Configuration du client VPN AnyConnect sur FTD : exemption Hairpin et NAT

Table des matières

Introduction

Ce document décrit comment configurer la solution VPN d'accès à distance Cisco (AnyConnect) sur Firepower Threat Defense (FTD), v6.3, gérée par FMC.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base en matière de VPN d’accès à distance, de protocole SSL (Secure Sockets Layer) et d’échange de clés Internet version 2 (IKEv2)
- Connaissances de base en authentification, autorisation et comptabilité (AAA) et RADIUS
- Connaissances FMC de base
- Connaissances FTD de base

Composants utilisés

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

- Cisco FMC 6.4
- Cisco FTD 6.3
- AnyConnect 4.7

Ce document décrit la procédure de configuration de la solution VPN d'accès à distance Cisco (AnyConnect) sur Firepower Threat Defense (FTD), version 6.3, gérée par Firepower Management Center (FMC).

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 est destiné à couvrir la configuration sur les périphériques FTD. Si vous recherchez l'exemple de configuration ASA, veuillez vous reporter au document : https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html

Limites:

Actuellement, ces fonctionnalités ne sont pas prises en charge sur FTD, mais sont toujours disponibles sur les périphériques ASA :

- Double authentification AAA (disponible sur FTD version 6.5)
- Politique d'accès dynamique
- Analyse des hôtes
- posture ISE
- RADIUS CoA
- Équilibreur de charge VPN
- Authentification locale (disponible dans Firepower Device Manager 6.3). ID de bogue Cisco CSCvf92680)
- Mappage des attributs LDAP (disponible via FlexConfig, ID de bogue Cisco CSCvd64585)
- Personnalisation AnyConnect
- scripts AnyConnect
- Localisation AnyConnect
- VPN par application
- Proxy SCEP
- Intégration WSA
- SSO SAML (ID de bogue Cisco CSCvq90789)
- Crypto-carte dynamique IKEv2 simultanée pour RA et VPN L2L
- Modules AnyConnect (NAM, Hostscan, AMP Enabler, SBL, Umbrella, Web Security, etc.) DART est le seul module installé par défaut sur cette version.
- TACACS, Kerberos (authentification KCD et RSA SDI)
- Proxy du navigateur

Configurer

Afin de passer par l'assistant VPN d'accès à distance dans le FMC, ces étapes doivent être effectuées :

Étape 1. Importer un certificat SSL

Les certificats sont essentiels lorsque vous configurez AnyConnect. Seuls les certificats RSA sont pris en charge pour SSL et IPSec.

Les certificats ECDSA (Elliptic Curve Digital Signature Algorithm) sont pris en charge dans IPSec, mais il n'est pas possible de déployer un nouveau package AnyConnect ou un nouveau profil XML lorsque le certificat basé sur ECDSA est utilisé.

Il peut être utilisé pour IPSec, mais vous devez pré-déployer les packages AnyConnect avec le profil XML, toutes les mises à jour de profil XML doivent être poussées manuellement sur chaque client (ID de bogue Cisco CSCtx42595).

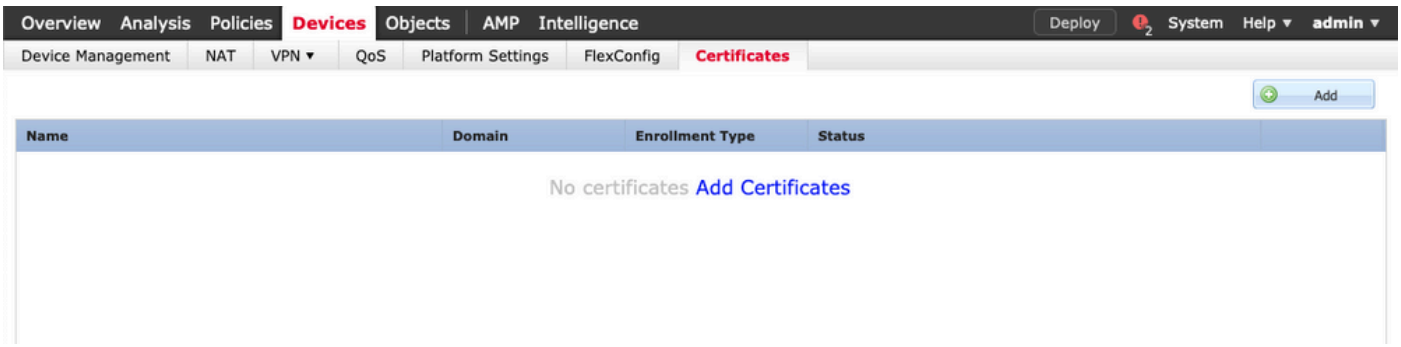
En outre, le certificat doit contenir une extension de nom commun (CN) avec un nom DNS et/ou une adresse IP afin d'éviter les erreurs de « certificat de serveur non approuvé » dans les navigateurs Web.

Remarque : sur les périphériques FTD, le certificat de l'autorité de certification (CA) est nécessaire avant la génération de la demande de signature de certificat (CSR).

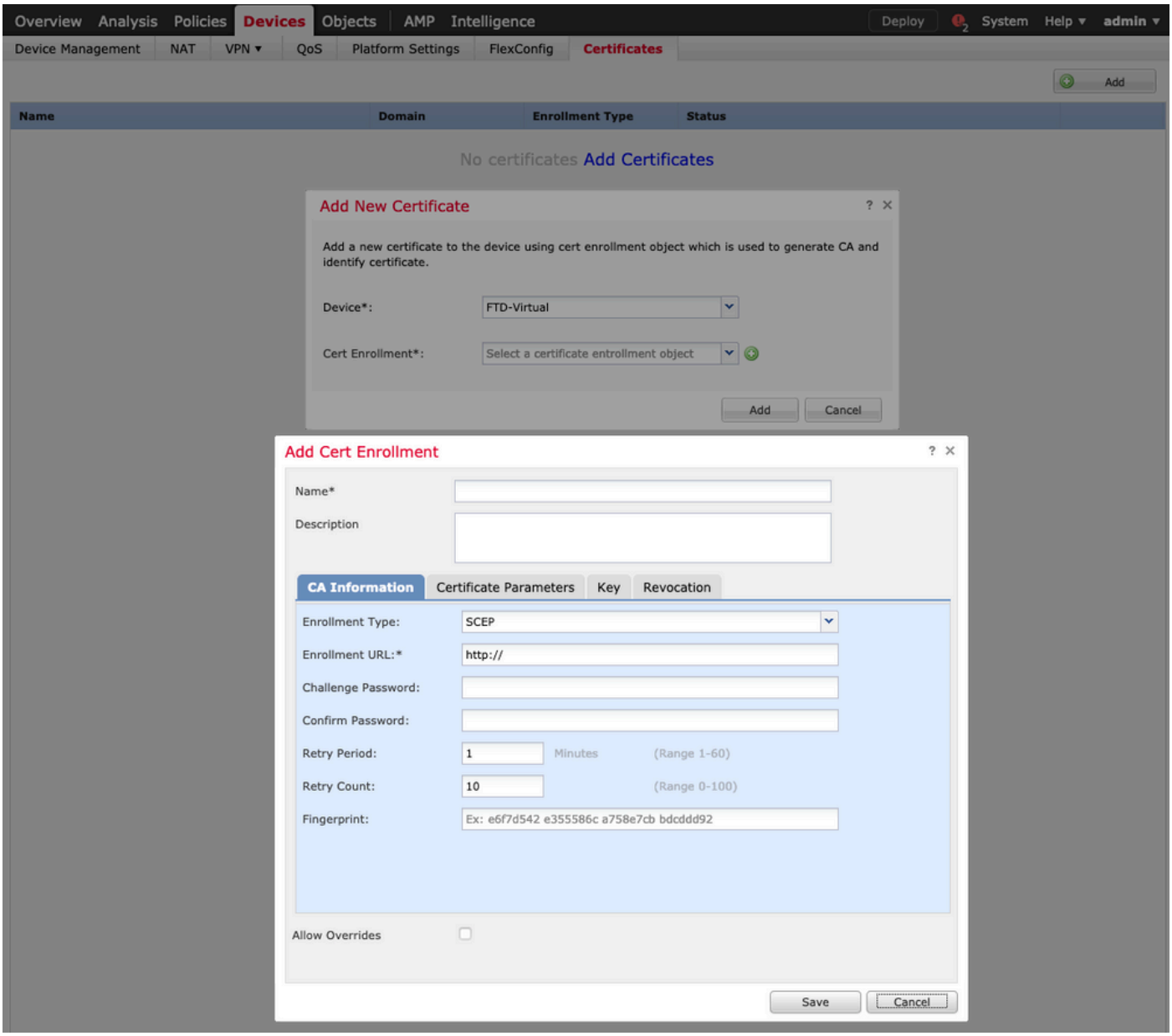
- Si le CSR est généré dans un serveur externe (tel que Windows Server ou OpenSSL), la méthode d'inscription manuelle est censée échouer, car FTD ne prend pas en charge l'inscription manuelle de clé.
- Une autre méthode doit être utilisée, telle que PKCS12.

Pour obtenir un certificat pour l'appareil FTD avec la méthode d'inscription manuelle, un CSR doit être généré, signé avec une autorité de certification, puis importé le certificat d'identité.

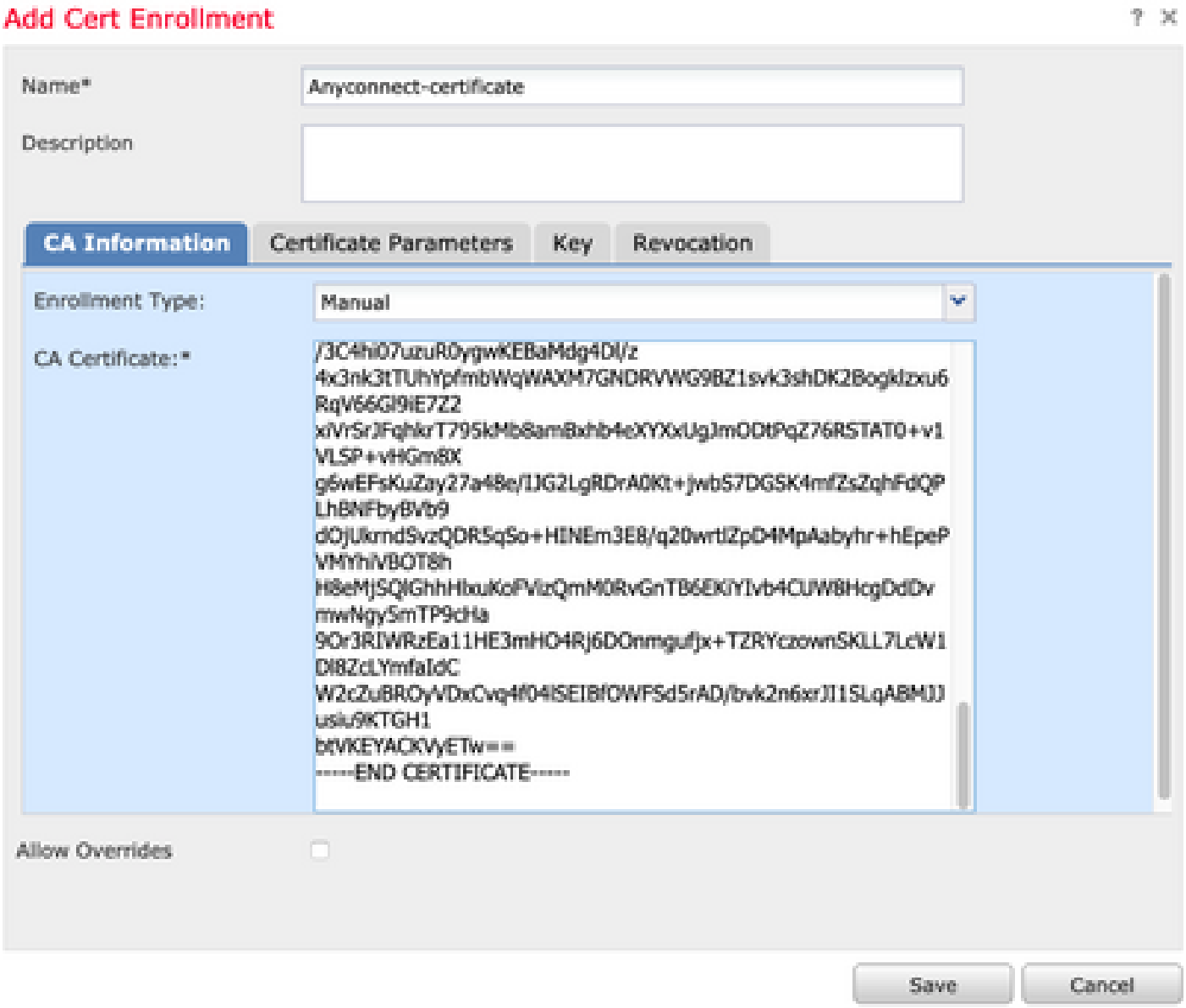
1. Accédez à Périphériques > Certificats et sélectionnez Ajouter comme indiqué dans l'image.



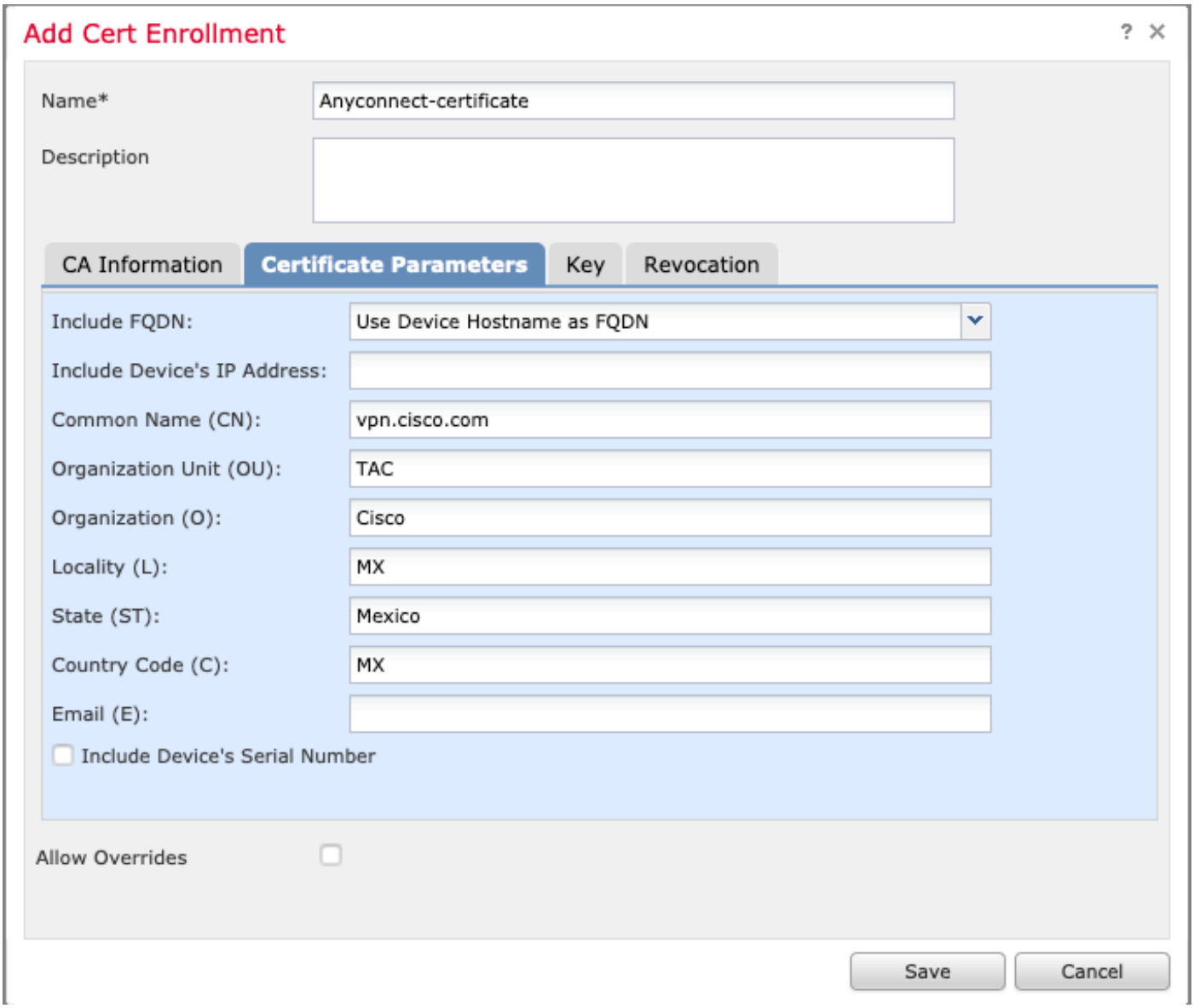
2. Sélectionnez le périphérique et ajoutez un nouvel objet Inscription de certificat comme illustré dans l'image.



