

配置AnyConnect以透過IPSec隧道訪問伺服器。

目錄

[簡介:](#)

[必要條件:](#)

[基本要求](#)

[採用元件](#)

[網路圖表](#)

[FMC上的配置](#)

[FTD上由FMC管理的RAVPN組態。](#)

[FTD上由FMC管理的IKEv2 VPN。](#)

[驗證](#)

[疑難排解](#)

簡介:

本檔案介紹在FMC管理的FTD上部署RAVPN設定以及FTD之間的月台對站台通道的程式。

必要條件:

基本要求

- 對站點到站點VPN和RAVPN的基本瞭解是有益的。
- 瞭解在Cisco Firepower平台上配置基於IKEv2策略的隧道的基礎知識至關重要。

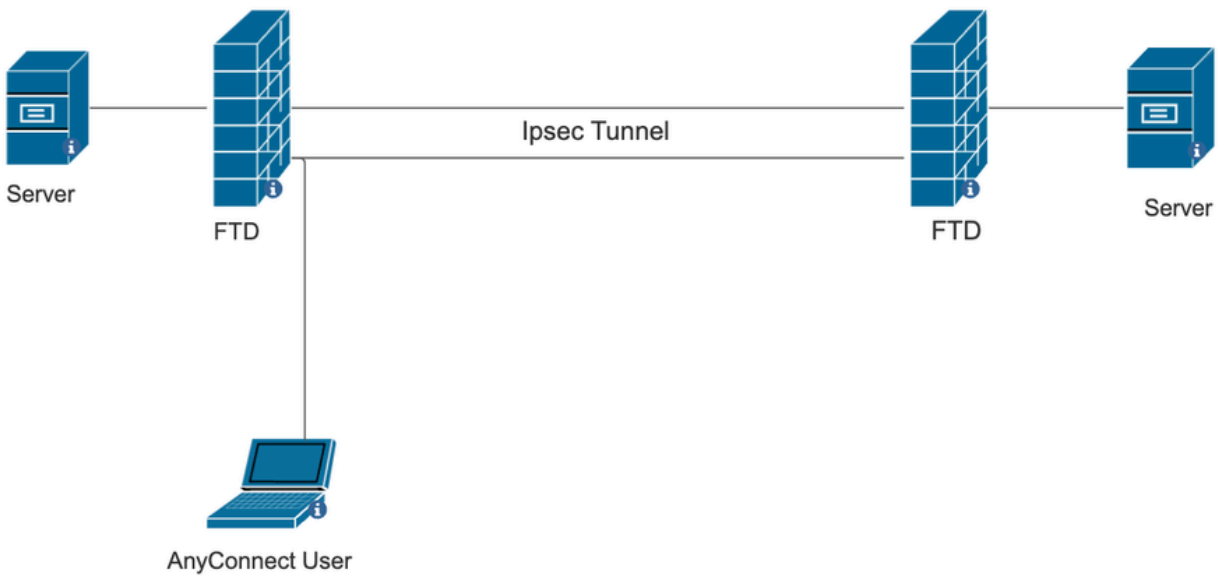
此程式適用於在由FMC管理的FTD上部署RAVPN設定，以及在FTD之間部署站點到站點隧道，AnyConnect使用者可在此處訪問其他FTD對等體之後的伺服器。

採用元件

- 適用於VMware的Cisco Firepower威脅防禦：版本7.0.0
- Firepower管理中心：版本7.2.4 (內部版本169)

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。 .

