Configure AAA and Cert Auth for Secure Client on FTD via FDM

Contents

Introduction

This document describes the steps for configuring Cisco Secure Client over SSL on FTD managed by FDM with AAA and certificate authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Firepower Device Manager (FDM) Virtual
- Firewall Threat Defense (FTD) Virtual
- VPN Authentication Flow

Components Used

- Cisco Firepower Device Manager Virtual 7.2.8
- Cisco Firewall Threat Defense Virtual 7.2.8

- Cisco Secure Client 5.1.4.74

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

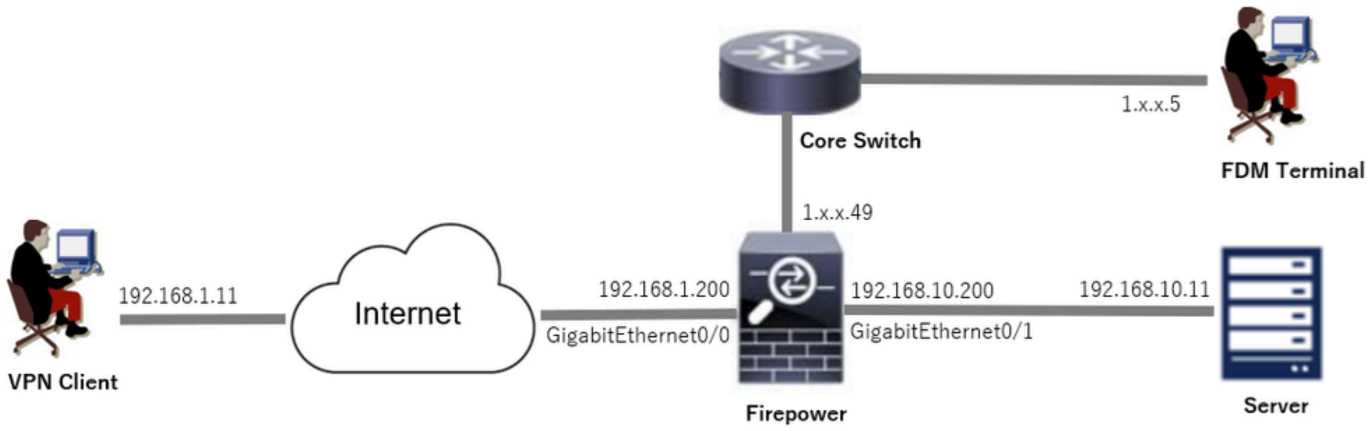
Firepower Device Manager (FDM) is a simplified, web-based management interface used for managing Cisco Firepower Threat Defense (FTD) devices. The Firepower Device Manager allows network administrators to configure and manage their FTD appliances without using the more complex Firepower Management Center (FMC). FDM provides an intuitive user interface for basic operations such as setting up network interfaces, security zones, access control policies, and VPNs, as well as for monitoring the device performance and security events. It is suitable for small to medium-sized deployments where simplified management is desired.
This document describes how to integrate pre-filled usernames with Cisco Secure Client on FTD managed by FDM.
If you are managing FTD with FMC, please refer to the Configure AAA and Cert Auth for Secure Client on FTD via FMC guide.

This is the certificate chain with the common name of each certificate used in the document.

- CA: ftd-ra-ca-common-name
- Client Certificate: sslVPNClientCN
- Server Certificate: 192.168.1.200

Network Diagram

This image shows the topology that is used for the example of this document.



Network Diagram

Configurations

Configuration in FDM

Step 1. Configure FTD Interface

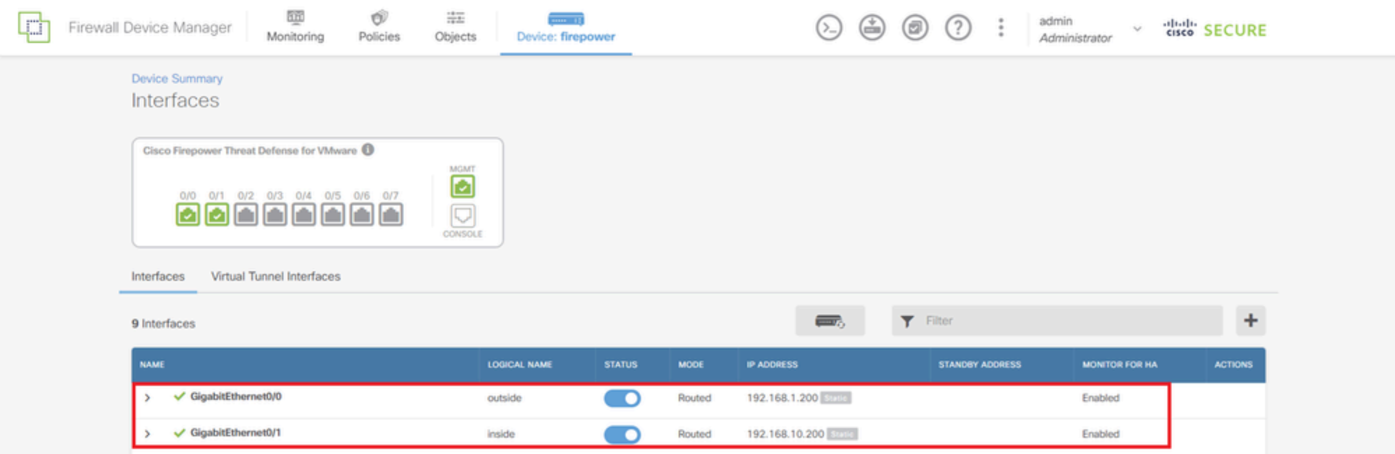
Navigate to **Device** > **Interfaces** > **View All Interfaces**, configure inside and outside interface for FTD in**Interfaces**tab.

For GigabitEthernet0/0,

- Name: outside
- IP Address: 192.168.1.200/24

For GigabitEthernet0/1,

- Name: inside
- IP Address: 192.168.10.200/24

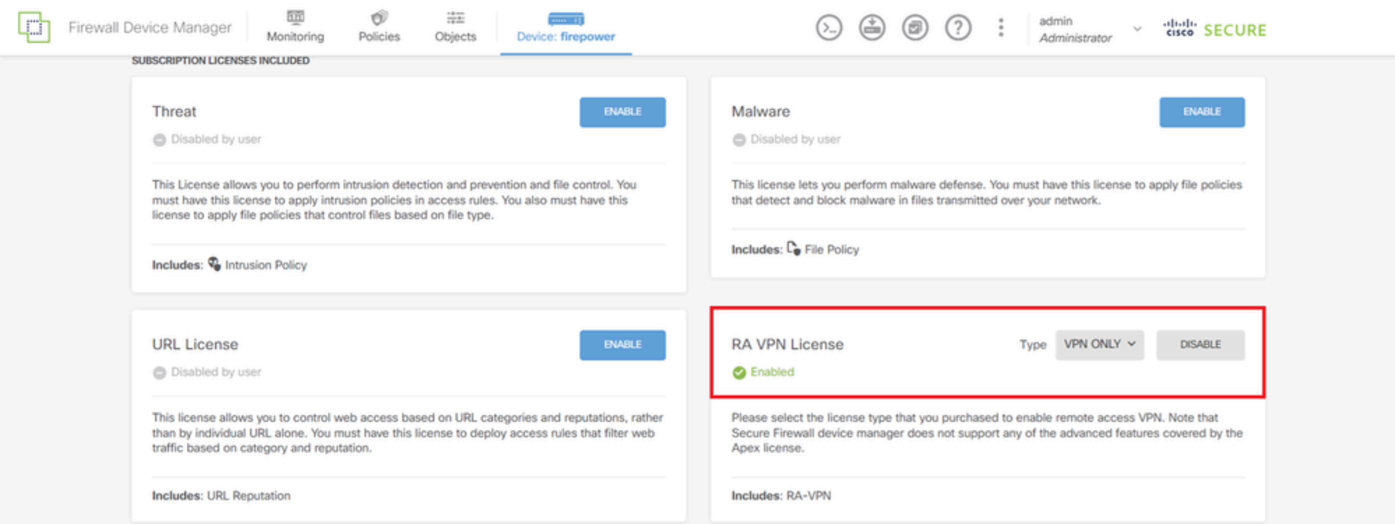


NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
✓ GigabitEthernet0/0	outside	●	Routed	192.168.1.200 Static		Enabled	
✓ GigabitEthernet0/1	inside	●	Routed	192.168.10.200 Static		Enabled	

FTD Interface

Step 2. Confirm Cisco Secure Client License

Navigate to **Device** > **Smart License** > **View Configuration**, confirm the Cisco Secure Client license in **RA VPN License**item.



