

Configurar ISP VTI duplo no FTD gerenciado pelo FMC

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos básicos](#)

[Componentes Utilizados](#)

[Configurações no FMC](#)

[Configuração de Topologia](#)

[Configuração do endpoint](#)

[configuração de IKE](#)

[configuração de IPsec](#)

[Configuração de roteamento](#)

Introdução

Este documento descreve a implantação de configuração de ISP duplo usando interfaces de túnel virtual em um dispositivo FTD gerenciado pelo FMC.

Pré-requisitos

Requisitos básicos

- Uma compreensão básica de VPNs site a site seria benéfica. Esse histórico ajuda a compreender o processo de configuração do VTI, incluindo os conceitos e as configurações principais envolvidas.
- Entender os fundamentos da configuração e do gerenciamento de VTIs na plataforma Cisco Firepower é essencial. Tal inclui o conhecimento do funcionamento dos VTI no âmbito do FTD e do modo como são controlados através da interface do FMC.

Componentes Utilizados

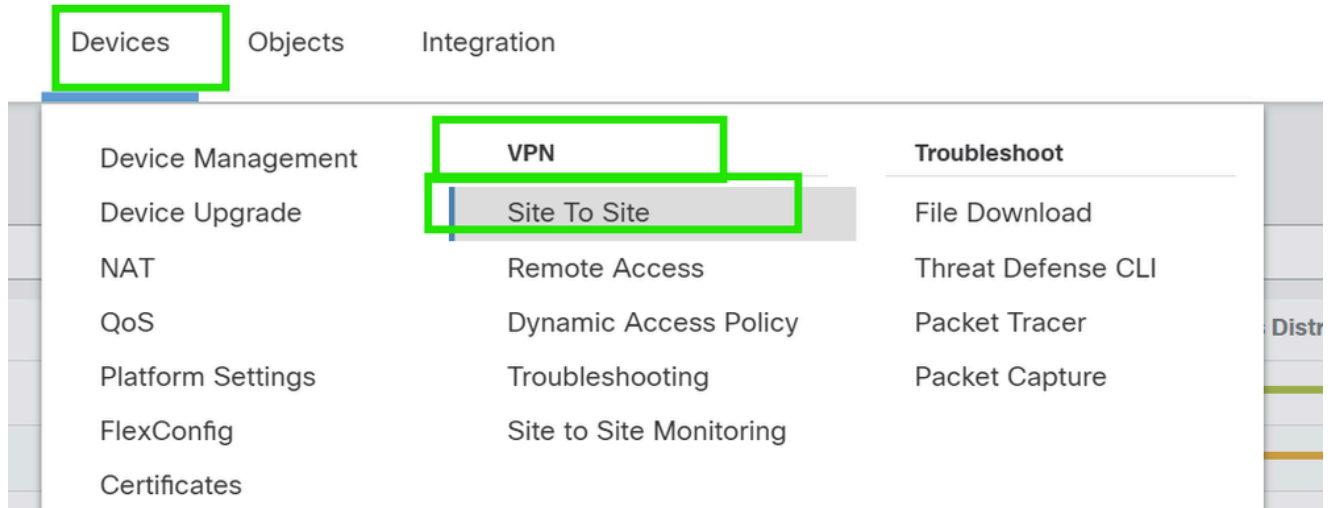
- Cisco Firepower Threat Defense (FTD) para VMware: versão 7.0.0
- Firepower Management Center (FMC): versão 7.2.4 (build 169)

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.

