

FTD上由FMC管理的站點到站點VPN配置

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[組態](#)

[步驟 1.定義VPN拓撲。](#)

[步驟 2.配置IKE引數。](#)

[步驟 3.配置IPsec引數。](#)

[步驟 4.繞過訪問控制。](#)

[步驟 5.建立訪問控制策略。](#)

[步驟 6.配置NAT免除。](#)

[步驟 7.配置ASA。](#)

[驗證](#)

[疑難排解和偵錯](#)

[初始連線問題](#)

[流量特定的問題](#)

簡介

本檔案介紹如何在由FMC管理的Firepower威脅防禦(FTD)上設定站點到站點VPN。

必要條件

需求

您應該對以下主題有一定認識：

- 對VPN有基礎認識
- 使用Firepower管理中心的經驗
- 使用ASA命令列體驗

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科FTD 6.5
- ASA 9.10(1)32
- IKEv2

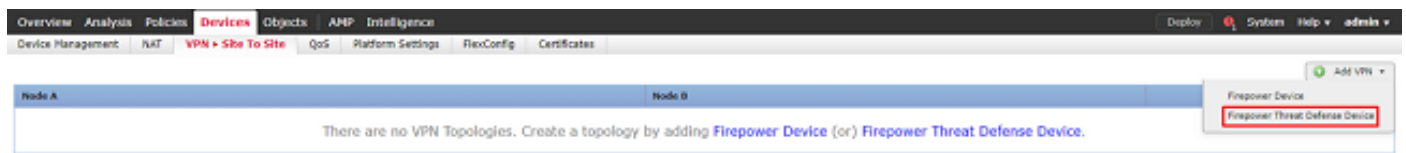
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

組態

從使用FirePower管理中心的FTD配置開始。

步驟 1. 定義VPN拓撲。

1. 導航到Devices > VPN > Site To Site。在Add VPN下，按一下Firepower Threat Defense Device，如下圖所示。



2. 出現Create New VPN Topology框。為VPN提供一個易於識別的名稱。

網路拓撲：點對點

IKE版本：IKEv2

在此示例中，當您選擇終端時，節點A是FTD，節點B是ASA。按一下綠色加號按鈕將裝置新增到拓撲中，如下圖所示。

Create New VPN Topology

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.將FTD新增為第一個端點。

選擇放置加密對映的介面。IP地址應從裝置配置中自動填充。

點選Protected Networks下的綠色加號（如圖所示），選擇此VPN中應加密哪些子網。

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)



