FDMを使用したFTD上のセキュア・クライアントのAAAおよび証明書認証の構成

内容

はじめに

このドキュメントでは、FDMによって管理されるFTD上でAAAおよび証明書認証を使用して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 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

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

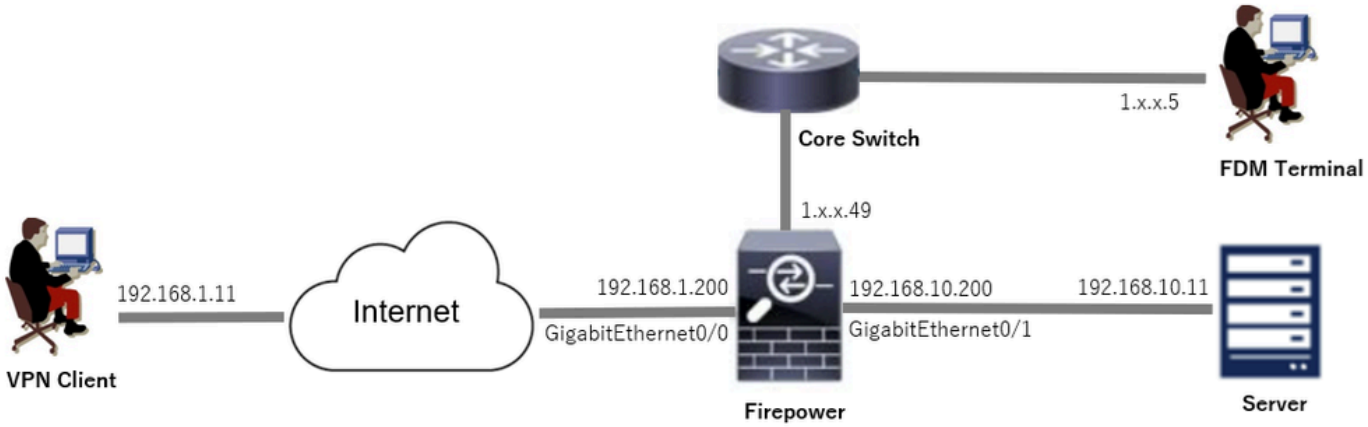
Firepower Device Manager(FDM)は、Cisco Firepower Threat Defense(FTD)デバイスの管理に使用される簡素化されたWebベースの管理インターフェイスです。Firepower Device Manager(FDM)を使用すると、ネットワーク管理者は、より複雑なFirepower Management Center(FMC)を使用せずに、FTDアプライアンスを設定および管理できます。FDMは、デバイスのパフォーマンスやセキュリティ・イベントの監視だけでなく、ネットワーク・インタフェース、セキュリティ・ゾーン、アクセス制御ポリシー、VPNの設定などの基本操作に対する直感的なユーザー・インタフェースを提供します。シンプルな管理が求められる中小規模の導入に適しています。
このドキュメントでは、FDMによって管理されるFTDで、事前に入力されたユーザ名をCisco Secure Clientと統合する方法について説明します。
FMCでFTDを管理している場合は、「FMCを介したFTD上のセキュアクライアントに対するAAAおよび証明書認証の設定」ガイドを参照してください。

これは、ドキュメントで使用される各証明書の共通名を持つ証明書チェーンです。

- 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

FDMでの構成

ステップ 1：FTDインターフェイスの設定

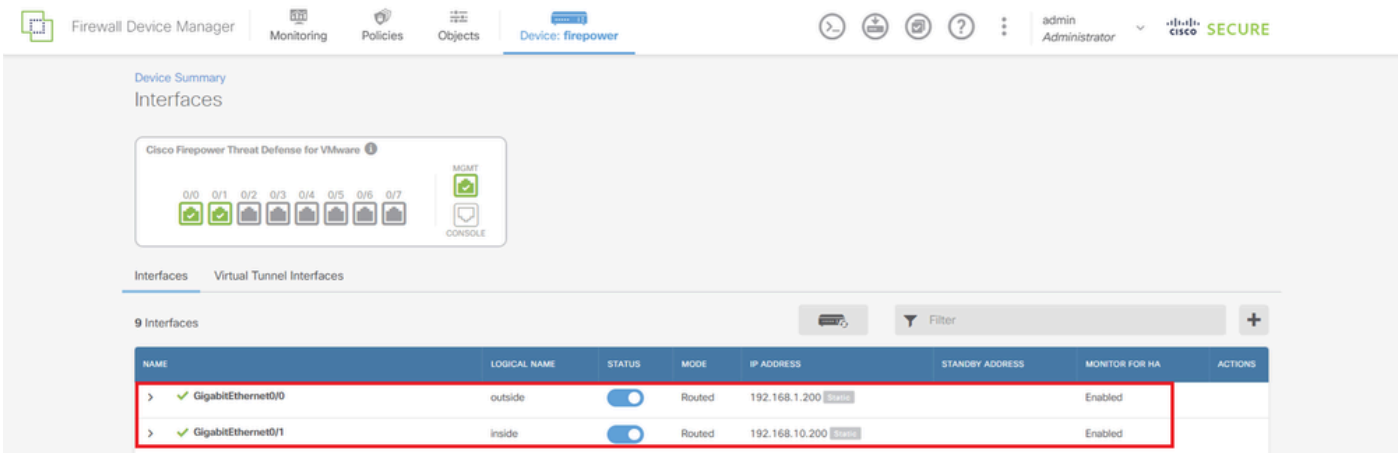
Device > Interfaces > View All Interfacesの順に移動し、FTD inInterfacestabの内部および外部インターフェイスを設定します。

