# FMCによって管理されるFTDでのルートベース のサイト間VPNトンネルの設定

| 内容                 |  |  |
|--------------------|--|--|
| <u>はじめに</u>        |  |  |
| <u>前提条件</u>        |  |  |
| <u>要件</u>          |  |  |
| <u>使用するコンポーネント</u> |  |  |
| <u>背景説明</u>        |  |  |
| <u>制限と制約事項</u>     |  |  |
| <u>FMCでの設定手順</u>   |  |  |
| <u>確認</u>          |  |  |
| <u>FMCのGUIから</u>   |  |  |
| FTD CLIから          |  |  |

## はじめに

このドキュメントでは、Firepower Management Center(CMC)によって管理されるFirepower Threat Defense(FTD)で、スタティックルートベースのサイト間VPNトンネルを設定する方法につ いて説明します。

## 前提条件

要件

次の項目に関する知識があることが推奨されます。

- VPNトンネルの動作方法に関する基本的な知識。
- FMCのナビゲート方法を理解していること。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- ・ CiscoFirepowerマネジメントセンター(FMC)バージョン6.7.0
- CiscoFirepower脅威対策(FTD)バージョン6.7.0

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。

## 背景説明

ルートベースのVPNでは、暗号化する対象トラフィック、またはVPNトンネル経由で送信する対 象トラフィックを判別でき、ポリシーベースまたはクリプトマップベースのVPNのように、ポリ シー/アクセスリストの代わりにトラフィックルーティングを使用できます。 暗号化ドメインは、 IPSecトンネルに入るすべてのトラフィックを許可するように設定されます。IPsecローカルおよ びリモートトラフィックセレクタは0.0.0/0.0.0.0に設定されます。つまり、IPSecトンネルにル ーティングされるすべてのトラフィックは、送信元/宛先サブネットに関係なく暗号化されます。

このドキュメントでは、スタティック仮想トンネルインターフェイス(SVTI)の設定を中心に説明 します。セキュアファイアウォールでのダイナミック仮想トンネルインターフェイス(DVTI)の設 定については、この<u>ドキュメント</u>を参照してください。

#### 制限と制約事項

次に、FTDのルートベーストンネルに関する既知の制限事項と制約事項を示します。

- IPsecのみをサポートします。GREはサポートされていません。
- IPv4インターフェイスと、IPv4、保護されたネットワーク、またはVPNペイロードのみをサポートします(IPv6はサポートされません)。
- VPNのトラフィックを分類するVTIインターフェイスでは、スタティックルーティングと BGPダイナミックルーティングプロトコルだけがサポートされます(OSPF、RIPなどの他 のプロトコルはサポートされません)。
- ・ インターフェイスごとに100のVTIだけがサポートされます。
- VTIはFTDクラスタではサポートされていません。
- VTIは、次のポリシーではサポートされていません。

•QoS

•NAT

・プラットフォームの設定

FMC/FTDバージョン6.7.0では、新しいVPNトンネルに対して次のアルゴリズムはサポートされ ていません(FMCは、FTD < 6.7を管理するために削除されたすべての暗号をサポートします )。

• 3DES、DES、およびNULL暗号化は、IKEポリシーではサポートされていません。

- DHグループ1、2、および24は、IKEポリシーおよびIPsecプロポーザルではサポートされて いません。
- MD5整合性はIKEポリシーではサポートされていません。
- PRF MD5はIKEポリシーでサポートされていません。
- IPSecプロポーザルでは、DES、3DES、AES-GMAC、AES-GMAC-192、およびAES-GMAC-256暗号化アルゴリズムはサポートされていません。
- ◆ 注:これは、サイト間ルートベースおよびポリシーベースのVPNトンネルの両方に当てはまります。古いFTDをFMCから6.7にアップグレードするために、アップグレードをブロックする削除された暗号に関連する変更についてユーザに警告する事前検証チェックがトリガーされます。

