

FMCによって管理されるFTD上のデュアルISP VTIの設定

内容

[はじめに](#)

[前提条件](#)

[基本的な要件](#)

[使用するコンポーネント](#)

[FMCでの設定](#)

[トポロジの設定](#)

[エンドポイントの設定](#)

[IKEの設定。](#)

[IPSecの設定](#)

[ルーティング設定](#)

はじめに

このドキュメントでは、FMCによって管理されるFTDデバイス上で仮想トンネルインターフェイスを使用してデュアルISP設定を展開する方法について説明します。

前提条件

基本的な要件

- サイト間VPNの基本的な知識があると役に立ちます。この背景説明は、関連する主要な概念と設定を含め、VTIのセットアッププロセスを把握するのに役立ちます。
- Cisco FirepowerプラットフォームでのVTIの設定と管理の基礎を理解することが不可欠です。これには、VTIがFTD内でどのように機能し、FMCインターフェイスを介してどのように制御されるかについての知識が含まれます。

使用するコンポーネント

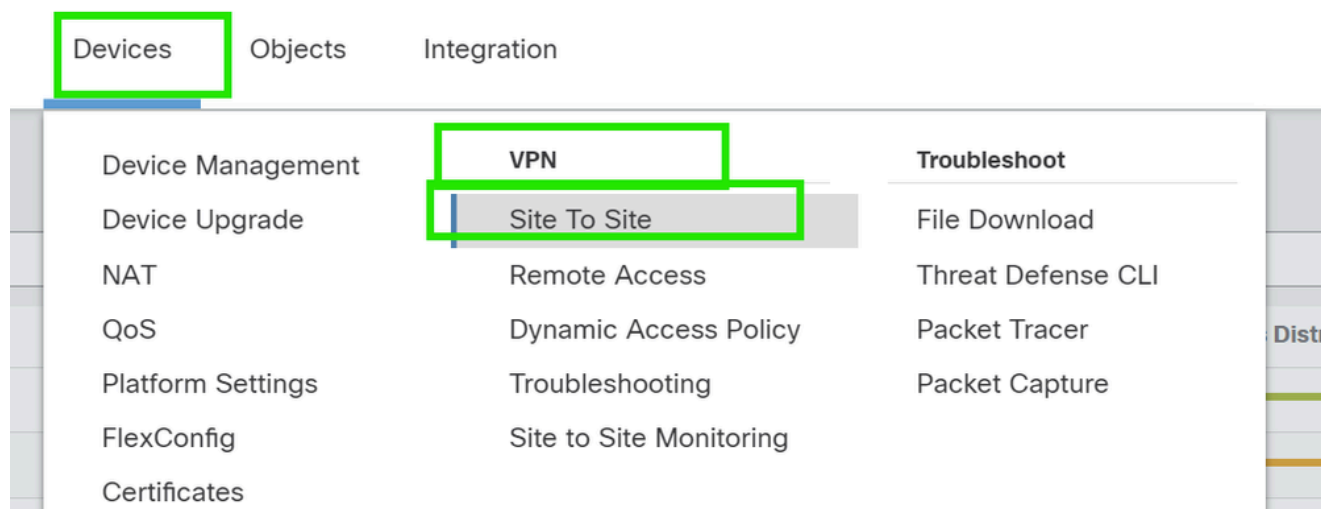
- Cisco Firepower Threat Defense(FTD)for VMware : バージョン7.0.0
- Firepower Management Center(FMC) : バージョン7.2.4 (ビルド169)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