GigabitEthernet0/0の場合、

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

GigabitEthernet0/1の場合、

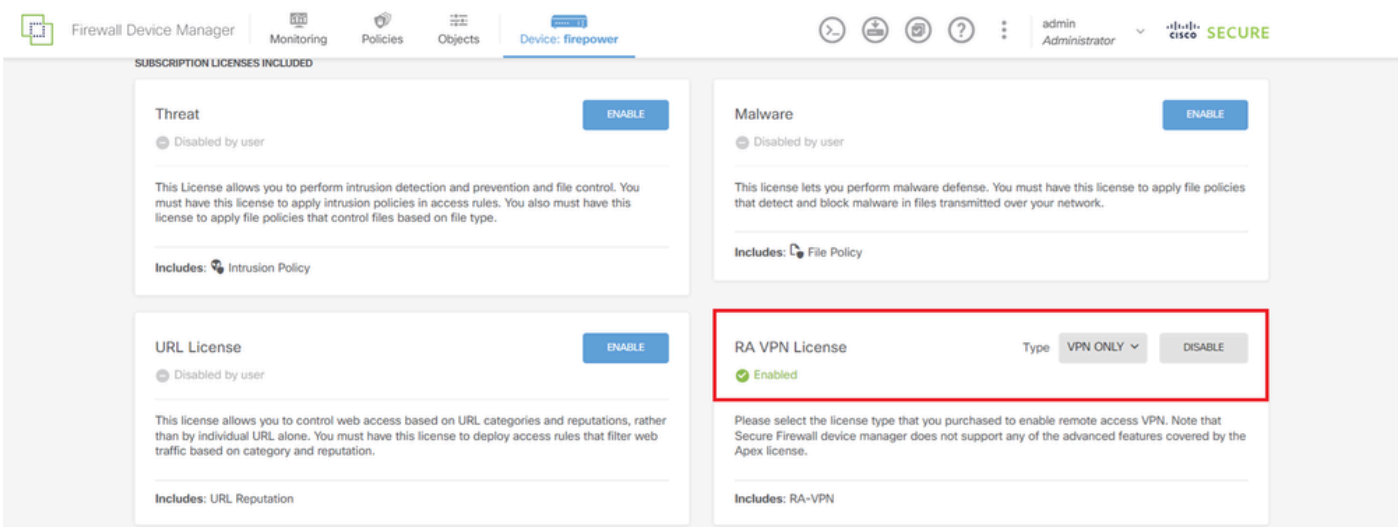
- 名前：inside
- IPアドレス：192.168.10.200/24



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

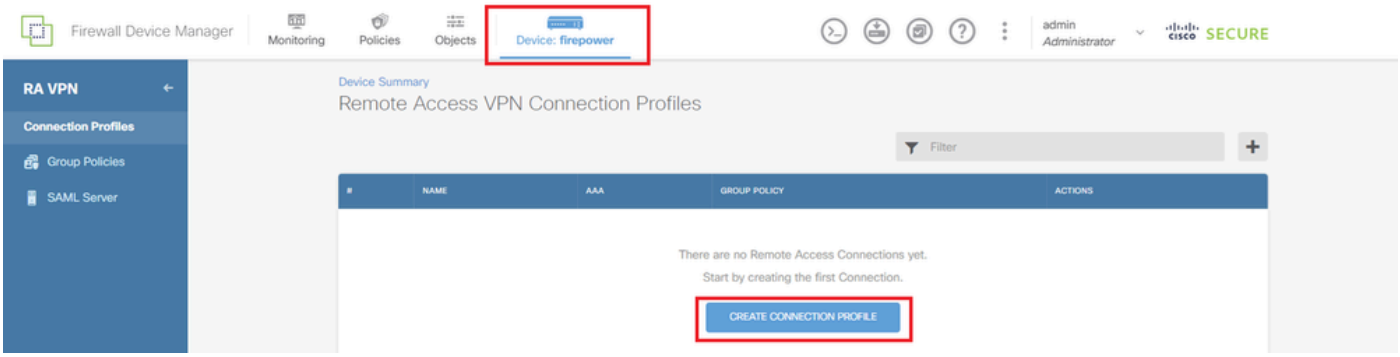
Device > Smart License > View Configurationの順に移動し、RA VPN LicenseitemでCisco Secure Clientライセンスを確認します。



セキュアクライアントライセンス

ステップ 3：リモートアクセスVPN接続プロファイルの追加

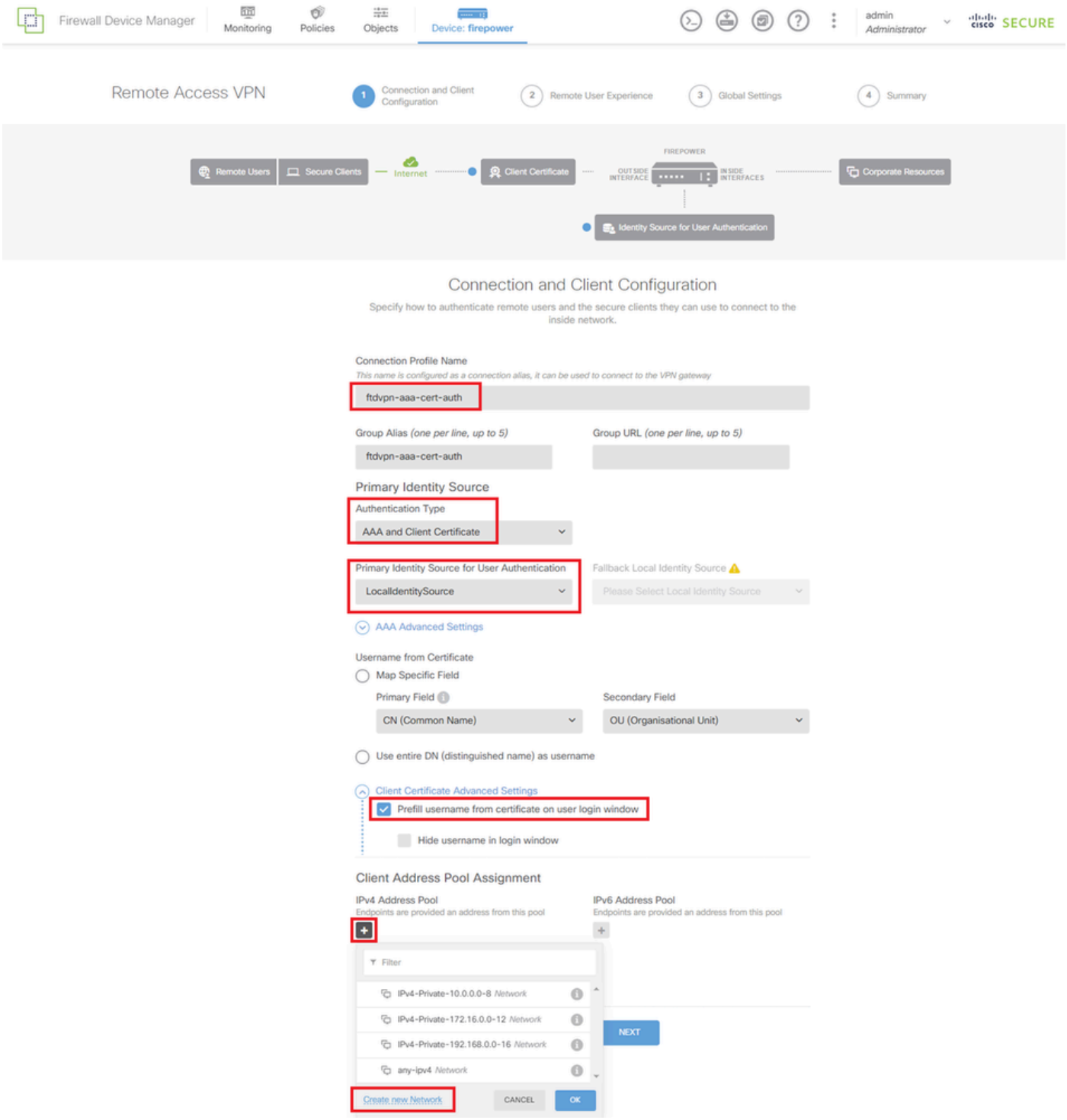
Device > Remote Access VPN > View Configurationの順に移動し、CREATE CONNECTION PROFILEボタンをクリックします。



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、IPv4 Address Pool項目でCreate new Networkボタンをクリックします。

- 接続プロファイル名：ftdvpn-aaa-cert-auth
- 認証タイプ：AAAおよびクライアント証明書
- ユーザ認証用のプライマリアイデンティティソース：LocalIdentitySource
- クライアント証明書の詳細設定：ユーザログインウィンドウで証明書からユーザ名を入力