| FTD 6.7はFMC 6.7で管理                              | 使用可能な設定   | サイト間VPNトンネル   |
|---|---|---|
| 新規インストール  | 脆弱な暗号を使用できますが、<br>FTD 6.7デバイスの設定には使<br>用できません。                                      | 脆弱な暗号を使用できますが、<br>FTD 6.7デバイスの設定には使<br>用できません。                |
| アップグレード:FTDは脆弱な<br>暗号のみで設定されている                 | FMC 6.7 UIからアップグレード<br>すると、検証前チェックでエラ<br>ーが表示されます。アップグレ<br>ードは再構成されるまでブロッ<br>クされます。 | FTDのアップグレード後、ピア<br>がその設定を変更していないと<br>想定すると、トンネルが終了し<br>ます。    |
| アップグレード:FTDは一部の<br>弱い暗号と一部の強い暗号での<br>み設定されています。 | FMC 6.7 UIからアップグレード<br>すると、検証前チェックでエラ<br>ーが表示されます。アップグレ<br>ードは再構成されるまでブロッ<br>クされます。 | FTDのアップグレード後、ピア<br>に強力な暗号が設定されている<br>と想定すると、トンネルが再確<br>立されます。 |
| アップグレード:クラスCの国<br>(強力な暗号ライセンスを持た<br>ない)         | DESを許可する  | DESを許可する  |

を参照。

✤ 注:追加のライセンスは必要ありません。ルートベースVPNは、ライセンスモードと評価モードで設定できます。 暗号化に準拠していない場合(輸出規制機能が有効)、暗号化アルゴリズムとして使用できるのはDESだけです。

## FMCでの設定手順

ステップ1: Devices >VPN > Site To Siteの順に移動します。

| Overview Analysis | Policies | Devic              | es Obj | jects | AMP Inte      | lligence         |                  |       |
|-------------------|----------|--------------------|--------|-------|---------------|------------------|------------------|-------|
| Device Management | NAT      | VPN 🔻              | QoS    | Pla   | form Settings | FlexConfig       | Certificates     |       |
|                   |          | Site To S          | Site   |       |               |                  |                  |       |
| View By : Group   | į        | Remote<br>Troubles | Access | D)    | Warning (0)   | Offline (0)   No | ormal (1)   Depl | oymer |

ステップ 2:Add VPNをクリックし、図に示すように、Firepower Threat Defense Deviceを選択 します。

| 0   | Deploy | System      | Help 🔻      | admin 🔻  |
|-----|--------|-------------|-------------|----------|
|     |        |             |             |          |
|     |        |             | 💿 A         | dd VPN 👻 |
|     | Fire   | epower Dev  | ice         |          |
| Ø 6 | Fire   | epower Thre | eat Defense | e Device |

ステップ 3:トポロジ名を入力し、VPNのタイプとしてルートベース(VTI)を選択します。IKE Versionを選択します。

このデモンストレーションの目的は次のとおりです。

トポロジ名:VTI-ASA

IKEバージョン:IKEv2

| ○ Policy Based (Crypto Map) ○ Route Based (VTI)         Network Topology:       Image: Point to Point image: Point image | Topology Name:*   | VTI-ASA                    |             |             |
|---|-------------------|----------------------------|-------------|-------------|
| Network Topology:   |                   | O Policy Based (Crypto Map | ) 💿 Route B | ased (VTI)  |
| IKE Version:*   | Network Topology: | ↔ Point to Point 🛠 H       |             | 💠 Full Mesh |
|   | IKE Version:*     | 🗌 IKEv1 🗹 IKEv2            |             |             |

