

FMCによって管理されるFTDのサイト間VPN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](#)

[コンフィギュレーション](#)

[ステップ 1: VPNトポロジを定義します。](#)

[ステップ 2: IKEパラメータを設定します。](#)

[ステップ 3: IPSecパラメータを設定します。](#)

[ステップ 4: アクセスコントロールのバイパス。](#)

[ステップ 5: アクセスコントロールポリシーを作成します。](#)

[手順 6: NAT免除を設定します。](#)

[手順 7: ASA の設定](#)

[確認](#)

[トラブルシューティングとデバッグ](#)

[初期接続の問題](#)

[トラフィック固有の問題](#)

はじめに

このドキュメントでは、FMCによって管理されるFirepower Threat Defense(FTD)でサイト間(L2L)VPN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必要です。

- VPNの基本的な知識
- firepower Management Centerの経験
- ASAコマンドラインの経験

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco FTD 6.5

- ASA 9.10(1)32
- IKEv2

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。

コンフィギュレーション

firepower Management Centerを使用したFTDの設定から始めます。

ステップ 1 : VPNトポロジを定義します。

1. Devices > VPN > Site To Siteの順に移動します。 firepower Add VPNの下で、次の図に示すようにThreat Defense Deviceをクリックします。



2. Create New VPN Topologyボックスが表示されます。VPNに識別しやすい名前を付けます。

ネットワークトポロジ : ポイントツーポイント

IKEバージョン : IKEv2

この例では、エンドポイントを選択すると、ノードAがFTD、ノードBがASAになります。緑色のプラス記号のボタンをクリックして、次の図に示すようにトポロジにデバイスを追加します。

Create New VPN Topology ? X

Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints | IKE | IPsec | Advanced

Node A: +

Device Name	VPN Interface	Protected Networks

Node B: +

Device Name	VPN Interface	Protected Networks

i Ensure the protected networks are allowed by access control policy of each device.

3. FTDを最初のエンドポイントとして追加します。

暗号マップが配置されるインターフェイスを選択します。IPアドレスは、デバイス設定から自動的に入力されます。

Protected Networksの下にある緑色のプラス記号をクリックして、このVPNで暗号化するサブネットを選択します（次の図を参照）。

Add Endpoint



Device:*

FTD



Interface:*

outside



IP Address:*

172.16.100.20



This IP is Private

Connection Type:

Bidirectional



Certificate Map:



Protected Networks:*

Subnet / IP Address (Network) Access List (Extended)



