

# Configuration de deux interfaces VTI ISP sur FTD géré par FMC

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences de base](#)

[Composants utilisés](#)

[Configurations sur FMC](#)

[Configuration topologique](#)

[Configuration des terminaux](#)

[Configuration IKE](#)

[Configuration IPsec](#)

[Configuration du routage](#)

---

## Introduction

Ce document décrit le déploiement d'une configuration ISP double à l'aide d'interfaces de tunnel virtuel sur un périphérique FTD géré par FMC.

## Conditions préalables

### Exigences de base

- Une compréhension fondamentale des VPN de site à site serait bénéfique. Cette formation vous aide à comprendre le processus de configuration de VTI, y compris les principaux concepts et configurations impliqués.
- Il est essentiel de comprendre les principes fondamentaux de la configuration et de la gestion des interfaces VTI sur la plate-forme Cisco Firepower. Cela inclut la connaissance du fonctionnement des interfaces VTI dans le FTD et de la manière dont elles sont contrôlées via l'interface FMC.

### Composants utilisés

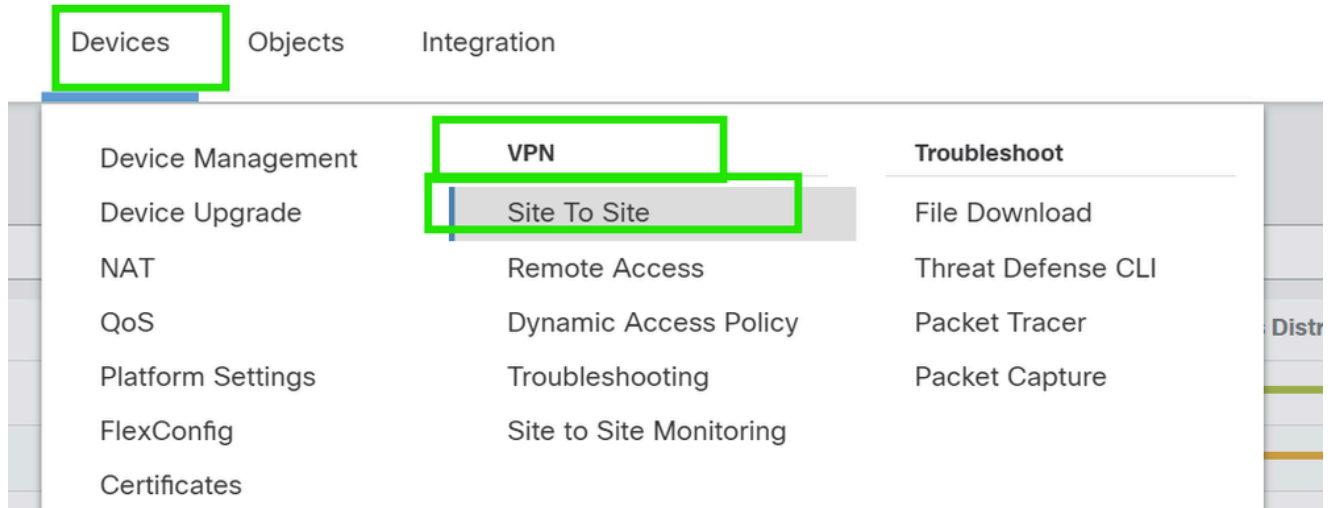
- Cisco Firepower Threat Defense (FTD) pour VMware : version 7.0.0
- Firepower Management Center (FMC) : version 7.2.4 (build 169)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