ステップ 4:トンネルを設定する必要があるデバイスを選択します。新しい仮想テンプレートイ ンターフェイスを追加するか(+アイコンをクリック)、または既存のリストから仮想テンプレート インターフェイスを選択できます。

| ndpoints                         | IKE  | IPsec   | Advanced |  |                   |
|----------------------------------|--|---------|----------|--|-------------------|
|                                  | Node A   |         |          | Node B   |                   |
| Device:*                         | :  |         |          | Device:*   |                   |
| FTD                              |  | *       |          | Empty  | *                 |
| Connecti                         | I Source IP is Private                               | Edit VI | 0        | Empty Tunnel Source IP is Private Connection Type:*                              | ► <u>Edit VTI</u> |
| Bidirectio                       | onal   | *       |          | Bidirectional  | *                 |
| Tunnel I<br>Tunnel S<br>Tunnel S | P Address<br>Source Interface<br>Source Interface IP | :       |          | Tunnel IP Address :<br>Tunnel Source Interface :<br>Tunnel Source Interface IP : |                   |

ステップ5: New Virtual Tunnel Interfaceのパラメータを定義します。[OK] をクリックします。

このデモンストレーションの目的は次のとおりです。

名前:VTI-ASA

説明(オプション):エクストラネットASAを使用したVTIトンネル

セキュリティゾーン:VTIゾーン

トンネルID:1

IPアドレス: 192.168.100.1/30

トンネル送信元: GigabitEthernet0/0(外部)

| k.I      | Add Virtual Tunne | el Interface                 | ? ×              |
|----------|-------------------|------------------------------|------------------|
| rs       | General           |                              |                  |
|          | Name *:           | VTI-ASA                      | Enabled          |
|          | Description:      | VTI Tunnel with Extranet ASA |                  |
| 2        | Security Zone:    | VTI-Zone V                   | ·                |
| r<br>/i  | Tunnel ID *:      | 1                            | Range: 0 - 10413 |
| E        | IP Address *:     | 192.168.100.1/30             | 0                |
| B        | Tunnel Source *:  | GigabitEthernet0/0 (Outside) | ~                |
| TL<br>TL |                   |                              |                  |
|          |                   |                              | OK Cancel        |

手順 6:新しいVTIが作成されたことを示すポップアップでOKをクリックします。

|   |   | Node B   |
|---|---|----------|
| Virtual Tunnel Interfa  | ce Added  |          |
| VTI has been cre<br>Please go to the<br>Interfaces page<br>the VTI. | eated successfully.<br>Device ><br>to delete/update | erface:  |
|   | ОК  | is Priva |
|   | Connection Typ                                      | e:*      |

手順 7:新しく作成したVTIか、Virtual Tunnel Interfaceの下に存在するVTIを選択します。ノード B(ピアデバイス)の情報を提供します。

このデモンストレーションの目的は次のとおりです。

#### デバイス:エクストラネット

#### デバイス名:ASA-Peer

### エンドポイントIPアドレス:10.106.67.252

| Create New VPN Topo   | logy   |             |   |            | ? × |
|---|--|-------------|---|------------|-----|
| Topology Name:*   | VTI-ASA  |             |   |            |     |
|   | O Policy Based (Crypto Map)  | Route Based | t (VTI)   |            |     |
| Network Topology:   | Point to Point 💥 Hu  | o and Spoke | Full Mesh   |            |     |
| IKE Version:*   | 🗌 IKEv1 🗹 IKEv2  |             |   |            |     |
|   |  |             |   |            |     |
| Endpoints IKE   | IPsec  | Advanced    |   |            |     |
| Nor<br>Device:*<br>FTD<br>Virtual Tunnel Inter<br>VII-ASA<br>Tunnel Source IP II<br>Connection Type:*<br>Bidirectional<br>Tunnel IP Address<br>Tunnel Source Inter<br>Tunnel Source Inter<br>Tunnel Source Inter<br>Tunnel Source Inter<br>Additional Configure<br>Route traffic to the<br>Permit VPN traffic | de A  rface:*  is Private  : 192.168.100.1  rface IP : 10.197.224.90  ration  : KVTI : Routing Policy : AC Policy : AC Policy : 10.197.224 |             | Node B Device:* Extranet Device Name*: ASA-Peer Endpoint IP Address*: 10.106.67.252 |            |     |
|   |  |             |   | Save Cance | 4   |