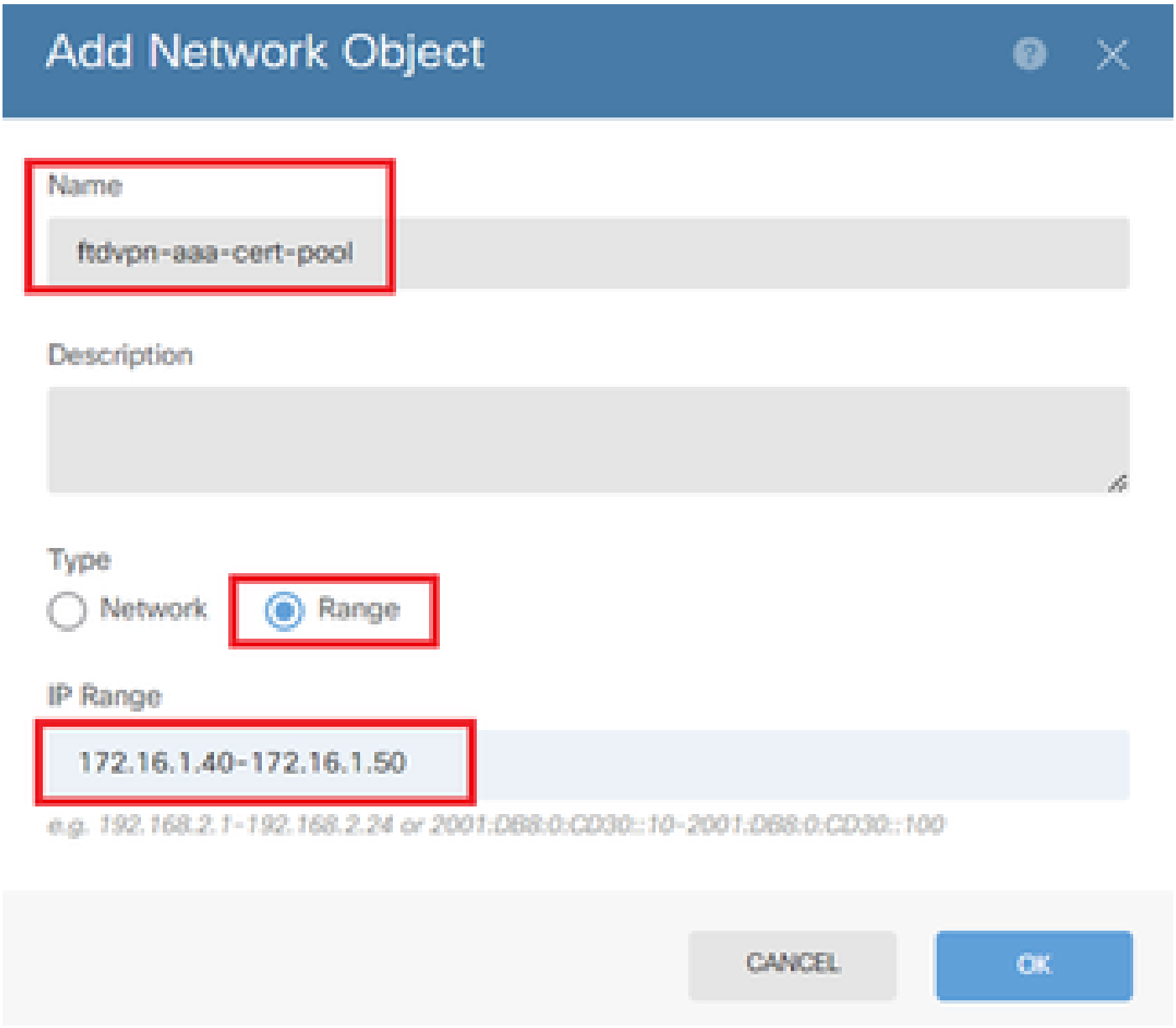


VPN接続プロファイルの詳細

ステップ 4：接続プロファイル用の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。接続プロファイル用に新しく追加されたIPv4アドレスプールを選択し、Nextボタンをクリックします。

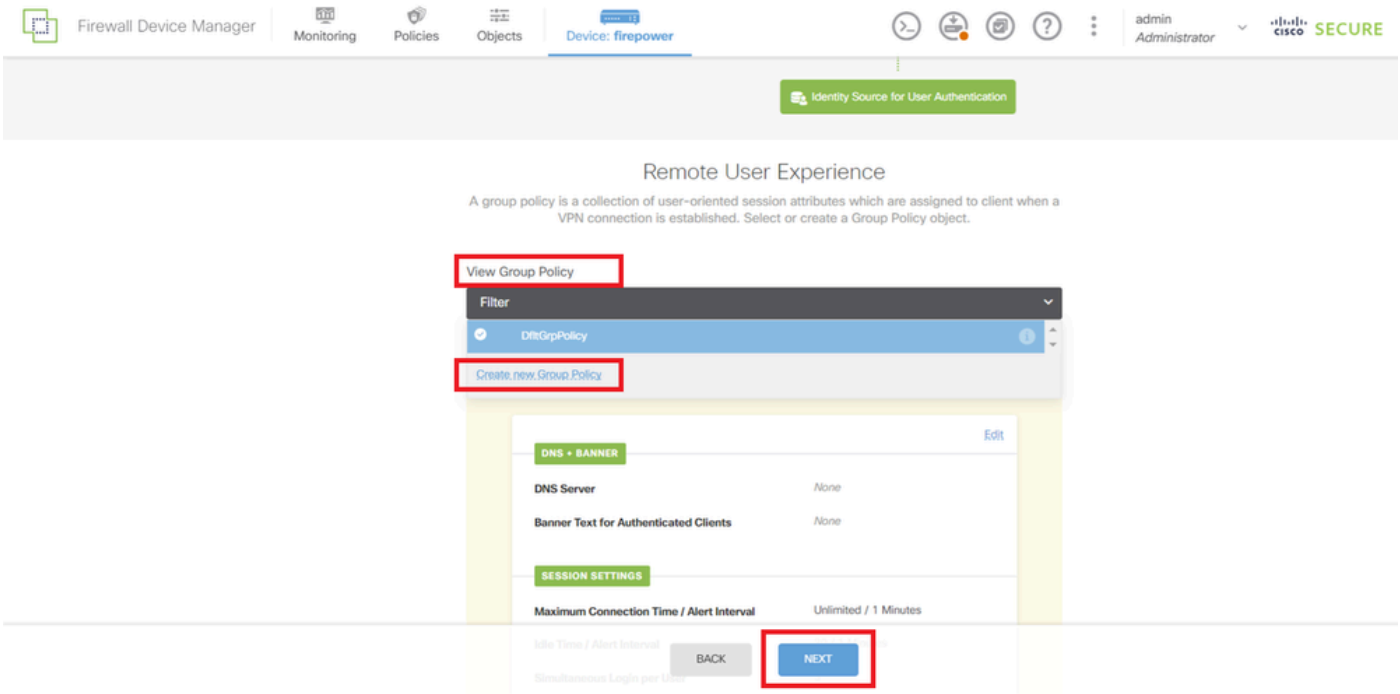
- 名前： ftdvpn-aaa-cert-pool
- タイプ：範囲
- IP範囲：172.16.1.40 ~ 172.16.1.50



Ipv4アドレスプールの詳細

ステップ 5：接続プロファイルのグループポリシーの追加

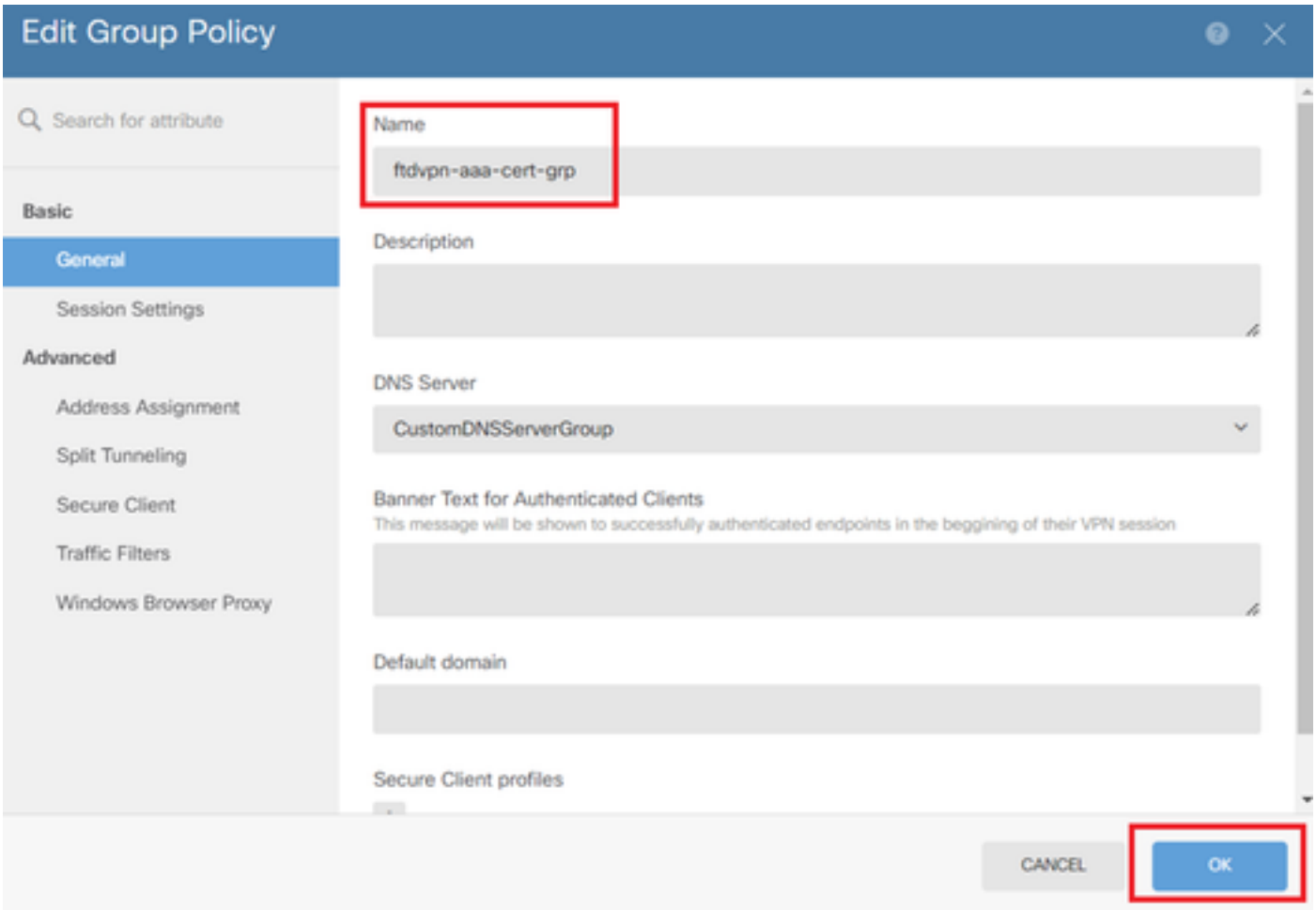
View Group Policy項目で、Create New Group Policyをクリックします。



