透過FDM為FTD上的安全使用者端設定AAA和憑證驗證

目錄

簡介

本檔案介紹在由FDM管理的FTD上，透過SSL設定Cisco Secure Client，並具有AAA和憑證驗證的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Firepower裝置管理員(FDM)虛擬
- 防火牆威脅防禦(FTD)虛擬
- VPN身份驗證流程

採用元件

- 思科Firepower裝置管理器虛擬7.2.8
- 思科防火牆威脅防禦虛擬7.2.8
- 思科安全客戶端5.1.4.74

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

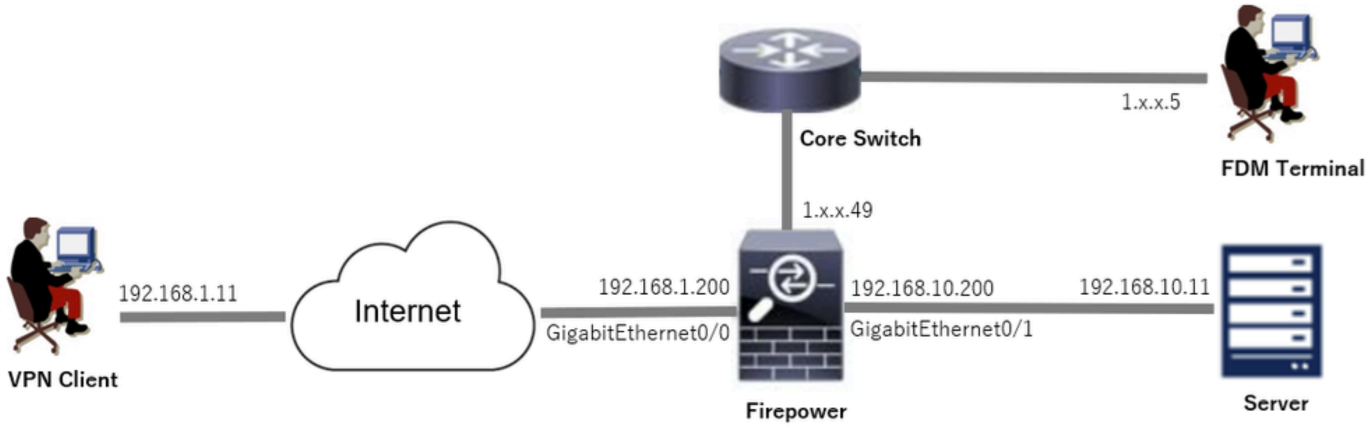
Firepower裝置管理器(FDM)是一個基於Web的簡化管理介面，用於管理Cisco Firepower威脅防禦(FTD)裝置。Firepower裝置管理器允許網路管理員配置和管理其FTD裝置，而無需使用更複雜的Firepower管理中心(FMC)。FDM為基本操作（如設定網路介面、安全區域、訪問控制策略和VPN）以及監控裝置效能和安全事件提供直觀的使用者介面。它適用於需要簡化管理的中小型部署。
本檔案介紹如何將預先填入的使用者名稱與FDM管理的FTD上的Cisco Secure Client整合。
如果您使用FMC管理FTD，請參閱透過FMC為FTD上的安全使用者端設定AAA和憑證驗證指南。

這是憑證鏈結，其中包含檔案中使用的每個憑證的一般名稱。

- CA： ftd-ra-ca-common-name
- 客戶端證書：sslVPNClientCN
- 伺服器證書：192.168.1.200

網路圖表

下圖顯示本文檔示例中使用的拓撲。



網路圖表

組態

FDM中的組態

步驟 1.設定FTD介面

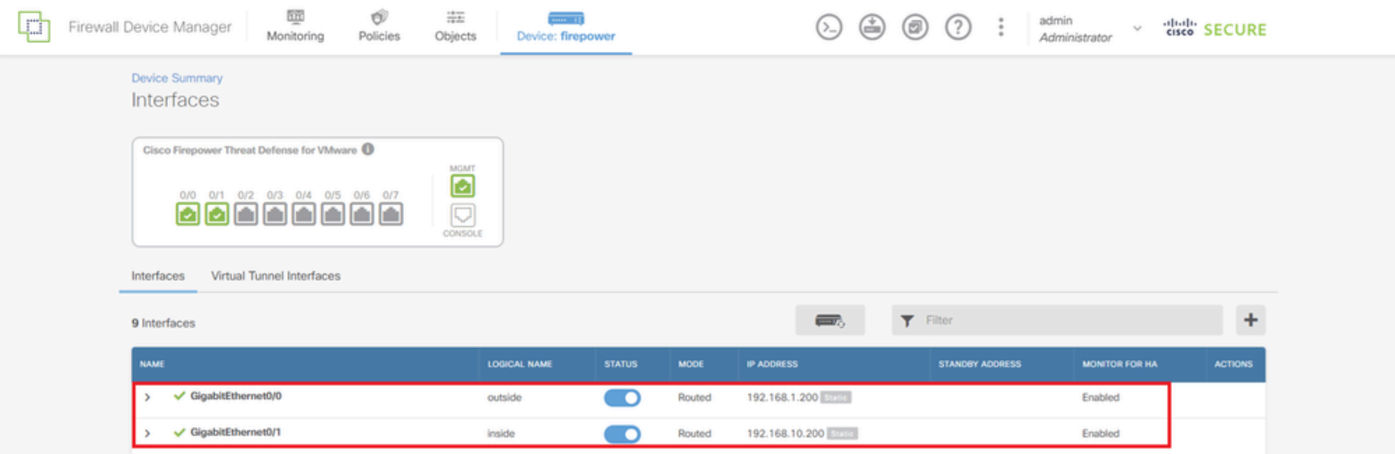
導覽至Device > Interfaces > View All Interfaces，設定FTD的內部與外部介面inInterfacestab。

對於GigabitEthernet0/0，

- 名稱：outside
- IP地址：192.168.1.200/24

對於GigabitEthernet0/1，

- 名稱：inside
- IP地址：192.168.10.200/24

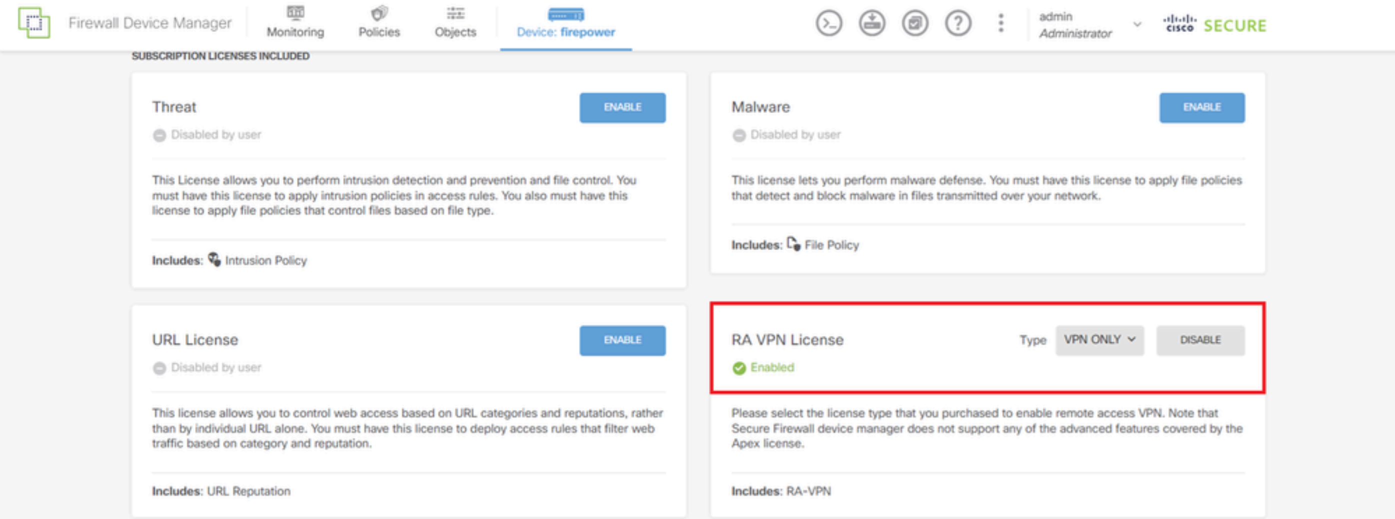


NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
GigabitEthernet0/0	outside		Routed	192.168.1.200 Static		Enabled	
GigabitEthernet0/1	inside		Routed	192.168.10.200 Static		Enabled	

FTD介面

步驟 2.確認思科安全客戶端許可證

導航到裝置>智慧許可證>檢視配置，在RA VPN許可證項中確認Cisco Secure Client許可證。



Threat — ENABLE

Disabled by user

This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.

Includes: Intrusion Policy

Malware — ENABLE

Disabled by user

This license lets you perform malware defense. You must have this license to apply file policies that detect and block malware in files transmitted over your network.

Includes: File Policy

URL License — ENABLE

Disabled by user

This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.

