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

内容

はじめに

このドキュメントでは、バージョン6.5.0以降を実行するオンボックスマネージャFDMによって管理されるFTD上のRA VPNの展開を設定する方法について説明します。

前提条件

要件

シスコでは、Firepower Device Manager(FDM)でのリモートアクセス仮想プライベートネットワーク(RA VPN)の設定に関する知識があることを推奨します。

ライセンス

- Firepower脅威対策(FTD)がスマートライセンスポータルに登録され、エクスポート制御機能が有効になっている（RA VPN設定タブを有効にするために）
- 有効なAnyConnectライセンス（APEX、Plus、またはVPN-Only）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- バージョン6.5.0-115が稼働するCisco FTD
- Cisco AnyConnect セキュア モビリティ クライアント バージョン 4.7.01076

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。

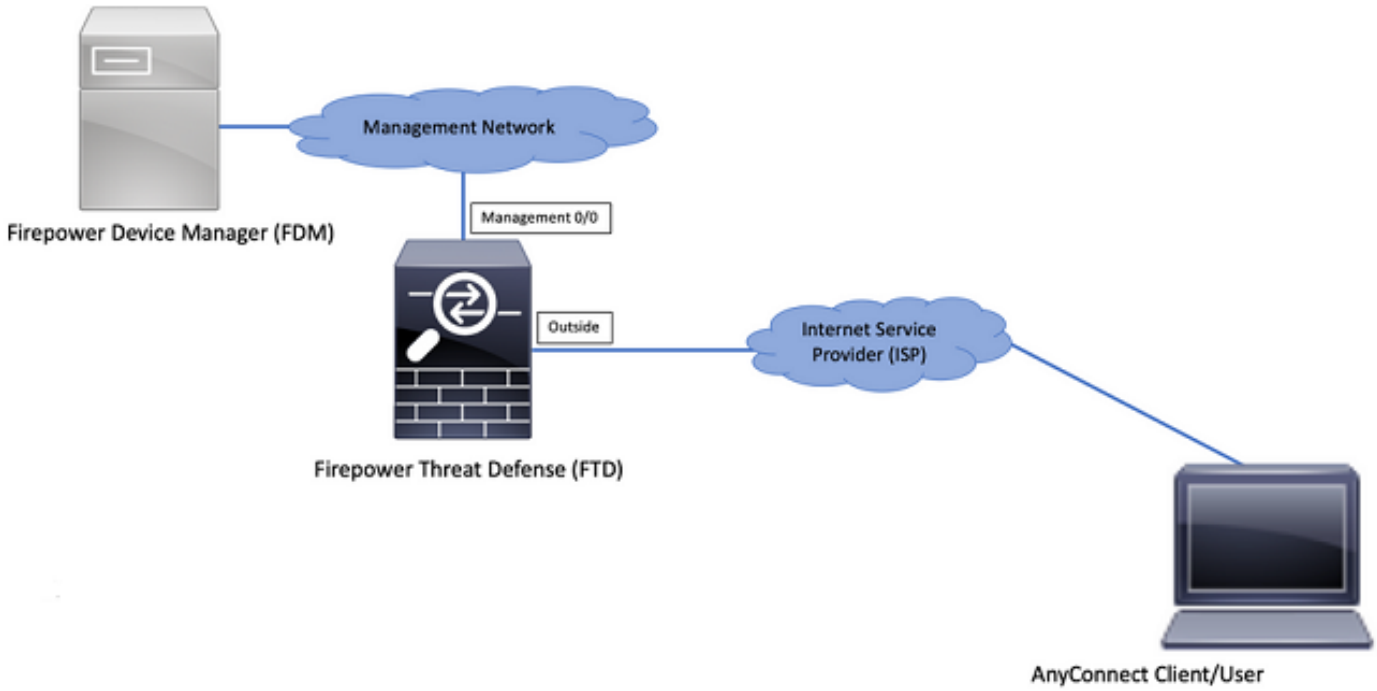
背景説明

FDMを使用したFTDの設定では、同じインターフェイスから管理にアクセスしている間に、外部インターフェイスを使用してAnyConnectクライアントの接続を確立しようとすると困難が生じます。これは、FDMの既知の制限です。この問題については、機能拡張要求CSCvm76499が提起されています。

