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

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。

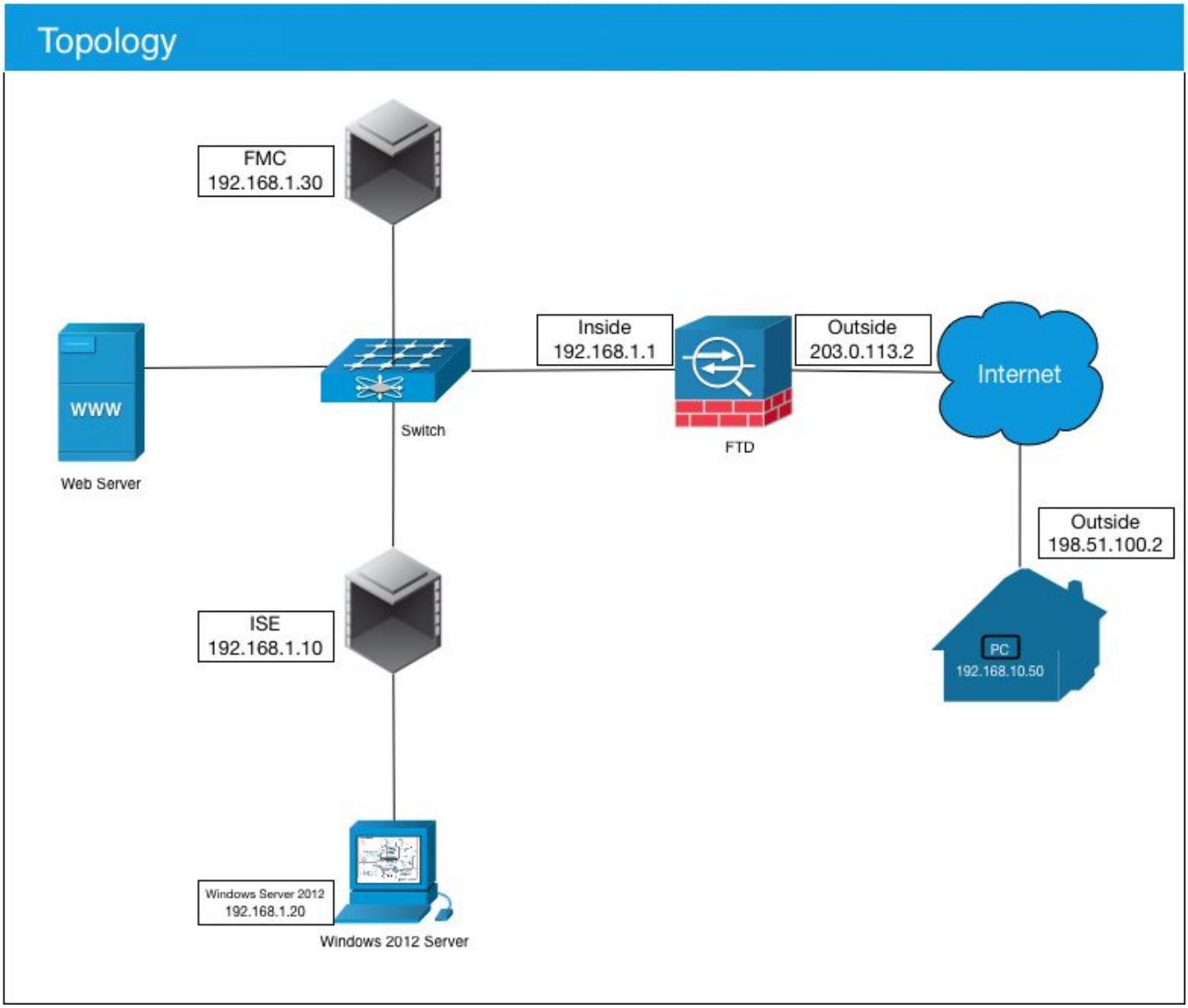
採用元件

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



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	ciscodc.cisco.com	-	192.168.1.20	-
內部伺服器	-	-	192.168.1.x	-

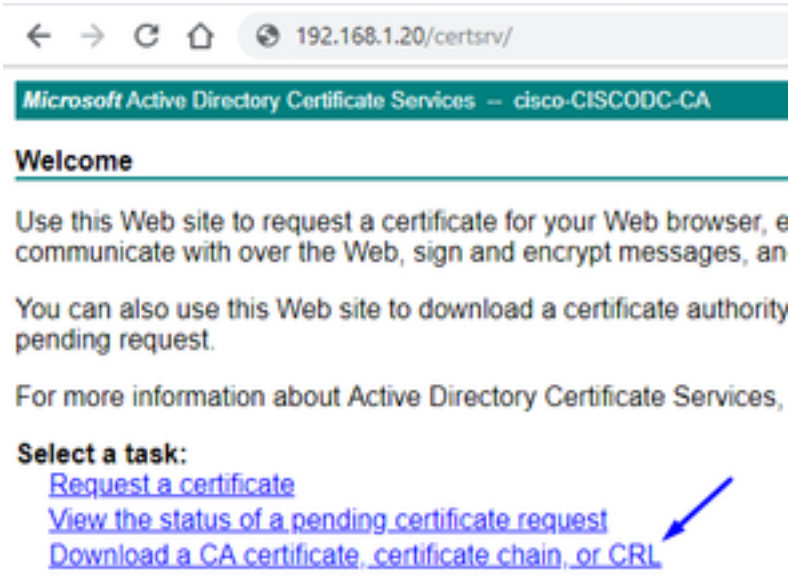
組態

從Windows Server匯出根CA證書

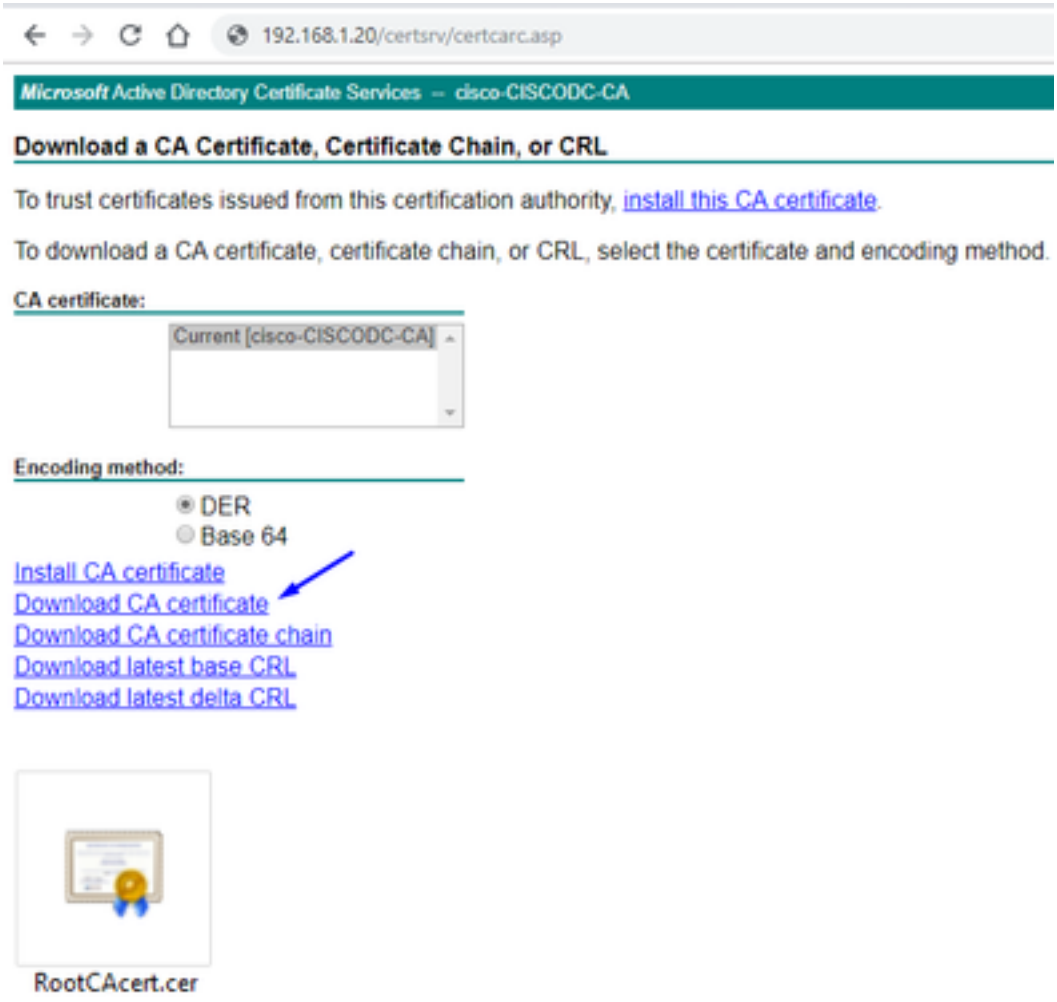
在本文檔中，我們將使用Microsoft Windows Server 2012作為證書的根CA。使用者端PC會信任此根CA通過VPN安全連線到FTD（請參閱以下步驟）。 這樣可以確保使用者通過Internet安全連線到FTD，並從家中訪問內部資源。他們的PC將信任其瀏覽器和AnyConnect客戶端中的連線。

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**」



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



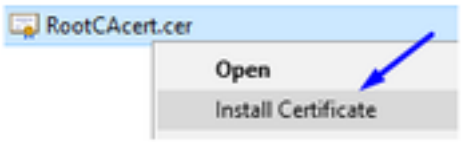
在員工Windows/Mac PC上安裝根CA證書

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]

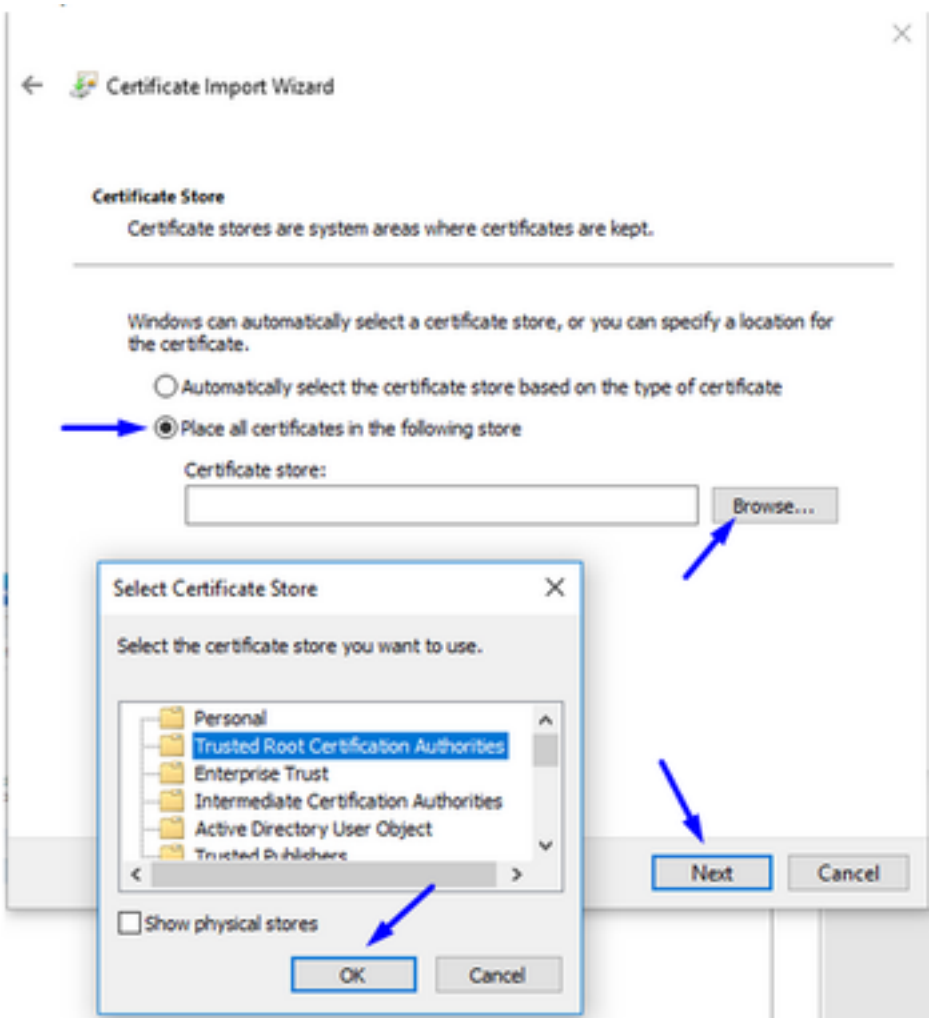
方法2:通過在每台PC上單獨安裝證書，在所有員工PC上安裝證書（非常適合測試一個VPN使用者）：

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」

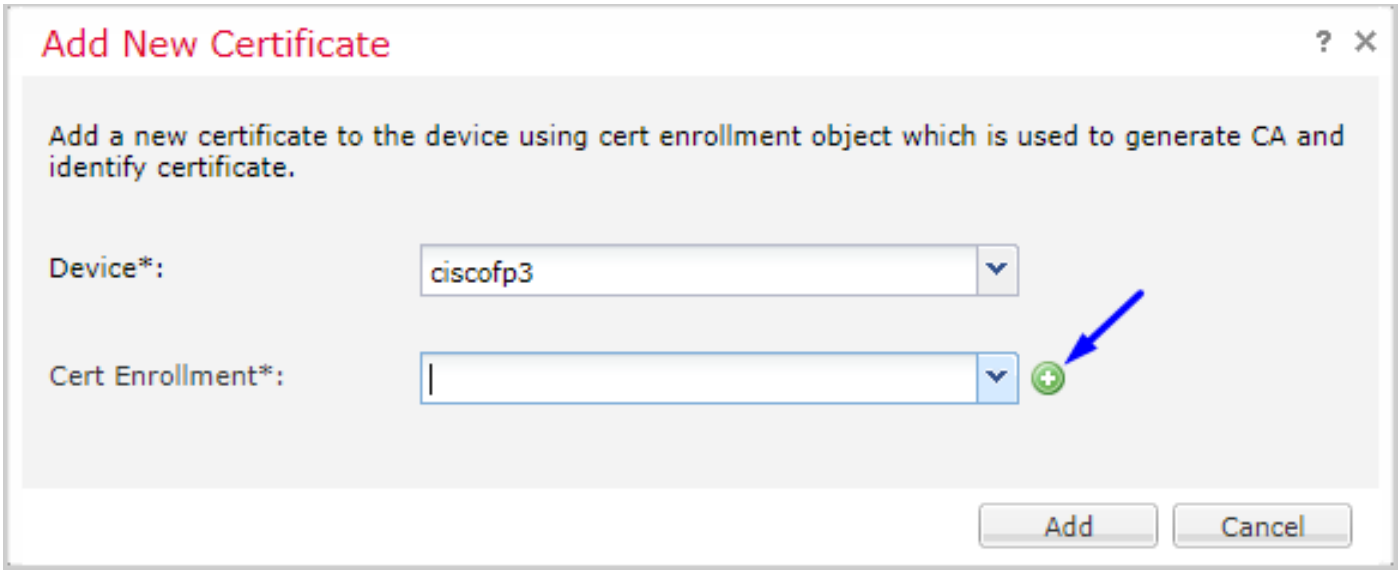
選擇**將所有證書放入以下儲存**，然後選擇**Trusted Root Certification Authorities**，按一下**Ok**，按一下**Next**，然後按一下**Finish**



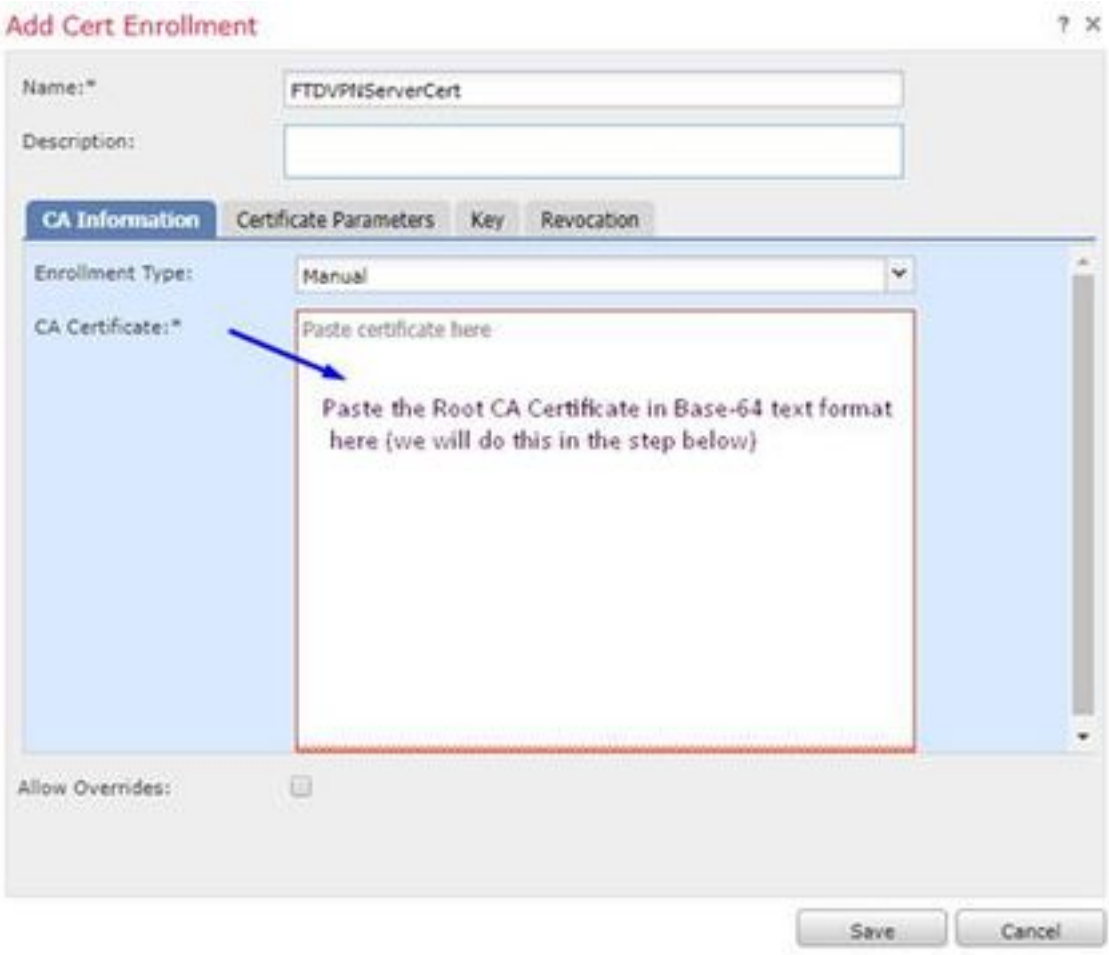
在FTD上產生CSR、取得Windows伺服器根CA簽名的CSR，然後在FTD上安裝已簽署的憑證

轉至Objects > Object Management > **PKI** > **Cert** Enrollment，按一下**AddCert Enrollment**

按一下**Add Cert Enrollment**按鈕



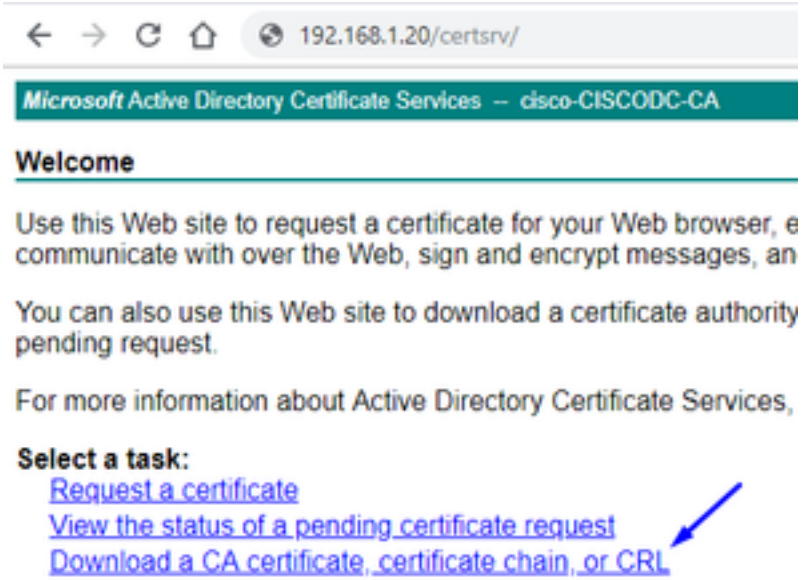
選擇**Enrollment Type > Manual**
如下圖所示，我們需要將根CA證書貼上到此處：