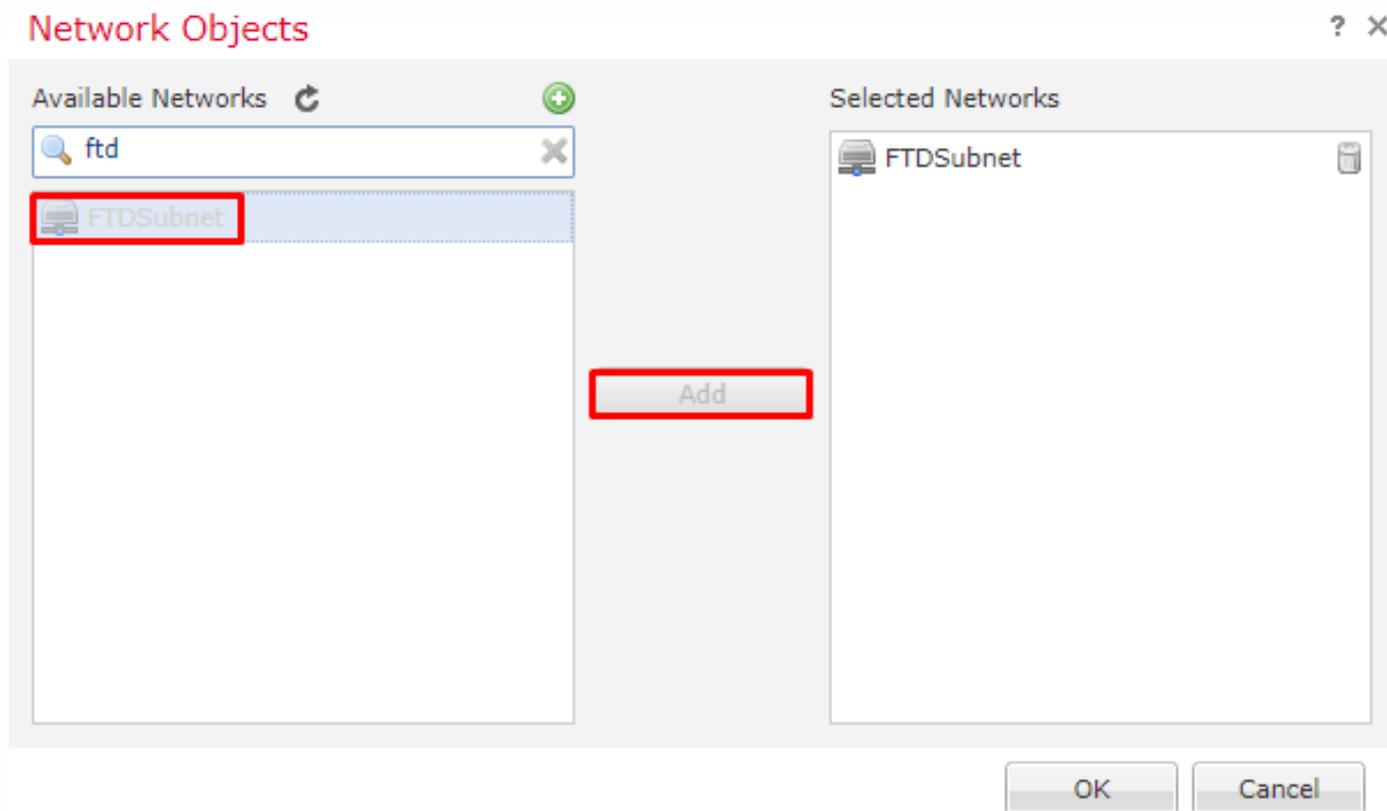
OK

Cancel

4.緑色のプラス記号をクリックすると、ここにネットワークオブジェクトが作成されます。

5.暗号化する必要があるFTDにローカルなすべてのサブネットを追加します。Addをクリックして、選択したネットワークに移動します。次の図に示すように、OKをクリックします。

FTDSubnet = 10.10.113.0/24



ノードA: (FTD)エンドポイントが完了しました。図に示すように、ノードBの緑色のプラス記号をクリックします。

Create New VPN Topology

Topology Name: RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version: IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Node A:

Device Name	VPN Interface	Protected Networks
FTD	outside/172.16.100.20	FTDSubnet

Node B:

Device Name	VPN Interface	Protected Networks
-------------	---------------	--------------------

ⓘ Ensure the protected networks are allowed by access control policy of each device.

Save Cancel

ノードBはASAです。FMCによって管理されていないデバイスは、エクストラネットとみなされます。

6. デバイス名とIPアドレスを追加します。図に示すように、緑色のプラス記号をクリックして、保護されたネットワークを追加します。

Edit Endpoint



Device:*

Device Name:*

IP Address:* Static Dynamic

Certificate Map:

Protected Networks:*
 Subnet / IP Address (Network) Access List (Extended)



