Configuration du tunnel de gestion VPN du client sécurisé sur le pare-feu sécurisé

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

- Limites

Configurer

- Configurations
  - Étape 1 : création d'un profil VPN de gestion AnyConnect
  - Étape 2 : création d'un profil VPN AnyConnect
  - Étape 3. Télécharger le profil VPN de gestion AnyConnect et le profil VPN AnyConnect vers FMC
  - Étape 4. Créer une stratégie de groupe
  - Étape 5. Création d'une configuration AnyConnect
  - Étape 6. Créer un objet URL
  - Étape 7. Définir un alias d'URL

Vérifier

Dépannage

Introduction

Ce document décrit comment configurer un tunnel de gestion VPN de client sécurisé sur un pare-feu sécurisé de défense contre les menaces géré par Cisco FMC.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Authentification du certificat client
- Éditeur de profil Cisco AnyConnect
- Configuration SSL AnyConnect via Firewall Management Center (FMC)

Composants utilisés

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

- Cisco FMC version 6.7.0 (build 65)
- Cisco Firewall Threat Defense (FTD) version 6.7.0 (build 65)
- Cisco AnyConnect 4.9.01095 installé sur une machine 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

Dans cet exemple, SSL (Secure Sockets Layer) est utilisé pour créer un réseau privé virtuel (VPN) entre FTD et un client Windows 10.

Depuis la version 6.7, Cisco FTD prend en charge la configuration des tunnels de gestion AnyConnect. Ce correctif a déjà ouvert la demande d'amélioration ID de bogue Cisco CSCvs78215.

La fonctionnalité Gestion AnyConnect vous permet de créer un tunnel VPN immédiatement après le démarrage du point d'extrémité. Les utilisateurs n'ont pas besoin de lancer manuellement l'application AnyConnect. Une fois le système mis 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 de l'ordinateur est pris en charge pour les clients Windows.
- Non pris en charge sur Cisco Firepower Device Manager (FDM) ID de bogue Cisco CSCvx90058.
- Non pris en charge pour les clients Linux.

Limitations complètes décrites dans le Guide de l'administrateur du client sécurisé Cisco, version

5.

Configurer

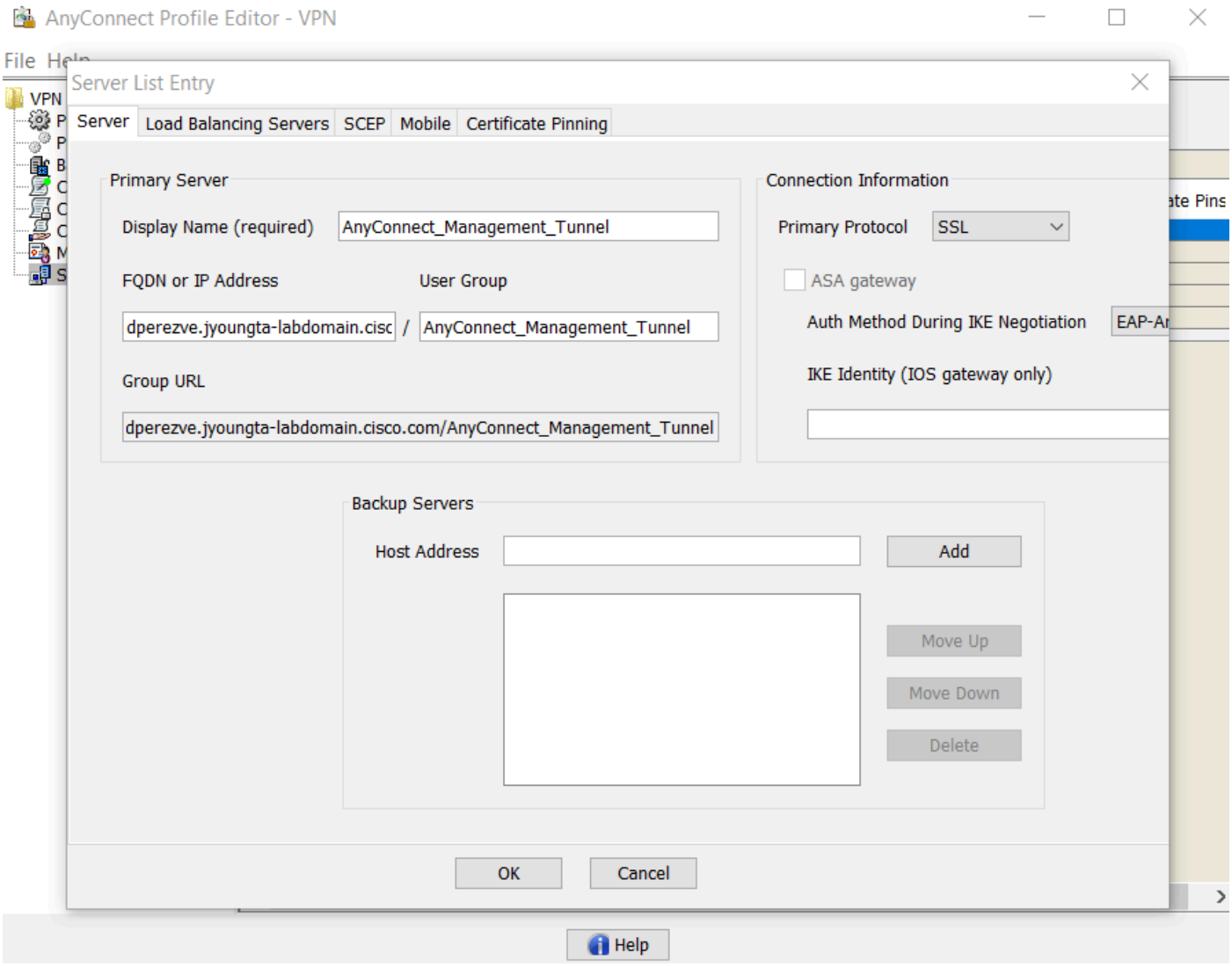
Configurations

Étape 1 : création d’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.

---

1. Dans cet exemple, une entrée de liste de serveurs pointe vers le nom de domaine complet (FQDN) dperezve.jyoungta-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 obligatoires et enregistrez vos modifications.