Includes: URL Reputation

RA VPN License — Type: VPN ONLY — DISABLE

Enabled

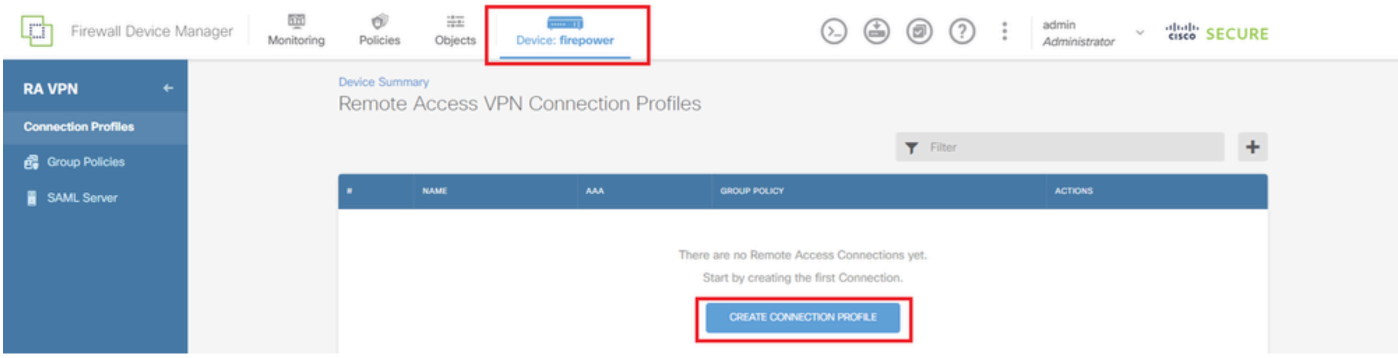
Please select the license type that you purchased to enable remote access VPN. Note that Secure Firewall device manager does not support any of the advanced features covered by the Apex license.

Includes: RA-VPN

安全使用者端授權

步驟 3.增加遠端訪問VPN連線配置檔案

導航到裝置>遠端接入VPN >檢視配置，點選建立連線配置檔案按鈕。



Remote Access VPN Connection Profiles

#	NAME	AAA	GROUP POLICY	ACTIONS

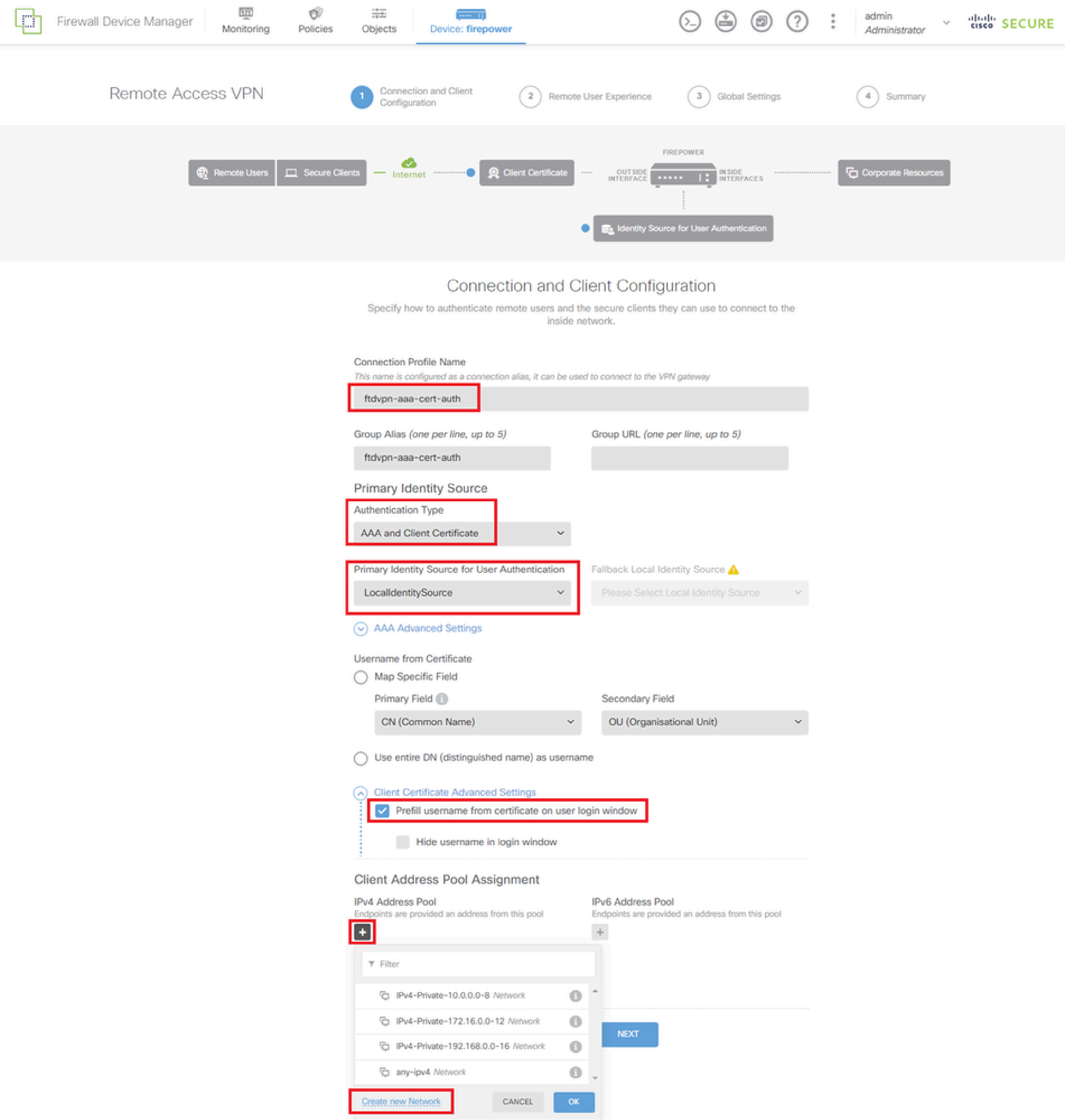
There are no Remote Access Connections yet.

Start by creating the first Connection.

增加遠端訪問VPN連線配置檔案

輸入連線配置檔案的必要資訊，然後按一下IPv4地址池專案中的Create new Network按鈕。

- 連線配置檔名稱：ftdvpn-aaa-cert-auth
- 身份驗證型別：AAA和客戶端證書
- 用於使用者身份驗證的主要身份源：LocalIdentitySource
- 使用者端憑證進階設定：在使用者登入視窗中，從憑證預先填入使用者名稱



Connection and Client Configuration

Specify how to authenticate remote users and the secure clients they can use to connect to the inside network.

Connection Profile Name
This name is configured as a connection alias, it can be used to connect to the VPN gateway
ftdvpn-aaa-cert-auth

Group Alias (*one per line, up to 5*): ftdvpn-aaa-cert-auth
Group URL (*one per line, up to 5*):

Primary Identity Source
Authentication Type: AAA and Client Certificate

Primary Identity Source for User Authentication: LocalIdentitySource
Fallback Local Identity Source: Please Select Local Identity Source

AAA Advanced Settings

Username from Certificate
○ Map Specific Field
Primary Field: CN (Common Name)
Secondary Field: OU (Organisational Unit)
○ Use entire DN (distinguished name) as username

Client Certificate Advanced Settings
☑ Prefill username from certificate on user login window
□ Hide username in login window

Client Address Pool Assignment
IPv4 Address Pool
Endpoints are provided an address from this pool
IPv6 Address Pool
Endpoints are provided an address from this pool

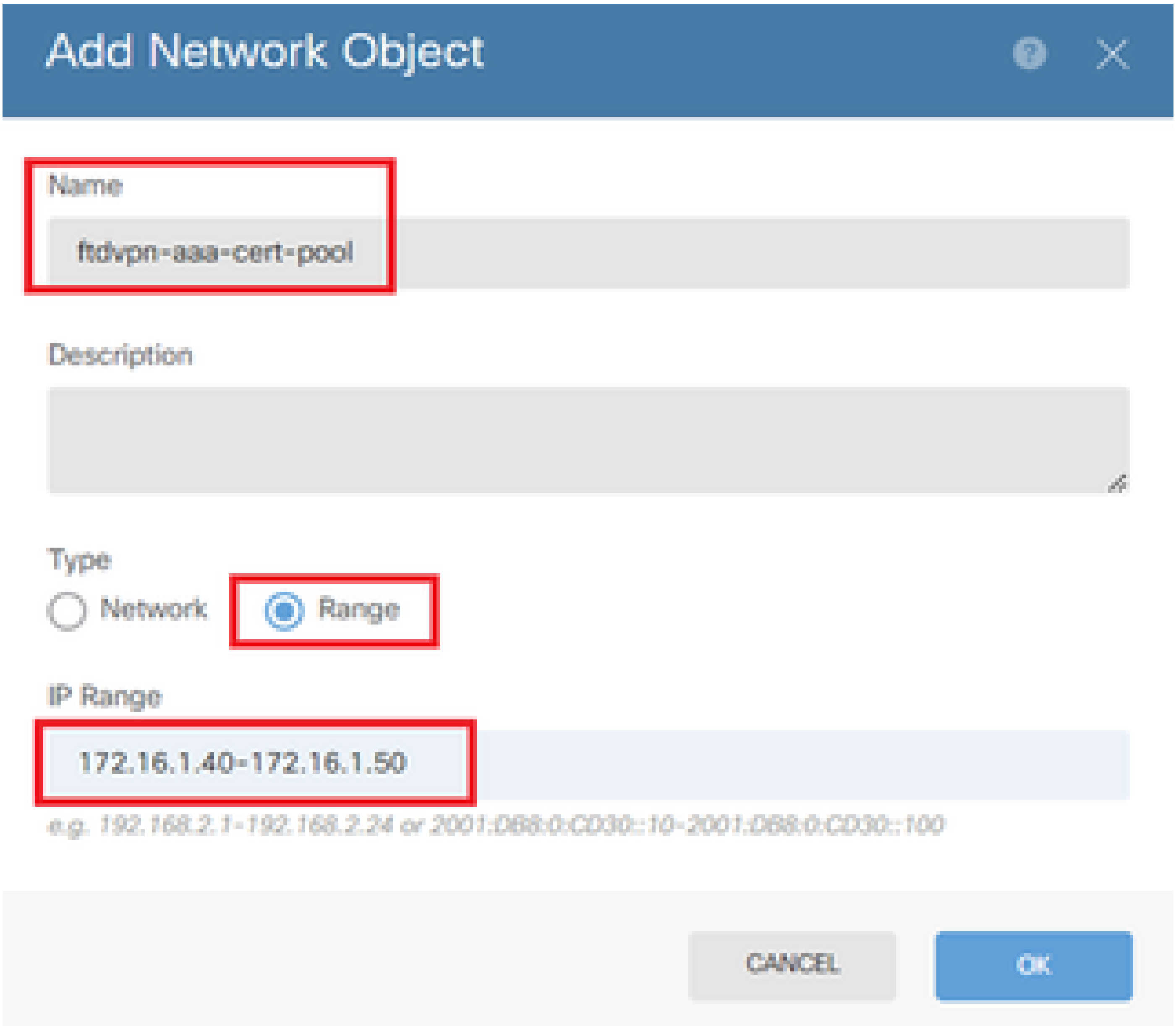
+
Filter
IPv4-Private-10.0.0.0-8 Network
IPv4-Private-172.16.0.0-12 Network
IPv4-Private-192.168.0.0-16 Network
any-ipv4 Network
Create new Network
CANCEL
OK
NEXT

