FTDでのAnyConnectリモートアクセスVPNの設定

内容

概要

このドキュメントでは、FTDでのAnyConnectリモートアクセスVPNの設定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。

- VPN、TLS、およびIKEv2の基礎知識
- 認証、認可、およびアカウンティング（AAA）、および RADIUS に関する基本的な知識
- Firepower Management Centerの使用経験

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。

- Cisco FTD 7.2.0
- Cisco FMC 7.2.1

- AnyConnect 4.10

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、初期（デフォルト）設定の状態から起動しています。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

このドキュメントでは、リモートアクセスVPNでTransport Layer Security(TLS)とInternet Key Exchange(IKEv2)バージョン2(IKEv2)を使用できるようにする、Firepower Threat Defense(FTD)バージョン7.2.0以降の設定例について説明します。Cisco AnyConnectはクライアントとして使用でき、複数のプラットフォームでサポートされています。

コンフィギュレーション

1. 前提条件

Firepower Management Center(FMC)でリモートアクセスウィザードを実行するには、次の手順を実行します。

- サーバ認証に使用する証明書を作成します。
- ユーザ認証用にRADIUSサーバまたはLDAPサーバを設定します。
- VPNユーザ用のアドレスプールを作成します。
- 異なるプラットフォームのAnyConnectイメージをアップロードします。

a) SSL証明書のインポート

証明書は、AnyConnectを設定するときに不可欠です。Webブラウザでのエラーを回避するために、証明書にはDNS名やIPアドレスを含むサブジェクト代替名拡張子が必要です。

注：内部ツールとバグ情報にアクセスできるのは、登録されたシスコユーザだけです。

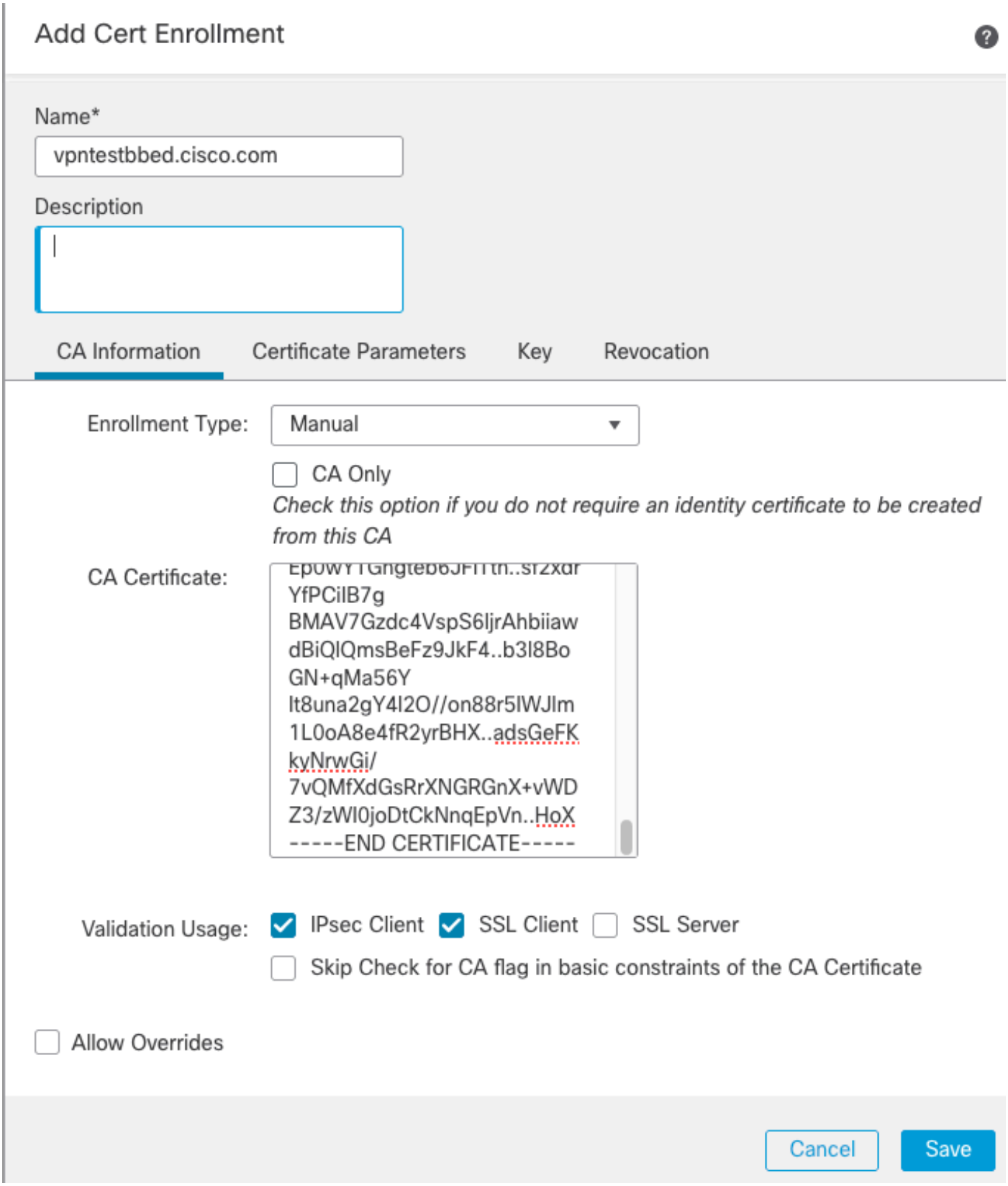
証明書の手動登録には、次のような制限があります。

- FTDでは、CSRを生成する前にCA証明書が必要です。

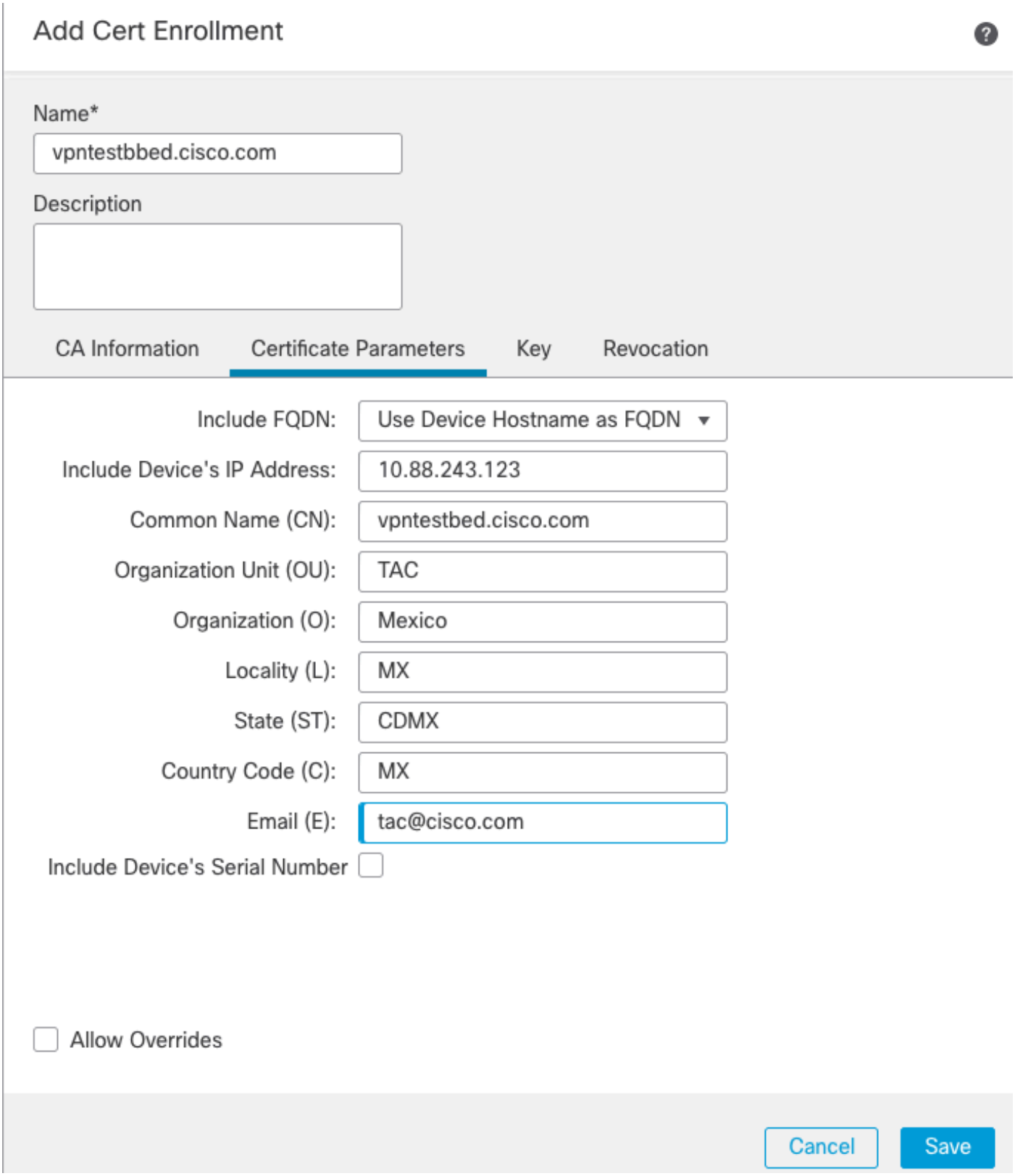
- CSRが外部で生成された場合、手動の方法が失敗し、別の方法を使用する必要があります(PKCS12)。

