Configuration du VPN de gestion AnyConnect SSL sur FTD

Contenu

Introduction

Ce document décrit comment configurer un tunnel de gestion Cisco AnyConnect sur un pare-feu Cisco Firepower Threat Defense (FTD) géré par Cisco Firepower Management Center (FMC). Par exemple, sous Secure Sockets Layer (SSL) est utilisé pour créer un réseau privé virtuel (VPN) entre FTD et un client Windows 10.

Contribué par Daniel Perez Vertti Vazquez, ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Éditeur de profil Cisco AnyConnect
- Configuration SSL AnyConnect via FMC.
- Authentification du certificat client

Components Used

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

- Cisco FTD version 6.7.0 (build 65)
- Cisco FMC version 6.7.0 (build 65)
- Cisco AnyConnect 4.9.01095 installé sur l'ordinateur Windows 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

Depuis la version 6.7, Cisco FTD prend en charge la configuration des tunnels de gestion AnyConnect. Cela corrige la demande d'amélioration précédemment ouverte CSCvs78215.

La fonction de gestion AnyConnect permet de créer un tunnel VPN immédiatement après le démarrage du point d'extrémité. Il n'est pas nécessaire que les utilisateurs lancent manuellement l'application AnyConnect, dès que leur système est sous tension, le service d'agent VPN AnyConnect détecte la fonctionnalité VPN de gestion et lance une session AnyConnect à l'aide de l'entrée d'hôte définie dans la liste de serveurs du profil VPN de gestion AnyConnect.

Limites

- Seule l'authentification du certificat client est prise en charge.
- Seul le magasin de certificats d'ordinateur est pris en charge pour les clients Windows.
- Non pris en charge par Cisco Firepower Device Manager (FDM) CSCvx90058.
- Non pris en charge sur les clients Linux.

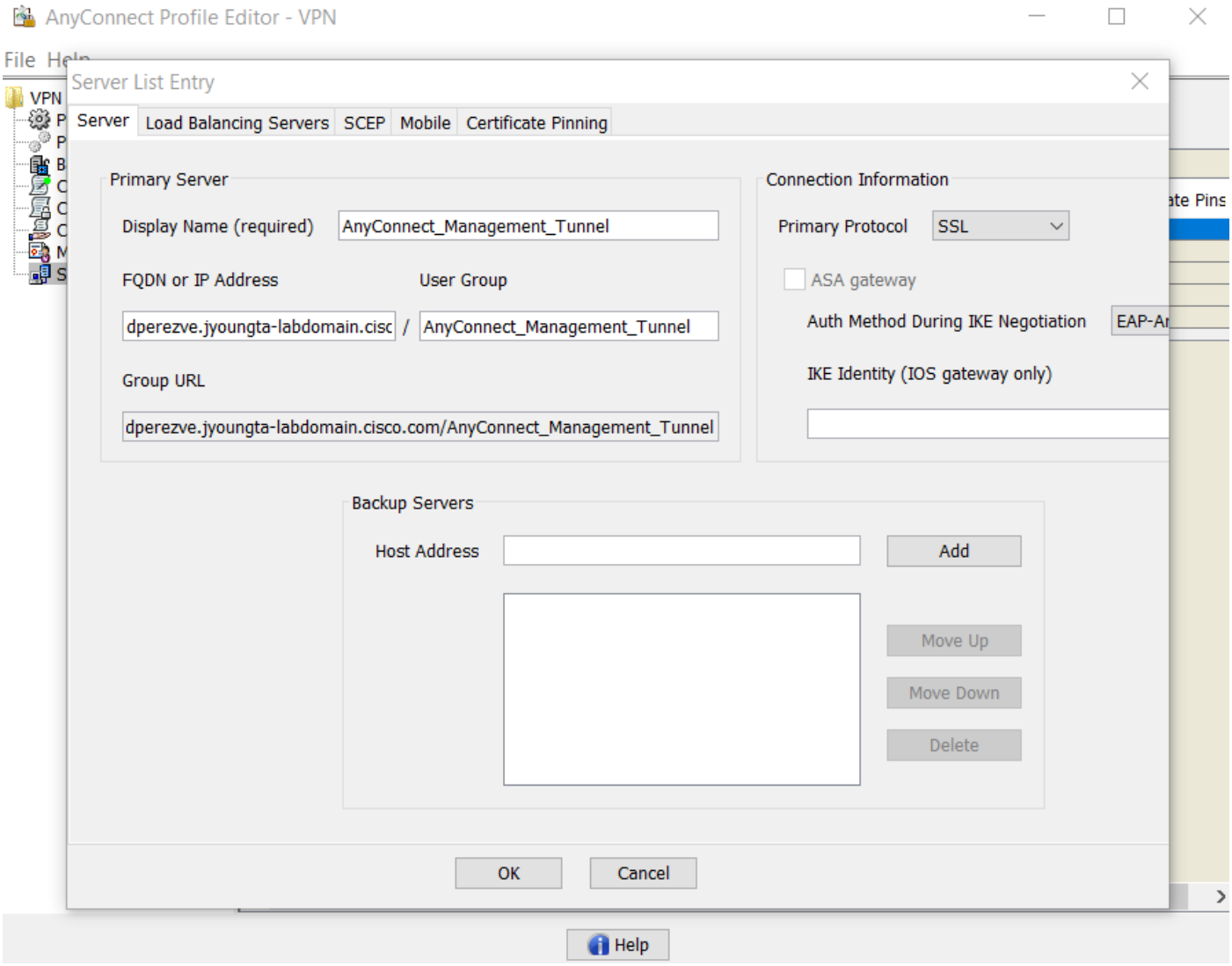
Configuration

Configurations

Étape 1. Créer un profil VPN de gestion AnyConnect

Ouvrez l'Éditeur de profil AnyConnect pour créer un profil VPN de gestion AnyConnect. Le profil de gestion contient tous les paramètres utilisés pour établir le tunnel VPN après le démarrage du point d'extrémité.

