

FDMによって管理されるFTDのスタティックルートを使用したルートベースのVPN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](#)

[FDMでの構成手順](#)

[確認](#)

[関連情報](#)

はじめに

このドキュメントでは、FDMによって管理される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。
- Firepower Device Manager(FDM)を使用したナビゲーションに関する予備知識。

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。

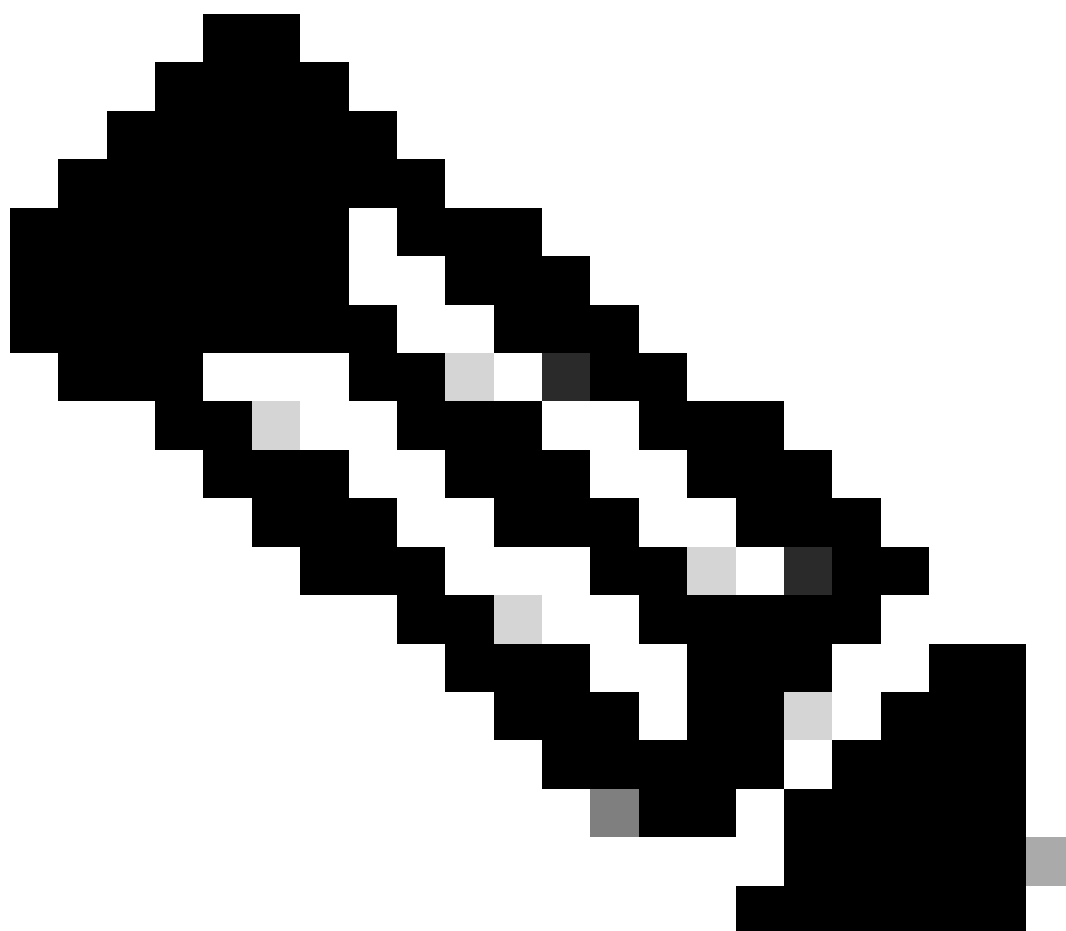
- Firepower Device Manager(FDM)で管理されるCisco Firepower Threat Defense(FTD)バージョン7.0。

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、VPNトンネルを介して暗号化または送信され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します。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トは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。