グループポリシーの追加

必要な情報を入力して新しいグループポリシーを追加し、OKボタンをクリックします。接続プロファイルの新しい追加グループポリシーを選択します。

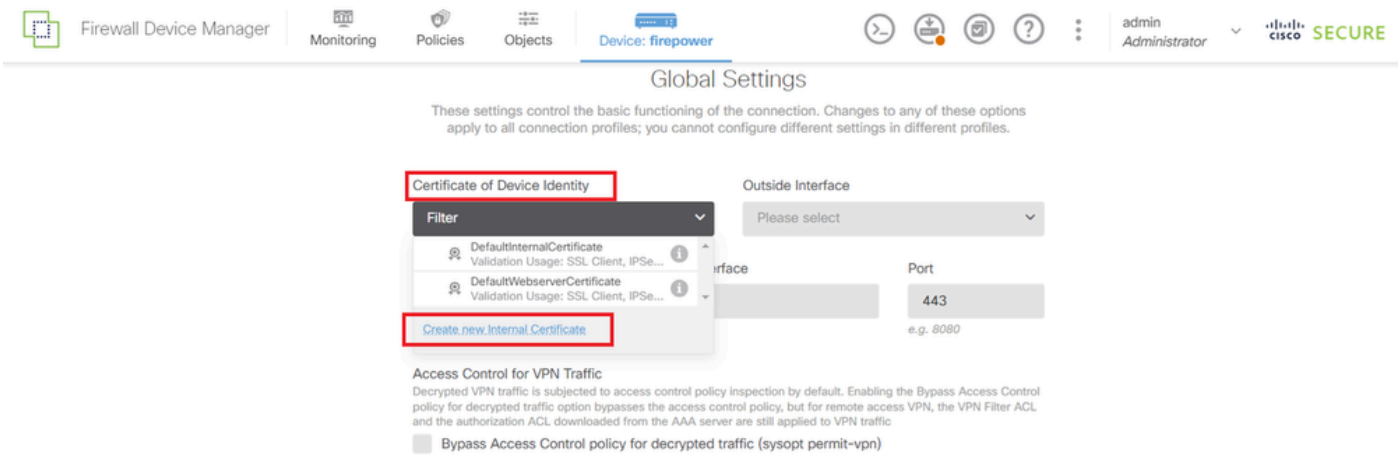
- 名前： ftdvpn-aaa-cert-grp



グループポリシーの詳細

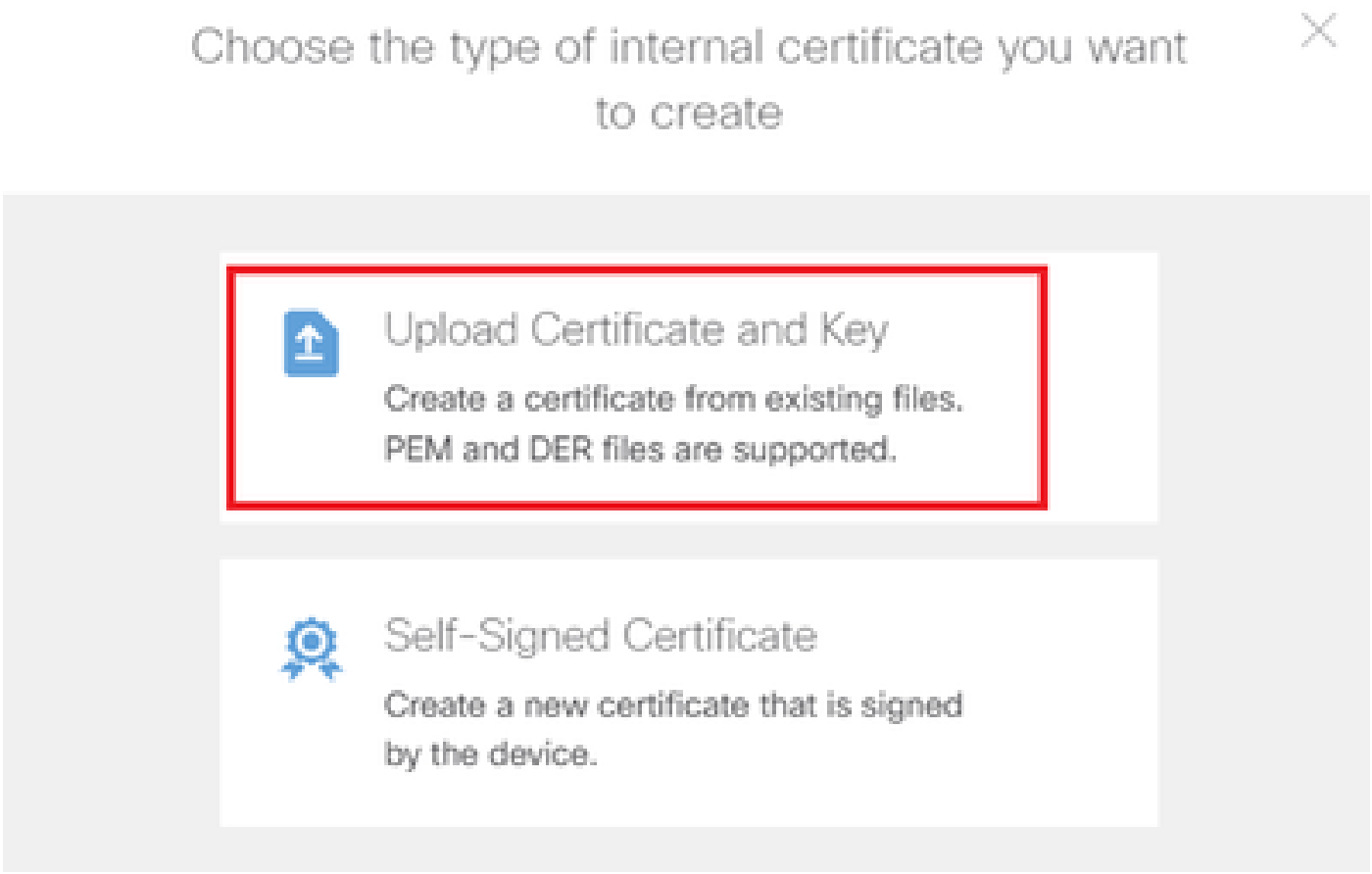
手順 6：接続プロファイル用のデバイスIDおよび外部インターフェイスの証明書の設定

