# FMCを介したFTD上のセキュアクライアントのAAAおよび証明書認証の設定

## 内容



## はじめに

このドキュメントでは、AAAおよび証明書認証を使用してFMCによって管理されるFTDでCisco Secure Client over SSLを設定する手順について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco Firepower Management Center（FMC）
- ファイアウォール脅威防御の仮想(FTD)
- VPN認証のフロー

### 使用するコンポーネント

- VMWare 7.4.1向けCisco Firepower Management Center
- シスコファイアウォール脅威対策の仮想7.4.1

- Cisco Secureクライアント5.1.3.62

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

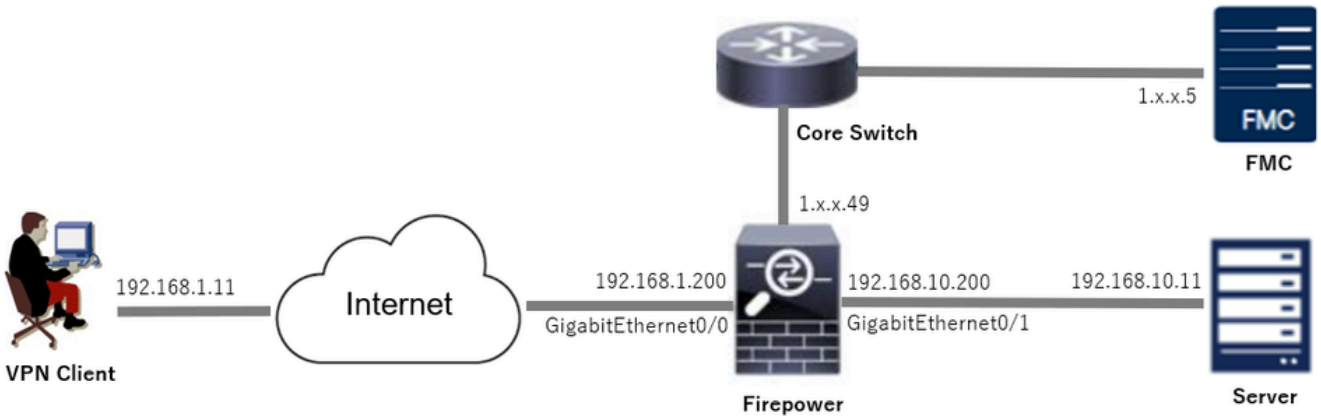
組織がより厳格なセキュリティ対策を採用するにつれ、2要素認証(2FA)と証明書ベースの認証を組み合わせることが、セキュリティを強化し、不正アクセスから保護するための一般的な方法になってきています。 ユーザエクスペリエンスとセキュリティを大幅に向上させる機能の1つは、Cisco Secure Clientでユーザ名をあらかじめ入力する機能です。この機能により、ログインプロセスが簡素化され、リモートアクセスの全体的な効率が向上します。
このドキュメントでは、事前に入力されたユーザ名をFTD上のCisco Secure Clientと統合し、ユーザがネットワークに迅速かつ安全に接続できるようにする方法について説明します。

これらの証明書には共通の名前が含まれており、認証の目的で使用されます。

- CA:ftd-ra-ca-common-name
- クライアント証明書:sslVPNClientCN
- サーバ証明書:192.168.1.200

## ネットワーク図

次の図は、このドキュメントの例で使用するトポロジを示しています。




ネットワーク図

# コンフィギュレーション

## FMCでの設定

### ステップ 1：FTDインターフェイスの設定

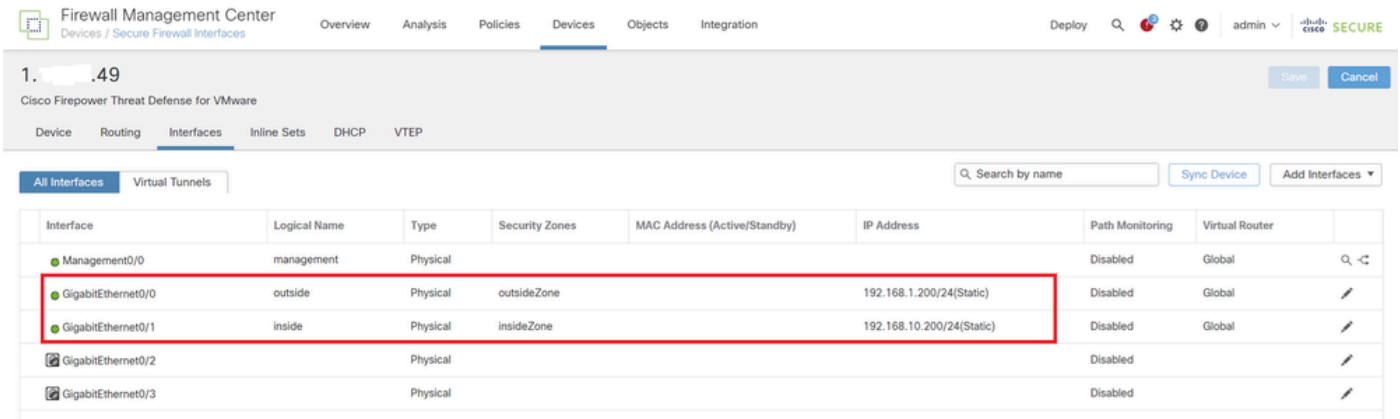
Devices > Device Managementの順に移動し、ターゲットFTDデバイスを編集して、InterfacesタブでFTDのInsideおよびOutsideインターフェイスを設定します。

GigabitEthernet0/0の場合、

- 名前:outside
- セキュリティゾーン:outsideZone
- IPアドレス:192.168.1.200/24

GigabitEthernet0/1の場合、

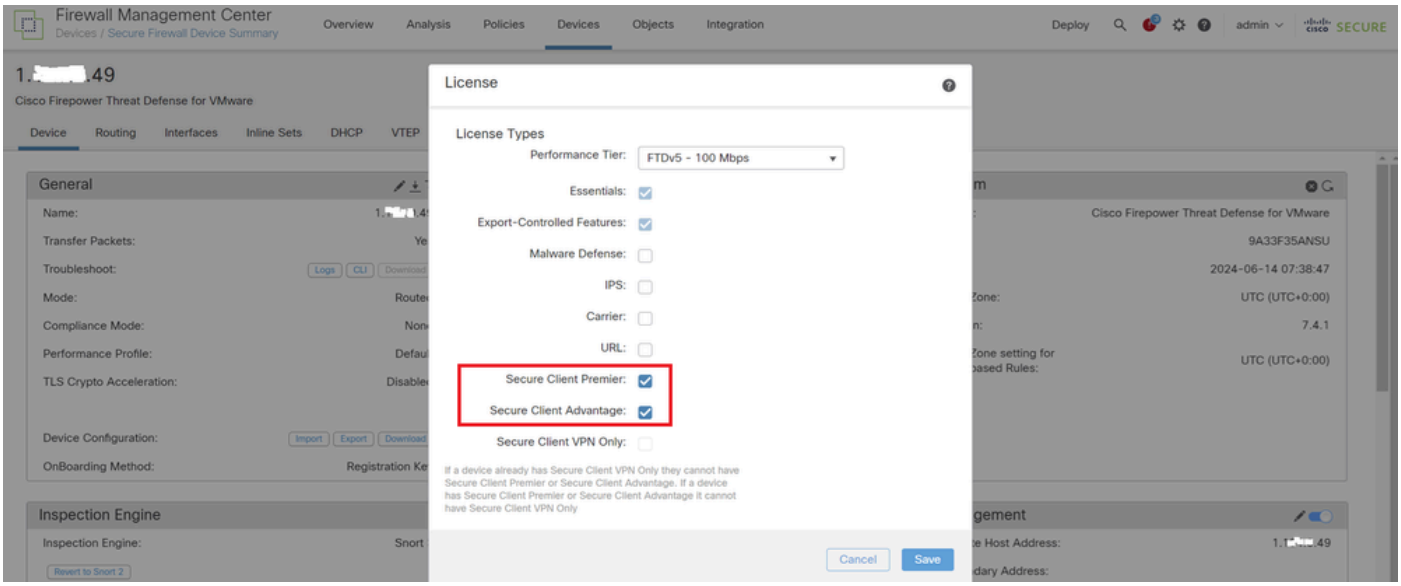
- 名前:inside
- セキュリティゾーン:insideZone
- IPアドレス:192.168.10.200/24




FTDインターフェイス

### ステップ 2：Cisco Secure Clientライセンスの確認

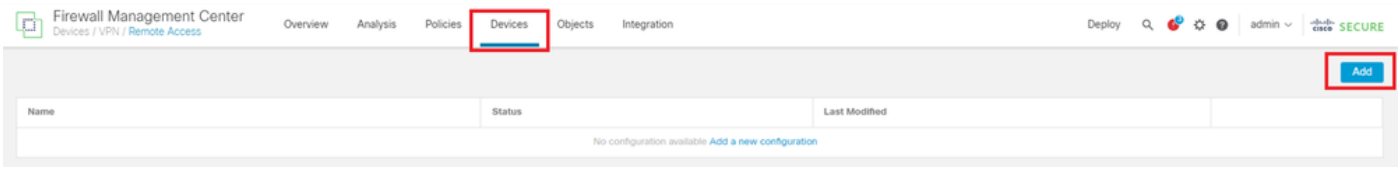
Devices > Device Managementに移動し、ターゲットFTDデバイスを編集し、DeviceタブでCisco Secure Clientライセンスを確認します。