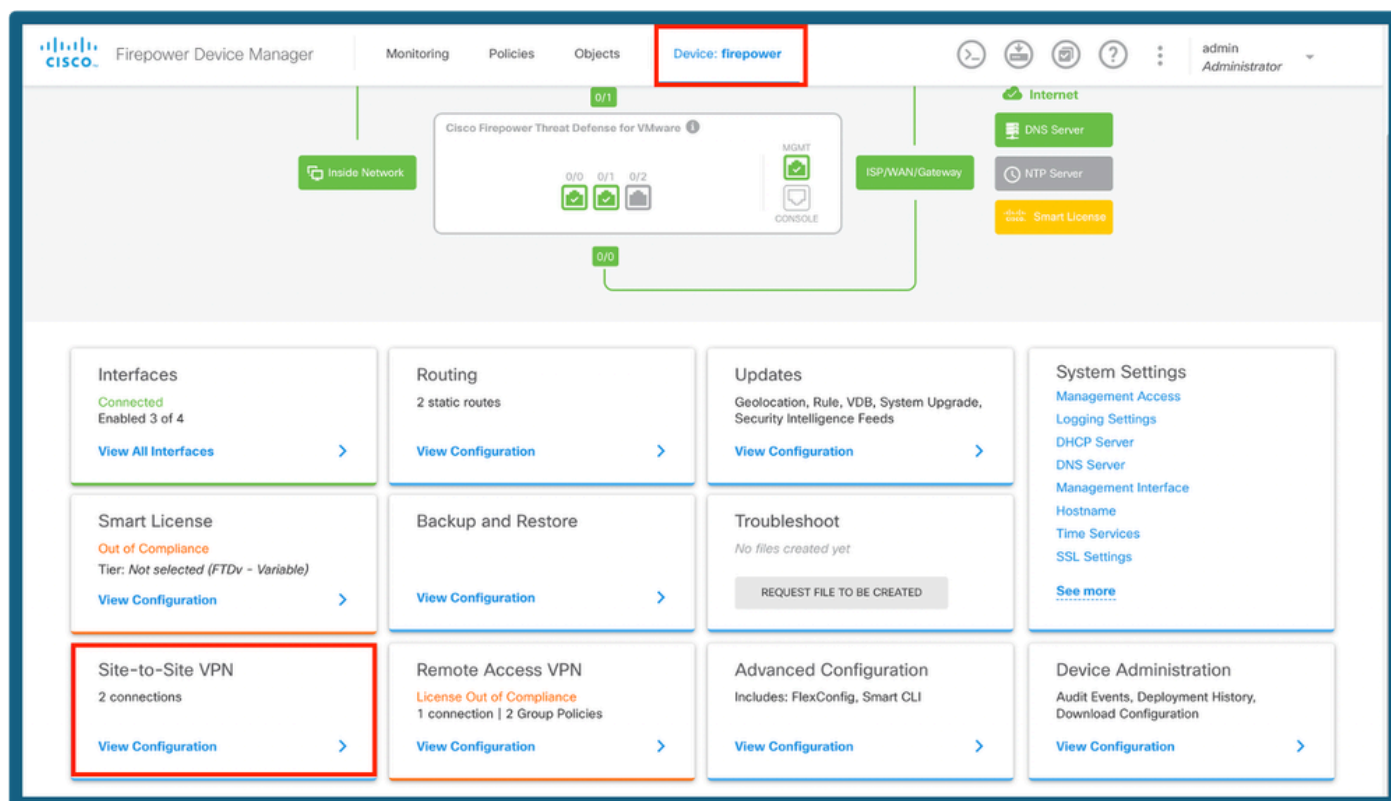
このドキュメントでは、スタティック仮想トンネルインターフェイス(SVTI)の設定を中心に説明します。



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

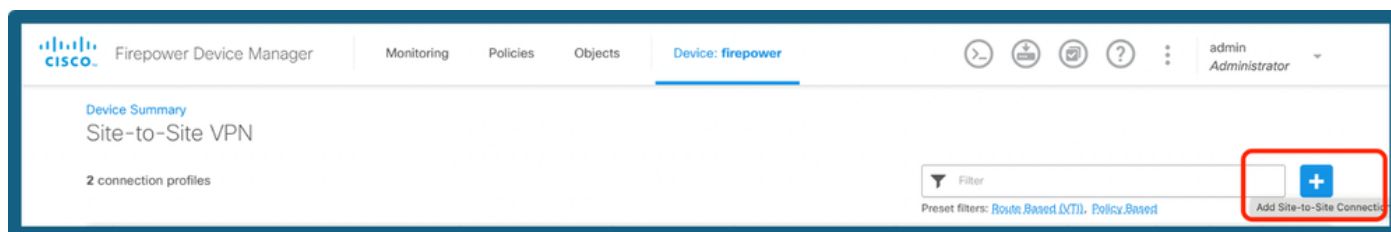
FDMでの構成手順

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



FDMダッシュボード

ステップ 2 : +アイコンをクリックして、新しいサイト間接続を追加します。



S2S接続の追加

ステップ3: トポロジ名を指定し、ルートベース(VTI)としてVPNのタイプを選択します。

Local VPN Access InterfaceをクリックしてからCreate new Virtual Tunnel Interfaceをクリックするか、既存のリストから1つ選択します。

Firepower Device Manager | Monitoring | Policies | Objects | Device: firepower | admin Administrator

Local Network | FIREPOWER | VPN TUNNEL | INTERNET | OUTSIDE INTERFACE | PEER ENDPOINT | Remote Network

Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name
vdi-ipsec

Type
Route Based (VTI) | Policy Based

Sites Configuration

LOCAL SITE
Local VPN Access Interface
Please select
Filter
Nothing found
[Create new Virtual Tunnel Interface](#)

REMOTE SITE
Remote IP Address
NEXT

トンネルインターフェイスの追加

ステップ 4 : 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。

Create Virtual Tunnel Interface

?

