

在FDM管理的FTD上使用靜態路由配置基於路由的VPN

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[FDM的配置步驟](#)

[驗證](#)

[相關資訊](#)

簡介

本檔案介紹如何在FDM管理的FTD上設定靜態路由型站對站VPN通道。

必要條件

需求

思科建議您瞭解以下主題：

- 對VPN隧道工作方式有基礎認識。
- 預先瞭解通過Firepower裝置管理器(FDM)的導航。

採用元件

本檔案中的資訊是根據以下軟體版本：

- 由Firepower裝置管理器(FDM)管理的Cisco Firepower威脅防禦(FTD)版本7.0。

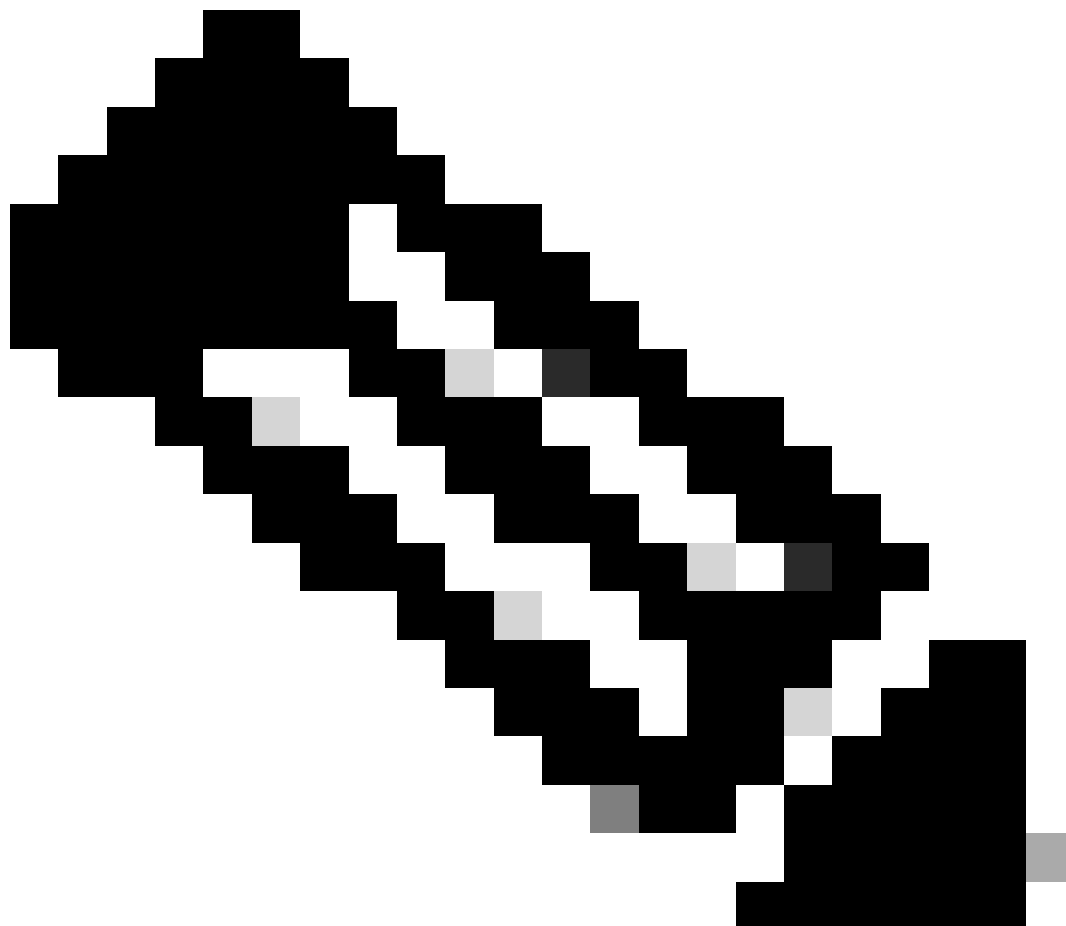
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