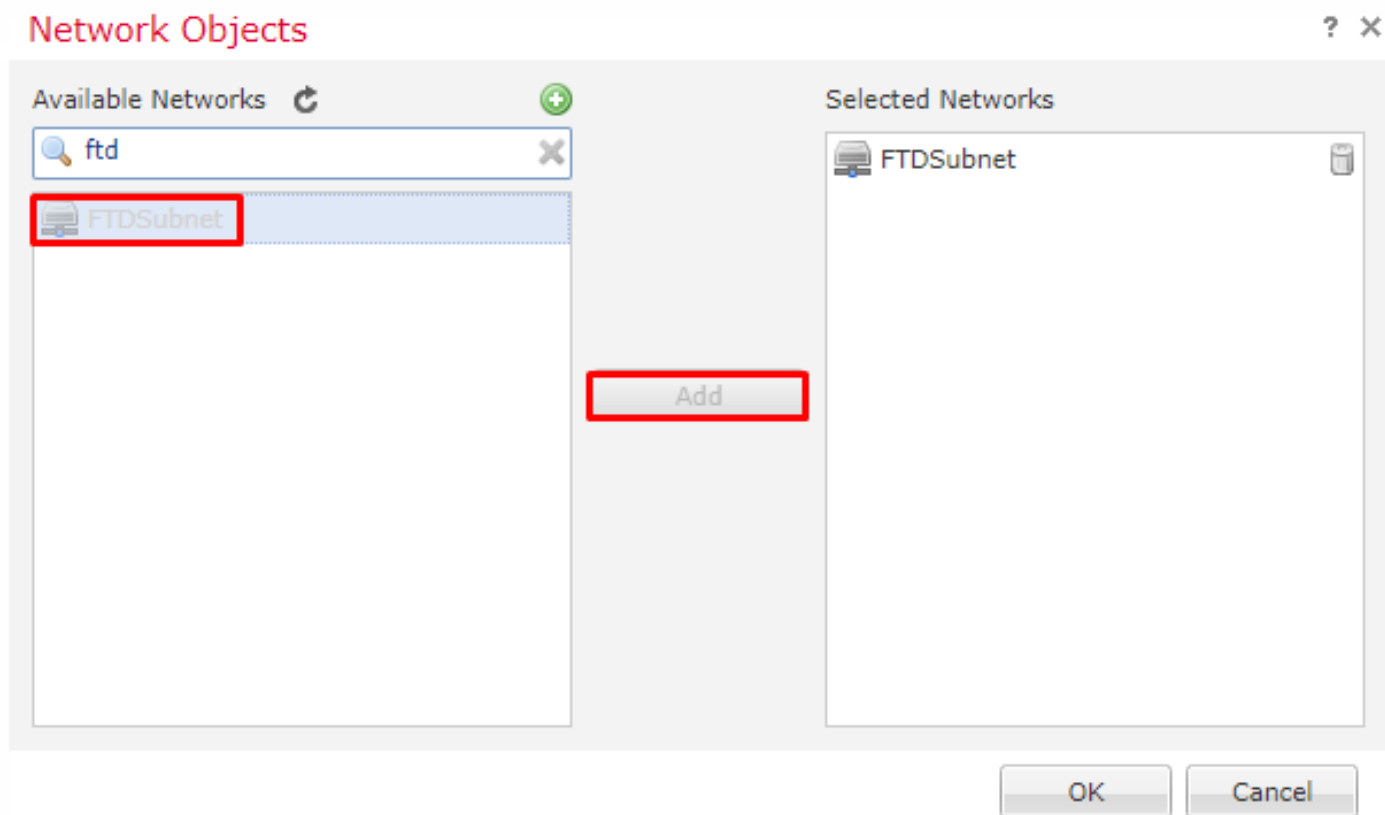
OK

Cancel

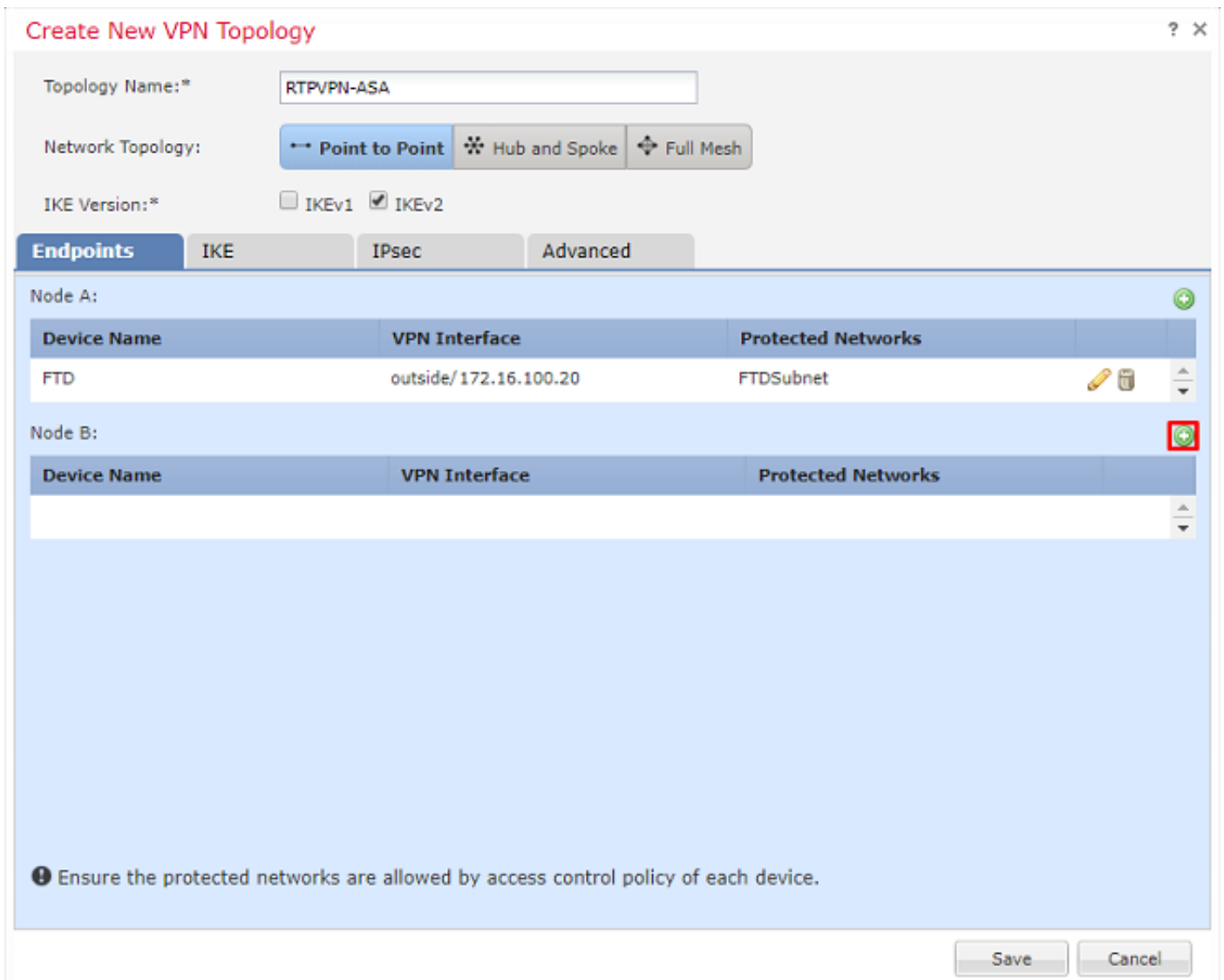
4.按一下綠色plus，此時將建立網路對象。

5.將所有本地子網新增到需要加密的FTD中。按一下Add將其移動到Selected Networks。現在，按一下「OK」，如下圖所示。

FTDSubnet = 10.10.113.0/24



節點A:(FTD)終結點已完成。按一下節點B的綠色加號，如下圖所示。



節點B是ASA。不受FMC管理的裝置被視為外聯網裝置。

6. 新增裝置名稱和IP地址。按綠色加號新增受保護的網路，如下圖所示。

Edit Endpoint



Device:*

Device Name:*

IP Address:* Static Dynamic

Certificate Map:

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

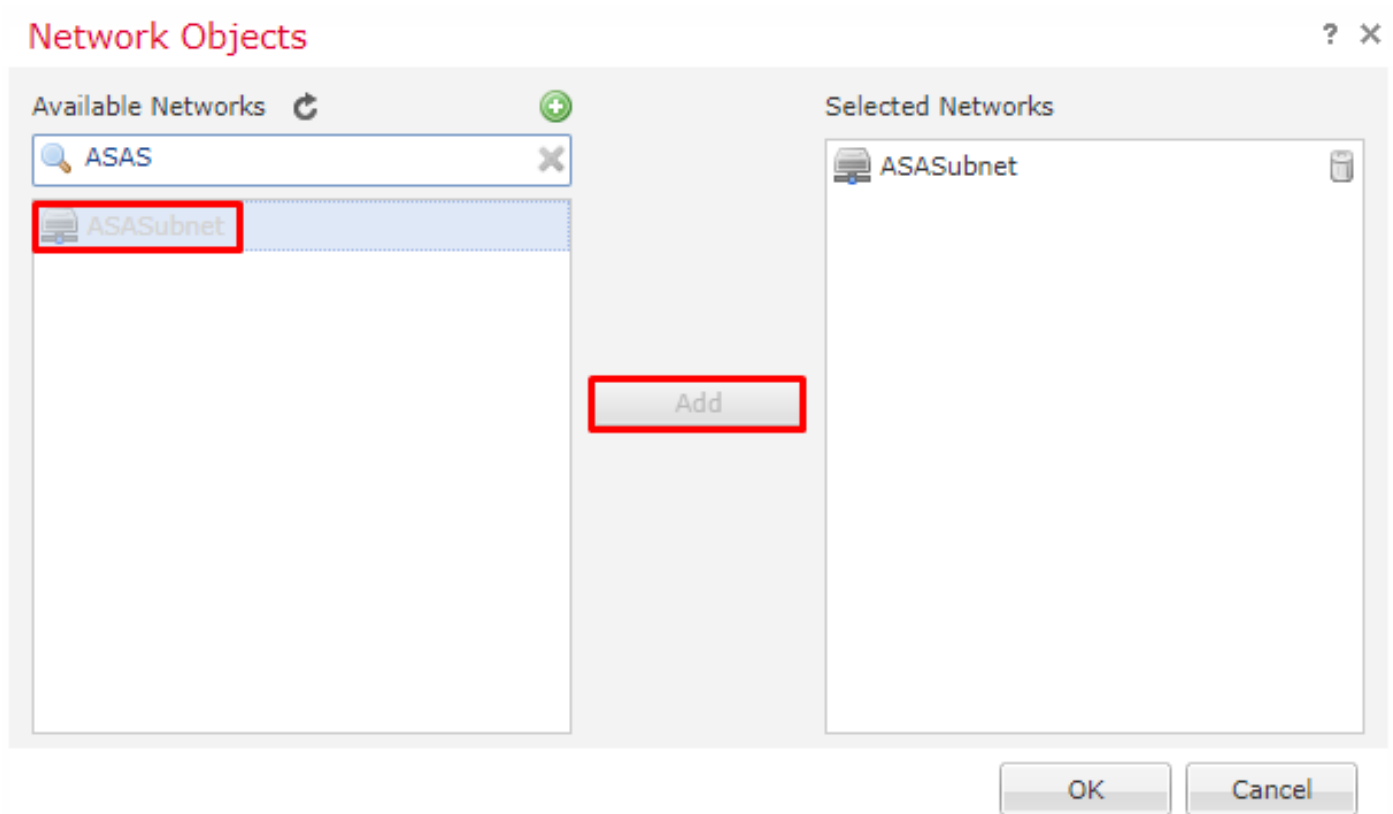


OK

Cancel

7.如圖所示，選擇需要加密的ASA子網，然後將其新增到選定的網路。

ASASubnet = 10.10.110.0/24



步驟 2. 配置IKE引數。

現在，兩個終端均已到位，通過IKE/IPSEC配置。

1. 在IKE頁籤下，指定用於IKEv2初始交換的引數。按一下綠色加號可建立新的IKE策略，如圖所示。

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.在新的IKE策略中，指定連線的優先順序編號和階段1的生存期。本文檔在初始交換中使用以下引數：完整性(SHA256)、加密(AES-256)、PRF(SHA256)和Diffie-Hellman組 (組14)

 注意：無論所選策略部分中有什麼，裝置上的所有IKE策略都將傳送到遠端對等裝置。將為VPN連線選擇由遠端對等項匹配的第一個IKE策略。使用優先順序欄位選擇首先傳送的策略。優先順序1將首先傳送。

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)

Integrity Algorithms	Available Groups	Selected Groups
Encryption Algorithms		
PRF Algorithms	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 5 <input checked="" type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21	<input type="checkbox"/> 14
Diffie-Hellman Group		

3. 新增引數後，選擇此策略，然後選擇驗證型別。

4. 選擇pre-shared-key手冊。本文檔使用PSK思科123。

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:* **ASA** +

Authentication Type: **Pre-shared Manual Key**

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

Save Cancel

步驟 3. 配置IPsec引數。

1. 在IPsec下，按一下鉛筆編輯轉換集並建立新的IPsec提議，如下圖所示。

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 + IKEv2 IPsec Proposals* +

tunnel_aes256_sha 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.要建立新的IKEv2 IPsec建議，請按一下綠色加號並輸入階段2引數。