×

Name

tunnel10

Status

Most features work with named interfaces only, although some require unnamed interfaces.

Description

Tunnel ID

i

10

0 - 10413

Tunnel Source

i

outside (GigabitEthernet0/0)

IP Address and Subnet Mask

192.168.1.1

/

255.255.255.252

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

CANCEL

OK

VTIの設定

ステップ 5 : 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。リモートIPアドレスを指定します。

New Site-to-site VPN

1 Endpoints 2 Configuration 3 Summary

Local Network FIREPOWER VPN TUNNEL INTERNET OUTSIDE INTERFACE PEER ENDPOINT Remote Network

Define Endpoints

Identify the interface on this device, and the remote peer's interface IP address, that form the point-to-point VPN connection. Then, identify the local and remote networks that can use the connection. Traffic between these networks is protected using IPsec encryption.

Connection Profile Name:

Type: ☒ Route Based (VTI) ☐ Policy Based

Sites Configuration

LOCAL SITE

Local VPN Access Interface:

REMOTE SITE

Remote IP Address:

ピアIPの追加

手順 6 : IKE Versionを選択し、Editボタンを選択して、図に示すようにIKEおよびIPSecパラメータを設定します。

IKE Policy

i IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE Policies are available to all VPN connections.

IKE VERSION 2 ☒ **IKE VERSION 1** ☐

IKE Policy

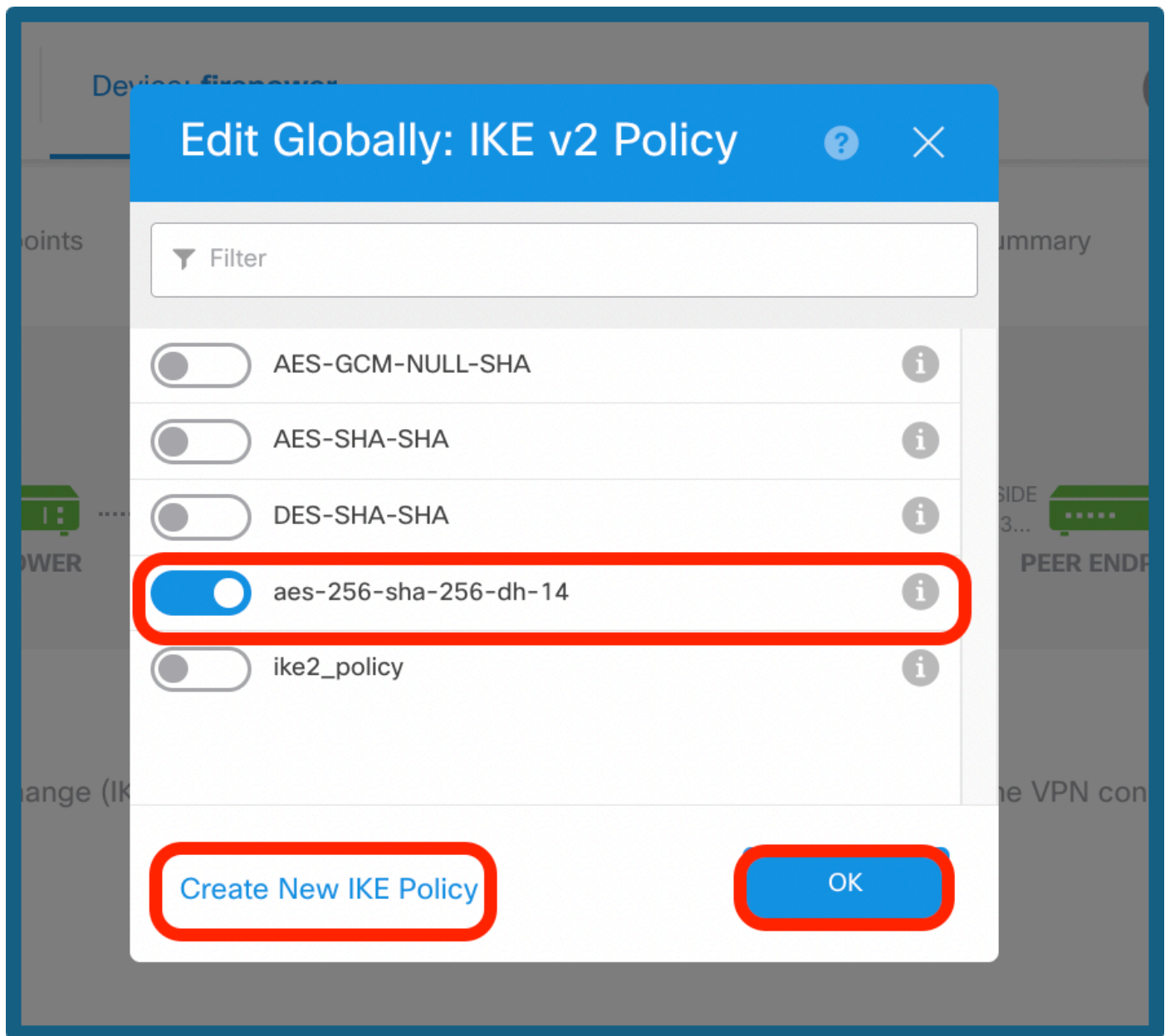
Globally applied

IPSec Proposal

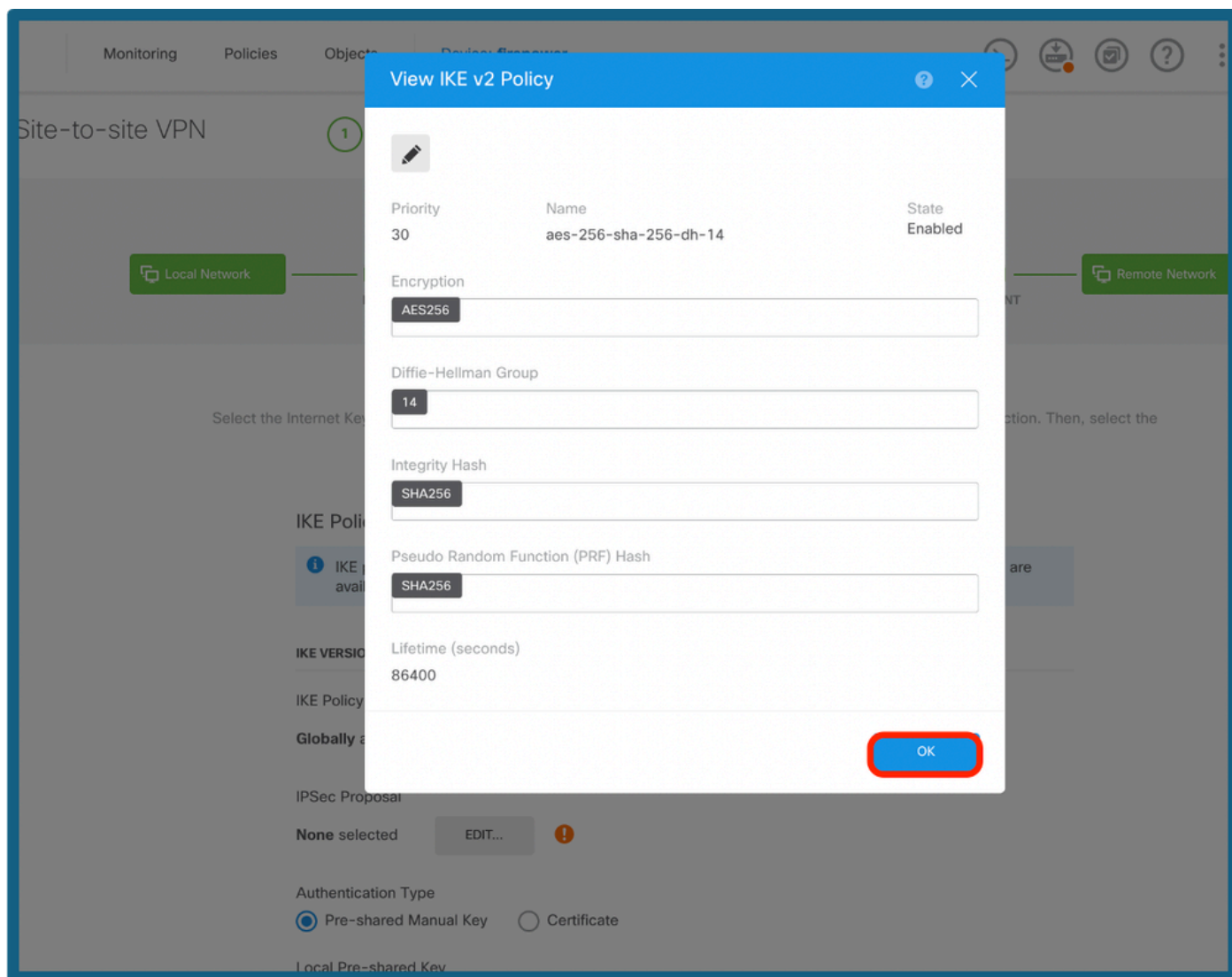
Custom set selected

IKEバージョンの設定

ステップ7a:図に示すようにIKE Policyボタンを選択し、新しいポリシーを作成する場合はokボタンまたはCreate New IKE Policyをクリックします。