SUBSCRIPTION LICENSES INCLUDED

Threat

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

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

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

✓ Enabled

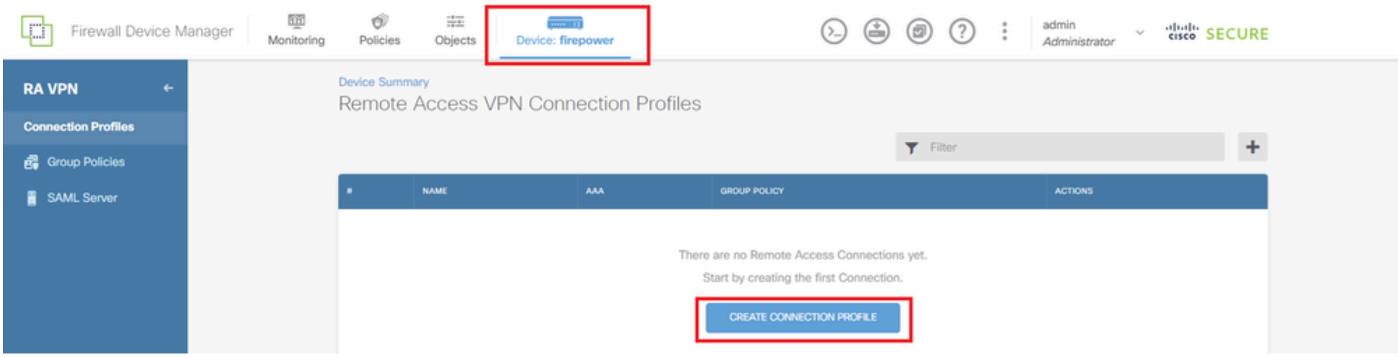
Please select the license type that you purchased to enable remote access VPN. Note that Secure Firewall device manager does not support any of the advanced features covered by the Apex license.

Includes: RA-VPN

Secure Client License

Step 3. Add Remote Access VPN Connection Profile

Navigate to **Device** > **Remote Access VPN** > **View Configuration**, click **CREATE CONNECTION PROFILE** button.

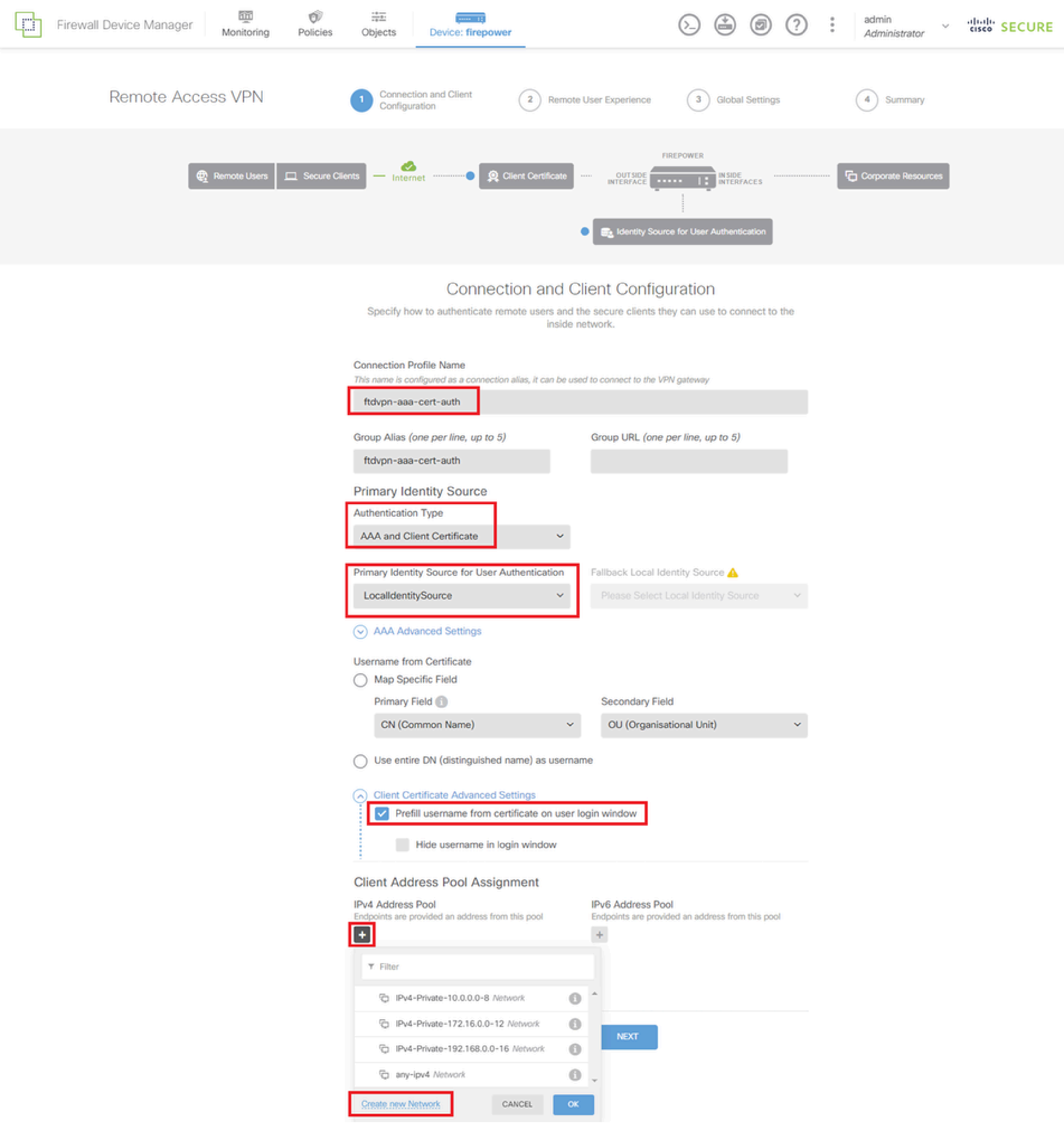


There are no Remote Access Connections yet.
Start by creating the first Connection.

Add Remote Access VPN Connection Profile

Input necessary information for connection profile and click **Create new Network** button in the **IPv4 Address Pool** item.

