

在FTD上配置AnyConnect VPN客戶端：髮夾和NAT免除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[步驟 1. 匯入SSL證書](#)

[步驟 2. 設定RADIUS伺服器](#)

[步驟 3. 建立IP池](#)

[步驟 4. 建立XML配置檔案](#)

[步驟 5. 上傳Anyconnect XML配置檔案](#)

[步驟 6. 上傳AnyConnect映像](#)

[步驟 7. 遠端訪問VPN嚮導](#)

[NAT免除和發卡](#)

[步驟 1. NAT免除配置](#)

[步驟 2. 髮夾配置](#)

[驗證](#)

[疑難排解](#)

簡介

本檔案介紹如何在FMC管理的Firepower威脅防禦(FTD)v6.3上配置思科遠端訪問VPN解決方案(AnyConnect)。

必要條件

需求

思科建議您瞭解以下主題：

- 基本遠端訪問VPN、安全套接字層(SSL)和網際網路金鑰交換版本2(IKEv2)知識
- 基本驗證、授權及記帳(AAA)和RADIUS知識
- 基本的FMC知識
- 基本FTD知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科FMC 6.4
- 思科FTD 6.3
- AnyConnect 4.7

本檔案介紹在Firepower威脅防禦(FTD)版本6.3(由Firepower管理中心(FMC)管理)上配置思科遠端訪問VPN解決方案(AnyConnect)的程式。

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

本文檔旨在介紹FTD裝置上的配置。如果您查詢ASA配置示例，請參閱文檔

：<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html>

限制：

目前，這些功能在FTD上不受支援，但在ASA裝置上仍然可用：

- 雙AAA驗證 (在FTD 6.5版上可用)
- 動態訪問策略
- 主機掃描
- ISE狀態
- RADIUS CoA
- VPN負載平衡器
- 本地身份驗證(在Firepower裝置管理器6.3上可用。思科錯誤ID [CSCvf92680](#))
- LDAP屬性對映(通過FlexConfig提供，思科錯誤ID [CSCvd64585](#))
- AnyConnect自定義
- AnyConnect指令碼
- AnyConnect本地化
- 每應用VPN
- SCEP代理
- WSA整合
- SAML SSO(思科錯誤ID [CSCvq90789](#))
- 適用於RA和L2L VPN的同步IKEv2動態加密對映
- AnyConnect模組 (NAM、Hostscan、AMP Enabler、SBL、Umbrella、Web Security等)。DART是此版本中預設安裝的唯一模組。
- TACACS、Kerberos (KCD身份驗證和RSA SDI)
- 瀏覽器代理

設定

要通過FMC中的遠端訪問VPN嚮導，必須完成以下步驟：

步驟 1. 匯入SSL證書

設定AnyConnect時，憑證是必需的。SSL和IPSec僅支援基於RSA的證書。

IPSec支援橢圓曲線數位簽章演演算法(ECDSA)憑證，但使用基於ECDSA的憑證時，無法部署新的AnyConnect封包或XML設定檔。

它可用於IPSec，但必須預先部署AnyConnect軟體包和XML配置檔案，所有XML配置檔案更新必須在每個客戶端上手動推送(思科錯誤ID [CSCtx42595](#))。

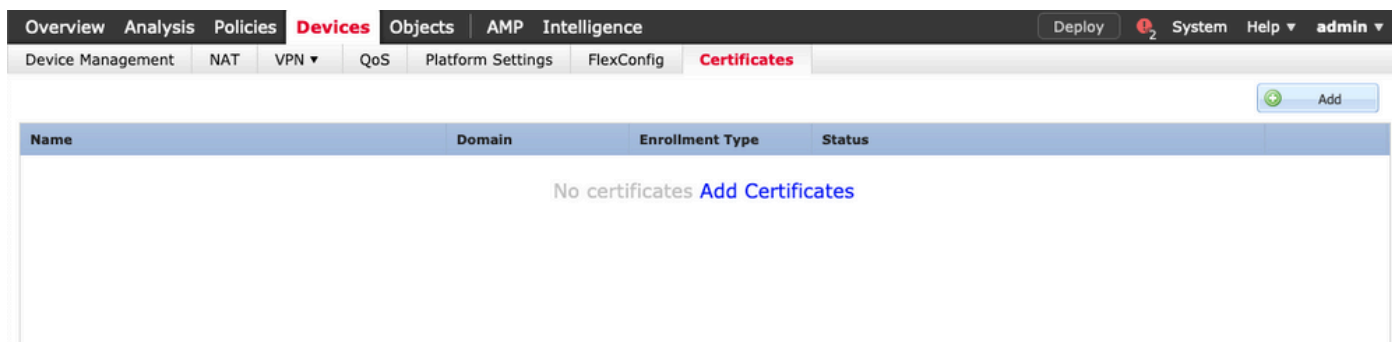
此外，憑證必須包含具有DNS名稱和/或IP位址的通用名稱(CN)擴充模組，才能避免Web瀏覽器中的「Untrusted server certificate」錯誤。

