

將Cisco ISE作為RADIUS伺服器與Windows Server 2012根CA在FTD上配置AnyConnect VPN

目錄

[目錄](#)

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[組態](#)

[從Windows Server匯出根CA證書](#)

[在員工Windows/Mac PC上安裝根CA證書](#)

[在FTD上產生CSR、取得Windows伺服器根CA簽名的CSR，然後在FTD上安裝已簽署的憑證](#)

[下載AnyConnect映像+ AnyConnect配置檔案編輯器並建立.xml配置檔案](#)

[設定FTD上的Anyconnect VPN \(使用根CA憑證 \)](#)

[配置FTD NAT規則以將VPN流量免於NAT，因為該VPN流量無論如何都將解密，並建立訪問控制策略/規則](#)

[新增FTD作為網路裝置並配置思科ISE上的策略集 \(使用RADIUS共用金鑰 \)](#)

[在員工Windows/Mac PC上使用AnyConnect VPN客戶端下載、安裝並連線到FTD](#)

[驗證](#)

[FTD](#)

[Cisco ISE](#)

[AnyConnect VPN客戶端](#)

[疑難排解](#)

[DNS](#)

[證書強度 \(用於瀏覽器相容性 \)](#)

[連線和防火牆配置](#)

目錄

簡介

本文說明如何使用Cisco ISE (身份服務引擎) 作為RADIUS伺服器在FTD (Firepower威脅防禦) 防火牆上配置AnyConnect VPN (虛擬專用網路)。我們使用Windows Server 2012作為我們的根CA (證書頒發機構)，以便通過VPN的通訊由證書保護，即員工PC將信任FTD的證書，因為FTD VPN證書已由Windows Server 2012根CA簽署

必要條件

需求

必須在網路中部署和運行以下內容：

- 部署了具有基本連線的Firepower管理中心和Firepower威脅防禦防火牆
- 在您的網路中部署和運行思科ISE
- 部署了Windows Server (具有Active Directory) ，並且員工的Windows/Mac PC已加入AD(Active Directory)域

在下面的示例中，員工將在其Windows/Mac PC上開啟AnyConnect客戶端，並使用其憑據通過VPN安全地連線到FTD的外部介面。FTD會根據Cisco ISE檢查其使用者名稱和密碼(Cisco ISE會檢查Windows Server Active Directory以驗證其使用者名稱、密碼和組，即只有AD組「Employees」中的使用者才能通過VPN進入公司網路。

採用元件

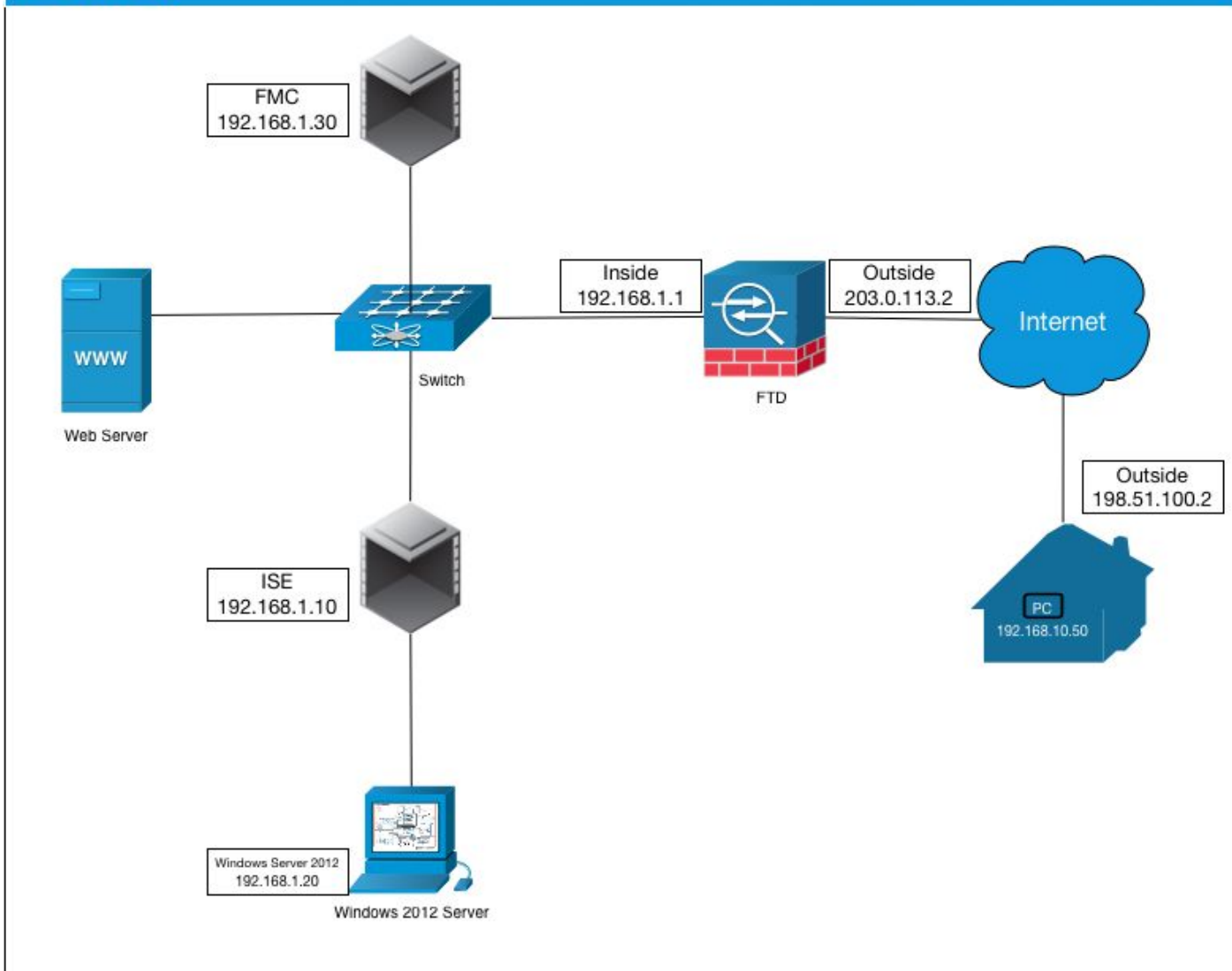
本檔案中的資訊是根據以下軟體版本：

- 運行6.2.3的Firepower管理中心和Firepower威脅防禦
- 執行2.4的思科身分識別服務引擎
- 執行4.6.0的Cisco AnyConnect安全行動化使用者03049
- 運行Active Directory和證書服務的Windows Server 2012 R2 (這是所有證書的根CA)
- Windows 7、Windows 10、Mac PC

設定

網路圖表

Topology



在此使用案例中，運行Anyconnect VPN客戶端的員工的Windows/Mac PC將連線到FTD防火牆的外部公共IP地址，並且Cisco ISE會在他們通過VPN連線後（取決於他們是Active Directory中的AD組的成員），動態授予他們對某些內部或網際網路資源（可配置）的有限或完全訪問許可權

裝置	主機名/FQDN	公用IP地址	專用IP地址	AnyConnect IP地址
Windows電腦	-	198.51.100.2	10.0.0.1	192.168.10.50
FTD	ciscofp3.cisco.com	203.0.113.2	192.168.1.1	-
FMC	-	-	192.168.1.30	-
Cisco ISE	ciscoise.cisco.com	-	192.168.1.10	-
Windows Server 2012 內部伺服器	ciscodc.cisco.com	-	192.168.1.20	-
			192.168.1.x	-

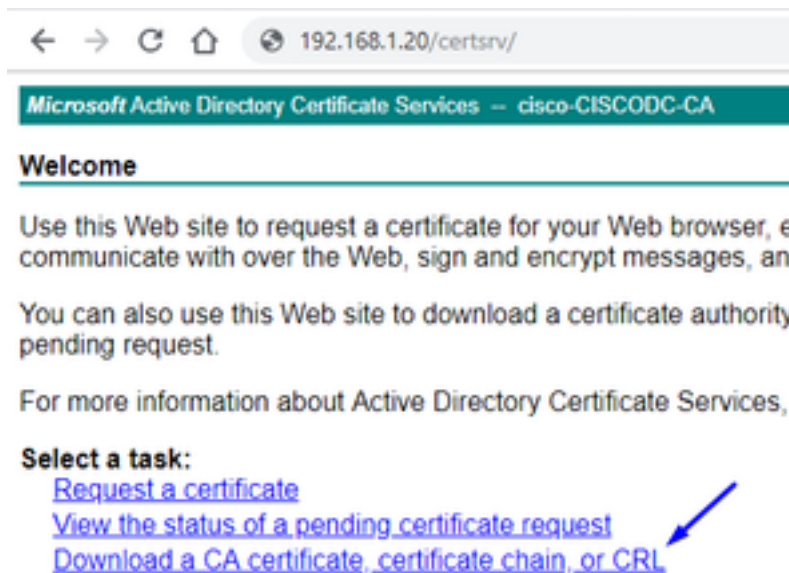
組態

從Windows Server匯出根CA證書

在本文檔中，我們將使用Microsoft Windows Server 2012作為證書的根CA。使用者端PC會信任此根CA通過VPN安全連線到FTD（請參閱以下步驟）。這樣可以確保使用者通過Internet安全連線到FTD，並從家中訪問內部資源。他們的PC將信任其瀏覽器和AnyConnect客戶端中的連線。

轉到<http://192.168.1.20/certsrv>，然後按照以下步驟下載您的Windows Server根CA證書：

按一下「Download a CA certificate , certificate chain , or CRL」



← → ↻ 🏠 192.168.1.20/certsrv/

Microsoft Active Directory Certificate Services – cisco-CISCODC-CA

Welcome

Use this Web site to request a certificate for your Web browser, e communicate with over the Web, sign and encrypt messages, an

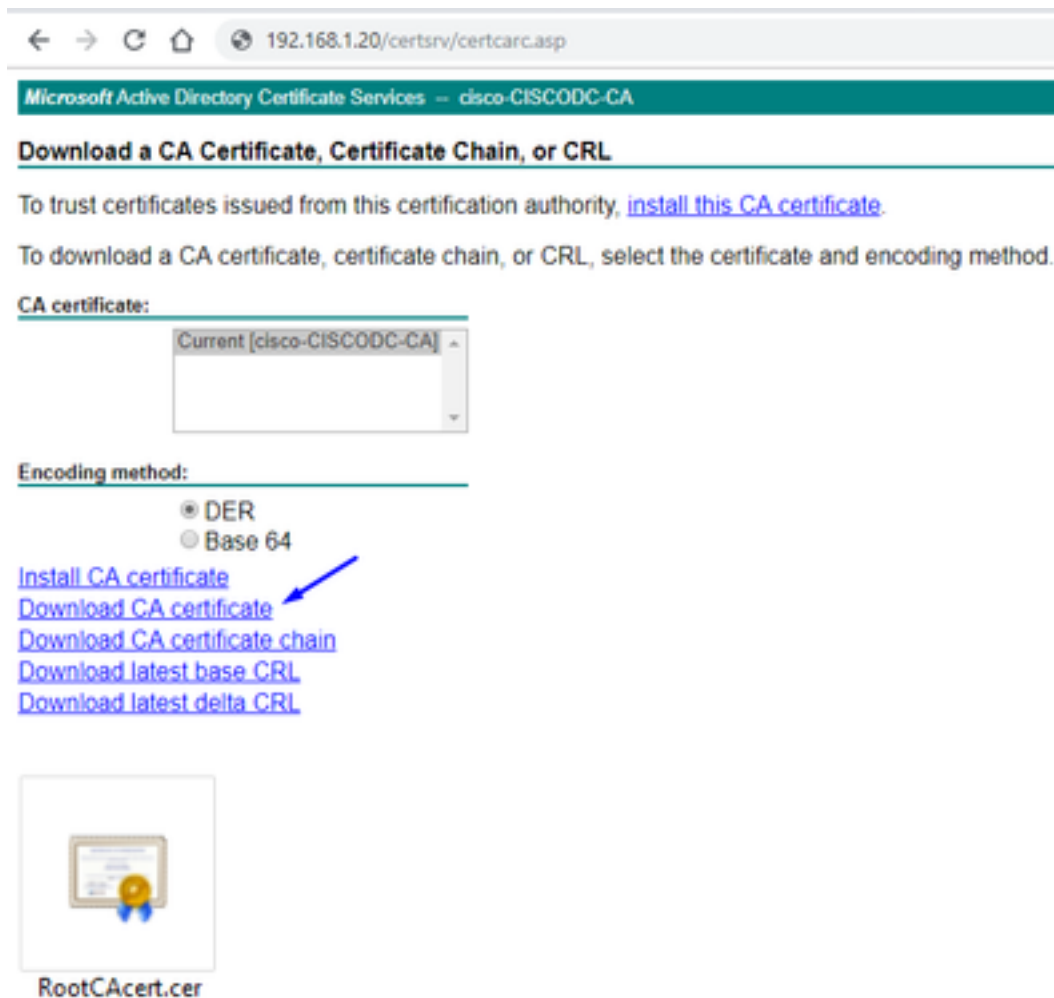
You can also use this Web site to download a certificate authority pending request.

For more information about Active Directory Certificate Services,

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

按一下Download Certificate , 並將其重新命名為「RootCAcert3.cer」



← → ↻ 🏠 192.168.1.20/certsrv/certcar.asp

Microsoft Active Directory Certificate Services – cisco-CISCODC-CA

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.


CA certificate:

Current [cisco-CISCODC-CA]

Encoding method:

- DER
- Base 64

- [Install CA certificate](#)
- [Download CA certificate](#)
- [Download CA certificate chain](#)
- [Download latest base CRL](#)
- [Download latest delta CRL](#)


RootCAcert.cer

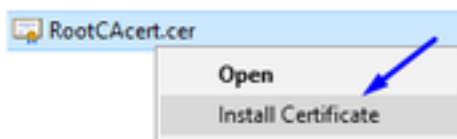
在員工Windows/Mac PC上安裝根CA證書

方法1:通過Windows Server組策略在所有員工PC上安裝證書 (對於超過10個VPN使用者的理想選擇) :

[如何使用組策略使用Windows Server向客戶端電腦分發證書](#)

方法2:通過在每台PC上單獨安裝證書，在所有員工PC上安裝證書（非常適合測試一個VPN使用者）：

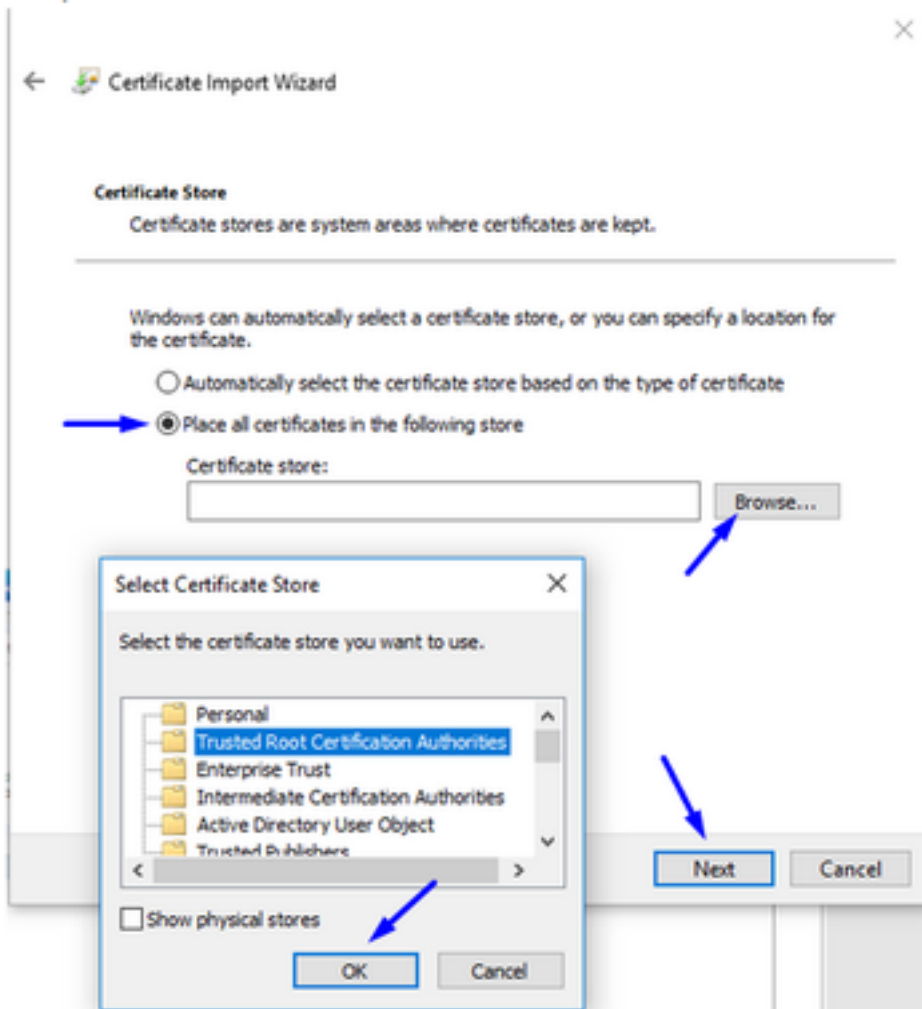
按一下右鍵員工的Windows/Mac PC上的證書，然後按一下Install Certificate



選擇「當前使用者」

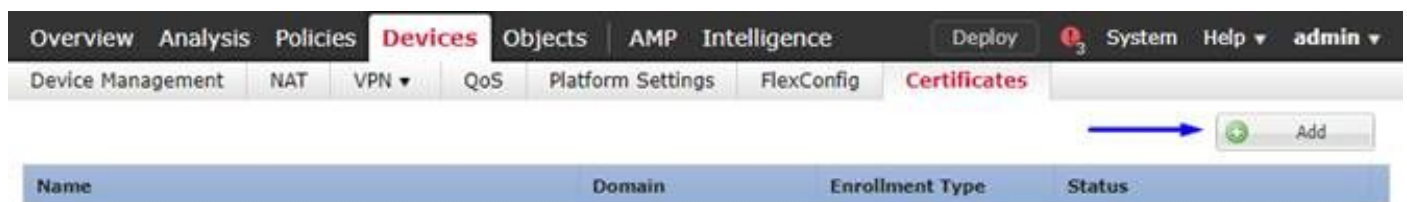


選擇將所有證書放入以下儲存，然後選擇Trusted Root Certification Authorities，按一下Ok，按一下Next，然後按一下Finish

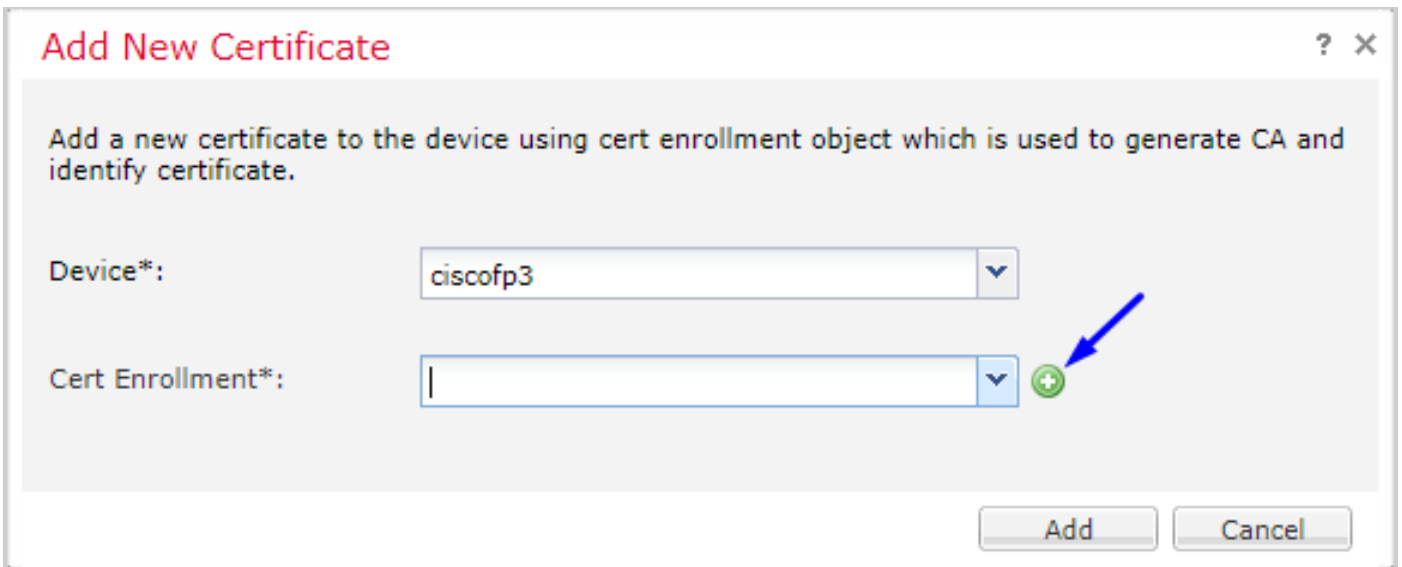


在FTD上產生CSR、取得Windows伺服器根CA簽名的CSR，然後在FTD上安裝已簽署的憑證

轉至Objects > Object Management > PKI > Cert Enrollment，按一下Add Cert Enrollment




按一下Add Cert Enrollment按鈕



Add New Certificate ? X

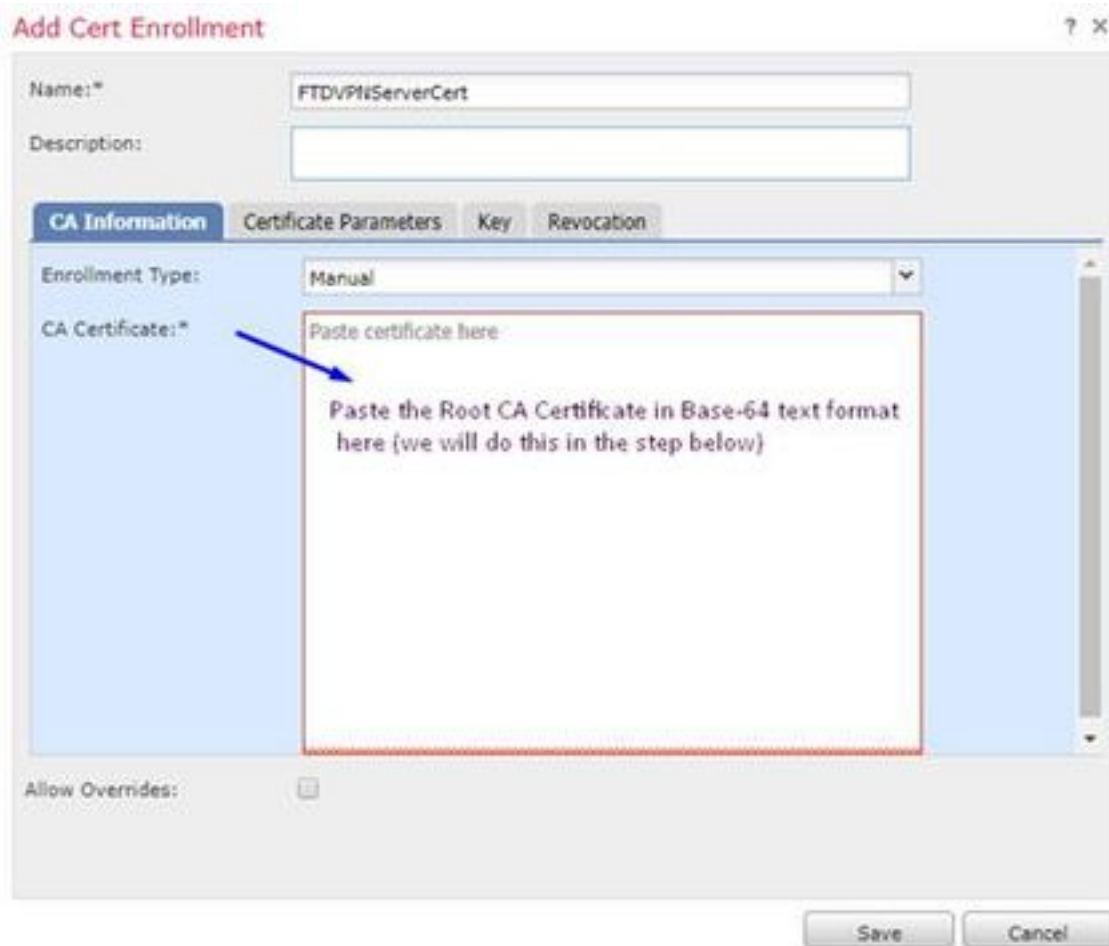
Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*: ▼

Cert Enrollment*: ▼ 

選擇 Enrollment Type > Manual

如下圖所示，我們需要將根CA證書貼上到此處：




Add Cert Enrollment ? X

Name:*

Description:

CA Information | Certificate Parameters | Key | Revocation

Enrollment Type: ▼

CA Certificate:* 
Paste the Root CA Certificate in Base-64 text format here (we will do this in the step below)

Allow Overrides:

以下是下載根CA憑證、以文字格式檢視並將其貼上到以上方塊中的方式：

轉到<http://192.168.1.20/certsrv>

按一下「Download a CA certificate , certificate chain , or CRL」

← → ↻ 🏠 192.168.1.20/certsrv/

Microsoft Active Directory Certificate Services – cisco-CISCODC-CA

Welcome

Use this Web site to request a certificate for your Web browser, e communicate with over the Web, sign and encrypt messages, an

You can also use this Web site to download a certificate authority pending request.

