Configuration d'AnyConnect Remote Access VPN sur FTD

Table des matières

Introduction

Ce document décrit une configuration pour AnyConnect Remote Access VPN sur FTD.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base en VPN, TLS et IKEv2
- Connaissances de base en authentification, autorisation et comptabilité (AAA) et RADIUS
- Expérience avec Firepower Management Center

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco FTD 7.2.0

- Cisco FMC 7.2.1
- AnyConnect 4.10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document fournit un exemple de configuration pour Firepower Threat Defense (FTD) version 7.2.0 et ultérieure, qui permet au VPN d'accès à distance d'utiliser Transport Layer Security (TLS) et Internet Key Exchange version 2 (IKEv2). En tant que client, Cisco AnyConnect peut être utilisé, qui est pris en charge sur plusieurs plates-formes.

Configuration

1. Conditions préalables

Afin de passer par l'assistant d'accès à distance dans Firepower Management Center :

- Créez un certificat utilisé pour l'authentification du serveur.
- Configurez le serveur RADIUS ou LDAP pour l'authentification des utilisateurs.
- Créez un pool d'adresses pour les utilisateurs VPN.
- Téléchargez des images AnyConnect pour différentes plates-formes.

a) Importer le certificat SSL

Les certificats sont essentiels lorsque vous configurez AnyConnect. Le certificat doit avoir une extension Subject Alternative Name avec un nom DNS et/ou une adresse IP pour éviter des erreurs dans les navigateurs Web.

> **Remarque** : seuls les utilisateurs Cisco enregistrés ont accès aux outils internes et aux informations de bogue.

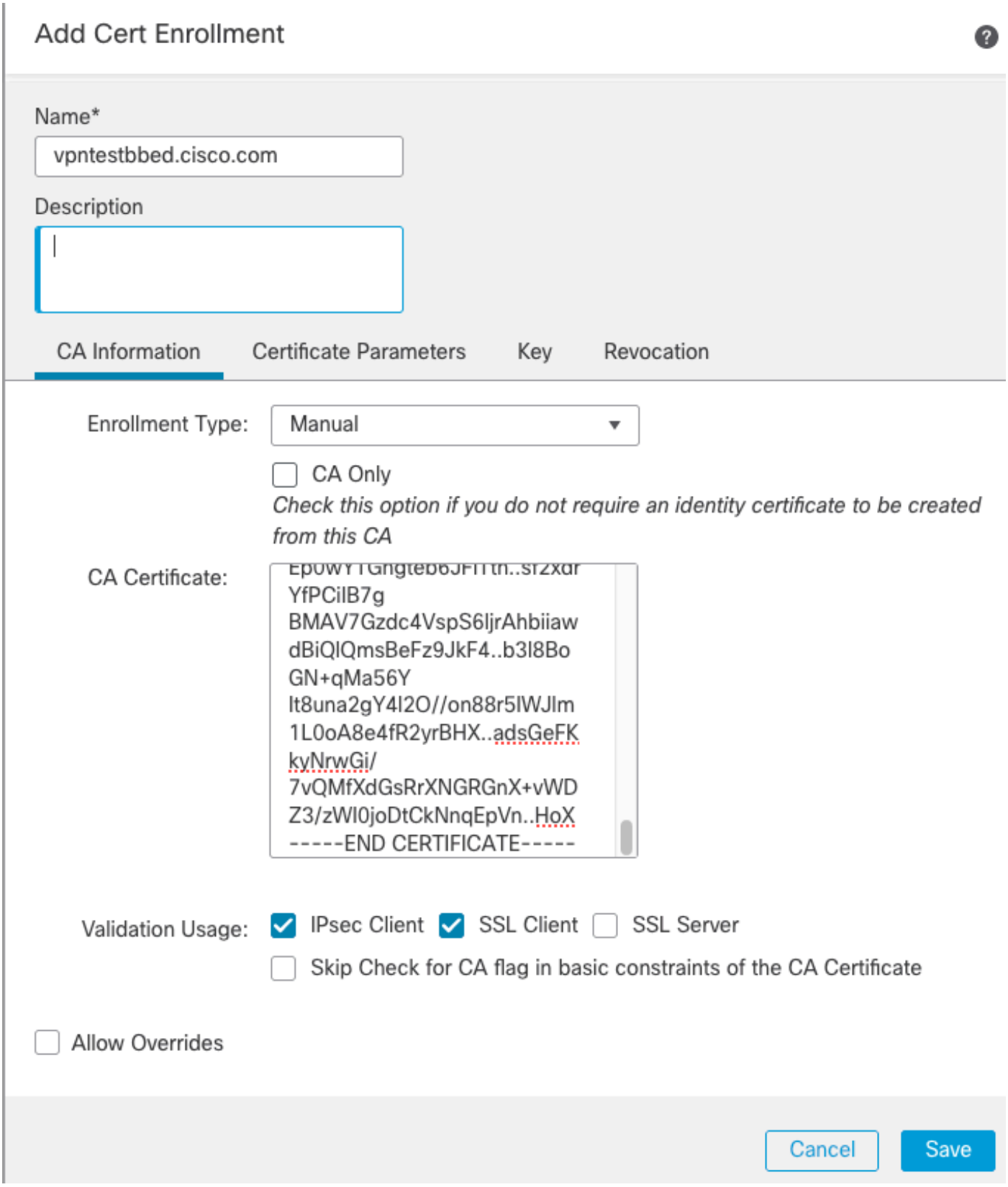
L'inscription manuelle des certificats comporte des limites :

- Sur FTD, vous avez besoin du certificat CA avant de générer le CSR.

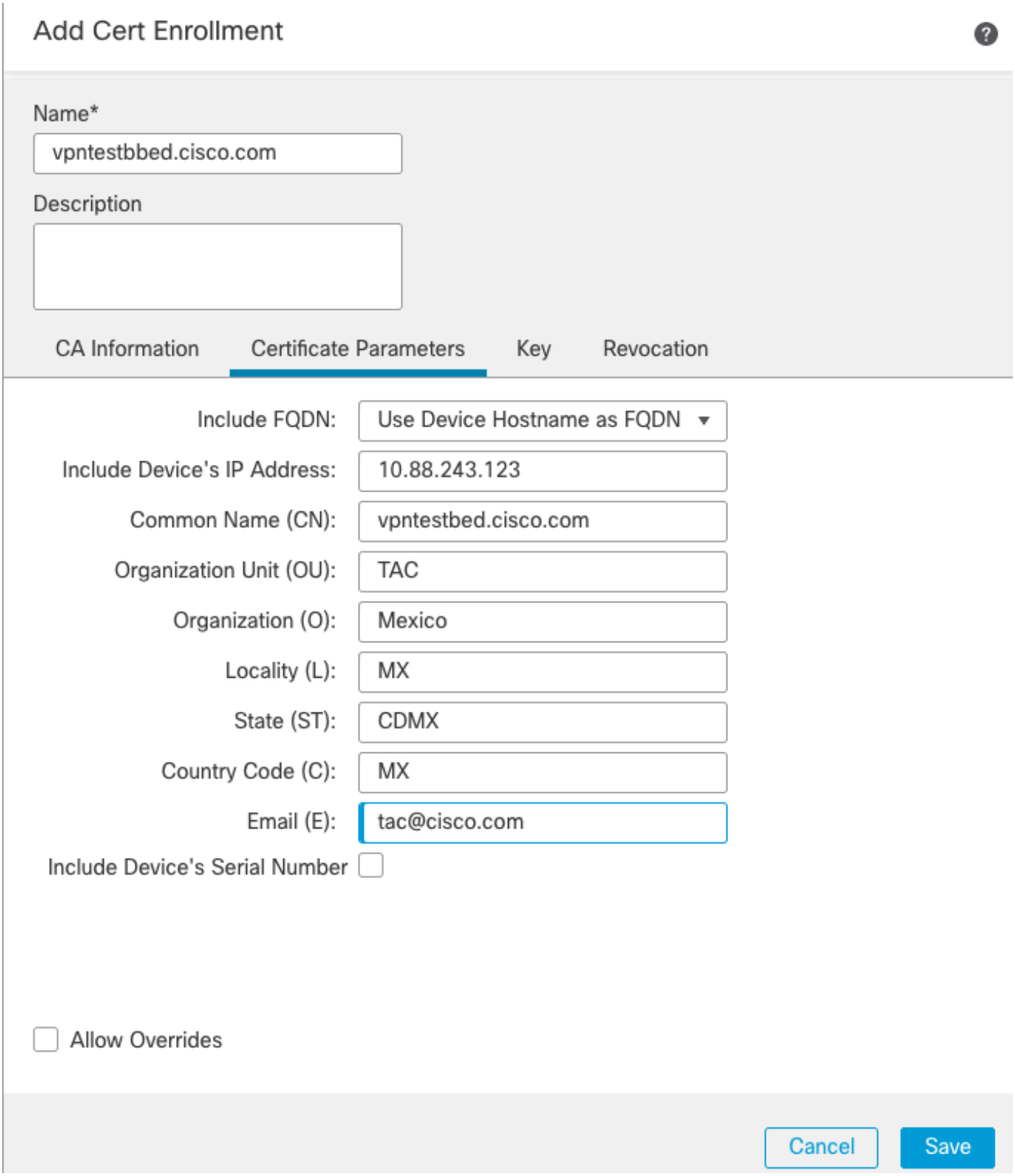
- Si le CSR est généré en externe, la méthode manuelle échoue, une autre méthode doit être utilisée (PKCS12).