設定

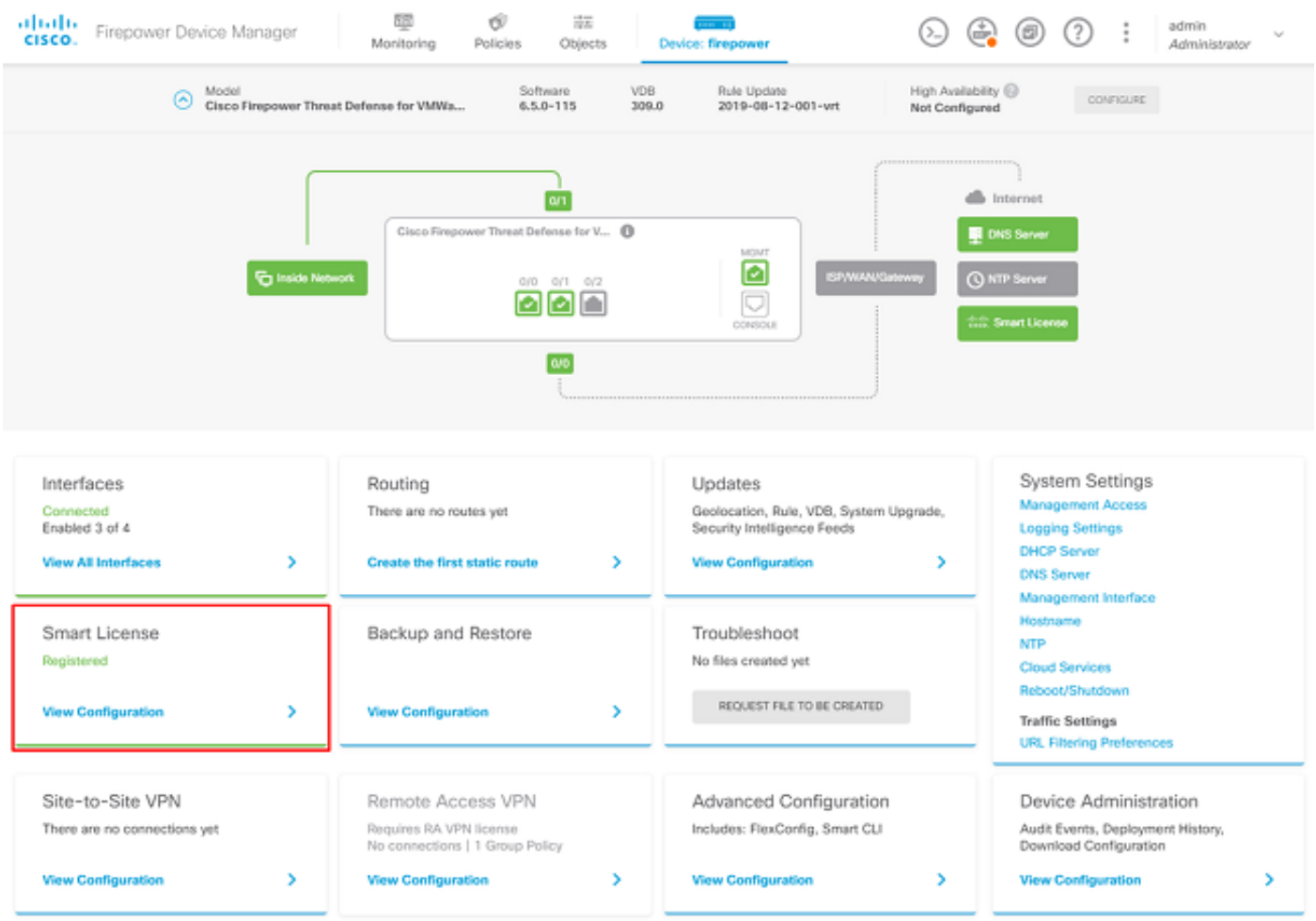
ネットワーク図

ローカルを使用したAnyConnectクライアント認証。

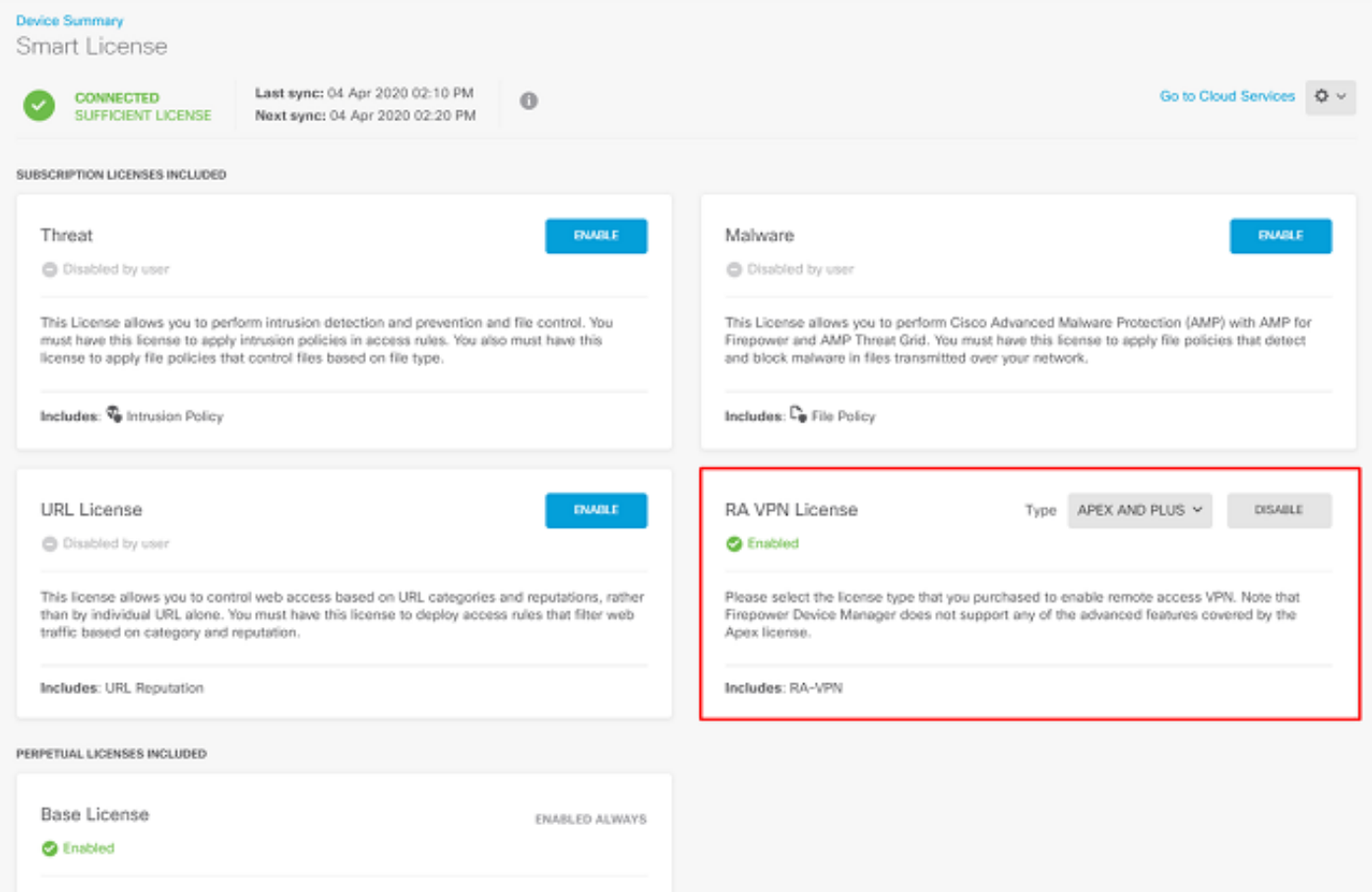


FTDでのライセンスの確認

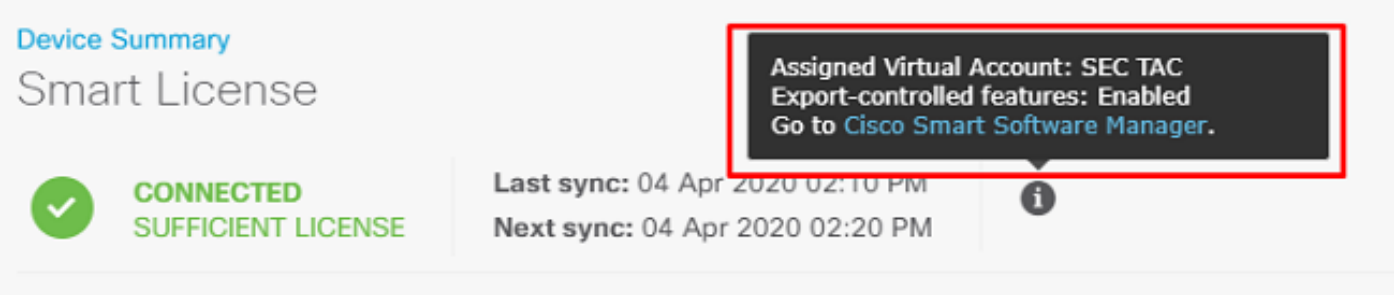
ステップ 1：図に示すように、デバイスがスマートライセンスに登録されていることを確認します。



ステップ 2： 次の図に示すように、デバイスでAnyConnectライセンスが有効になっていることを確認します。

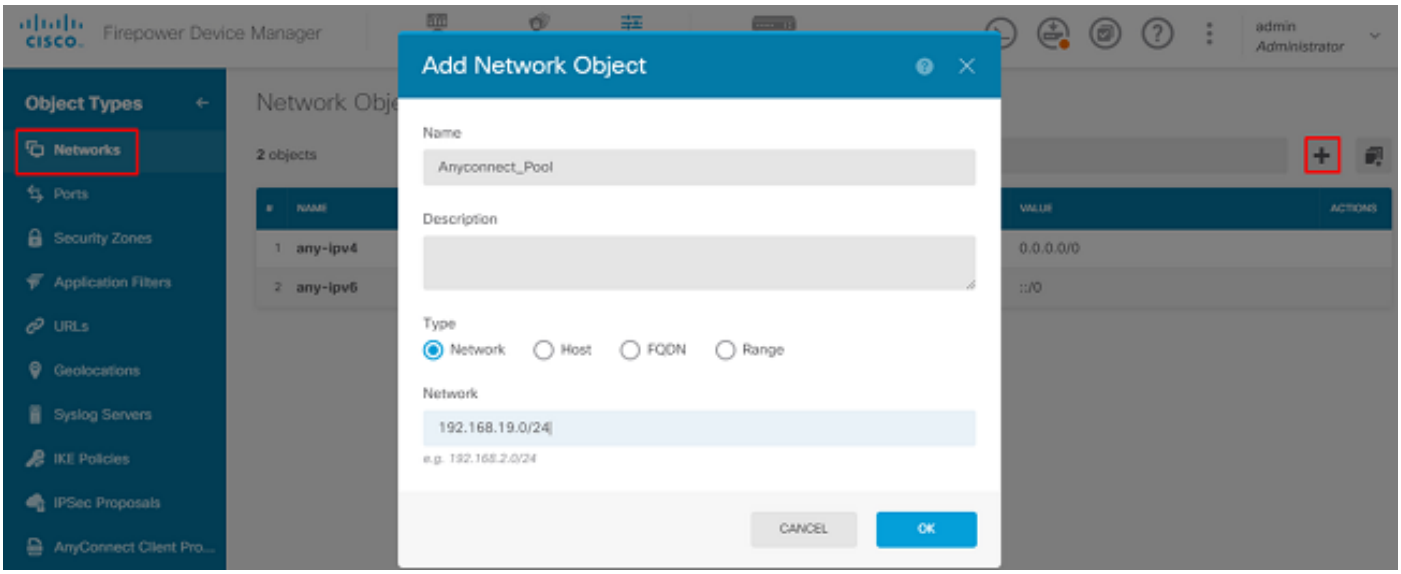


ステップ 3： 図に示すように、トークンでエクスポート制御の機能が有効になっていることを確認します。

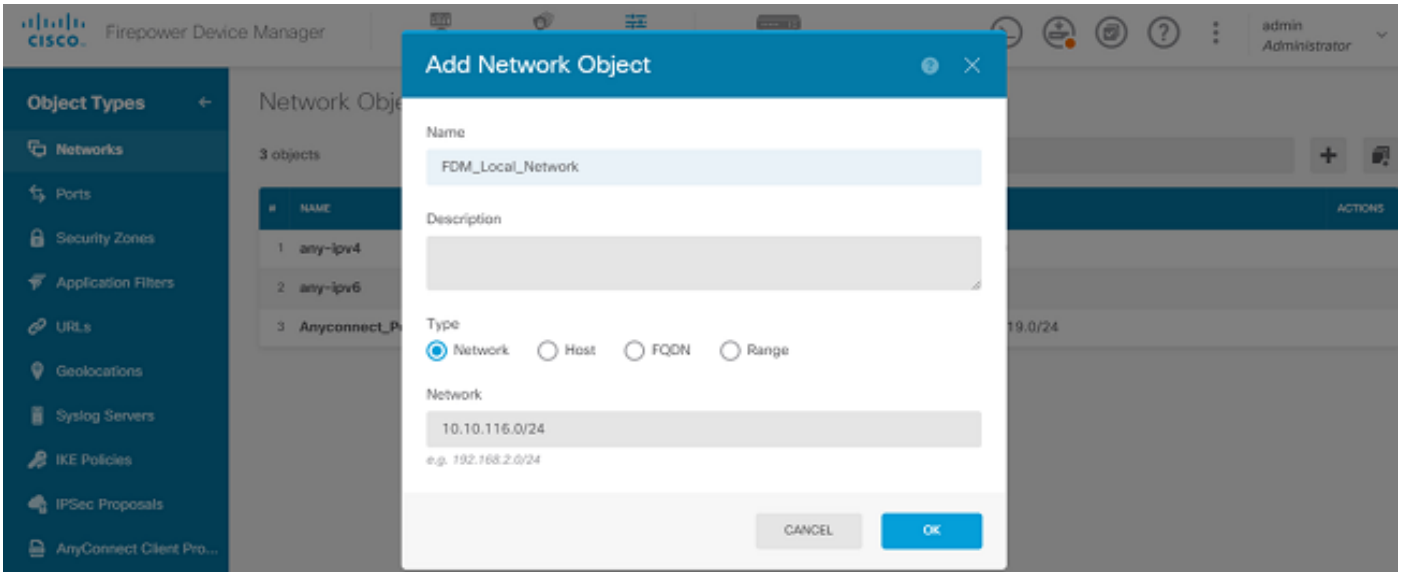


保護されたネットワークの定義

移動先 Objects > Networks > Add new Networkを参照。FDM GUIからVPNプールとLANネットワークを構成します。 図に示すように、AnyConnectユーザへのローカルアドレス割り当てに使用するVPNプールを作成します。