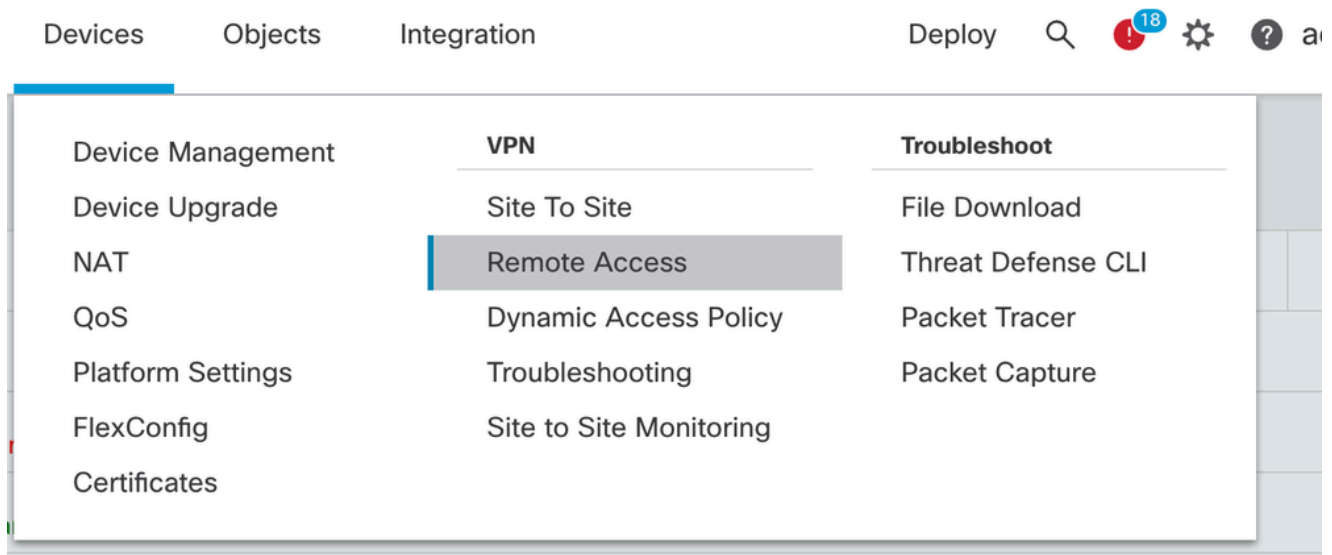
網路圖表



FMC上的配置

FTD上由FMC管理的RAVPN組態。

1. 導航到裝置>遠端訪問。



2. 按一下Add。
3. 設定名稱並從可用裝置中選擇FTD，然後按一下「Next」。

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:*

Description:

VPN Protocols:

SSL
 IPsec-IKEv2

Targeted Devices:

Available Devices	Selected Devices
<input type="text" value="Search"/> <div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #0070c0; color: white; padding: 2px;">10.106.50.55</div> <div style="padding: 2px;">10.88.146.35</div> <div style="padding: 2px;">New_FTD</div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="padding: 2px;">10.106.50.55 ✕</div> </div>

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure [LOCAL](#) or [Realm](#) or [RADIUS Server Group](#) or [SSO](#) to authenticate VPN clients.

AnyConnect Client Package

Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted [devices](#) so that they can be used as a security zone or interface group to enable VPN access.

4. 配置連線配置檔名稱並選擇身份驗證方法。

注意：對於此配置示例，我們僅使用AAA和本地身份驗證。但是，請根據您的要求進行配置。

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:*

i This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method:

Authentication Server:* +
(LOCAL or Realm or RADIUS)

Local Realm:* +

Authorization Server: +
(Realm or RADIUS)

Accounting Server: +
(RADIUS)

5. 配置用於AnyConnect的IP地址分配的VPN池。

(RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ●

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: 

IPv6 Address Pools: 

6. 建立組策略。按一下+建立組策略。增加組策略的名稱。

Edit Group Policy ?

Name:*

Description:

General AnyConnect Advanced

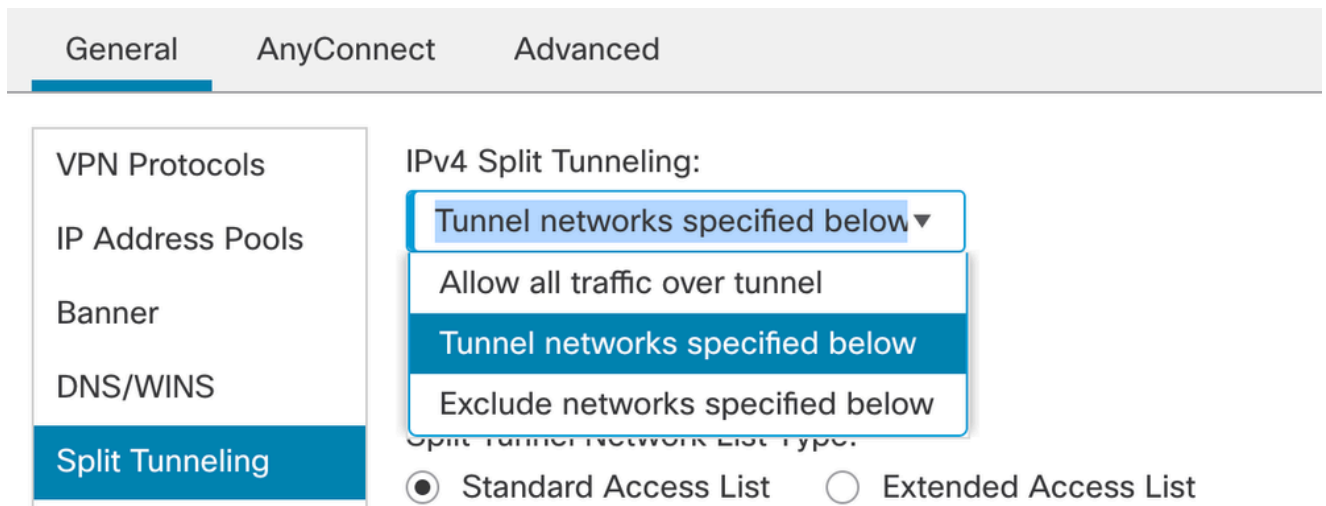
VPN Protocols

- IP Address Pools
- Banner
- DNS/WINS
- Split Tunneling

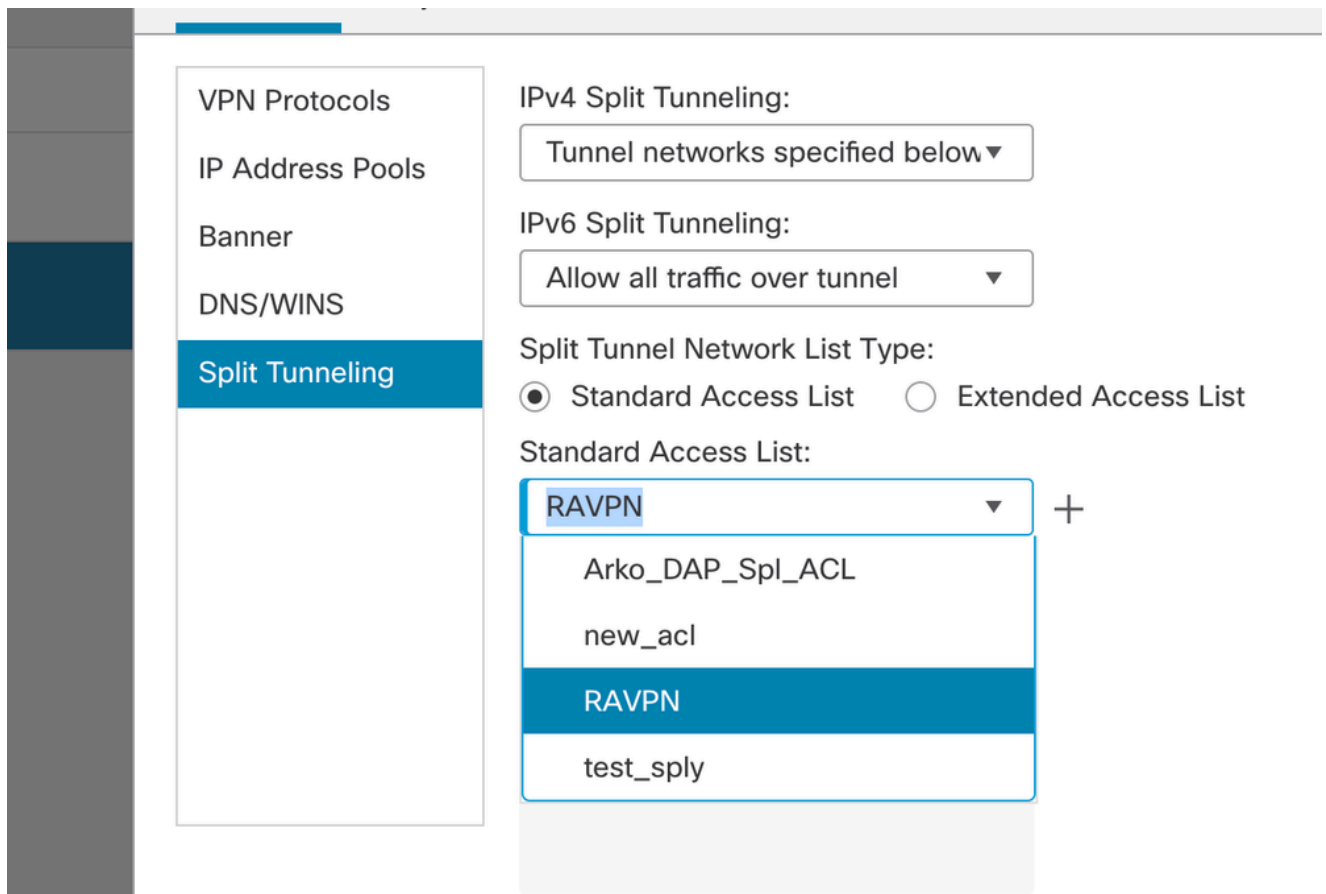
VPN Tunnel Protocol:
Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

