FDMを介したFTDでのセキュア・クライアント認証のための証明書照合の構成

内容

はじめに

このドキュメントでは、認証に証明書照合を使用して、FDMを介してFTD上でSSLを使用するCisco Secure Client(CSC)を設定する方法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 Device Manager(FDM)仮想
- ファイアウォール脅威対策(FTD)仮想
- VPN認証のフロー

使用するコンポーネント

- Cisco Firepower Device Manager(FDM)仮想7.2.8
- シスコファイアウォール脅威対策の仮想7.2.8

- Cisco Secureクライアント5.1.4.74
- プロファイルエディタ(Windows) 5.1.4.74

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

CertificateMatchは、管理者がVPNサーバとの認証用のクライアント証明書を選択するために使用する必要がある基準を設定できるようにする機能です。この設定はクライアントプロファイルで指定されます。クライアントプロファイルは、プロファイルエディタを使用して管理するか、手動で編集できるXMLファイルです。CertificateMatch機能を使用すると、特定の属性を持つ証明書のみがVPN接続に使用されるようにすることで、VPN接続のセキュリティを強化できます。

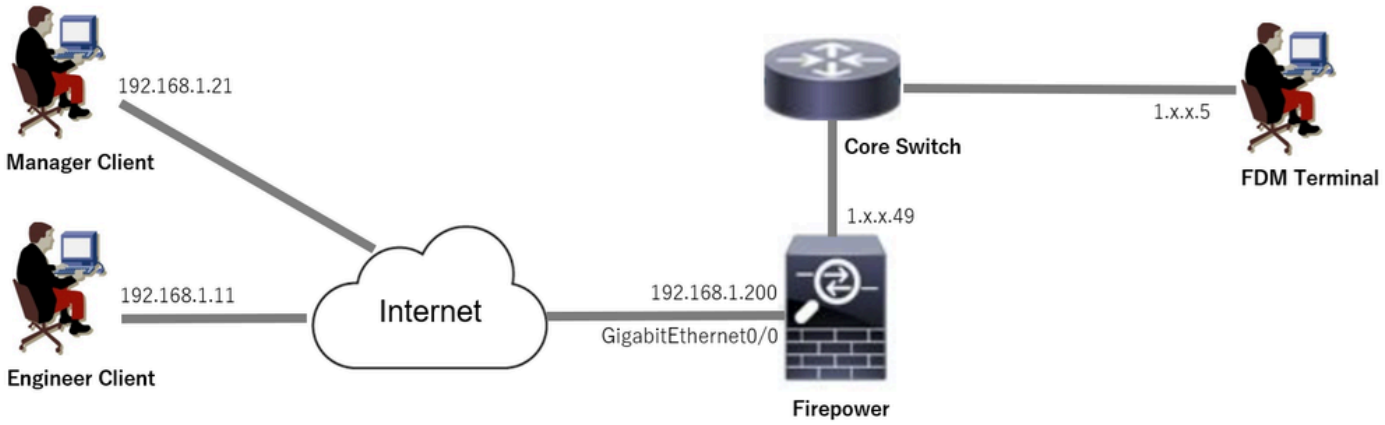
このドキュメントでは、SSL証明書の共通名を使用してCisco Secure Client(CSA)を認証する方法について説明します。

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
- エンジニアVPNクライアント証明書：vpnEngineerClientCN
- マネージャVPNクライアント証明書：vpnManagerClientCN
- 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

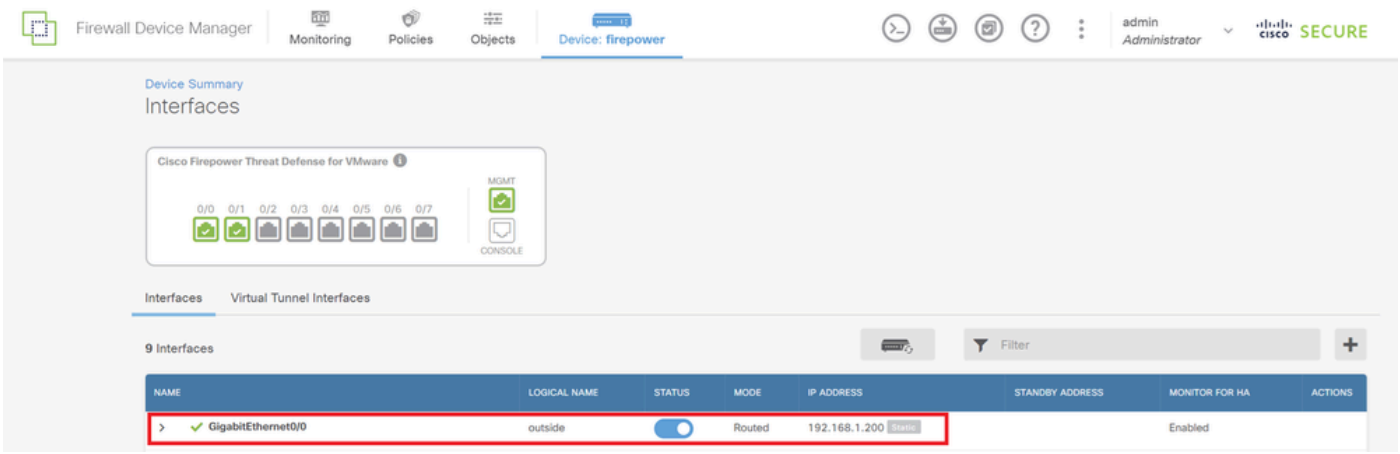
FDMでの構成

ステップ 1：FTDインターフェイスの設定

Device > Interfaces > View All Interfacesの順に移動し、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、

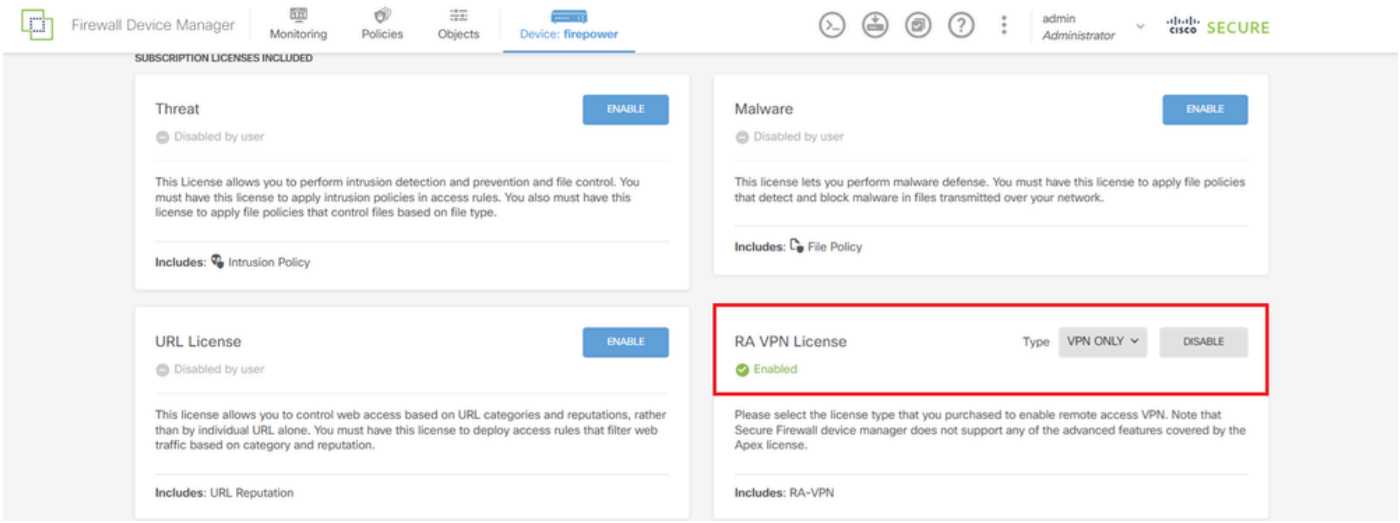
- 名前：outside
- IPアドレス：192.168.1.200/24



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

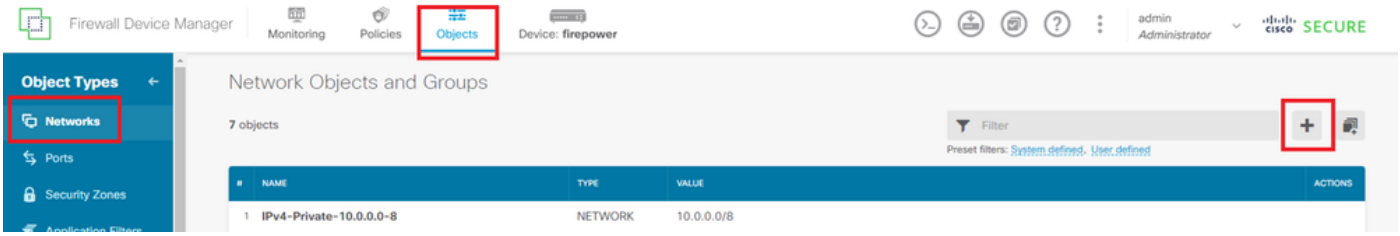
Device > Smart License > View Configurationの順に移動し、RA VPN License項目のCisco Secure Clientライセンスを確認します。