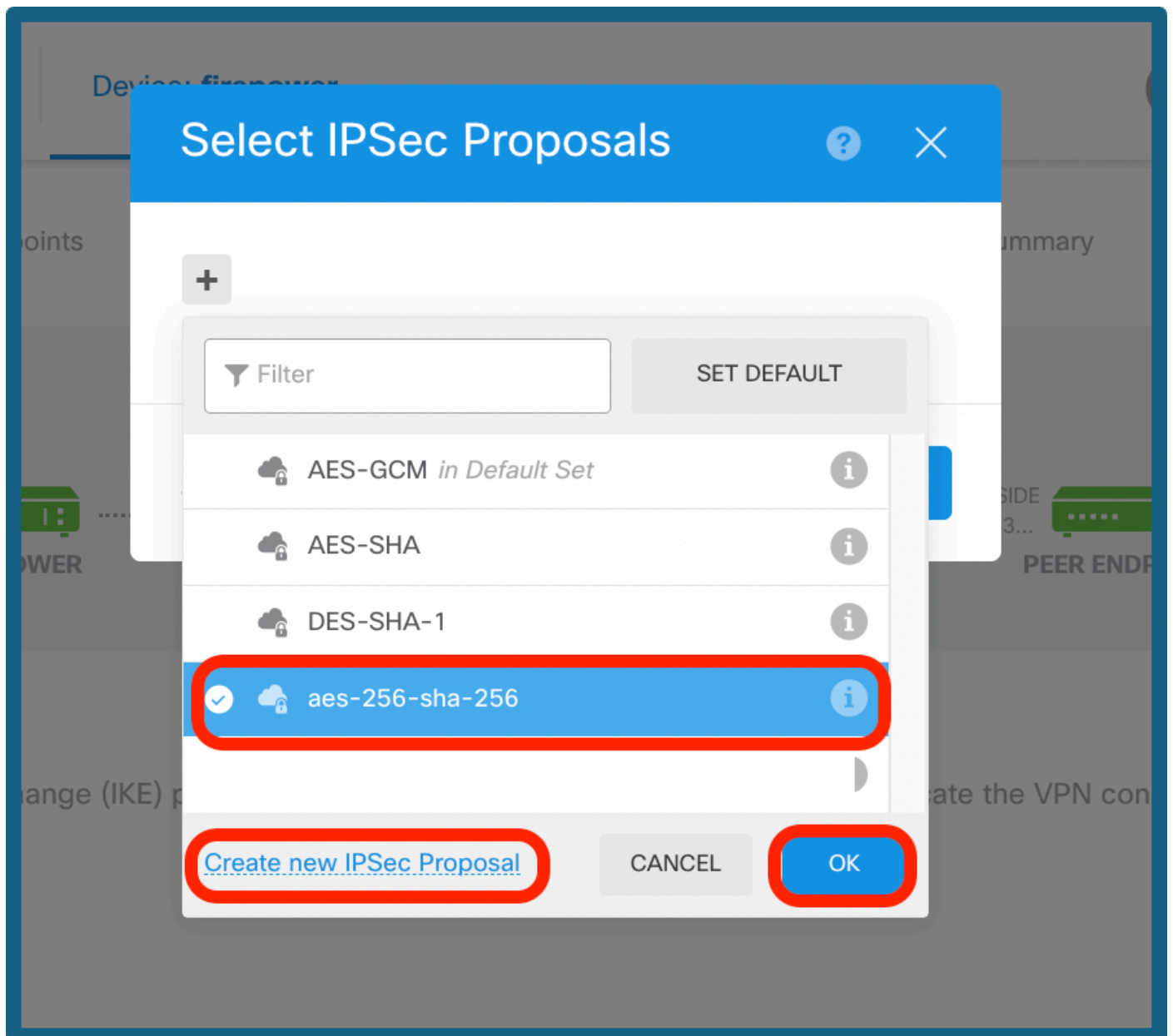


IKEポリシーの選択



IKEポリシーの設定

ステップ7b:図に示すようにIPSec Policyボタンを選択し、新しいプロポーザルを作成する場合はokボタンまたはCreate New IPSsec Proposalをクリックします。



