Configuration du VPN d'accès à distance Secure Client (AnyConnect) sur FTD

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configuration
  - 1.Conditions préalables
    - a) Importer le certificat SSL
    - b) Configurer le serveur RADIUS
    - c) Créer un pool d'adresses pour les utilisateurs VPN
    - d) Créer un profil XML
    - e) Télécharger des images AnyConnect
  - 2. Assistant Accès à distance
- Connexion
- Limites
- Considérations de sécurité
  - a) Activer uRPF
  - b) Activez la connexion sysopt permit-vpnOption
- Informations connexes

Introduction

Ce document décrit la configuration du VPN d'accès à distance Secure Client (AnyConnect) sur Secure Firewall Threat Defense.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base en matière de VPN, TLS et IKEv2

- Connaissances de base en authentification, autorisation et comptabilité (AAA) et RADIUS
- Expérience avec Secure Firewall Management Center

Composants utilisés

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

- Protection pare-feu contre les menaces (SFTD) 7.2.5
- Centre de gestion du pare-feu sécurisé (SFMC) 7.2.9
- Client sécurisé (AnyConnect) 5.1.6

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 Secure Firewall Threat Defense (FTD) version 7.2.5 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, Secure Client (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 le Centre de gestion du pare-feu sécurisé :

- 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 lors de la configuration du client sécurisé. Le certificat doit avoir une extension Subject Alternative Name avec un nom DNS et/ou une adresse IP pour éviter les 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 :

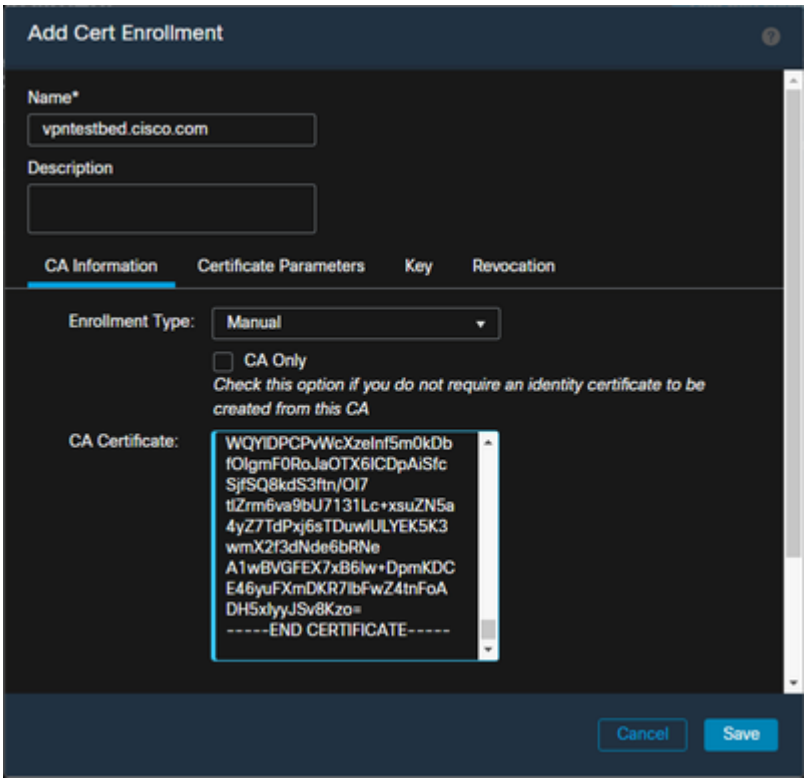
- Sur SFTD, vous avez besoin du certificat CA avant de générer le CSR.
- Si la CSR est générée en externe, la méthode manuelle échoue. Par conséquent, une autre méthode doit être utilisée (PKCS12).

Il existe plusieurs méthodes pour obtenir un certificat sur l'appliance SFTD, mais la méthode la plus sûre et la plus simple consiste à créer une demande de signature de certificat (CSR), à la signer avec une autorité de certification (CA), puis à importer le certificat émis pour la clé publique, qui se trouvait dans la CSR.

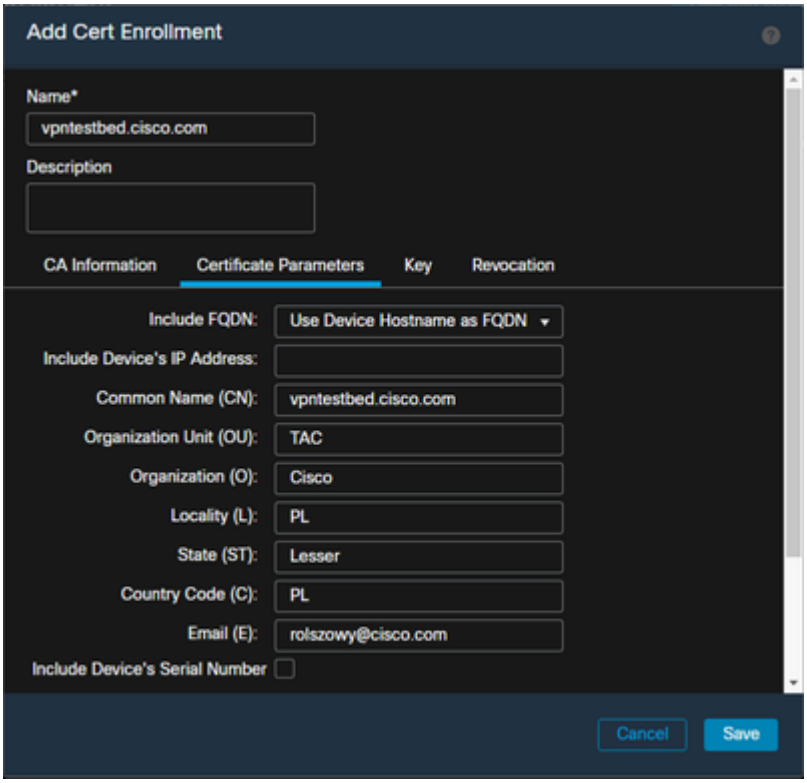
Étapes à suivre :

- Accédez à Objets > Gestion des objets > PKI > Inscription de certificat, cliquez sur Ajouter une inscription de certificat.