Il existe plusieurs méthodes pour obtenir un certificat sur l'appareil FTD, mais la plus sûre et la plus simple est de créer une demande de signature de certificat (CSR), de la signer avec une autorité de certification (CA), puis d'importer le certificat émis pour la clé publique, qui était dans CSR. Voici comment procéder :

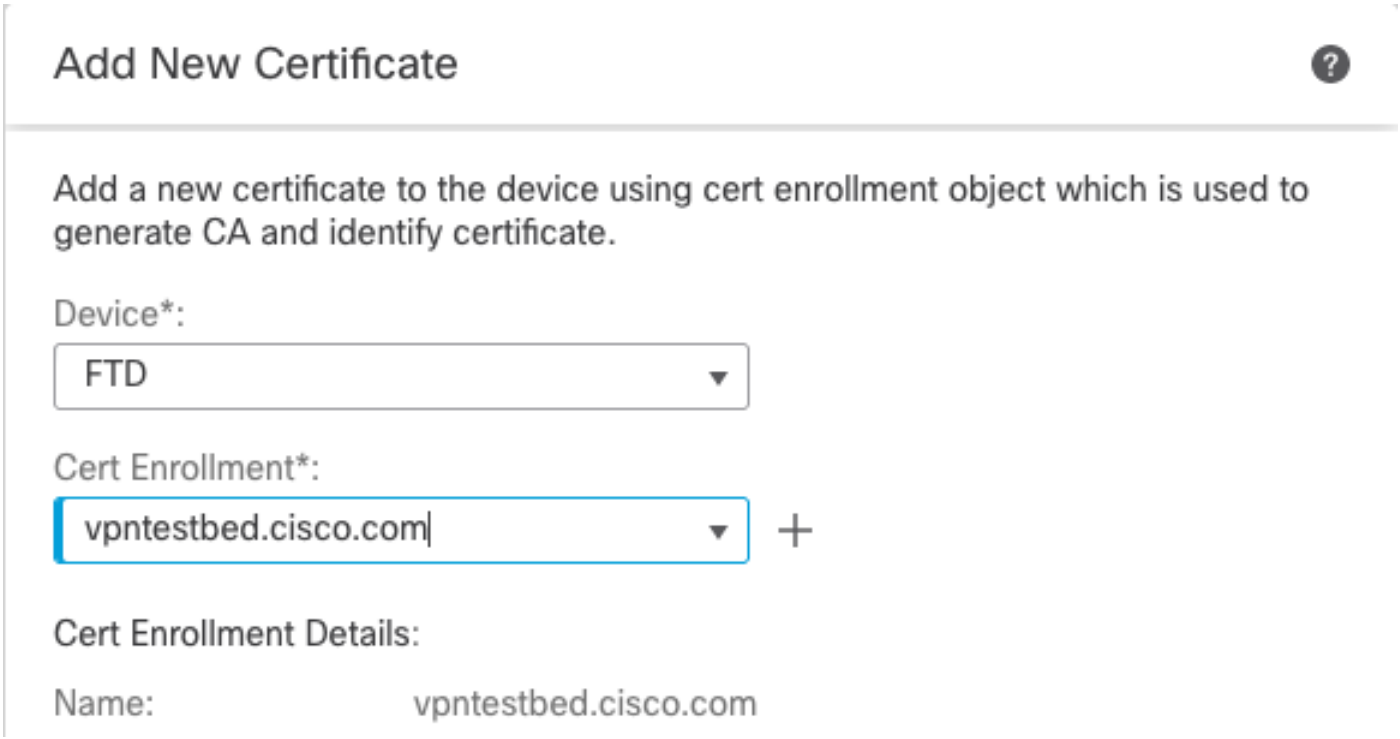
- Aller à Objects > **Object Management > PKI > Cert Enrollment** , cliquez sur **Ajouter une inscription de certificat**.



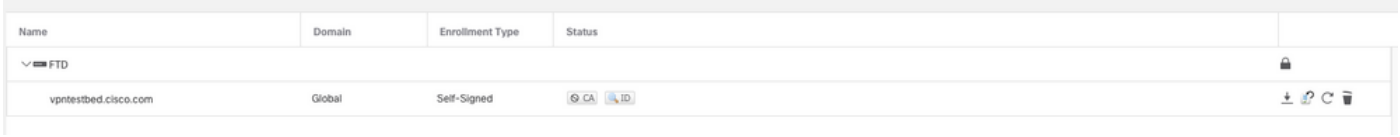
- Sélectionner Enrollment Type et collez le certificat de l'autorité de certification (le certificat utilisé pour signer le CSR).
- Accédez ensuite au deuxième onglet et sélectionnez Custom FQDN et remplissez tous les champs nécessaires, par exemple :



- Dans le troisième onglet, sélectionnez Key Type, choisissez le nom et la taille. Pour RSA, 2048 bits est minimum.
- Cliquez sur Enregistrer et accédez à Devices > Certificates > Add > New Certificate.
- Sélectionnez ensuite Device, et sous Cert Enrollment sélectionnez le point de confiance que vous venez de créer, puis cliquez sur Add:

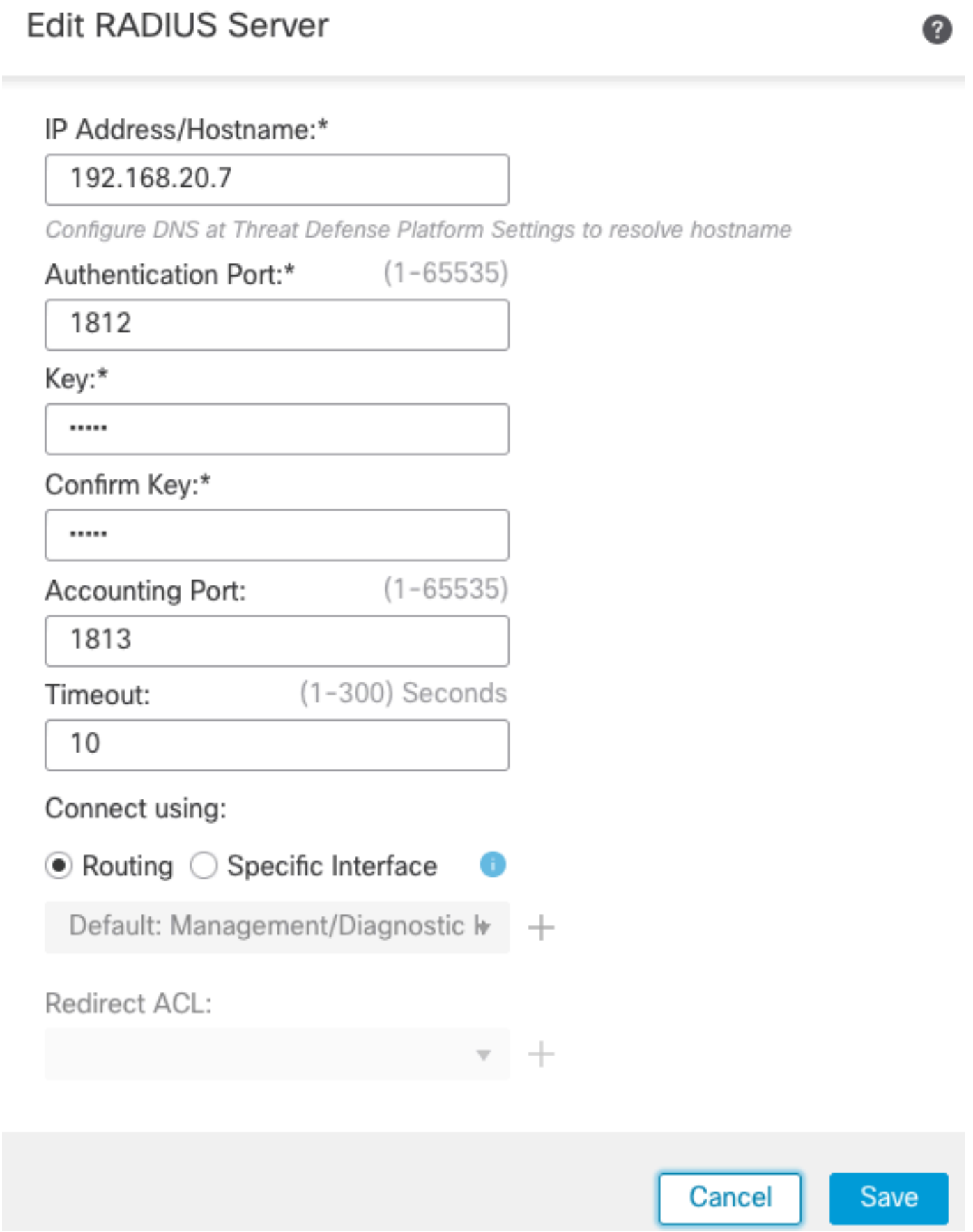


- Plus tard, en regard du nom du point de confiance, cliquez sur le bouton , puis Yes, puis copiez CSR à CA et signez-le. Les attributs du certificat doivent être identiques à ceux d'un serveur HTTPS normal.
- Après avoir reçu le certificat de CA au format base64, sélectionnez-le sur le disque et cliquez sur Import. Lorsque cette opération réussit, vous voyez :