3. Sélectionnez le type d'inscription manuelle et collez le certificat de l'autorité de certification (le certificat destiné à signer le CSR).

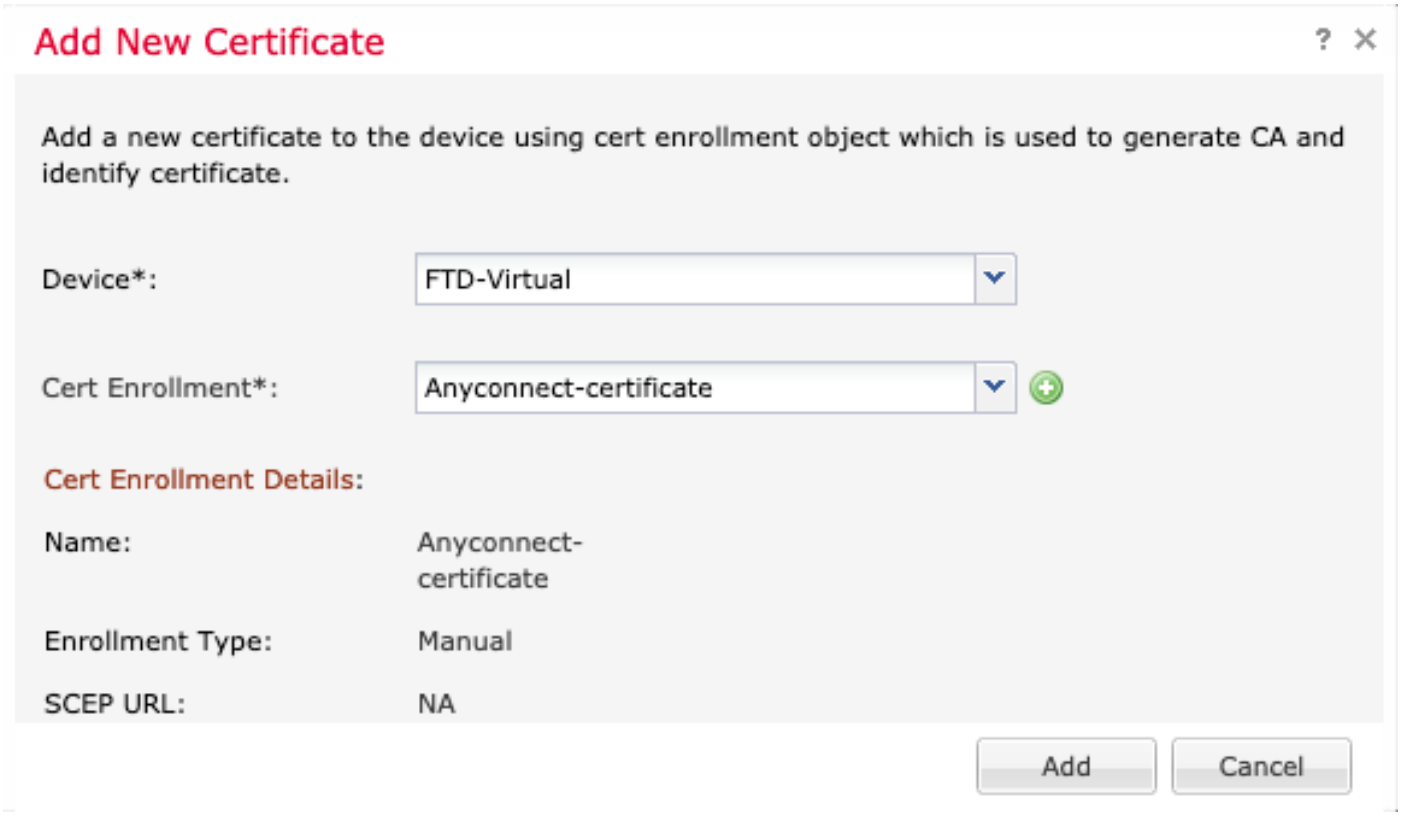


4. Sélectionnez l'onglet Certificate Parameters et sélectionnez "Custom FQDN" pour le champ Include FQDN et remplissez les détails du certificat comme indiqué dans l'image.

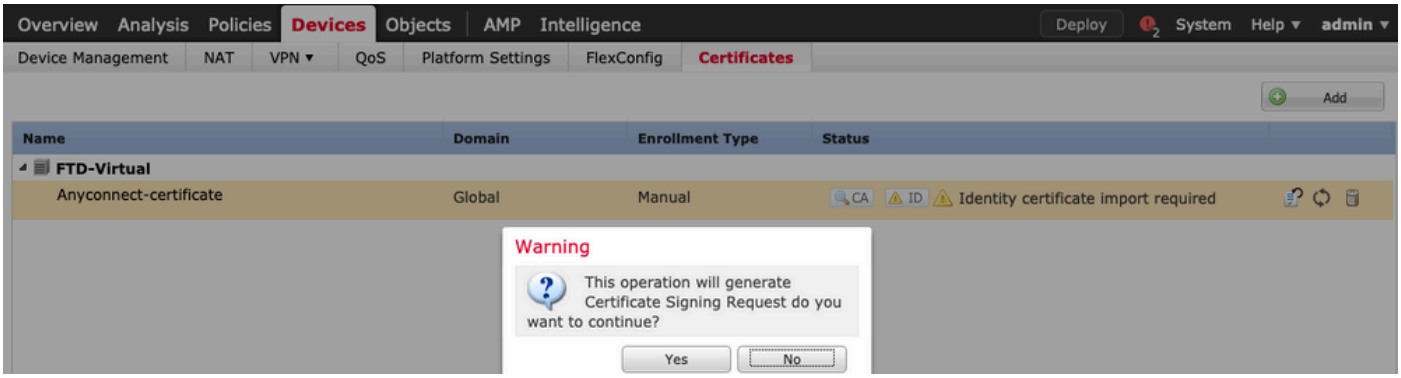


5. Sélectionnez l'onglet Clé, puis sélectionnez le type de clé, vous pouvez choisir le nom et la taille. Pour RSA, 2 048 octets sont requis au minimum.

6. Sélectionnez save, confirm the Device, et sous Cert Enrollment sélectionnez le point de confiance qui vient d'être créé, sélectionnez Add afin de déployer le certificat.

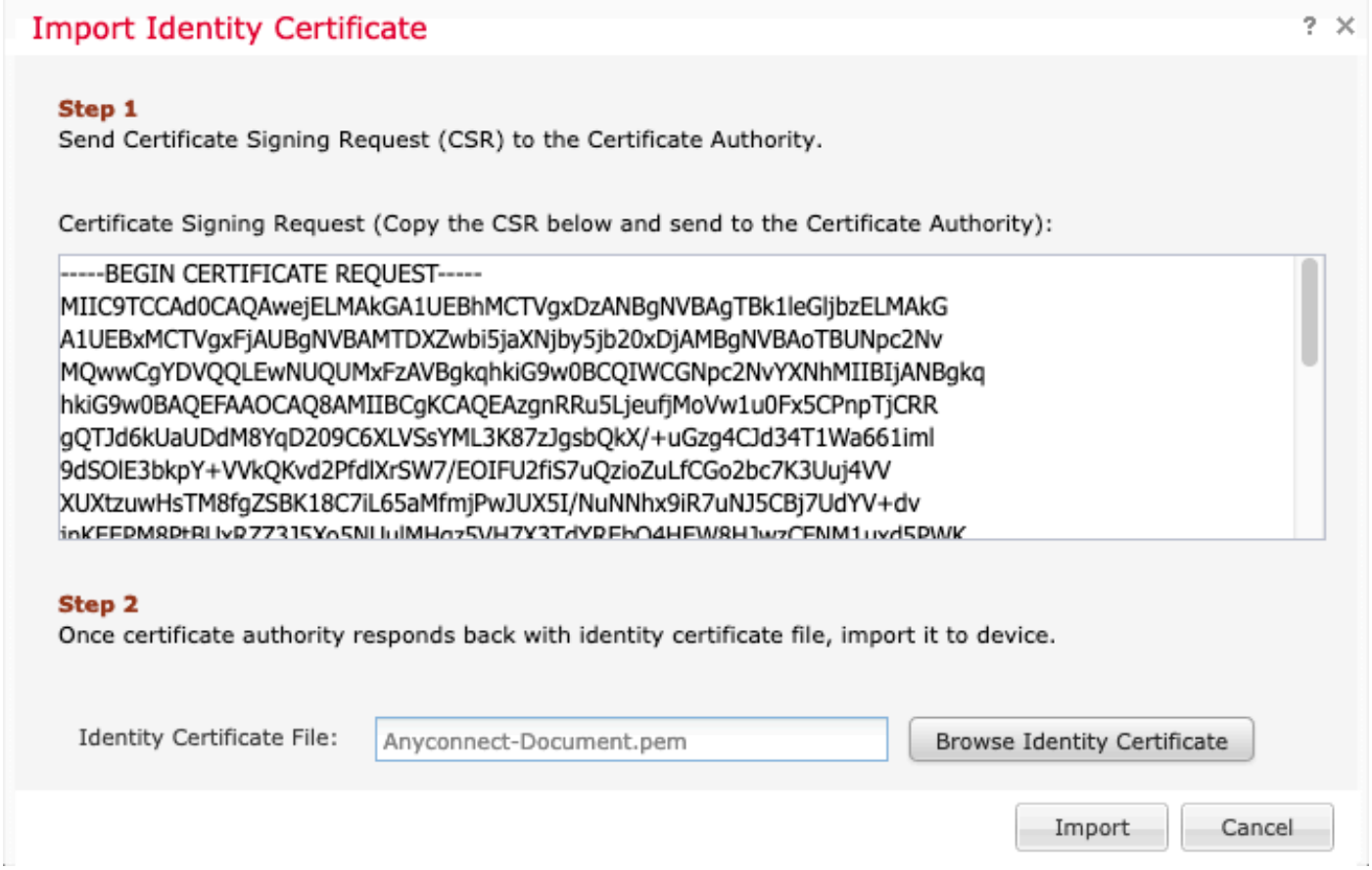


7. Dans la colonne Statut, sélectionnez l'icône ID et sélectionnez Oui pour générer le CSR comme indiqué dans l'image.

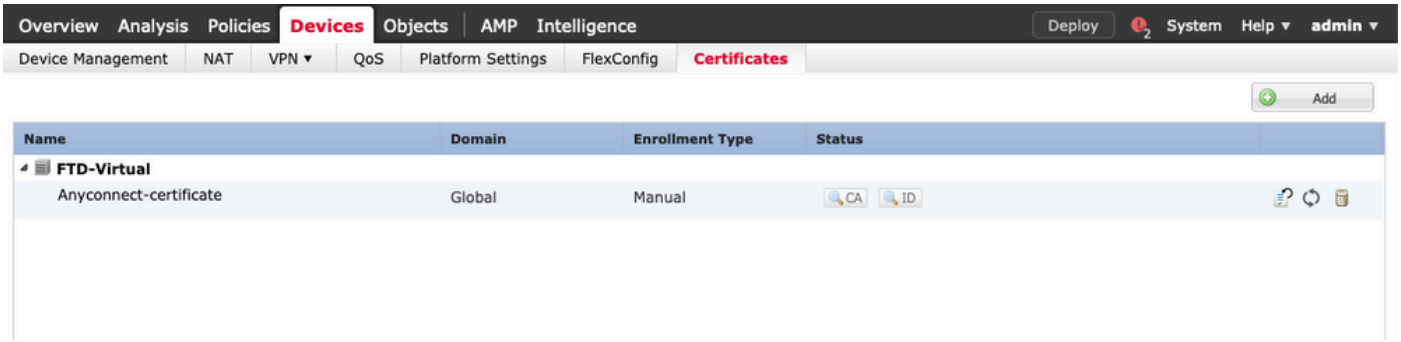


8. Copiez CSR et signez-le avec votre CA préférée (par exemple GoDaddy ou DigiCert).

9. Une fois le certificat d'identité reçu de l'autorité de certification (qui doit être au format base64), sélectionnez Browse Identity Certificate et recherchez le certificat sur l'ordinateur local. Sélectionnez Importer.