VPN連線配置檔案的詳細資訊

步驟 4.為連線配置檔案增加地址池

輸入必要的資訊以新增新的IPv4位址集區。為連線配置檔案選擇新的已增加IPv4地址池，然後按一下Next按鈕。

- 名稱：ftdvpn-aaa-cert-pool
- 型別：範圍
- IP範圍：172.16.1.40-172.16.1.50



Name

ftdvpn-aaa-cert-pool

Description

Type

○ Network ● Range

IP Range

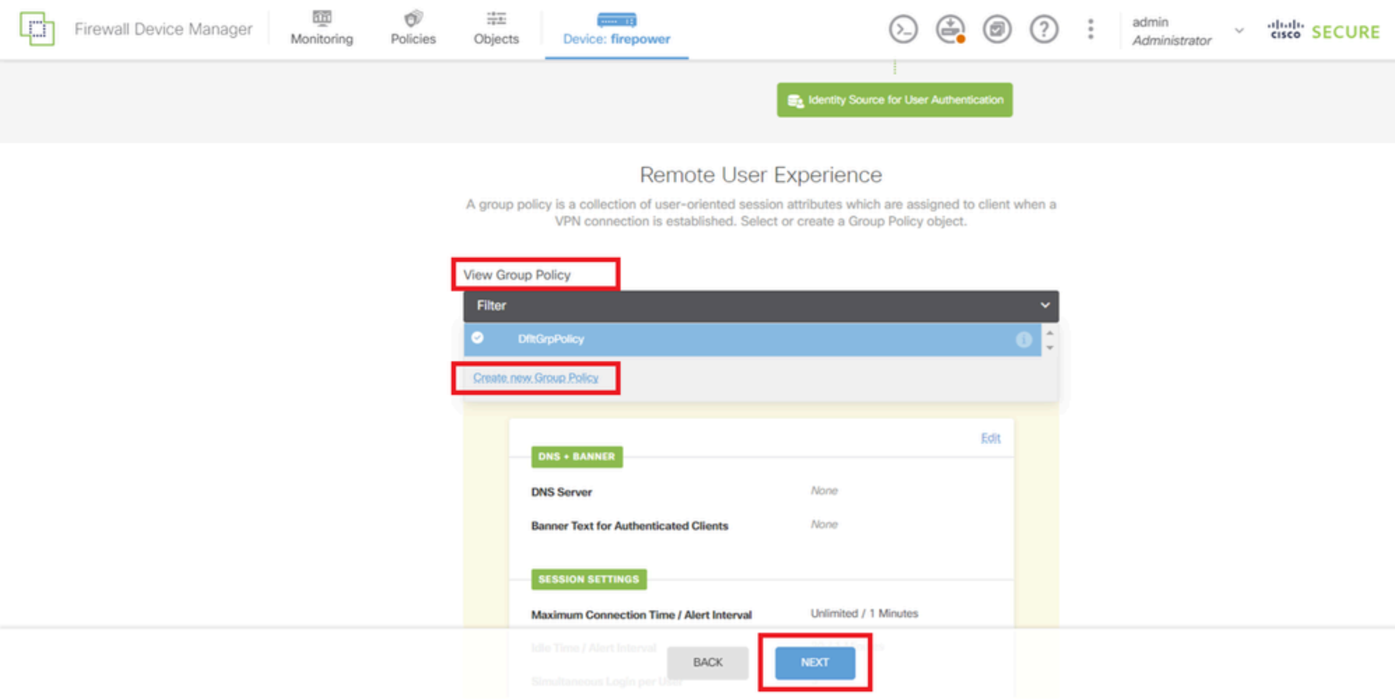
172.16.1.40-172.16.1.50

e.g. 192.168.2.1-192.168.2.24 or 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100

IPv4地址池的詳細資訊

步驟 5.新增連線設定檔的群組原則

在檢視組策略專案中按一下建立新組策略。



Remote User Experience

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

View Group Policy

DNS + BANNER

DNS Server	None
Banner Text for Authenticated Clients	None

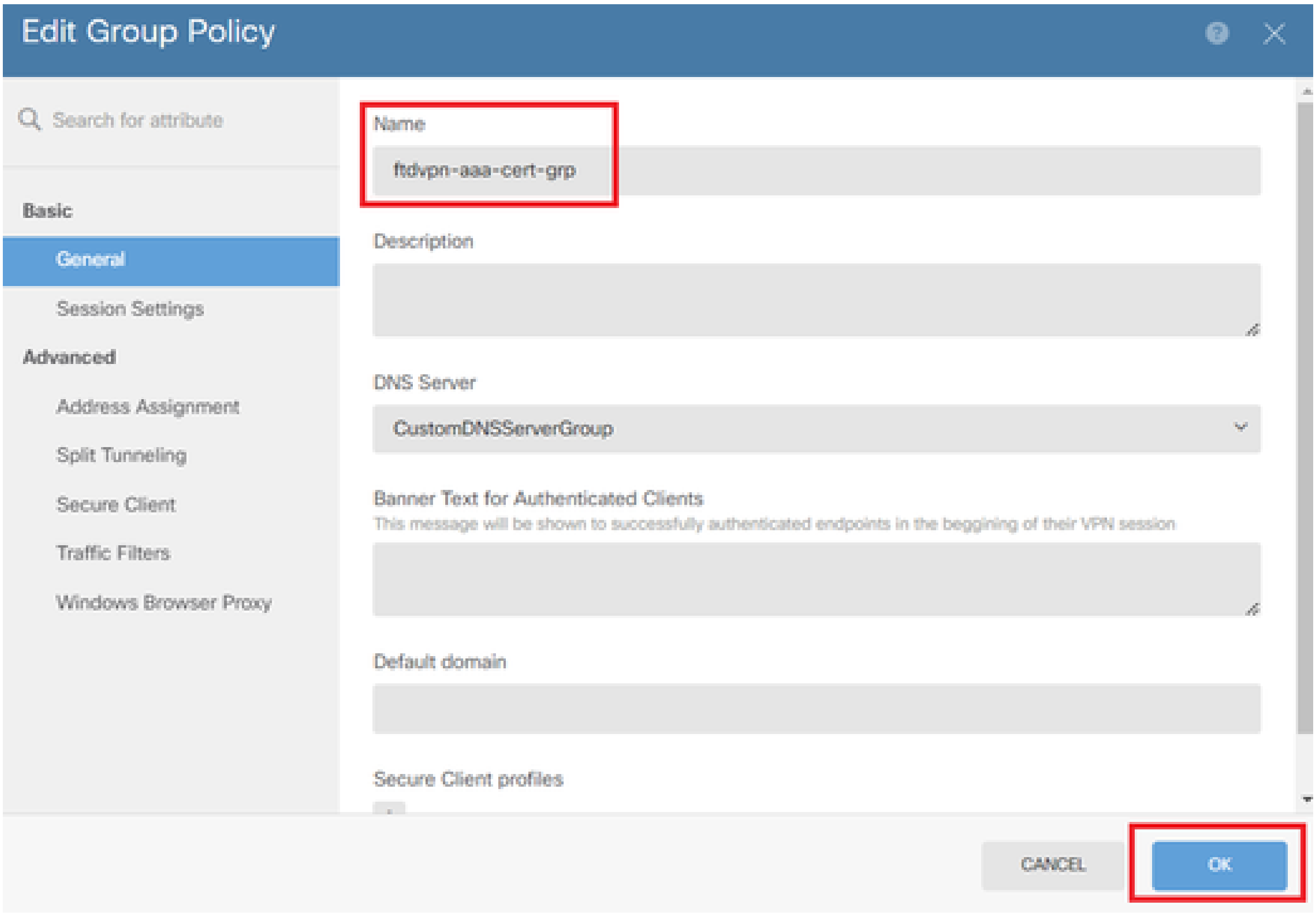
SESSION SETTINGS

Maximum Connection Time / Alert Interval	Unlimited / 1 Minutes

增加組策略

輸入必要資訊以增加新組策略，然後按一下OK按鈕。為連線配置檔案選擇新增加的組策略。

- 名稱：ftdvpn-aaa-cert-grp


Edit Group Policy

Name: ftdvpn-aaa-cert-grp

Description

DNS Server: CustomDNSServerGroup

Banner Text for Authenticated Clients
This message will be shown to successfully authenticated endpoints in the beggining of their VPN session