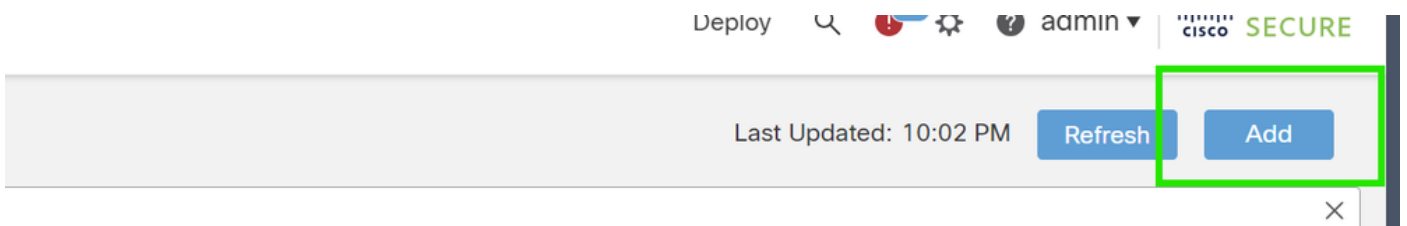
# Configurations sur FMC

## Configuration topologique

1. Accédez à Périphériques > VPN > Site à site.



2. Cliquez sur Add pour ajouter une topologie VPN.



3. Donnez un nom à la topologie, choisissez VTI et Point-to-Point, puis sélectionnez une version IKE (IKEv2 dans ce cas).



## Configuration des terminaux

1. Choisissez le périphérique sur lequel le tunnel doit être configuré.

Ajoutez les détails de l'homologue distant.

Vous pouvez ajouter une nouvelle interface de modèle virtuel en cliquant sur l'icône "+" ou en sélectionner une dans la liste existante.

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 vous créez une nouvelle interface VTI, ajoutez les paramètres appropriés, activez-la et cliquez sur « OK ».

REMARQUE : il s'agit de la VTI principale.

## 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. Cliquez sur "+ ". Add Backup VIT" pour ajouter une VIT secondaire.

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. Cliquez sur "+" pour ajouter un paramètre pour le VTI secondaire (s'il n'est pas déjà configuré).

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 vous créez une nouvelle interface VTI, ajoutez les paramètres appropriés, activez-la et cliquez sur « OK ».

REMARQUE : devient la VTI secondaire.

## 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

## Configuration IKE

1. Accédez à l'onglet IKE. Vous pouvez choisir d'utiliser une stratégie prédéfinie ou cliquer sur le bouton représentant un crayon en regard de l'onglet Stratégie pour en créer une nouvelle ou sélectionner une autre stratégie disponible en fonction de vos besoins.

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  

Q 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. Sélectionnez le type d'authentification. Si une clé manuelle pré-partagée est utilisée, fournissez-la dans les zones Clé et Confirmer la clé.



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

## Configuration IPsec

Accédez à l'onglet IPsec. Vous pouvez choisir d'utiliser une proposition prédéfinie en cliquant sur le bouton crayon situé en regard de l'onglet Proposition pour en créer une nouvelle ou en sélectionner une autre en fonction de vos besoins.

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

IKEv2 Mode: Tunnel 

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals\* 

tunnel\_aes256\_sha AES-GCM

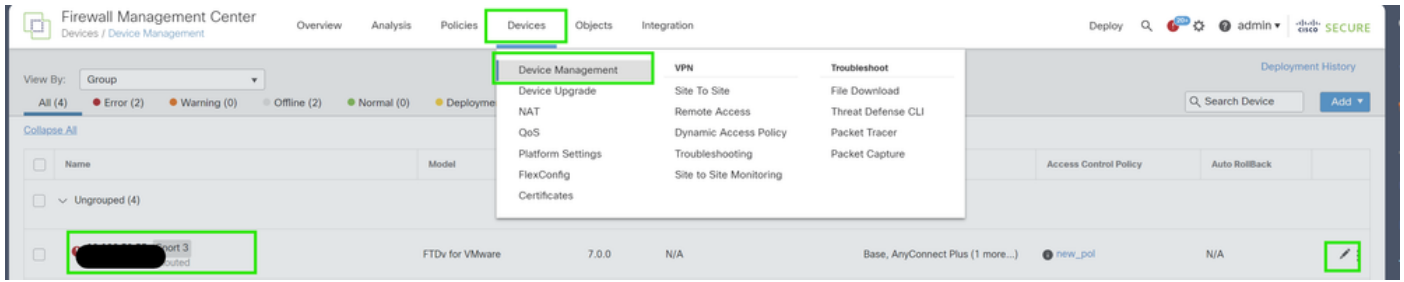
Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