- Connection Profile Name: ftdvpn-aaa-cert-auth
- Authentication Type: AAA and Client Certificate
- Primary Identity Source for User Authentication: LocalIdentitySource
- Client Certificate Advanced Settings: Prefill username from certificate on user login window



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

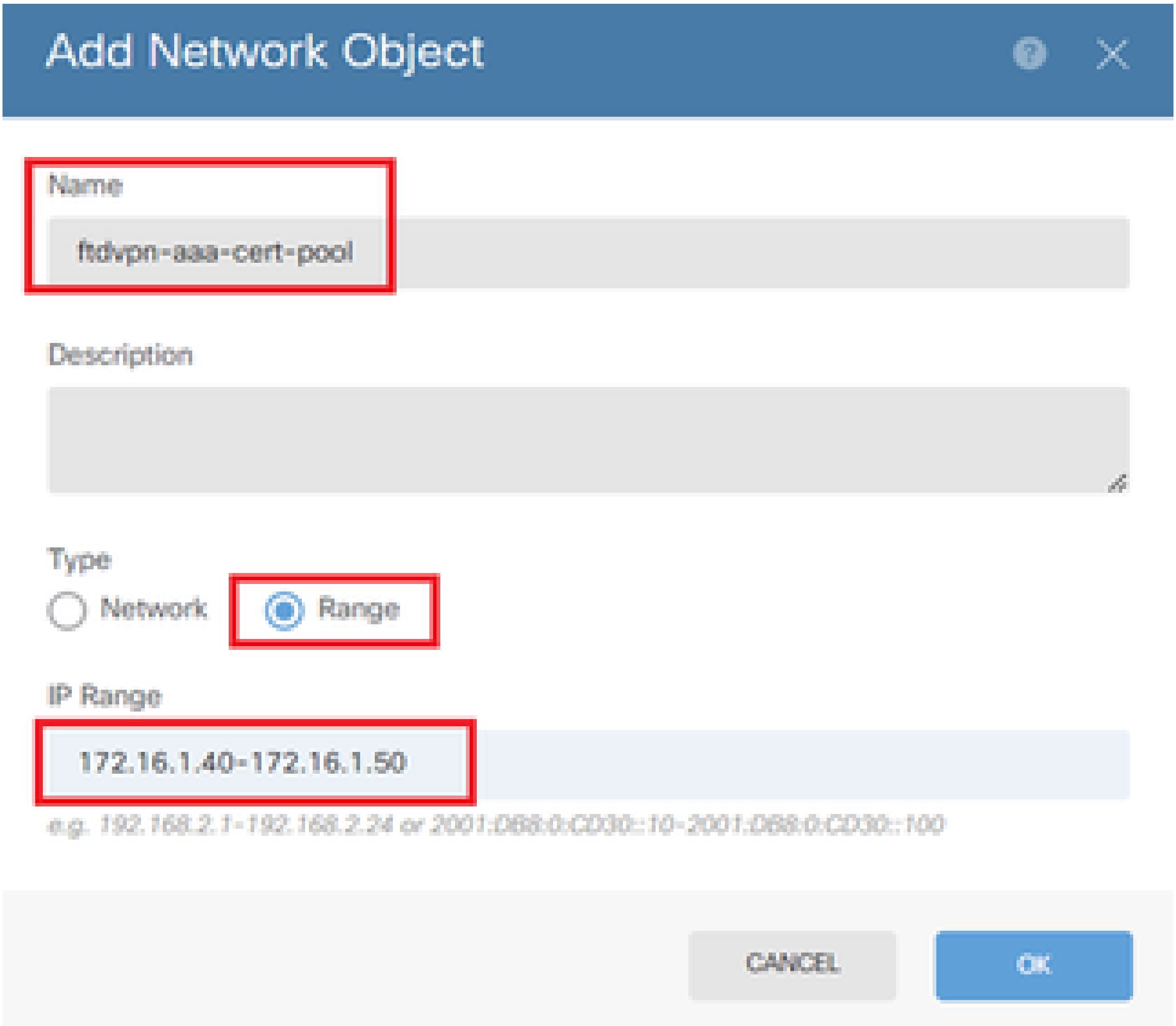
- IPv4-Private-10.0.0.0-8 *Network*
- IPv4-Private-172.16.0.0-12 *Network*
- IPv4-Private-192.168.0.0-16 *Network*
- any-ipv4 *Network*

Details of VPN Connection Profile

Step 4. Add Address Pool for Connection Profile

Input necessary information to add a new IPv4 address pool. Select new added IPv4 address pool for connection profile and click **Next** button.

- Name: ftdvpn-aaa-cert-pool
- Type: Range
- IP Range: 172.16.1.40-172.16.1.50



Add Network Object
Name
Description
Type
○ Network
● Range
IP Range
e.g. 192.168.2.1-192.168.2.24 or 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100
CANCEL
OK

Name: ftdvpn-aaa-cert-pool

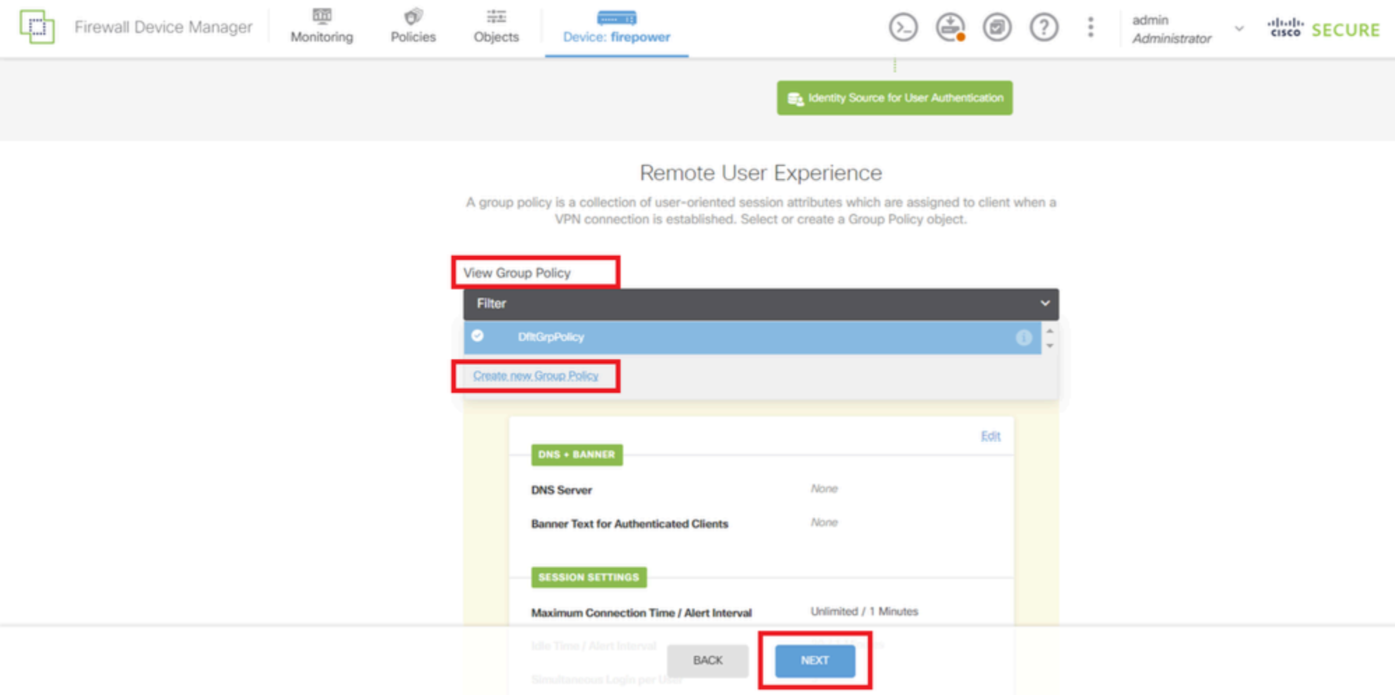
Type: ● Range

IP Range: 172.16.1.40-172.16.1.50

Details of IPv4 Address Pool

Step 5. Add Group Policy for Connection Profile

Click **Create new Group Policy** in the **View Group Policy** item.



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.