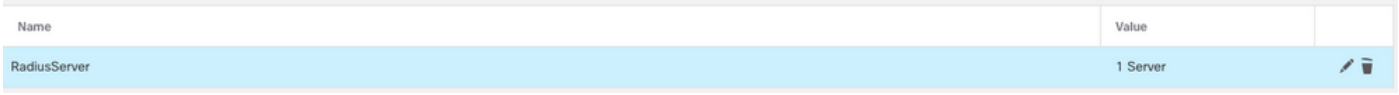


b) Configurer le serveur RADIUS

- Aller à **Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group**.
- Remplissez le nom et ajoutez l'adresse IP avec le secret partagé, cliquez sur Save:

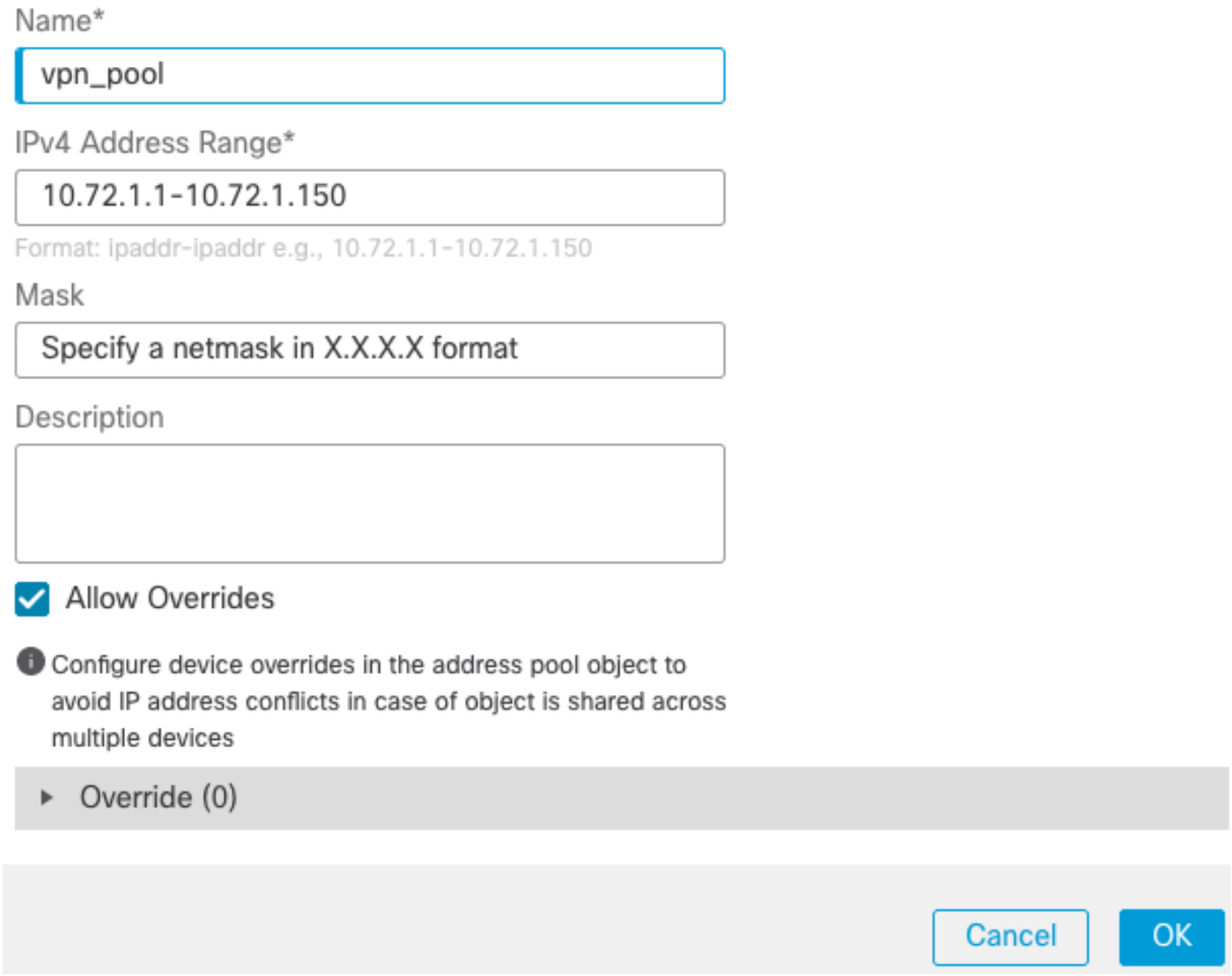


- Après cela, vous voyez le serveur sur la liste :



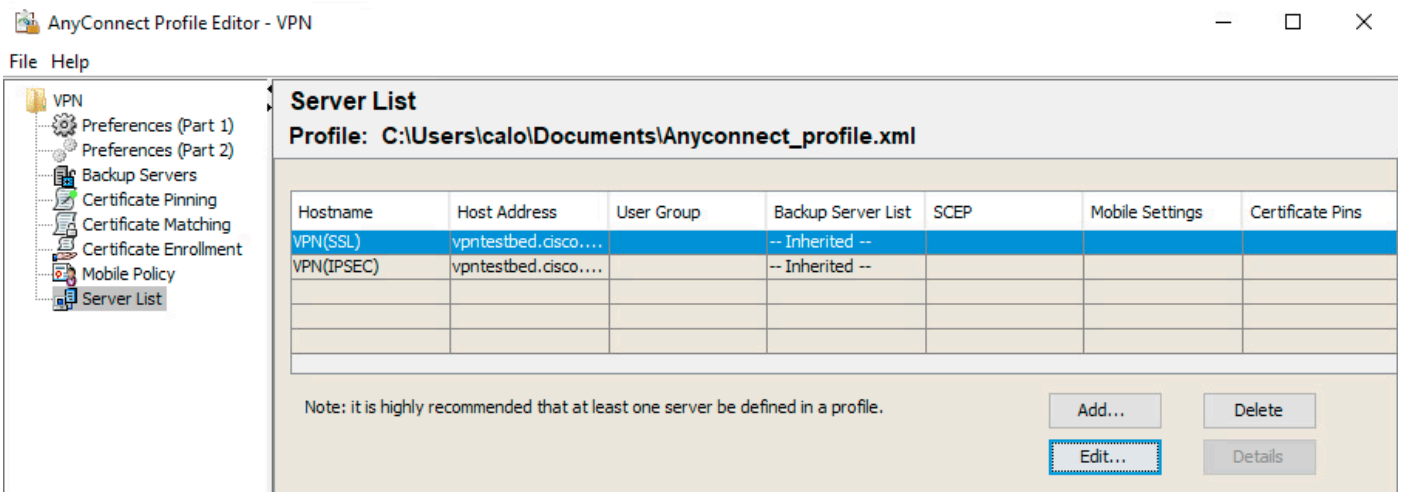
c) Créer un pool d'adresses pour les utilisateurs VPN