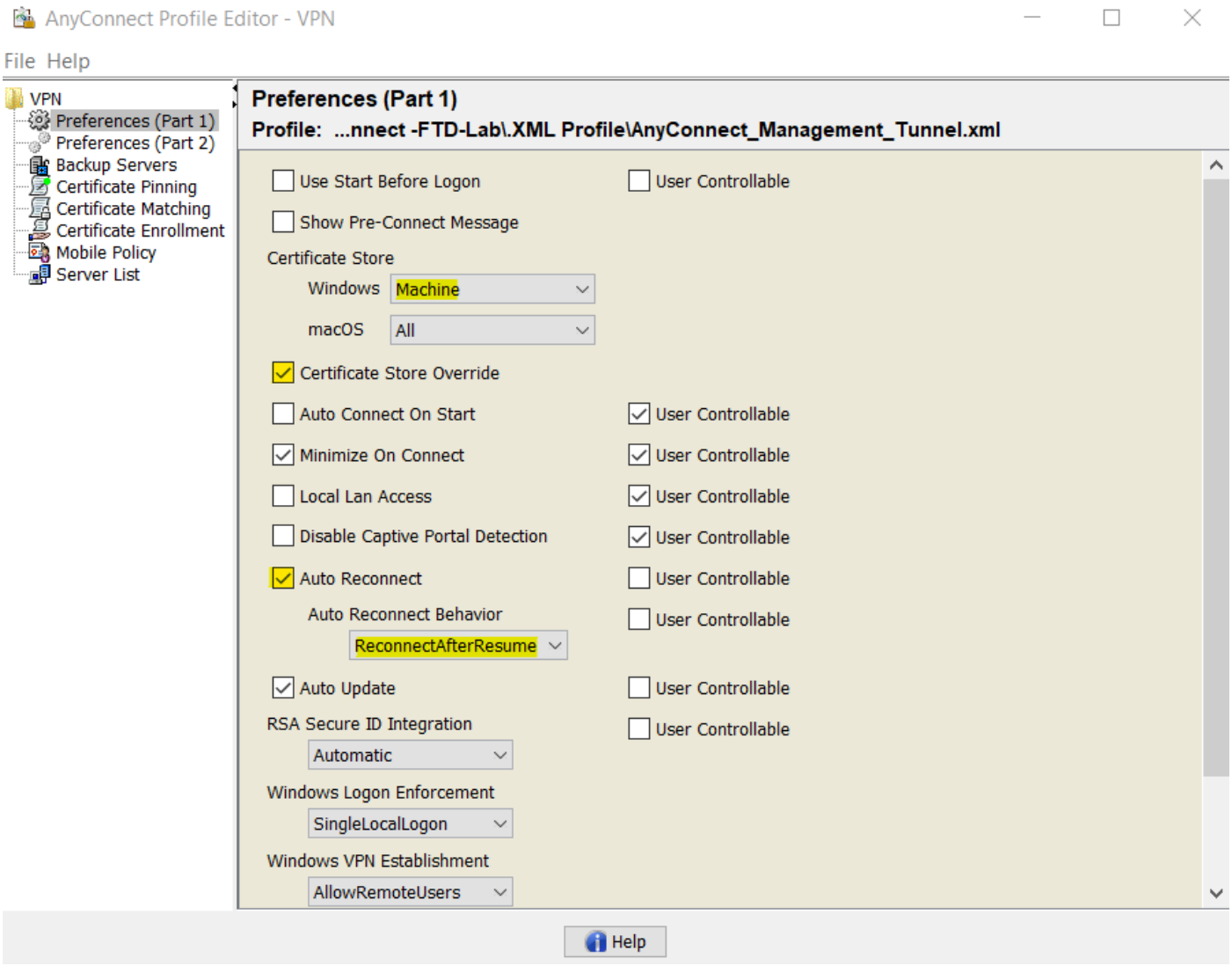
Dans cet exemple, une entrée de liste de serveurs pointant sur Nom de domaine complet (FQDN) dperezve.jyoung-labdomain.cisco.com est définie et SSL est sélectionné comme protocole principal. Pour ajouter une liste de serveurs, accédez à **Liste de serveurs** et sélectionnez le bouton **Ajouter**, remplissez les champs requis et enregistrez les modifications.



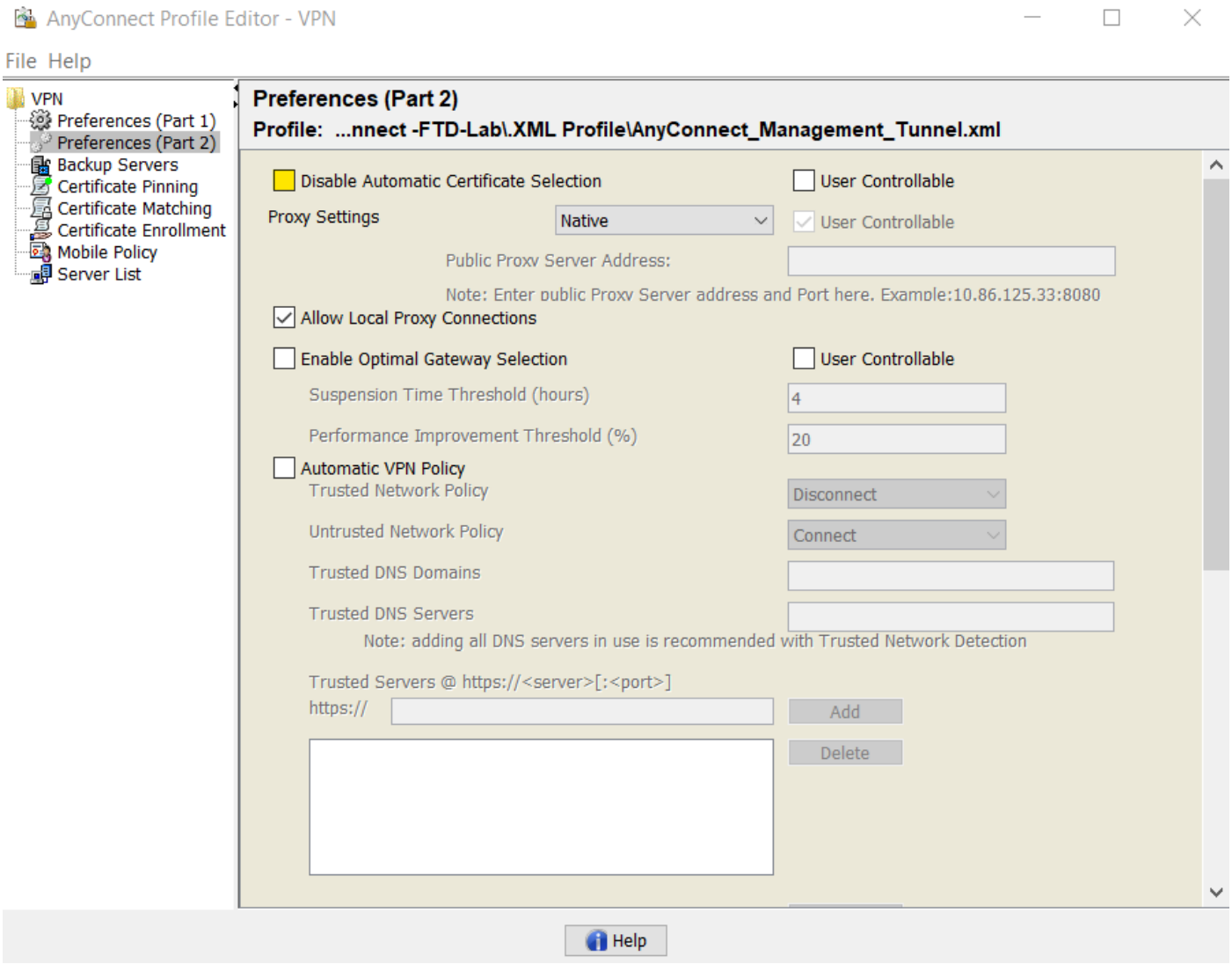
Outre la liste des serveurs, le profil VPN de gestion doit contenir certaines préférences obligatoires :

- **AutomaticCertSelection** doit être défini sur **true**.
- **La reconnexion automatique** doit être définie sur **true**.
- **AutoReconnectBehavior** doit être configuré pour **ReconnectAfterResume**.
- **AutoUpdate** doit avoir la valeur **false**.
- **BlockUntrustServers** doit être défini sur **true**.
- **CertificateStore** doit être configuré pour **MachineStore**.
- **CertificateStoreOverride** doit être défini sur **true**.
- **EnableAutomaticServerSelection** doit avoir la valeur **false**.
- **EnableScripting** doit avoir la valeur **false**.
- **RetainVPNOnLogoff** doit être défini sur **true**.

Dans AnyConnect Profile Editor, accédez à **Préférences (Partie 1)** et réglez les paramètres comme suit :



Ensuite, accédez à **Préférences (Partie 2)** et décochez l'option **Désactiver la sélection automatique de certificats**.



Étape 2. Créer un profil VPN AnyConnect

Outre le profil VPN de gestion, le profil VPN AnyConnect standard doit être configuré. Le profil VPN AnyConnect est utilisé lors de la première tentative de connexion. Au cours de cette session, le profil VPN de gestion est téléchargé à partir de FTD.