- SSL
- IPsec-IKEv2

7. 轉到Split tunneling。選擇此處指定的隧道網路：



8. 從下拉選單中選擇正確的訪問清單。如果尚未配置ACL：按一下+圖示增加標準訪問清單並建立一個新訪問清單。
按一下Save。



9. 選擇所增加的組策略，然後按一下Next。

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* +

[Edit Group Policy](#)

10. 選擇AnyConnect映像。

AnyConnect Client Image

The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#).

[Show Re-order buttons](#) +

<input type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input type="checkbox"/>	anyconnect	anyconnect410.pkg	<input type="text" value="Windows"/>
<input checked="" type="checkbox"/>	anyconnect-win-4.10.07073-we...	anyconnect-win-4.10.07073-webdeploy-k9...	<input type="text" value="Windows"/>
<input type="checkbox"/>	secure_client_5-1-2	cisco-secure-client-win-5_1_2_42-webde...	<input type="text" value="Windows"/>

11. 選擇必須啟用AnyConnect連線的介面，增加證書，為解密的資料流選擇繞過訪問控制策略

Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* +

Enable DTLS on member interfaces

▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

，然後按一下Next。

12. 稽核配置並按一下Finish。

Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name: RAVPN
 Device Targets: 10.106.50.55
 Connection Profile: RAVPN
 Connection Alias: RAVPN
 AAA:
 Authentication Method: AAA Only
 Authentication Server: sid_tes_local (Local)
 Authorization Server: -
 Accounting Server: -
 Address Assignment:
 Address from AAA: -
 DHCP Servers: -
 Address Pools (IPv4): vpn_pool
 Address Pools (IPv6): -
 Group Policy: DfltGrpPolicy
 AnyConnect Images: anyconnect-win-4.10.07073-webdeploy-k9.pkg
 Interface Objects: sid_outside
 Device Certificates: cert1_1

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update
An Access Control rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption
If NAT is enabled on the targeted devices, you must define a NAT Policy to exempt VPN traffic.
- DNS Configuration
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using FlexConfig Policy on the targeted devices.
- Port Configuration
SSL will be enabled on port 443. IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Anyconnect image download. NAT-Traversal will be enabled by default and will use port 4500. Please ensure that these ports are not used in NAT Policy or other services before deploying the configuration.

Cancel Back Finish

13. 按一下Save並進行部署。

RAVPN

Enter Description

You have unsaved changes Save Cancel

Policy Assignments (1)

Local Realm: New_Realm Dynamic Access Policy: None

Connection Profile Access Interfaces Advanced

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
RAVPN	Authentication: LOCAL Authorization: None Accounting: None	RAVPN

FTD上由FMC管理的IKEv2 VPN：

1. 導航到裝置>站點到站點。

Devices Objects Integration Deploy 🔍 19 ⚙️ ? ad

Device Management	VPN	Troubleshoot
Device Upgrade	Site To Site	File Download
NAT	Remote Access	Threat Defense CLI
QoS	Dynamic Access Policy	Packet Tracer
Platform Settings	Troubleshooting	Packet Capture
FlexConfig	Site to Site Monitoring	
Certificates		

- 按一下Add。
- 點選+ (對於節點A) :

Center

Create New VPN Topology

Topology Name:*

Policy Based (Crypto Map) Route Based (VTI)

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	

- 從裝置選擇FTD，選擇介面，增加必須透過IPSec隧道加密的本地子網（在本例中還包含VPN池地址），然後按一下OK。

Edit Endpoint



Device:*

Interface:*

IP Address:*

This IP is Private

Connection Type:

Certificate Map:

 +

Protected Networks:*

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

FTD-Lan	
VPN_Pool_Subnet	

+

5. 點選+ (在節點B上) :

>從裝置中選擇外聯網，然後指定對等裝置的名稱。

>配置對等體詳細資訊並增加需要透過VPN隧道訪問的遠端子網，然後按一下OK。

Edit Endpoint ?