IPSecプロポーザルの選択

IKE v2 IPSec Proposal

Name
aes-256-sha-256

Encryption
AES256

Integrity Hash
SHA256

OK

IPSecプロポーザルの設定

ステップ8a: Authentication Typeを選択します。事前共有手動キーを使用する場合は、ローカルおよびリモート事前共有キーを指定します。

ステップ8b: (オプション) Perfect Forward Secrecy設定を選択します。IPsec Lifetime DurationとLifetime Sizeを設定し、nextをクリックします。

IKE VERSION 2 ☒

IKE VERSION 1 ☐

IKE Policy

Globally applied

EDIT...

IPSec Proposal

Custom set selected

EDIT...

Authentication Type

☒ Pre-shared Manual Key ☐ Certificate

Local Pre-shared Key

●●●●●●●●

Remote Peer Pre-shared Key

●●●●●●●●

IPSEC SETTINGS

Lifetime Duration

28800

seconds

120 - 2147483647; (Default: 28800)

Lifetime Size

4608000

kilobytes

10 - 2147483647; (Default: 4608000).
Leave empty for Unlimited.

Additional Options

Diffie-Hellman Group for Perfect Forward Secrecy

No Perfect Forward Secrecy (turned off)

BACK

NEXT

PSKおよびライフタイム設定

ステップ 9 : 設定を確認し、Finishをクリックします。

Summary

Review your configuration. Click Finish to save the connection, or Back to edit settings. When you click Finish, this information will be copied to the clipboard so that you can save it and use it to configure the remote endpoint.

Vti-Ipsec Connection Profile

 Peer endpoint needs to be configured according to specified below configuration.

**VPN Access
Interface IP**  tunnel10 (1.1.1.1)



Peer IP Address 10.106.63.23

IKE V2

IKE Policy aes-256-sha256-sha256-14

IPSec Proposal aes-256-sha-256

**Authentication
Type** Pre-shared Manual Key

IKE V1: DISABLED

IPSEC SETTINGS

**Lifetime
Duration** 28800 seconds

Lifetime Size 4608000 kilobytes

ADDITIONAL OPTIONS

**Diffie-Hellman
Group** Null (not selected)

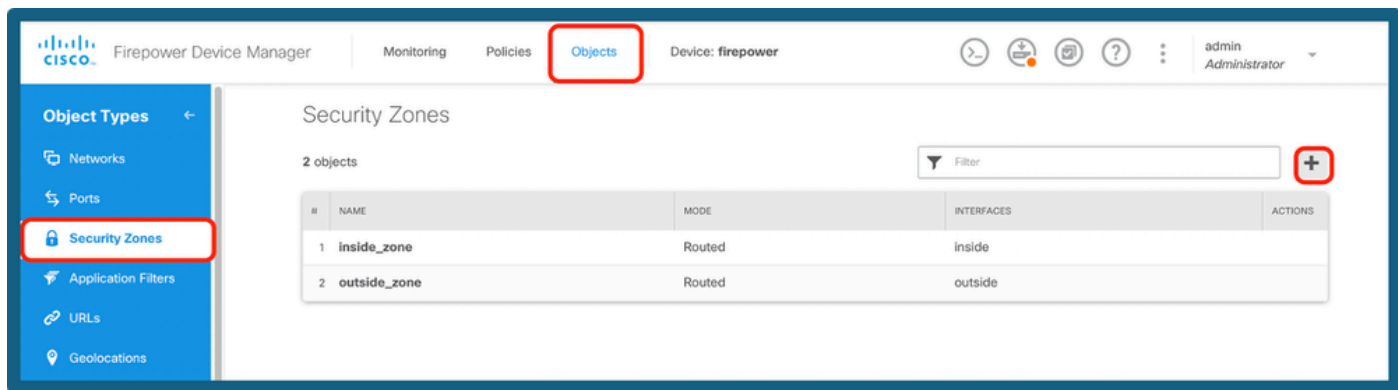
 Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