註：在FTD裝置上，需要先取得憑證授權單位(CA)憑證，才能產生憑證簽署請求(CSR)。

- 如果在外部伺服器（例如Windows Server或OpenSSL）中產生CSR，則手動註冊方法會失敗，因為FTD不支援手動金鑰註冊。
- 必須使用其他方法，例如PKCS12。

若要使用手動註冊方法取得FTD裝置的憑證，需要產生CSR，使用CA對其進行簽名，然後匯入身分憑證。

1.導覽至Devices > Certificates，然後選擇Add，如下圖所示。



2.選擇Device並新增新的Cert Enrollment對象，如下圖所示。

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

Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates** Add

Name	Domain	Enrollment Type	Status
No certificates Add Certificates			

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*: FTD-Virtual

Cert Enrollment*: Select a certificate enrollment object

Add Cancel

Add Cert Enrollment

Name* Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: SCEP

Enrollment URL:* http://

Challenge Password:

Confirm Password:

Retry Period: 1 Minutes (Range 1-60)

Retry Count: 10 (Range 0-100)

Fingerprint: Ex: e6f7d542 e355586c a758e7cb bdcddd92

Allow Overrides

Save Cancel

3.選擇手動註冊型別，然後貼上CA證書（用於簽署CSR的證書）。

Add Cert Enrollment



Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate:*

```
/3C4hi07uzuR0ygwKEBaMdg4Dl/z
4x3nk3tTUhYpfbmblWqWAXM7GNDRVWG9BZ1svk3shDK2Bogklzou6
RqV66Gj9IE7Z2
xIVrSrJFqhrT795kMb8am8xhb4eXYXxUgJmODIPqZ76RSTAT0+v1
VLSP+vHGm8X
g6wEFsKuZay27a48e/lJG2LgRDraOKt+jwbS7DGSK4mfZsZqhFdQP
LhBNFbyBvb9
dOjUkmdSvzQDRSqSo+HINEm3E8/q20wrtZp04MpAabyhr+hEpeP
VMrhvBOT8h
H8eMjSQjGhhHbuKofVlzQmM0RvGnTB6EKYlVb4CUW8HcgDdDr
mwNgy5mTP9cHa
9Cr3RlWRzEa11HE3mHC4Rj6DOnmgufjx+TZRYczownSKILL7LcW1
Dl8ZclYmfaldC
W2cZuBR0yVDxcCvq4f04ISElBfOWFsd5rAD/bvk2n6xrJl1SLqABMJJ
uslu9KTGH1
bYKEYACKVvETw==
-----END CERTIFICATE-----
```

Allow Overrides

4.選擇「Certificate Parameters」頁籤，然後為「Include FQDN」欄位選擇「自定義FQDN」，並填寫證書詳細資訊，如下圖所示。

Add Cert Enrollment ? X

Name*

Description

CA Information **Certificate Parameters** Key Revocation

Include FQDN:

Include Device's IP Address:

Common Name (CN):

Organization Unit (OU):

Organization (O):

Locality (L):

State (ST):

Country Code (C):

Email (E):

Include Device's Serial Number

Allow Overrides

5.選擇鍵頁籤，然後選擇鍵型別，您可以選擇名稱和大小。對於RSA，最低要求為2048位元組。

6.選擇儲存，確認裝置，然後在證書註冊下選擇剛建立的信任點，選擇新增以部署證書。

Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*:

Cert Enrollment Details:

Name: Anyconnect-certificate

Enrollment Type: Manual

SCEP URL: NA

Add

Cancel

7. 在Status列中，選擇ID圖示，然後選擇Yes以產生CSR，如下圖所示。

The screenshot shows the Cisco FTD GUI with the 'Certificates' tab selected. The table below shows the certificate configuration:

Name	Domain	Enrollment Type	Status
Anyconnect-certificate	Global	Manual	Identity certificate import required

A warning dialog box is displayed in the foreground:

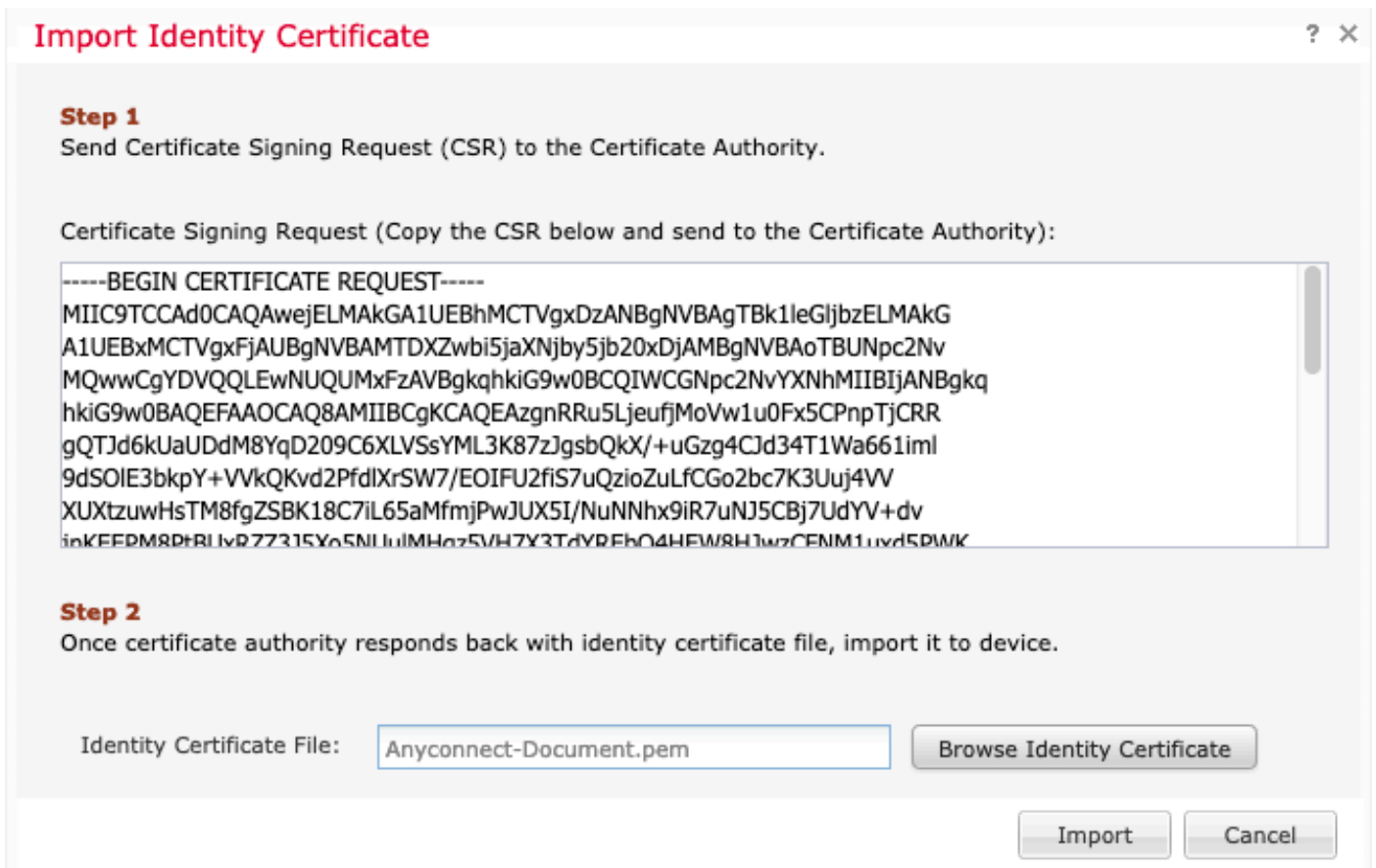
Warning

This operation will generate Certificate Signing Request do you want to continue?

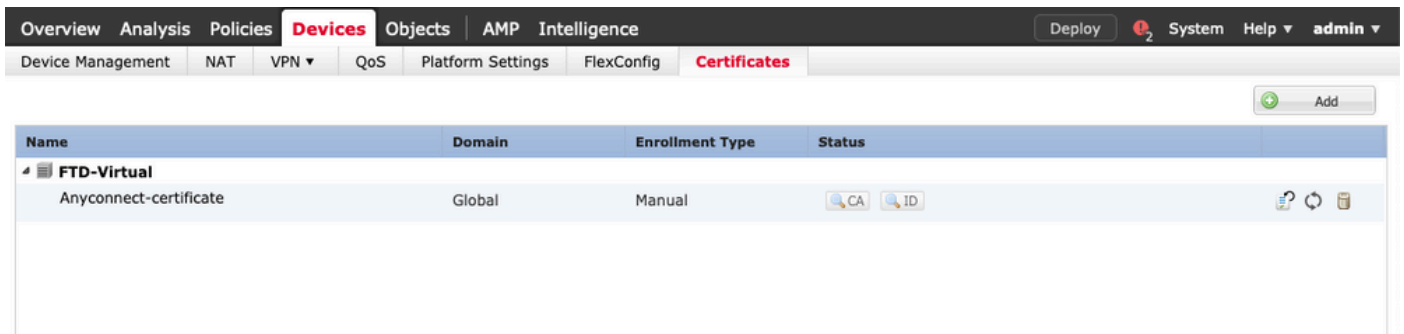
Yes No

8. 複製CSR並用您首選的CA（例如GoDaddy或DigiCert）簽名。

9. 從CA收到身份證書（必須採用base64格式）後，選擇Browse Identity Certificate，然後在本地電腦中查詢該證書。選擇匯入。



10. 匯入後，CA和ID證書詳細資訊可供顯示。



步驟 2. 設定RADIUS伺服器

在FMC管理的FTD裝置上，不支援本地使用者資料庫，必須使用其他身份驗證方法，例如RADIUS或LDAP。

1. 導覽至Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group，如下圖所示。

Add RADIUS Server Group



Name:*

Description:

Group Accounting Mode: ▼

Retry Interval:* (1-10) Seconds

Realms:


Enable authorize only

Enable interim account update

Interval:* (1-120) hours

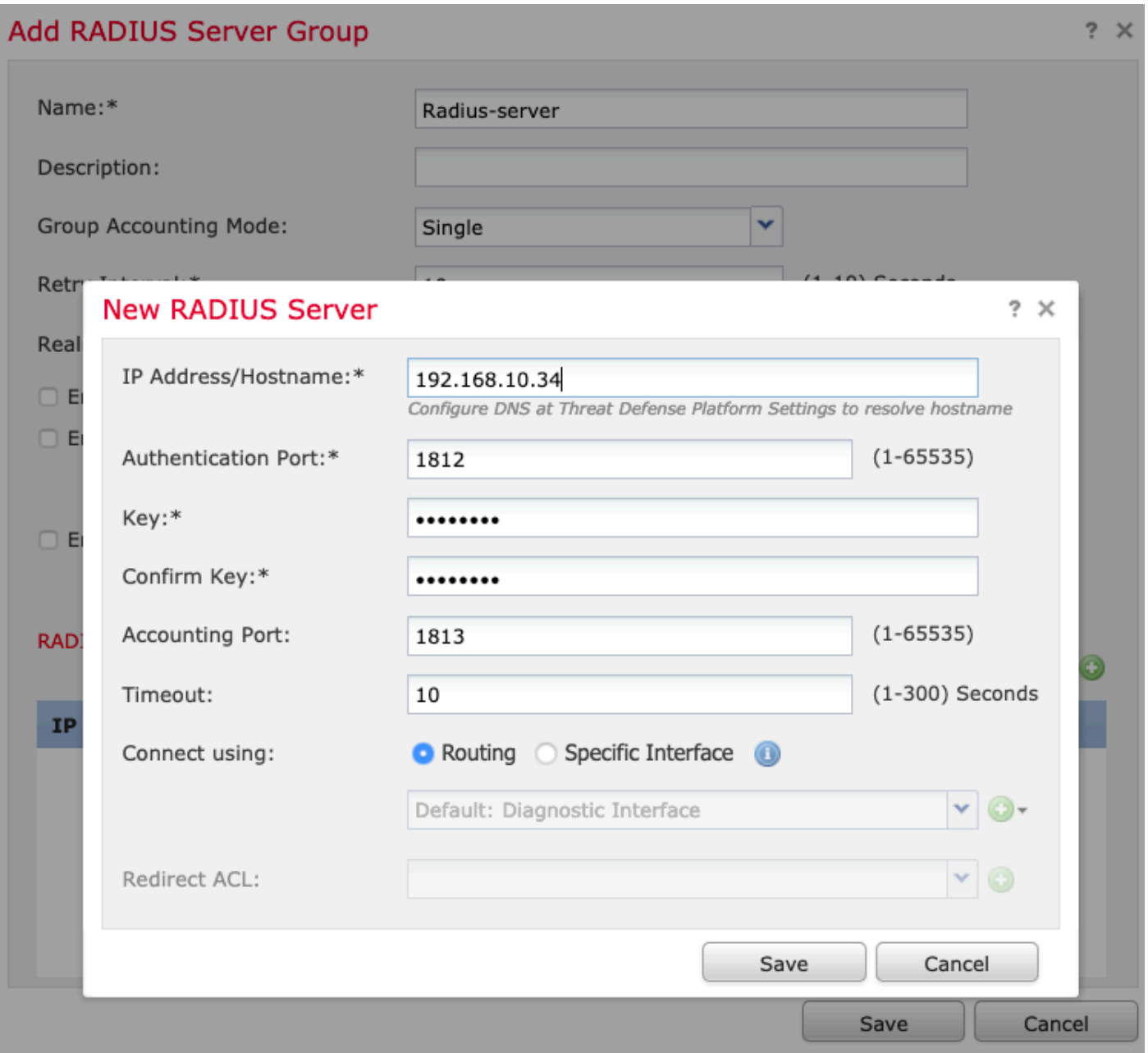
Enable dynamic authorization

Port:* (1024-65535)

RADIUS Servers (Maximum 16 servers) 

IP Address/Hostname	
No records to display	

2. 為Radius Server Group指定名稱，並將Radius伺服器IP地址與共用金鑰一起新增（需要共用金鑰才能將FTD與Radius伺服器配對），完成此表單後，選擇Save，如下圖所示。