- Aller à **Objects > Object Management > Address Pools > Add IPv4 Pools**.
- Mettez le nom et la plage, le masque n'est pas nécessaire :



d) Créer un profil XML

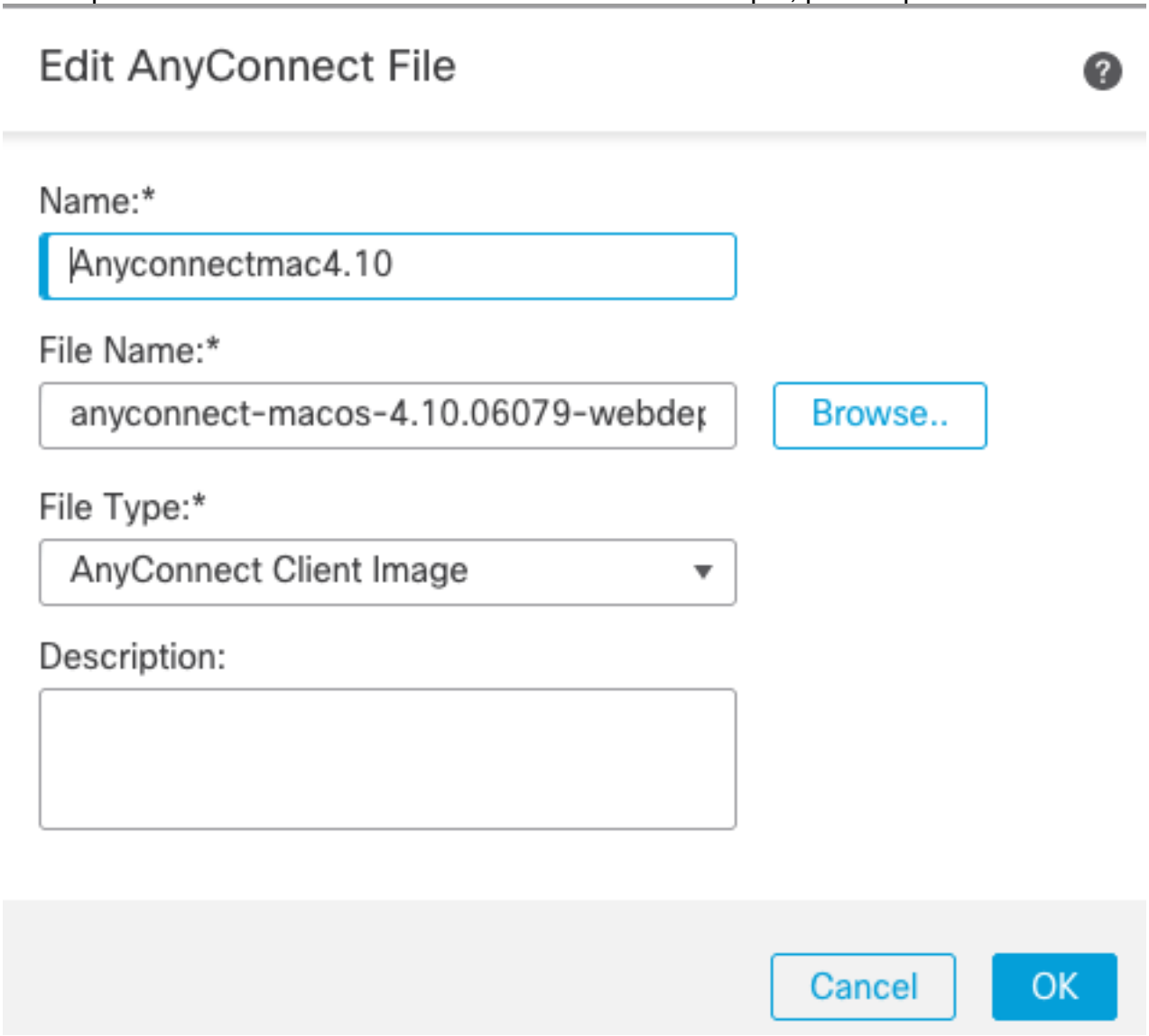
- Téléchargez l'Éditeur de profil depuis le site Cisco et ouvrez-le.
- Aller à Server List > Add...
- Placez le nom d'affichage et le FQDN. Vous voyez des entrées dans la liste des serveurs :



- Cliquer OKet **File** > **Save as...**

e) Télécharger des images AnyConnect

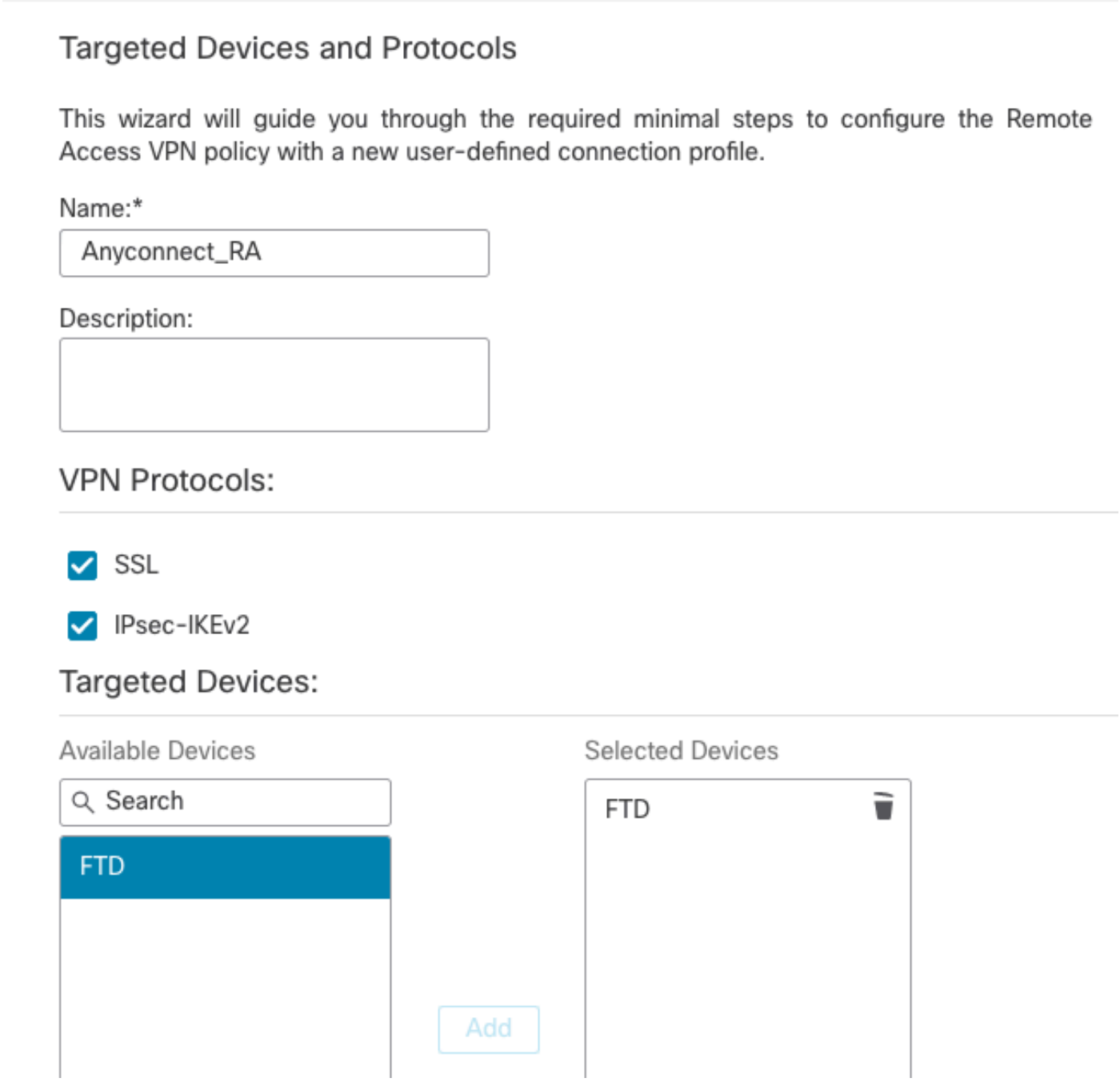
- Téléchargez les images du package depuis le site Cisco.
- Aller à Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
- Tapez le nom et sélectionnez le fichier PKG sur le disque, puis cliquez sur Save:



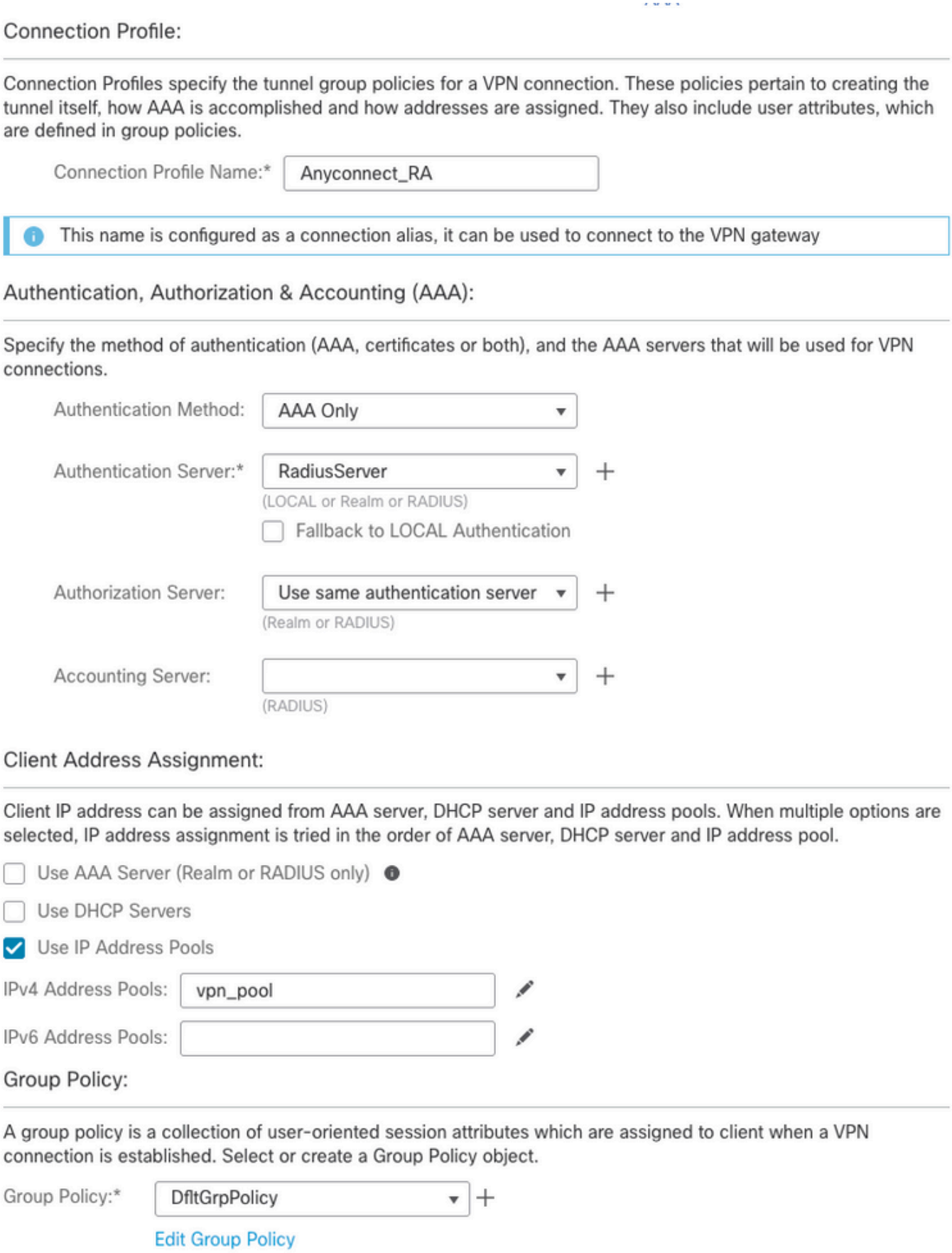
- Ajoutez d'autres packages en fonction de vos propres besoins.

2. Assistant Accès à distance

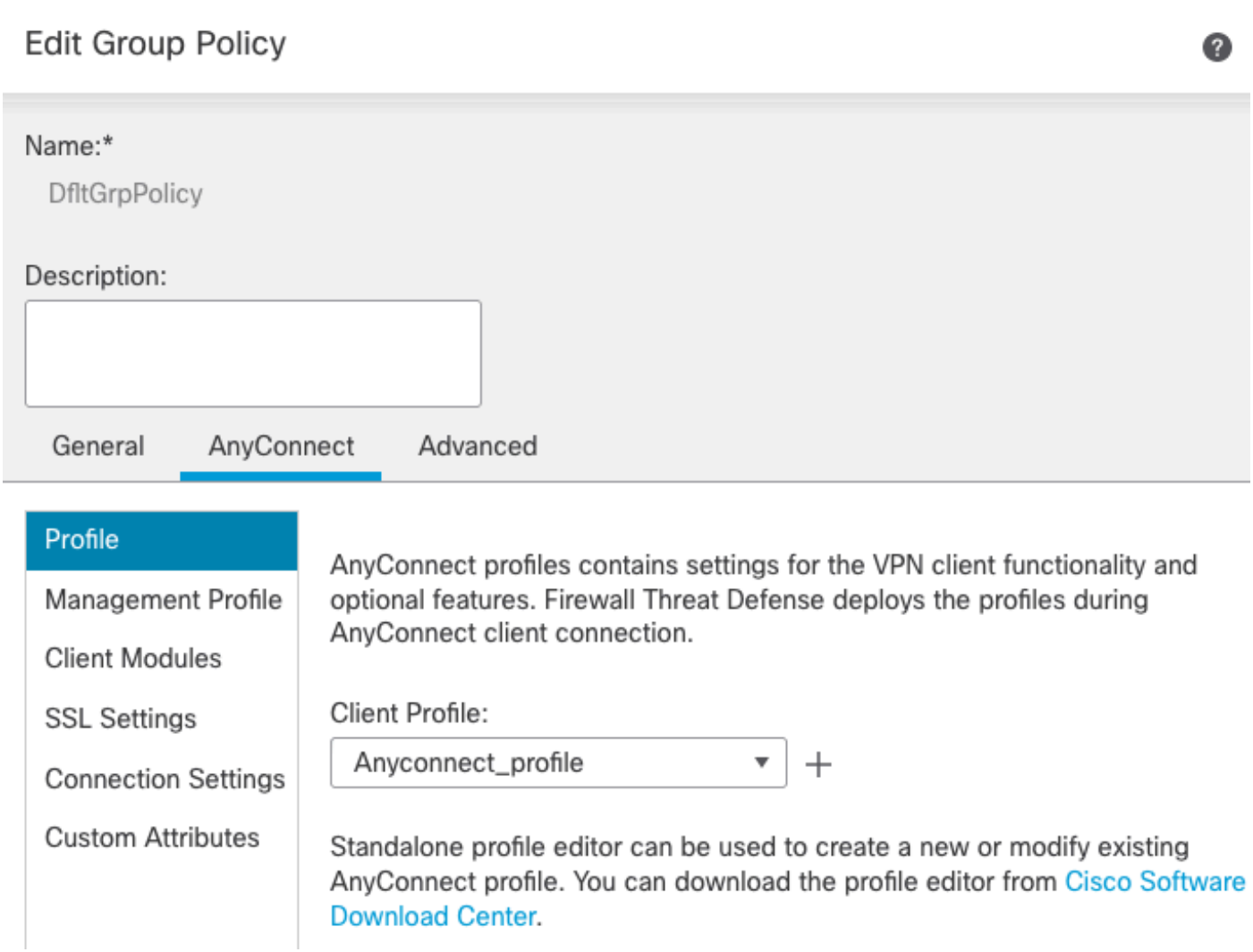
- Aller à Devices > VPN > Remote Access > Add a new configuration.
- Nommez le profil et sélectionnez le périphérique FTD :



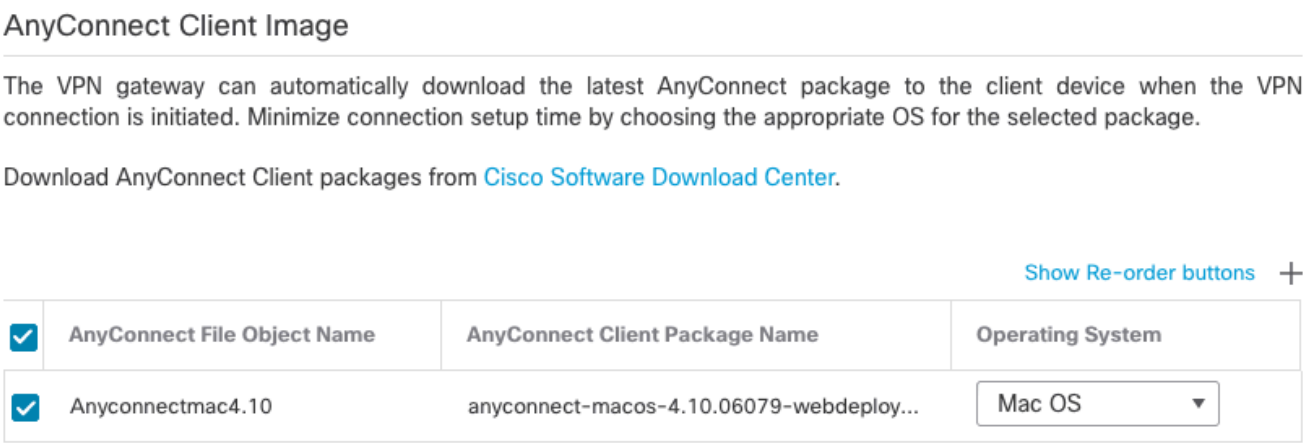
- Dans l'étape Profil de connexion, tapez **Connection Profile Name**, sélectionnez l'option **Authentication Server** et Address Pools que vous avez créé précédemment :