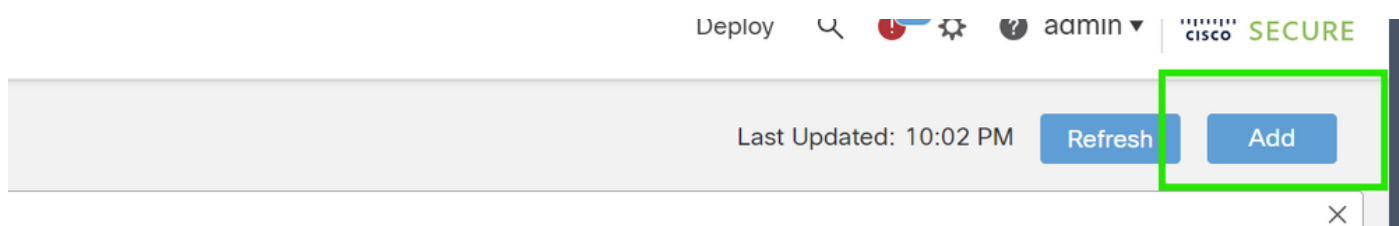
FMCでの設定

トポロジの設定

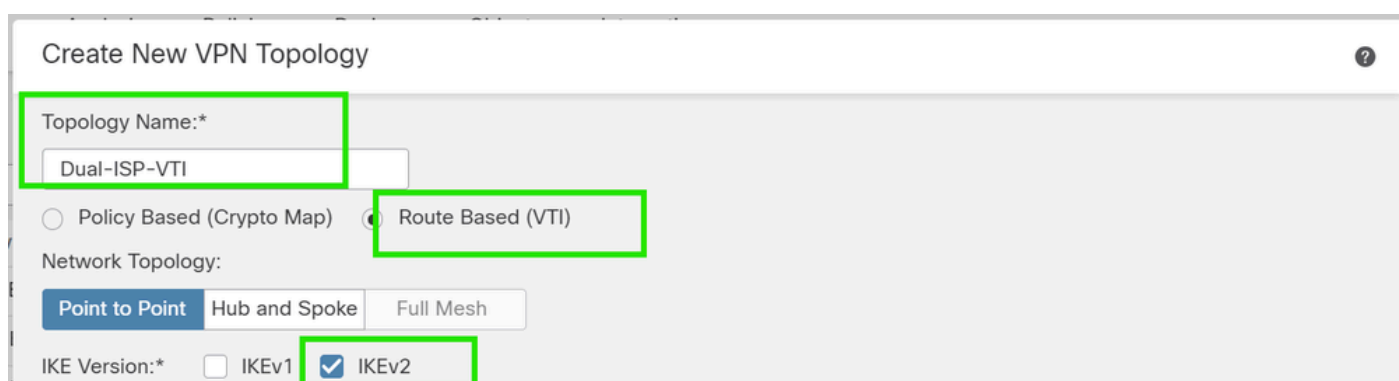
1. Devices > VPN > Site To Siteの順に移動します。



2. Addをクリックして、VPNトポロジを追加します。



3. トポロジに名前を付け、VTIとポイントツーポイントを選択し、IKEバージョン (この場合はIKEv2) を選択します。



エンドポイントの設定

1. トンネルを設定する必要があるデバイスを選択します。

リモートピアの詳細を追加します。

新しい仮想プレートインターフェイスを追加するには、「+」アイコンをクリックするか、既存のリストから選択します。

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

新しいVTIインターフェイスを作成する場合は、正しいパラメータを追加して有効にし、「OK」をクリックします。

注：これがプライマリVTIになります。

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. [+]をクリックします。「Add Backup VIT」を使用して、セカンダリVITを追加します。

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. セカンダリVTIのパラメータを追加するには、「+」をクリックします（まだ設定されていない場合）。

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. 新しいVTIインターフェイスを作成する場合は、正しいパラメータを追加して有効にし、[OK]をクリックします。

注：これはセカンダリVTIになります。

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 の設定。

1. IKEタブに移動します。定義済みのポリシーを使用するか、または[ポリシー]タブの横にある鉛筆ボタンをクリックして新しいポリシーを作成するか、要件に応じて別の使用可能なポリシーを選択できます。

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. 認証タイプを選択します。事前共有手動キーを使用する場合は、[キー]ボックスと[確認キー]ボックスにキーを入力します。

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 の設定

IPsecタブに移動します。事前定義済み提案を使用するには、「提案」タブの横にある鉛筆ボタンをクリックして新しい提案を作成するか、要件に応じて別の使用可能な提案を選択します。

IKEv2 Mode: Tunnel Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals* 

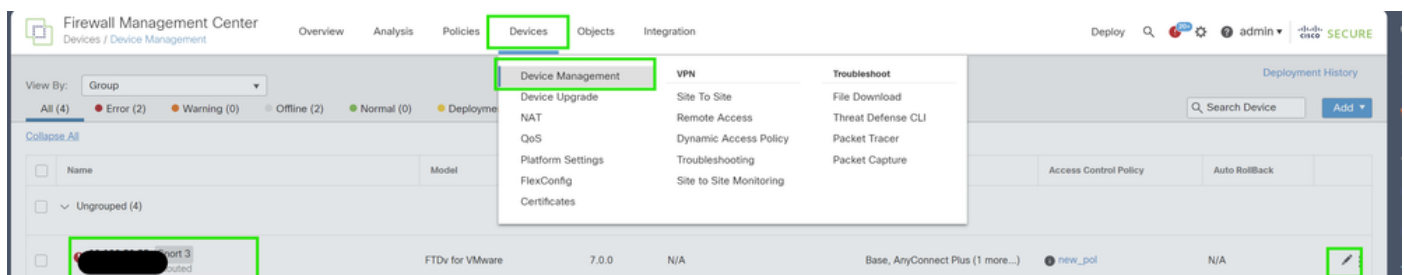
tunnel_aes256_sha

AES-GCM

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

ルーティング設定

1. Device > Device Managementの順に移動し、鉛筆のアイコンをクリックしてデバイス(FTD)を編集します。



Firewall Management Center
Devices / Device Management

Overview Analysis Policies **Devices** Objects Integration

View By: Group

All (4) Error (2) Warning (0) Offline (2) Normal (0) Deployment (0)

Collapse All

| Name | Model |
|---------------|-----------------|
| Ungrouped (4) | |
| ... | FTDv for VMware |

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

Deployment History

Search Device Add

Access Control Policy Auto Rollback

new_pol N/A

2. Routing > Static Routeの順に選択し、「+」ボタンをクリックしてプライマリおよびセカンダリVTIにルートを追加します。

注：トラフィックがトンネルインターフェイスを通過するための適切なルーティング方式を設定できます。この例では、スタティックルートが使用されています。

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 the button, there are expandable sections for 'IPv4 Routes' and 'IPv6 Routes'.

3. 保護ネットワーク用に2つのルートを追加し、セカンダリルート用により高いAD値（この場合は2）を設定します。

最初のルートはVTI-1インターフェイスを使用し、2番目のルートはVTI-2インターフェイスを使用します。

| 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 |

確認

1. Devices > VPN > Site to Site Monitoringの順に選択します。

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. 目をクリックして、トンネルのステータスの詳細を確認します。

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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。