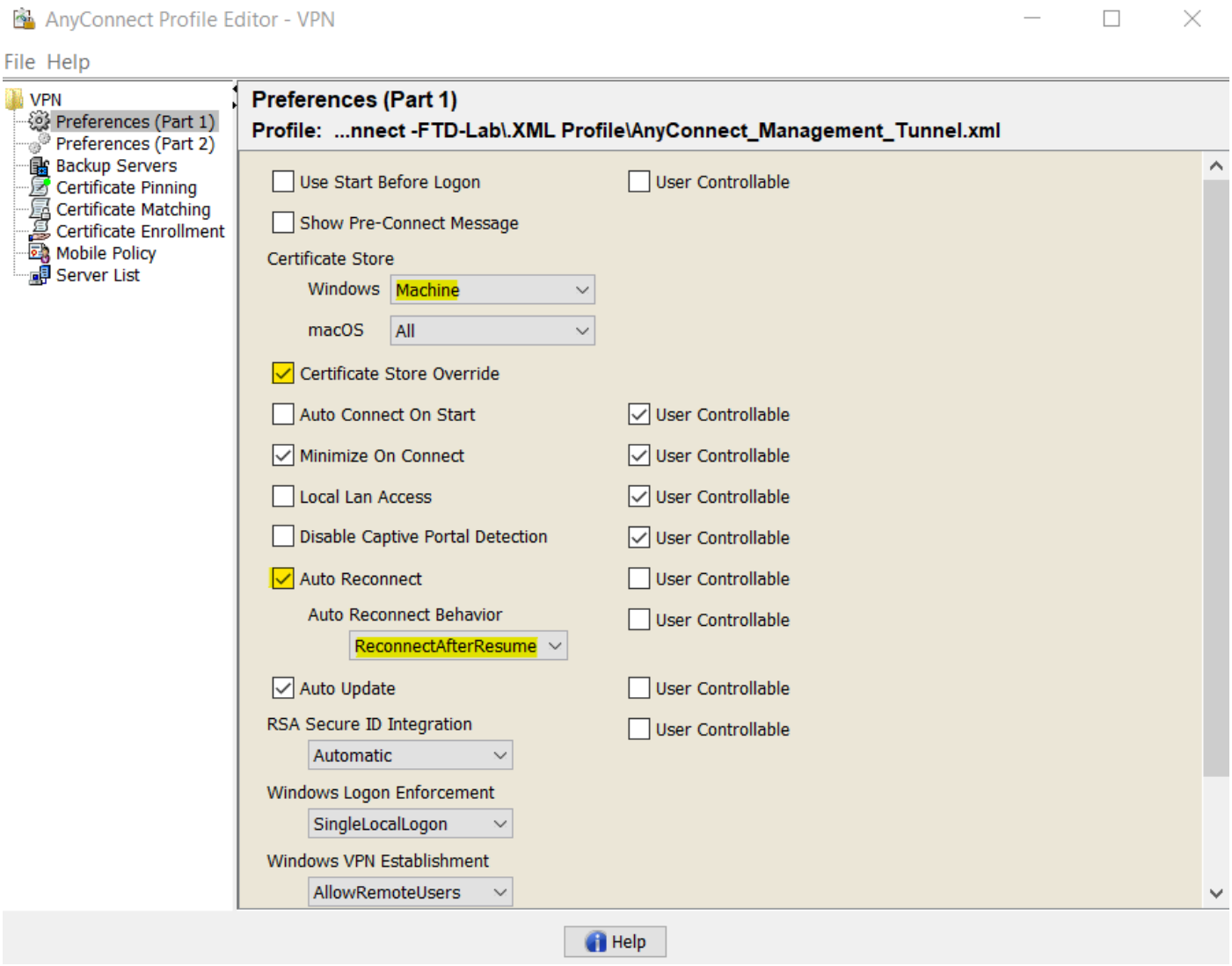
---

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

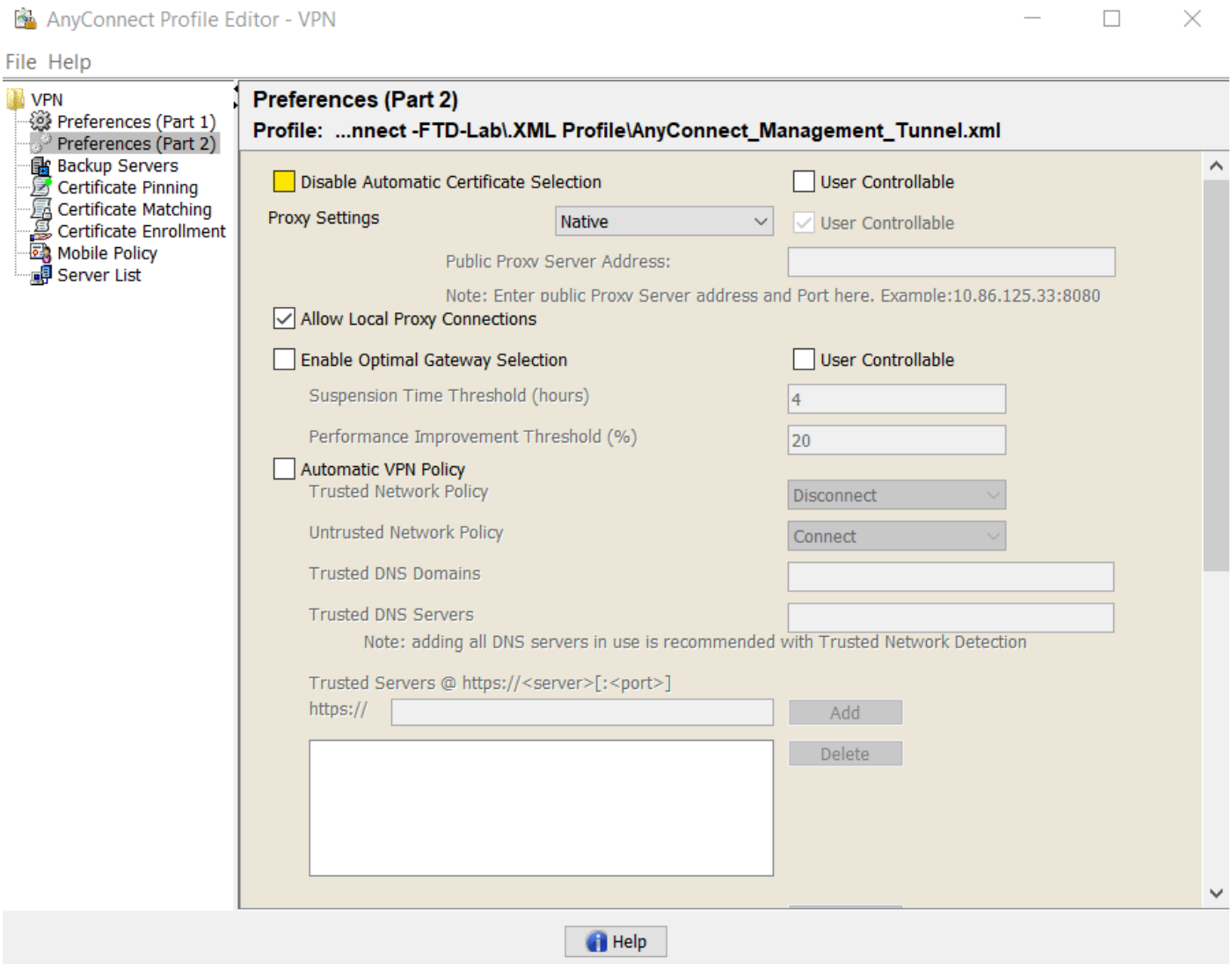
- AutomaticCertSelection doit avoir la valeur true.
- La reconnexion automatique doit être définie sur true.
- AutoReconnectBehavior doit être configuré pour ReconnectAfterResume.
- AutoUpdate doit être défini sur false.
- BlockUntrustedServers doit avoir la valeur true.
- CertificateStore doit être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

---

3. Dans l'Éditeur de profil AnyConnect, accédez à Préférences (Partie 1) et réglez les paramètres comme indiqué dans l'image :



4. Accédez à Préférences (Partie 2) et décochez la case Désactiver la sélection automatique de certificat option.



Étape 2 : création d'un profil VPN AnyConnect

En plus du 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 contenant les mêmes paramètres, la même procédure peut être utilisée.