3. RADIUS伺服器資訊現在在Radius伺服器清單中可用，如下圖所示。

Add RADIUS Server Group



Name:*

Description:

Group Accounting Mode: ▼

Retry Interval:* (1-10) Seconds

Realms: ▼

Enable authorize only

Enable interim account update

Interval:* (1-120) hours

Enable dynamic authorization

Port:* (1024-65535)

RADIUS Servers (Maximum 16 servers)



IP Address/Hostname

192.168.10.34



Save

Cancel

步驟 3. 建立IP池

1. 導航到對象 > 對象管理 > 地址池 > 新增IPv4池。
2. 指定IP地址的名稱和範圍，不需要Mask欄位，但可以指定該欄位，如下圖所示。

Add IPv4 Pool



Name*

IPv4 Address Range*
Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

Description

Allow Overrides

ⓘ Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

步驟 4. 建立XML配置檔案

1. 從Cisco.com下載配置檔案編輯器工具並運行應用程式。
2. 在「配置檔案編輯器」應用程式中，導航到伺服器清單，然後選擇新增，如下圖所示。

The screenshot shows the VPN configuration interface. On the left is a navigation menu with the following items: VPN, Preferences (Part 1), Preferences (Part 2), Backup Servers, Certificate Pinning, Certificate Matching, Certificate Enrollment, Mobile Policy, and Server List. The main area is titled 'Server List' and contains a table with the following columns: Hostname, Host Address, User Group, Backup Server List, SCEP, Mobile Settings, and Certificate Pins. Below the table, there is a note: 'Note: it is highly recommended that at least one server be defined in a profile.' To the right of the note are four buttons: 'Add...' (highlighted with a red box), 'Delete', 'Edit...', and 'Details'.

3. 指定顯示名稱、完全限定域名(FQDN)或IP地址，然後選擇OK，如下圖所示。

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required) Corporate - FTD (SSL)

FQDN or IP Address vpn.cisco.com / User Group ssl

Group URL

Connection Information

Primary Protocol SSL

ASA gateway

Auth Method During IKE Negotiation EAP-AnyConnect

IKE Identity (IOS gateway only)

Backup Servers

Host Address Add

Move Up

Move Down

Delete

OK Cancel

4.現在可在Server List選單中看到該條目：

VPN

- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Server List
Profile: Untitled

Hostname	Host Address	User Group	Backup Server ...	SCEP	Mobile Settings	Certificate Pins
Corporate - FTD (SSL)	vpn.cisco.com	ssl	-- Inherited --			

Note: it is highly recommended that at least one server be defined in a profile.

Add... Delete

Edit... Details

5.導覽至File > Save as。

注意：使用.xml副檔名儲存帶有易於識別名稱的配置檔案。

步驟 5.上傳Anyconnect XML配置檔案

1.在FMC中，導覽至Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File。

2.為對象指定名稱，然後按一下瀏覽，在本地系統中找到客戶端配置檔案，然後選擇儲存。

 注意：確保選擇Anyconnect Client Profile作為檔案型別。




Add AnyConnect File



Name:*	<input type="text" value="Corporate-profile(SSL)"/>
File Name:*	<input type="text" value="FTD-corp-ssl.xml"/> <input type="button" value="Browse.."/>
File Type:*	<input type="text" value="AnyConnect Client Profile"/> <input type="button" value="v"/>
Description:	<input type="text"/>

步驟 6.上傳AnyConnect映像

1.從思科下載網頁下載webdeploy(.pkg)映像。

AnyConnect Headend Deployment Package (Mac OS)	26-Jun-2019	51.22 MB	  
anyconnect-macos-4.7.04056-webdeploy-k9.pkg			

2.導航到Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File。

3.為Anyconnect軟體包檔案指定名稱，並在選擇檔案後從本地系統中選擇.pkg檔案。

4.選擇儲存。

Add AnyConnect File

Name:*

File Name:*

File Type:*

Description:

注意：您可以根據您的要求(Windows、Mac、Linux)上傳其他軟體包。

步驟 7.遠端訪問VPN嚮導

根據以上步驟，可以相應地執行遠端訪問嚮導。

1.導航至Devices > VPN > Remote Access。

2.分配遠端訪問策略的名稱，並從可用裝置中選擇FTD裝置。

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

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

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**

Available Devices	Selected Devices
<input type="text" value="Search"/> <input type="text" value="FTD-Virtual"/>	<input type="text" value="FTD-Virtual"/>

Before You Start

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

Authentication Server
Configure [Realm](#) or [RADIUS Server Group](#) 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.

