

# 在由FMC管理的FTD上配置双ISP VTI

## 目录

---

[简介](#)

[先决条件](#)

[基本要求](#)

[使用的组件](#)

[FMC上的配置](#)

[拓扑配置](#)

[终端配置](#)

[IKE 配置](#)

[IPSec 配置](#)

[路由配置](#)

---

## 简介

本文档介绍在FMC管理的FTD设备上使用虚拟隧道接口部署双ISP设置。

## 先决条件

### 基本要求

- 对站点到站点VPN有基本了解将非常有益。此背景有助于掌握VTI设置过程，包括涉及的关键概念和配置。
- 了解在Cisco Firepower平台上配置和管理VTI的基础知识至关重要。这包括了解VTI如何在FTD中运行，以及如何通过FMC界面控制它们。

### 使用的组件

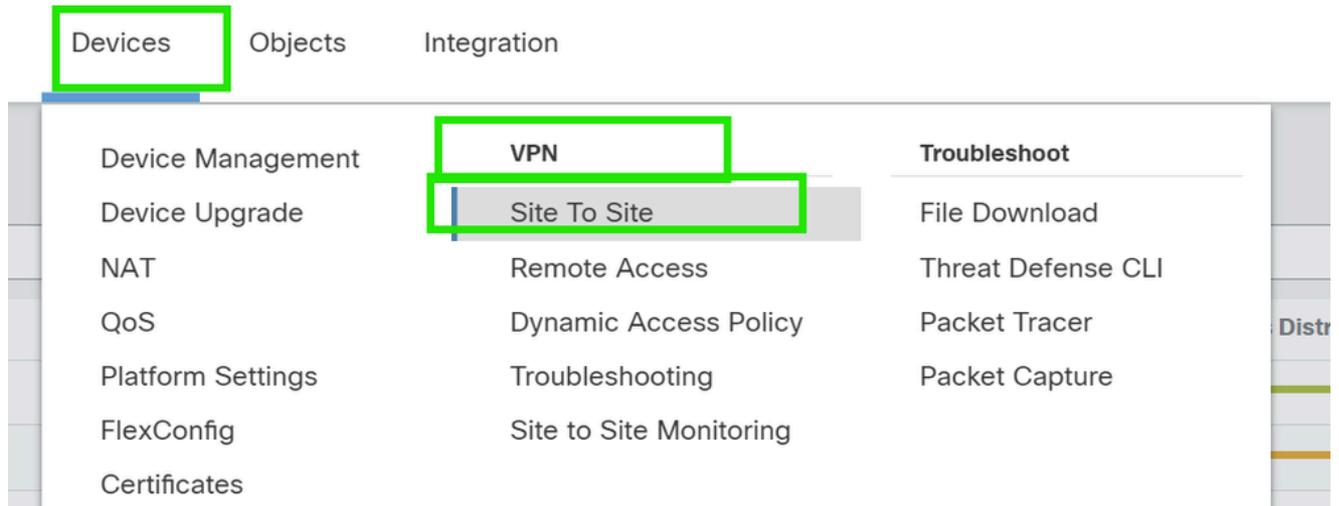
- 适用于VMware的思科Firepower威胁防御(FTD)：版本7.0.0
- Firepower管理中心(FMC)：版本7.2.4 ( 内部版本169 )