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

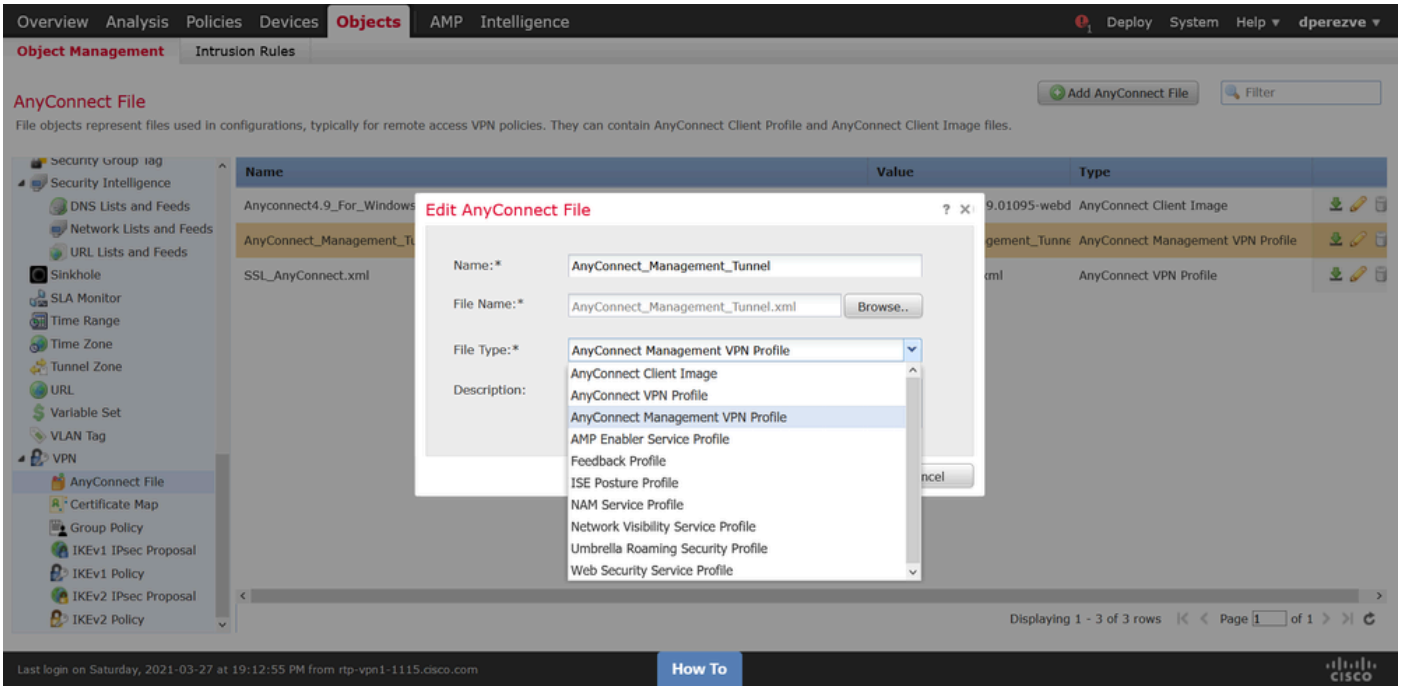
1. Une fois les profils créés, téléchargez-les dans FMC en tant qu'objets Fichier AnyConnect.

---

2. Pour télécharger le nouveau profil VPN de gestion AnyConnect vers FMC, accédez à Objets > Gestion d'objets et choisissez l'option VPN dans la table des matières. Cliquez sur le bouton Ajouter un fichier AnyConnect.

---

3. Entrez un nom pour le fichier. Choisissez AnyConnect Management VPN Profile comme type de fichier et enregistrez l'objet.

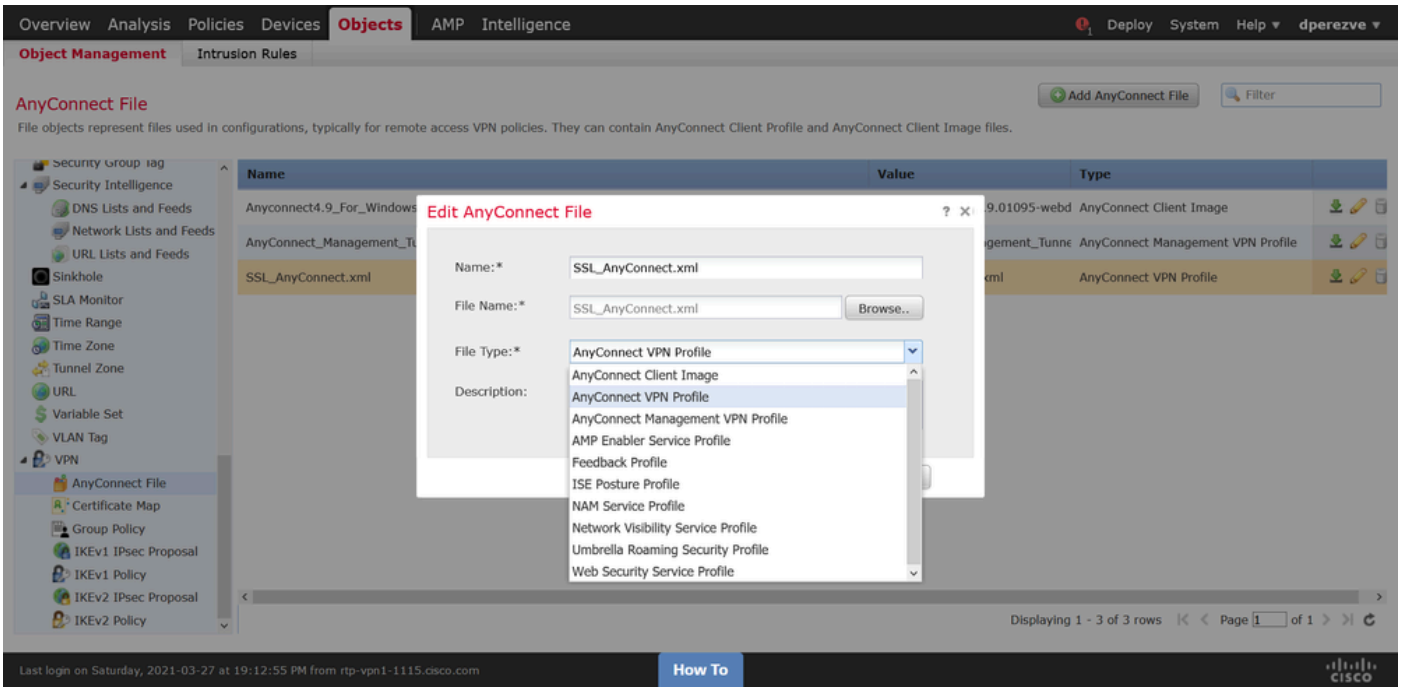


---

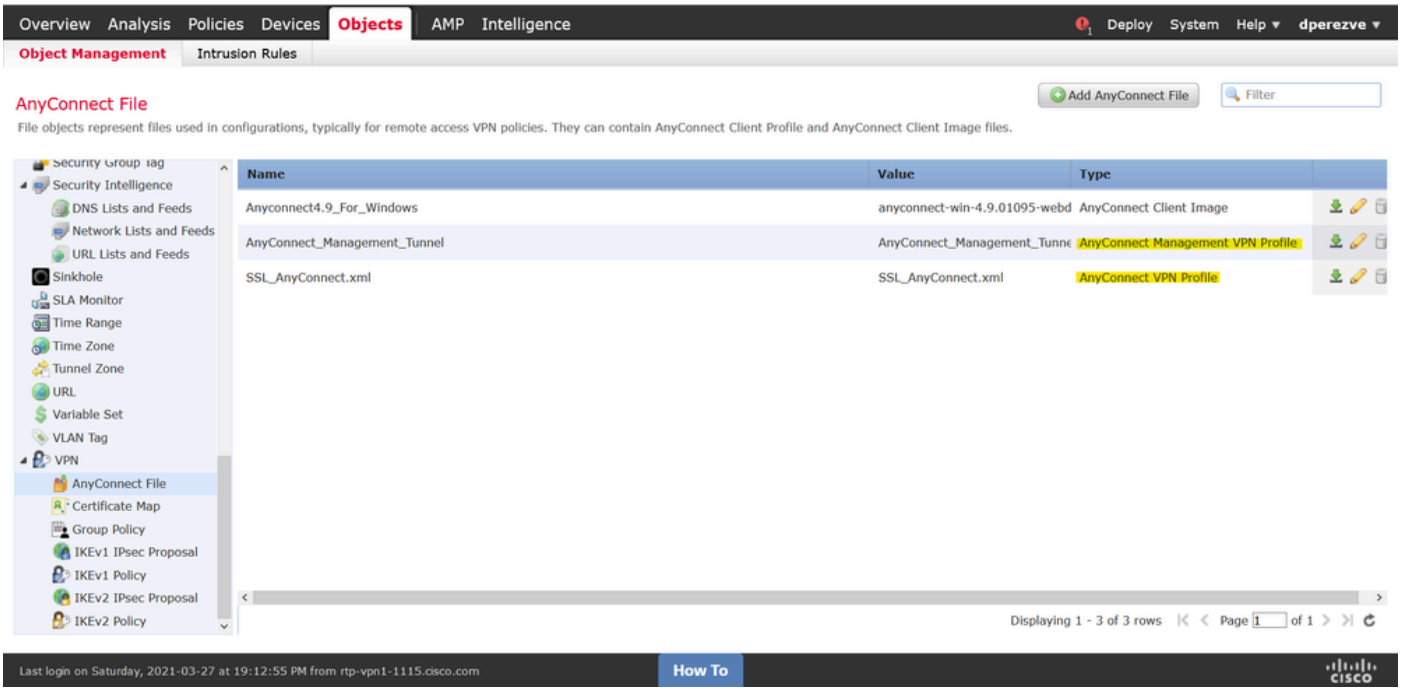
4. Pour télécharger le profil VPN AnyConnect, accédez à Objets > Gestion des objets et choisissez l'option VPN dans la table des matières. Cliquez sur le bouton Ajouter un fichier AnyConnect.