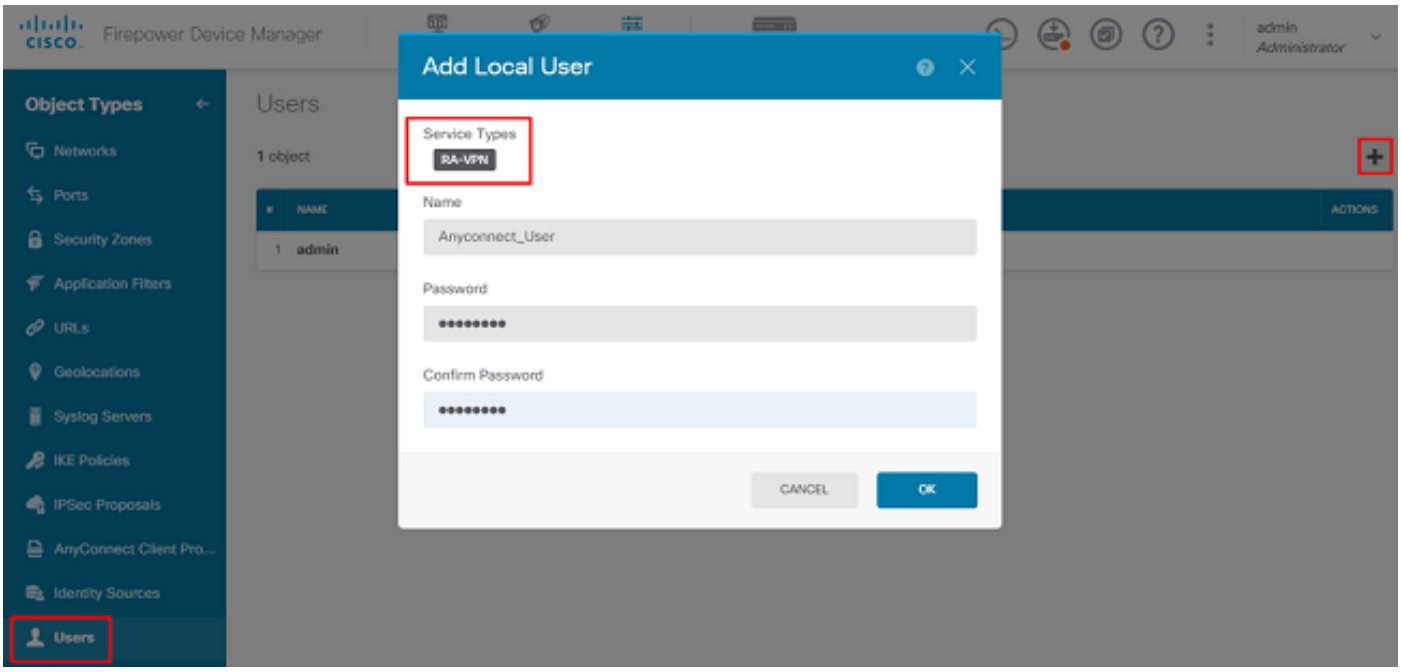


図に示すように、FDMデバイスの背後にあるローカル・ネットワークのオブジェクトを作成します：



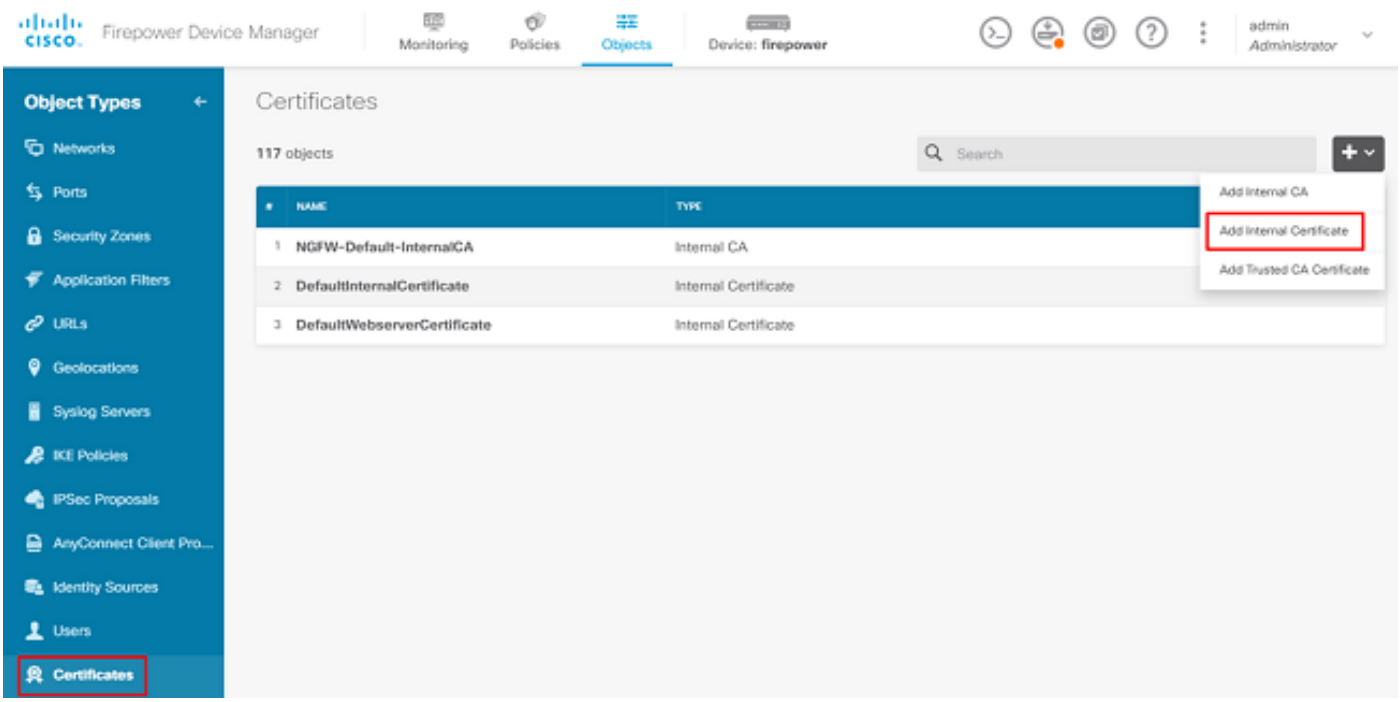
ローカル ユーザの作成

移動先 Objects > Users > Add Userを参照。Anyconnect経由でFTDに接続するVPNローカルユーザを追加します。次の図に示すように、ローカルユーザを作成します。