基於路由的VPN允許確定要加密或通過VPN隧道傳送的相關流量，並且使用流量路由而不是策略/訪問清單（如基於策略或基於加密對映的VPN中所示）。加密域設定為允許任何進入IPsec隧道的流量。IPsec本地和遠端流量選擇器設定為0.0.0.0/0.0.0.0。這意味著路由到IPsec隧道的所有流量都會被

加密，無論源/目標子網如何。

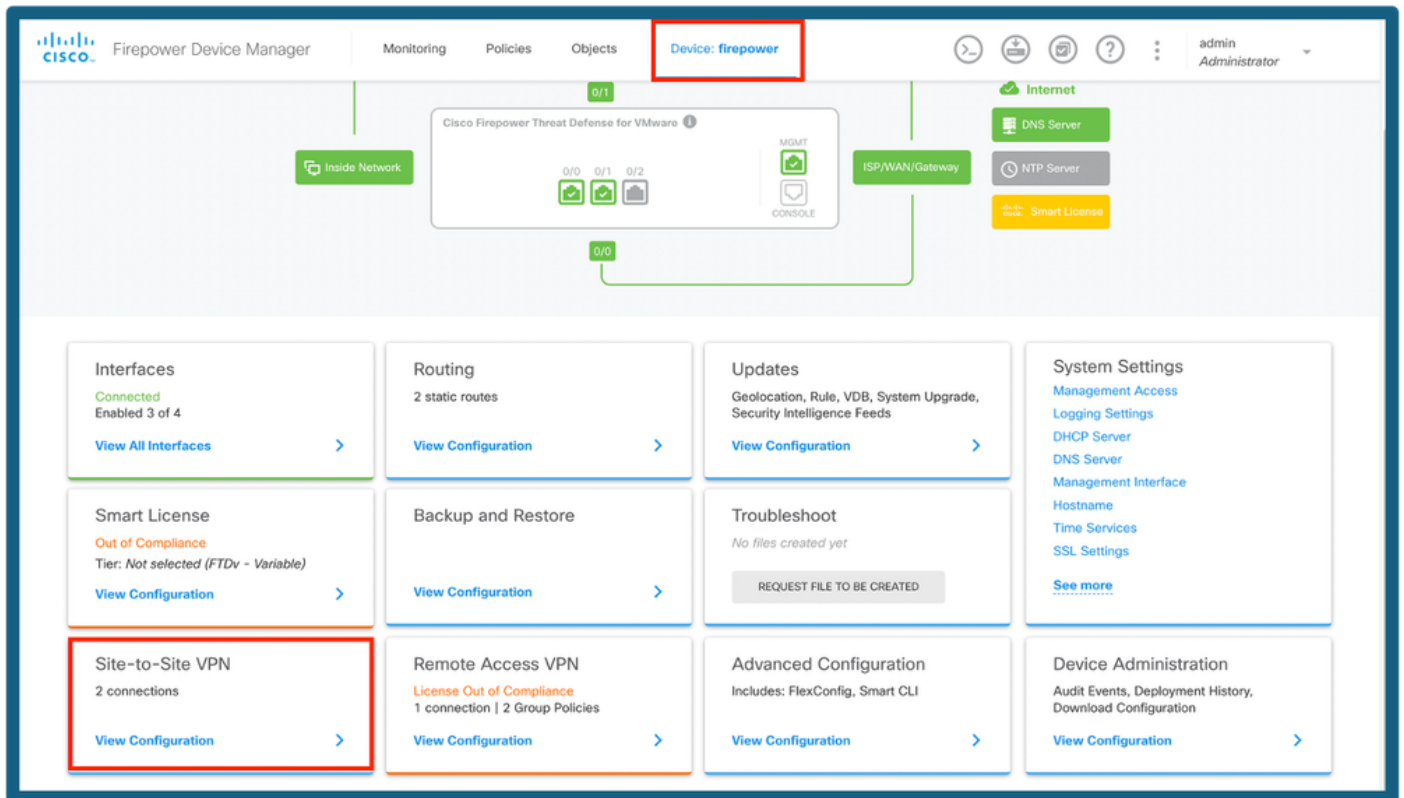
本檔案將重點介紹靜態虛擬通道介面(SVTI)組態。



附註：不需要其他許可，可以在許可模式和評估模式下配置基於路由的VPN。如果沒有加密合規（已啟用匯出控制功能），只有DES可用作加密演算法。

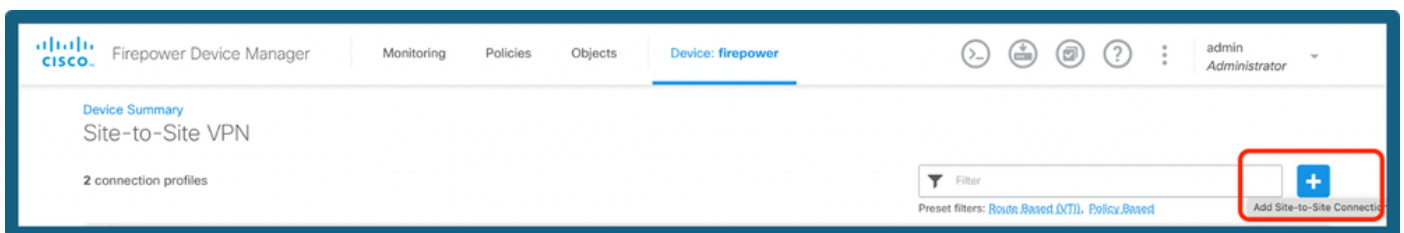
FDM的配置步驟

步驟1。導覽至Device > Site To Site。



FDM儀表板

步驟2. 按一下+圖示將新站點新增到站點連線。



新增S2S連線

步驟3. 提供拓撲名稱並選擇VPN的型別作為基於路由(VTI)。

按一下Local VPN Access Interface，然後按一下Create new Virtual Tunnel Interface或從現有清單中選擇一個。

Firepower Device Manager

Monitoring Policies Objects **Device: firepower**

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: **vti-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

新增隧道介面

步驟4.定義新虛擬通道介面的引數。按一下「OK」（確定）。

Create Virtual Tunnel Interface

Name

tunnel10

Status

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

Description

Tunnel ID

10

Tunnel Source

outside (GigabitEthernet0/0)

0 - 10413

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配置

步驟5.選擇新建立的VTI或虛擬通道介面下存在的VTI。提供遠端IP地址。

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	REMOTE SITE
Local VPN Access Interface tunnel10 (Tunnel10)	Remote IP Address 10.106.63.23