---

5. Fournissez un nom pour le fichier et cette fois, choisissez le profil VPN AnyConnect comme type de fichier et enregistrez le nouvel objet.



6. Les profils doivent être ajoutés à la liste d'objets et marqués comme AnyConnect Management VPN Profile et AnyConnect VPN Profile respectivement.



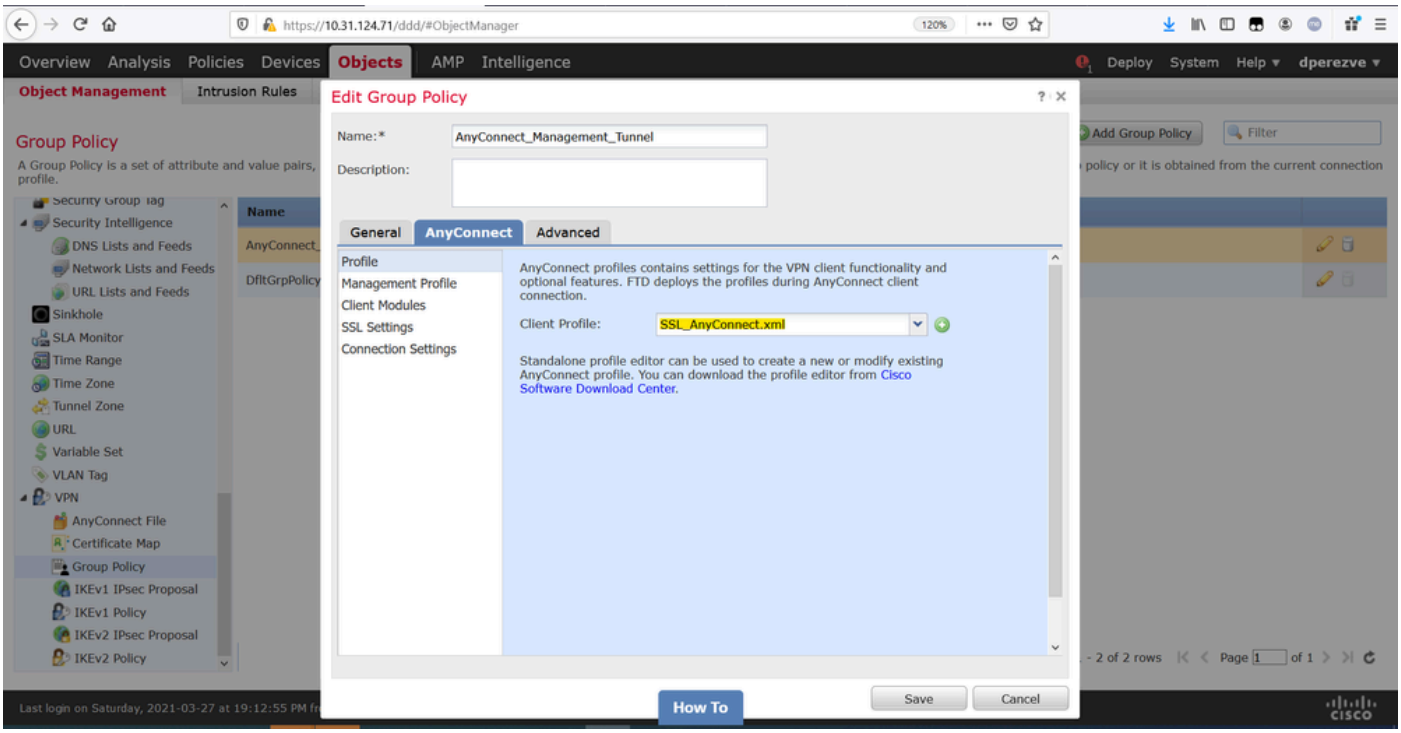
Étape 4. Créer une stratégie de groupe

1. Pour créer une nouvelle stratégie de groupe, accédez à Objets > Gestion des objets et choisissez l'option VPN dans la table des matières. Sélectionnez Group Policy et cliquez sur le

bouton Add Group Policy.

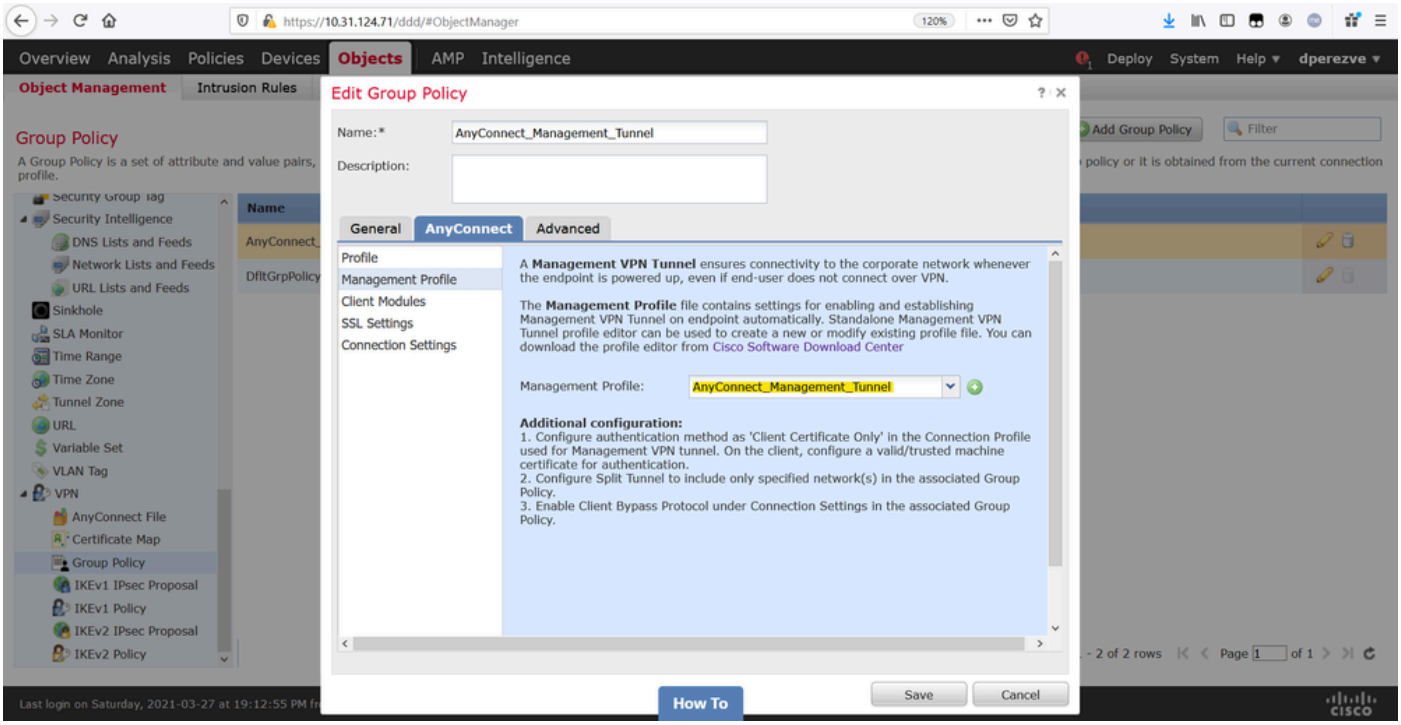
2. Une fois la fenêtre Ajouter une stratégie de groupe ouverte, attribuez un nom et définissez un pool AnyConnect et ouvrez l'onglet AnyConnect.

