Configuration du VPN d'Accès à distance d'AnyConnect sur FTD

Contenu

Introduction

Ce document fournit un exemple de configuration pour la version 6.2.2 et ultérieures de la défense contre des menaces de FirePOWER (FTD), cela permet l'Accès à distance VPN pour utiliser la version 2 (IKEv2) de Transport Layer Security (TLS) et d'échange de clés Internet (IKE). En tant que client, le Cisco AnyConnect sera utilisé, qui est pris en charge sur des plates-formes multiples.

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- VPN, TLS et connaissance IKEv2 de base
- Authentification, autorisation et comptabilité (AAA) et connaissance de base de RAYON
- Éprouvez avec le centre de Gestion de FirePOWER

Composants utilisés

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

- Cisco FTD 6.2.2
- AnyConnect 4.5

Configuration

1. Preresiquites

Afin de passer par l'assistant d'Accès à distance au centre de Gestion de FirePOWER, d'abord vous devrez suivre ces étapes :

- créez un certificat utilisé pour l'authentification de serveur,
- configurez le RAYON ou le serveur LDAP pour l'authentification de l'utilisateur,
- créez le groupe d'adresses pour des utilisateurs VPN,
- images d'AnyConnect de téléchargement pour différentes Plateformes.

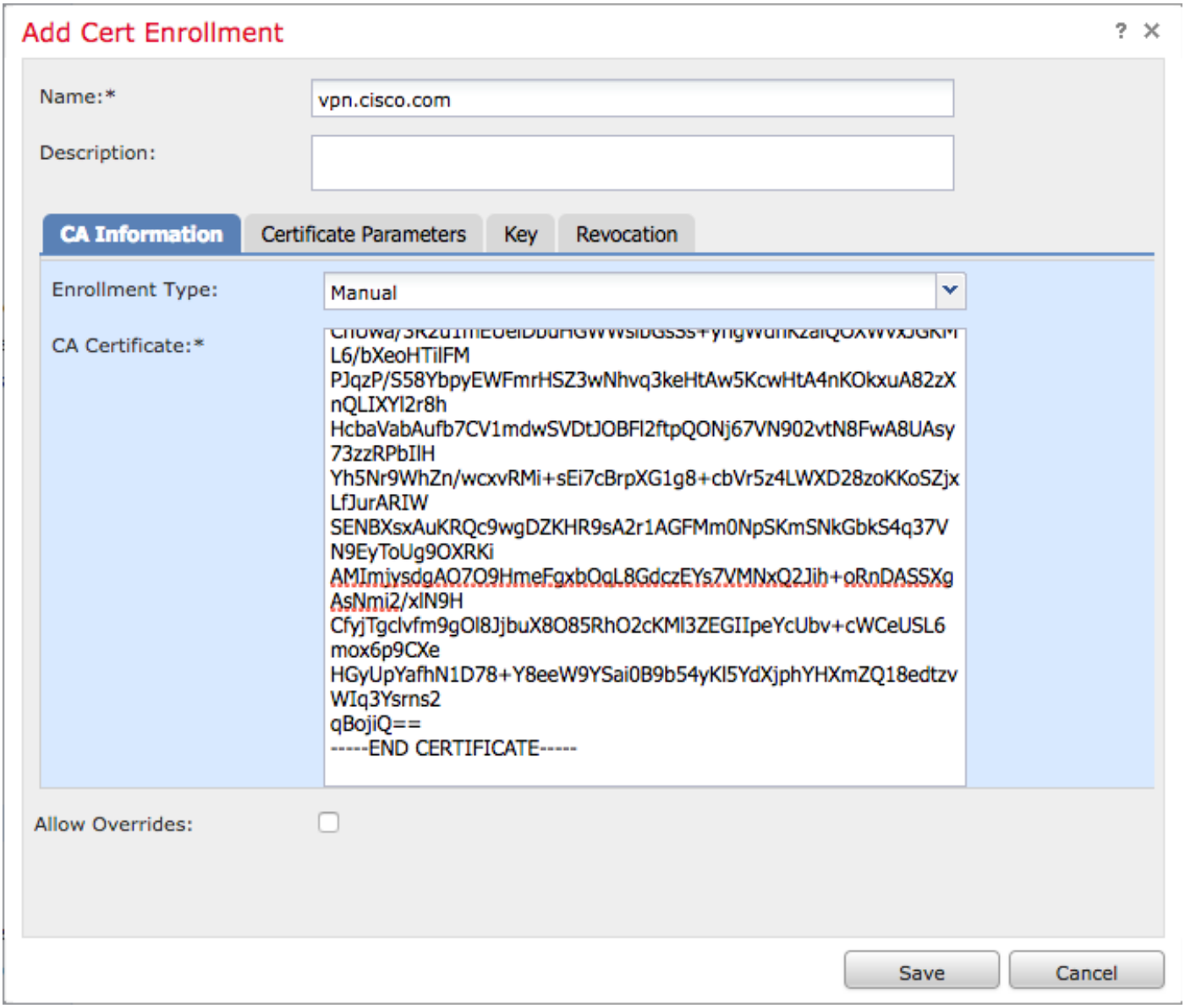
a) importer le certificat ssl

Les Certificats sont essentiels quand vous configurez AnyConnect. Seulement des Certificats basés par RSA sont pris en charge dans le SSL et l'IPSec. Les Certificats elliptiques d'algorithme de signature numérique de curve (ECDSA) sont pris en charge dans IPSec, mais lui ne sont pas possibles pour déployer le nouveau module d'AnyConnect ou le profil XML quand le certificat basé par ECDSA est utilisé. Il signifie que vous pouvez l'utiliser pour IPSec, mais vous devrez déployer à l'avance le module d'AnyConnect et le profil XML à chaque utilisateur et n'importe quel changement de profil XML devront être