FTDアプライアンスで証明書を取得するには複数の方法がありますが、安全かつ簡単な方法は、証明書署名要求(CSR)を作成し、認証局(CA)で署名してから、CSRに含まれる公開キーに対して発行された証明書をインポートすることです。その方法を次に示します。

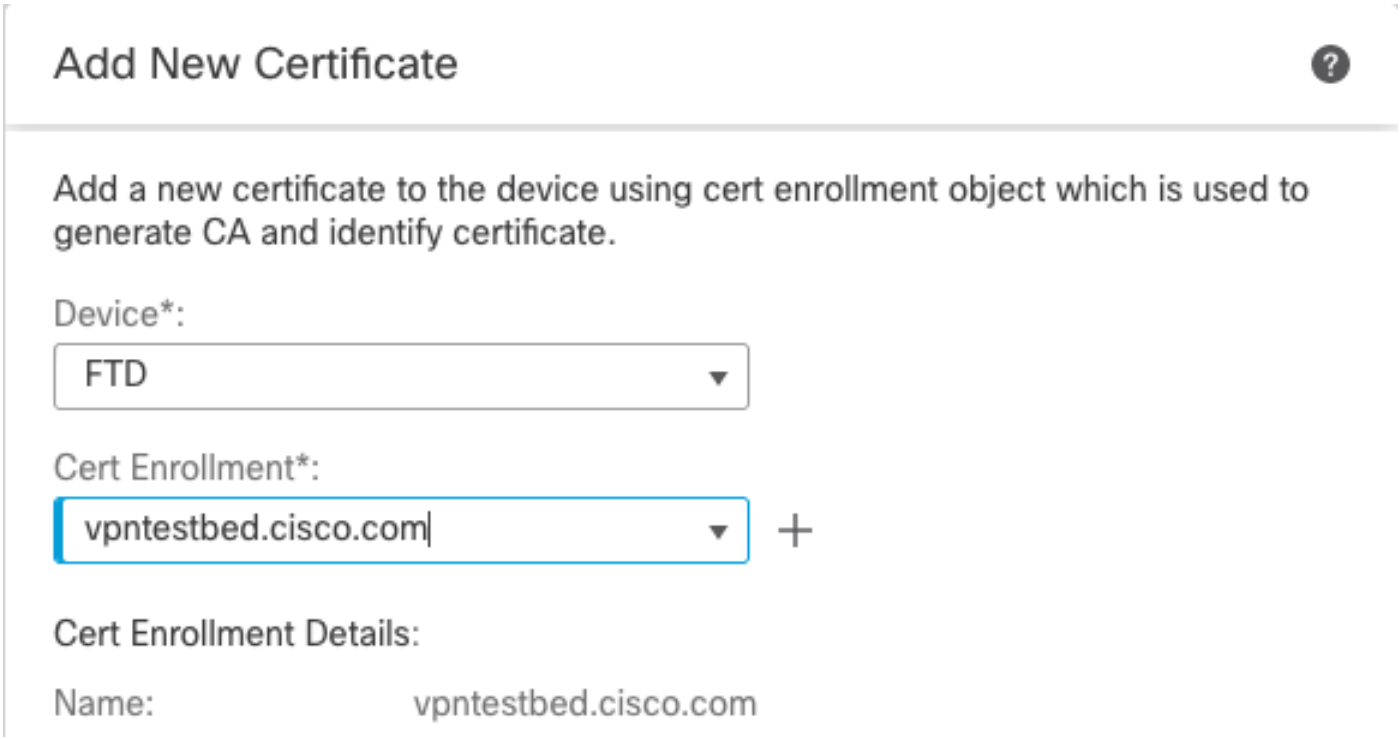
- 次に Objects > Object Management > PKI > Cert Enrollment [Add Cert Enrollment] をクリックします。



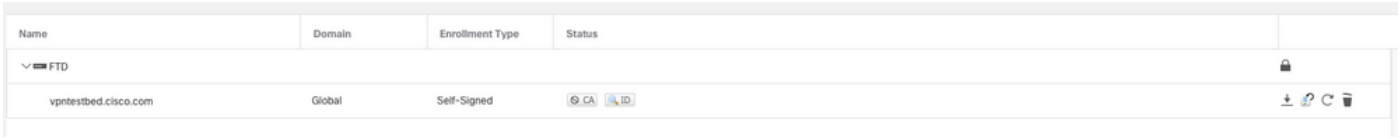
- 選択 Enrollment Type [Certificate Authority (CA) certificate （CSRの署名に使用される証明書）]を貼り付けます。
- 次に、2番目のタブに移動し、 Custom FQDN 必要なフィールドをすべて入力します。次に例を示します。



- 3番目のタブで、 Key Type、名前とサイズを選択します。RSAの場合、2048ビット以上です。
- [保存(Save)]をクリックして、 Devices > Certificates > Add > New Certificate.
- 次に、 Device、およびの下 Cert Enrollment 作成したトラストポイントを選択し、 Add:

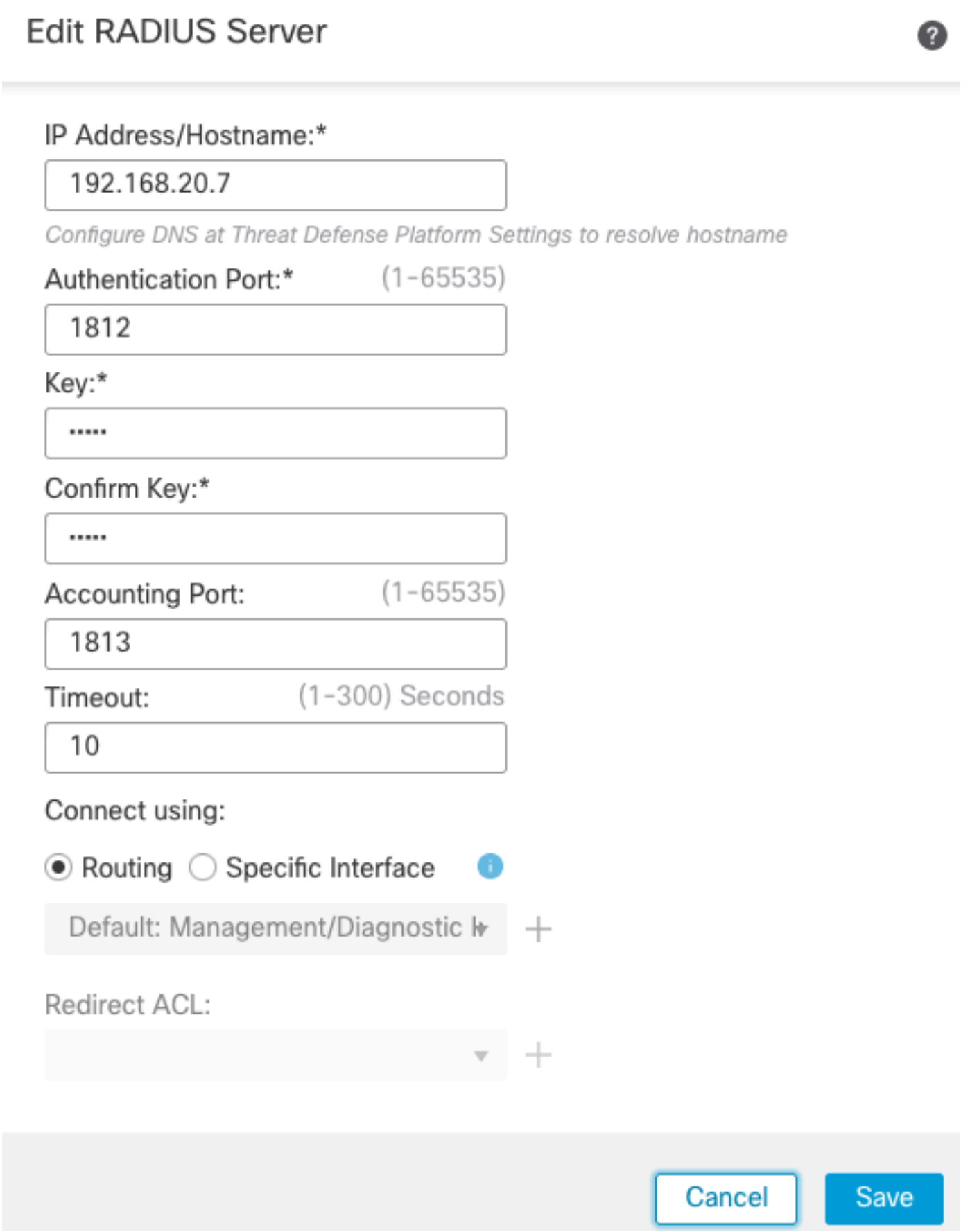


- 後で、トラストポイント名の横にある アイコンをクリックし、 Yesその後、CSRをCAにコピーして署名します。 証明書には、通常のHTTPSサーバと同じ属性が必要です。
- CAからbase64形式の証明書を受信したら、ディスクから選択し、 Import.これが成功すると、次のように表示されます。

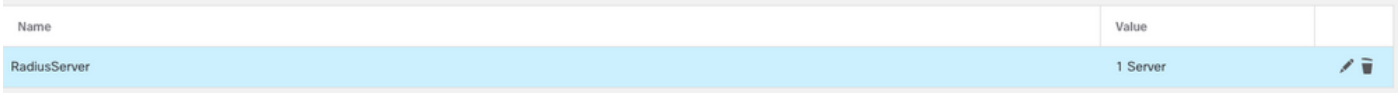


b) RADIUSサーバの設定

- 次に **Objects > Object Management > RADIUS Server Group > Add RADIUS Server Grou**p.
- 名前を入力し、IPアドレスと共有秘密を追加して、 Save:

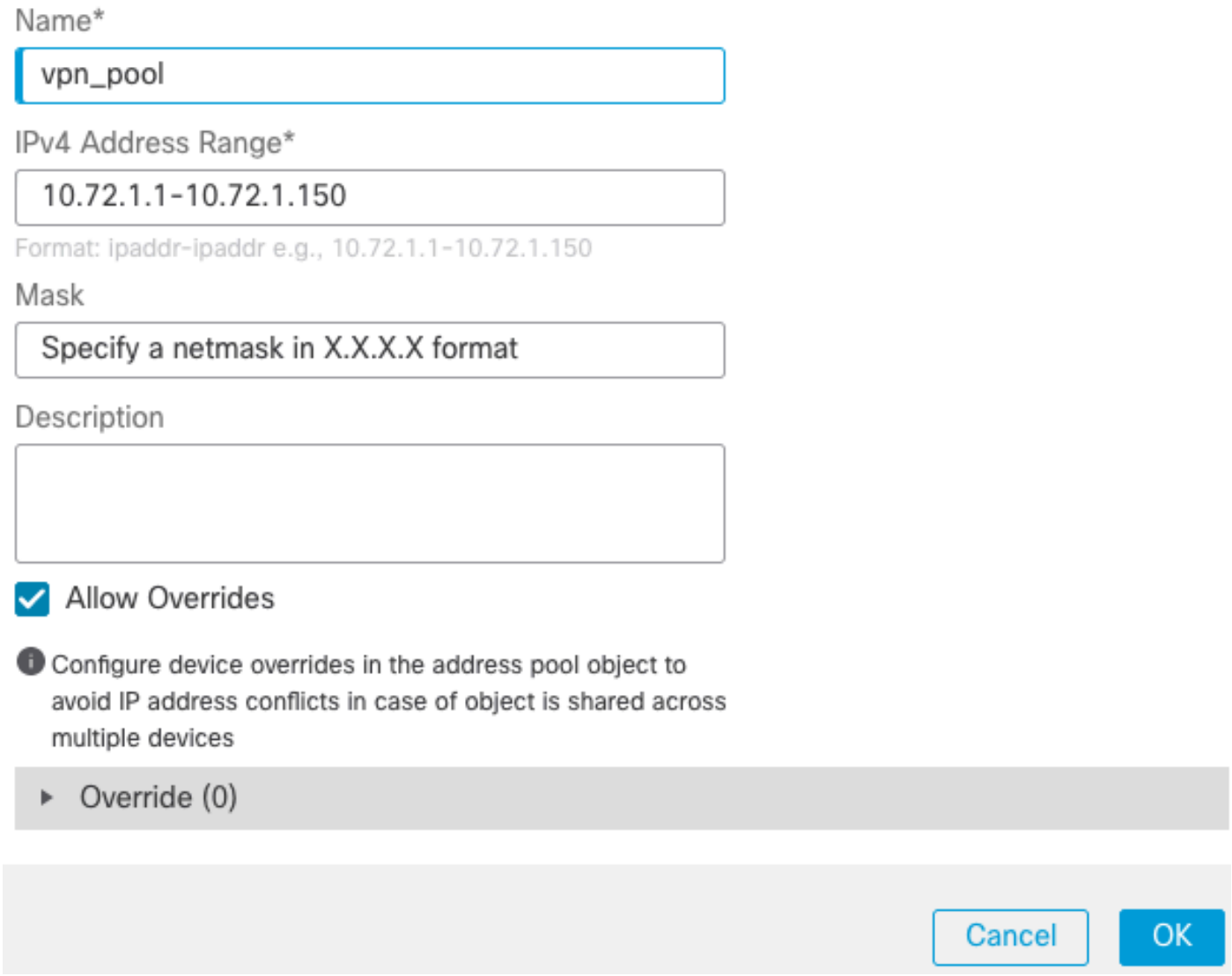


- その後、サーバがリストに表示されます。



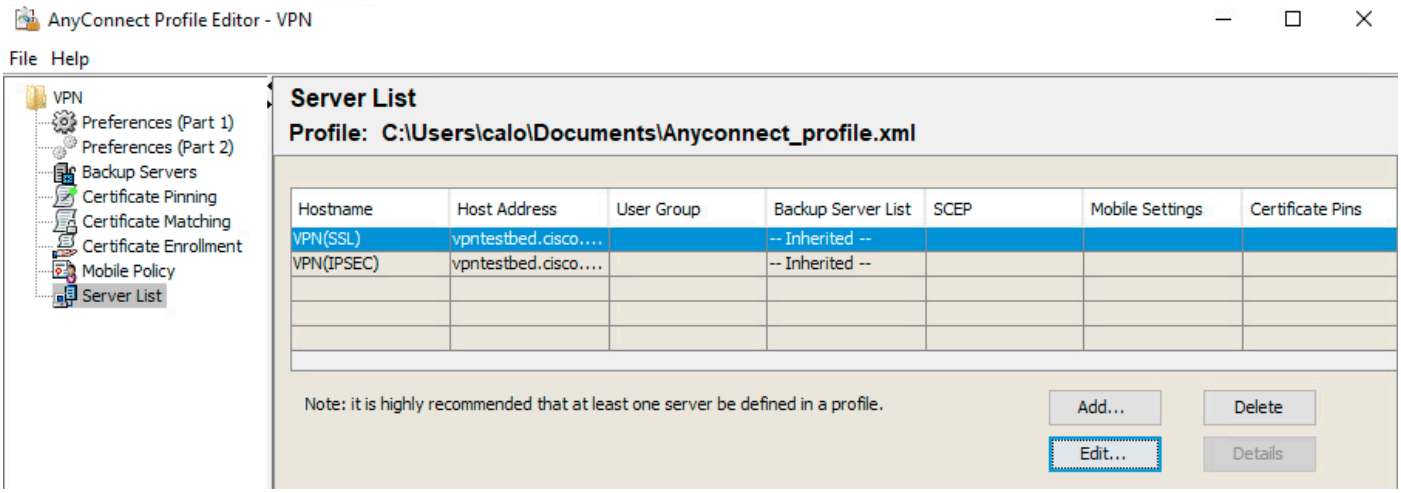
c) VPNユーザのアドレスプールの作成

- 次に **Objects > Object Management > Address Pools > Add IPv4 Pools**.
- 名前と範囲を入力します。マスクは必要ありません。