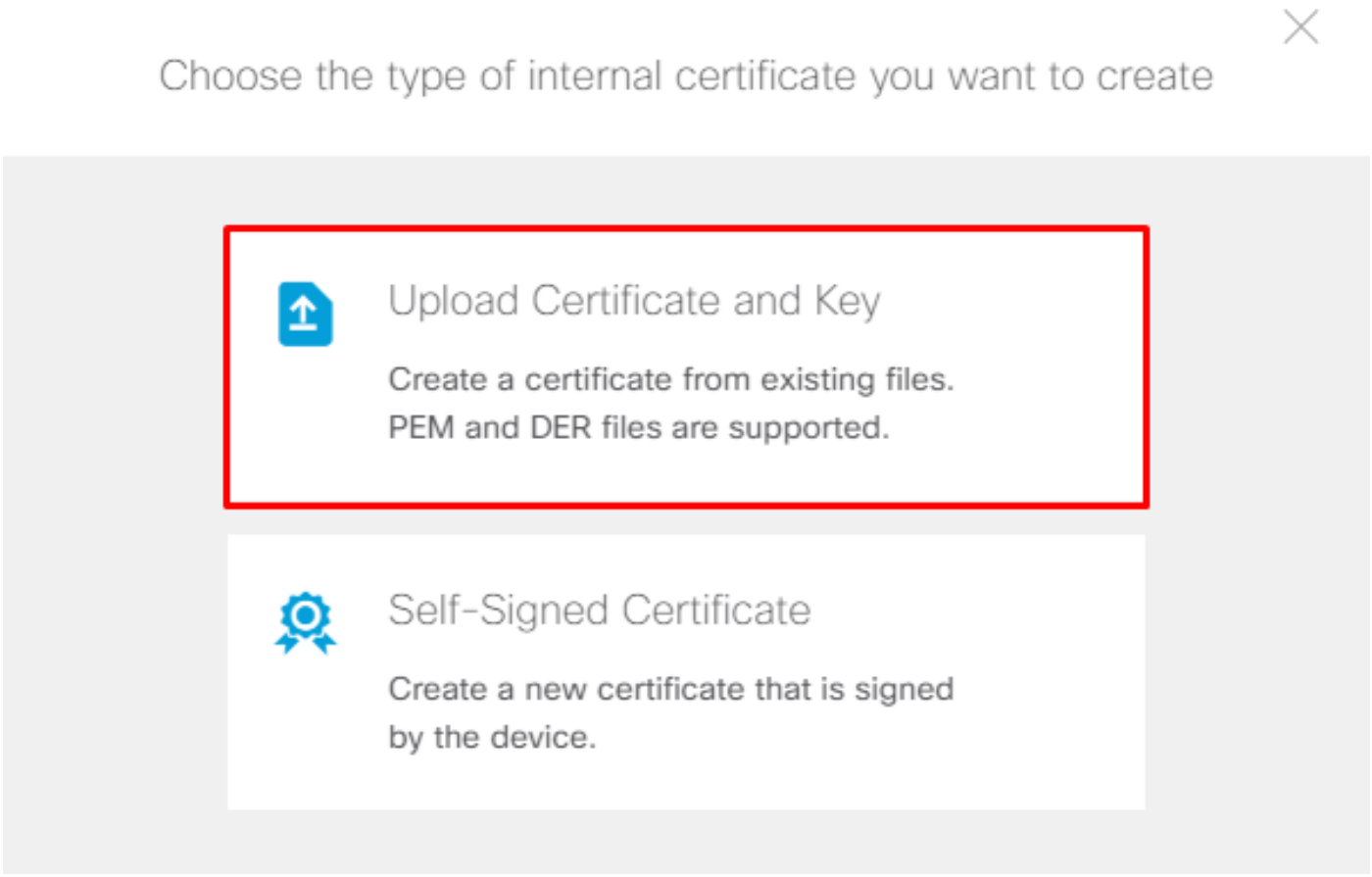


証明書の追加

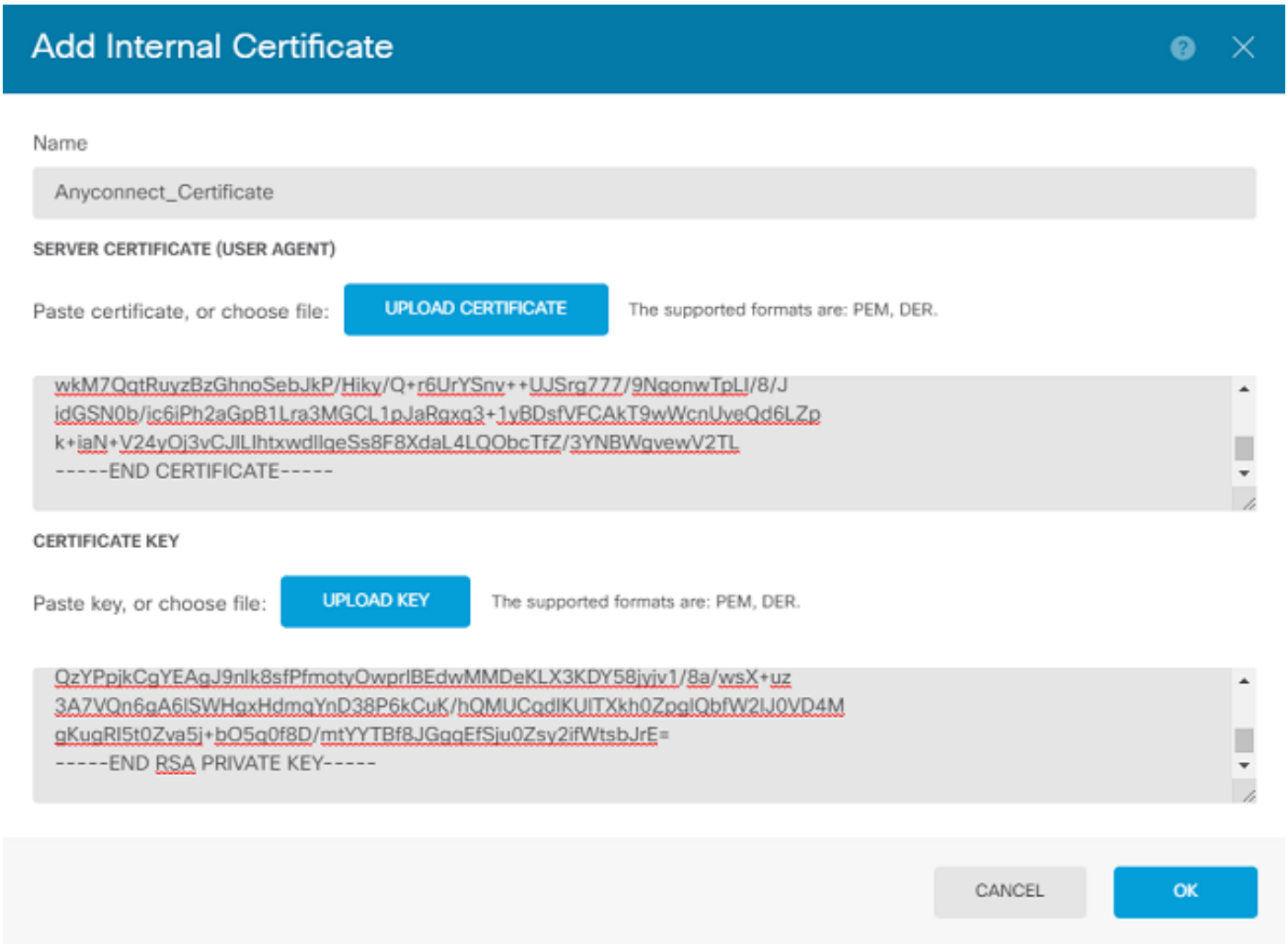
移動先 Objects > Certificates > Add Internal Certificateを参照。 図に示すように、証明書を設定します。