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

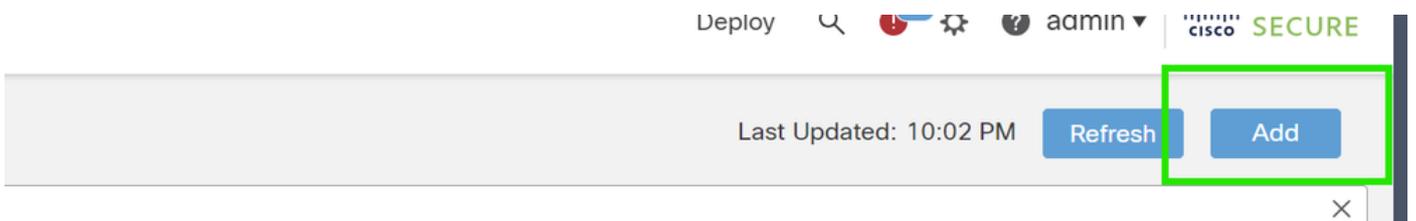
## FMC上的配置

### 拓扑配置

1. 导航到设备>VPN >站点到站点。



2. 单击Add以添加VPN拓扑。



3. 为拓扑命名，选择VTI和点对点，然后选择IKE版本（本例中为IKEv2）。



## 终端配置

1. 选择需要配置隧道的设备。

添加远程对等体详细信息。

您可以通过点击“+”图标添加新的虚拟模板接口，或从现有列表选择一个虚拟模板接口。

**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

如果要创建新的VTI接口，请添加正确的参数，启用该接口，然后单击“确定”。

注意：这将成为主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. 单击“+”。添加备份VIT”以添加辅助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. 点击“+”添加辅助VTI的参数（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. 如果要创建新的VTI接口，请添加正确的参数，启用该接口，然后单击“确定”。

注意：这将成为辅助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. 导航至IKE选项卡。您可以选择使用预定义的策略，也可以点击Policy选项卡旁边的铅笔按钮创建新策略，或者根据需要选择其他可用策略。