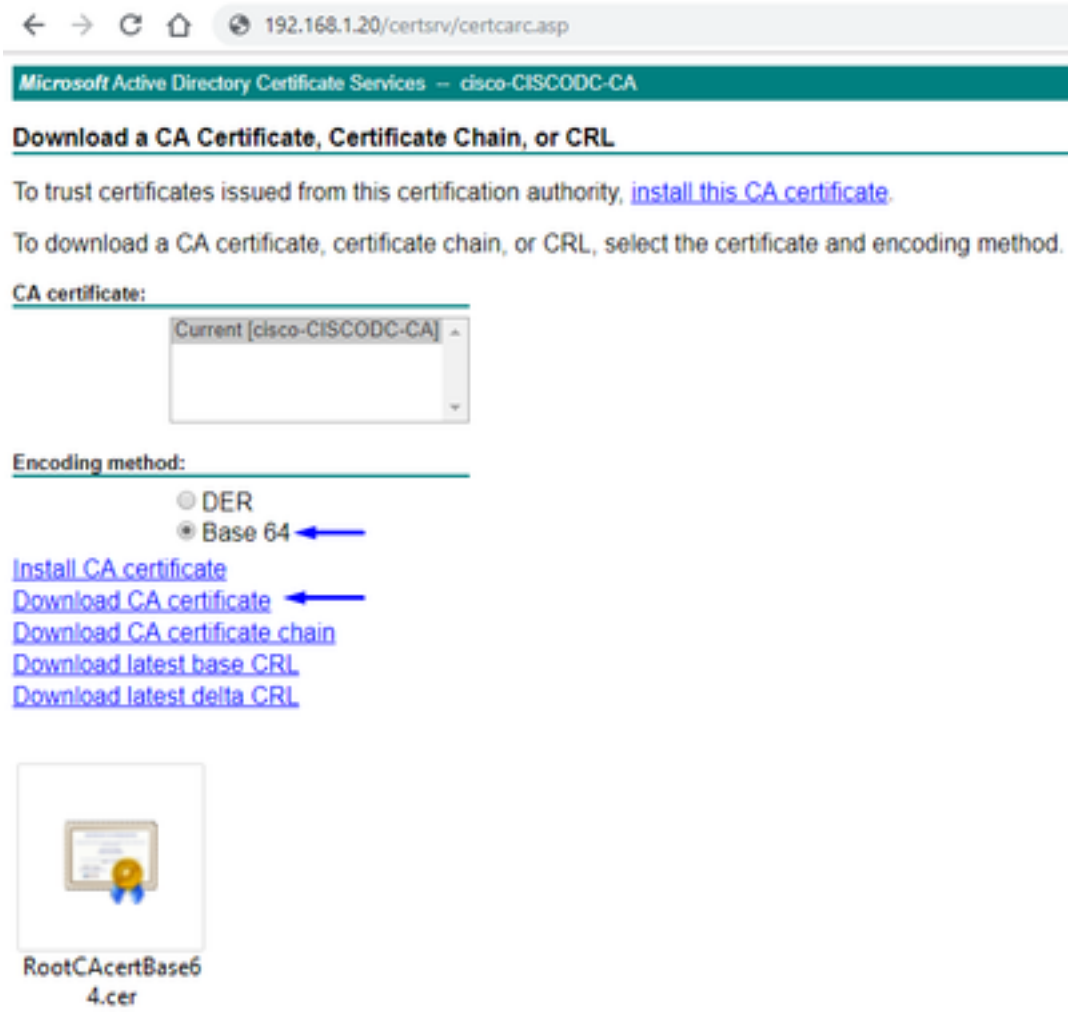
以下是下載根CA憑證、以文字格式檢視並將其貼上到以上方塊中的方式：

轉到http://192.168.1.20/certsrv

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

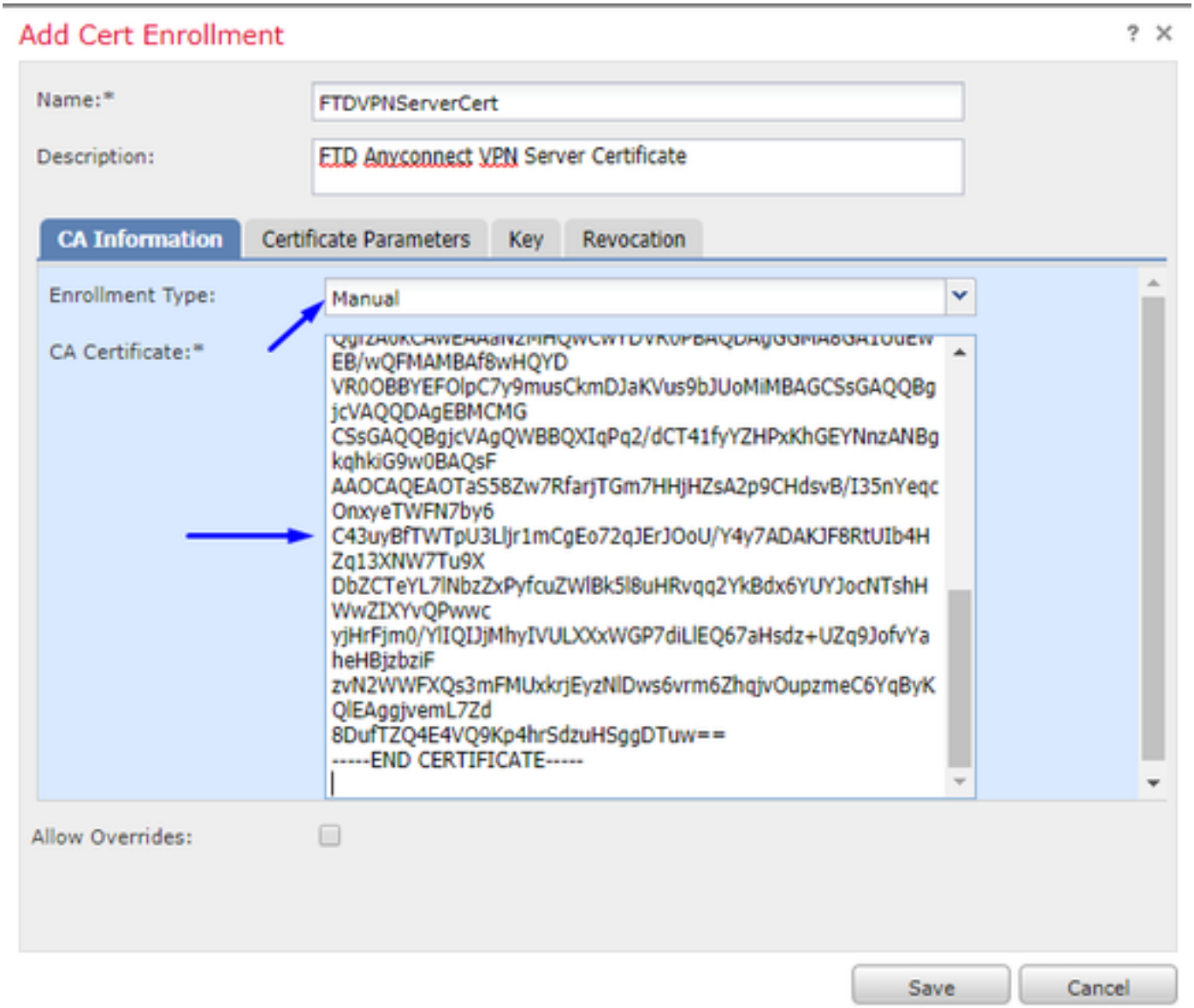


按一下**Base 64**按鈕>按一下**Download CA Certificate**



在記事本中開啟RootCAcertBase64.cer檔案

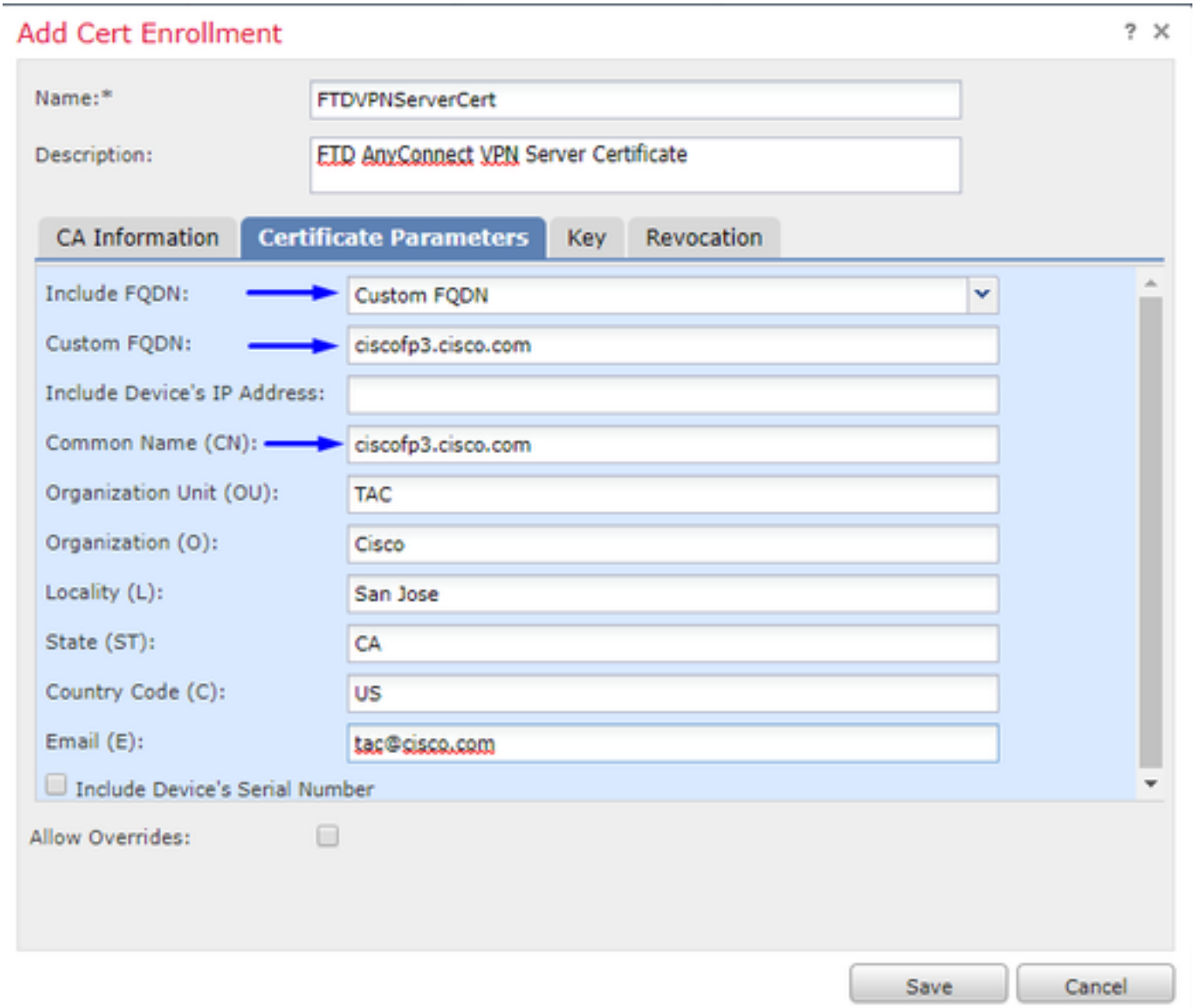
從以下Windows AD Server複製並貼上.cer內容（根CA證書）：



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

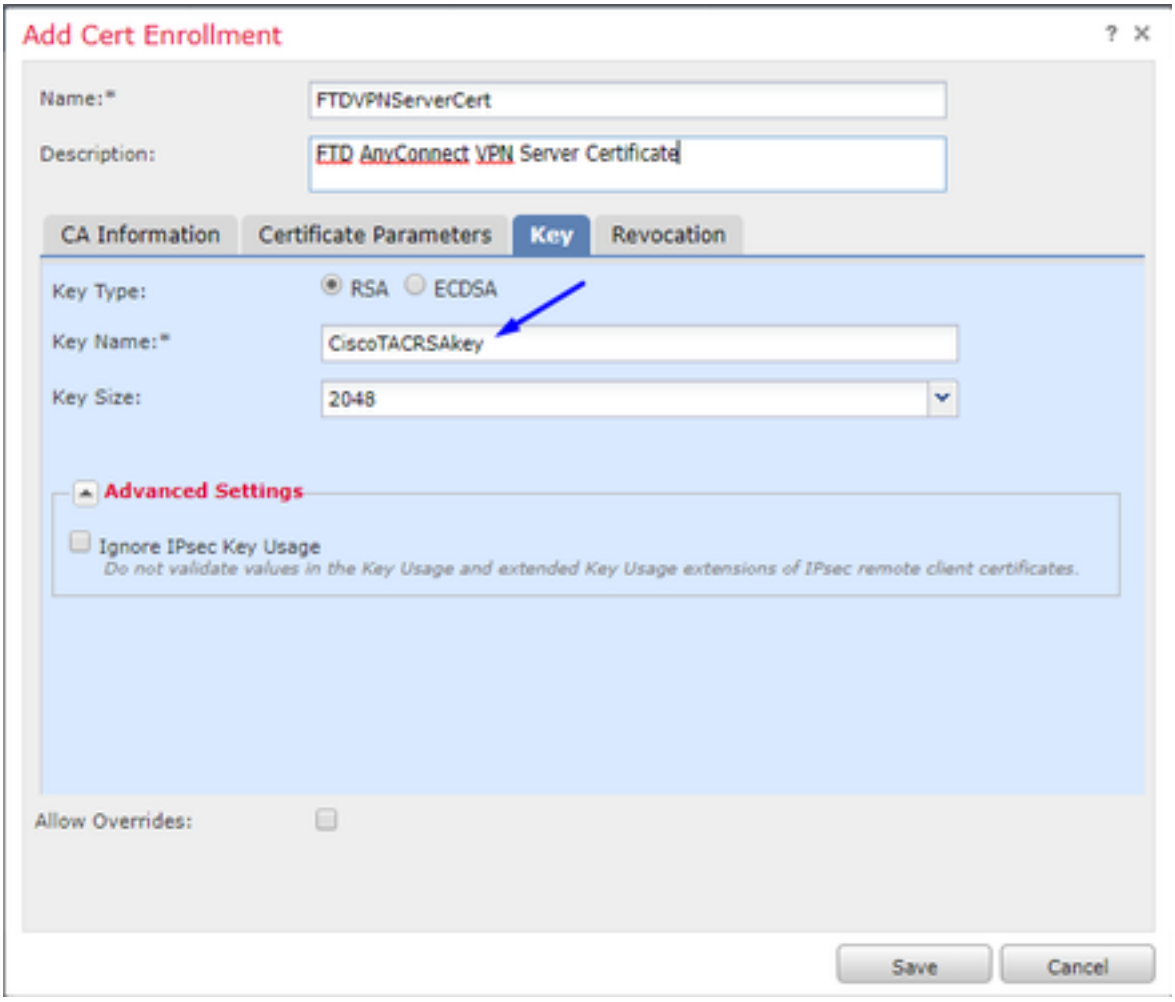
「公用名稱」欄位必須是FTD的FQDN



提示：您可以從FTD CLI輸入以下命令，以取得FTD的FQDN:

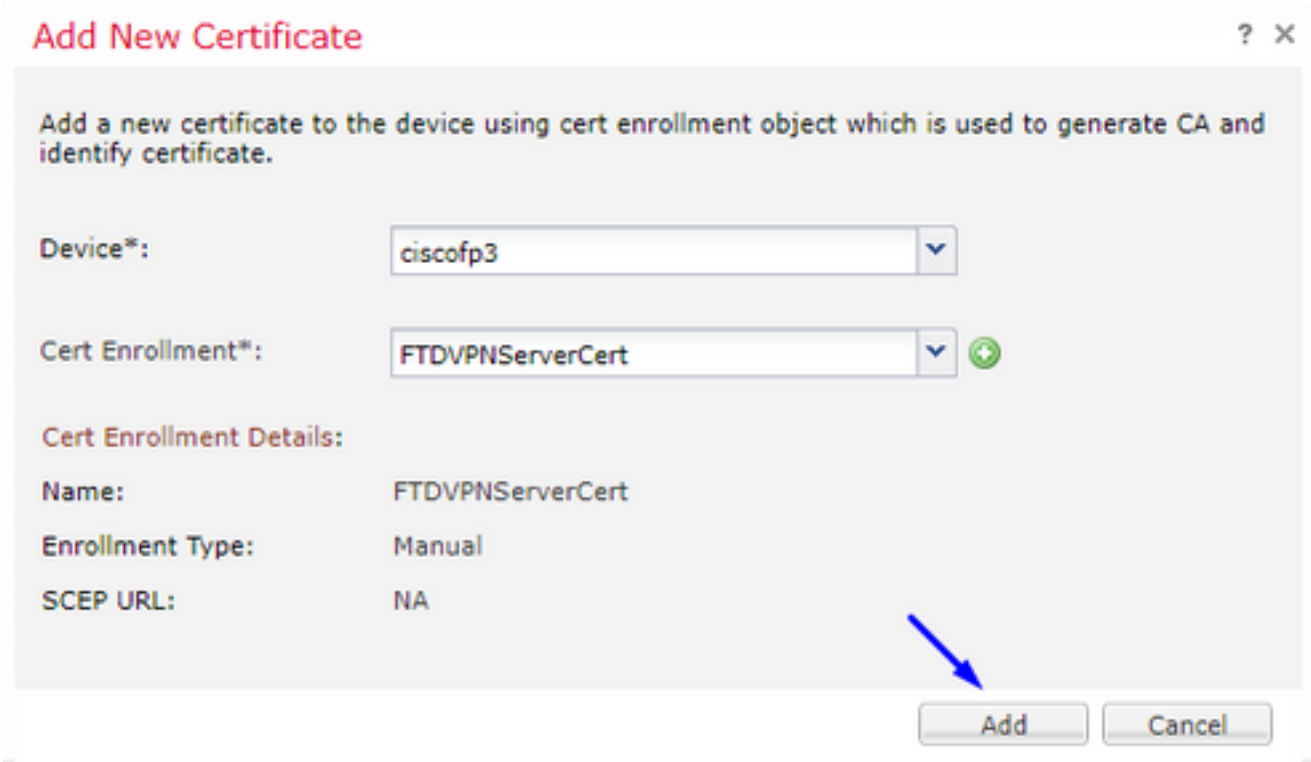
```
> show network
===============[ System Information ]===============
Hostname : ciscofp3.cisco.com
Domains : cisco
DNS Servers : 192.168.1.20
Management port : 8305
IPv4 Default route
Gateway : 192.168.1.1

======================[ 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**



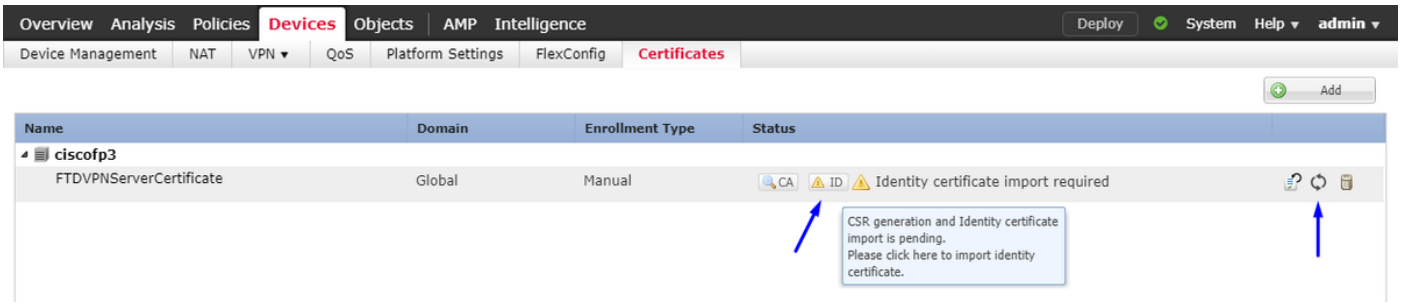
按一下「**Save**」

選擇上面剛建立的FTDVPNServerCert，然後按一下**Add**

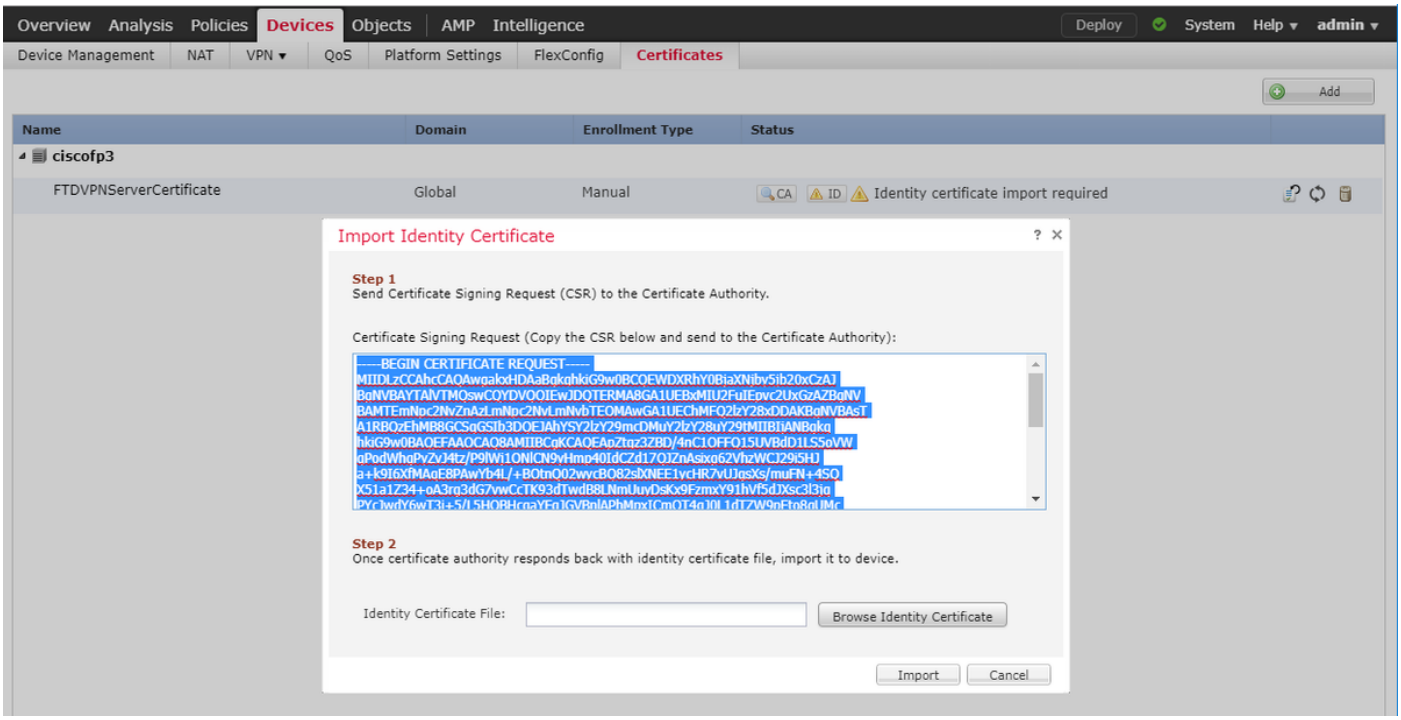


提示：等待約10-30秒鐘，等待FMC + FTD驗證和安裝根CA證書（如果未顯示，請按一下「刷新」圖示）

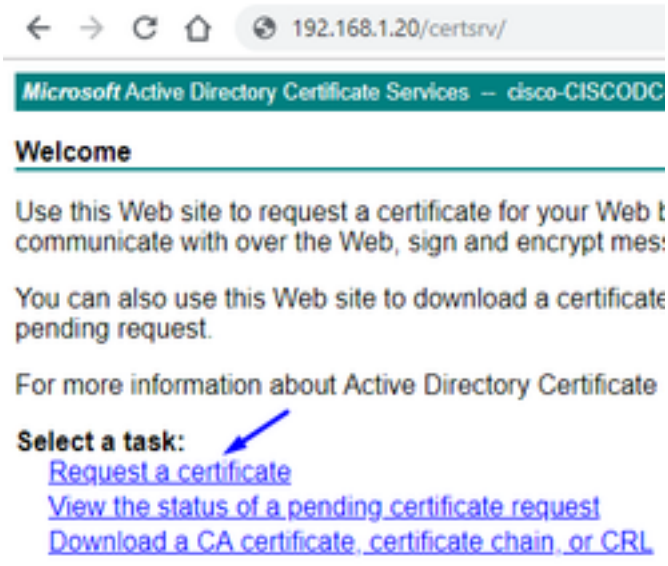
按一下ID按鈕：



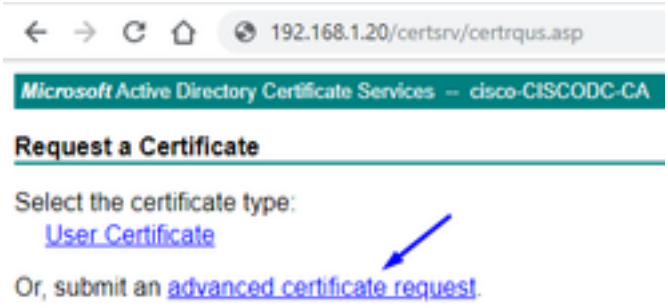
複製並貼上此CSR，並將其帶到Windows Server根CA:



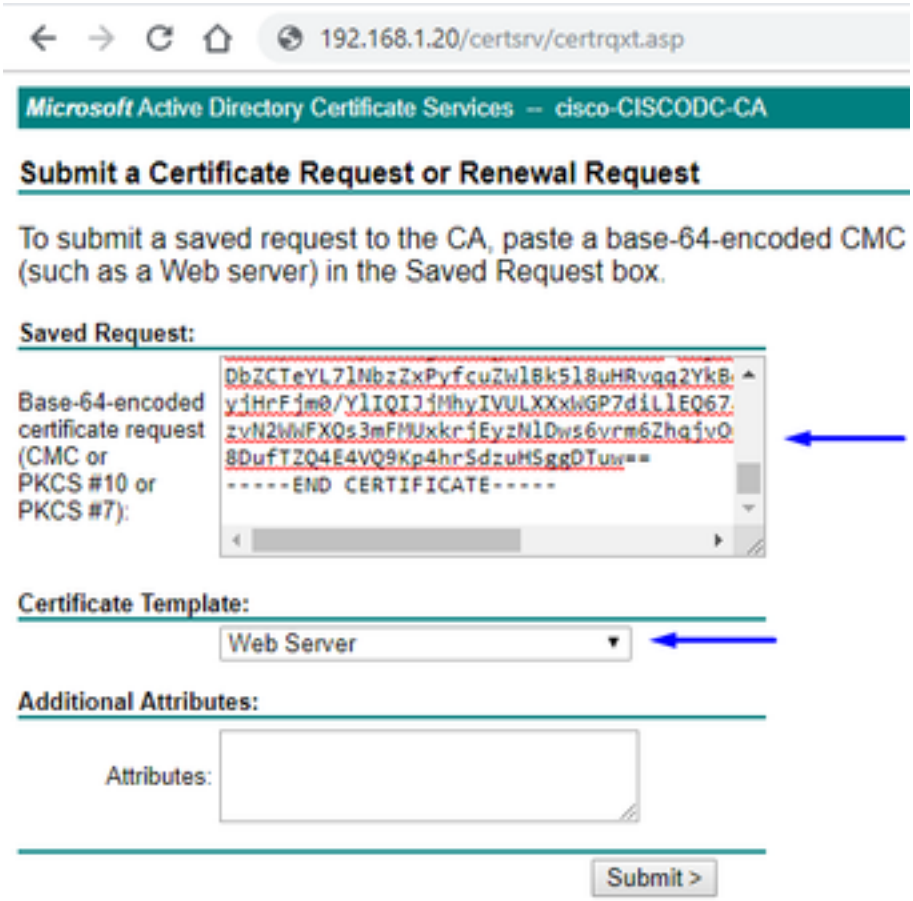
轉到http://192.168.1.20/certsrv



按一下「advanced certificate request」

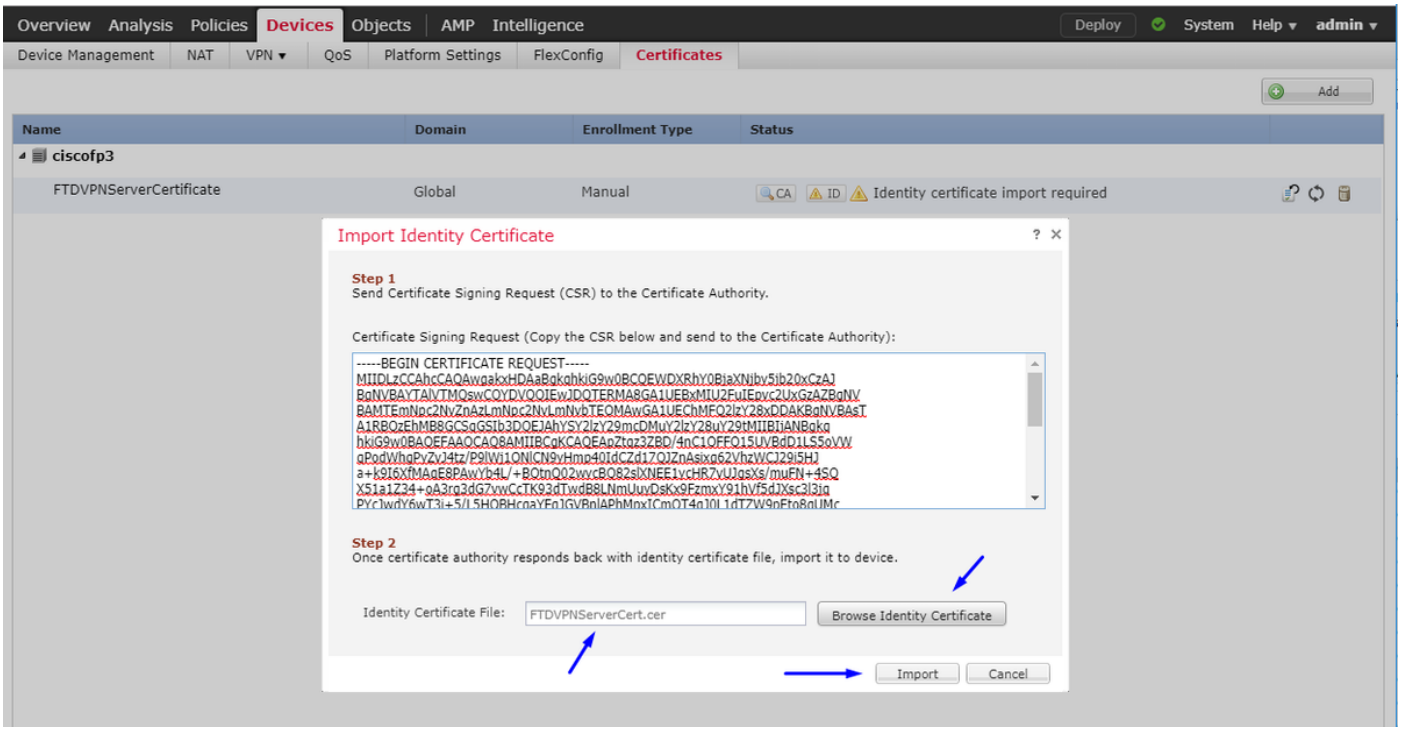


將您的證書簽名請求(CSR)貼上到下面的欄位，然後選擇**Web Server**作為證書模板

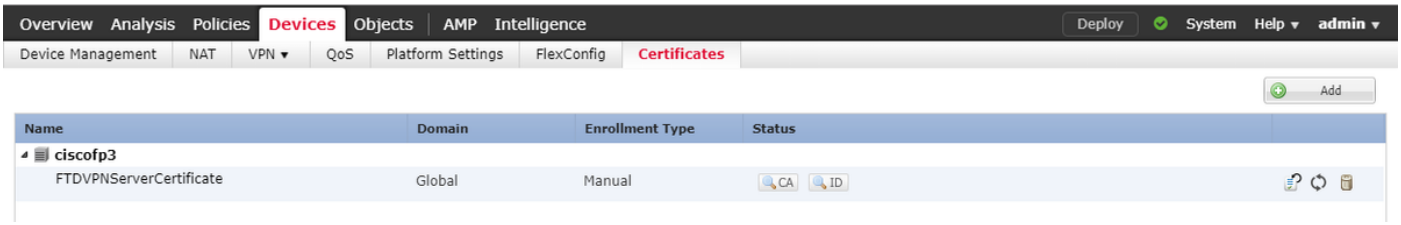


按一下**Submit**
按一下「**Base 64 encoded**」按鈕，然後按一下「**Download certificate**」

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



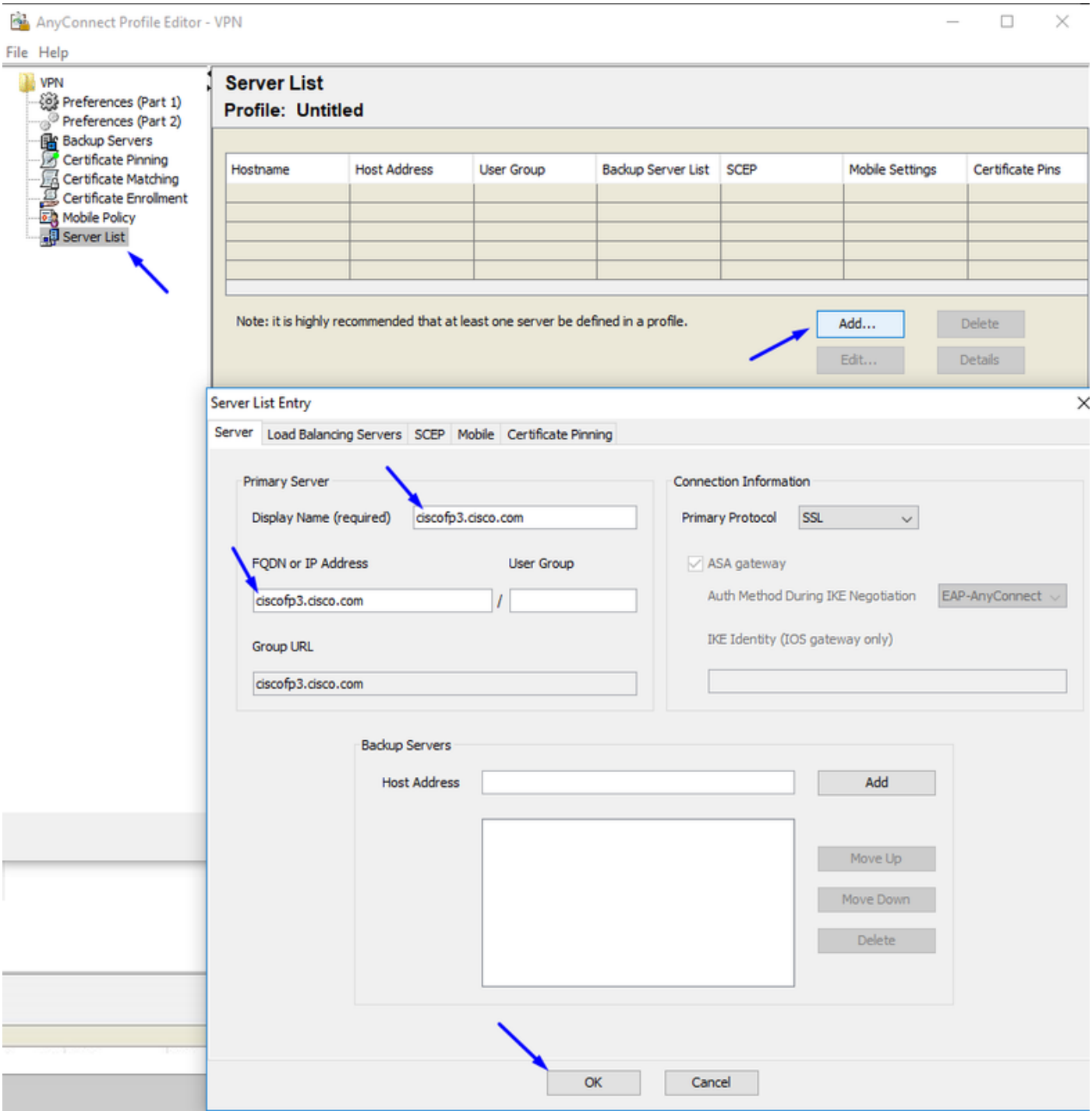
已成功安裝FTD VPN伺服器證書（由Windows Server根CA簽名）

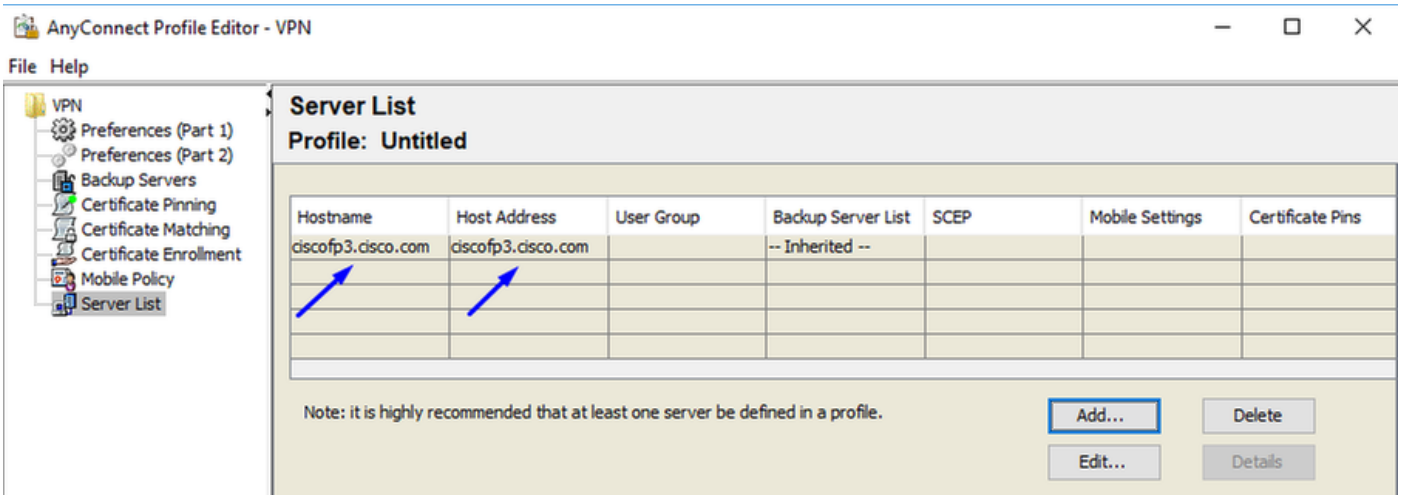


下載AnyConnect映像+ AnyConnect配置檔案編輯器並建立.xml配置檔案

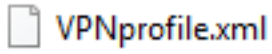
下載並安裝Cisco AnyConnect Profile Editor

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



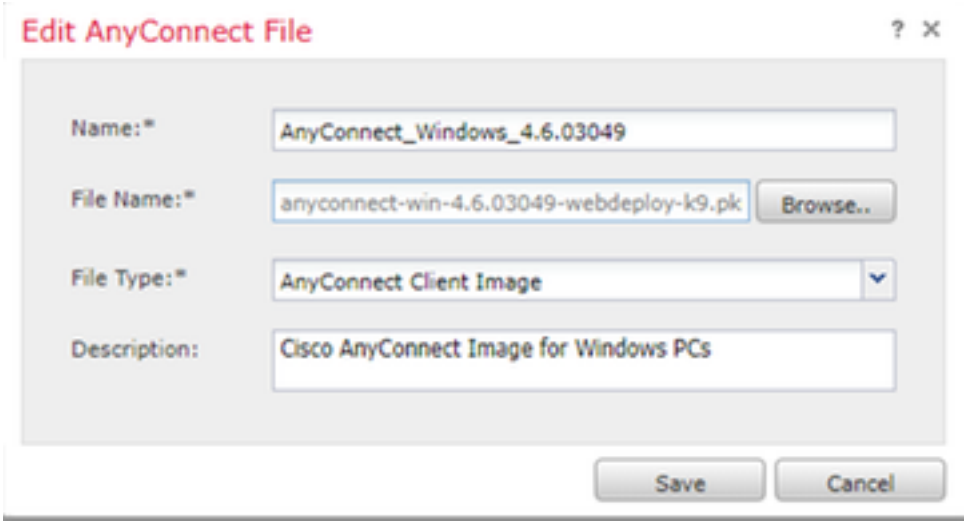


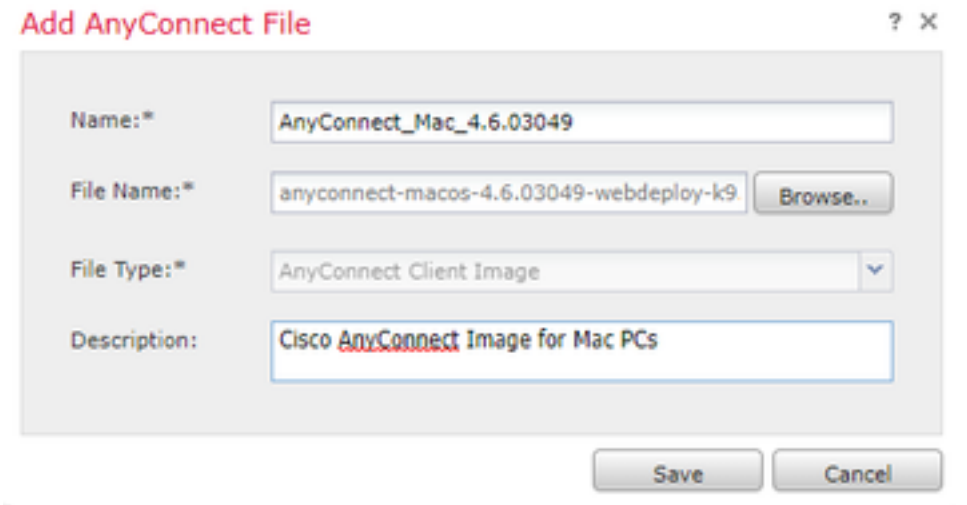
按一下「OK」和「File」>「Save as...」。



從此處下載Windows和Mac .pkg映像

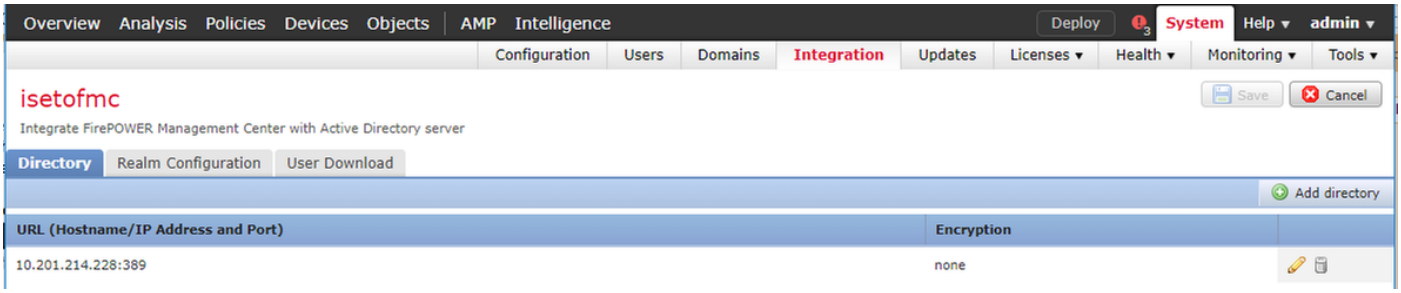
轉至**Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File**

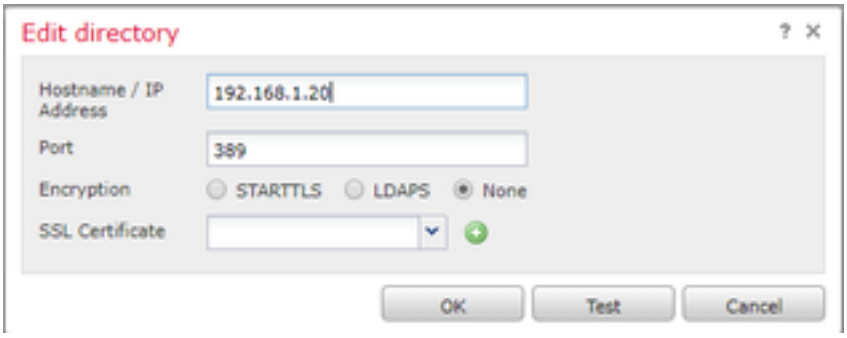




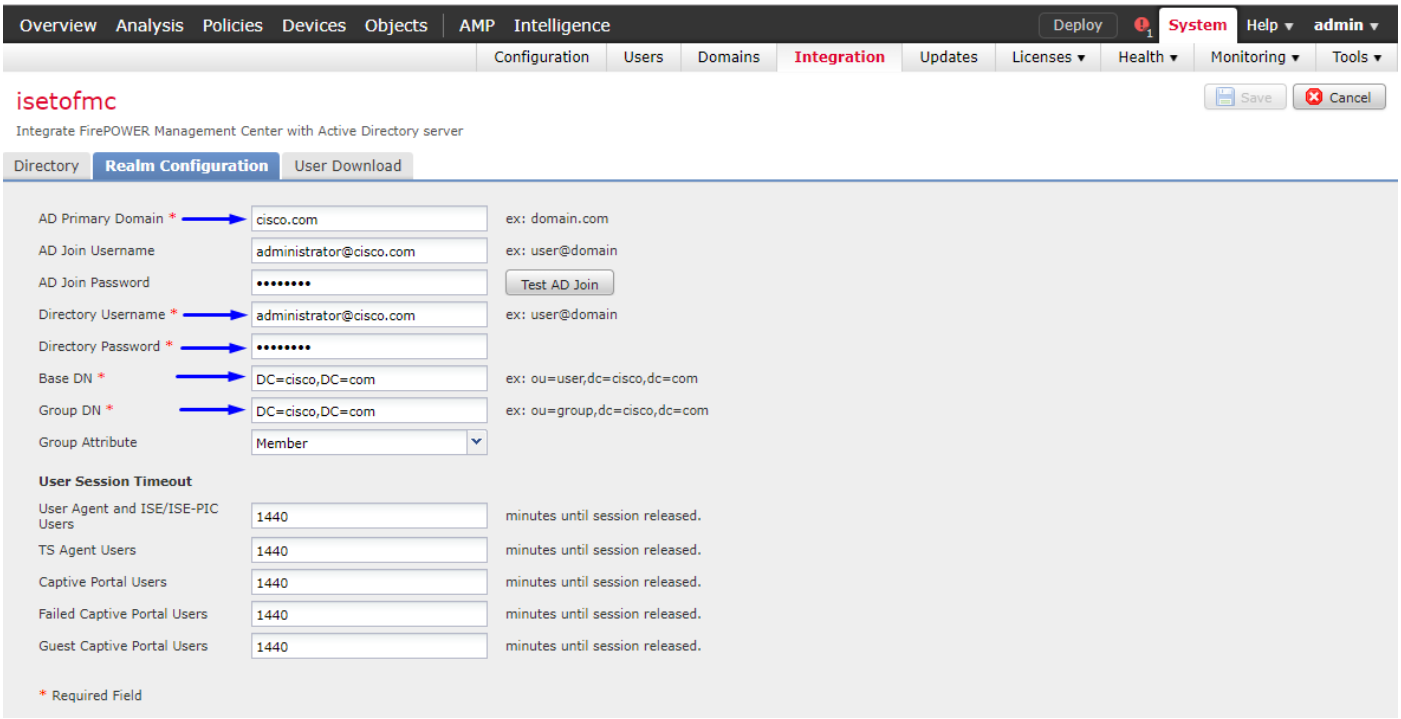
設定FTD上的Anyconnect VPN（使用根CA憑證）

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