3. Accédez à Profile et sélectionnez l'objet qui représente le profil VPN AnyConnect normal dans le menu déroulant Client Profile.

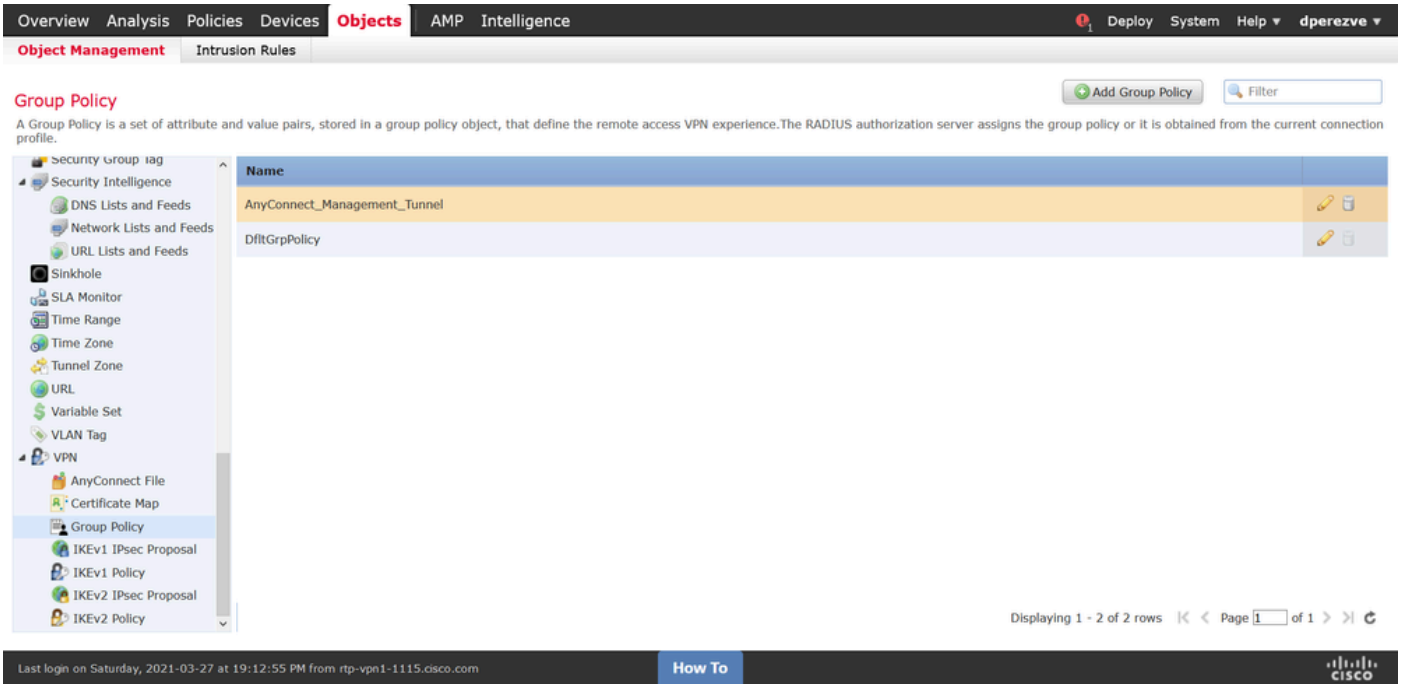


---

4. 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.



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

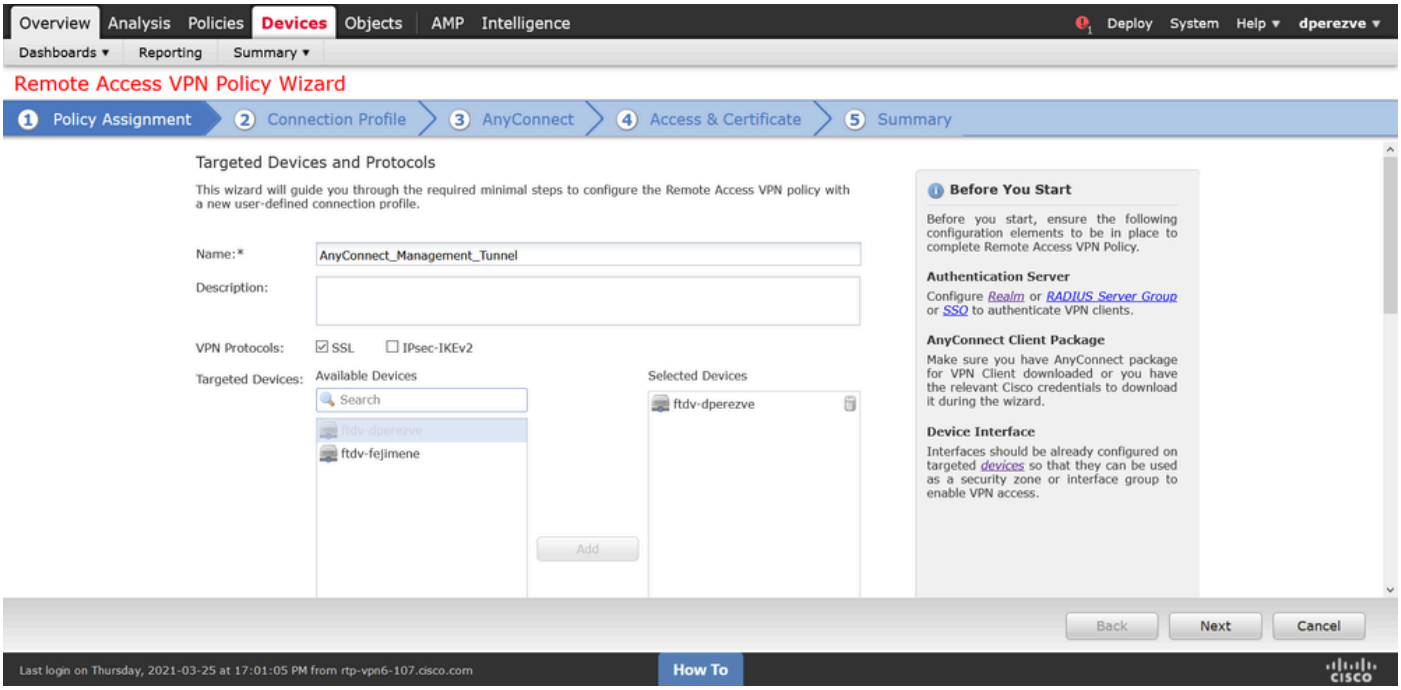


Étape 5. Création d’une configuration AnyConnect

1. La configuration de SSL AnyConnect dans FMC se compose de 4 étapes différentes. Pour configurer AnyConnect, accédez à Devices > VPN > Remote Access et sélectionnez le bouton