新增對等IP

步驟6.選擇IKE版本，然後選擇Edit按鈕以設定IKE和IPsec引數，如下圖所示。

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

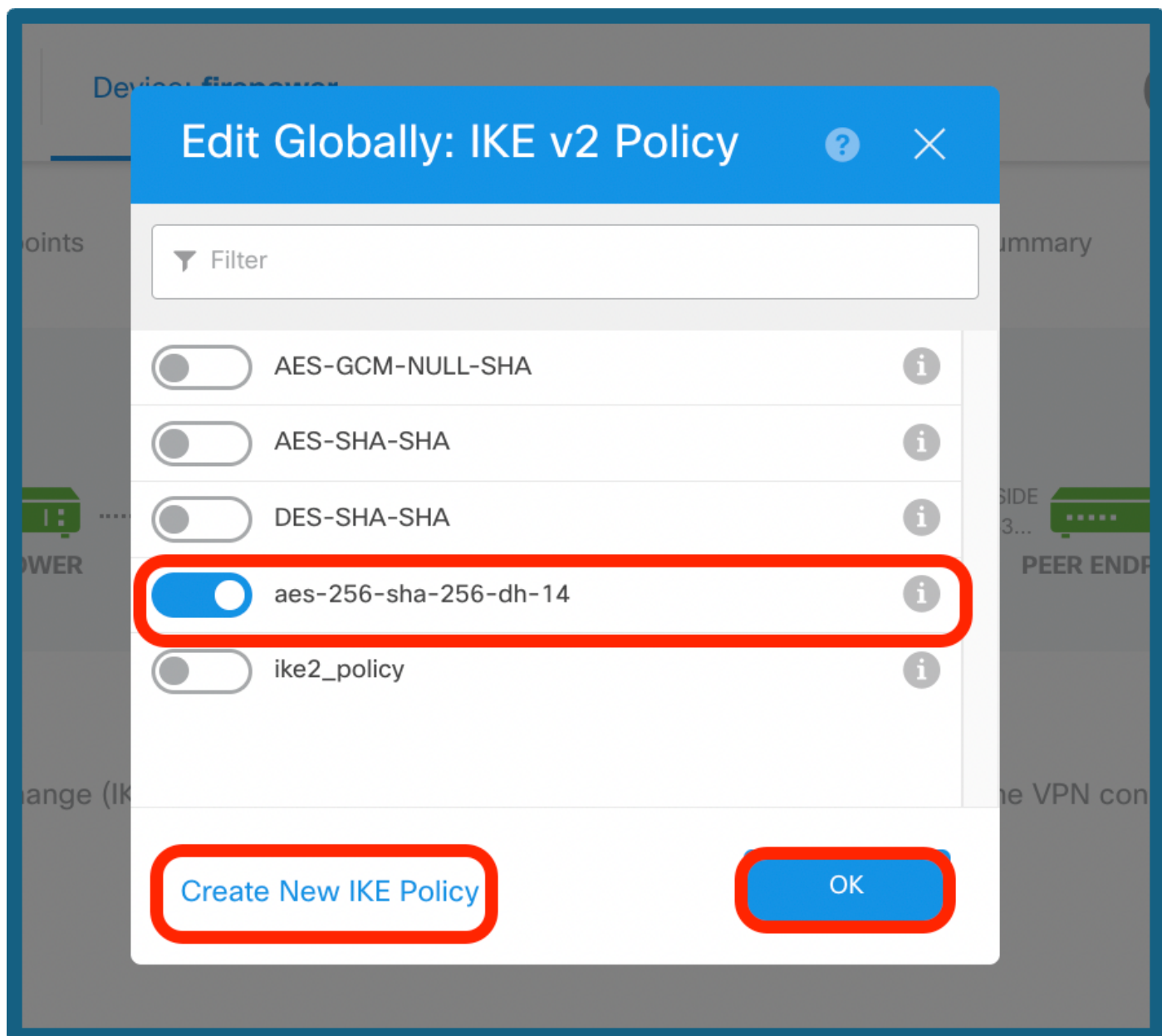
Globally applied

IPSec Proposal

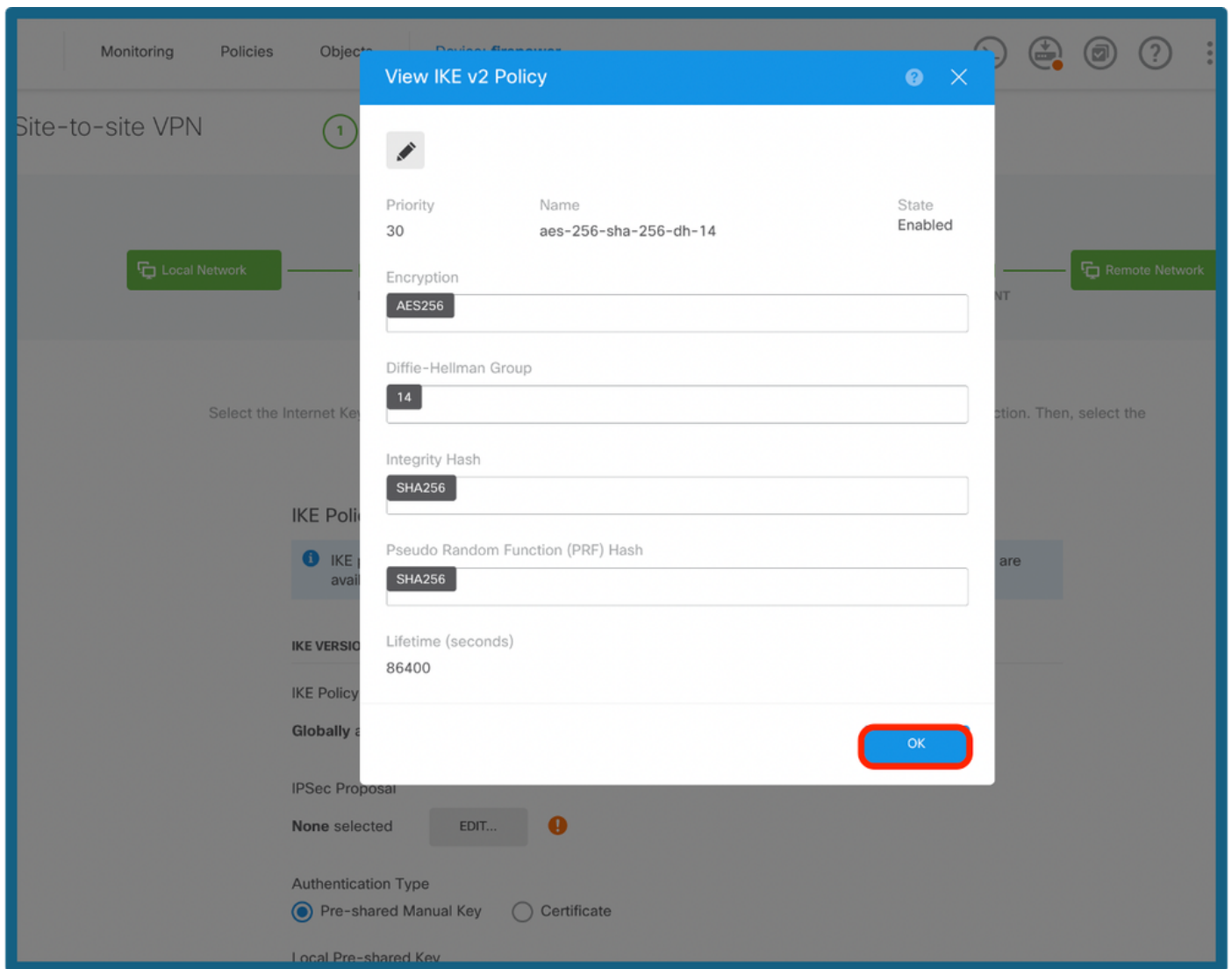
Custom set selected

配置IKE版本