セキュアクライアントライセンス

ステップ 3：アドレスプールの追加

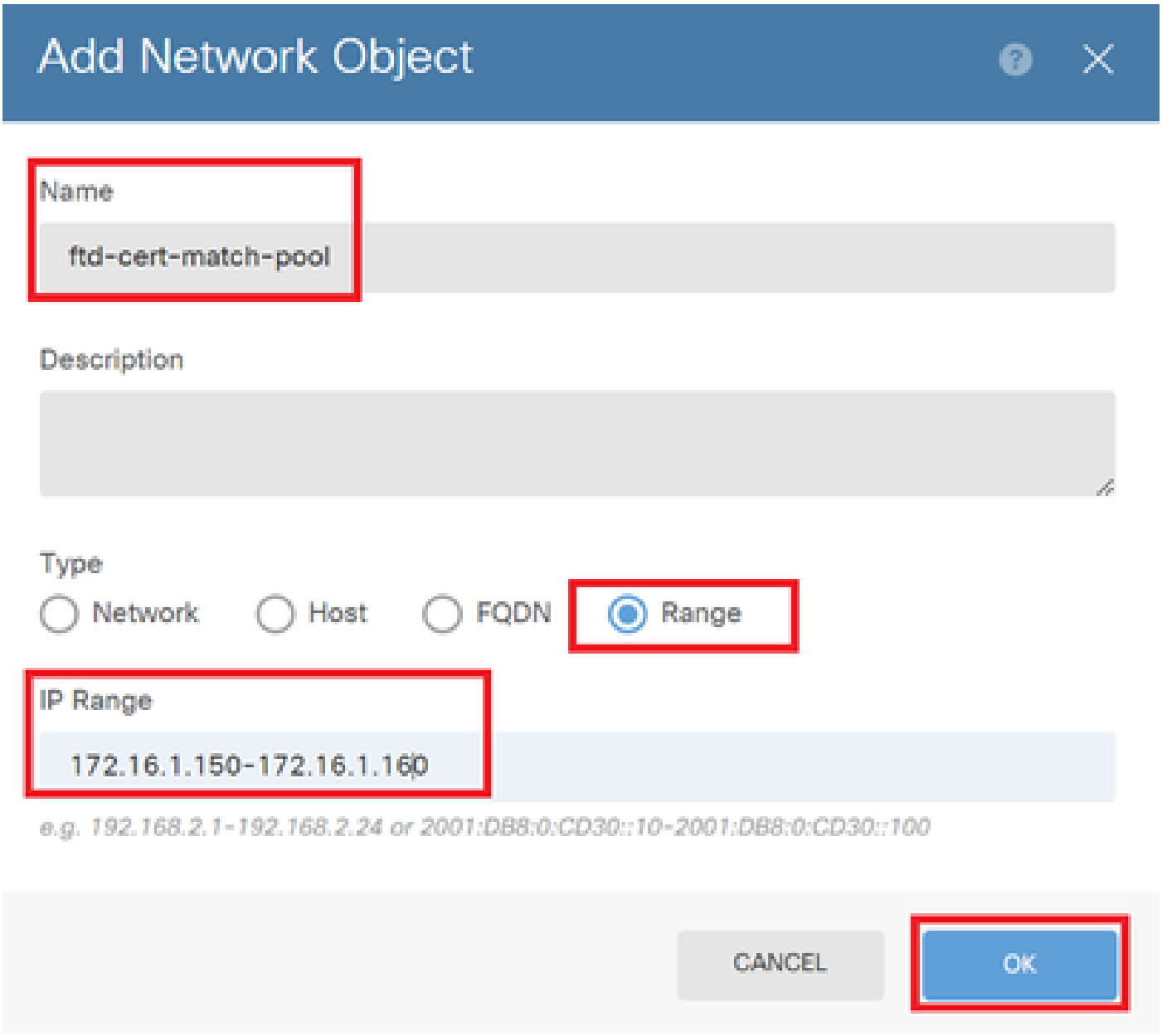
Objects > Networksに移動し、+ボタンをクリックします。



アドレスプールの追加

必要な情報を入力して新しいIPv4アドレスプールを追加します。OKボタンをクリックします。

- 名前：ftd-cert-match-pool
- タイプ：範囲
- IP範囲：172.16.1.150 ~ 172.16.1.160

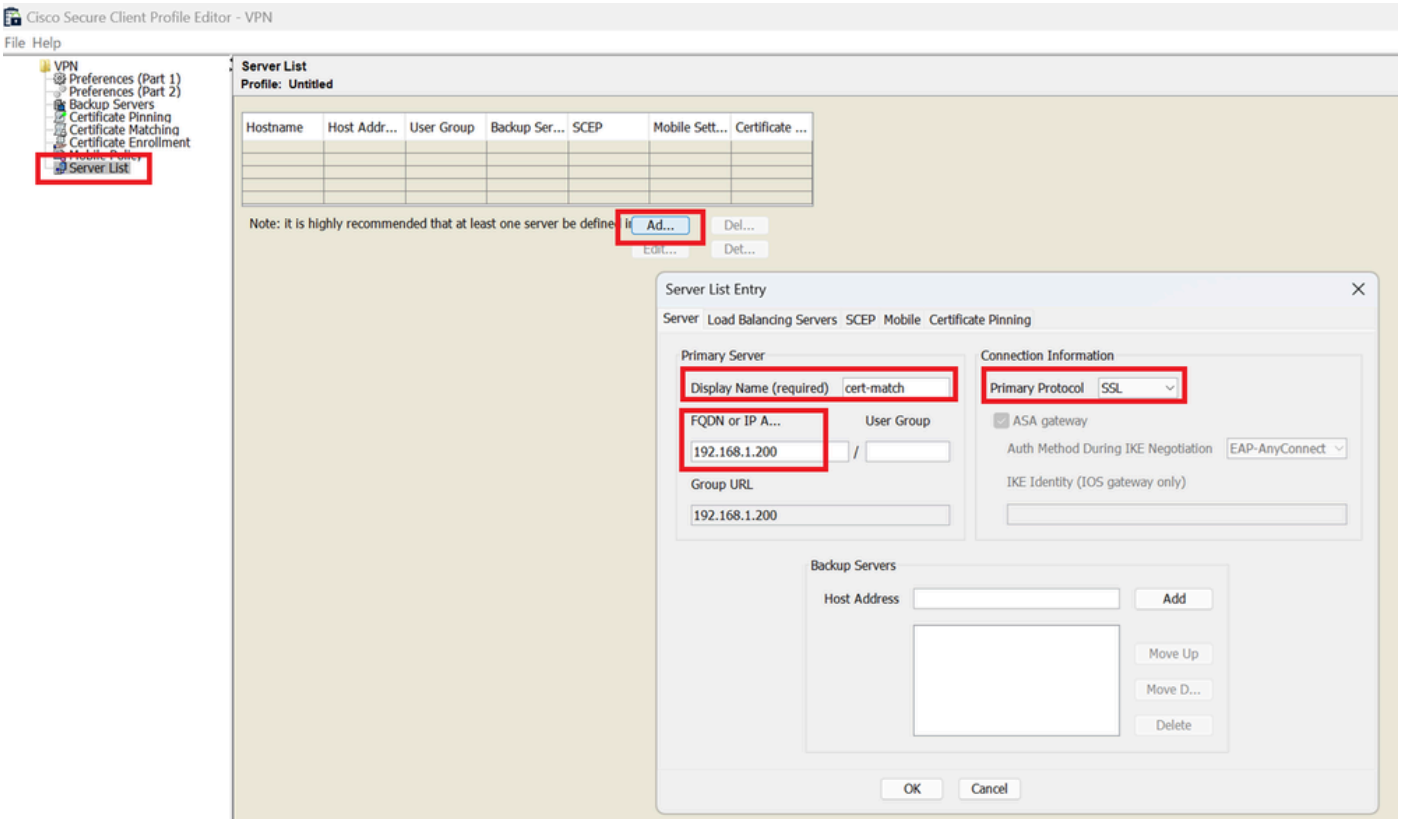


Ipv4アドレスプールの詳細

ステップ 4：セキュアクライアントプロファイルの作成

Secure Client Profile EditorをCiscoソフトウェアサイトからダウンロードしてインストールします。 Server Listに移動し、Addボタンをクリックします。 必要な情報を入力してServer List Entryを追加し、OKボタンをクリックします。

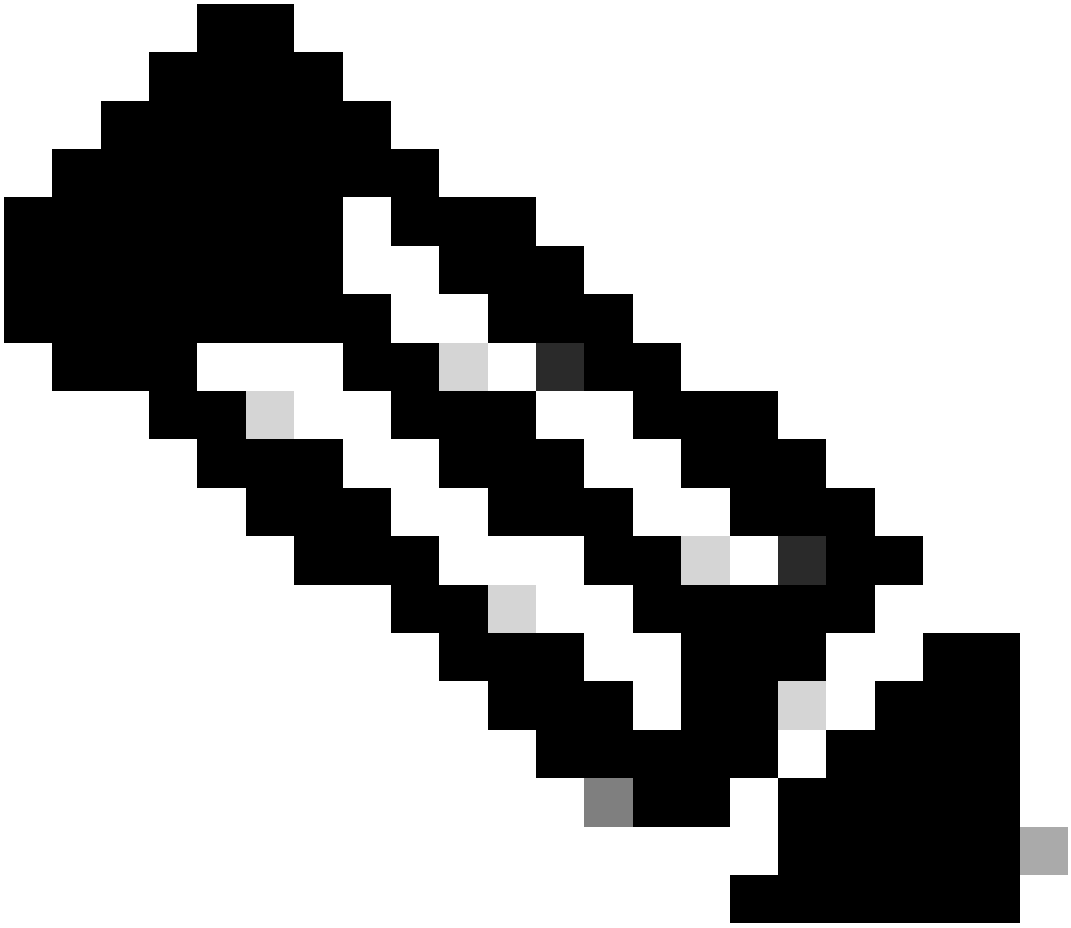
- 表示名：cert-match
- FQDNまたはIPアドレス：192.168.1.200
- プライマリプロトコル：SSL