For more information about Active Directory Certificate Services,

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

按一下Base 64按鈕>按一下Download CA Certificate

← → ↻ 🏠 192.168.1.20/certsrv/certcarc.asp

Microsoft Active Directory Certificate Services – cisco-CISCODC-CA

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.


CA certificate:

Current [cisco-CISCODC-CA]

Encoding method:

- DER
- Base 64

- [Install CA certificate](#)
- [Download CA certificate](#)
- [Download CA certificate chain](#)
- [Download latest base CRL](#)
- [Download latest delta CRL](#)



RootCAcertBase64.cer

在記事本中開啟RootCAcertBase64.cer檔案

從以下Windows AD Server複製並貼上.cer內容（根CA證書）：

Add Cert Enrollment



Name:*

Description:

CA Information Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate:*

```
QqjzA0KCRWERA8iNZPnQWCWTDVk0PBRQDgJGDMR6GR10UEW
EB/wQFMAMBAf8wHQYD
VR00BBYEF0lpC7y9musCkmDJaKVus9bJUoMIMBAGCSsGAQQBg
jcVAQQDAgEBMCMG
CSsGAQQBgjcVAgQWBBQXIqPq2/dCT41fyYZHPxKhGEYNnzANBg
kqhkiG9w0BAQsF
AAOCAQEAOTa5S8Zw7RfarjTGm7HHJHZsA2p9CHdsvB/I35nYeqc
OnxyeTWFN7by6
C43uyBFTWTPu3LlJr1mCgEo72qJErJOoU/Y4y7ADAKJF8RtUIb4H
Zq13XNW7Tu9X
DbZCTeYL7INbzZxPyfcuZWIBk5I8uHRvqq2YkBdx6YUYJocNTshH
WwZIXYvQPwwc
yjHrFjm0/YIQIJMhyIVULXXxWGP7diLIEQ67aHsdz+UZq9JofVYa
heHBjzbzIF
zvN2WWFXQs3mFMUxkrjEyzNlDws6vrm6ZhqjvOupzmeC6YqByK
QIEAggjevemL7Zd
8DufTZQ4E4VQ9Kp4hrSdzuHSggDTuw==
-----END CERTIFICATE-----
```

Allow Overrides:

按一下**Certificate Parameters**頁籤>>鍵入您的證書資訊

附註：

自定義FQDN欄位必須是FTD的FQDN

「公用名稱」欄位必須是FTD的FQDN

Add Cert Enrollment

? X

Name:*

Description:

CA Information Certificate Parameters Key Revocation

Include FQDN:

Custom 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:

Save Cancel

提示：您可以從FTD CLI輸入以下命令，以取得FTD的FQDN:

```
> show network
===== [ System Information ] =====
Hostname : ciscofp3.cisco.com
Domains : cisco
DNS Servers : 192.168.1.20
Management port : 8305
IPv4 Default route
Gateway : 192.168.1.1

===== [ br1 ] =====
State : Enabled
Channels : Management & Events
Mode : Non-Autonegotiation
MDI/MDIX : Auto/MDIX
MTU : 1500
MAC Address : 00:0C:29:4F:AC:71
----- [ IPv4 ] -----
Configuration : Manual
Address : 192.168.1.2
Netmask : 255.255.255.0
```

按一下Key頁籤並鍵入任何Key Name

Add Cert Enrollment ? X

Name:*

Description:

CA Information Certificate Parameters **Key** Revocation

Key Type: RSA ECDSA

Key Name:*

Key Size:

Advanced Settings

Ignore IPsec Key Usage
Do not validate values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates.

Allow Overrides:

Save Cancel

按一下「Save」

選擇上面剛建立的FTDVPNServerCert，然後按一下Add

Add New Certificate ? X

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: FTDVPNServerCert

Enrollment Type: Manual

SCEP URL: NA

Add Cancel

提示：等待約10-30秒鐘，等待FMC + FTD驗證和安裝根CA證書（如果未顯示，請按一下「刷新」圖示）

← → ↻ 🏠 192.168.1.20/certsrv/certrqus.asp

Microsoft Active Directory Certificate Services – cisco-CISCODC-CA

Request a Certificate

Select the certificate type:
[User Certificate](#)

Or, submit an [advanced certificate request](#).