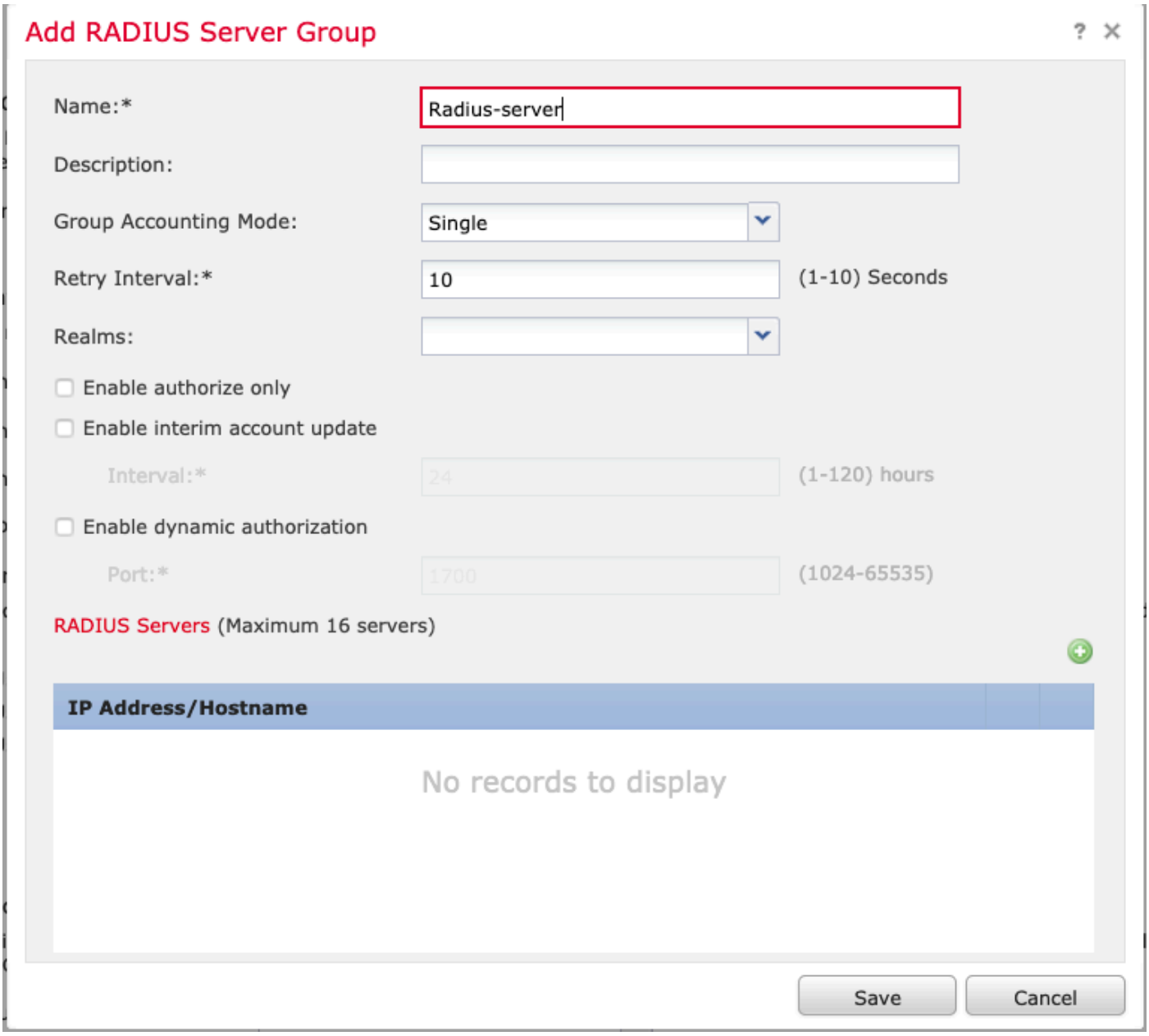
10. Une fois importés, les détails du certificat CA et ID peuvent être affichés.



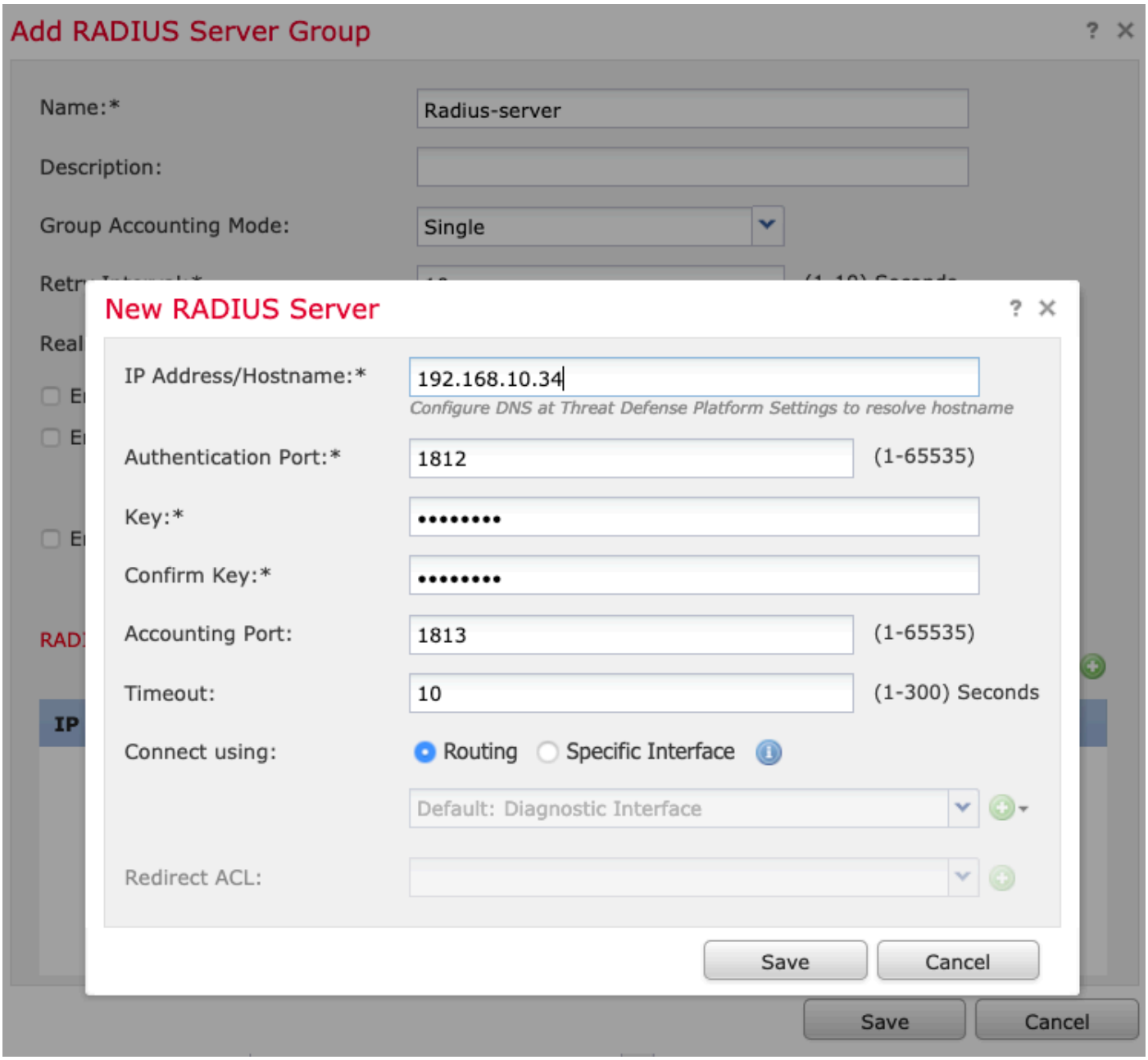
Étape 2. Configurer un serveur RADIUS

Sur les périphériques FTD gérés par FMC, la base de données utilisateur locale n'est pas prise en charge, une autre méthode d'authentification doit être utilisée, telle que RADIUS ou LDAP.

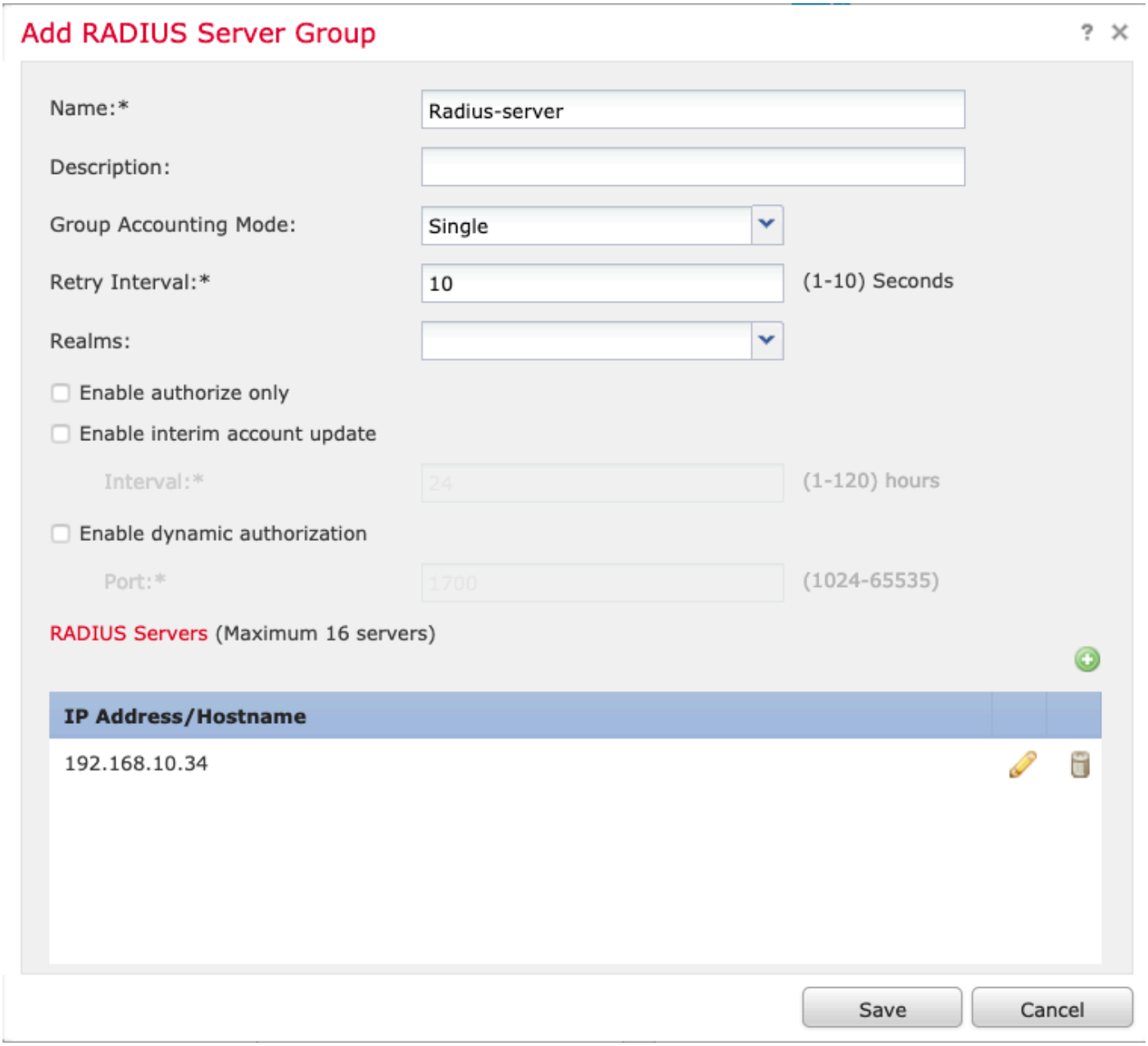
1. Accédez à Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group comme indiqué dans l'image.



2. Attribuez un nom au groupe de serveurs Radius et ajoutez l'adresse IP du serveur Radius avec un secret partagé (le secret partagé est requis pour associer le FTD au serveur Radius), sélectionnez Enregistrer une fois que ce formulaire est rempli comme indiqué dans l'image.



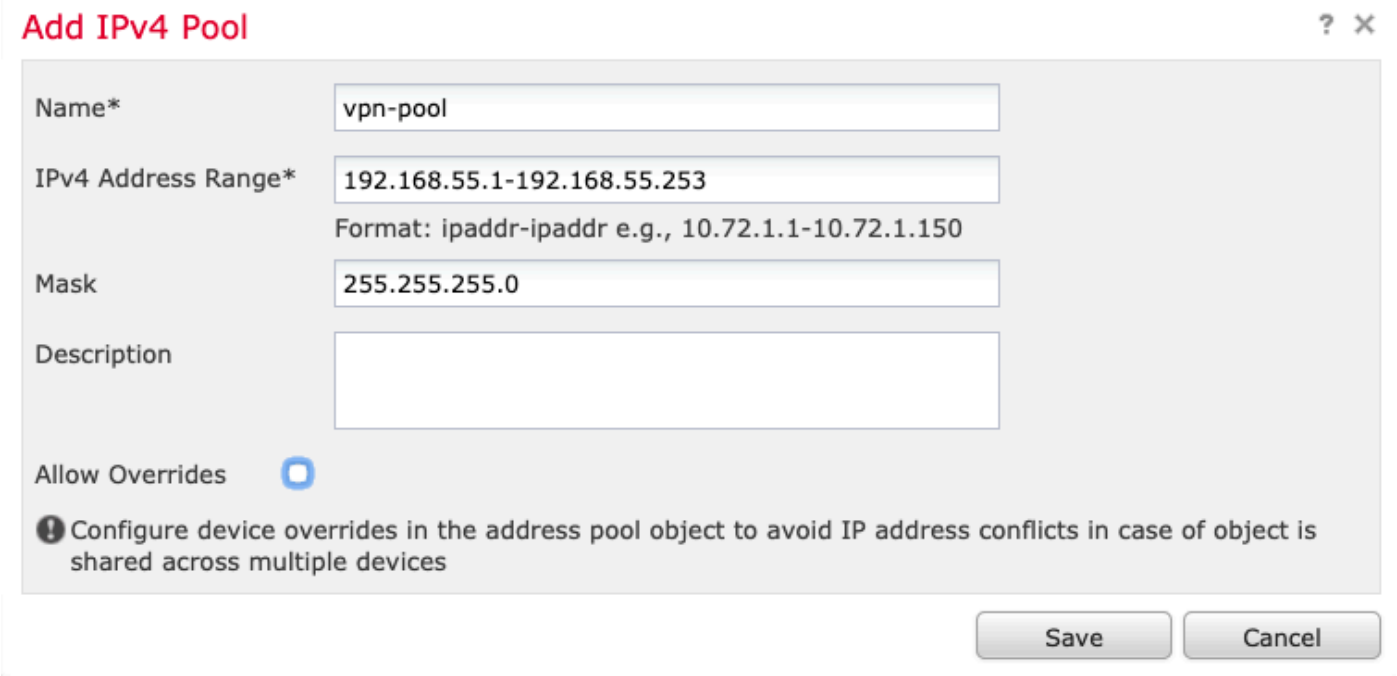
3. Les informations sur le serveur RADIUS sont désormais disponibles dans la liste des serveurs RADIUS, comme illustré dans l'image.



Étape 3. Créer un pool d'adresses IP

1. Accédez à Objets > Gestion des objets > Pools d'adresses > Ajouter des pools IPv4.

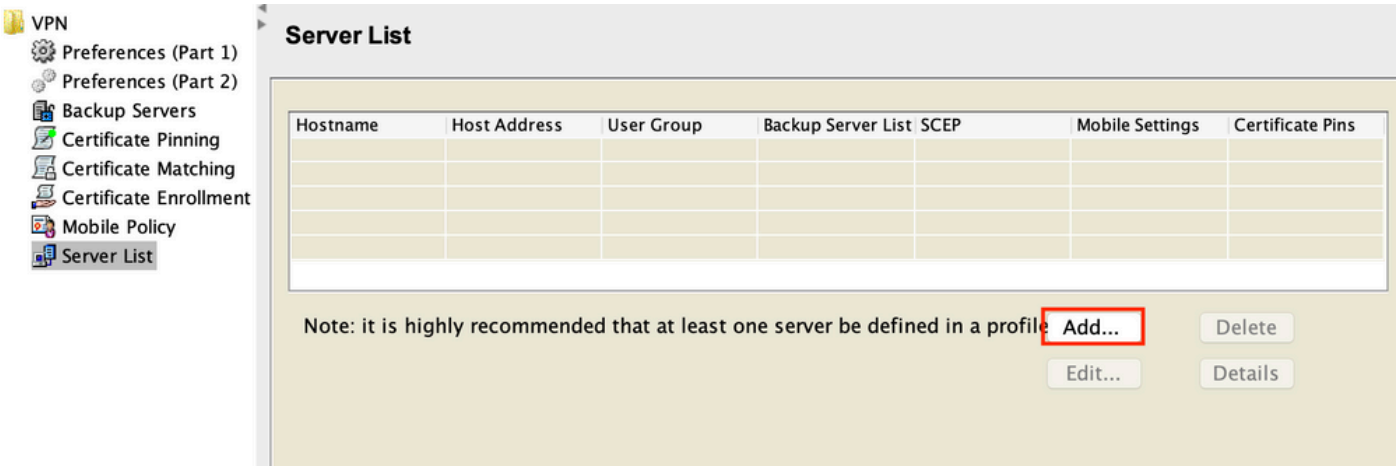
2. Attribuez le nom et la plage d'adresses IP, le champ Mask n'est pas obligatoire mais il peut être spécifié comme indiqué dans l'image.