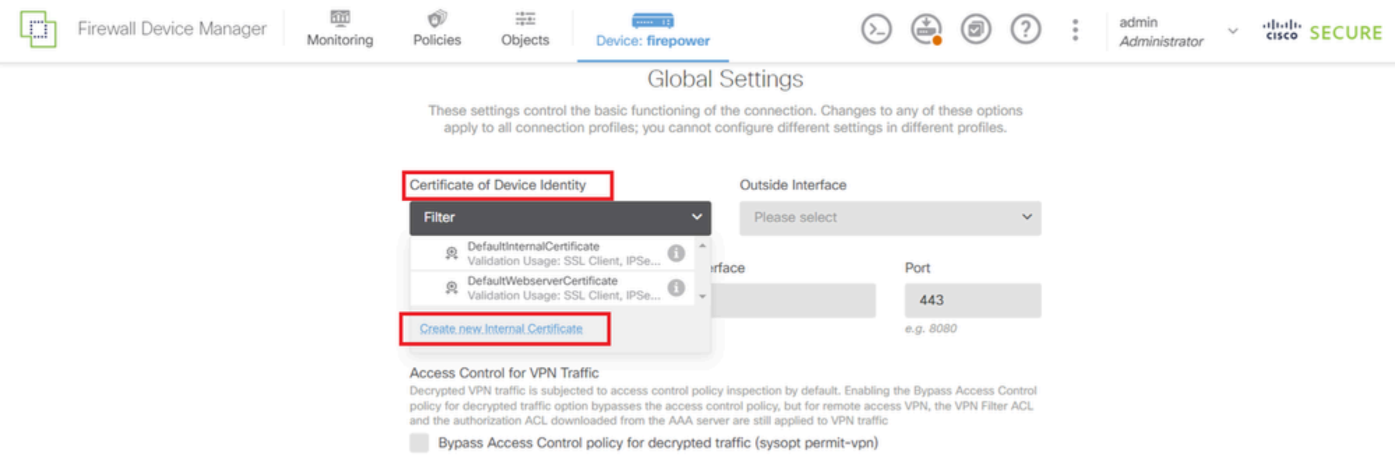
Default domain

Secure Client profiles

組策略的詳細資訊

步驟 6.為連線配置檔案配置裝置身份和外部介面的證書

按一下Certificate of Device Identity專案中的Create new Internal certificate。



Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

Certificate of Device Identity

Filter

DefaultInternalCertificate
Validation Usage: SSL Client, IPSe...

DefaultWebserverCertificate
Validation Usage: SSL Client, IPSe...

Create new Internal Certificate

Outside Interface

Please select

rface

Port

443

e.g. 8080

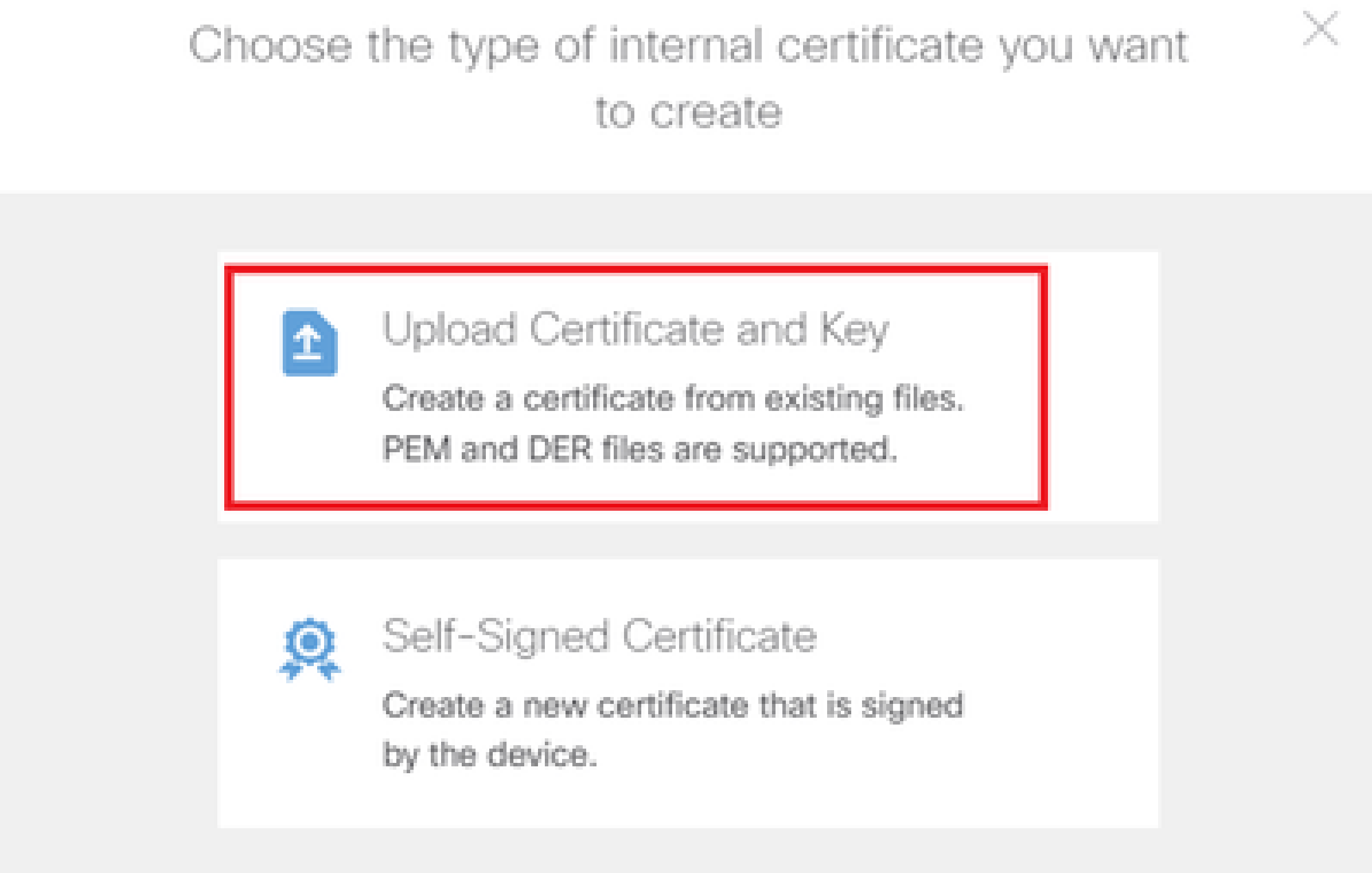
Access Control for VPN Traffic

Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic

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

增加內部證書

按一下Upload Certificate and Key。



Choose the type of internal certificate you want to create

Upload Certificate and Key

Create a certificate from existing files. PEM and DER files are supported.