選擇ESP Encryption > AES-GCM-256。使用GCM演算法加密時，不需要雜湊演算法。使用GCM時，雜湊函式是內建的。

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. 建立新的IPsec方案後，將其新增到選定的轉換集。

IKEv2 IPsec Proposal



Available Transform Sets

Search

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

Add

Selected Transform Sets

- ASA

OK Cancel

新選擇的IPsec方案現在列在IKEv2 IPsec方案下。

如果需要，可在此處編輯階段2生存期和PFS。在本例中，生存期將被設定為預設值，PFS將被禁用。

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

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

可選 — 必須完成旁路訪問控制選項或建立訪問控制策略。

步驟 4. 繞過訪問控制。

或者，可以在Advanced > Tunnel下啟用sysopt permit-vpn。

這樣消除了使用訪問控制策略檢查來自使用者的流量的可能性。VPN過濾器或可下載ACL仍可用於過濾使用者流量。這是一個全域性命令，如果選中此竅取方塊，該命令將應用於所有VPN。

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**

IKE
IPsec
Tunnel

NAT Settings

Keepalive Messages Traversal
Interval: 20 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

Save Cancel

如果未啟用sysopt permit-vpn，則必須建立訪問控制策略，以允許VPN流量通過FTD裝置。如果啟用sysopt permit-vpn，請跳過建立訪問控制策略。

步驟 5. 建立訪問控制策略。

在Access Control Policies下，導覽至Policies > Access Control > Access Control，然後選擇針對FTD裝置的策略。要新增規則，請點選Add Rule，如下圖所示。

必須允許流量從內部網路傳出到外部網路以及從外部網路傳到內部網路。建立一個規則以同時執行這兩個操作，或者建立兩個規則以將其分開。在此示例中，建立一條規則以同時執行這兩個操作。

Editing Rule - VPN_Traffic

Name: VPN_Traffic Enabled Move

Action: Allow Deny Log Log All

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 Zone	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	Any	<input checked="" type="checkbox"/> Allow <input type="checkbox"/> Deny <input type="checkbox"/> Log <input type="checkbox"/> Log All 0

Default Action: Access Control: Block All Traffic

步驟 6. 配置 NAT 免除。

為 VPN 流量配置 NAT 免除語句。NAT 豁免必須到位，以防止 VPN 流量進入另一個 NAT 語句並錯誤地轉換 VPN 流量。

1. 導航到 Devices > NAT，選擇以 FTD 為目標的 NAT 策略。按一下 Add Rule 按鈕時建立新規則。

Overview Analysis Policies Devices Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