Device:*

Device Name:*

IP Address:*
 Static Dynamic

Certificate Map:
 +

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

Remote-Lan2 +

Remote-Lan +

6. 點選IKE頁籤：根據需要配置IKEv2設定

Edit VPN Topology



Topology Name:*

FTD-S2S-FTD

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

Point to Point Hub and Spoke Full Mesh

IKE Version:*

IKEv1

IKEv2

Endpoints

IKE

IPsec

Advanced

IKEv2 Settings

Policies:*

FTD-ASA

Authentication Type:

Pre-shared Manual Key

Key:*

.....

Confirm Key:*

.....

Enforce hex-based pre-shared key only

Cancel

Save

7. 按一下IPsec頁籤：根據您的要求配置IPSec設定。

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*

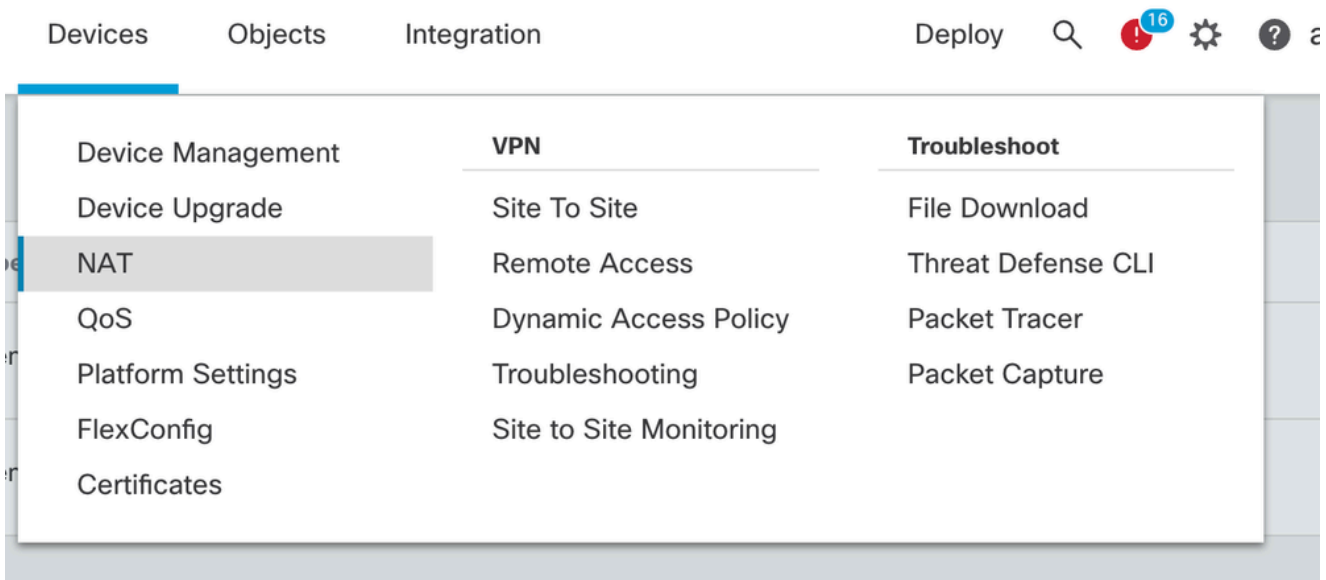
Enable Security Association (SA) Strength Enforcement
 Enable Reverse Route Injection
 Enable Perfect Forward Secrecy

Modulus Group:

Lifetime Duration*: Seconds (Range 120-2147483647)

Lifetime Size: Kbytes (Range 10-2147483647)

8. 為相關流量配置Nat-Exempt (可選)
 按一下Devices > NAT



9. 此處配置的NAT允許RAVPN和內部使用者透過S2S IPsec隧道訪問伺服器。

☐	#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options	
						Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services		
<input type="checkbox"/>	3	↔	Static	sid_outside	sid_outside	VPN_Pool_Subnet	Remote-Lan		VPN_Pool_Subnet	Remote-Lan		Dns: false route-lookup no-proxy-arp	
<input type="checkbox"/>	4	↔	Static	sid_inside	sid_outside	FTD-Lan	Remote-Lan2		FTD-Lan	Remote-Lan2		Dns: false route-lookup no-proxy-arp	
<input type="checkbox"/>	5	↔	Static	sid_inside	sid_outside	FTD-Lan	Remote-Lan		FTD-Lan	Remote-Lan		Dns: false route-lookup no-proxy-arp	