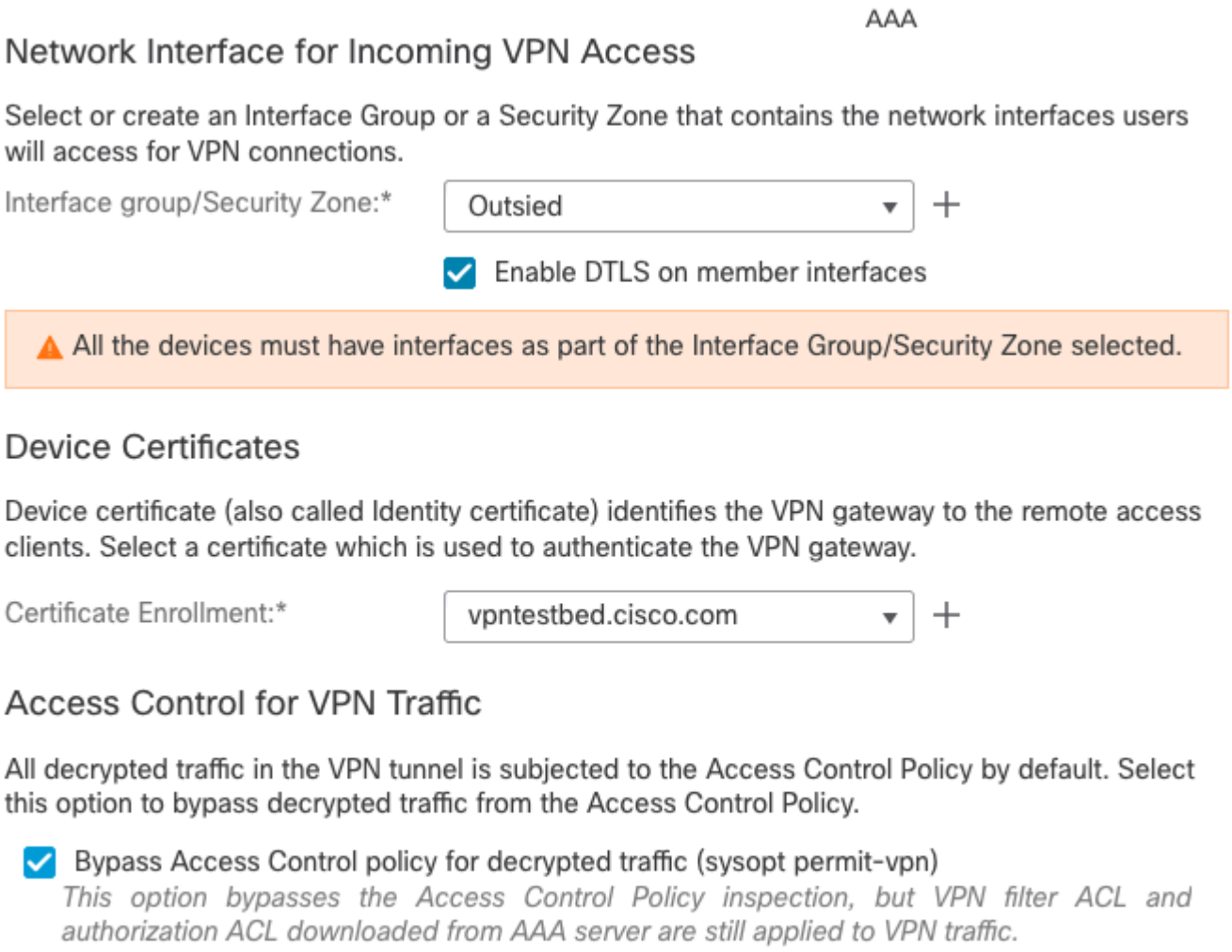
- Cliquez sur **Edit Group Policy** et dans l'onglet AnyConnect, sélectionnez Client Profile, puis cliquez sur Save:



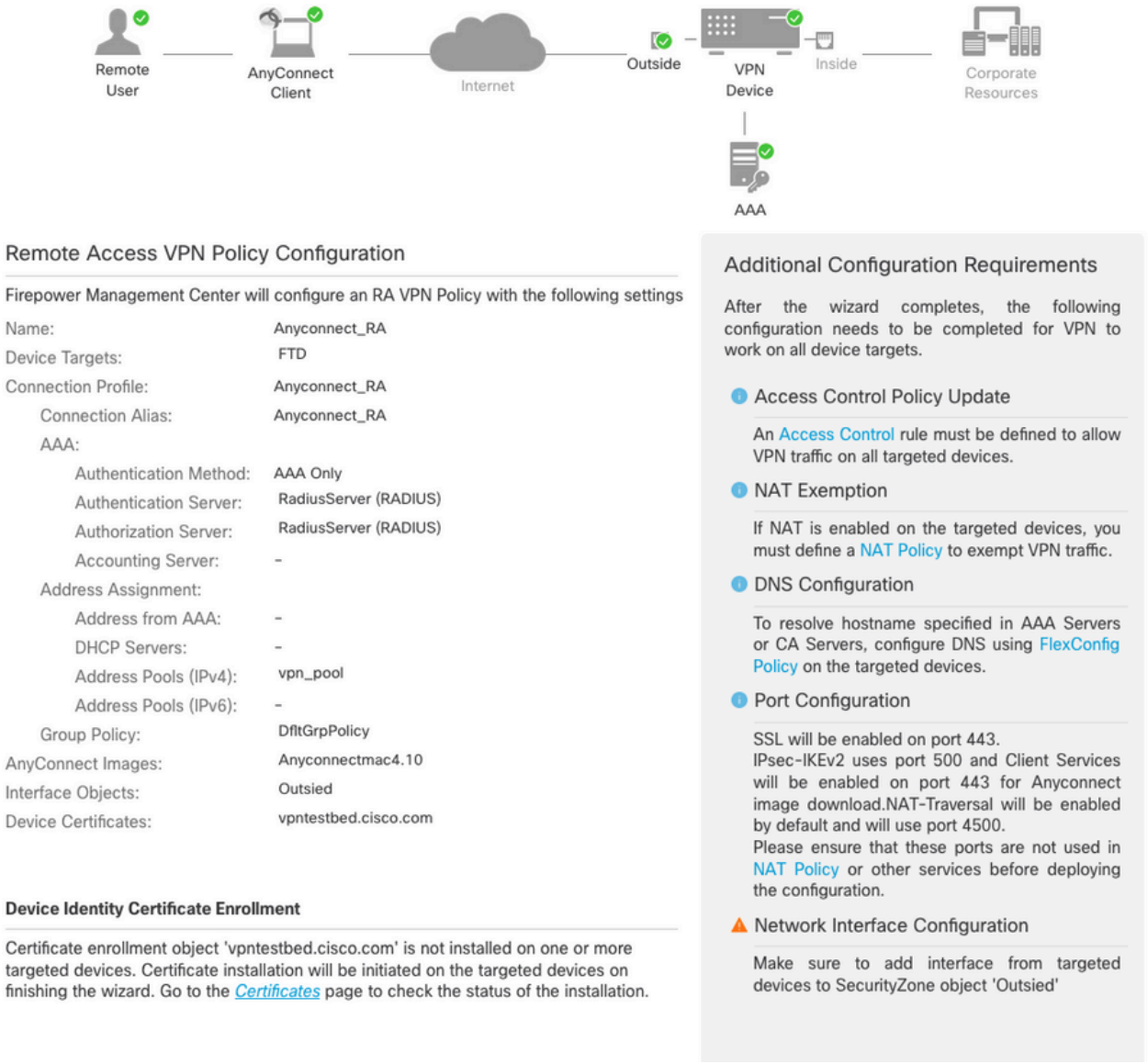
- Sur la page suivante, sélectionnez Images AnyConnect et cliquez sur Next.



- Dans l'écran suivant, sélectionnez **Network Interface and Device Certificates**:



- Lorsque tout est correctement configuré, vous pouvez cliquer sur Finish et ensuite Deploy:



- Cette opération copie l'intégralité de la configuration avec les certificats et les packages AnyConnect vers l'appliance FTD.

Connexion

Pour vous connecter à FTD, vous devez ouvrir un navigateur, tapez le nom DNS ou l'adresse IP qui pointe vers l'interface externe. Vous vous connectez ensuite avec les informations d'identification stockées sur le serveur RADIUS et suivez les instructions à l'écran. Une fois AnyConnect installé, vous devez placer la même adresse dans la fenêtre AnyConnect et cliquer sur Connect.

Limites

Actuellement non pris en charge sur FTD, mais disponible sur ASA :

- La sélection d'interface dans le serveur RADIUS n'est pas prise en charge sur Firepower Threat Defense6.2.3 ou les versions antérieures. L'option d'interface est ignorée pendant le déploiement.
- Un serveur RADIUS activé pour l'autorisation dynamique nécessite Firepower Threat

Defense6.3 ou version ultérieure pour que l'autorisation dynamique fonctionne.
- Le VPN FTDposture ne prend pas en charge la modification de stratégie de groupe via l'autorisation dynamique ou la modification d'autorisation RADIUS (CoA).
- Personnalisation AnyConnect (amélioration : ID de bogue Cisco CSCvq87631)
- scripts AnyConnect
- Localisation AnyConnect
- Intégration WSA
- Carte de cryptage dynamique IKEv2 simultanée pour les VPN RA et L2L (amélioration : ID de bogue Cisco CSCvr52047)
- Modules AnyConnect (NAM, Hostscan, AMP Enabler, SBL, Umbrella, Web Security, etc.) - DART est installé par défaut (améliorations pour AMP Enabler et Umbrella : ID de bogue Cisco CSCvs03562 et ID de bogue Cisco CSCvs06642).
- TACACS, Kerberos (authentification KCD et RSA SDI)
- Proxy du navigateur

