

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

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[制限事項と制約事項](#)

[FMCでの設定手順](#)

[確認](#)

[FMCのGUIから](#)

[FTD CLIから](#)

はじめに

このドキュメントでは、Firepower Management Center(FMC)によって管理されるFirepower Threat Defense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の移動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。

- Cisco Firepower Management Center(FMC)バージョン6.7.0
- Cisco Firepower Threat Defense(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、暗号化するトラフィック、またはVPNトンネルを介して送信するトラフィックを判別できません。また、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せん。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クタは0.0.0.0/0.0.0.0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[ドキュメント](#)を参照してください。

制限事項と制約事項


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 (IPv6はサポートされない)。
- VPN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ています (OSPF、RIPなどの他のプロトコルはサポートされていません)。
- インターフェイスあたり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
 - プラットフォーム設定


これらのアルゴリズムは、新しいVPNトンネル用のFMC/FTDバージョン6.7.0ではサポートされなくなりました (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、およびヌル暗号化は、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ポリシーではサポートされていません。
- DES、3DES、AES-GMAC、AES-GMAC-192、およびAES-GMAC-256暗号化アルゴリズムは、IPsec Proposalではサポートされていません。

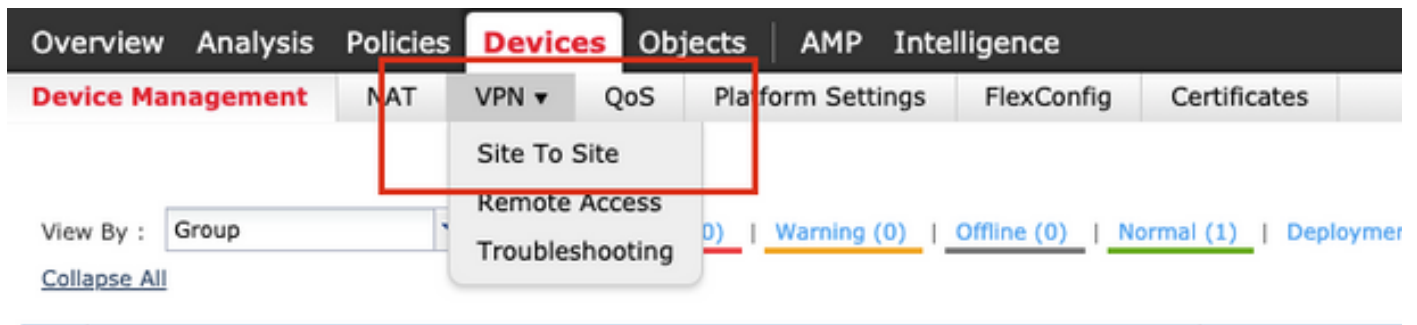
 注：これは、サイト間ルートベースおよびポリシーベースのVPNトンネルの両方に当てはまります。古いFTDをFMCから6.7にアップグレードするために、アップグレードをブロックする削除された暗号に関連する変更について、ユーザに警告する事前検証チェックがトリガーされます。

FTD 6.7はFMC 6.7で管理	利用可能な構成	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、FTD 6.7デバイスの設定には使用できません。	脆弱な暗号を使用できますが、FTD 6.7デバイスの設定には使用できません。
アップグレード：FTDは弱い暗号のみで設定	FMC 6.7 UIからのアップグレード。検証前チェックでエラーが表示されます。アップグレードは再設定されるまでブロックされます。	FTDアップグレード後、ピアがその設定を変更していないと想定すると、トンネルが終了します。
アップグレード：FTDは一部の弱い暗号と一部の強い暗号でのみ設定	FMC 6.7 UIからのアップグレード。検証前チェックでエラーが表示されます。アップグレードは再設定されるまでブロックされます。	FTDアップグレード後、ピアに強力な暗号が設定されていると仮定すると、トンネルが再確立されます。
アップグレード：クラスC国（強力な暗号ライセンスを持たない）	DESを許可する	DESを許可する

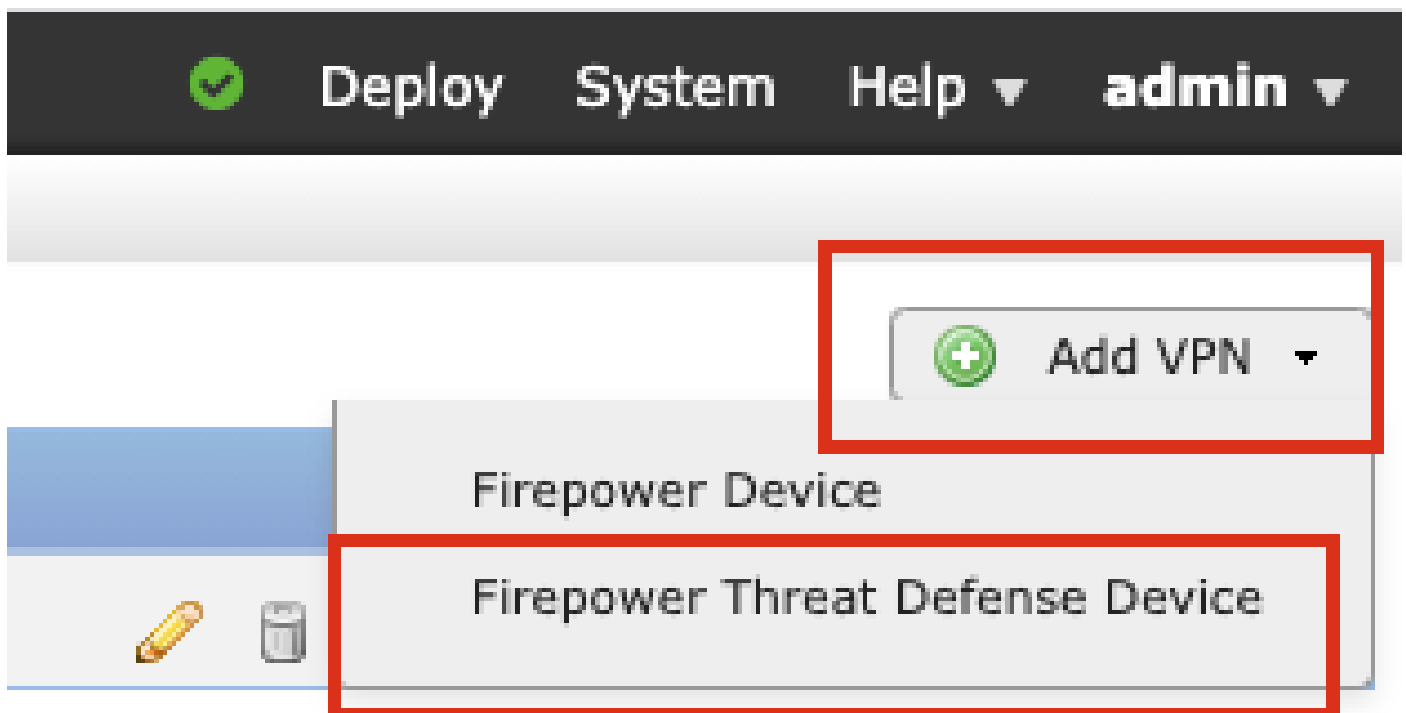
 注：追加のライセンスは必要ありません。ルートベースVPNは、ライセンスモードと評価モードで設定できます。暗号化に準拠していない場合（輸出規制機能が有効）、暗号化アルゴリズムとして使用できるのはDESだけです。