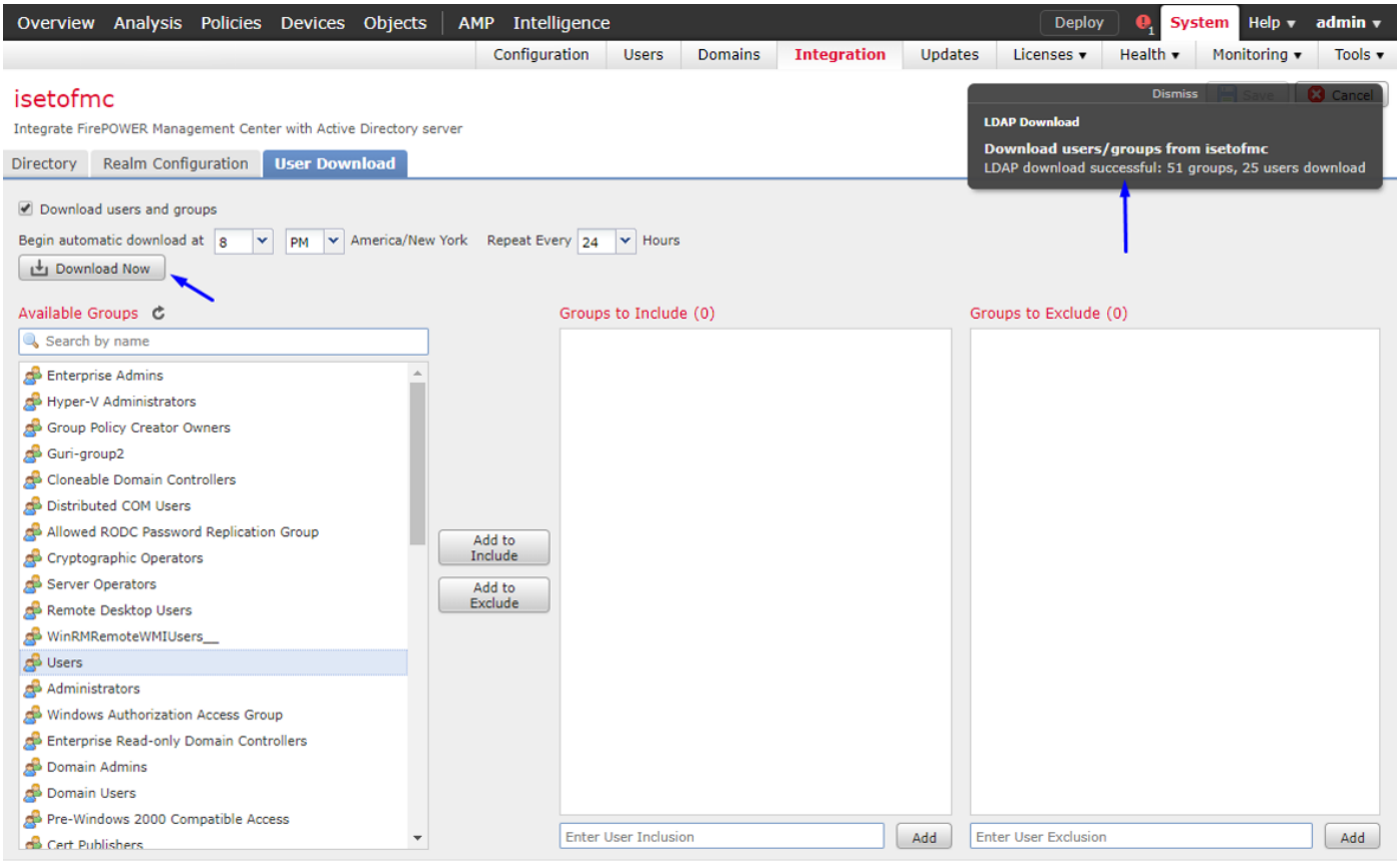


按一下**Realm Configuration**頁籤 — 在此處配置域控制器資訊

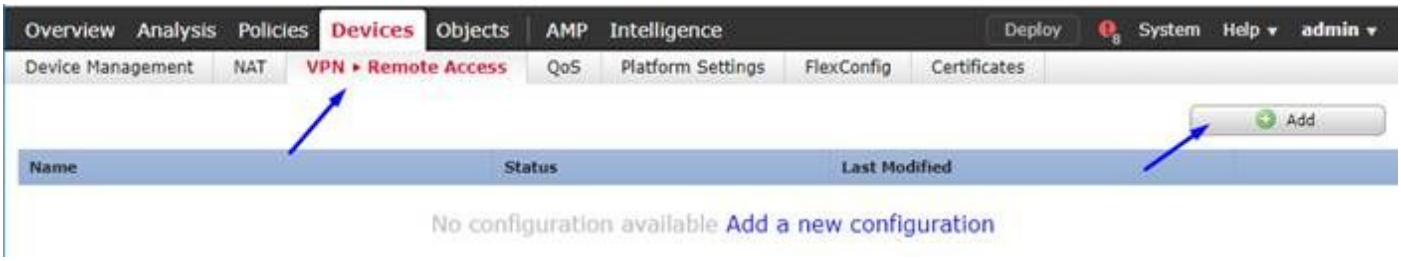


附註：在上面的示例中，使用在Windows AD伺服器中具有「域管理」許可權的AD使用者名稱。如果要配置使用者，使其具有更具體的最小許可權，以使FMC加入您的領域配置的Active Directory域，您可以在這裡看到步驟

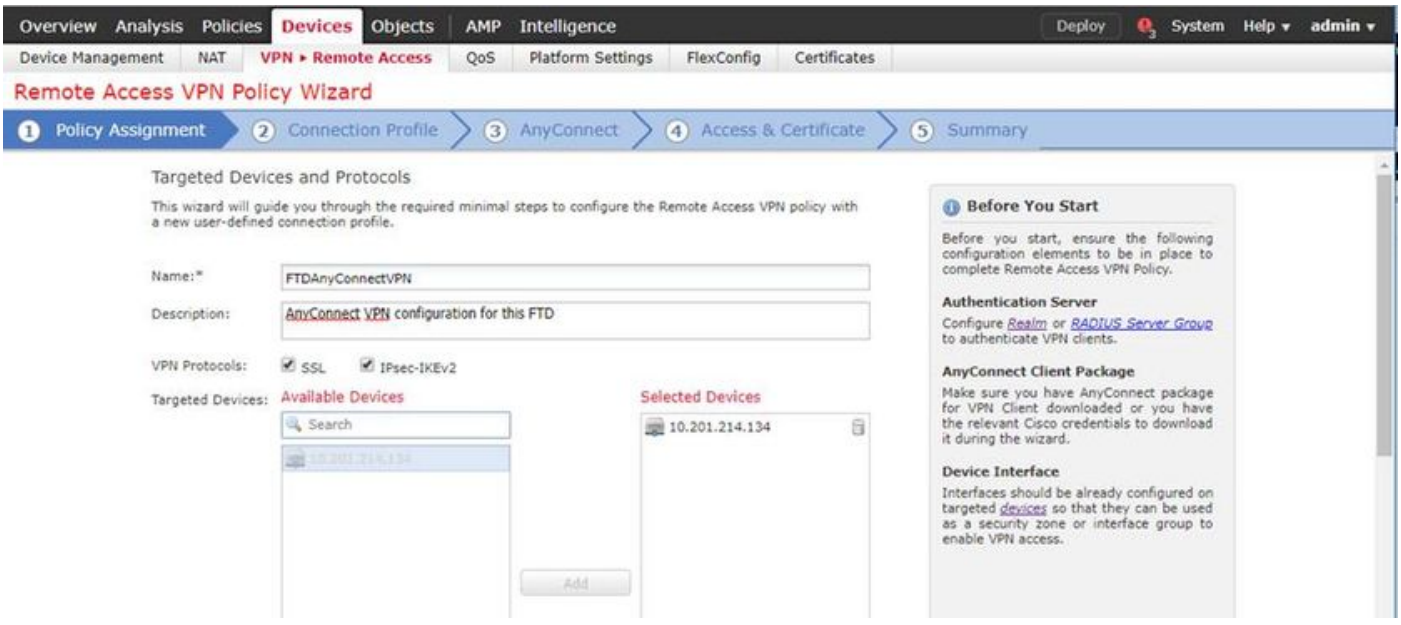
按一下**User Download**頁籤 — 確保使用者下載成功



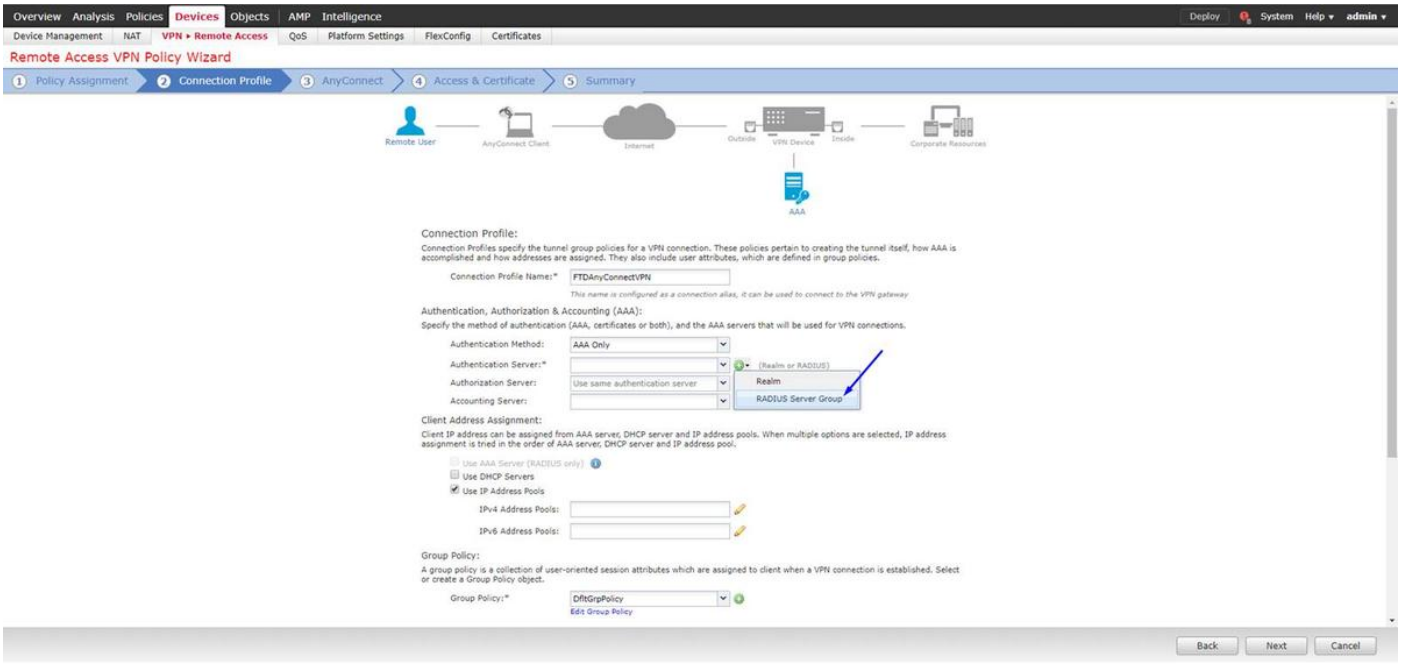
按一下「**Devices**」>「**VPN**」>「**Remote Access**」>按一下「**Add**」



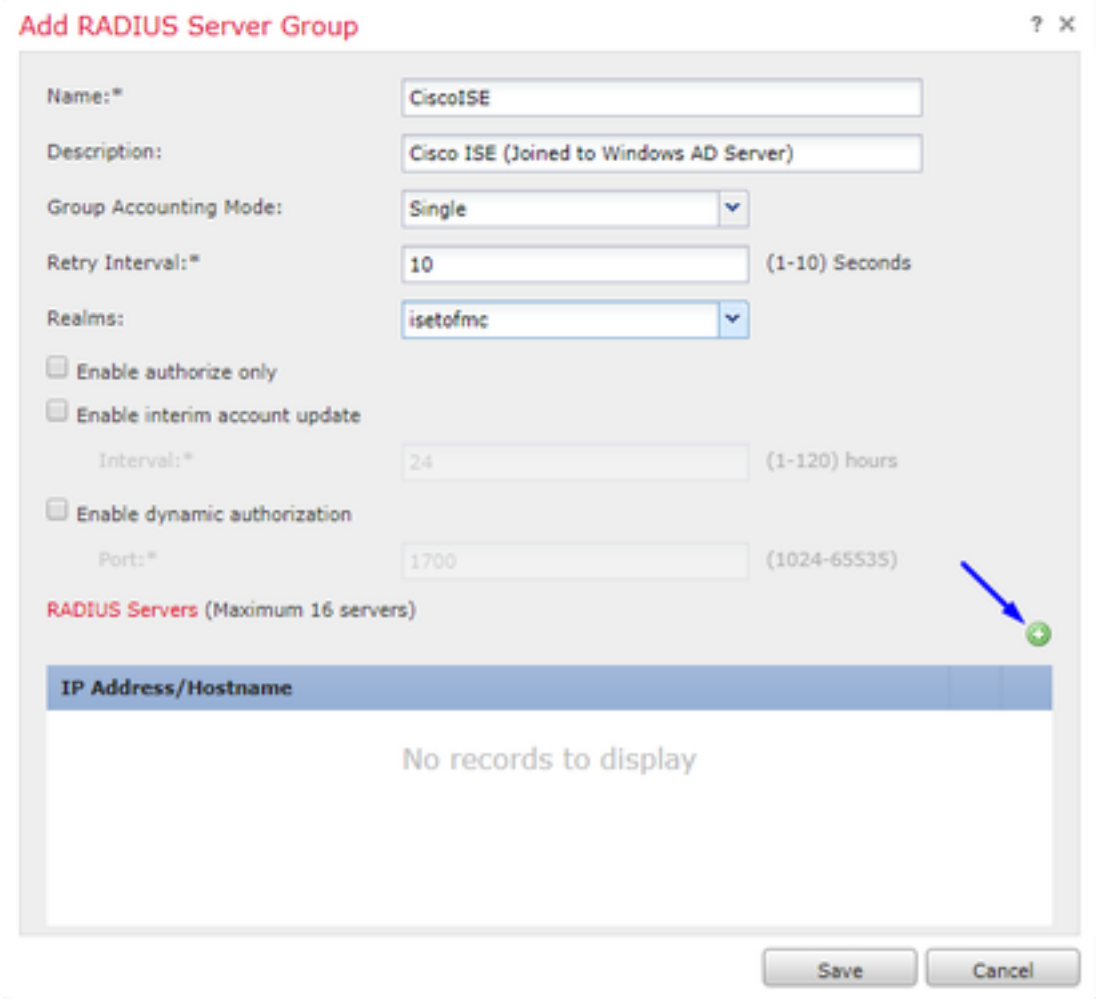
輸入**Name**、**Description**，然後按一下**Add**，以選擇要在其上設定Anyconnect VPN的FTD裝置



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）

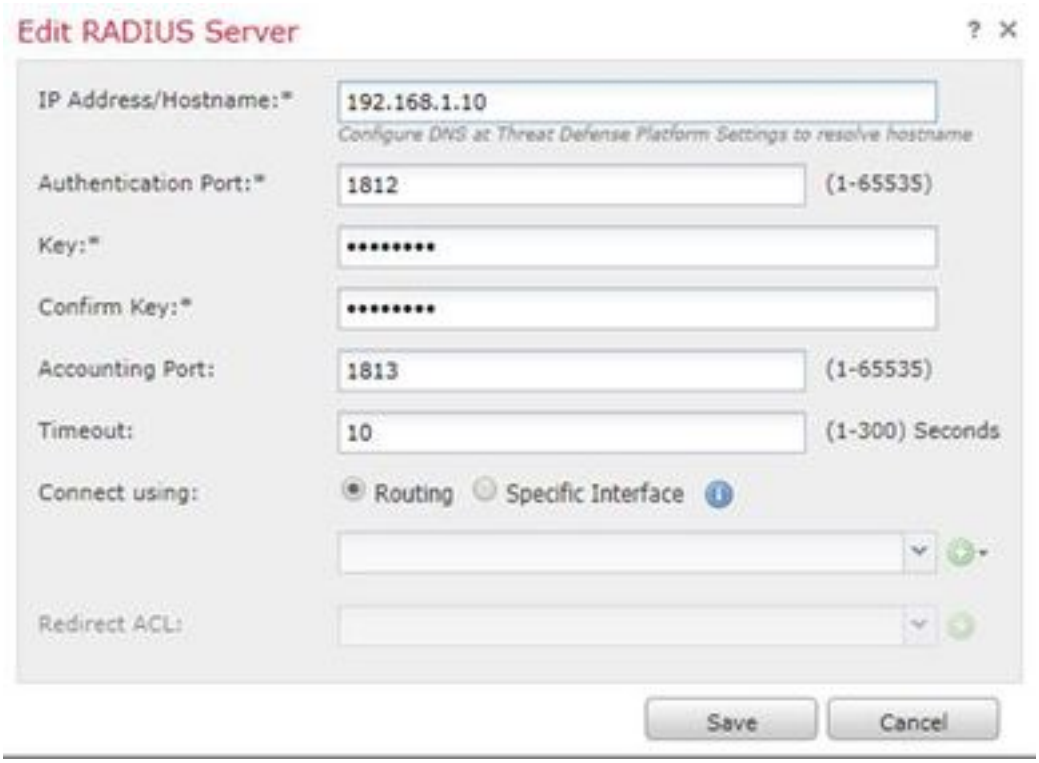


輸入RADIUS伺服器的**名稱**
選擇上面配**置的**您的領域
按一下**「Add」**

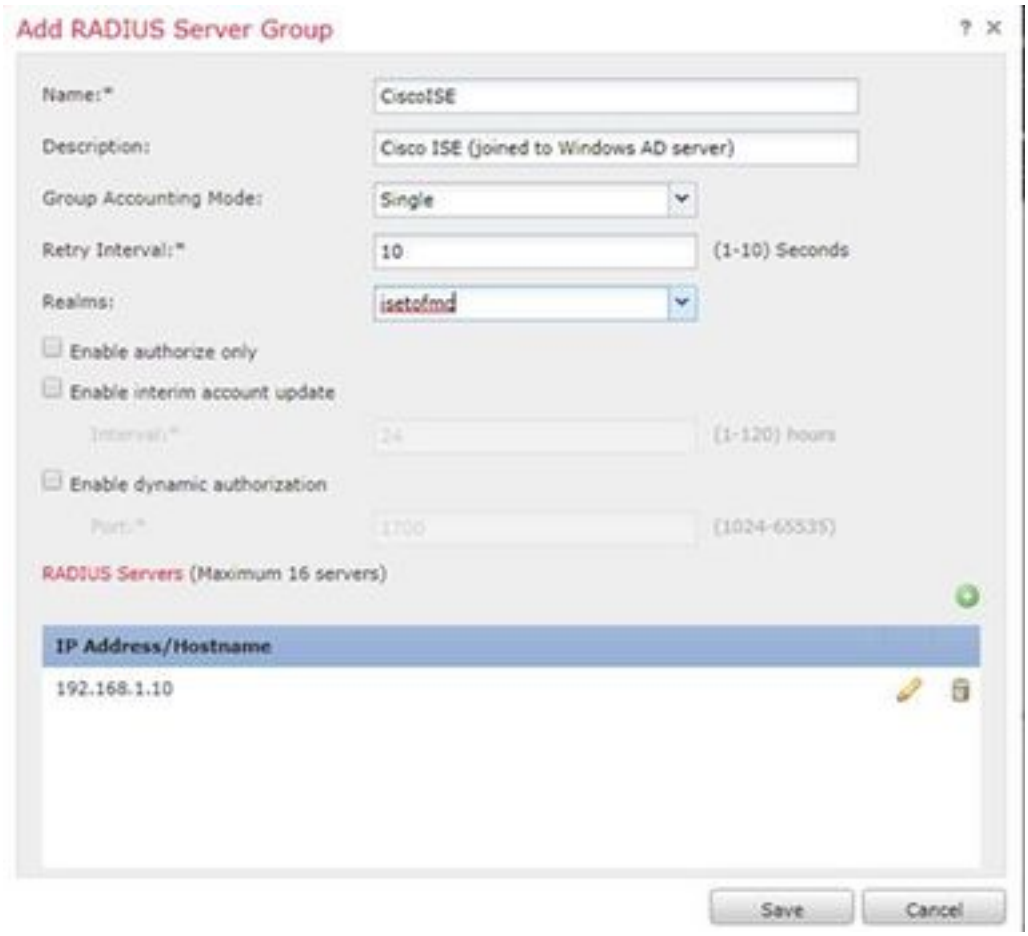


為思科ISE節點鍵入以下資訊：
IP地址/主機名:思科ISE PSN（策略服務節點）的IP地址 — 這是身份驗證請求將到達的地方
主要:cisco123
確認**金鑰**:cisco123

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

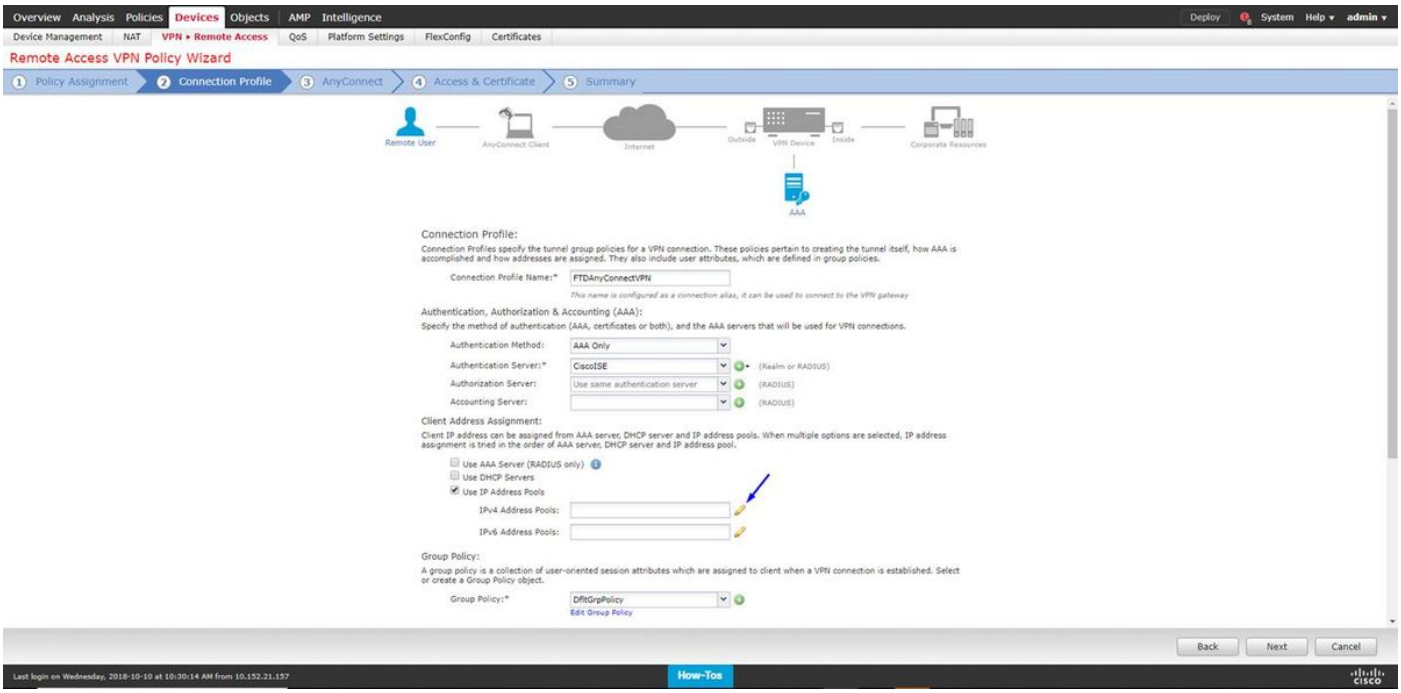


附註：當終端使用者嘗試透過AnyConnect VPN連線到FTD時，他們輸入的使用者名稱+密碼將會作為驗證要求傳送到此FTD。FTD會將該請求轉送到思科ISE PSN節點進行身份驗證（然後，思科ISE會檢查Windows Active Directory的使用者名稱和密碼，並根據我們當前在思科ISE中配置的條件實施訪問控制/網路訪問）

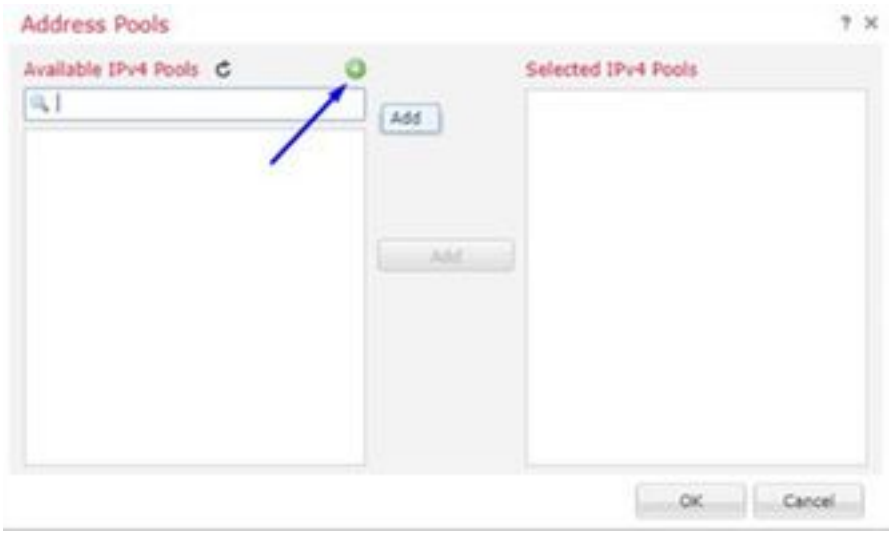


按一下「Save」

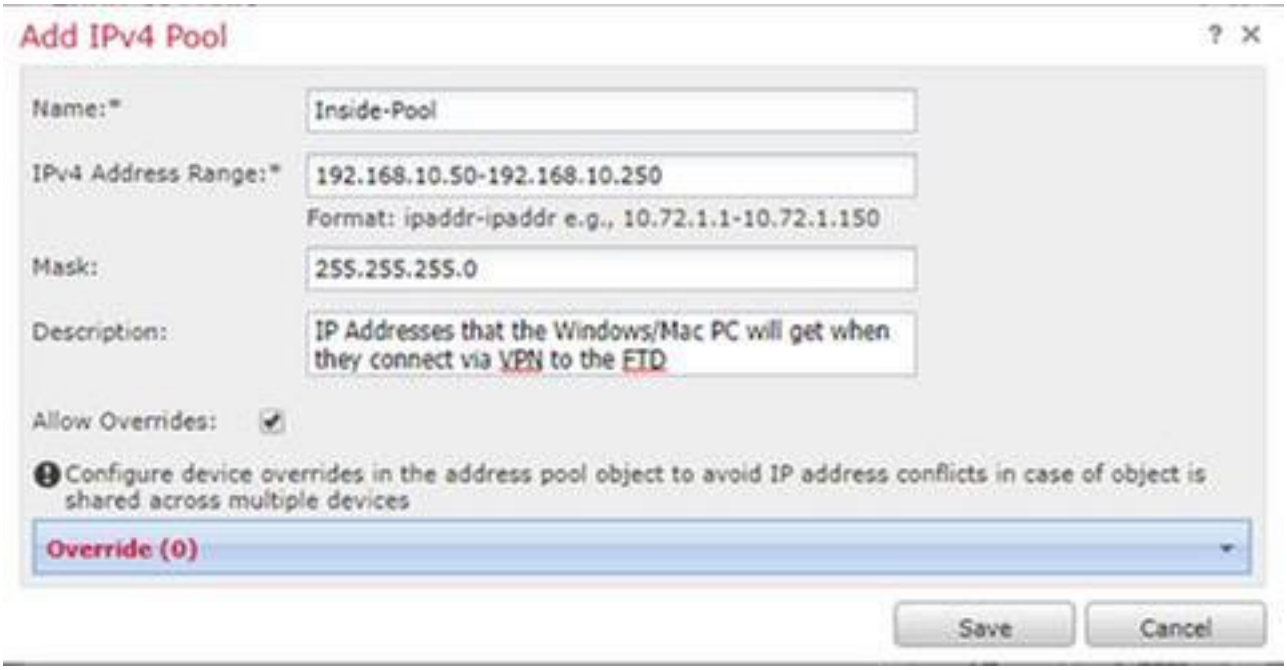
按一下Edit for IPv4 Address Pool



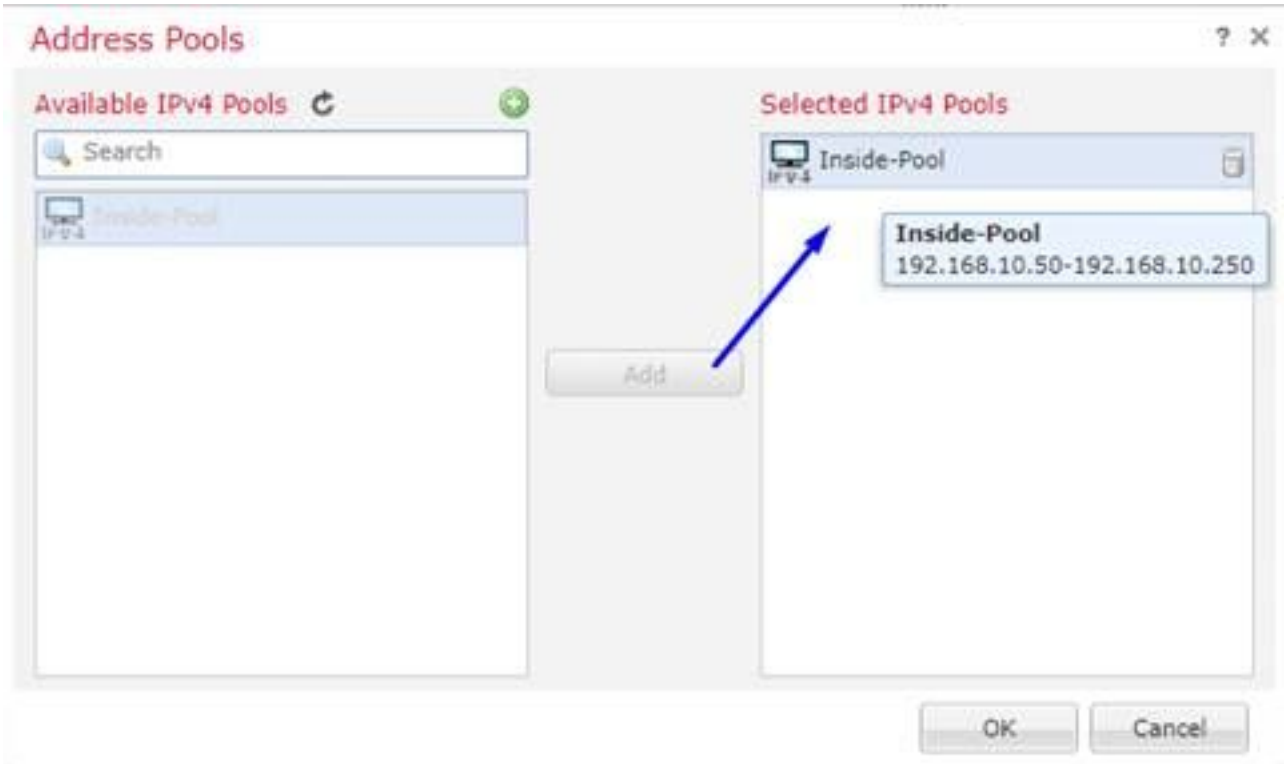
按一下「Add」



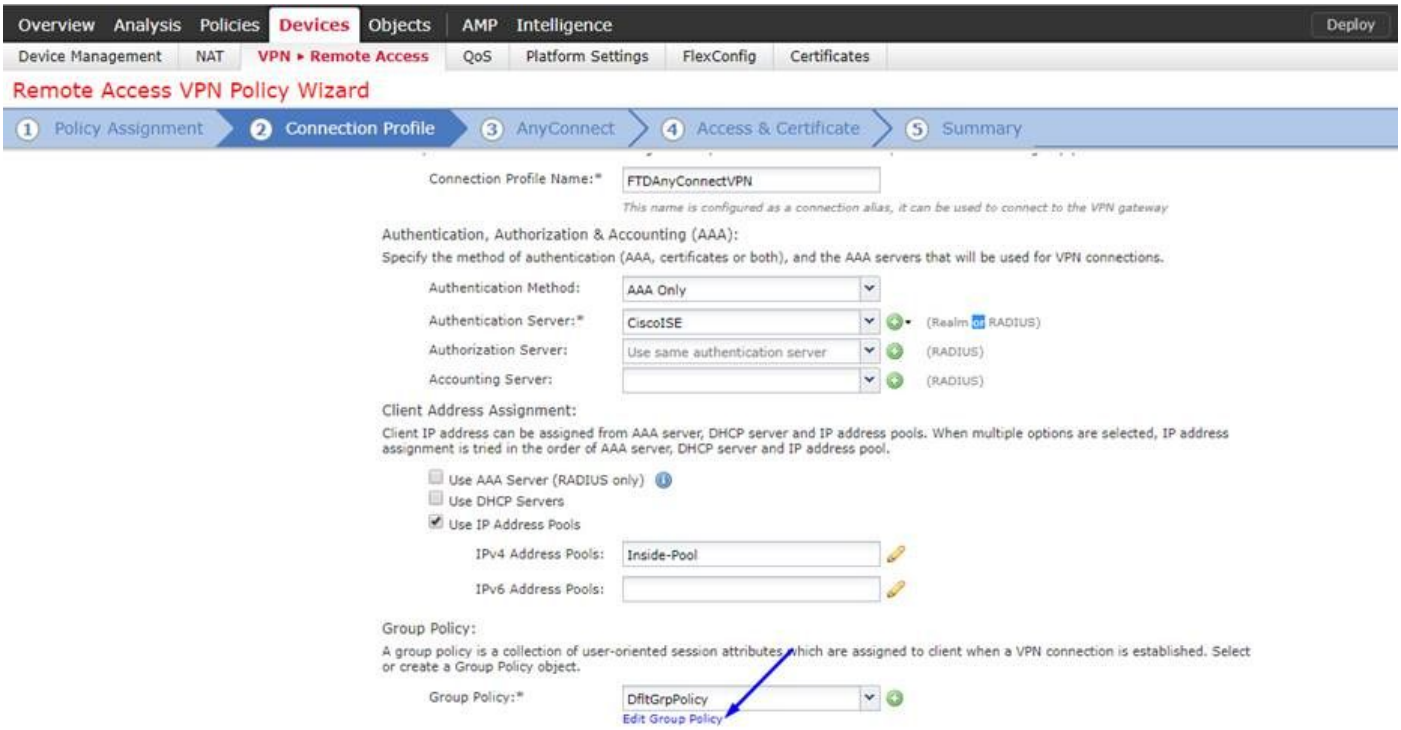
輸入名稱、IPv4地址範圍和子網掩碼



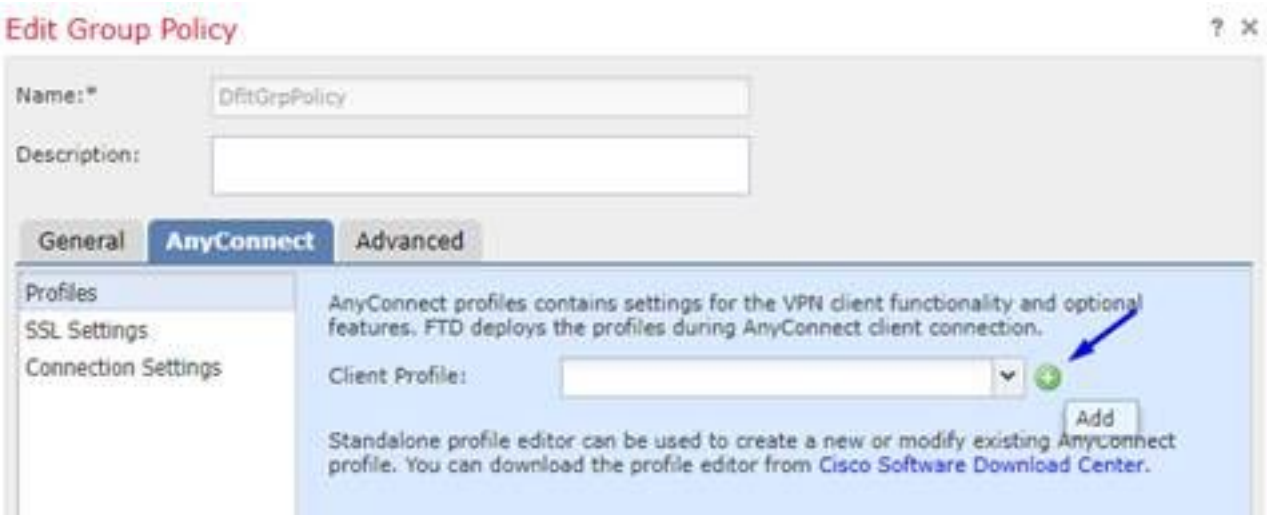
選擇您的IP地址池，然後按一下**Ok（確定）**



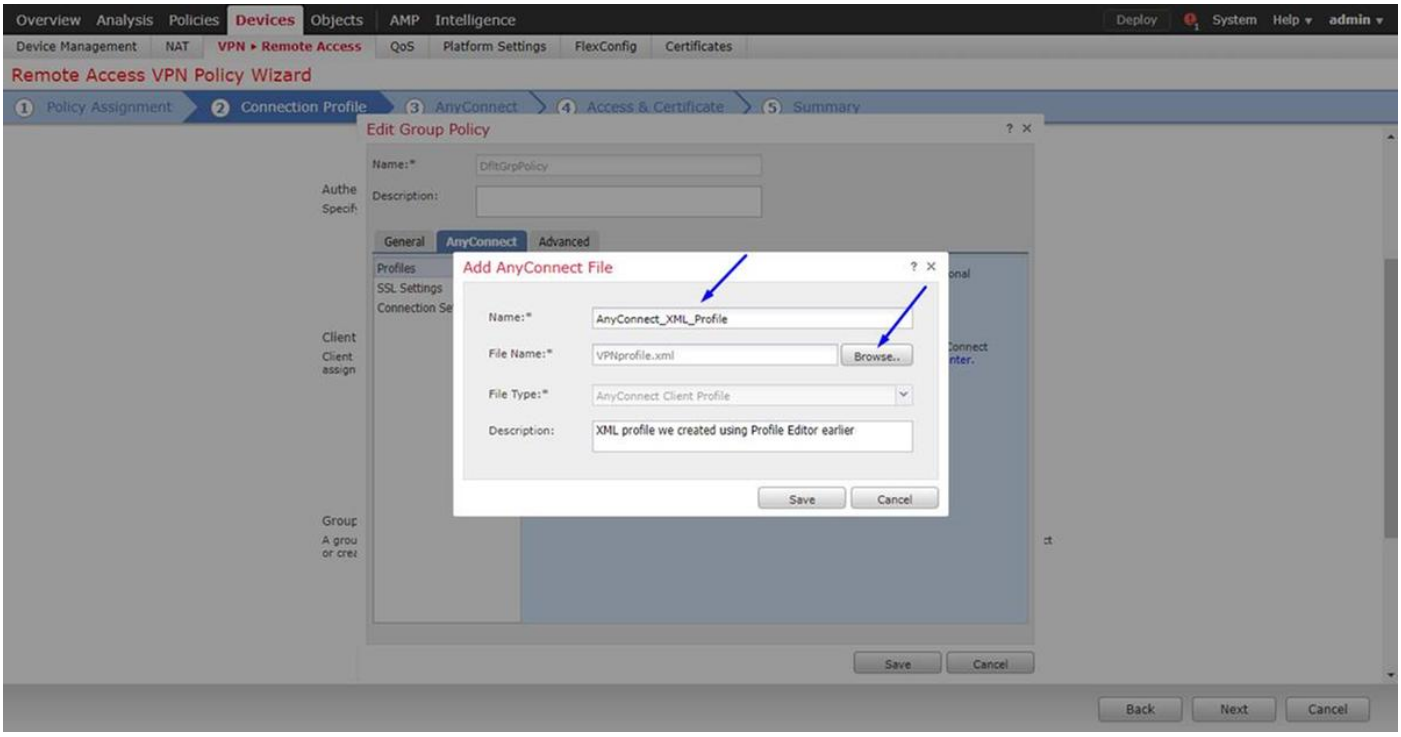
按一下**編輯**組策略



按一下**Anyconnect**頁籤> **Profiles** >按一下**Add**

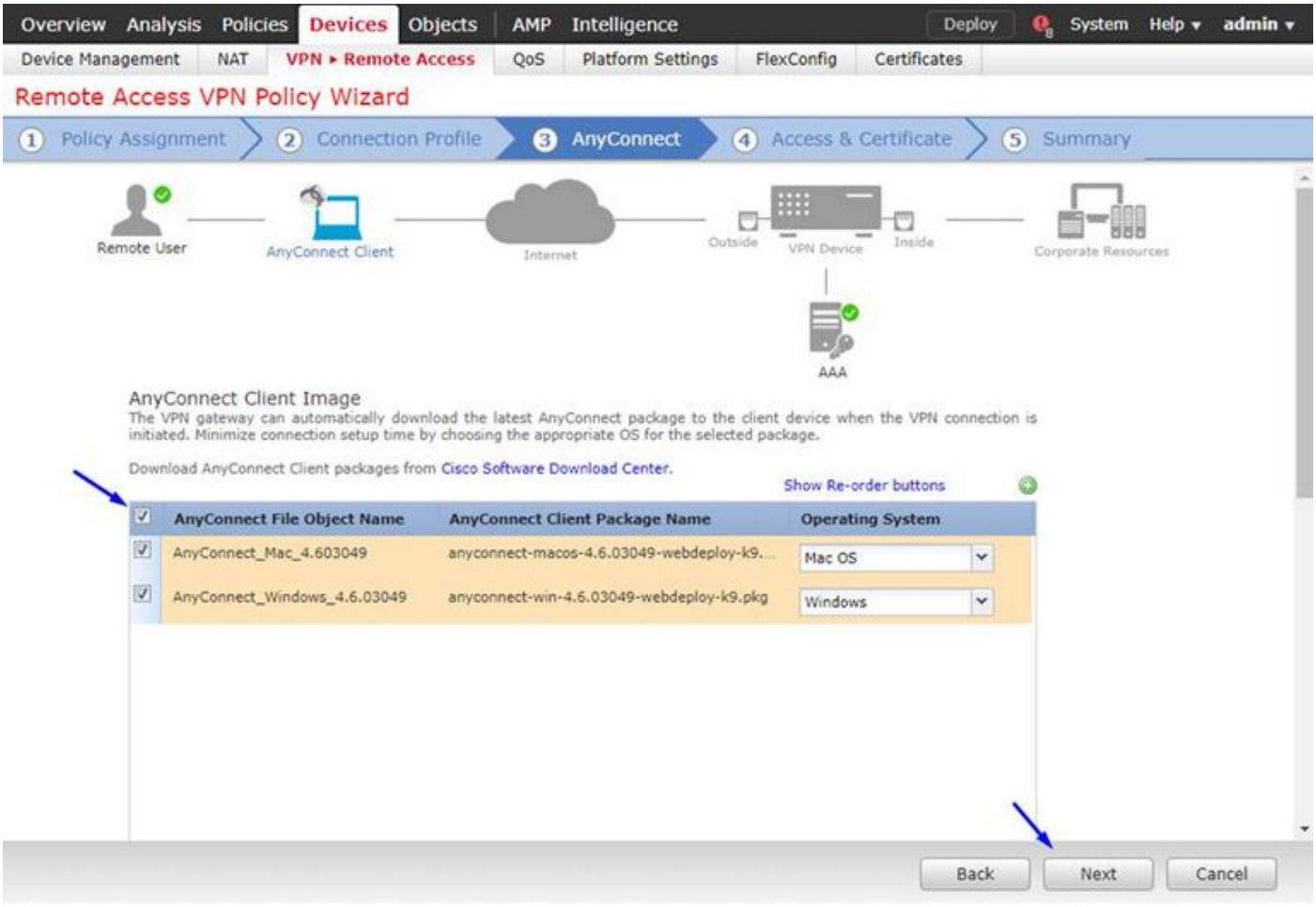


鍵入**Name**並按一下**Browse**...並從上述步驟4中選擇您的VPNprofile.xml檔案

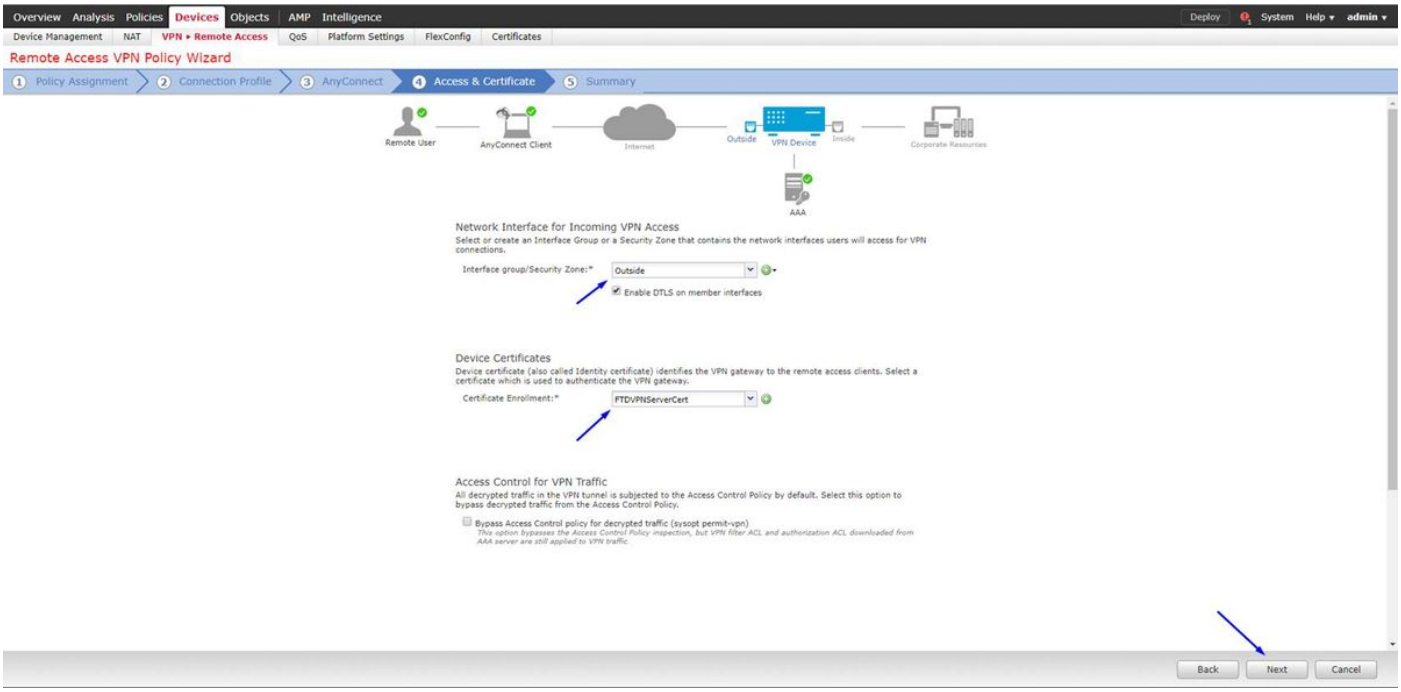


按一下**Save**，然後按一下**Next**

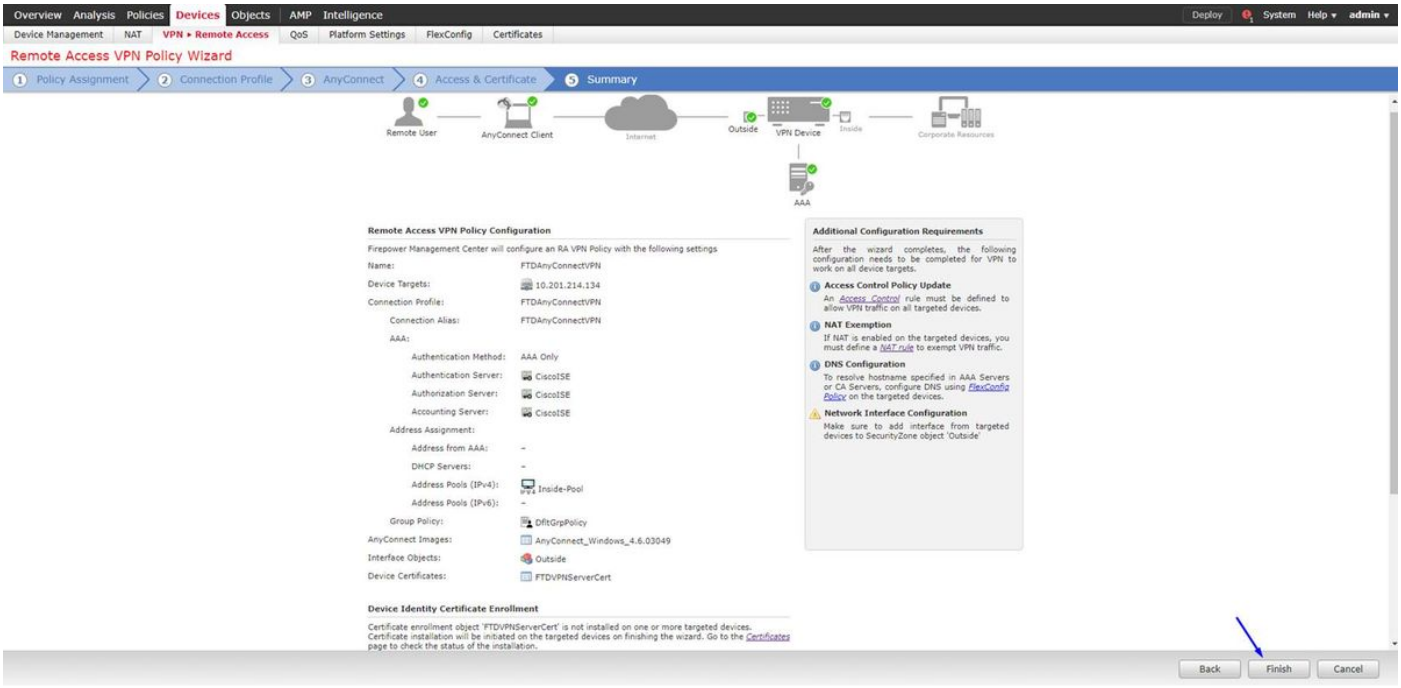
從上述步驟4中選擇您的AnyConnect Windows/Mac檔案的覈取方塊