d) XMLプロファイルの作成

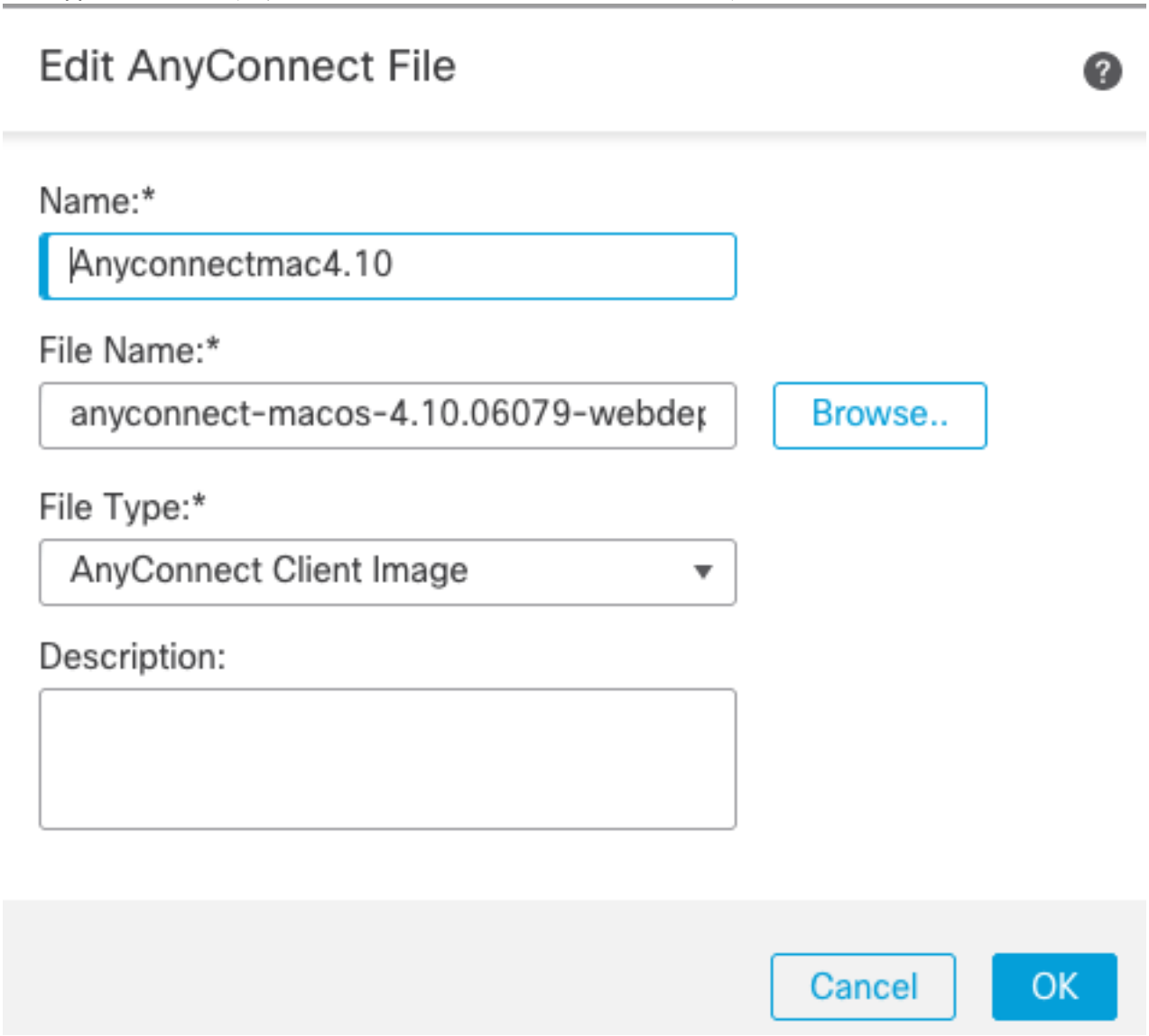
- シスコのサイトからProfile Editorをダウンロードして開きます。
- 次に Server List > Add...
- [Display Name]と[FQDN]を入力します。[Server List]に次のエントリがあります。



- クリック OKと **File** > **Save as...**

e) AnyConnectイメージのアップロード

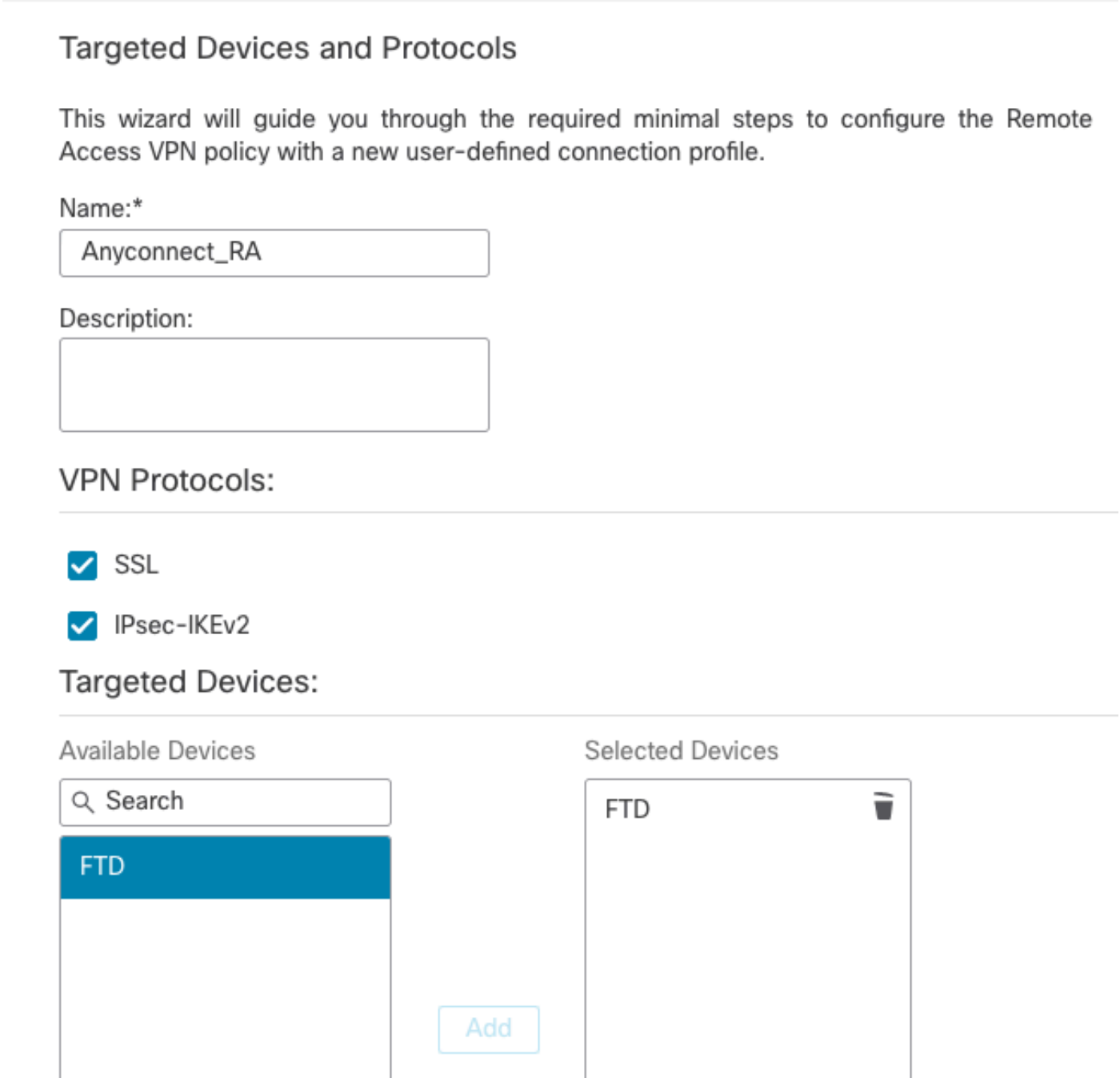
- シスコサイトからpkgイメージをダウンロードします。
- 次に Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
- 名前を入力し、ディスクからPKGファイルを選択し、 Save:



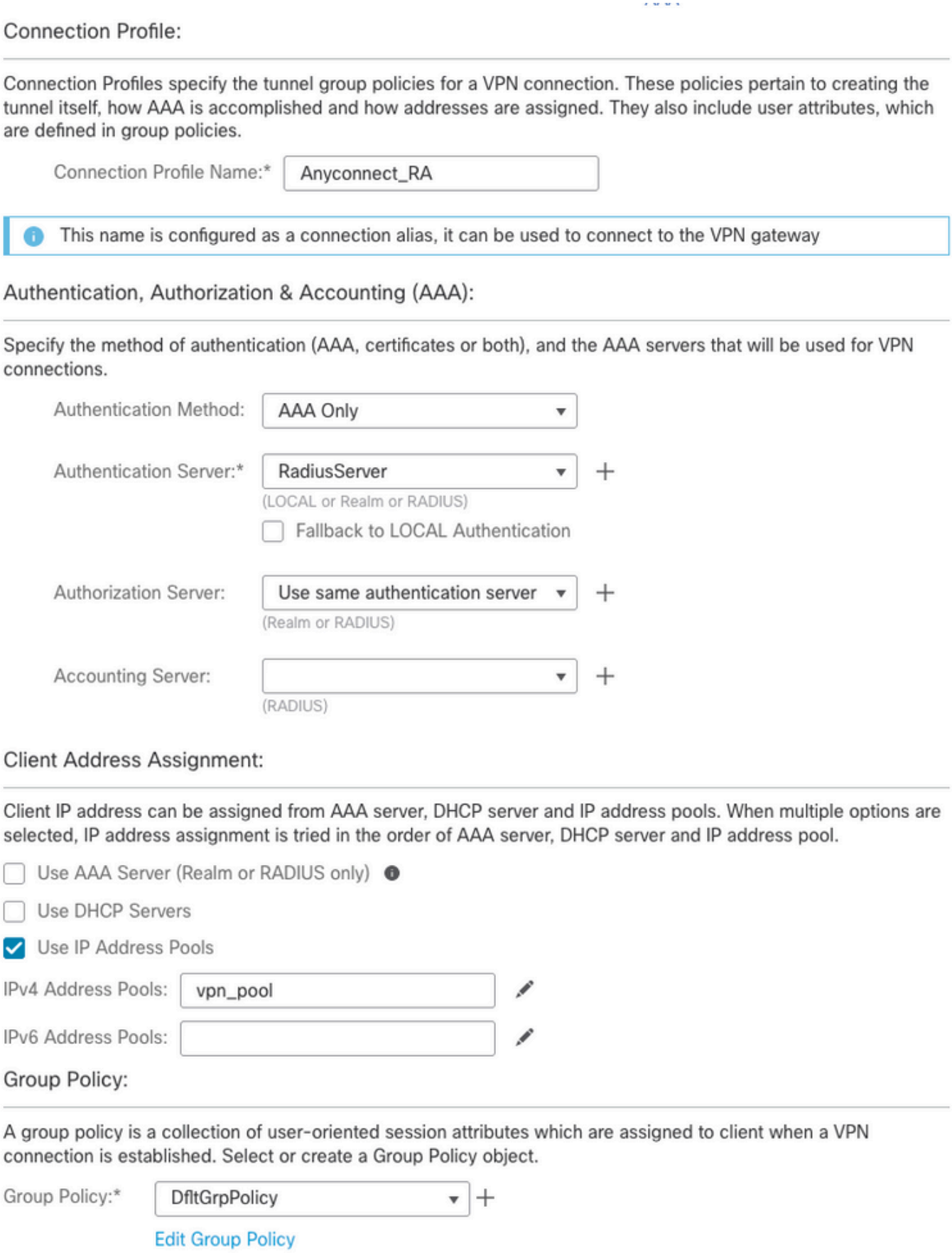
- 独自の要件に基づいてパッケージを追加します。

2.リモートアクセスウィザード

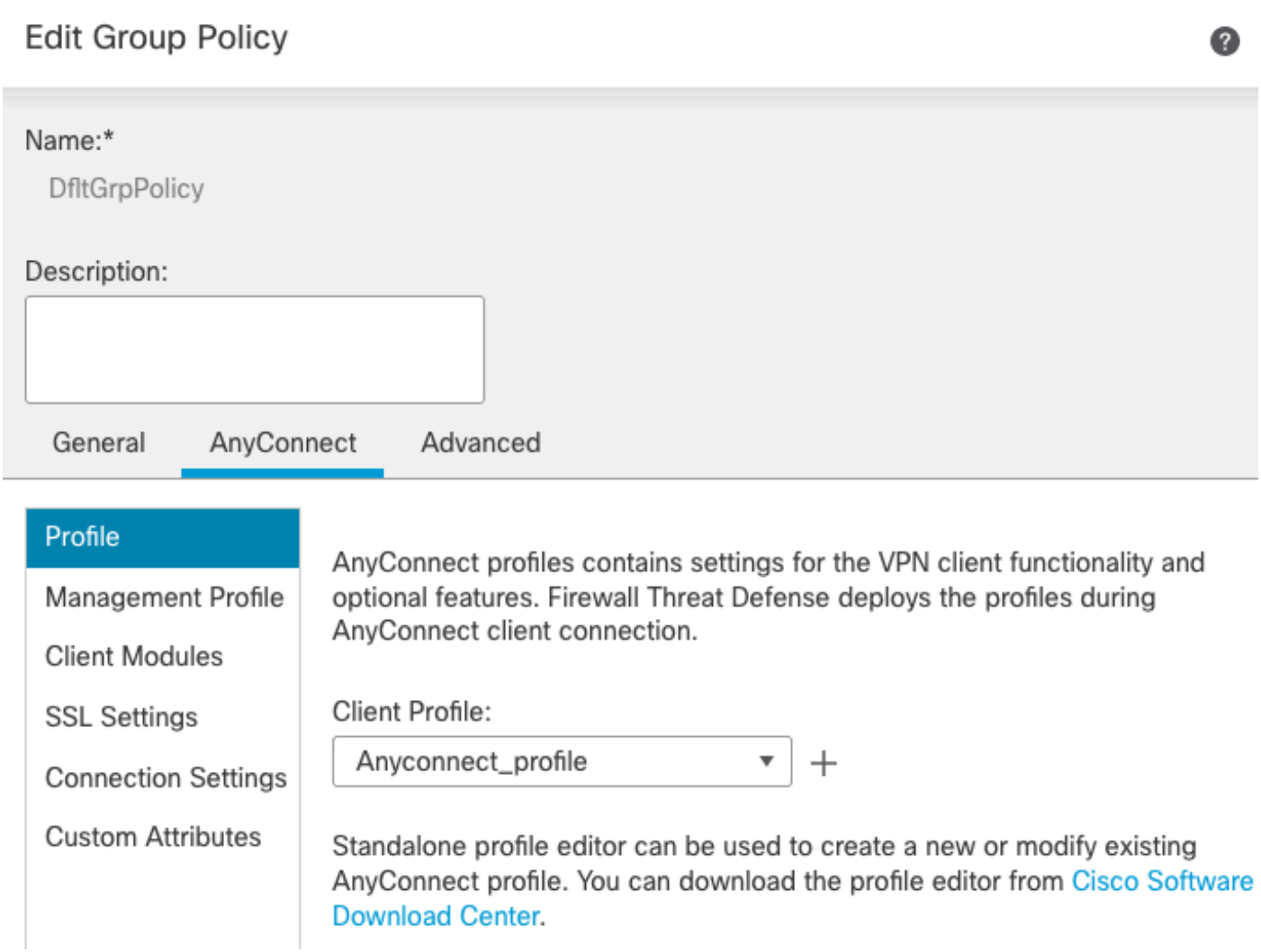
- 次に Devices > VPN > Remote Access > Add a new configuration.
- プロファイルに名前を付け、FTDデバイスを選択します。