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。



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。



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では、次の操作を行います。

トポロジ名 : VTI-ASA

IKEバージョン : IKEv2

Topology Name:*

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

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。新しい仮想トンネルインターフェイス(VTI)を追加する(+アイコンをクリックする)か、既存のリストからVTIを選択できます。

Endpoints | IKE | IPsec | Advanced

Node A

Device:*

Virtual Tunnel Interface:*

Tunnel Source IP is Private [Edit VTI](#)

Connection Type:*

Tunnel IP Address :
Tunnel Source Interface :
Tunnel Source Interface IP :

Node B

Device:*

Virtual Tunnel Interface:*

Tunnel Source IP is Private [Edit VTI](#)

Connection Type:*

Tunnel IP Address :
Tunnel Source Interface :
Tunnel Source Interface IP :

ステップ 5 : 新しい仮想トンネルインターフェイス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では、次の操作を行います。

名前 : VTI-ASA

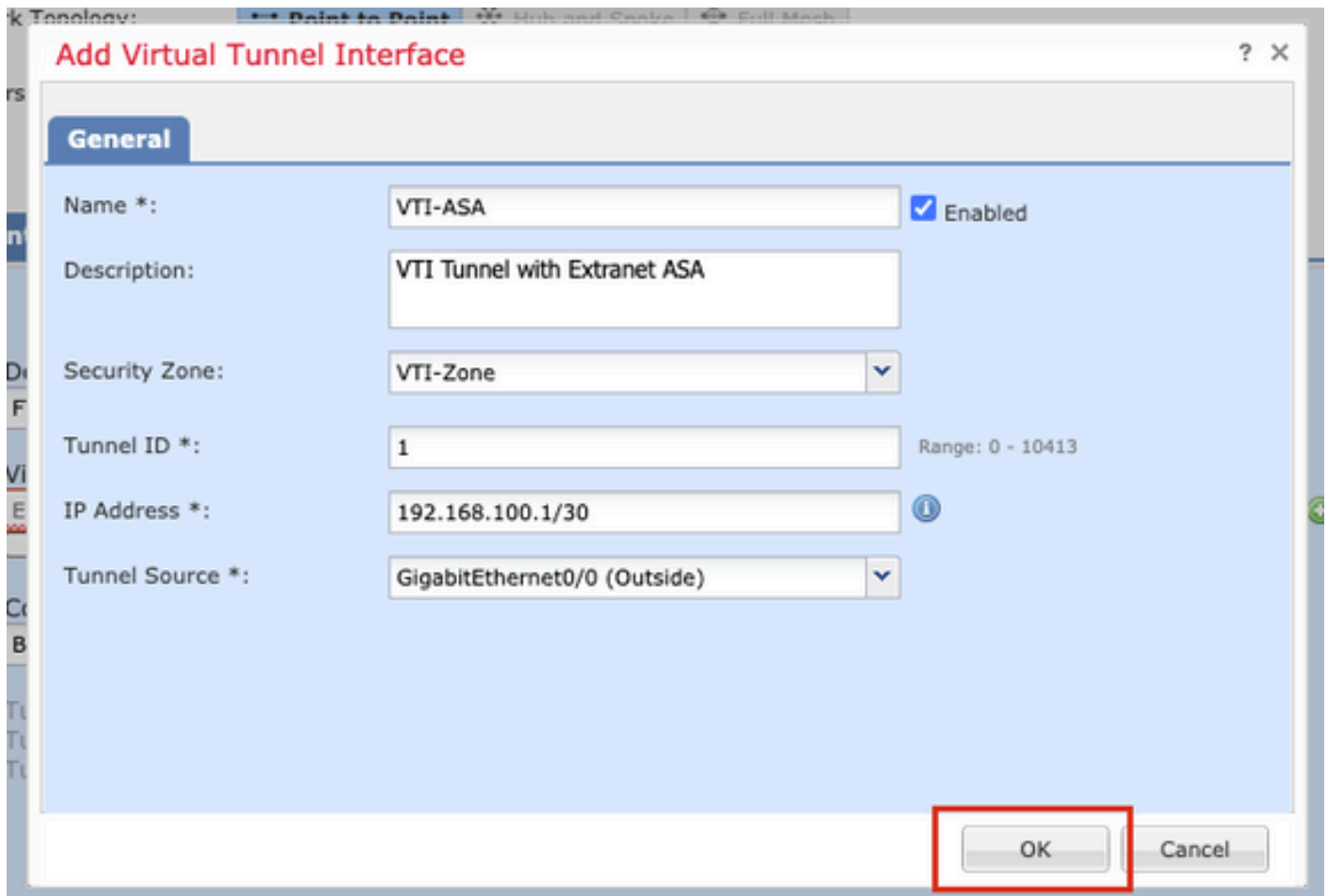
説明 (オプション) : エクストラネットASAを使用したVTIトンネル

セキュリティゾーン : VTIゾーン

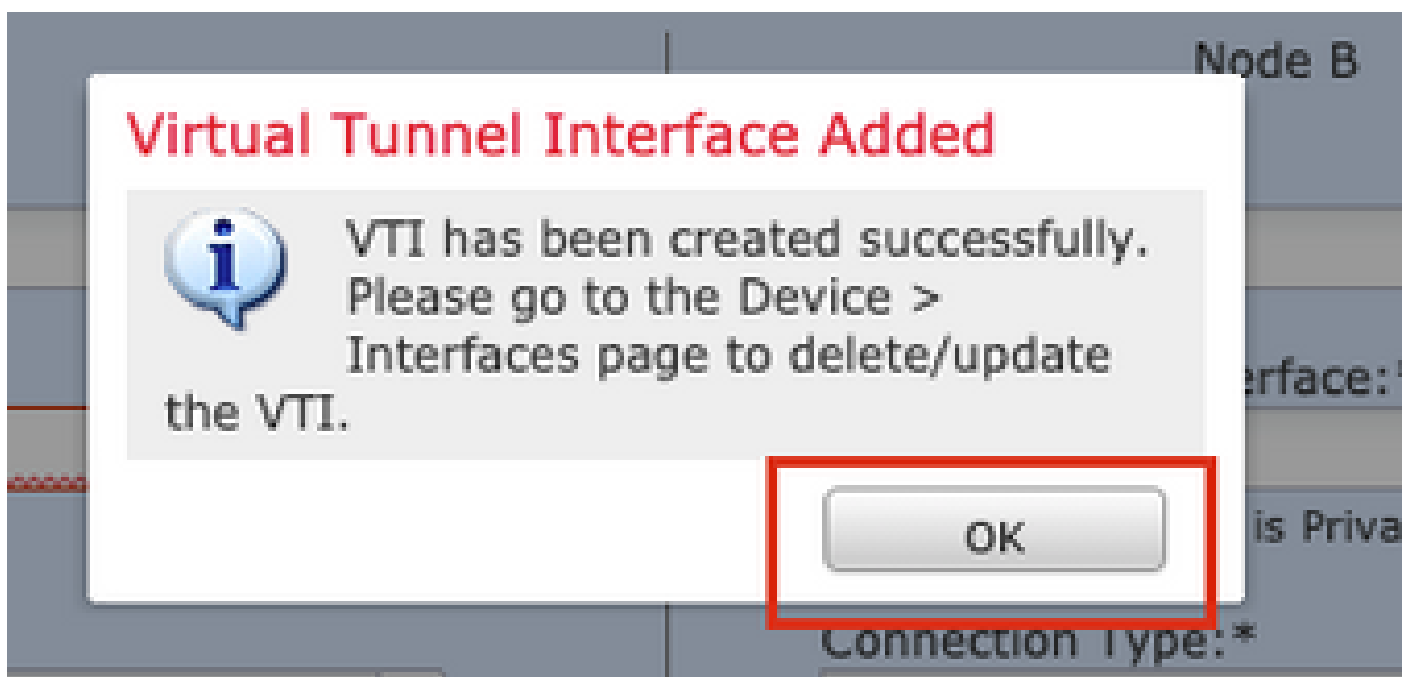
トンネルID:1

IPアドレス : 192.168.100.1/30

トンネル送信元 : GigabitEthernet0/0 (外部)



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。



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) の情報を入力します。

このデモンストレーションでは、次の操作を行います。

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 Topology

Topology Name: *

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

IKE Version: * IKEv1 IKEv2

Endpoints | IKE | IPsec | Advanced

Node A

Device: *

Virtual Tunnel Interface: * Tunnel Source IP is Private [Edit VTI](#)

Connection Type: *

Tunnel IP Address : 192.168.100.1
Tunnel Source Interface : Outside
Tunnel Source Interface IP : 10.197.224.90

Additional Configuration ⓘ
Route traffic to the VTI : [Routing Policy](#)
Permit VPN traffic : [AC Policy](#)

Node B


Device: *

Device Name: *

Endpoint IP Address: *

ステップ 8 : IKEタブに移動します。事前定義されたポリシーを使用するか、またはポリシータブの横の+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-LATEST 

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:* 24 Characters (Range 1-127)

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) ポリシーに名前を指定し、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では、次の操作を行います。