步驟7a.選擇IKE Policy按鈕（如圖所示），然後按一下ok按鈕或Create New IKE Policy（如果要建立新策略）。

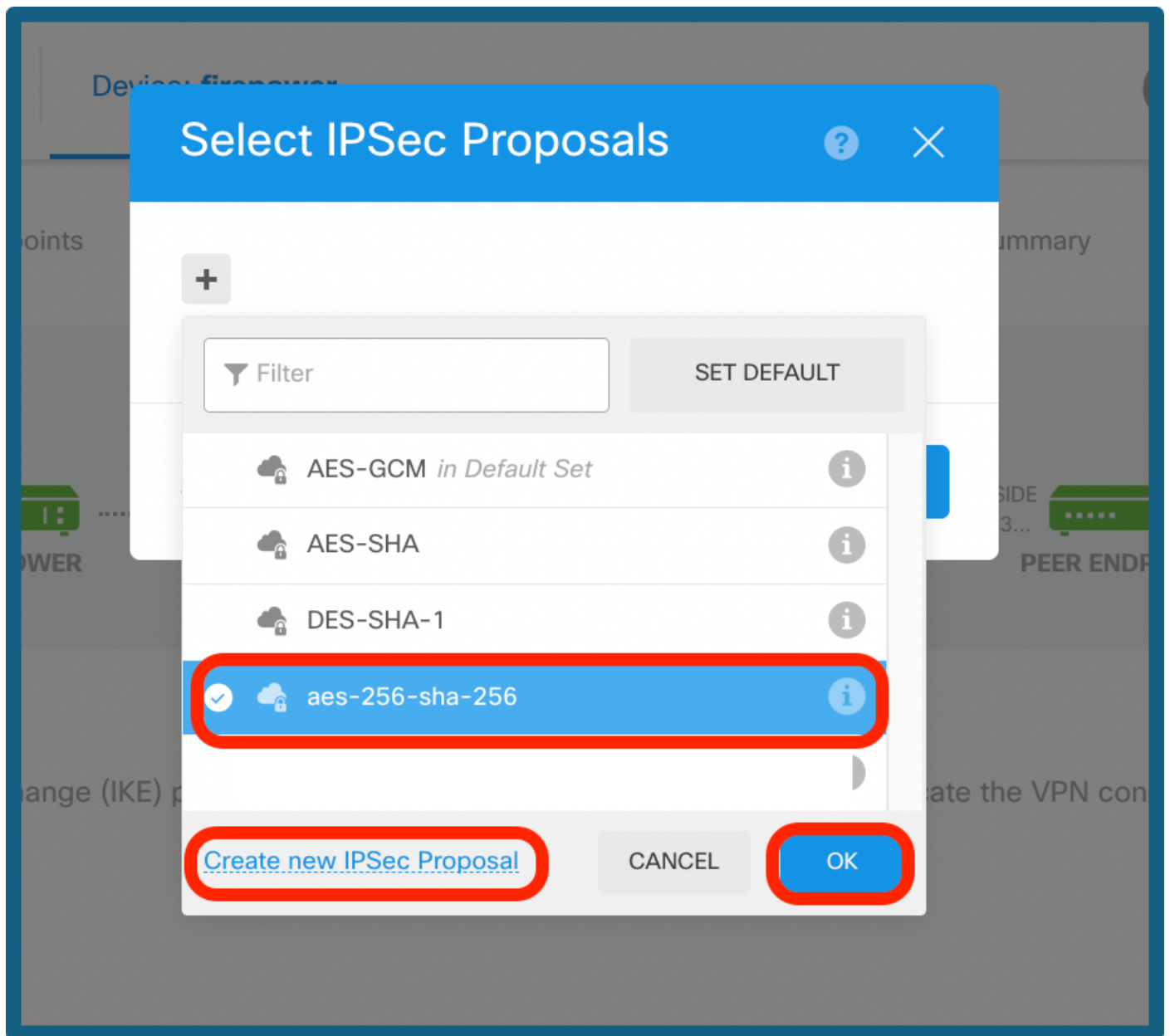


選擇IKE策略



IKE策略的配置

第7b步：選擇IPSec Policy按鈕（如圖所示），然後按一下ok按鈕或Create New IPsec Proposal（如果要建立新提議）。



選擇IPsec方案

IKE v2 IPSec Proposal

Name
aes-256-sha-256

Encryption
AES256

Integrity Hash
SHA256

OK

IPsec提議配置

步驟8a.選擇Authentication Type。如果使用預共用手動金鑰，請提供本地和遠端預共用金鑰。

步驟8b. (可選) 選擇完全向前保密設定。配置IPsec Lifetime Duration and Lifetime Size，然後按一下next。

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和生存期配置

步驟9.檢查配置並按一下Finish。

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)