3.指定連線配置檔名稱 (連線配置檔名稱是隧道組名稱) , 選擇Authentication Server和Address Pools , 如下圖所示。

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

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

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

Remote User AnyConnect Client Internet VPN Device (Outside/Inside) Corporate Resources AAA

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:*
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: (v)
Authentication Server:* (+) (Realm or RADIUS)
Authorization Server: (+) (RADIUS)
Accounting Server: (+) (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 (RADIUS only) (i)
 Use DHCP Servers
 Use IP Address Pools

IPv4 Address Pools: (pencil)
IPv6 Address Pools: (pencil)

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](#)

Back Next Cancel

4.選擇+符號以建立組策略。

Add 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

Save Cancel

5. (可選) 可以基於組策略配置本地IP地址池。如果未配置，則從連線配置檔案 (隧道組) 中配置的池繼承該池。

Add Group Policy



Name:* RemoteAccess-GP

Description:

General

AnyConnect

Advanced

VPN Protocols



IP Address Pools

Banner

DNS/WINS

Split Tunneling

IP Address Pools:

Name	IP Address Range	
vpn-pool	192.168.55.1-192.168.55.253	 

Save

Cancel

6.在此案例中，所有流量都透過通道路由，IPv4分割通道原則設定為允許所有流量透過通道，如下圖所示。

Edit Group Policy



Name: *

Description:

General AnyConnect Advanced

VPN Protocols
IP Address Pools
Banner
DNS/WINS
Split Tunneling

IPv4 Split Tunneling:

IPv6 Split Tunneling:

Split Tunnel Network List Type: Standard Access List Extended Access List

Standard Access List:

DNS Request Split Tunneling

DNS Requests:

Domain List:

Save Cancel

7. 選擇Anyconnect配置檔案的.xml配置檔案，然後選擇Save，如下圖所示。

Add Group Policy



Name:*

Description:

General

AnyConnect



Advanced

Profiles

SSL Settings

Connection Settings

AnyConnect profiles contains settings for the VPN client functionality and optional features. FTD deploys the profiles during AnyConnect client connection.

Client Profile:  

Standalone profile editor can be used to create a new or modify existing AnyConnect profile. You can download the profile editor from [Cisco Software Download Center](#).

Save

Cancel

8. 根據運行的系統要求選擇所需的AnyConnect映像，然後選擇Next（圖中所示）。

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy 2 System Help admin

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

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

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 checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	MAC4.7	anyconnect-macos-4.7.04056-webdeploy-k9....	Mac OS

Back Next Cancel

9.選擇Security Zone和DeviceCertificates:

- 此配置定義VPN終止的介面以及通過SSL連線提供的證書。

注意:在此案例中，FTD設定為不檢查任何VPN流量，並繞過存取控制原則(ACP)選項。

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

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

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

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

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.

Back Next Cancel

10.選擇Finish和Deploy更改：

- 與VPN、SSL證書和AnyConnect軟體包相關的所有配置均通過FMC部署進行推送，如下圖所示。

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

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

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

Remote Access VPN Policy Configuration

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

Name:	TAC
Device Targets:	FTD-Virtual
Connection Profile:	TAC
Connection Alias:	TAC
AAA:	
Authentication Method:	AAA Only
Authentication Server:	Radius-server
Authorization Server:	Radius-server
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	vpn-pool
Address Pools (IPv6):	-
Group Policy:	RemoteAccess-GP-SSL
AnyConnect Images:	MAC4.7
Interface Objects:	outside
Device Certificates:	Anyconnect-certificate

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.
- Network Interface Configuration**
Make sure to add interface from targeted devices to SecurityZone object 'outside'

Device Identity Certificate Enrollment

Certificate enrollment object 'Anyconnect-certificate' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the [Certificates](#) page to check the status of the installation.

Back Finish Cancel

NAT免除和發卡

步驟 1. NAT免除配置

NAT免除是一種首選轉換方法，用於在流量通過VPN隧道（遠端訪問或站點到站點）時防止將其路由到網際網路。

當來自內部網路的流量要流經隧道而不進行任何轉換時，就需要使用此功能。


1.導覽至對象>網路>新增網路>新增對象，如下圖所示。

New Network Object

? X

Name	<input type="text" value="vpn-pool"/>
Description	<input type="text"/>
Network	<input type="radio"/> Host <input type="radio"/> Range <input checked="" type="radio"/> Network <input type="radio"/> FQDN
	<input type="text" value="192.168.55.0/24"/>
Allow Overrides	<input type="checkbox"/>

2.導航到Device > NAT，選擇相關裝置使用的NAT策略，然後建立新語句。

 註：流量從內部流向外部。

Add NAT Rule

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

- calo-internal-outside
- inside-zone
- outside-zone
- outsideFW

Source Interface Objects (1):

Destination Interface Objects (1):