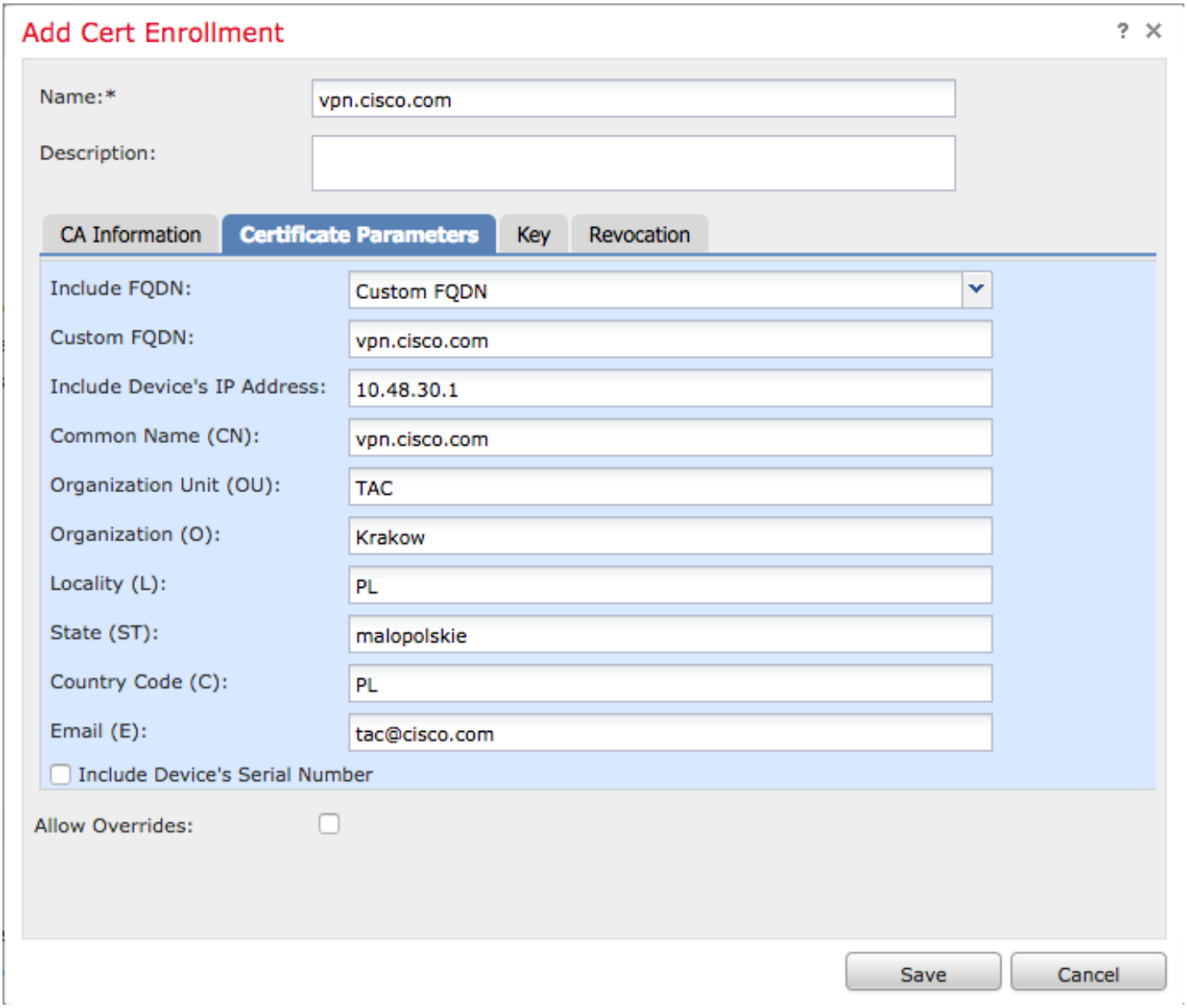
manuellement réfléchis sur chaque client (bogue : CSCtx42595). Supplémentaire le certificat devrait avoir l'extension alternative soumise de nom avec le nom DNS et/ou l'adresse IP pour éviter des erreurs en navigateurs Web.

Il y a plusieurs méthodes pour obtenir un certificat sur l'appliance FTD, mais le coffre-fort et celui facile est de créer une demande de signature de certificat (CSR), signe elle et puis le certificat d'importation délivrés pour la clé publique, qui était dans le CSR. Voici comment faire cela :

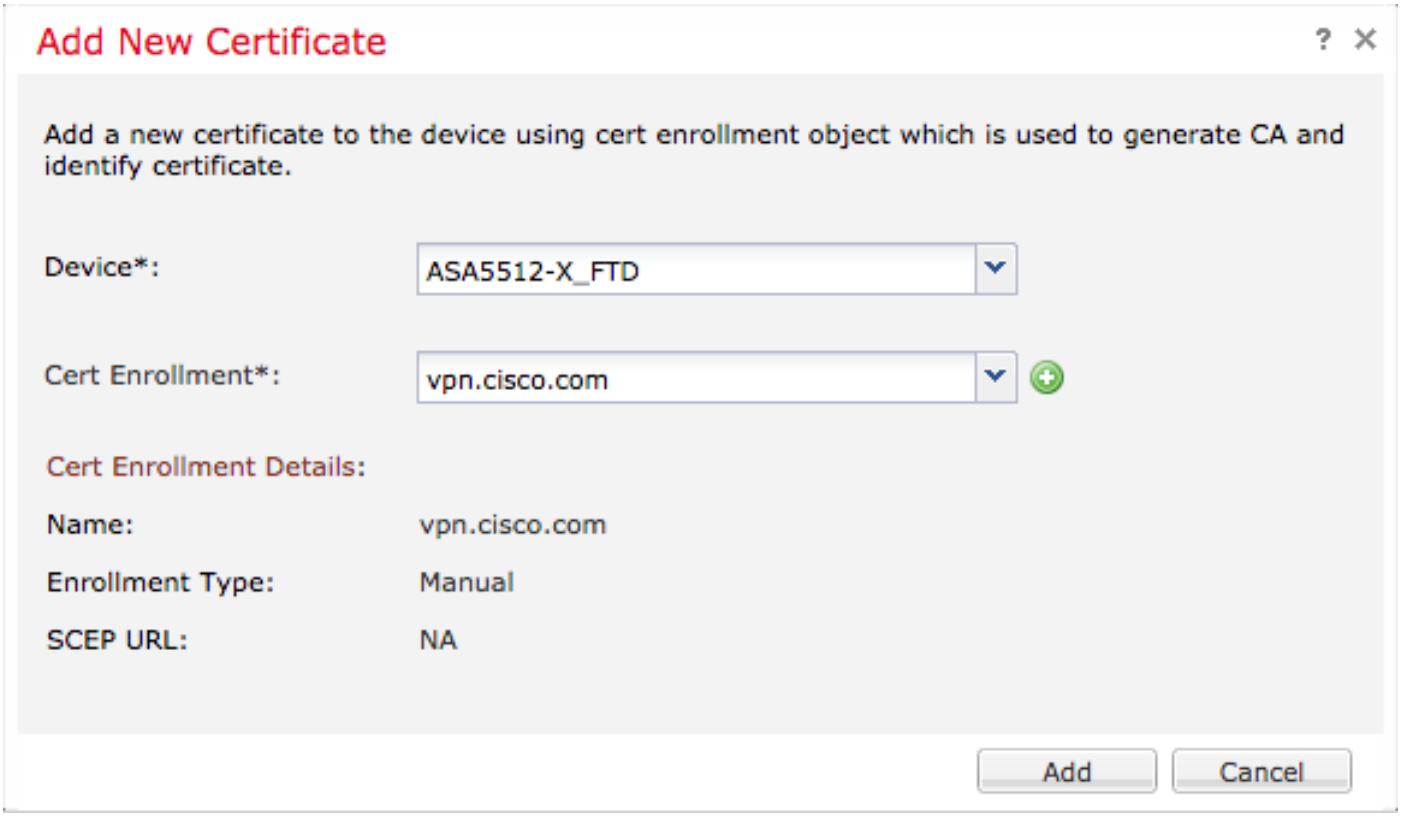
- Allez aux **objets >** à la **Gestion d'objet >** à l'**inscription de PKI >** de **CERT**, cliquez sur en fonction l'**inscription de CERT Add** :



- **Type d'inscription et certificat choisis d'Autorité de certification (CA) de pâte,**
- Allez alors en second lieu tabuler et sélectionner le **FQDN de coutume** et remplir tous les champs nécessaires, par exemple :



- Sur le troisième onglet, le type principal choisi, choisissent le nom et la taille. Pour la RSA, 2048 octets est minimum.
- Cliquez sur la sauvegarde et allez aux **périphériques** > aux **Certificats** > **ajoutent** > **nouveau certificat**. Sélectionnez alors le **périphérique,** et sous l'**inscription de CERT** sélectionnez le point de confiance que vous avez juste créé, cliquent sur Add :