Certificate of Device Identity項目で、Create new Internal certificateをクリックします。



内部証明書の追加

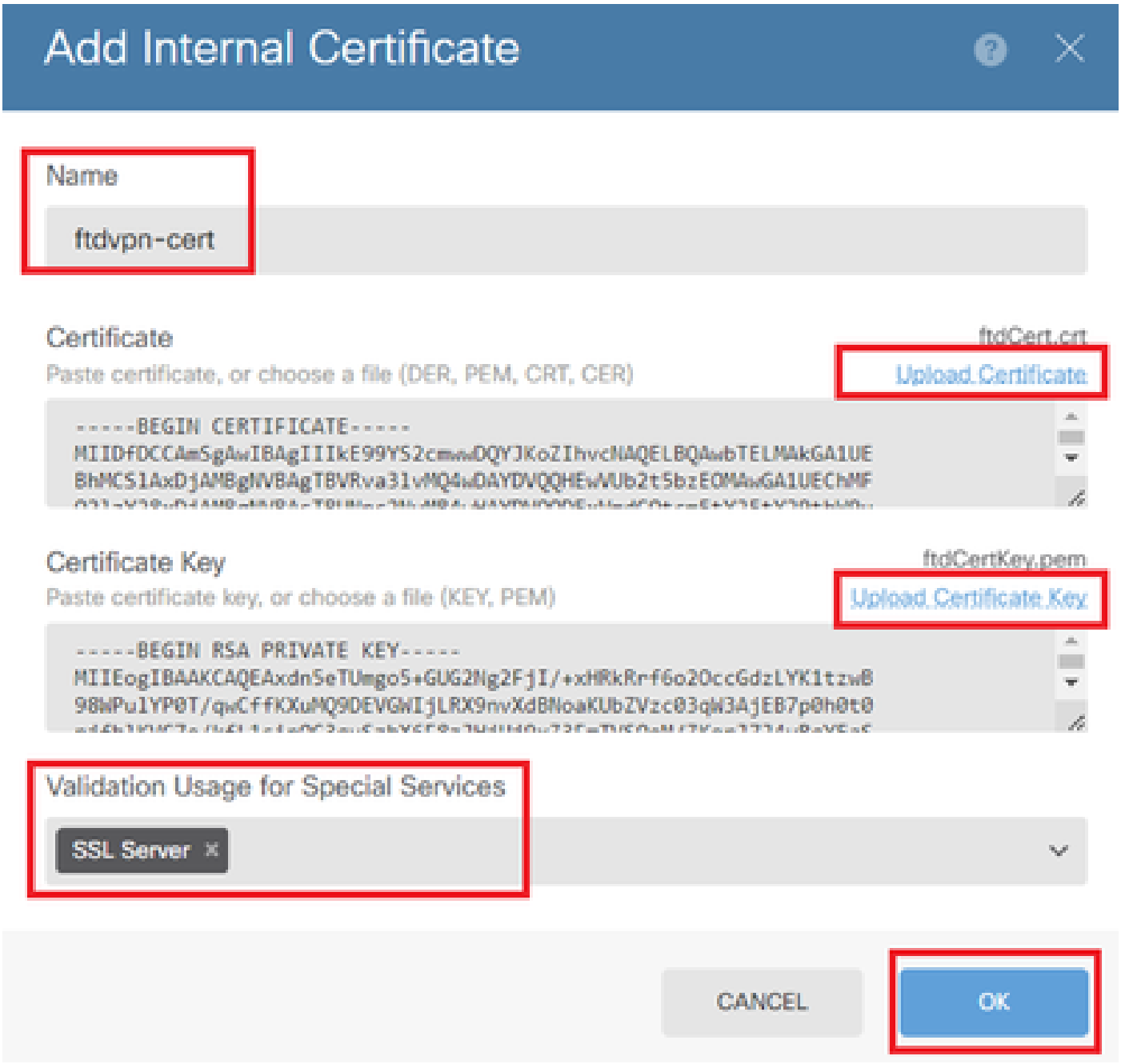
Upload Certificate and Keyをクリックします。



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。

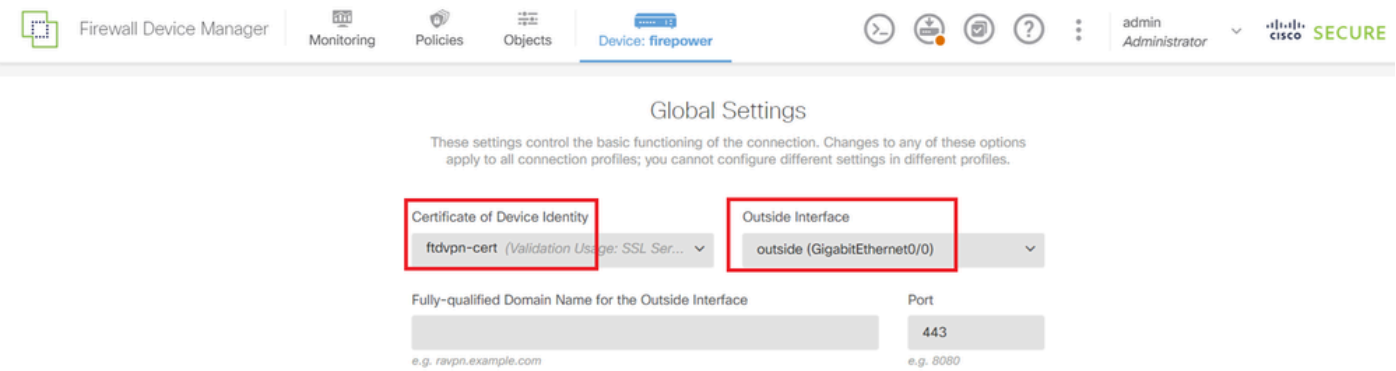
- 名前： ftdvpn-cert
- 特殊サービスの検証用途：SSLサーバ



内部証明書の詳細

VPN接続には、Certificate of Device IdentityとOutside Interfaceを選択します。

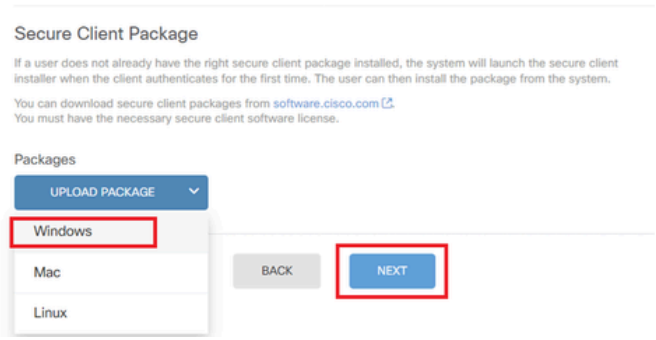
- デバイスIDの証明書：ftdvpn-cert
- 外部インターフェイス：外部(GigabitEthernet0/0)