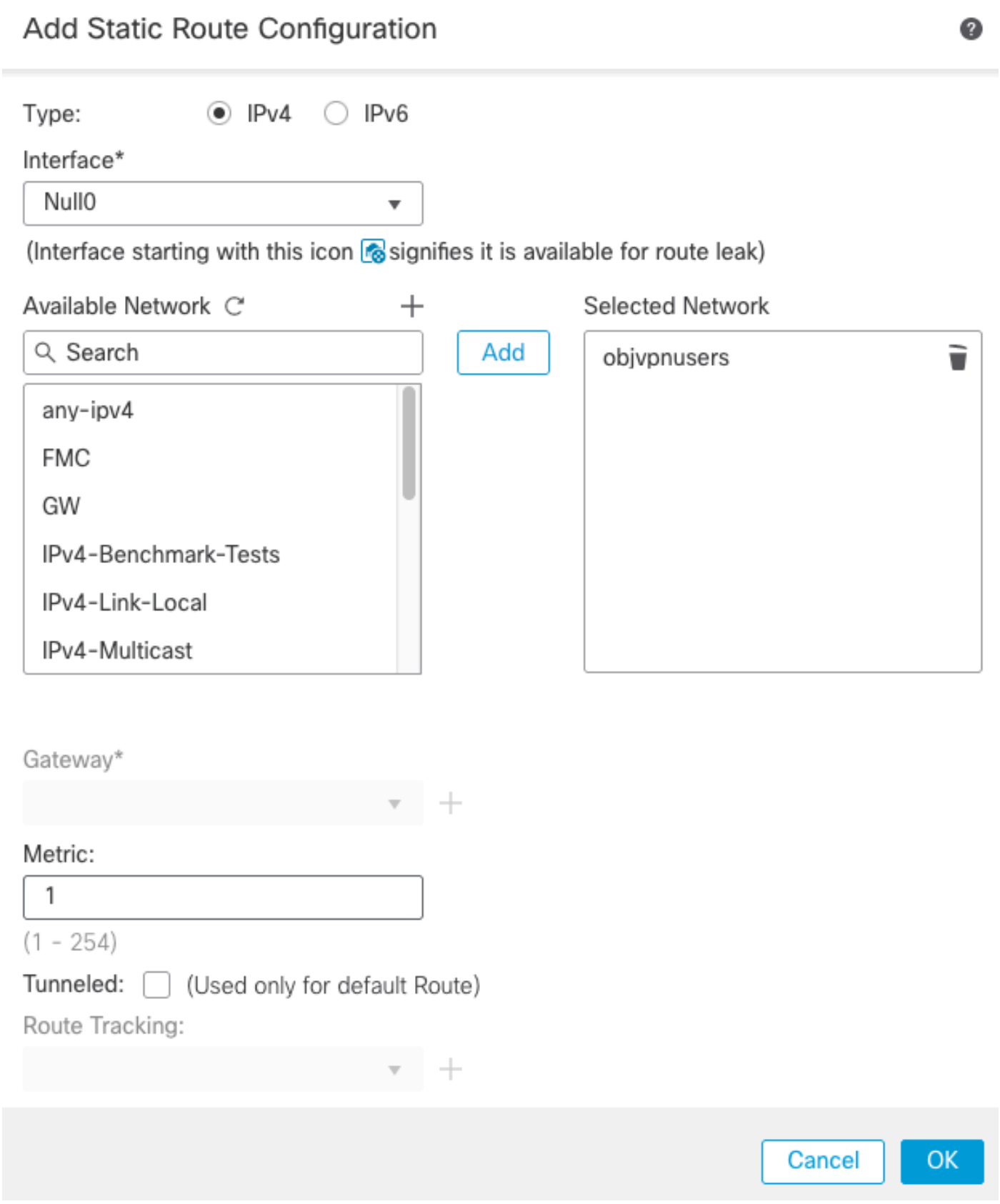
Considérations de sécurité

Par défaut, le sysopt connection permit-vpnest désactivée. Cela signifie que vous devez autoriser le trafic provenant du pool d'adresses sur l'interface externe via la politique de contrôle d'accès. Bien que la règle de préfiltrage ou de contrôle d'accès soit ajoutée pour autoriser uniquement le trafic VPN, si le trafic en texte clair correspond aux critères de la règle, il est autorisé par erreur.

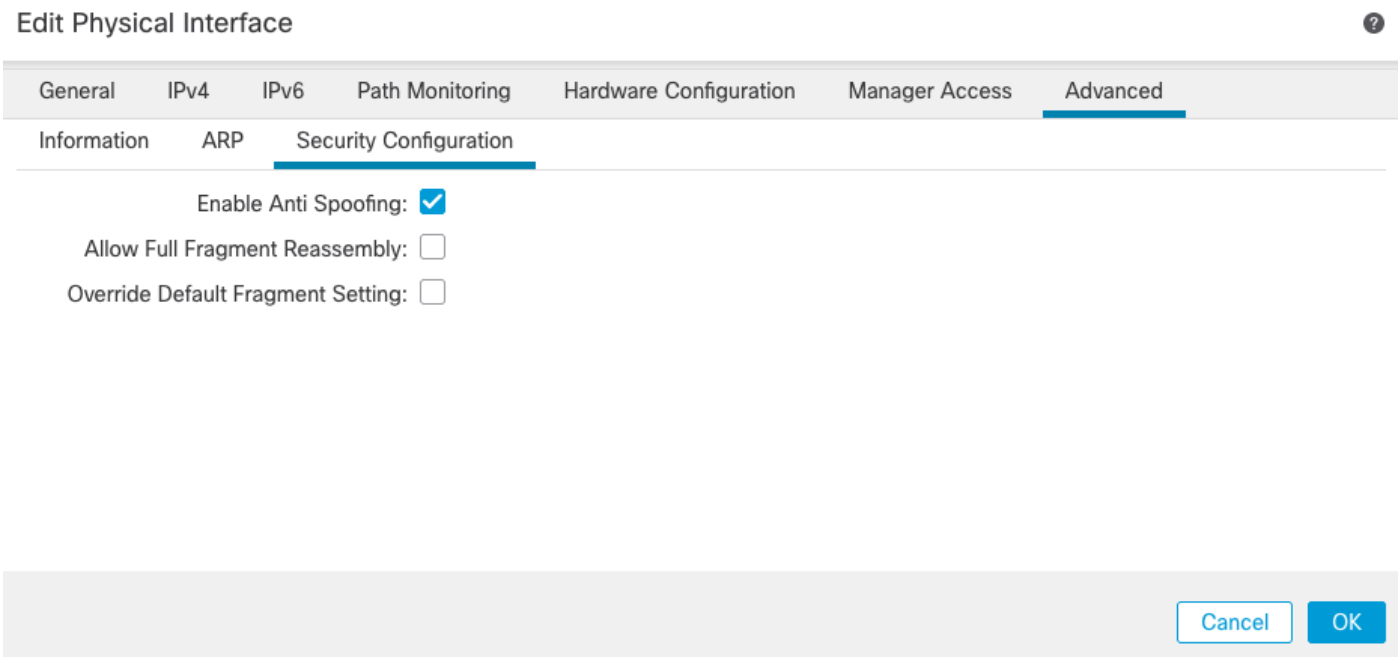
Il y a deux approches à ce problème. Premièrement, l'option recommandée par le TAC est d'activer l'anti-usurpation (sur ASA, il était connu sous le nom de Unicast Reverse Path Forwarding - uRPF) pour l'interface externe, et deuxièmement, est d'activer sysopt connection permit-vpn pour contourner complètement l'inspection Snort. La première option permet une inspection normale du trafic qui va vers et depuis les utilisateurs VPN.

a) Activer uRPF

- Créez une route Null pour le réseau utilisé pour les utilisateurs d'accès à distance, défini dans la section C. Accédez à Devices > Device Management > Edit > Routing > Static Route et sélectionnez Add route



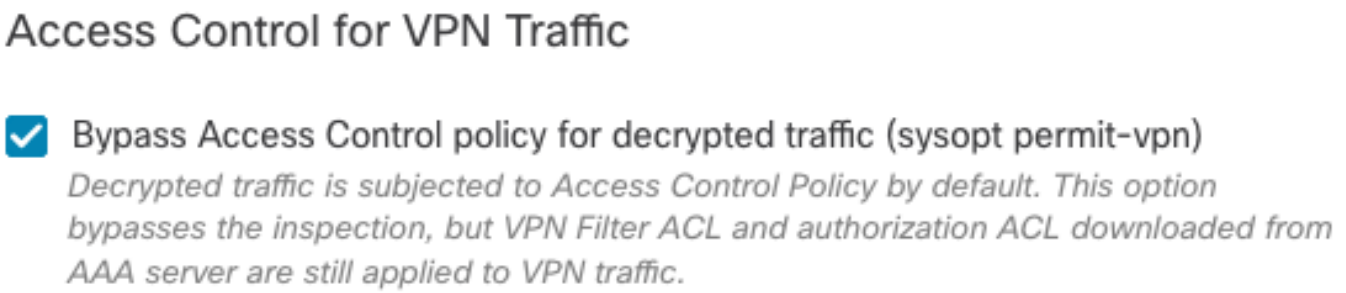
- Activez ensuite uRPF sur l'interface où se terminent les connexions VPN. Pour le trouver, accédez à **Devices > Device Management > Edit > Interfaces > Edit > Advanced > Security Configuration > Enable Anti Spoofing**.