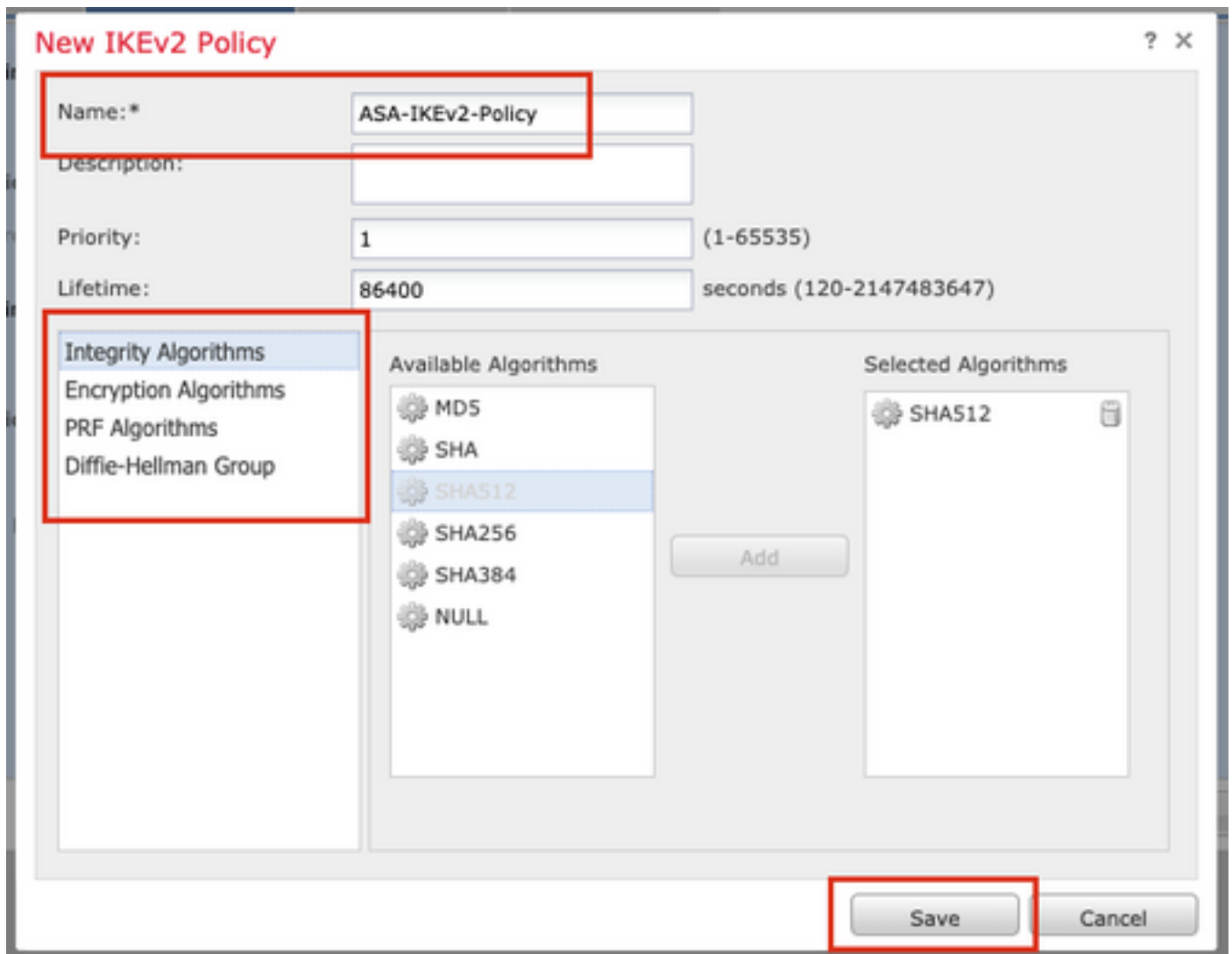
名前 : ASA-IKEv2-Policy

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



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では、次の操作を行います。

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

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:* preshared_sha_aes256_dh14_3 [v] [+]

Authentication Type: Pre-shared Automatic Key [v]

Pre-shared Key Length:* 24 Characters (Range 1-127)

IKEv2 Settings


Policy:* ASA-IKEv2-Policy [v] [+]

Authentication Type: Pre-shared Manual Key [v]

Key:* [*****]

Confirm Key:* [*****]

Enforce hex-based pre-shared key only



 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、事前共有自動キーのオプションも使用できます。

ステップ 11 IPsec タブに移動します。事前に定義された 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 Dynamic

IKEv2 Mode: Tunnel [v]

Transform Sets:

<p>IKEv1 IPsec Proposals </p> <div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;">tunnel_aes256_sha</div>	<p>IKEv2 IPsec Proposals* </p> <div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;">AES-GCM</div>
--	---