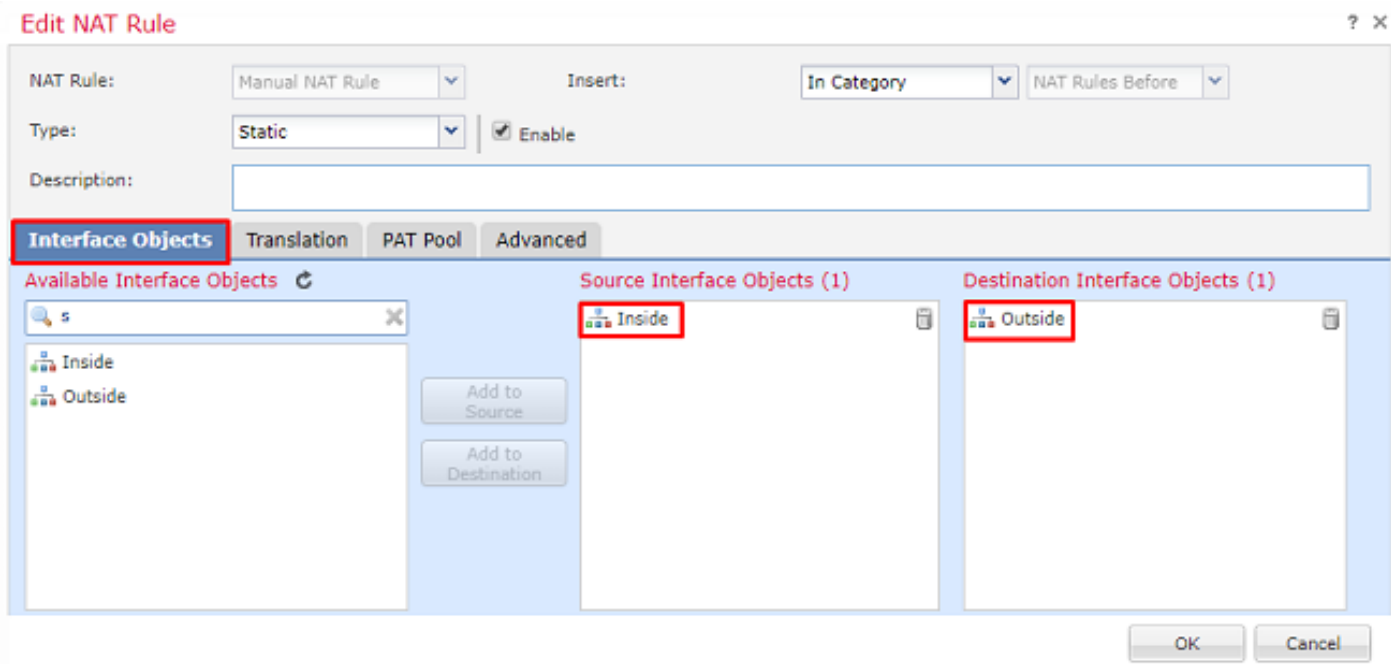
VirtualFTDNAT

Rules

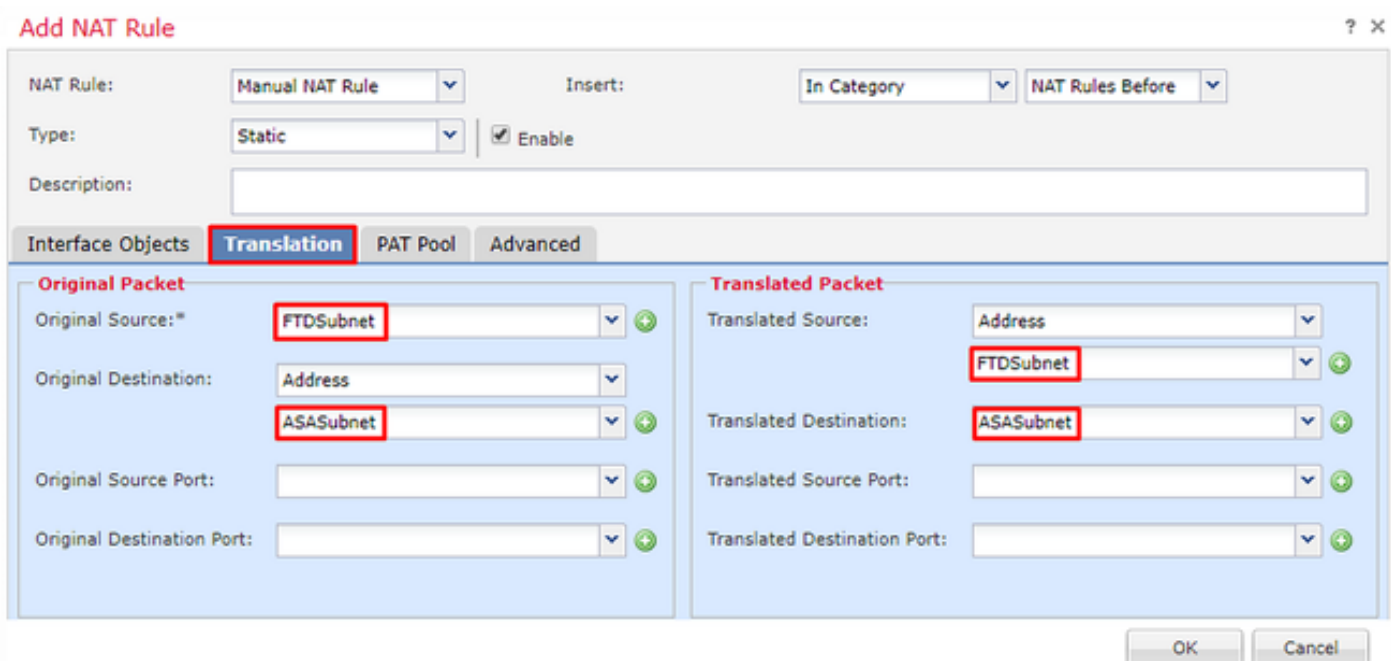
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
NAT Rules Before											
Auto NAT Rules											