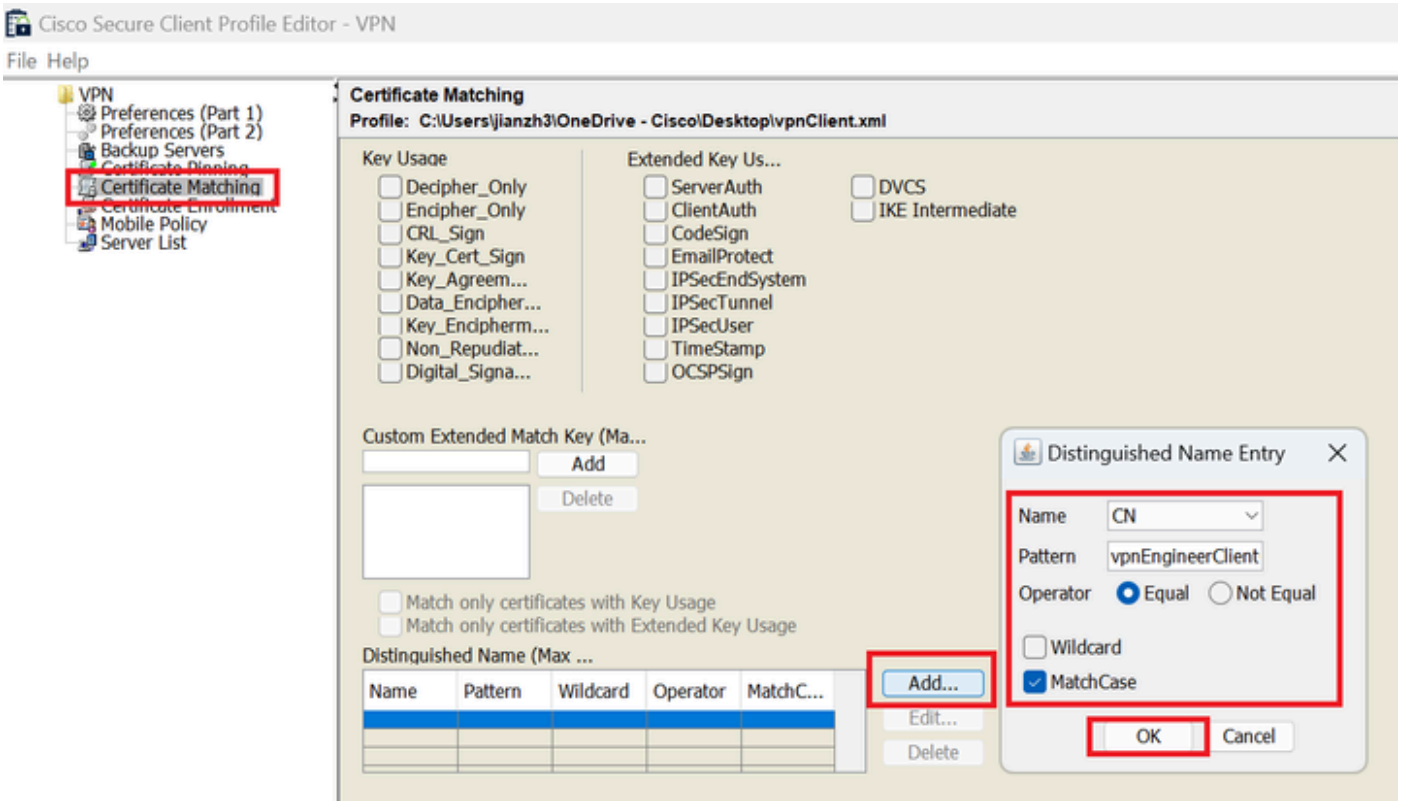
サーバリストエントリ

Certificate Matchingに移動し、Addボタンをクリックします。 必要な情報を入力して識別名エントリを追加し、OKボタンをクリックします。

- 名前：CN
- パターン：vpnEngineerClientCN
- 演算子：等しい



注：このドキュメントの「MatchCase」オプションをチェックしてください。



識別名エントリ

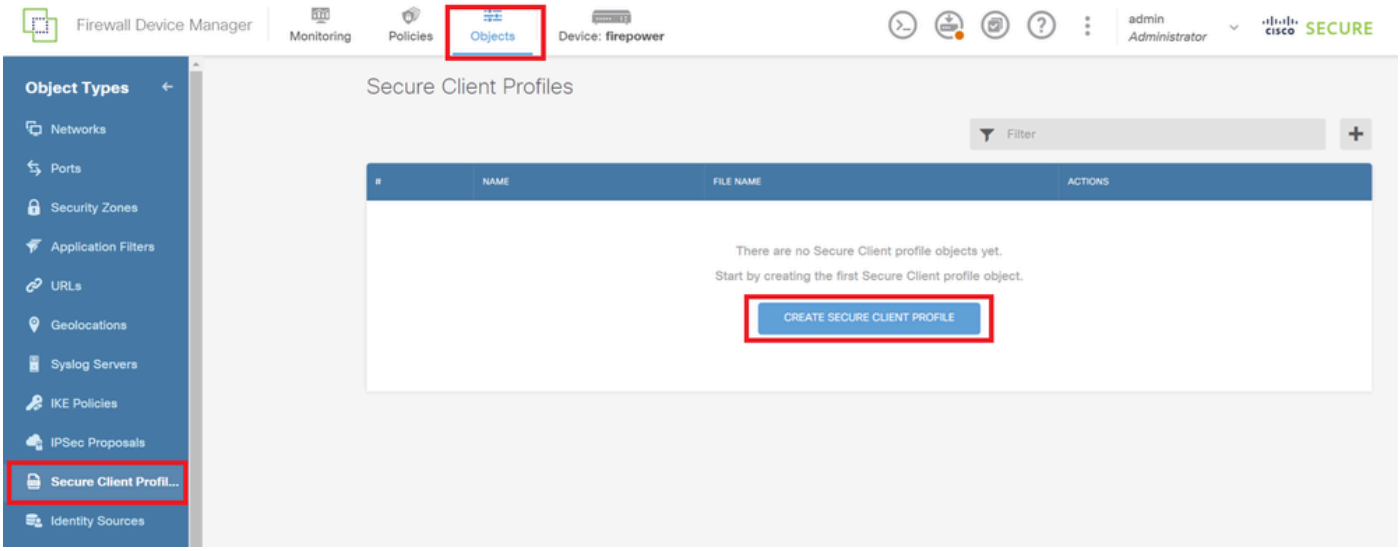
セキュアクライアントプロファイルをローカルコンピュータに保存し、プロファイルの詳細を確認します。

```
▼<CertificateMatch>
  <MatchOnlyCertsWithKU>false</MatchOnlyCertsWithKU>
  ▼<DistinguishedName>
    ▼<DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled" MatchCase="Enabled">
      <Name>CN</Name>
      <Pattern>vpnEngineerClientCN</Pattern>
    </DistinguishedNameDefinition>
  </DistinguishedName>
</CertificateMatch>
▼<EnableAutomaticServerSelection UserControllable="false">
  false
  <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
  <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false </RetainVpnOnLogoff>
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
▼<ServerList>
  ▼<HostEntry>
    <HostName>cert-match</HostName>
    <HostAddress>192.168.1.200</HostAddress>
  </HostEntry>
</ServerList>
</AnyConnectProfile>
```

セキュアなクライアントプロファイル

ステップ 5：FDMへのセキュア・クライアント・プロファイルのアップロード

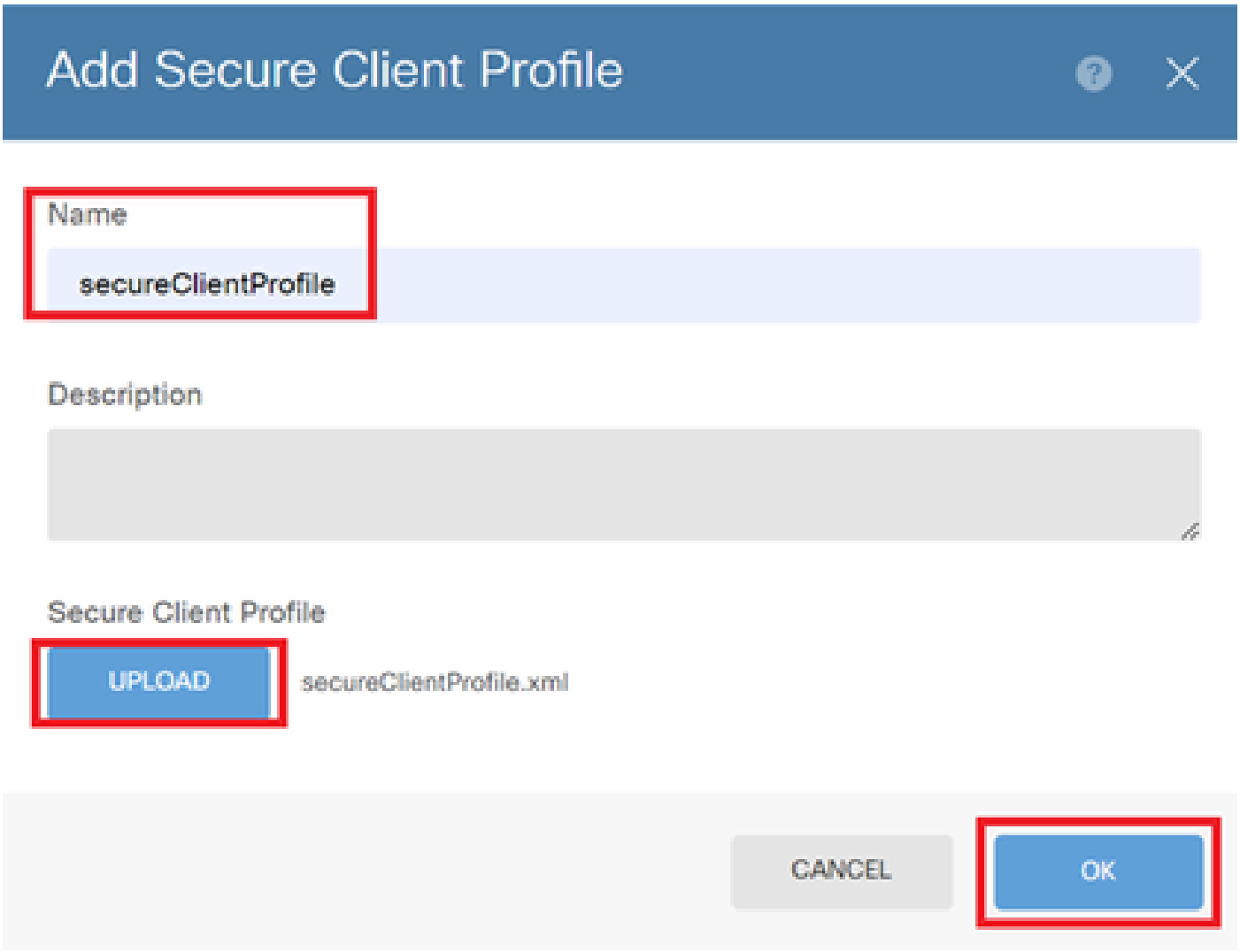
Objects > Secure Client Profileの順に移動し、CREATE SECURE CLIENT PROFILEボタンをクリックします。



セキュアクライアントプロファイルの作成

必要な情報を入力してセキュアなクライアントプロファイルを追加し、OKボタンをクリックします。

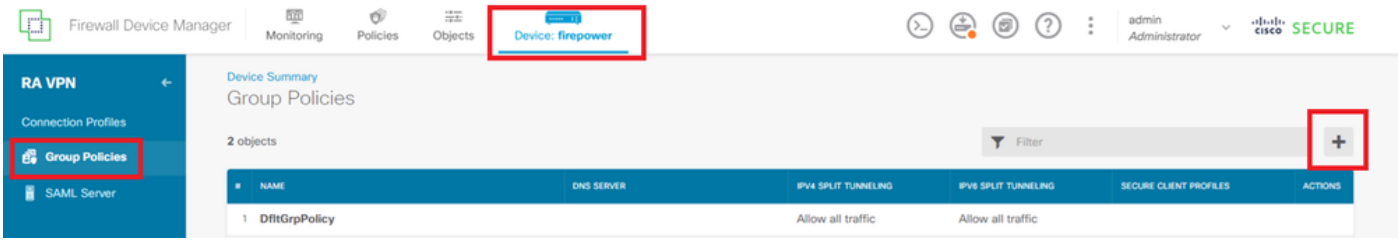
- 名前： secureClientProfile
- セキュアクライアントプロファイル：secureClientProfile.xml (ローカルコンピュータからのアップロード)



セキュアクライアントプロファイルの追加

手順 6：グループポリシーの追加

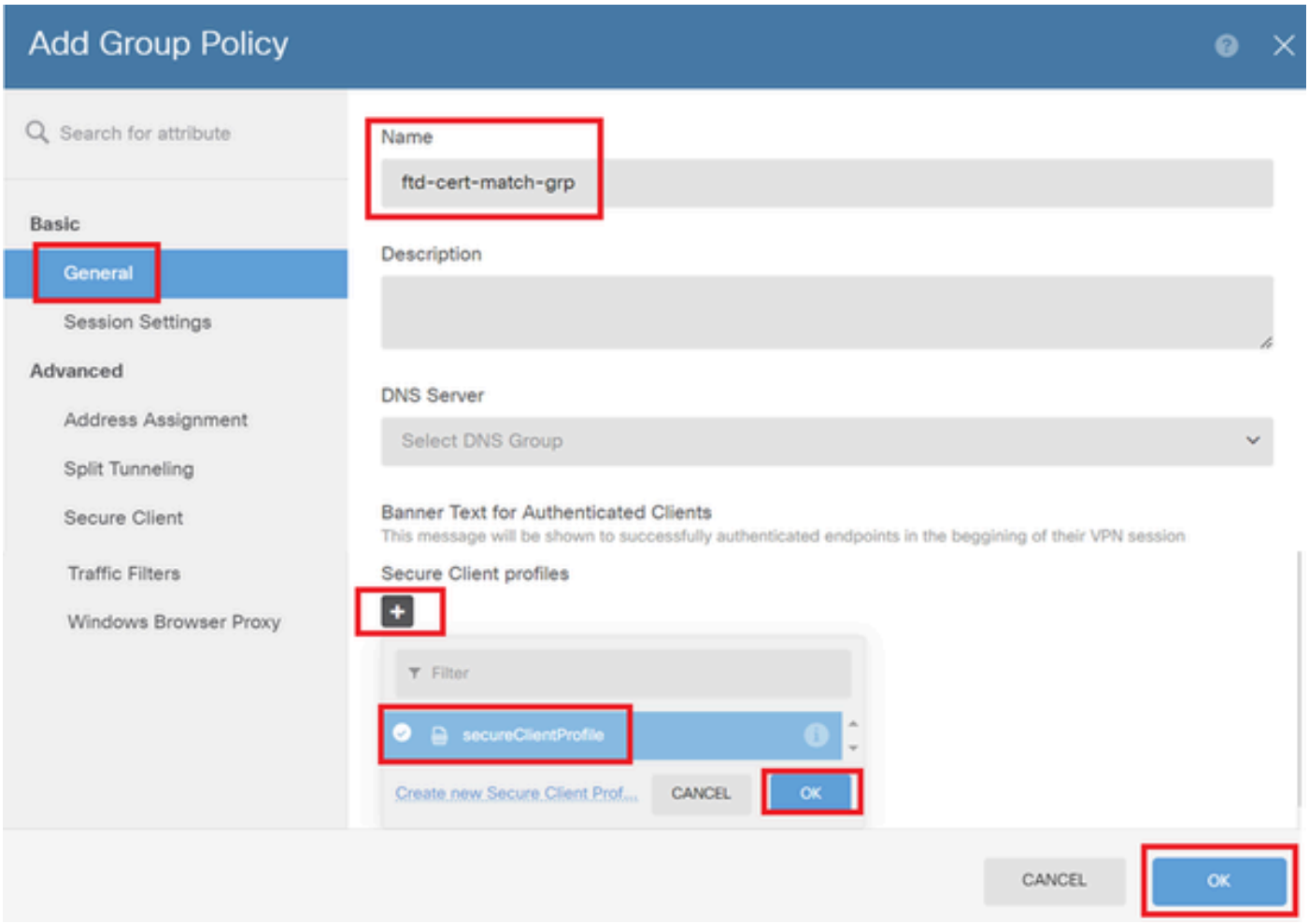
Device > Remote Access VPN > View Configuration > Group Policiesの順に移動し、+ボタンをクリックします。