セキュアクライアントライセンス

## ステップ 3：ポリシー割り当ての追加

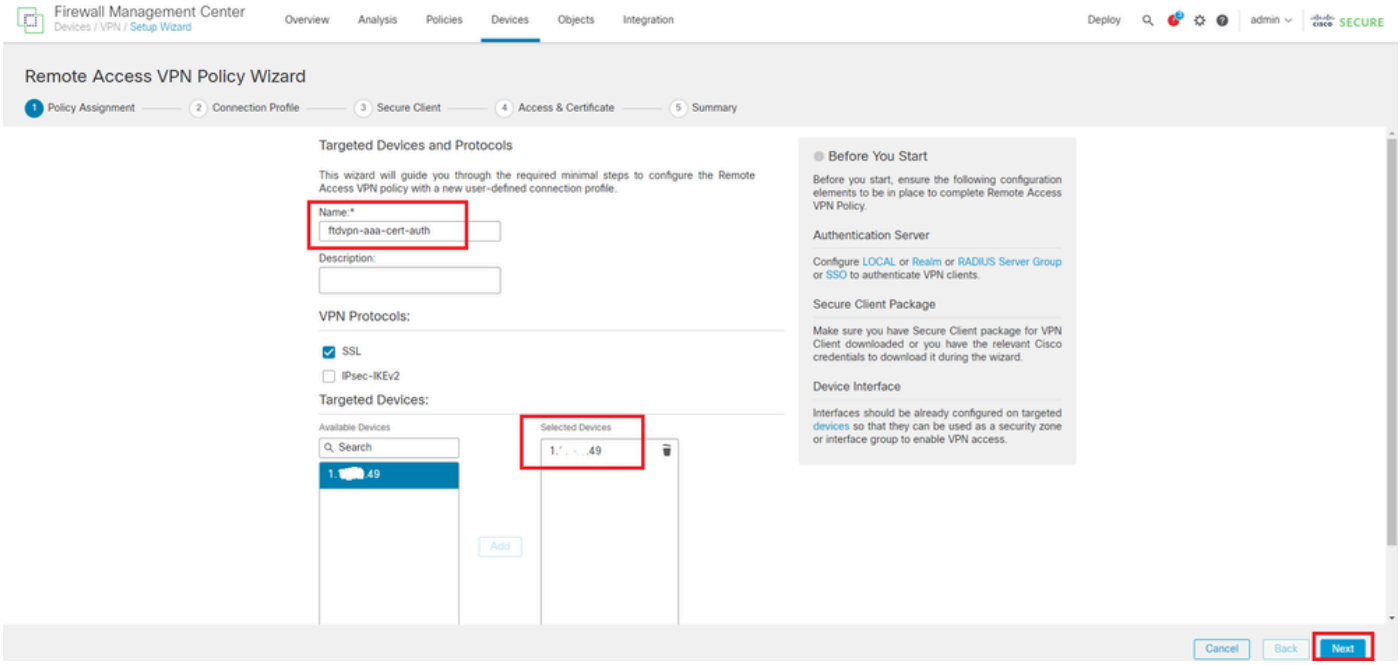
Devices > VPN > Remote Accessの順に移動し、Addボタンをクリックします。




リモートアクセスVPNの追加

必要な情報を入力して、Nextボタンをクリックします。

- 名前:ftdvpn-aaa-cert-auth
- VPNプロトコル:SSL
- ターゲットデバイス:1.x.x.49

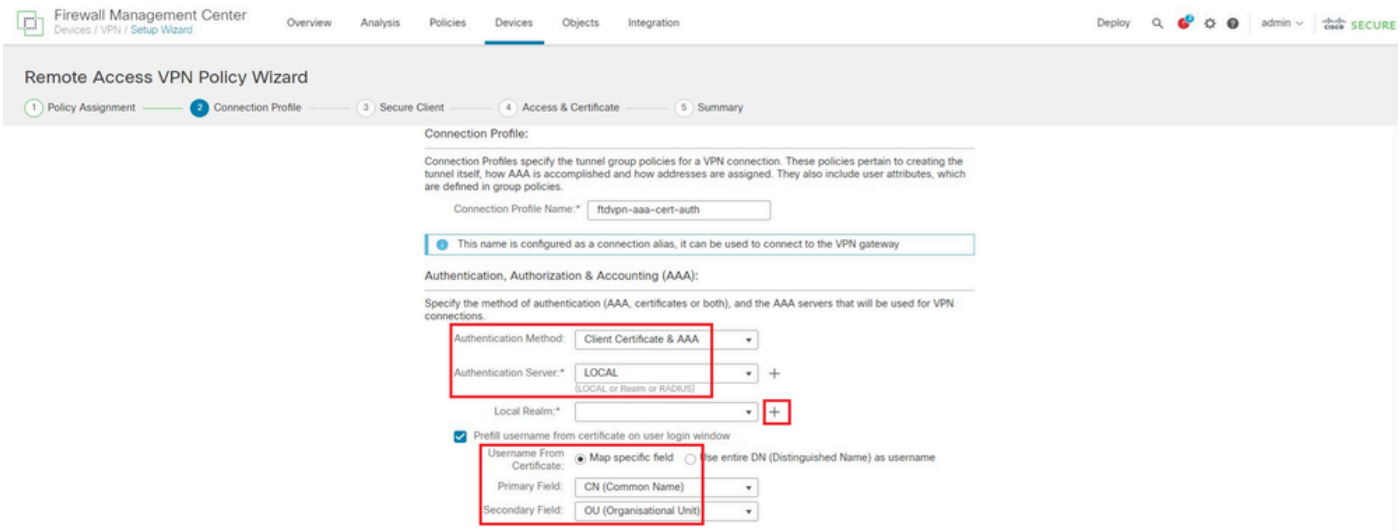



ポリシーの割り当て

## ステップ 4：接続プロファイルの設定の詳細

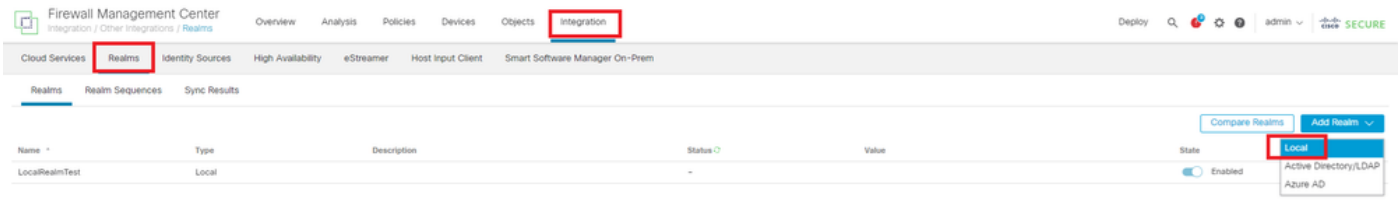
接続プロファイルに必要な情報を入力し、Local Realm項目の横にある+ボタンをクリックします。

- 認証方式：クライアント証明書とAAA
- 認証サーバ:LOCAL
- 証明書からのユーザ名：特定のフィールドのマッピング
- 主フィールド:CN（共通名）
- セカンダリフィールド:OU（組織ユニット）