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

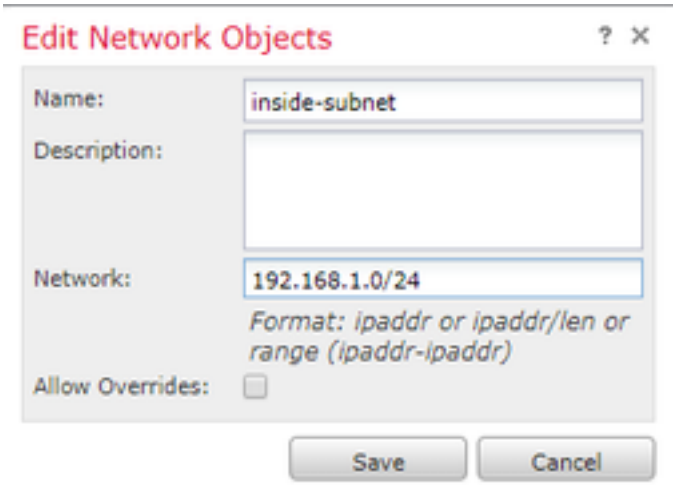


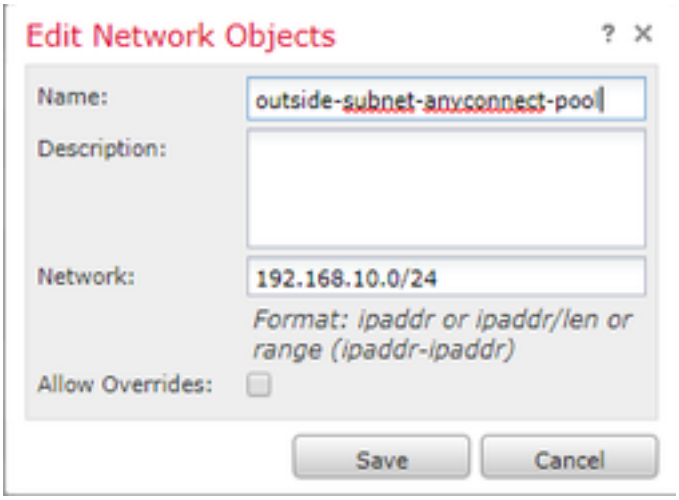
檢查您的配置，然後按一下**下一步**

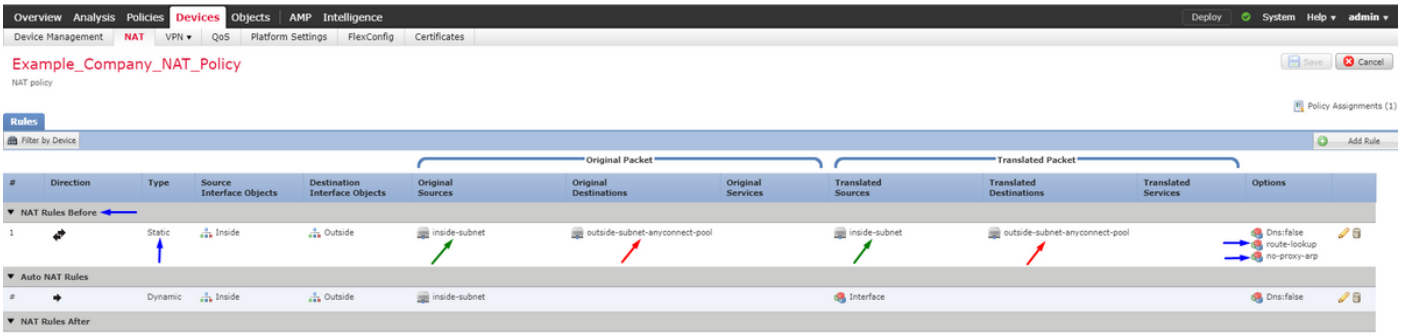


配置FTD NAT規則以將VPN流量免於NAT，因為該VPN流量無論如何都將解密，並建立訪問控制策略/規則

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**





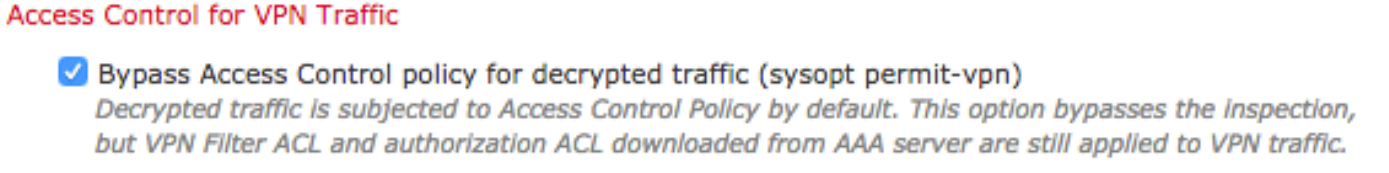


此外，您還必須在使用者VPN進入後允許資料流量。有兩種選擇：

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**:

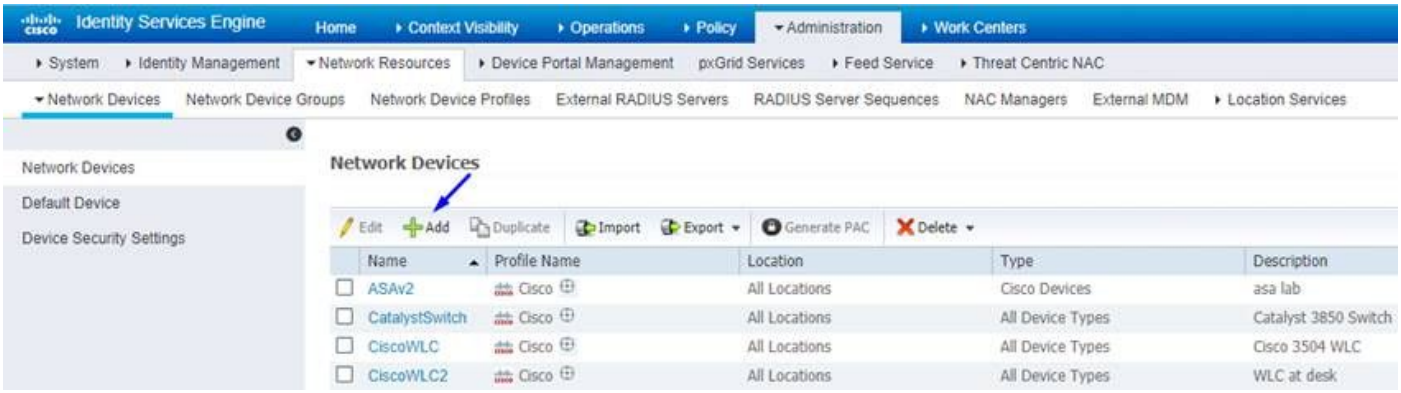


附註：如果未啟用此選項，則需要轉到**Policies > Access Control Policy**，並建立Allow規則，以便VPN使用者能夠訪問內部或dmz後面的內容

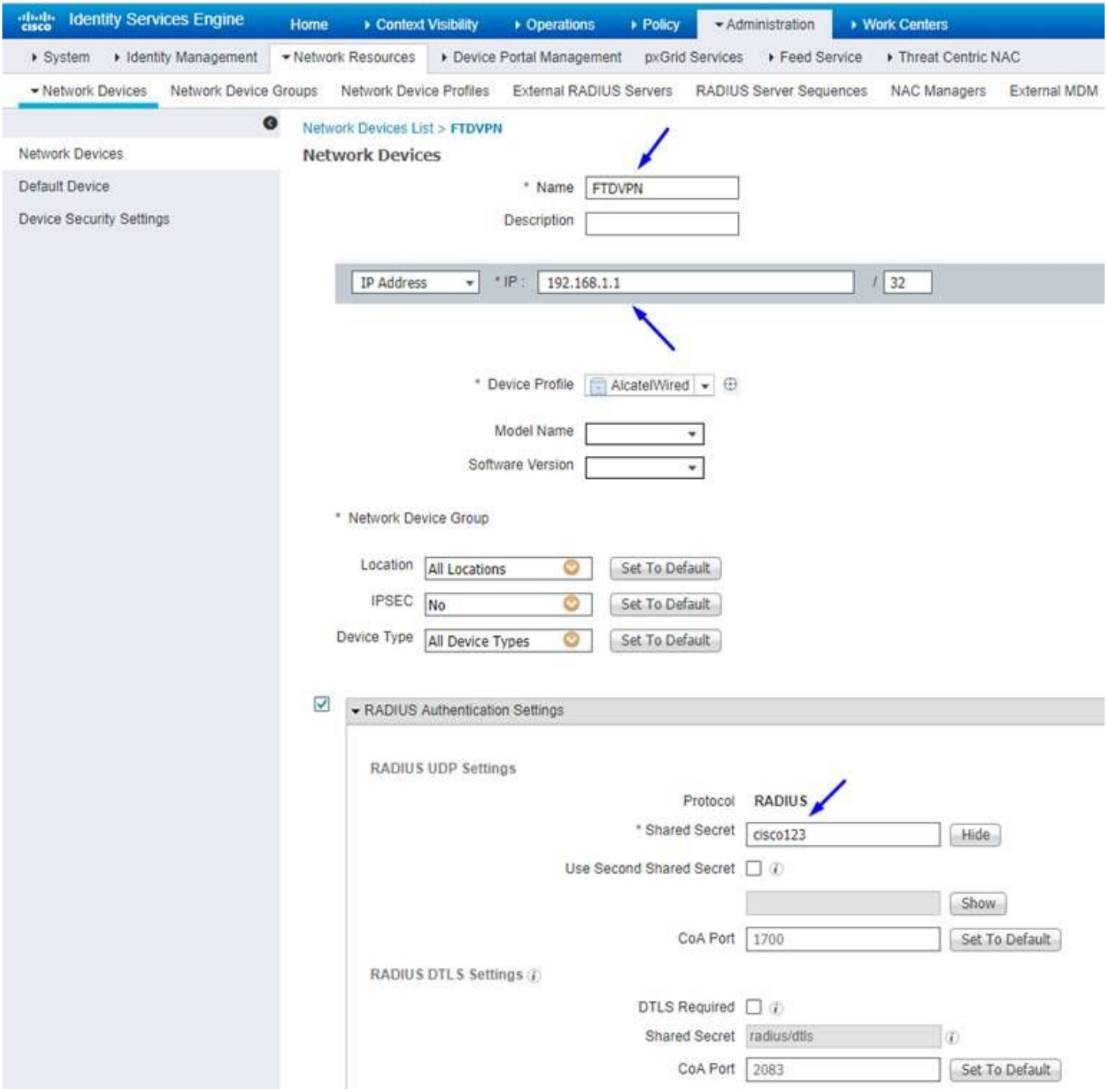
按一下FirePOWER管理中心右上角的「部署」

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）

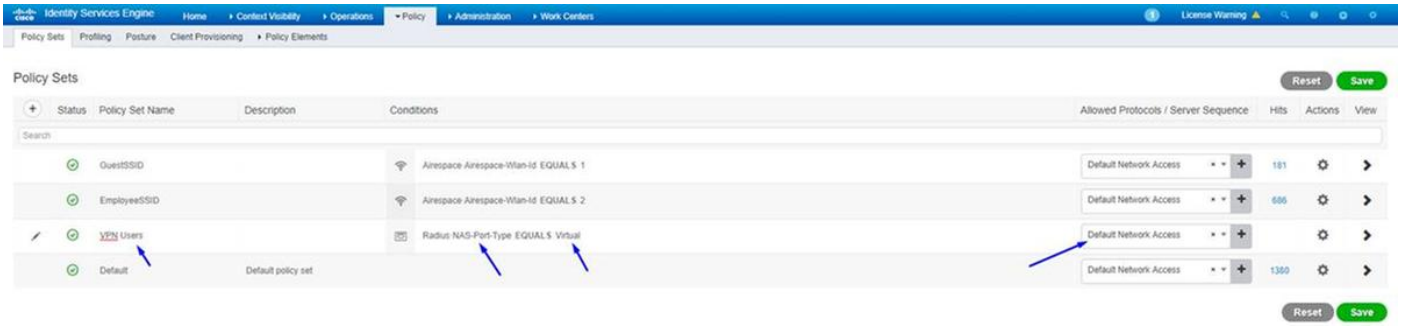
登入到Cisco Identity Services Engine，然後點選**Administration > Network Devices >**點選**Add**



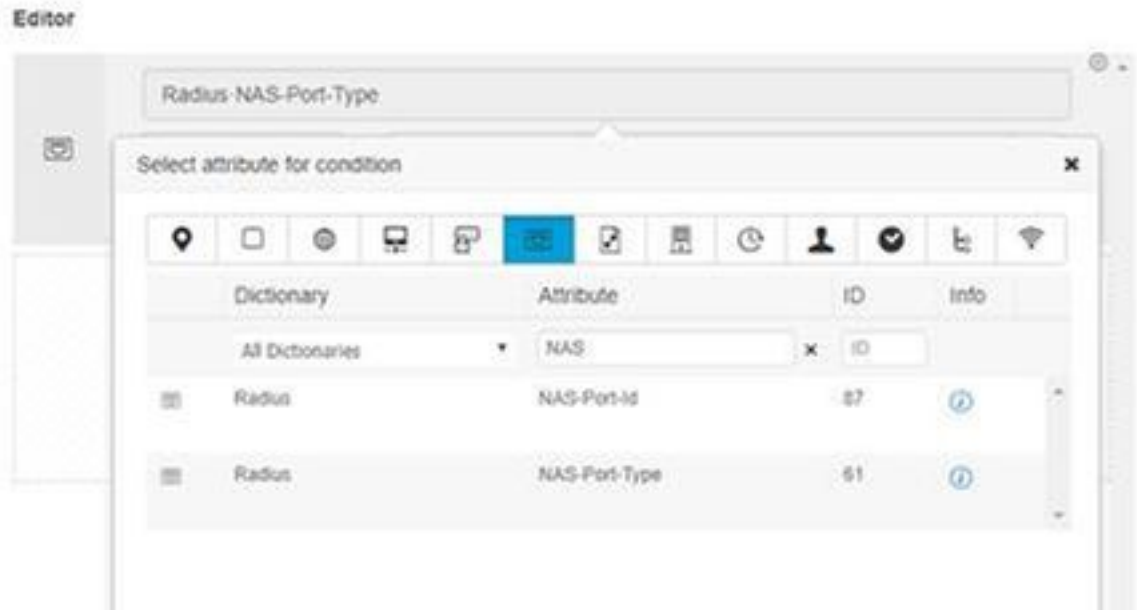
按上述步驟輸入**名稱**、輸入FTD的**IP位址**，然後輸入**RADIUS共用密碼**
注意：此地址必須是FTD可以到達您的思科ISE（RADIUS伺服器）的介面/IP地址，即您的思科ISE可以通過FTD到達的FTD介面



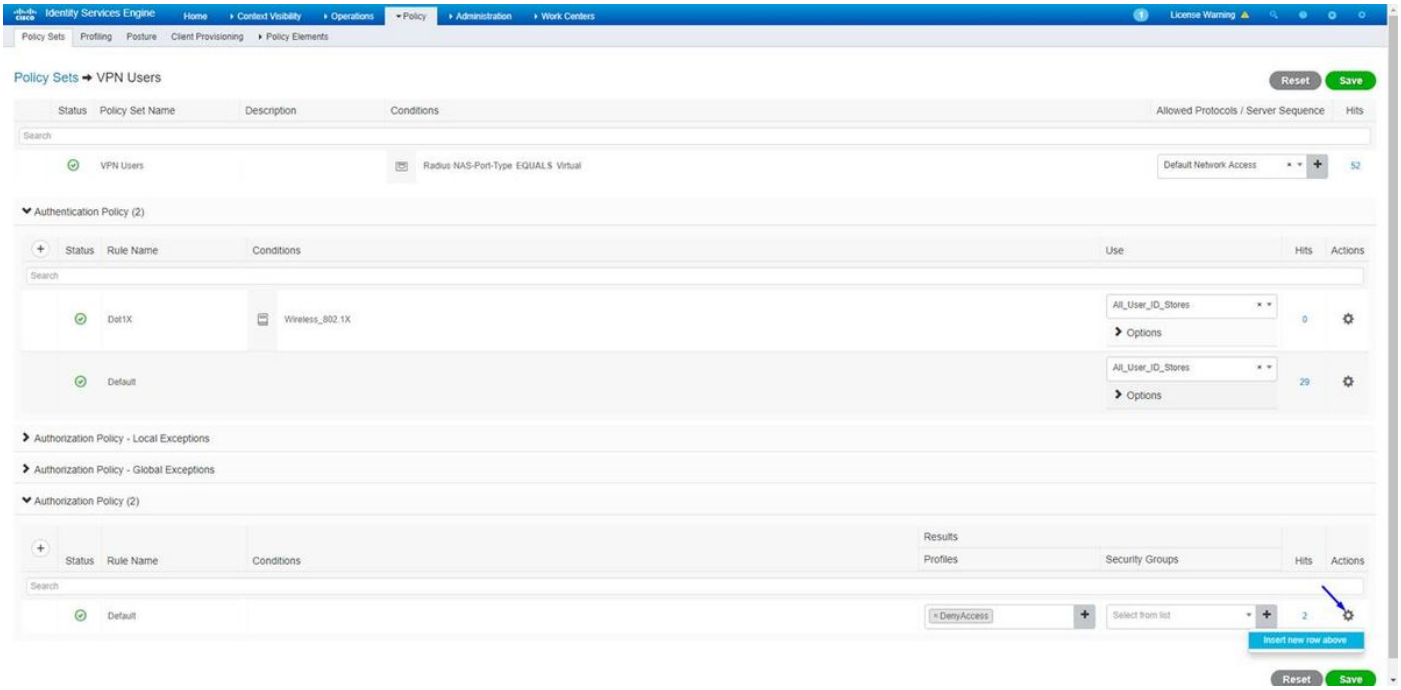
按一下**Policy > Policy** Set >為以下型別的任何身份驗證請求建立Policy **Set**:
Radius-NAS-Port-Type EQUALS Virtual
這意味著，如果任何進入ISE的RADIUS請求看起來像VPN連線，它們將訪問此策略集



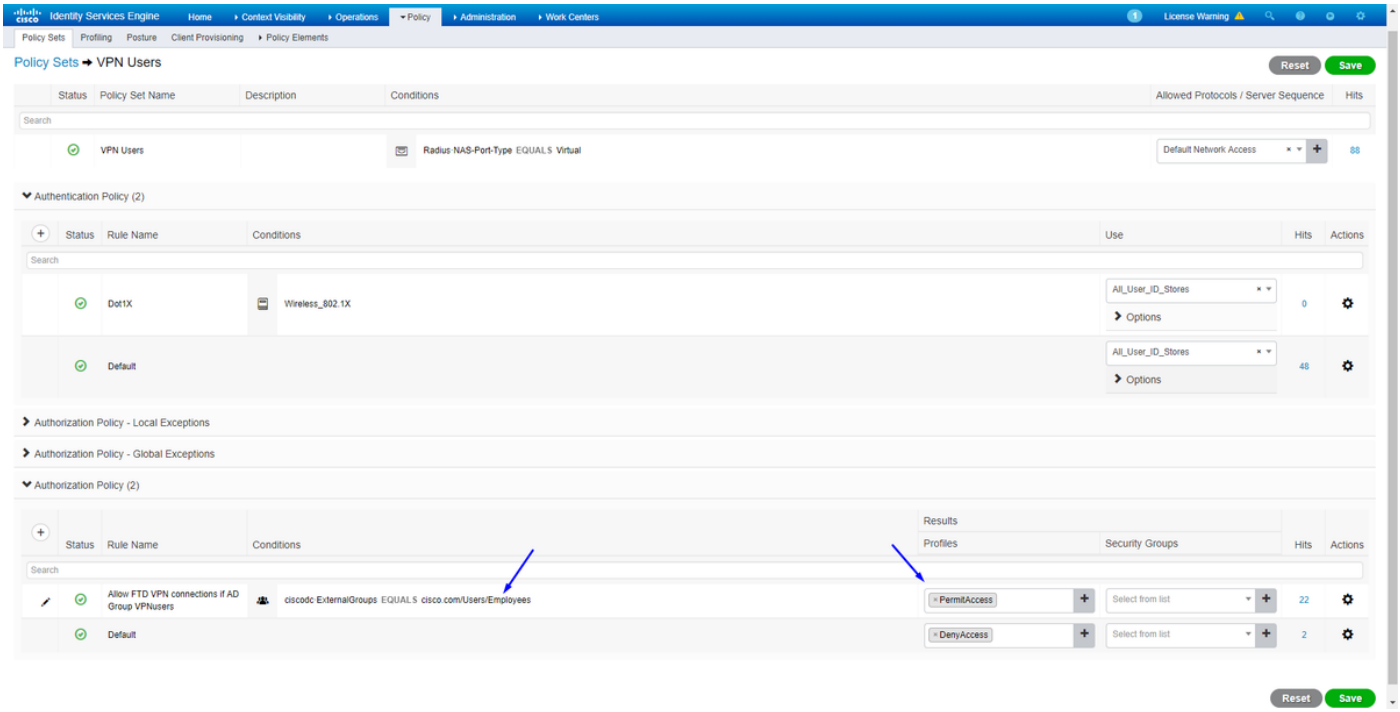
您可以在以下位置找到思科ISE中的條件：



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：

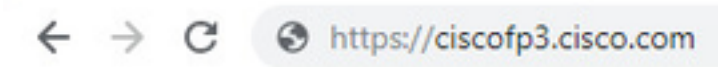


下面是完成規則後的外觀

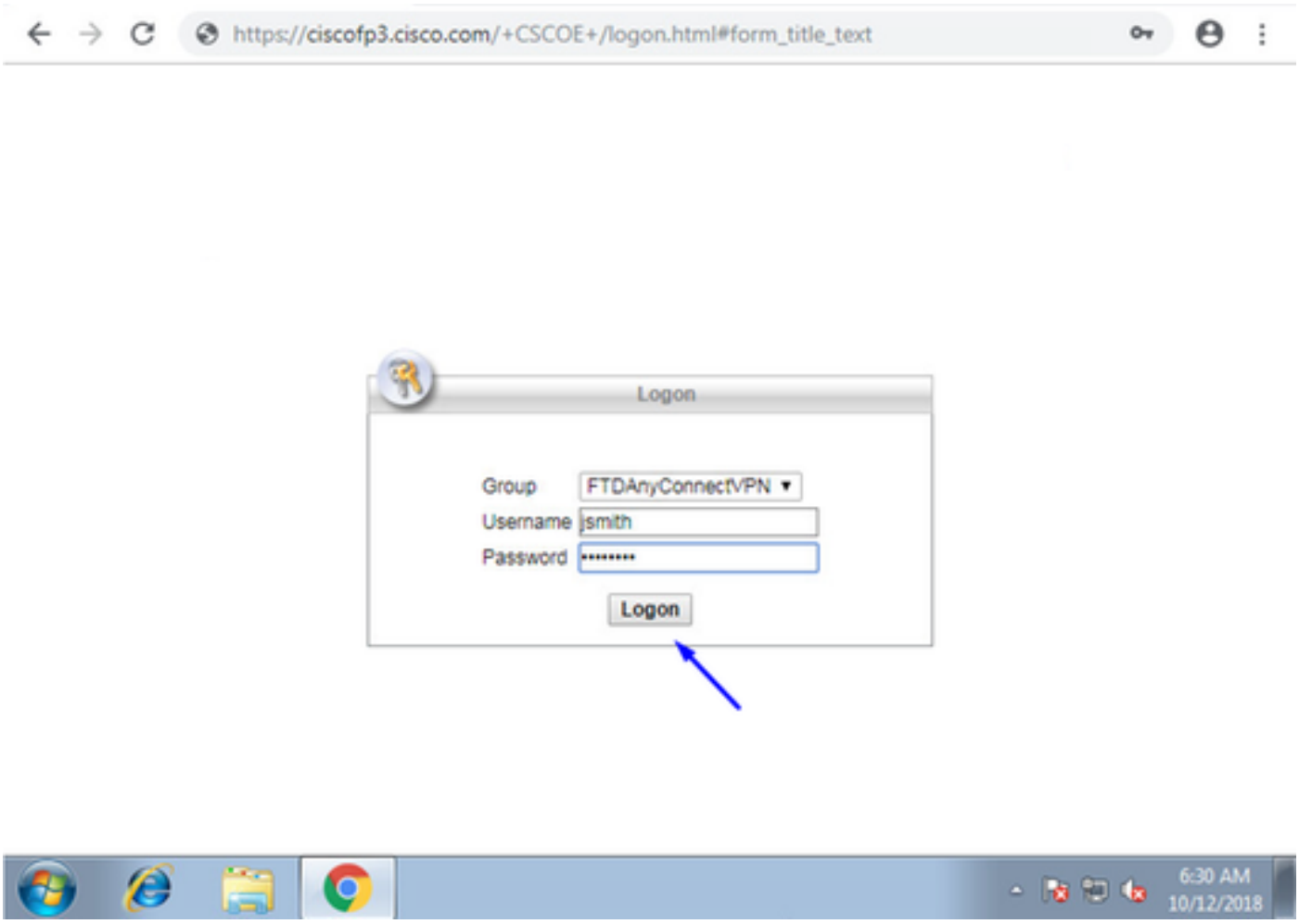


在員工Windows/Mac PC上使用AnyConnect VPN客戶端下載、安裝並連線到FTD

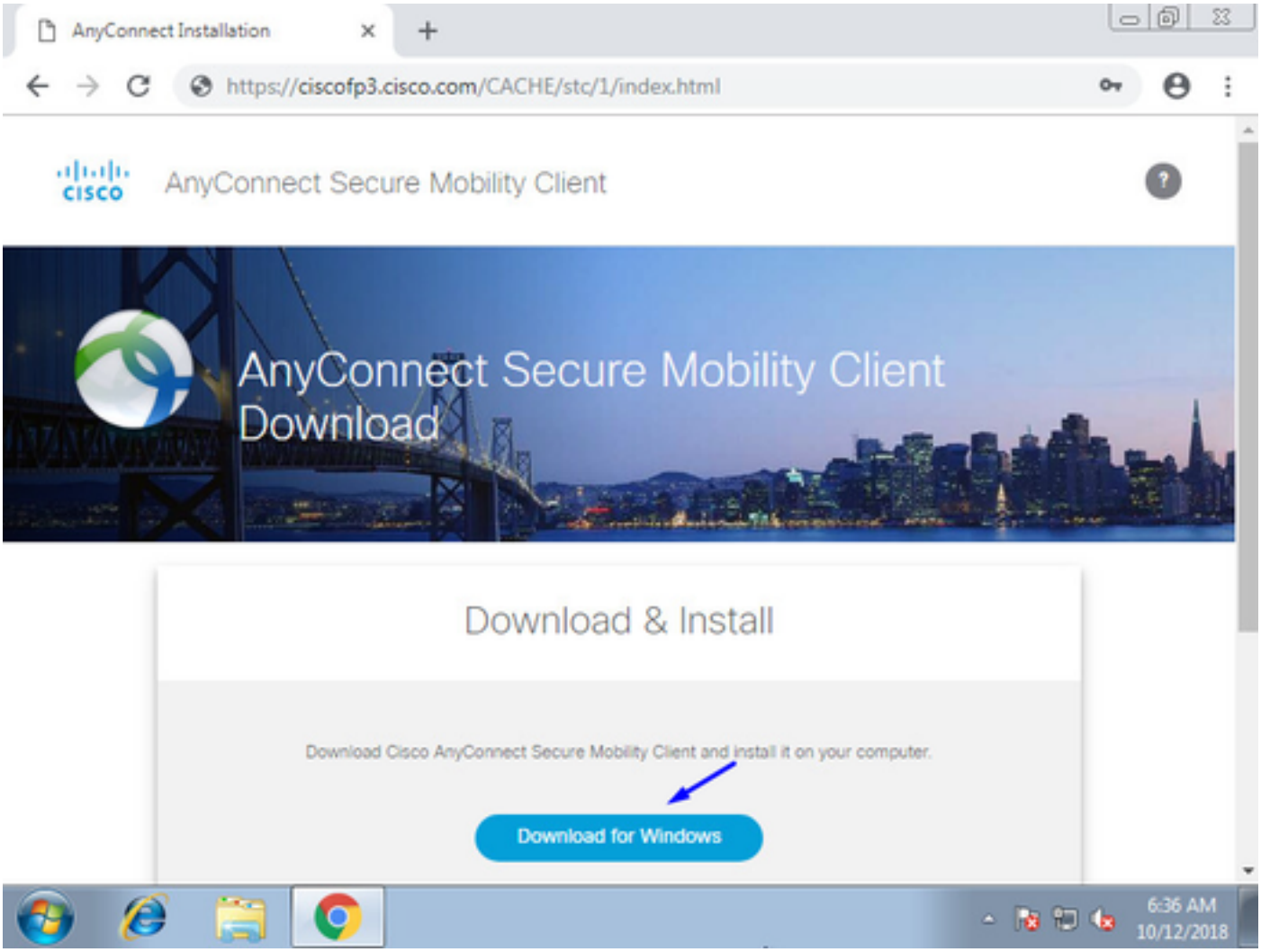
在員工Windows/Mac PC上開啟瀏覽器，在瀏覽器中轉到FTD的外部地址



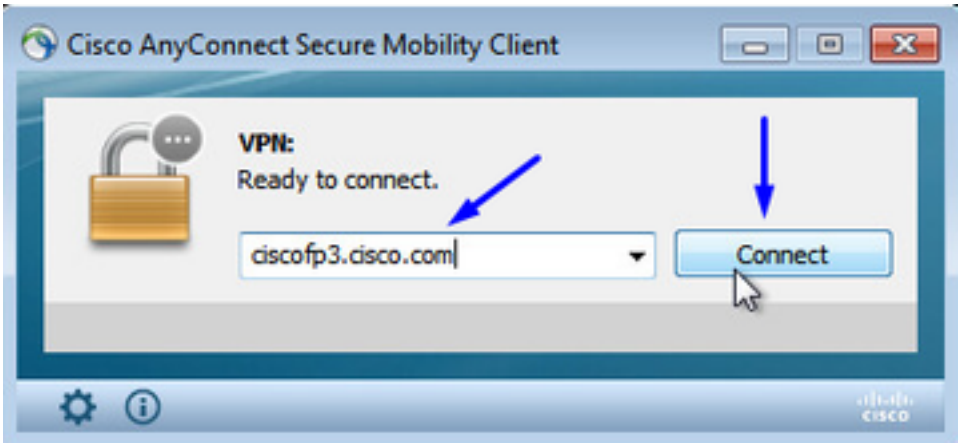
鍵入您的Active Directory使用者名稱和密碼



按一下「Download」

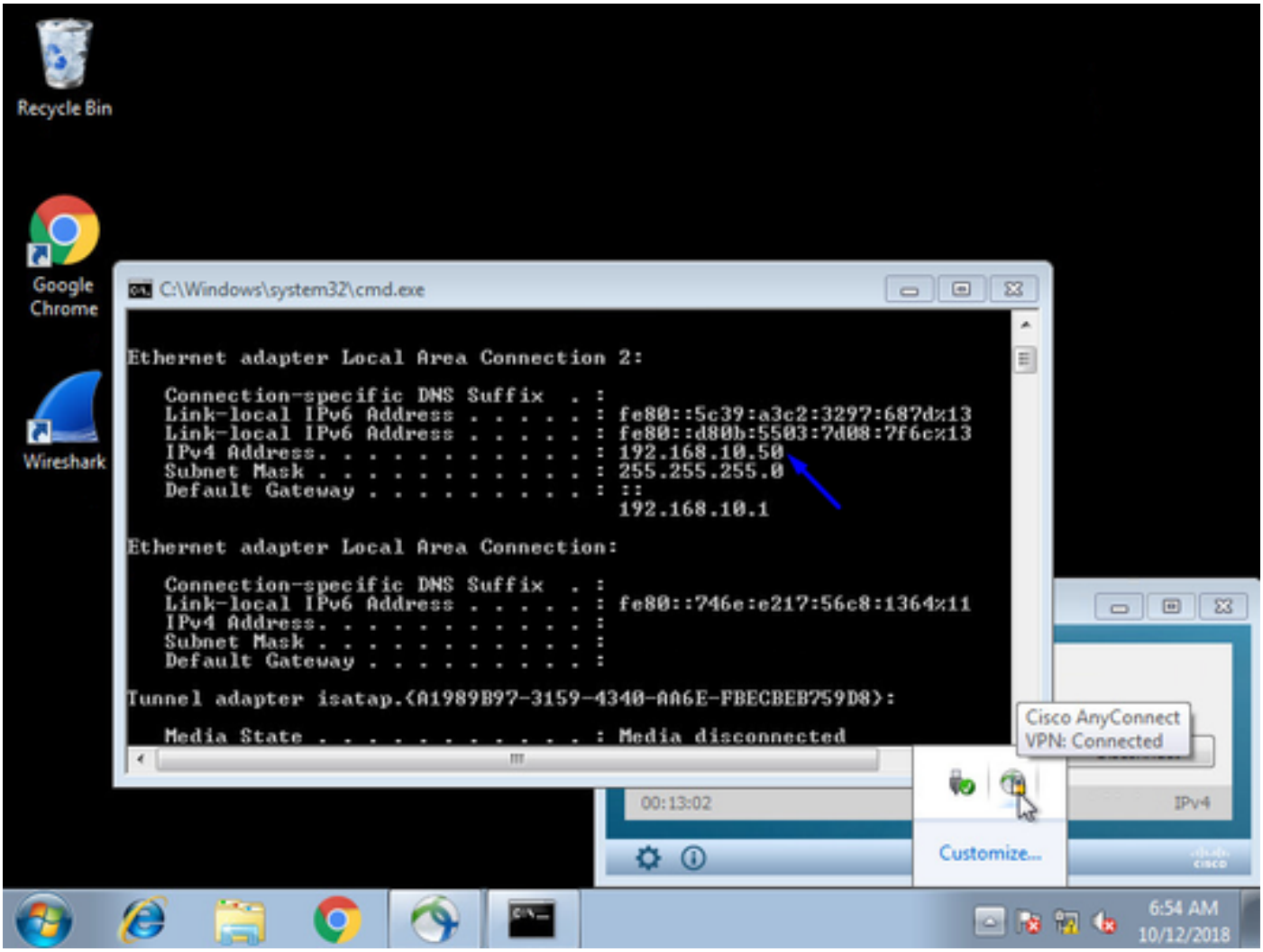


在Windows/Mac PC上安裝並運行AnyConnect VPN安全移動客戶端



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)
```