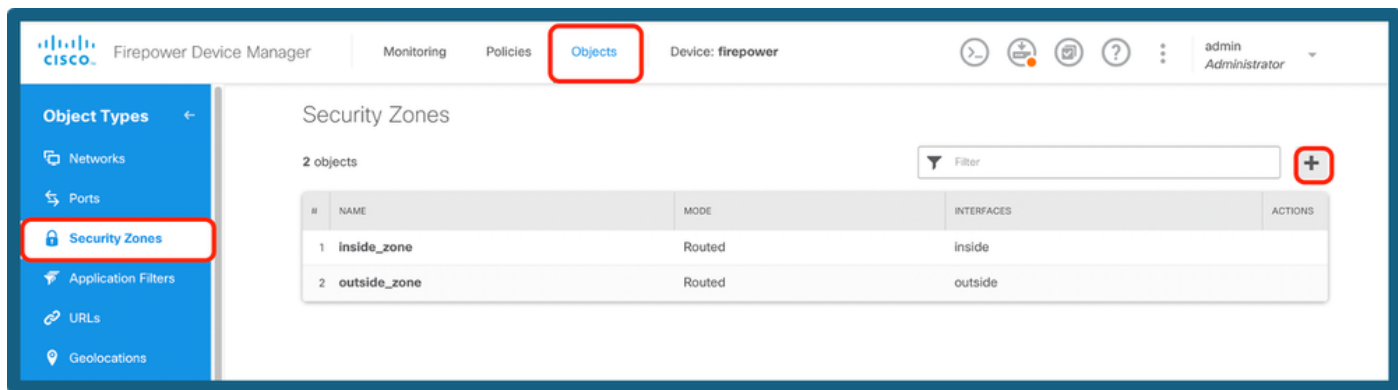
 Information is copied to the clipboard when you click Finish. You must allow the browser to access your clipboard for the copy to be successful.

BACK

FINISH

配置摘要

步驟10a。導航到Objects > Security Zones，然後按一下+圖示。



新增安全區域

步驟10b. 建立一個區域，然後選擇VTI介面，如下所示。

Add Security Zone

Name

vti-zone

Description

Mode

☒ Routed ☐ Passive

Interfaces

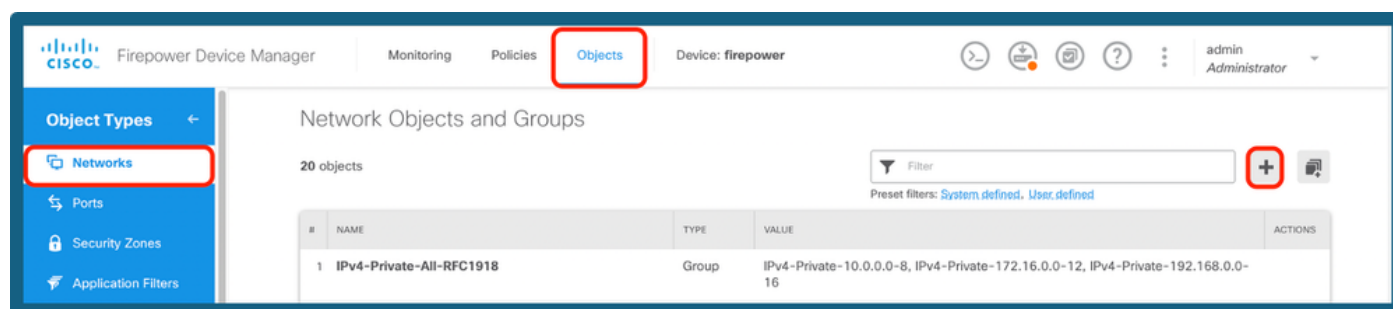
+

0 tunnel10 (Tunnel10)

CANCEL OK

安全區域配置

步驟11a.導航到Objects > Networks，按一下+圖示。



新增網路對象

步驟11b. 新增host對象，並使用對等端的隧道ip建立網關。

The screenshot shows the 'Edit Network Object' dialog box. The 'Name' field (highlighted with a red box) 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'. Below the 'Host' radio button, the 'Host' field (highlighted with a red box) contains '192.168.1.2'. Below this field, there is a hint text: 'e.g. 192.168.2.1 or 2001:DB8::0DB8:800:200C:417A'. At the bottom right, there are two buttons: 'CANCEL' and 'OK' (highlighted with a red box).