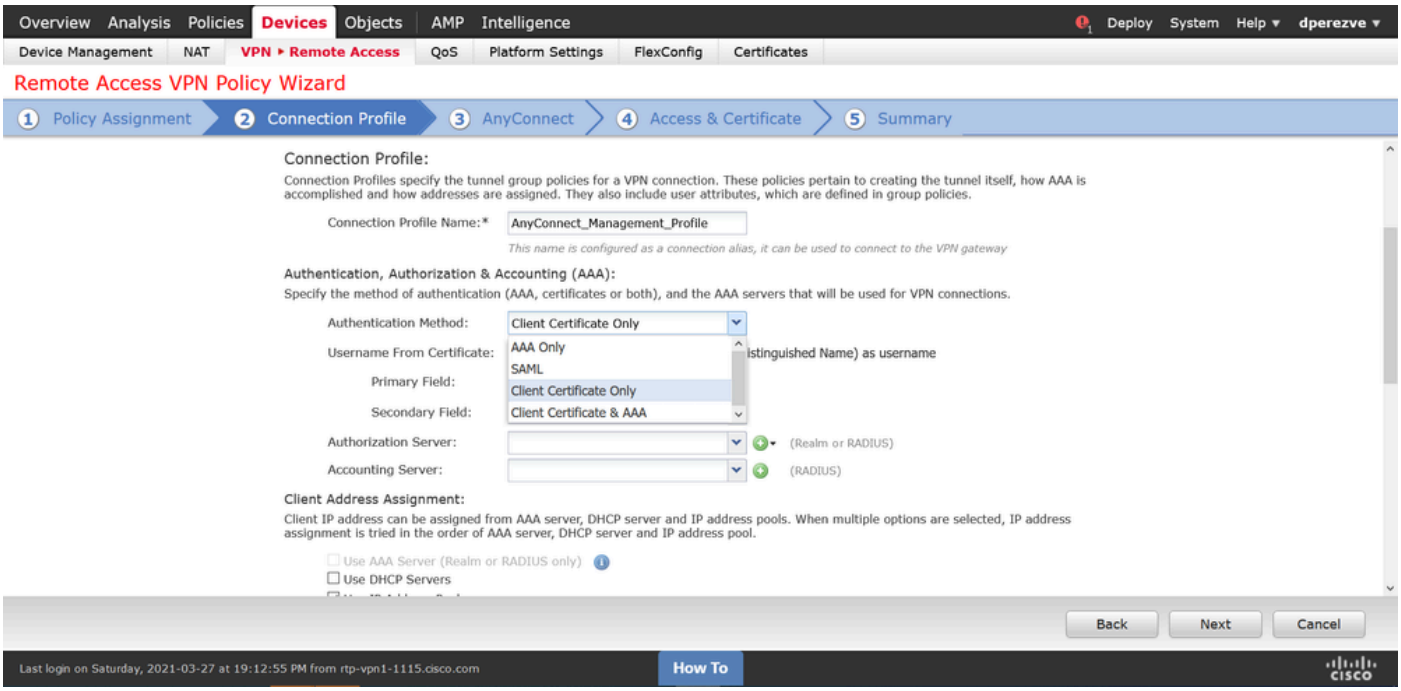
Add. Cette opération doit ouvrir l'Assistant Stratégie VPN d'accès à distance.

2. Sous l'onglet Affectation de stratégie, sélectionnez le périphérique FTD disponible, définissez un nom pour le profil de connexion et cochez la case SSL.

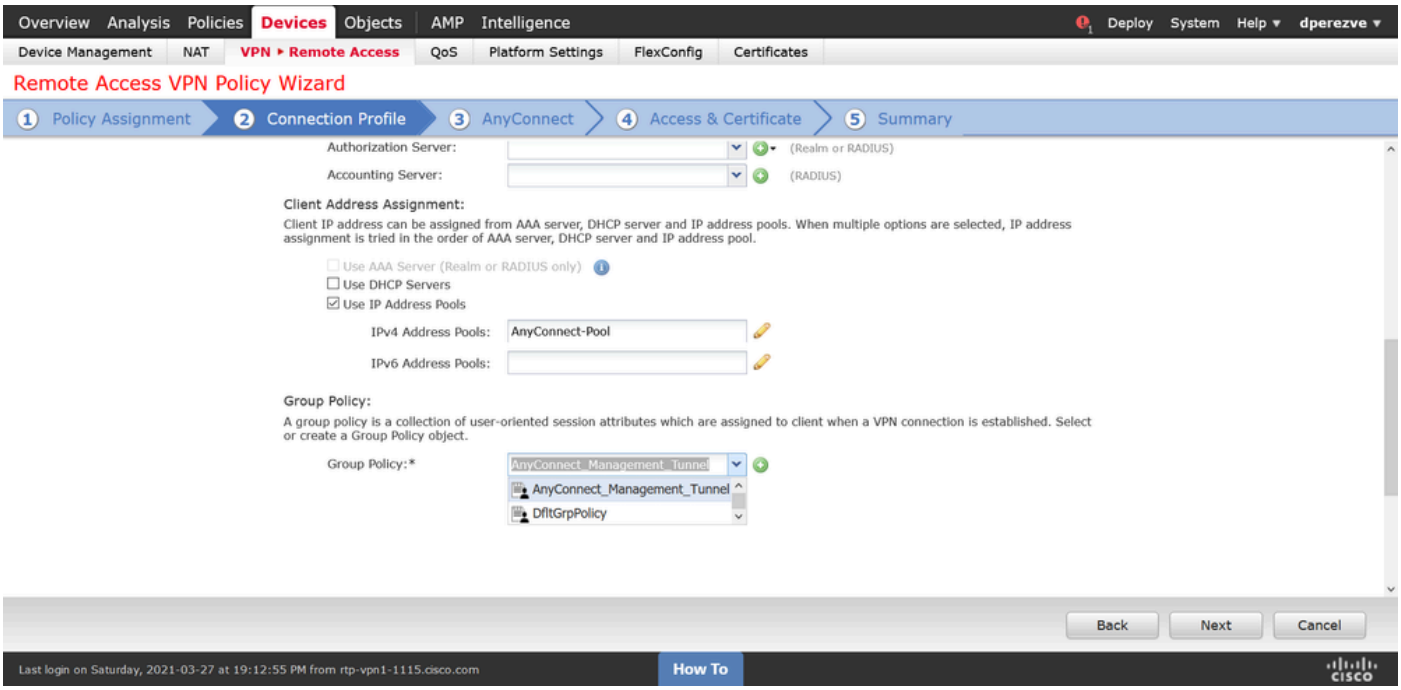


---

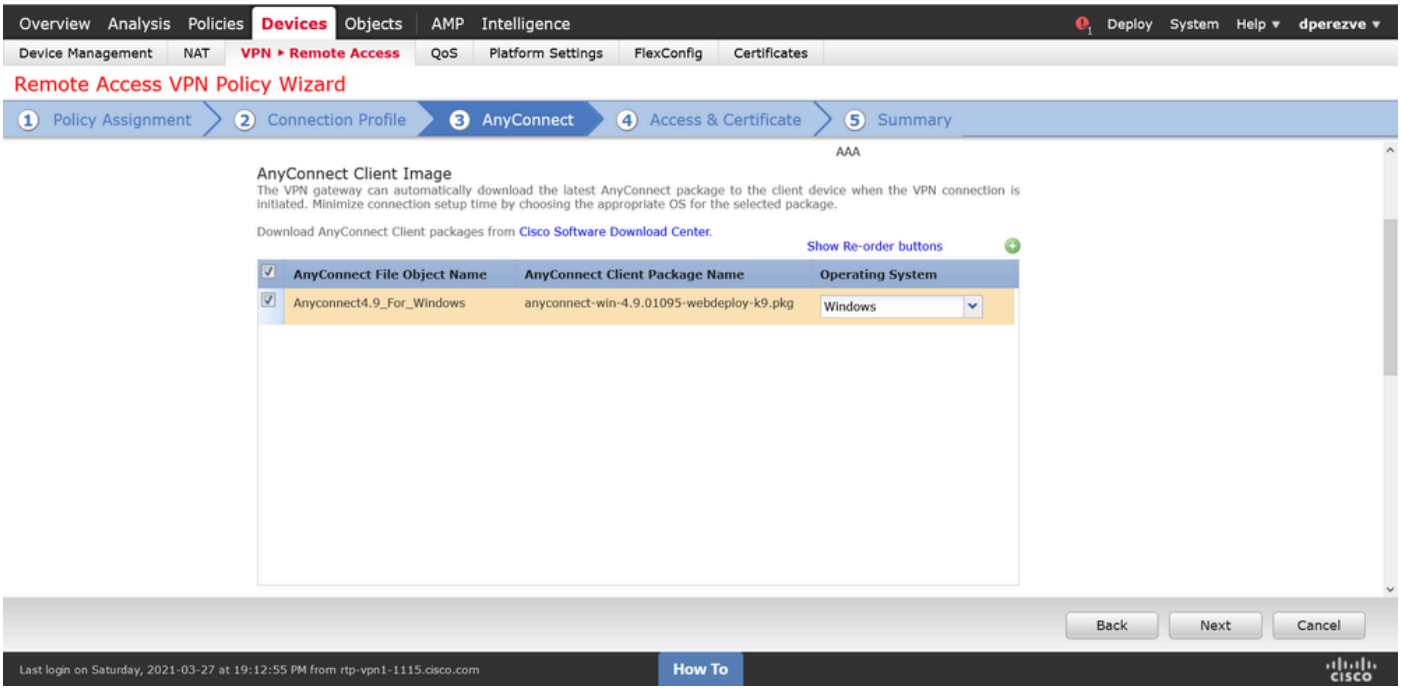
2. Dans le profil de connexion, sélectionnez Client Certificate Only, comme méthode d'authentification. Il s'agit de la seule authentification prise en charge pour la fonctionnalité.