図に示すように、証明書と秘密キーの両方をアップロードします。

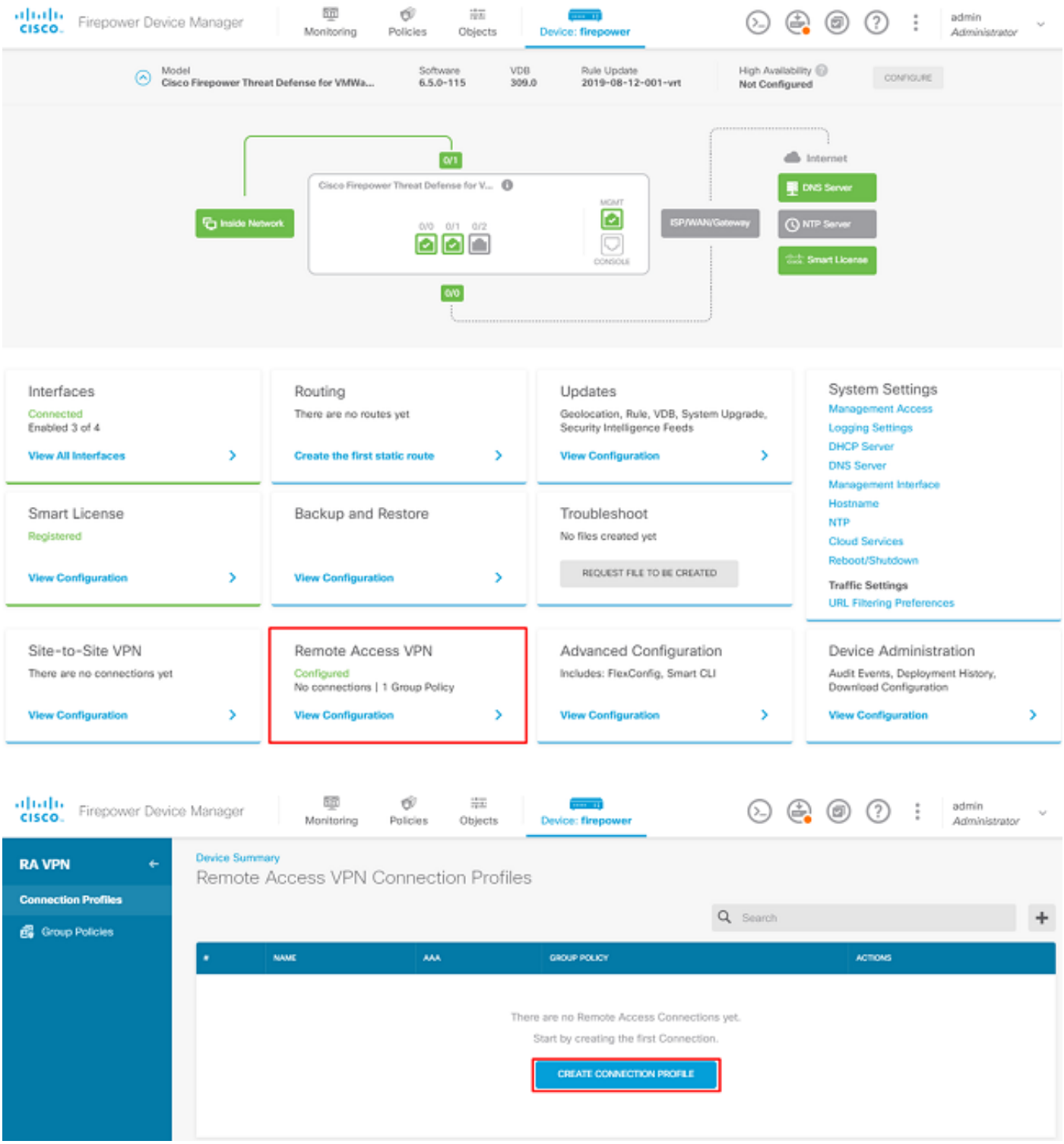


証明書とキーは、次の図に示すように、コピーアンドペーストまたは各ファイルのアップロードボタンでアップロードできます。

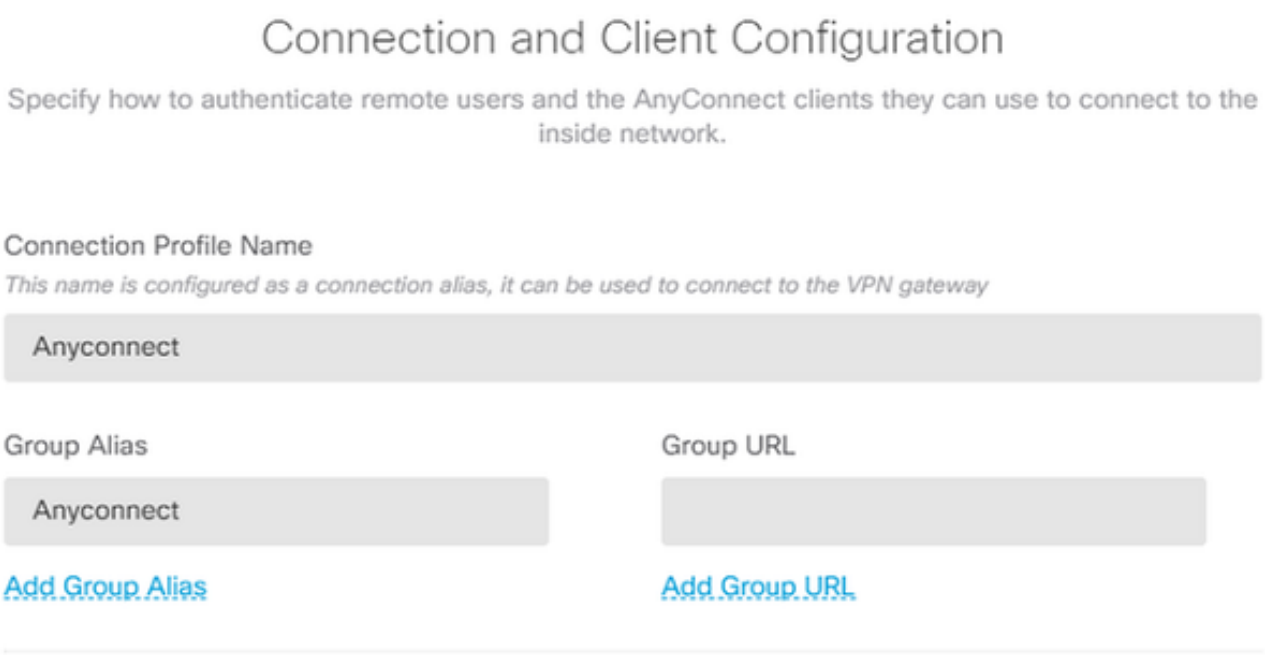


リモートアクセスVPNの設定

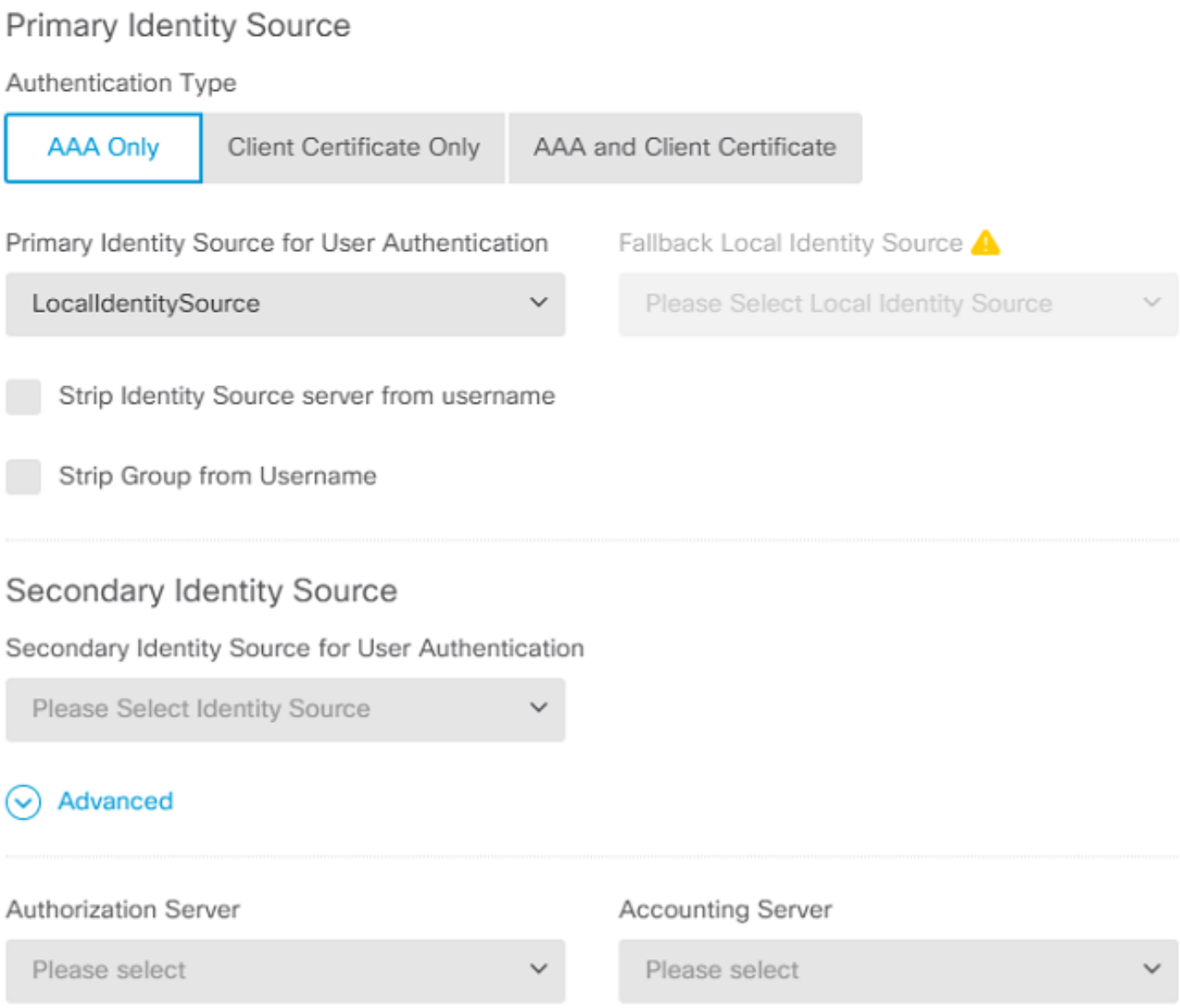
移動先 Remote Access VPN > Create Connection Profileを参照。 図に示すように、FDMでRA VPNウィザードを移動します。



