb::1
```

```
access-list CRYPTO_ACL extended permit ip 2001:aaaa::/64 2001:dddd::/64
local ident (addr/mask/prot/port): (2001:aaaa::/64/0/0)
remote ident (addr/mask/prot/port): (2001:dddd::/64/0/0)
current_peer: 2001:cccc::1
```

```
#pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 11
#pkts decaps: 11, #pkts decrypt: 11, #pkts verify: 11
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#pkts no sa (send): 0, #pkts invalid sa (rcv): 0
#pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
#pkts invalid prot (rcv): 0, #pkts verify failed: 0
#pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
```

#pkts invalid pad (rcv): 0,
#pkts invalid ip version (rcv): 0,
#pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
#pkts replay failed (rcv): 0
#pkts min mtu frag failed (send): 0, #pkts bad frag offset (rcv): 0
#pkts internal err (send): 0, #pkts internal err (rcv): 0

local crypto endpt.: 2001:bbbb::1/500, remote crypto endpt.: 2001:cccc::1/500
path mtu 1500, ipsec overhead 94(64), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: D95ECDB8
current inbound spi : A0FD3FE6

inbound esp sas:

spi: 0xA0FD3FE6 (2700951526)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 1937408, crypto-map: VP
sa timing: remaining key lifetime (kB/sec): (4055040/28535)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

outbound esp sas:

spi: 0xD95ECDB8 (3646868920)
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv2, }
slot: 0, conn_id: 1937408, crypto-map: VPN
sa timing: remaining key lifetime (kB/sec): (4193280/28535)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

ciscoasa# **show vpn-sessiondb detail l2l filter name 2001:cccc::1**

Session Type: LAN-to-LAN Detailed

Connection : 2001:cccc::1
Index : 473 IP Addr : 2001:cccc::1
Protocol : IKEv2 IPsec
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing : IKEv2: (1)SHA256 IPsec: (1)SHA1
Bytes Tx : 352 Bytes Rx : 352
Login Time : 12:27:36 UTC Sun Apr 12 2020
Duration : 0h:06m:40s

IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:

Tunnel ID : 473.1
UDP Src Port : 500 UDP Dst Port : 500
Rem Auth Mode: preSharedKeys
Loc Auth Mode: preSharedKeys
Encryption : AES256 Hashing : SHA256
Rekey Int (T): 86400 Seconds Rekey Left(T): 86000 Seconds
PRF : SHA256 D/H Group : 14
Filter Name :

IPsec:

Tunnel ID : 473.2

```
Local Addr   : 2001:aaaa::/64/0/0
Remote Addr  : 2001:dddd::/64/0/0
Encryption   : AES256                Hashing      : SHA1
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds          Rekey Left(T): 28400 Seconds
Rekey Int (D): 4608000 K-Bytes       Rekey Left(D): 4608000 K-Bytes
Idle Time Out: 30 Minutes            Idle TO Left : 23 Minutes
Bytes Tx     : 352                    Bytes Rx     : 352
Pkts Tx     : 11                      Pkts Rx     : 11
```

Troubleshoot

Para solucionar problemas de estabelecimento de túnel IKEv2 no ASA e FTD, execute os seguintes comandos de depuração:

```
debug crypto condition peer <peer IP>
debug crypto ikev2 protocol 255
debug crypto ikev2 platform 255
```

Aqui está um exemplo de depuração de IKEv2 em funcionamento para referência:

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115935-asa-ikev2-debug.html>

Referências

<https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/119425-configure-ipsec-00.html>

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/81824-common-ipsec-trouble.html>

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa95/configuration/vpn/asa-95-vpn-config/vpn-site2site.html>