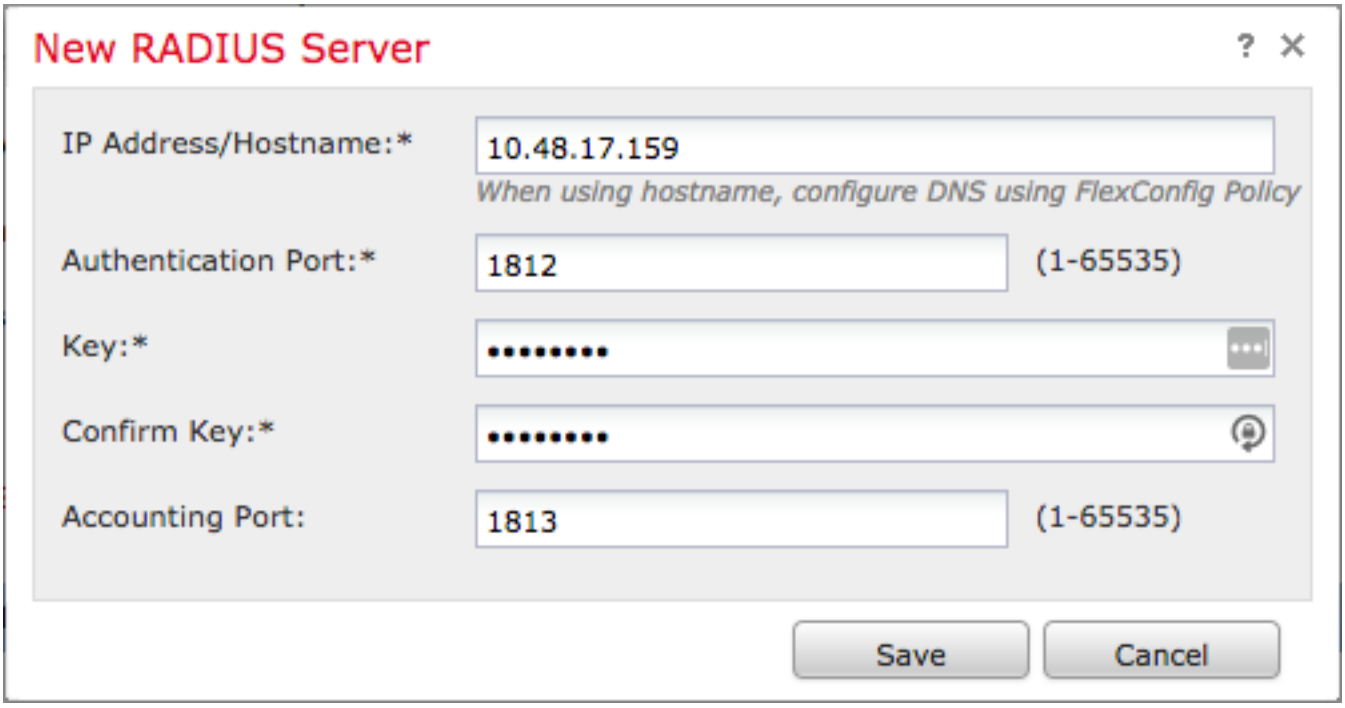
- Plus tard, à côté du nom de point de confiance, cliquez sur en fonction l'icône, puis **oui et ensuite ce CSR de copie au CA et signez-la. Le certificat devrait avoir des attributs en tant que serveur normal HTTPS.**
- Après réception du certificat du CA dans le format base64, sélectionnez-le à partir du disque et cliquez sur l'**importation**. Quand ceci réussit, vous devriez voir :

Name	Enrollment Type	CA Certificate	Identity Certificate
ASA5512-X_FTD			
vpn.cisco.com	Manual	Available	Available

b) configurez le serveur de RAYON

Sur le platftorm FTD, la base de données locale des utilisateurs ne peut pas être utilisée, ainsi vous avez besoin du RAYON ou du serveur LDAP pour l'authentification de l'utilisateur. Pour configurer le RAYON :

- Allez aux **objets** > à la **Gestion d'objet** > au **groupe de serveurs de RAYON** > **ajoutent le groupe de serveurs de RAYON**.
- Remplissez nom et ajoutez l'adresse IP avec le secret partagé, **sauvegarde de** clic :



- Ensuite que vous devriez voir le serveur sur la liste :

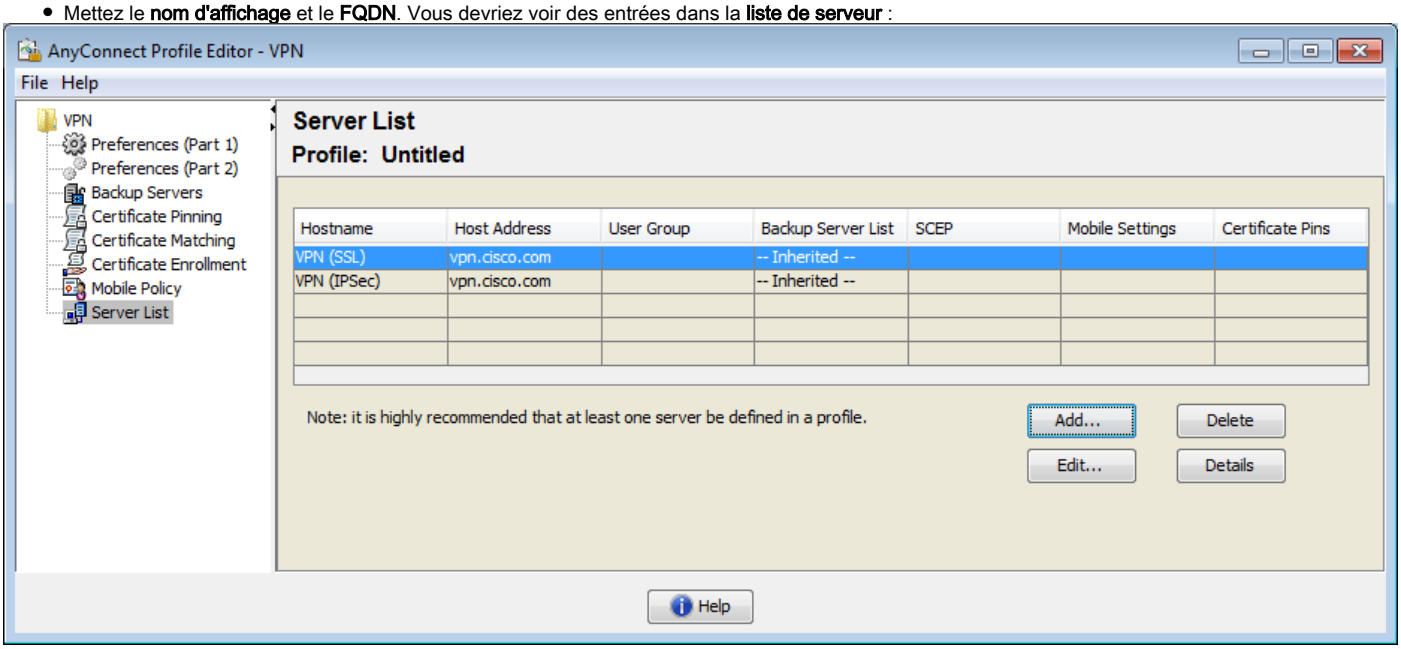
c) création du groupe d'adresses pour des utilisateurs VPN

- Allez aux **objets** > à la **Gestion** > aux **pools d'adresses d'objet** > **ajoutent des groupes d'ipv4** :
- Mettez le nom et la plage, masque n'est pas nécessaire :

d) création du profil XML

- Téléchargez l'éditeur de profil du site de Cisco et ouvrez-le.
- Allez à la **liste de serveur** > **ajoutent...**