將您的證書簽名請求(CSR)貼上到下面的欄位，然後選擇Web Server作為證書模板

← → ↻ 🏠 192.168.1.20/certsrv/certrqxt.asp

Microsoft Active Directory Certificate Services – cisco-CISCODC-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
DbZCTeYL71MbzZxPyfcuZw18k518uHRvqq2Yk8.
y1HrFjm0/Y1IQI7jMhyIVULXXxMGP7diL1EQ67.
zvN2WwFXQs3mFMUxkrfEyzN1Dws6vrm6Zhaiv0.
8DufT2Q4E4VQ9Kp4hr5dzuH5ggDTuw==
-----END CERTIFICATE-----
```

Certificate Template:
Web Server

Additional Attributes:
Attributes:

Submit >


按一下Submit

按一下「Base 64 encoded」按鈕，然後按一下「Download certificate」

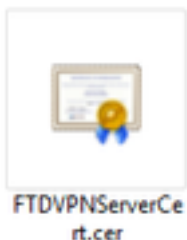
Certificate Issued

The certificate you requested was issued to you.

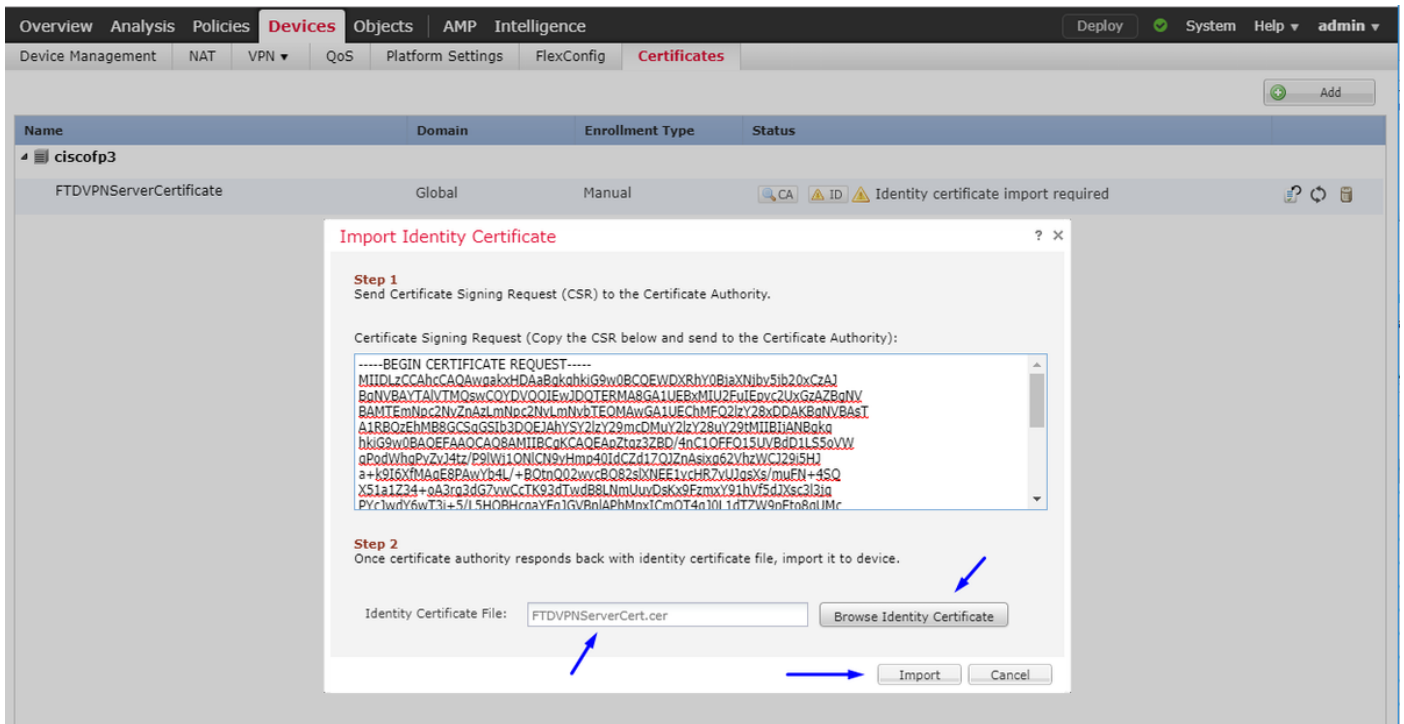
DER encoded or Base 64 encoded

 [Download certificate](#)

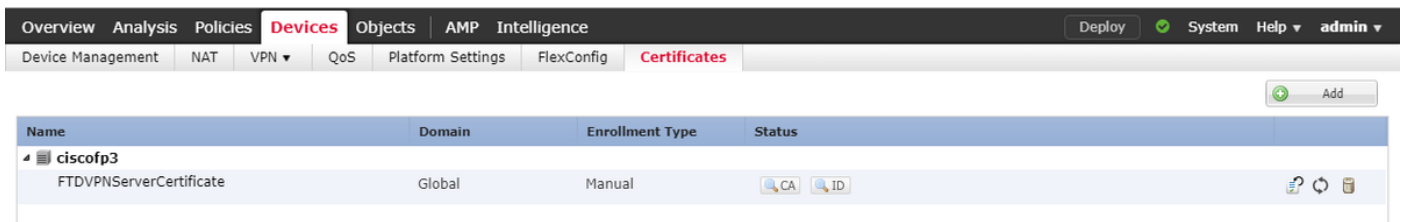
[Download certificate chain](#)



按一下 **Browse Identity Certificate**，然後選擇我們剛下載的證書



已成功安裝FTD VPN伺服器證書 (由Windows Server根CA簽名)



下載AnyConnect映像+ AnyConnect配置檔案編輯器並建立.xml配置檔案

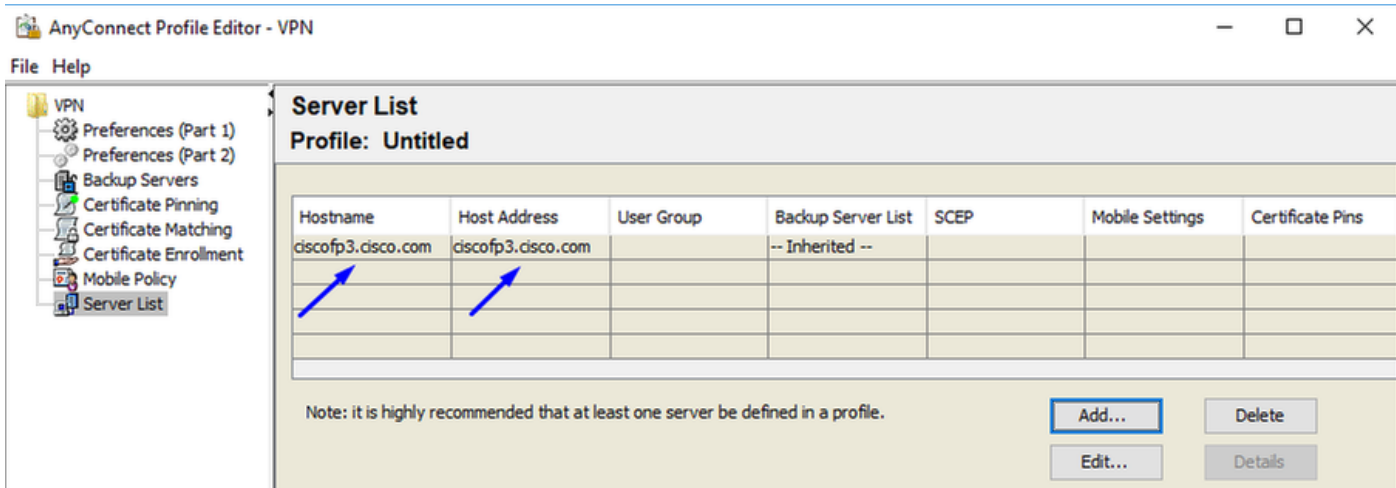
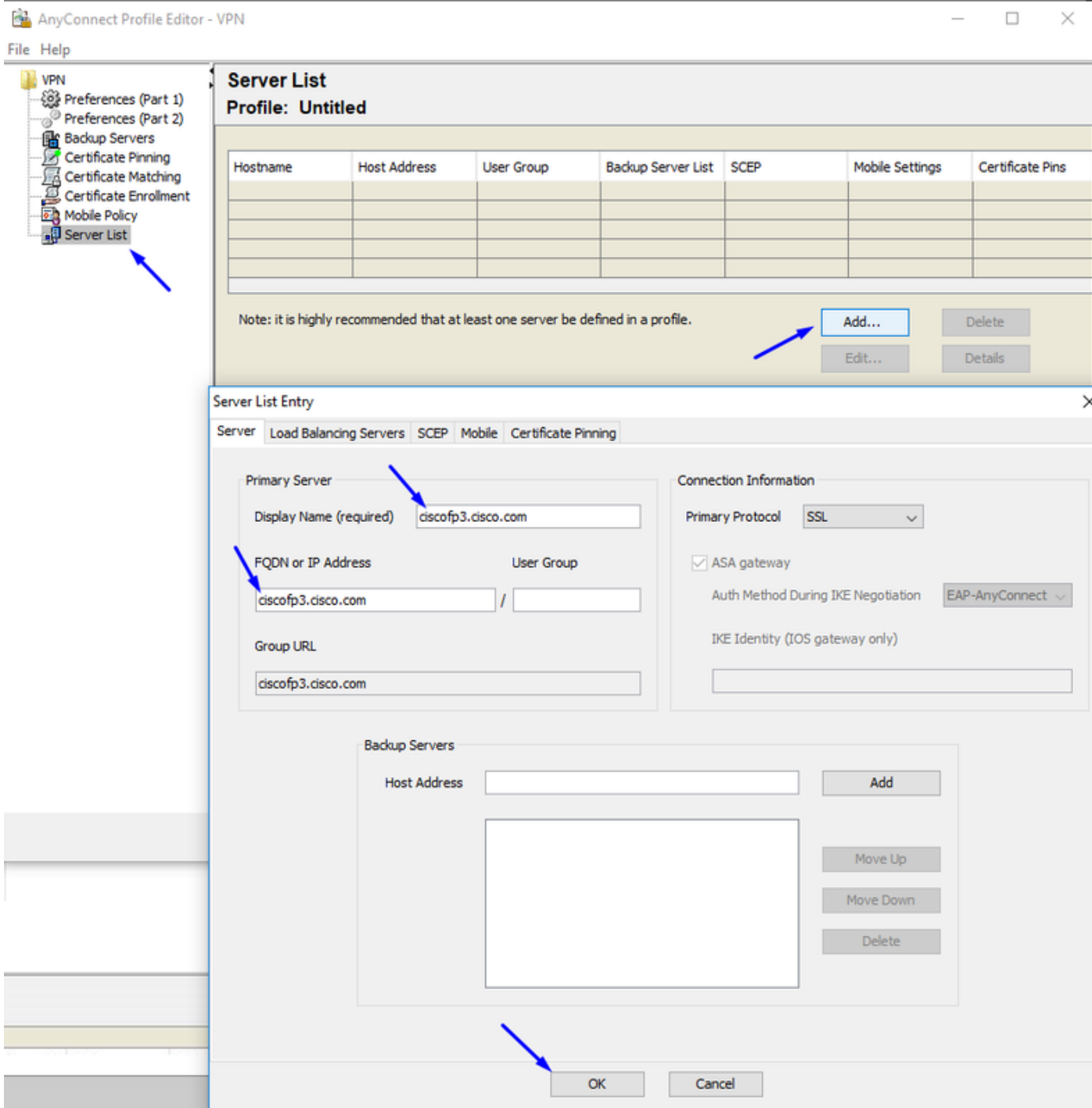
下載並安裝 [Cisco AnyConnect Profile Editor](#)



開啟AnyConnect配置檔案編輯器

按一下 **Server List >**；按一下 **Add...**

輸入 **顯示名稱** 和FTD的外部介面IP地址的 **FQDN**。您應該會看到伺服器清單中的條目



按一下「OK」和「File」>「Save as...」。

VPNprofile.xml

從此處下載Windows和Mac .pkg映像

AnyConnect Headend Deployment Package (Windows) 	20-SEP-2018	41.34 MB
anyconnect-win-4.6.03049-webdeploy-k9.pkg		
AnyConnect Headend Deployment Package (Mac OS) 	20-SEP-2018	41.13 MB
anyconnect-macos-4.6.03049-webdeploy-k9.pkg		

轉至Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File

Edit AnyConnect File ? x

Name: *

File Name: *

File Type: * ▾

Description:

Add AnyConnect File ? x

Name: *

File Name: *

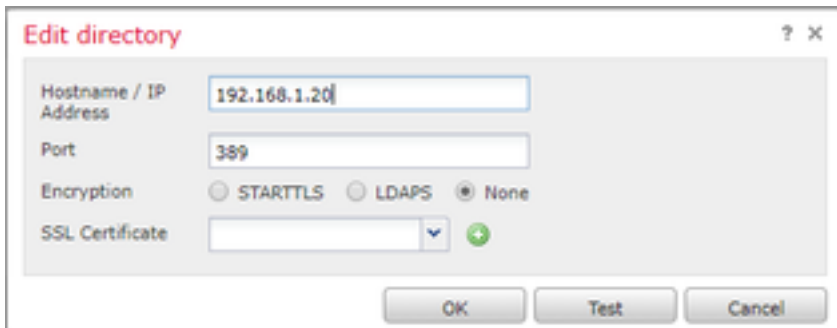
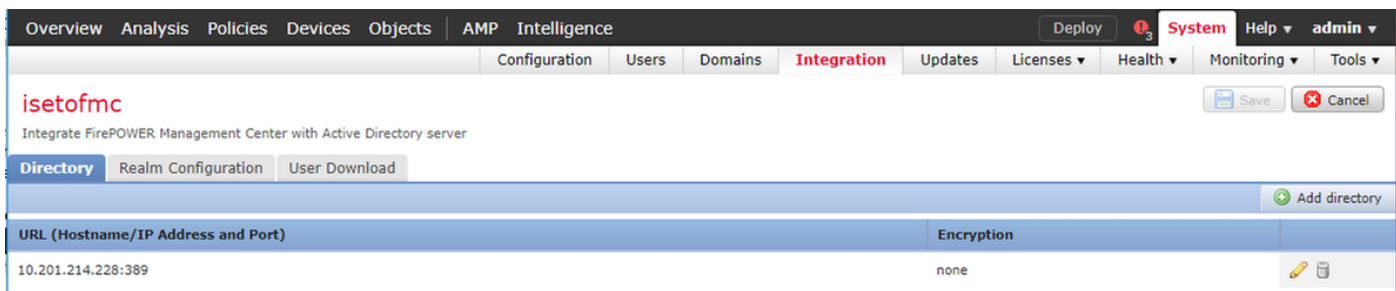
File Type: * ▾

Description:

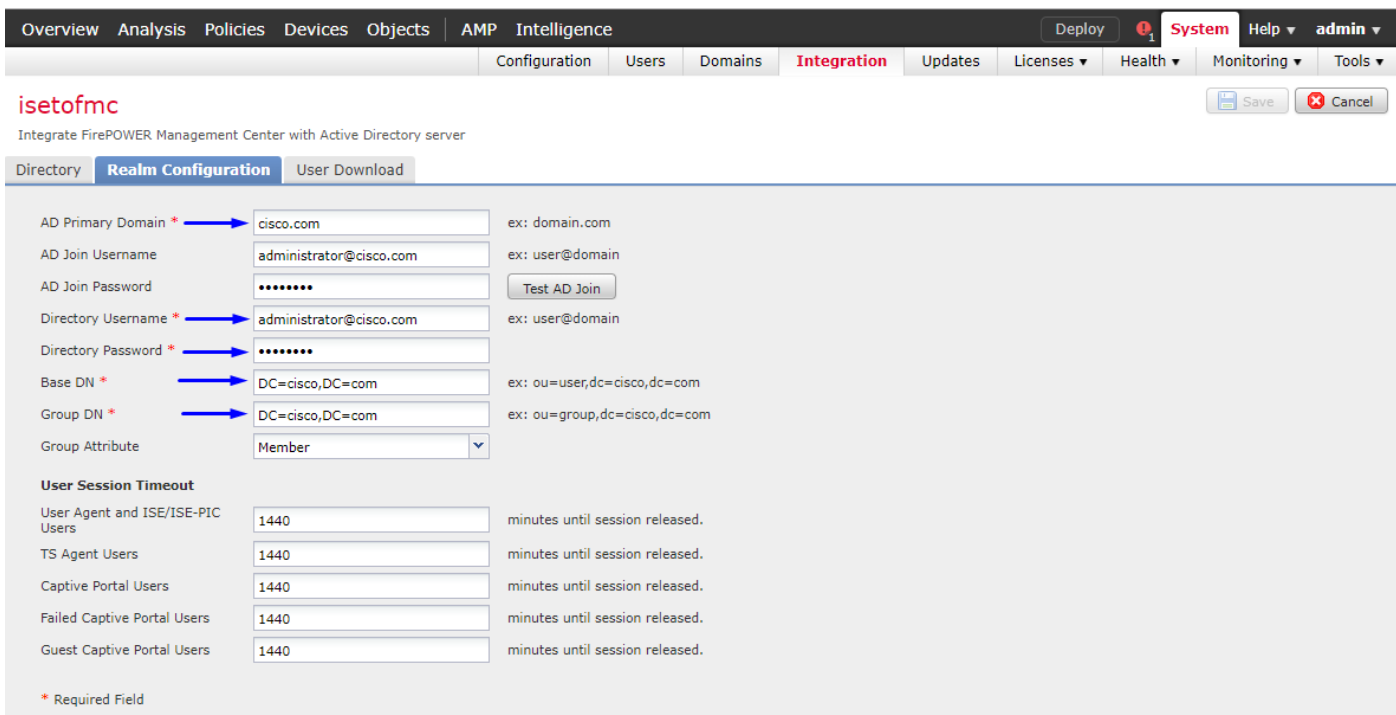
設定FTD上的Anyconnect VPN (使用根CA憑證)

登入到FirePOWER管理中心

按一下系統>整合> 領域>按一下 新建領域>>按一下 目錄頁籤>按一下新增目錄



按一下**Realm Configuration**頁籤 — 在此處配置域控制器資訊



附註：在上面的示例中，使用在Windows AD伺服器中具有「域管理」許可權的AD使用者名稱。如果要配置使用者，使其具有更具體的最小許可權，以使FMC加入您的領域配置的Active Directory域，您可以在這裡看到[步驟](#)

按一下**User Download**頁籤 — 確保使用者下載成功

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains **Integration** Updates Licenses Health Monitoring Tools

isetofmc
Integrate FirePOWER Management Center with Active Directory server

Directory Realm Configuration **User Download**

Download users and groups
Begin automatic download at 8 PM America/New York Repeat Every 24 Hours
Download Now

Available Groups

- Enterprise Admins
- Hyper-V Administrators
- Group Policy Creator Owners
- Guri-group2
- Cloneable Domain Controllers
- Distributed COM Users
- Allowed RODC Password Replication Group
- Cryptographic Operators
- Server Operators
- Remote Desktop Users
- WinRMRemoteWMIUsers_
- Users
- Administrators
- Windows Authorization Access Group
- Enterprise Read-only Domain Controllers
- Domain Admins
- Domain Users
- Pre-Windows 2000 Compatible Access
- Cert. Publishers

Groups to Include (0) Groups to Exclude (0)

Enter User Inclusion Add Enter User Exclusion Add

LDAP Download
Download users/groups from isetofmc
LDAP download successful: 51 groups, 25 users download

按一下「Devices」>「VPN」>「Remote Access」>按一下「Add」

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

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

Add

Name	Status	Last Modified
No configuration available Add a new configuration		

輸入Name、Description，然後按一下Add，以選擇要在其上設定Anyconnect VPN的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

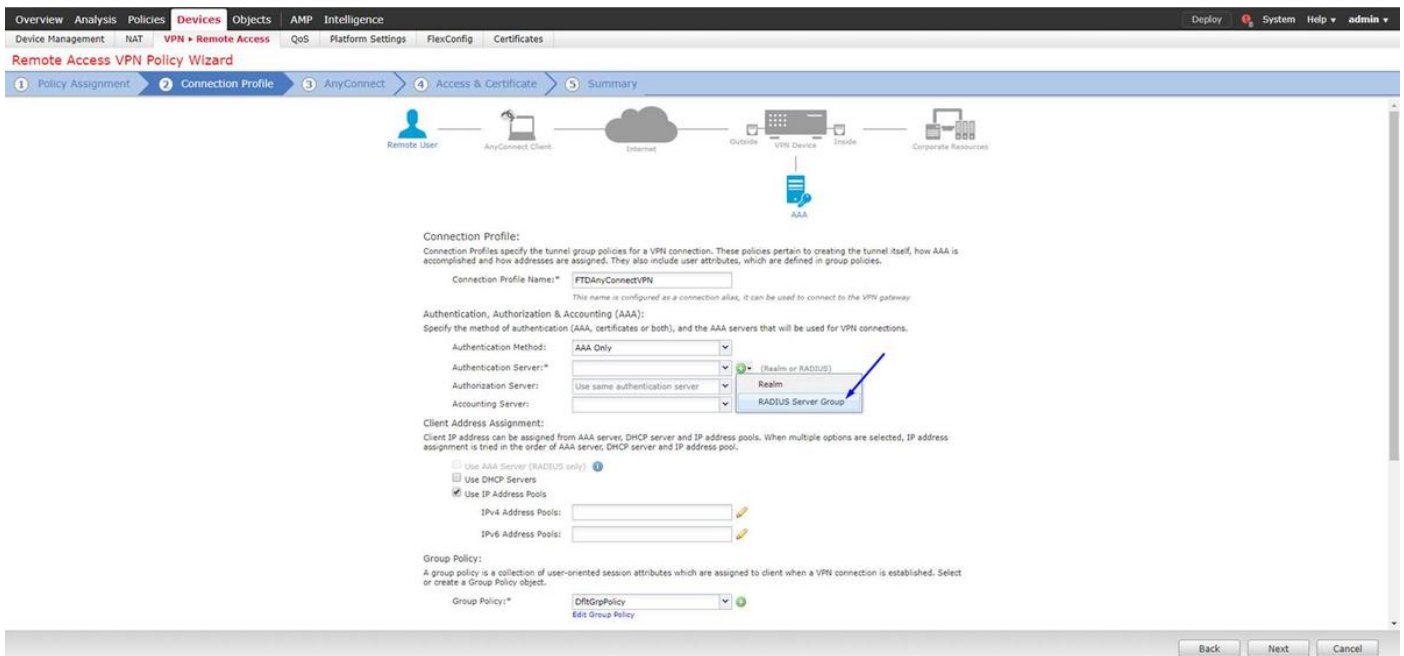
Targeted Devices and Protocols
This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:
Description:
VPN Protocols: SSL IPsec-IKEv2
Targeted Devices: Available Devices Selected Devices

Add

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.

點選Add以訪問身份驗證伺服器，然後選擇RADIUS Server Group — 這將是您的思科身份服務引擎 PSN (策略服務節點)



輸入RADIUS伺服器的名稱
 選擇上面配置的您的領域
 按一下「Add」

Add RADIUS Server Group

Name: CiscoISE

Description: Cisco ISE (Joined to Windows AD Server)

Group Accounting Mode: Single

Retry Interval: 10 (1-10) Seconds

Realms: isetofmc

Enable authorize only

Enable interim account update
Interval: 24 (1-120) hours

Enable dynamic authorization
Port: 1700 (1024-65535)

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname
No records to display

Save Cancel

為思科ISE節點鍵入以下資訊：

IP地址/主機名:思科ISE PSN (策略服務節點) 的IP地址 — 這是身份驗證請求將到達的地方

主要:cisco123

確認金鑰:cisco123

注意：上面是您的RADIUS共用金鑰 — 我們將在後續步驟中使用此金鑰

Edit RADIUS Server ? X

IP Address/Hostname:* 192.168.1.10
Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* 1812 (1-65535)

Key:* *****

Confirm Key:* *****

Accounting Port: 1813 (1-65535)

Timeout: 10 (1-300) Seconds

Connect using: Routing Specific Interface ⓘ

Redirect ACL:

Save Cancel

附註：當終端使用者嘗試透過AnyConnect VPN連線到FTD時，他們輸入的使用者名稱+密碼將會作為驗證要求傳送到此FTD。FTD會將該請求轉送到思科ISE PSN節點進行身份驗證（然後，思科ISE會檢查Windows Active Directory的使用者名稱和密碼，並根據我們當前在思科ISE中配置的條件實施訪問控制/網路訪問）

Add RADIUS Server Group ? X

Name:* CiscoISE

Description: Cisco ISE (joined to Windows AD server)

Group Accounting Mode: Single

Retry Interval:* 10 (1-10) Seconds

Realms: isetofmd

Enable authorize only

Enable interim account update
Interval:* 24 (1-120) hours

Enable dynamic authorization
Port:* 1700 (1024-65535)

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname
192.168.1.10

Save Cancel

按一下「Save」

按一下Edit for IPv4 Address Pool

Overview Analysis Policies **Devices** Objects AMP Intelligence

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 & Certify 5 Summary

Remote User AnyConnect Client Internet VPN Device 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:

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) ⓘ

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:

IPv6 Address Pools:

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

Last login on Wednesday, 2018-10-10 at 10:30:14 AM from 10.152.21.157

How-To Cisco

按一下「Add」

Address Pools

Available IPv4 Pools

Add

Selected IPv4 Pools

Add

OK Cancel

輸入名稱、IPv4地址範圍和子網掩碼

Add IPv4 Pool

? X

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

Override (0)

Save

Cancel

選擇您的IP地址池，然後按一下Ok (確定)

Address Pools

? X

Available IPv4 Pools

Search

Inside-Pool
IPv4

Selected IPv4 Pools

Inside-Pool
IPv4

Inside-Pool
192.168.10.50-192.168.10.250

Add

OK

Cancel

按一下編輯組策略

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy

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

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: (RADIUS)

Authentication Server: * (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) ⓘ

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: ⓘ

IPv6 Address Pools: ⓘ

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](#)

按一下Anyconnect頁籤 > Profiles > 按一下Add

Edit Group Policy

Name: *

Description:

General **AnyConnect** Advanced

Profiles

SSL Settings

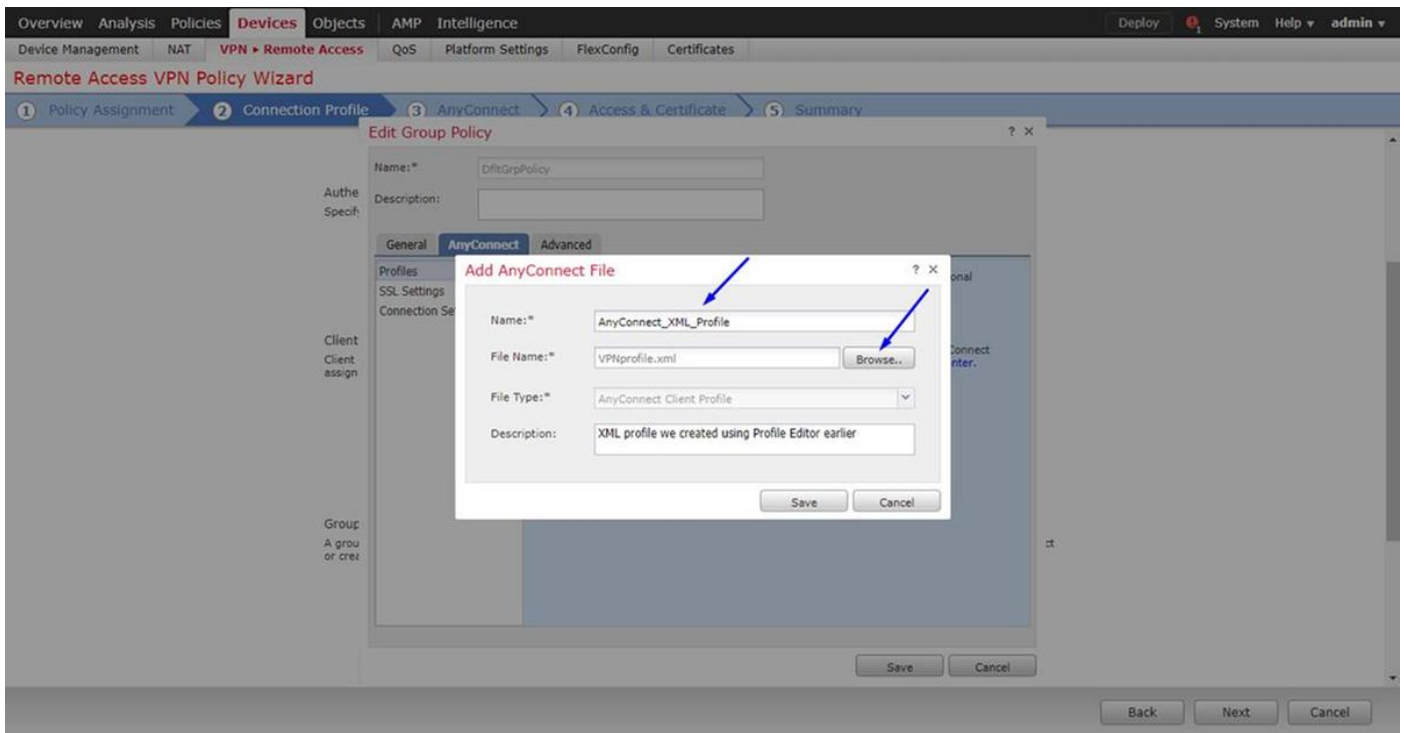
Connection Settings

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

Client Profile: ⓘ

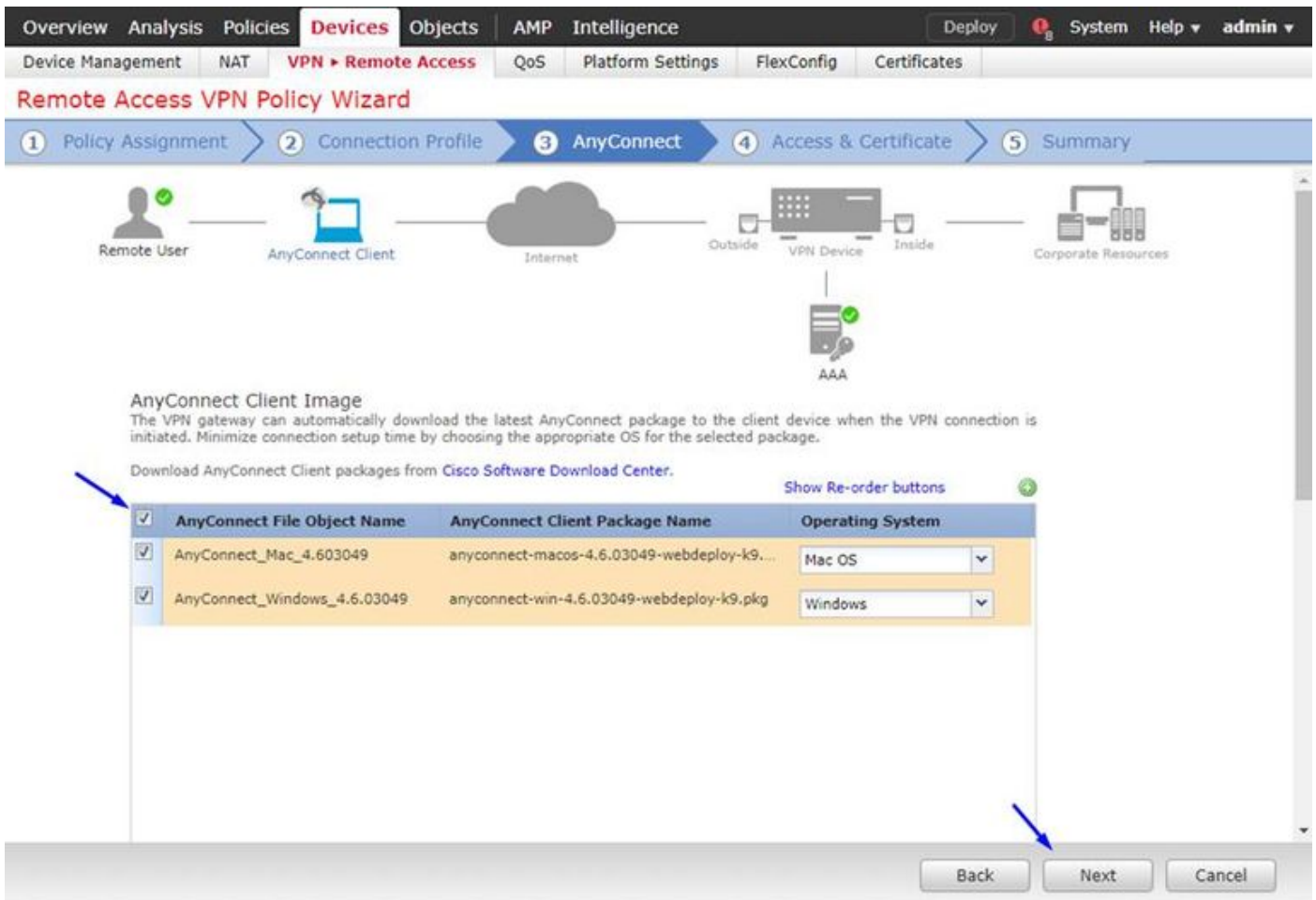
Standalone profile editor can be used to create a new or modify existing Anyconnect profile. You can download the profile editor from [Cisco Software Download Center](#).

鍵入Name並按一下Browse...並從上述步驟4中選擇您的VPNprofile.xml檔案



按一下**Save**，然後按一下**Next**

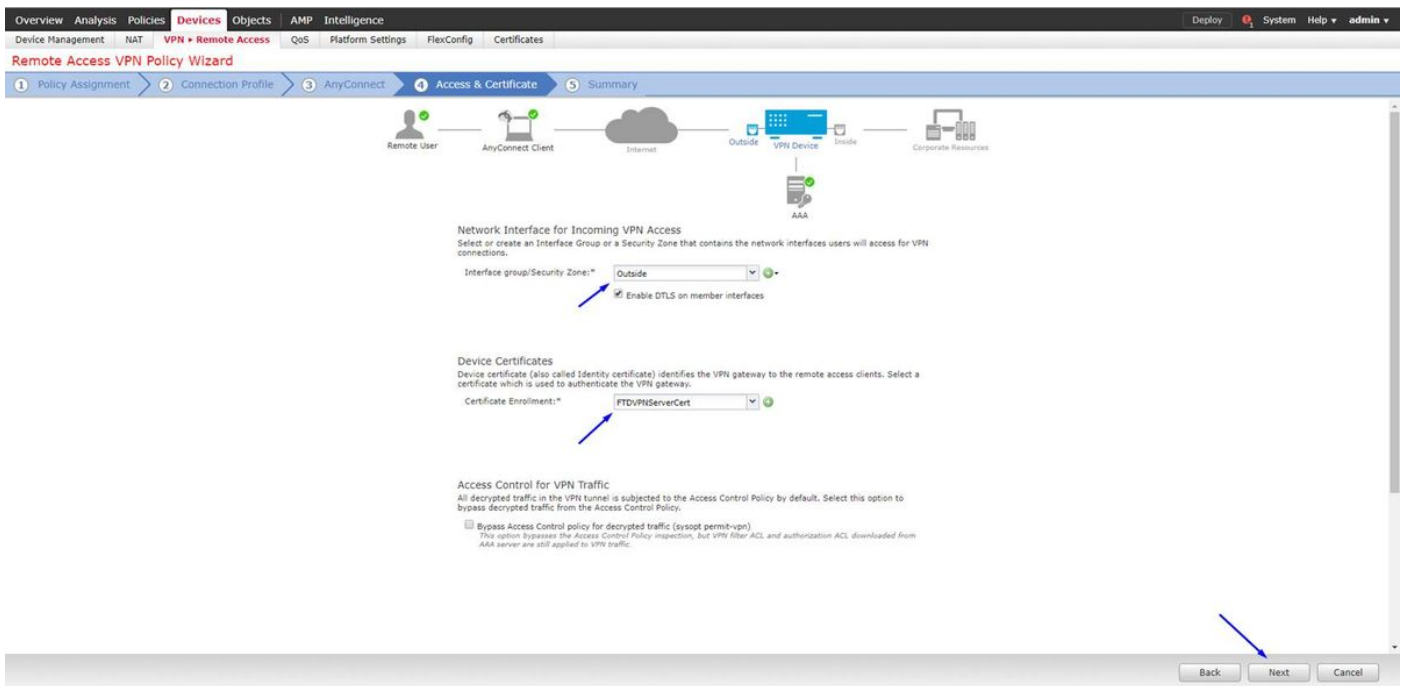
從上述步驟4中選擇您的AnyConnect Windows/Mac檔案的覈取方塊



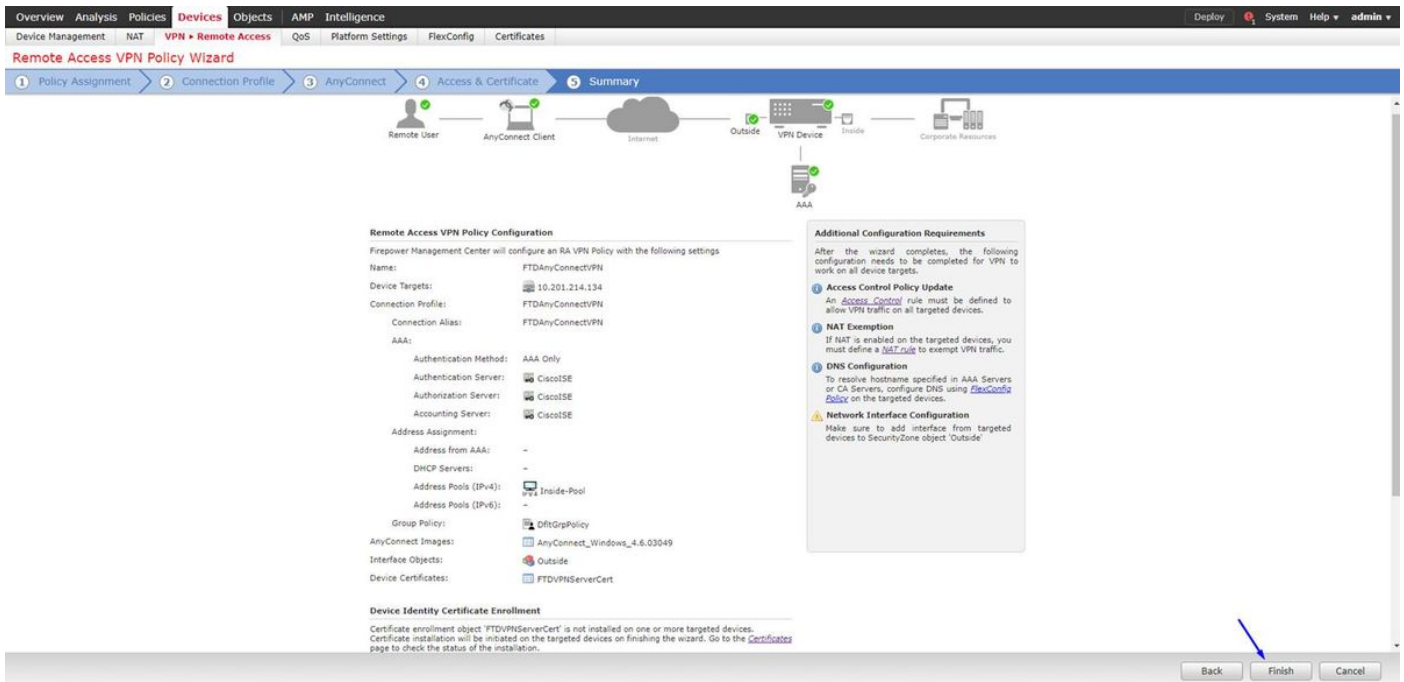
按一下**下一步**

選擇Interface Group/Security Zone作為**Outside**

選擇**Certificate Enrollment**，作為我們在上述步驟3中建立的證書