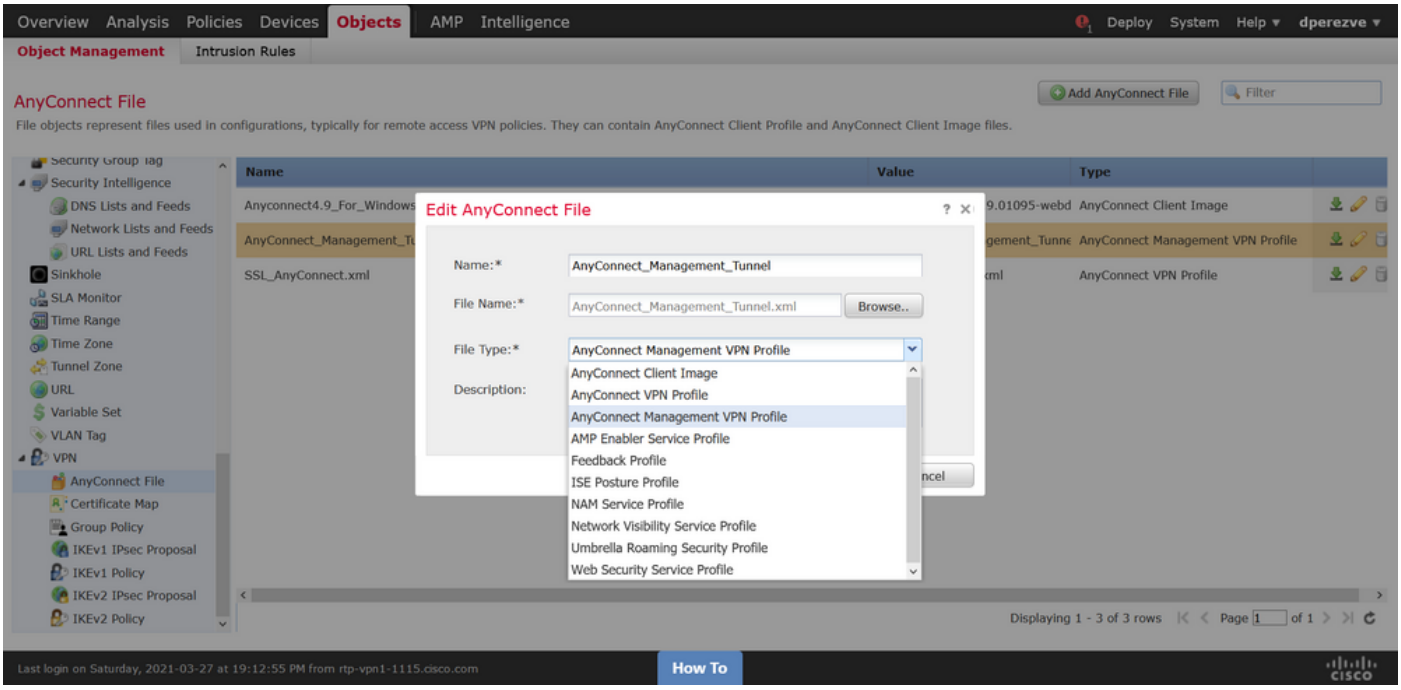
Utilisez l'éditeur de profil AnyConnect pour créer le profil VPN AnyConnect. Dans ce cas, les deux fichiers contiennent les mêmes paramètres afin que la même procédure puisse être suivie.

Étape 3. Télécharger le profil VPN de gestion AnyConnect et le profil VPN AnyConnect sur FMC

Une fois les profils créés, l'étape suivante consiste à les télécharger sur le FMC en tant qu'objets de fichier AnyConnect.

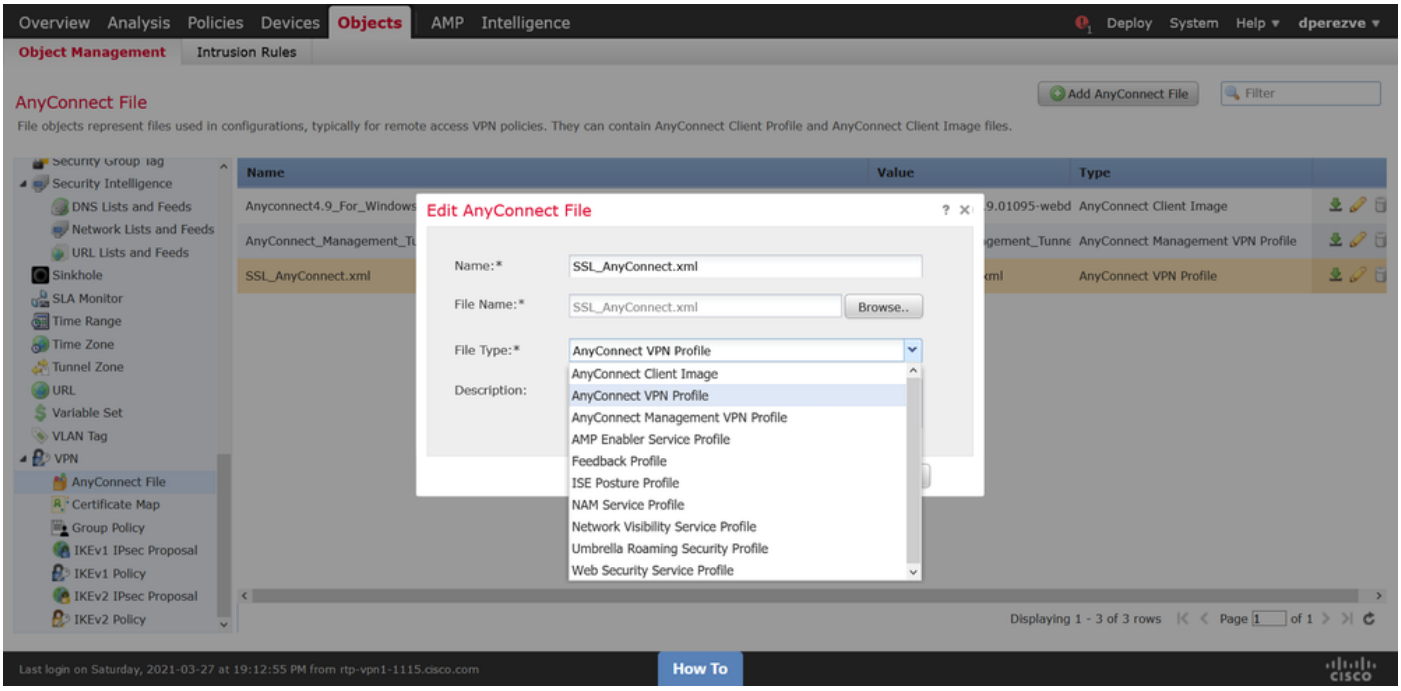
Afin de télécharger le nouveau profil VPN de gestion AnyConnect sur FMC, accédez à **Objets > Gestion des objets** et choisissez l'option **VPN** dans la table des matières, puis sélectionnez le bouton **Ajouter un fichier AnyConnect**.

Indiquez un nom pour le fichier, choisissez **AnyConnect Management VPN Profile** comme type de fichier et enregistrez l'objet.