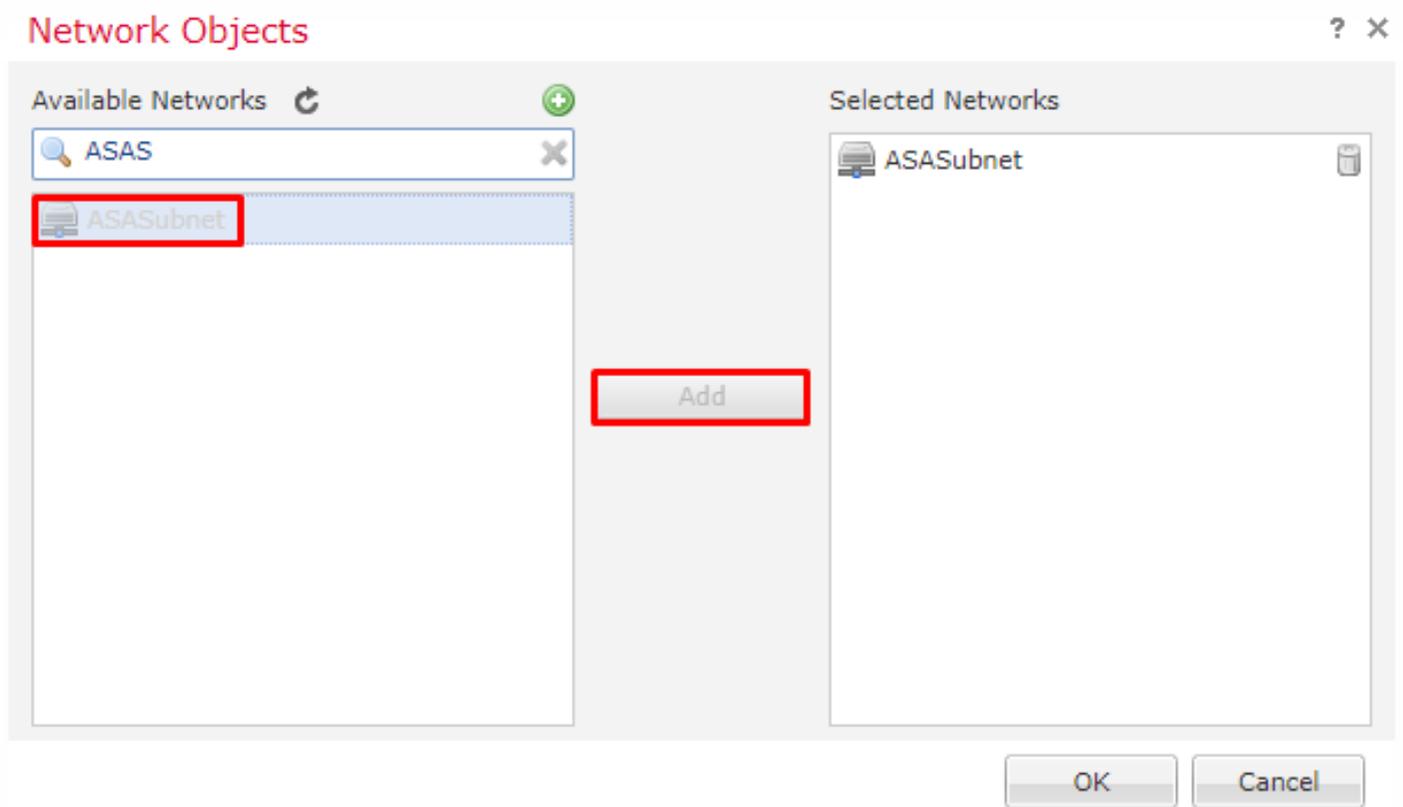
OK

Cancel

7.次の図に示すように、暗号化する必要があるASAサブネットを選択し、選択したネットワーク

に追加します。

ASASubnet = 10.10.110.0/24



ステップ 2 : IKEパラメータを設定します。

これで、両方のエンドポイントがIKE/IPSEC設定を通過します。

1. IKEタブで、IKEv2の初期交換に使用されるパラメータを指定します。図に示すように、緑色のプラス記号をクリックして新しいIKEポリシーを作成します。

Create New VPN Topology

? X

Topology Name:* RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:* preshared_sha_aes256_dh5_5

Authentication Type: Pre-shared Automatic Key

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

IKEv2 Settings

Policy:* AES-GCM-NULL-SHA

Authentication Type: Pre-shared Automatic Key

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

Save Cancel

2.新しいIKEポリシーで、接続のフェーズ1のライフタイムとプライオリティ番号を指定します。このドキュメントでは、最初の交換に次のパラメータを使用します。整合性(SHA256)、暗号化(AES-256)、PRF(SHA256)、およびDiffie-Hellmanグループ (グループ14)

 注：デバイス上のすべてのIKEポリシーは、選択したポリシーセクションの内容に関係なく、リモートピアに送信されます。リモートピアと一致する最初のIKEポリシーがVPN接続用を選択されます。プライオリティフィールドを使用して、最初に送信するポリシーを選択します。プライオリティ1が最初に送信される

New IKEv2 Policy

Name:*

Description:

Priority: (1-65535)

Lifetime: seconds (120-2147483647)

- Integrity Algorithms**
- Encryption Algorithms
- PRF Algorithms
- Diffie-Hellman Group

- Available Algorithms
- MD5
 - SHA
 - SHA512
 - SHA256**
 - SHA384
 - NULL

Add

- Selected Algorithms
- SHA256

Save Cancel

New IKEv2 Policy

Name:*

Description:

Priority: (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms

Encryption Algorithms

PRF Algorithms

Diffie-Hellman Group

Available Algorithms

- AES
- AES-256**
- DES
- 3DES
- AES-192
- AES-GCM
- AES-GCM-192
- AES-GCM-256
- NULL

Add

Selected Algorithms

- AES-256

Save Cancel

New IKEv2 Policy



Name:*

Description:

Priority: (1-65535)

Lifetime: seconds (120-2147483647)

- Integrity Algorithms
- Encryption Algorithms
- PRF Algorithms**
- Diffie-Hellman Group

- Available Algorithms
- MD5
 - SHA
 - SHA512
 - SHA256**
 - SHA384

Add

- Selected Algorithms
- SHA256

Save Cancel

New IKEv2 Policy

? X

Name:*	<input type="text" value="ASA"/>
Description:	<input type="text"/>
Priority:	<input type="text" value="1"/> (1-65535)
Lifetime:	<input type="text" value="86400"/> seconds (120-2147483647)

<p>Integrity Algorithms</p> <p>Encryption Algorithms</p> <p>PRF Algorithms</p> <p>Diffie-Hellman Group</p>	<p>Available Groups</p> <ul style="list-style-type: none">125141516192021	<p>Selected Groups</p> <ul style="list-style-type: none">14
---	--	---

3.パラメータを追加したら、このポリシーを選択し、認証タイプを選択します。

4. pre-shared-keyマニュアルを選択します。このドキュメントでは、PSK cisco123を使用します。

Create New VPN Topology ? X

Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints **IKE** IPsec Advanced

IKEv1 Settings

Policy:* +

Authentication Type:

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

IKEv2 Settings

Policy:* +

Authentication Type:

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

ステップ 3 : IPsecパラメータを設定します。

1. IPsecで、鉛筆をクリックしてトランスフォームセットを編集し、次の図に示すように新しいIPsecプロファイルを作成します。

Create New VPN Topology

? X

Topology Name:* RTPVPN-ASA

Network Topology: **Point to Point** Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints IKE **IPsec** Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals  tunnel_aes256_sha

IKEv2 IPsec Proposals*  AES-GCM

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group: 14

Lifetime Duration*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

— **ESPv3 Settings**

Save Cancel

2.新しいIKEv2 IPsecプロポーザルを作成するには、緑色のプラス記号をクリックし、フェーズ2パラメータを入力します。

ESP Encryption > AES-GCM-256の順に選択します。暗号化にGCMアルゴリズムを使用する場合、ハッシュアルゴリズムは不要です。GCMにはハッシュ関数が組み込まれています。

Edit IKEv2 IPsec Proposal



Name:* ASA

Description:

ESP Hash

ESP Encryption

Available Algorithms

- AES-GCM-256
- AES-256
- AES-GCM-192
- AES-192
- AES-GCM
- AES
- 3DES
- DES
- AES-GMAC-25

Add

Selected Algorithms

- AES-GCM-256

Save Cancel

3.新しいIPsecプロポーザルが作成されたら、それを選択したトランスフォームセットに追加します。

IKEv2 IPsec Proposal



Available Transform Sets

Search

- AES-GCM
- AES-SHA
- ASA
- DES_SHA-1

Add

Selected Transform Sets

- ASA

OK Cancel

新しく選択したIPsecプロポーザルが、IKEv2 IPsecプロポーザルの下にリストされます。

必要に応じて、ここでフェーズ2のライフタイムとPFSを編集できます。この例では、ライフタイムはデフォルトに設定され、PFSは無効になります。

Topology Name: RTPVPN-ASA

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version: IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals: tunnel_aes256_sha; IKEv2 IPsec Proposals*: ASA

Enable Security Association (SA) Strength Enforcement

Enable Reverse Route Injection

Enable Perfect Forward Secrecy

Modulus Group: 14

Lifetime Duration*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

ESPv3 Settings

Save Cancel

オプション：アクセス制御をバイパスするオプションを完了するか、アクセス制御ポリシーを作成する必要があります。

ステップ 4：アクセスコントロールのバイパス。

オプションで、sysopt permit-vpnはAdvanced > Tunnelで有効にできます。

これにより、アクセスコントロールポリシーを使用してユーザから着信するトラフィックを検査する可能性がなくなります。ユーザトラフィックのフィルタリングには、VPNフィルタまたはダウンロード可能ACLを使用できます。これはグローバルコマンドであり、このチェックボックスが有効になっている場合はすべてのVPNに適用されます。

Create New VPN Topology ? x

Topology Name:*

Network Topology: Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints IKE IPsec **Advanced**

