在FDM管理的FTD上配置啟用IPv6的RAVPN和AAA身份驗證

目錄

簡介

本文檔介紹在FDM管理的FTD上配置啟用IPv6的遠端訪問VPN的AAA身份驗證的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Secure Firepower Device Manager(FDM)虛擬
- 思科安全防火牆威脅防禦(FTD)虛擬
- VPN身份驗證流程

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco安全FDM虛擬7.6.0
- Cisco安全FTD虛擬7.6.0
- 思科安全使用者端5.1.6.103

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

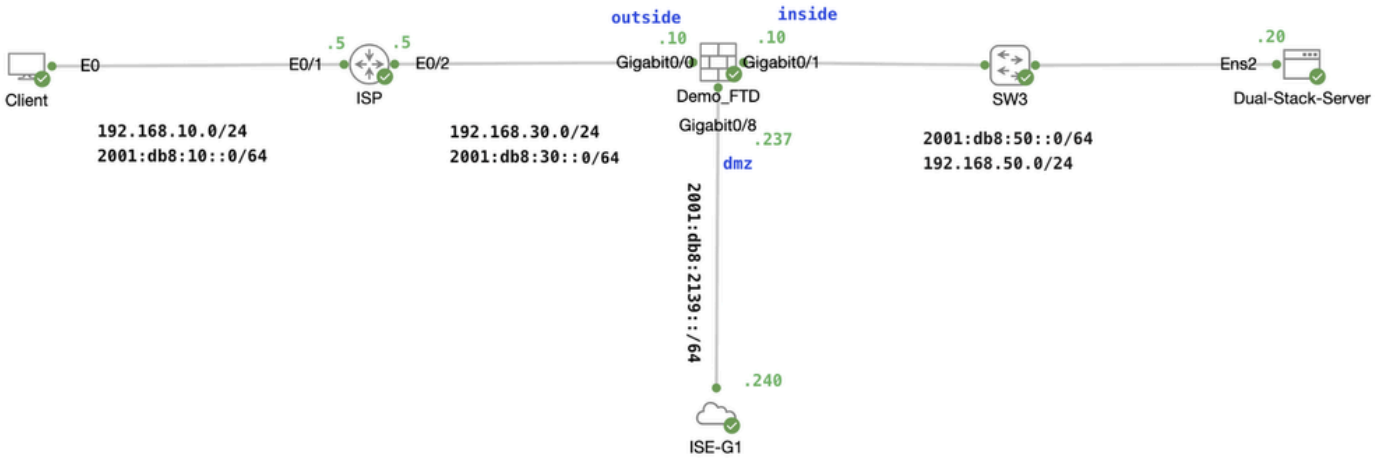
背景資訊

IPv6遠端訪問VPN(RAVPN)越來越重要，因為世界從IPv4過渡到IPv6，因為IPv4地址有限且幾乎已用盡，而IPv6提供的地址空間幾乎是無限的，可適應網際網路連線裝置數量的不斷增長。隨著更多網路和服務遷移到IPv6，具有IPv6功能可確保您的網路保持相容和可訪問。IPv6 RAVPN可幫助組織為未來的網路做好準備，確保安全且可擴展的遠端連線。

在本示例中，客戶端使用服務提供商提供的IPv6地址與VPN網關通訊，但從VPN池接收IPv4和IPv6地址，並使用思科身份服務引擎(ISE)作為身份驗證身份源。ISE僅配置了IPv6地址。內部伺服器配置了IPv4和IPv6地址，代表雙堆疊主機。客戶端可使用IPv4或IPv6 VPN地址訪問內部資源。

設定

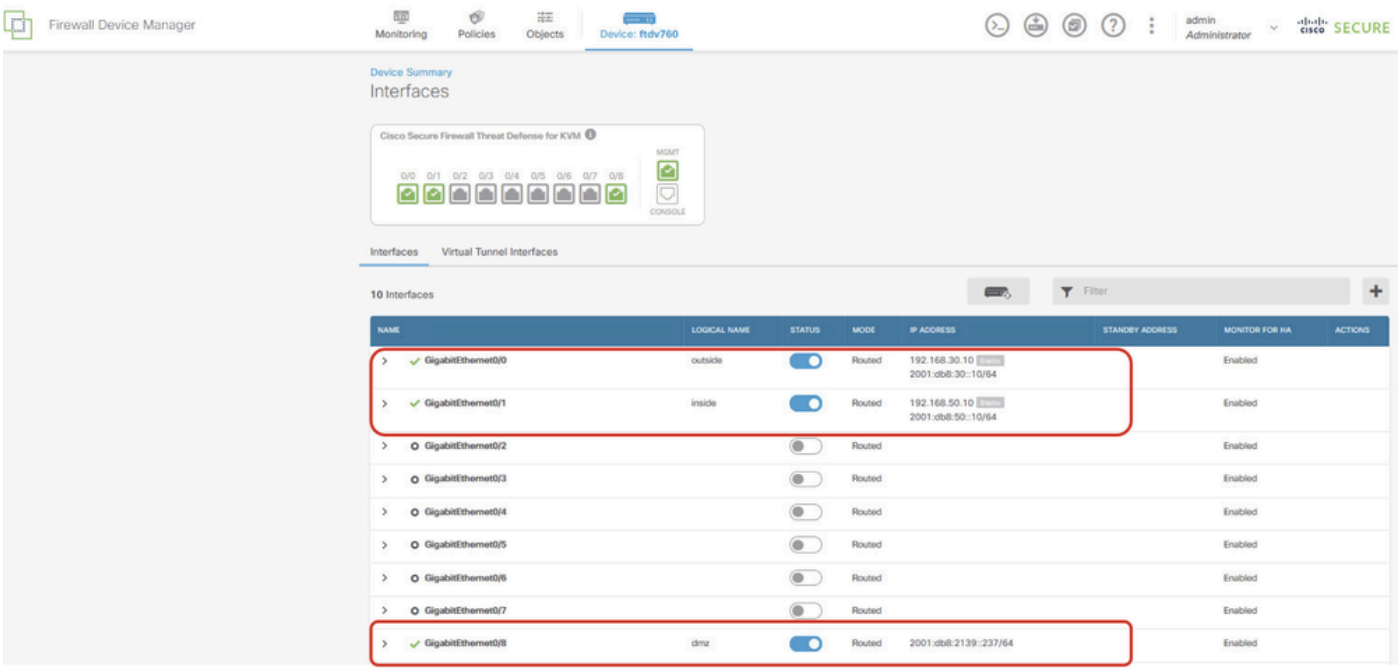
網路圖表



拓撲

FDM上的配置

步驟1.確保節點之間IPv4和IPv6互連的初步配置已順利完成。客戶端和FTD的網關是相關的ISP地址。伺服器的閘道位於FTD的IP內。ISE位於FTD的DMZ區域。

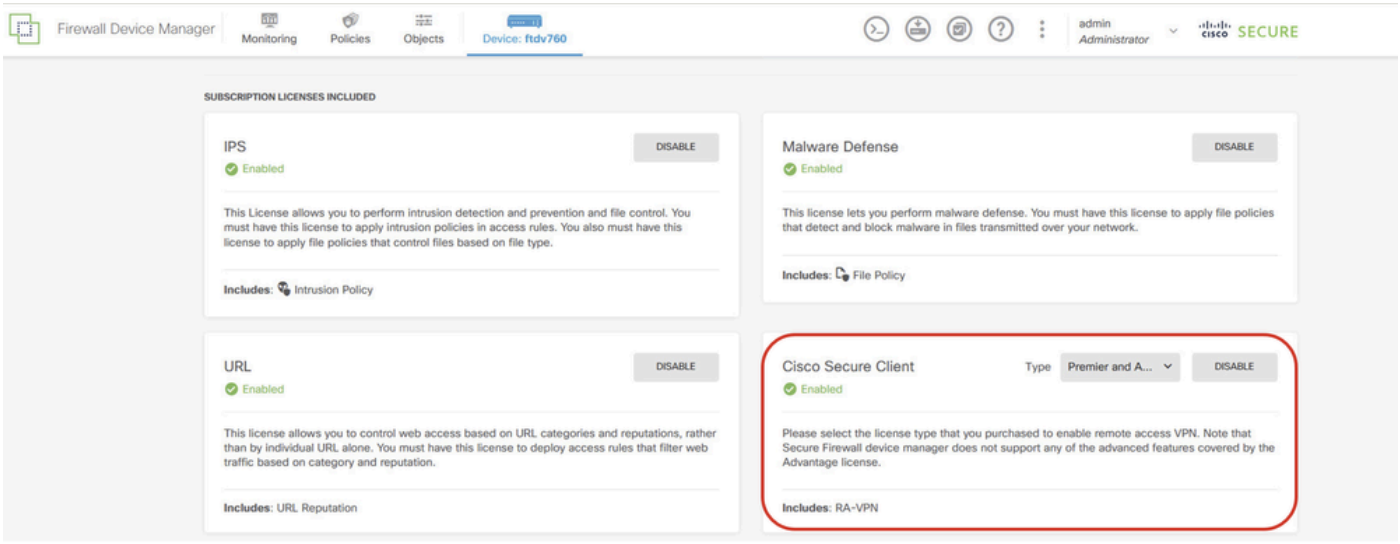


FTD_Interface_IP

FTD_Default_Route

步驟2. 從「Cisco Software Download」下載Cisco Secure Client軟體包nameccisco-secure-client-win-5.1.6.103-webdeploy-k9.pkg，並確認下載檔案的md5校驗和與「Cisco Software Download」頁面相同，以確保下載後檔案完好。