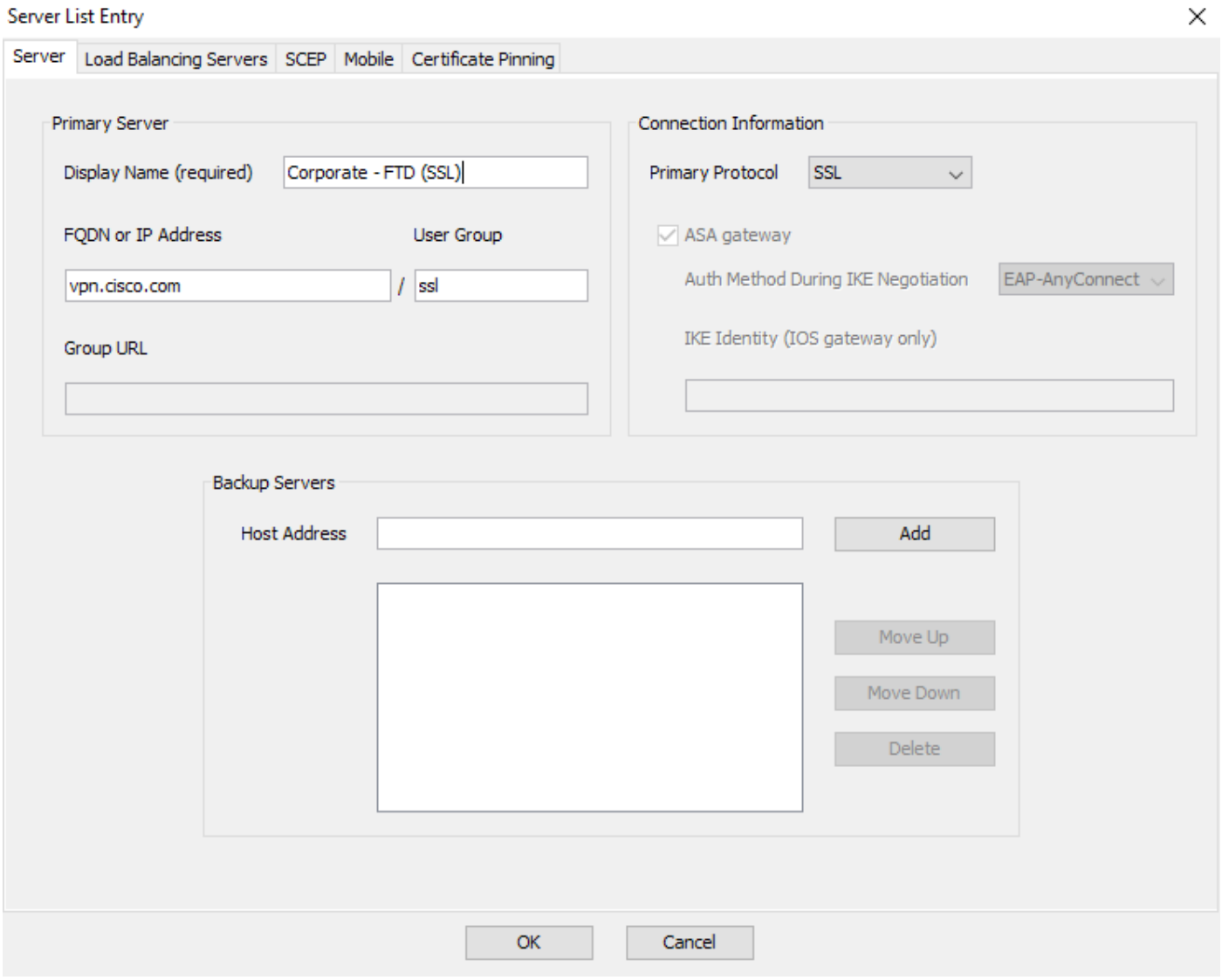
Étape 4. Créer un profil XML

1. Téléchargez l'outil Éditeur de profil à partir de Cisco.com et exécutez l'application.

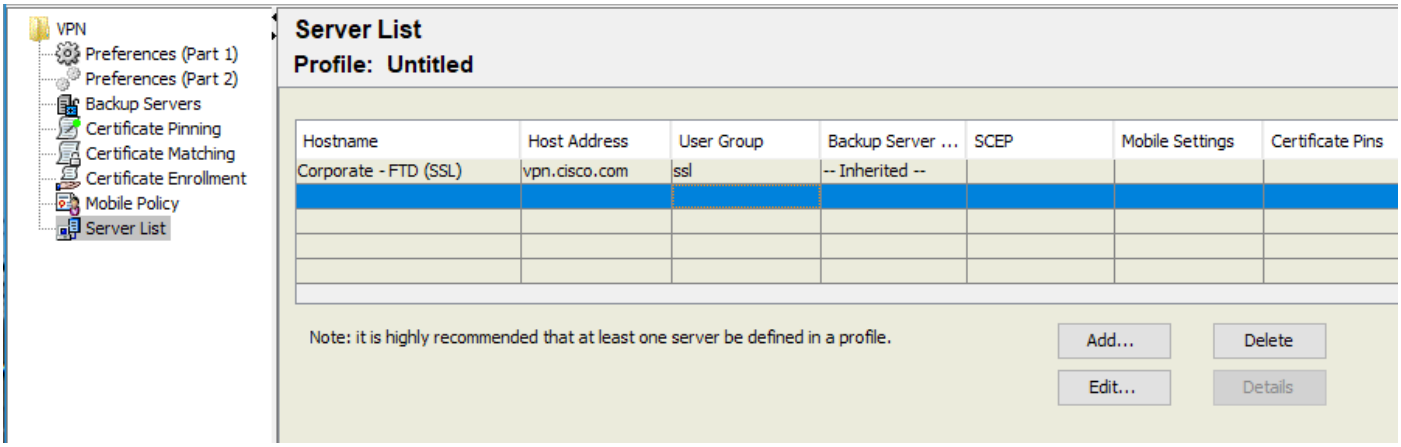
2. Dans l'application Éditeur de profil, naviguez jusqu'à Liste des serveurs et sélectionnez Ajouter comme indiqué dans l'image.



3. Attribuez un nom d'affichage, un nom de domaine complet (FQDN) ou une adresse IP et sélectionnez OK comme indiqué dans l'image.



4. L'entrée est maintenant visible dans le menu Liste de serveurs :



5. Accédez à Fichier > Enregistrer sous.

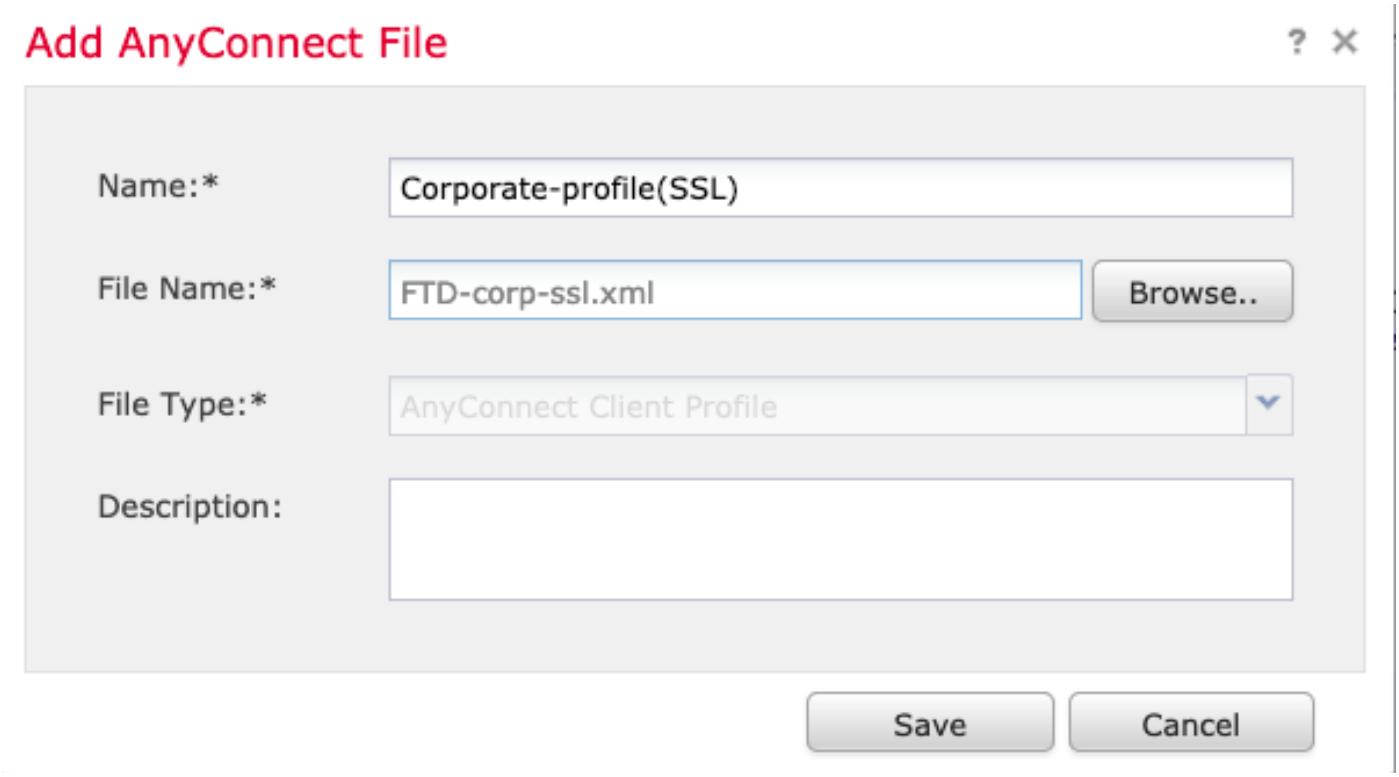
Remarque : enregistrez le profil sous un nom facilement identifiable avec une extension .xml.

Étape 5. Télécharger un profil XML Anyconnect

1. Dans FMC, accédez à Objets > Gestion des objets > VPN > Fichier AnyConnect > Ajouter un fichier AnyConnect.

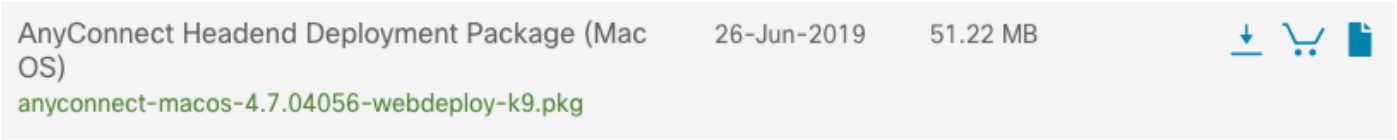
2. Attribuez un nom à l'objet et cliquez sur Parcourir, localisez le profil client dans votre système local et sélectionnez Enregistrer.

⚠ Attention : veillez à sélectionner Anyconnect Client Profile comme type de fichier.



Étape 6. Télécharger des images AnyConnect

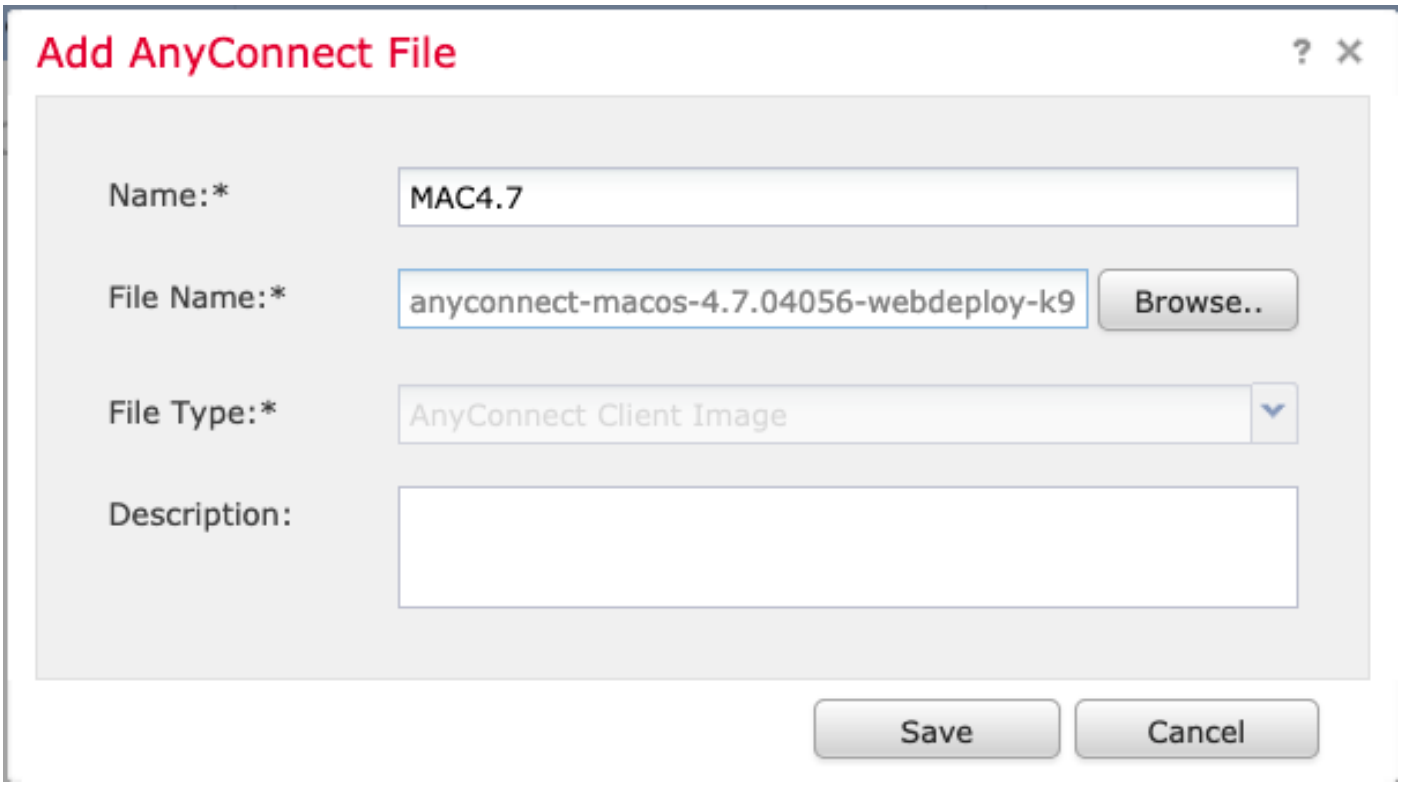
1. Téléchargez les images webdeploy (.pkg) à partir de la page Web de téléchargement de Cisco.