ステップ 8: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+ボタンをクリックして新しいポリシーを作成するかを選択できます。

| IKEv2 Settings          |            |                 |             |     |   |
|-------------------------|------------|-----------------|-------------|-----|---|
| Policy:*                | AES-GCM-   | NULL-SHA-LATES  | Г           | ~   | 0 |
| Authentication Type:    | Pre-shared | l Automatic Key |             | Y   |   |
| Pre-shared Key Length:* | 24         | Characters      | (Range 1-12 | 27) |   |
|                         |            |                 |             |     |   |

ステップ9:(新しいIKEv2ポリシーを作成する場合はオプション) ポリシーの名前を指定し、ポリシーで使用するアルゴリズムを選択します。[Save] をクリックします。

このデモンストレーションの目的は次のとおりです。

名前:ASA-IKEv2-Policy

- 整合性アルゴリズム: SHA-512
- 暗号化アルゴリズム:AES-256

PRFアルゴリズム:SHA-512

Diffie-Hellmanグループ:21

| lew IKEv2 Policy                       |   |              |                    | ? :    |
|--|---|--------------|--------------------|--------|
| Name:*                                 | ASA-IKEv2-Policy  |              |                    |        |
| Description:                           |   |              |                    |        |
| Priority:                              | 1   | (1-65535)    |                    |        |
| Lifetime:                              | 86400   | seconds (120 | -2147483647)       |        |
| Integrity Algorithms                   | Available Algorithms  |              | Selected Algorithm | ıs     |
| PRF Algorithms<br>Diffie-Hellman Group | Image: MD5         Image: SHA         Image: SHA512         Image: SHA256         Image: SHA384         Image | Add          | ⇔ SHA512           |        |
|  |   | Γ            | Save               | Cancel |

ステップ 10:新しく作成したポリシーまたは既存のポリシーを選択します。Authentication Typeを選択します。事前共有手動キーを使用する場合は、KeyボックスとConfirm Keyボックスに キーを入力します。

このデモンストレーションの目的は次のとおりです。

ポリシー: ASA-IKEv2-Policy

認証タイプ:事前共有手動キー

キー: cisco123

確認キー: cisco123

| preshared_sha_  | aes256_dh14   | _3 🗸 🗸  | 0   |
|-----------------|---|---|---|
| Pre-shared Auto | matic Key   | ~   |   |
| 24 Cha          | racters   | (Range 1-127)   |   |
|                 |   |   |   |
| u               |   |   | _   |
| ASA-IKEv2-Polic | γ.  | ~   | 0   |
| Pre-shared Man  | ual Key   | ~   |   |
| •••••           |   |   | ]   |
| •••••           |   |   | ]   |
| Enforce hex-b   | ased pre-sha  | red key only  |   |
|                 | preshared_sha_<br>Pre-shared Auto<br>24 Cha<br>ASA-IKEv2-Polic<br>Pre-shared Manu<br> | preshared_sha_aes256_dh14   Pre-shared Automatic Key   24   Characters   ASA-IKEv2-Policy   Pre-shared Manual Key   •••••••   •••••••   •••••••   •••••••   •••••••   •••••••   •••••••   •••••••   •••••••   •••••••   ••••••• | preshared_sha_aes256_dh14_3   Pre-shared Automatic Key   24   Characters   (Range 1-127)   ASA-IKEv2-Policy   Pre-shared Manual Key   •••••••   •••••••   •••••••   •••••••   •••••••   •••••••   •••••••   •••••••   •••••••   •••••••   •••••••   •••••••   •••••••   •••••••   •••••••   •••••••   ••••••• |