グローバル設定の詳細

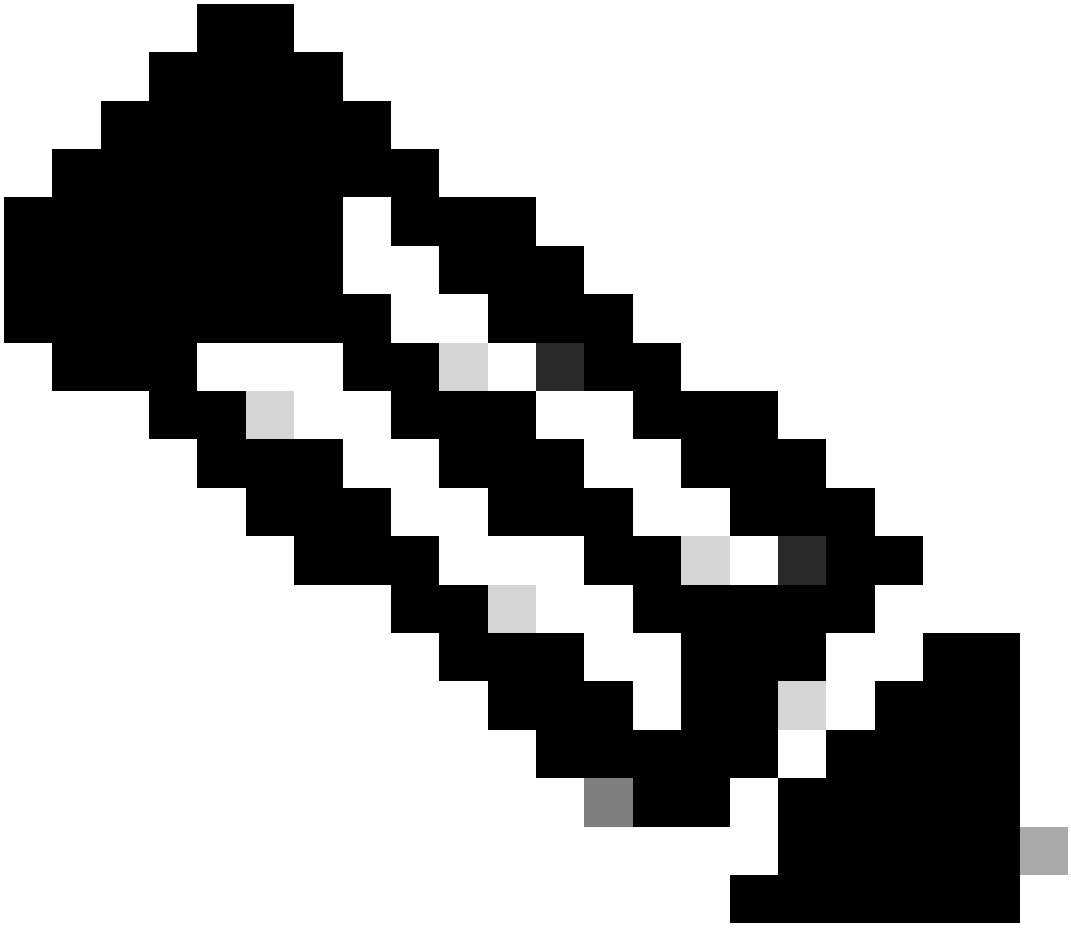
手順 7：接続プロファイル用のセキュアクライアントイメージの設定

PackagesアイテムでWindowsを選択します

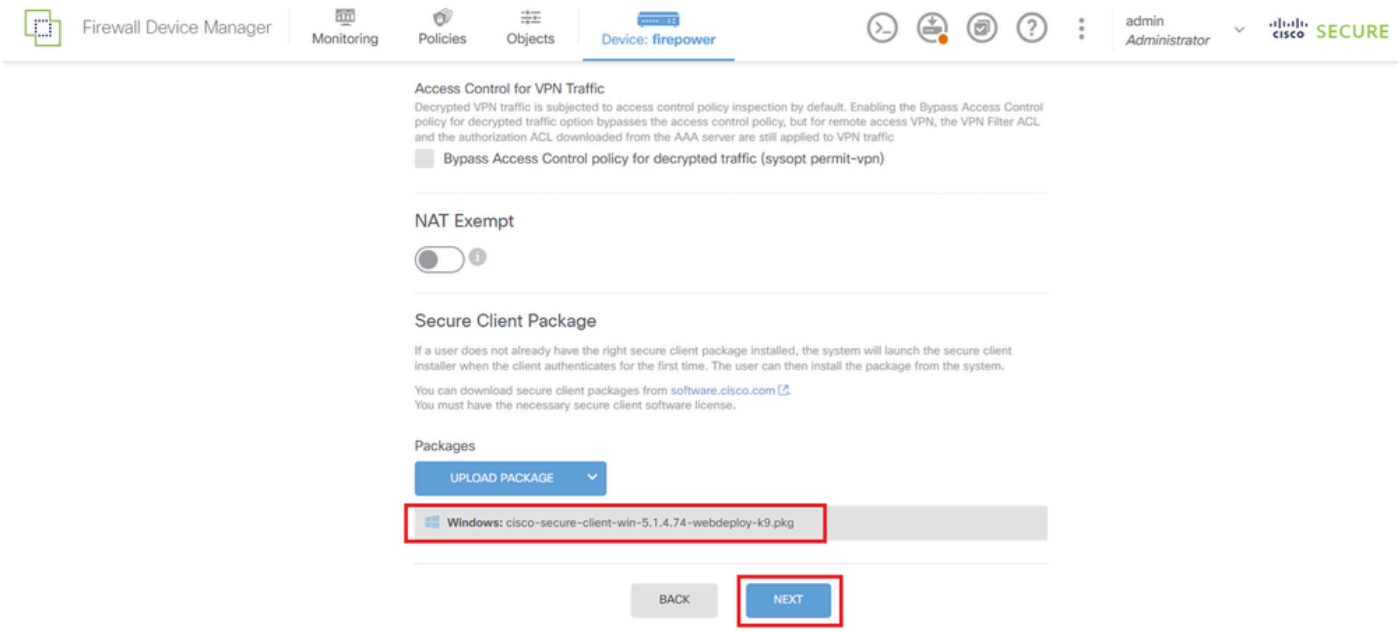


セキュアクライアントイメージパッケージのアップロード

ローカルコンピュータからセキュアクライアントイメージファイルをアップロードし、Nextbuttonをクリックします。



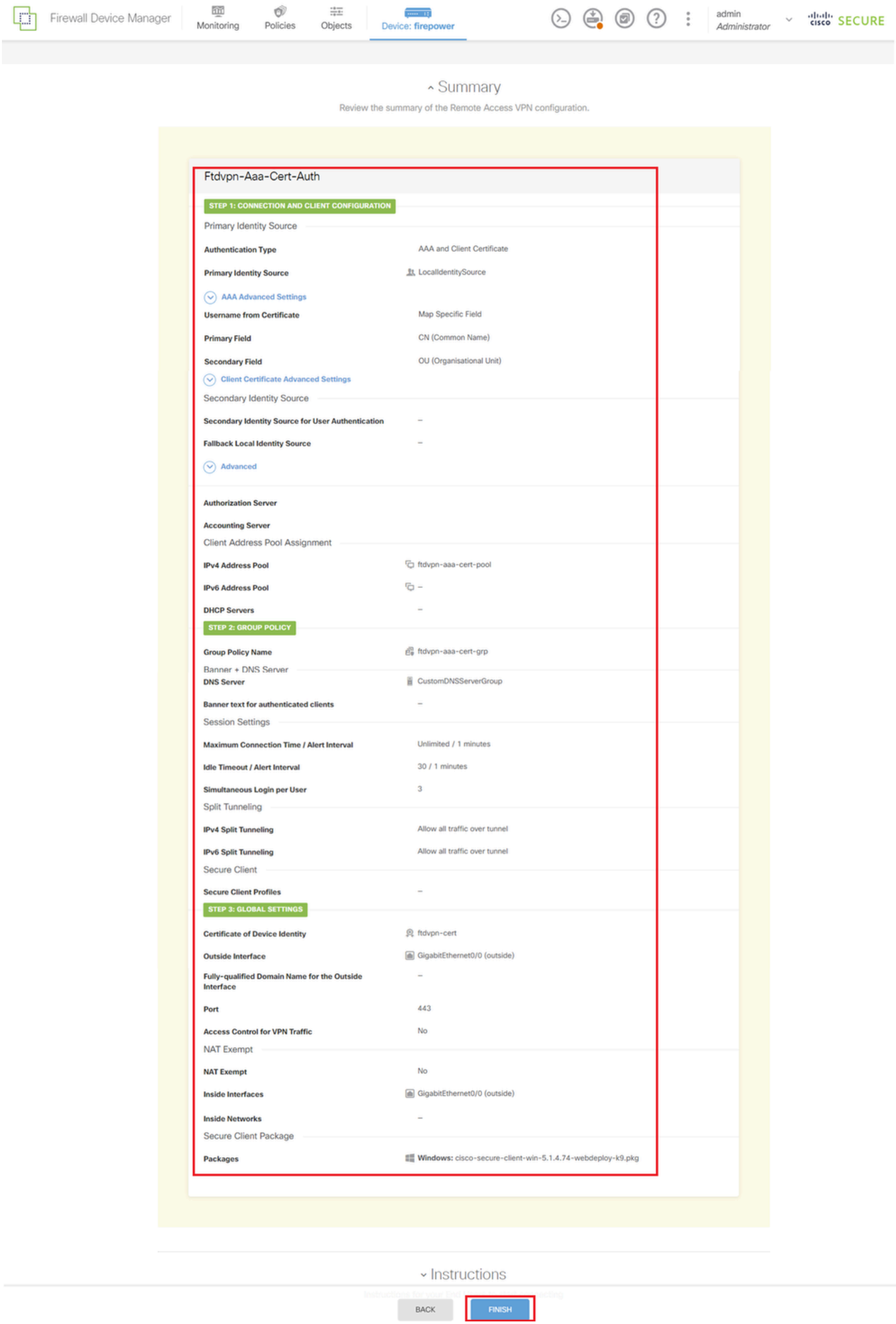
注：このドキュメントでは、NAT免除の機能は無効になっています。デフォルトでは、Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)オプションはディセーブルになっています。これは、復号化されたVPNトラフィックに対してアクセスコントロールポリシーの検査が実行されることを意味します。