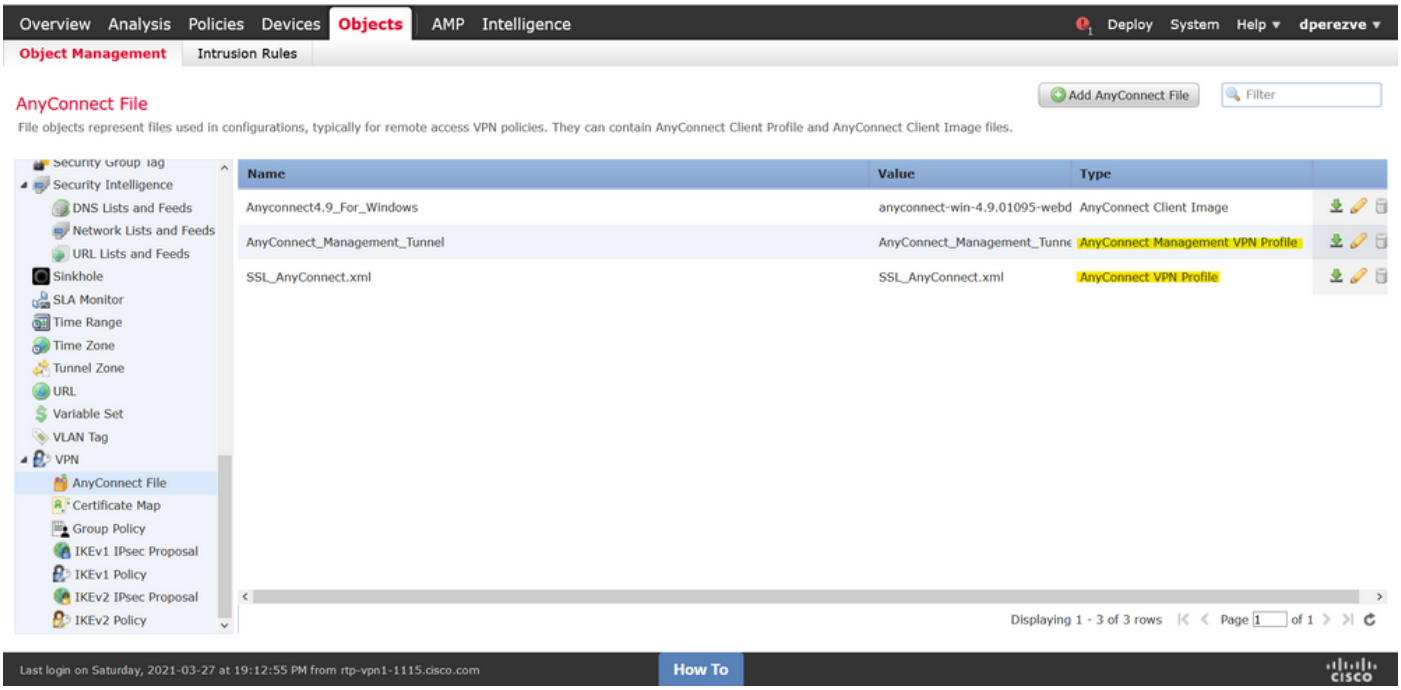


Maintenant, afin de télécharger le profil VPN AnyConnect naviguez à nouveau vers **Objets > Gestion des objets** et choisissez l'option **VPN** dans la table des matières, puis sélectionnez le bouton **Ajouter un fichier AnyConnect**.

Indiquez un nom pour le fichier, mais cette fois, choisissez **AnyConnect VPN Profile** comme type de fichier et enregistrez le nouvel objet.



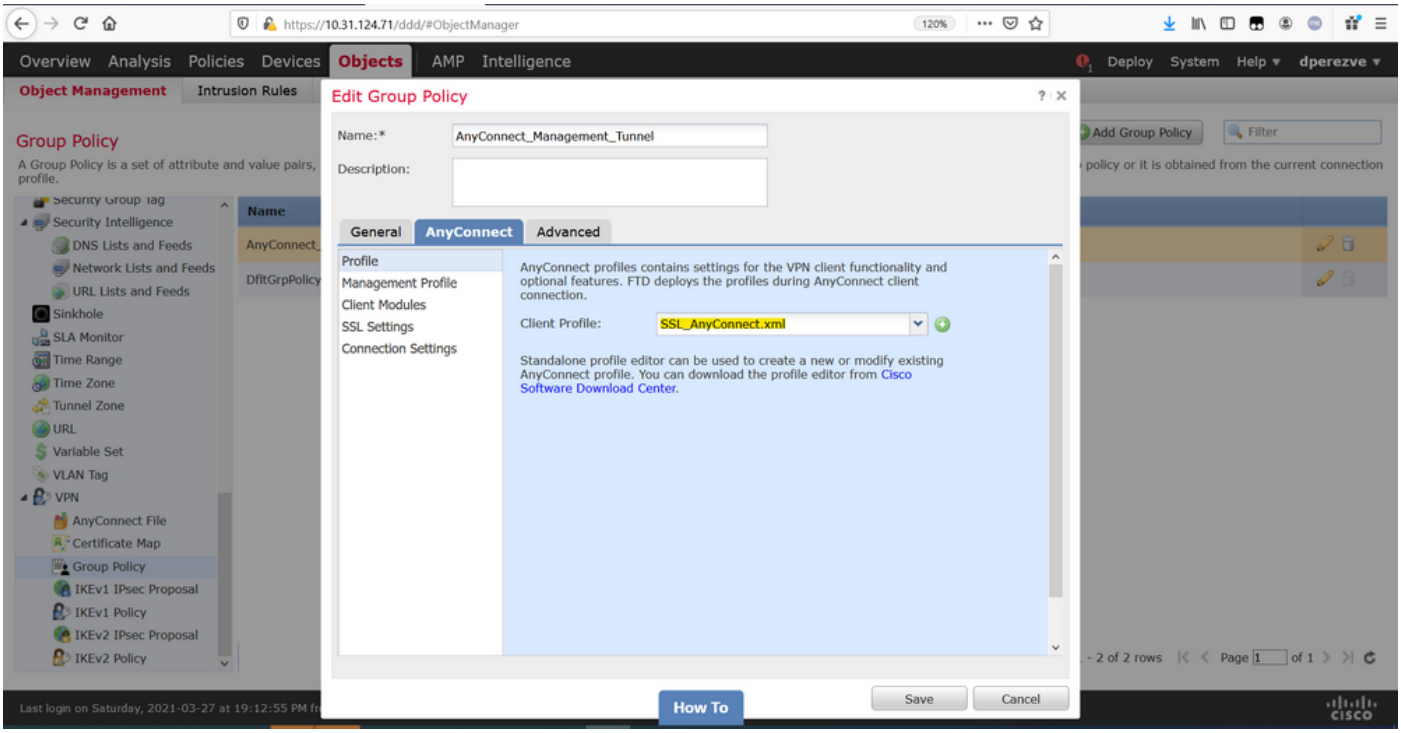
Les profils doivent être ajoutés à la liste des objets et marqués comme **Profil VPN de gestion AnyConnect** et **Profil VPN AnyConnect** respectivement.