№ 注:両方のエンドポイントが同じFMCに登録されている場合は、Pre-shared Automatic Keyオプションも使用できます。

ステップ 11IPsecタブに移動します。 定義済みのIKEv2 IPsecプロポーザルを使用するか、新し いプロポーザルを作成するかを選択できます。IKEv2 IPsec Proposalタブの横にあるEditボタンを クリックします。

| Crypto Map Type:                                      | Static Opynamic         |                          |  |  |  |
|---|-------------------------|--------------------------|--|--|--|
| IKEv2 Mode:   | Tunnel                  |                          |  |  |  |
| Transform Sets:                                       | IKEv1 IPsec Proposals 🥜 | IKEv2 IPsec Proposals* 🥜 |  |  |  |
| Transform Sets.                                       | tunnel_aes256_sha       | AES-GCM                  |  |  |  |
| Enable Security Accociation (SA) Strength Enforcement |                         |                          |  |  |  |

ステップ12:(新しいIKEv2 IPsecプロポーザルを作成する場合はオプション) 提案の名前を入力 し、提案で使用するアルゴリズムを選択します。[Save] をクリックします。 このデモンストレーションの目的は次のとおりです。

名前:ASA-IPSec-Policy

ESPハッシュ: SHA-512

ESP暗号化:AES-256

| New IKEv2 IPsec P | roposal              |              | ? >     |
|-------------------|----------------------|--------------|---------|
| Name:*            | ASA-IPSec-Policy     |              |         |
| ESP Hash          | Available Algorithms | Selected Alg | orithms |
| ESP Encryption    | AES-GCM-256          | ( AES-256    |         |
|                   | 🔅 AES-256            | -9-          | -       |
|                   | AES-GCM-192          |              |         |
|                   | @ AES-192            | Add          |         |
|                   | AES-GCM              | AUG          |         |
|                   | AES                  |              |         |
|                   | ige 3DES             |              |         |
|                   | AES-GMAC-256         |              |         |
|                   | Lalla                |              |         |
|                   |                      |              |         |
|                   |                      |              |         |
|                   |                      |              |         |
|                   |                      | Save         | Cancel  |

ステップ 13 使用可能なプロポーザルのリストから、新しく作成したプロポーザルまたはプロポ ーザルを選択します。[OK] をクリックします。

| on:*       | IKEv2 IPsec Proposal         |     |                         | ? ×    |
|------------|------------------------------|-----|-------------------------|--------|
|            | Available Transform Sets 🖒 😳 | Γ   | Selected Transform Sets |        |
|            | 🔍 Search                     |     | ASA-IPSec-Policy        | 6      |
| N TO       | AES-GCM                      | L   |                         |        |
|            | (AES-SHA)                    |     |                         |        |
| C.         | ASA-IPSec-Policy             |     |                         |        |
| 50         | @ DES_SHA-1                  | Add |                         |        |
| Sec        |                              |     |                         |        |
| Perl       |                              |     |                         |        |
| s G        |                              |     |                         | _      |
| ura<br>ze: |                              |     | ок                      | Cancel |

ステップ14:(オプション)Perfect Forward Secrecy設定を選択します。IPSecのライフタイム期間とライフタイムサイズを設定します。

このデモンストレーションの目的は次のとおりです。

Perfect Forward Secrecy (完全転送秘密):モジュラスグループ21

Lifetime Duration (ライフタイム期間):28800(デフォルト)

Lifetime Size (ライフタイムサイズ):4608000 (デフォルト)

| ŀ | Enable Security Ass | sociation (SA) St | rength Enforcer | nent                           |
|---|---------------------|-------------------|-----------------|--------------------------------|
| L | Enable Perfect Forw | ard Secrecy       |                 |                                |
| L | Modulus Group:      | 21                | ~               |                                |
| L | Lifetime Duration*: | 28800             |                 | Seconds (Range 120-2147483647) |
| L | Lifetime Size:      | 4608000           |                 | Kbytes (Range 10-2147483647)   |
|   | - ESPv3 Settings    | •                 |                 |                                |

