

Configuración de Dual ISP VTI en FTD gestionado por FMC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requisitos básicos](#)

[Componentes Utilizados](#)

[Configuraciones en FMC](#)

[Configuración de topología](#)

[Configuración de terminales](#)

[configuración IKE](#)

[configuración de IPsec](#)

[Configuración de Ruteo](#)

Introducción

Este documento describe la implementación de la configuración de ISP dual mediante interfaces de túnel virtual en un dispositivo FTD administrado por FMC.

Prerequisites

Requisitos básicos

- Una comprensión básica de las VPN de sitio a sitio sería beneficiosa. Estos antecedentes ayudan a comprender el proceso de configuración de VTI, incluidos los conceptos y configuraciones clave implicados.
- Es fundamental comprender los aspectos básicos de la configuración y la administración de las VTI en la plataforma Cisco Firepower. Esto incluye el conocimiento de cómo funcionan las VTI en el FTD y cómo se controlan a través de la interfaz FMC.

Componentes Utilizados

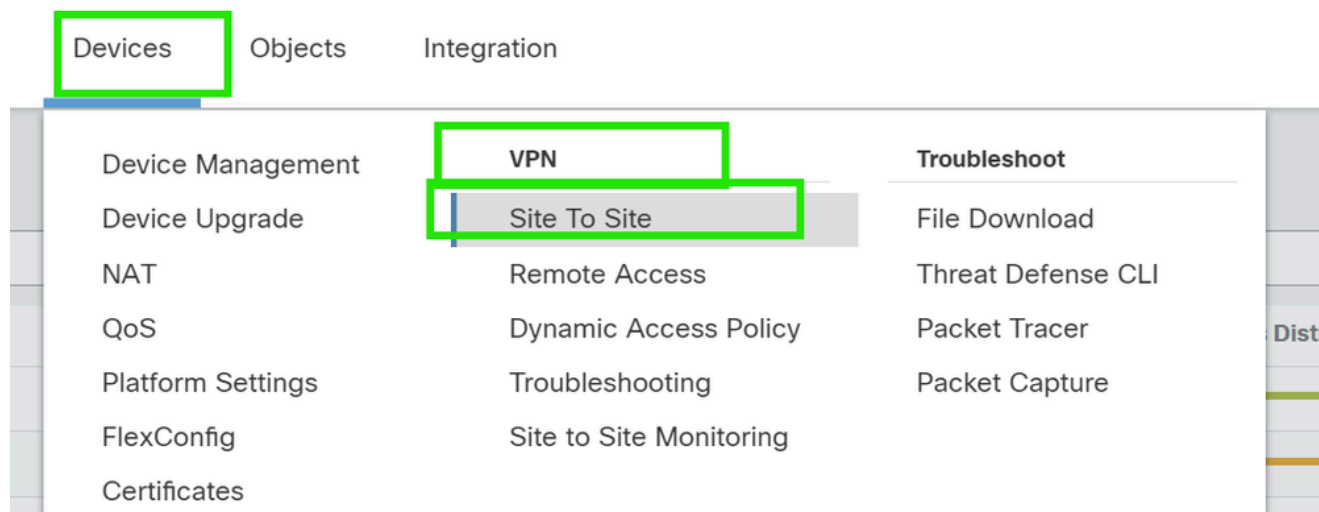
- Cisco Firepower Threat Defense (FTD) para VMware: versión 7.0.0
- Firepower Management Center (FMC): versión 7.2.4 (compilación 169)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