DNS Server None

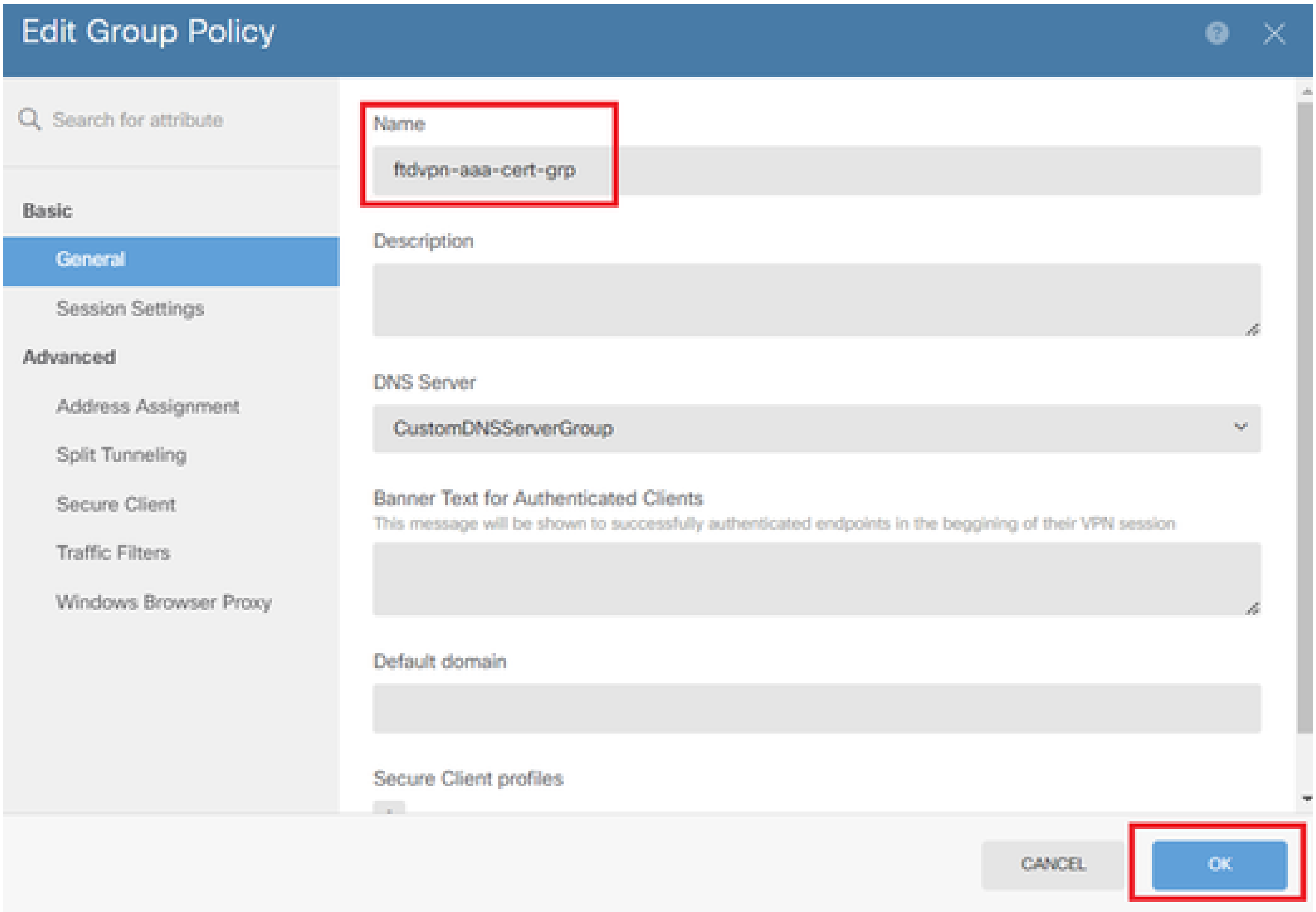
Banner Text for Authenticated Clients None

Maximum Connection Time / Alert Interval Unlimited / 1 Minutes

Add Group Policy

Input necessary information to add a new group policy and click **OK** button. Select new added group policy for connection profile.

- Name: ftdvpn-aaa-cert-grp



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

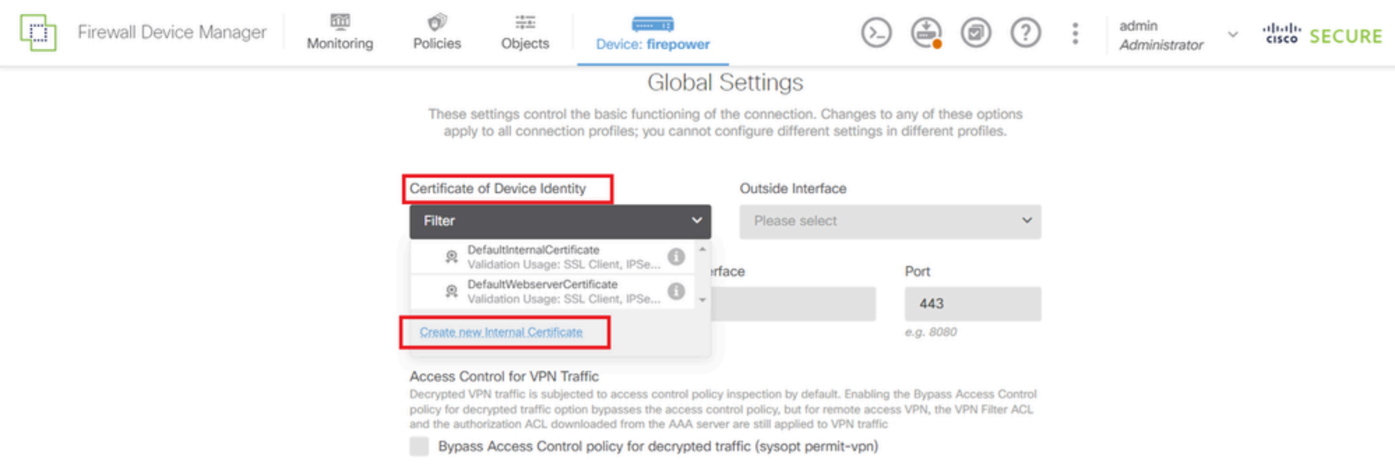
Default domain

Secure Client profiles

Details of Group Policy

Step 6. Configure Certificate of Device Identity and Outside Interface for Connection Profile

Click **Create new Internal certificate** in the **Certificate of Device Identity** item.