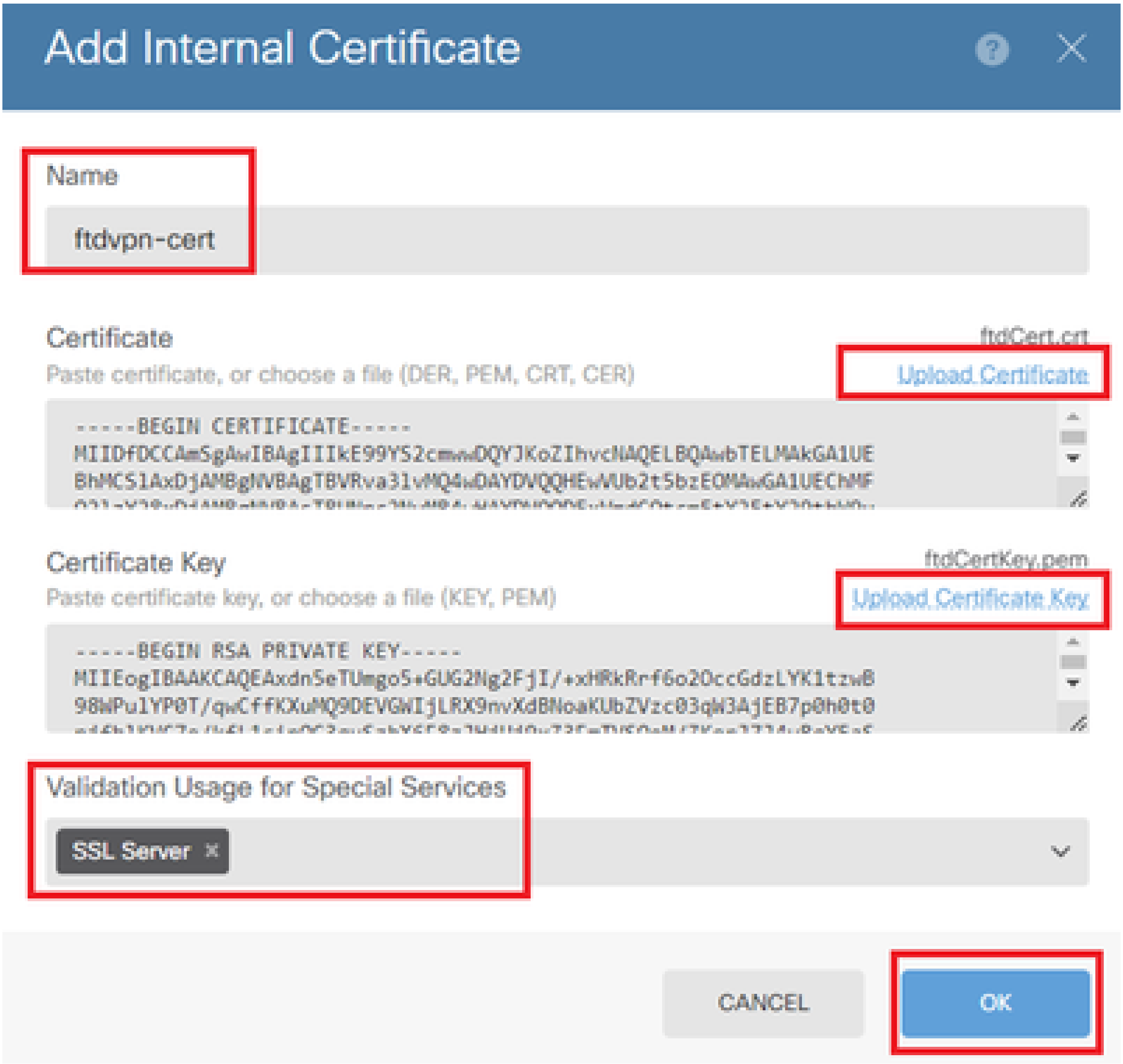
Self-Signed Certificate

Create a new certificate that is signed by the device.

上傳憑證和金鑰

輸入FTD憑證的必要資訊、從本機電腦匯入憑證和憑證金鑰，然後按一下OK按鈕。

- 名稱：ftdvpn-cert
- 特殊服務的驗證用法：SSL伺服器



Add Internal Certificate

Name

ftdvpn-cert

Certificate

Paste certificate, or choose a file (DER, PEM, CRT, CER)

ftdCert.crt

Upload Certificate

```
-----BEGIN CERTIFICATE-----
MIIDfDCCAmSgAwIBAgIIIkE99YS2cmwwDQYJKoZIhvcNAQELBQAwbTELMAkGA1UE
BhMCS1AxDjAMBgNVBAgTBVRva31vMQ4wDAYDVQQHEwVUb2t5bzEOMAwGA1UEChMF
```

Certificate Key

Paste certificate key, or choose a file (KEY, PEM)