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

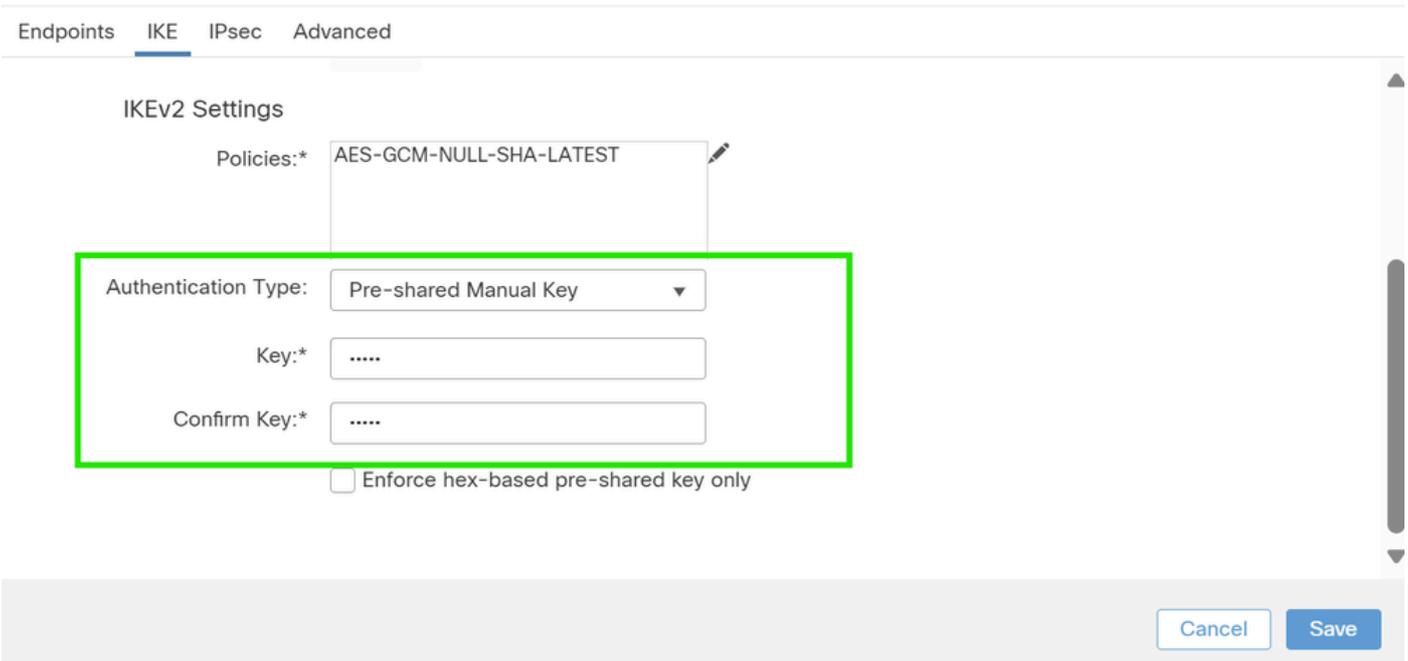
Add

Selected IKEv2 Policy

- AES-GCM-NULL-SHA-LATEST 

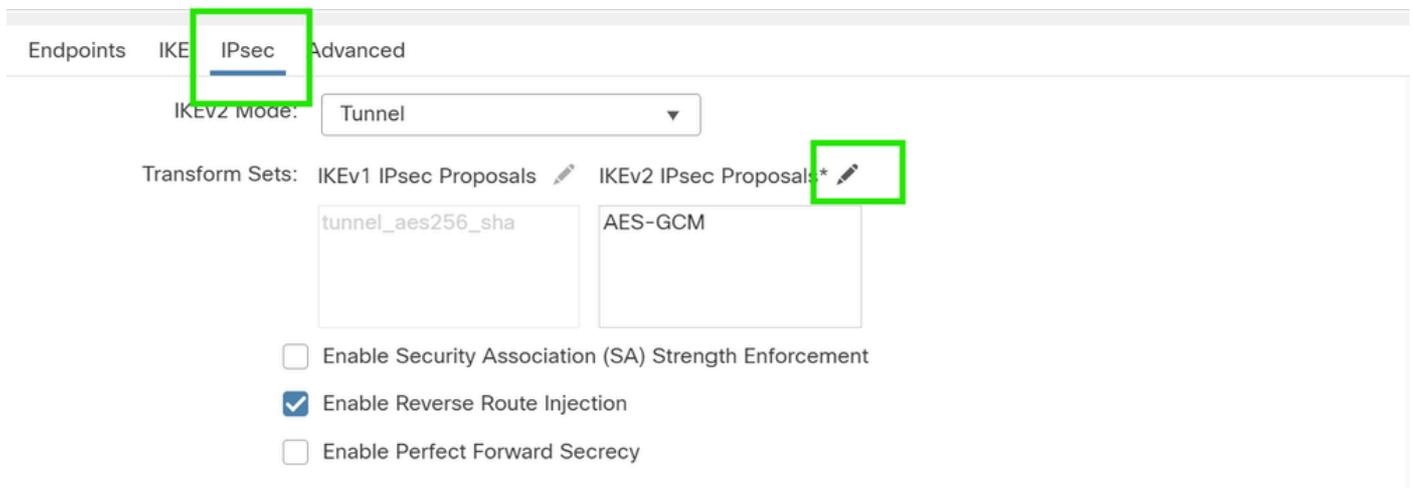
Cancel OK

2. 选择身份验证类型。如果使用预共享手动密钥，请在Key和Confirm Key框中提供密钥。



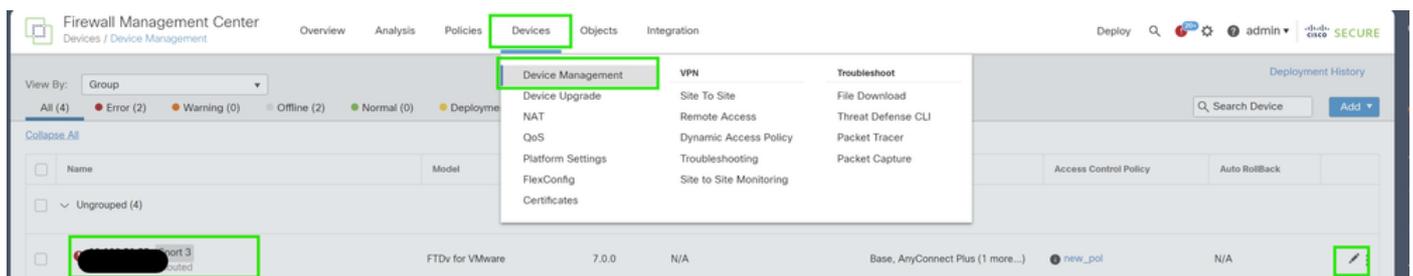
## IPSec 配置

导航到IPsec选项卡。您可以点击proposal ( 建议 ) 选项卡旁边的铅笔按钮选择使用预定义的建议创建新建议，也可以根据需要进行另一个可用建议。



## 路由配置

1. 转至Device > Device Management，并单击铅笔图标编辑设备(FTD)。



2. 转至Routing ( 路由 ) > Static Route ( 静态路由 )，然后单击“+”按钮，将路由添加到主要和辅助VTI。

注意：您可以配置适当的路由方法，让流量通过隧道接口。在本例中，使用了静态路由。

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 in the top right corner. Below the button is a table with columns: Network, Interface, Leaked from Virtual Router, Gateway, Tunneled, Metric, and Tracked. The table is currently empty, with expandable sections for IPv4 and IPv6 routes.