グループポリシーの追加

グループポリシーの追加に必要な情報を入力し、OKボタンをクリックします。

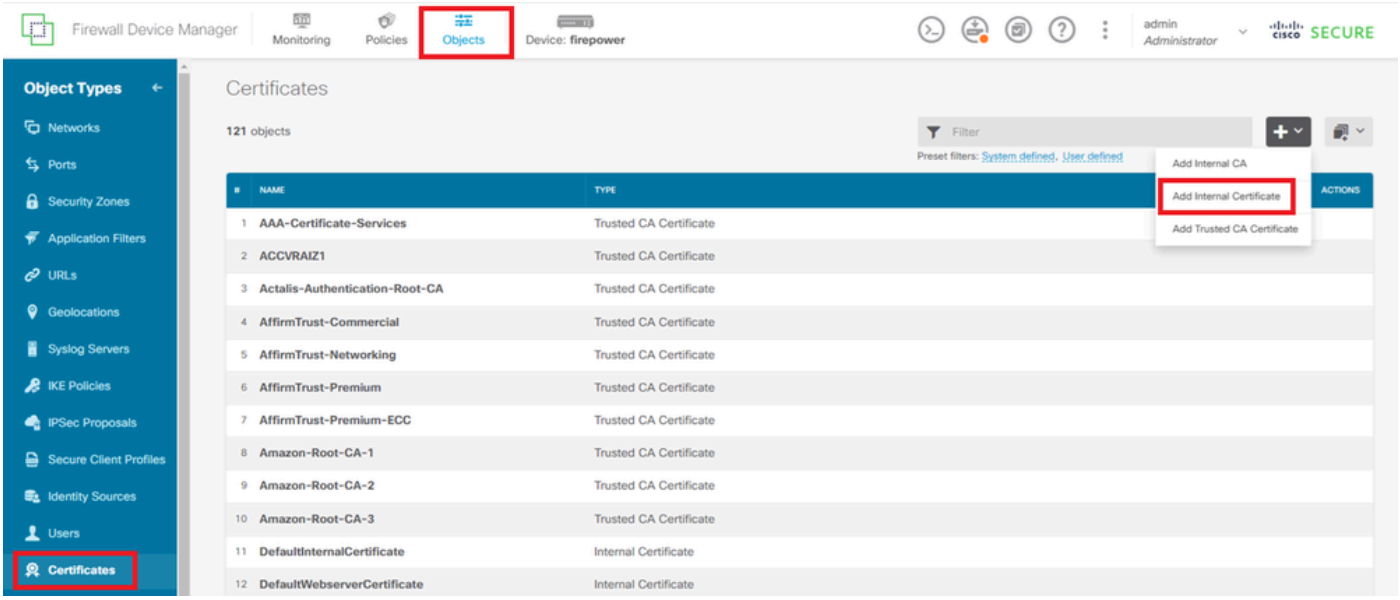
- 名前：ftd-cert-match-grp
- セキュアクライアントプロファイル：secureClientProfile