BACK

FINISH

設定の概要

ステップ10a: Objects > Security Zonesの順に移動し、+アイコンをクリックします。



セキュリティゾーンの追加

ステップ10b:ゾーンを作成し、次に示すようにVTIインターフェイスを選択します。

Add Security Zone

Name

vti-zone

Description

Mode

☒ Routed ☐ Passive

Interfaces

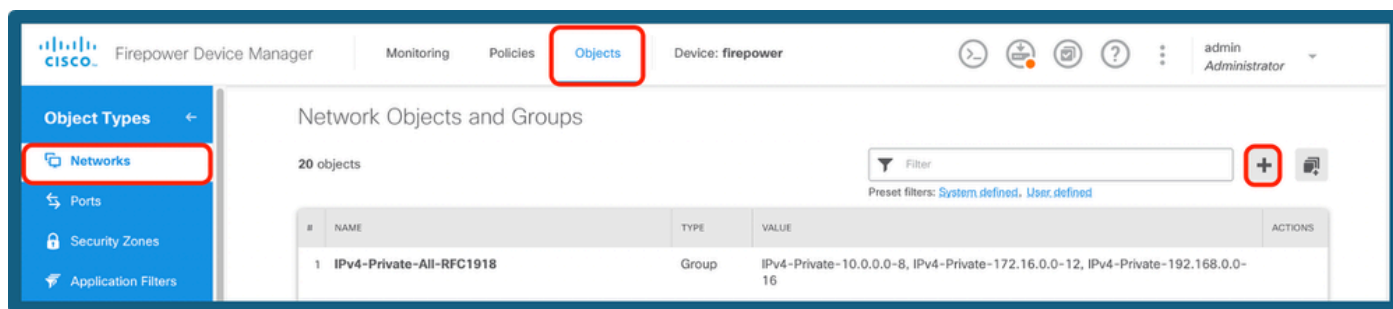
+

0 tunnel10 (Tunnel10)

CANCEL OK

セキュリティゾーンの構成

ステップ11a:Objects > Networksの順に移動し、+アイコンをクリックします。



ネットワーク オブジェクトの追加

ステップ11b:hostオブジェクトを追加し、ピアエンドのトンネルIPを持つゲートウェイを作成します。

The screenshot shows the 'Edit Network Object' dialog box. The 'Name' field is highlighted with a red box and contains 'vpn-gateway'. The 'Description' field is empty. The 'Type' section has three radio buttons: 'Network', 'Host' (selected and highlighted with a red box), and 'FQDN'. The 'Range' radio button is also present. The 'Host' field is highlighted with a red box and contains '192.168.1.2'. Below the 'Host' field, there is a hint: 'e.g. 192.168.2.1 or 2001:DB8::0DB8:800:200C:417A'. At the bottom right, there are 'CANCEL' and 'OK' buttons, with the 'OK' button highlighted with a red box.

VPNゲートウェイの設定

ステップ11c: リモートサブネットとローカルサブネットを追加します。

Edit Network Object

?

×

Name

remote-vpn-network

Description

Type

☒ Network

☐ Host

☐ FQDN

☐ Range

Network

172.16.10.0/24

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

リモートIP設定

Edit Network Object

?

×

Name

inside-network

Description

Type

☒ Network

☐ Host

☐ FQDN

☐ Range

Network

10.10.10.0/24

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

ローカルIP設定

ステップ 12Device > Policiesに移動し、アクセスコントロールポリシーを設定します。

Add Access Rule

Order: 1 | Title: vti-acl | Action: Allow

SOURCE

Zones	Networks	Ports	SGT Groups
inside_zone	inside-network	ANY	ANY
vti-zone	remote-vpn-...		