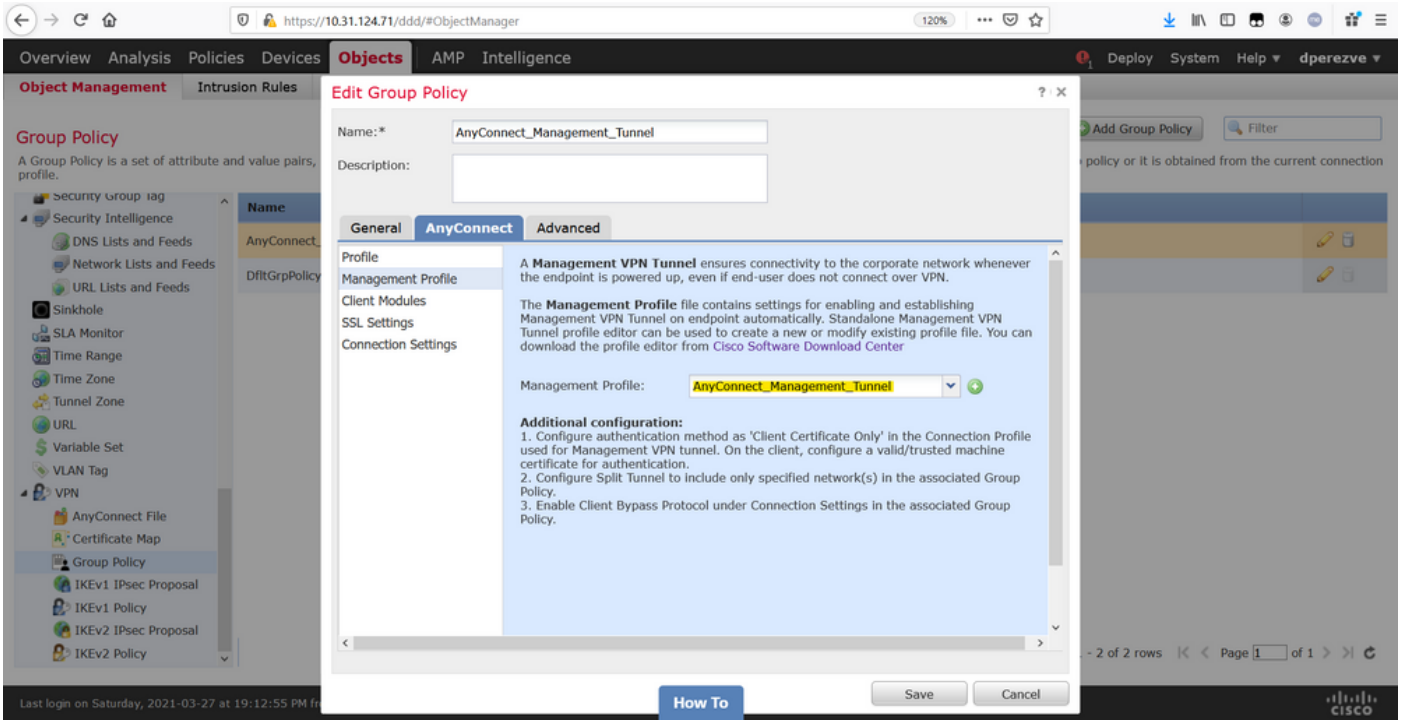
Étape 4. Créer une stratégie de groupe

Afin de créer une nouvelle stratégie de groupe, accédez à **Objets > Gestion des objets** et choisissez l'option **VPN** dans la table des matières, puis sélectionnez **Stratégie de groupe** et cliquez sur le bouton **Ajouter une stratégie de groupe**.

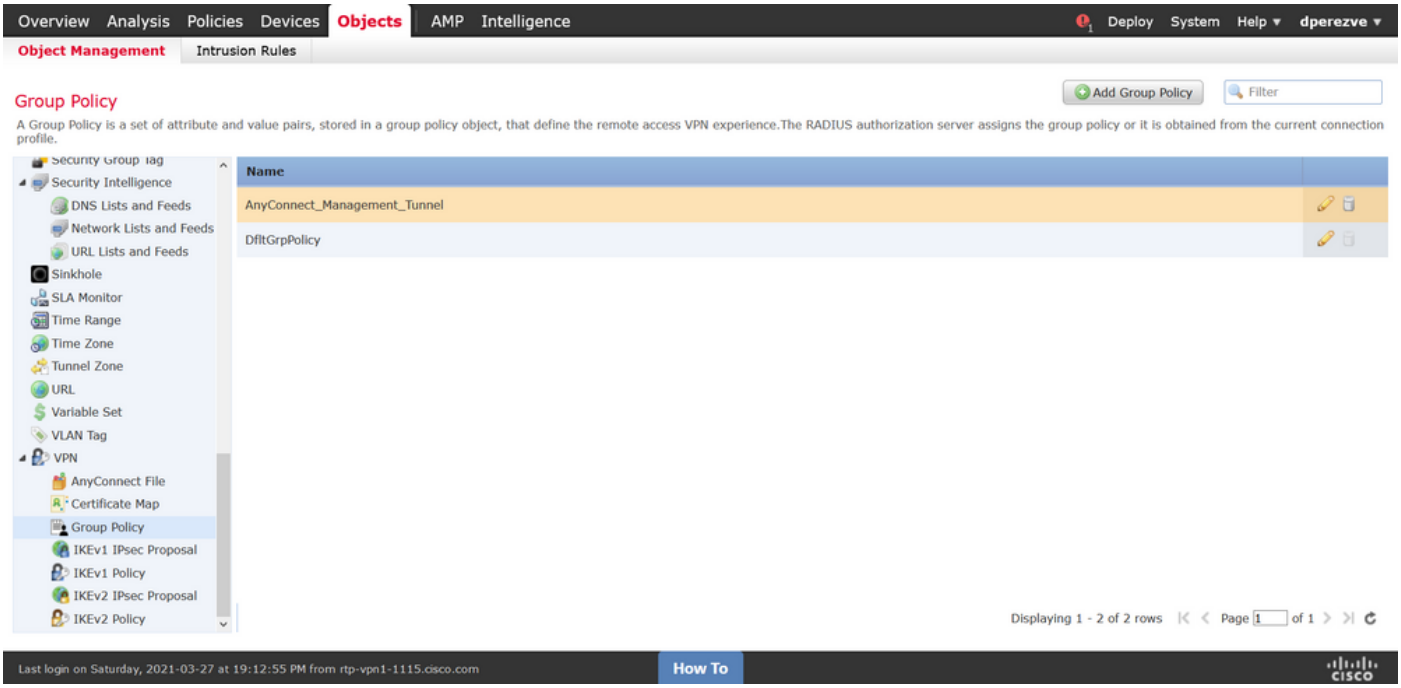
Une fois la fenêtre **Ajouter une stratégie de groupe** ouverte, attribuez un nom, définissez un pool AnyConnect et ouvrez l'onglet **AnyConnect**. Accédez à **Profil** et sélectionnez l'objet qui représente le profil VPN AnyConnect régulier dans le menu déroulant **Profil client**.



Ensuite, accédez à l'onglet **Profil de gestion** et sélectionnez l'objet qui contient le profil VPN de gestion dans le menu déroulant **Profil de gestion**.



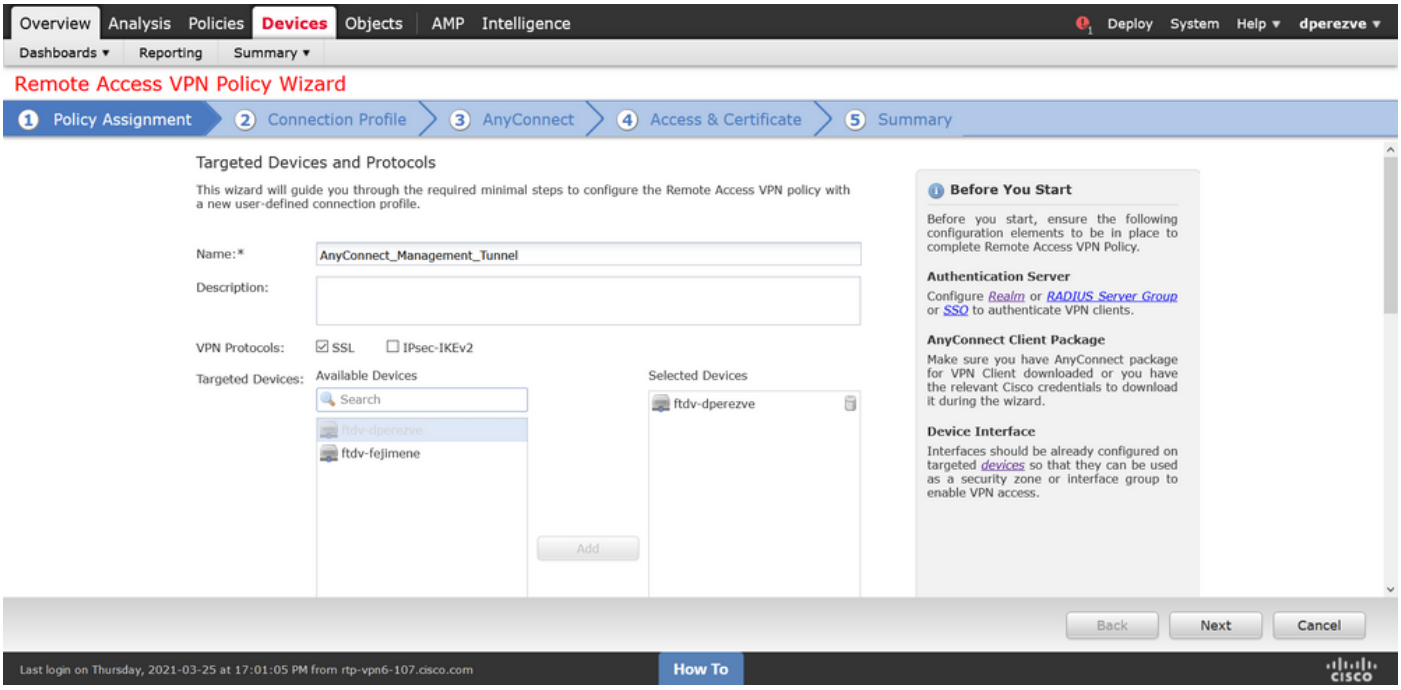
Enregistrez les modifications pour ajouter le nouvel objet aux stratégies de groupe existantes.