ステップ15:設定を確認します。次の図に示すように、Saveをクリックします。

| Topology Name:*         | VTI-ASA               |                   |                      | ]        |   |      |        |
|-------------------------|-----------------------|-------------------|----------------------|----------|---|------|--------|
|                         |                       | ased (Crypto Map) | Route Based (VT)     | I)       |   |      |        |
| Network Topology        | ⊷ Point               | to Point 🛠 Hub    | and Spoke 💠 Full     |          |   |      |        |
| IKE Version:*           | □ IKEv1               | ✓ IKEv2           |                      |          |   |      |        |
|                         |                       |                   |                      |          |   |      |        |
| Endpoints               | IKE                   | IPsec             | Advanced             |          |   |      |        |
| Crypto Map Type:        | Static O Dyna         | amic              |                      |          |   |      |        |
| IKEv2 Mode:             | Tunnel                | v                 |                      |          |   |      |        |
| Transform Sets:         | IKEv1 IPsec Propo     | sals 🥜 🛛 IK       | Ev2 IPsec Proposals* | 0        |   |      |        |
|                         | tunnel_aes256_sh      | na A              | SA-IPSec-Policy      |          |   |      |        |
| Enable Security A       | ssociation (SA) Stree | ngth Enforcement  |                      |          |   |      |        |
| Enable Perfect Fo       | rward Secrecy         |                   |                      |          |   |      |        |
| Modulus Group:          | 21                    | ~                 |                      |          |   |      |        |
| Lifetime Duration*:     | 28800                 | Secon             | nds (Range 120-2147  | 7483647) |   |      |        |
| Lifetime Size:          | 4608000               | Kbyte             | es (Range 10-214748  | 33647)   |   |      |        |
| — <b>▼ ESPv3 Settin</b> | gs                    |                   |                      |          |   |      |        |
|                         |                       |                   |                      |          |   |      |        |
|                         |                       |                   |                      |          |   |      |        |
|                         |                       |                   |                      |          |   |      |        |
|                         |                       |                   |                      |          | 5 | Save | Cancel |

ステップ 16 : アクセスコントロールポリシーを設定します。[Policies] > [Access Control] > [Access Control] の順に移動します。FTDに適用されるポリシーを編集します。

◆ 注:sysopt connection permit-vpnは、ルートベースのVPNトンネルでは機能しません。アクセスコントロールルールは、IN-> OUTゾーンとOUT -> INゾーンの両方に設定する必要があります。