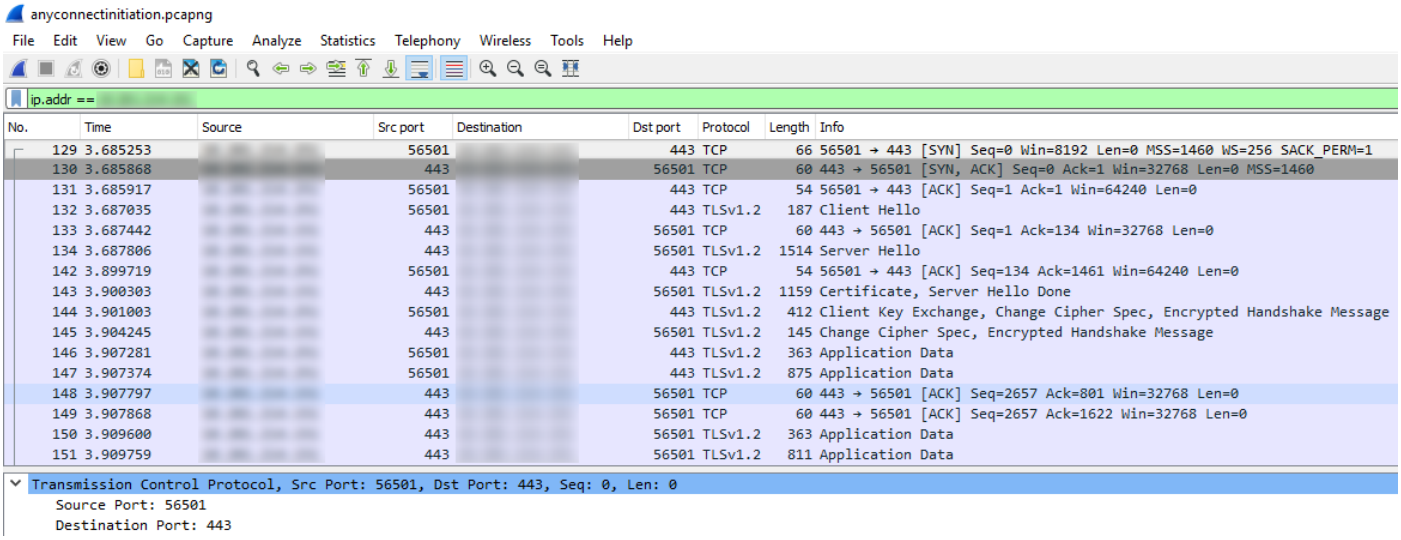
驗證NAT規則是否配置正確：

```
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
```