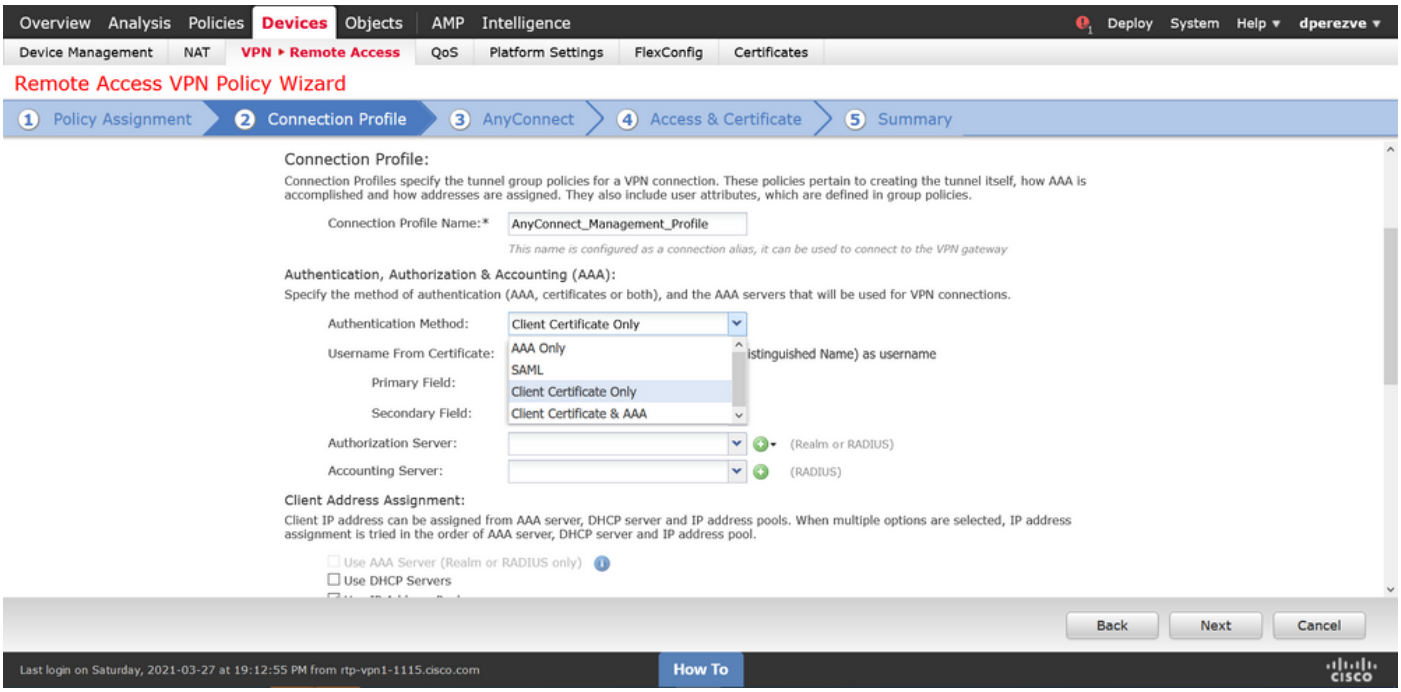
Étape 5. Créer une nouvelle configuration AnyConnect

La configuration de SSL AnyConnect dans FMC est composée de 4 étapes différentes. Pour configurer AnyConnect, accédez à **Devices > VPN > Remote Access** et sélectionnez le bouton **Add**. Ceci doit ouvrir l'**Assistant Stratégie VPN d'accès à distance**.

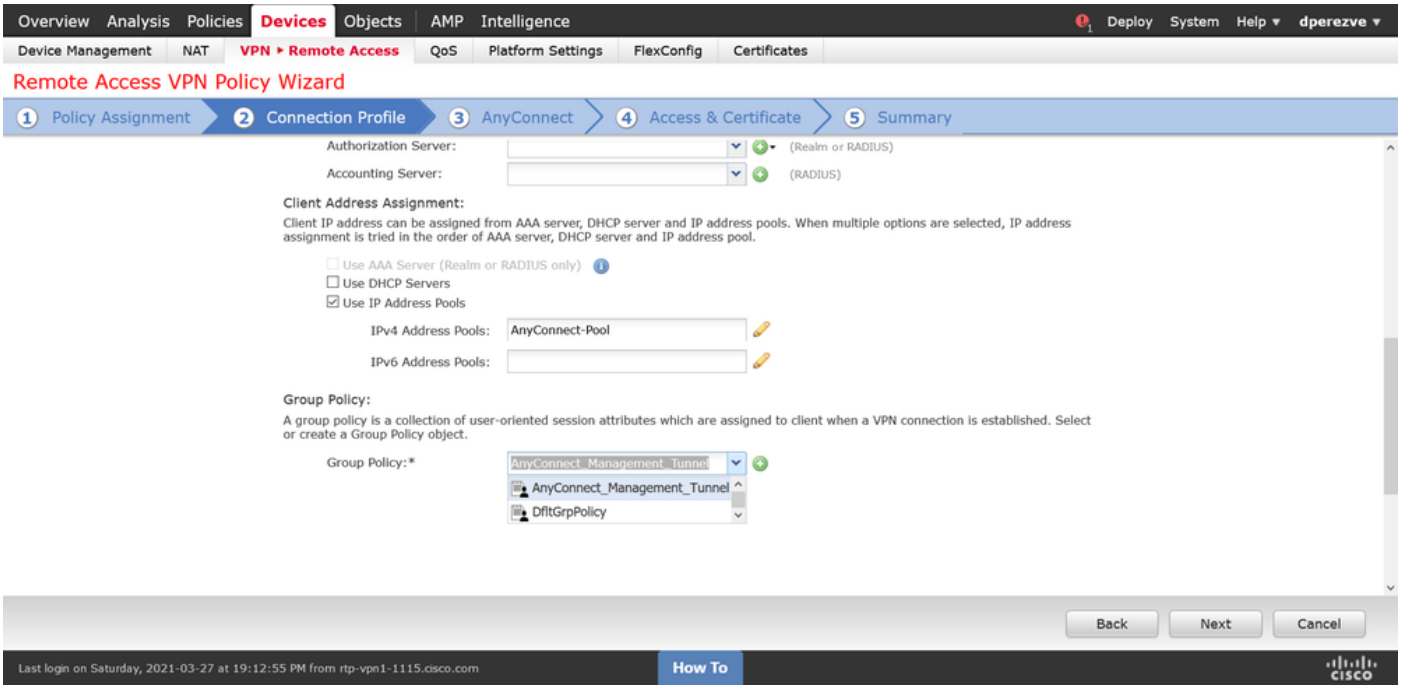
Dans l'onglet **Affectation de stratégie**, sélectionnez le périphérique FTD en main, définissez un nom pour le profil de connexion et cochez la case SSL.