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

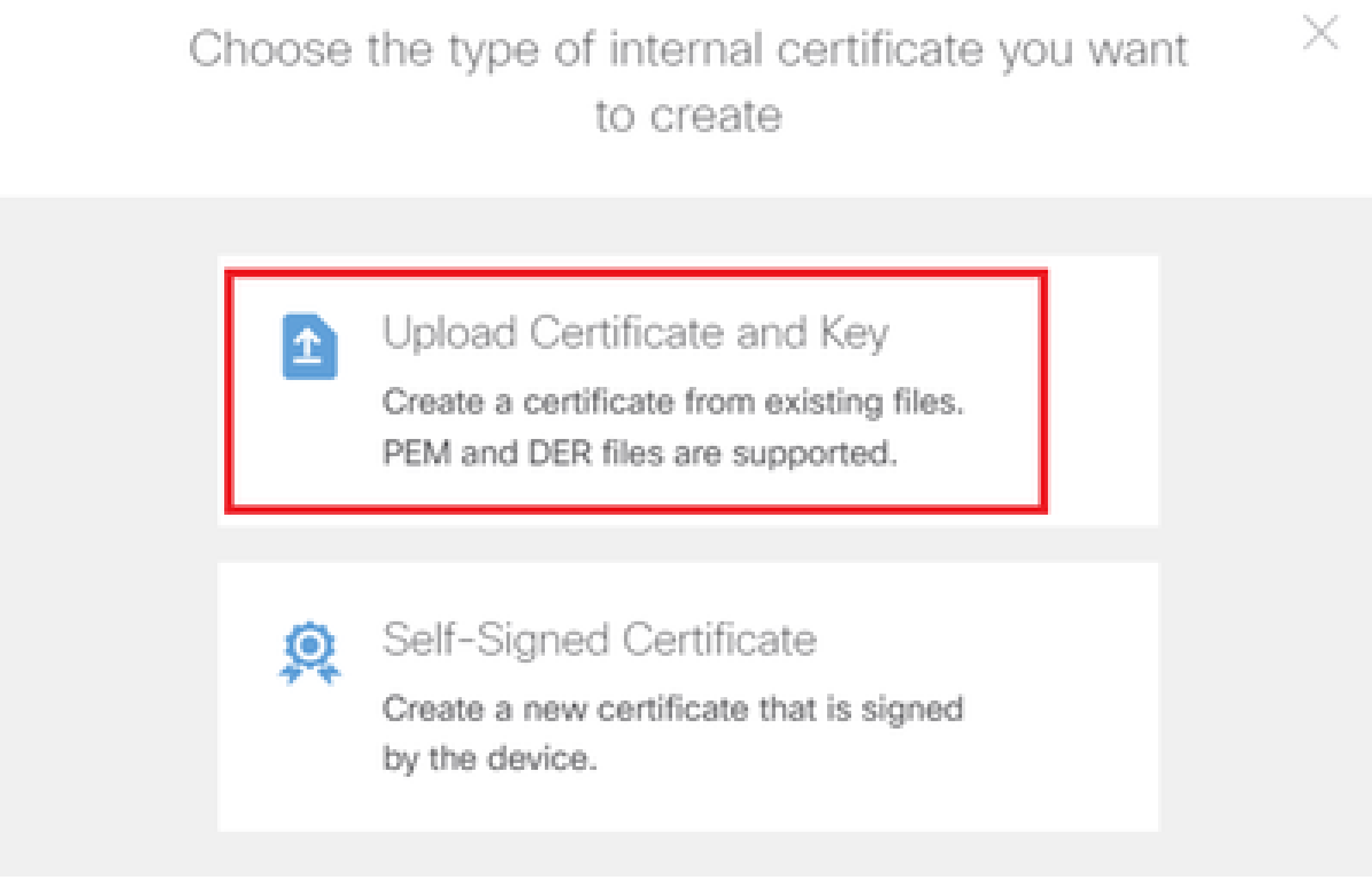
Access Control for VPN Traffic

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)

Add Internal Certificate

Click **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.

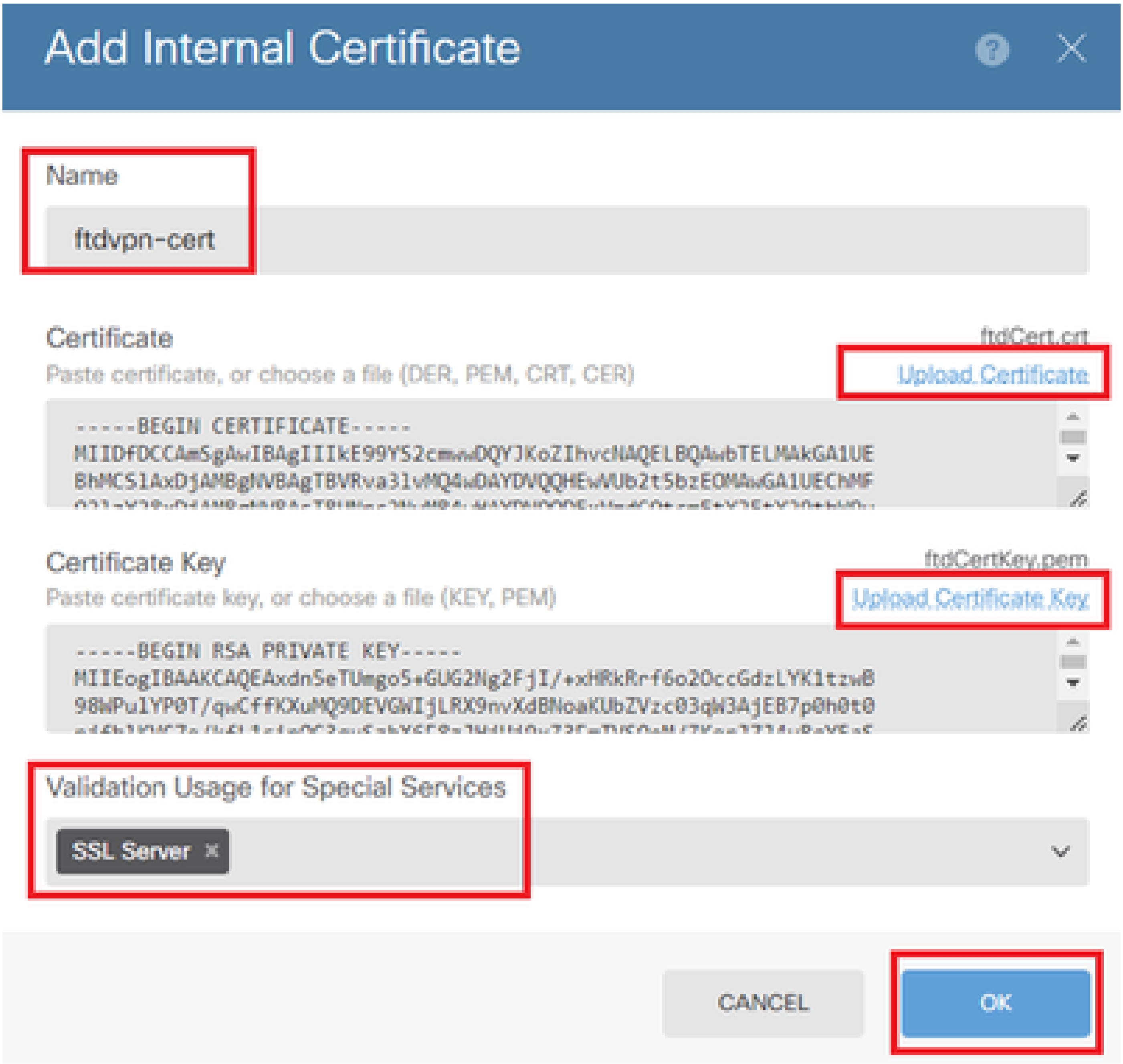
Self-Signed Certificate

Create a new certificate that is signed by the device.

Upload Certificate and Key

Input necessary information for FTD certificate, import a certificate and a certificate key from local computer and then Click **OK** button.