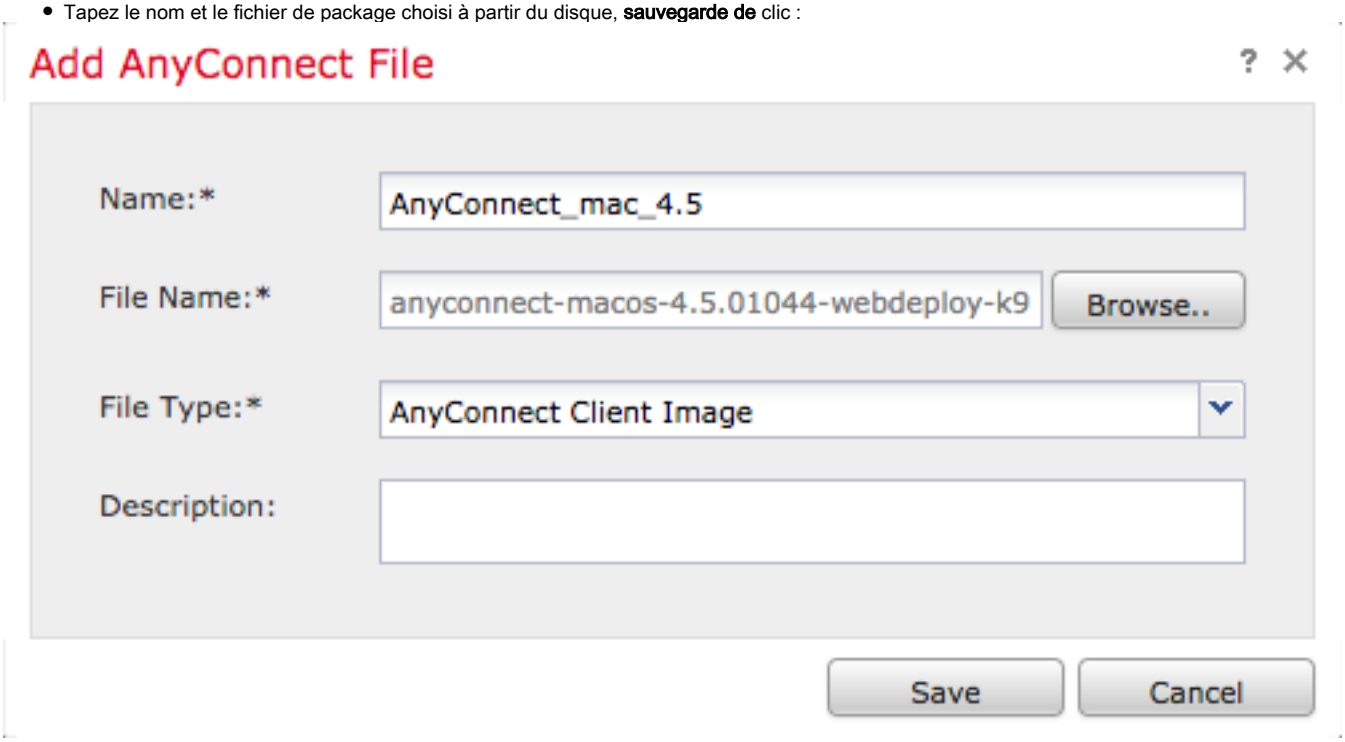
- Mettez le **nom d'affichage** et le **FQDN**. Vous devriez voir des entrées dans la **liste de serveur** :



- Cliquez sur OK et **fichier > sauvegarde en tant que...**

e) télécharger des images d'AnyConnect

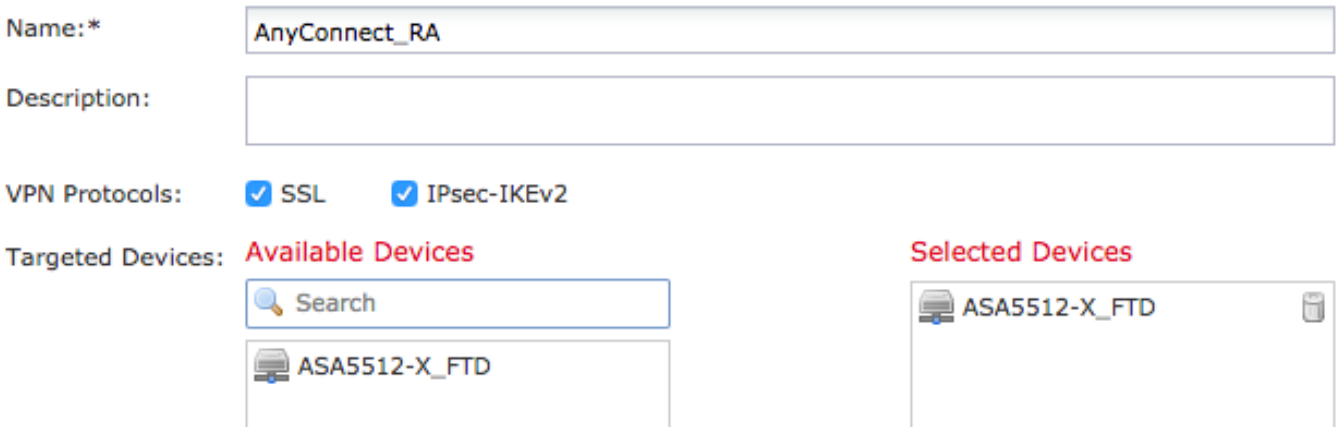
- Images de module de téléchargement de site de Cisco.
- Allez aux **objets** > à la **Gestion d'objet** > au **fichier VPN** > d'**AnyConnect** > **ajoutent le fichier d'AnyConnect**.
- Tapez le nom et le fichier de package choisi à partir du disque, **sauvegarde de** clic :



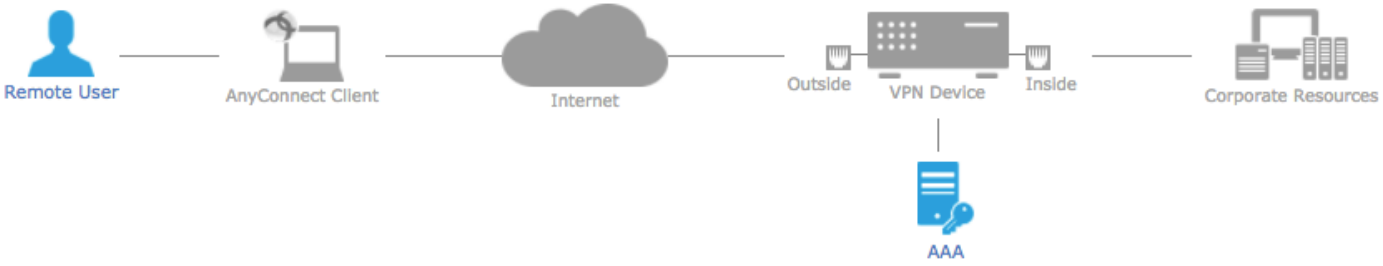
- Ajoutez plus de modules selon vos conditions requises.