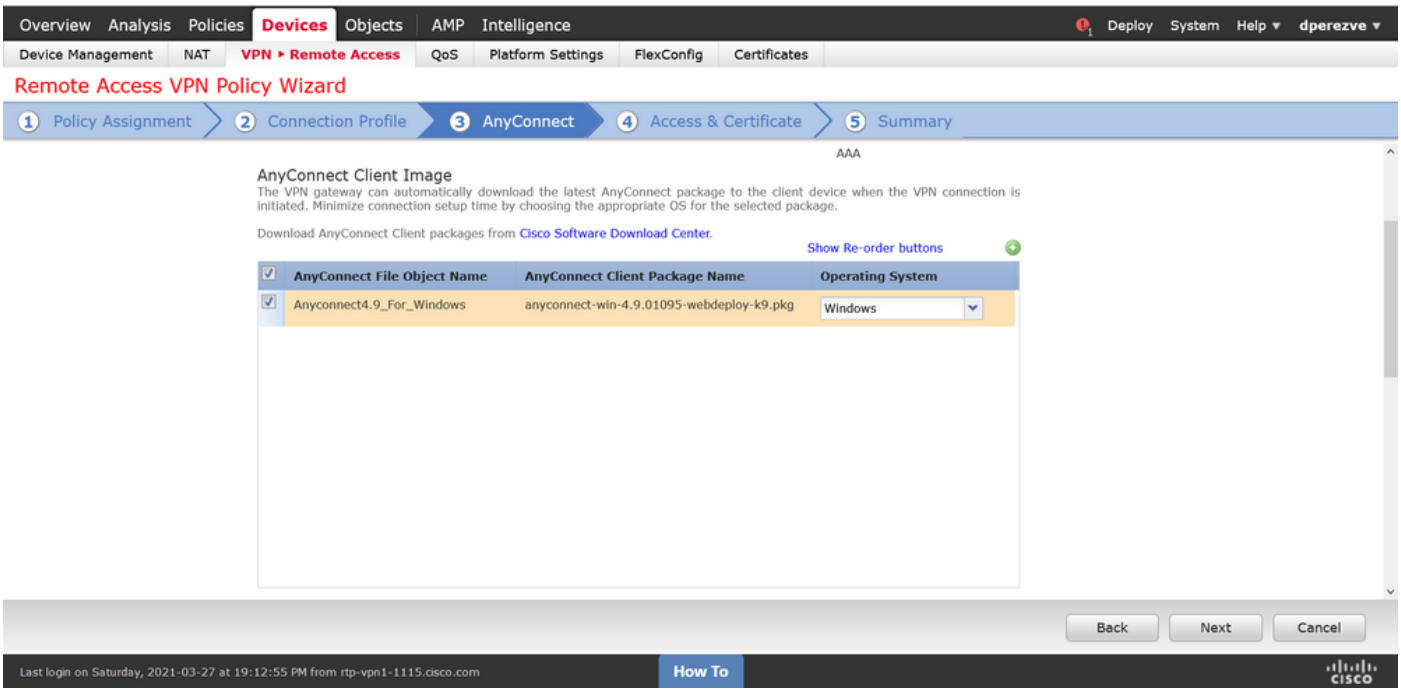
Dans **Profil de connexion** sélectionnez **Certificat client uniquement** comme méthode d'authentification. Il s'agit de la seule authentification prise en charge pour la fonctionnalité.



Sélectionnez ensuite l'objet Stratégie de groupe créé à l'étape 3 dans la liste déroulante **Stratégie de groupe**.



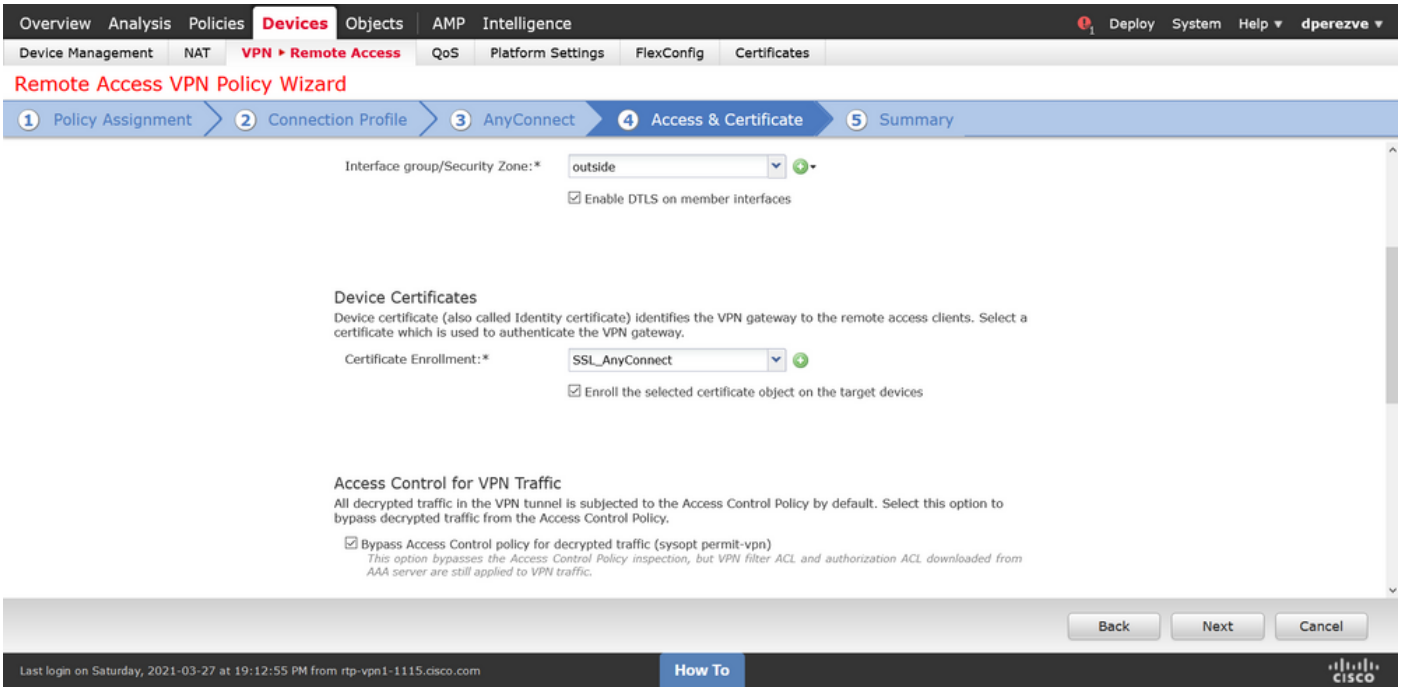
Sous l'onglet **AnyConnect**, sélectionnez l'**objet de fichier AnyConnect** en fonction du système d'exploitation (OS) du point de terminaison.