ftdCertKey.pem

Upload Certificate Key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAxdnSeTUmgo5+GUG2Ng2FjI/+xHRkRrf6o2OccGdzLYK1tzwB
98WPulYP0T/qwCffKXuMQ9DEVGWIjLRX9nvXdBNoaKUbZVzc03qW3AjEB7p0h0t0
```

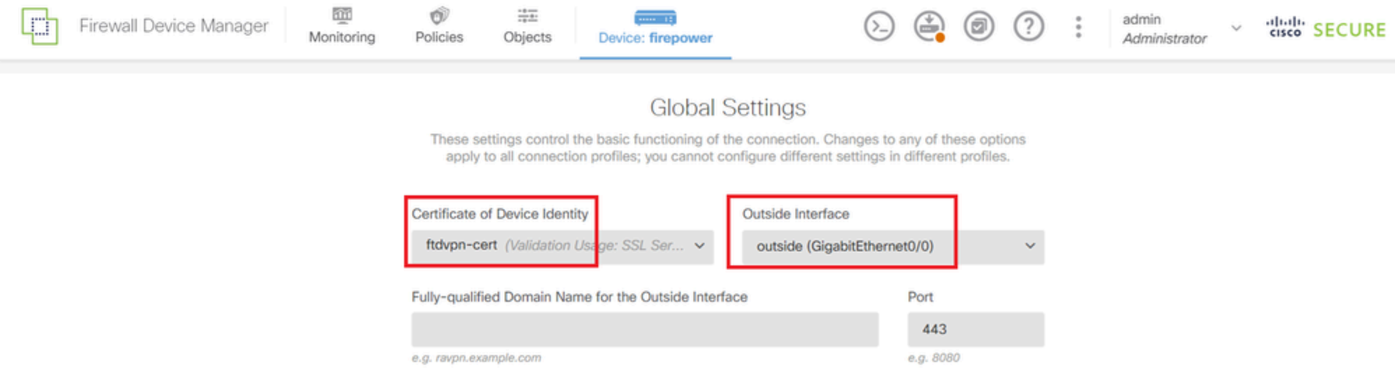
Validation Usage for Special Services

SSL Server ×

內部證書的詳細資訊

為VPN連線選擇Certificate of Device Identity和Outside Interface。

- 裝置身份證書：ftdvpn-cert
- 外部介面：外部(GigabitEthernet0/0)



Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

Certificate of Device Identity: ftdvpn-cert (Validation Usage: SSL Ser...

Outside Interface: outside (GigabitEthernet0/0)

Fully-qualified Domain Name for the Outside Interface

e.g. ravpn.example.com

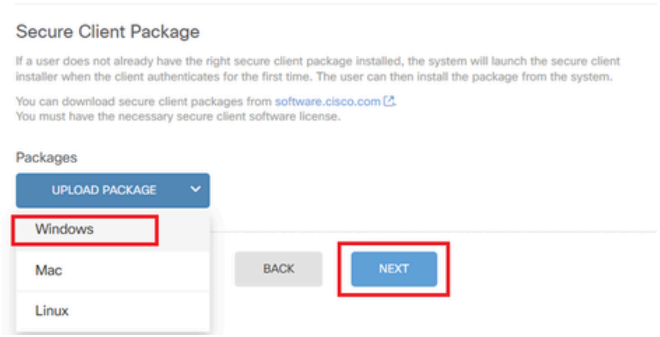
Port: 443

e.g. 8080

全局設定的詳細資訊

步驟 7.設定連線設定檔的安全使用者端映像

在程式包專案中選擇Windows



Secure Client Package

If a user does not already have the right secure client package installed, the system will launch the secure client installer when the client authenticates for the first time. The user can then install the package from the system.

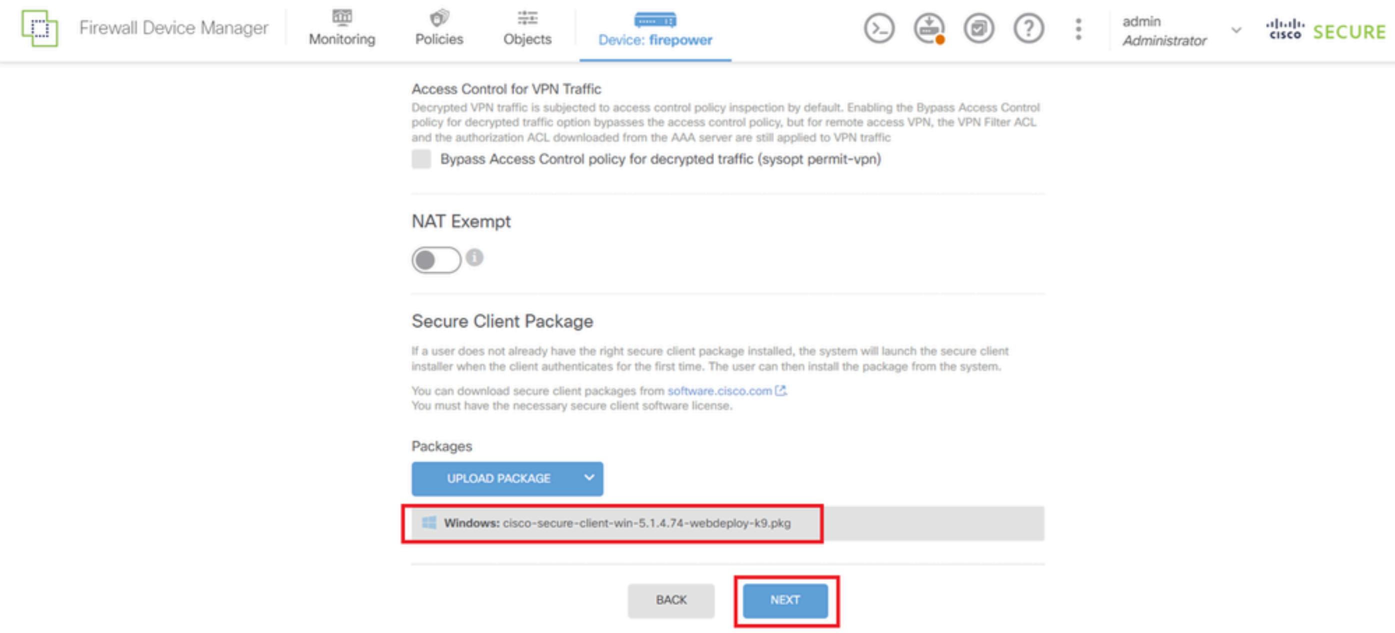
You can download secure client packages from software.cisco.com.
You must have the necessary secure client software license.

Packages

上傳安全客戶端映像包

從本地電腦上傳安全客戶端映象檔案，然後按一下下一步按鈕。

注意：本文檔中停用了NAT免除功能。預設情況下，已停用解密流量的旁路訪問控制策略(sysopt permit-vpn)選項，這意味著已解密的VPN流量將接受訪問控制策略檢查。



Access Control for VPN Traffic

Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic

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

NAT Exempt

Secure Client Package

If a user does not already have the right secure client package installed, the system will launch the secure client installer when the client authenticates for the first time. The user can then install the package from the system.

You can download secure client packages from software.cisco.com
You must have the necessary secure client software license.

Packages

UPLOAD PACKAGE

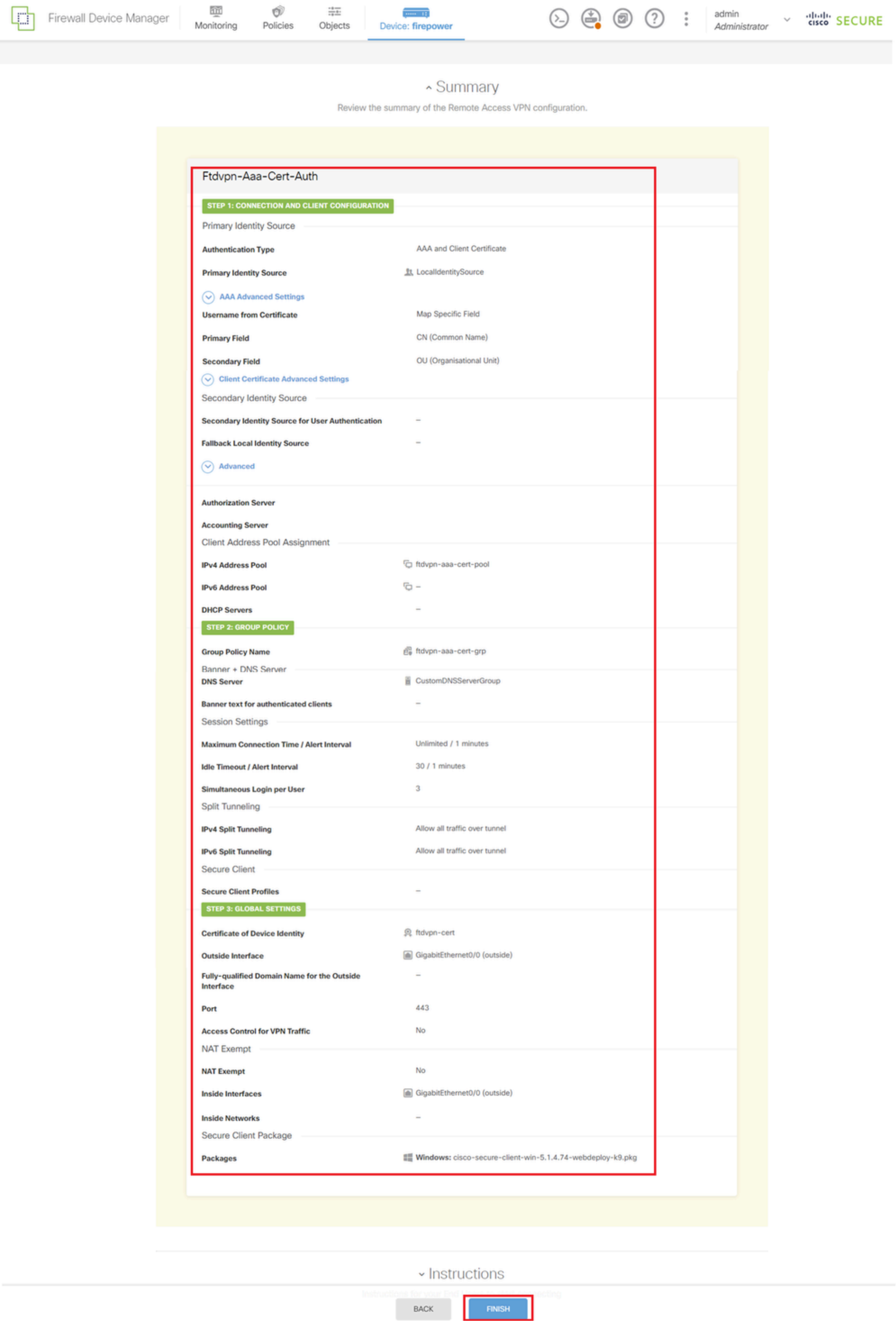
Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

BACK NEXT

選擇安全客戶端映像包

步驟 8.確認連線設定檔摘要

確認輸入的VPN連線資訊，然後按一下FINISH按鈕。



⌃ Summary

Review the summary of the Remote Access VPN configuration.

Ftdvpn-Aaa-Cert-Auth

STEP 1: CONNECTION AND CLIENT CONFIGURATION

Primary Identity Source	
Authentication Type	AAA and Client Certificate
Primary Identity Source	LocalIdentitySource
AAA Advanced Settings	
Username from Certificate	Map Specific Field
Primary Field	CN (Common Name)
Secondary Field	OU (Organisational Unit)
Client Certificate Advanced Settings	
Secondary Identity Source	
Secondary Identity Source for User Authentication	–
Fallback Local Identity Source	–
Advanced	
Authorization Server	
Accounting Server	
Client Address Pool Assignment	
IPv4 Address Pool	ftdvpn-aaa-cert-pool
IPv6 Address Pool	–
DHCP Servers	–

STEP 2: GROUP POLICY

Group Policy Name	ftdvpn-aaa-cert-grp
Banner + DNS Server	
DNS Server	CustomDNSServerGroup
Banner text for authenticated clients	–
Session Settings	
Maximum Connection Time / Alert Interval	Unlimited / 1 minutes
Idle Timeout / Alert Interval	30 / 1 minutes
Simultaneous Login per User	3
Split Tunneling	
IPv4 Split Tunneling	Allow all traffic over tunnel
IPv6 Split Tunneling	Allow all traffic over tunnel
Secure Client	
Secure Client Profiles	–

STEP 3: GLOBAL SETTINGS

Certificate of Device Identity	ftdvpn-cert
Outside Interface	GigabitEthernet0/0 (outside)
Fully-qualified Domain Name for the Outside Interface	–
Port	443
Access Control for VPN Traffic	No
NAT Exempt	
NAT Exempt	No
Inside Interfaces	GigabitEthernet0/0 (outside)
Inside Networks	–
Secure Client Package	
Packages	**Windows:** cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

⌄ Instructions

Instructions for your End Users to start connecting

確認連線設定檔的設定

```
interface GigabitEthernet0/0
speed auto
nameif outside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.1.200 255.255.255.0
!
interface GigabitEthernet0/1
speed auto
nameif inside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.10.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftdvpn-aaa-cert-pool 172.16.1.40-172.16.1.50

// Defines a local user
username sslVPNClientCN password ***** pbkdf2

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftdvpn-cert
enrollment terminal
keypair ftdvpn-cert
validation-usage ssl-server
crl configure

// Server Certificate
crypto ca certificate chain ftdvpn-cert
certificate 22413df584b6726c
3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7
......
quit

// Defines Trustpoint for CA
crypto ca trustpoint ftdvpn-ca-cert
enrollment terminal
validation-usage ssl-client ssl-server
crl configure

// CA
crypto ca certificate chain ftdvpn-ca-cert
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
......
quit

// Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
```

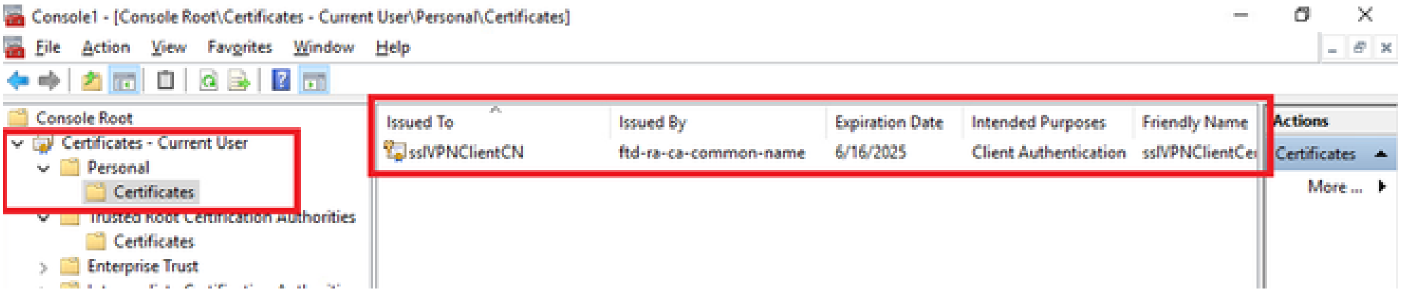
```
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/anyconnpkgs/cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg 2
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Configures the group-policy to allow SSL connections
group-policy ftdvpn-aaa-cert-grp internal
group-policy ftdvpn-aaa-cert-grp attributes
dns-server value 64.x.x.245 64.x.x.184
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
msie-proxy method no-modify
vlan none
address-pools none
ipv6-address-pools none
webvpn
anyconnect ssl dtls none
anyconnect mtu 1406
anyconnect ssl keepalive none
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client none
anyconnect dpd-interval gateway none
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules none
anyconnect profiles none
anyconnect ssl df-bit-ignore disable
always-on-vpn profile-setting