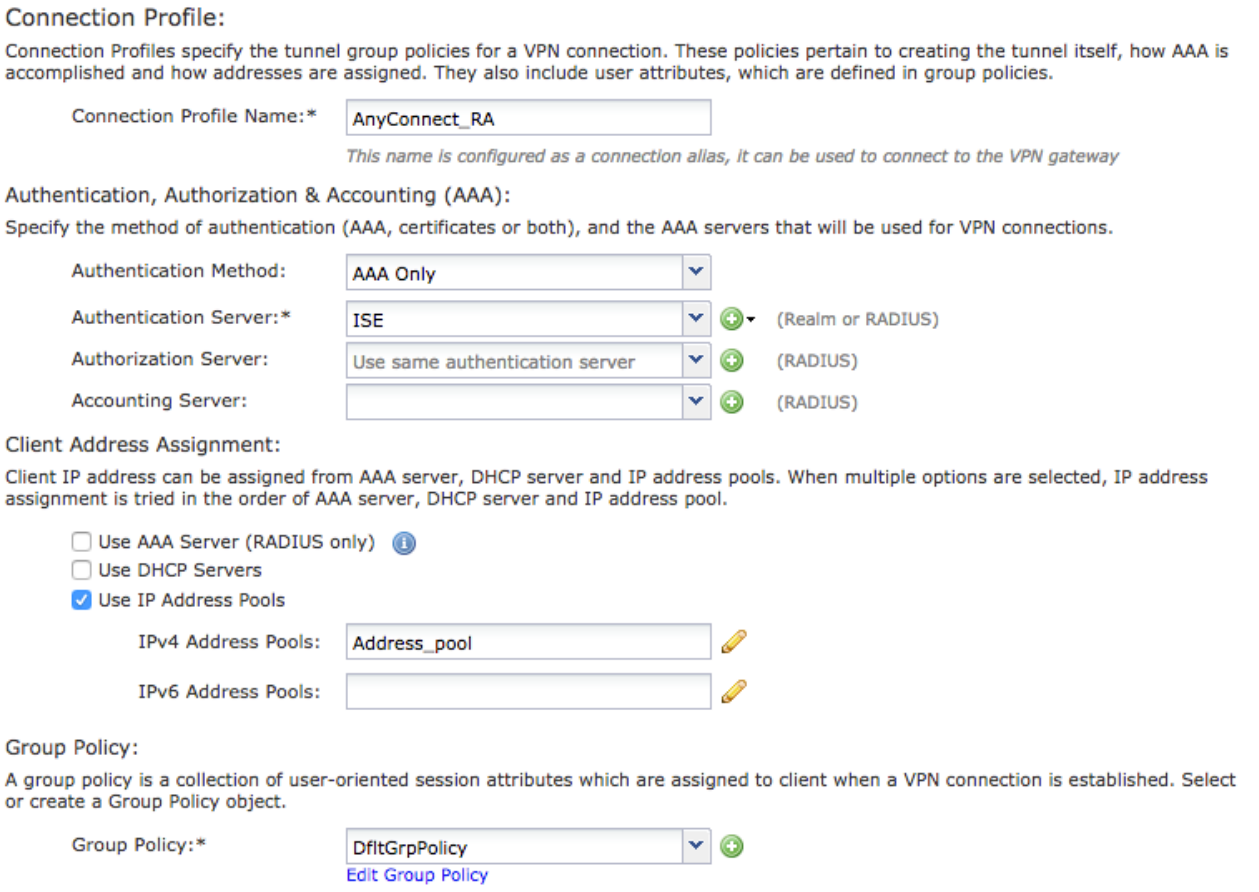
2. Assistant d'Accès à distance

- Allez aux **périphériques** > au **VPN** > à l'**Accès à distance** > **ajoutent une nouvelle configuration**.
- Nommez le profil selon vos besoins, périphérique choisi FTD :

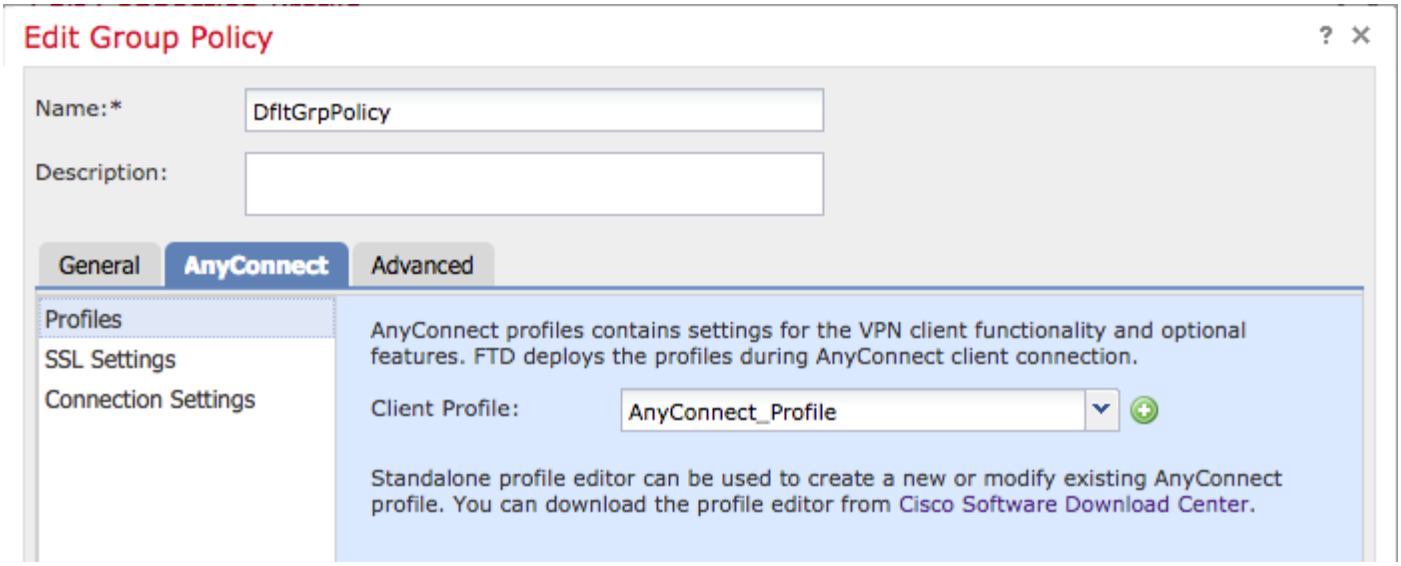


- Dans le **profil de connexion d'**étape, le **nom de profil de connexion de** type, le **serveur** choisi d'**authentification** et les **pools d'adresses** que vous avez créés plus tôt :