接続プロファイルの詳細

新しいローカルレルムを追加するには、Add Realmドロップダウンリストから Localをクリックします。

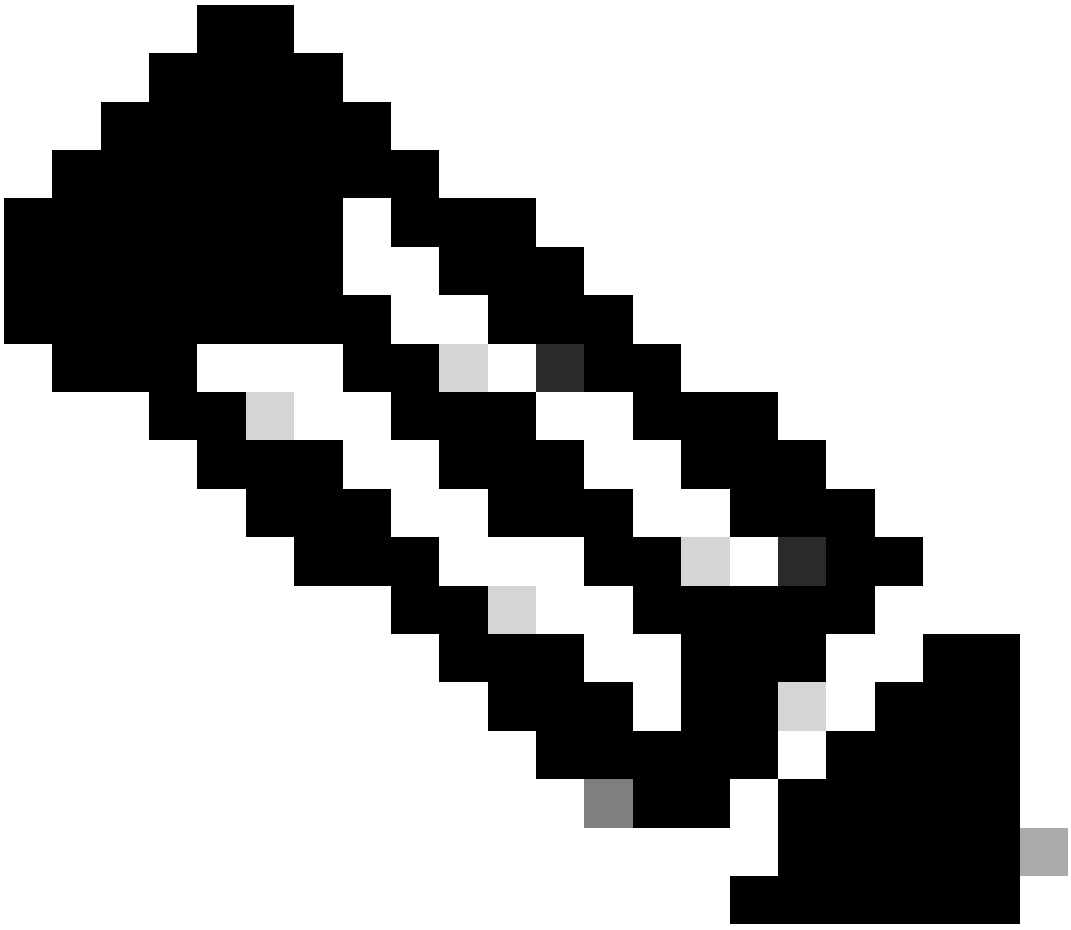



ローカルレルムの追加

ローカルレルムに必要な情報を入力して、Saveボタンをクリックします。

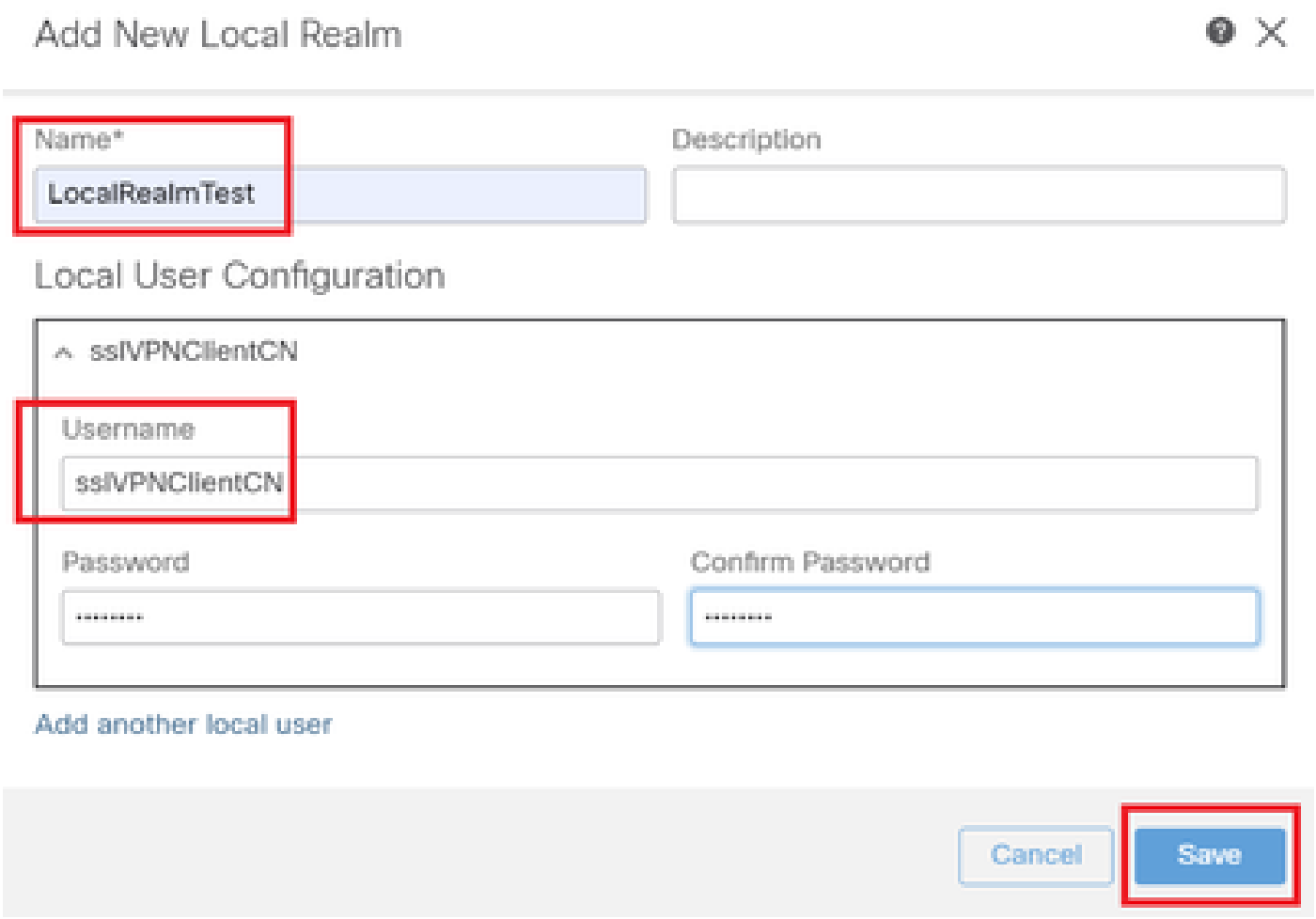
- 名前: LocalRealmTest
- ユーザ名:sslVPNClientCN