10. 類似地，在另一端對S2S隧道的配置也會出現。

注意：加密ACL或相關流量子網必須在兩個對等體上互為映象副本。

驗證

1. 驗證RAVPN連線：

```
<#root>
```

```
firepower# show vpn-sessiondb anyconnect
```

```
Session Type: AnyConnect
```

```
Username : test
```

```
Index : 5869
```

```
Assigned IP : 2.2.2.1 Public IP : 10.106.50.179
```

```
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

```
License : AnyConnect Premium
```

```
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
```

```
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
```

```
Bytes Tx : 15470 Bytes Rx : 2147
```

```
Group Policy : RAVPN Tunnel Group : RAVPN
```

```
Login Time : 03:04:27 UTC Fri Jun 28 2024
```

```
Duration : 0h:14m:08s
```

```
Inactivity : 0h:00m:00s
```

```
VLAN Mapping : N/A VLAN : none
```

```
Audt Sess ID : 0a6a3468016ed000667e283b
```

```
Security Grp : none Tunnel Zone : 0
```

2. 要驗證IKEv2連線，請執行以下操作：

```
<#root>
```

```
firepower# show crypto ikev2 sa
```

```
IKEv2 SAs:
```

```
Session-id:2443, Status:UP-ACTIVE
```

```
, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Remote Status Role
```

```
3363898555
```

```
10.106.52.104/500 10.106.52.127/500 READY INITIATOR
```

```
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
```

```
Life/Active Time: 86400/259 sec
```

```
Child sa: local selector 2.2.2.0/0 - 2.2.2.255/65535
```

```
remote selector 10.106.54.0/0 - 10.106.54.255/65535
```

```
ESP spi in/out: 0x4588dc5b/0x284a685
```

3. 要驗證IPSec連線，請執行以下操作：

```
<#root>
```

```
firepower# show crypto ipsec sa peer 10.106.52.127
```

```
peer address: 10.106.52.127
```

```
Crypto map tag: CSM_outside1_map
```

```
,
```

```
seq num: 2, local addr: 10.106.52.104
```

```
access-list CSM_IPSEC_ACL_1 extended permit ip 2.2.2.0 255.255.255.0 10.106.54.0 255.255.255.0
```

```
local ident (addr/mask/prot/port): (2.2.2.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (10.106.54.0/255.255.255.0/0/0)
```

current_peer: 10.106.52.127

#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3

#pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 3, #pkts comp failed: 0, #pkts decomp failed: 0

#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0

#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0

#TFC rcvd: 0, #TFC sent: 0

#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0

#send errors: 0, #recv errors: 0

Local crypto endpt.: 10.106.52.104/500, remote crypto endpt.: 10.106.52.127/500

path mtu 1500, ipsec overhead 94(44), media mtu 1500

PMTU time remaining (sec): 0, DF policy: copy-df

ICMP error validation: disabled, TFC packets: disabled

current outbound spi: 0284A685

current inbound spi : 4588DC5B

i

nbound esp sas:

spi: 0x4588DC5B (1166597211)

SA State: active

transform: esp-aes-256 esp-sha-512-hmac no compression

in use settings ={L2L, Tunnel, IKEv2, }

slot: 0, conn_id: 5882, crypto-map: CSM_outside1_map

sa timing: remaining key lifetime (kB/sec): (3962879/28734)

IV size: 16 bytes

replay detection support: Y

Anti replay bitmap:

0x00000000 0x0000000F

outbound esp sas:

spi: 0x0284A685 (42247813)

SA State: active

```
transform: esp-aes-256 esp-sha-512-hmac no compression
```

```
in use settings ={L2L, Tunnel, IKEv2, }  
slot: 0, conn_id: 5882, crypto-map: CSM_outside1_map  
sa timing: remaining key lifetime (kB/sec): (4285439/28734)  
IV size: 16 bytes  
replay detection support: Y  
Anti replay bitmap:  
0x00000000 0x00000001
```

疑難排解

1. 要排除AnyConnect連線問題，請收集DART捆綁包或啟用AnyConnect調試。
2. 要排除IKEv2隧道的故障，請使用以下調試：

```
debug crypto condition peer <peer IP address>  
debug crypto ikev2 platform 255  
debug crypto ikev2 protocol 255  
debug crypto ipsec 255
```

3. 若要疑難排解FTD上的流量問題，請進行封包擷取並檢查設定。

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）。