IKE
IPsec
Tunnel

NAT Settings

Keepalive Messages Traversal
Interval: Seconds (Range 10 - 3600)

Access Control for VPN Traffic

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Certificate Map Settings

Use the certificate map configured in the Endpoints to determine the tunnel

Use the certificate OU field to determine the tunnel

Use the IKE identity to determine the tunnel

Use the peer IP address to determine the tunnel

sysopt permit-vpnがイネーブルになっていない場合は、FTDデバイス経由のVPNトラフィックを許可するようにアクセスコントロールポリシーを作成する必要があります。sysopt permit-vpnがイネーブルになっている場合、アクセスコントロールポリシーの作成をスキップします。

ステップ 5 : アクセスコントロールポリシーを作成します。

Access Control Policiesの下で、Policies > Access Control > Access Controlの順に移動し、FTDデバイスを対象とするポリシーを選択します。ルールを追加するには、次の図に示すように、Add Ruleをクリックします。

トラフィックは、内部ネットワークから外部ネットワークへ、および外部ネットワークから内部ネットワークへ許可される必要があります。両方を実行するルールを1つ作成するか、別々に保持するルールを2つ作成します。この例では、両方を実行する1つのルールが作成されます。

Editing Rule - VPN_Traffic

Name: VPN_Traffic Enabled Move

Action: Allow

Zones: Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Available Networks: subnet

Source Networks (2): ASASubnet, FTDSubnet

Destination Networks (2): ASASubnet, FTDSubnet

Buttons: Add To Source Networks, Add to Destination, Save, Cancel

Rules Security Intelligence HTTP Responses Logging Advanced

Filter by Device Show Rule Conflicts Add Category Add Rule Search Rules

Name	Source Zon...	Dest Zones	Source Networks	Dest Networks	VL...	Us...	Ap...	So...	De...	URLs	So...	De...	A...
1 VPN_Traffic	Inside Outside	Inside Outside	ASASubnet FTDSubnet	ASASubnet FTDSubnet	Any	Any	Any	Any	Any	Any	Any	Any	Allow

Default Action: Access Control: Block All Traffic

手順 6 : NAT免除を設定します。

VPNトラフィックのNAT免除ステートメントを設定します。VPNトラフィックが別のNATステートメントにヒットしてVPNトラフィックが誤って変換されるのを防ぐために、NAT免除を設定する必要があります。

1. Devices > NATの順に移動し、FTDを対象とするNATポリシーを選択します。Add Ruleボタンをクリックすると、新しいルールが作成されます。

Overview Analysis Policies **NAT** VPN QoS Platform Settings FlexConfig Certificates