檢查您的配置，然後按一下下一步



配置FTD NAT規則以將VPN流量免於NAT，因為該VPN流量無論如何都將解密，並建立訪問控制策略/規則

建立靜態NAT規則以確保VPN流量未獲得NAT'd(FTD在進入Outside介面時已解密AnyConnect資料包，因此該PC已經位於內部介面之後，並且它們已經具有私有IP地址 — 我們仍需要為該VPN流量配置NAT免除 (無NAT) 規則):

轉到Objects >按一下Add Network >按一下Add Object

Edit Network Objects



Name:

Description:

Network:
Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

Edit Network Objects



Name:

Description:

Network:
Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
1		Static	Inside	Outside	inside-subnet	outside-subnet-anyconnect-pool		inside-subnet	outside-subnet-anyconnect-pool		Dns: false route-lookup no-proxy-arp
#		Dynamic	Inside	Outside	inside-subnet		Interface				Dns: false

此外，您還必須在使用者VPN進入後允許資料流量。有兩種選擇：

a. 建立允許或拒絕規則以允許或拒絕VPN使用者訪問某些資源

b. 啟用「為已解密流量繞過存取控制原則」— 這允許任何能夠透過VPN略過ACL成功連線到FTD並存取FTD後方的任何內容，而無需通過存取控制原則中的「允許」或「拒絕」規則

在以下位置為已解密的流量啟用旁路訪問控制策略：**裝置 > VPN > 遠端存取 > VPN配置檔案 > 存取介面：**

Access Control for VPN Traffic

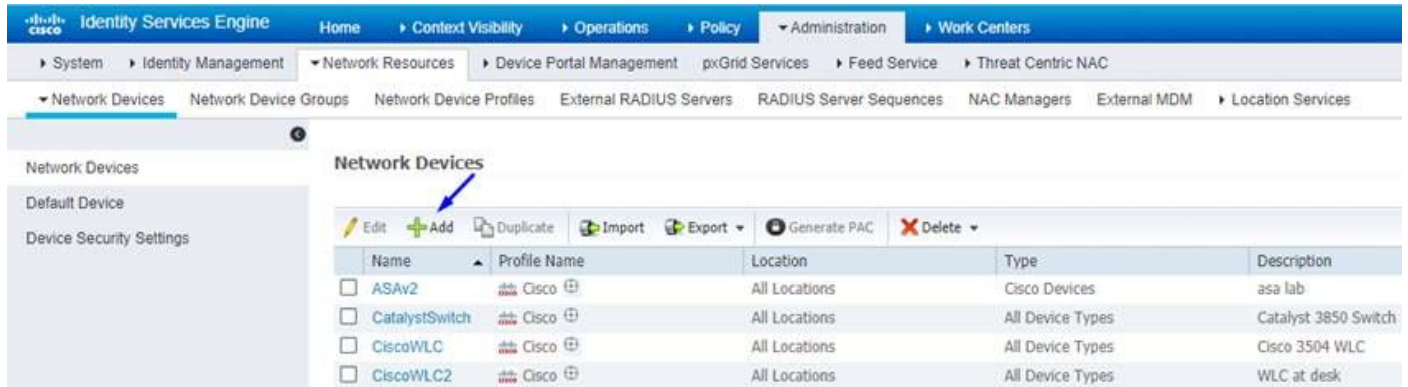
- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

附註：如果未啟用此選項，則需要轉到Policies > Access Control Policy，並建立Allow規則，以便VPN使用者能夠訪問內部或dmz後面的內容

按一下FirePOWER管理中心右上角的「部署」

新增FTD作為網路裝置並配置思科ISE上的策略集（使用RADIUS共用金鑰）

登入到Cisco Identity Services Engine，然後點選Administration > Network Devices > 點選Add



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Under Administration, the 'Network Devices' section is selected. The main content area displays a table of network devices with columns for Name, Profile Name, Location, Type, and Description. The 'Add' button is highlighted with a blue arrow.

Name	Profile Name	Location	Type	Description
ASAv2	Cisco	All Locations	Cisco Devices	asa lab
CatalystSwitch	Cisco	All Locations	All Device Types	Catalyst 3850 Switch
CiscoWLC	Cisco	All Locations	All Device Types	Cisco 3504 WLC
CiscoWLC2	Cisco	All Locations	All Device Types	WLC at desk

按上述步驟輸入名稱、輸入FTD的IP位址，然後輸入RADIUS共用密碼

注意：此地址必須是FTD可以到達您的思科ISE（RADIUS伺服器）的介面/IP地址，即您的思科ISE可以通過FTD到達的FTD介面

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM

Network Devices List > FTDVPN

Network Devices

Default Device

Device Security Settings

* Name

Description

IP Address * IP: /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

* Shared Secret

Use Second Shared Secret

CoA Port

RADIUS DTLS Settings

DTLS Required

Shared Secret

CoA Port

按一下Policy > Policy Set > 為以下型別的任何身份驗證請求建立Policy Set:
Radius-NAS-Port-Type EQUALS Virtual
 這意味著，如果任何進入ISE的RADIUS請求看起來像VPN連線，它們將訪問此策略集

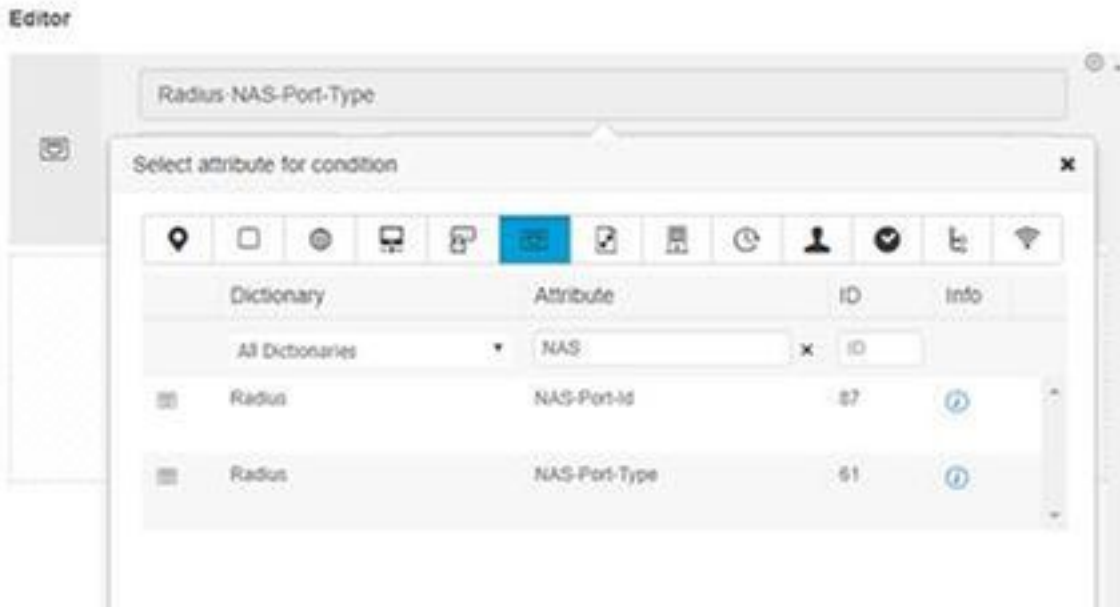
Identity Services Engine Administration Work Centers License Warning

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets

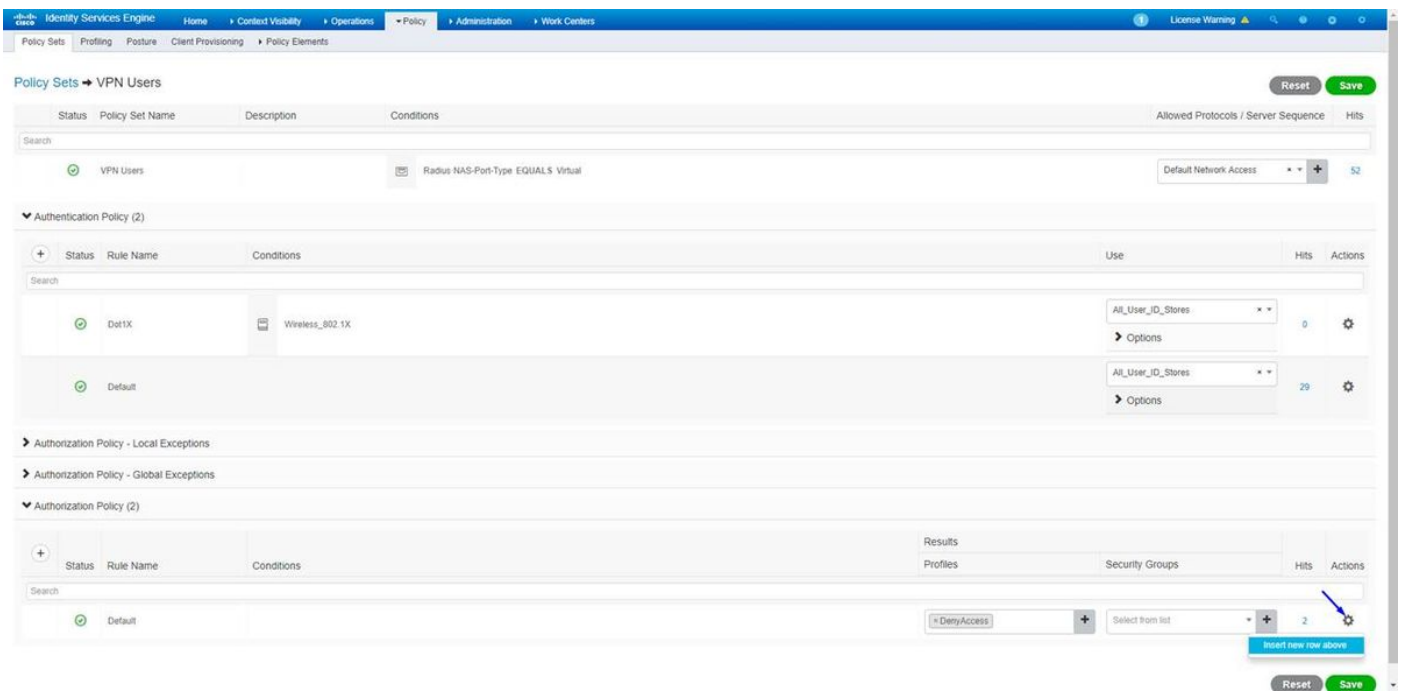
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<input checked="" type="checkbox"/>	QuestSSID		Airspace Airspace-Wan-Id EQUALS 1	Default Network Access	181	<input type="button" value="+"/> <input type="button" value="x"/>	<input type="button" value="i"/> <input type="button" value="x"/>
<input checked="" type="checkbox"/>	EmployeeSSID		Airspace Airspace-Wan-Id EQUALS 2	Default Network Access	686	<input type="button" value="+"/> <input type="button" value="x"/>	<input type="button" value="i"/> <input type="button" value="x"/>
<input checked="" type="checkbox"/>	123 Users		Radius-NAS-Port-Type EQUALS Virtual	Default Network Access		<input type="button" value="+"/> <input type="button" value="x"/>	<input type="button" value="i"/> <input type="button" value="x"/>
<input checked="" type="checkbox"/>	Default	Default policy set		Default Network Access	1300	<input type="button" value="+"/> <input type="button" value="x"/>	<input type="button" value="i"/> <input type="button" value="x"/>

您可以在以下位置找到思科ISE中的條件：



編輯上面創建的策略集

在預設阻止規則之上新增規則，僅在人員位於名為「Employees」的Active Directory組中時才為其提供「Permit Access」授權配置檔案：



下面是完成規則後的外觀

The screenshot displays the Cisco ISE Policy Sets configuration interface. At the top, the navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The main heading is 'Policy Sets → VPN Users'. Below this, there are sections for 'Authentication Policy (2)' and 'Authorization Policy (2)'. The 'Authentication Policy' table lists rules like 'Dot1X' and 'Default'. The 'Authorization Policy' table lists rules like 'Allow FTD VPN connections if AD Group VPNUsers' and 'Default'. Two blue arrows point to the 'Conditions' column of the 'Allow FTD VPN connections if AD Group VPNUsers' rule and the 'PermitAccess' action in the 'Results' column.

在員工Windows/Mac PC上使用AnyConnect VPN客戶端下載、安裝並連線到FTD

在員工Windows/Mac PC上開啟瀏覽器，在瀏覽器中轉到FTD的外部地址

← → ↻ <https://cisconfp3.cisco.com>

鍵入您的Active Directory使用者名稱和密碼

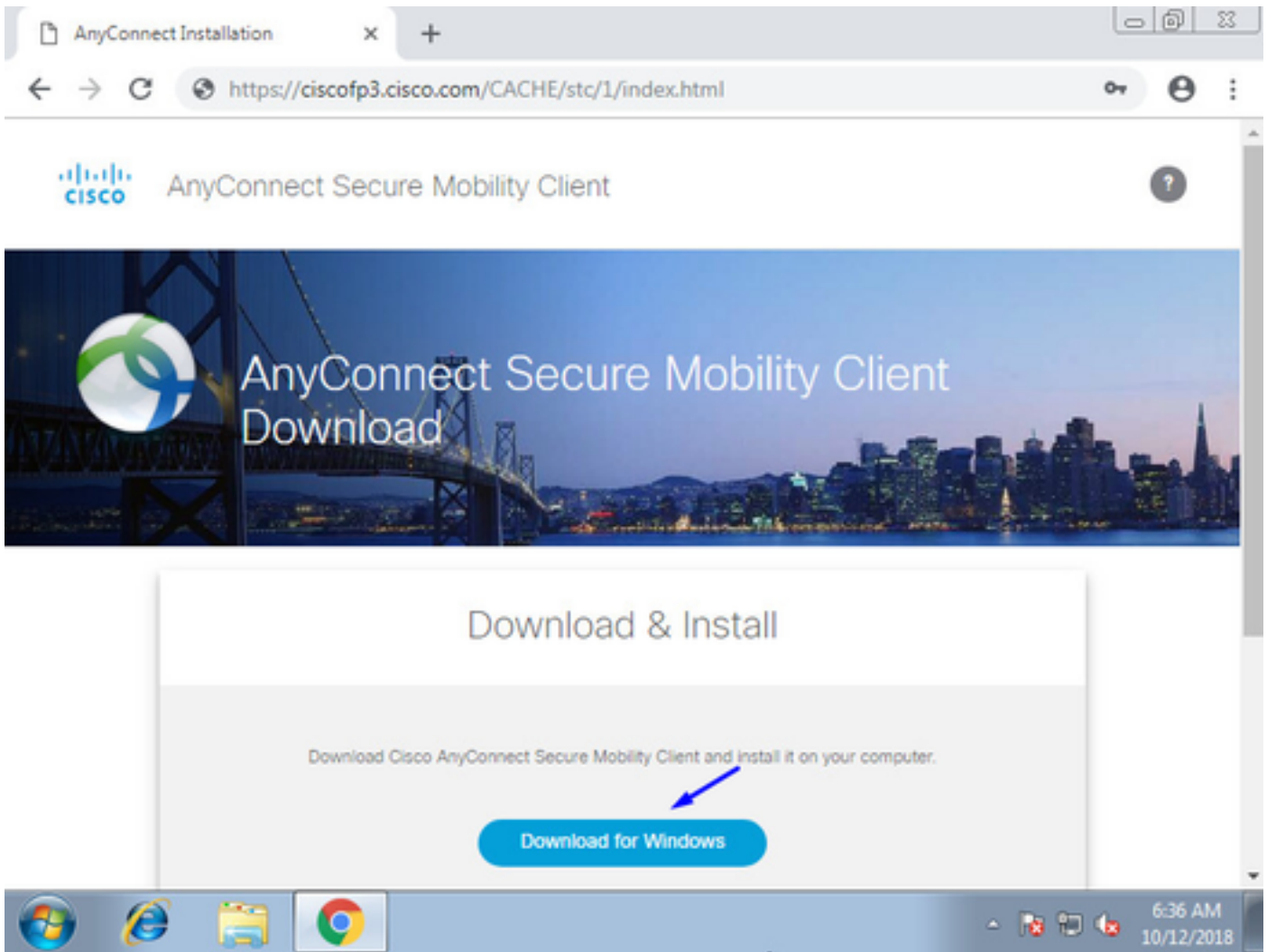
Logon

Group

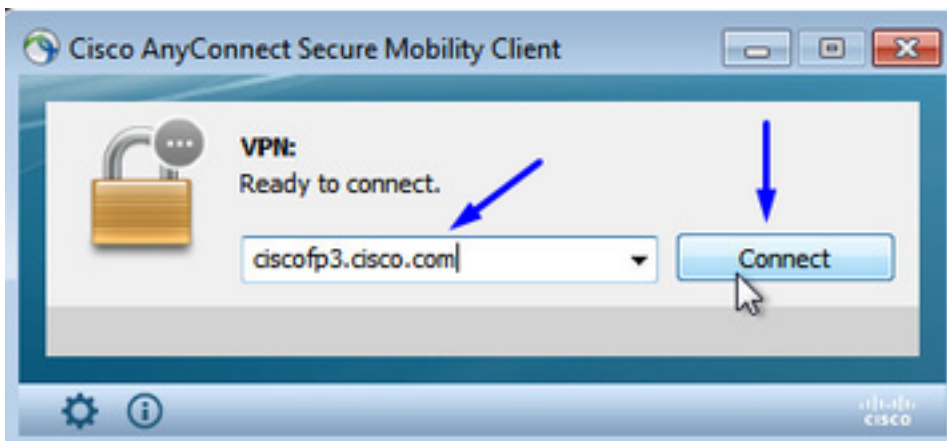
Username

Password

按一下「Download」

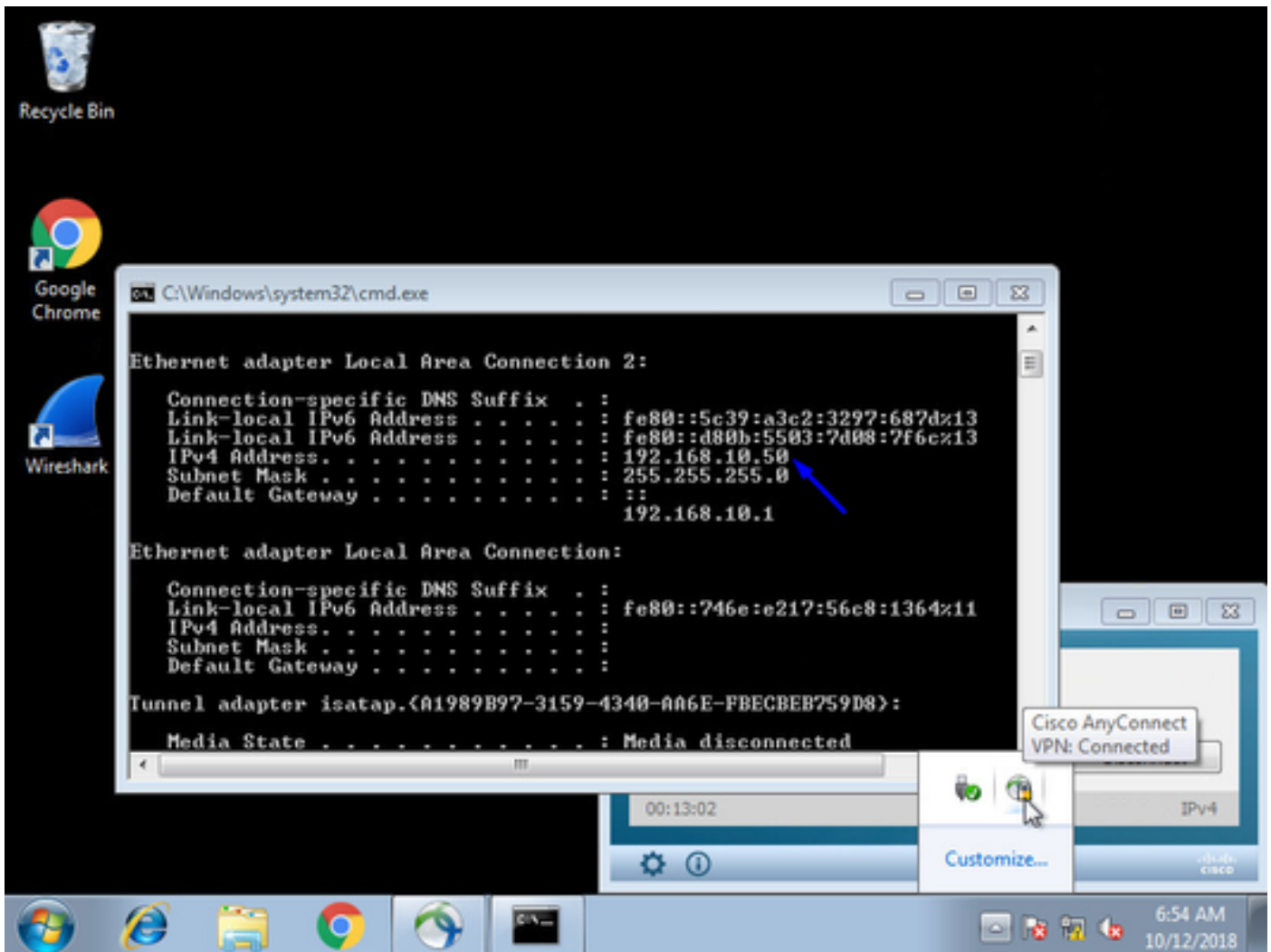


在Windows/Mac PC上安裝並運行AnyConnect VPN安全移動客戶端



出現提示時，鍵入您的Active Directory使用者名稱和密碼

您將在步驟5中從上面建立的IP地址池獲得IP地址，並在該子網中獲得。1的預設網關



驗證

FTD

顯示命令

在FTD上驗證終端使用者是否已連線到AnyConnect VPN:

> **show ip**

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0	inside	192.168.1.1	255.255.255.240	CONFIG
GigabitEthernet0/1	outside	203.0.113.2	255.255.255.240	CONFIG

Current IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0	inside	192.168.1.1	255.255.255.240	CONFIG
GigabitEthernet0/1	outside	203.0.113.2	255.255.255.240	CONFIG

> **show vpn-sessiondb detail anyconnect**

Session Type: AnyConnect Detailed

Username : **jsmith** Index : 2

Assigned IP : **192.168.10.50** Public IP : 198.51.100.2

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel

License : AnyConnect Premium

Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256

Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx : 18458 Bytes Rx : 2706024
Pkts Tx : 12 Pkts Rx : 50799
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy Tunnel Group : FTDAnyConnectVPN
Login Time : 15:08:19 UTC Wed Oct 10 2018
Duration : 0h:30m:11s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0ac9d68a000020005bbe15e3
Security Grp : none Tunnel Zone : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 2.1

Public IP : 198.51.100.2

Encryption : none Hashing : none

TCP Src Port : 53956 TCP Dst Port : 443

Auth Mode : userPassword

Idle Time Out: 30 Minutes Idle TO Left : 0 Minutes

Client OS : win

Client OS Ver: 6.1.7601 Service Pack 1

Client Type : AnyConnect

Client Ver : Cisco AnyConnect VPN Agent for Windows 4.6.03049

Bytes Tx : 10572 Bytes Rx : 289

Pkts Tx : 6 Pkts Rx : 0

Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 2.2

Assigned IP : 192.168.10.50 Public IP : 198.51.100.2

Encryption : AES-GCM-256 Hashing : SHA384

Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384

Encapsulation: TLSv1.2 TCP Src Port : 54634

TCP Dst Port : 443 Auth Mode : userPassword

Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes

Client OS : Windows

Client Type : SSL VPN Client

Client Ver : Cisco AnyConnect VPN Agent for Windows 4.6.03049

Bytes Tx : 7886 Bytes Rx : 2519

Pkts Tx : 6 Pkts Rx : 24

Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 2.3

Assigned IP : 192.168.10.50 Public IP : 198.51.100.2

Encryption : AES256 Hashing : SHA1

Ciphersuite : DHE-RSA-AES256-SHA

Encapsulation: DTLSv1.0 UDP Src Port : 61113

UDP Dst Port : 443 Auth Mode : userPassword

Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes

Client OS : Windows

Client Type : DTLS VPN Client

Client Ver : Cisco AnyConnect VPN Agent for Windows 4.6.03049

Bytes Tx : 0 Bytes Rx : 2703216

Pkts Tx : 0 Pkts Rx : 50775

Pkts Tx Drop : 0 Pkts Rx Drop : 0

進入Windows 7 PC並在Cisco AnyConnect客戶端上按一下「斷開連線」後，您將獲得：