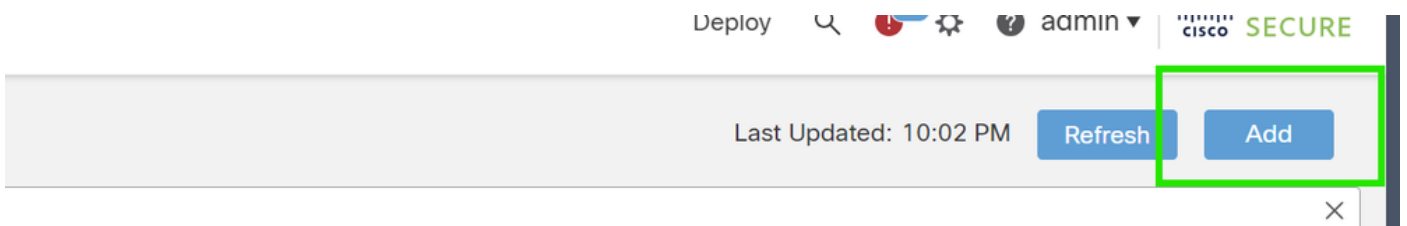
Configurações no FMC

Configuração de Topologia

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



2. Clique em Add para adicionar a topologia VPN.



3. Dê um nome para a topologia, escolha VTI e Ponto a Ponto e selecione uma versão IKE (IKEv2 neste caso).



Configuração do endpoint

1. Escolha o dispositivo no qual o túnel precisa ser configurado.

Adicione os detalhes do peer remoto.

Você pode adicionar uma nova Interface de Modelo Virtual clicando no ícone "+" ou selecionar um na lista existente.

Endpoints IKE IPsec Advanced

Node A

Device:*
New_FTD

Virtual Tunnel Interface:*
 [] +

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

Send Local Identity to Peers

[+ Add Backup VTI \(optional\)](#)

Connection Type:*
Bidirectional

Node B

Device:*
Extranet

Device Name*:
VTI-Peer

Endpoint IP Address*:
10.10.10.2

Cancel Save

Se estiver criando uma nova interface VTI, adicione os parâmetros corretos, ative-os e clique em "OK".

OBSERVAÇÃO: este se torna o VTI principal.

Add Virtual Tunnel Interface



General

Name:*

VTI-1

Enabled

Description:

This is the primary VTI tunnel.
This VTI goes through ISP 1.

Security Zone:

OUT

Priority:

0

(0 - 65535)

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)

Tunnel Source:*

GigabitEthernet0/0 (outside1)

10.106.52.104

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

IPv4 IPv6

192.168.10.1/30

Cancel

OK

3. Clique em "+ ". Add Backup VIT" (Adicionar VIT de backup) para adicionar um VIT secundário.

Device:*

10.106.50.55 ▼

Virtual Tunnel Interface:*

VTI-1 (IP: 192.168.10.1) ▼ +

Tunnel Source: *outside1 (IP: 10.106.52.104)* [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

+ Add Backup VTI (optional)

Connection Type:*

Bidirectional ▼

Additional Configuration ⓘ

Route traffic to the VTI : [Routing Policy](#)

Permit VPN traffic : [AC Policy](#)

4. Clique em "+" para adicionar parâmetro para VTI secundário (se ainda não estiver configurado).

Endpoints IKE IPsec Advanced

10.106.50.55 ▼

Virtual Tunnel Interface:*

VTI-1 (IP: 192.168.10.1) ▼



Tunnel Source: outside1 (IP: 10.106.52.104) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Backup VTI:

[Remove](#)

Virtual Tunnel Interface:*

▼



Tunnel Source IP is Private

[Edit VTI](#)

Send Local Identity to Peers

Connection Type:*

5. Se estiver criando uma nova interface VTI, adicione os parâmetros corretos, ative-os e clique em "OK".

OBSERVAÇÃO: este se torna o VTI secundário.

Add Virtual Tunnel Interface



General

Name:

VTI-2

Enabled

Description:

This is the secondary VTI tunnel..
VTI goes through ISP 2.

Security Zone:

OUT

Priority:

0

(0 - 65535)

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:*

2

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/1 (outside2)

10.106.53.10

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

IPv4 IPv6

192.168.20.1/30



Cancel

OK

configuração de IKE


1. Navegue até a guia IKE. Você pode optar por usar uma política predefinida ou clicar no botão de lápis ao lado da guia Política para criar uma nova ou selecionar outra política disponível com base em sua exigência.