配置VPN網關

步驟11c.新增遠端子網和本地子網。

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

遠端IP配置

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

本地IP配置

步驟12.導航到Device > Policies，然後配置Access Control Policy。

Add Access Rule

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

Source/Destination | Applications | URLs | Users | Intrusion Policy | File policy | Logging

SOURCE

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

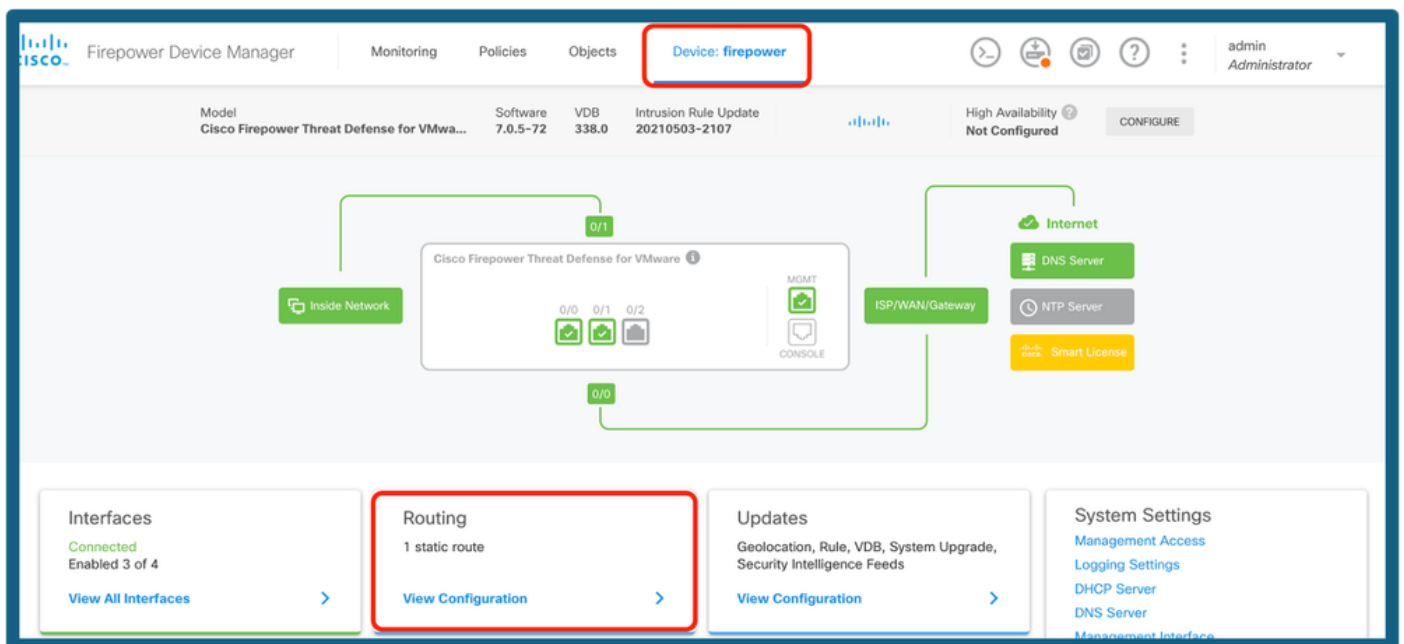
DESTINATION

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

Show Diagram: ☐ | CANCEL | OK

新增訪問控制策略

步驟13a.透過VTI通道新增路由。導覽至Device > Routing。



選擇工藝路線

步驟13b。導覽至Routing 索引標籤下的Static Route。按一下+圖示。

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	

新增路由

步驟13c.提供Interface，選擇Network，提供Gateway。按一下「OK」（確定）。

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

配置靜態路由

步驟14.導覽至Deploy。檢視更改，然後按一下Deploy Now。

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

部署配置

驗證

部署完成後，可以使用以下命令在CLI上驗證隧道狀態：

- show crypto ikev2 sa
- show crypto ipsec sa <peer-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
```

顯示命令

相關資訊

有關由FDM管理的FTD上的站點到站點VPN的詳細資訊，可在此處找到完整的配置指南：

[FDM管理的FTD配置指南](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。