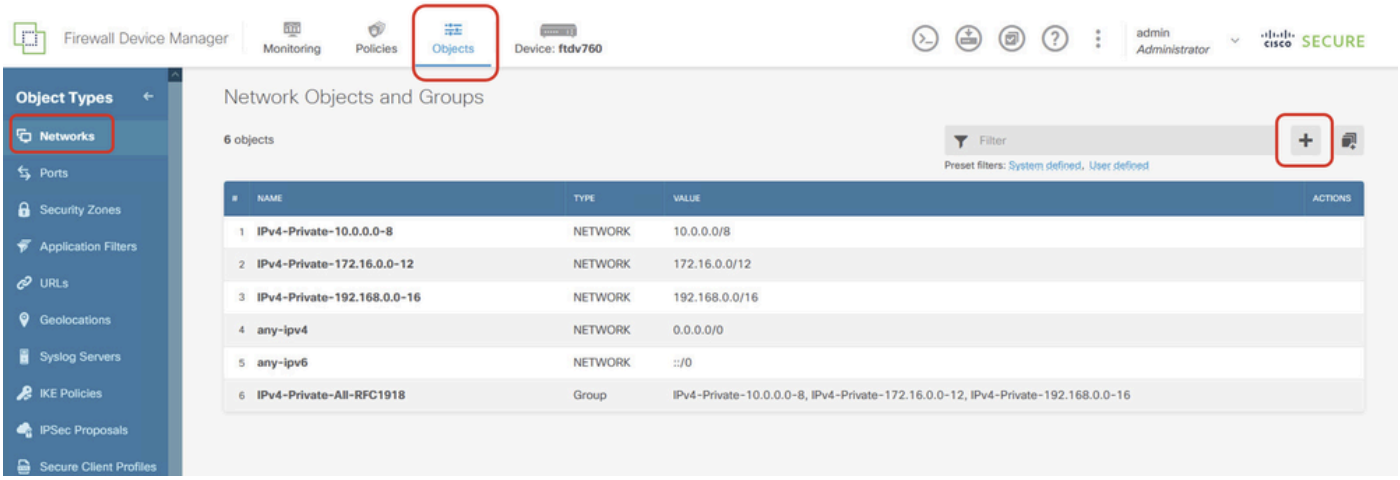
步驟3.驗證FTD上是否已啟用RAVPN相關授權。



FDM_License

步驟4.建立VPN地址池。

步驟4.1.通過建立網路對象建立IPv6和IPv4地址池。導航到對象>網絡並按一下+按鈕。

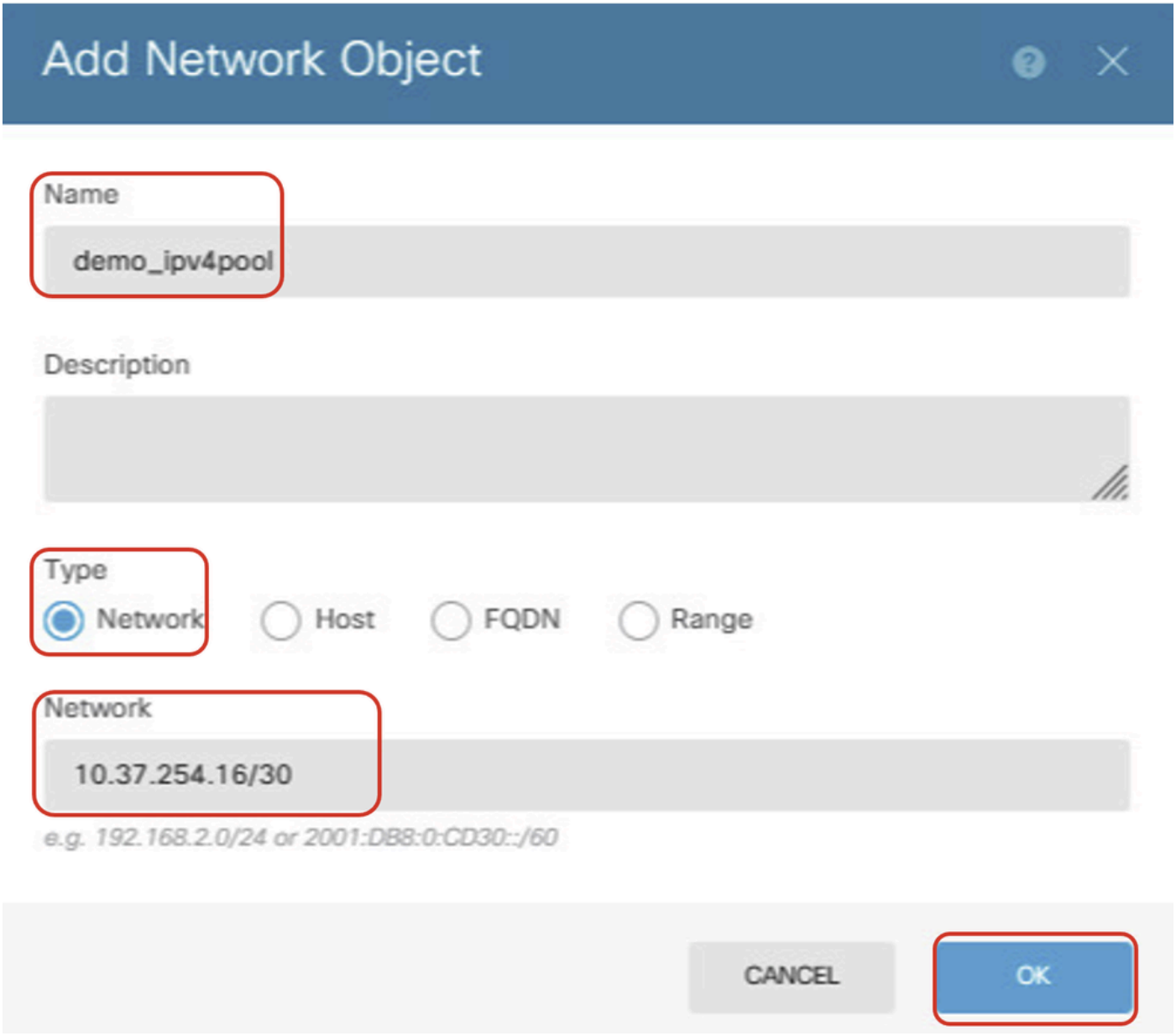


Create_VPN_Address_Pool_1

步驟4.2.提供每個網路對象的必要資訊。按一下OK按鈕。

對於IPv4池，可以使用「網路」或「範圍」選擇對象型別。在此示例中，為演示目的選擇對象型別「網路」。

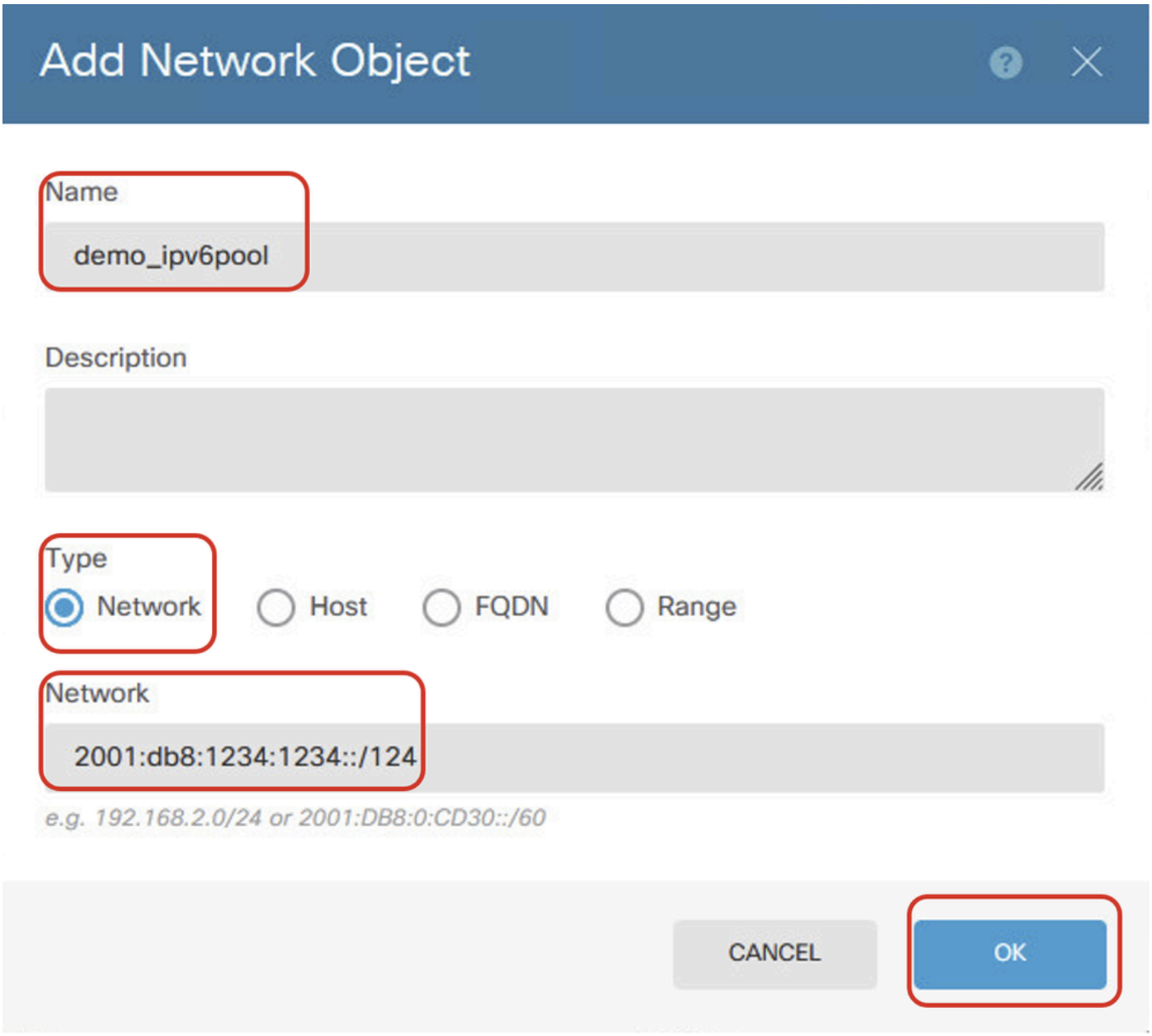
- 名稱:demo_ipv4pool
- Type:網路
- 網路：10.37.254.16/30



Create_VPN_Address_Pool_2_IPv4

對於IPv6池，現在只能使用網路選擇對象型別。

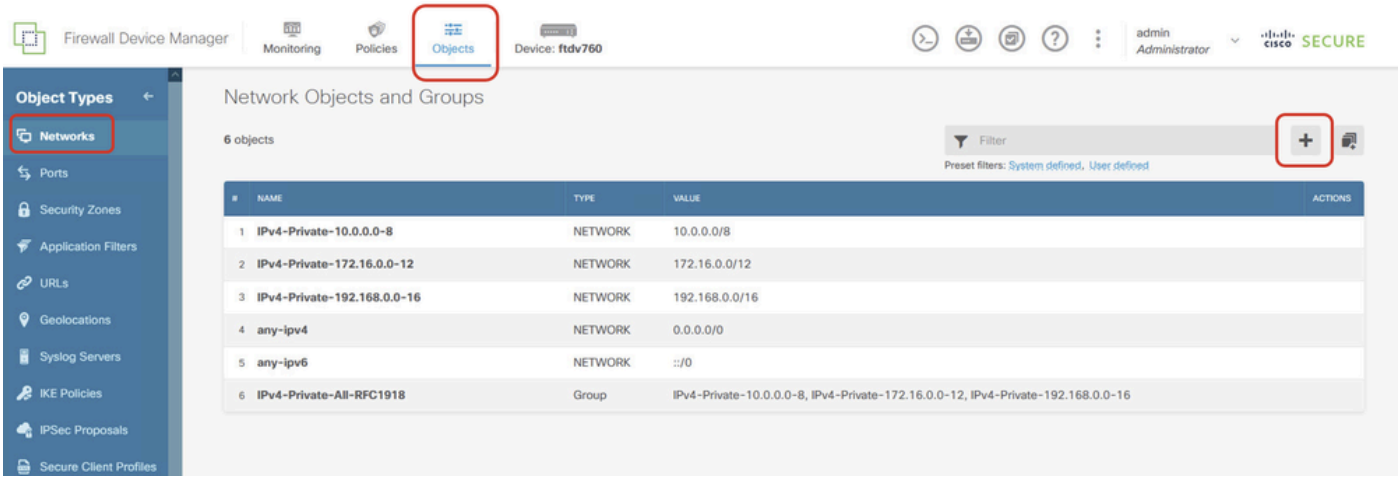
- 名稱:demo_ipv6pool
- Type:網路
- 網路：2001:db8:1234:1234::/124