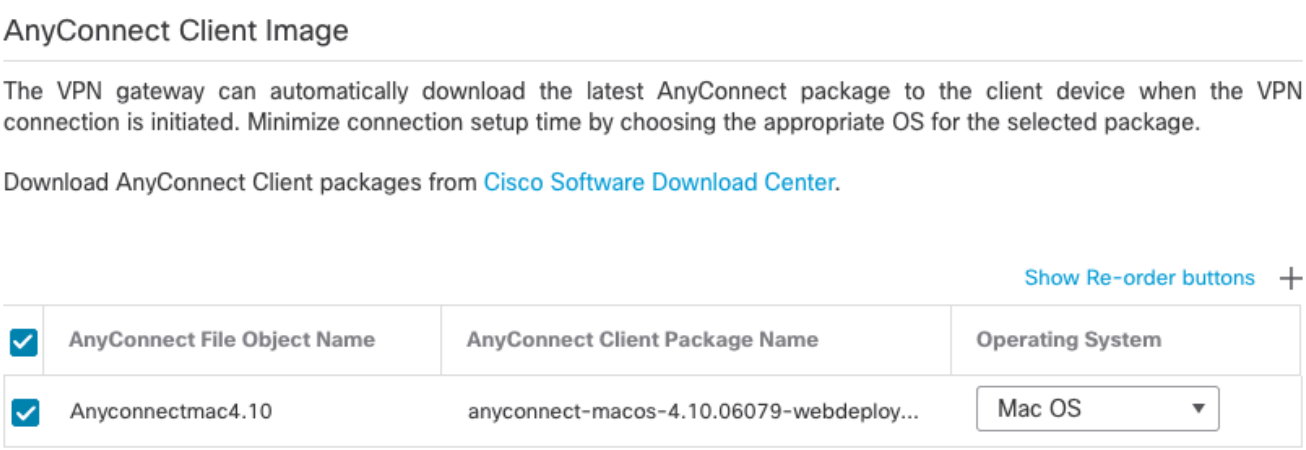
- [Connection Profile]ステップで、次のように入力します **Connection Profile Name**を選択し、**Authentication Server** と Address Pools 以前に作成したもの：



- クリック **Edit Group Policy** [AnyConnect]タブで、 Client Profileをクリックし、 Save:



- 次のページで、[AnyConnect images]を選択し、 Next.



- 次の画面で、 **Network Interface and Device Certificates**:

AAA

Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* Outsied

Enable DTLS on member interfaces

All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* vpntestbed.cisco.com

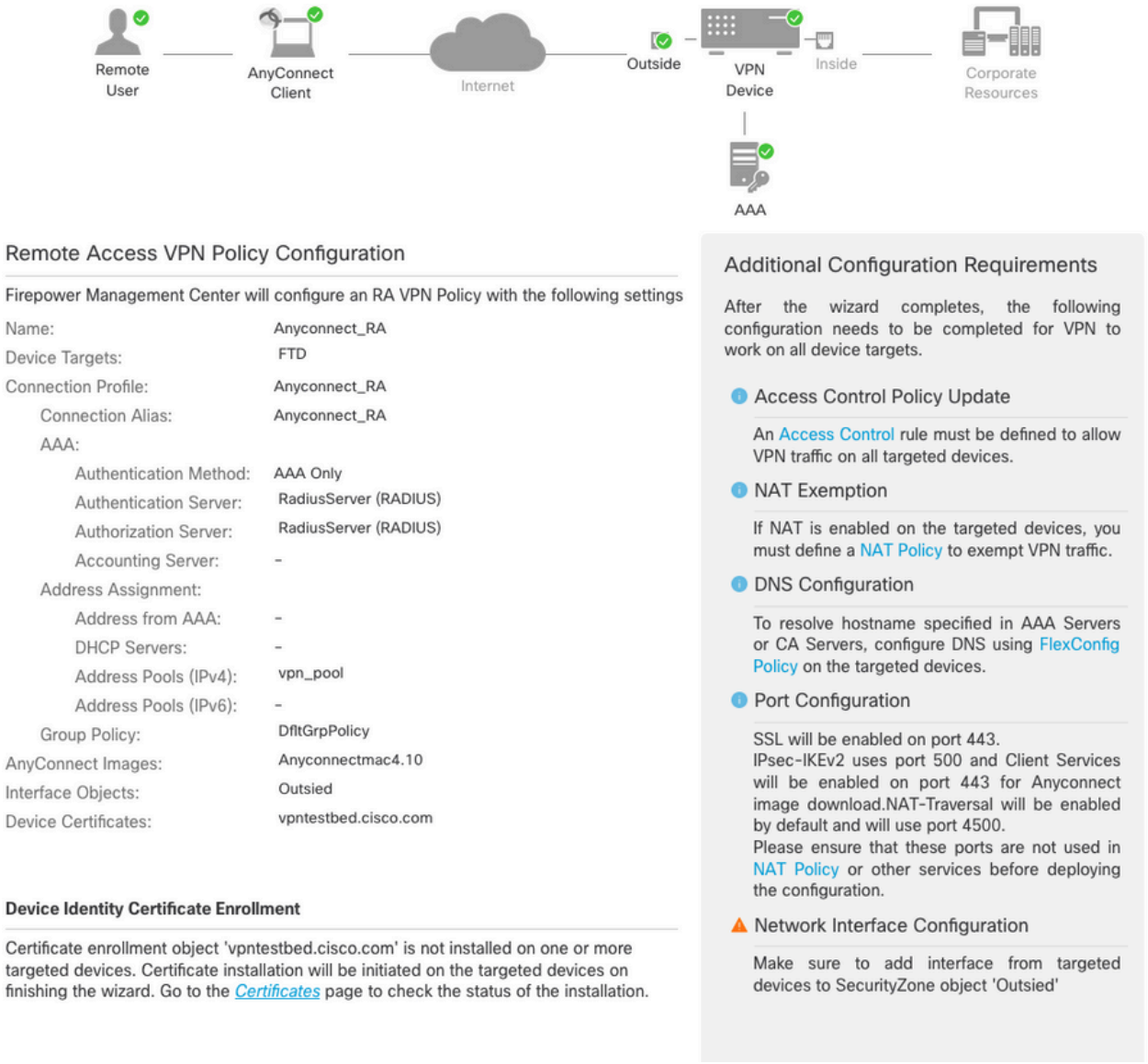
Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

- すべてが正しく設定されたら、 Finish その後 Deploy:



- これにより、証明書およびAnyConnectパッケージとともに設定全体がFTDアプライアンスにコピーされます。

Connection

FTDに接続するには、ブラウザを開き、外部インターフェイスをポイントするDNS名またはIPアドレスを入力する必要があります。次に、RADIUSサーバに保存されたクレデンシャルを使用してログインし、画面の指示に従います。 AnyConnectがインストールされたら、AnyConnectウィンドウに同じアドレスを入力し、 Connect.

制限

現在FTDではサポートされていませんが、ASAでは使用可能です。

- RADIUSサーバでのインターフェイスの選択は、Firepower Threat Defense6.2.3以前のバージョンではサポートされていません。interfaceオプションは導入時に無視されます。
- ダイナミック認証が有効なRADIUSサーバが動作するには、Firepower Threat Defense 6.3以降が必要です。
- FTDポスチャVPNは、動的認可またはRADIUS認可変更(CoA)によるグループポリシーの変更

をサポートしていません。
- AnyConnectのカスタマイズ(機能拡張：Cisco Bug ID CSCvq87631)
- AnyConnectスクリプト
- AnyConnectのローカリゼーション
- WSAの統合
- RAおよびL2L VPNの同時IKEv2ダイナミッククリプトマップ(機能拡張：Cisco Bug ID CSCvr52047)
- AnyConnectモジュール（NAM、Hostscan、AMPイネーブラ、SBL、Umbrella、Webセキュリティなど）:DARTはデフォルトでインストールされます(AMPイネーブラおよびUmbrellaの機能拡張：Cisco Bug ID CSCvs03562およびCisco Bug ID CSCvs06642)。
- TACACS、Kerberos（KCD認証およびRSA SDI）
- ブラウザプロキシ