Enable Security Association (SA) Strength Enforcement

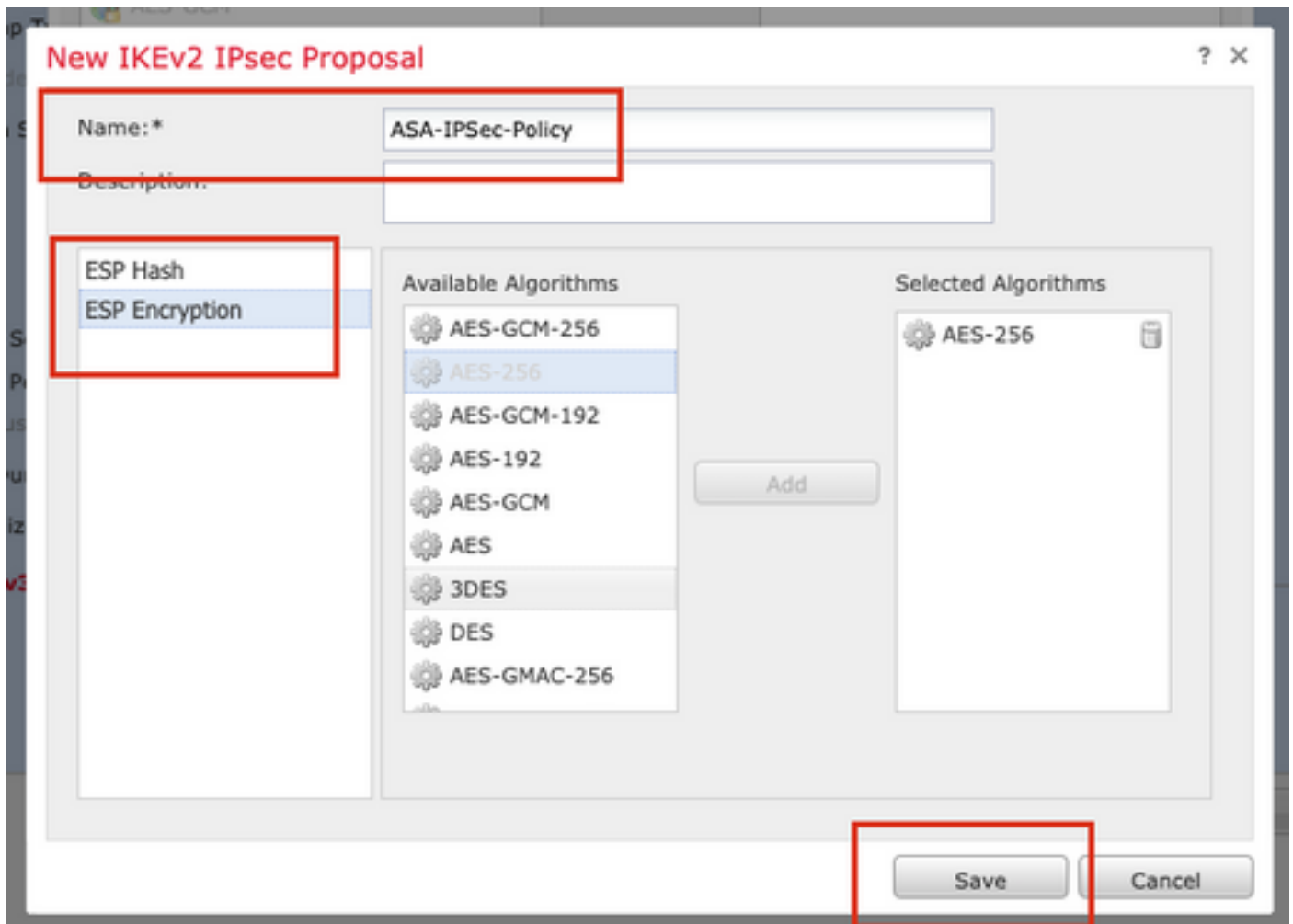
ステップ 12. (新しい IKEv2 IPsec プロポーザルを作成する場合はオプション) 提案の名前を入力し、提案で使用するアルゴリズムを選択します。[Save] をクリックします。