Create_VPN_Address_Pool_2_IPv6

步驟5.為NAT豁免建立內部網路。

步驟5.1.導航到Objects > Networks，然後單擊+按鈕。

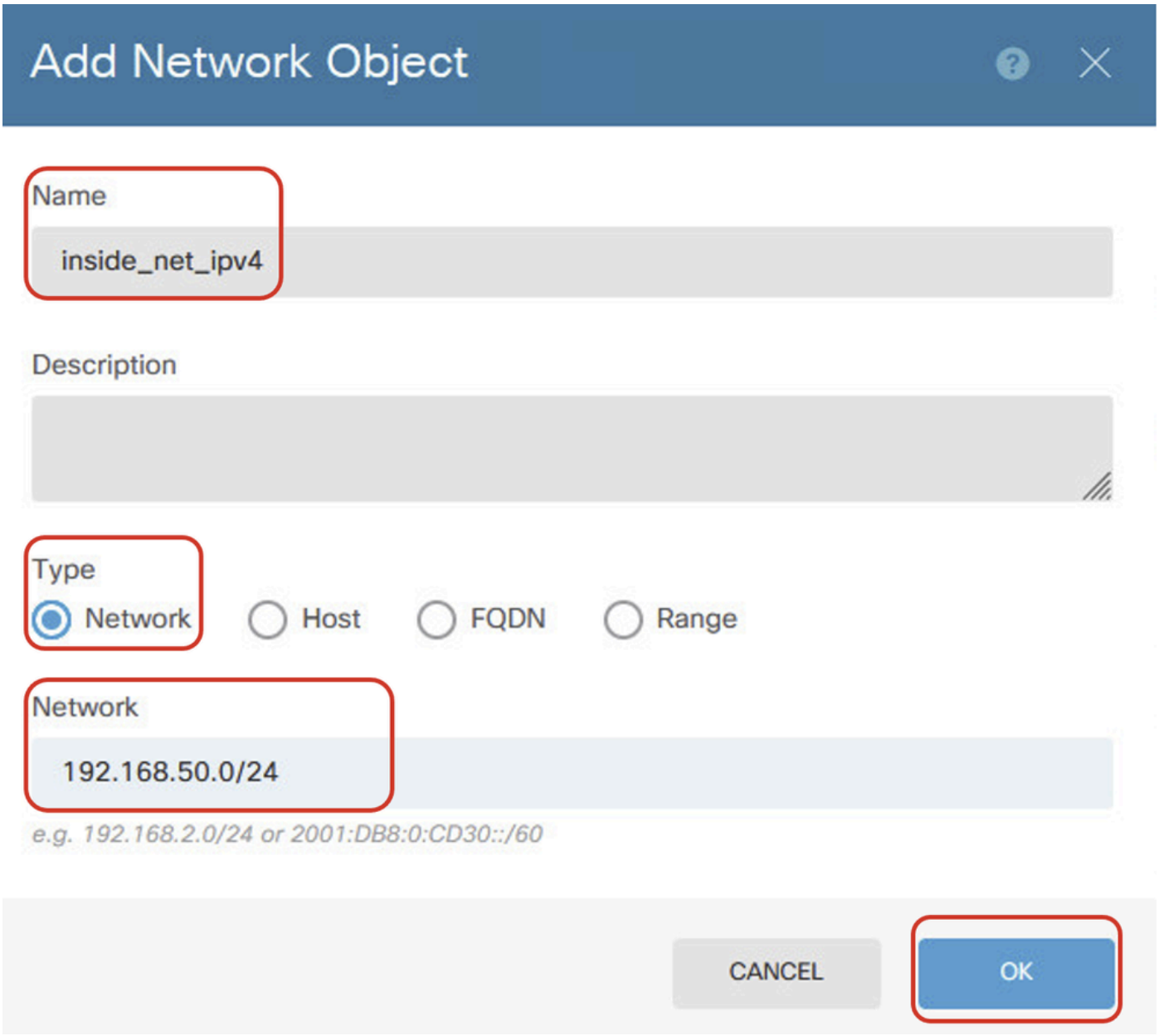


Create_NAT_Exempt_Network_1

步驟5.2.提供每個網路對象的必要資訊。按一下OK按鈕。

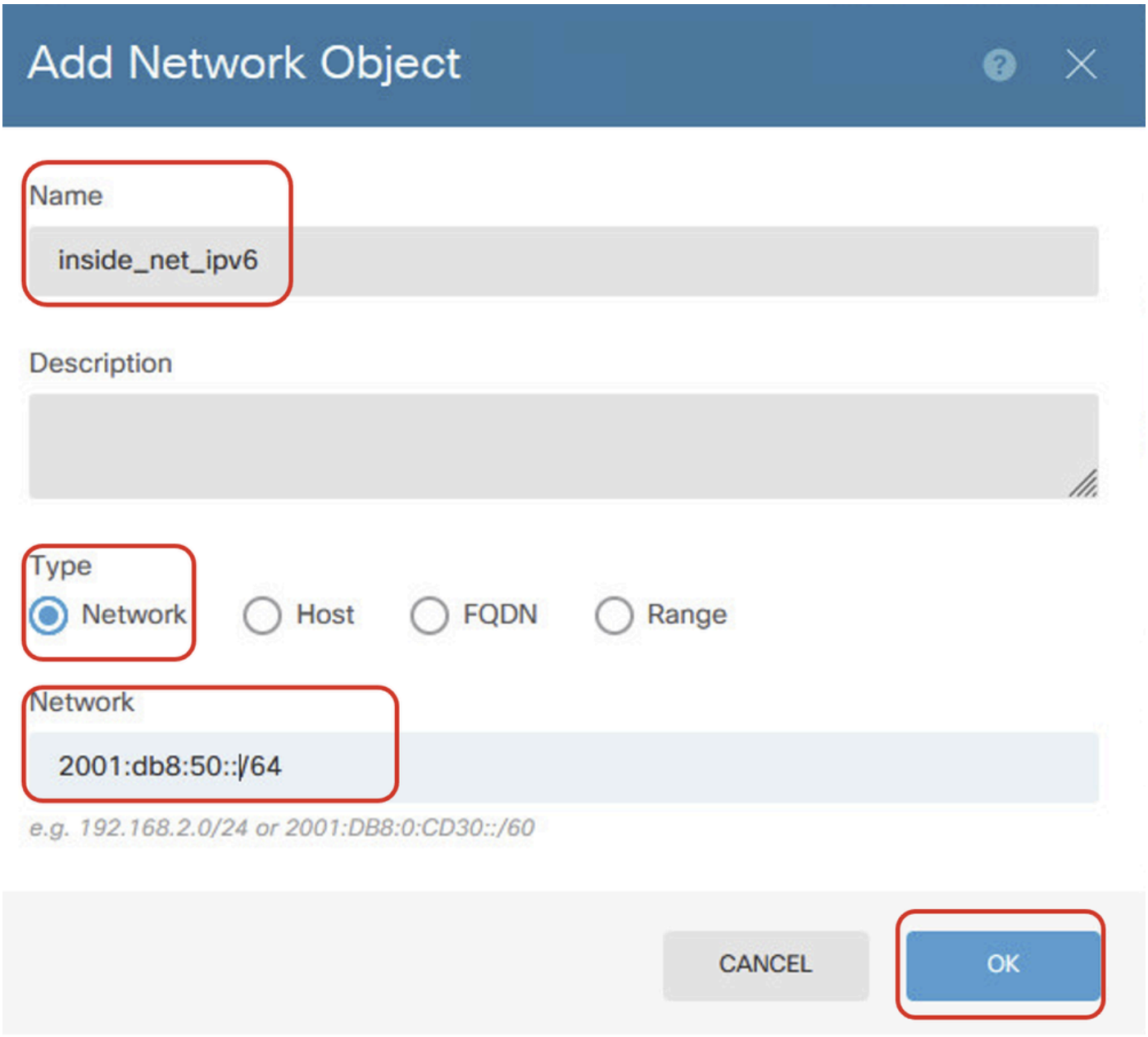
在本示例中，配置了IPv4和IPv6網路。

- 名稱:inside_net_ipv4
- Type:網路
- 網路：192.168.50.0/24



Create_NAT_Exempt_Network_2_IPv4

- 名稱:inside_net_ipv6
- Type:網路
- 網路：2001:db8:50::/64

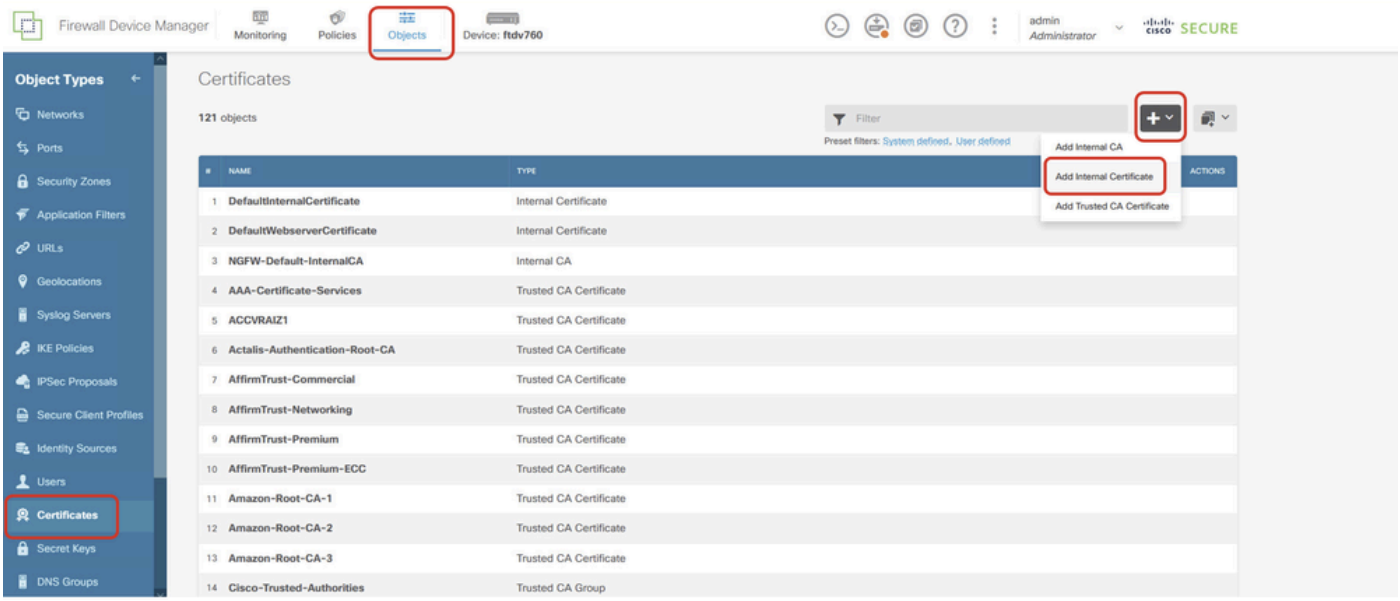


Create_NAT_Exempt_Network_2_IPv6

步驟6.建立用於RAVPN的證書。有兩種選擇：您可以上傳由第三方憑證授權單位(CA)簽署的憑證，或產生新的自簽署憑證。

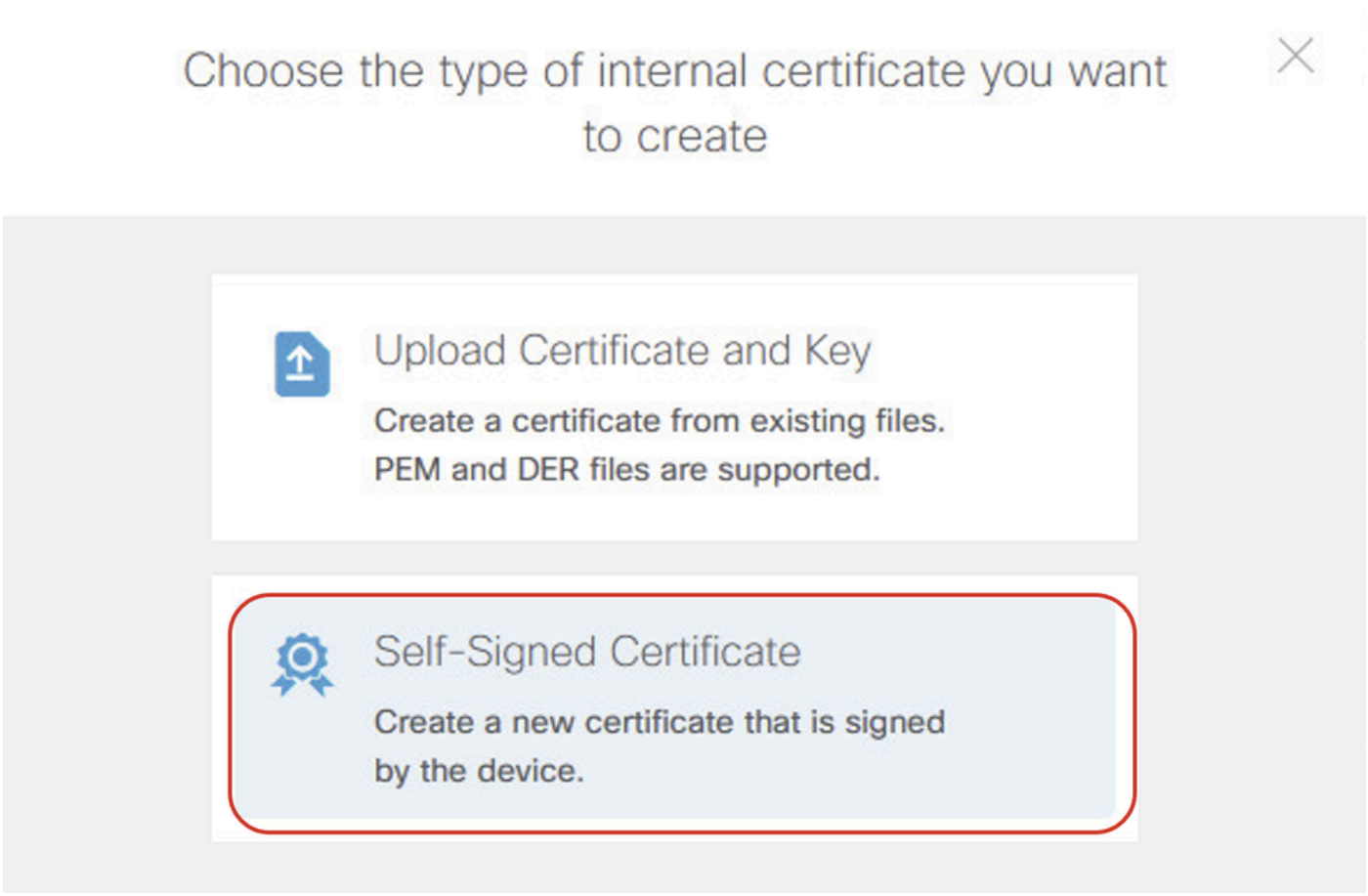
在本示例中，新的自簽名證書與自定義的證書內容一起使用，用於演示目的。

步驟6.1.導航至Objects > Certificates。按一下+按鈕並選擇Add Internal Certificate。



Create_Certificate_1

步驟6.2.按一下Self-Signed Certificate。



步驟6.3.按一下General頁籤並提供必要資訊。

名稱:demovpn

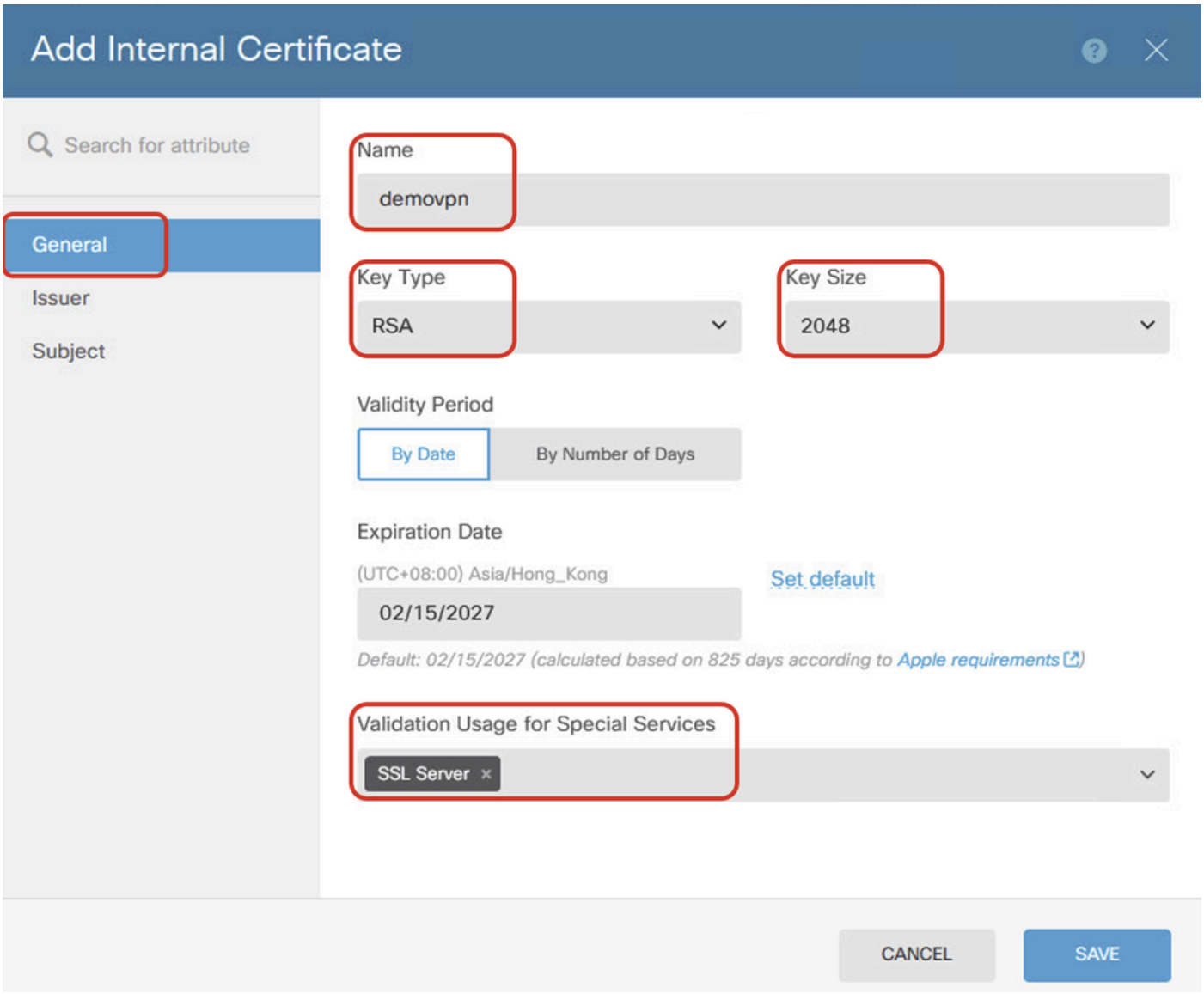
金鑰型別：RSA

金鑰大小：2048

有效期：預設

到期日期：預設