3. Ensuite, sélectionnez l'objet Stratégie de groupe créé à l'étape 3 dans le menu déroulant Stratégie de groupe.



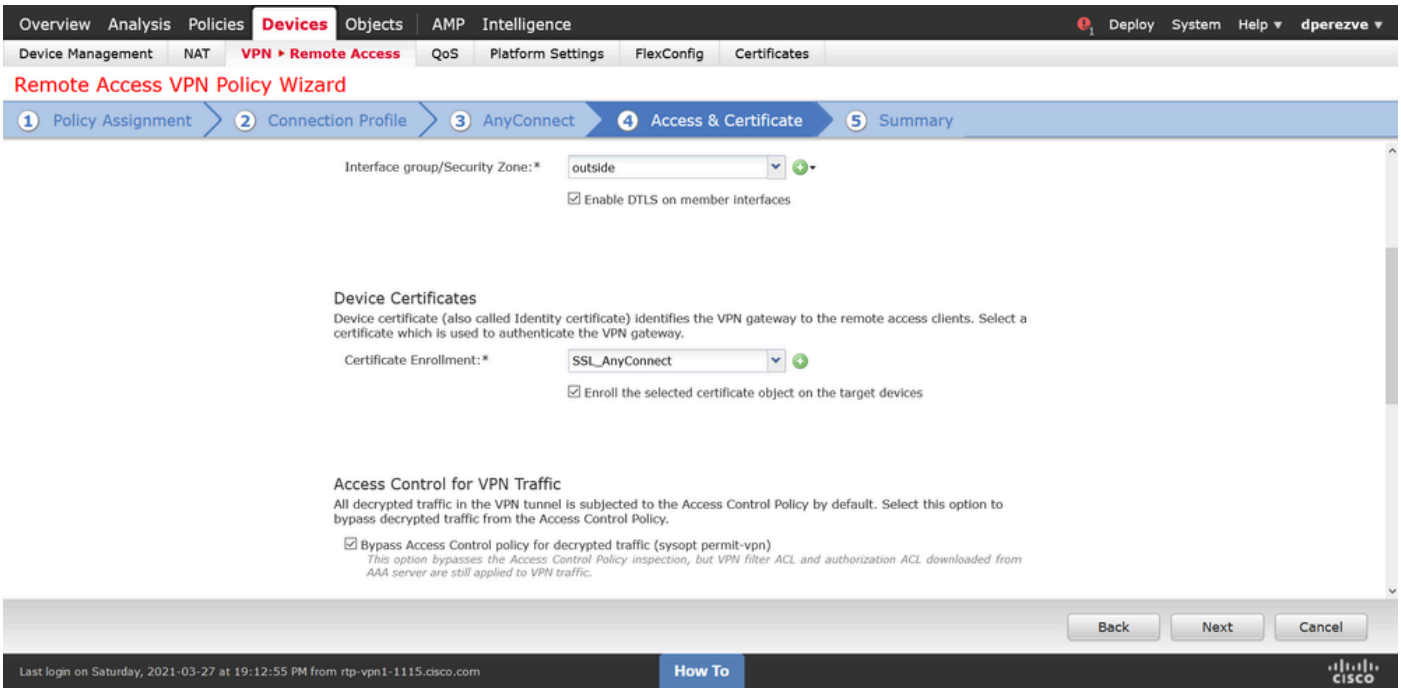
4. Dans l'onglet AnyConnect, sélectionnez l'objet fichier AnyConnect en fonction du système d'exploitation (SE) sur le point d'extrémité.



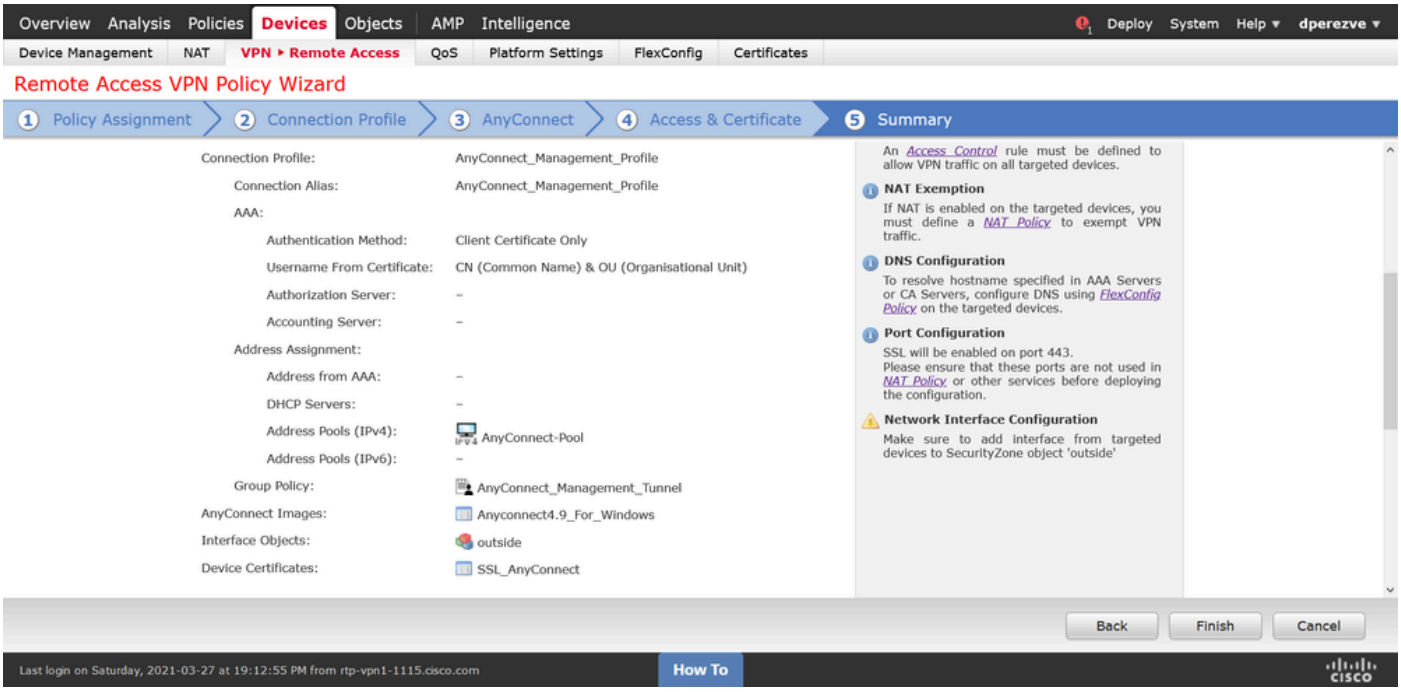
5. Sur le Access & Certificate, spécifiez le certificat qui doit être utilisé par le FTD pour sonder son identité au client Windows.

Remarque : Étant donné que les utilisateurs ne peuvent pas interagir avec l'application AnyConnect lorsqu'ils utilisent la fonctionnalité VPN de gestion, le certificat doit être entièrement fiable et ne doit pas imprimer de message d'avertissement.