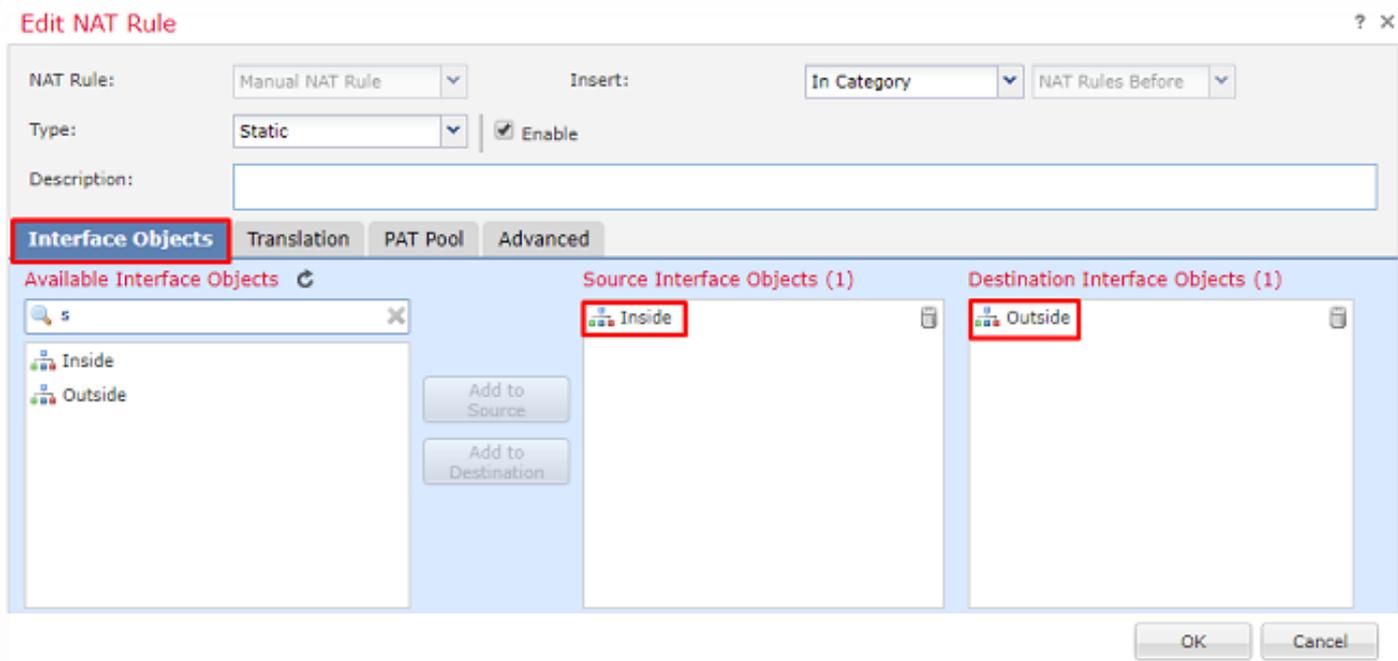
VirtualFTDNAT

Rules

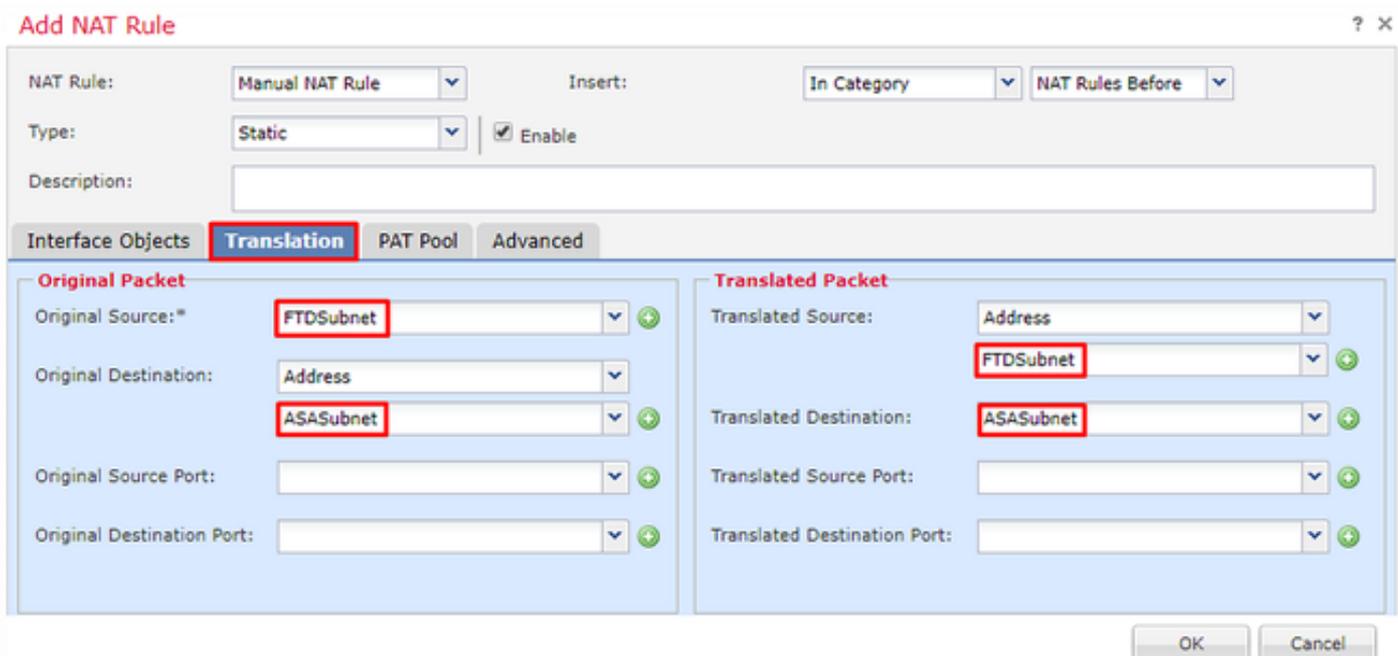
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
NAT Rules Before											
Auto NAT Rules											