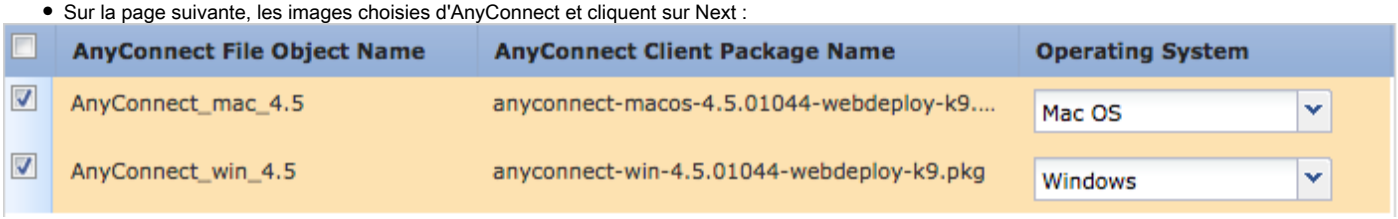




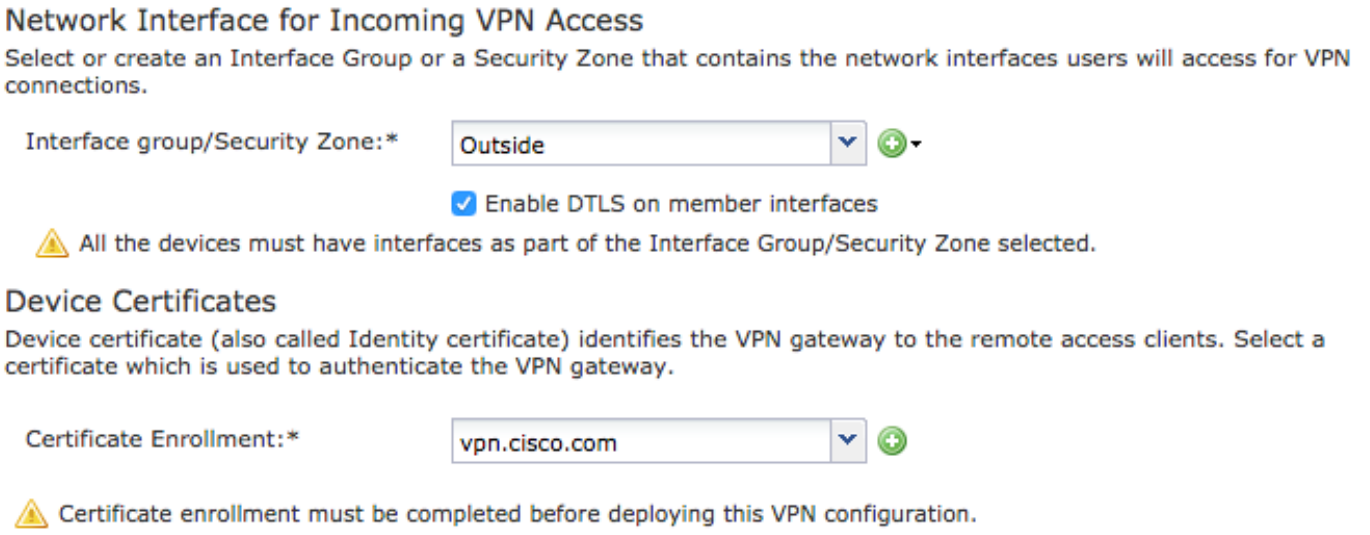
- Cliquez sur en fonction la **stratégie de groupe Edit** et sur l'onglet **AnyConnect**, **profil** choisi de **client**, puis cliquez sur la **sauvegarde** :



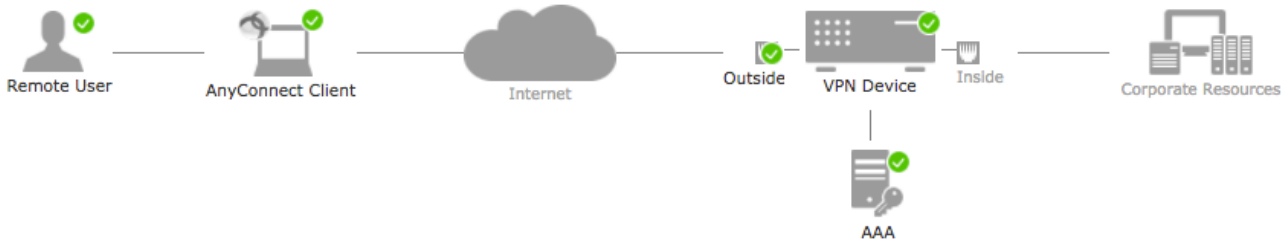
- Sur la page suivante, les images choisies d'AnyConnect et cliquent sur Next :



- Sur l'écran suivant, l'**interface réseau** choisie et le **DeviceCertificates** :



- Quand tout est configuré correctement, vous pouvez cliquer sur Finish et puis **se déployer** :



Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name:	AnyConnect_RA
Device Targets:	ASA5512-X_FTD
Connection Profile:	AnyConnect_RA
Connection Alias:	AnyConnect_RA
AAA:	
Authentication Method:	AAA Only
Authentication Server:	ISE
Authorization Server:	ISE
Accounting Server:	–
Address Assignment:	
Address from AAA:	–
DHCP Servers:	–
Address Pools (IPv4):	Address_pool
Address Pools (IPv6):	–
Group Policy:	DfltGrpPolicy
AnyConnect Images:	AnyConnect_mac_4.5 AnyConnect_win_4.5
Interface Objects:	Outside
Device Certificates:	vpn.cisco.com

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

Access Control Policy Update
An *Access Control* rule must be defined to allow VPN traffic on all targeted devices.

NAT Exemption
If NAT is enabled on the targeted devices, you must define a *NAT rule* to exempt VPN traffic.

DNS Configuration
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using *FlexConfig Policy* on the targeted devices.

Network Interface Configuration
Make sure to add interface from targeted devices to SecurityZone object 'Outside'

Device Identity Certificate Enrollment
Make sure to install identity certificate on targeted devices using PKI Cert object 'vpn.cisco.com'

- Ceci copiera la configuration entière avec des Certificats et des modules d'AnyConnect sur l'appliance FTD.

Connexion

Pour se connecter à FTD que vous devez ouvrir un navigateur, à nom DNS de type ou à adresse IP indiquant l'interface extérieure, dans cet exemple *https://vpn.cisco.com*. Vous devrez alors ouvrir une session utilisant des qualifications enregistrées dans le serveur de RAYON et suivre des instructions à l'écran. Une fois qu'AnyConnect installe, vous devez alors mettre la même adresse dans la fenêtre d'AnyConnect et le clic **se connectent**.

Limites

Actuellement non vérifié sur FTD, mais disponible sur l'ASA :

- Double authentification d'AAA
- Stratégie d'accès dynamique
- Balayage d'hôte
- Posture ISE
- CoA de RAYON
- Équilibreur de charge VPN
- Authentification locale (amélioration : CSCvf92680)
- Carte d'attribut de LDAP
- Personnalisation d'AnyConnect
- Scripts d'AnyConnect

- Localisation d'AnyConnect
- Par-app VPN
- Proxy SCEP
- Intégration WSA
- SAML SSO
- Crypto-carte dynamique IKEv2 simultanée pour le RA et le L2L VPN
- Des modules d'AnyConnect (NAM, Hostscan, Enabler etc. d'AMPÈRE) – DART est installés par défaut
- TACACS, Kerberos (authentification KCD et SDI RSA)
- Navigateur proxy