グループポリシーの詳細

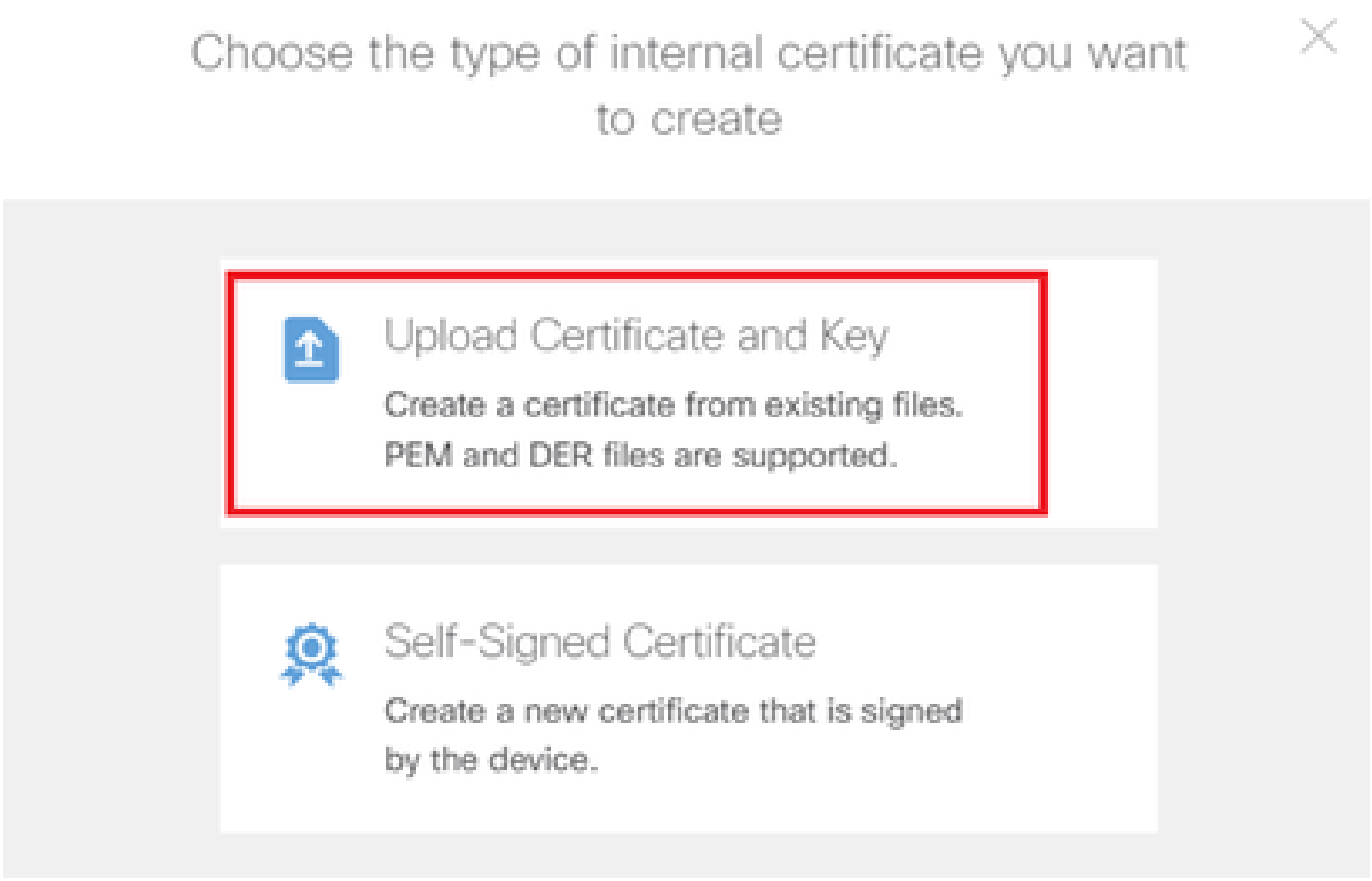
手順 7：FTD証明書の追加

Objects > Certificatesの順に移動し、Add Internal Certificate from +をクリックします。



内部証明書の追加

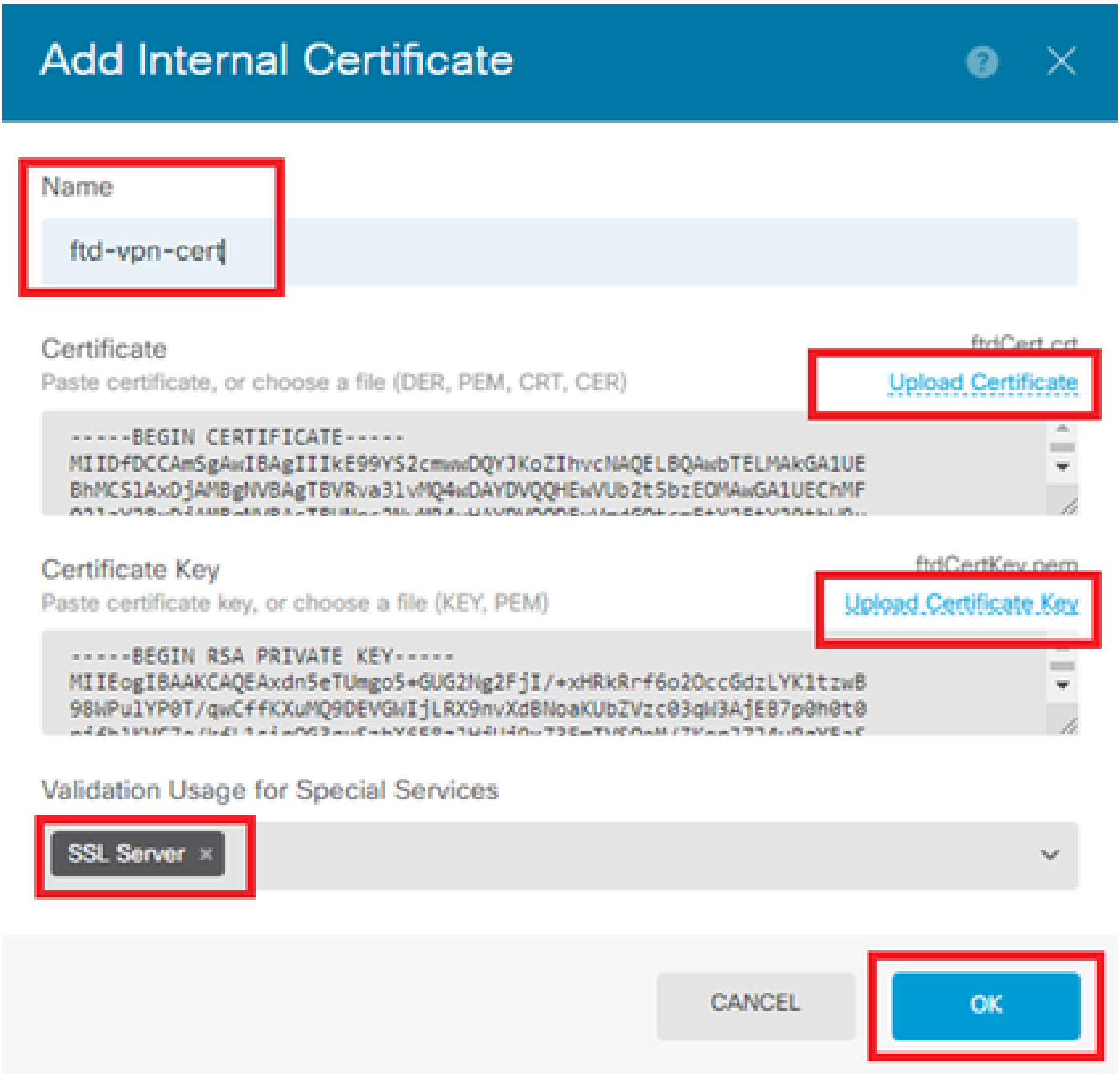
Upload Certificate and Keyをクリックします。



証明書とキーのアップロード

FTD証明書に必要な情報を入力し、証明書と証明書キーをローカルコンピュータからインポートして、OKボタンをクリックします。

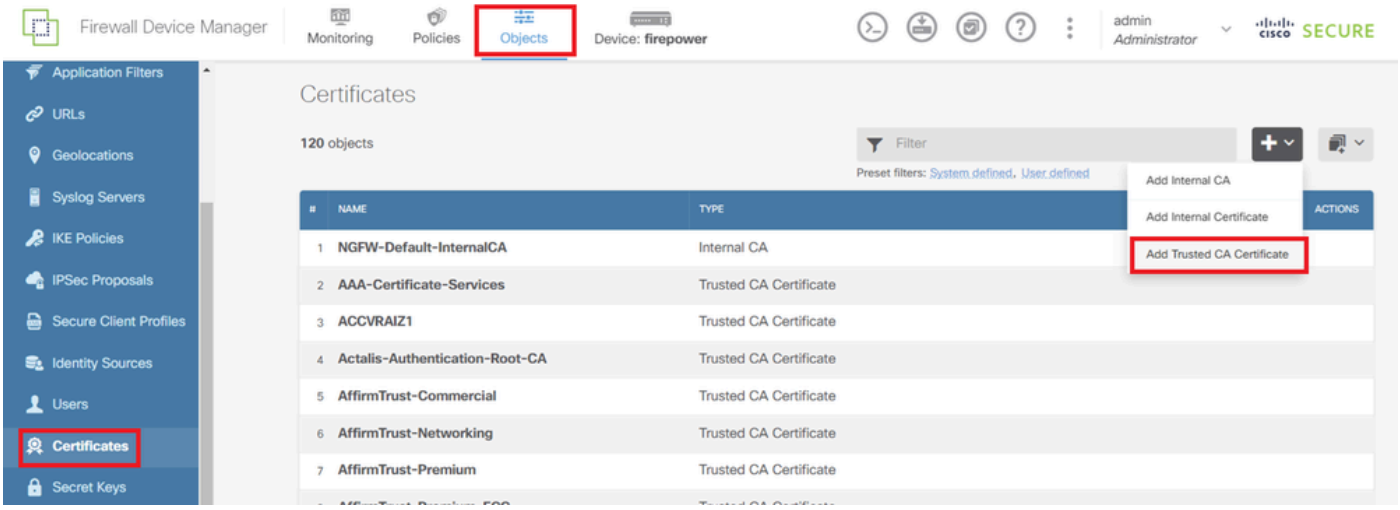
- 名前：ftd-vpn-cert
- 特殊サービスの検証用途：SSLサーバ



内部証明書の詳細

ステップ 8：FTDへのCAの追加

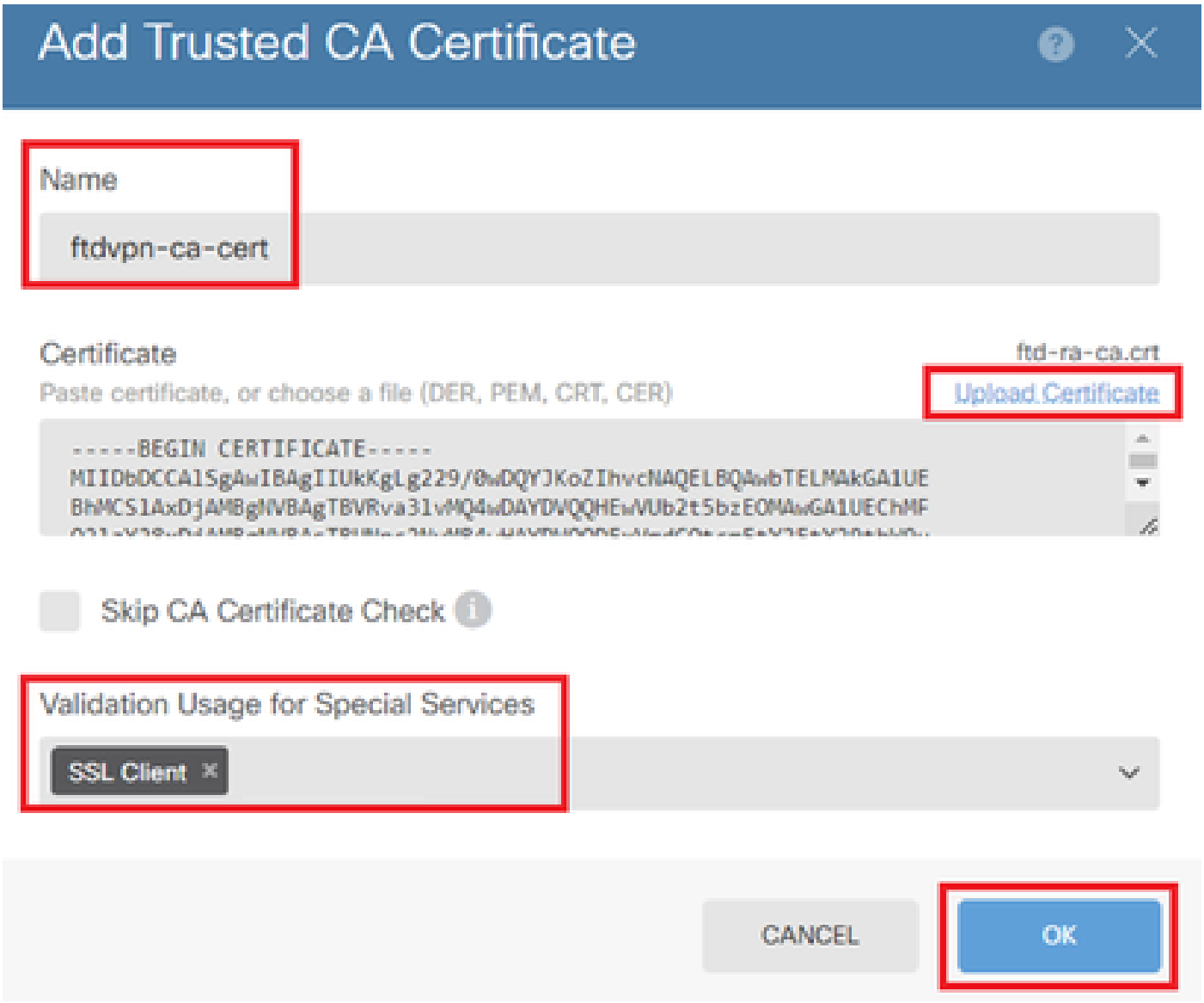
Objects > Certificatesの順に移動し、Add Trusted CA Certificate from +をクリックします。



信頼済みCA証明書の追加

CAに必要な情報を入力し、ローカルコンピュータから証明書をインポートします。

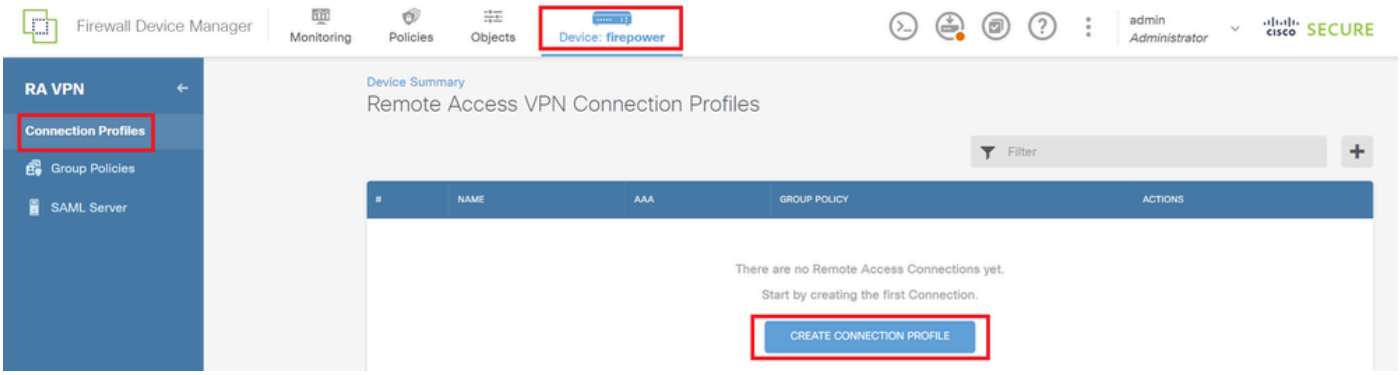
- 名前：ftdvpn-ca-cert
- 特殊サービスの検証用途：SSLクライアント



信頼済みCA証明書の詳細

ステップ 9：リモートアクセスVPN接続プロファイルの追加

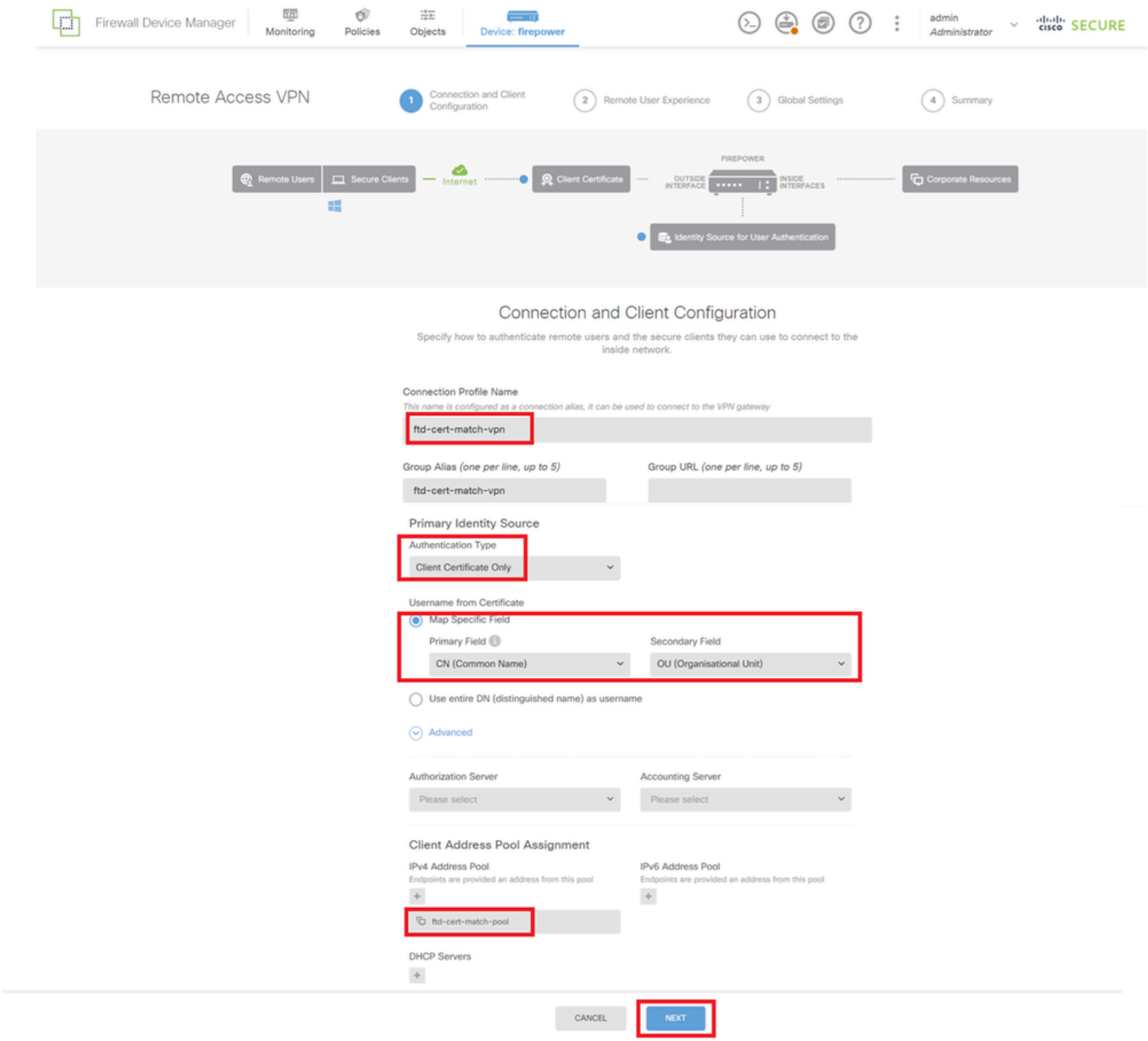
Device > Remote Access VPN > View Configuration > Connection Profilesの順に移動し、CREATE CONNECTION PROFILEボタンをクリックします。