```
> show vpn-sessiondb detail anyconnect
INFO: There are presently no active sessions
```

擷取

在AnyConnect客戶端上按一下connect時，外部介面上的工作捕獲的外觀

範例：

例如，終端使用者的公共IP是其在家路由器的公共IP

```
ciscofp3# capture capin interface outside trace detail trace-count 100 match ip any host
```

```
<now hit Connect on AnyConnect Client from employee PC>
```

```
ciscofp3# show cap
```

```
capture capin type raw-data trace detail trace-count 100 interface outside [Buffer Full - 524153 bytes]
```

```
match ip any host 198.51.100.2
```

檢視從終端使用者的PC傳至FTD外部介面的封包，確保它們到達我們的外部FTD介面：

```
ciscofp3# show cap capin
```

```
2375 packets captured
```

```
1: 17:05:56.580994      198.51.100.2.55928 > 203.0.113.2.443: S 2933933902:2933933902(0) win
8192 <mss 1460,nop,wscale 8,nop,nop,sackOK>
2: 17:05:56.581375      203.0.113.2.443 > 198.51.100.2.55928: S 430674106:430674106(0) ack
2933933903 win 32768 <mss 1460>
3: 17:05:56.581757      198.51.100.2.55928 > 203.0.113.2.443: . ack 430674107 win 64240
4: 17:05:56.582382      198.51.100.2.55928 > 203.0.113.2.443: P 2933933903:2933934036(133) ack
430674107 win 64240
5: 17:05:56.582458      203.0.113.2.443 > 198.51.100.2.55928: . ack 2933934036 win 32768
6: 17:05:56.582733      203.0.113.2.443 > 198.51.100.2.55928: P 430674107:430675567(1460) ack
2933934036 win 32768
7: 17:05:56.790211      198.51.100.2.55928 > 203.0.113.2.443: . ack 430675567 win 64240
8: 17:05:56.790349      203.0.113.2.443 > 198.51.100.2.55928: P 430675567:430676672(1105) ack
2933934036 win 32768
9: 17:05:56.791691      198.51.100.2.55928 > 203.0.113.2.443: P 2933934036:2933934394(358) ack
430676672 win 63135
10: 17:05:56.794911      203.0.113.2.443 > 198.51.100.2.55928: P 430676672:430676763(91) ack
2933934394 win 32768
11: 17:05:56.797077      198.51.100.2.55928 > 203.0.113.2.443: P 2933934394:2933934703(309) ack
430676763 win 63044
12: 17:05:56.797169      203.0.113.2.443 > 198.51.100.2.55928: . ack 2933934703 win 32768
13: 17:05:56.797199      198.51.100.2.55928 > 203.0.113.2.443: P 2933934703:2933935524(821) ack
430676763 win 63044
14: 17:05:56.797276      203.0.113.2.443 > 198.51.100.2.55928: . ack 2933935524 win 32768
15: 17:05:56.798634      203.0.113.2.443 > 198.51.100.2.55928: P 430676763:430677072(309) ack
2933935524 win 32768
16: 17:05:56.798786      203.0.113.2.443 > 198.51.100.2.55928: P 430677072:430677829(757) ack
2933935524 win 32768
17: 17:05:56.798817      203.0.113.2.443 > 198.51.100.2.55928: P 430677829:430677898(69) ack
2933935524 win 32768
18: 17:05:56.799397      198.51.100.2.55928 > 203.0.113.2.443: . ack 430677898 win 64240
19: 17:05:56.810215      198.51.100.2.55928 > 203.0.113.2.443: P 2933935524:2933935593(69) ack
430677898 win 64240
20: 17:05:56.810398      203.0.113.2.443 > 198.51.100.2.55928: . ack 2933935593 win 32768
21: 17:05:56.810428      198.51.100.2.55928 > 203.0.113.2.443: F 2933935593:2933935593(0) ack
430677898 win 64240
```

22: 17:05:56.810489 203.0.113.2.443 > 198.51.100.2.55928: . ack 2933935594 win 32768
23: 17:05:56.810627 203.0.113.2.443 > 198.51.100.2.55928: FP 430677898:430677898(0) ack
2933935594 win 32768
24: 17:05:56.811008 198.51.100.2.55928 > 203.0.113.2.443: . ack 430677899 win 64240
25: 17:05:59.250566 198.51.100.2.56228 > 203.0.113.2.443: S 2614357960:2614357960(0) win
8192 <mss 1460,nop,wscale 8,nop,nop,sackOK>
26: 17:05:59.250963 203.0.113.2.443 > 198.51.100.2.56228: S 3940915253:3940915253(0) ack
2614357961 win 32768 <mss 1460>
27: 17:05:59.251406 198.51.100.2.56228 > 203.0.113.2.443: . ack 3940915254 win 64240
28: 17:05:59.252062 198.51.100.2.56228 > 203.0.113.2.443: P 2614357961:2614358126(165) ack
3940915254 win 64240
29: 17:05:59.252138 203.0.113.2.443 > 198.51.100.2.56228: . ack 2614358126 win 32768
30: 17:05:59.252458 203.0.113.2.443 > 198.51.100.2.56228: P 3940915254:3940915431(177) ack
2614358126 win 32768
31: 17:05:59.253450 198.51.100.2.56228 > 203.0.113.2.443: P 2614358126:2614358217(91) ack
3940915431 win 64063
32: 17:05:59.253679 203.0.113.2.443 > 198.51.100.2.56228: . ack 2614358217 win 32768
33: 17:05:59.255235 198.51.100.2.56228 > 203.0.113.2.443: P 2614358217:2614358526(309) ack
3940915431 win 64063
34: 17:05:59.255357 203.0.113.2.443 > 198.51.100.2.56228: . ack 2614358526 win 32768
35: 17:05:59.255388 198.51.100.2.56228 > 203.0.113.2.443: P 2614358526:2614359555(1029)
ack 3940915431 win 64063
36: 17:05:59.255495 203.0.113.2.443 > 198.51.100.2.56228: . ack 2614359555 win 32768
37: 17:05:59.400110 203.0.113.2.443 > 198.51.100.2.56228: P 3940915431:3940915740(309) ack
2614359555 win 32768
38: 17:05:59.400186 203.0.113.2.443 > 198.51.100.2.56228: P 3940915740:3940917069(1329)
ack 2614359555 win 32768
39: 17:05:59.400675 198.51.100.2.56228 > 203.0.113.2.443: . ack 3940917069 win 64240
40: 17:05:59.400736 203.0.113.2.443 > 198.51.100.2.56228: P 3940917069:3940918529(1460)
ack 2614359555 win 32768
41: 17:05:59.400751 203.0.113.2.443 > 198.51.100.2.56228: P 3940918529:3940919979(1450)
ack 2614359555 win 32768
42: 17:05:59.401544 198.51.100.2.56228 > 203.0.113.2.443: . ack 3940919979 win 64240
43: 17:05:59.401605 203.0.113.2.443 > 198.51.100.2.56228: P 3940919979:3940921439(1460)
ack 2614359555 win 32768
44: 17:05:59.401666 203.0.113.2.443 > 198.51.100.2.56228: P 3940921439:3940922899(1460)
ack 2614359555 win 32768
45: 17:05:59.401727 203.0.113.2.443 > 198.51.100.2.56228: P 3940922899:3940923306(407) ack
2614359555 win 32768
46: 17:05:59.401743 203.0.113.2.443 > 198.51.100.2.56228: P 3940923306:3940923375(69) ack
2614359555 win 32768
47: 17:05:59.402185 198.51.100.2.56228 > 203.0.113.2.443: . ack 3940923375 win 64240
48: 17:05:59.402475 198.51.100.2.56228 > 203.0.113.2.443: P 2614359555:2614359624(69) ack
3940923375 win 64240
49: 17:05:59.402597 203.0.113.2.443 > 198.51.100.2.56228: . ack 2614359624 win 32768
50: 17:05:59.402628 198.51.100.2.56228 > 203.0.113.2.443: F 2614359624:2614359624(0) ack
3940923375 win 64240
51: 17:05:59.402673 203.0.113.2.443 > 198.51.100.2.56228: . ack 2614359625 win 32768
52: 17:05:59.402765 203.0.113.2.443 > 198.51.100.2.56228: FP 3940923375:3940923375(0) ack
2614359625 win 32768
53: 17:05:59.413384 198.51.100.2.56228 > 203.0.113.2.443: . ack 3940923376 win 64240
54: 17:05:59.555665 198.51.100.2.56280 > 203.0.113.2.443: S 1903869753:1903869753(0) win
8192 <mss 1460,nop,wscale 8,nop,nop,sackOK>
55: 17:05:59.556154 203.0.113.2.443 > 198.51.100.2.56280: S 2583094766:2583094766(0) ack
1903869754 win 32768 <mss 1460>
56: 17:05:59.556627 198.51.100.2.56280 > 203.0.113.2.443: . ack 2583094767 win 64240
57: 17:05:59.560502 198.51.100.2.56280 > 203.0.113.2.443: P 1903869754:1903869906(152) ack
2583094767 win 64240
58: 17:05:59.560578 203.0.113.2.443 > 198.51.100.2.56280: . ack 1903869906 win 32768
59: 17:05:59.563996 203.0.113.2.443 > 198.51.100.2.56280: P 2583094767:2583096227(1460)
ack 1903869906 win 32768
60: 17:05:59.780034 198.51.100.2.56280 > 203.0.113.2.443: . ack 2583096227 win 64240
61: 17:05:59.780141 203.0.113.2.443 > 198.51.100.2.56280: P 2583096227:2583097673(1446)
ack 1903869906 win 32768

```

62: 17:05:59.998376      198.51.100.2.56280 > 203.0.113.2.443: . ack 2583097673 win 62794
63: 17:06:14.809253      198.51.100.2.56280 > 203.0.113.2.443: P 1903869906:1903870032(126) ack
2583097673 win 62794
64: 17:06:14.809970      203.0.113.2.443 > 198.51.100.2.56280: P 2583097673:2583097724(51) ack
1903870032 win 32768
65: 17:06:14.815768      198.51.100.2.56280 > 203.0.113.2.443: P 1903870032:1903870968(936) ack
2583097724 win 64240
66: 17:06:14.815860      203.0.113.2.443 > 198.51.100.2.56280: . ack 1903870968 win 32768
67: 17:06:14.816913      203.0.113.2.443 > 198.51.100.2.56280: P 2583097724:2583099184(1460)
ack 1903870968 win 32768
68: 17:06:14.816928      203.0.113.2.443 > 198.51.100.2.56280: P 2583099184:2583099306(122) ack
1903870968 win 32768
69: 17:06:14.816959      203.0.113.2.443 > 198.51.100.2.56280: P 2583099306:2583100766(1460)
ack 1903870968 win 32768
70: 17:06:14.816974      203.0.113.2.443 > 198.51.100.2.56280: P 2583100766:2583100888(122) ack
1903870968 win 32768
71: 17:06:14.816989      203.0.113.2.443 > 198.51.100.2.56280: P 2583100888:2583102142(1254)
ack 1903870968 win 32768
72: 17:06:14.817554      198.51.100.2.56280 > 203.0.113.2.443: . ack 2583102142 win 64240
73: 17:06:14.817615      203.0.113.2.443 > 198.51.100.2.56280: P 2583102142:2583103602(1460)
ack 1903870968 win 32768
74: 17:06:14.817630      203.0.113.2.443 > 198.51.100.2.56280: P 2583103602:2583103930(328) ack
1903870968 win 32768
75: 17:06:14.817630      203.0.113.2.443 > 198.51.100.2.56280: P 2583103930:2583104052(122) ack
1903870968 win 32768
76: 17:06:14.817645      203.0.113.2.443 > 198.51.100.2.56280: P 2583104052:2583105512(1460)
ack 1903870968 win 32768
77: 17:06:14.817645      203.0.113.2.443 > 198.51.100.2.56280: P 2583105512:2583105634(122) ack
1903870968 win 32768
78: 17:06:14.817660      203.0.113.2.443 > 198.51.100.2.56280: P 2583105634:2583105738(104) ack
1903870968 win 32768
79: 17:06:14.818088      198.51.100.2.56280 > 203.0.113.2.443: . ack 2583105512 win 64240
80: 17:06:14.818530      198.51.100.2.56280 > 203.0.113.2.443: . ack 2583105738 win 64014
81: 17:06:18.215122      198.51.100.2.58944 > 203.0.113.2.443: udp 99
82: 17:06:18.215610      203.0.113.2.443 > 198.51.100.2.58944: udp 48
83: 17:06:18.215671      198.51.100.2.56280 > 203.0.113.2.443: P 1903870968:1903872025(1057)
ack 2583105738 win 64014
84: 17:06:18.215763      203.0.113.2.443 > 198.51.100.2.56280: . ack 1903872025 win 32768
85: 17:06:18.247011      198.51.100.2.58944 > 203.0.113.2.443: udp 119
86: 17:06:18.247728      203.0.113.2.443 > 198.51.100.2.58944: udp 188
87: 17:06:18.249285      198.51.100.2.58944 > 203.0.113.2.443: udp 93
88: 17:06:18.272309      198.51.100.2.58944 > 203.0.113.2.443: udp 93
89: 17:06:18.277680      198.51.100.2.58944 > 203.0.113.2.443: udp 93
90: 17:06:18.334501      198.51.100.2.58944 > 203.0.113.2.443: udp 221
91: 17:06:18.381541      198.51.100.2.58944 > 203.0.113.2.443: udp 109
92: 17:06:18.443565      198.51.100.2.58944 > 203.0.113.2.443: udp 109
93: 17:06:18.786702      198.51.100.2.58944 > 203.0.113.2.443: udp 157
94: 17:06:18.786870      198.51.100.2.58944 > 203.0.113.2.443: udp 157
95: 17:06:18.786931      198.51.100.2.58944 > 203.0.113.2.443: udp 157
96: 17:06:18.952755      198.51.100.2.58944 > 203.0.113.2.443: udp 109
97: 17:06:18.968272      198.51.100.2.58944 > 203.0.113.2.443: udp 109
98: 17:06:18.973902      198.51.100.2.58944 > 203.0.113.2.443: udp 109
99: 17:06:18.973994      198.51.100.2.58944 > 203.0.113.2.443: udp 109
100: 17:06:18.989267      198.51.100.2.58944 > 203.0.113.2.443: udp 109

```

檢視防火牆內來自終端使用者的封包發生什麼情況的詳細資訊

```

ciscofp3# show cap capin packet-number 1 trace detail
2943 packets captured

```

```

1: 17:05:56.580994 006b.f1e7.6c5e 000c.294f.ac84 0x0800 Length: 66

```

198.51.100.2.55928 > 203.0.113.2.443: S [tcp sum ok] 2933933902:2933933902(0) win 8192 <mss 1460,nop,wscale 8,nop,nop,sackOK> (DF) (ttl 127, id 31008)

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2ace13beec90, priority=13, domain=capture, deny=false

hits=2737, user_data=0x2ace1232af40, cs_id=0x0, l3_type=0x0

src mac=0000.0000.0000, mask=0000.0000.0000

dst mac=0000.0000.0000, mask=0000.0000.0000

input_ifc=outside, output_ifc=any

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2ace107c8480, priority=1, domain=permit, deny=false

hits=183698, user_data=0x0, cs_id=0x0, l3_type=0x8

src mac=0000.0000.0000, mask=0000.0000.0000

dst mac=0000.0000.0000, mask=0100.0000.0000

input_ifc=outside, output_ifc=any

Phase: 3

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

found next-hop 203.0.113.2 using egress ifc identity

Phase: 4

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2ace1199f680, priority=119, domain=permit, deny=false

hits=68, user_data=0x0, cs_id=0x0, flags=0x0, protocol=6

src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any

dst ip/id=0.0.0.0, mask=0.0.0.0, port=443, tag=any, dscp=0x0

input_ifc=outside, output_ifc=identity

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2ace1199efd0, priority=8, domain=conn-set, deny=false

hits=68, user_data=0x2ace1199e5d0, cs_id=0x0, reverse, flags=0x0, protocol=6

src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any

dst ip/id=0.0.0.0, mask=0.0.0.0, port=443, tag=any, dscp=0x0

input_ifc=outside, output_ifc=identity

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ace0fa81330, priority=0, domain=nat-per-session, deny=false
hits=178978, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ace107cdb00, priority=0, domain=inspect-ip-options, deny=true
hits=174376, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=any

Phase: 8
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ace107c90c0, priority=208, domain=cluster-redirect, deny=false
hits=78, user_data=0x0, cs_id=0x0, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=identity

Phase: 9
Type: TCP-MODULE
Subtype: webvpn
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ace1199df20, priority=13, domain=soft-np-tcp-module, deny=false
hits=58, user_data=0x2ace061efb00, cs_id=0x0, reverse, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=443, tag=any, dscp=0x0
input_ifc=outside, output_ifc=identity

Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ace11d455e0, priority=13, domain=ipsec-tunnel-flow, deny=true
hits=87214, user_data=0x0, cs_id=0x0, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0

input_ifc=outside, output_ifc=any

Phase: 11

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

in id=0x2ace11da7000, priority=13, domain=capture, deny=false
hits=635, user_data=0x2ace1232af40, cs_id=0x2ace11f21620, reverse, flags=0x0, protocol=0
src ip/id=198.51.100.2, mask=255.255.255.255, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=any

Phase: 12

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

Reverse Flow based lookup yields rule:

out id=0x2ace10691780, priority=13, domain=capture, deny=false
hits=9, user_data=0x2ace1232af40, cs_id=0x2ace11f21620, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=198.51.100.2, mask=255.255.255.255, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=outside

Phase: 13

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 87237, packet dispatched to next module

Module information for forward flow ...

snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_tcp_mod
snp_fp_adjacency
snp_fp_fragment
snp_fp_drop

Module information for reverse flow ...

snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Result:

input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow

1 packet shown

ciscofp3#

將捕獲複製到disk0:FTD的IP地址。然後您可以透過SCP、FTP或TFTP下載

(或者從FirePOWER管理中心Web UI >> System >> Health >> Health Monitor >> Click Advanced Troubleshooting >> click Download File頁籤)


```
ciscofp3# copy /pcap capture:capin disk0:/capin.pcap
```

```
Source capture name [capin]? <hit Enter>
```

```
Destination filename [capin.pcap]? <hit Enter>
```

```
!!!!!!!!!!!!!!!!!!!!
```

```
207 packets copied in 0.0 secs
```

```
ciscofp3# dir
```

```
Directory of disk0:/
```

```
122 -rwx 198 05:13:44 Apr 01 2018 lina_phase1.log
```

```
49 drwx 4096 21:42:20 Jun 30 2018 log
```

```
53 drwx 4096 21:42:36 Jun 30 2018 coredumpinfo
```

```
110 drwx 4096 14:59:51 Oct 10 2018 csm
```

```
123 -rwx 21074 01:26:44 Oct 10 2018 backup-config.cfg
```

```
124 -rwx 21074 01:26:44 Oct 10 2018 startup-config
```

```
125 -rwx 20354 01:26:44 Oct 10 2018 modified-config.cfg
```

```
160 -rwx 60124 17:06:22 Oct 10 2018 capin.pcap
```

```
ciscofp3# copy disk0:/capin.pcap tftp:/
```

```
Source filename [capin.pcap]? <hit Enter>
```

```
Address or name of remote host []? 192.168.1.25 (your TFTP server IP address (your PC if using  
tftpd32 or Solarwinds TFTP Server))
```

```
Destination filename [capin.pcap]? <hit Enter>
```

```
113645 bytes copied in 21.800 secs (5411 bytes/sec)
```

```
ciscofp3#
```

(or from FirePOWER Management Center Web GUI >> System >> Health >> Health Monitor >> click
Advanced Troubleshooting >> click Download File tab)

驗證NAT規則是否配置正確：

```
ciscofp3# packet-tracer input outside tcp 192.168.10.50 1234 192.168.1.30 443 detailed
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
Forward Flow based lookup yields rule:
```