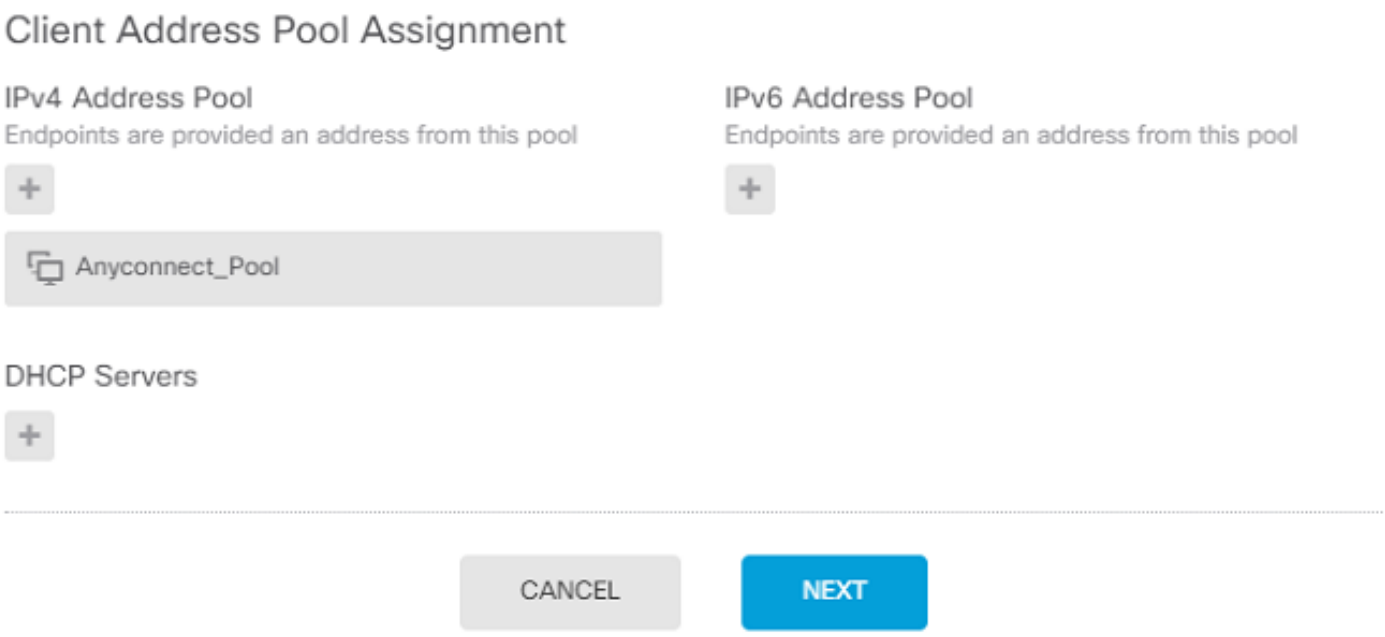
図に示すように、接続プロファイルを作成し、設定を開始します。



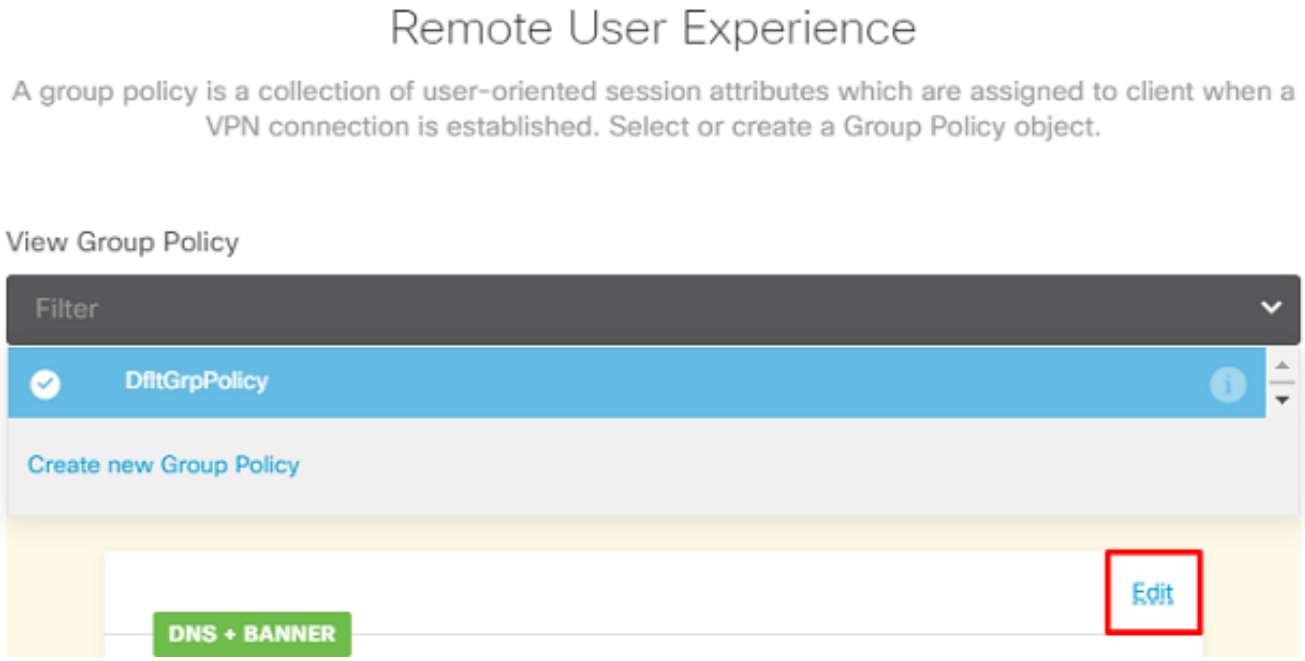
図に示すように、認証方式を選択します。このガイドでは、ローカル認証を使用します。



次のいずれかを選択します Anyconnect_Pool 図に示すオブジェクト：

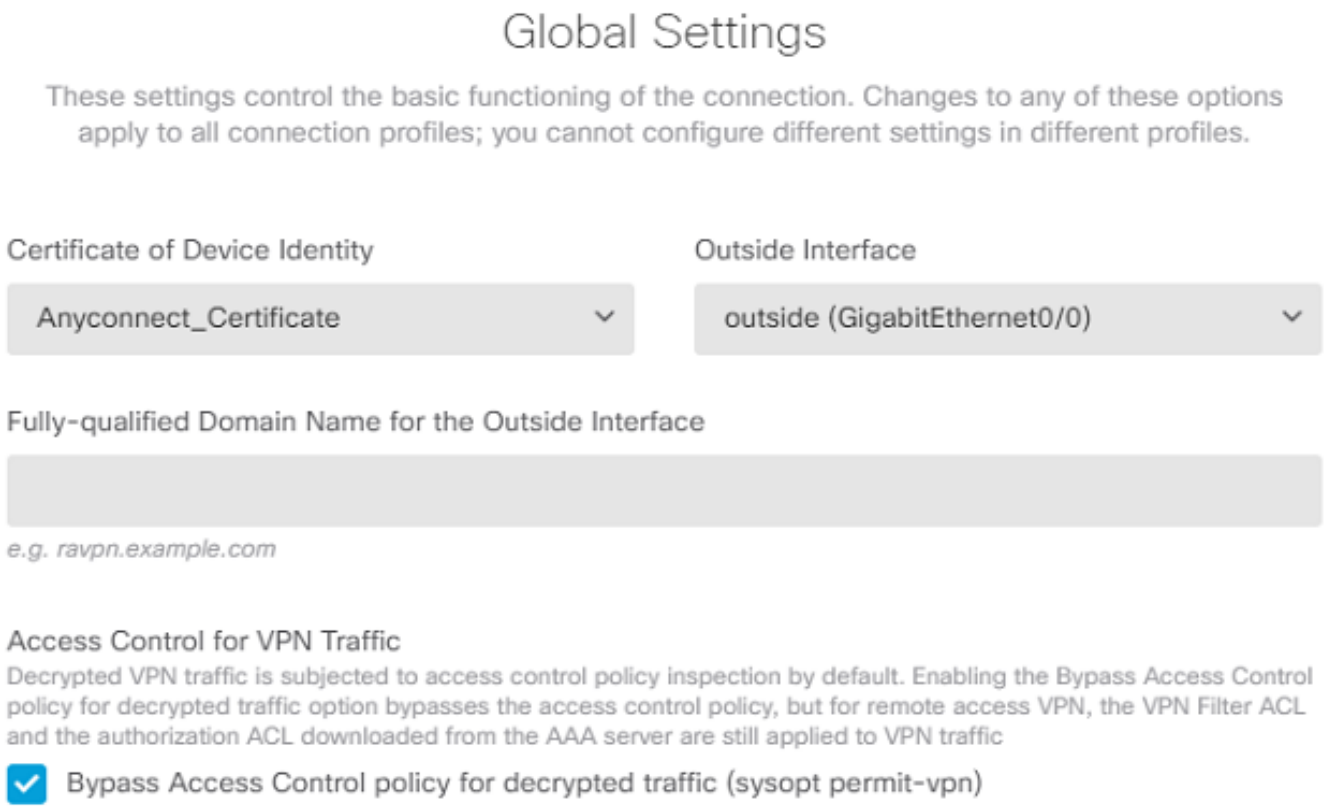


デフォルトのグループポリシーの要約が次のページに表示されます。新しいグループポリシーは、ドロップダウンをクリックして次のオプションを選択すると作成できます Create a new Group Policyを参照。このガイドでは、デフォルトのグループポリシーが使用されます。図に示すように、ポリシーの上部にある編集オプションを選択します。