---



注:usernameは、クライアント証明書内の共通名です

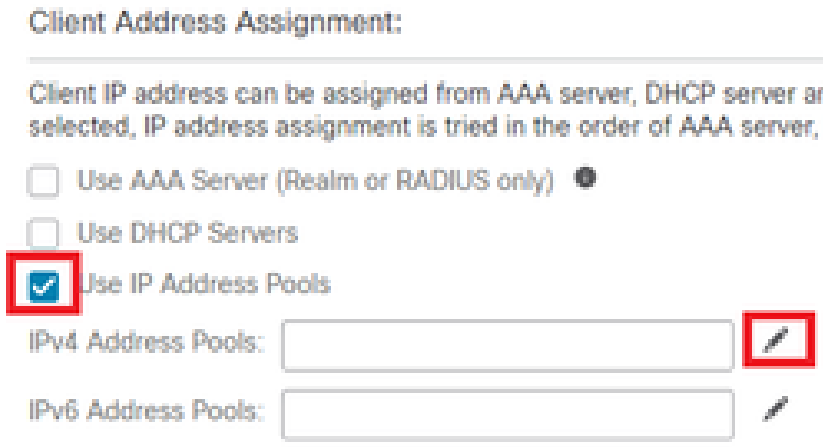
---




ローカルレルムの詳細

ステップ 5：接続プロファイル用のアドレスプールの追加

IPv4 Address Pools項目の横にあるeditボタンをクリックします。

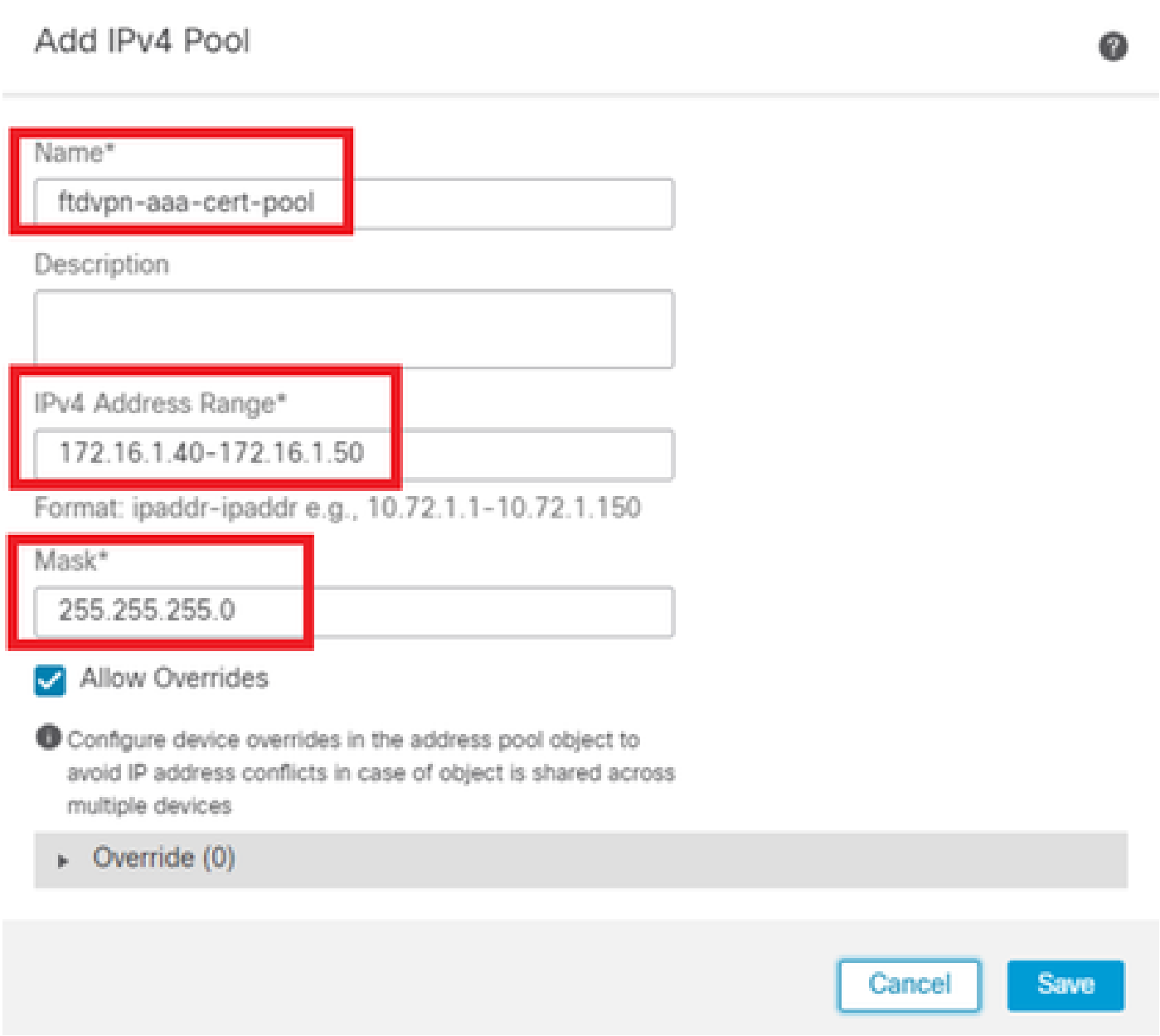



IPv4アドレスプールの追加

新しいIPv4アドレスプールを追加するために必要な情報を入力します。接続プロファイルの新しいIPv4アドレスプールを選択します。

- 名前:ftdvpn-aaa-cert-pool
- IPv4アドレス範囲:172.16.1.40 ~ 172.16.1.50

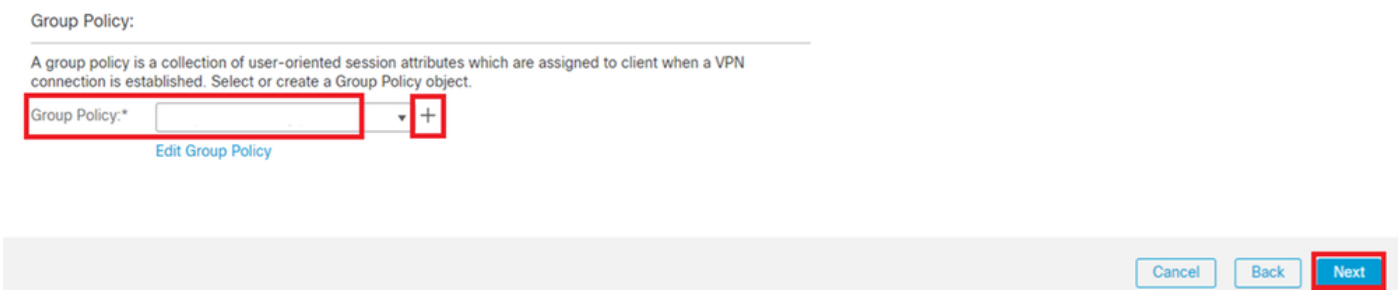
- マスク:255.255.255.0




Ipv4アドレスプールの詳細

手順 6：接続プロファイルのグループポリシーの追加

Group Policy項目の横にある+ボタンをクリックします。

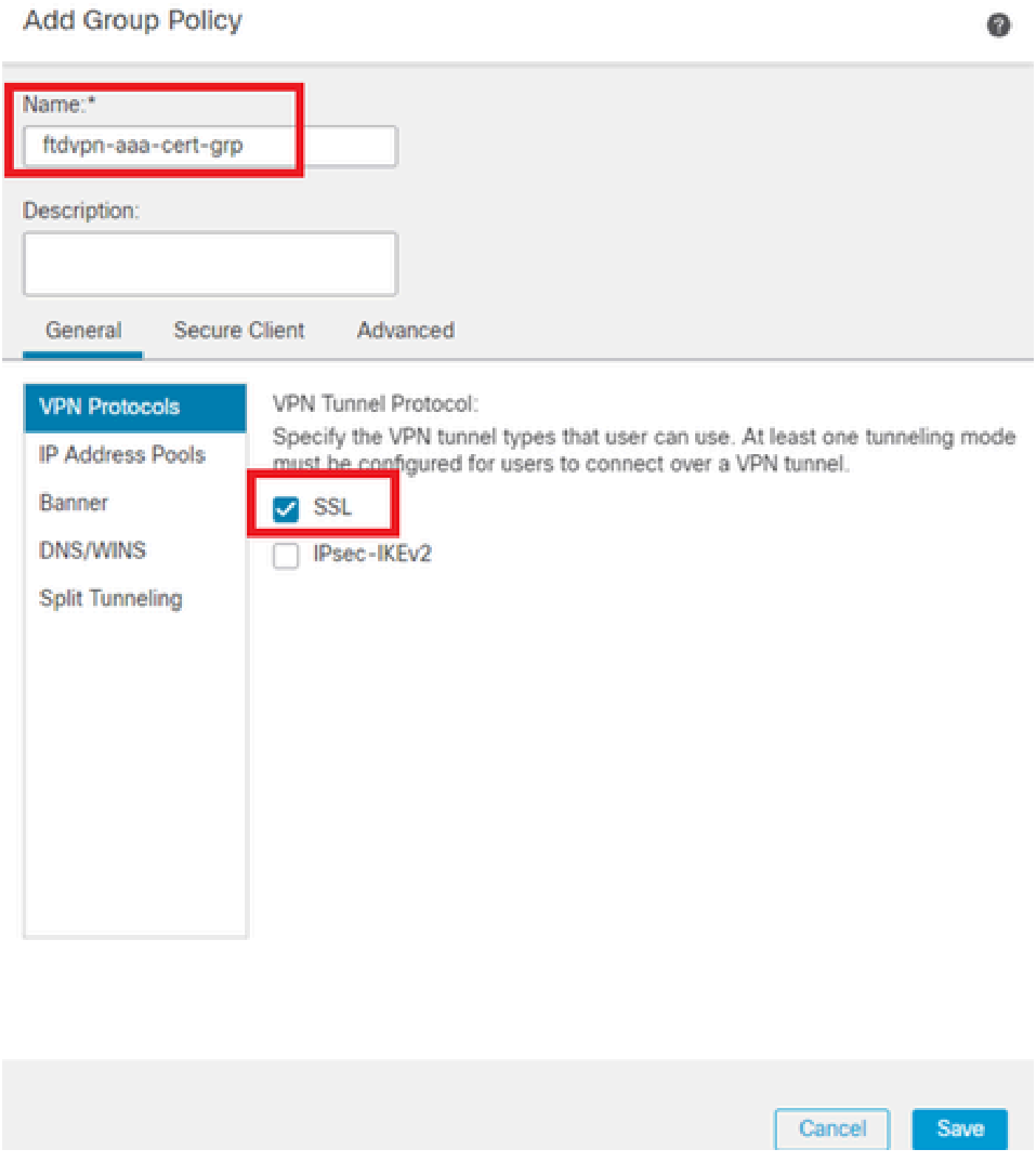



グループポリシーの追加