特殊服務的驗證用法：SSL伺服器

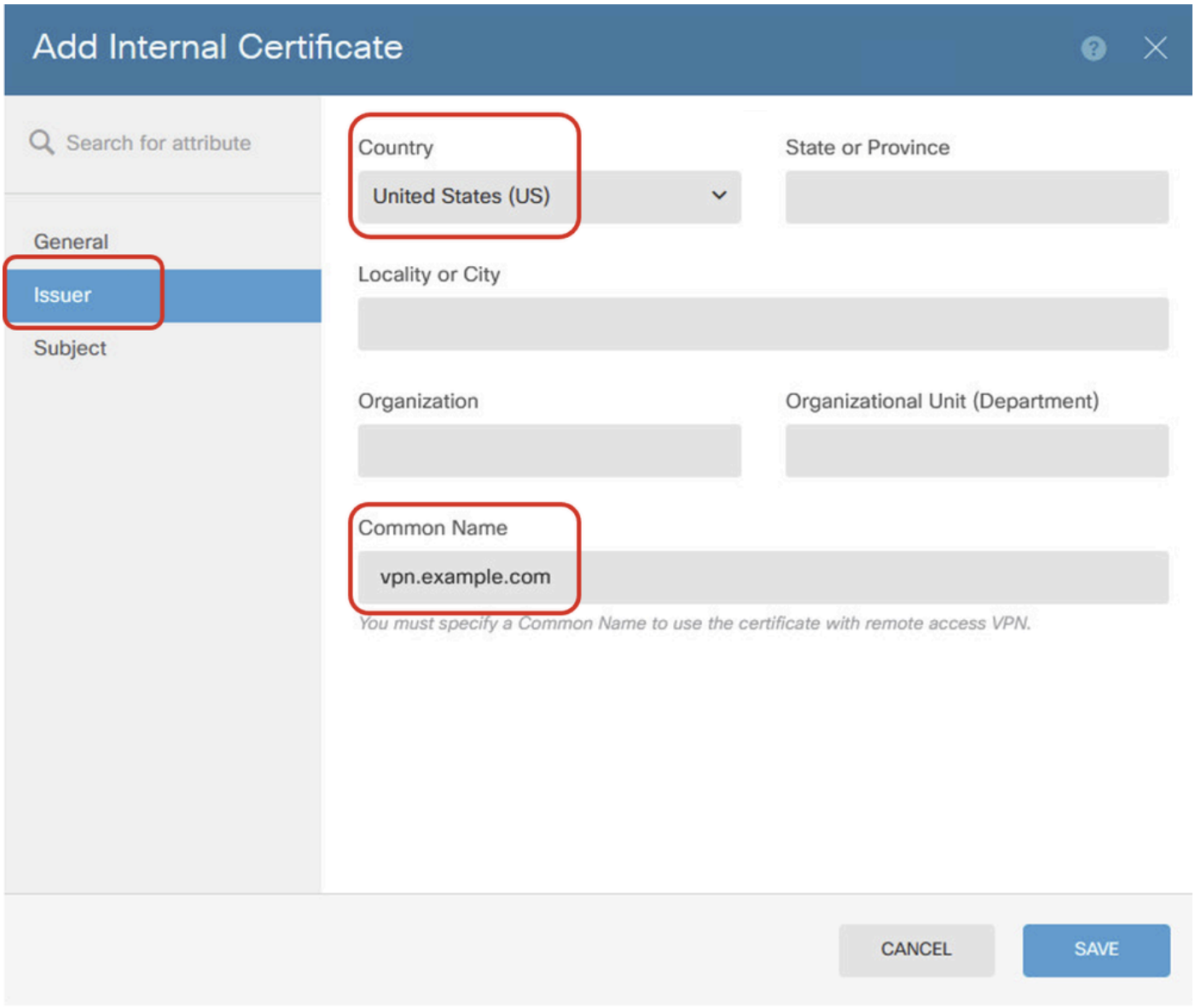


Create_Certificate_3

步驟6.4.按一下Issuer頁籤並提供必要資訊。

國家：美國

公用名：vpn.example.com

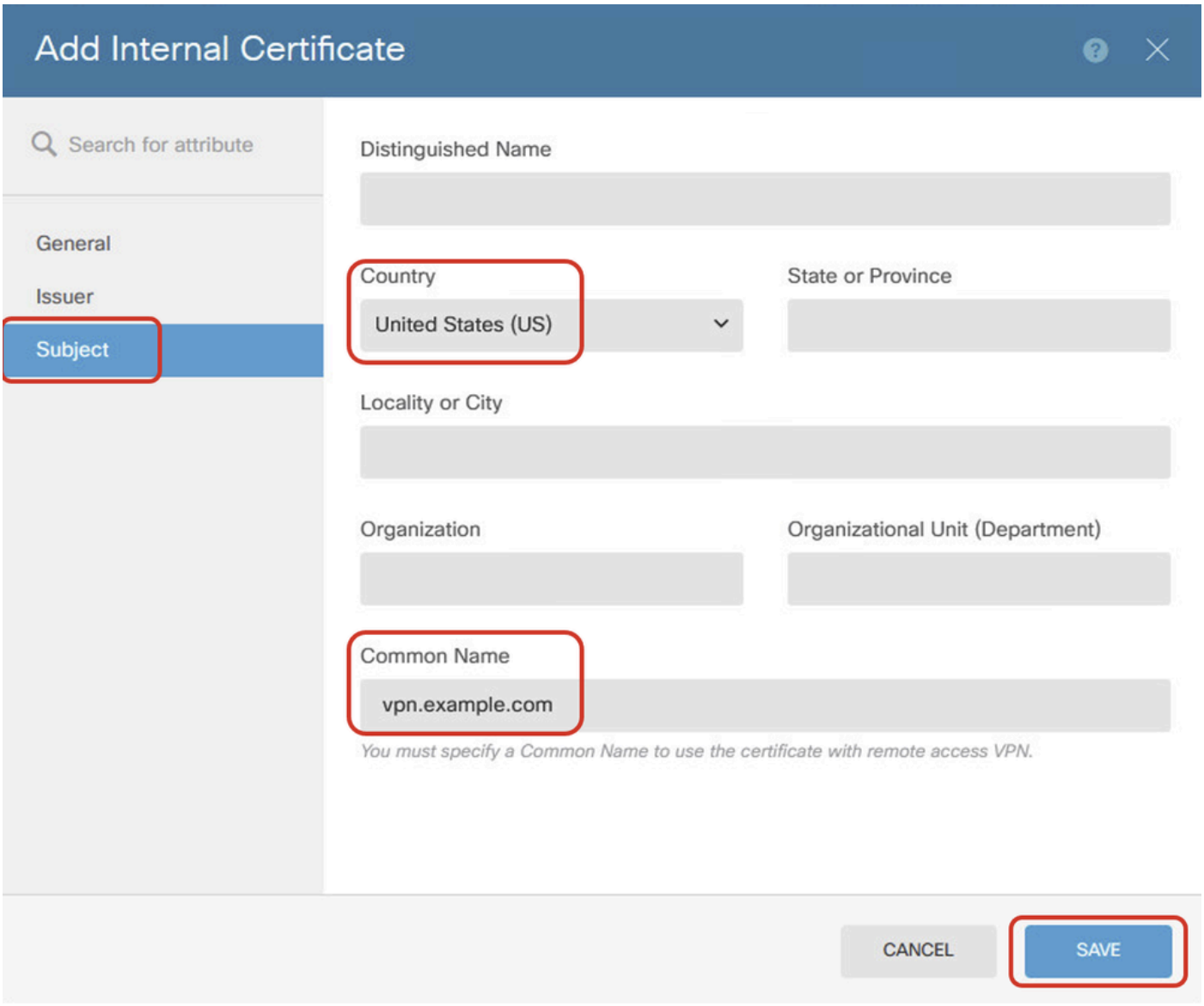


Create_Certificate_4

步驟6.5.按一下Subject頁籤，提供必要的資訊，然後按一下SAVE。

國家：美國

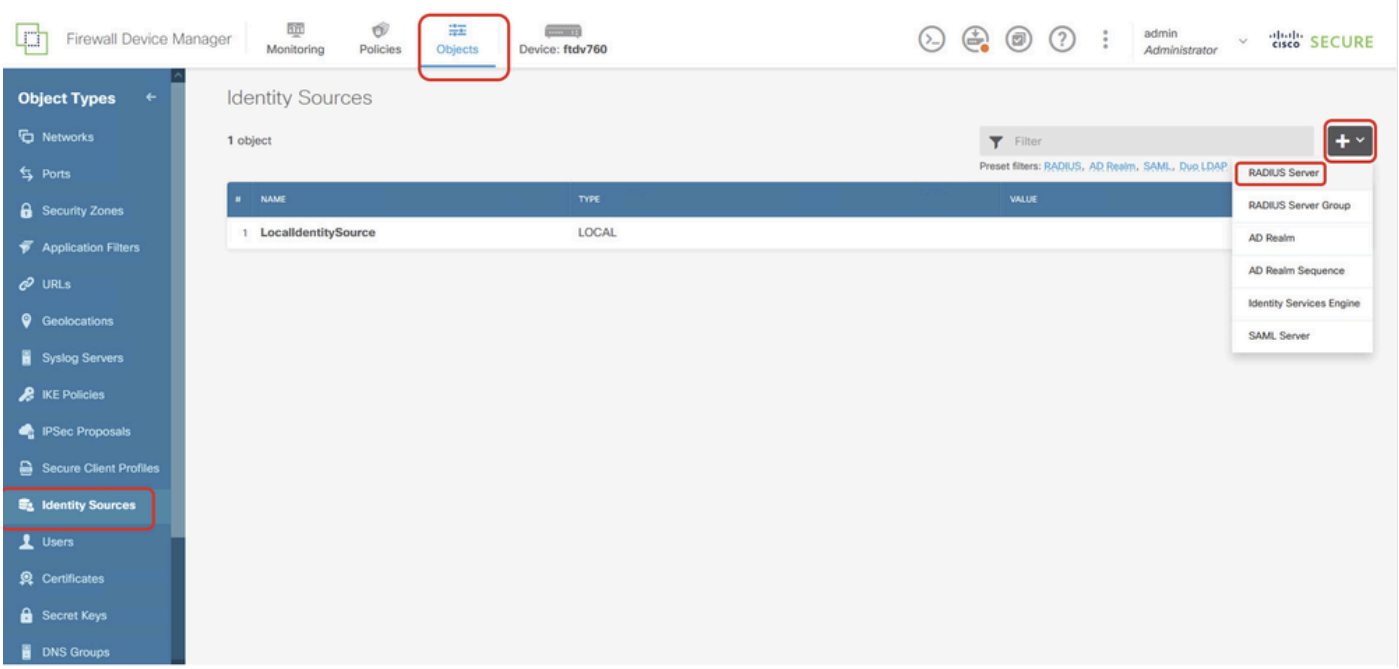
公用名：vpn.example.com



Create_Certificate_5

步驟7.建立RADIUS伺服器身份源。

步驟7.1. 導覽至Objects > Identity Sources,按一下+按鈕，然後選擇RADIUS Server。



Create_Radius_Source_1

步驟7.2.提供radius伺服器的必要資訊。按一下OK按鈕。

名稱:演示_ise

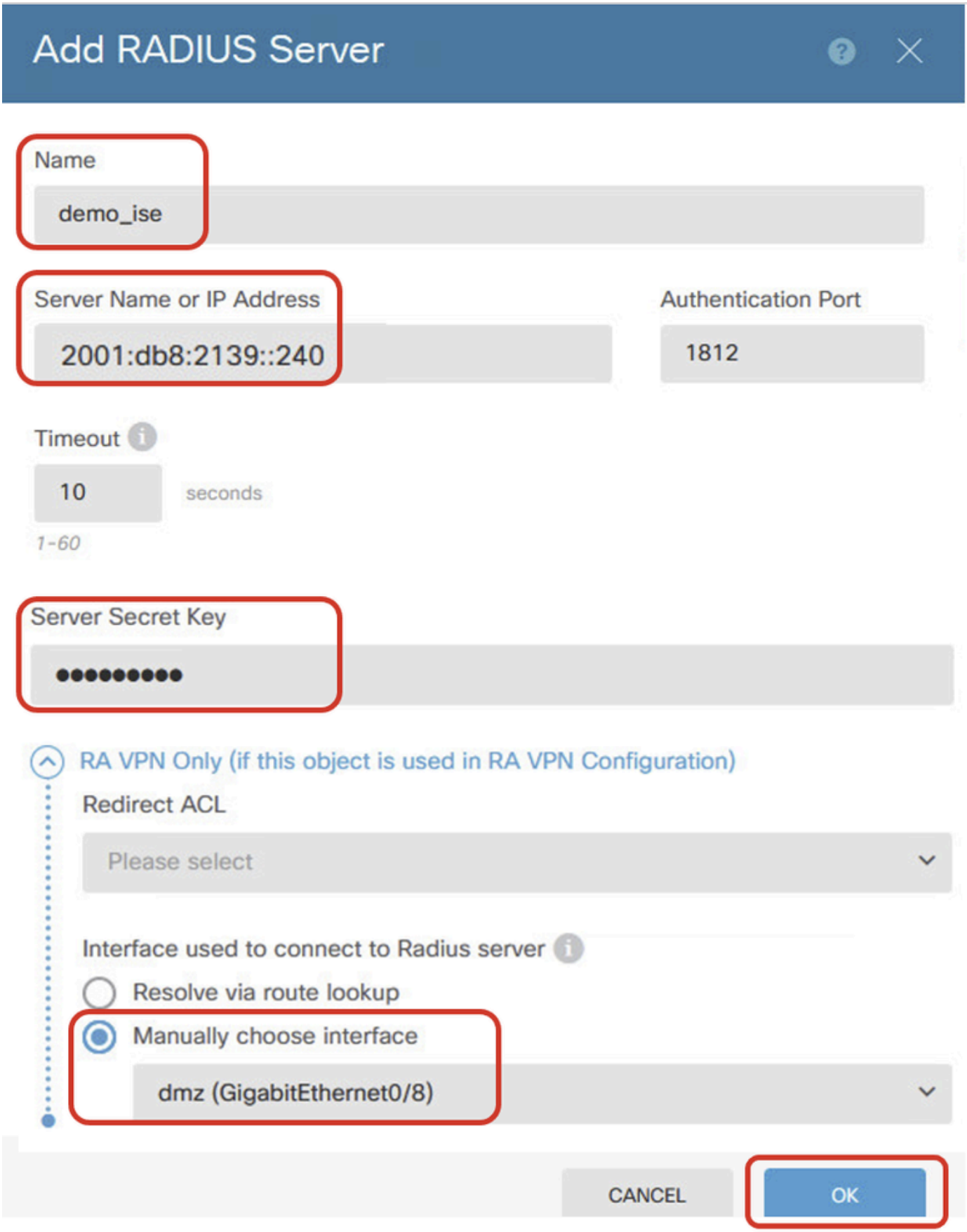
伺服器名稱或IP地址：2001:db8:2139::240

驗證連線埠：1812（預設）

逾時:10（預設）

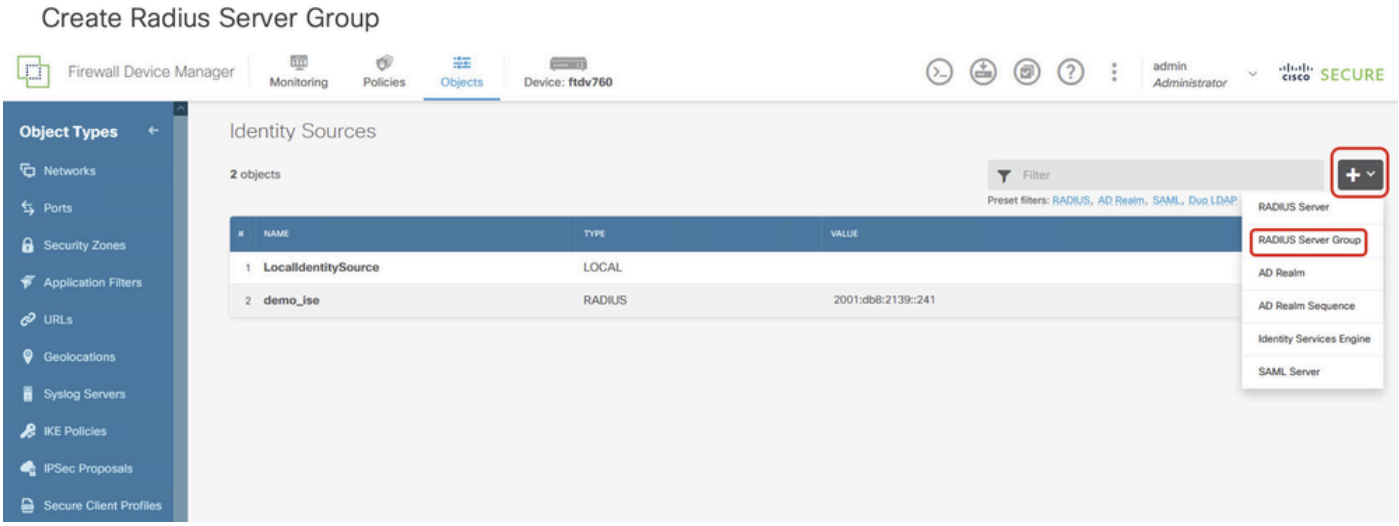
伺服器金鑰：cisco

用於連線到Radius伺服器的介面：手動選擇介面。在本例中，選擇dmz(GigabitEthernet0/8)。



Create_Radius_Source_2

步驟7.3.導航至Objects > Identity Sources。按一下+按鈕並選擇RADIUS Server Group。



Create_Radius_Source_3

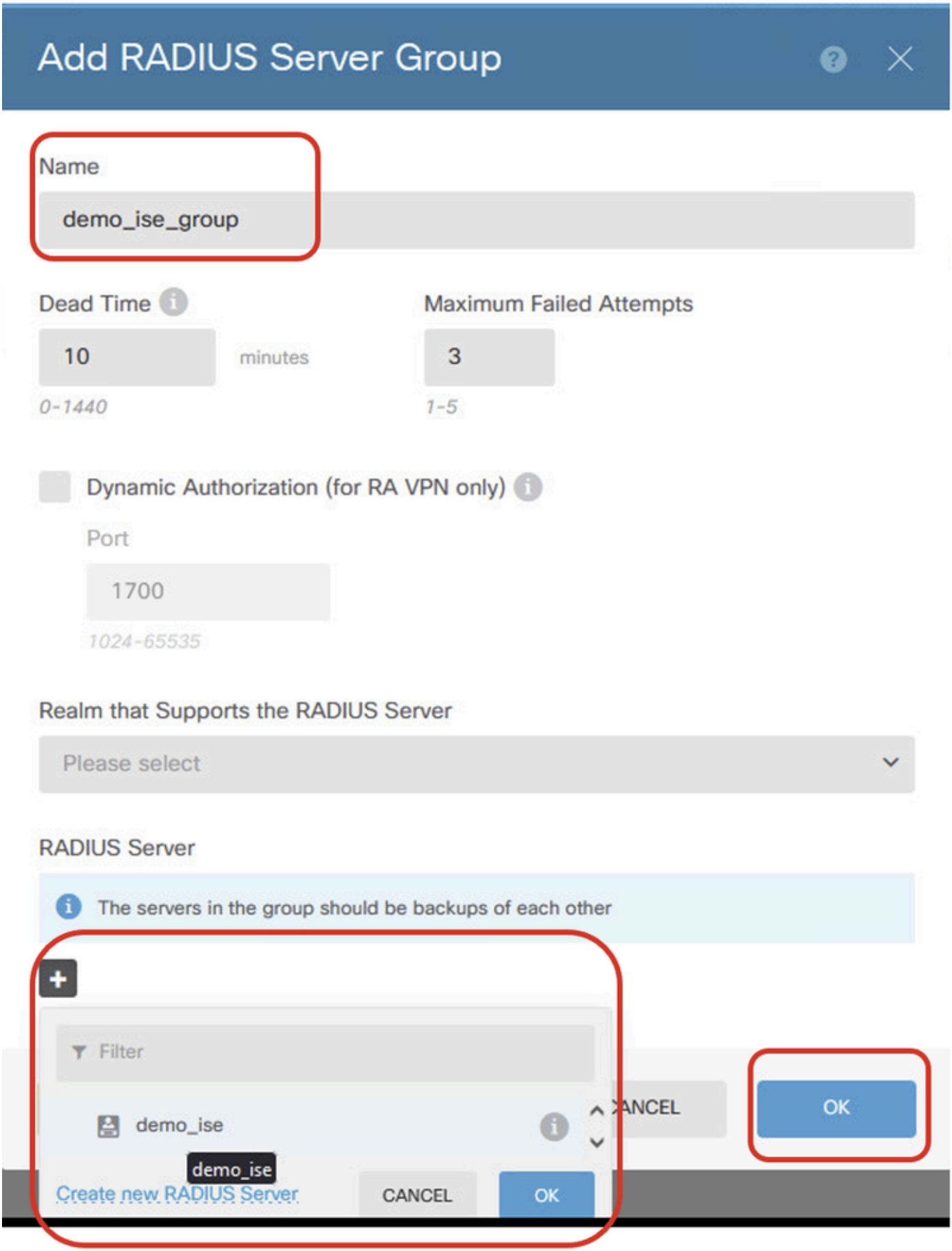