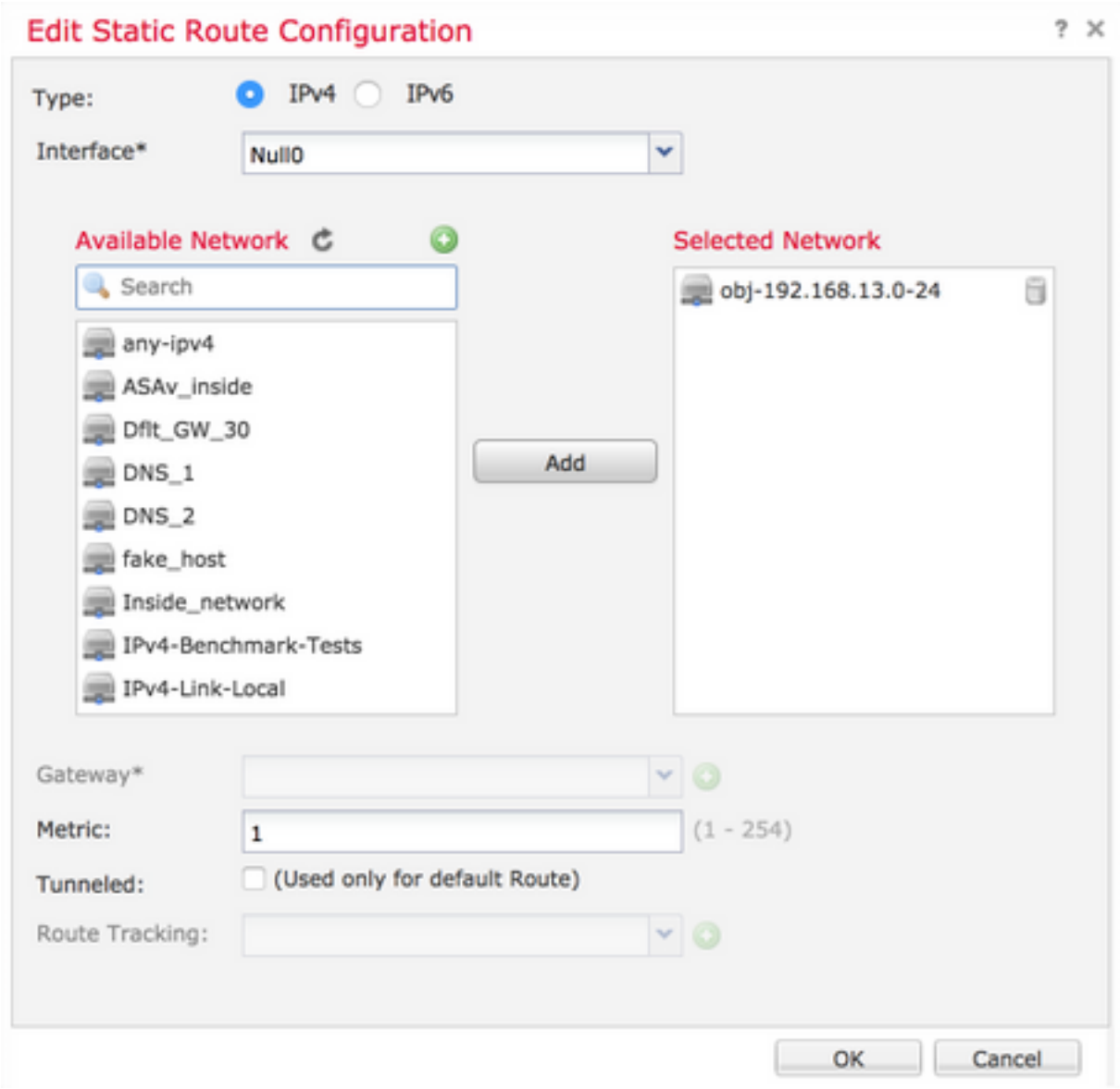
Considérations liées à la sécurité

Vous devez se souvenir cela par défaut, option d'autorisation-VPN de connexion de sysopt est désactivé. Ce moyens, cela que vous devez permettre le trafic provenant le groupe d'adresses sur l'interface extérieure par l'intermédiaire de la stratégie de contrôle d'accès. Bien que la règle de pré-filtre ou de contrôle d'accès soit destiner ajouté pour permettre le trafic VPN seulement, si le trafic de libellé s'avère justement apparier les critères de règle, on lui permet incorrectement.

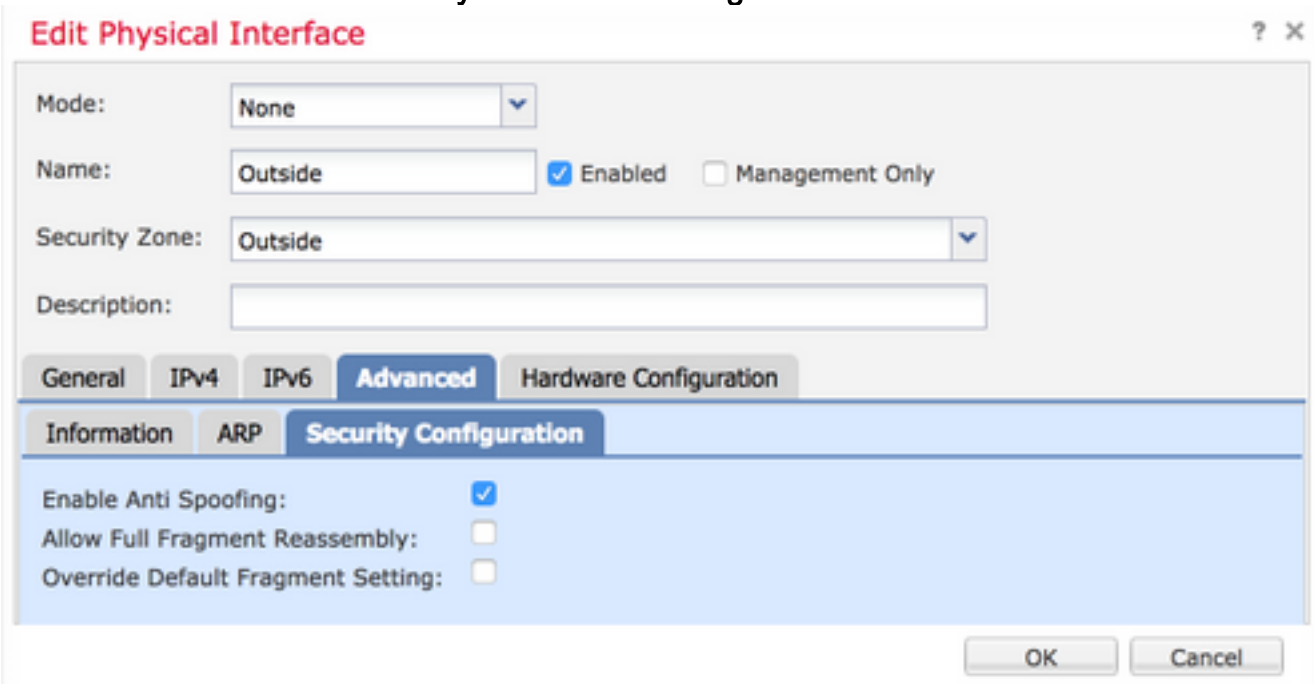
Il y a deux approches à ce problème. D'abord, l'option recommandée par TAC, est d'activer l'Anti-mystification (sur l'ASA connue sous le nom d'Unicast Reverse Path Forwarding - uRPF) pour l'interface extérieure, et la deuxième est de permettre à la connexion autorisation-VPN de sysopt de sauter reniflent l'inspection complètement. Le premier choix laisse examiner normalement le trafic allant à et des utilisateurs VPN.

a) Activation de l'uRPF

- créez une artère nulle pour le réseau utilisé pour des utilisateurs d'Accès à distance, défini dans la section C. Allez juste aux **périphériques >** à la **Gestion de périphériques > éditent > routage > artère statique > ajoutent l'artère** :



- deuxièmement, vous devez activer l'uRPF sur l'interface qui termine des connexions VPN. Vous pouvez le trouver en **périphériques > Gestion de périphériques > éditez > Interfaces > Edit > avez avancé > anti mystification de configuration de sécurité >** d'**enable** :