リモートアクセスVPN接続プロファイルの追加

接続プロファイルに必要な情報を入力し、Nextボタンをクリックします。

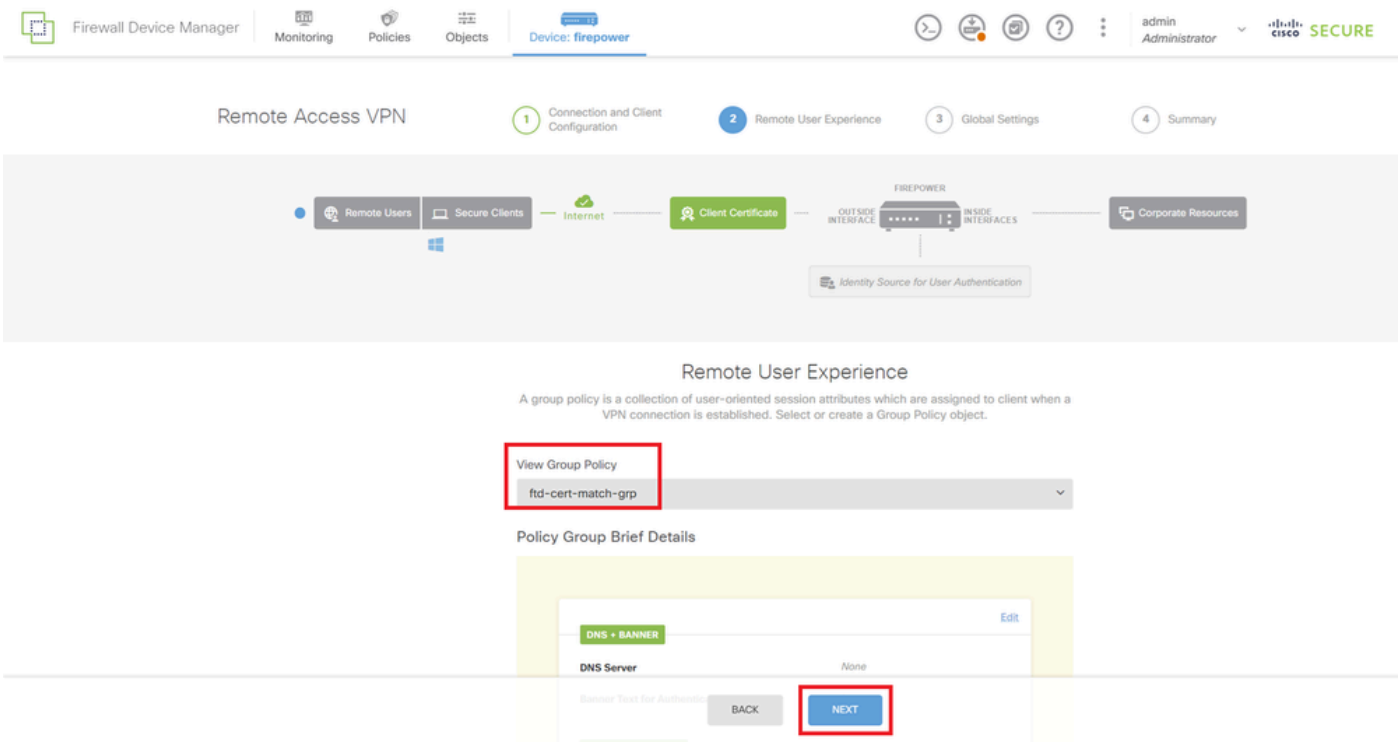
- 接続プロファイル名：ftd-cert-match-vpn
- 認証の種類：クライアント証明書のみ
- 証明書からのユーザ名：特定のフィールドのマッピング
- 主フィールド：CN (共通名)
- セカンダリフィールド：OU(Organizational Unit)
- IPv4アドレスプール：ftd-cert-match-pool



VPN接続プロファイルの詳細

グループポリシーに必要な情報を入力し、Nextボタンをクリックします。

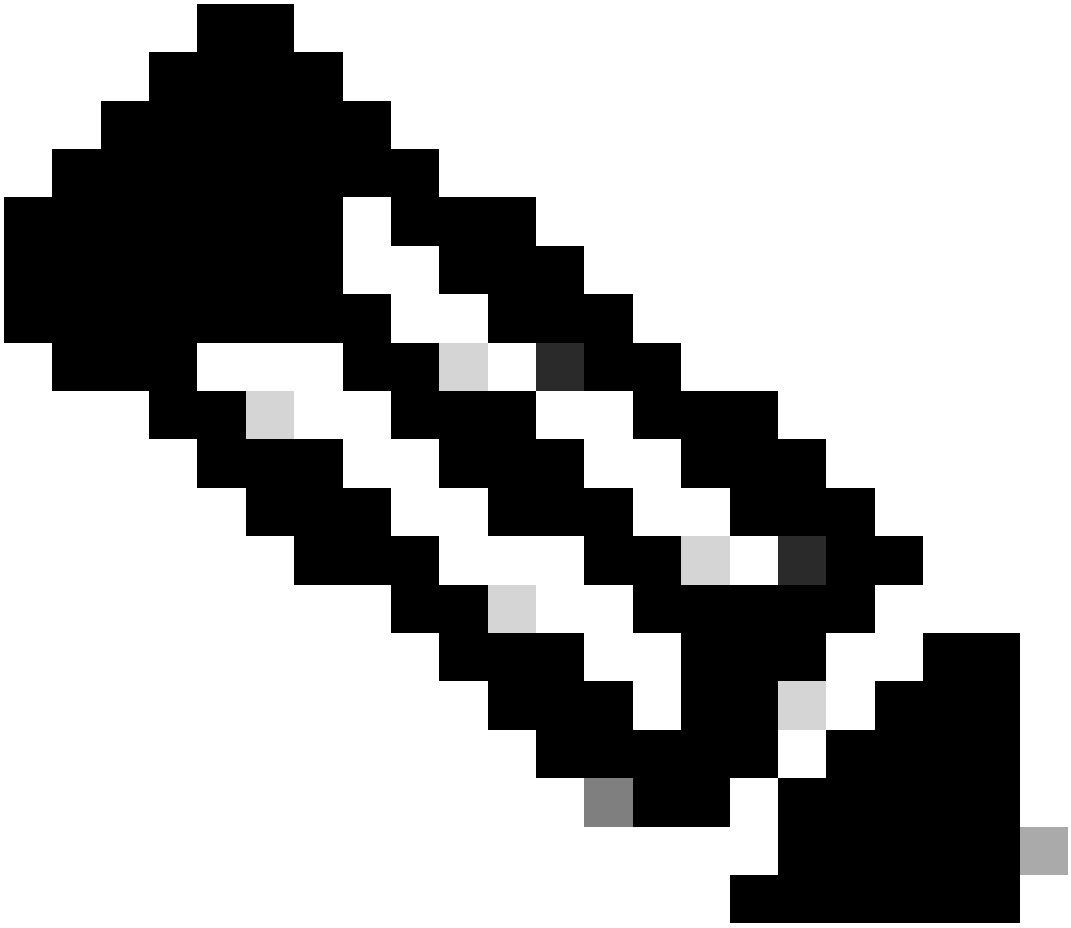
- グループポリシーの表示：ftd-cert-match-grp



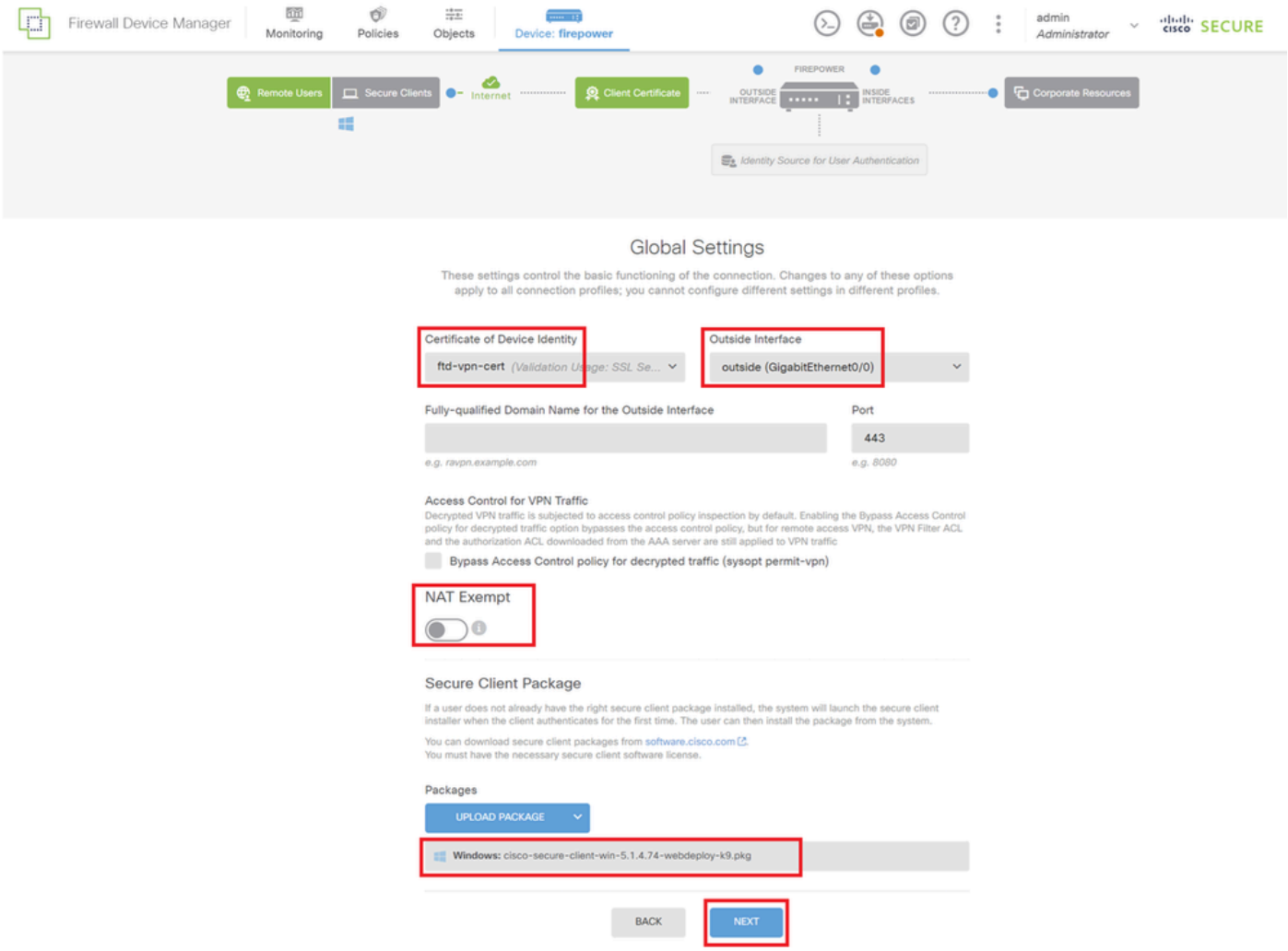
グループポリシーの選択

Certificate of Device Identity、Outside Interface、Secure Client Package for VPN connectionの順に選択します。

- デバイスIDの証明書：ftd-vpn-cert
- 外部インターフェイス：外部(GigabitEthernet0/0)
- セキュアクライアントパッケージ：cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg



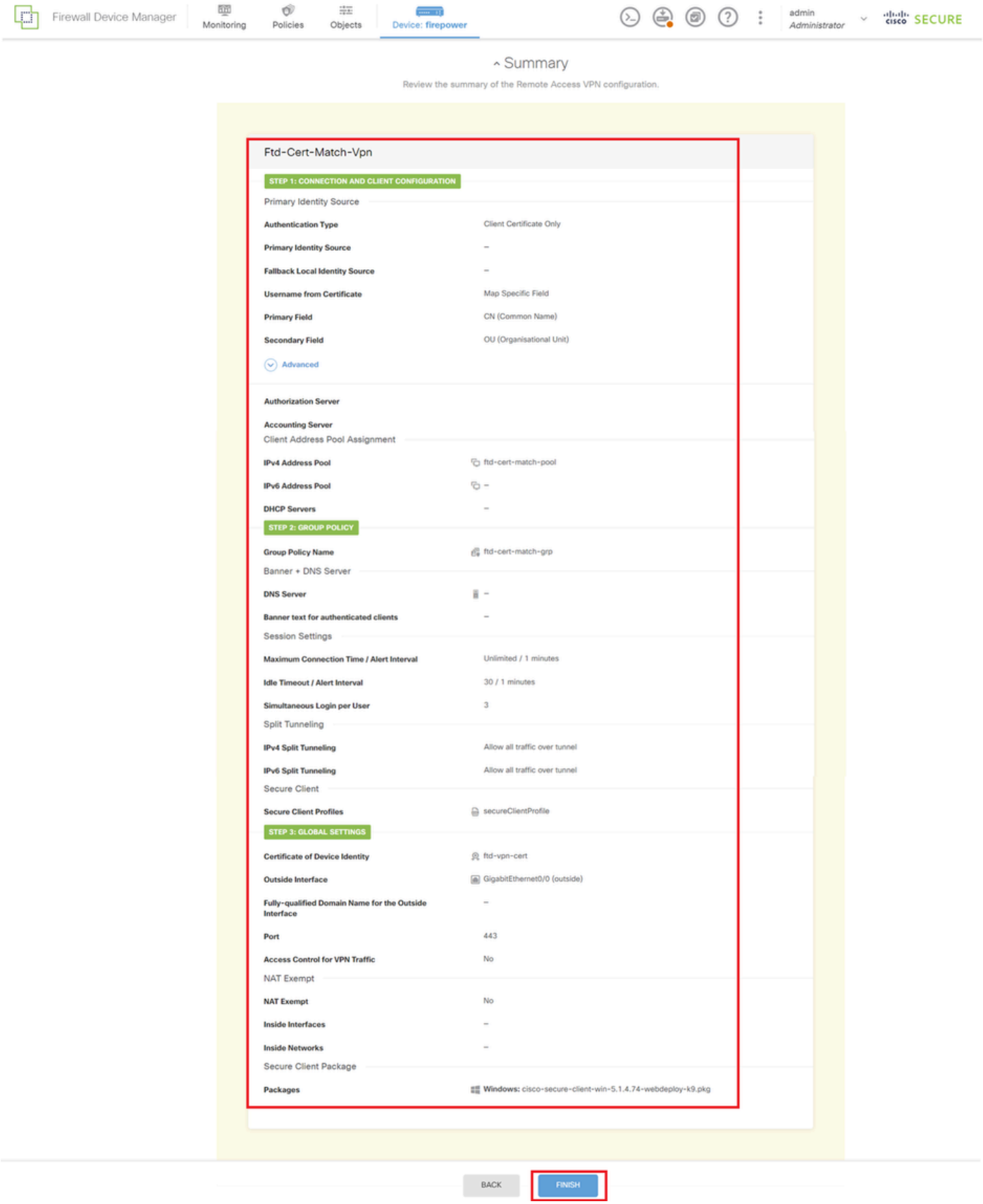
注：このドキュメントのNAT免除の機能は無効になっています。



グローバル設定の詳細

ステップ 10：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。



接続プロファイルの概要の確認

FTD CLIで確認

FDMから展開した後、FTD CLIでVPN接続設定を確認します。

```
// Defines IP of interface
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

// Defines a pool of addresses
ip local pool ftd-cert-match-pool 172.16.1.150-172.16.1.160

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftd-vpn-cert
enrollment terminal
keypair ftd-vpn-cert
crl configure

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

// Defines Trustpoint for CA
crypto ca trustpoint ftdvpn-ca-cert
enrollment terminal
validation-usage ssl-client
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 profiles secureClientProfile disk0:/anyconncprofs/secureClientProfile.xml
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Configures the group-policy to allow SSL connections
```