Endpoints **IKE** IPsec Advanced

Authentication Type: Pre-shared Automatic Key

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

IKEv2 Settings



Policies:* AES-GCM-NULL-SHA-LATEST 

Authentication Type: Pre-shared Automatic Key

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

Cancel Save


IKEv2 Policy ?

Available IKEv2 Policy  

- AES-GCM-NULL-SHA
- AES-GCM-NULL-SHA-LAT...
- AES-SHA-SHA
- AES-SHA-SHA-LATEST
- Arko_Test_IKEv2
- DES-SHA-SHA

Add

Selected IKEv2 Policy


AES-GCM-NULL-SHA-LATEST 

Cancel OK

2. Selecione o Tipo de autenticação. Se uma chave manual pré-compartilhada for usada, forneça a chave nas caixas Key e Confirm Key.

Endpoints **IKE** IPsec Advanced

IKEv2 Settings

Policies:* AES-GCM-NULL-SHA-LATEST 

Authentication Type: Pre-shared Manual Key ▼

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only



Cancel Save

configuração de IPsec

Navegue até a guia IPsec. Você pode optar por usar uma proposta predefinida clicando no botão do lápis ao lado da guia de proposta para criar uma nova proposta ou selecionar outra proposta disponível com base em sua necessidade.

Endpoints **IKE** **IPsec** Advanced

IKEv2 Mode: Tunnel ▼

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals* 

tunnel_aes256_sha AES-GCM

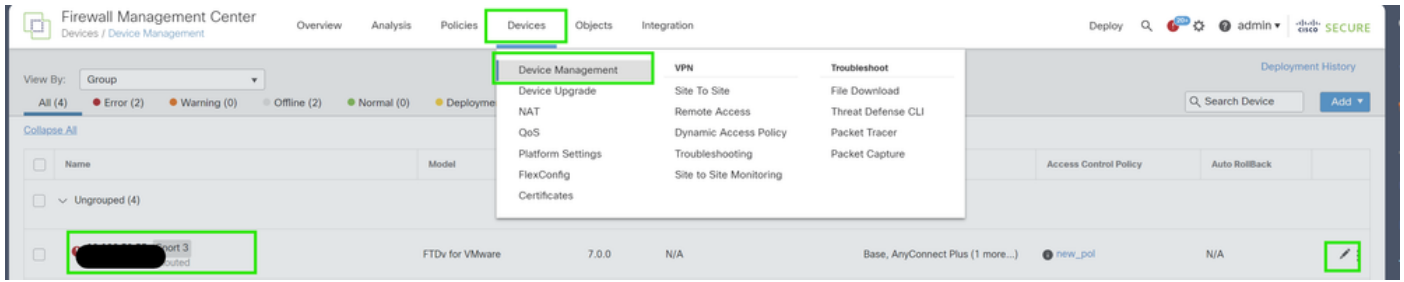
Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