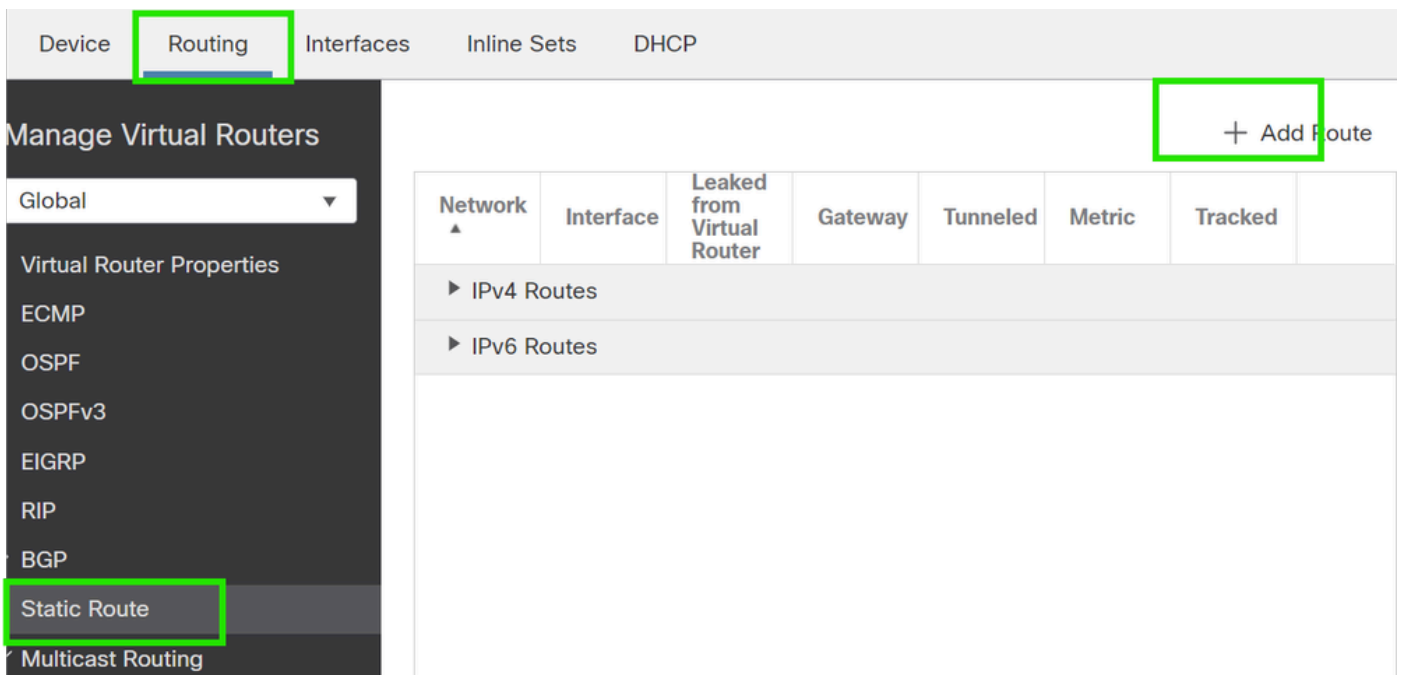
## Configuration du routage

1. Accédez à Device > Device Management et cliquez sur l'icône du crayon pour modifier le périphérique (FTD).



2. Accédez à Routing > Static Route et cliquez sur le bouton "+" pour ajouter une route à l'interface VTI principale et secondaire.

REMARQUE : Vous pouvez configurer la méthode de routage appropriée pour que votre trafic passe par l'interface du tunnel. Dans ce cas, des routes statiques ont été utilisées.



3. Ajoutez deux routes pour votre réseau protégé et définissez une valeur de distance administrative plus élevée (dans ce cas 2) pour la route secondaire.

La première route utilise l'interface VTI-1 et la seconde l'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

## Vérifier

1. Accédez à 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. Cliquez sur l'oeil pour vérifier plus de détails sur l'état du tunnel.

	Dual-ISP-VTI	Active	2024-06-11 06:55:26
<a href="#">View full information</a>	Dual-ISP-VTI	Active	2024-06-12 14:27:22

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.