Remarque : Pour éviter les erreurs de validation de certificat, le champ Common Name (CN) inclus dans le champ Subject Name du certificat doit correspondre au nom de domaine complet défini dans la liste de serveurs des profils XML (étapes 1 et 2).



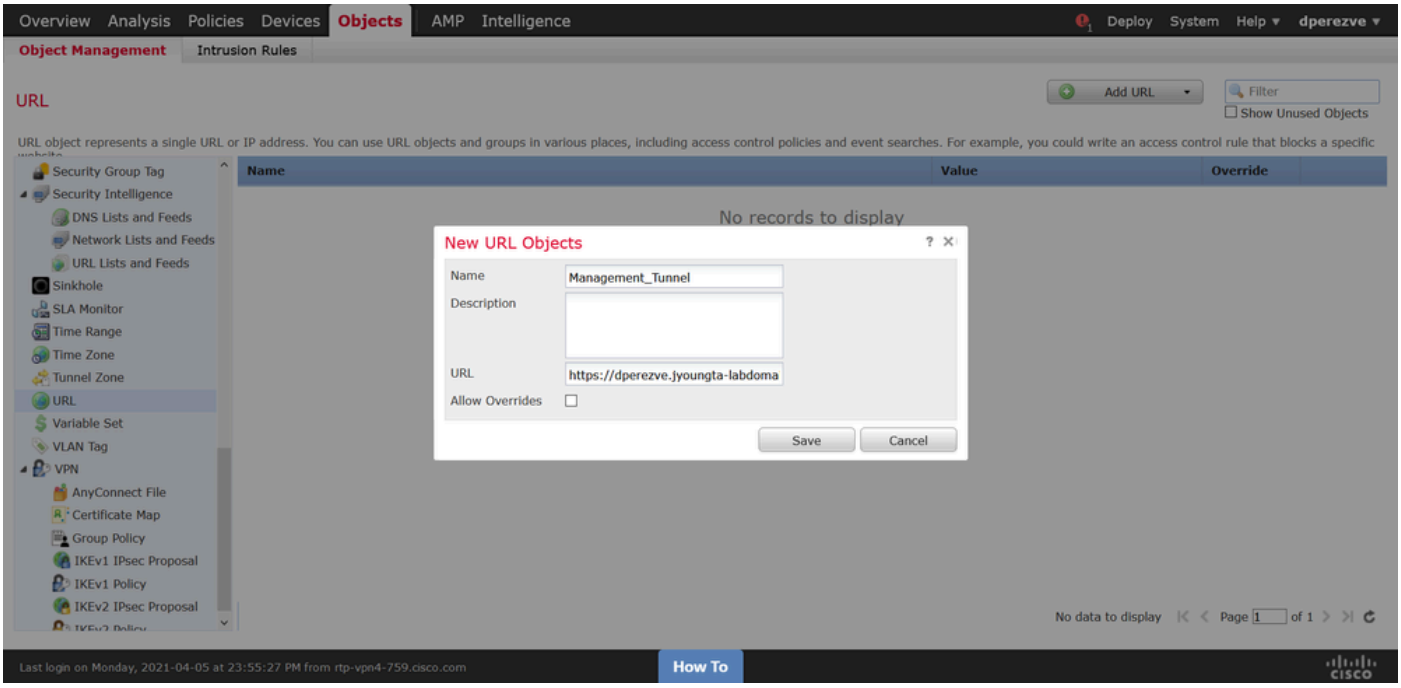
6. Enfin, sélectionnez le bouton Finish sur l'onglet Summary pour ajouter la nouvelle configuration AnyConnect.



Étape 6. Créer un objet URL

1. Accédez à Objets > Gestion des objets et sélectionnez URL dans la table des matières. Sélectionnez ensuite Add Object dans le menu déroulant Add URL.

2. Attribuez un nom à l'objet et définissez l'URL en utilisant le même nom de domaine complet/groupe d'utilisateurs que celui spécifié dans la liste des serveurs de profils VPN de gestion (étape 2). Dans cet exemple, l'URL doit être dperezve.jyoungta-labdomain.cisco.com/AnyConnect_Management_Tunnel.



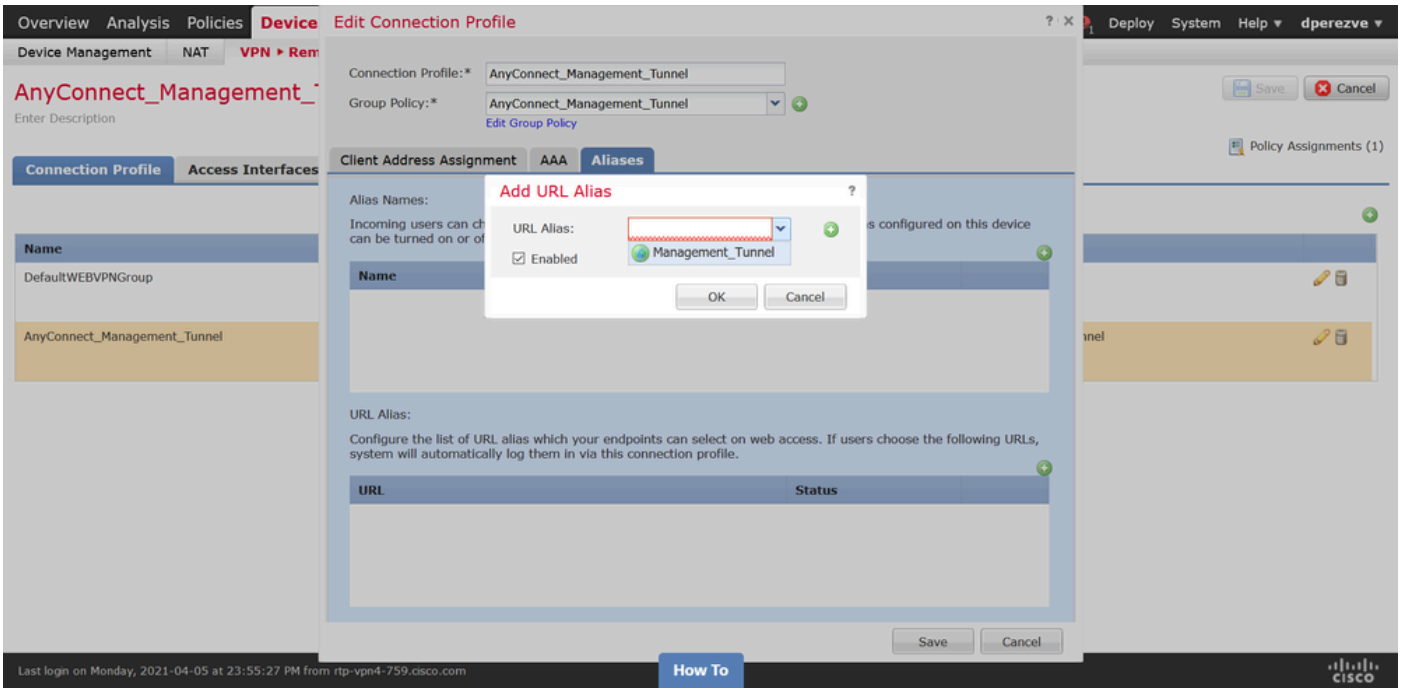
---

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

Étape 7. Définir un alias d'URL

1. Pour activer l'alias d'URL dans la configuration AnyConnect, accédez à Devices > VPN > Remote Access et cliquez sur l'icône de crayon pour modifier.

2. Dans l'onglet Profil de connexion, sélectionnez la configuration disponible, accédez à Alias, cliquez sur le bouton Ajouter. Sélectionnez ensuite l'objet URL dans le menu déroulant Alias URL. Assurez-vous que la case Activé est cochée.



---

3. Enregistrez vos modifications et déployez les configurations sur FTD.

Vérifier

Une fois le déploiement terminé, une première connexion AnyConnect manuelle avec le profil VPN AnyConnect est requise. Au cours de 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 de l'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 de serveurs du profil VPN de gestion et au nom de domaine complet défini dans l'alias d'URL.

Pour le tunnel de gestion non initié :

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

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

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.