// Configures the tunnel-group to use the aaa & certificate authentication
tunnel-group ftdvpn-aaa-cert-auth type remote-access
tunnel-group ftdvpn-aaa-cert-auth general-attributes
address-pool ftdvpn-aaa-cert-pool
default-group-policy ftdvpn-aaa-cert-grp
// These settings are displayed in the 'show run all' command output. Start
authentication-server-group LOCAL
secondary-authentication-server-group none
no accounting-server-group
default-group-policy ftdvpn-aaa-cert-grp
username-from-certificate CN OU
secondary-username-from-certificate CN OU
authentication-attr-from-server primary
authenticated-session-username primary
username-from-certificate-choice second-certificate
```

```
secondary-username-from-certificate-choice second-certificate
// These settings are displayed in the 'show run all' command output. End
tunnel-group ftdvpn-aaa-cert-auth webvpn-attributes
authentication aaa certificate
pre-fill-username client
group-alias ftdvpn-aaa-cert-auth enable
```

在VPN客戶端中確認

步驟 1.確認使用者端憑證

導航到證書- Current User > Personal > Certificates，檢查用於身份驗證的客戶端證書。



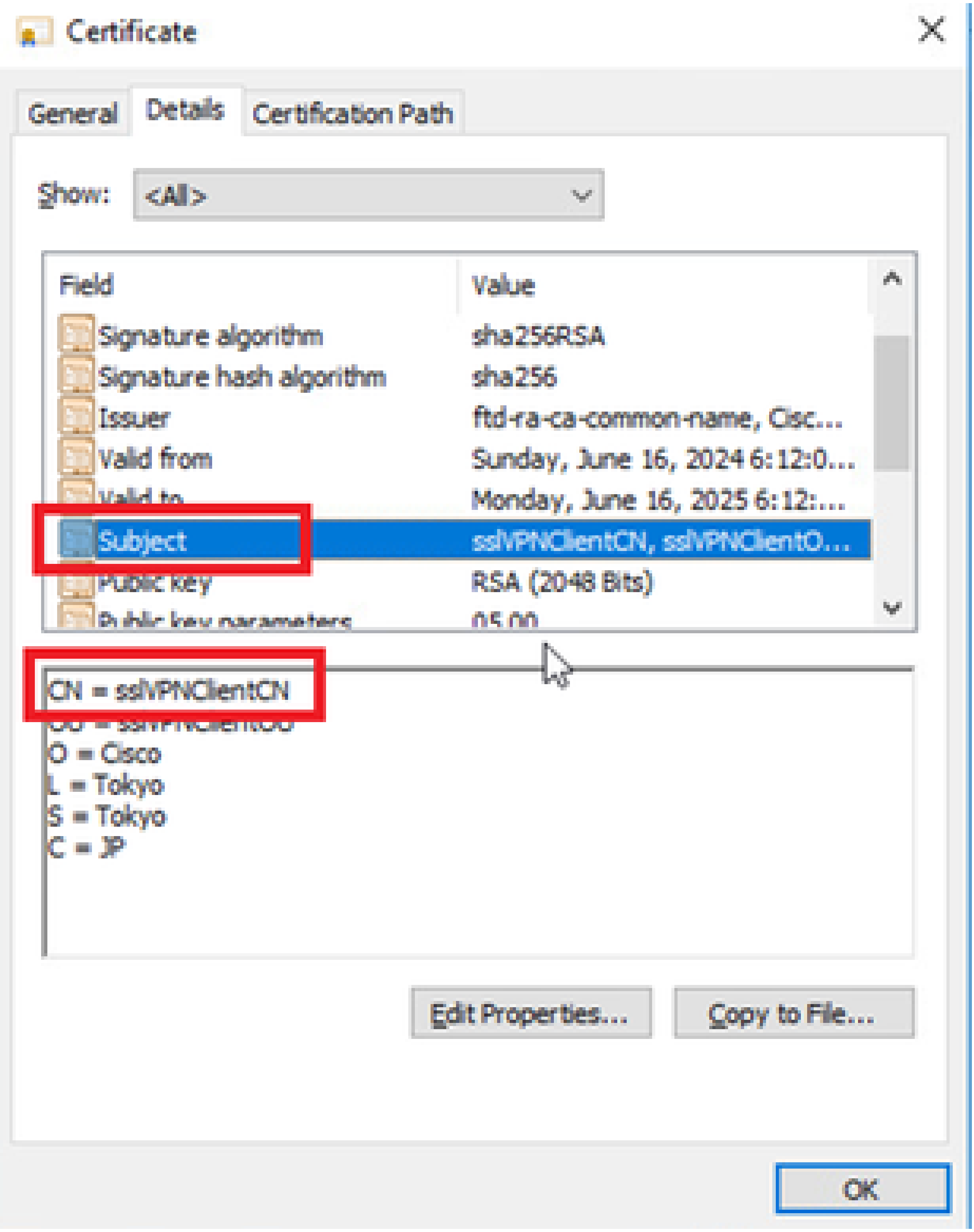
Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
sslVPNClientCN	ftd-ra-ca-common-name	6/16/2025	Client Authentication	sslVPNClientCe

確認使用者端憑證

按兩下客戶端證書，導航至詳細資訊，檢查主題的詳細資訊。

- 主題：CN = sslVPNClientCN



Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ftd-ra-ca-common-name, Cisc...
Valid from	Sunday, June 16, 2024 6:12:0...
Valid to	Monday, June 16, 2025 6:12:...
Subject	sslVPNClientCN, sslVPNClientO...
Public key	RSA (2048 Bits)
Public key parameters	05 00

