

在FMC管理的FTD上設定雙ISP VTI

目錄

[簡介](#)

[必要條件](#)

[基本要求](#)

[採用元件](#)

[FMC上的配置](#)

[拓撲配置](#)

[終端配置](#)

[IKE配置](#)

[IPsec配置](#)

[路由配置](#)

簡介

本檔案將說明如何使用FMC管理的FTD裝置上的虛擬通道介面部署雙ISP設定。

必要條件

基本要求

- 對站點到站點VPN的基本瞭解將非常有益。此背景有助於掌握VTI設定過程，包括涉及的關鍵概念和配置。
- 瞭解在Cisco Firepower平台上配置和管理VTI的基本知識至關重要。這包括瞭解VTI在FTD中的運作方式以及如何透過FMC介面對其進行控制。

採用元件

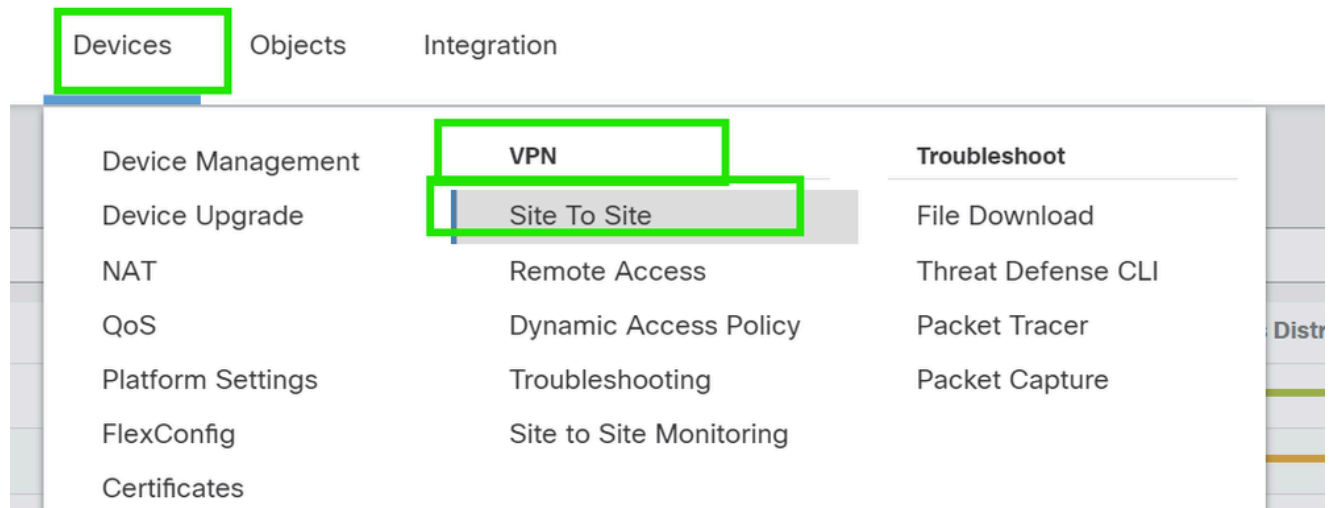
- 適用於VMware的Cisco Firepower威脅防禦(FTD)：版本7.0.0
- Firepower管理中心(FMC)：版本7.2.4 (內部版本169)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