步驟7.4.提供radius伺服器群組的必要資訊。按一下OK按鈕。

名稱:demo_ise_group

停頓時間：10（預設）

最大失敗嘗試次數：3（預設）

RADIUS伺服器：按一下+按鈕，選擇在步驟6.2中建立的名稱。在本例中為demo_ise。



Create_Radius_Source_4

步驟8.建立用於RAVPN的組策略。在此示例中，為演示目的配置了自定義橫幅和超時設定。您可以根據實際需求進行修改。

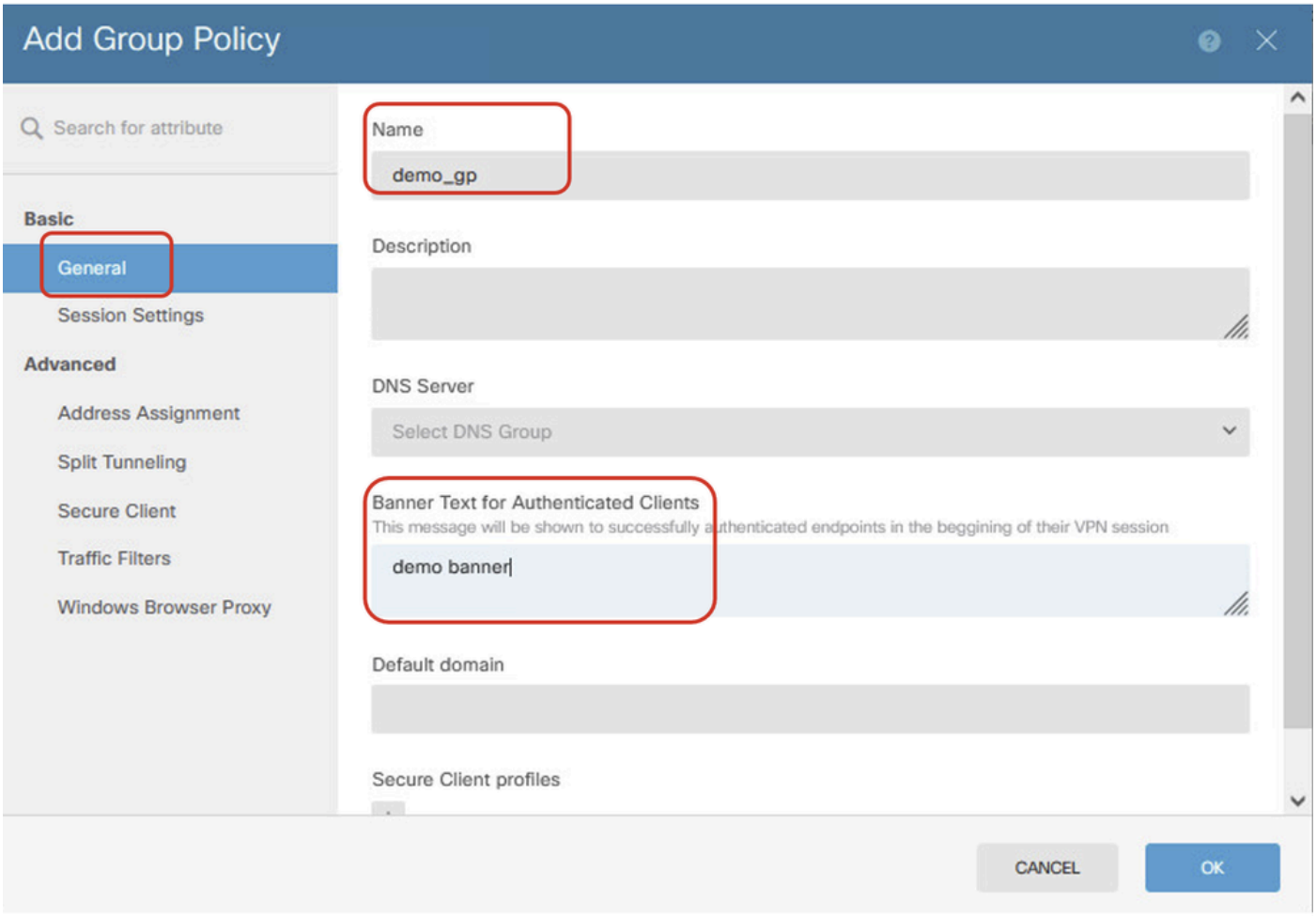
步驟8.1.導覽至Remote Access VPN > View Configuration。按一下左側欄中的Group Policies，然後按一下+按鈕。

建立_組_策略_1

步驟8.2. ClickGeneral 並提供必要資訊。

名稱:demo_gp

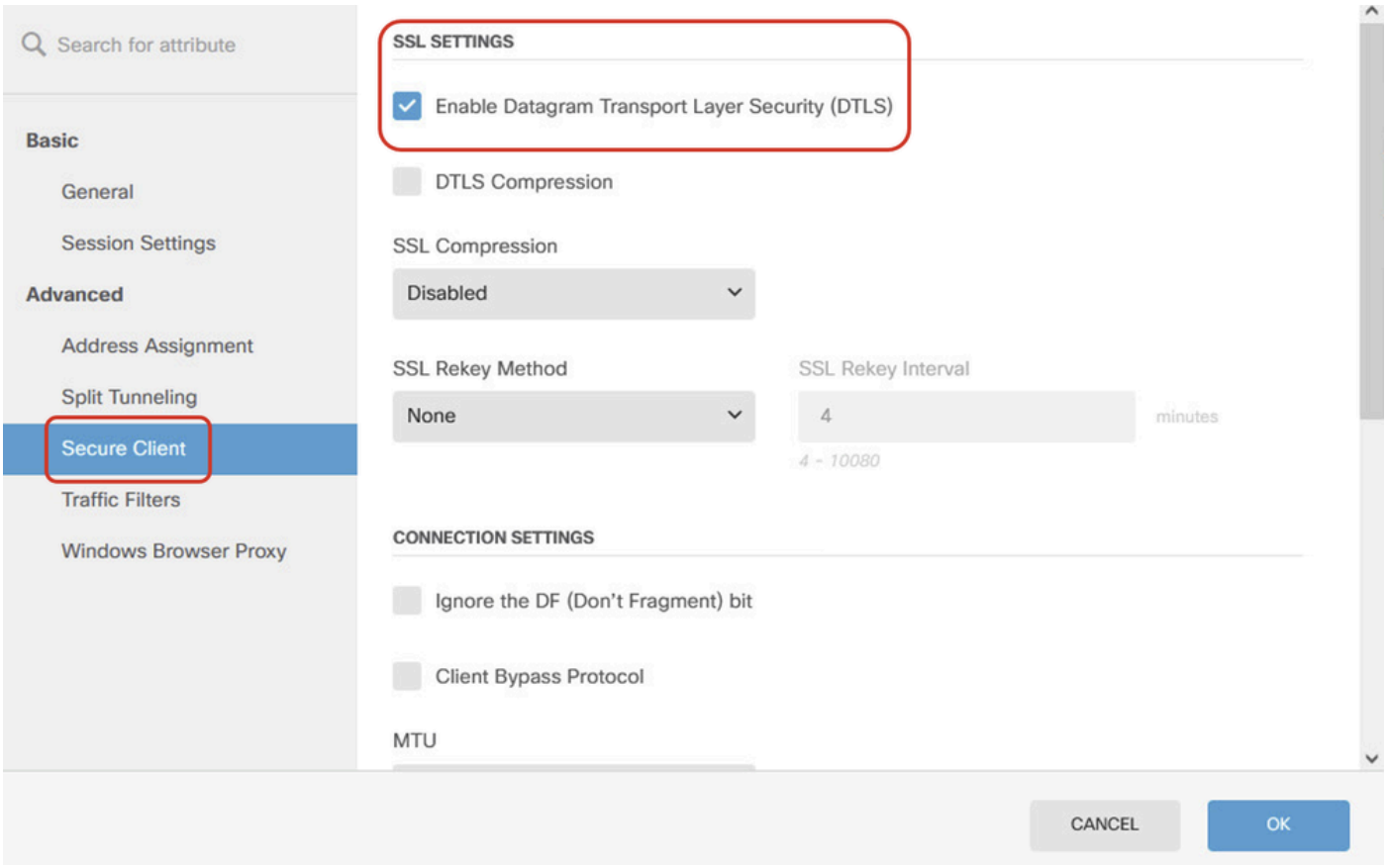
經過身份驗證的客戶端的橫幅文本：演示橫幅



Create_Group_Policy_2

步驟8.3.按一下Secure Client並提供必要資訊。

選中Enable Datagram Transport Layer Security(DTLS)。

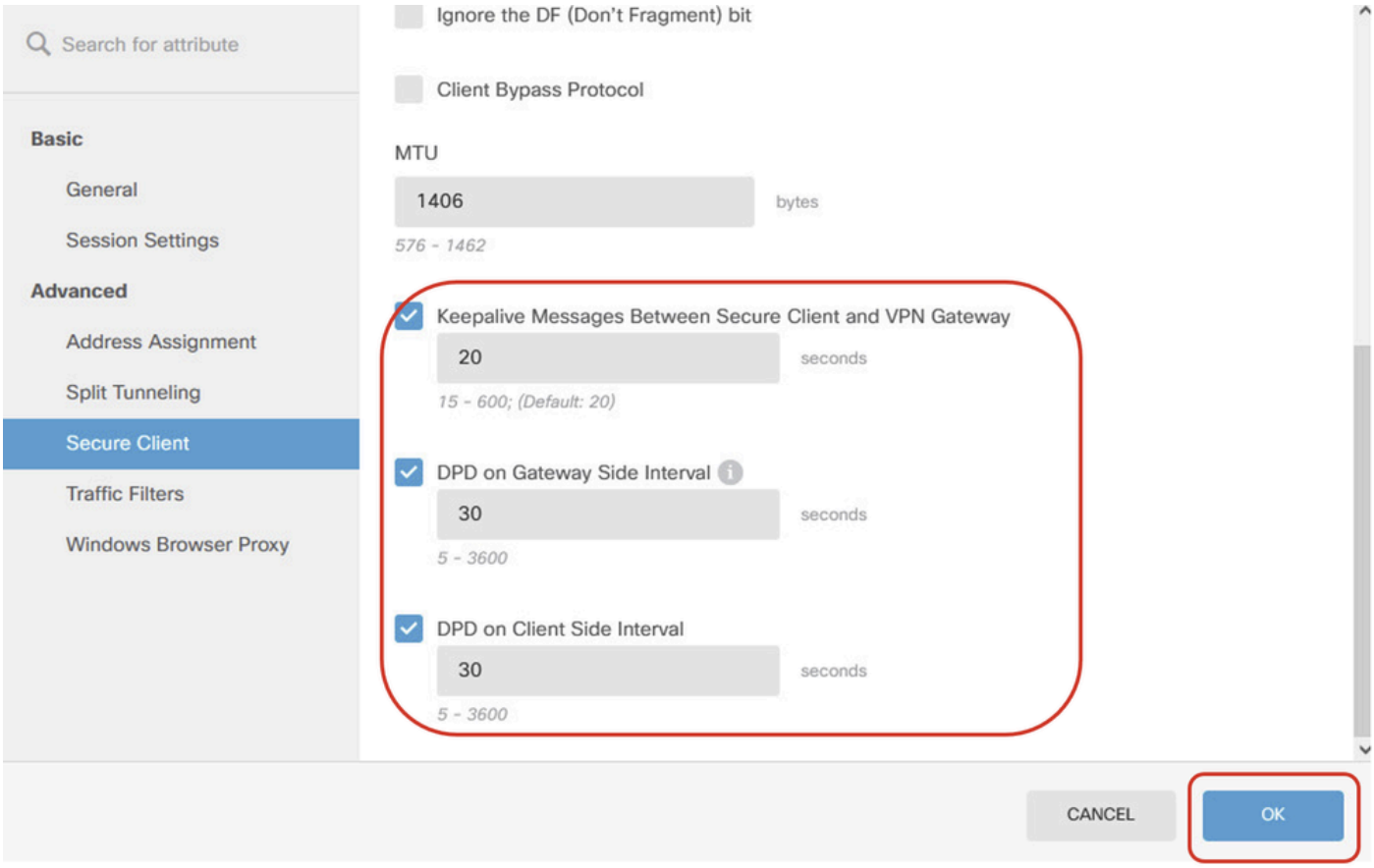


Create_Group_Policy_3

檢查安全客戶端和VPN網關之間的Keepalive消息（預設值）。

檢查網關端間隔上的DPD（預設值）。

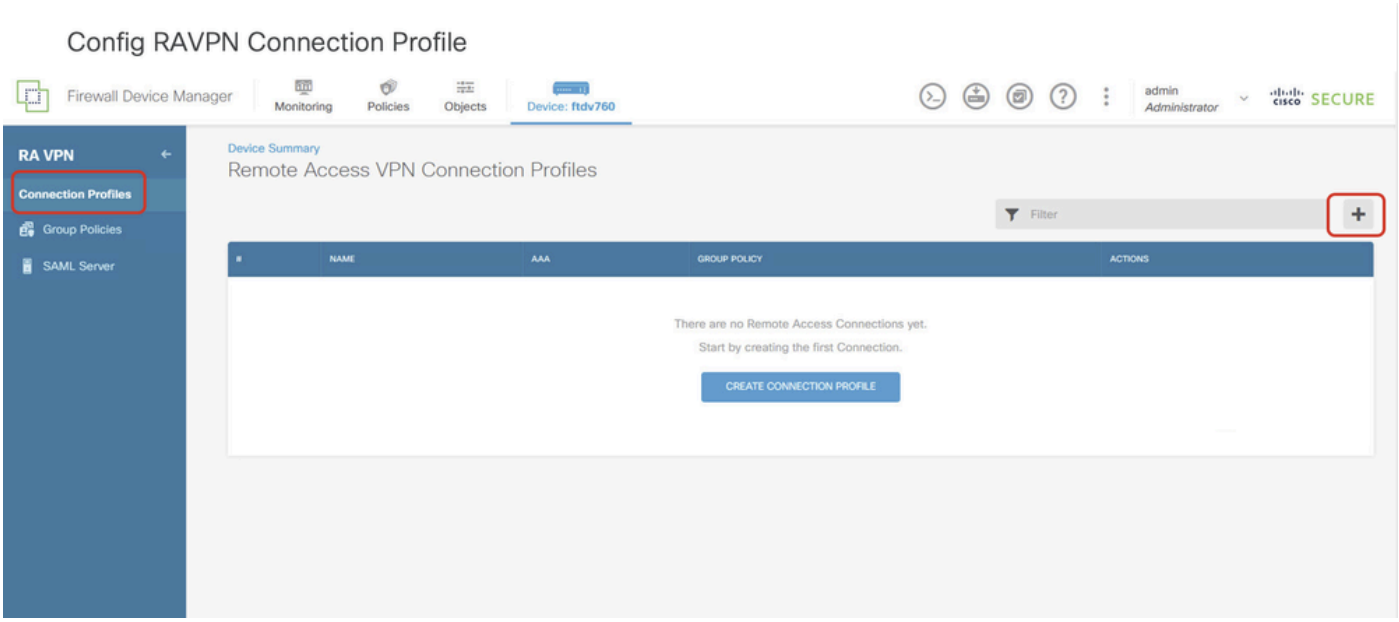
檢查客戶端間隔上的DPD（預設值）。



Create_Group_Policy_3_Cont

步驟9.建立RAVPN連線配置檔案。

步驟9.1.導航到Remote Access VPN > View Configuration。按一下左側欄中的Connection Profile，然後按一下+按鈕以啟動嚮導。