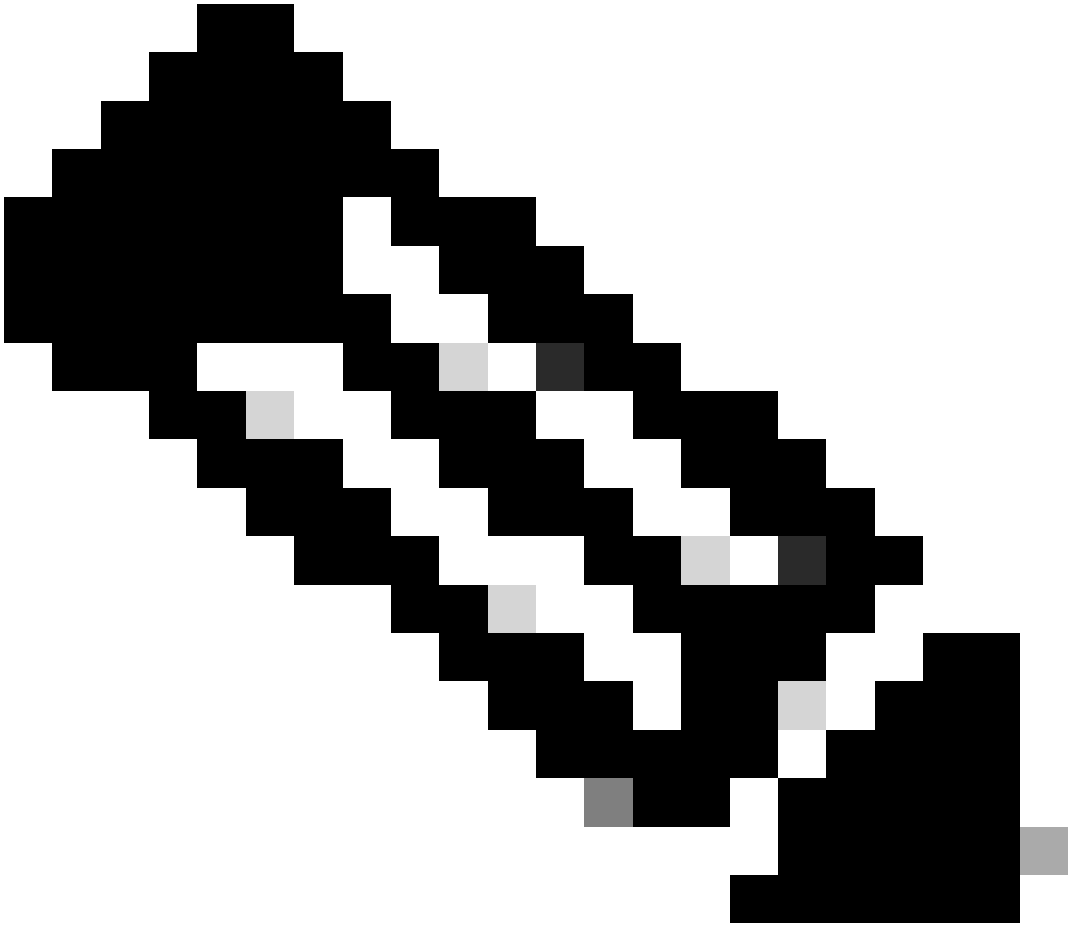
```
group-policy ftd-cert-match-grp internal
group-policy ftd-cert-match-grp attributes
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
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 value secureClientProfile type user
anyconnect ssl df-bit-ignore disable
always-on-vpn profile-setting

// Configures the tunnel-group to use the certificate authentication
tunnel-group ftd-cert-match-vpn type remote-access
tunnel-group ftd-cert-match-vpn general-attributes
address-pool ftd-cert-match-pool
default-group-policy ftd-cert-match-grp
tunnel-group ftd-cert-match-vpn webvpn-attributes
authentication certificate
group-alias ftd-cert-match-vpn enable
```

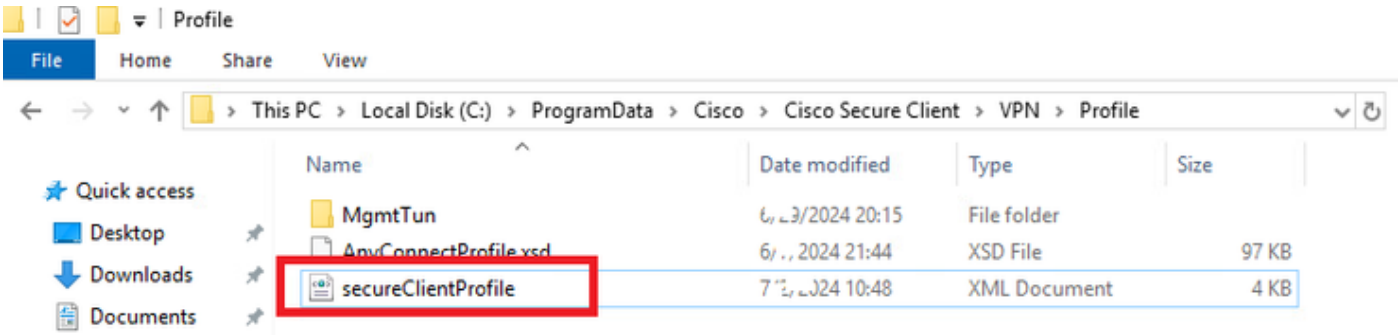
VPNクライアントでの確認

ステップ 1：VPNクライアントへのセキュアなクライアントプロファイルのコピー

VPNクライアントとマネージャのVPNクライアントを設計するために、セキュアなクライアントプロファイルをコピーします。



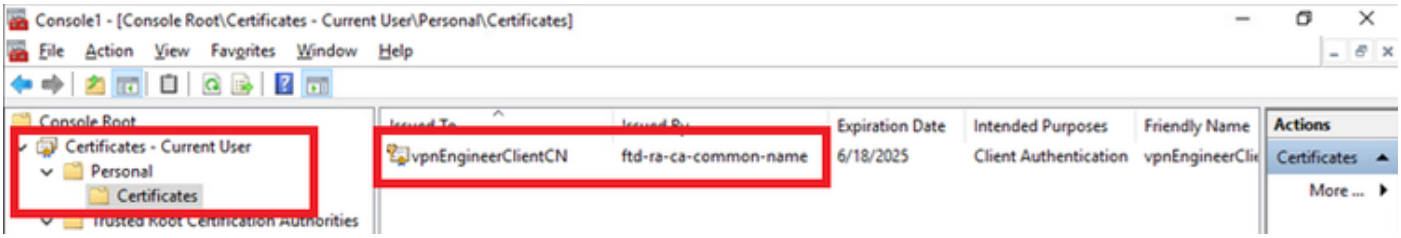
注:Windowsコンピュータのセキュアクライアントプロファイルのディレクトリ：C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile



VPNクライアントへのセキュアなクライアントプロファイルのコピー

ステップ 2：クライアント証明書の確認

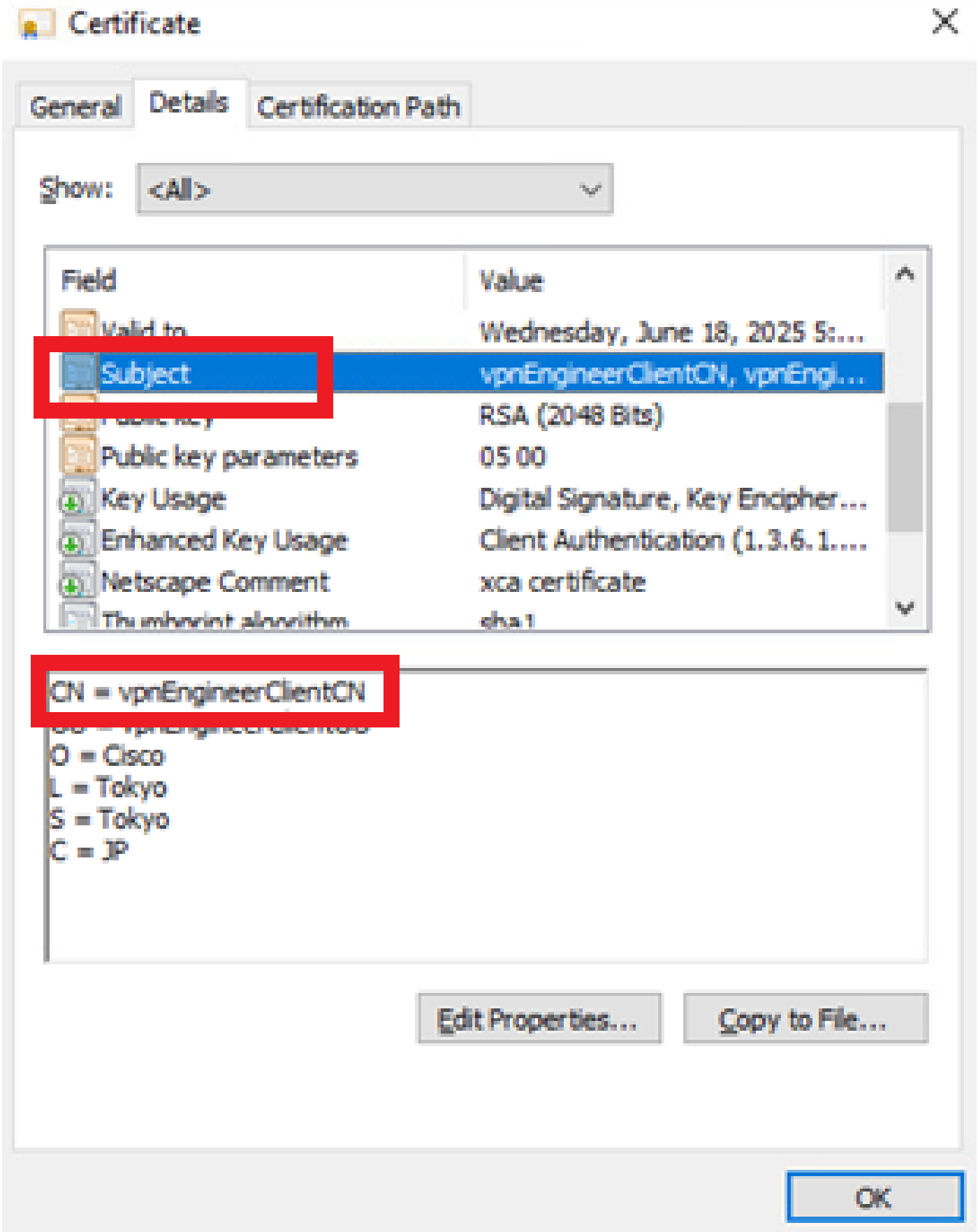
VPN Clientエンジニアで、Certificates - Current User > Personal > Certificatesの順に移動し、認証に使用するクライアント証明書を確認します。