2. Accédez à Objets > Gestion des objets > VPN > Fichier AnyConnect > Ajouter un fichier AnyConnect.

3. Attribuez un nom au fichier de package Anyconnect et sélectionnez le fichier .pkg dans votre système local, une fois le fichier sélectionné.

4. Sélectionnez Enregistrer.



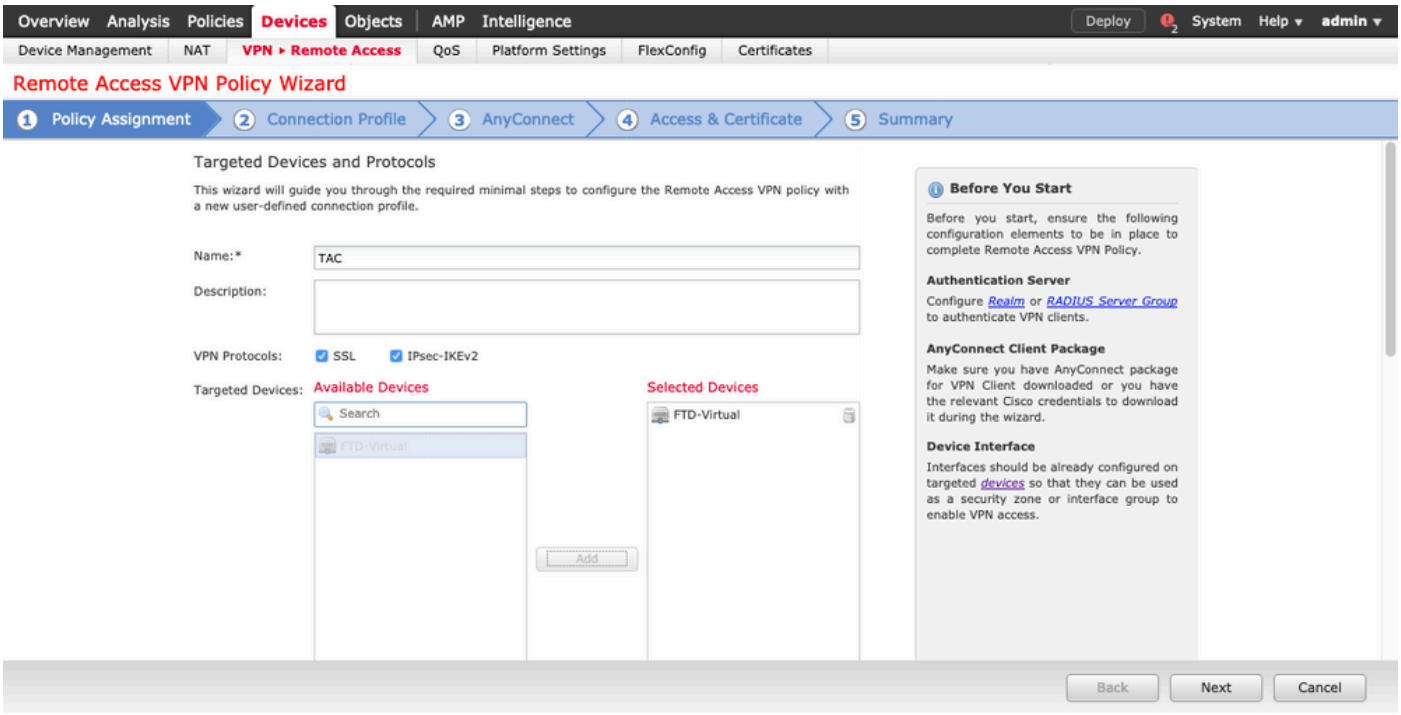
Remarque : des paquets supplémentaires peuvent être téléchargés, en fonction de vos besoins (Windows, Mac, Linux).

Étape 7. Assistant VPN d'accès à distance

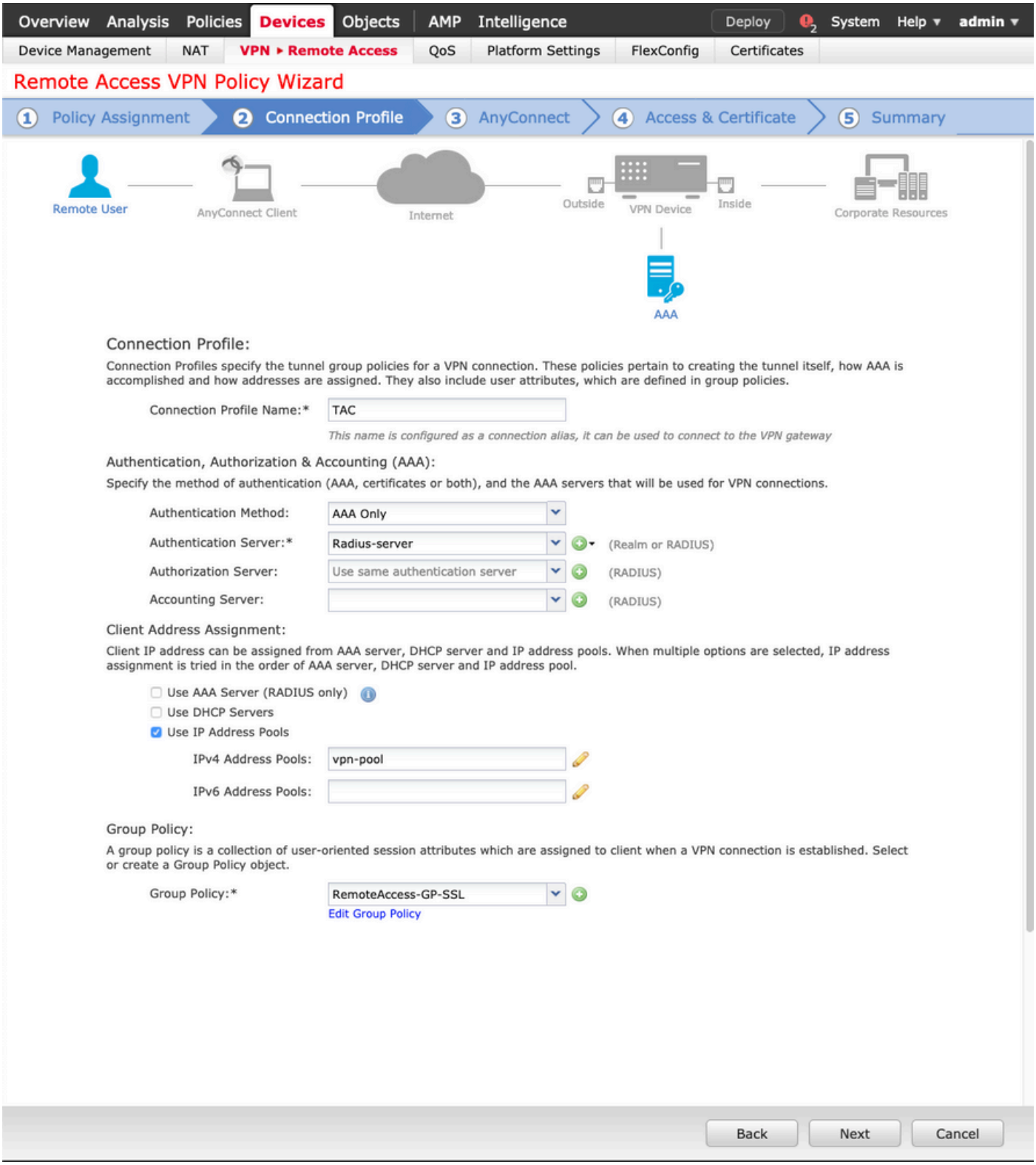
D'après les étapes précédentes, l'assistant d'accès à distance peut être suivi en conséquence.

1. Accédez à Devices > VPN > Remote Access.

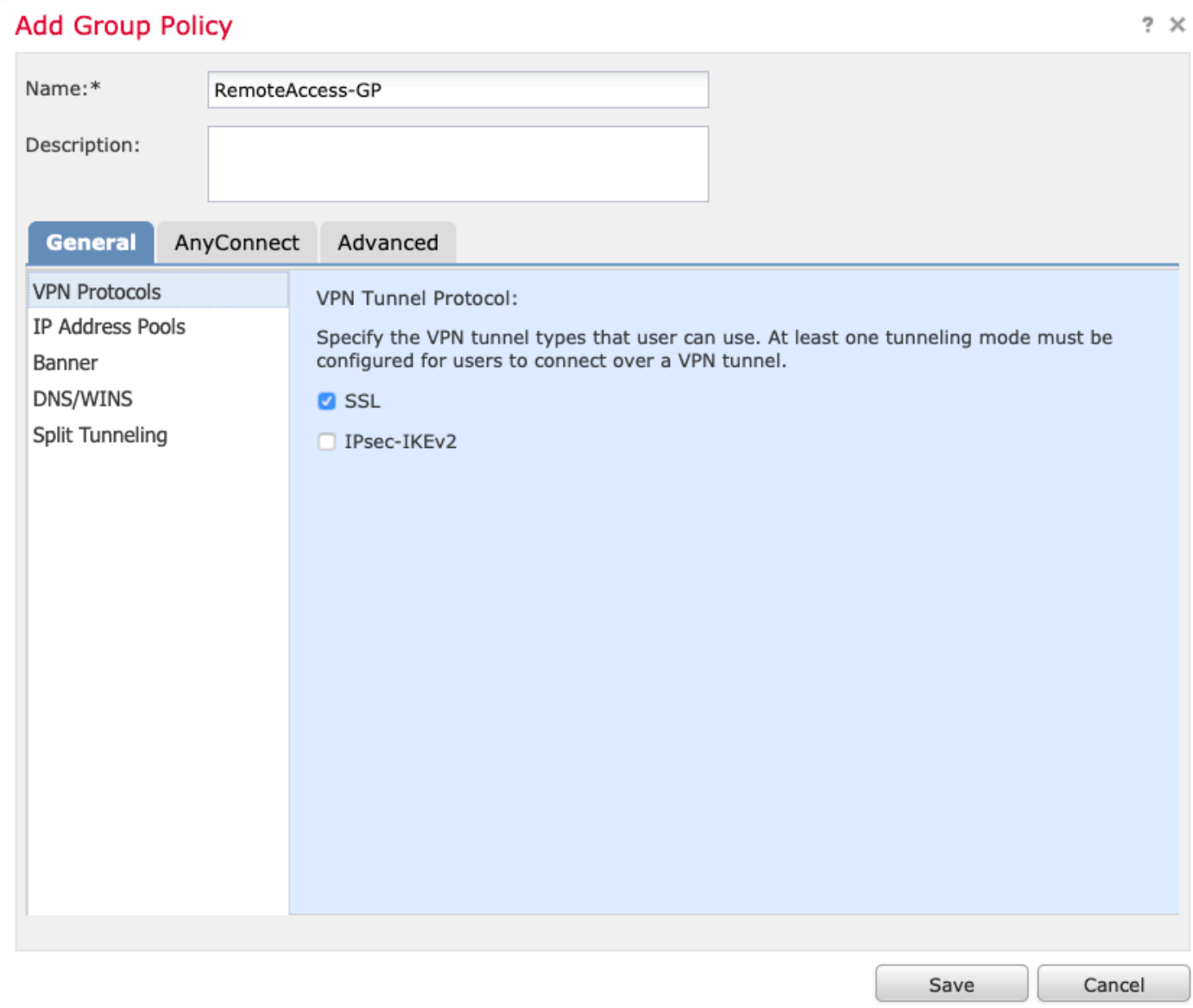
2. Attribuez le nom de la stratégie d'accès à distance et sélectionnez un périphérique FTD dans Périphériques disponibles.



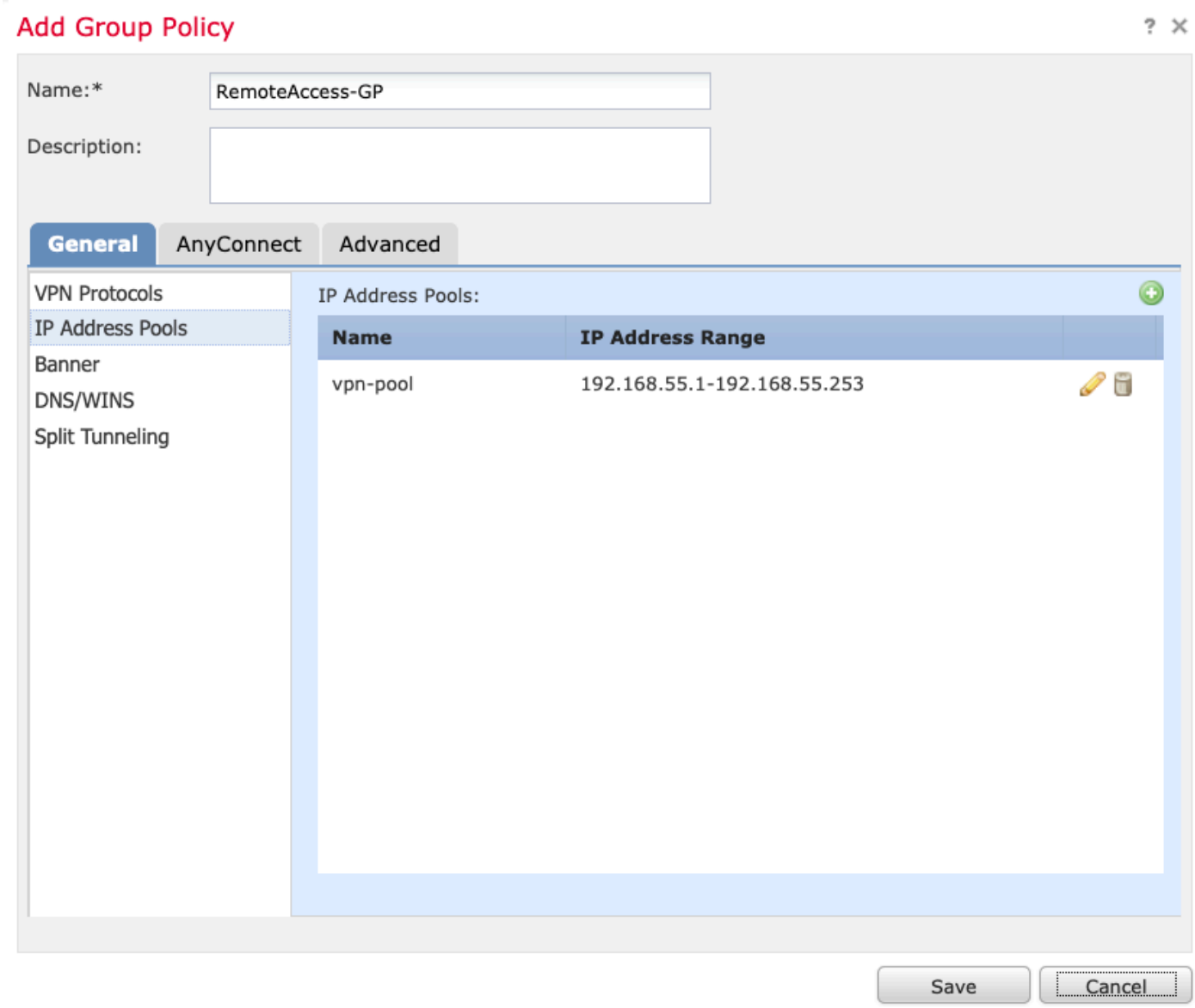
3. Attribuez le nom du profil de connexion (le nom du profil de connexion est le nom du groupe de tunnels), sélectionnez Authentication Server et Address Pools comme indiqué dans l'image.