Zonesタブで、Source ZonesとDestination Zonesを指定します。

Networksタブで、Source NetworksとDestination Networksを指定します。[Add] をクリックします。

このデモンストレーションの目的は次のとおりです。

送信元ゾーン: In-ZoneおよびOut-Zone

宛先ゾーン:アウトゾーンおよびインゾーン

送信元ネットワーク:ネットワーク内およびリモートネットワーク

#### 宛先ネットワーク: リモートネットワークおよびネットワーク内

| Add Rule       |                            |                       |                     |                   |                          | ? ×          |
|----------------|----------------------------|-----------------------|---------------------|-------------------|--------------------------|--------------|
| Name           | VTI-Traffic                |                       | Enabled             | Insert into Manda | itory                    | ~            |
| Action         | 🖌 Allow                    | V 00.8                | th 5                |                   |                          |              |
| Time Range     | None 🗸 🕥                   |                       |                     |                   |                          |              |
|                |                            | Annillantinan         | Deste UDI - COTIN   | a stallar to a    | Transition               | Commenter 1  |
| Zones I        | vetworks VLAN rags 🛆 Users | Applications          | Ports URLS SGI/I:   | SE Attributes     | Inspection Logg          | ng Comments  |
| Available Zon  | name                       |                       | Source Zones (Z)    |                   | Destination Zones (2)    |              |
| Search by      | name                       |                       | -20ne               |                   | - Out-Zone               |              |
| - In-Zone      |                            |                       |                     | 0                 | and a series             | 9            |
| VTI-Zone       |                            | Add to                |                     |                   |                          |              |
|                |                            | Source                |                     |                   |                          |              |
|                |                            | Add to<br>Destination |                     |                   |                          |              |
|                |                            | Destination           |                     |                   |                          |              |
|                |                            |                       |                     |                   |                          |              |
| Add Rule       |                            |                       |                     |                   |                          | ? ×          |
|                |                            |                       |                     |                   |                          |              |
| Name           | VTI-Traffic                |                       | Enabled             | Insert into Manda | atory                    | *            |
| Action         | Allow                      | S. O U 💌              | 'ta 💵               |                   |                          |              |
| Time Range     | None 🗸 🔾                   |                       |                     |                   |                          |              |
| Zones N        | etworks VLAN Tags 🔺 Users  | s Applications        | Ports URLs SGT/     | SE Attributes     | Inspection Logo          | ing Comments |
| Available Netv | vorks C 🖸                  |                       | Source Networks (2) |                   | Destination Networks (2) |              |
|                |                            |                       | Source              | Original Client   | 📻 In-Netwrk              | 5            |
| Netwo          | rks Geolocation            |                       | 📻 In-Netwrk         | 8                 | Remote-Network           |              |
| IPv4-Privat    | e-172.16.0.0-12            |                       | Remote-Network      | 6                 |                          |              |
| IPv4-Privat    | e-192.168.0.0-16           | Add To<br>Source      |                     |                   |                          |              |
| Pv4-Privat     | e-All-RFC1918              | Networks              |                     |                   |                          |              |
| IPv6-Link-L    | ocal                       | Add to<br>Destination |                     |                   |                          |              |
| IPv6-Privat    | e-Unique-Local-Addresses   |                       |                     |                   |                          |              |
| IPv6-to-IPv    | /4-Relay-Anycast           |                       |                     |                   |                          |              |
| Remote-Ne      | twork                      |                       |                     |                   |                          |              |
| VTI-ASA-TU     | unnel                      |                       | Enter an IP address | Add               | Enter an IP address      | Add          |
|                |                            |                       |                     |                   |                          |              |
|                |                            |                       |                     |                   | Add                      | Cancel       |

ステップ 17:VTIトンネル経由のルーティングを追加します。[Device] > [Device Management]に 移動します。VTIトンネルが設定されているデバイスを編集します。

Routingタブの下のStatic Routeに移動します。[Add Route] をクリックします。

Interfaceを指定し、Networkを選択して、Gatewayを指定します。[OK] をクリックします。

このデモンストレーションの目的は次のとおりです。

インターフェイス:VTI-ASA

ネットワーク:リモートネットワーク

ゲートウェイ:VTI-ASA-Tunnel

| Add Static Ro   | ute Configuration   | ? X       |
|---|---|-----------|
| Type:<br>Interface*   | ● IPv4 ○ IPv6<br>VTI-ASA  | ute leak) |
| Available Ne<br>Search<br>any-ipv4<br>In-Netwrk<br>IPv4-Benk<br>IPv4-Link<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPv4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive<br>IPV4-Prive | twork C   Selected Network   Remote-Network   Image: Remote-Network   Add   Add   Add   Image: Remote-Network   Image: Remote-Network |           |
| Gateway*<br>Metric:<br>Tunneled:<br>Route Tracking:   | VTI-ASA-Tunnel  VTI-ASA-Tunnel  (1 - 254)  (Used only for default Route)  VK  | Cancel    |