Buttons: Show Warnings, Add Rule

2. 建立新的靜態手動 NAT 規則。參照內部和外部介面。



3.在Translation頁籤下，選擇源子網和目標子網。由於這是NAT免除規則，因此請使原始源/目標與轉換後的源/目標相同，如下圖所示：



4.最後轉到Advanced索引標籤，並啟用無代理arp和路由查詢。

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. 儲存此規則，然後在NAT清單中檢視最終結果。

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:fal route-lx no-prox
▼ Auto NAT Rules											
#	↔	Dynamic	Inside	Outside	any-obj			Interface			Dns:fal
▼ NAT Rules After											

6. 完成組態後，將組態儲存並部署到FTD。

步驟 7. 配置ASA。

1. 在ASA的外部介面上啟用IKEv2:

```
Crypto ikev2 enable outside
```

2. 建立定義在FTD上配置的相同引數的IKEv2策略：

```
Crypto ikev2 policy 1
```

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

3. 建立允許ikev2協定的組策略：

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

4. 為對等FTD公用IP位址建立通道組。引用組策略並指定預共用金鑰：

```
Tunnel-group 172.16.100.20 type ipsec-121
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. 建立定義要加密的流量的訪問清單：(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. 建立一個引用FTD上指定的演算法的ikev2 ipsec提議：

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


7. 建立將配置關聯在一起的加密對映條目：

```
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. 建立阻止防火牆NAT的NAT免除語句：

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

驗證

 註：此時無法從FMC檢視VPN隧道狀態。此功能有一個增強請求[CSCvh77603](https://cisco.com/bugtools/bugsearch/show/CSCvh77603)。

嘗試通過VPN隧道發起流量。通過訪問ASA或FTD的命令列，可以使用packet tracer命令完成此操作。使用packet Tracer命令啟動VPN隧道時，必須運行兩次以驗證隧道是否啟動。第一次發出該命令時，VPN隧道關閉，因此Packet Tracer命令將因VPN encrypt DROP而失敗。請勿將防火牆的內部IP地址用作Packet Tracer中的源IP地址，因為此操作將始終失敗。

```
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
```

若要監控通道狀態，請導覽至FTD或ASA的CLI。

在FTD CLI中，使用以下命令驗證第1階段和第2階段：

```
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
```

疑難排解和偵錯

初始連線問題

構建VPN時，雙方會協商隧道。因此，當您排除任何型別的通道故障時，最好讓對話雙方都參與進來。有關如何調試IKEv2隧道的詳細指南可在此處找到：[如何調試IKEv2 VPN](#)

通道故障的最常見原因是連線問題。確定這一點的最佳方法是在裝置上捕獲資料包。使用以下命令獲取裝置上的資料包捕獲：

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

捕獲到位後，嘗試通過VPN傳送流量，並在資料包捕獲中檢查雙向流量。

使用以下命令檢視封包擷取：

```
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
```

流量特定的問題

您遇到的常見流量問題包括：

- FTD背後的路由問題 — 內部網路無法將封包路由回指派的IP位址和VPN使用者端。
- 訪問控制清單阻止流量。
- VPN流量不會繞過網路地址轉換。

有關FMC管理的FTD上的VPN的詳細資訊，可在此處找到完整的配置指南：[FMC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）。