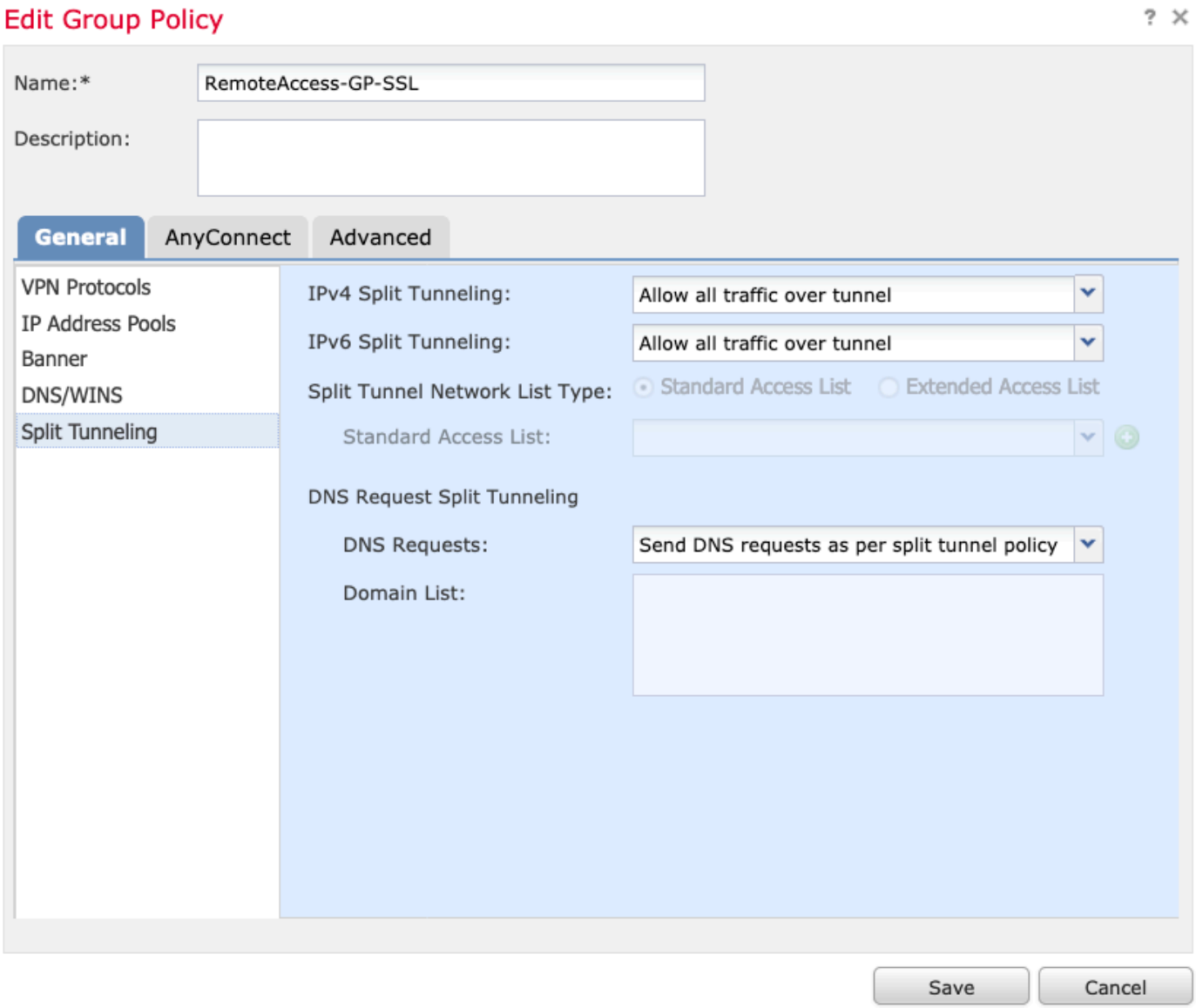
4. Sélectionnez le symbole + afin de créer une stratégie de groupe.



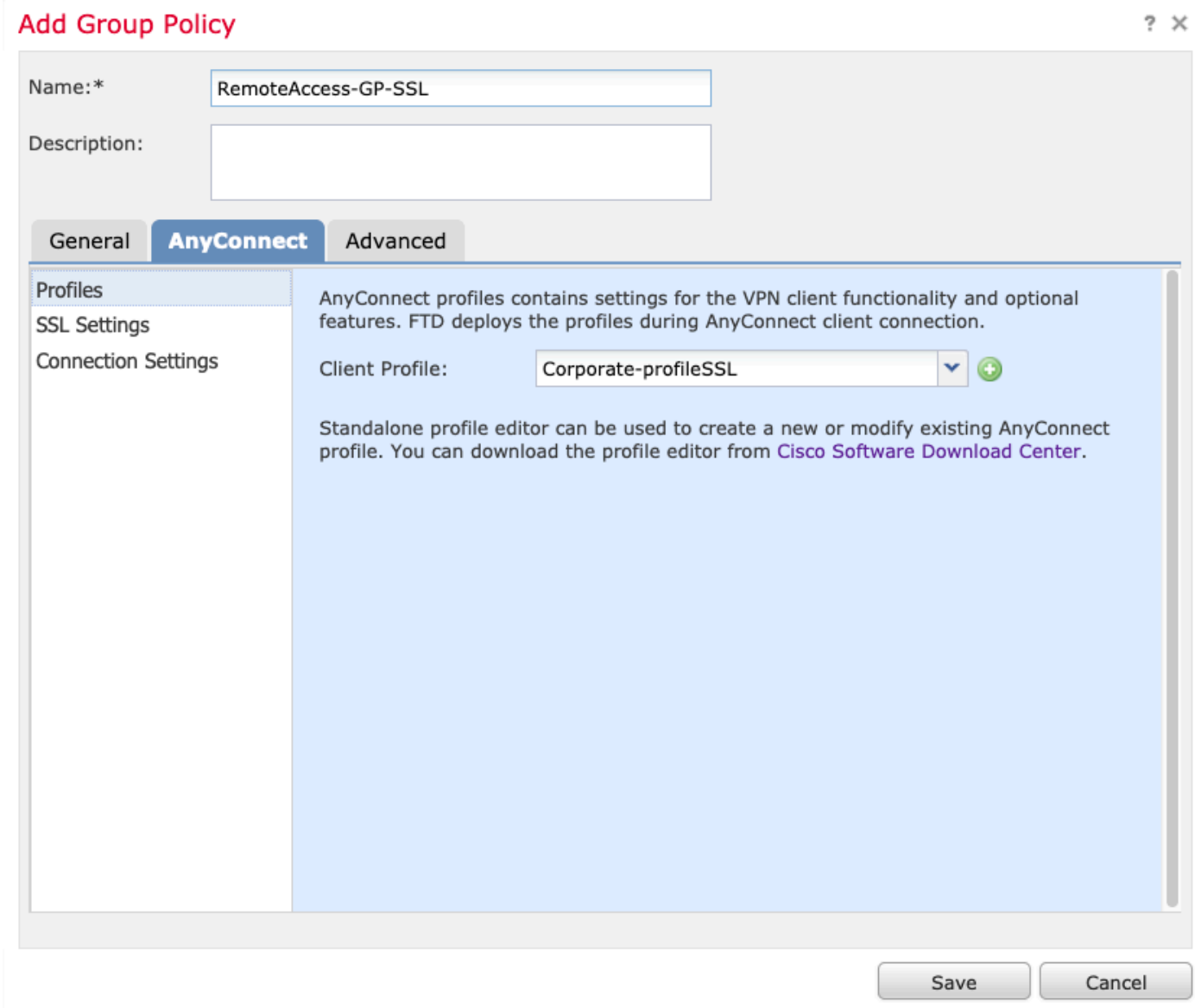
5. (Facultatif) Un pool d’adresses IP locales peut être configuré sur la base d’une stratégie de groupe. S'il n'est pas configuré, le pool est hérité du pool configuré dans le profil de connexion (tunnel-group).



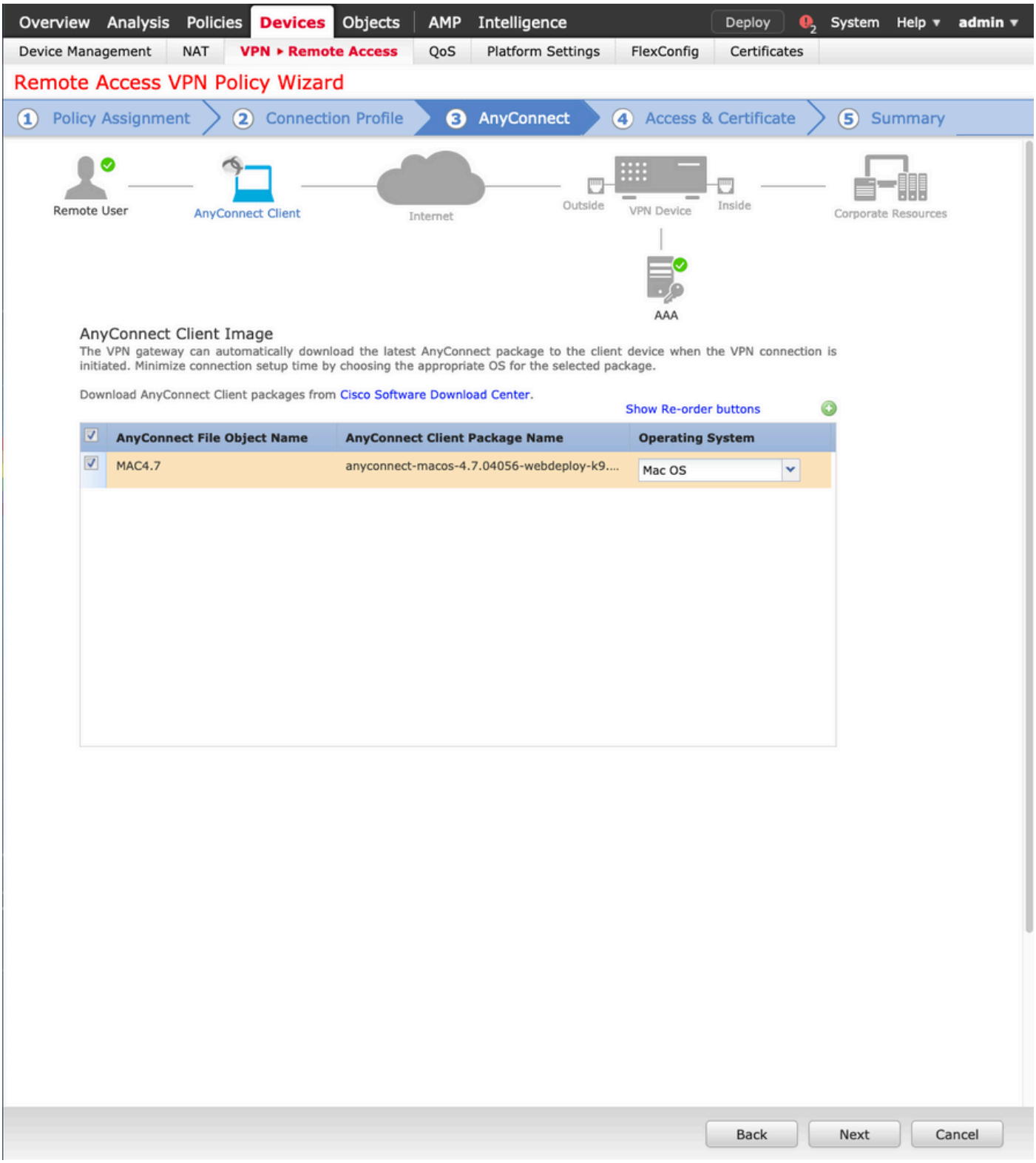
6. Pour ce scénario, tout le trafic est routé sur le tunnel, la politique de Fractionnement de tunnel IPv4 est définie sur Autoriser tout le trafic sur le tunnel comme indiqué dans l'image.



7. Sélectionnez le profil .xml pour Anyconnect et sélectionnez Enregistrer comme indiqué dans l'image.



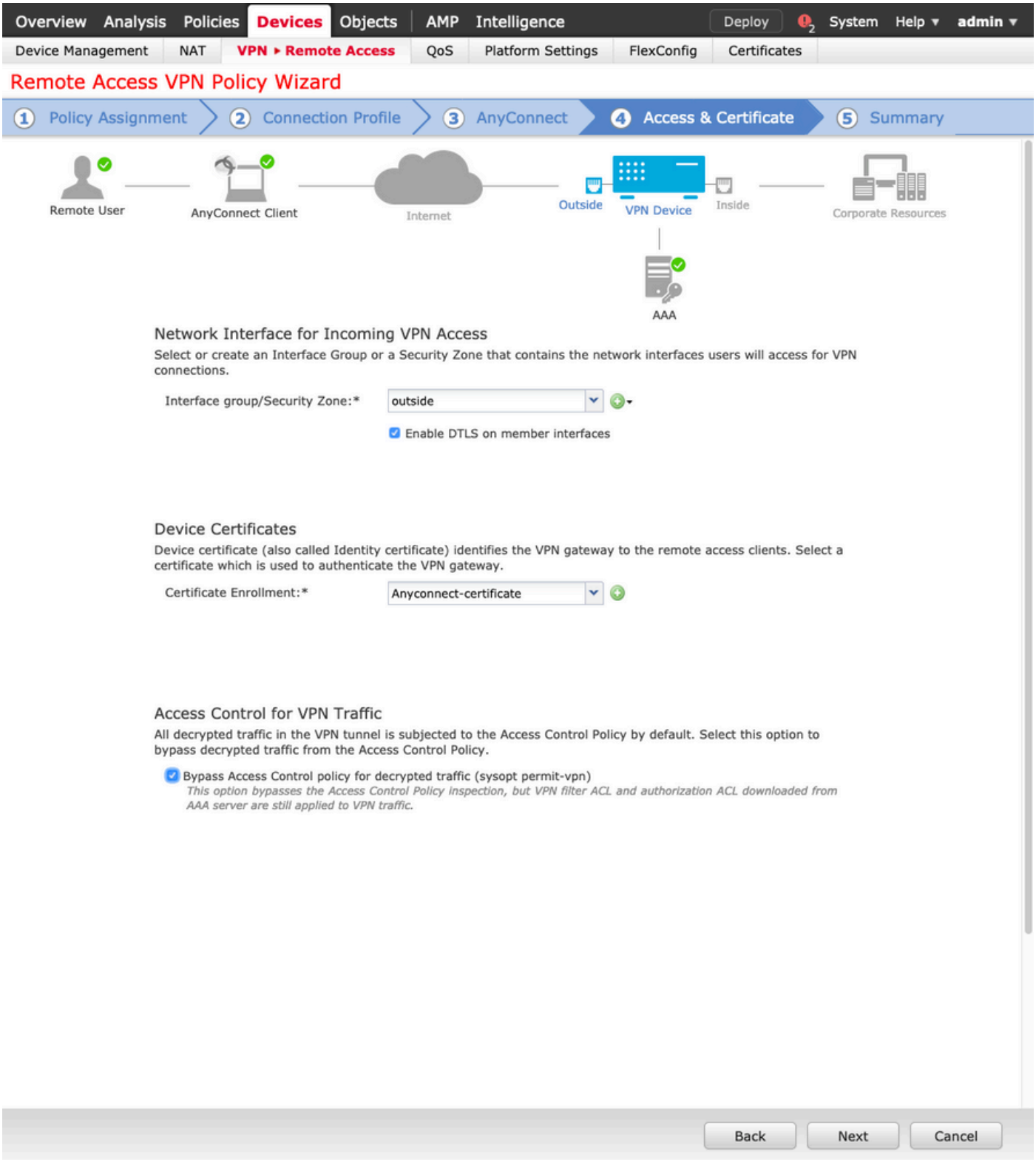
8. Sélectionnez les images AnyConnect souhaitées en fonction de la configuration système requise, puis sélectionnez Next a dans l'image.