Buttons: Add Rule

2.新しいスタティック手動NATルールを作成します。内部インターフェイスと外部インターフェイスを参照します。



3. Translationタブで、送信元サブネットと宛先サブネットを選択します。これはNAT免除ルールであるため、次の図に示すように、元の送信元/宛先と変換後の送信元/宛先を同じにします。



4.最後に、Advancedタブに移動し、no-proxy-arpとroute-lookupを有効にしました。

Add NAT Rule ? X

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Fallthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Unidirectional

5.このルールを保存し、NATリストの最終結果を確認します。

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates Show Warnings Save Cancel

VirtualFTDNAT
Enter Description Policy Assignments

Rules Filter by Device Add Rule

#	Direction	Type	Source Interface...	Destination Interface...	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
▼ NAT Rules Before											
1	↔	Static	Inside	Outside	FTDSubnet	ASASubnet		FTDSubnet	ASASubnet		Dns:fail route-ik no-pro
▼ Auto NAT Rules											
#	↔	Dynamic	Inside	Outside	any-obj			Interface			Dns:fail
▼ NAT Rules After											

6.設定が完了したら、設定を保存してFTDに展開します。

手順 7 : ASA の設定.

1. ASAの外部インターフェイスでIKEv2を有効にします。

```
Crypto ikev2 enable outside
```

2. FTDで設定されているのと同じパラメータを定義するIKEv2ポリシーを作成します。

```
Crypto ikev2 policy 1
```

```
Encryption aes-256
Integrity sha256
Group 14
Prf sha256
Lifetime seconds 86400
```

3. ikev2プロトコルを許可するグループポリシーを作成します。

```
Group-policy FTD_GP internal
Group-policy FTD_GP attributes
Vpn-tunnel-protocol ikev2
```

4. ピアFTDパブリックIPアドレスのトンネルグループを作成します。グループポリシーを参照し、事前共有キーを指定します。

```
Tunnel-group 172.16.100.20 type ipsec-l2l
Tunnel-group 172.16.100.20 general-attributes
Default-group-policy FTD_GP
Tunnel-group 172.16.100.20 ipsec-attributes
ikev2 local-authentication pre-shared-key cisco123
ikev2 remote-authentication pre-shared-key cisco123
```

5. 暗号化するトラフィックを定義するアクセスリストを作成します(FTDSubnet 10.10.113.0/24)(ASASubnet 10.10.110.0/24)。

```
Object network FTDSUBNET
Subnet 10.10.113.0 255.255.255.0
Object network ASASUBNET
Subnet 10.10.110.0 255.255.255.0
Access-list ASAToFTD extended permit ip object ASASUBNET object FTDSUBNET
```

6. FTDで指定されたアルゴリズムを参照するikev2 ipsec-proposalを作成します。

```
Crypto ipsec ikev2 ipsec-proposal FTD
Protocol esp encryption aes-gcm-256
```

7. 設定を結び付けるクリプトマップエントリを作成します。

```
Crypto map outside_map 10 set peer 172.16.100.20
```

```
Crypto map outside_map 10 match address ASAtoFTD
Crypto map outside_map 10 set ikev2 ipsec-proposal FTD
Crypto map outside_map 10 interface outside
```

8. VPNトラフィックがファイアウォールによってNATされることを防止するNAT免除ステートメントを作成します。

```
Nat (inside,outside) 1 source static ASASubnet ASASubnet destination static FTDSubnet FTDSubnet no-
```

確認

 注：現時点では、FMCからVPNトンネルのステータスを確認する方法はありません。この機能 [CSCvh77603](#) に対する拡張要求があります。

VPNトンネル経由でトラフィックを開始してみます。ASAまたはFTDのコマンドラインにアクセスするには、packet tracerコマンドを使用します。packet-tracerコマンドを使用してVPNトンネルを起動する場合は、トンネルが起動することを確認するために2回実行する必要があります。このコマンドを初めて発行したときにVPNトンネルがダウンしているため、packet-tracerコマンドはVPN encrypt DROPで失敗します。ファイアウォールの内部IPアドレスをパケットトレーサの送信元IPアドレスとして使用しないでください。使用すると常に失敗します。

```
firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10
```

```
Phase: 10
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:
```

```
firepower# packet-tracer input inside icmp 10.10.113.10 8 0 10.10.110.10
```

```
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 172.16.100.1 using egress ifc outside
```

```
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (Inside,outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet no-proxy-
Additional Information:
```

```
NAT divert to egress interface outside
Untranslate 10.10.110.10/0 to 10.10.110.10/0
```