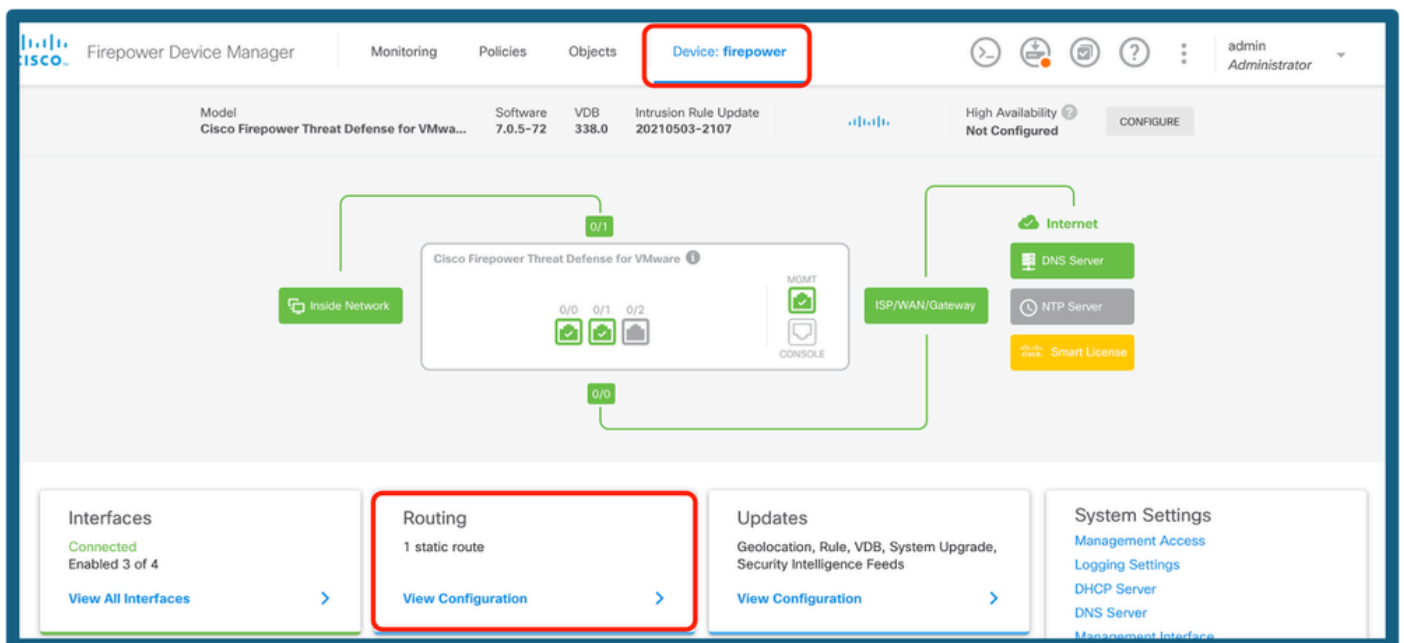
DESTINATION

Zones	Networks	Ports	SGT Groups
inside_zone	inside-network	ANY	ANY
vti-zone	remote-vpn-...		

Show Diagram: ☐ | CANCEL | OK

アクセスコントロールポリシーの追加

ステップ13a:VTIトンネルを介したルーティングを追加します。Device > Routingの順に移動します。



工順の選択

ステップ13b:Routingタブの下にあるStatic Routeに移動します。+アイコンをクリックします。

Device Summary

Routing

Add Multiple Virtual Routers

Static Routing BGP OSPF EIGRP ECMP Traffic Zones

1 route

Filter

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	default	outside	IPv4	0.0.0.0/0	10.106.52.1		1	

ルートの追加

ステップ13c: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。

Add Static Route

Name

vti-route

Description

Interface

tunnel10 (Tunnel10)

Protocol

☒ IPv4

☐ IPv6

Networks

+

remote-vpn-network

Gateway

vpn-gateway

Metric

1

SLA Monitor

Applicable only for IPv4 Protocol type

Please select an SLA Monitor

CANCEL

OK

スタティックルートの設定

ステップ 14 : Deployに移動します。変更内容を確認し、Deploy Nowをクリックします。

Pending Changes

✓

Last Deployment Completed Successfully

26 Jun 2025 05:27 PM. [See Deployment History](#)

Deployed Version (26 Jun 2025 05:27 PM)

Pending Version

LEGEND

+

Static Route Added: *vti-route*

-

-

-

iface:

-

gateway:

-

networks:

-

metricValue: 1

ipType: IPv4

name: vti-route

tunnel10

vpn-gateway

remote-vpn-network

+

Access Rule Added: *vti-acl*

-

-

-

-

sourceZones:

-

-

destinationZones:

-

-

sourceNetworks:

-

-

destinationNetworks:

logFiles: false

eventLogAction: LOG_NONE

ruleId: 268435458

name: vti-acl

vti-zone

inside_zone

vti-zone

inside_zone

remote-vpn-network

inside-network

MORE ACTIONS

CANCEL

DEPLOY NOW

構成の展開

確認

導入が完了したら、次のコマンドを使用してCLIでトンネルステータスを確認できます。

- show crypto ikev2 sa
- show crypto ipsec sa <ピアIP>

```
> show crypto ikev2 sa
```

```
IKEv2 SAs:
```

```
Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

Tunnel-id	Local	Remote	Status	Role
3294213359	10.106.52.222/500	10.106.63.23/500	READY	INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK				
Life/Active Time: 86400/141 sec				
Child sa:	local selector 0.0.0.0/0 - 255.255.255.255/65535			
	remote selector 0.0.0.0/0 - 255.255.255.255/65535			
	ESP spi in/out: 0x26a14554/0xd5db88bc			

```
> show crypto ipsec sa
```

```
interface: tunnel10
```

```
Crypto map tag: __vti-crypto-map-5-0-10, seq num: 65280, local addr: 10.106.52.222
```

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)  
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)  
current_peer: 10.106.63.23
```

show コマンド

関連情報

FDMによって管理されるFTDのサイト間VPNの詳細については、次のサイトで完全な構成ガイドを参照してください。

[FDMで管理されるFTDの構成ガイド](#)

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。