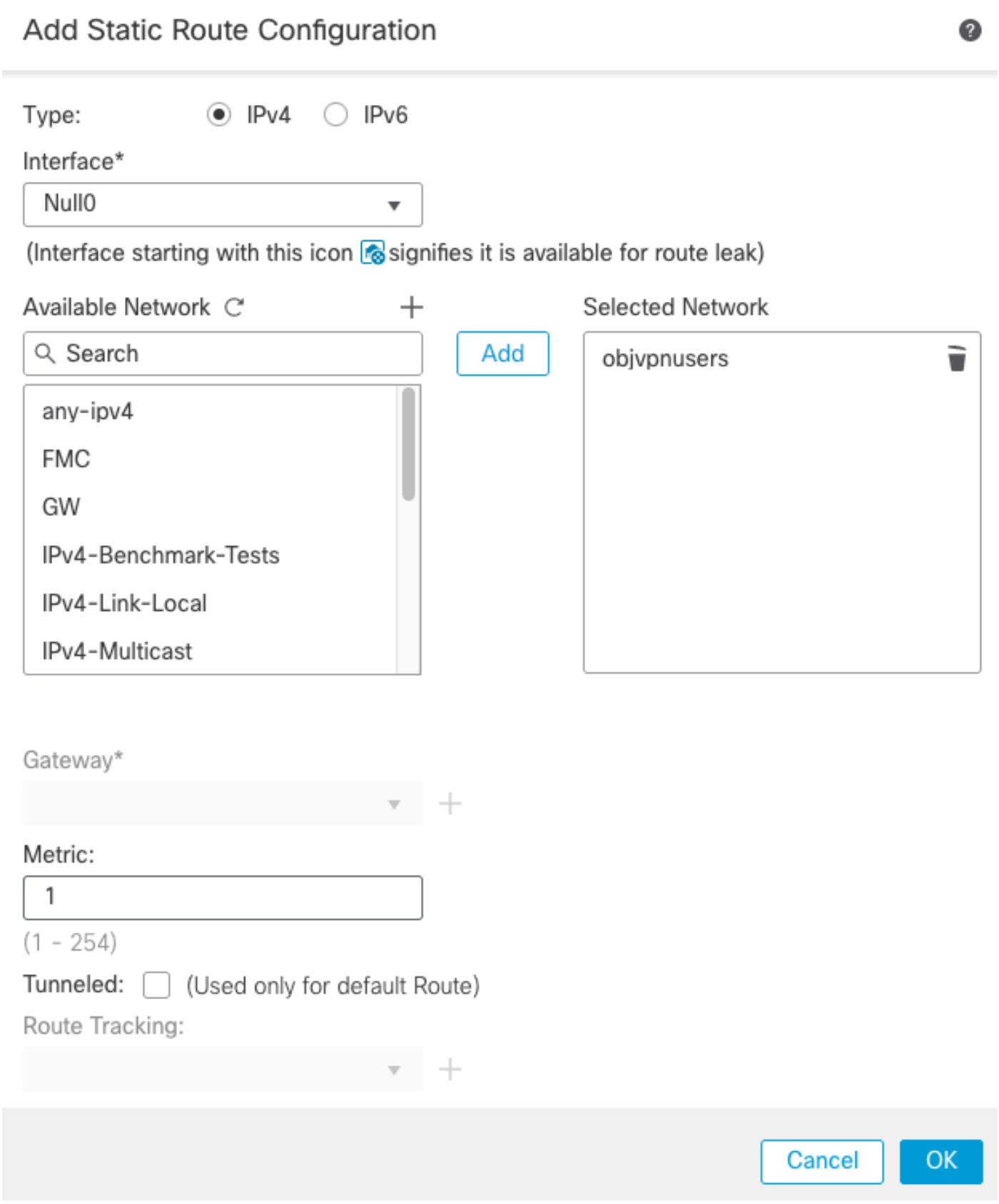
セキュリティに関する考慮事項

デフォルトでは、 sysopt connection permit-vpnオプションは無効です。つまり、アクセスコントロールポリシーを介して外部インターフェイスのアドレスプールから送信されるトラフィックを許可する必要があります。VPNトラフィックのみを許可するためにプレフィルタまたはアクセス制御ルールが追加されますが、クリアテキストトラフィックがルールの条件に一致する場合は、誤って許可されます。

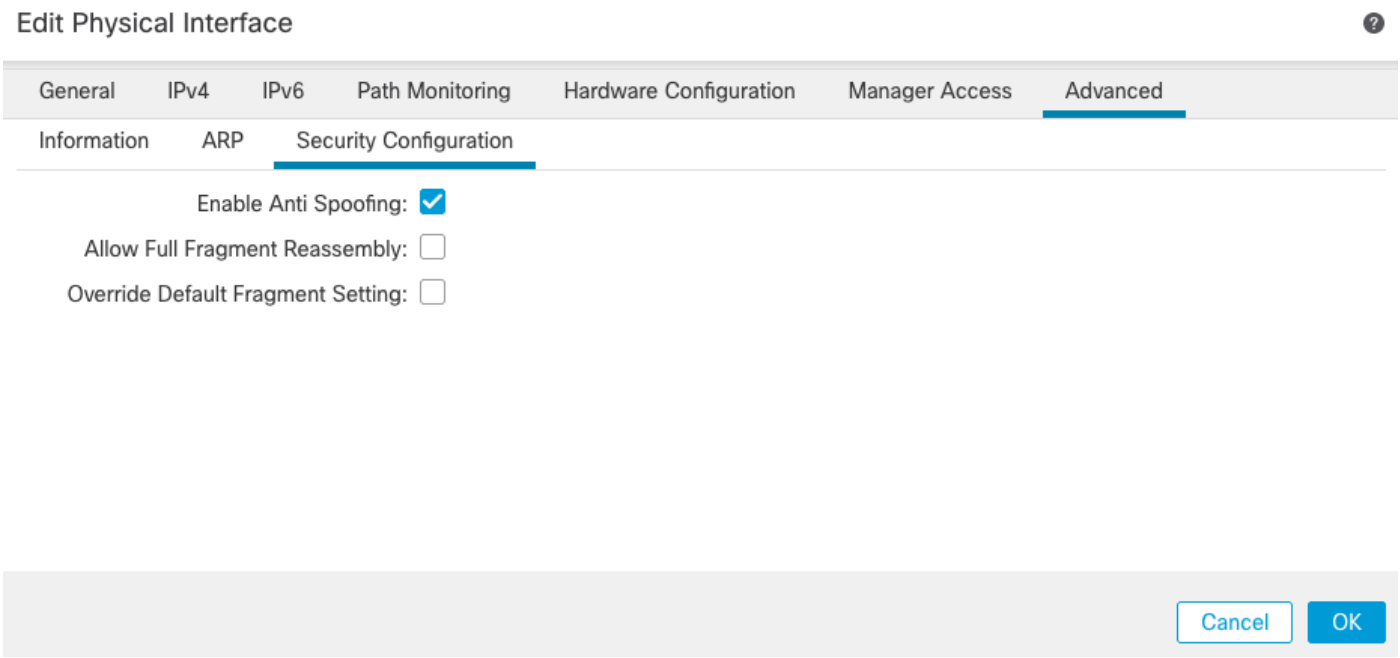
この問題には2つのアプローチがあります。1つ目は、TACが推奨するオプションで、外部インターフェイスに対してアンチスプーフィングを有効にすることです(ASAではUnicast Reverse Path Forwarding(uRPF)と呼ばれていました)。2つ目は、有効にすることです sysopt connection permit-vpn Snort検査を完全にバイパスします。最初のオプションでは、VPNユーザとの間でやり取りされるトラフィックを通常の方法で検査できます。

a) uRPFの有効化

- セクションCで定義した、リモートアクセスユーザに使用するネットワークのヌルルートを作成します。 Devices > Device Management > Edit > Routing > Static Route を選択し、 Add route



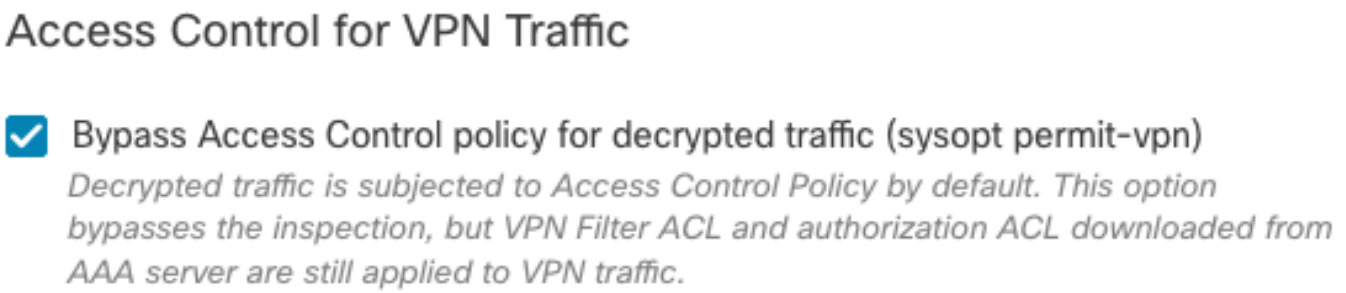
- 次に、VPN接続が終端するインターフェイスでuRPFを有効にします。これを見つけるには、**Devices > Device Management > Edit > Interfaces > Edit > Advanced > Security Configuration > Enable Anti Spoofing**.