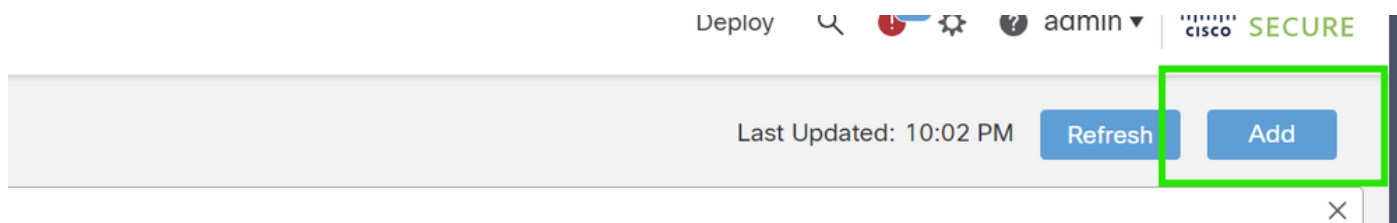
Configuraciones en FMC

Configuración de topología

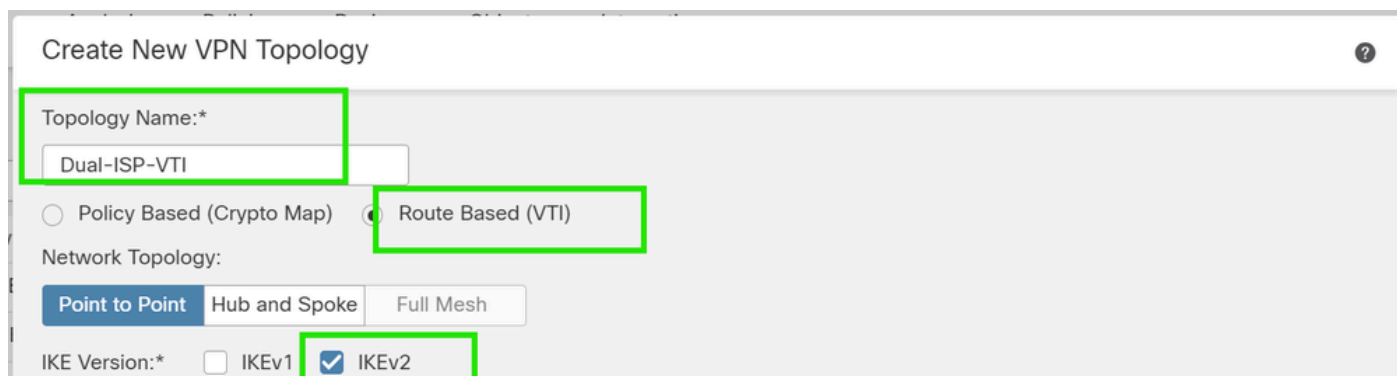
1. Vaya a Devices > VPN > Site To Site.



2. Haga clic en Agregar para agregar la topología VPN.



3. Dé un nombre a la topología, elija VTI y Point-to-Point, y seleccione una versión IKE (IKEv2 en este caso).



Configuración de terminales

1. Seleccione el dispositivo en el que debe configurarse el túnel.

Agregue los detalles del par remoto.

Puede agregar una nueva interfaz de plantilla virtual haciendo clic en el icono "+" o seleccionar una de la 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

Si está creando una nueva interfaz VTI, agregue los parámetros correctos, habilítela y haga clic en "Aceptar".

NOTA: Se convierte en la 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. Haga clic en "+ ". Add Backup VIT" para agregar un VIT secundario.

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. Haga clic en "+" para agregar un parámetro para VTI secundario (si no está ya configurado).

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. Si está creando una nueva interfaz VTI, agregue los parámetros correctos, actívela y haga clic en "Aceptar".

NOTA: Se convierte en la VTI secundaria.

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

configuración IKE

1. Acceda a la pestaña IKE. Si lo desea, puede utilizar una directiva predefinida; de lo contrario, haga clic en el botón de lápiz situado junto a la ficha Directiva para crear una nueva directiva o seleccione otra directiva disponible en función de sus necesidades.

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  

Search

- 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. Seleccione el tipo de autenticación. Si se utiliza una clave manual previamente compartida, especifíquela en los cuadros Key (Clave) y Confirm Key (Confirmar clave).

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

configuración de IPsec

Vaya a la ficha IPsec. Puede optar por utilizar una propuesta predefinida haciendo clic en el botón de lápiz situado junto a la ficha de propuesta para crear una nueva propuesta o seleccionar otra propuesta disponible en función de sus necesidades.

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

IKEv2 Mode: Tunnel ▼

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals* 

tunnel_aes256_sha AES-GCM

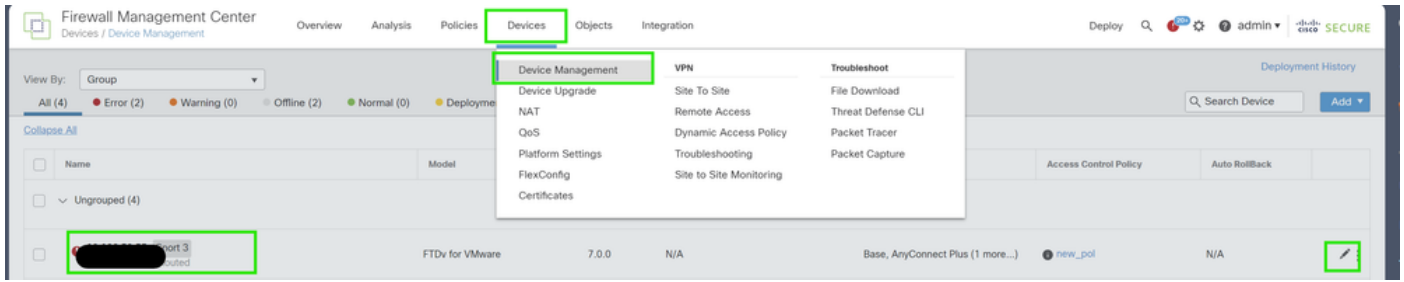
Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