新しいグループポリシーを追加するために必要な情報を入力します。接続プロファイルの新しい

グループポリシーを選択します。

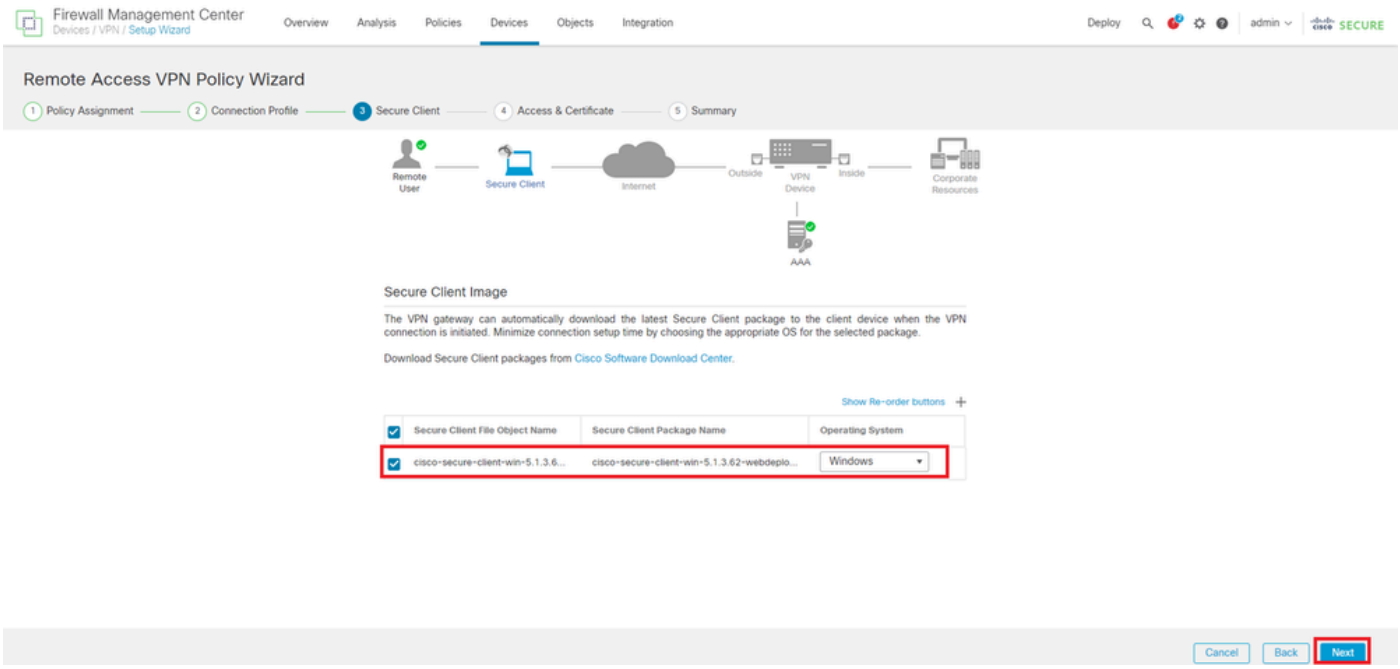
- 名前:ftdvpn-aaa-cert-grp
- VPNプロトコル:SSL




グループポリシーの詳細

手順 7：接続プロファイル用のセキュアクライアントイメージの設定

secure client image fileを選択し、Nextボタンをクリックします。




Secure Client Imageの選択

## ステップ 8：接続プロファイルのアクセスと証明書の設定

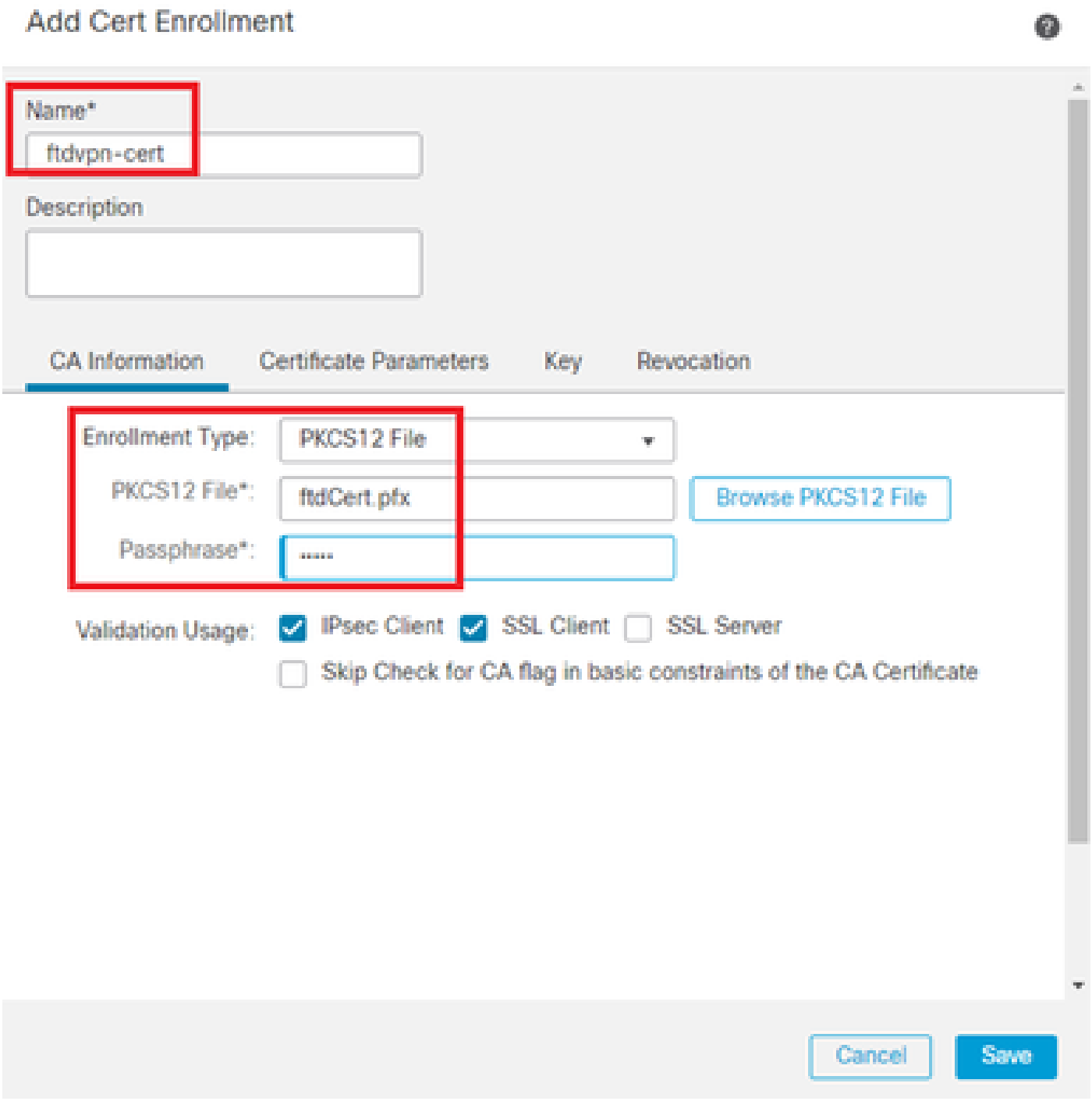
VPN接続にSecurity Zoneを選択し、Certificate Enrollment項目の横にある+ボタンをクリックします。

- インターフェイスグループ/セキュリティゾーン:outsideZone


セキュリティゾーンの選択

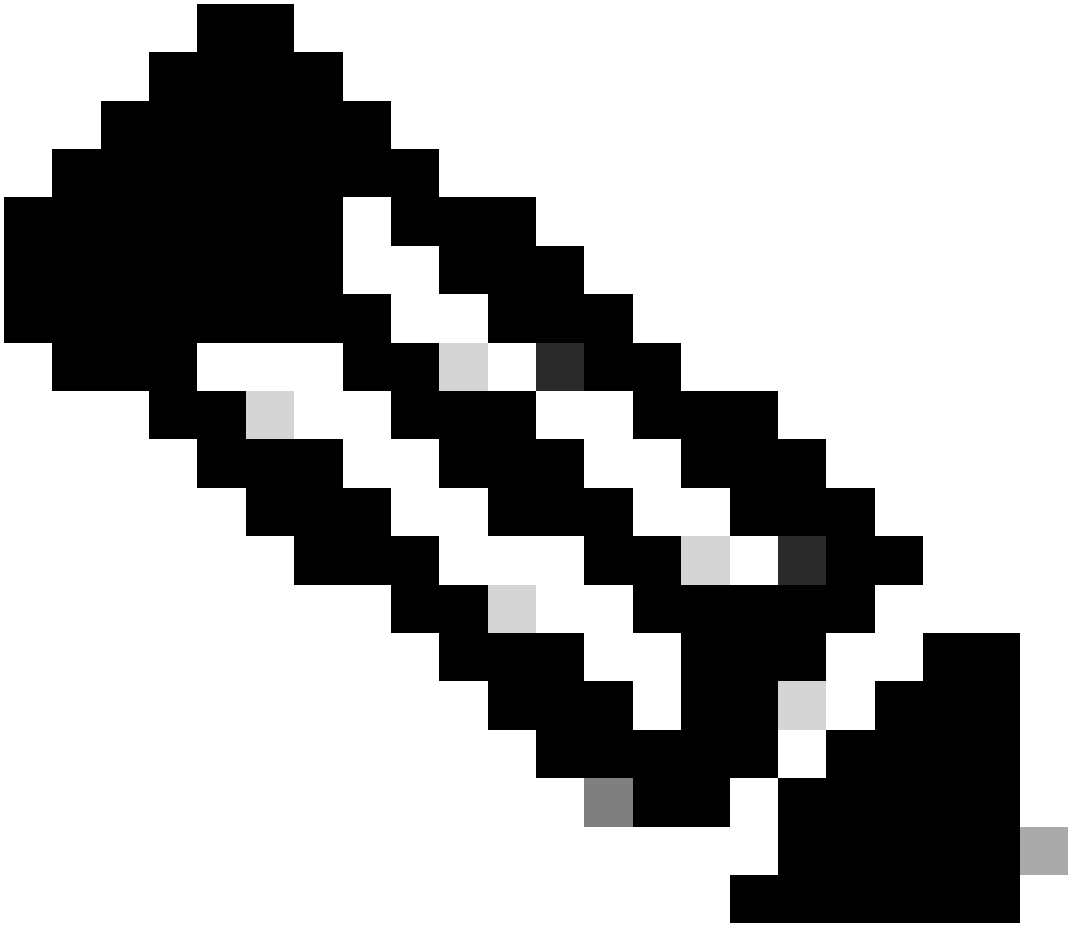
FTD証明書に必要な情報を入力し、ローカルコンピュータからPKCS12ファイルをインポートします。