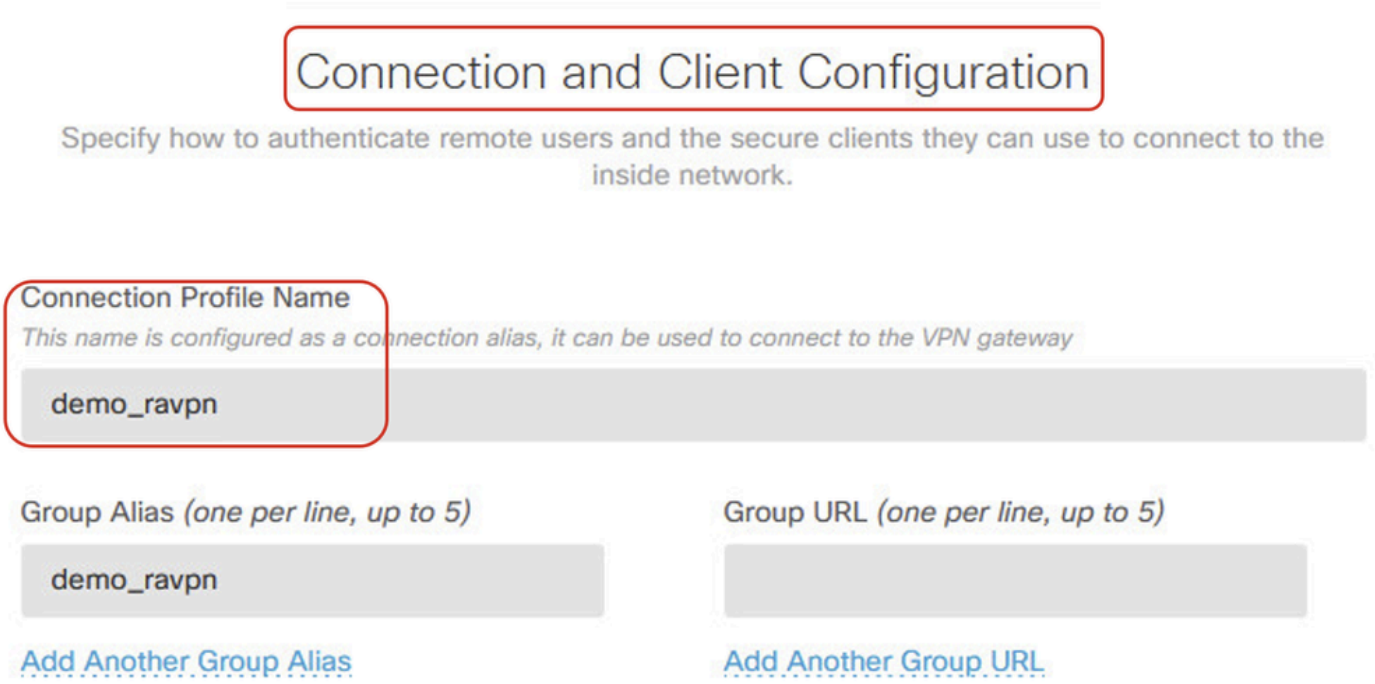


Create_RAVPN_Wizard_1

步驟9.2.在Connection and Client Configuration部分提供必要的資訊，然後按一下NEXT按鈕。

連線配置檔名稱：demo_ravpn

組別名：demo_ravpn



Create_RAVPN_Wizard_2_Conn_Name

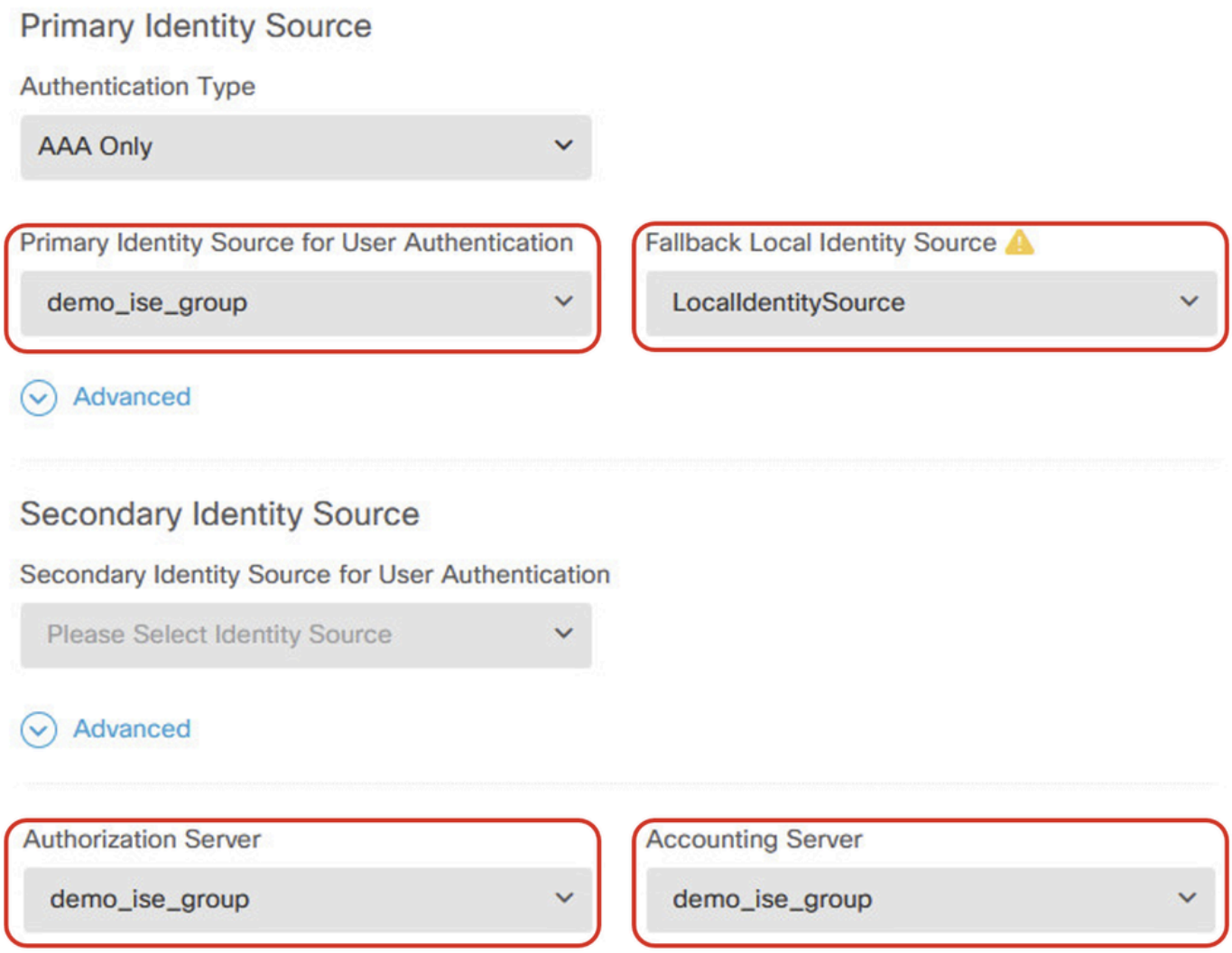
主身份源>身份驗證型別：僅限AAA

主身份源>主身份源：demo_ise_group（在步驟7.4中配置的名稱。）

回退本地身份源：LocalIdentitySource

授權伺服器：demo_ise_group（在步驟7.4中配置的名稱。）

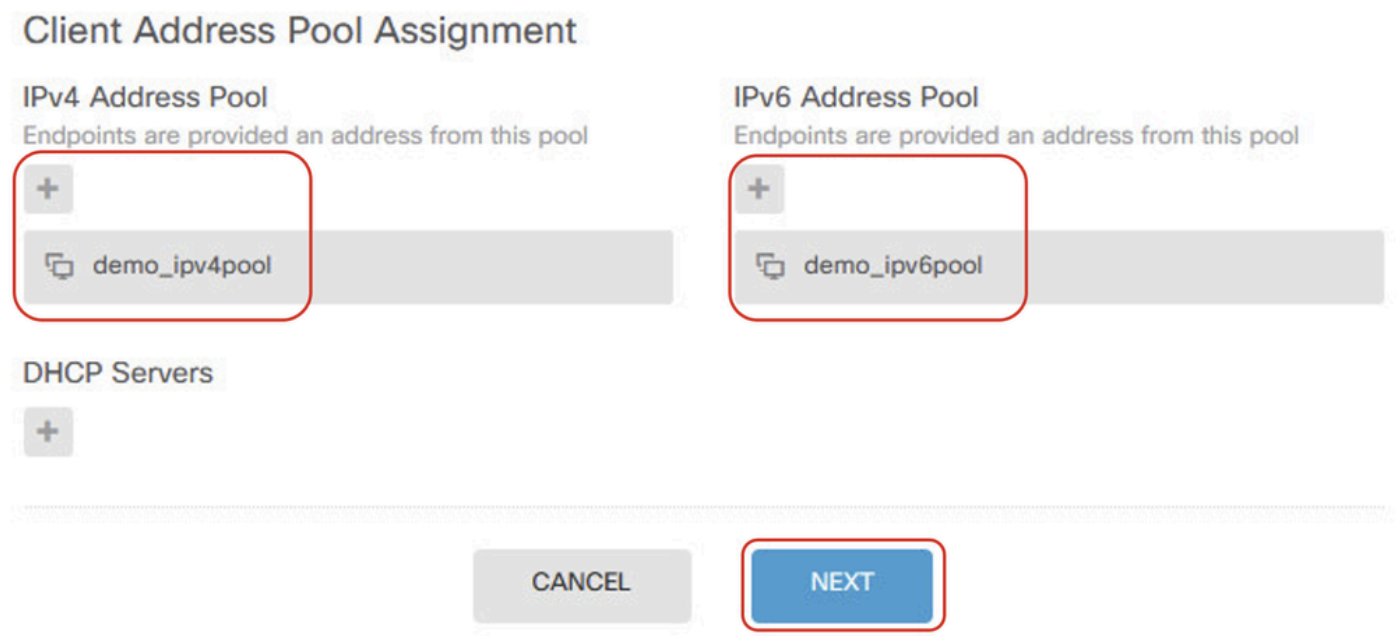
記帳伺服器：demo_ise_group（在步驟7.4中配置的名稱。）



Create_RAVPN_Wizard_2_Identity_Source

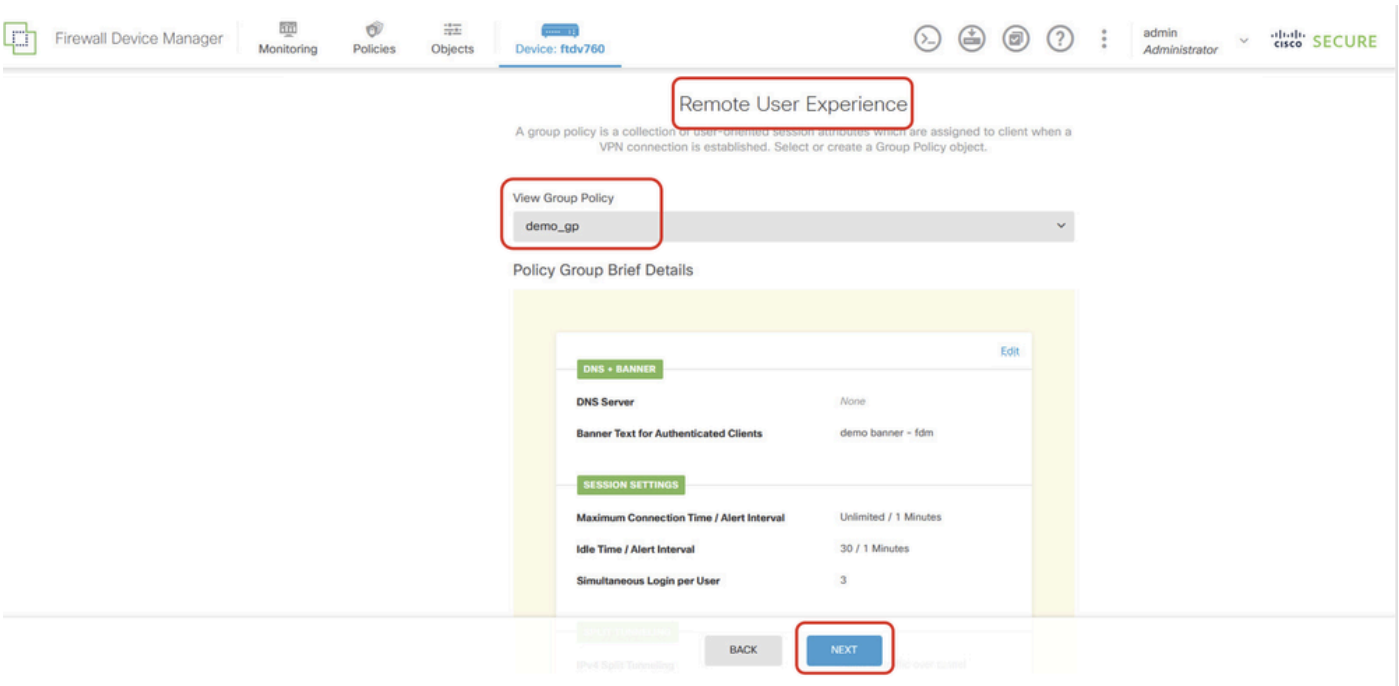
IPv4地址池：demo_ipv4pool（步驟4.2中配置的名稱。）

IPv6地址池：demo_ipv6pool（在步驟4.2中配置的名稱。）



Create_RAVPN_Wizard_2_Address_Pool

步驟9.3.在遠端使用者體驗部分選擇步驟8.2中配置的組策略，然後按一下NEXT按鈕。

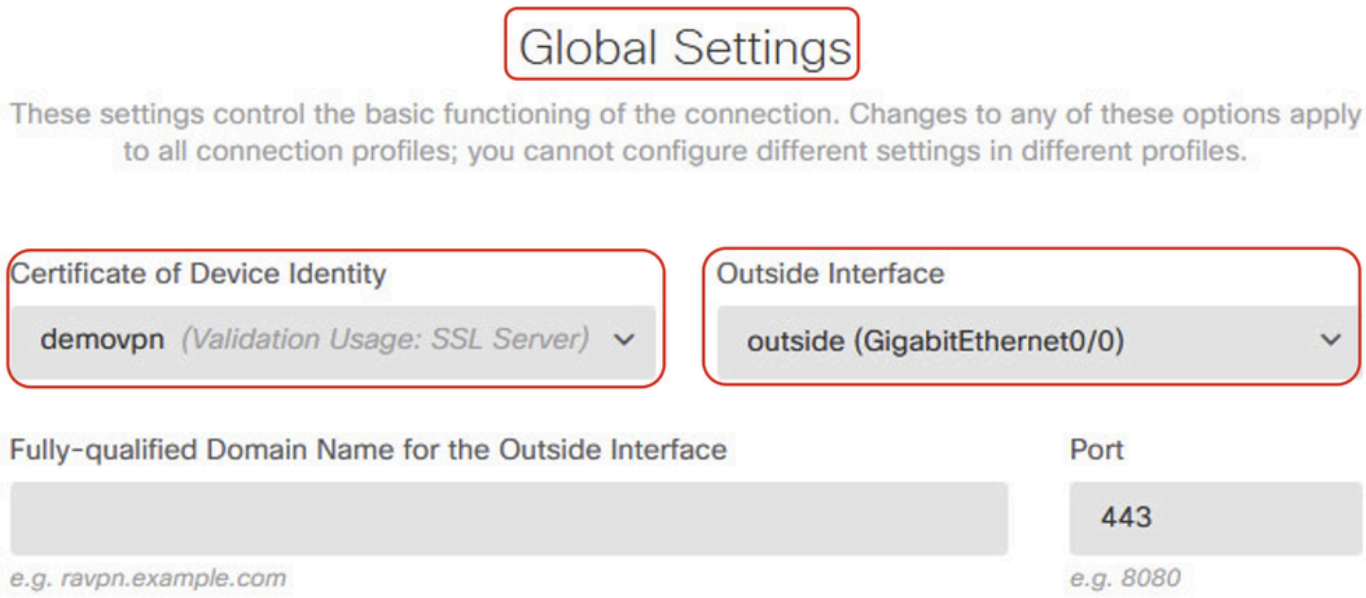


Create_RAVPN_Wizard_3

步驟9.4.在Global Setting(全域性設定)部分中提供必要的資訊，然後按一下NEXT(下一步)按鈕。

裝置標識證書：demovpn(步驟6.3中配置的名稱。)

Outside interface:outside



Create_RAVPN_Wizard_4

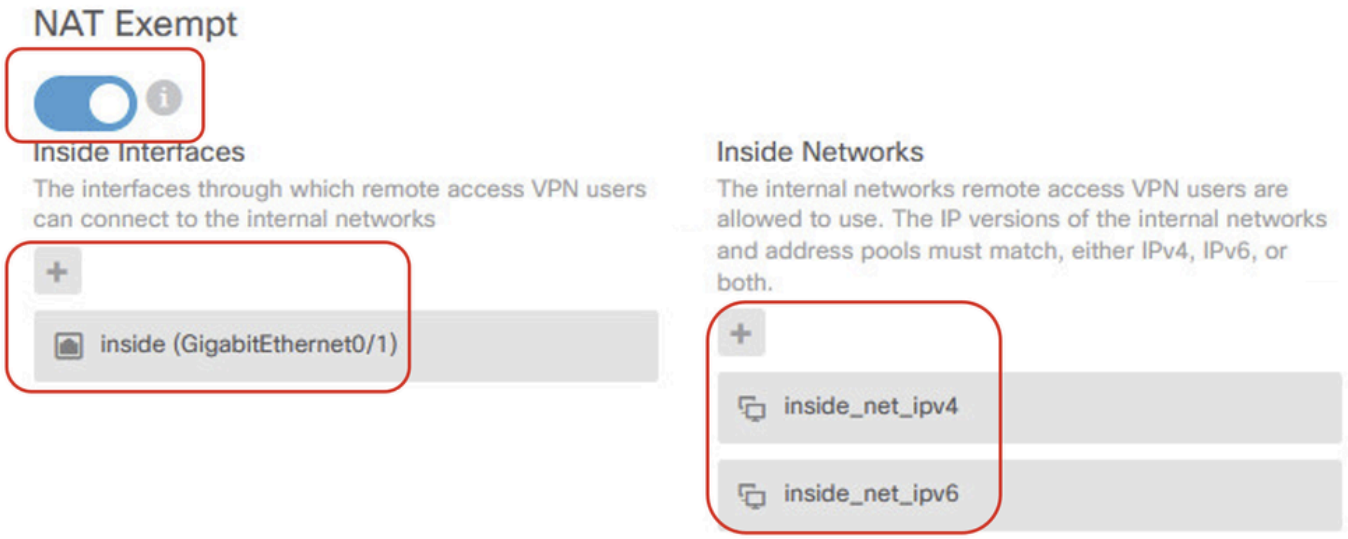
VPN流量的訪問控制：檢查Bypass Access Control policy for decrypted traffic(sysopt permit-vpn)。