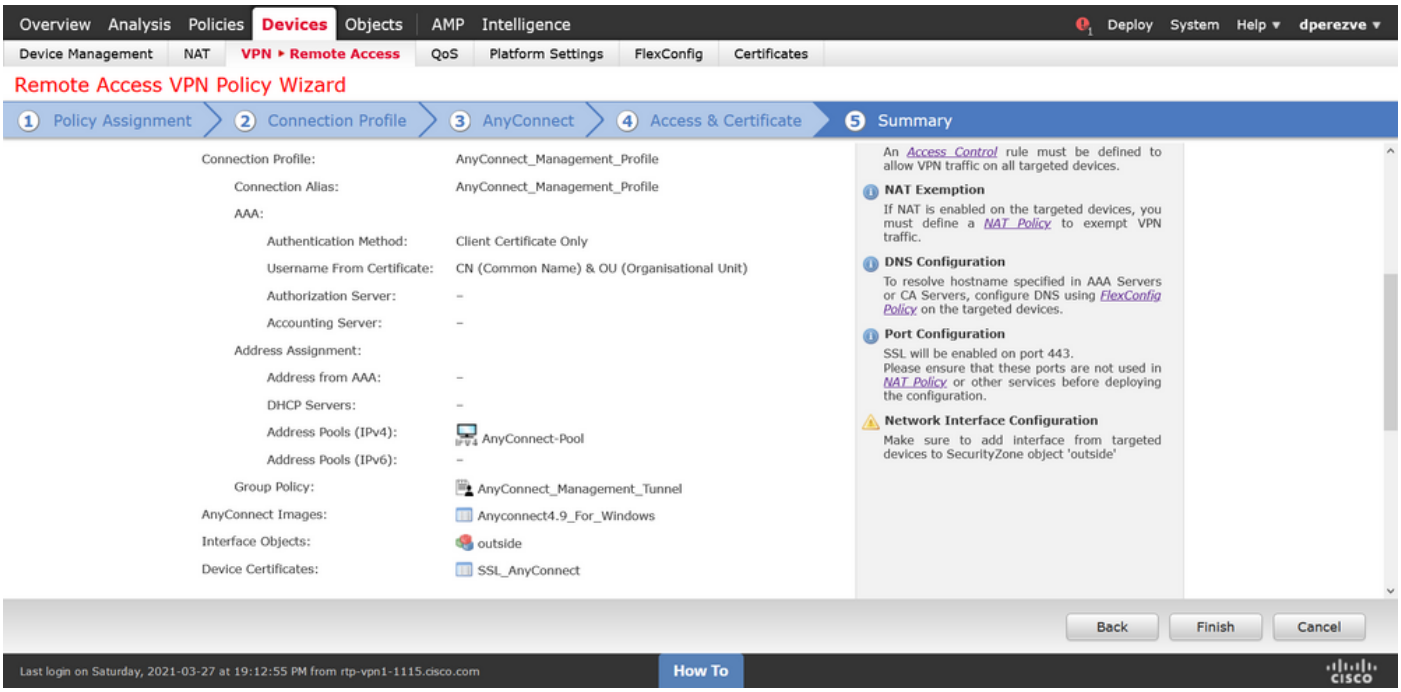
Sur **Access & Certificate** spécifiez le certificat qui doit être utilisé par le FTD pour tester son identité sur le client Windows.

> **Note**: Puisque les utilisateurs ne doivent pas interagir avec l'application AnyConnect lors de l'utilisation de la fonctionnalité VPN de gestion, le certificat doit être entièrement fiable et ne doit pas imprimer de message d'avertissement.

> **Note**: Afin d'empêcher les erreurs de validation de certificat, le champ Nom commun (CN) inclus dans le nom d'objet du certificat doit correspondre au nom de domaine complet défini dans la liste des profils XML du serveur (Étape 1 et Étape 2).



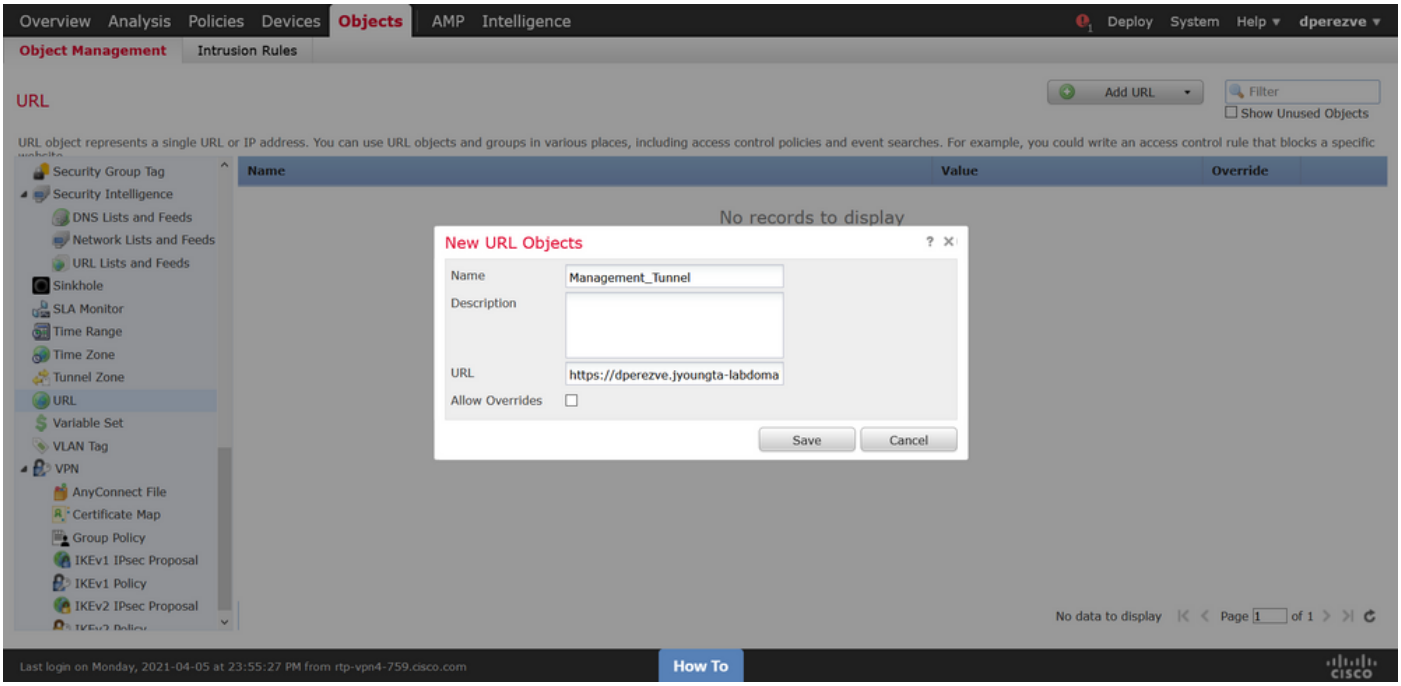
Enfin, sélectionnez **Terminer** dans l'onglet **Résumé** pour ajouter la nouvelle configuration AnyConnect.



Étape 6. Créer un objet URL

Accédez à **Objets > Gestion des objets** et sélectionnez **URL** dans la table des matières. Sélectionnez ensuite **Ajouter un objet** dans la liste déroulante **Ajouter une URL**.

Fournissez un nom pour l'objet et définissez l'URL à l'aide du même nom de domaine complet/groupe d'utilisateurs spécifié dans la liste Management VPN Profile Server (Étape 2). Dans cet exemple, l'URL doit être dperezve.jyoungta-labdomain.cisco.com/AnyConnect_Management_Tunnel.



Enregistrez les modifications pour ajouter l'objet à la liste des objets.

Étape 7. Définir l'alias d'URL

Afin d'activer l'alias d'URL dans la configuration AnyConnect, accédez à **Devices > VPN > Remote Access** et cliquez sur l'icône représentant un crayon pour la modifier.

Ensuite, dans l'onglet Profil de connexion, sélectionnez la configuration à portée de main, accédez à **Alias**, cliquez sur le bouton **Ajouter** et sélectionnez l'**objet URL** dans la **liste déroulante Alias URL** . Assurez-vous que la case **Enabled** est cochée.

Enregistrez les modifications et déployez les configurations sur FTD.

Vérification

Une fois le déploiement terminé, une première connexion AnyConnect manuelle avec le profil VPN AnyConnect est nécessaire. Pendant cette connexion, le profil VPN de gestion est téléchargé à partir de FTD et stocké dans **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**. À partir de ce point, les connexions suivantes doivent être initiées via le profil VPN de gestion sans aucune interaction utilisateur.

Dépannage

Pour les erreurs de validation de certificat :

- Assurez-vous que le certificat racine de l'autorité de certification (CA) est installé sur le FTD.
- Assurez-vous qu'un certificat d'identité signé par la même autorité de certification est installé sur le Windows Machine Store.
- Assurez-vous que le champ CN est inclus dans le certificat et qu'il est identique au nom de domaine complet défini dans la liste des serveurs du profil VPN de gestion et du nom de domaine complet défini dans l'alias d'URL.

Pour le tunnel de gestion non initialisé :

- Vérifiez que le profil VPN de gestion a été téléchargé et stocké dans **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**.
- Vérifiez que le nom du profil VPN de gestion est **VpnMgmtTunProfile.xml**.

Pour les problèmes de connectivité, collectez l'offre DART et contactez le TAC Cisco pour plus d'informations.