Secure Client Image Packageの選択

ステップ 8：接続プロファイルの概要の確認

入力したVPN接続の情報を確認し、FINISHボタンをクリックします。



接続プロファイルの設定の確認

```
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
```

VPNクライアントでの確認

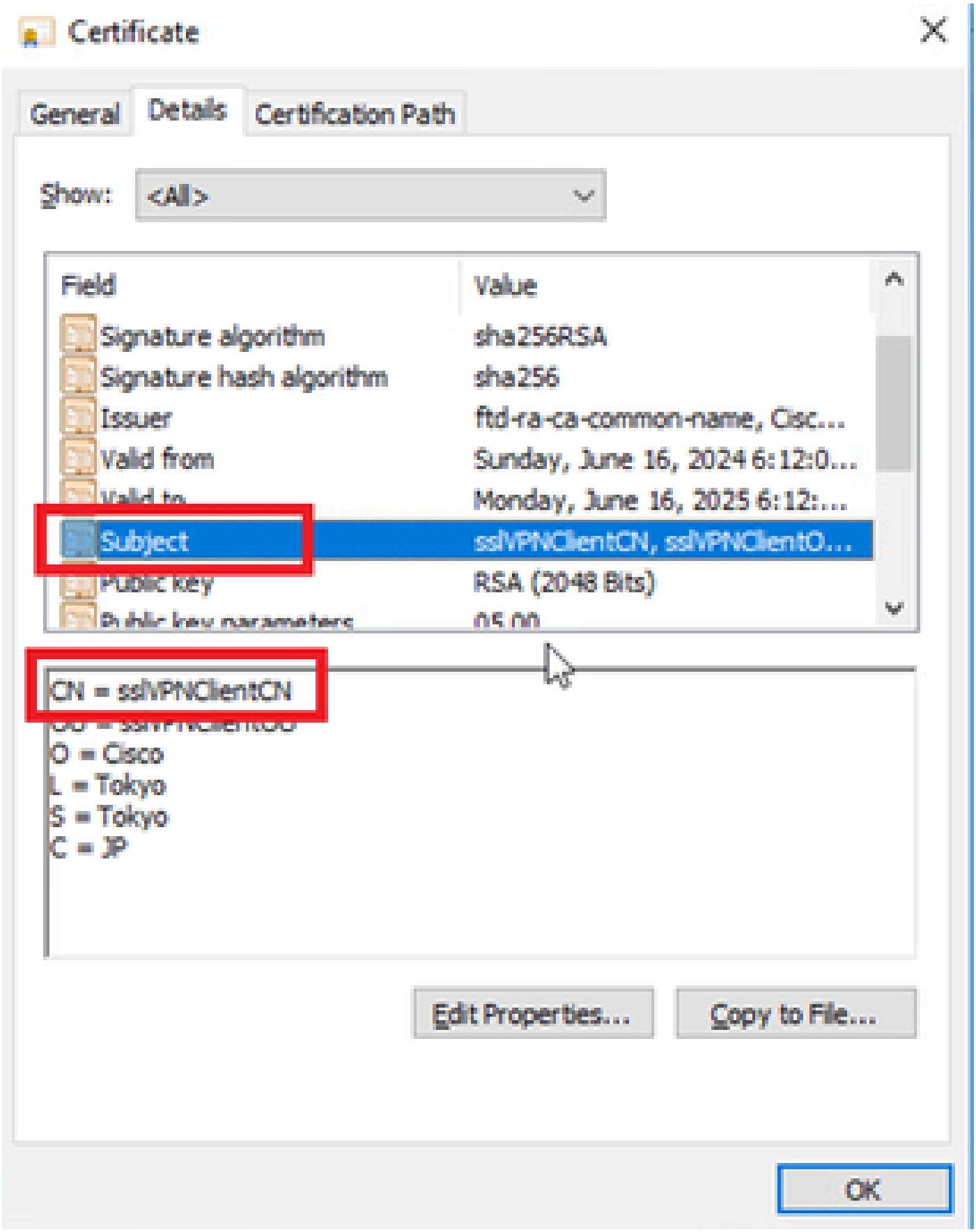
ステップ 1：クライアント証明書の確認

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、ofSubjectの詳細を確認します。

- 件名：CN = sslVPNClientCN



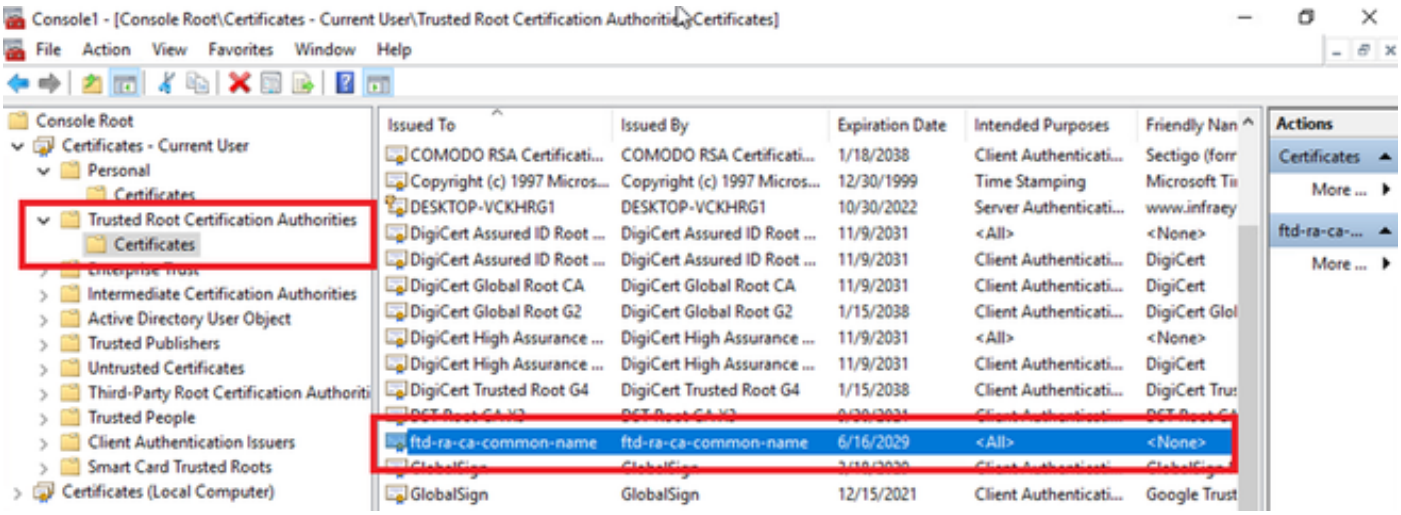
クライアント証明書の詳細

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

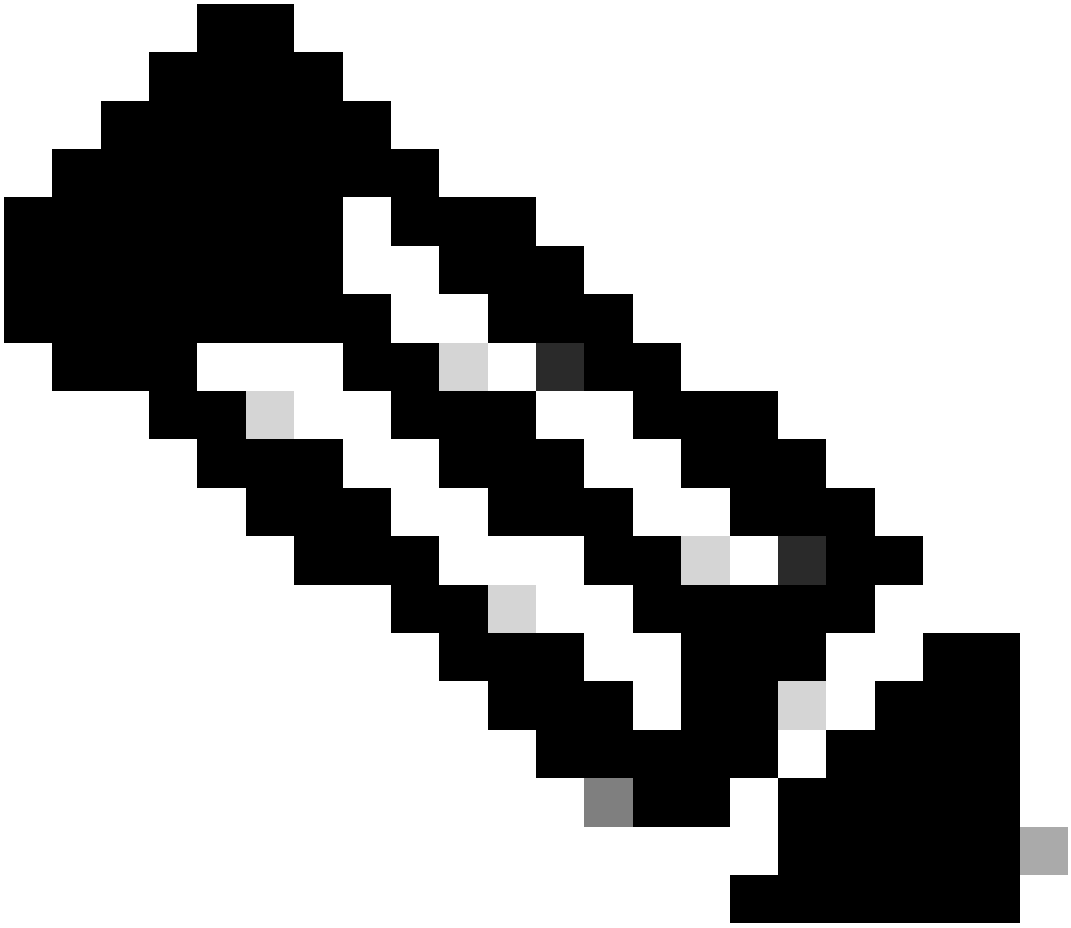


CAの確認

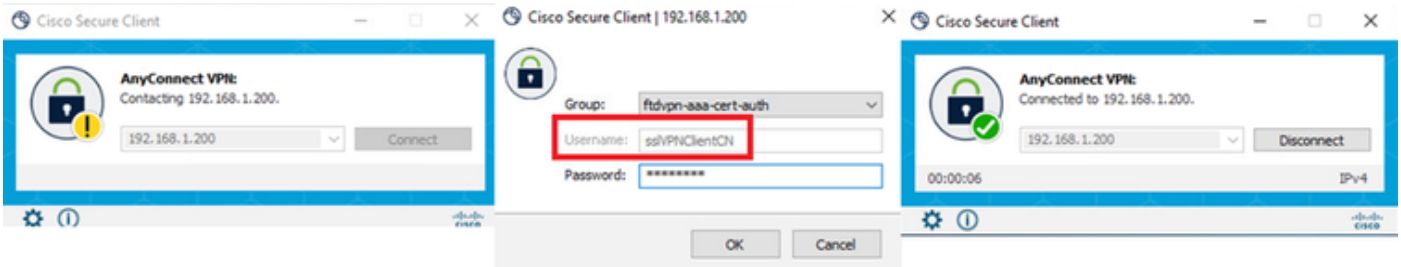
確認

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Common Name（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：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。

```
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 : 000000000004000667ff45e
Security Grp : none Tunnel Zone : 0

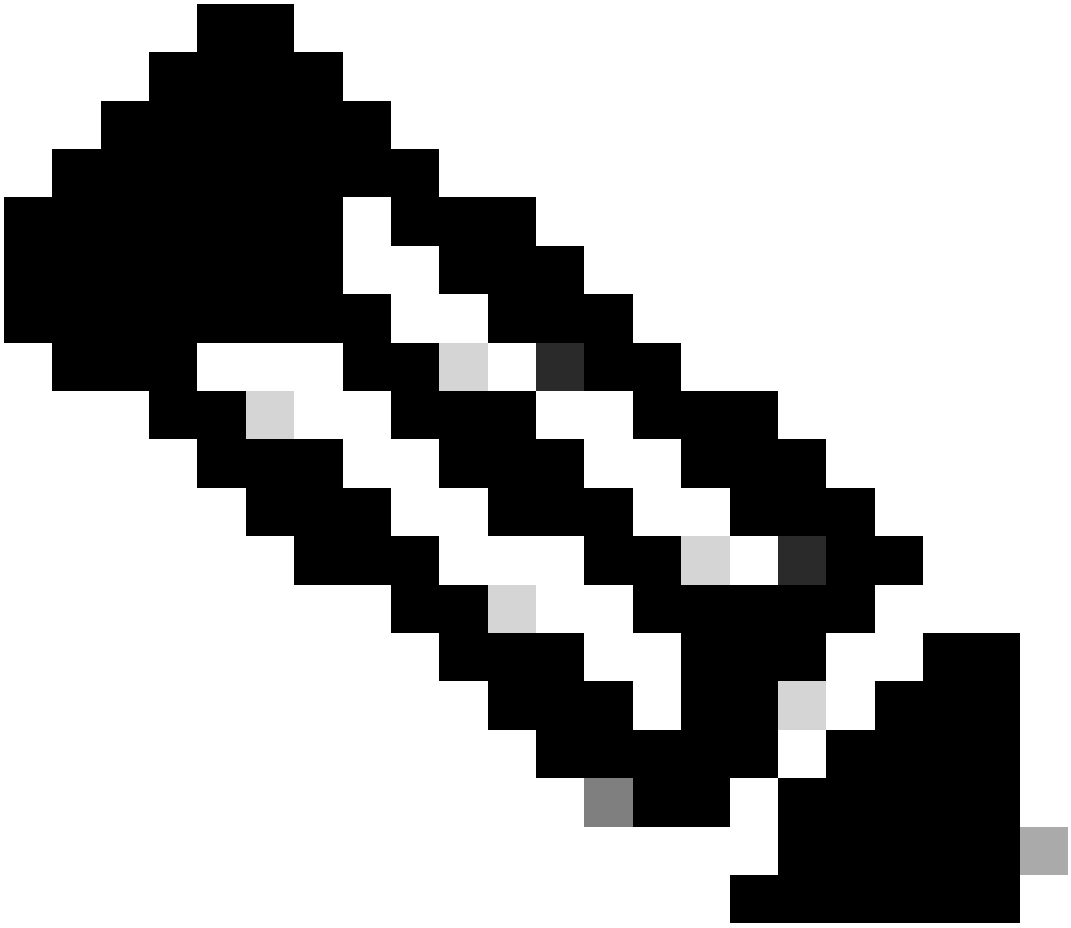