Create_RAVPN_Wizard_4_VPN_ACP

NAT免除：按一下滑塊到「已啟用」位置

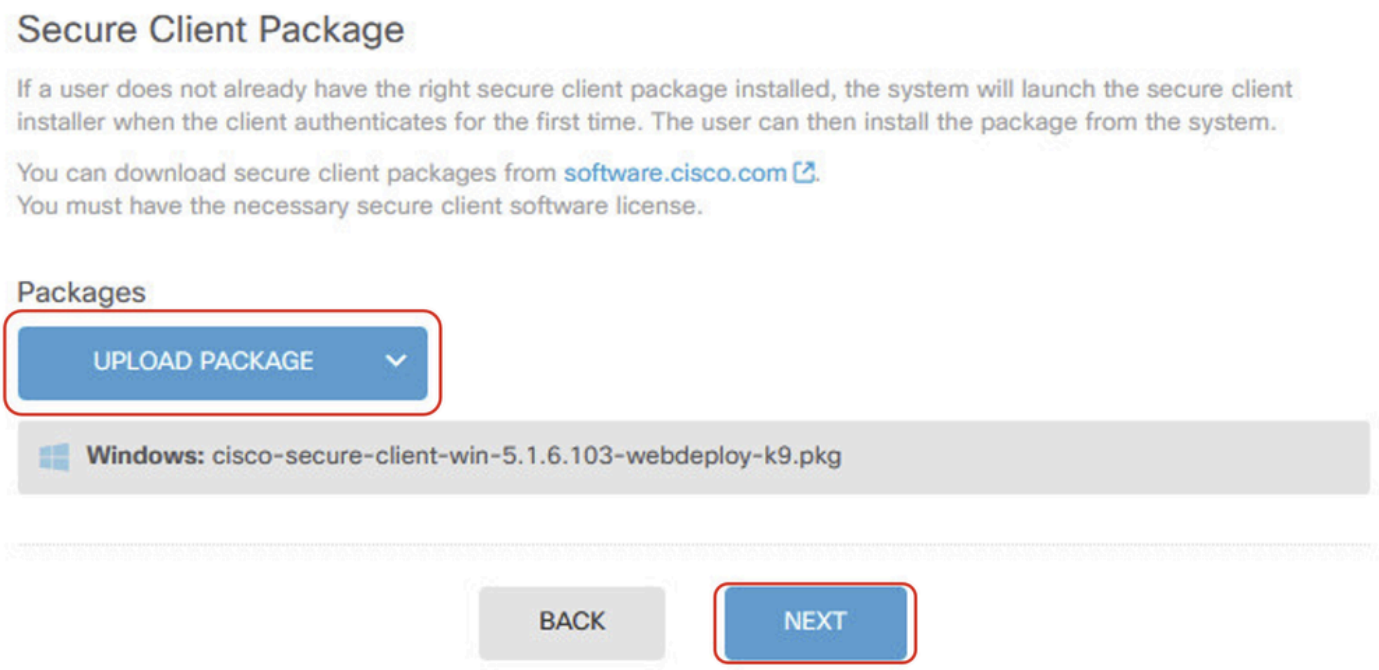
內部介面：inside

內部網路：inside_net_ipv4、inside_net_ipv6（在步驟5.2中配置的名稱。）



Create_RAVPN_Wizard_4_VPN_NATExempt

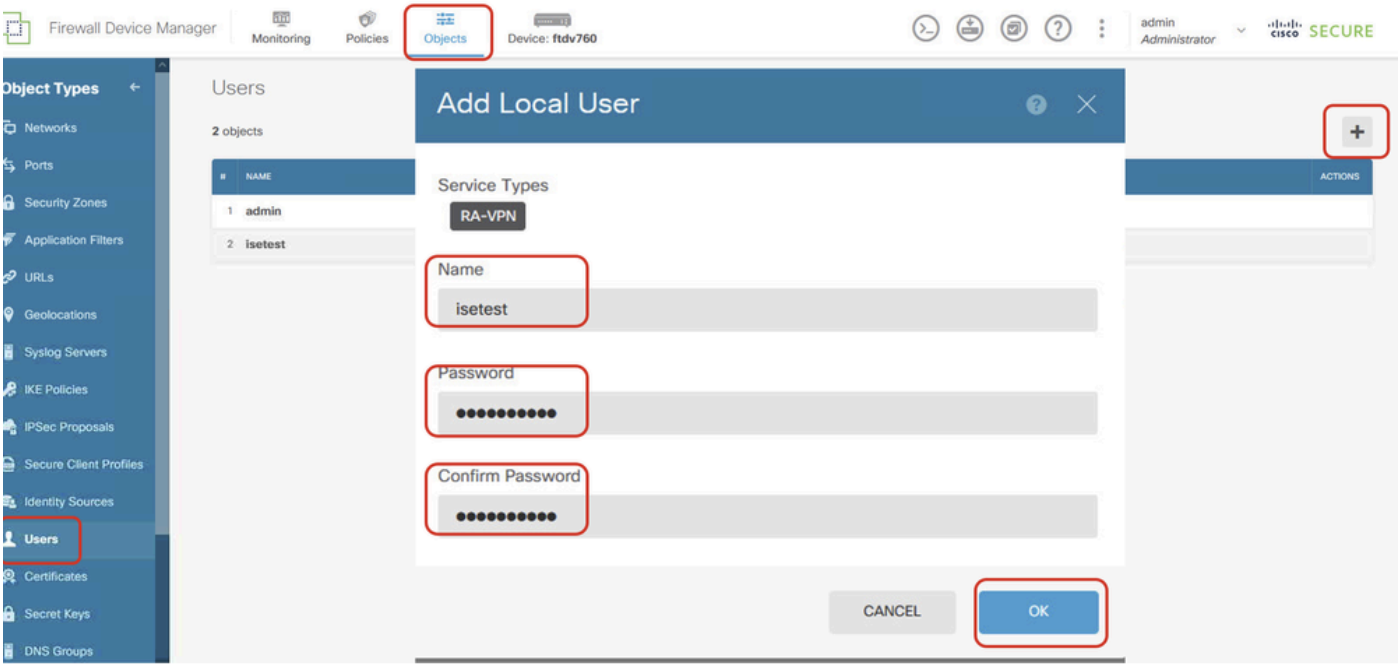
安全客戶端包：按一下「UPLOAD PACKAGE」，然後相應地上傳包。在此範例中，系統會上傳Windows程式包。



Create_RAVPN_Wizard_4_Image

步驟9.5.審查摘要。如果需要修改任何內容，請按一下BACK按鈕。如果一切正常，請按一下FINISH按鈕。

步驟10.如果步驟9.2中的Fallback Local Identity Source是使用LocalIdentitySource選擇的，則建立本地使用者。本地使用者的密碼需要與ISE上配置的密碼相同。



Create_Local_User

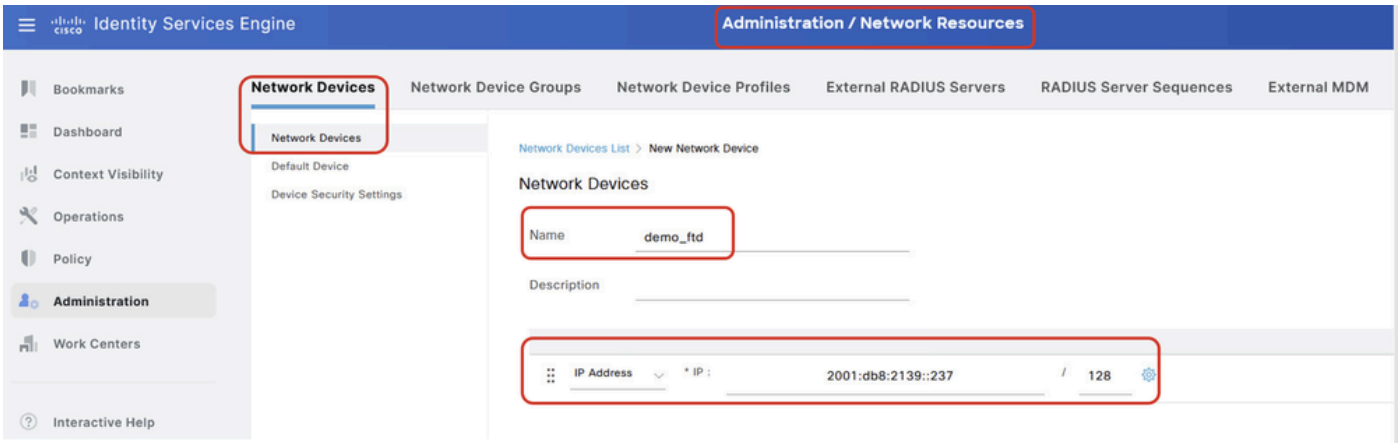
步驟11.部署配置更改。

部署_更改

ISE上的配置

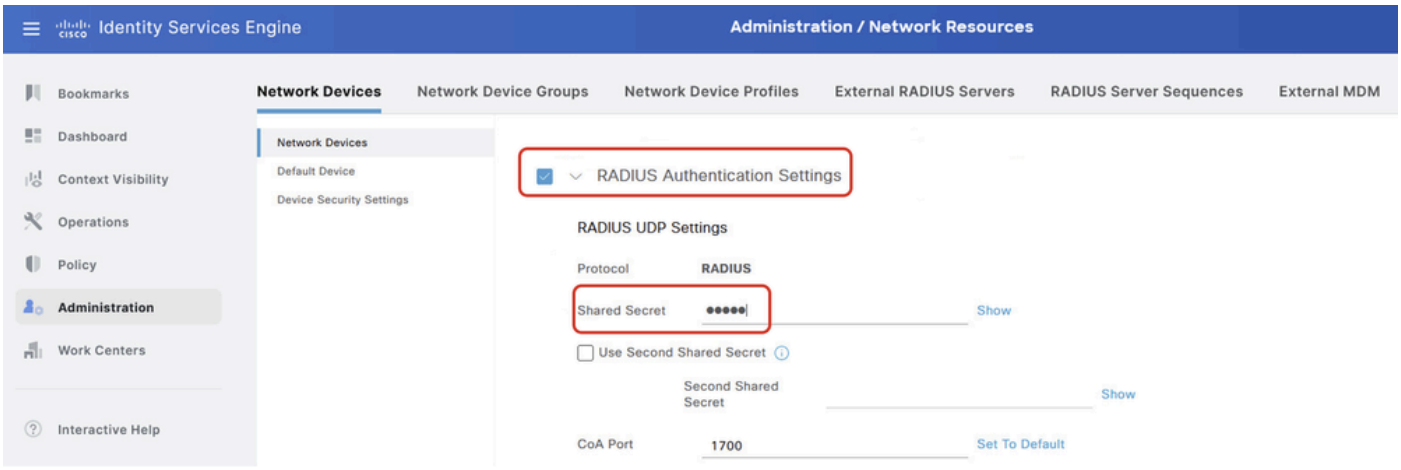
步驟12.建立網路裝置。

步驟12.1.導覽至Administration > Network Resources > Network Devices，按一下Add，提供Name， IP Address，然後向下滾動頁面。