- Name: ftdvpn-cert
- Validation Usage for Special Services: SSL Server



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-----
MIIEogIBAAKCAQEAxdn5eTUmgo5+GUG2Ng2FjI/+xHRkRrf6o2OccGdzLYK1tzwB
98WPulYP0T/qwCffKXuMQ9DEVGWIjLRX9nvXdBNoaKUbZVzc03qW3AjEB7p0h0t0
```

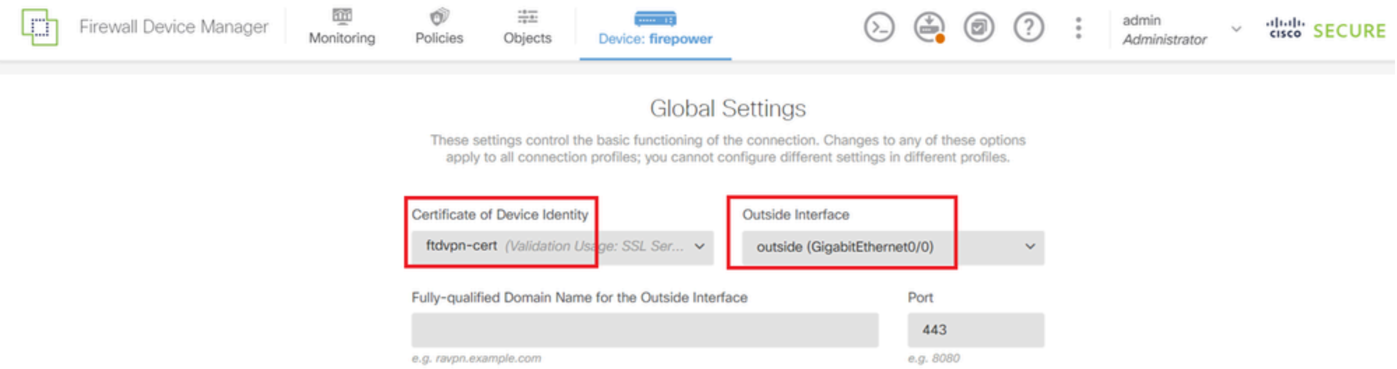
Validation Usage for Special Services

SSL Server ×

Details of Internal Certificate

Select **Certificate of Device Identity** and **Outside Interface** for VPN connection.

- Certificate of Device Identity: ftdvpn-cert
- Outside Interface: outside (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)

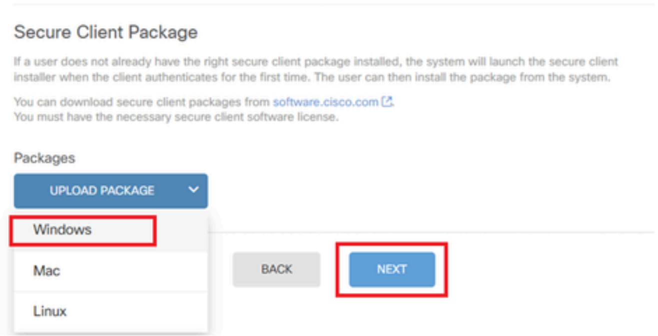
Fully-qualified Domain Name for the Outside Interface: e.g. ravpn.example.com

Port: 443 e.g. 8080

Details of Global Settings

Step 7. Configure Secure Client Image for Connection Profile

Select **Windows** in **Packages** item



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.

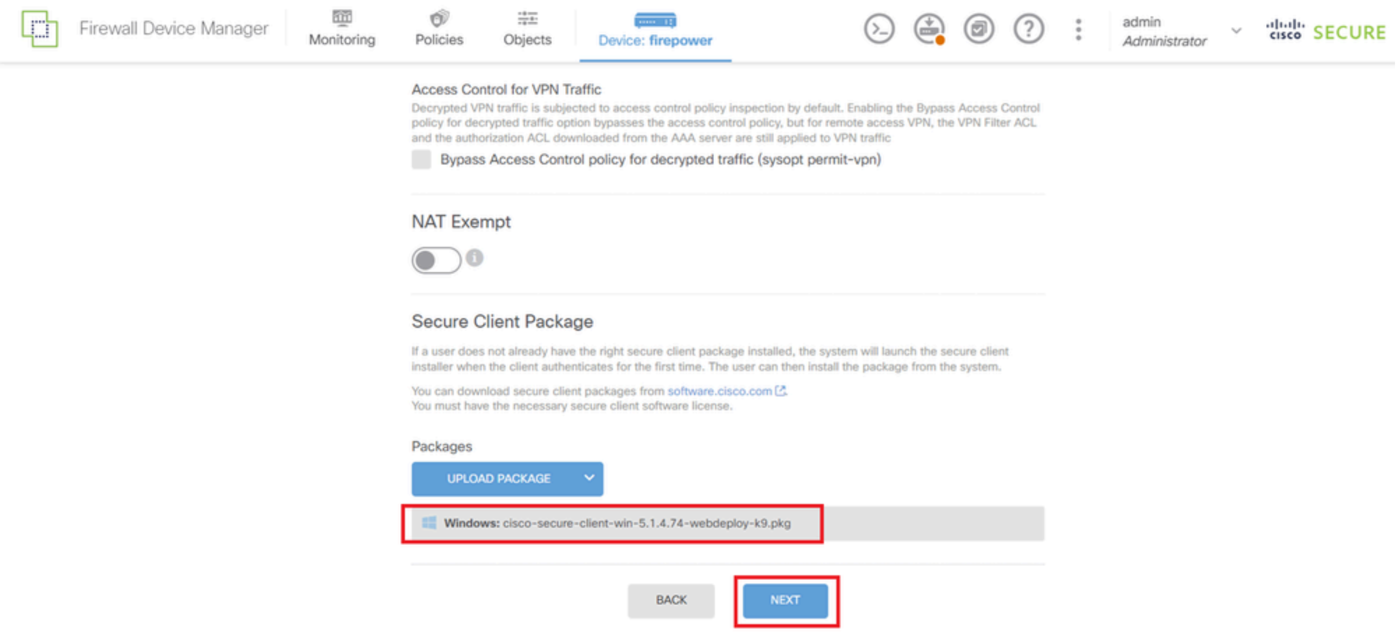
You can download secure client packages from software.cisco.com.
You must have the necessary secure client software license.

Packages

Upload Secure Client Image Package

Upload **secure client image** file from local computer and click**Next**button.

Note: The NAT Exempt feature is disabled in this document. By default, the Bypass Access Control policy for decrypted traffic (sysopt permit-vpn) option is disabled, which means that decrypted VPN traffic is subjected to access control policy inspection.



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.

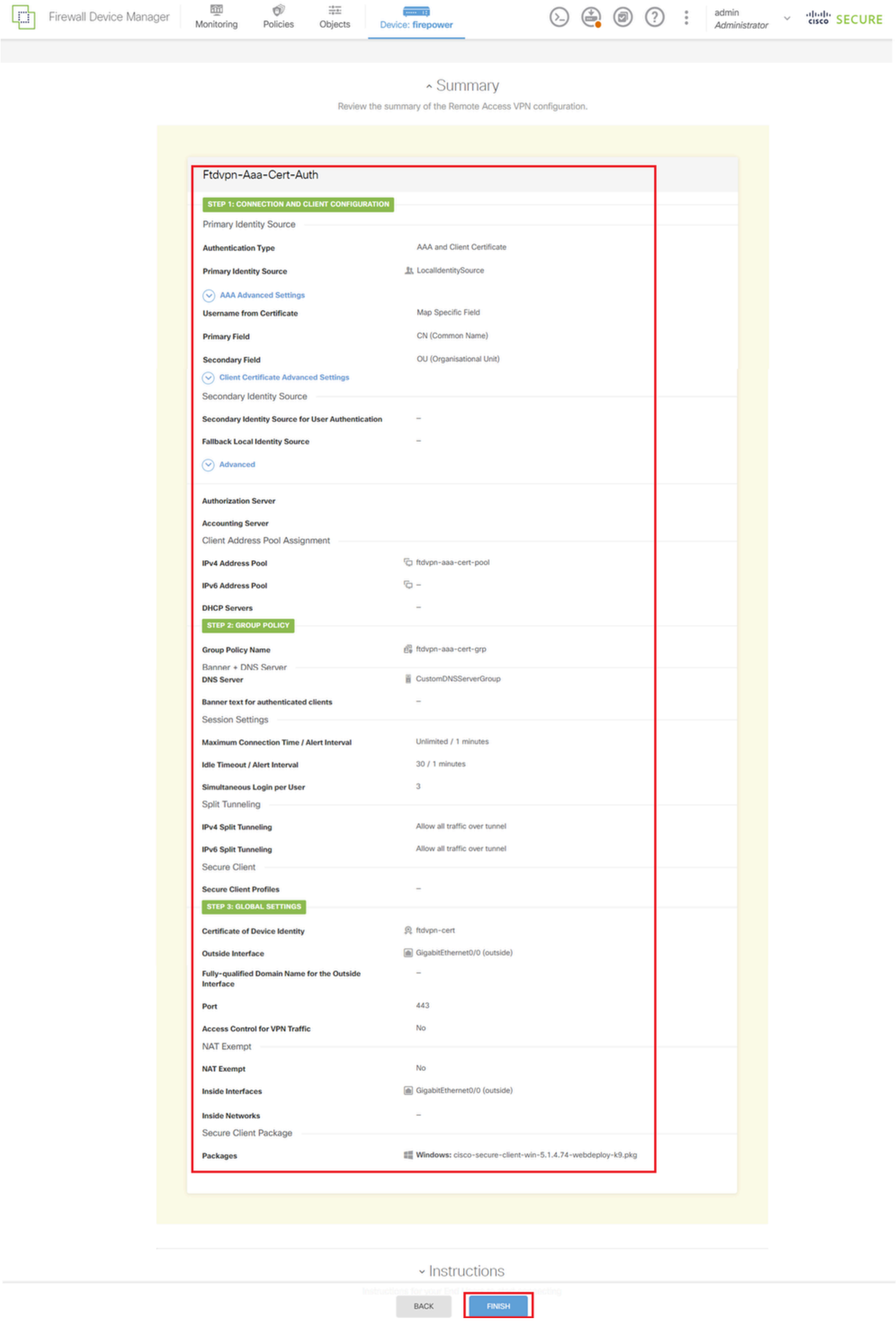
Packages

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

Select Secure Client Image Package

Step 8. Confirm Summary for Connection Profile

Confirm the information entered for VPN connection and click **FINISH**button.



⌃ 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

Confirm Settings for Connection Profile