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1

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

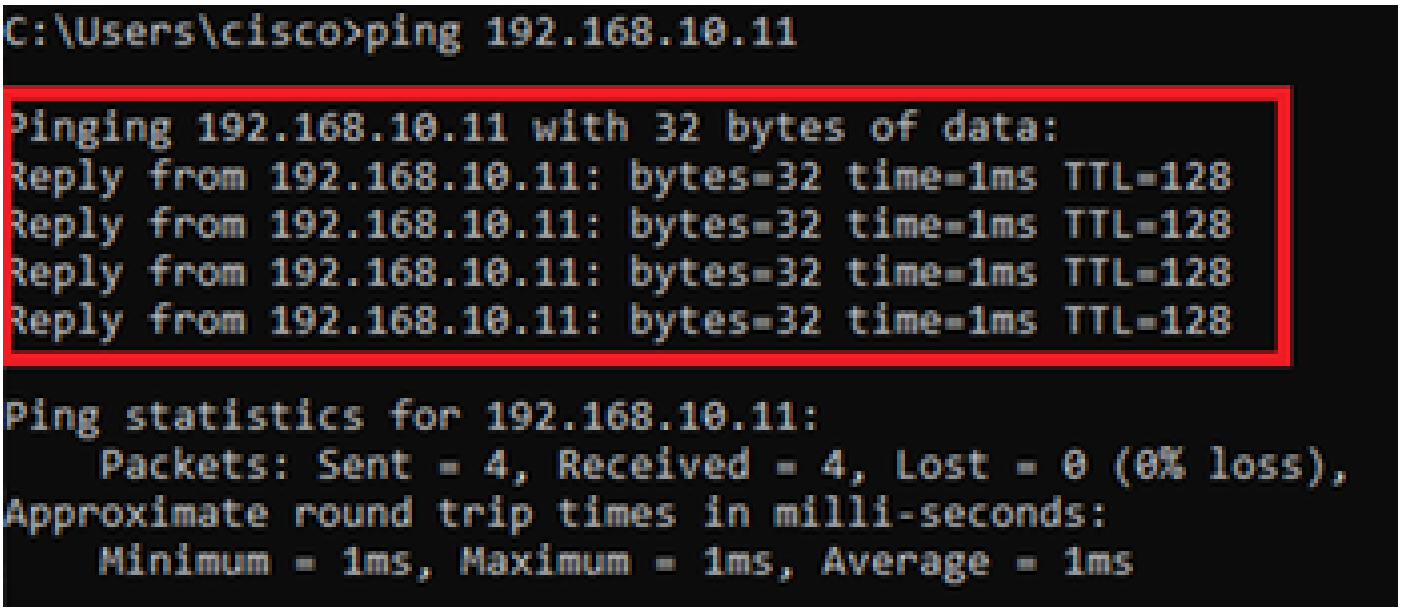
SSL-Tunnel:
Tunnel ID : 4.3
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 49788
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO 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

ステップ 3：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。



注：ステップ7で「復号化されたトラフィックにアクセスコントロールポリシーをバイパスする(sysopt permit-vpn)」オプションが無効になっているため、IPv4アドレスプールがサーバにアクセスできるようにするアクセスコントロールルールを作成する必要があります。



*ping*は成功しました

capture in interface inside real-timeFTD(Lina)CLIでコマンドを実行して、パケットキャプチャを確認します。

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

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、Linaエンジンのデバッグログの例を示します。

// 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
```

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

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。