9. Sélectionnez la zone de sécurité et les certificats de périphérique :

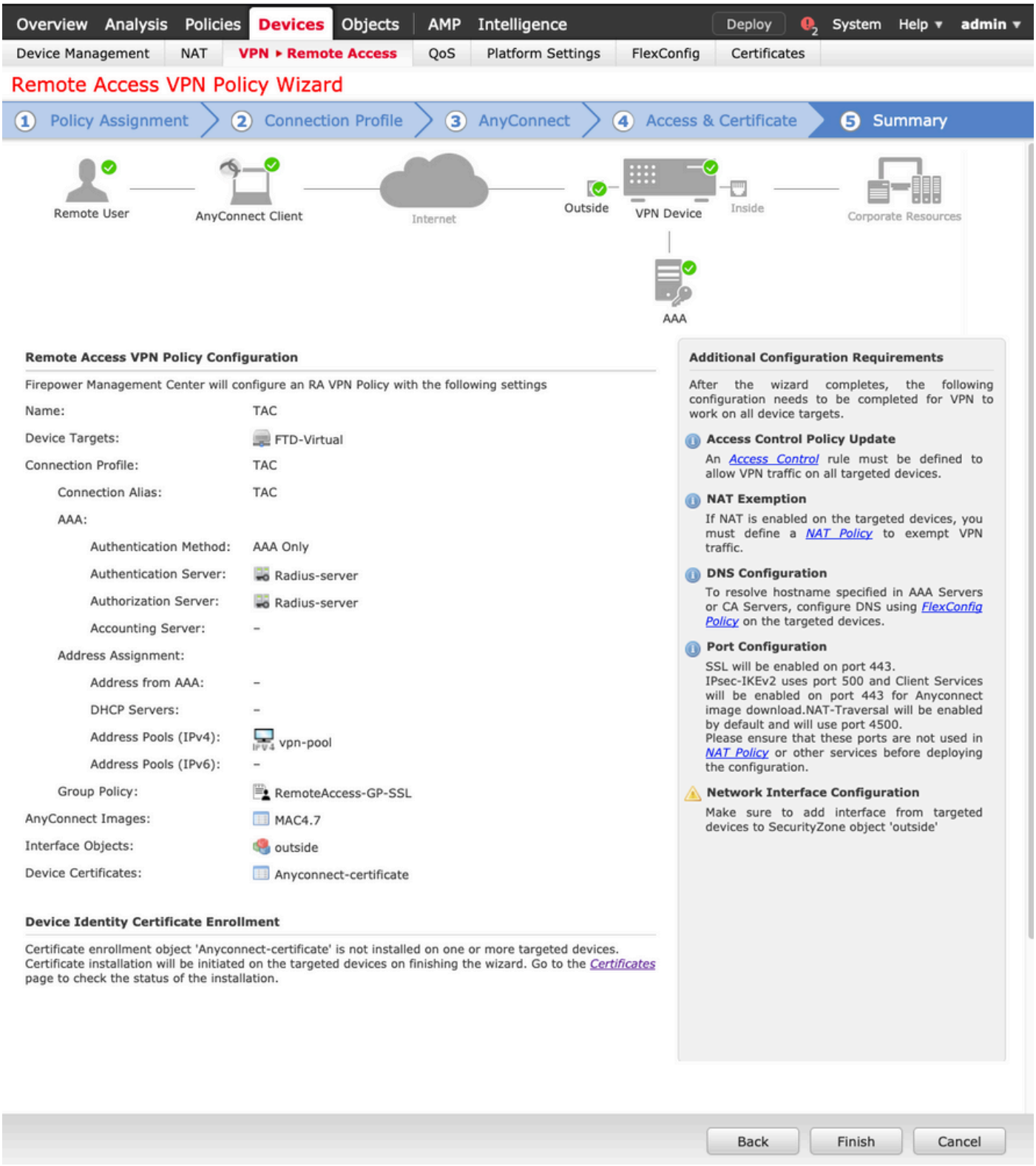
- Cette configuration définit l'interface sur laquelle le VPN se termine et le certificat qui est présenté sur une connexion SSL.

Remarque : dans ce scénario, le FTD est configuré pour ne pas inspecter le trafic VPN, contourner l'option Access Control Policies (ACP) est basculé.



10. Sélectionnez Terminer et Déployer les modifications :

- Toutes les configurations relatives aux VPN, aux certificats SSL et aux packages AnyConnect sont transmises via FMC Deploy, comme illustré dans l'image.



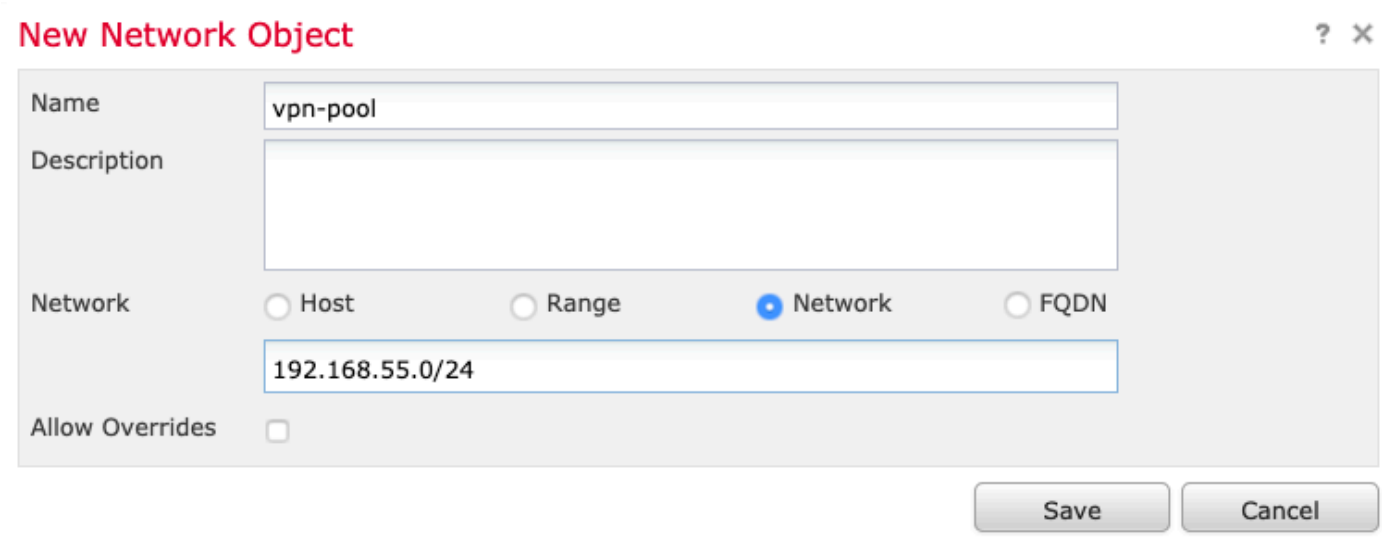
Exemption NAT et épingle à cheveux

Étape 1. Configuration des exemptions NAT

L'exemption NAT est une méthode de traduction préférée utilisée pour empêcher le trafic d'être routé vers Internet lorsqu'il est destiné à circuler sur un tunnel VPN (accès à distance ou site à site).

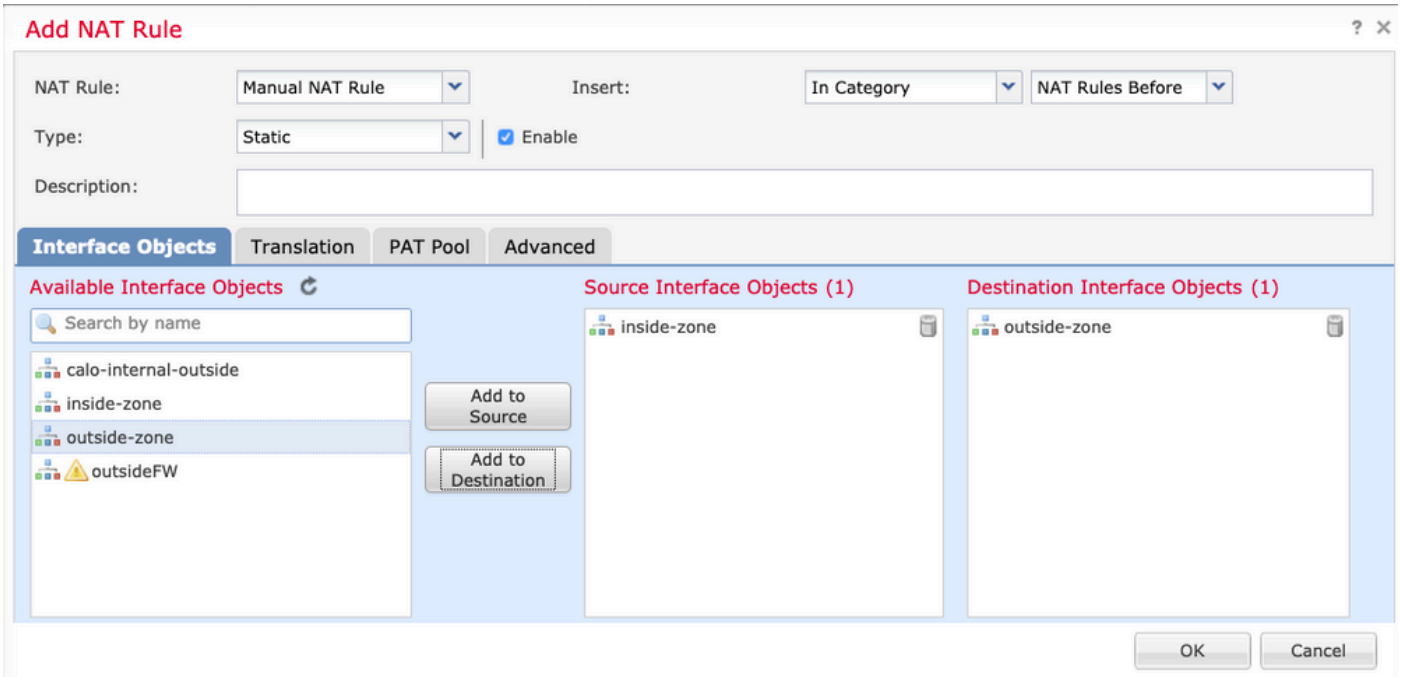
Cela est nécessaire lorsque le trafic provenant de votre réseau interne est destiné à circuler sur les tunnels sans aucune traduction.

1. Accédez à Objets > Réseau > Ajouter un réseau > Ajouter un objet comme indiqué dans l'image.

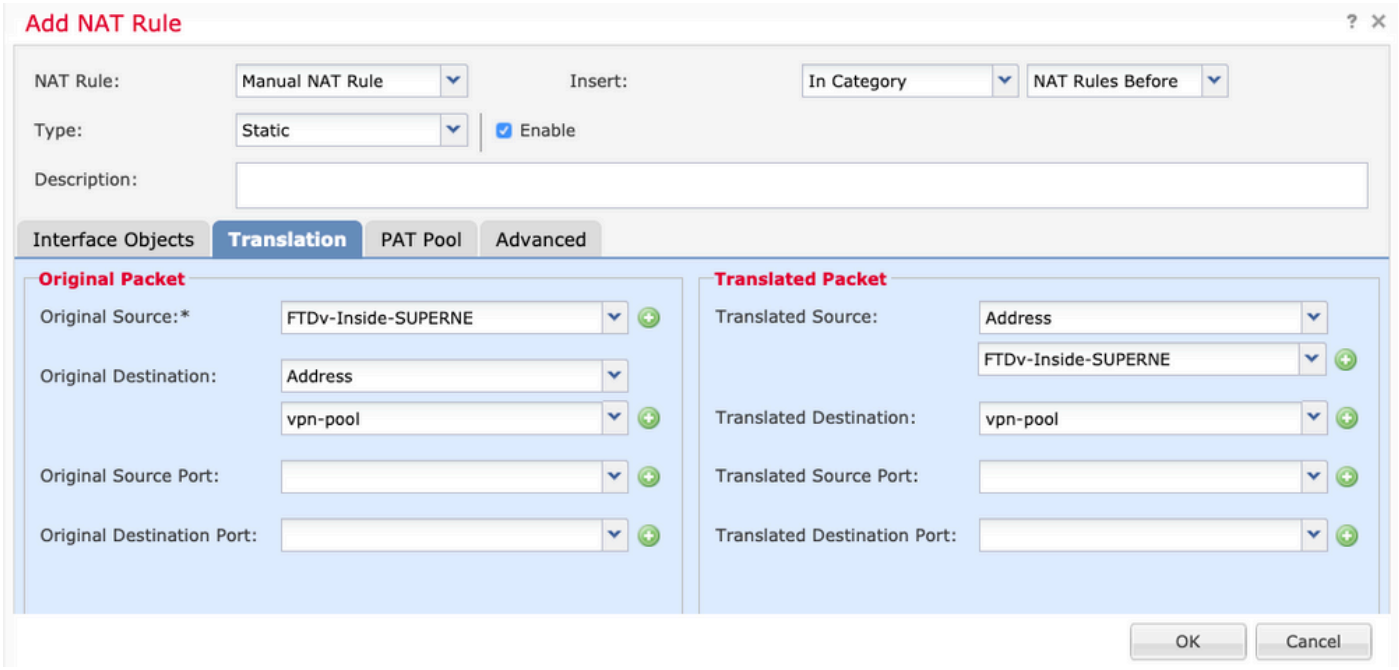


2. Accédez à Device > NAT, sélectionnez la stratégie NAT qui est utilisée par le périphérique en question et créez une nouvelle instruction.