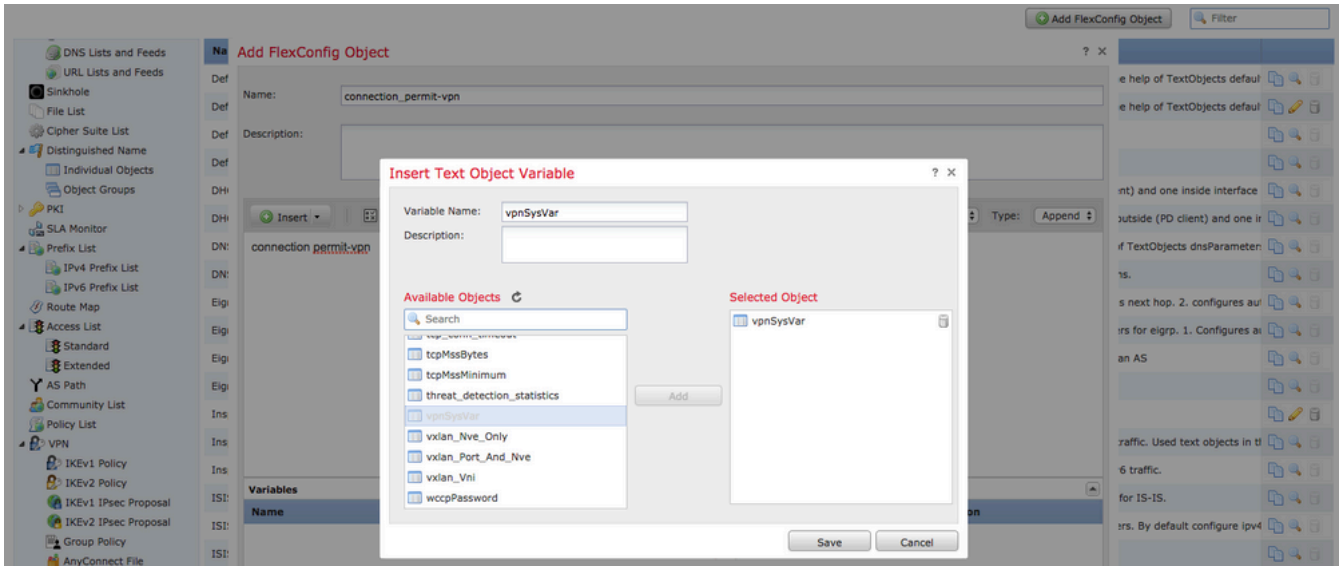
Lorsqu'un utilisateur est connecté, la route 32 bits est installée pour cet utilisateur dans la table de routage. Effacer le trafic texte provenant des autres adresses IP inutilisées du pool est abandonné par uRFP. Pour afficher une description de **Anti-Spoofing**référez-vous à [Définir les paramètres de configuration de sécurité sur Firepower Threat Defense.]

b) Activer Sysopt connection permit-vpn Option

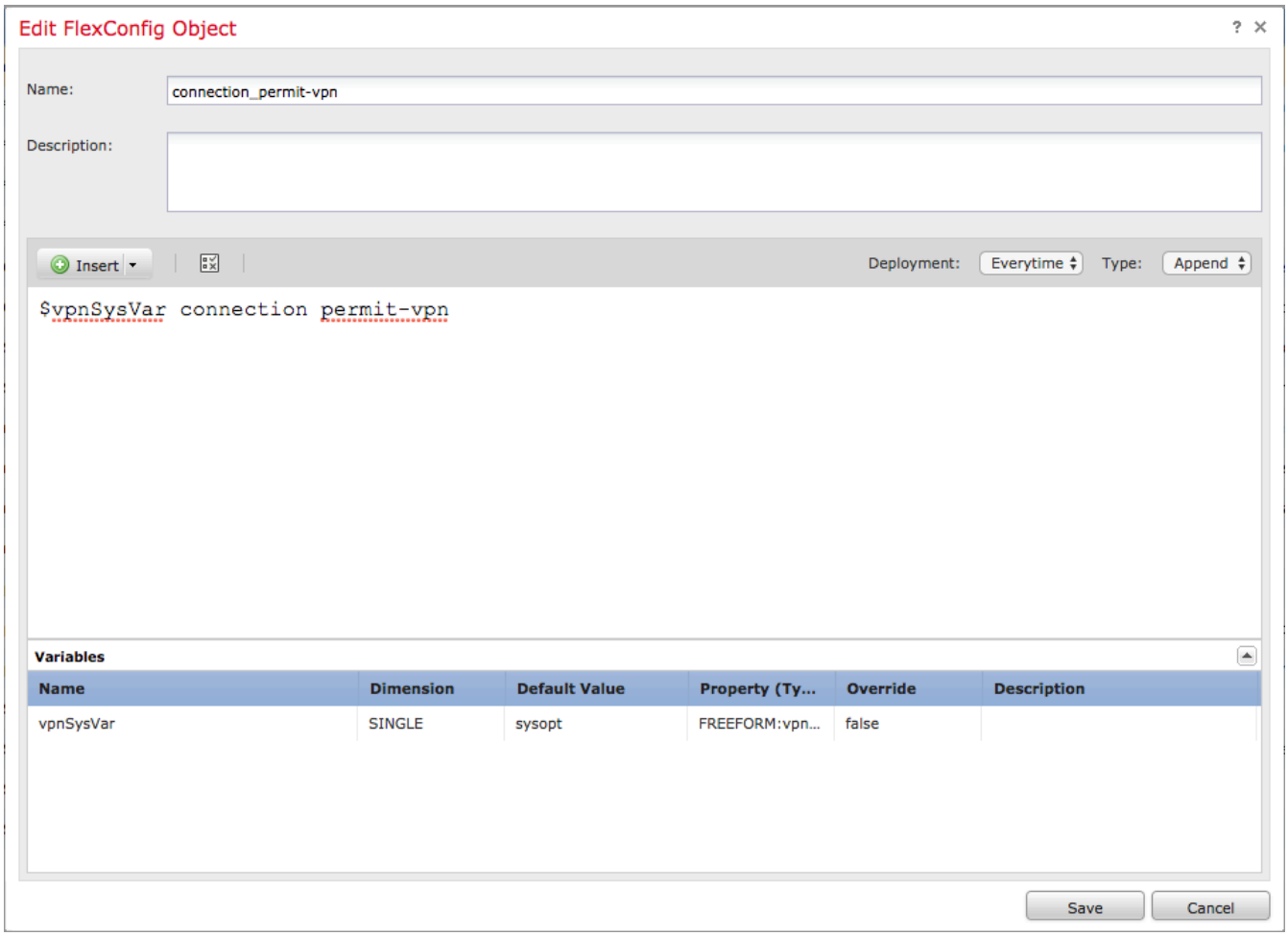
- Si vous disposez de la version 6.2.3 ou d'une version ultérieure, vous pouvez le faire avec l'Assistant ou sous Devices > VPN > Remote Access > VPN Profile > Access Interfaces.



- Pour les versions antérieures à la version 6.2.3, accédez à Objects > Object Management > FlexConfig > Text Object > Add Text Object.
- Créez une variable d'objet texte, par exemple : vpnSysVar une entrée unique avec une valeur sysopt.
- Aller à Objects**> Object Management > FlexConfig > FlexConfig Object > Add FlexConfig Object.**
- Créez le FlexConfig objet avec CLI connection permit-vpn.
- Insère la variable d'objet texte dans le FlexConfig au niveau de l'interface CLI avec **$vpnSysVar connection permit-vpn**. Cliquer Save:



- Appliquez le FlexConfigobjet en tant que **Append** et sélectionnez le déploiement à Everytime:



- Aller à**Devices > FlexConfig** et modifiez la stratégie actuelle ou créez-en une nouvelle avec New Policy s'affiche.
- Ajoutez uniquement le fichier créé FlexConfig, cliquez sur Save.
- Déployer la configuration pour provisionner**sysopt connection permit-vpn**sur le périphérique.

Après cela, cependant, vous ne pouvez pas utiliser la stratégie de contrôle d'accès pour inspecter le trafic provenant des utilisateurs. Vous pouvez toujours utiliser un filtre VPN ou une liste de contrôle d'accès téléchargeable pour filtrer le trafic utilisateur.

Si vous voyez des paquets abandonnés avec Snort provenant des utilisateurs VPN, contactez le TAC et référencez l'ID de bogue Cisco CSCvg91399.

Informations connexes

- Assistance technique et téléchargements Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.