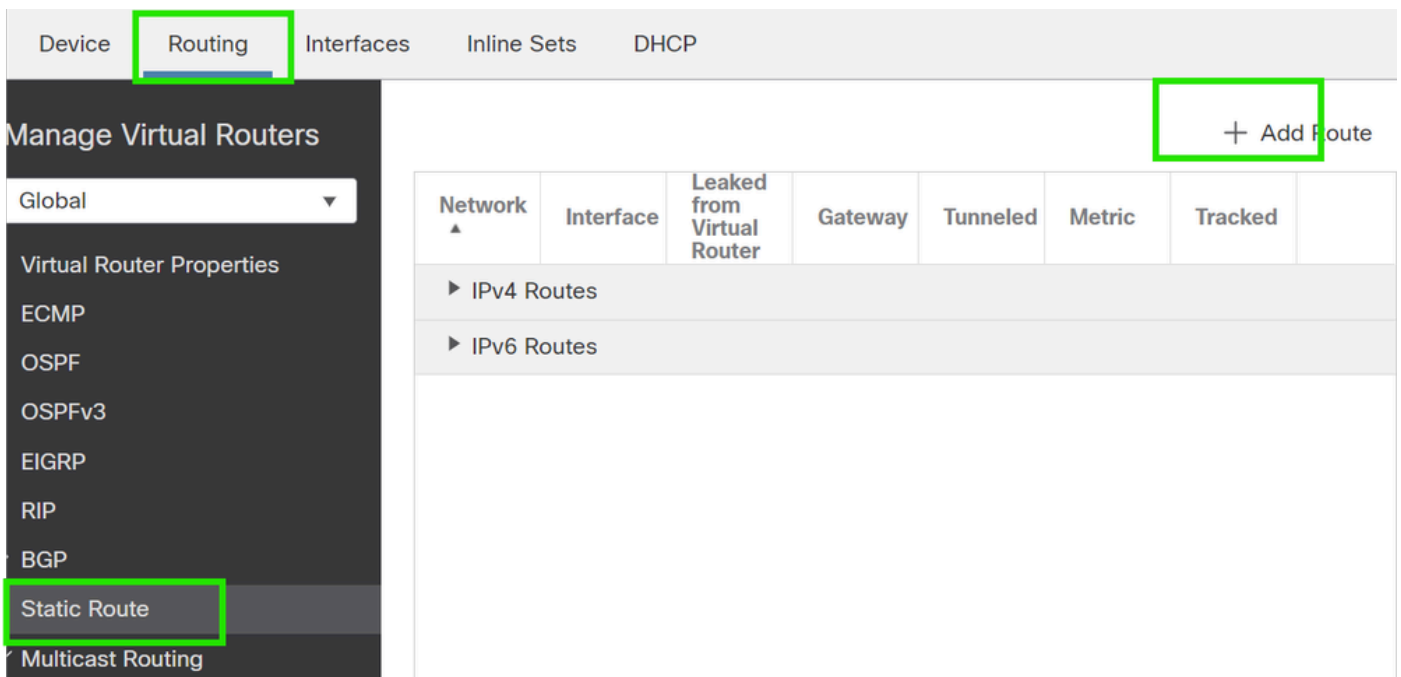
Configuración de Ruteo

1. Vaya a Device > Device Management y haga clic en el icono del lápiz para editar el dispositivo (FTD).



2. Vaya a Routing > Static Route (Enrutamiento > Ruta estática) y haga clic en el botón "+" para agregar una ruta al VTI principal y secundario.

NOTA: Puede configurar el método de routing adecuado para que el tráfico pase a través de la interfaz de túnel. En este caso, se han utilizado rutas estáticas.



3. Agregue dos rutas para su red protegida y establezca un valor AD más alto (en este caso, 2) para la ruta secundaria.

La primera ruta utiliza la interfaz VTI-1 y la segunda la interfaz 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

Verificación

1. Vaya a Dispositivos > VPN > Supervisión de sitio a sitio .

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. Haga clic en el ojo para ver más detalles sobre el estado del túnel.



View full information

Dual-ISP-VTI

Active

2024-06-11 06:55:26

Dual-ISP-VTI

Active

2024-06-12 14:27:22

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).