Phase: 3

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced permit ip ifc Inside object-group FMC_INLINE_src_rule_268436483 ifc ou
```

```
access-list CSM_FW_ACL_ remark rule-id 268436483: ACCESS POLICY: FTD-Access-Control-Policy - Mandatory
```

```
access-list CSM_FW_ACL_ remark rule-id 268436483: L7 RULE: VPN_Traffic
```

```
object-group network FMC_INLINE_src_rule_268436483
```

```
description: Auto Generated by FMC from src of UnifiedNGFWRule# 1 (FTD-Access-Control-Policy/mandatory)
```

```
network-object object ASASubnet
```

```
network-object object FTDSubnet
```

```
object-group network FMC_INLINE_dst_rule_268436483
```

```
description: Auto Generated by FMC from dst of UnifiedNGFWRule# 1 (FTD-Access-Control-Policy/mandatory)
```

```
network-object object ASASubnet
```

```
network-object object FTDSubnet
```

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: NAT

Subtype:

Result: ALLOW

Config:

```
nat (Inside,outside) source static FTDSubnet FTDSubnet destination static ASASubnet ASASubnet no-proxy-
```

Additional Information:

```
Static translate 10.10.113.10/0 to 10.10.113.10/0
```

Phase: 10

Type: VPN

Subtype: encrypt

Result: ALLOW

Config:

Additional Information:

Result:

```
input-interface: Inside
```

```
input-status: up
```

```
input-line-status: up
```

```
output-interface: outside
```

```
output-status: up
```

```
output-line-status: up
```

```
Action: allow
```

トンネルステータスを監視するには、FTDまたはASAのCLIに移動します。

FTD CLIから、次のコマンドを使用してphase-1とphase-2を確認します。

```
Show crypto ikev2 sa
```

```
<#root>
```

```
> show crypto ikev2 sa
```

IKEv2 SAs:

Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote
	9528731 172.16.100.20/500	192.168.200.10/500

READY

INITIATOR

Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/118 sec

Child sa: local selector

10.10.113.0/0 - 10.10.113.255/65535

remote selector

10.10.110.0/0 - 10.10.110.255/65535

ESP spi in/out:

0x66be357d/0xb74c8753

トラブルシューティングとデバッグ

初期接続の問題

VPNを構築する際、トンネルをネゴシエートしている2つの側があります。したがって、あらゆるタイプのトンネル障害をトラブルシューティングする場合は、会話の両側を取得するのが最善です。IKEv2トンネルのデバッグ方法の詳細については、『[IKEv2 VPNのデバッグ方法](#)』を参照してください。

トンネル障害の最も一般的な原因は、接続の問題です。これを判断する最善の方法は、デバイスでパケットキャプチャを取得することです。デバイスでパケットキャプチャを取得するには、次のコマンドを使用します。

```
Capture capout interface outside match ip host 172.16.100.20 host 192.168.200.10
```

キャプチャが実行されたら、VPN経由でトラフィックを送信し、パケットキャプチャに双方向トラフィックが含まれていないかを確認します。

次のコマンドを使用して、パケットキャプチャを確認します。

```
show cap capout
```

```
firepower# show cap capout
```

4 packets captured

```
1: 11:51:12.059628      172.16.100.20.500 > 192.168.200.10.500:  udp 690
2: 11:51:12.065243      192.168.200.10.500 > 172.16.100.20.500:  udp 619
3: 11:51:12.066692      172.16.100.20.500 > 192.168.200.10.500:  udp 288
4: 11:51:12.069835      192.168.200.10.500 > 172.16.100.20.500:  udp 240
```

トラフィック固有の問題

発生する一般的なトラフィックの問題は次のとおりです。

- FTDのルーティングの問題：内部ネットワークが、割り当てられたIPアドレスとVPNクライアントにパケットをルーティングして戻すことができません。
- トラフィックをブロックするアクセスコントロールリスト。
- Network Address Translation (NAT ; ネットワークアドレス変換) がVPNトラフィックにバイパスされていない。

FMCによって管理されるFTDのVPNの詳細については、次のURLで完全なコンフィギュレーションガイドを参照してください。[FMCによって管理されるFTDコンフィギュレーションガイド](#)

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。