このデモンストレーションでは、次の操作を行います。

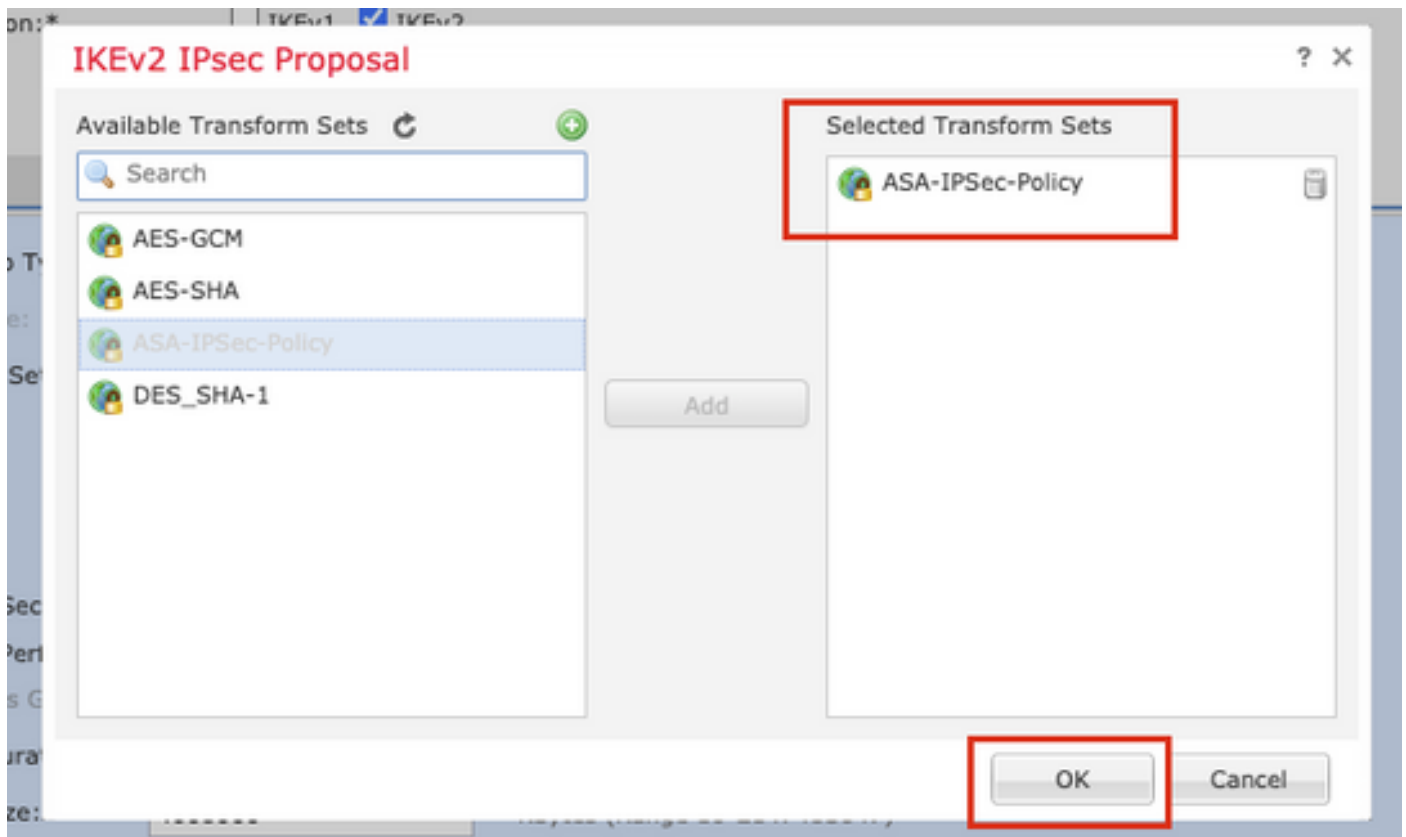
名前 : ASA-IPSec-Policy

ESPハッシュ : SHA-512

ESP暗号化 : AES-256



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。



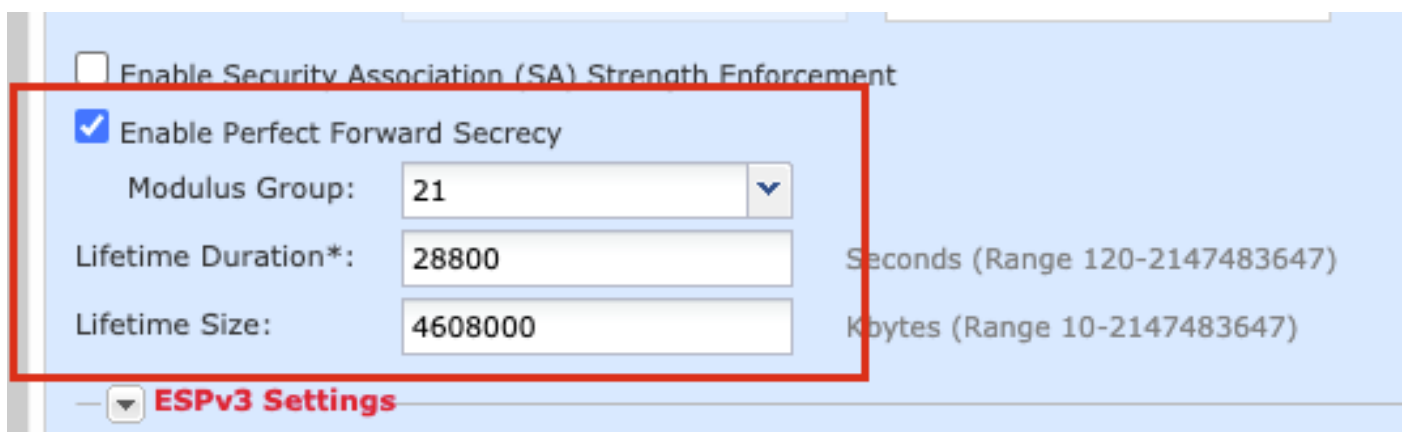
ステップ14: (オプション) Perfect Forward Secrecy設定を選択します。IPSecのライフタイム期間とライフタイムサイズを設定します。

このデモンストレーションでは、次の操作を行います。

完全転送秘密 : モジュラスグループ21

有効期間 : 28800 (既定値)

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



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:*

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

IKE Version:* IKEv1 IKEv2