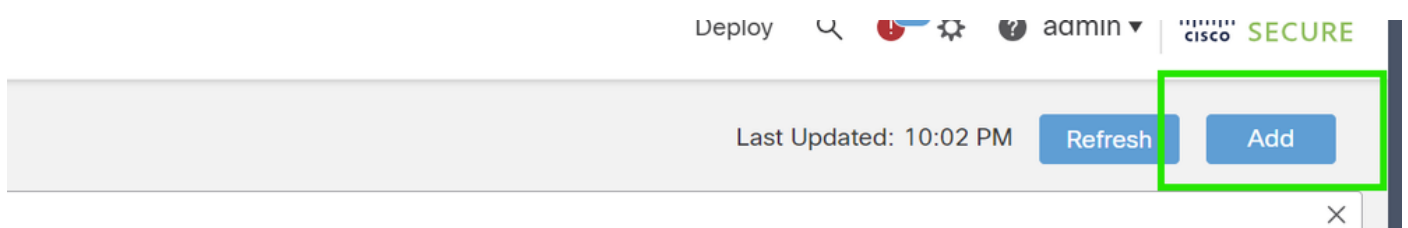
FMC上的配置

拓撲配置

1. 導航到裝置>VPN >站點到站點。



2. 按一下Add以增加VPN拓撲。



3. 為拓撲命名，選擇VTI和點對點，然後選擇IKE版本（在此例中為IKEv2）。



終端配置

1. 選擇需要配置隧道的裝置。

增加遠端對等體詳細資訊。

您可以按一下「+」圖示來新增虛擬範本介面，或從現有清單中選取一個虛擬範本介面。

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

如果要建立新的VTI介面，請增加正確的引數，將其啟用，然後按一下「確定」。

註：這成為主VTI。

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. 按一下「+」。增加備用VIT」以增加輔助VIT。

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. 按一下「+」增加輔助VTI的引數 (如果尚未配置)。

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. 如果要建立新的VTI介面，請增加正確的引數，將其啟用，然後按一下「確定」。

註：這成為輔助VTI。

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

IKE配置


1. 導航至IKE頁籤。您可以選擇使用預定義的策略，也可以按一下「策略」頁籤旁邊的鉛筆按鈕建立新策略或根據您的要求選擇另一個可用策略。

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. 選取「驗證型態」。如果使用預共用的手動金鑰，請在「金鑰」和「確認金鑰」框中提供金鑰。

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

IPsec配置

導航到IPSec頁籤。您可以按一下「提案」標籤旁的鉛筆按鈕，選擇使用預先定義的提案，來建立新的提案，或根據您的需求選取其他可用的提案。

IKEv2 Mode: Tunnel ▼

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals* 

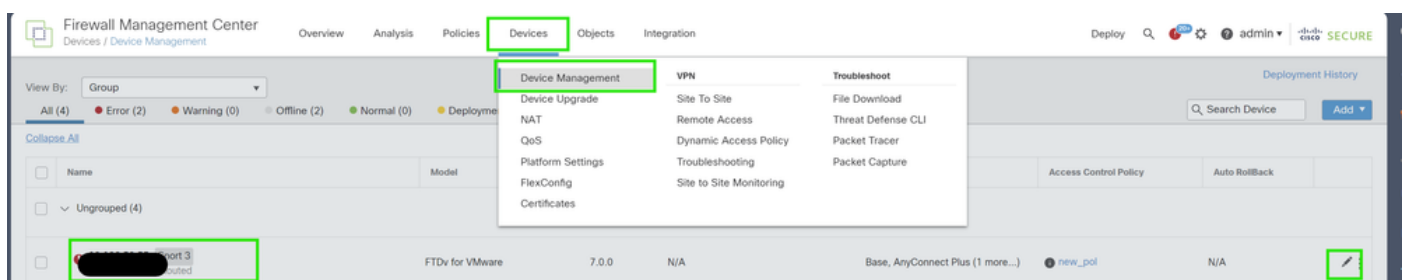
tunnel_aes256_sha

AES-GCM

 Enable Security Association (SA) Strength Enforcement Enable Reverse Route Injection Enable Perfect Forward Secrecy

路由配置

1. 轉到Device > Device Management，然後按一下鉛筆圖示以編輯裝置(FTD)。



The screenshot shows the Firewall Management Center interface. The 'Devices' tab is selected, and the 'Device Management' menu item is highlighted. A list of devices is displayed, with one device selected. The device name is partially obscured by a redaction box. The device details show it is an FTDv for VMware, version 7.0.0, with a model of N/A. The device is associated with the 'new_pol' policy.

2. 轉至Routing > Static Route，然後按一下「+」按鈕，將路由增加到主要和輔助VTI。

注意：您可以配置適當的路由方法，讓流量透過隧道介面。在本例中，使用了靜態路由。

The screenshot shows the 'Routing' tab selected in the top navigation bar. On the left, a sidebar titled 'Manage Virtual Routers' has 'Static Route' highlighted. In the main content area, the '+ Add Route' button is highlighted with a green box. Below it, a table lists route categories: IPv4 Routes and IPv6 Routes.

3. 為受保護的網路增加兩條路由，並為輔助路由設定更高的AD值（在本例中為2）。

第一條路由使用VTI-1介面，第二條路由使用VTI-2介面。

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

驗證

1. 轉至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. 按一下眼睛檢視有關隧道狀態的更多詳細資訊。

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。