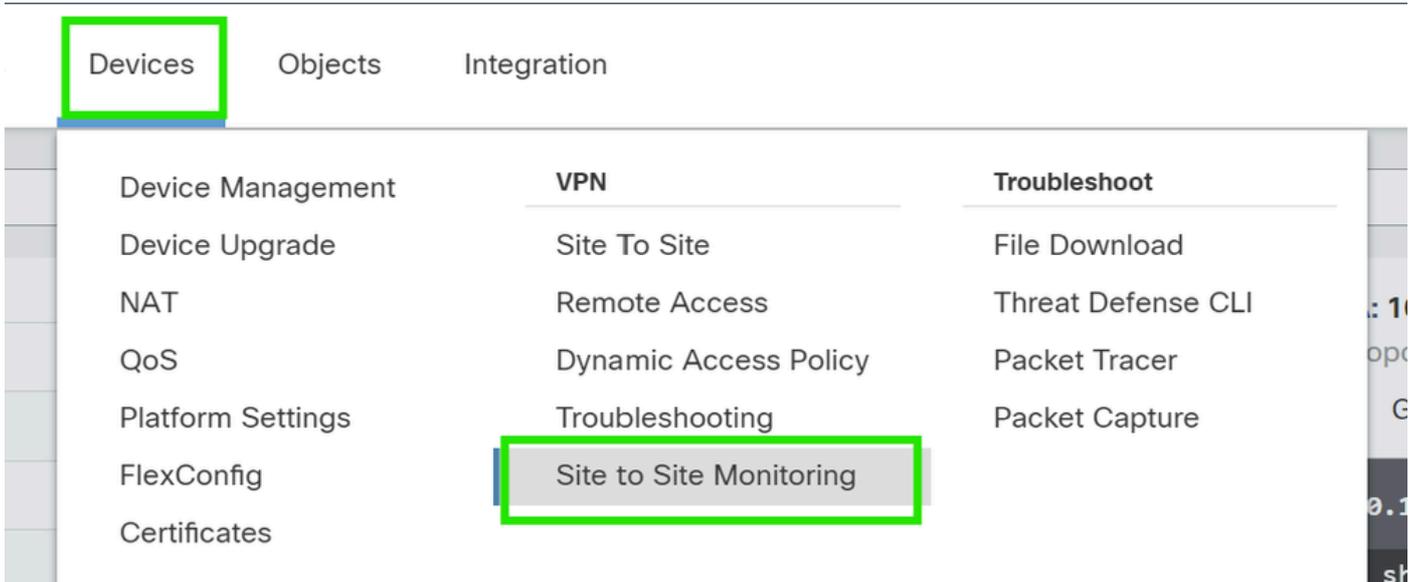
3. 为受保护网络添加两个路由，并为辅助路由设置更高的AD值（本例中为2）。

第一条路由使用VTI-1接口，第二条路由使用VTI-2接口。

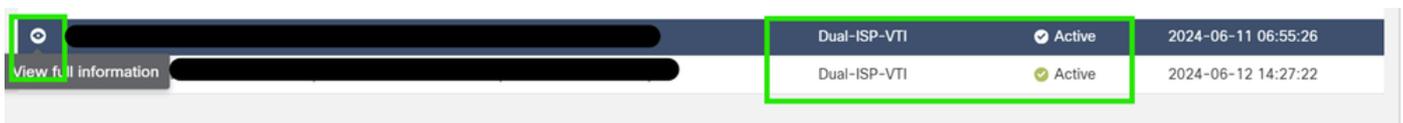
Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric
▼ IPv4 Routes					
protected-network	VTI-1	Global	VTI-1-Gateway	false	1
protected-network	VTI-2	Global	VTI-2-Gateway	false	2

## 验证

1. 转至Devices > VPN > Site to Site Monitoring。



2. 单击眼睛查看有关隧道状态的更多详细信息。



## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。