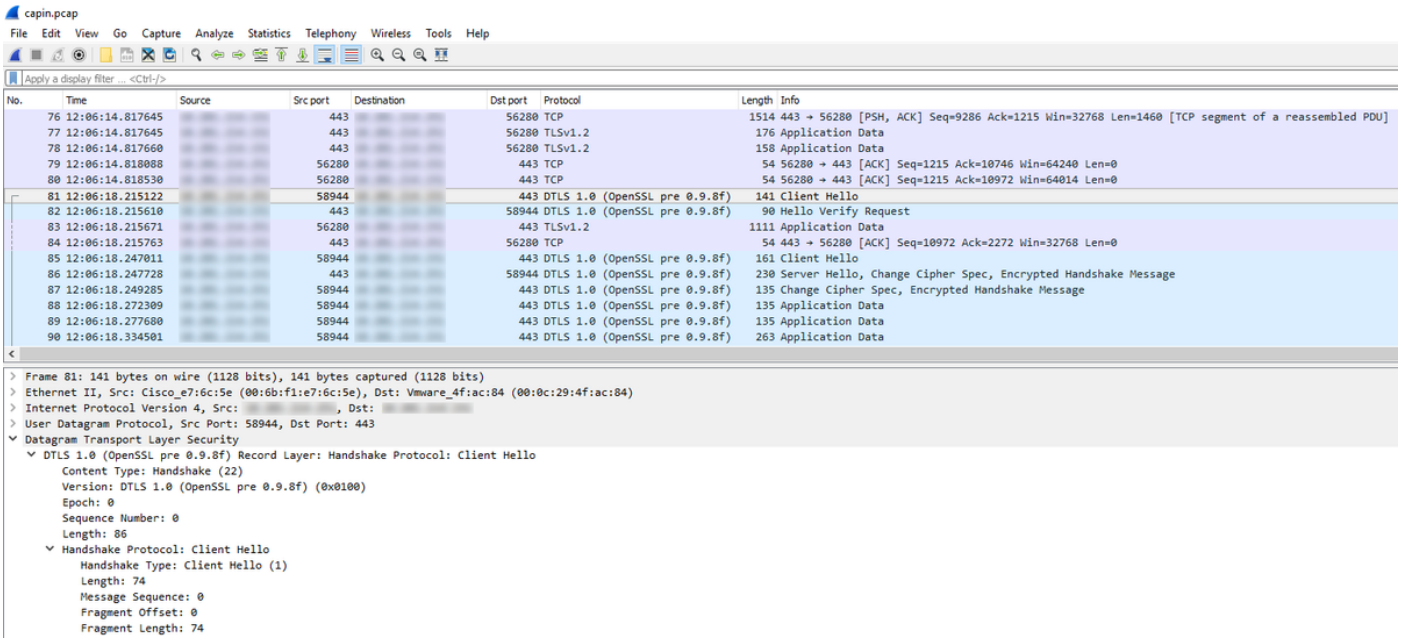
```
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.1.30 using egress ifc inside

Phase: 4
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static inside-subnet inside-subnet destination static outside-
subnet-anyconnect-po ol 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-po ol 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-po ol 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#
```