ステップ 18 : Deploy > Deploymentの順に移動します。設定を展開する必要があるFTDを選択し、Deployをクリックします。

導入が成功した後、設定がFTD CLIにプッシュされました。

<#root>

crypto ikev2 policy 1

encryption aes-256 integrity sha512 group 21 prf sha512 lifetime seconds 86400

```
crypto ikev2 enable Outside
crypto ipsec ikev2 ipsec-proposal CSM_IP_1
 protocol esp encryption aes-256
protocol esp integrity sha-512
crypto ipsec profile FMC_IPSEC_PROFILE_1
set ikev2 ipsec-proposal CSM_IP_1
set pfs group21
group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ikev1 ikev2
tunnel-group 10.106.67.252 type ipsec-121
tunnel-group 10.106.67.252 general-attributes
 default-group-policy .DefaultS2SGroupPolicy
tunnel-group 10.106.67.252 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
interface Tunnel1
description VTI Tunnel with Extranet ASA
nameif VTI-ASA
 ip address 192.168.100.1 255.255.255.252
```

tunnel source interface Outside tunnel destination 10.106.67.252 tunnel mode ipsec ipv4

tunnel protection ipsec profile FMC\_IPSEC\_PROFILE\_1

## 確認

#### FMCのGUIから

Check Statusオプションをクリックして、GUI自体からVPNトンネルのライブステータスを監視 します



#### これには、FTD CLIから取得した次のコマンドが含まれます。

- show crypto ipsec sa peer <Peer IP address>
- ・ show vpn-sessiondb detail I2I filter ipaddress <ピアIPアドレス>

| extranet : ASA-Peer                            | The FTD/VTI-ASA  |
|--|--|
| > show crypto ipsec sa peer                    | > show crypto ipsec sa peer 10.106.67.252  |
| Not applicable for extranet peer               | <pre>peer address: 10 106 67 252<br/>Crypto map tag:vti-crypto-map-4-0-1, seq num: 65280, local addr<br/>10.197.224.90<br/>local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)<br/>remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)<br/>current_peer: 10.106.67.252<br/>#pkts encaps: 100, #pkts encrypt: 100, #pkts digest: 100<br/>#pkts decaps: 100, #pkts decrypt: 100, #pkts verify: 100<br/>#pkts compressed: 0, #pkts decompressed: 0<br/>#pkts not compressed: 100, #pkts comp failed: 0, #pkts decomp<br/>failed: 0<br/>#pre-frag successes: 0, #pre-frag failures: 0, #fragments<br/>created: 0<br/>#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing<br/>reassembly: 0<br/>#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0<br/>#send errors: 0, #recv errors: 0<br/>local crypto endpt.: 10.197.224.90/500, remote crypto endpt.:<br/>10.106.67.252/500</pre> |
| show vpn-sessiondb detail l2l filter ipaddress | > show von-sessiondb detail l2l filter ipaddress 10.106.67.252   |
| Not applicable for extranet peer               | Session Type: LAN-to-LAN Detailed<br>Connection : 10.106.67.252<br>Index : 44 IP Addr : 10.106.67.252<br>Protocol : IKEV2 IPsec<br>Encryption : IKEV2: (1)AES256 IPsec: (1)AES256<br>Hashing : IKEV2: (1)SHA512 IPsec: (1)SHA512<br>Bytes Tx : 10000 Bytes Rx : 10000<br>Login Time : 03:54:57 UTC Thu Nov 12 2020<br>Duration : 0h:02m:12s<br>Tunnel Zone : 0<br>IKEV2 Tunnels: 1<br>IPsec Tunnels: 1   |
|  | IKEV2:<br>Tunnel ID : 44.1<br>UDP Src Port : 500<br>Rem Auth Mode: preSharedKeys<br>Loc Auth Mode: preSharedKeys<br>Encryption : AES256 Hashing : SHA512<br>Rekey Int (T): 86400 Seconds Rekey Left(T): 86268 Seconds<br>PRF : SHA512 D/H Group : 21   |

### FTD CLIから

これらのコマンドは、FTD CLIから使用して、VPNトンネルの設定とステータスを表示できます。

show running-config route show crypto ikev1 sa detailed show crypto ikev2 sa detailed show crypto ipsec sa detailed show vpn-sessiondb detail 121 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。