Endpoints | IKE | **IPsec** | Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode:

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

Enable Security Association (SA) Strength Enforcement

Enable Perfect Forward Secrecy


Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

— **ESPv3 Settings** —

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に適用されてい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トンネルでは動作しません。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。

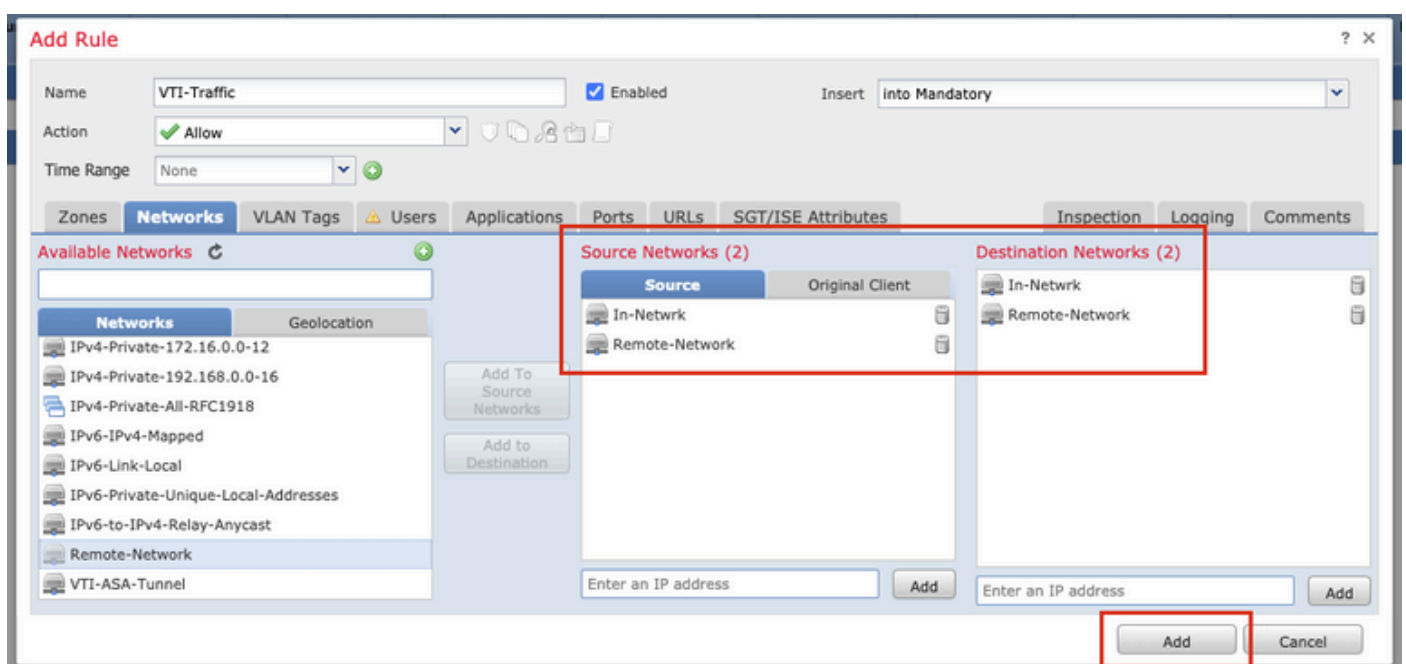
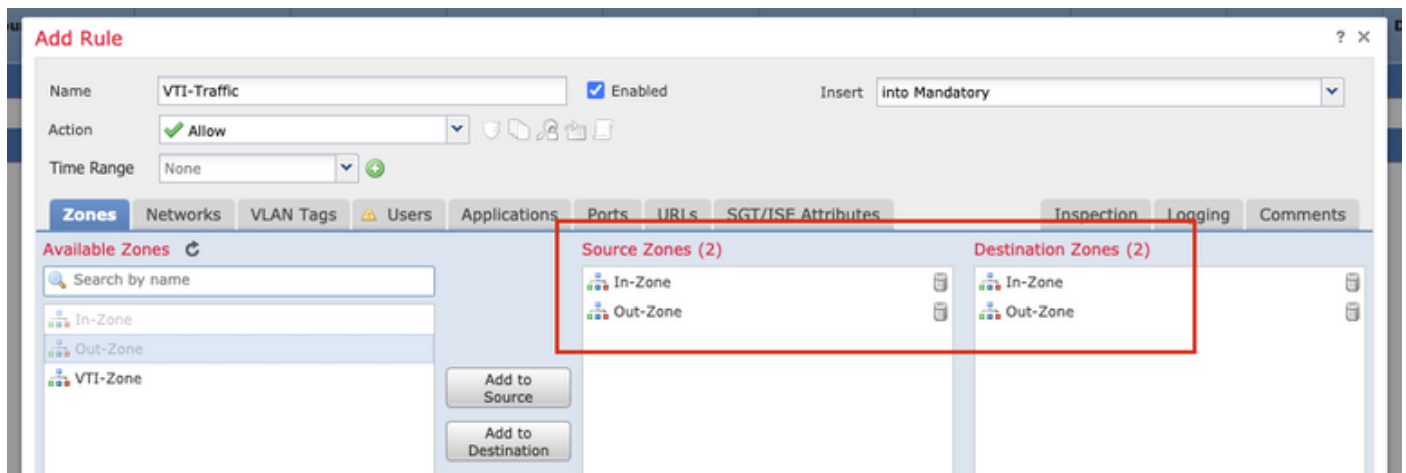
このデモンストレーションでは、次の操作を行います。