エンジニア用VPN Clientの証明書の確認

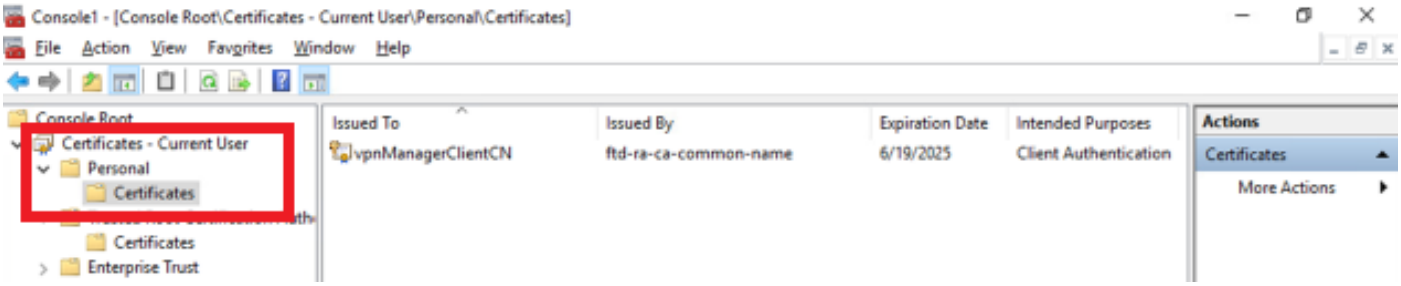
クライアント証明書をダブルクリックし、Detailsに移動して、Subjectの詳細を確認します。

- 件名：CN = vpnEngineerClientCN



技術士免状の内容

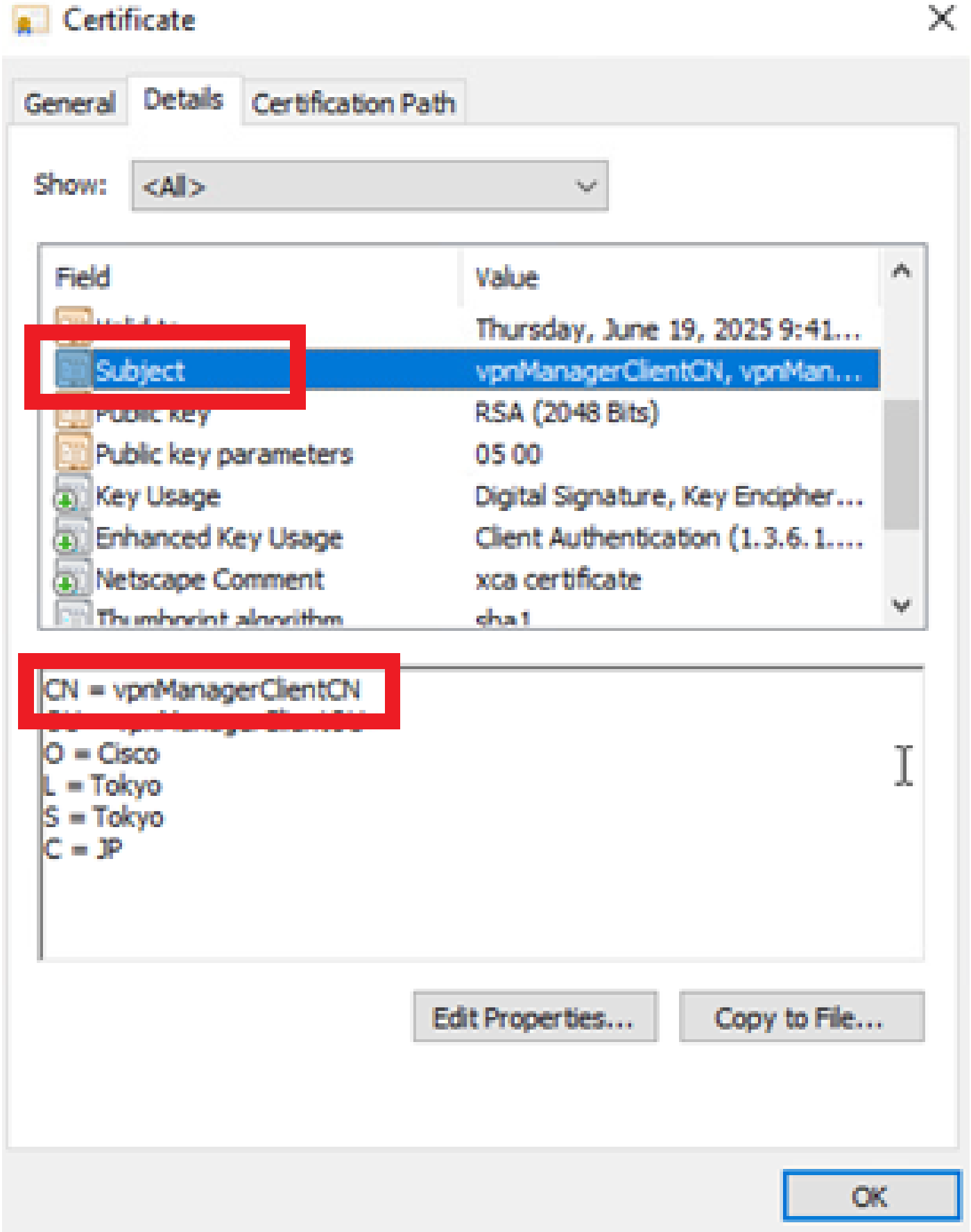
マネージャのVPN Clientで、Certificates - Current User > Personal > Certificatesの順に移動し、認証に使用するクライアント証明書を確認します。



Manager VPN Clientの証明書の確認

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 = vpnManagerClientCN

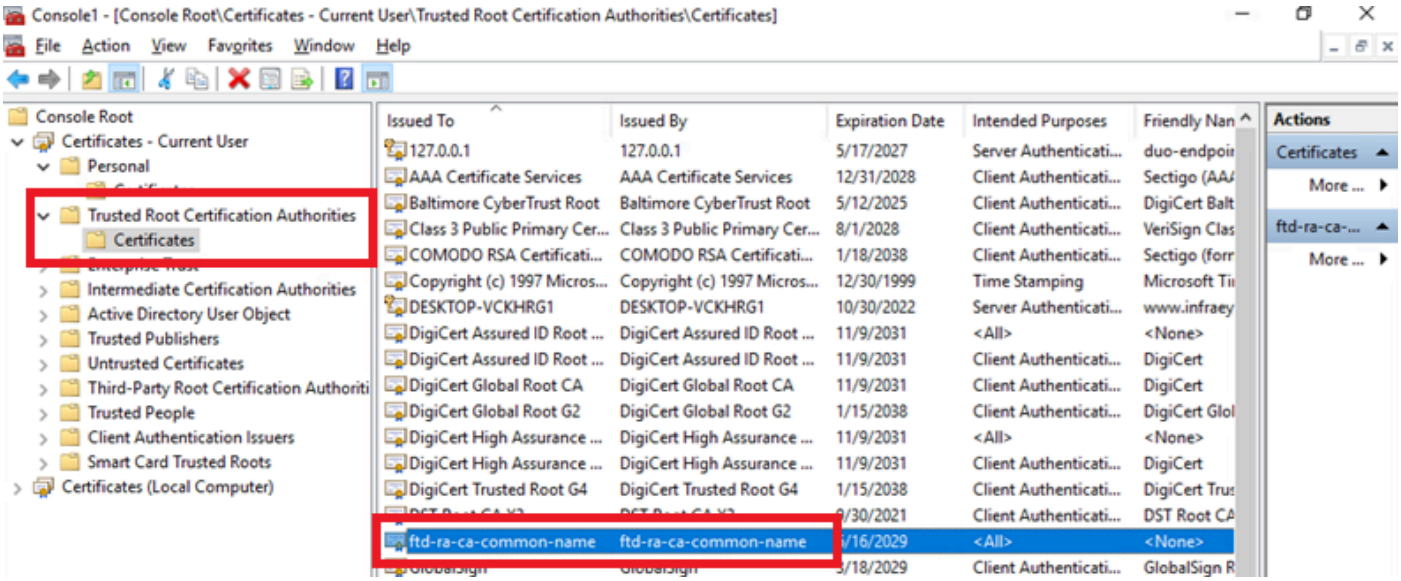


マネージャクライアント証明書の詳細

ステップ 3：CAの確認

エンジニアのVPNクライアントとマネージャのVPNクライアントの両方で、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

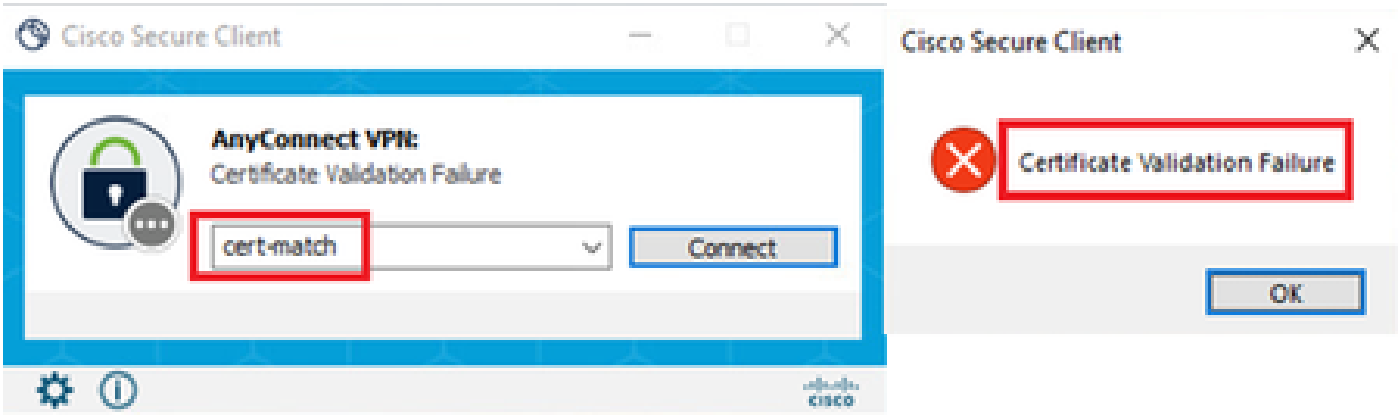
確認

ステップ 1：VPN接続の開始

エンジニアのVPNクライアントで、Cisco Secure Client接続を開始します。ユーザ名とパスワードを入力する必要はなく、VPNは正常に接続されました。

エンジニアのVPN ClientのVPN接続に成功しました

マネージャのVPNクライアントで、Cisco Secure Client接続を開始します。証明書の検証エラーが原因で、VPNの接続に失敗しました。



Manager VPN ClientのVPN接続の失敗

ステップ 2：FTD CLIでのVPNセッションの確認

エンジニアのVPNセッションを確認するためにFTD(Lina)CLIでshow vpn-sessiondb detail anyconnectコマンドを実行します。

```
firepower# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : vpnEngineerClientCN Index : 32
Assigned IP : 172.16.1.150 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 : 14718 Bytes Rx : 12919
Pkts Tx : 2 Pkts Rx : 51
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftd-cert-match-grp Tunnel Group : ftd-cert-match-vpn
Login Time : 05:42:03 UTC Tue Jul 2 2024
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 00000000000200006683932b
Security Grp : none Tunnel Zone : 0

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

AnyConnect-Parent:
Tunnel ID : 32.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50170 TCP Dst Port : 443
Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 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 : 7359 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 32.2
Assigned IP : 172.16.1.150 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 50177
TCP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 7359 Bytes Rx : 12919
Pkts Tx : 1 Pkts Rx : 51
Pkts Tx Drop : 0 Pkts Rx Drop : 0

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コンピュータのDARTファイルに記載されています。

次に、エンジニアクライアントからのVPN接続中のLinaエンジンのデバッグログの例を示します。

Jul 02 2024 04:16:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpn
Jul 02 2024 04:16:03: %FTD-6-717022: Certificate was successfully validated. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClie
Jul 02 2024 04:16:04: %FTD-6-113009: AAA retrieved default group policy (ftd-cert-match-grp) for user = vpnEngineerClientCN
Jul 02 2024 04:16:09: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50158 to 192.168.1.200/443 for TLSv1.2 sessi

関連情報

Firepower 2100用のFDM On-Box Management Serviceの設定
FDMによって管理されるFTDでのリモート・アクセスVPNの構成
Firepower Device Manager(FDM)でのsyslogの設定と確認

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。