```
in id=0x2ace0fa90e70, priority=13, domain=capture, deny=false
```

```
hits=11145169, user_data=0x2ace120c4910, cs_id=0x0, l3_type=0x0
```

```
src mac=0000.0000.0000, mask=0000.0000.0000
```

```
dst mac=0000.0000.0000, mask=0000.0000.0000
```

```
input_ifc=outside, output_ifc=any
```

```
Phase: 2
```

```
Type: ACCESS-LIST
```

```
Subtype:
```

```
Result: ALLOW
```

```
Config:
```

```
Implicit Rule
```

```
Additional Information:
```

```
Forward Flow based lookup yields rule:
```

```
in id=0x2ace107c8480, priority=1, domain=permit, deny=false
```

```
hits=6866095, user_data=0x0, cs_id=0x0, l3_type=0x8
```

```
src mac=0000.0000.0000, mask=0000.0000.0000
```

```
dst mac=0000.0000.0000, mask=0100.0000.0000
```

```
input_ifc=outside, output_ifc=any
```

```
Phase: 3
```

```
Type: ROUTE-LOOKUP
```

```
Subtype: Resolve Egress Interface
```

Result: ALLOW
Config:
Additional Information:
found next-hop **192.168.1.30** using egress ifc inside

Phase: 4
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:

nat (inside,outside) source static inside-subnet inside-subnet destination static outside-subnet-anyconnect-pool outside-subnet-anyconnect-pool no-proxy-arp route-lookup

Additional Information:
NAT divert to egress interface inside
Untranslate 192.168.1.30/443 to 192.168.1.30/443

Phase: 5
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:

access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust ip ifc outside any any rule-id 268436481 event-log flow-end
access-list CSM_FW_ACL_ remark rule-id 268436481: PREFILTER POLICY:
Example_Company_Prefilter_Policy
access-list CSM_FW_ACL_ remark rule-id 268436481: RULE: AllowtoVPNOutsideinterface

Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ace0fa8f4e0, priority=12, domain=permit, trust
hits=318637, user_data=0x2ace057b9a80, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=outside
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

...

Phase: 7
Type: NAT
Subtype:
Result: ALLOW
Config:

nat (inside,outside) source static inside-subnet inside-subnet destination static outside-subnet-anyconnect-pool outside-subnet-anyconnect-pool no-proxy-arp route-lookup

Additional Information:
Static translate 192.168.10.50/1234 to 192.168.10.50/1234
Forward Flow based lookup yields rule:
in id=0x2ace11975cb0, priority=6, domain=nat, deny=false
hits=120, user_data=0x2ace0f29c4a0, cs_id=0x0, flags=0x0, protocol=0
src ip/id=192.168.10.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=10.201.214.128, mask=255.255.255.240, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=inside

...

Phase: 10 Type: VPN Subtype: ipsec-tunnel-flow Result: ALLOW Config: Additional Information:
Forward Flow based lookup yields rule: in id=0x2ace11d455e0, priority=13, domain=ipsec-tunnel-flow, deny=true hits=3276174, user_data=0x0, cs_id=0x0, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=any Phase: 11 Type: NAT Subtype: rpf-check Result: ALLOW Config:
nat (inside,outside) source static inside-subnet inside-subnet destination static outside-subnet-anyconnect-pool outside-subnet-anyconnect-pool no-proxy-arp route-lookup

Additional Information:
Forward Flow based lookup yields rule:
out id=0x2ace0d5a9800, priority=6, domain=nat-reverse, deny=false

```
hits=121, user_data=0x2ace1232a4c0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.10.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=10.201.214.128, mask=255.255.255.240, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=inside
```

...

Phase: 14

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 3279248, packet dispatched to next module

Module information for reverse flow ...

...

Phase: 15

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

found next-hop **192.168.1.30** using egress ifc inside

Result:

input-interface: **outside**

input-status: up

input-line-status: up

output-interface: **inside**

output-status: up

output-line-status: up

Action: allow

ciscofp3#

在PC的員工PC上捕獲並成功通過AnyConnect VPN連線到FTD

The screenshot shows a network capture tool interface with a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. The main window displays a list of captured packets with columns for No., Time, Source, Src port, Destination, Dst port, Protocol, Length, and Info. The packets show a sequence of TCP and TLSv1.2 traffic between source port 56501 and destination port 443. A detailed view of a selected packet is shown at the bottom, indicating it is a Transmission Control Protocol packet with Source Port: 56501 and Destination Port: 443.

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
129	3.685253		56501		443	TCP	66	56501 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
130	3.685868			443		56501	TCP	60 443 → 56501 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
131	3.685917		56501		443	TCP	54	56501 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
132	3.687035		56501		443	TLSv1.2	187	Client Hello
133	3.687442			443		56501	TCP	60 443 → 56501 [ACK] Seq=1 Ack=134 Win=32768 Len=0
134	3.687806			443		56501	TLSv1.2	1514 Server Hello
142	3.899719		56501		443	TCP	54	56501 → 443 [ACK] Seq=134 Ack=1461 Win=64240 Len=0
143	3.900303			443		56501	TLSv1.2	1159 Certificate, Server Hello Done
144	3.901003		56501		443	TLSv1.2	412	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
145	3.904245			443		56501	TLSv1.2	145 Change Cipher Spec, Encrypted Handshake Message
146	3.907281		56501		443	TLSv1.2	363	Application Data
147	3.907374		56501		443	TLSv1.2	875	Application Data
148	3.907797			443		56501	TCP	60 443 → 56501 [ACK] Seq=2657 Ack=801 Win=32768 Len=0
149	3.907868			443		56501	TCP	60 443 → 56501 [ACK] Seq=2657 Ack=1622 Win=32768 Len=0
150	3.909600			443		56501	TLSv1.2	363 Application Data
151	3.909759			443		56501	TLSv1.2	811 Application Data

Transmission Control Protocol, Src Port: 56501, Dst Port: 443, Seq: 0, Len: 0
Source Port: 56501
Destination Port: 443

您還可以在同一捕獲中看到稍後形成的DTLS隧道

capin.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
76	12:06:14.817645			443		56280 TCP	1514	443 → 56280 [PSH, ACK] Seq=9286 Ack=1215 Win=32768 Len=1460 [TCP segment of a reassembled PDU]
77	12:06:14.817645			443		56280 TLSv1.2	176	Application Data
78	12:06:14.817660			443		56280 TLSv1.2	158	Application Data
79	12:06:14.818088			56280		443 TCP	54	56280 → 443 [ACK] Seq=1215 Ack=10746 Win=64240 Len=0
80	12:06:14.818530			56280		443 TCP	54	56280 → 443 [ACK] Seq=1215 Ack=10972 Win=64014 Len=0
81	12:06:18.215122		58944			443 DTLS 1.0 (OpenSSL pre 0.9.8f)	141	Client Hello
82	12:06:18.215619		443			58944 DTLS 1.0 (OpenSSL pre 0.9.8f)	90	Hello Verify Request
83	12:06:18.215671		56280			443 TLSv1.2	1111	Application Data
84	12:06:18.215763		443			56280 TCP	54	443 → 56280 [ACK] Seq=10972 Ack=2272 Win=32768 Len=0
85	12:06:18.247011		58944			443 DTLS 1.0 (OpenSSL pre 0.9.8f)	161	Client Hello
86	12:06:18.247728		443			58944 DTLS 1.0 (OpenSSL pre 0.9.8f)	230	Server Hello, Change Cipher Spec, Encrypted Handshake Message
87	12:06:18.249285		58944			443 DTLS 1.0 (OpenSSL pre 0.9.8f)	135	Change Cipher Spec, Encrypted Handshake Message
88	12:06:18.272309		58944			443 DTLS 1.0 (OpenSSL pre 0.9.8f)	135	Application Data
89	12:06:18.277680		58944			443 DTLS 1.0 (OpenSSL pre 0.9.8f)	135	Application Data
90	12:06:18.334501		58944			443 DTLS 1.0 (OpenSSL pre 0.9.8f)	263	Application Data

> Frame 81: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits)

> Ethernet II, Src: Cisco_e7:6c:5e (00:6b:f1:e7:6c:5e), Dst: Vmware_4f:ac:84 (00:0c:29:4f:ac:84)

> Internet Protocol Version 4, Src: , Dst:

> User Datagram Protocol, Src Port: 58944, Dst Port: 443

> Datagram Transport Layer Security

- DTLS 1.0 (OpenSSL pre 0.9.8f) Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: DTLS 1.0 (OpenSSL pre 0.9.8f) (0x0100)
 - Epoch: 0
 - Sequence Number: 0
 - Length: 86
 - Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 74
 - Message Sequence: 0
 - Fragment Offset: 0
 - Fragment Length: 74

在FTD的外部介面上擷取，顯示AnyConnect PC成功連線到VPN

capin.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
1	12:05:56.580994			55928		443 TCP	66	55928 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	12:05:56.581375			443		55928 TCP	58	443 → 55928 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
3	12:05:56.581757			55928		443 TCP	54	55928 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	12:05:56.582382			55928		443 TLSv1.2	187	Client Hello
5	12:05:56.582458			443		55928 TCP	54	443 → 55928 [ACK] Seq=1 Ack=134 Win=32768 Len=0
6	12:05:56.582733			443		55928 TLSv1.2	1514	Server Hello
7	12:05:56.790211			55928		443 TCP	54	55928 → 443 [ACK] Seq=134 Ack=1461 Win=64240 Len=0
8	12:05:56.790349			443		55928 TLSv1.2	1159	Certificate, Server Hello Done
9	12:05:56.791691			55928		443 TLSv1.2	412	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	12:05:56.794911			443		55928 TLSv1.2	145	Change Cipher Spec, Encrypted Handshake Message
11	12:05:56.797077			55928		443 TLSv1.2	363	Application Data
12	12:05:56.797169			443		55928 TCP	54	443 → 55928 [ACK] Seq=2657 Ack=801 Win=32768 Len=0
13	12:05:56.797199			55928		443 TLSv1.2	875	Application Data
14	12:05:56.797276			443		55928 TCP	54	443 → 55928 [ACK] Seq=2657 Ack=1622 Win=32768 Len=0
15	12:05:56.798634			443		55928 TLSv1.2	363	Application Data
16	12:05:56.798786			443		55928 TLSv1.2	811	Application Data

> Frame 6: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

> Ethernet II, Src: Vmware_4f:ac:84 (00:0c:29:4f:ac:84), Dst: Cisco_e7:6c:5e (00:6b:f1:e7:6c:5e)

> Internet Protocol Version 4, Src: , Dst:

> Transmission Control Protocol, Src Port: 443, Dst Port: 55928, Seq: 1, Ack: 134, Len: 1460

Source Port: 443

Destination Port: 55928

[Stream index: 0]

[TCP Segment Len: 1460]

Sequence number: 1 (relative sequence number)

[Next sequence number: 1461 (relative sequence number)]

Acknowledgment number: 134 (relative ack number)

0101 = Header Length: 20 bytes (5)

> Flags: 0x018 (PSH, ACK)

Window size value: 32768

[Calculated window size: 32768]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x3693 [unverified]

```

00c0 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30 51 31 15  .*.H....001
00d0 30 13 06 0a 09 92 26 89 93 f2 2c 64 01 19 16 05  0.....&...d...
00e0 6c 6f 63 61 6c 31 19 30 17 06 0a 09 92 26 89 93  local1-0....&..
00f0 f2 2c 64 01 19 16 09 63 6f 68 61 64 6c 65 79 33  .,d....c...
0100 31 1d 30 1b 06 03 55 04 03 13 14 63 6f 68 61 64  1-0...U....
0110 6c 65 79 33 2d 43 4f 52 42 44 43 33 2d 43 41 30  6c.65.79.33.2d.43.4f.52.42.44.43.33.2d.43.41.30
0120 1e 17 0d 31 38 31 30 31 30 30 32 34 35 30 30 5a  ..18101 00245002
0130 17 0d 32 30 31 30 30 39 30 32 34 35 30 30 5a 30  ..201009 02450020
0140 61 b3 31 26 30 24 06 09 2a 86 48 86 f7 0d 01 09  ..1805...*.H....
0150 02 13 17 63 6f 72 62 66 70 33 2e 63 6f 68 61 64  .... f p3....
0160 6c 65 79 33 2e 6c 6f 63 61 6c 31 0b 30 09 06 03  6c.65.79.33.2e.6c.6f.63.61.6c.31.0b.30.09.06.03
0170 55 04 06 13 02 55 53 31 0b 30 09 06 03 55 04 08  U...US1-0...U...
0180 13 02 43 41 31 11 30 0f 06 03 55 04 07 13 08 53  ..CA1-0...U...S
0190 61 6e 20 4a 6f 73 65 31 0e 30 0c 06 03 55 04 0a  an Jose1-0...U...
01a0 13 05 43 69 73 63 6f 31 0c 30 0a 06 03 55 04 0b  ..Cisco1-0...U...
01b0 13 03 54 41 43 31 20 30 1e 06 03 55 04 03 13 17  ..TAC1 0...U...
01c0 63 6f 72 62 66 70 33 2e 63 6f 68 61 64 6c 65 79  6...f.p3....
01d0 33 2e 6c 6f 63 61 6c 31 1c 30 1a 06 09 2a 86 48  3.local1-0...*.H
01e0 86 f7 0d 01 09 01 16 0d 74 61 63 40 63 69 73 63  6.....tac@cis
01f0 6f 2e 63 6f 6d 30 82 01 22 30 0d 06 09 2a 86 48  o.com0...0...*.H
0200 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 30 82 01  6.....0...

```

附註：透過VPN連線到FTD的外部介面時，您可以在「Server Hello」封包中看到FTD VPN伺服器

憑證。僱員PC將信任此證書，因為僱員PC具有根CA證書，並且由該根CA簽署FTD VPN伺服器證書。

在FTD的FTD上擷取，詢問RADIUS伺服器使用者名稱+密碼是否正確(Cisco ISE)

The image shows a Wireshark capture of RADIUS traffic. The packet list pane shows several RADIUS messages, with the second packet (Frame 2) selected. The packet details pane shows the RADIUS Protocol section expanded to 'Code: Access-Accept (2)'. The raw data pane shows the hexadecimal and ASCII representation of the packet, with a blue arrow pointing to the ASCII text 'jsmith (' ReauthSe'.

No.	Time	Source	Src port	Destination	Dst port	Protocol	Length	Info
1	13:05:36.771841		3238		1812	RADIUS	701	Access-Request id=93
2	13:05:42.865342		1812		3238	RADIUS	201	Access-Accept id=93
3	13:05:42.865937		3238		1812	RADIUS	701	Access-Request id=94
4	13:05:42.911314		1812		3238	RADIUS	62	Access-Reject id=94
5	13:05:43.302825		19500		1813	RADIUS	756	Accounting-Request id=95
6	13:05:43.309294		1813		19500	RADIUS	62	Accounting-Response id=95

```

> Frame 2: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits)
> Ethernet II, Src: Cisco_e7:6c:5e (00:0b:f1:e7:6c:5e), Dst: Vmware_4f:ac:84 (00:0c:29:4f:ac:84)
> Internet Protocol Version 4, Src: ..., Dst: ...
> User Datagram Protocol, Src Port: 1812, Dst Port: 3238
RADIUS Protocol
  Code: Access-Accept (2)
0000  00 0c 29 4f ac 84 00 6b f1 e7 6c 5e 08 00 45 00  ..)O...k..l^..E.
0010  00 bb 5f 66 40 00 3f 11 18 bc 0a c9 d6 e6 0a c9  .._f@?.....
0020  d6 97 07 14 0c a6 00 a7 4e 17 02 5d 00 9f 7f b9  ....N..]....
0030  c7 a6 65 6d e7 75 c7 64 7f 0f d5 54 d7 59 01 08  ..em..u.d...T.Y..
0040  6a 73 6d 69 74 68 18 28 52 65 61 75 74 68 53 65  jsmith( ReauthSe
0050  73 73 69 6f 6e 3a 30 61 63 39 64 36 38 61 30 30  ssion:0a c9d68a00
0060  30 31 61 30 30 30 35 62 62 66 39 30 66 30 19 3b  01a0005b bf90f0.;
0070  43 41 43 53 3a 30 61 63 39 64 36 38 61 30 30 30  CACS:0ac 9d68a000
0080  31 61 30 30 30 35 62 62 66 39 30 66 30 3a 63 6f  1a0005bb f90f0:co
0090  72 62 69 6e 69 73 65 2f 33 32 32 33 34 34 30 38  rbinise/ 32234408
00a0  34 2f 31 39 37 34 32 39 39 1a 20 00 00 00 09 01  4/197429 9.....
00b0  1a 70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 57 6f  :profile -name=Wo
00c0  72 6b 73 74 61 74 69 6f 6e                               rkstatio n
  
```

正如您所看到的，我們的VPN連線獲得訪問接受，我們的AnyConnect VPN客戶端通過VPN成功連線到FTD

FTD的擷取(CLI)詢問思科ISE使用者名稱+密碼是否有效 (例如，確保RADIUS要求成功在FTD和ISE之間傳輸並確認它們離開的介面)

```

ciscofp3# capture capout interface inside trace detail trace-count 100 [Capturing - 35607 bytes]
ciscofp3# show cap
ciscofp3# show cap capout | i 192.168.1.10
37: 01:23:52.264512 192.168.1.1.3238 > 192.168.1.10.1812: udp 659
38: 01:23:52.310210 192.168.1.10.1812 > 192.168.1.1.3238: udp 159
39: 01:23:52.311064 192.168.1.1.3238 > 192.168.1.10.1812: udp 659
40: 01:23:52.326734 192.168.1.10.1812 > 192.168.1.1.3238: udp 20
82: 01:23:52.737663 192.168.1.1.19500 > 192.168.1.10.1813: udp 714
85: 01:23:52.744483 192.168.1.10.1813 > 192.168.1.1.19500: udp 20
  
```

思科ISE RADIUS伺服器下方顯示成功身份驗證。按一下放大鏡檢視成功身份驗證的詳細資訊

Time	Status	User	IP	Device	Group	Access
Oct 11, 2018 06:10:08.808 PM	●	jsmith	00:0C:29:37:EF:BF	Workstation	VPN Users >> Default	VPN Users >> Allow FTD VPN connections if AD Group VPNUsers
Oct 11, 2018 06:10:08.808 PM	■	jsmith	00:0C:29:37:EF:BF	FTDVPN	Workstation	VPN Users >> Default

Overview

Event	5200 Authentication succeeded
Username	jsmith
Endpoint Id	00:0C:29:37:EF:BF ⓘ
Endpoint Profile	Workstation
Authentication Policy	VPN Users >> Default
Authorization Policy	VPN Users >> Allow FTD VPN connections if AD Group VPNusers
Authorization Result	PermitAccess

在員工電腦的員工PC的AnyConnect介面卡上捕獲通過HTTPS訪問Inside網站 (即成功通過VPN登入) :

The image shows a Wireshark capture of network traffic on a local area connection. The filter is set to 'tcp.port == 443'. The capture shows a series of packets related to a TLS handshake. The first packet (No. 49) is a SYN packet from source 192.168.10.50 to destination 192.168.10.50. The second packet (No. 50) is a SYN, ACK packet from destination 192.168.10.50 back to source 192.168.10.50. Subsequent packets (Nos. 51-67) show the exchange of TLS records, including Client Hello, Server Hello, Key Exchange, Change Cipher Spec, and Application Data. The status bar at the bottom indicates 'Transmission Control Protocol (tcp), 32 bytes' and 'Packets: 260 · Displayed: 125 (48.1%) · Dropped: 0 (0.0%)'.

No.	Time	Source	Destination	Protocol	Length	Info
49	1.545946	192.168.10.50	192.168.10.50	TCP	66	63576 → 443 [SYN] Seq=0 Win=8192
50	1.547622	192.168.10.50	192.168.10.50	TCP	66	443 → 63576 [SYN, ACK] Seq=0 Ack=
51	1.547675	192.168.10.50	192.168.10.50	TCP	54	63576 → 443 [ACK] Seq=1 Ack=1 Win
52	1.549052	192.168.10.50	192.168.10.50	TLSv1.2	240	Client Hello
53	1.550413	192.168.10.50	192.168.10.50	TLSv1.2	900	Server Hello, Certificate, Server
54	1.550909	192.168.10.50	192.168.10.50	TLSv1.2	372	Client Key Exchange, Change Ciper
58	1.562066	192.168.10.50	192.168.10.50	TLSv1.2	105	Change Cipher Spec, Encrypted Har
59	1.562718	192.168.10.50	192.168.10.50	TLSv1.2	469	Application Data
60	1.595405	192.168.10.50	192.168.10.50	TLSv1.2	1007	Application Data
61	1.628938	192.168.10.50	192.168.10.50	TLSv1.2	437	Application Data
64	1.666995	192.168.10.50	192.168.10.50	TCP	1420	443 → 63576 [ACK] Seq=1851 Ack=13
65	1.667232	192.168.10.50	192.168.10.50	TCP	1420	443 → 63576 [ACK] Seq=3217 Ack=13
66	1.667284	192.168.10.50	192.168.10.50	TCP	54	63576 → 443 [ACK] Seq=1303 Ack=45
67	1.667423	192.168.10.50	192.168.10.50	TCP	1420	443 → 63576 [ACK] Seq=4583 Ack=13

調試

debug radius all

debug webvpn anyconnect 255

在FTD診斷CLI上運行「debug radius all」命令(>system support diagnostic-cli) , 並在Cisco Anyconnect客戶端的Windows/Mac PC上按一下「Connect」

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
ciscofp3> enable
Password: <hit enter>
ciscofp3# terminal monitor
ciscofp3# debug radius all
<hit Connect on Anyconnect client on PC>

radius mkreq: 0x15
alloc_rip 0x00002ace10875428
new request 0x15 --> 16 (0x00002ace10875428)
got user 'jsmith'
got password
add_req 0x00002ace10875428 session 0x15 id 16
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=198.51.100.2

RADIUS packet decode (authentication request)

-----
Raw packet data (length = 659).....
01 10 02 93 fb 19 19 df f6 b1 c7 3e 34 fc 88 ce | .....>4...
75 38 2d 55 01 08 6a 73 6d 69 74 68 02 12 a0 83 | u8-U..jsmith....
c9 bd ad 72 07 d1 bc 24 34 9e 63 a1 f5 93 05 06 | ...r...$4.c.....
00 00 50 00 1e 10 31 30 2e 32 30 31 2e 32 31 34 | ..P...198.51.100.2
2e 31 35 31 1f 10 31 30 2e 32 30 31 2e 32 31 34 | .151..198.51.100.2
2e 32 35 31 3d 06 00 00 05 42 10 31 30 2e 32 | .4=.....B.198.
30 31 2e 32 31 34 2e 32 35 31 1a 23 00 00 09 | 51.100.2#....
01 1d 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 | ..mdm-tlv=device
2d 70 6c 61 74 66 6f 72 6d 3d 77 69 6e 1a 2c 00 | -platform=win,..
00 00 09 01 26 6d 64 6d 2d 74 6c 76 3d 64 65 76 | ....&mdm-tlv=dev
69 63 65 2d 6d 61 63 3d 30 30 2d 30 63 2d 32 39 | ice-mac=00-0c-29
2d 33 37 2d 65 66 2d 62 66 1a 33 00 00 09 01 | -37-ef-bf.3.....
2d 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d | -mdm-tlv=device-
70 75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 | public-mac=00-0c
2d 32 39 2d 33 37 2d 65 66 2d 62 66 1a 3a 00 00 | -29-37-ef-bf...
00 09 01 34 6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 | ...4mdm-tlv=ac-u
73 65 72 2d 61 67 65 6e 74 3d 41 6e 79 43 6f 6e | ser-agent=AnyCon
6e 65 63 74 20 57 69 6e 64 6f 77 73 20 34 2e 36 | nect Windows 4.6
2e 30 33 30 34 39 1a 3f 00 00 09 01 39 6d 64 | .03049.?......9md
6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 6c 61 | m-tlv=device-pla
74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d 36 2e | tform-version=6.
31 2e 37 36 30 31 20 53 65 72 76 69 63 65 20 50 | 1.7601 Service P
61 63 6b 20 31 1a 40 00 00 09 01 3a 6d 64 6d | ack 1.@.....:mdm
2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 79 70 65 | -tlv=device-type
3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e 20 56 4d | =VMware, Inc. VM
77 61 72 65 20 56 69 72 74 75 61 6c 20 50 6c 61 | ware Virtual Pla
74 66 6f 72 6d 1a 5b 00 00 09 01 55 6d 64 6d | tform.[.....Umdm
2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 69 64 3d | -tlv=device-uid=
33 36 39 33 43 36 34 30 37 43 39 32 35 32 35 31 | 3693C6407C925251
46 46 37 32 42 36 34 39 33 42 44 44 38 37 33 31 | FF72B6493BDD8731
38 41 42 46 43 39 30 43 36 32 31 35 34 32 43 33 | 8ABFC90C621542C3
38 46 41 46 38 37 38 45 46 34 39 36 31 34 41 31 | 8FAF878EF49614A1
04 06 00 00 00 00 1a 31 00 00 09 01 2b 61 75 | .....1.....+au
64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 3d 30 | dit-session-id=0
61 63 39 64 36 38 61 30 30 30 30 35 30 30 30 35 | ac9d68a000050005
62 62 65 31 66 39 31 1a 23 00 00 09 01 1d 69 | bbe1f91.#.....i
70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e 32 | p:source-ip=192.1
```

```
30 31 2e 32 31 34 2e 32 35 31 1a 18 00 00 0c 04 | 68.10.50.....
92 12 46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 | ..FTDAnyConnectV
50 4e 1a 0c 00 00 0c 04 96 06 00 00 00 02 1a 15 | PN.....
00 00 00 09 01 0f 63 6f 61 2d 70 75 73 68 3d 74 | .....coa-push=t
72 75 65 | rue
```

Parsed packet data.....