3.選擇FTD(原始來源和已轉換來源)背後的內部資源，以及目的地作為Anyconnect使用者的ip本地池(原始目的地和已轉換目的地)，如下圖所示。

4.確保切換選項（如圖所示），要在NAT規則中啟用「no-proxy-arp」和「route-lookup」，請選擇OK（如圖所示）。

5.這是NAT免除配置的結果。



上一節中使用的對象如下所述。

Name	<input type="text" value="FTDv-Inside-SUPERNE"/>
Description	<input type="text"/>
Network	<input type="radio"/> Host <input type="radio"/> Range <input checked="" type="radio"/> Network <input type="radio"/> FQDN
	<input type="text" value="10.124.0.0/16"/>
Allow Overrides	<input type="checkbox"/>

Name	<input type="text" value="vpn-pool"/>
Description	<input type="text"/>
Network	<input type="radio"/> Host <input type="radio"/> Range <input checked="" type="radio"/> Network <input type="radio"/> FQDN
	<input type="text" value="192.168.55.0/24"/>
Allow Overrides	<input type="checkbox"/>

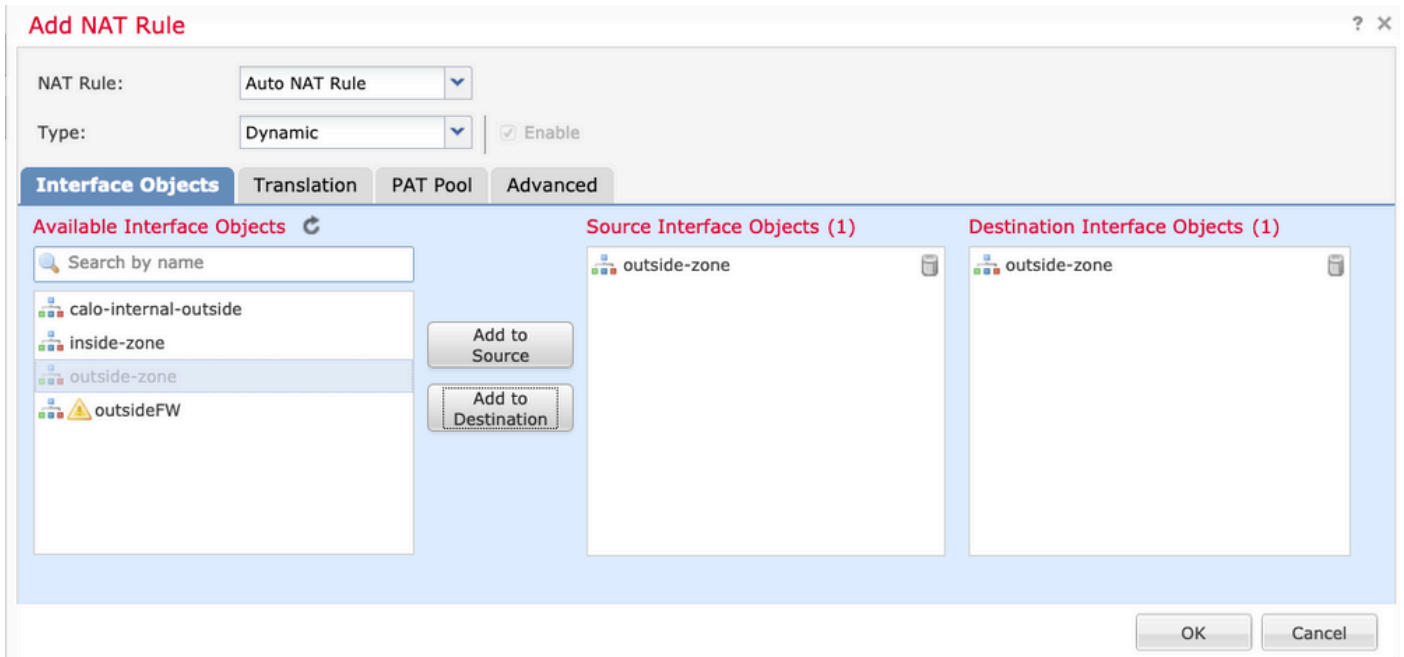
步驟 2. 髮夾配置