- 名前:ftdvpn-cert
- 登録タイプ:PKCS12ファイル

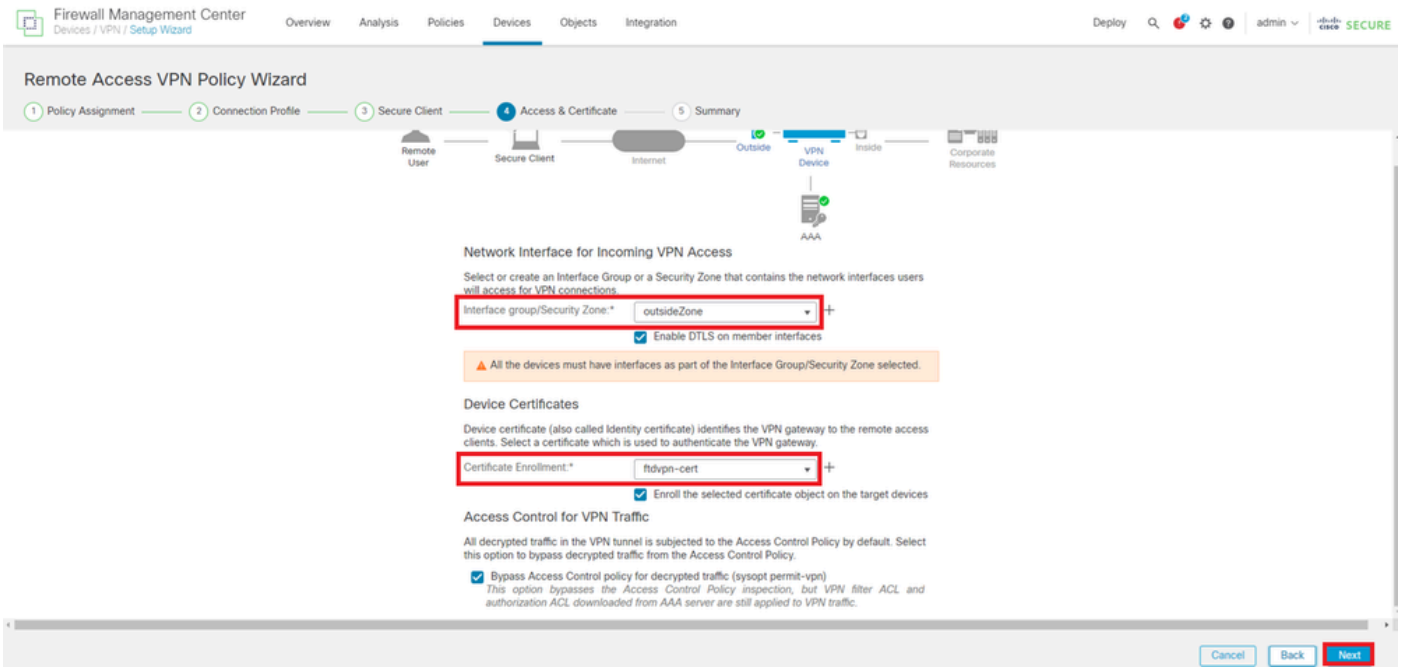



FTD証明書の追加

Access & Certificateウィザードで入力した情報を確認し、Nextボタンをクリックします。



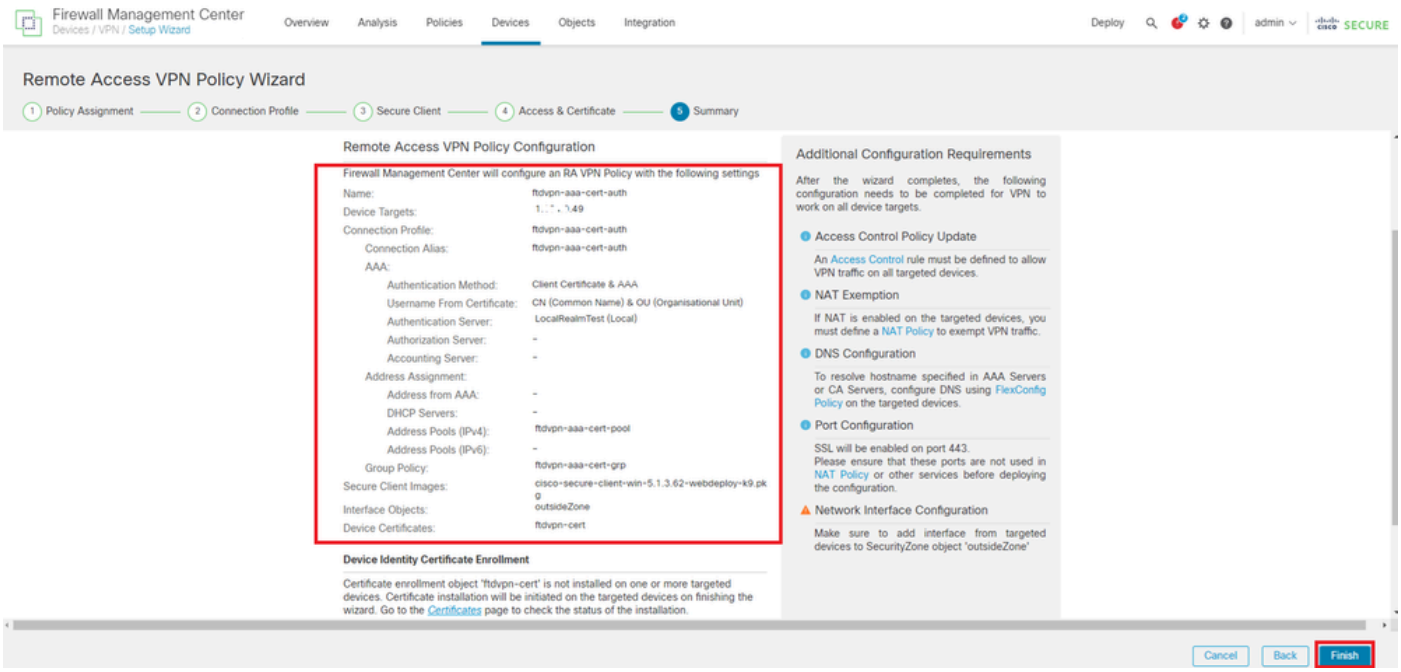
注：復号化されたVPNトラフィックがアクセスコントロールポリシー検査の対象にならないように、復号化されたトラフィックに対してアクセスコントロールポリシーのバイパス(sysopt permit-vpn)をイネーブルにします。




アクセスと証明書の設定の確認

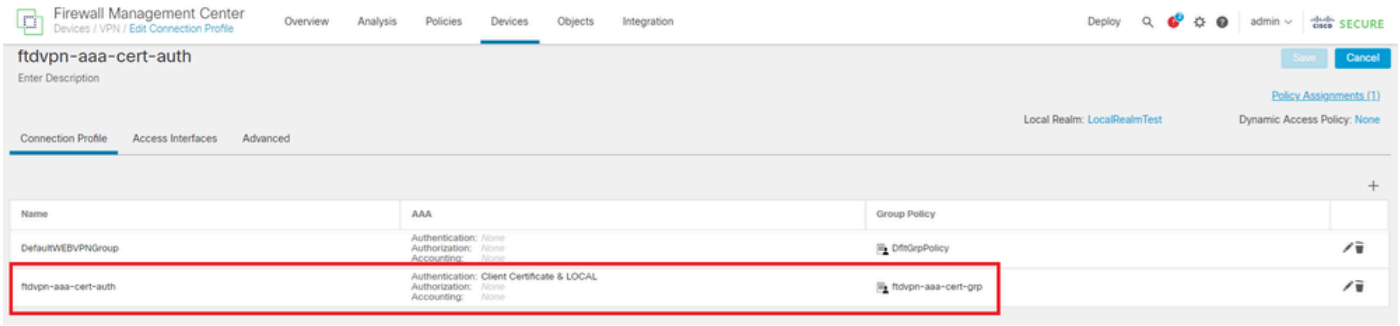
## ステップ 9：接続プロファイルの概要の確認

VPN接続のために入力した情報を確認し、Finishボタンをクリックします。




VPN接続の設定の確認

リモートアクセスVPNポリシーの概要を確認し、設定をFTDに展開します。




リモートアクセスVPNポリシーの概要

## FTD CLIで確認

FMCからの展開後に、FTD CLIでVPN接続設定を確認します。

```
// Defines IP of interface
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 192.168.1.200 255.255.255.0
interface GigabitEthernet0/1
nameif inside
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 mask 255.255.255.0

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

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftdvpn-cert
keypair ftdvpn-cert
crl configure

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

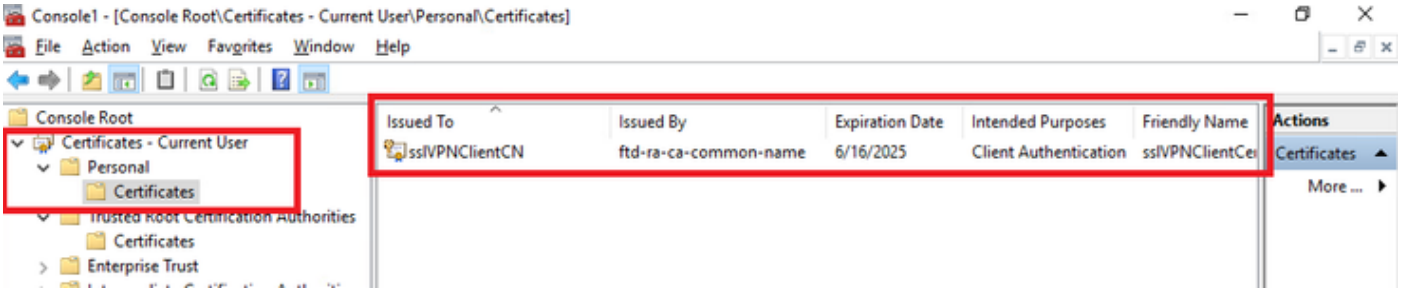
```
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Bypass Access Control policy for decrypted traffic
// This setting is displayed in the 'show run all' command output
sysopt connection permit-vpn

// Configures the group-policy to allow SSL connections
group-policy ftdvpn-aaa-cert-grp internal
group-policy ftdvpn-aaa-cert-grp attributes
banner none
wins-server none
dns-server none
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-tunnel-network-list none
default-domain none
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
vlan none
address-pools none
webvpn
anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface public none
anyconnect firewall-rule client-interface private none
anyconnect ssl keepalive 20
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules value none
anyconnect ask none default anyconnect
anyconnect ssl df-bit-ignore disable