```
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
```

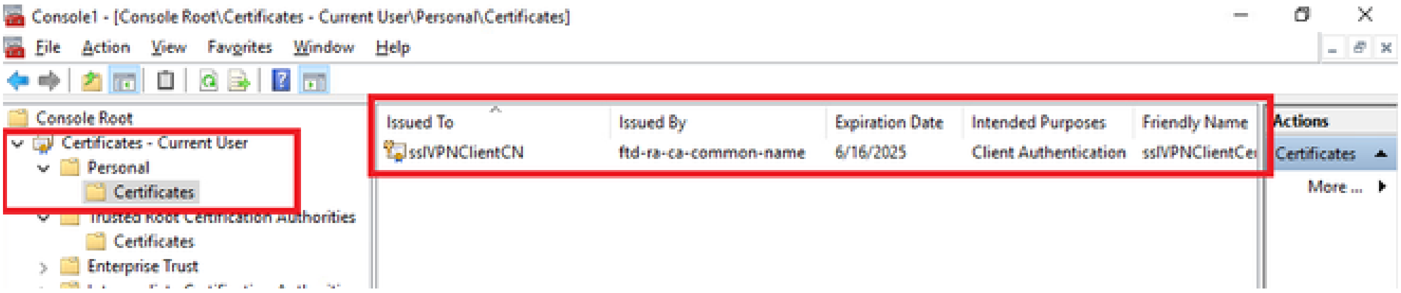
```
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/anyconnpkgs/cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg 2
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// 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
```

Confirm in VPN Client

Step 1. Confirm Client Certificate

Navigate to**Certificates - Current User** > **Personal** > **Certificates**, check the client certificate used for authentication.

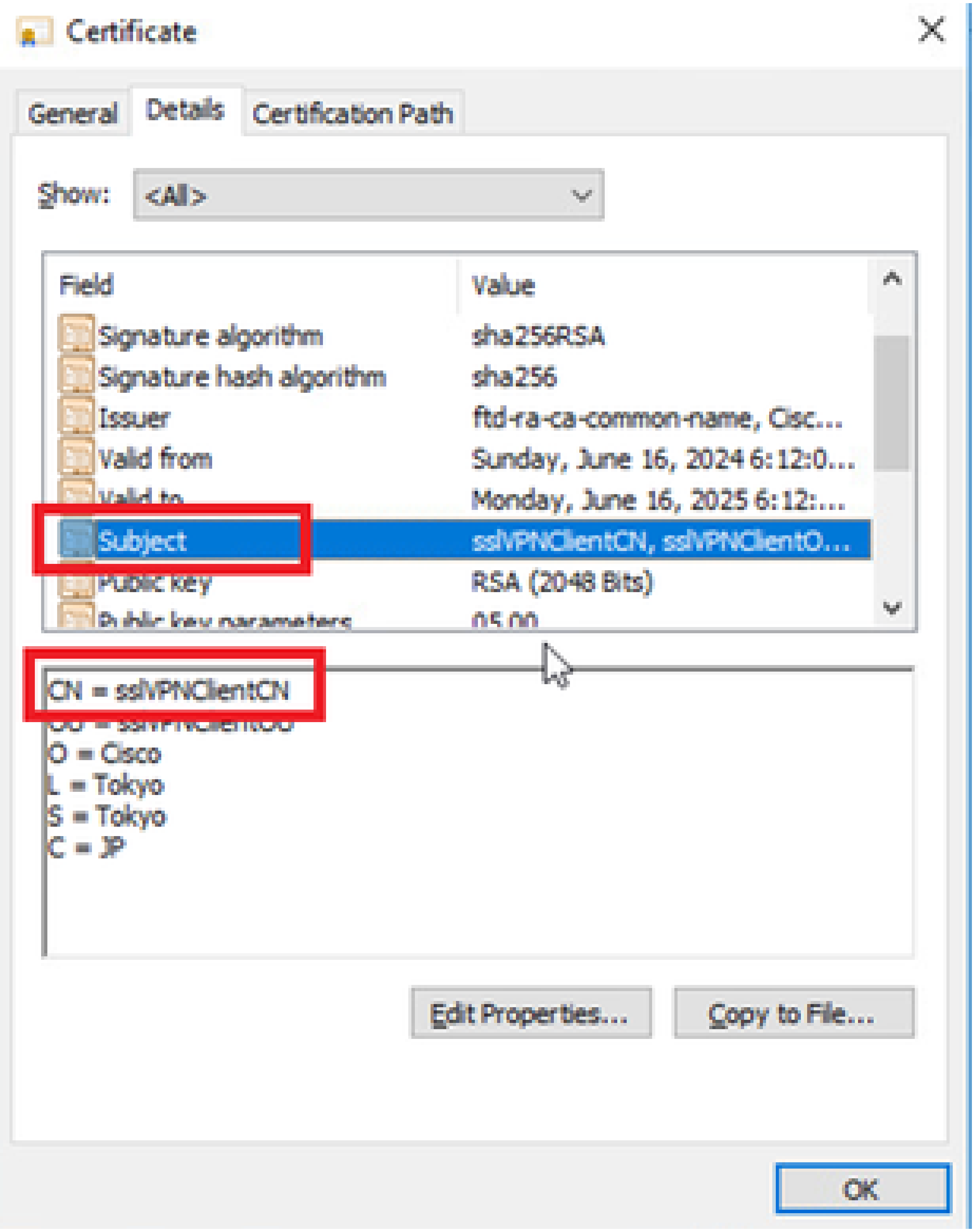

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Actions
Certificates
More ...

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

Confirm Client Certificate

Double click the **client certificate**, navigate to**Details**, check the detail of**Subject**.

- Subject: 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

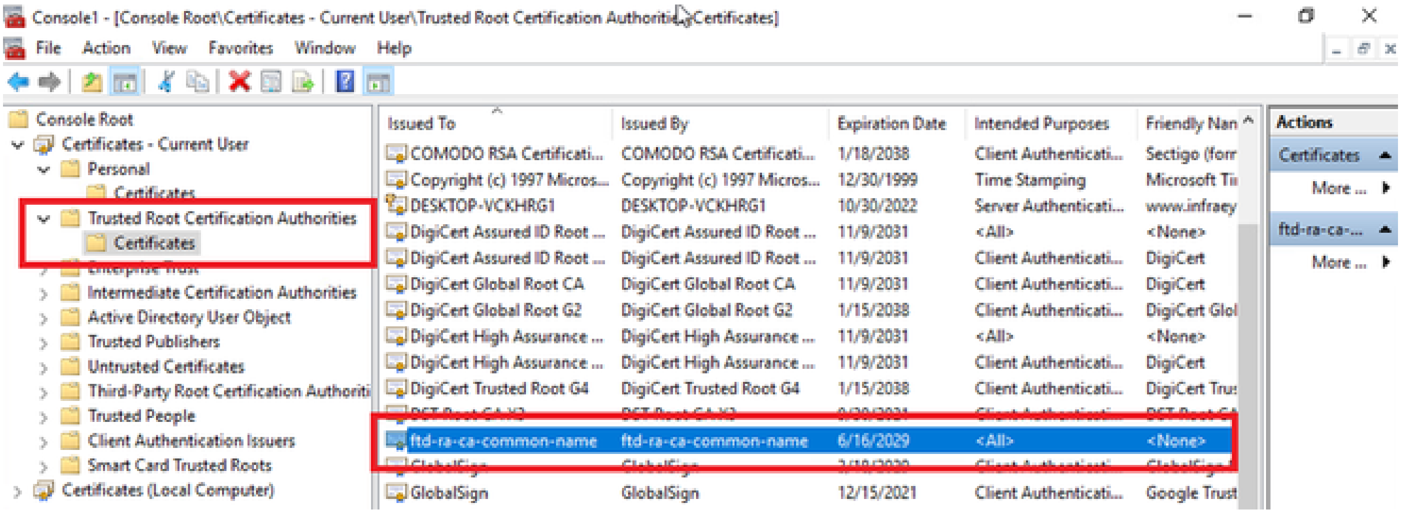
```
CN = sslVPNClientCN
OU = sslVPNClientOU
O = Cisco
L = Tokyo
S = Tokyo
C = JP
```

Details of Client Certificate

Step 2. Confirm CA

Navigate to**Certificates - Current User > Trusted Root Certification Authorities > Certificates**, check the CA used for authentication.

- Issued By: 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 (form
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

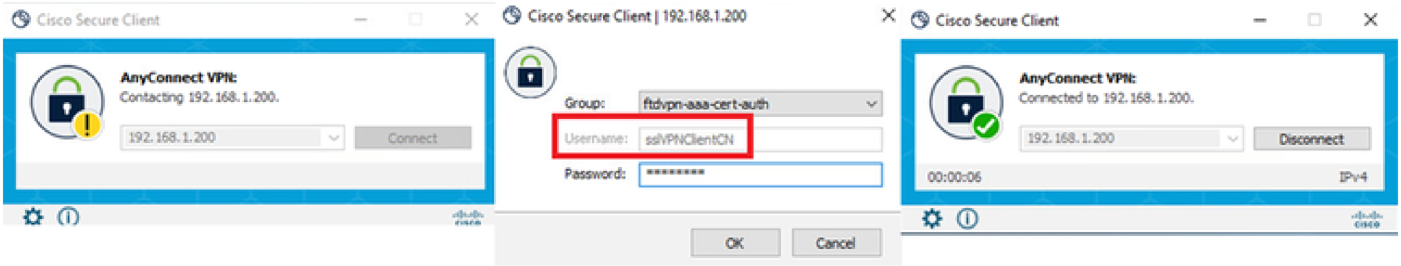
Confirm CA

Verify

Step 1. Initiate VPN Connection

On the endpoint, initiate the Cisco Secure Client connection. The username is extracted from the client certificate, you need to input the password for VPN authentication.

Note: The username is extracted from the Common Name (CN) field of the client certificate in this document.



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

Initiate VPN Connection

Step 2. Confirm VPN Session in FTD CLI

Runshow vpn-sessiondb detail anyconnect command in FTD (Lina) CLI to confirm the VPN session.

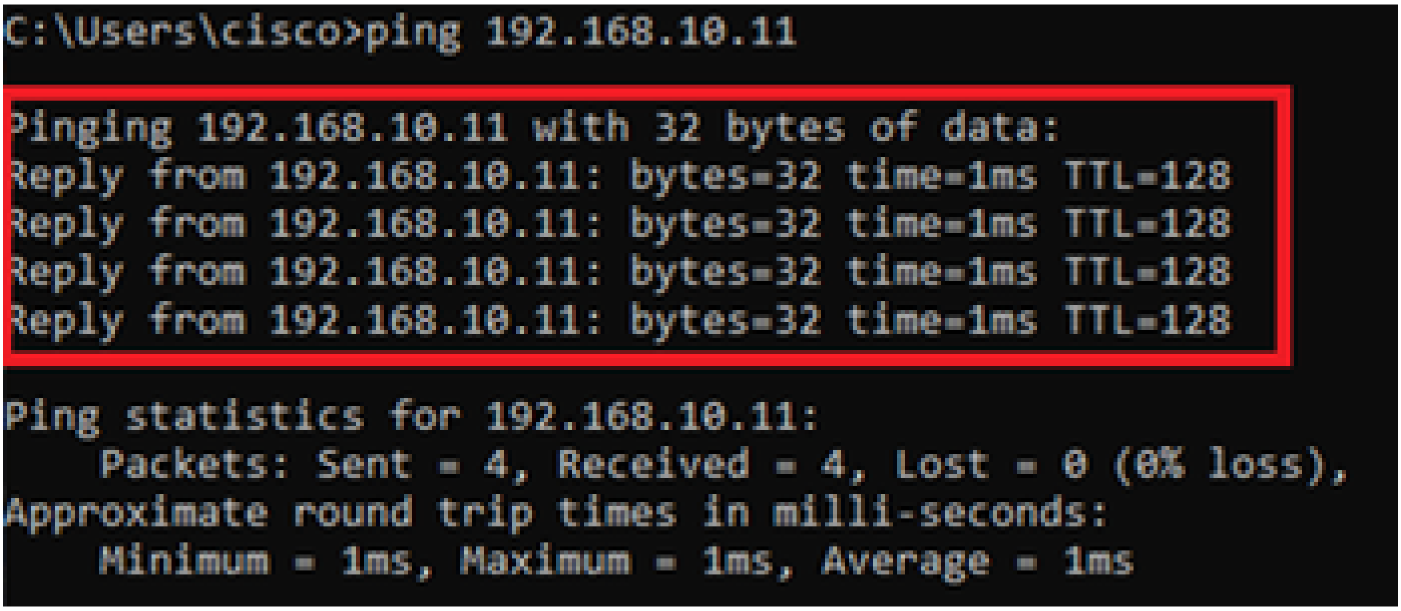
```
firepower# show vpn-sessiondb detail anyconnect
```