Radius: Code = 1 (0x01)

Radius: Identifier = 16 (0x10)

Radius: Length = 659 (0x0293)

Radius: Vector: FB1919DFF6B1C73E34FC88CE75382D55

Radius: Type = 1 (0x01) User-Name

Radius: Length = 8 (0x08)

Radius: Value (String) =

6a 73 6d 69 74 68 | jsmith

Radius: Type = 2 (0x02) User-Password

Radius: Length = 18 (0x12)

Radius: Value (String) =

a0 83 c9 bd ad 72 07 d1 bc 24 34 9e 63 a1 f5 93 |r...\$4.c...

Radius: Type = 5 (0x05) NAS-Port

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x5000

Radius: Type = 30 (0x1E) Called-Station-Id

Radius: Length = 16 (0x10)

Radius: Value (String) =

31 30 2e 32 30 31 2e 32 31 34 2e 31 35 31 | 203.0.113.2

Radius: Type = 31 (0x1F) Calling-Station-Id

Radius: Length = 16 (0x10)

Radius: Value (String) =

31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2

Radius: Type = 61 (0x3D) NAS-Port-Type

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x5

Radius: Type = 66 (0x42) Tunnel-Client-Endpoint

Radius: Length = 16 (0x10)

Radius: Value (String) =

31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 35 (0x23)

Radius: Vendor ID = 9 (0x00000009)

Radius: Type = 1 (0x01) Cisco-AV-pair

Radius: Length = 29 (0x1D)

Radius: Value (String) =

6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p

6c 61 74 66 6f 72 6d 3d 77 69 6e | latform=win

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 44 (0x2C)

Radius: Vendor ID = 9 (0x00000009)

Radius: Type = 1 (0x01) Cisco-AV-pair

Radius: Length = 38 (0x26)

Radius: Value (String) =

6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 6d | mdm-tlv=device-m

61 63 3d 30 30 2d 30 63 2d 32 39 2d 33 37 2d 65 | ac=00-0c-29-37-e

66 2d 62 66 | f-bf

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 51 (0x33)

Radius: Vendor ID = 9 (0x00000009)

Radius: Type = 1 (0x01) Cisco-AV-pair

Radius: Length = 45 (0x2D)

Radius: Value (String) =

6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p

75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 2d | ublic-mac=00-0c-

32 39 2d 33 37 2d 65 66 2d 62 66 | 29-37-ef-bf

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 58 (0x3A)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 52 (0x34)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 73 65 72 2d | mdm-tlv=ac-user-
61 67 65 6e 74 3d 41 6e 79 43 6f 6e 6e 65 63 74 | agent=AnyConnect
20 57 69 6e 64 6f 77 73 20 34 2e 36 2e 30 33 30 | Windows 4.6.030
34 39 | 49
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 63 (0x3F)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 57 (0x39)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
6c 61 74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d | latform-version=
36 2e 31 2e 37 36 30 31 20 53 65 72 76 69 63 65 | 6.1.7601 Service
20 50 61 63 6b 20 31 | Pack 1
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 64 (0x40)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 58 (0x3A)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 | mdm-tlv=device-t
79 70 65 3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e | ype=VMware, Inc.
20 56 4d 77 61 72 65 20 56 69 72 74 75 61 6c 20 | VMware Virtual
50 6c 61 74 66 6f 72 6d | Platform
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 91 (0x5B)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 85 (0x55)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 | mdm-tlv=device-u
69 64 3d 33 36 39 33 43 36 34 30 37 43 39 32 35 | id=3693C6407C925
32 35 31 46 46 37 32 42 36 34 39 33 42 44 44 38 | 251FF72B6493BDD8
37 33 31 38 41 42 46 43 39 30 43 36 32 31 35 34 | 7318ABFC90C62154
32 43 33 38 46 41 46 38 37 38 45 46 34 39 36 31 | 2C38FAF878EF4961
34 41 31 | 4A1
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 0.0.0.0 (0x00000000)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 49 (0x31)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 43 (0x2B)
Radius: Value (String) =
61 75 64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 | audit-session-id
3d 30 61 63 39 64 36 38 61 30 30 30 30 35 30 30 | =0ac9d68a0000500
30 35 62 62 65 31 66 39 31 | 05bbe1f91
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 35 (0x23)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 29 (0x1D)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e | ip:source-ip=192.
32 30 31 2e 32 31 34 2e 32 35 31 | 168.10.50
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 24 (0x18)
Radius: Vendor ID = 3076 (0x00000C04)

```
Radius: Type = 146 (0x92) Tunnel-Group-Name
Radius: Length = 18 (0x12)
Radius: Value (String) =
46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 50 4e | FTDAnyConnectVPN
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 150 (0x96) Client-Type
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 2 (0x0002)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 21 (0x15)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 15 (0x0F)
Radius: Value (String) =
63 6f 61 2d 70 75 73 68 3d 74 72 75 65 | coa-push=true
send pkt 192.168.1.10/1812
rip 0x00002ace10875428 state 7 id 16
rad_vrfy() : response message verified
rip 0x00002ace10875428
: chall_state ''
: state 0x7
: reqauth:
fb 19 19 df f6 b1 c7 3e 34 fc 88 ce 75 38 2d 55
: info 0x00002ace10875568
session_id 0x15
request_id 0x10
user 'jsmith'
response '****'
app 0
reason 0
skey 'cisco123'
sip 192.168.1.10
type 1
```

RADIUS packet decode (response)

```
-----
Raw packet data (length = 159).....
02 10 00 9f 39 45 43 cf 05 be df 2f 24 d5 d7 05 | ....9EC..../$...
47 67 b4 fd 01 08 6a 73 6d 69 74 68 18 28 52 65 | Gg....jsmith.(Re
61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61 63 39 | authSession:0ac9
64 36 38 61 30 30 30 30 35 30 30 30 35 62 62 65 | d68a000050005bbe
31 66 39 31 19 3b 43 41 43 53 3a 30 61 63 39 64 | 1f91.;CACS:0ac9d
36 38 61 30 30 30 30 35 30 30 30 35 62 62 65 31 | 68a000050005bbe1
66 39 31 3a 63 6f 72 62 69 6e 69 73 65 2f 33 32 | f91:corbinise/32
32 33 34 34 30 38 34 2f 31 39 33 31 36 38 32 1a | 2344084/1931682.
20 00 00 00 09 01 1a 70 72 6f 66 69 6c 65 2d 6e | .....profile-n
61 6d 65 3d 57 6f 72 6b 73 74 61 74 69 6f 6e | ame=Workstation
```

```
Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 16 (0x10)
Radius: Length = 159 (0x009F)
Radius: Vector: 394543CF05BEDF2F24D5D7054767B4FD
Radius: Type = 1 (0x01) User-Name
Radius: Length = 8 (0x08)
Radius: Value (String) =
6a 73 6d 69 74 68 | jsmith
Radius: Type = 24 (0x18) State
Radius: Length = 40 (0x28)
Radius: Value (String) =
52 65 61 75 74 68 53 65 73 73 69 6f 6e 3a 30 61 | ReauthSession:0a
```

```

63 39 64 36 38 61 30 30 30 30 35 30 30 30 35 62 | c9d68a000050005b
62 65 31 66 39 31 | be1f91
Radius: Type = 25 (0x19) Class
Radius: Length = 59 (0x3B)
Radius: Value (String) =
43 41 43 53 3a 30 61 63 39 64 36 38 61 30 30 30 | CACS:0ac9d68a000
30 35 30 30 30 35 62 62 65 31 66 39 31 3a 63 6f | 050005bbe1f91:co
72 62 69 6e 69 73 65 2f 33 32 32 33 34 34 30 38 | rbinise/32234408
34 2f 31 39 33 31 36 38 32 | 4/1931682
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 32 (0x20)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 26 (0x1A)
Radius: Value (String) =
70 72 6f 66 69 6c 65 2d 6e 61 6d 65 3d 57 6f 72 | profile-name=Wor
6b 73 74 61 74 69 6f 6e | kstation
rad_procpkt: ACCEPT
Got AV-Pair with value profile-name=Workstation
RADIUS_ACCESS_ACCEPT: normal termination
radius mkreq: 0x16
alloc_rip 0x00002ace10874b80
new request 0x16 --> 17 (0x00002ace10874b80)
got user 'jsmith'
got password
add_req 0x00002ace10874b80 session 0x16 id 17
RADIUS_DELETE
remove_req 0x00002ace10875428 session 0x15 id 16
free_rip 0x00002ace10875428
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=198.51.100.2

```

RADIUS packet decode (authentication request)

```

-----
Raw packet data (length = 659).....
01 11 02 93 c6 fc 11 c1 0e c4 81 ac 09 a7 85 a8 | .....
83 c1 e4 88 01 08 6a 73 6d 69 74 68 02 12 79 41 | .....jsmith..yA
0e 71 13 38 ae 9f 49 be 3c a9 e4 81 65 93 05 06 | .q.8..I.<...e...
00 00 50 00 1e 10 31 30 2e 32 30 31 2e 32 31 34 | ..P...203.0.113
2e 31 35 31 1f 10 31 30 2e 32 30 31 2e 32 31 34 | .2..203.0.113
2e 32 35 31 3d 06 00 00 05 42 10 31 30 2e 32 | .2=.....<ip addr
30 31 2e 32 31 34 2e 32 35 31 1a 23 00 00 00 09 | ess>.#....
01 1d 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 | ..mdm-tlv=device
2d 70 6c 61 74 66 6f 72 6d 3d 77 69 6e 1a 2c 00 | -platform=win,..
00 00 09 01 26 6d 64 6d 2d 74 6c 76 3d 64 65 76 | ...&mdm-tlv=dev
69 63 65 2d 6d 61 63 3d 30 30 2d 30 63 2d 32 39 | ice-mac=00-0c-29
2d 33 37 2d 65 66 2d 62 66 1a 33 00 00 00 09 01 | -37-ef-bf.3.....
2d 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d | -mdm-tlv=device-
70 75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 | public-mac=00-0c
2d 32 39 2d 33 37 2d 65 66 2d 62 66 1a 3a 00 00 | -29-37-ef-bf....
00 09 01 34 6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 | ...4mdm-tlv=ac-u
73 65 72 2d 61 67 65 6e 74 3d 41 6e 79 43 6f 6e | ser-agent=AnyCon
6e 65 63 74 20 57 69 6e 64 6f 77 73 20 34 2e 36 | nect Windows 4.6
2e 30 33 30 34 39 1a 3f 00 00 00 09 01 39 6d 64 | .03049.?.....9md
6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 6c 61 | m-tlv=device-pla
74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d 36 2e | tform-version=6.
31 2e 37 36 30 31 20 53 65 72 76 69 63 65 20 50 | 1.7601 Service P
61 63 6b 20 31 1a 40 00 00 00 09 01 3a 6d 64 6d | ack 1.@.....:mdm
2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 79 70 65 | -tlv=device-type
3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e 20 56 4d | =VMware, Inc. VM
77 61 72 65 20 56 69 72 74 75 61 6c 20 50 6c 61 | ware Virtual Pla
74 66 6f 72 6d 1a 5b 00 00 00 09 01 55 6d 64 6d | tform.[.....Umdm

```

```
2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 69 64 3d | -tlv=device-uid=
33 36 39 33 43 36 34 30 37 43 39 32 35 32 35 31 | 3693C6407C925251
46 46 37 32 42 36 34 39 33 42 44 44 38 37 33 31 | FF72B6493BDD8731
38 41 42 46 43 39 30 43 36 32 31 35 34 32 43 33 | 8ABFC90C621542C3
38 46 41 46 38 37 38 45 46 34 39 36 31 34 41 31 | 8FAF878EF49614A1
04 06 00 00 00 00 1a 31 00 00 00 09 01 2b 61 75 | .....1.....+au
64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 3d 30 | dit-session-id=0
61 63 39 64 36 38 61 30 30 30 30 35 30 30 30 35 | ac9d68a000050005
62 62 65 31 66 39 31 1a 23 00 00 00 09 01 1d 69 | bbe1f91.#.....i
70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e 32 | p:source-ip=192.1
30 31 2e 32 31 34 2e 32 35 31 1a 18 00 00 0c 04 | 68.10.50.....
92 12 46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 | ..FTDAnyConnectV
50 4e 1a 0c 00 00 0c 04 96 06 00 00 00 02 1a 15 | PN.....
00 00 00 09 01 0f 63 6f 61 2d 70 75 73 68 3d 74 | .....coa-push=t
72 75 65 | rue
```

Parsed packet data.....

Radius: Code = 1 (0x01)

Radius: Identifier = 17 (0x11)

Radius: Length = 659 (0x0293)

Radius: Vector: C6FC11C10EC481AC09A785A883C1E488

Radius: Type = 1 (0x01) User-Name

Radius: Length = 8 (0x08)

Radius: Value (String) =

6a 73 6d 69 74 68 | jsmith

Radius: Type = 2 (0x02) User-Password

Radius: Length = 18 (0x12)

Radius: Value (String) =

79 41 0e 71 13 38 ae 9f 49 be 3c a9 e4 81 65 93 | yA.q.8..I.<...e.

Radius: Type = 5 (0x05) NAS-Port

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x5000

Radius: Type = 30 (0x1E) Called-Station-Id

Radius: Length = 16 (0x10)

Radius: Value (String) =

31 30 2e 32 30 31 2e 32 31 34 2e 31 35 31 | 203.0.113.2

Radius: Type = 31 (0x1F) Calling-Station-Id

Radius: Length = 16 (0x10)

Radius: Value (String) =

31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2

Radius: Type = 61 (0x3D) NAS-Port-Type

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x5

Radius: Type = 66 (0x42) Tunnel-Client-Endpoint

Radius: Length = 16 (0x10)

Radius: Value (String) =

31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 35 (0x23)

Radius: Vendor ID = 9 (0x00000009)

Radius: Type = 1 (0x01) Cisco-AV-pair

Radius: Length = 29 (0x1D)

Radius: Value (String) =

6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p

6c 61 74 66 6f 72 6d 3d 77 69 6e | latform=win

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 44 (0x2C)

Radius: Vendor ID = 9 (0x00000009)

Radius: Type = 1 (0x01) Cisco-AV-pair

Radius: Length = 38 (0x26)

Radius: Value (String) =

6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 6d | mdm-tlv=device-m

61 63 3d 30 30 2d 30 63 2d 32 39 2d 33 37 2d 65 | ac=00-0c-29-37-e

66 2d 62 66 | f-bf

Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 51 (0x33)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 45 (0x2D)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 2d | ublic-mac=00-0c-
32 39 2d 33 37 2d 65 66 2d 62 66 | 29-37-ef-bf
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 58 (0x3A)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 52 (0x34)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 73 65 72 2d | mdm-tlv=ac-user-
61 67 65 6e 74 3d 41 6e 79 43 6f 6e 6e 65 63 74 | agent=AnyConnect
20 57 69 6e 64 6f 77 73 20 34 2e 36 2e 30 33 30 | Windows 4.6.030
34 39 | 49
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 63 (0x3F)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 57 (0x39)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
6c 61 74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d | latform-version=
36 2e 31 2e 37 36 30 31 20 53 65 72 76 69 63 65 | 6.1.7601 Service
20 50 61 63 6b 20 31 | Pack 1
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 64 (0x40)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 58 (0x3A)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 | mdm-tlv=device-t
79 70 65 3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e | ype=VMware, Inc.
20 56 4d 77 61 72 65 20 56 69 72 74 75 61 6c 20 | VMware Virtual
50 6c 61 74 66 6f 72 6d | Platform
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 91 (0x5B)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 85 (0x55)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 | mdm-tlv=device-u
69 64 3d 33 36 39 33 43 36 34 30 37 43 39 32 35 | id=3693C6407C925
32 35 31 46 46 37 32 42 36 34 39 33 42 44 44 38 | 251FF72B6493BDD8
37 33 31 38 41 42 46 43 39 30 43 36 32 31 35 34 | 7318ABFC90C62154
32 43 33 38 46 41 46 38 37 38 45 46 34 39 36 31 | 2C38FAF878EF4961
34 41 31 | 4A1
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 0.0.0.0 (0x00000000)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 49 (0x31)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 43 (0x2B)
Radius: Value (String) =
61 75 64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 | audit-session-id
3d 30 61 63 39 64 36 38 61 30 30 30 30 35 30 30 | =0ac9d68a0000500
30 35 62 62 65 31 66 39 31 | 05bbe1f91
Radius: Type = 26 (0x1A) Vendor-Specific

```
Radius: Length = 35 (0x23)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 29 (0x1D)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e | ip:source-ip=192.
32 30 31 2e 32 31 34 2e 32 35 31 | 168.10.50
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 24 (0x18)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 146 (0x92) Tunnel-Group-Name
Radius: Length = 18 (0x12)
Radius: Value (String) =
46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 50 4e | FTDAnyConnectVPN
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 150 (0x96) Client-Type
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 2 (0x0002)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 21 (0x15)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 15 (0x0F)
Radius: Value (String) =
63 6f 61 2d 70 75 73 68 3d 74 72 75 65 | coa-push=true
send pkt 192.168.1.10/1812
rip 0x00002ace10874b80 state 7 id 17
rad_vrfy() : response message verified
rip 0x00002ace10874b80
: chall_state ''
: state 0x7
: reqauth:
c6 fc 11 c1 0e c4 81 ac 09 a7 85 a8 83 c1 e4 88
: info 0x00002ace10874cc0
session_id 0x16
request_id 0x11
user 'jsmith'
response '****'
app 0
reason 0
skey 'cisco123'
sip 192.168.1.10
type 1
```

RADIUS packet decode (response)

```
-----
Raw packet data (length = 20).....
03 11 00 14 15 c3 44 44 7d a6 07 0d 7b 92 f2 3b | .....DD}...{...;
0b 06 ba 74 | ...t
```

Parsed packet data.....

```
Radius: Code = 3 (0x03)
Radius: Identifier = 17 (0x11)
Radius: Length = 20 (0x0014)
Radius: Vector: 15C344447DA6070D7B92F23B0B06BA74
rad_procpkt: REJECT
RADIUS_DELETE
remove_req 0x00002ace10874b80 session 0x16 id 17
free_rip 0x00002ace10874b80
radius: send queue empty
radius mkreq: 0x18
```

alloc_rip 0x00002ace10874b80
new request 0x18 --> 18 (0x00002ace10874b80)
add_req 0x00002ace10874b80 session 0x18 id 18
ACCT_REQUEST
radius.c: rad_mkpkt