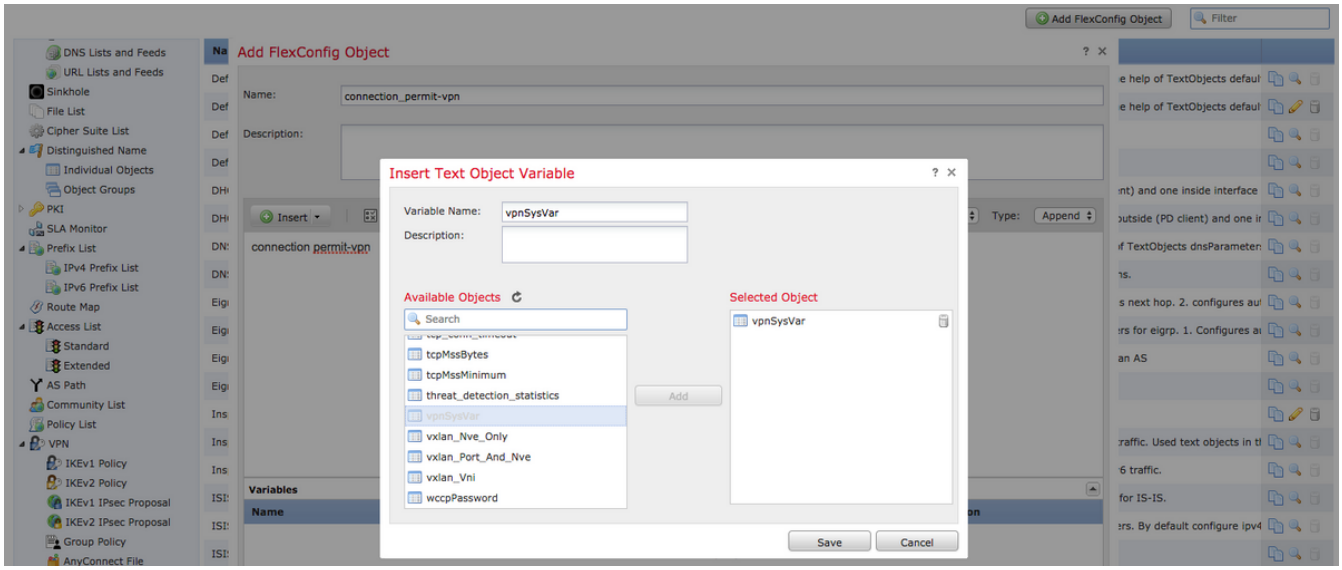


Quand l'utilisateur est connecté, l'artère de 32 bits est installée pour cet utilisateur dans la table de routage. Le trafic des textes clairs originaire d'autre, les adresses IP inutilisées du groupe est abandonné par l'uRFP. L'Anti-mystification a été décrite à cette page :

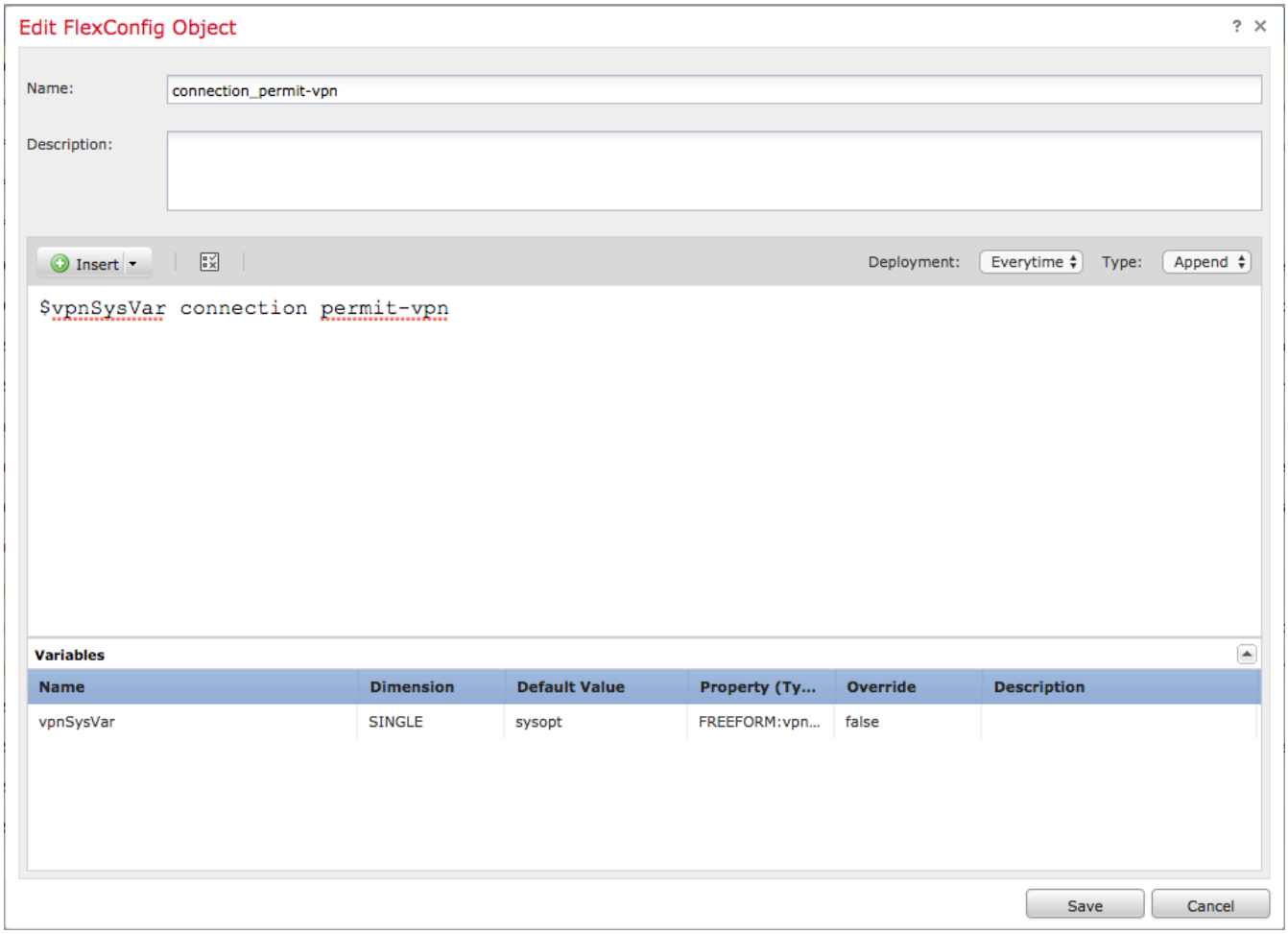
Placez les paramètres de configuration de sécurité sur la défense contre des menaces de FirePOWER

b) Activation de l'option d'autorisation-VPN de connexion de sysopt

- Allez aux **objets** > à la **Gestion d'objet** > au **FlexConfig** > à l'**objet des textes** > **ajoutent l'objet des textes**.
- Créez une variable d'objet des textes, par exemple : `vpnSysVar une` seule entrée avec la valeur « `sysopt` »
- Allez aux **objets** > à la **Gestion d'objet** > au **FlexConfig** > à l'**objet de FlexConfig** > **ajoutent l'objet de FlexConfig**.
- Créez l'objet de FlexConfig avec CLI « `connexion autorisation-VPN` » :
- Insérez la variable d'objet des textes dans l'objet de flexconfig au début du CLI en tant que « `connexion autorisation-VPN $vpnSysVar` », **sauvegarde de** clic **:**



- Appliquez l'objet de FlexConfig comme **s'ajoutent** et sélectionnez le déploiement à **chaque fois** :



- Allez aux **périphériques** > au **FlexConfig** et éditez la stratégie existante ou créez un neuf avec le bouton de **nouvelle stratégie**.
- Ajoutez juste FlexConfig créé, **sauvegarde de** clic.
- Déployez la configuration pour provision la commande « d'autorisation-VPN de connexion de sysopt » sur le périphérique.

Ceci cependant, retirera la possibilité pour employer la stratégie de contrôle d'accès pour examiner le trafic provenant les utilisateurs. Vous pouvez encore employer le filtre VPN ou l'ACL téléchargeable pour filtrer le trafic d'utilisateur.

Si vous voyez des problèmes avec les paquets de baisse Snort des utilisateurs VPN, entrez en contact avec le TAC mettant en référence CSCvg91399 .