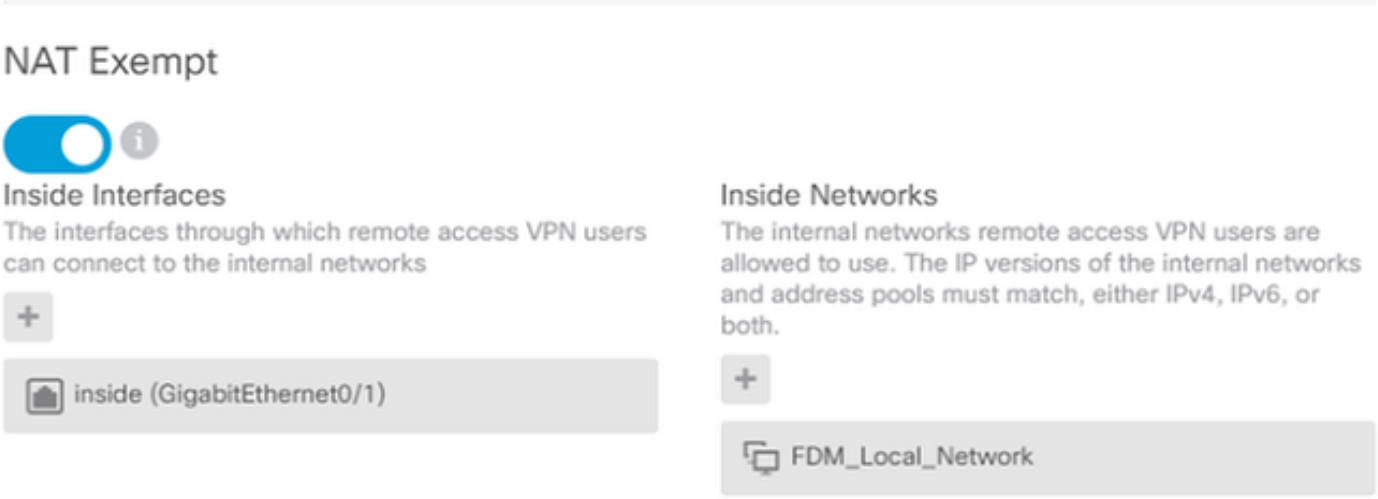


グループポリシーで、スプリットトンネリングを追加します。これにより、Anyconnectに接続されたユーザは、Anyconnectクライアントを介して内部FTDネットワーク宛てのトラフィックのみを送信し、他のすべてのトラフィックは図に示すようにユーザのISP接続から送信されます。

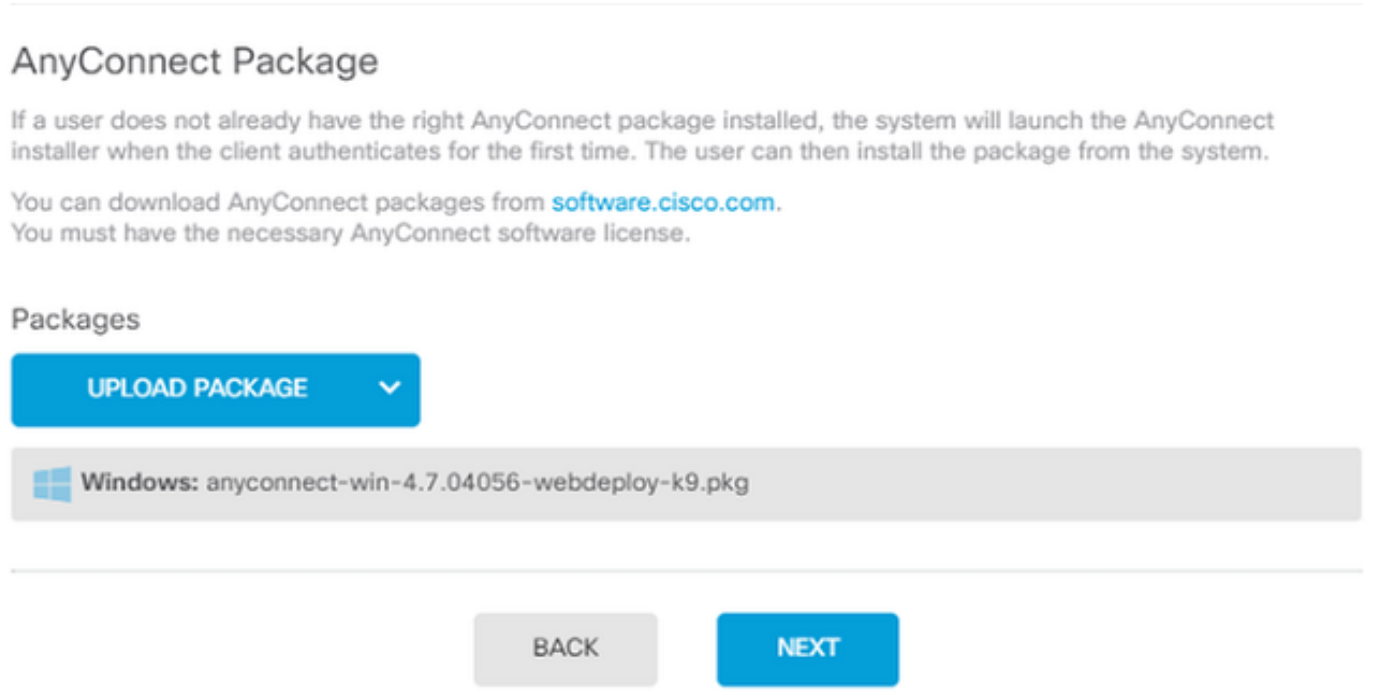
次のページで、 Anyconnect_Certificate 「証明書」セクションに追加されました。 次に、FTDがAnyConnect接続をリッスンするインターフェイスを選択します。 復号化されたトラフィックのBypass Access Controlポリシー(sysopt permit-vpn)。このコマンドは、 sysopt permit-vpn が選択されていません。次の図に示すように、Anyconnectクライアントからのトラフィックが内部ネットワークにアクセスできるようにするアクセスコントロールポリシーを作成する必要があります。



NAT免除は、 Policies > NAT または、ウィザードで自動的に設定することもできます。図に示すように、Anyconnectクライアントがアクセスするために必要な内部インターフェイスとネットワークを選択します。



図に示すように、ユーザが接続できる各オペレーティングシステム(Windows/Mac/Linux)のAnyconnectパッケージを選択します。



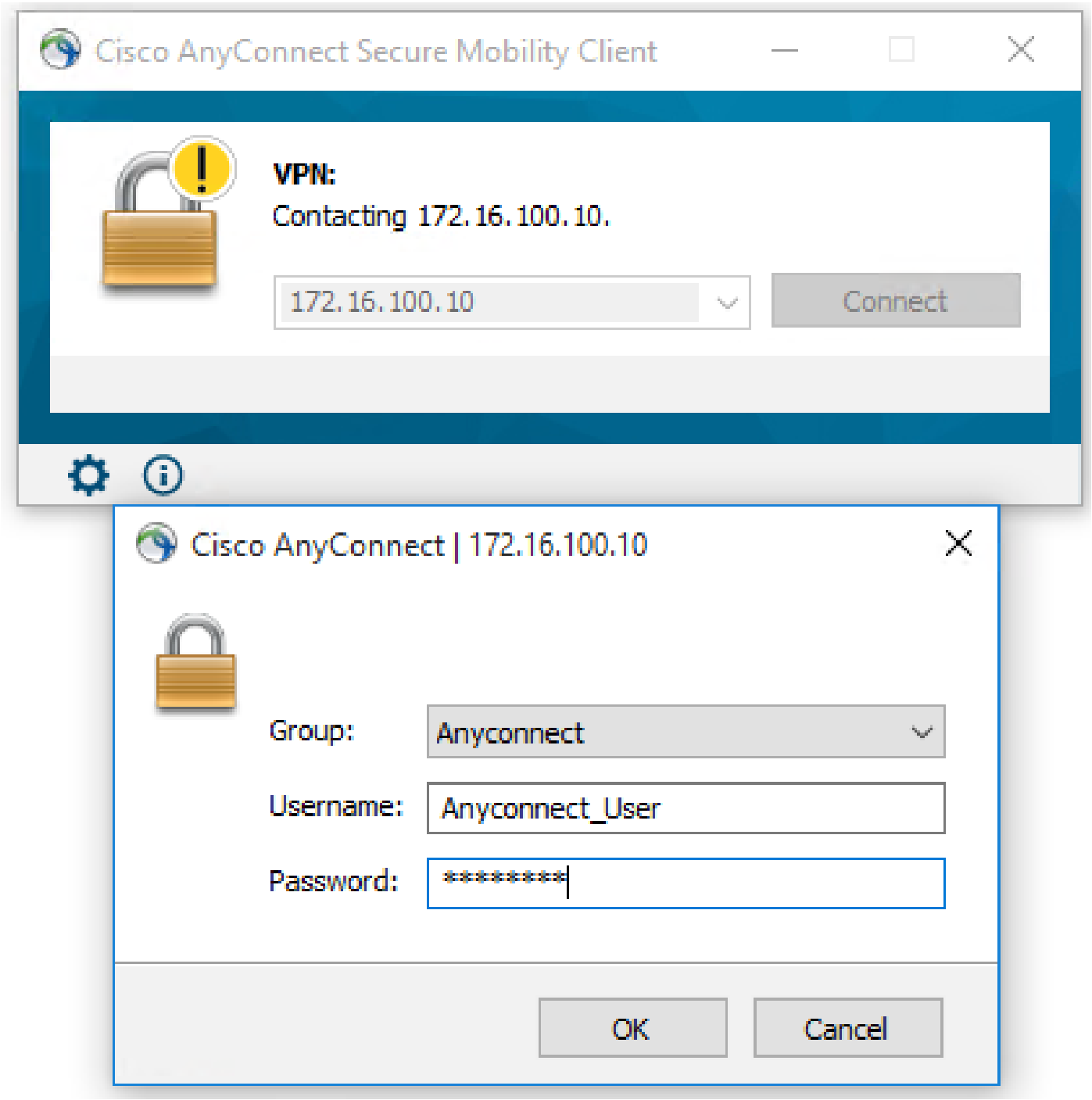
最後のページには、設定全体の概要が表示されます。正しいパラメータが設定されていることを確認し、Finishボタンを押して新しい設定を導入します。