```
CN = sslVPNClientCN
OU = sslVPNClientOU
O = Cisco
L = Tokyo
S = Tokyo
C = JP
```

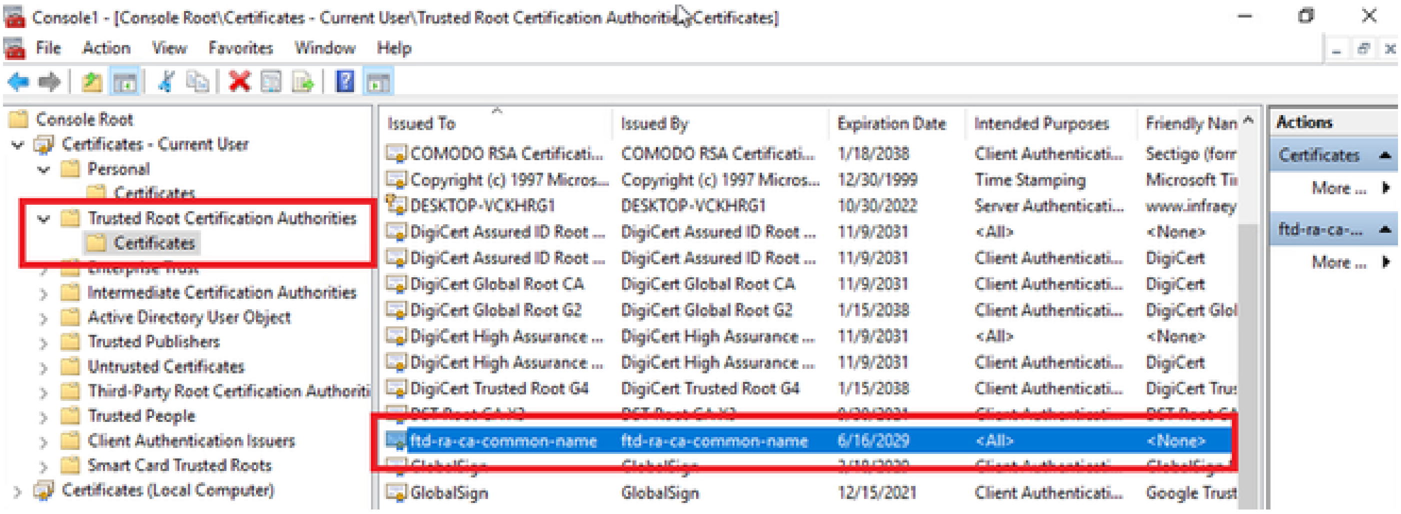
客戶端證書的詳細資訊

步驟 2.確認CA

導航到證書- Current User > Trusted Root Certification Authorities > Certificates，檢查用於身份驗

證的CA。

- 頒發者：ftd-ra-ca-common-name


Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authoriti
Trusted People
Client Authentication Issuers
Smart Card Trusted Roots
Certificates (Local Computer)
Actions
Certificates
More ...
ftd-ra-ca-...
More ...

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Nan
COMODO RSA Certificati...	COMODO RSA Certificati...	1/18/2038	Client Authenticati...	Sectigo (forr
Copyright (c) 1997 Micros...	Copyright (c) 1997 Micros...	12/30/1999	Time Stamping	Microsoft Ti
DESKTOP-VCKHRG1	DESKTOP-VCKHRG1	10/30/2022	Server Authenticati...	www.infraey
DigiCert Assured ID Root ...	DigiCert Assured ID Root ...	11/9/2031	<All>	<None>
DigiCert Assured ID Root ...	DigiCert Assured ID Root ...	11/9/2031	Client Authenticati...	DigiCert
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticati...	DigiCert
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati...	DigiCert Glol
DigiCert High Assurance ...	DigiCert High Assurance ...	11/9/2031	<All>	<None>
DigiCert High Assurance ...	DigiCert High Assurance ...	11/9/2031	Client Authenticati...	DigiCert
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticati...	DigiCert Trus
DST Root CA X3	DST Root CA X3	9/30/2021	Client Authenticati...	DST Root CA
ftd-ra-ca-common-name	ftd-ra-ca-common-name	6/16/2029	<All>	<None>
GlobalSign	GlobalSign	3/18/2029	Client Authenticati...	GlobalSign
GlobalSign	GlobalSign	12/15/2021	Client Authenticati...	Google Trust

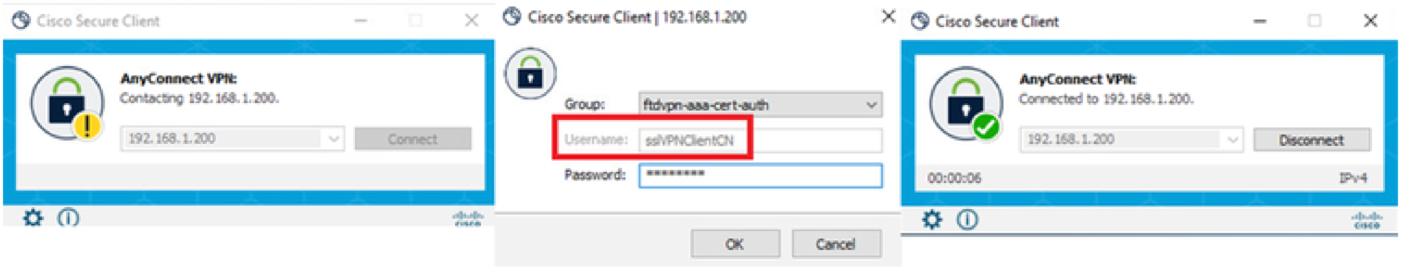
確認CA

驗證

步驟 1.啟動VPN連線

在終端上，啟動Cisco Secure Client連線。使用者名稱從客戶端證書中提取，您需要輸入密碼進行VPN身份驗證。

注意：使用者名稱是從本檔案中的使用者端憑證的一般名稱(CN)欄位中擷取的。


Cisco Secure Client

AnyConnect VPN:
Contacting 192.168.1.200.

192.168.1.200

Cisco Secure Client | 192.168.1.200

Group: ftdvpn-aaa-cert-auth

Username: sslVPNClientCN

Password: *********

Cisco Secure Client

AnyConnect VPN:
Connected to 192.168.1.200.

192.168.1.200

00:00:06 IPv4

啟動VPN連線

步驟 2.在FTD CLI中確認VPN作業階段

在FTD (Lina) CLI中執行show vpn-sessiondb detail anyconnect命令以確認VPN作業階段。

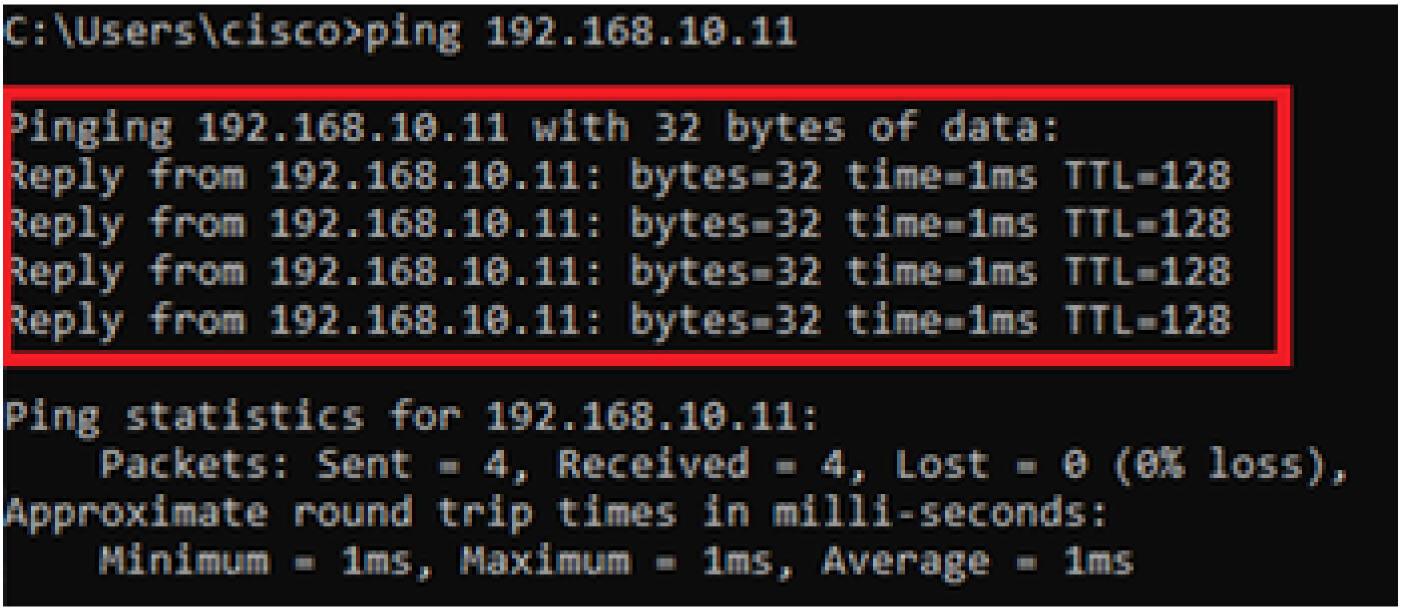
```
firepower# show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 4
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Protocol : AnyConnect-Parent SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384
Bytes Tx : 29072 Bytes Rx : 44412
Pkts Tx : 10 Pkts Rx : 442
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth
Login Time : 11:47:42 UTC Sat Jun 29 2024
Duration : 1h:09m:30s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0000000000004000667ff45e
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 4.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 49779 TCP Dst Port : 443
Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 7 Minutes
Client OS : win
Client OS Ver: 10.0.17763
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 14356 Bytes Rx : 0
Pkts Tx : 2 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 4.3
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 49788
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 7178 Bytes Rx : 10358
Pkts Tx : 1 Pkts Rx : 118
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

步驟 3.確認與伺服器的通訊

從VPN客戶端向伺服器發出ping命令，確認VPN客戶端與伺服器之間的通訊成功。

注意：由於步驟7中停用了用於解密流量的繞過訪問控制策略(sysopt permit-vpn)選項，因此需要建立允許您的IPv4地址池訪問伺服器的訪問控制規則。



```
C:\Users\cisco>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time=1ms TTL=128
Reply from 192.168.10.11: bytes=32 time=1ms TTL=128
Reply from 192.168.10.11: bytes=32 time=1ms TTL=128
Reply from 192.168.10.11: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Ping成功

capture in interface inside real-time在FTD (Lina) CLI中執行命令以確認封包擷取。

```
firepower# capture in interface inside real-time

Warning: using this option with a slow console connection may
result in an excessive amount of non-displayed packets
due to performance limitations.

Use ctrl-c to terminate real-time capture

1: 12:03:26.626691 172.16.1.40 > 192.168.10.11 icmp: echo request
2: 12:03:26.627134 192.168.10.11 > 172.16.1.40 icmp: echo reply
3: 12:03:27.634641 172.16.1.40 > 192.168.10.11 icmp: echo request
4: 12:03:27.635144 192.168.10.11 > 172.16.1.40 icmp: echo reply
5: 12:03:28.650189 172.16.1.40 > 192.168.10.11 icmp: echo request
6: 12:03:28.650601 192.168.10.11 > 172.16.1.40 icmp: echo reply
7: 12:03:29.665813 172.16.1.40 > 192.168.10.11 icmp: echo request
8: 12:03:29.666332 192.168.10.11 > 172.16.1.40 icmp: echo reply
```

疑難排解

您可以期待在Lina引擎的調試系統日誌和Windows電腦上的DART檔案中找到有關VPN身份驗證的資訊。

以下是Lina引擎中的偵錯日誌範例。

```
// Certificate Authentication
Jun 29 2024 11:29:37: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=sslV
Jun 29 2024 11:29:37: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked.
Jun 29 2024 11:29:37: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name: CN=sslVPNClientCN

// Extract username from the CN (Common Name) field
```

```
Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has been requested. [Request 3]
Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has completed. [Request 3]

// AAA Authentication
Jun 29 2024 11:29:53: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN
Jun 29 2024 11:29:53: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN
Jun 29 2024 11:29:53: %FTD-6-113008: AAA transaction status ACCEPT : user = sslVPNClientCN
```

您可以從FTD的診斷CLI執行這些偵錯，提供的資訊可用於排除組態故障。

- debug crypto ca 14
- debug webvpn anyconnect 255
- debug crypto ike-common 255

相關資訊

設定Firepower 2100的FDM機上管理服務

在FDM管理的FTD上設定遠端存取VPN

在Firepower裝置管理器中配置和驗證系統日誌

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）。