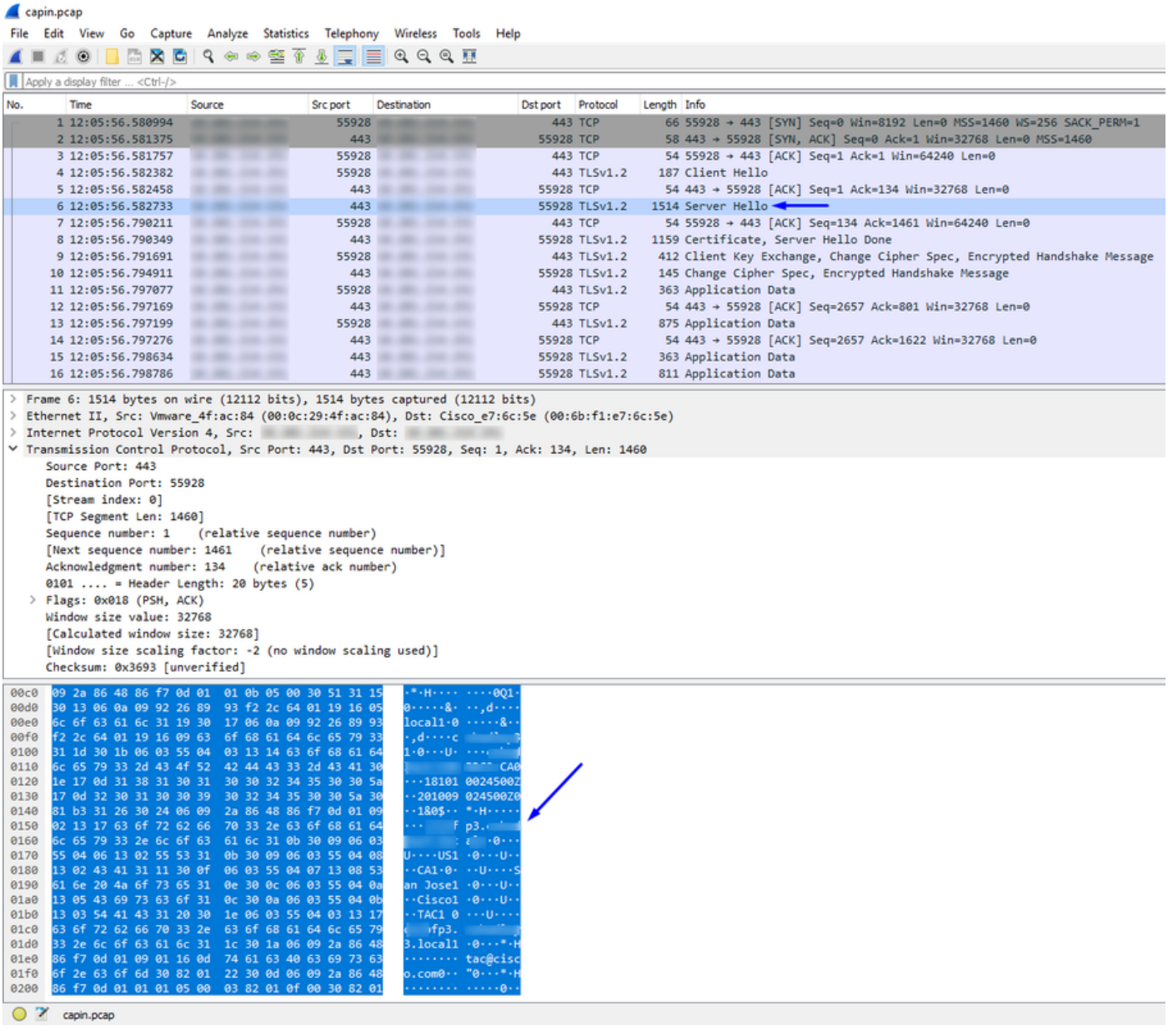
在PC的員工PC上捕獲並成功通過AnyConnect VPN連線到FTD



您還可以在同一捕獲中看到稍後形成的DTLS隧道



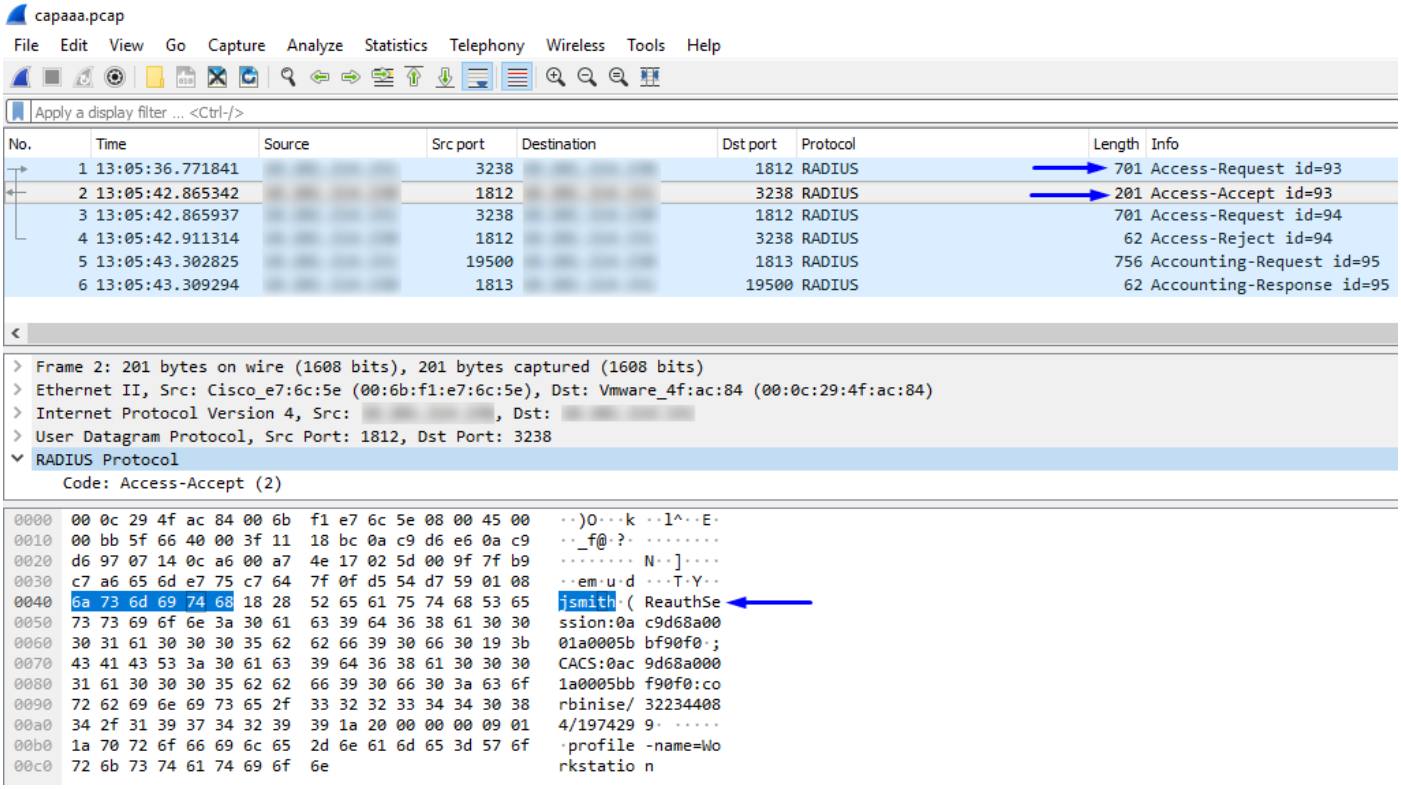
在FTD的外部介面上擷取，顯示AnyConnect PC成功連線到VPN



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)

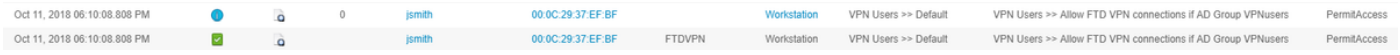


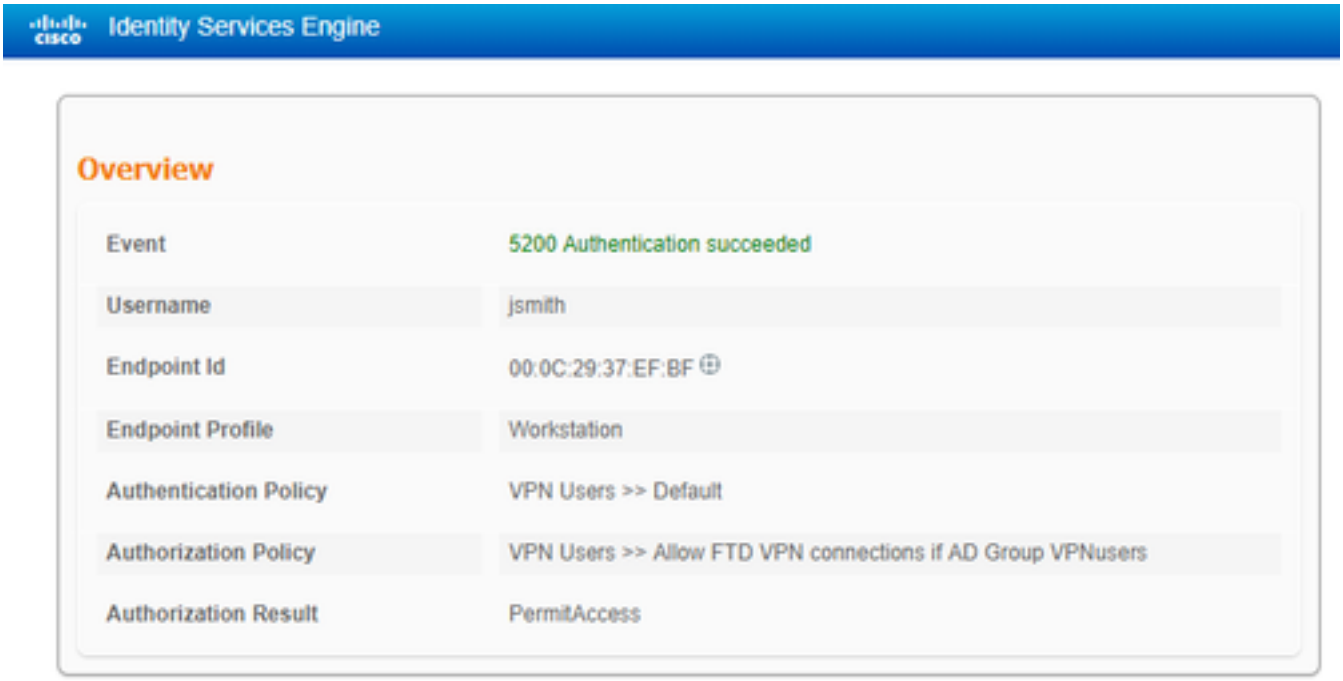
正如您所看到的，我們的VPN連線獲得訪問接受，我們的AnyConnect VPN客戶端通過VPN成功連線到FTD

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）

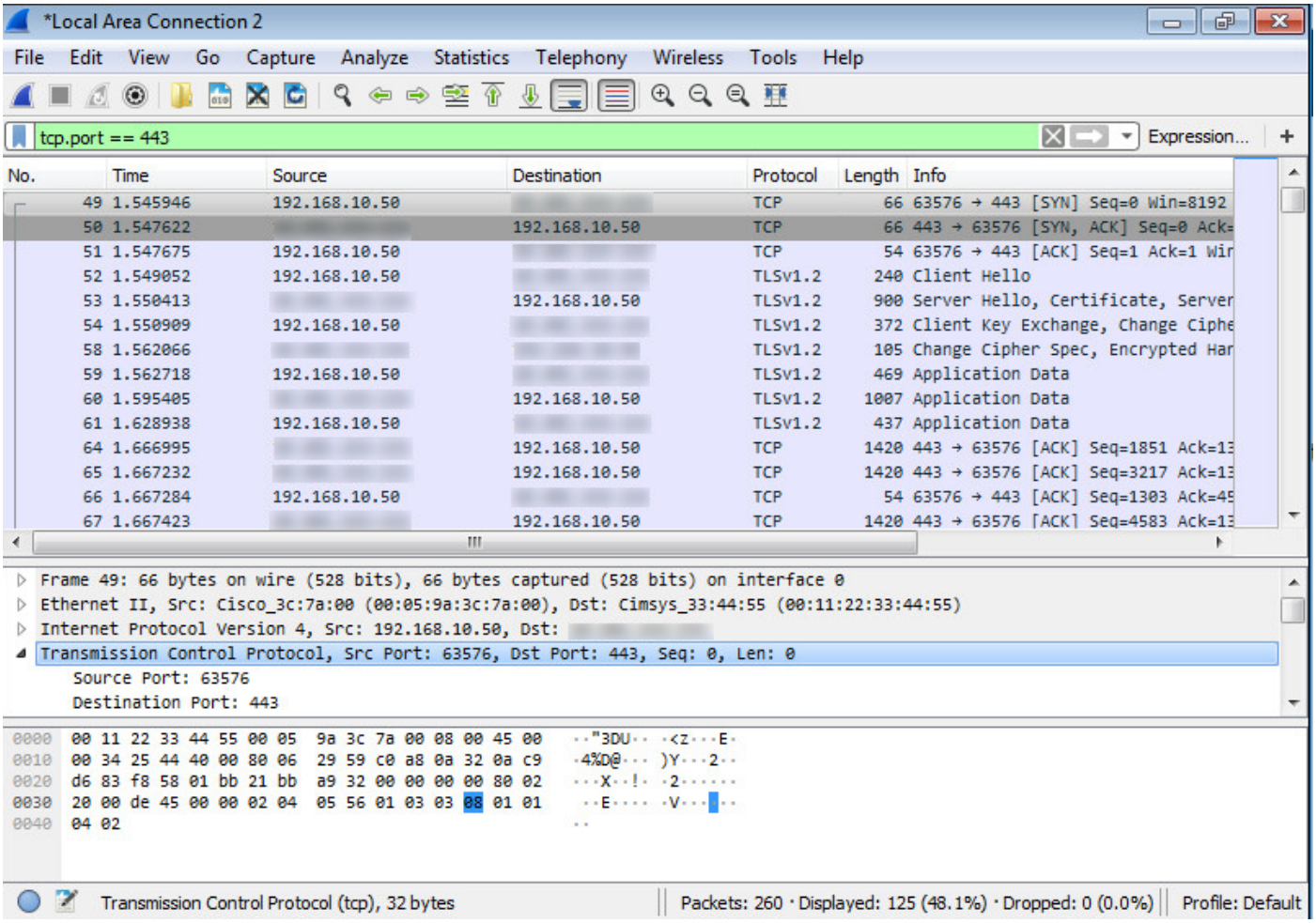
```
ciscofp3# capture capout interface inside trace detail trace-count 100 [Capturing - 35607 bytes]
ciscofp3# show cap
ciscofp3# show cap capout | i 192.168.1.10
37: 01:23:52.264512 192.168.1.1.3238 > 192.168.1.10.1812: udp 659
38: 01:23:52.310210 192.168.1.10.1812 > 192.168.1.1.3238: udp 159
39: 01:23:52.311064 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





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）：



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 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 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 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 = 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 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 | 050005bbe1f91.3.
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 | 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 = 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 | 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 = 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 asigned: 192.168.10.50
cstp_util_address_ipv6_accept: No IPv6 Address
np_svc_create_session(0x7000, 0x00002acdff1d6440, 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(dtlshdr) - 16(dtlsiv) = 1443
mod-mtu = 1443(mtu) & 0xfff0(complement) = 1440
dtls-mtu = 1440(mod-mtu) - 1(cdtp) - 20(mac) - 1(pad) = 1418
computed tls-mtu=1367 dtls-mtu=1418 conf-mtu=1406
DTLS enabled for intf=3 (outside)
overide 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

Identity Services Engine

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	00000000000070005bbc08c3
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

11002 Returned RADIUS Access-Accept

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

Identity Services Engine

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
DTLSSupport	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=0000000000070005bbc08c3, 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
```

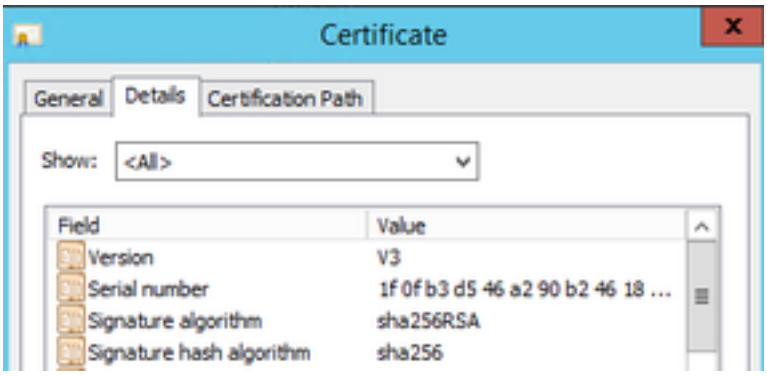
ISE CLI:

```
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=cicscofp3.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
...
```