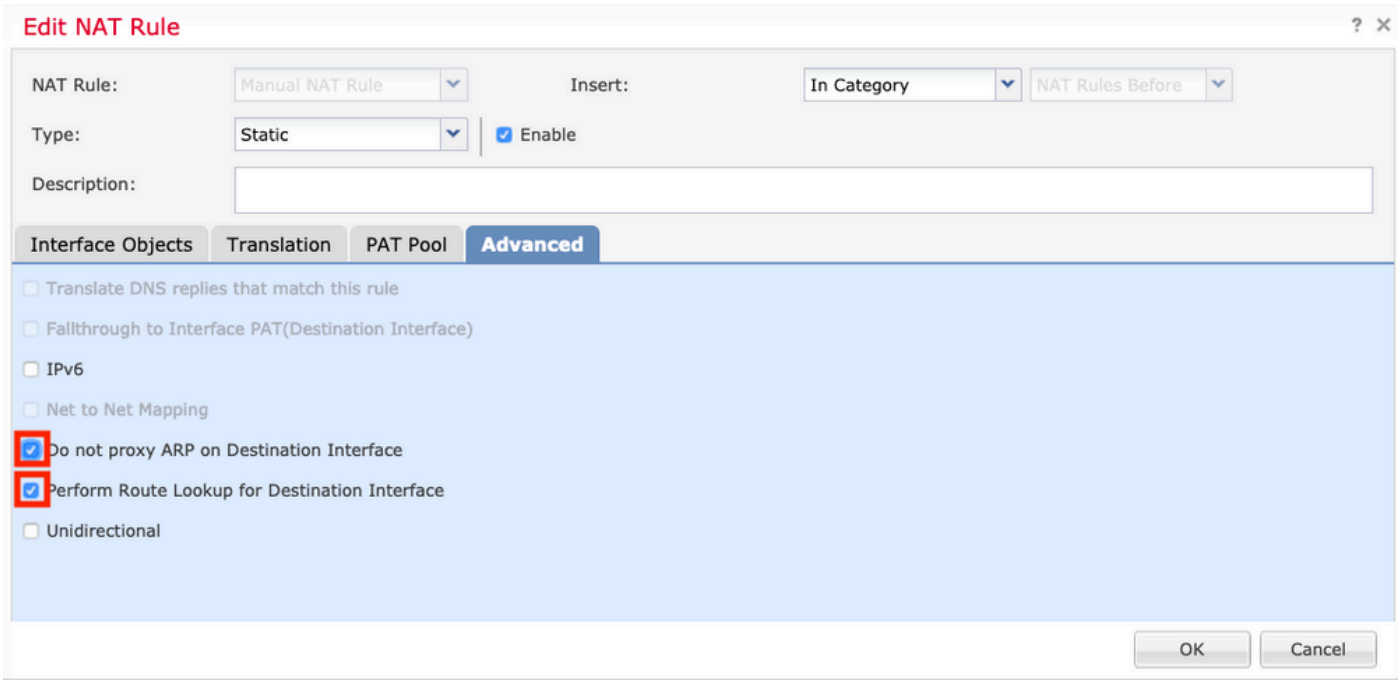
Remarque : le flux de trafic va de l'intérieur vers l'extérieur.



3. Sélectionnez les ressources internes derrière le FTD (source d'origine et source traduite) et la destination en tant que pool ip local pour les utilisateurs Anyconnect (destination d'origine et destination traduite) comme indiqué dans l'image.

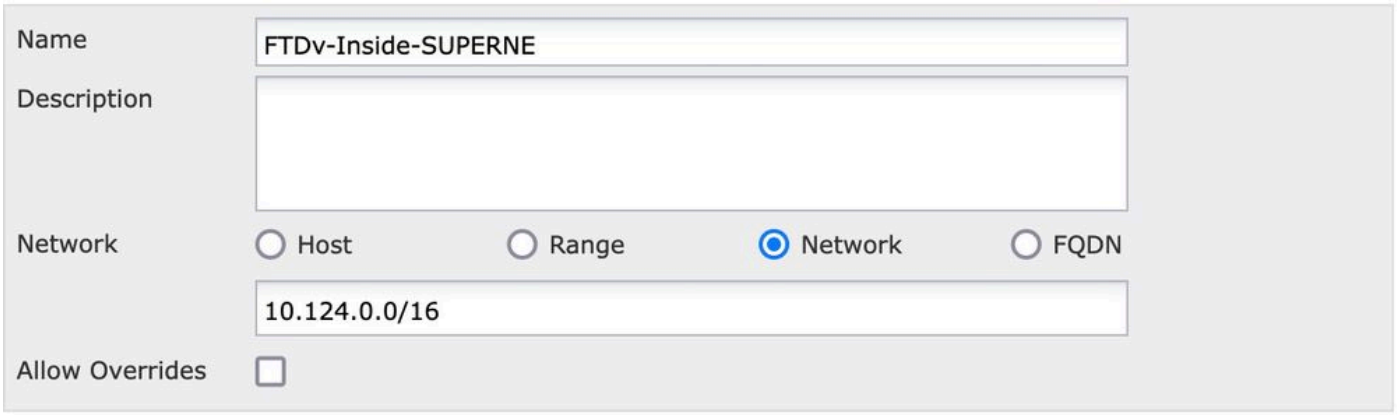


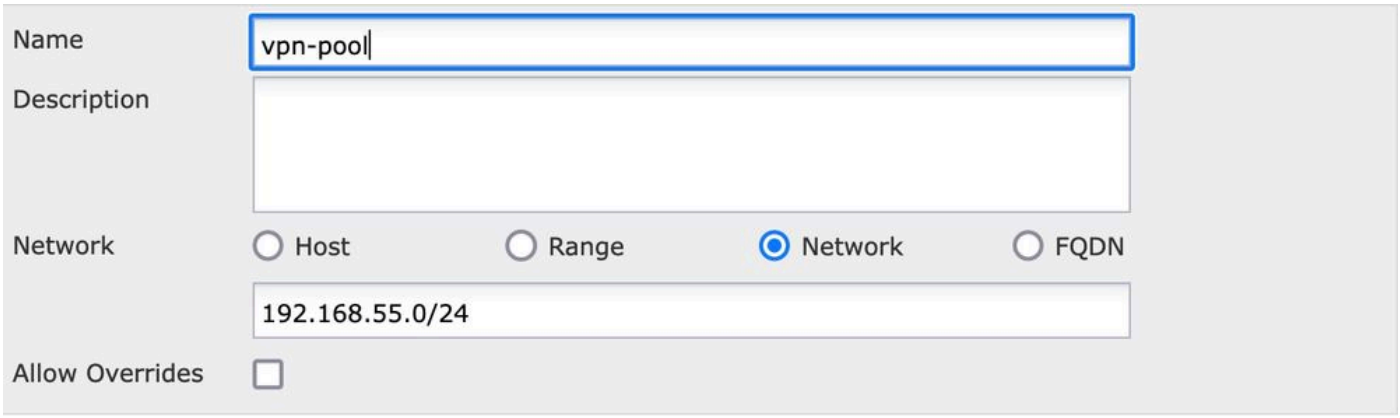
4. Assurez-vous de basculer les options (comme indiqué dans l'image), afin d'activer "no-proxy-arp" et "route-lookup" dans la règle NAT, sélectionnez OK comme indiqué dans l'image.



5. Il s’agit du résultat de la configuration d’exemption NAT.

Les objets utilisés dans la section précédente sont ceux décrits ci-dessous.





Étape 2. Configuration en épingle à cheveux

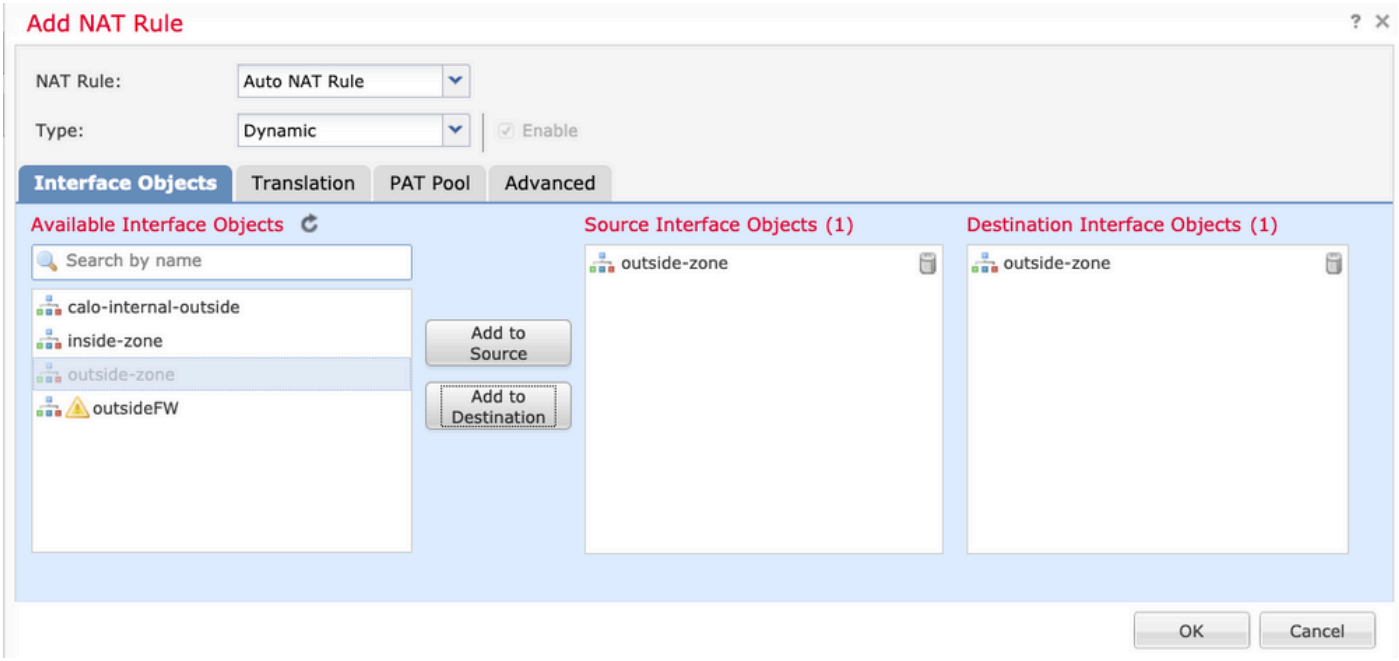
Également appelée U-turn, il s'agit d'une méthode de traduction qui permet au trafic de circuler sur la même interface sur laquelle le trafic est reçu.

Par exemple, quand Anyconnect est configuré avec une politique de tunnel Full split-tunnel, les ressources internes sont accédées selon la politique d'exemption NAT. Si le trafic client Anyconnect est destiné à atteindre un site externe sur Internet, la fonction NAT hairpin (ou U-turn) est chargée d'acheminer le trafic de l'extérieur vers l'extérieur.

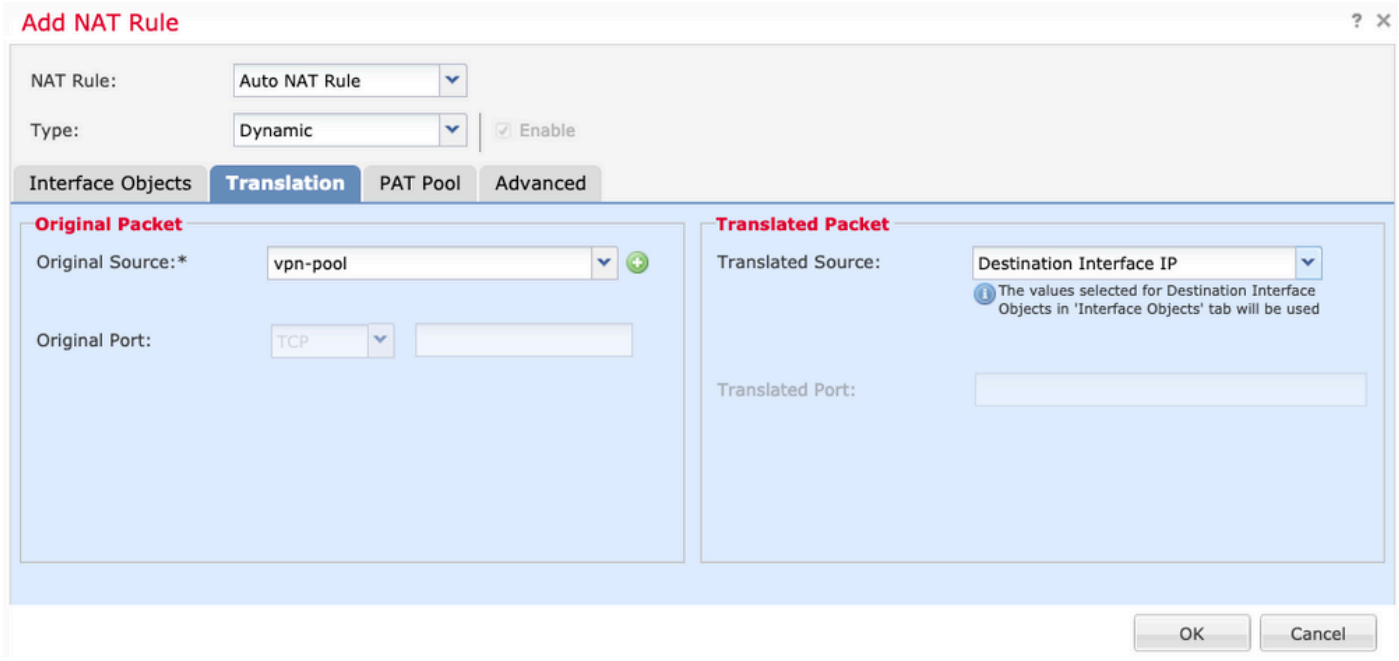
Un objet pool VPN doit être créé avant la configuration NAT.

1. Créez une nouvelle instruction NAT, sélectionnez Auto NAT Rule dans le champ NAT Rule et sélectionnez Dynamic comme NAT Type.

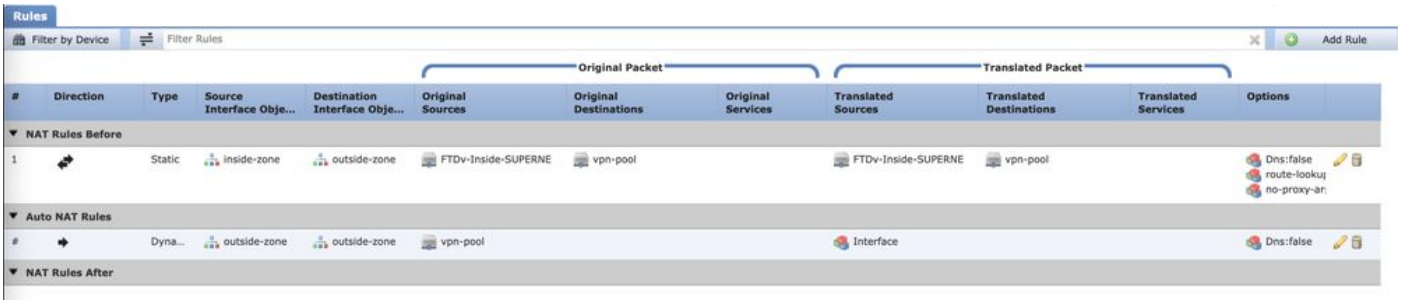
2. Sélectionnez la même interface pour les objets d'interface source et de destination (externe) :



3. Dans l'onglet Traduction, sélectionnez comme source d'origine l'objet vpn-pool et sélectionnez Destination Interface IP comme source traduite, sélectionnez OK comme indiqué dans l'image.



4. Ceci est le résumé de la configuration NAT telle qu'illustrée dans l'image.



5. Cliquez sur Enregistrer et déployer les modifications.

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Exécutez ces commandes dans la ligne de commande FTD.

- certificats sh crypto ca
- show running-config ip local pool
- show running-config webvpn
- show running-config tunnel-group
- show running-config group-policy
- show running-config ssl
- show running-config nat

Dépannage

Aucune information de dépannage spécifique n’est actuellement disponible pour cette configuration.</1>

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.

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.