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



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。

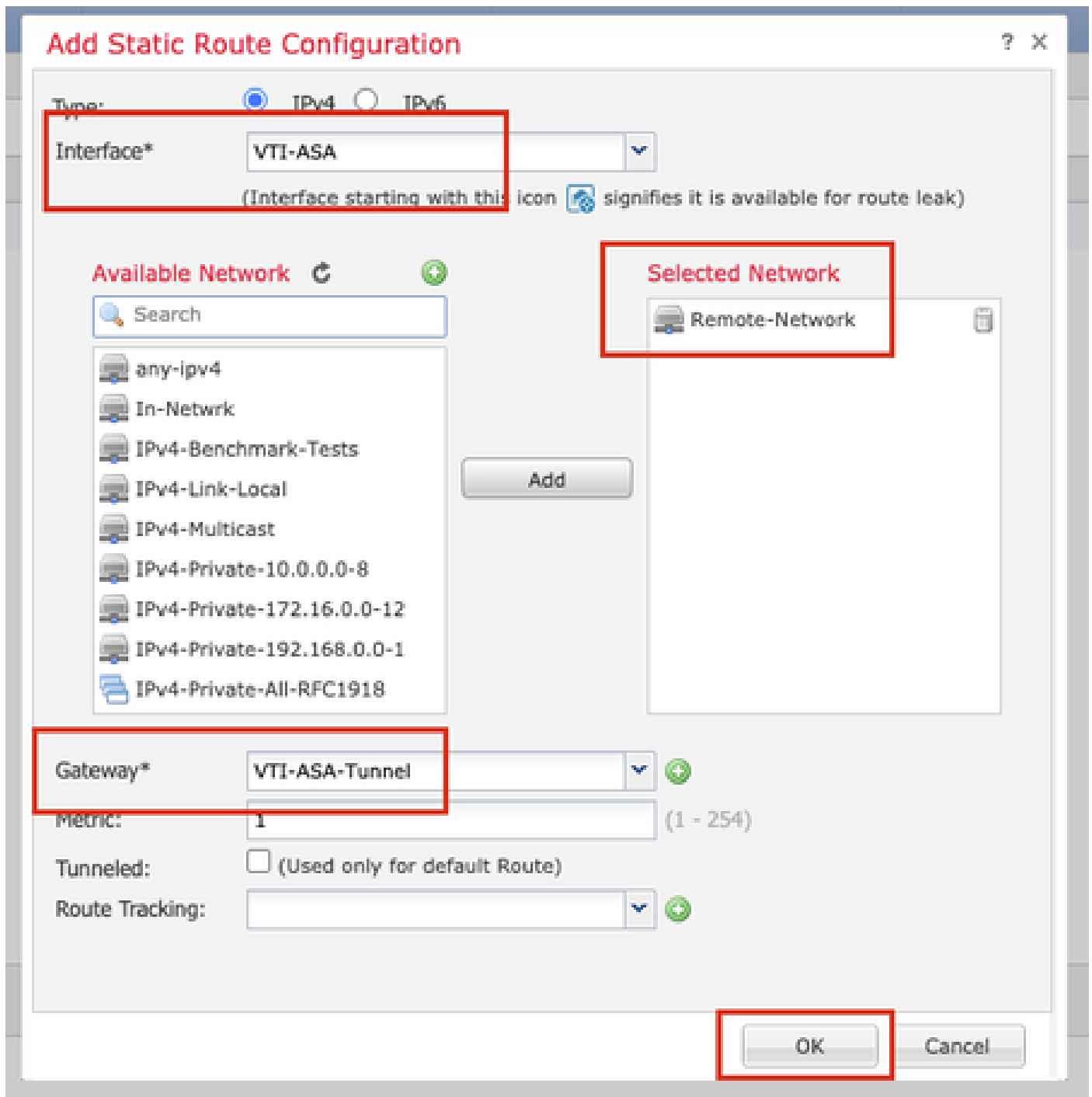
Interfaceを指定し、Networkを選択して、Gatewayを指定します。[OK] をクリックします。