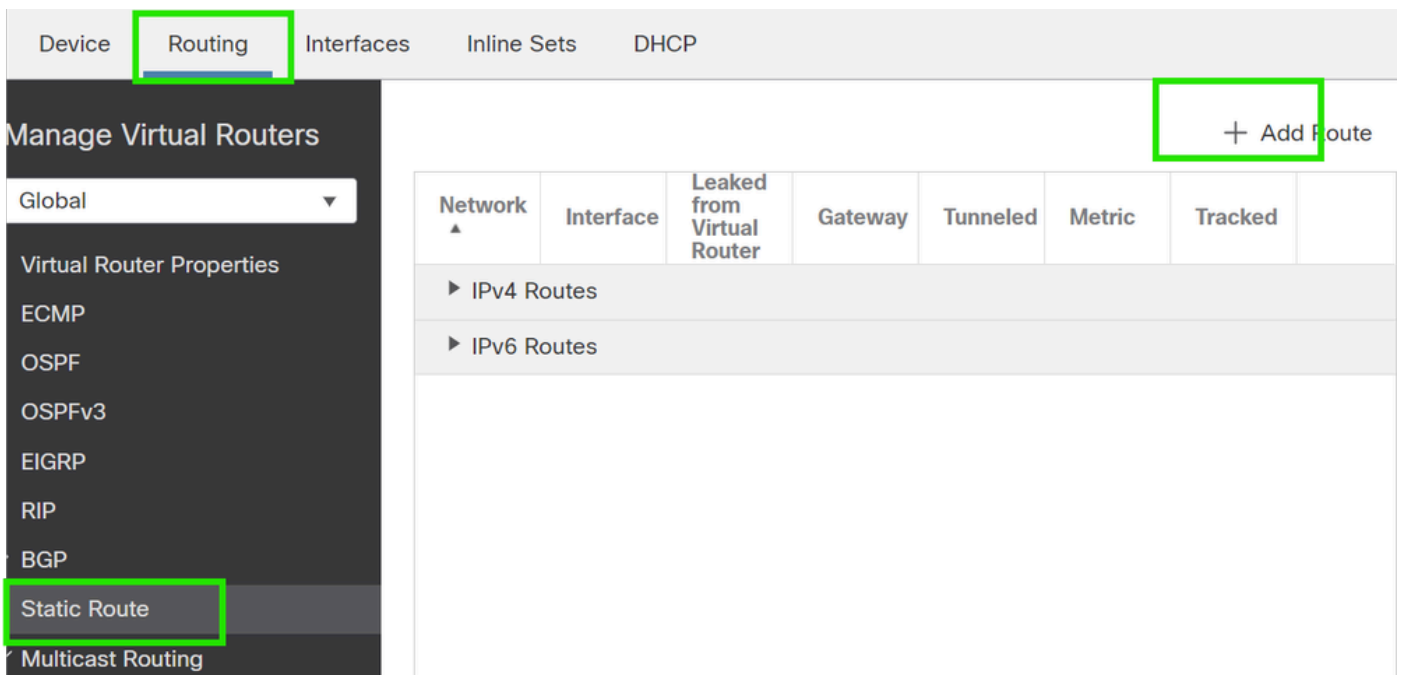
Configuração de roteamento

1. Vá para Device > Device Management e clique no ícone do lápis para editar o dispositivo (FTD).



2. Vá para Roteamento > Rota estática e clique no botão "+" para adicionar uma rota ao VTI primário e secundário.

OBSERVAÇÃO: você pode configurar o método de roteamento apropriado para que o tráfego passe pela interface de túnel. Nesse caso, foram usadas rotas estáticas.



3. Adicione duas rotas para sua rede protegida e defina um valor AD mais alto (neste caso, 2) para a rota secundária.

A primeira rota usa a interface VTI-1 e a segunda usa a interface VTI-2.

Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric
▼ IPv4 Routes					
protected-network	VTI-1	Global	VTI-1-Gateway	false	1
protected-network	VTI-2	Global	VTI-2-Gateway	false	2

Verificar

1. Vá para Devices > VPN > Site to Site Monitoring .

Devices

Objects

Integration

Device Management

Device Upgrade

NAT

QoS

Platform Settings

FlexConfig

Certificates

VPN

Site To Site

Remote Access

Dynamic Access Policy

Troubleshooting

Site to Site Monitoring

Troubleshoot

File Download

Threat Defense CLI

Packet Tracer

Packet Capture

2. Clique no olho para verificar mais detalhes sobre o status do túnel.

	Dual-ISP-VTI	Active	2024-06-11 06:55:26
View full information	Dual-ISP-VTI	Active	2024-06-12 14:27:22

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.