// 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
```

## VPNクライアントでの確認

### ステップ 1：クライアント証明書の確認

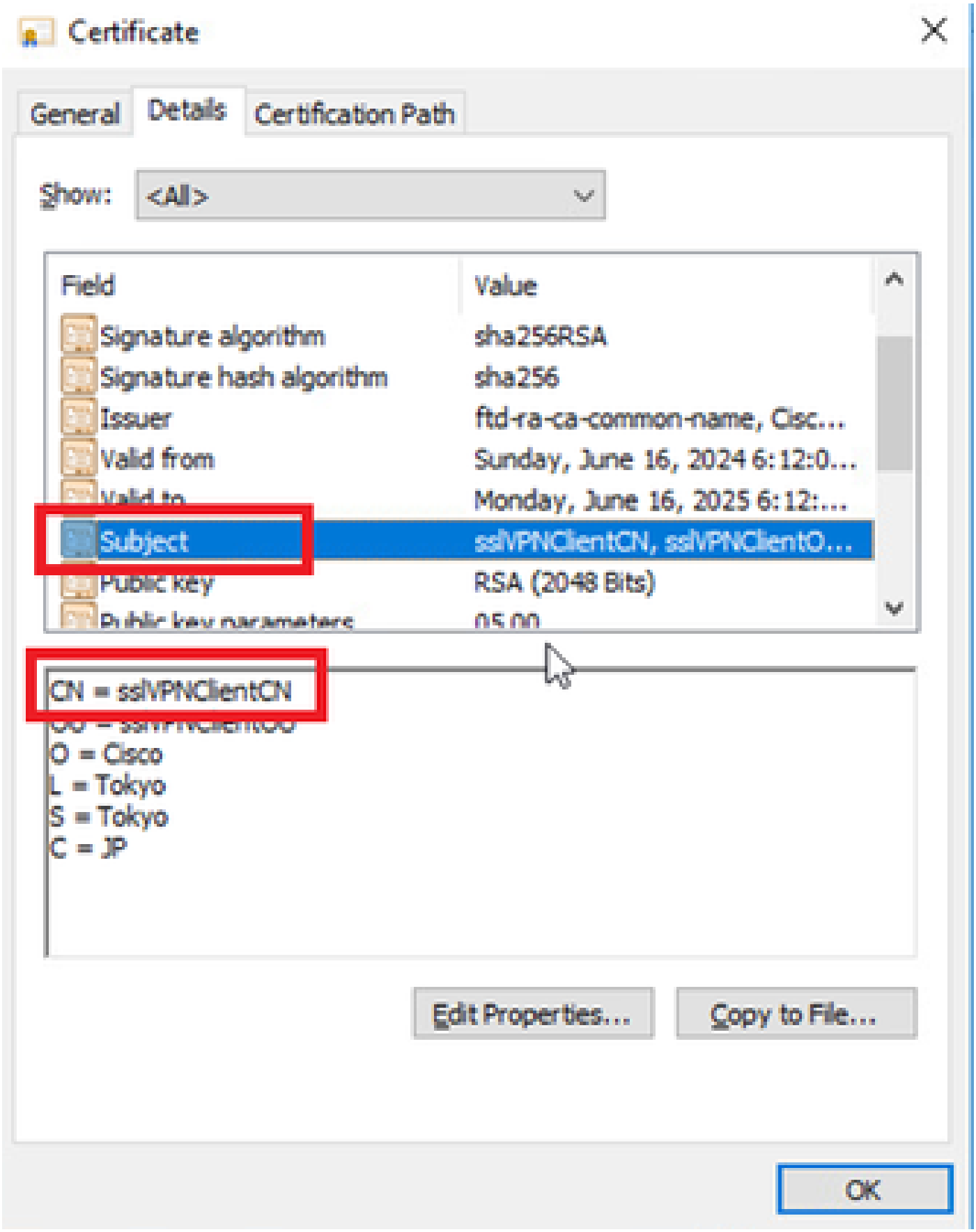
Certificates - Current User > Personal > Certificatesの順に移動し、認証に使用するクライアント証明書を確認します。




クライアント証明書の確認

クライアント証明書をダブルクリックし、Detailsに移動して、Subjectの詳細を確認します。

- 件名:CN = sslVPNClientCN



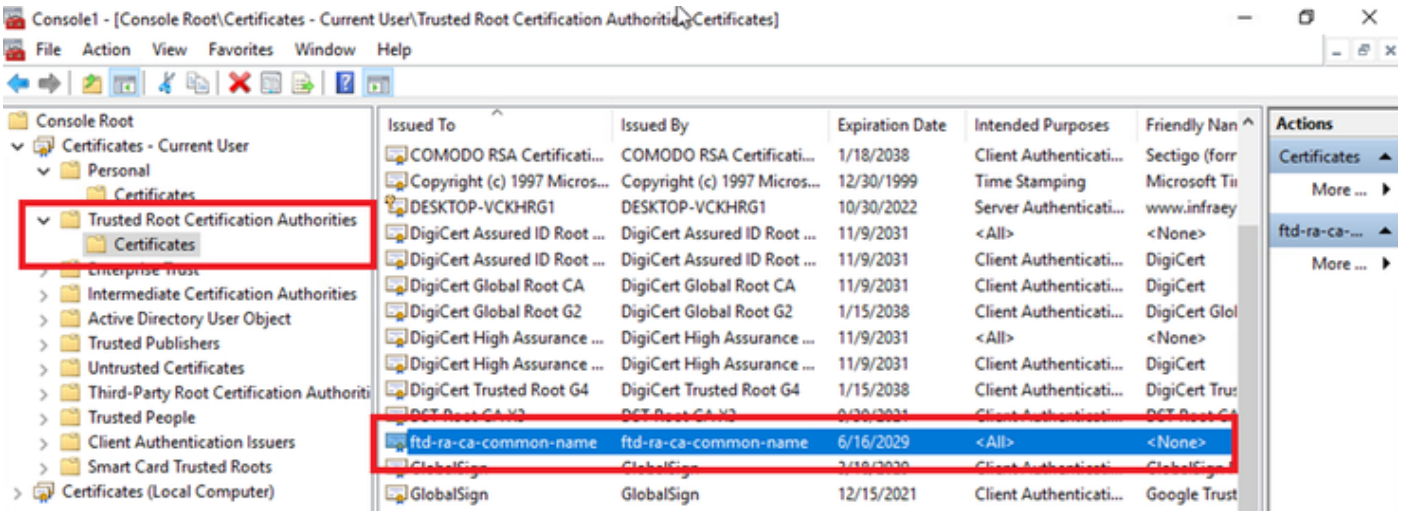

クライアント証明書の詳細

ステップ 2：CAの確認

Certificates - Current User > Trusted Root Certification Authorities > Certificatesの順に移動し、認

証に使用するCAを確認します。

- 発行元:ftd-ra-ca-common-name

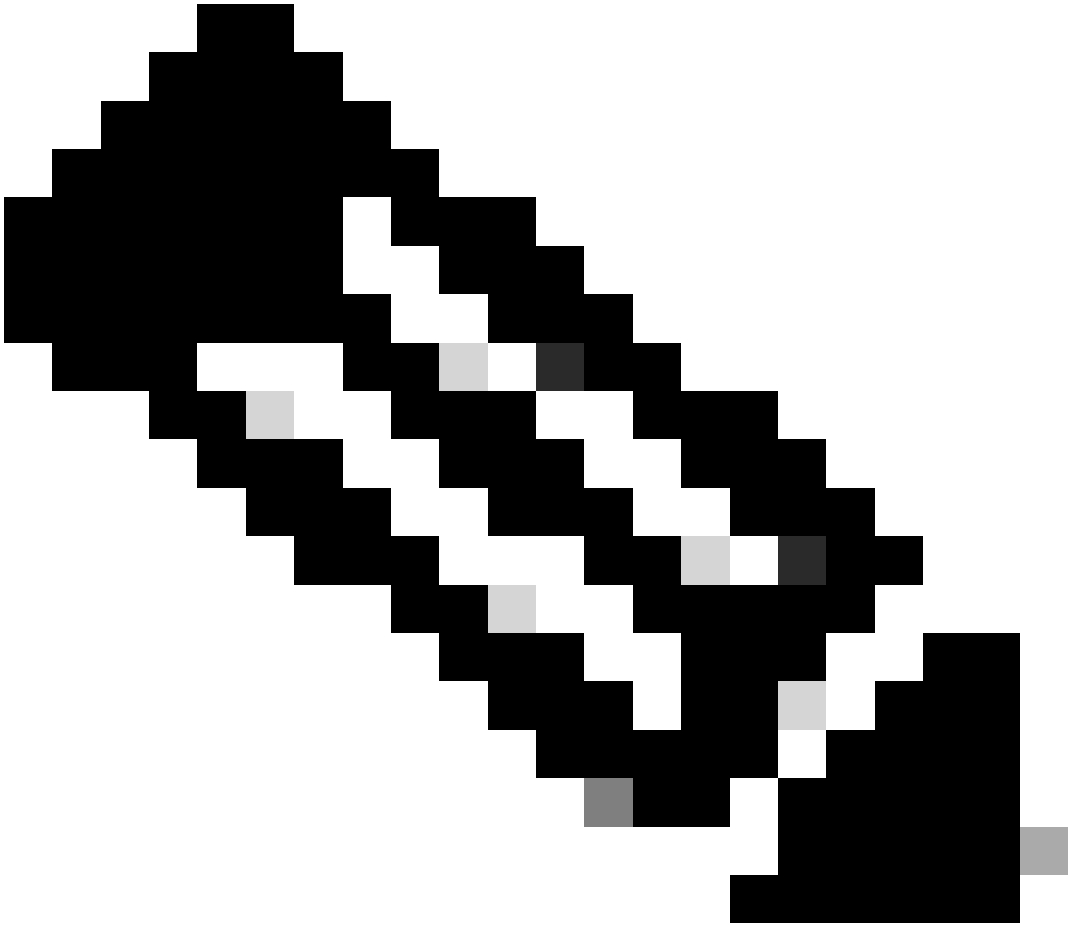



CAの確認

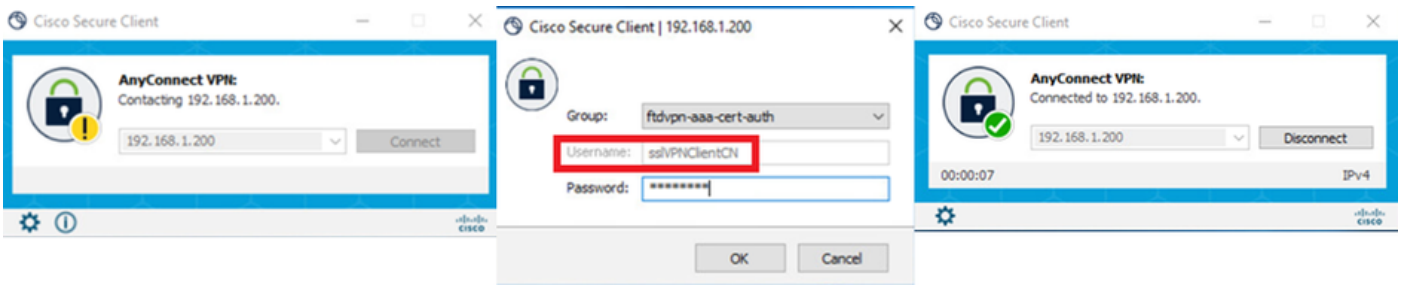
# 確認

ステップ 1：VPN接続の開始

エンドポイントで、Cisco Secure Client接続を開始します。ユーザ名はクライアント証明書から抽出されるため、VPN認証用のパスワードを入力する必要があります。



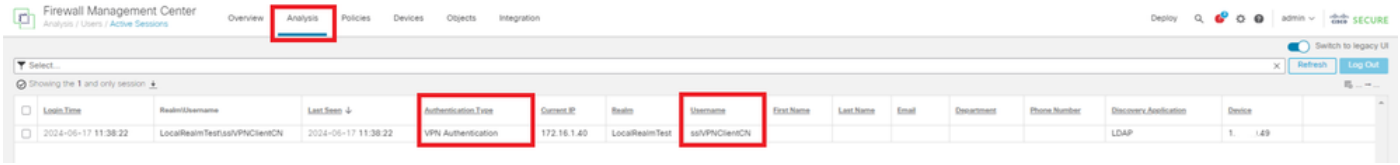
注：ユーザ名は、このドキュメントのクライアント証明書のCN（共通名）フィールドから抽出されたものです。




VPN接続の開始

ステップ 2：FMCでのアクティブセッションの確認

Analysis > Users > Active Sessionsの順に移動し、VPN認証のアクティブセッションを確認します。




アクティブセッションの確認

## ステップ 3：FTD CLIでのVPNセッションの確認

FTD(Lina)CLIでshow vpn-sessiondb detail anyconnectコマンドを実行して、VPNセッションを確認します。

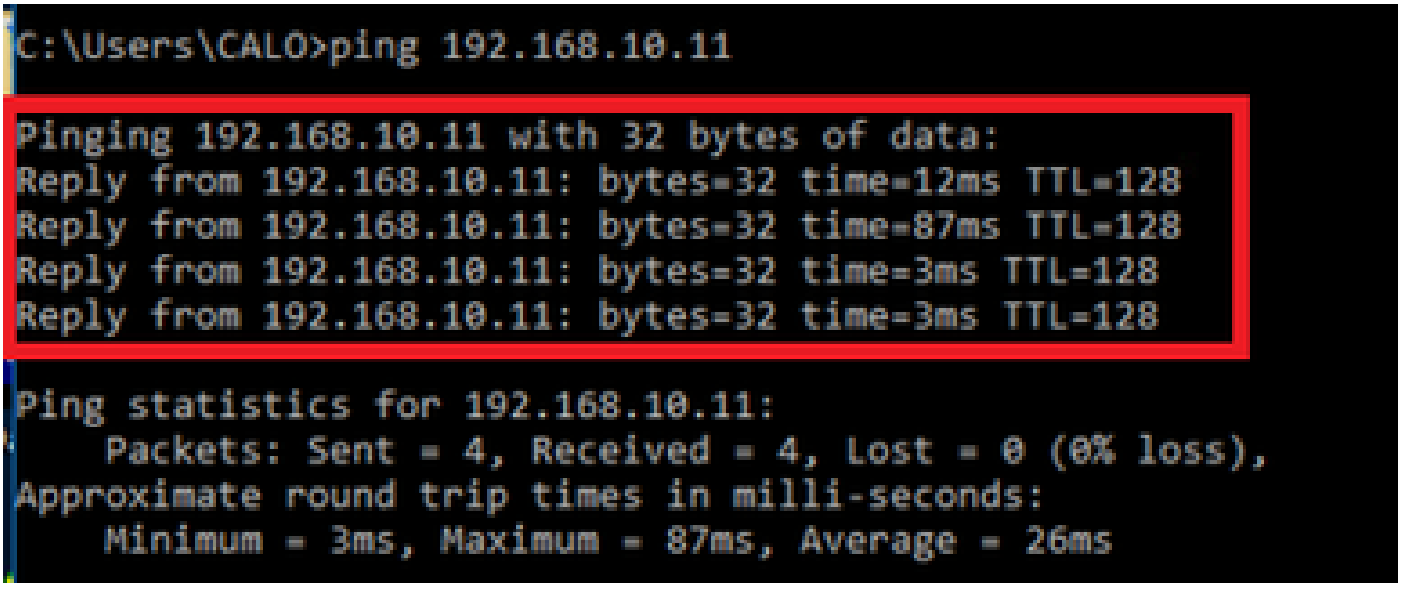
```
ftd702# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : sslVPNClientCN Index : 7
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
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 : 14780 Bytes Rx : 15386
Pkts Tx : 2 Pkts Rx : 37
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth
Login Time : 02:38:22 UTC Mon Jun 17 2024
Duration : 0h:01m:22s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb00718200007000666fa19e
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 7.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50035 TCP Dst Port : 443
Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7390 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 7.2
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-128 Hashing : SHA256
```

Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 50042
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7390 Bytes Rx : 2292
Pkts Tx : 1 Pkts Rx : 3
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 7.3
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 56382
UDP Dst Port : 443 Auth Mode : Certificate and 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 5.1.3.62
Bytes Tx : 0 Bytes Rx : 13094
Pkts Tx : 0 Pkts Rx : 34
Pkts Tx Drop : 0 Pkts Rx Drop : 0

ステップ 4：サーバとの通信の確認

VPNクライアントからサーバへのpingを開始し、VPNクライアントとサーバ間の通信が成功することを確認します。




*ping*に成功

パケットキャプチャを確認するには、FTD(Lina)CLIでcapture in interface inside real-timeコマンドを実行します。

ftd702#

**capture in interface inside real-time**