このデモンストレーションでは、次の操作を行います。

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トンネル



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-l2l
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

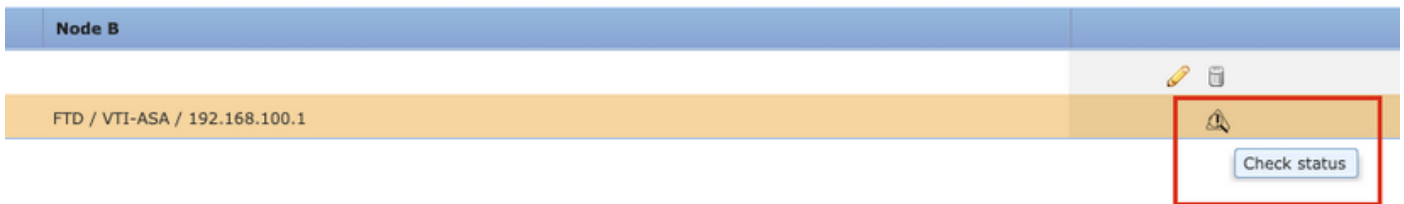
  ip address 192.168.100.1 255.255.255.252
  tunnel source interface Outside
  tunnel destination 10.106.67.252
  tunnel mode ipsec ipv4

  tunnel protection ipsec profile FMC_IPSEC_PROFILE_1
```

確認

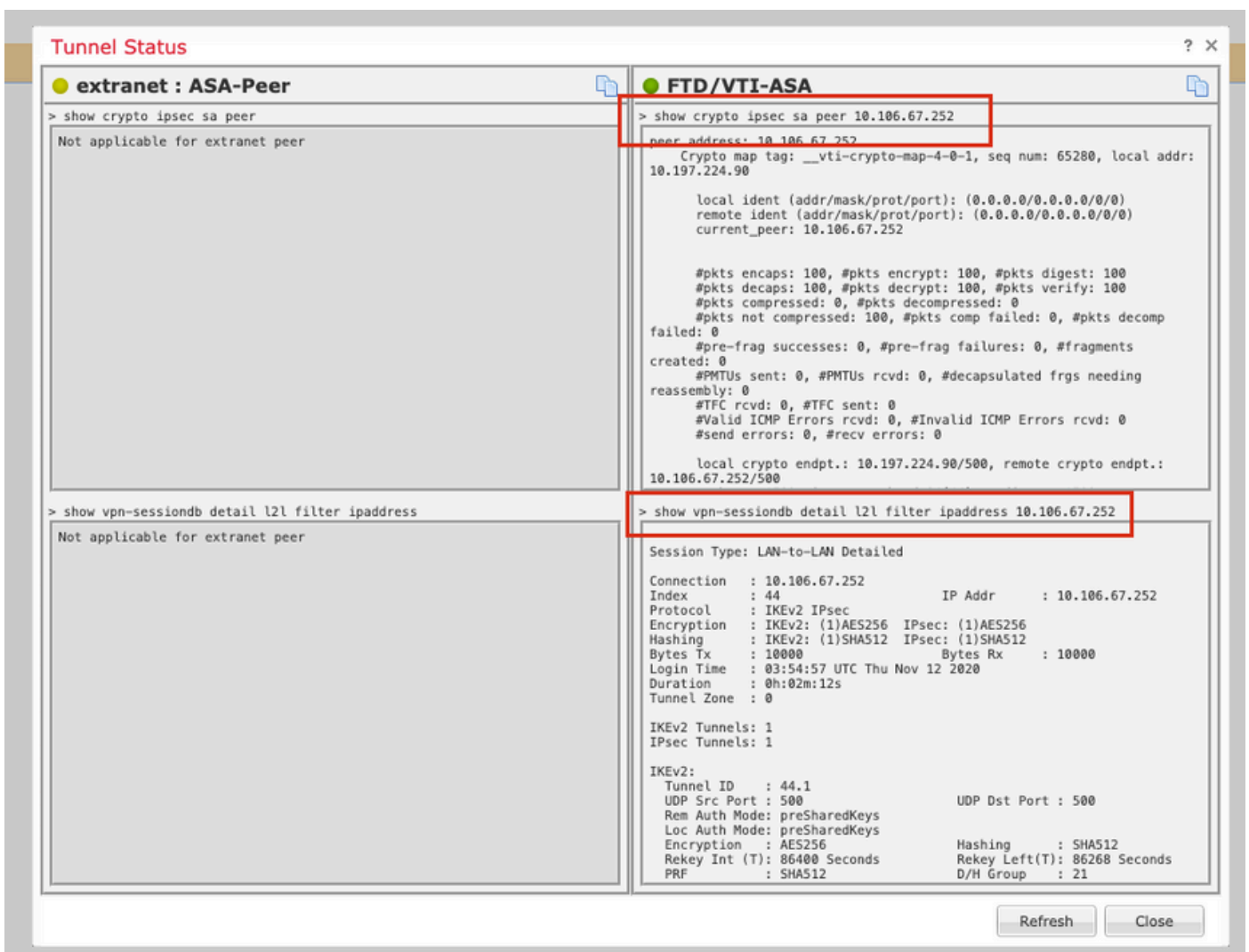
FMCのGUIから

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から取得され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 l2l filter ipaddress <ピアのIPアドレス>



FTD CLIから

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

```
show running-config crypto
show running-config nat
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。