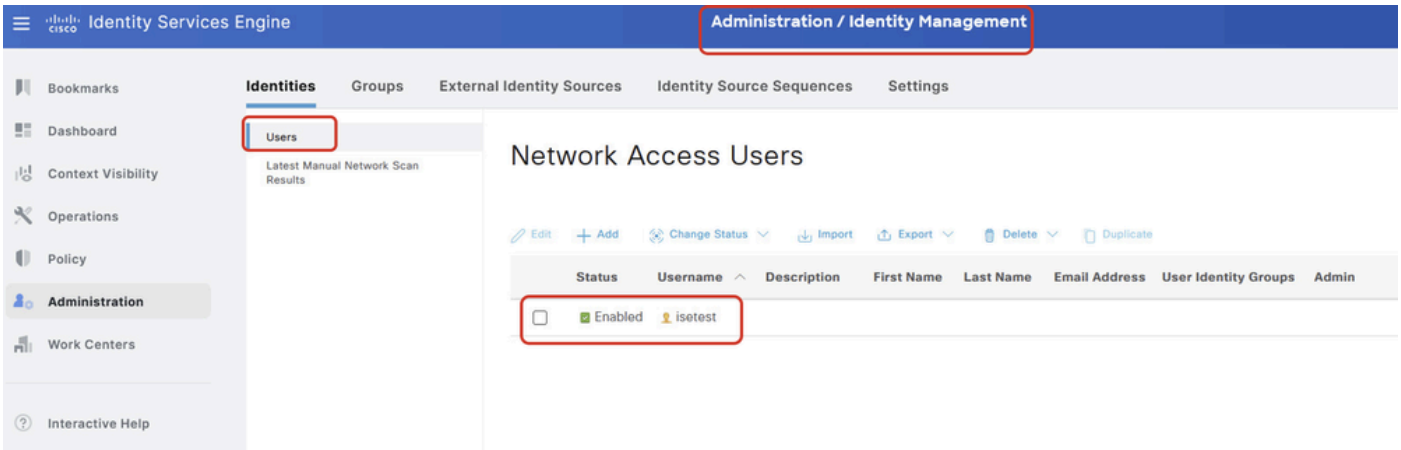
Create_Network_Devices

步驟12.2.選中RADIUS Authentication Settings覈取方塊。提供Shared Secret，然後按一下Submit。



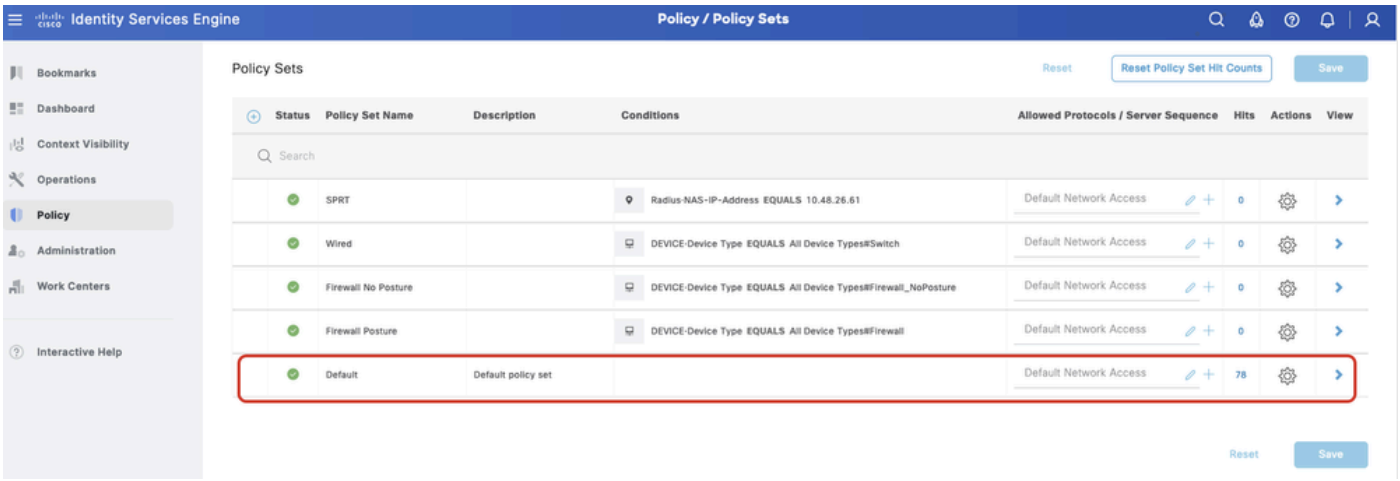
Create_Network_Devices_Cont

步驟13.建立網路訪問使用者。導航到管理>身份管理>身份。按一下「Add」以建立一個新使用者。密碼與在步驟10中建立的FDM本地使用者相同。以確保回退生效。



Create_ISE_User

步驟14.（可選）使用自定義身份驗證規則和授權規則建立新策略集。在本示例中，預設策略集用於演示目的。

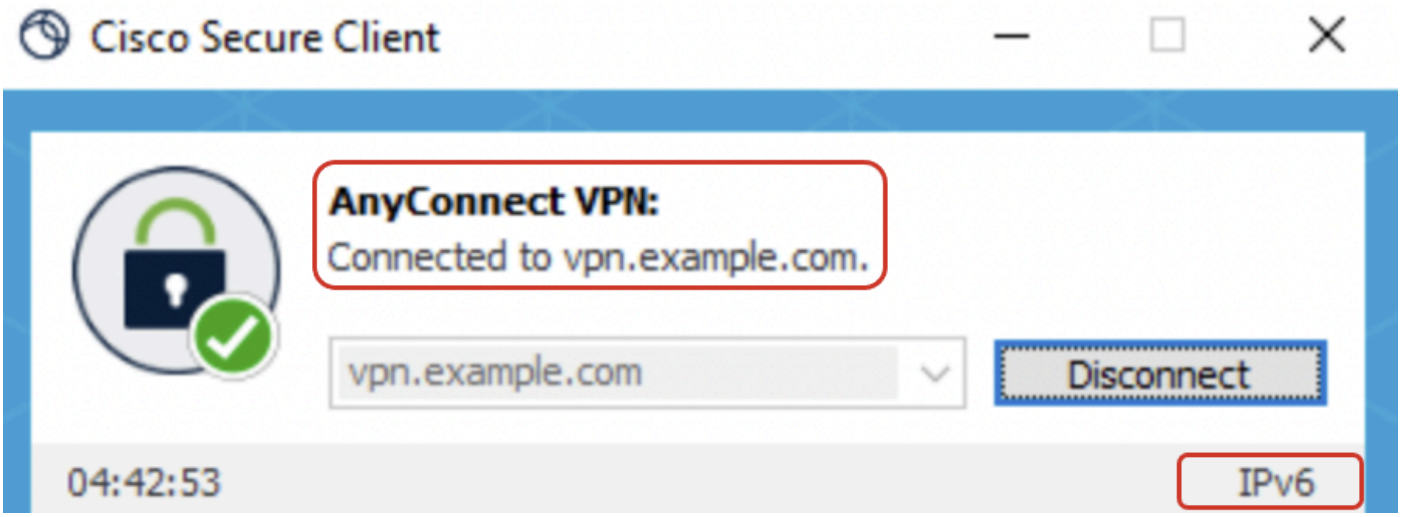


ISE_Default_Policyset

驗證

使用本節內容，確認您的組態是否正常運作。

步驟15.通過客戶端上的IPv6地址連線VPN網關。VPN連線成功。



Verify_Connection_Success

步驟16.透過SSH或主控台導覽至FTD的CLI。在FTD(Lina)CLI中執行命令show vpn-sessiondb detail anyconnect以檢查VPN作業階段詳細資訊。

```
<#root>

ftdv760# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : isetest

 Index : 2

Assigned IP : 10.37.254.17
```

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 15402 Bytes Rx : 14883
Pkts Tx : 10 Pkts Rx : 78
Pkts Tx Drop : 0 Pkts Rx Drop : 10
Group Policy : demo_gp Tunnel Group : demo_ravpn
Login Time : 05:22:30 UTC Mon Dec 23 2024
Duration : 0h:05m:05s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : c0a81e0a000020006768f396
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 : 2001:db8:10:0:a8a5:6647:b275:acc2

Encryption : none Hashing : none
TCP Src Port : 58339 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 24 Minutes
Client OS : win
Client OS Ver: 10.0.19042
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx : 7421 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 2.2

Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 58352
TCP Dst Port : 443 Auth Mode : userPassword

```
Idle Time Out: 30 Minutes Idle TO Left : 25 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx : 7421 Bytes Rx : 152
Pkts Tx : 1 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 2.3
```

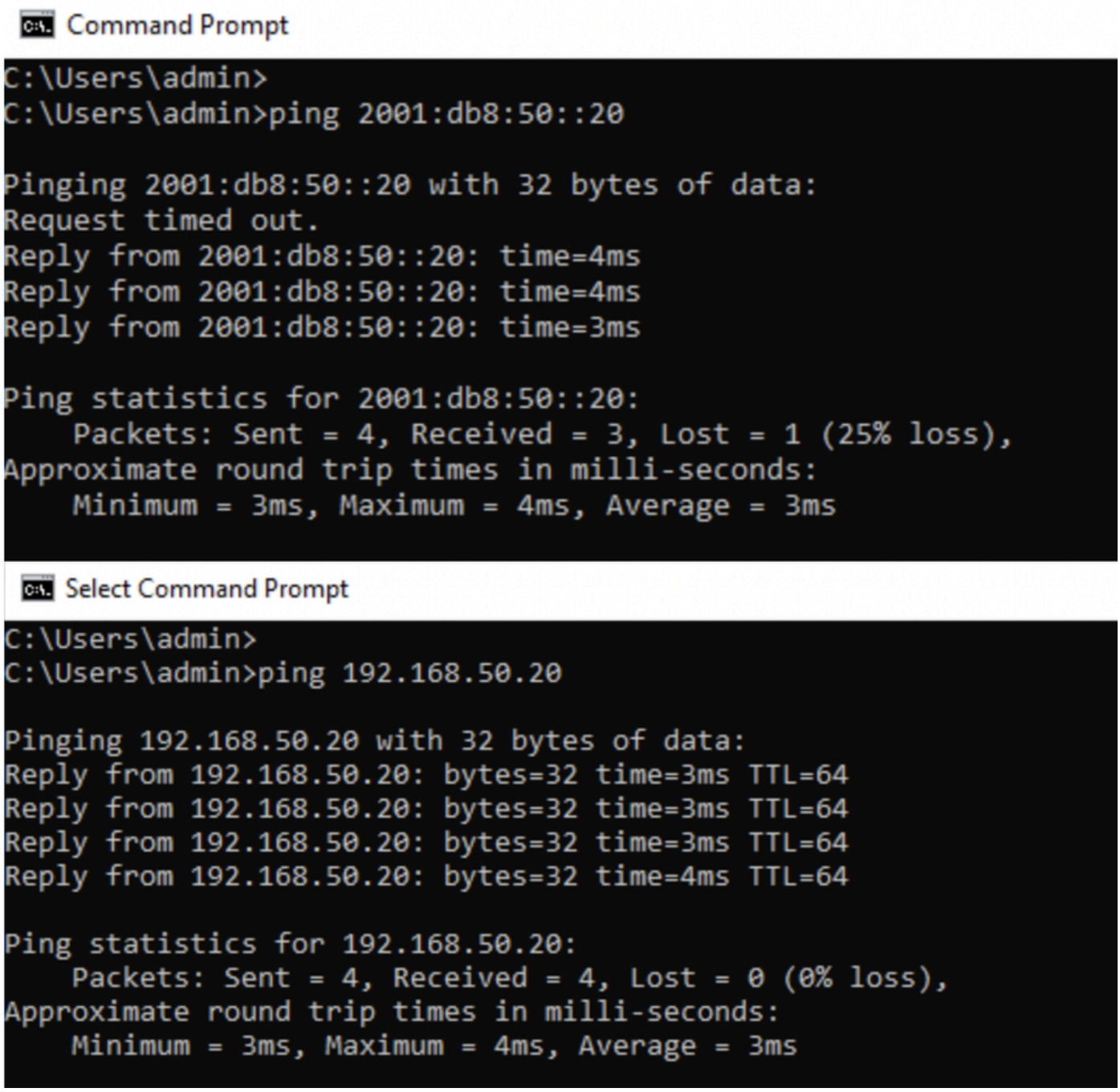
Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

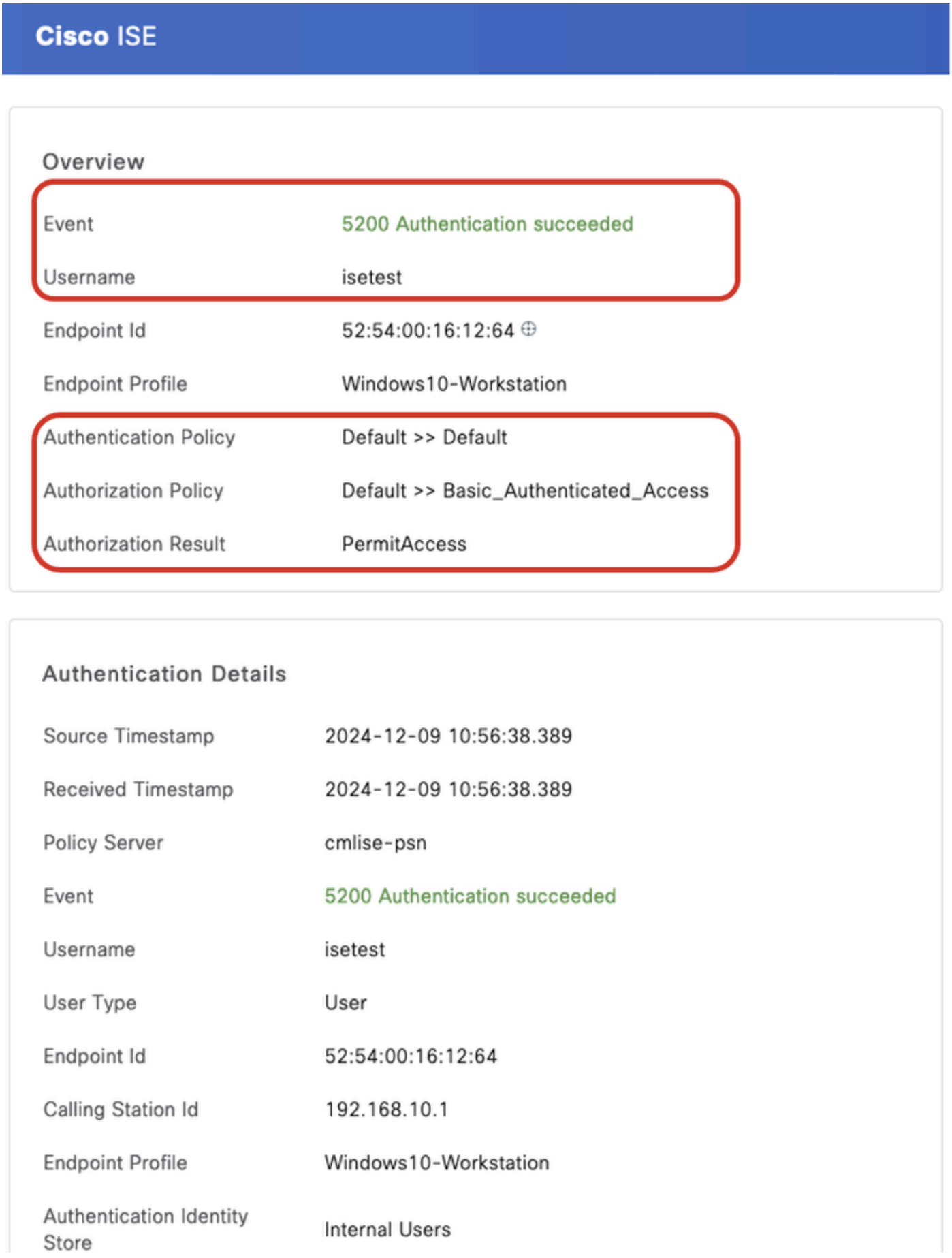
```
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 58191
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx : 560 Bytes Rx : 14731
Pkts Tx : 8 Pkts Rx : 76
Pkts Tx Drop : 0 Pkts Rx Drop : 10
```

步驟17.在客戶端上執行ping測試。在本例中，客戶端成功對伺服器的IPv4和IPv6地址執行ping操作。



Verify_Cisco_Secure_Client_Ping

步驟18. ISE radius即時日誌顯示身份驗證成功。



ISE_Authentication_Success_Log

步驟19.當FTD無法到達ISE時，測試FTD身份驗證轉為本地。

步驟19.1。當FTD驗證轉到ISE時，請在FTD(Lina)CLI中執行命令show aaa-server，以檢查統計資訊。

在本範例中，沒有LOCAL的計數器，且驗證被導向到RADIUS伺服器。

<#root>

```
ftdv760# show aaa-server

Server Group:    LOCAL
Server Protocol: Local database
Server Address:  None
Server port:     None
Server status:   ACTIVE, Last transaction at 08:18:11 UTC Fri Dec 6 2024
Number of pending requests              0
Average round trip time                 0ms
Number of authentication requests       0
Number of authorization requests        0
Number of accounting requests           0
Number of retransmissions               0
Number of accepts                       0
Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0
Server Group:    demo_ise_group
Server Protocol: radius


Server Address:  2001:db8:2139::240


Server port:     1812(authentication), 1646(accounting)
Server status:   ACTIVE, Last transaction at 02:56:41 UTC Mon Dec 9 2024
Number of pending requests              0
Average round trip time                 100ms

Number of authentication requests       1  <== Increased



Number of authorization requests        1  <== Increased



Number of accounting requests           1  <== Increased


Number of retransmissions               0

Number of accepts                       2  <== Increased


Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0
```

步驟19.2.關閉ISE介面以模擬FTD無法從ISE接收任何響應。

<#root>

ftdv760# ping 2001:db8:2139::240

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:2139::240, timeout is 2 seconds:
???
Success rate is 0 percent (0/3)
```

步驟19.3.客戶端發起VPN連線並輸入在步驟10中建立的相同使用者名稱密碼，VPN連線仍然成功。

在FTD(Lina)CLI中再次執行命令show aaa-server以檢查統計資訊，LOCAL的驗證、授權及接受計數器現在已增加。RADIUS伺服器的接受計數器沒有增加。

<#root>

```
ftdv760# show aaa-server
Server Group:    LOCAL
Server Protocol: Local database
Server Address:  None
Server port:     None
Server status:   ACTIVE, Last transaction at 03:36:26 UTC Mon Dec 9 2024
Number of pending requests              0
Average round trip time                 0ms
```

Number of authentication requests   1 <== Increased

Number of authorization requests   1 <== Increased

```
Number of accounting requests           0
Number of retransmissions               0
```

Number of accepts   2 <== Increased

```
Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      0
Number of unrecognized responses        0
Server Group:    demo_ise_group
Server Protocol: radius

Server Address:  2001:db8:2139::240
Server port:     1812(authentication), 1646(accounting)
Server status:   ACTIVE, Last transaction at 03:36:41 UTC Mon Dec 9 2024
Number of pending requests              0
Average round trip time                 100ms
Number of authentication requests       2
Number of authorization requests        1
```

```
Number of accounting requests           6
Number of retransmissions               0

Number of accepts                       2  <== Not increased


Number of rejects                       0
Number of challenges                    0
Number of bad authenticators            0
Number of timeouts                      6
Number of unrecognized responses        0
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

您可以在FTD Lina上執行這些命令，以對VPN一節進行疑難排解。

```
debug webvpn 255
debug webvpn anyconnect 255
```

您可以從客戶端收集DART檔案以進行VPN故障排除，以確定問題是否出在安全客戶端上。有關指南，請參閱相關的CCO文檔收集安全客戶端的DART捆綁包。

您可以在FTD Lina上運行這些命令，以對Radius一節進行疑難排解。

```
ftdv760# debug radius ?

all      All debug options
decode   Decode debug option
dynamic-authorization CoA listener debug option
session  Session debug option
user     User debug option
<cr>
```

```
ftdv760# debug aaa ?

accounting
authentication
authorization
common
condition
internal
shim
url-redirect
<cr>
```

您可以檢視這些資訊，以便在VPN連線成功後排除與流量相關的問題。

1. 在FTD Lina上擷取流量，以檢視Lina是否捨棄流量（請參閱此CCO檔案）；使用Firepower威脅防禦擷取和Packet Tracer - Cisco。
2. 檢查訪問控制策略，以確保如果禁用了解密流量的旁路訪問控制策略，則允許相關VPN流量通過。
3. 複查NAT免除以確保將VPN流量排除在NAT之外。

相關資訊

- RAVPN的FDM配置指南 — 思科
- 收集安全客戶端的DART捆綁包 — 思科
- 使用Firepower威脅防禦捕獲和Packet Tracer - Cisco
- 思科安全客戶端故障排除 — Cisco
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。