```
Use ctrl-c to terminate real-time capture

1: 03:39:25.729881 172.16.1.40 > 192.168.10.11 icmp: echo request
2: 03:39:25.730766 192.168.10.11 > 172.16.1.40 icmp: echo reply
3: 03:39:26.816211 172.16.1.40 > 192.168.10.11 icmp: echo request
4: 03:39:26.818683 192.168.10.11 > 172.16.1.40 icmp: echo reply
5: 03:39:27.791676 172.16.1.40 > 192.168.10.11 icmp: echo request
6: 03:39:27.792195 192.168.10.11 > 172.16.1.40 icmp: echo reply
7: 03:39:28.807789 172.16.1.40 > 192.168.10.11 icmp: echo request
8: 03:39:28.808399 192.168.10.11 > 172.16.1.40 icmp: echo reply
```

## トラブルシュート

VPN認証に関する情報は、Linaエンジンのdebug syslogおよびWindows PCのDARTファイルに記載されています。

次に、Linaエンジンのデバッグログの例を示します。

```
// Certificate Authentication
Jun 17 2024 02:38:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=sslV
Jun 17 2024 02:38:03: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked.
Jun 17 2024 02:38:03: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name:  CN=sslVPNClientCl

// Extract username from the CN (Common Name) field
Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has been requested.  [Request 5]
Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has completed.  [Request 5]

// AAA Authentication
Jun 17 2024 02:38:22: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN
Jun 17 2024 02:38:22: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN
Jun 17 2024 02:38:22: %FTD-6-113008: AAA transaction status ACCEPT : user = sslVPNClientCN
```

これらのデバッグは、設定のトラブルシューティングに使用できる情報を提供するFTDの診断CLIから実行できます。

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

## 参考

FTDでのAnyConnectリモートアクセスVPNの設定

モバイルアクセス用のAnyconnect証明書ベース認証の設定

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。