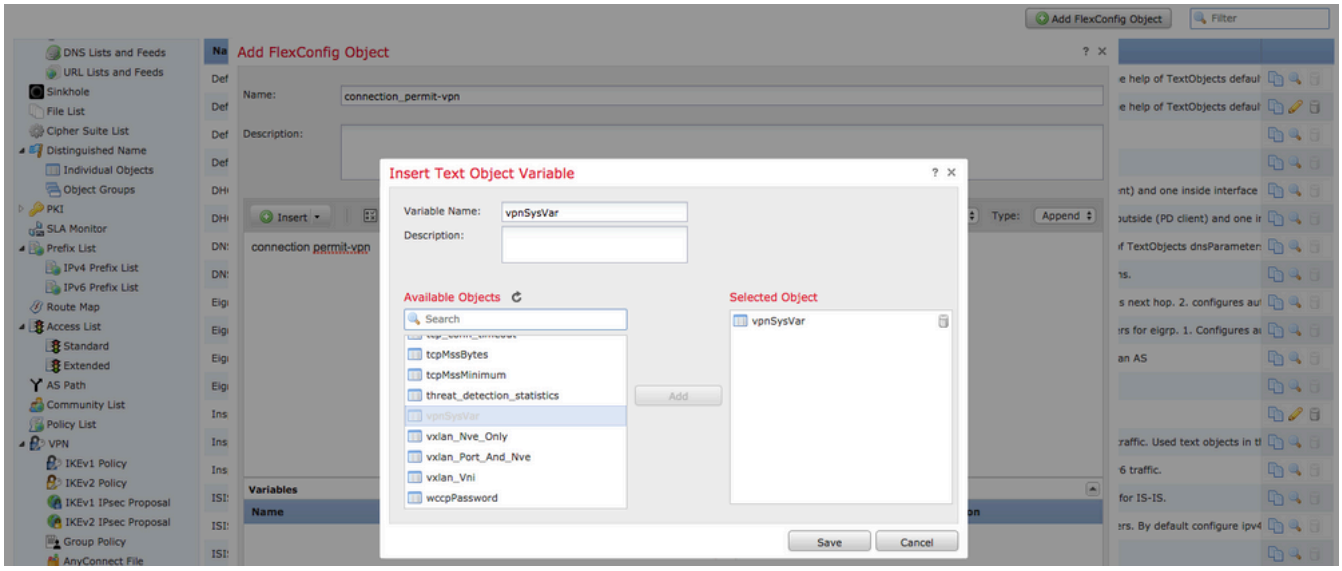
ユーザが接続されると、そのユーザの32ビットルートがルーティングテーブルにインストールされます。プールから送信された他の未使用IPアドレスから送信されたテキストトラフィックをクリアすると、uRFPによって廃棄されます。説明を表示するには **Anti-Spoofing**『Firepower Threat Defenseでのセキュリティ設定パラメータの設定』を参照してください。

b)有効 Sysopt connection permit-vpn オプション

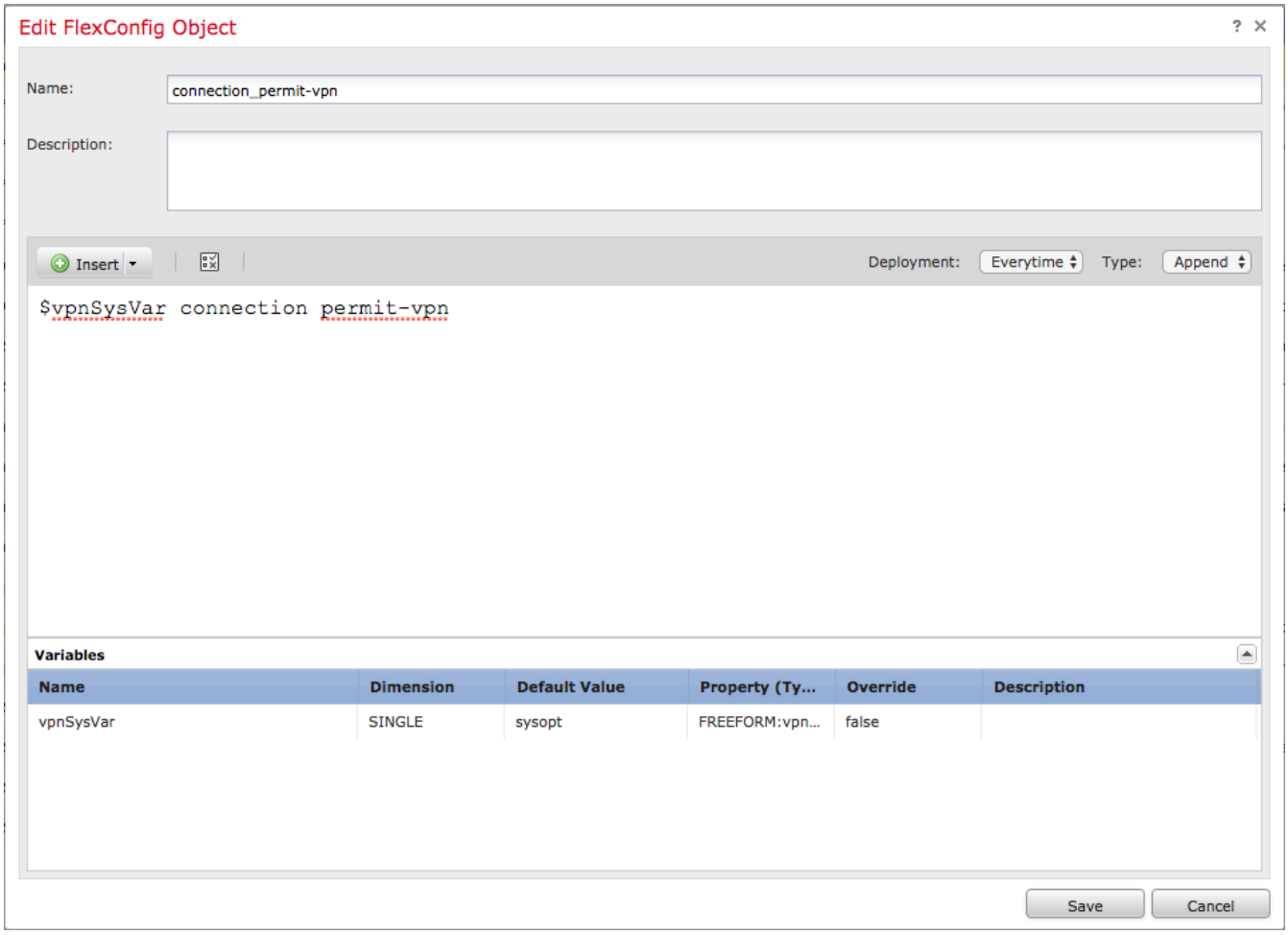
- バージョン6.2.3以降を使用している場合は、ウィザードまたはの下で実行するオプションがあります Devices > VPN > Remote Access > VPN Profile > Access Interfaces.



- 6.2.3より前のバージョンについては、を参照してください。 Objects > Object Management > FlexConfig > Text Object > Add Text Object.
- テキストオブジェクト変数を作成します。例： vpnSysVar値を持つ単一のエントリ sysopt.
- 次に Objects**> Object Management > FlexConfig > FlexConfig Object > Add FlexConfig Object.**
- Cisco Unified Communications Managerの FlexConfig CLIを使用したオブジェクト connection permit-vpn.
- テキストオブジェクト変数を FlexConfig CLIでオブジェクトを指定します。 **$vpnSysVar connection permit-vpn**. クリック Save:



- Cisco Unified Communications Managerの FlexConfig ~として異議を唱える **Append** 導入を選択して Everytime:



- 次に**Devices > FlexConfig** 現在のポリシーを編集するか、新しいポリシーを作成します。 New Policy をクリックして、クエリーを実行します。
- 作成した FlexConfigをクリックし、 Save.
- プロビジョニングする構成を展開します**sysopt connection permit-vpn**コマンドをデバイスで発行します。

ただし、この後は、アクセスコントロールポリシーを使用してユーザから着信するトラフィックを検査することはできません。ユーザトラフィックのフィルタリングには、引き続きVPNフィル

タまたはダウンロード可能ACLを使用できます。

VPNユーザからのSnortでパケットのドロップが見られる場合は、TACに問い合せてCisco Bug ID CSCvg91399を参照してください。

関連情報

- **シスコテクニカルサポートおよびダウンロード**

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。