這也稱為U-turn，這是一種轉換方法，允許流量在接收流量的同一介面上流動。

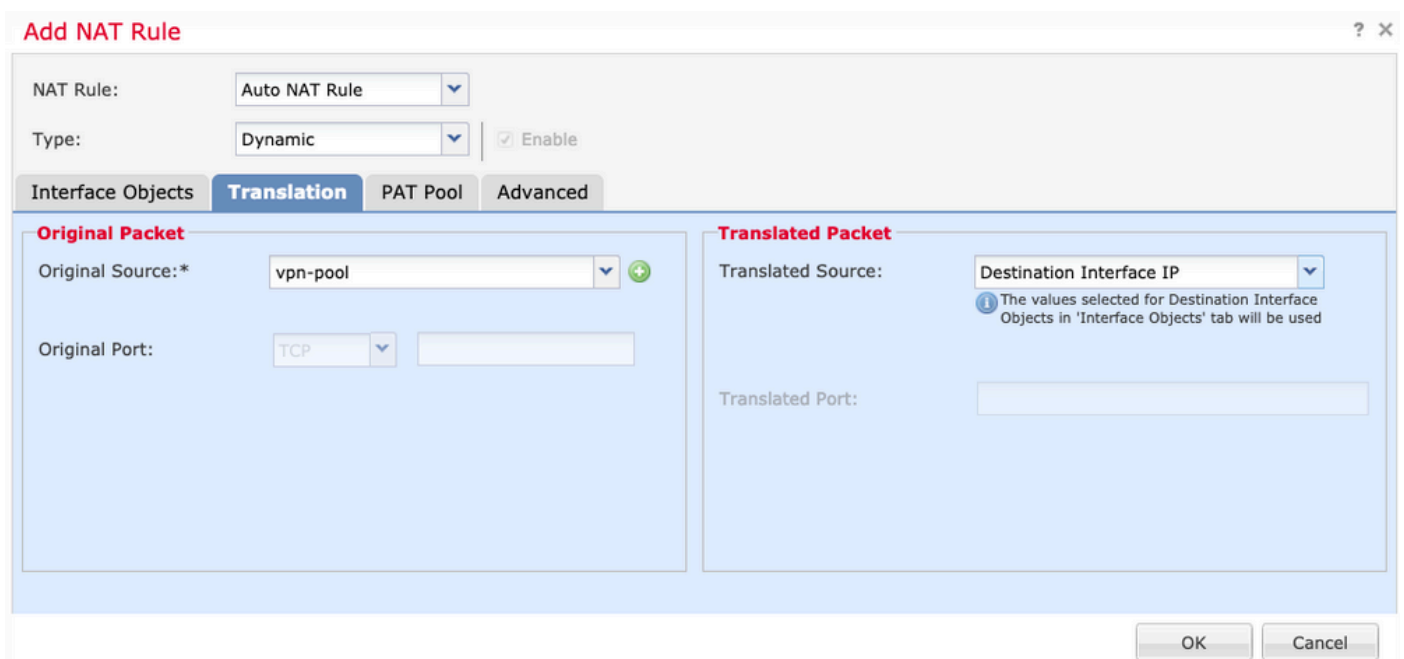
例如，當Anyconnect配置了Full tunnel split-tunnel策略時，根據NAT免除策略訪問內部資源。如果Anyconnect客戶端流量要到達網際網路上的外部站點，髮夾NAT（或U-turn）負責將流量從外部路由到外部。

在NAT配置之前必須建立VPN池對象。

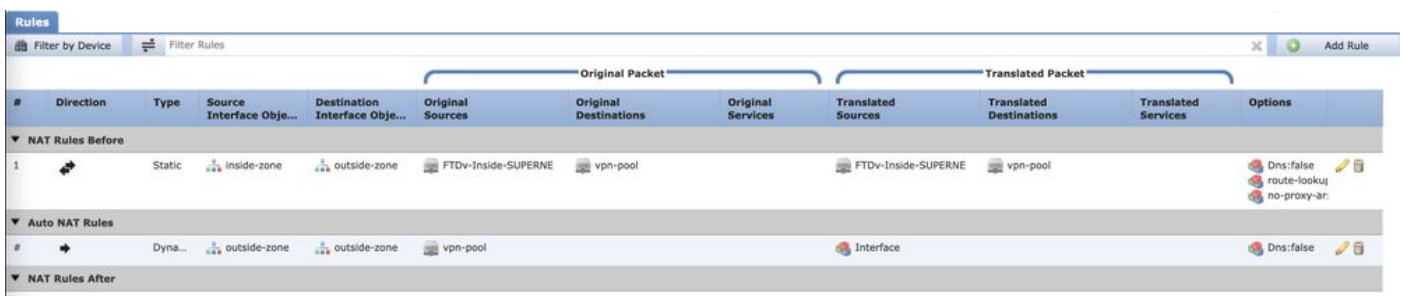
1. 建立新的NAT語句，在NAT Rule欄位中選擇自動NAT規則，然後選擇Dynamic作為NAT型別。
2. 為源介面對象和目標介面對象（外部）選擇相同的介面：



3.在「轉換」選項卡中，選擇vpn-pool對象作為原始源，然後選擇Destination Interface IP作為轉換源，選擇OK，如下圖所示。



4.這是NAT配置的摘要，如下圖所示。



5.按一下儲存並部署更改。

驗證

使用本節內容，確認您的組態是否正常運作。

在FTD命令列中運行這些命令。

- sh crypto ca certificates
- show running-config ip local pool
- show running-config webvpn
- show running-config tunnel-group
- show running-config group-policy
- show running-config ssl
- show running-config nat

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

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）。