確認

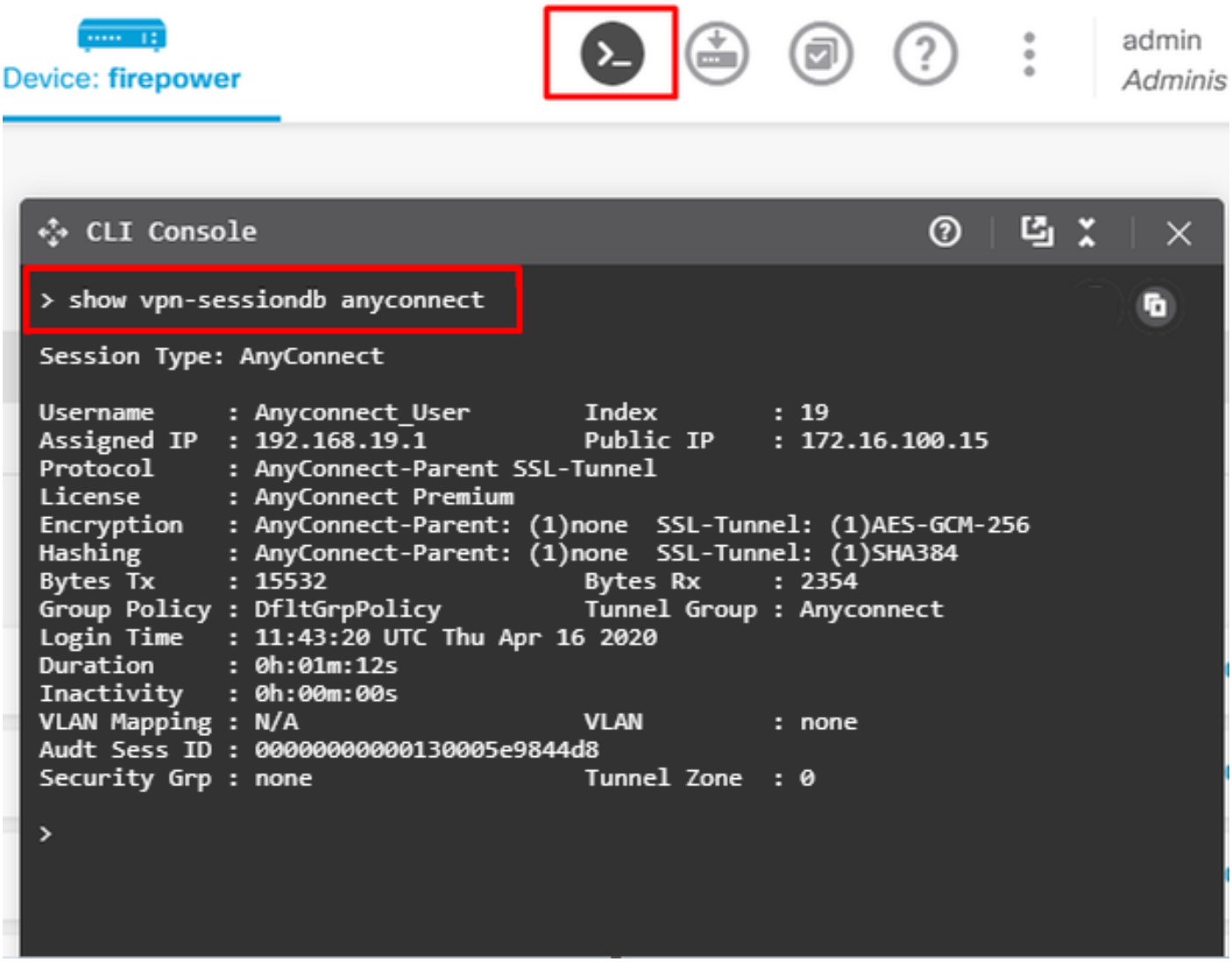
ここでは、設定が正常に機能しているかどうかを確認します。

設定を展開したら、接続を試みます。FTDの外部IPに解決されるFQDNがある場合は、それをAnyconnect接続ボックスに入力します。この例では、FTDの外部IPアドレスが使用されます。図に示すように、FDMのオブジェクト・セクションで作成されたユーザー名/パスワードを使用しま

す。



FDM 6.5.0の時点では、FDM GUIを使用してAnyconnectユーザを監視する方法はありません。唯一のオプションは、CLIを介してAnyconnectユーザをモニタすることです。FDM GUIのCLIコンソールを使用して、ユーザーが接続されていることを確認することもできます。次のコマンドを使用します。 Show vpn-sessiondb anyconnect.



同じコマンドをCLIから直接実行できます。

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : Anyconnect_User        Index        : 15
Assigned IP  : 192.168.19.1           Public IP    : 172.16.100.15
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     : 38830                  Bytes Rx     : 172
Group Policy : DfltGrpPolicy          Tunnel Group : Anyconnect
Login Time   : 01:08:10 UTC Thu Apr 9 2020
Duration     : 0h:00m:53s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 000000000000f0005e8e757a
Security Grp : none                   Tunnel Zone  : 0
```

トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を説明します。

ユーザがSSLを使用してFTDに接続できない場合は、次の手順を実行してSSLネゴシエーションの問題を切り分けます。

1. FTDの外部のIPアドレスにユーザのコンピュータからpingが通ることを確認します。
2. TCPスリーウェイハンドシェイクが成功しているかどうかを確認するには、外部スニファを使用します。

AnyConnectクライアントの問題

このセクションでは、AnyConnect VPN Clientに関する最も一般的な2つの問題をトラブルシューティングするためのガイドラインを示します。AnyConnectクライアントのトラブルシューティングガイドについては、『AnyConnect VPN Client Troubleshooting Guide』を参照してください。

初期接続の問題

ユーザに初期接続の問題がある場合は、debugを有効にします webvpn FTDでAnyConnectを使用して、デバッグメッセージを分析します。デバッグはFTDのCLIで実行する必要があります。次のコマンドを使用します。 debug webvpn anyconnect 255を参照。

AnyConnectからログを取得するために、クライアントマシンからDARTバンドルを収集します。DARTバンドルの収集方法については、「DARTバンドルの収集」を参照してください。

トラフィック固有の問題

接続が成功しても、トラフィックがSSL VPNトンネルで失敗する場合は、クライアントのトラフィック統計情報を調べて、トラフィックがクライアントで送受信されていることを確認します。クライアントの詳細な統計情報は、AnyConnectのすべてのバージョンで利用できます。クライアントがトラフィックの送受信を示している場合は、FTDで送受信されたトラフィックを確認します。FTDがフィルタを適用している場合、フィルタ名が表示され、トラフィックがドロップされているかどうかを確認するためにACLエントリを調べることができます。ユーザが経験する一般的なトラフィックの問題は次のとおりです。

- FTDのルーティングの問題：内部ネットワークが、割り当てられたIPアドレスとVPNクライアントにパケットをルーティングして戻すことができません。
- トラフィックをブロックするアクセスコントロールリスト
- VPNトラフィックに対するネットワークアドレス変換(NAT)がバイパスされていない

FDMによって管理されるFTDでのリモートアクセスVPNの詳細については、FDMによって管理されるリモートアクセスFTDの完全なコンフィギュレーションガイドを参照してください。

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。