```
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
```

Step 3. Confirm Communication with Server

Initiate ping from VPN client to the Server, confirm that communication between the VPN client and the server is successful.

Note: Because the Bypass Access Control policy for decrypted traffic (sysopt permit-vpn) option is disabled in step 7, you need to create access control rules that allow your IPv4 address pool access to the server.



```
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 Succeeded

Runcapture in interface inside real-timecommand in FTD (Lina) CLI to confirm packet capture.

```
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
```

Troubleshoot

You can expect to find information about VPN authentication in the debug syslog of Lina engine and in the DART file on Windows computer.

This is an example of debug logs in the Lina engine.

```
// Certificate Authentication
Jun 29 2024 11:29:37: %FTD-7-717029: Identified client certificate within certificate chain. serial numb
Jun 29 2024 11:29:37: %FTD-6-717028: Certificate chain was successfully validated with warning, revocat
Jun 29 2024 11:29:37: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B23

// 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 reques
Jun 29 2024 11:29:53: %FTD-7-113028: Extraction of username from VPN client certificate has completed.

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

These debugs can be run from the diagnostic CLI of the FTD, which provides information you can use in order to troubleshoot your configuration.

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

Related Information

Configure FDM On-Box Management Service for Firepower 2100

Configure Remote Access VPN on FTD Managed by FDM

Configure and Verify Syslog in Firepower Device Manager