RADIUS packet decode (accounting request)

```
-----  
Raw packet data (length = 714).....  
04 12 02 ca be a0 6e 46 71 af 5c 65 82 77 c7 b5 | .....nFq.\e.w..  
50 78 61 d7 01 08 6a 73 6d 69 74 68 05 06 00 00 | Pxa...jsmith....  
50 00 06 06 00 00 00 02 07 06 00 00 00 01 08 06 | P.....  
c0 a8 0a 32 19 3b 43 41 43 53 3a 30 61 63 39 64 | ...2.;CACS:0ac9d  
36 38 61 30 30 30 30 35 30 30 30 35 62 62 65 31 | 68a000050005bbe1  
66 39 31 3a 63 6f 72 62 69 6e 69 73 65 2f 33 32 | f91:corbinise/32  
32 33 34 34 30 38 34 2f 31 39 33 31 36 38 32 1e | 2344084/1931682.  
10 31 30 2e 32 30 31 2e 32 31 34 2e 31 35 31 1f | .203.0.113.2.  
10 31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 28 | .198.51.100.2(  
06 00 00 00 01 29 06 00 00 00 00 2c 0a 43 31 46 | .....),.....,C1F  
30 30 30 30 35 2d 06 00 00 00 01 3d 06 00 00 00 | 00005-.....=....  
05 42 10 31 30 2e 32 30 31 2e 32 31 34 2e 32 35 | .B.203.0.113.2  
31 1a 18 00 00 0c 04 92 12 46 54 44 41 6e 79 43 | .....FTDAnyC  
6f 6e 6e 65 63 74 56 50 4e 1a 0c 00 00 0c 04 96 | onnectVPN.....  
06 00 00 00 02 1a 0c 00 00 0c 04 97 06 00 00 00 | .....  
01 1a 0c 00 00 0c 04 98 06 00 00 00 03 1a 23 00 | .....#.  
00 00 09 01 1d 6d 64 6d 2d 74 6c 76 3d 64 65 76 | ....mdm-tlv=dev  
69 63 65 2d 70 6c 61 74 66 6f 72 6d 3d 77 69 6e | ice-platform=win  
1a 2c 00 00 00 09 01 26 6d 64 6d 2d 74 6c 76 3d | ,.....&mdm-tlv=  
64 65 76 69 63 65 2d 6d 61 63 3d 30 30 2d 30 63 | device-mac=00-0c  
2d 32 39 2d 33 37 2d 65 66 2d 62 66 1a 31 00 00 | -29-37-ef-bf.1..  
00 09 01 2b 61 75 64 69 74 2d 73 65 73 73 69 6f | ...+audit-sessio  
6e 2d 69 64 3d 30 61 63 39 64 36 38 61 30 30 30 | n-id=0ac9d68a000  
30 35 30 30 30 35 62 62 65 31 66 39 31 1a 33 00 | 050005bbelf91.3.  
00 00 09 01 2d 6d 64 6d 2d 74 6c 76 3d 64 65 76 | ....-mdm-tlv=dev  
69 63 65 2d 70 75 62 6c 69 63 2d 6d 61 63 3d 30 | ice-public-mac=0  
30 2d 30 63 2d 32 39 2d 33 37 2d 65 66 2d 62 66 | 0-0c-29-37-ef-bf  
1a 3a 00 00 00 09 01 34 6d 64 6d 2d 74 6c 76 3d | :.....4mdm-tlv=  
61 63 2d 75 73 65 72 2d 61 67 65 6e 74 3d 41 6e | ac-user-agent=An  
79 43 6f 6e 6e 65 63 74 20 57 69 6e 64 6f 77 73 | yConnect Windows  
20 34 2e 36 2e 30 33 30 34 39 1a 3f 00 00 00 09 | 4.6.03049.?....  
01 39 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 | .9mdm-tlv=device  
2d 70 6c 61 74 66 6f 72 6d 2d 76 65 72 73 69 6f | -platform-versio  
6e 3d 36 2e 31 2e 37 36 30 31 20 53 65 72 76 69 | n=6.1.7601 Servi  
63 65 20 50 61 63 6b 20 31 1a 40 00 00 00 09 01 | ce Pack 1.@.....  
3a 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d | :mdm-tlv=device-  
74 79 70 65 3d 56 4d 77 61 72 65 2c 20 49 6e 63 | type=VMware, Inc  
2e 20 56 4d 77 61 72 65 20 56 69 72 74 75 61 6c | . VMware Virtual  
20 50 6c 61 74 66 6f 72 6d 1a 5b 00 00 00 09 01 | Platform.[.....  
55 6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d | Umdm-tlv=device-  
75 69 64 3d 33 36 39 33 43 36 34 30 37 43 39 32 | uid=3693C6407C92  
35 32 35 31 46 46 37 32 42 36 34 39 33 42 44 44 | 5251FF72B6493BDD  
38 37 33 31 38 41 42 46 43 39 30 43 36 32 31 35 | 87318ABFC90C6215  
34 32 43 33 38 46 41 46 38 37 38 45 46 34 39 36 | 42C38FAF878EF496  
31 34 41 31 04 06 00 00 00 00 | 14A1.....
```

Parsed packet data.....
Radius: Code = 4 (0x04)
Radius: Identifier = 18 (0x12)
Radius: Length = 714 (0x02CA)
Radius: Vector: BEA06E4671AF5C658277C7B5507861D7
Radius: Type = 1 (0x01) User-Name
Radius: Length = 8 (0x08)
Radius: Value (String) =

6a 73 6d 69 74 68 | jsmith
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5000
Radius: Type = 6 (0x06) Service-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x2
Radius: Type = 7 (0x07) Framed-Protocol
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 8 (0x08) Framed-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 192.168.10.50 (0xC0A80A32)
Radius: Type = 25 (0x19) Class
Radius: Length = 59 (0x3B)
Radius: Value (String) =
43 41 43 53 3a 30 61 63 39 64 36 38 61 30 30 30 | CACS:0ac9d68a000
30 35 30 30 30 35 62 62 65 31 66 39 31 3a 63 6f | 050005bbelf91:co
72 62 69 6e 69 73 65 2f 33 32 32 33 34 34 30 38 | rbinise/32234408
34 2f 31 39 33 31 36 38 32 | 4/1931682
Radius: Type = 30 (0x1E) Called-Station-Id
Radius: Length = 16 (0x10)
Radius: Value (String) =
31 30 2e 32 30 31 2e 32 31 34 2e 31 35 31 | 203.0.113.2
Radius: Type = 31 (0x1F) Calling-Station-Id
Radius: Length = 16 (0x10)
Radius: Value (String) =
31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2
Radius: Type = 40 (0x28) Acct-Status-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 41 (0x29) Acct-Delay-Time
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x0
Radius: Type = 44 (0x2C) Acct-Session-Id
Radius: Length = 10 (0x0A)
Radius: Value (String) =
43 31 46 30 30 30 30 35 | C1F00005
Radius: Type = 45 (0x2D) Acct-Authentic
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 61 (0x3D) NAS-Port-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5
Radius: Type = 66 (0x42) Tunnel-Client-Endpoint
Radius: Length = 16 (0x10)
Radius: Value (String) =
31 30 2e 32 30 31 2e 32 31 34 2e 32 35 31 | 198.51.100.2
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 24 (0x18)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 146 (0x92) Tunnel-Group-Name
Radius: Length = 18 (0x12)
Radius: Value (String) =
46 54 44 41 6e 79 43 6f 6e 6e 65 63 74 56 50 4e | FTDAAnyConnectVPN
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 150 (0x96) Client-Type
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 2 (0x0002)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)

Radius: Type = 151 (0x97) VPN-Session-Type
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 1 (0x0001)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 12 (0x0C)
Radius: Vendor ID = 3076 (0x00000C04)
Radius: Type = 152 (0x98) VPN-Session-Subtype
Radius: Length = 6 (0x06)
Radius: Value (Integer) = 3 (0x0003)
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 35 (0x23)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 29 (0x1D)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
6c 61 74 66 6f 72 6d 3d 77 69 6e | latform=win
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 44 (0x2C)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 38 (0x26)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 6d | mdm-tlv=device-m
61 63 3d 30 30 2d 30 63 2d 32 39 2d 33 37 2d 65 | ac=00-0c-29-37-e
66 2d 62 66 | f-bf
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 49 (0x31)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 43 (0x2B)
Radius: Value (String) =
61 75 64 69 74 2d 73 65 73 73 69 6f 6e 2d 69 64 | audit-session-id
3d 30 61 63 39 64 36 38 61 30 30 30 30 35 30 30 | =0ac9d68a0000500
30 35 62 62 65 31 66 39 31 | 05bbe1f91
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 51 (0x33)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 45 (0x2D)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
75 62 6c 69 63 2d 6d 61 63 3d 30 30 2d 30 63 2d | ublic-mac=00-0c-
32 39 2d 33 37 2d 65 66 2d 62 66 | 29-37-ef-bf
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 58 (0x3A)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 52 (0x34)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 61 63 2d 75 73 65 72 2d | mdm-tlv=ac-user-
61 67 65 6e 74 3d 41 6e 79 43 6f 6e 6e 65 63 74 | agent=AnyConnect
20 57 69 6e 64 6f 77 73 20 34 2e 36 2e 30 33 30 | Windows 4.6.030
34 39 | 49
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 63 (0x3F)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 57 (0x39)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 70 | mdm-tlv=device-p
6c 61 74 66 6f 72 6d 2d 76 65 72 73 69 6f 6e 3d | latform-version=
36 2e 31 2e 37 36 30 31 20 53 65 72 76 69 63 65 | 6.1.7601 Service
20 50 61 63 6b 20 31 | Pack 1

```

Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 64 (0x40)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 58 (0x3A)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 74 | mdm-tlv=device-t
79 70 65 3d 56 4d 77 61 72 65 2c 20 49 6e 63 2e | ype=VMware, Inc.
20 56 4d 77 61 72 65 20 56 69 72 74 75 61 6c 20 | VMware Virtual
50 6c 61 74 66 6f 72 6d | Platform
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 91 (0x5B)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 85 (0x55)
Radius: Value (String) =
6d 64 6d 2d 74 6c 76 3d 64 65 76 69 63 65 2d 75 | mdm-tlv=device-u
69 64 3d 33 36 39 33 43 36 34 30 37 43 39 32 35 | id=3693C6407C925
32 35 31 46 46 37 32 42 36 34 39 33 42 44 44 38 | 251FF72B6493BDD8
37 33 31 38 41 42 46 43 39 30 43 36 32 31 35 34 | 7318ABFC90C62154
32 43 33 38 46 41 46 38 37 38 45 46 34 39 36 31 | 2C38FAF878EF4961
34 41 31 | 4A1
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 0.0.0.0 (0x00000000)
send pkt 192.168.1.10/1813
rip 0x00002ace10874b80 state 6 id 18
rad_vrfy() : response message verified
rip 0x00002ace10874b80
: chall_state ''
: state 0x6
: reqauth:
be a0 6e 46 71 af 5c 65 82 77 c7 b5 50 78 61 d7
: info 0x00002ace10874cc0
session_id 0x18
request_id 0x12
user 'jsmith'
response '****'
app 0
reason 0
skey 'cisco123'
sip 192.168.1.10
type 3

```

RADIUS packet decode (response)

```

-----
Raw packet data (length = 20).....
05 12 00 14 e5 fd b1 6d fb ee 58 f0 89 79 73 8e | .....m..X..ys.
90 dc a7 20 | ...

```

```

Parsed packet data.....
Radius: Code = 5 (0x05)
Radius: Identifier = 18 (0x12)
Radius: Length = 20 (0x0014)
Radius: Vector: E5FDB16DFBEE58F08979738E90DCA720
rad_procpkt: ACCOUNTING_RESPONSE
RADIUS_DELETE
remove_req 0x00002ace10874b80 session 0x18 id 18
free_rip 0x00002ace10874b80
radius: send queue empty
ciscofp3#

```

在FTD診斷CLI上運行「debug webvpn anyconnect 255」命令(>system support diagnostic-cli) , 並

在Cisco Anyconnect客戶端的Windows/Mac PC上按一下「Connect」

```
> system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
```

```
ciscofp3> enable
```

```
Password: <hit enter>
```

```
ciscofp3# terminal monitor
```

```
ciscofp3# debug webvpn anyconnect 255
```

```
<hit Connect on Anyconnect client on PC>
```

```
http_parse_cstp_method()
```

```
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'Host: ciscofp3.cisco.com'
```

```
Processing CSTP header line: 'Host: ciscofp3.cisco.com'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 4.6.03049'
```

```
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 4.6.03049'
```

```
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 4.6.03049'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'Cookie: webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
```

```
Processing CSTP header line: 'Cookie:
```

```
webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
```

```
Found WebVPN cookie: 'webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
```

```
WebVPN Cookie: 'webvpn=2B0E85@28672@6501@2FF4AE4D1F69B98F26E8CAD62D5496E5E6AE5282'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Version: 1'
```

```
Processing CSTP header line: 'X-CSTP-Version: 1'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Hostname: jsmith-PC'
```

```
Processing CSTP header line: 'X-CSTP-Hostname: jsmith-PC'
```

```
Setting hostname to: 'jsmith-PC'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-MTU: 1399'
```

```
Processing CSTP header line: 'X-CSTP-MTU: 1399'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Address-Type: IPv6,IPv4'
```

```
Processing CSTP header line: 'X-CSTP-Address-Type: IPv6,IPv4'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Local-Address-IP4: 198.51.100.2'
```

```
Processing CSTP header line: 'X-CSTP-Local-Address-IP4: 198.51.100.2'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Base-MTU: 1500'
```

```
Processing CSTP header line: 'X-CSTP-Base-MTU: 1500'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Remote-Address-IP4: 203.0.113.2'
```

```
Processing CSTP header line: 'X-CSTP-Remote-Address-IP4: 203.0.113.2'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Full-IPv6-Capability: true'
```

```
Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-DTLS-Master-Secret:
```

```
1FA92A96D5E82C13CB3A5758F11371EE6B54C6F36F0A8DCE8F4DECB73A034EEF4FE95DA614A5872E1EE5557C3BF4765A
```

```
'
```

```
Processing CSTP header line: 'X-DTLS-Master-Secret:
```

```
1FA92A96D5E82C13CB3A5758F11371EE6B54C6F36F0A8DCE8F4DECB73A034EEF4FE95DA614A5872E1EE5557C3BF4765A
```

```
'
```

```
webvpn_cstp_parse_request_field()
```

```
...input: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-
```

```
SHA:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:AES256-SHA:AES128-
```

```
SHA:DES-CBC3-SHA'
```

```
Processing CSTP header line: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-
```

```
SHA256:DHE-RSA-AES256-SHA:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-
SHA:AES256-SHA:AES128-SHA:DES-CBC3-SHA'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Accept-Encoding: lzs'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: lzs,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
cstp_util_address_ipv4_accept: address assigned: 192.168.10.50
cstp_util_address_ipv6_accept: No IPv6 Address
np_svc_create_session(0x7000, 0x00002acdffd6440, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
vpn_put_uauth success for ip 192.168.10.50!
No SVC ACL
Iphdr=20 base-mtu=1500 def-mtu=1500 conf-mtu=1406
tcp-mss = 1460
path-mtu = 1460(mss)
TLS Block size = 16, version = 0x303
mtu = 1460(path-mtu) - 0(opts) - 5(ssl) - 16(iv) = 1439
mod-mtu = 1439(mtu) & 0xfff0(complement) = 1424
tls-mtu = 1424(mod-mtu) - 8(cstp) - 48(mac) - 1(pad) = 1367
DTLS Block size = 16
mtu = 1500(base-mtu) - 20(ip) - 8(udp) - 13(dtls_hdr) - 16(dtls_iv) = 1443
mod-mtu = 1443(mtu) & 0xfff0(complement) = 1440
dtls-mtu = 1440(mod-mtu) - 1(cstp) - 20(mac) - 1(pad) = 1418
computed tls-mtu=1367 dtls-mtu=1418 conf-mtu=1406
DTLS enabled for intf=3 (outside)
override computed dtls-mtu=1418 with conf-mtu=1406
tls-mtu=1367 dtls-mtu=1406
SVC: adding to sessmgmt
Sending X-CSTP-MTU: 1367
Sending X-DTLS-MTU: 1406
Sending X-CSTP-FW-RULE msgs: Start
Sending X-CSTP-FW-RULE msgs: Done
Sending X-CSTP-Quarantine: false
Sending X-CSTP-Disable-Always-On-VPN: false
Sending X-CSTP-Client-Bypass-Protocol: false
```

Cisco ISE

Cisco ISE > Operations > RADIUS > Live Logs > 點選每個身份驗證的詳細資訊

在Cisco ISE驗證您的VPN登入並給出ACL結果「PermitAccess」
即時日誌顯示通過VPN成功向FTD驗證的jsmith

Overview

Event	5200 Authentication succeeded
Username	jsmith
Endpoint Id	
Endpoint Profile	
Authentication Policy	VPN Users >> Default
Authorization Policy	VPN Users >> Allow ASA VPN connections if AD Group VPNUsers
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2018-10-09 01:47:55.112
Received Timestamp	2018-10-09 01:47:55.113
Policy Server	corbinise
Event	5200 Authentication succeeded
Username	jsmith
Endpoint Id	
Calling Station Id	
Authentication Identity Store	corbdc3
Audit Session Id	0000000000070005bbc08c3
Authentication Method	PAP_ASCII
Authentication Protocol	PAP_ASCII
Network Device	FTDVPN
Device Type	All Device Types
Location	All Locations

Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - Airespace Airespace-Wlan-Id
- 15048 Queried PIP - Radius.NAS-Port-Type
- 15041 Evaluating Identity Policy
- 15048 Queried PIP - Normalised Radius.RadiusFlowType
- 22072 Selected identity source sequence - All_User_ID_Stores
- 15013 Selected Identity Source - Internal Users
- 24210 Looking up User in Internal Users IDStore - jsmith
- 24216 The user is not found in the internal users identity store
- 15013 Selected Identity Source - All_AD_Join_Points
- 24430 Authenticating user against Active Directory - All_AD_Join_Points
- 24325 Resolving identity - jsmith (Step latency=7106 ms)
- 24313 Search for matching accounts at join point -
- 24319 Single matching account found in forest -
- 24313 Search for matching accounts at join point - windows_ad_server.com
- 24366 Skipping unjoined domain - Windows_AD_Server.com
- 24323 Identity resolution detected single matching account
- 24343 RPC Logon request succeeded - jsmith
- 24402 User authentication against Active Directory succeeded - All_AD_Join_Points
- 22037 Authentication Passed
- 24715 ISE has not confirmed locally previous successful machine authentication for user in Active Directory
- 15036 Evaluating Authorization Policy
- 24432 Looking up user in Active Directory -
- 24355 LDAP fetch succeeded -
- 24416 User's Groups retrieval from Active Directory succeeded -
- 15048 Queried PIP - ExternalGroups
- 15016 Selected Authorization Profile - PermitAccess
- 22081 Max sessions policy passed
- 22080 New accounting session created in Session cache
- 11002 Returned RADIUS Access-Accept

Location	All Locations
NAS IPv4 Address	0.0.0.0
NAS Port Type	Virtual
Authorization Profile	PermitAccess
Response Time	7294 milliseconds

Other Attributes

ConfigVersionId	257
DestinationPort	1812
Protocol	Radius
NAS-Port	28672
Tunnel-Client-Endpoint	(tag=0)
CVPN3000/ASA/PIX7x-Tunnel-Group-Name	FTDAnyConnectVPN
OriginalUserName	jsmith
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
CVPN3000/ASA/PIX7x-Client-Type	3
AcsSessionID	corbinise/322344084/1870108
SelectedAuthenticationIdentityStores	Internal Users
SelectedAuthenticationIdentityStores	All_AD_Join_Points
SelectedAuthenticationIdentityStores	Guest Users
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatchedRule	Allow ASA VPN connections if AD Group VPNusers
CPMSessionID	00000000000070005bbc08c3

CPMSessionID	00000000000070005bbc08c3
ISEPolicySetName	VPN Users
IdentitySelectionMatchedRule	Default
StepLatency	14=7106
AD-User-Resolved-Identities	jsmith@cohadley3.local
AD-User-Candidate-Identities	jsmith@cohadley3.local
AD-User-Join-Point	COHADLEY3.LOCAL
AD-User-Resolved-DNs	CN=John Smith,CN=Users,DC=cohadley3,DC=local
AD-User-DNS-Domain	cohadley3.local

AD-User-NetBios-Name	COHADLEY3
IsMachineIdentity	false
UserAccountControl	66048
AD-User-SamAccount-Name	jsmith
AD-User-Qualified-Name	jsmith@cohadley3.local
DTLS Support	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
ExternalGroups	S-1-5-21-872014162-156988481-842954196-1121
IdentityAccessRestricted	false
RADIUS Username	jsmith
Device IP Address	
Called-Station-ID	
CiscoAVPair	audit-session-id=00000000000070005bbc08c3, ip:source-ip= coa-push=true

AnyConnect VPN客戶端

DART捆綁包

[如何收集AnyConnect的DART捆綁包](#)

疑難排解

DNS

驗證Cisco ISE、FTD、Windows Server 2012和Windows/Mac PC均可以相互進行正向和反向解析
(檢查所有裝置上的DNS)

Windows電腦

啟動命令提示符，並確保可以對FTD的主機名執行「nslookup」

FTD CLI

```
>show network
```

```
> nslookup 192.168.1.10
Server: 192.168.1.10
Address: 192.168.1.10#53
10.1.168.192.in-addr.arpa name = ciscoise.cisco.com
```

ISE CLI:

```
ciscoise/admin# nslookup 192.168.1.20
Trying "20.1.168.192.in-addr.arpa"
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 56529
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;20.1.168.192.in-addr.arpa. IN PTR

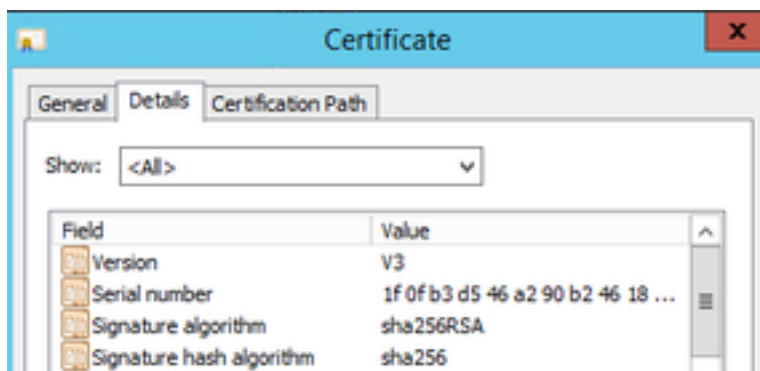
;; ANSWER SECTION:
20.1.168.192.in-addr.arpa. 1200 IN PTR ciscodc.cisco.com
```

Windows Server 2012

啟動命令提示符，並確保可以對FTD的主機名/FQDN執行「nslookup」

證書強度 (用於瀏覽器相容性)

驗證Windows Server 2012將證書標籤為SHA256或更高版本。在Windows中按兩下您的根CA證書，然後檢查「簽名演算法」欄位



如果是SHA1，則大多數瀏覽器都會顯示這些證書的瀏覽器警告。若要變更此檔案，您可以檢視此處：

[如何將Windows Server Certification Authority升級到SHA256](#)

驗證FTD VPN伺服器憑證是否具有以下欄位正確 (在瀏覽器中連線到FTD時)

公用名= <FTDFQDN>

使用者替代名稱(SAN)= <FTDFQDN>

範例：

公用名：ciscofp3.cisco.com

使用者替代名稱(SAN):DNS名稱=ciscofp3.cisco.com

連線和防火牆配置

在FTD CLI上使用擷取進行驗證，並在員工PC上使用Wireshark進行驗證，以驗證封包是否通過TCP+UDP 443到達FTD的外部IP。驗證這些資料包是否來自員工的家庭路由器的公用IP地址

```
ciscofp3# capture capin interface outside trace detail trace-count 100 match ip any host
```

```
<now hit Connect on AnyConnect Client from employee PC>
```

```
ciscofp3# show cap
```

```
capture capin type raw-data trace detail trace-count 100 interface outside [Buffer Full - 524153 bytes]
```

```
match ip any host 198.51.100.2
```

```
ciscofp3# show cap capin
```

```
2375 packets captured
```

```
1: 17:05:56.580994 198.51.100.2.55928 > 203.0.113.2.443: S 2933933902:2933933902(0) win 8192
```

```
2: 17:05:56.581375 203.0.113.2.443 > 198.51.100.2.55928: S 430674106:430674106(0) ack 2933933903 win 32768
```

```
3: 17:05:56.581757 198.51.100.2.55928 > 203.0.113.2.443: . ack 430674107 win 64240
```

```
...
```