- Sélectionnez le type d'inscription et collez le certificat de l'autorité de certification (le certificat utilisé pour signer le CSR).

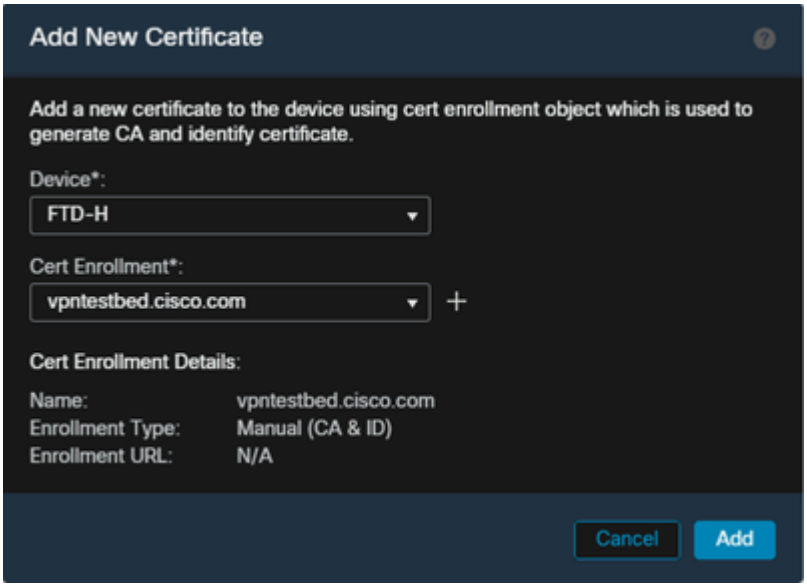


- Ensuite, accédez au deuxième onglet et sélectionnez Custom FQDN et remplissez tous les champs nécessaires, par exemple :

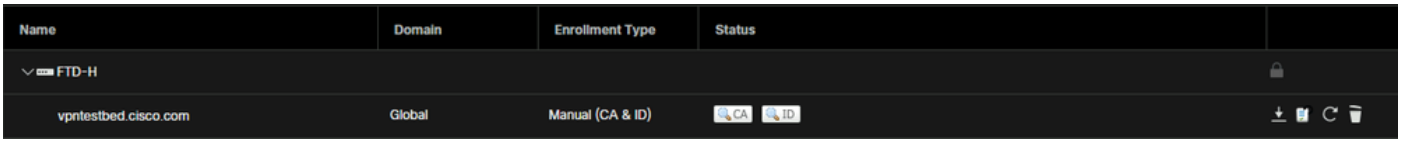


- Dans le troisième onglet, sélectionnez Key Type, choisissez name and size. Pour RSA, 2048 bits est minimum.
- Cliquez sur Save et accédez à Devices > Certificates > Add.

- Sélectionnez ensuite Device, et sous Cert Enrollment, sélectionnez le point de confiance que vous venez de créer, et cliquez sur Add :

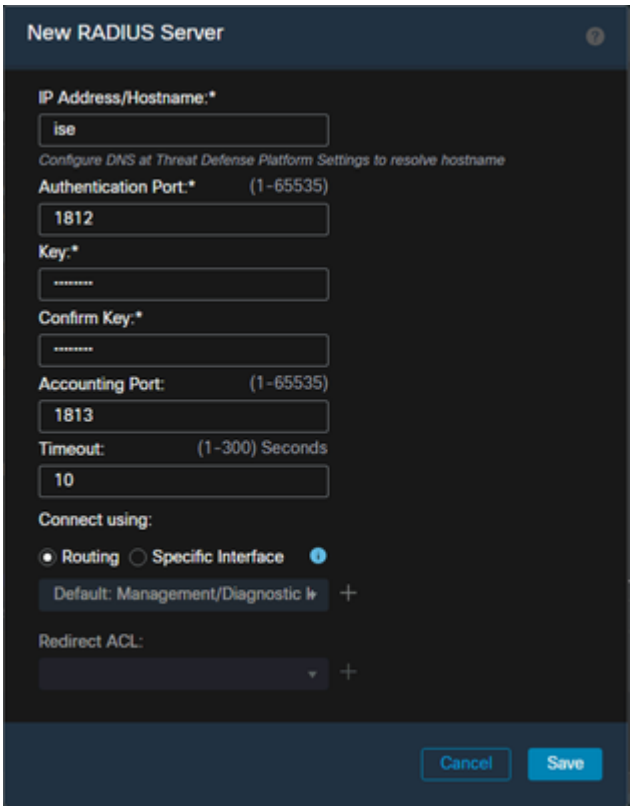


- Plus tard, en regard du nom du point de confiance, cliquez sur le bouton ID , puis Oui, et après cela, copiez CSR dans CA et signez. Les attributs du certificat doivent être identiques à ceux d'un serveur HTTPS normal.
- Après avoir reçu le certificat de l'autorité de certification au format base64,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



b) Configurer le serveur RADIUS

- Accédez à Objets > Gestion des objets > Groupe de serveurs RADIUS > Ajouter un groupe de serveurs RADIUS > +.
- Remplissez le nom et ajoutez l'adresse IP avec le secret partagé et cliquez sur Enregistrer :

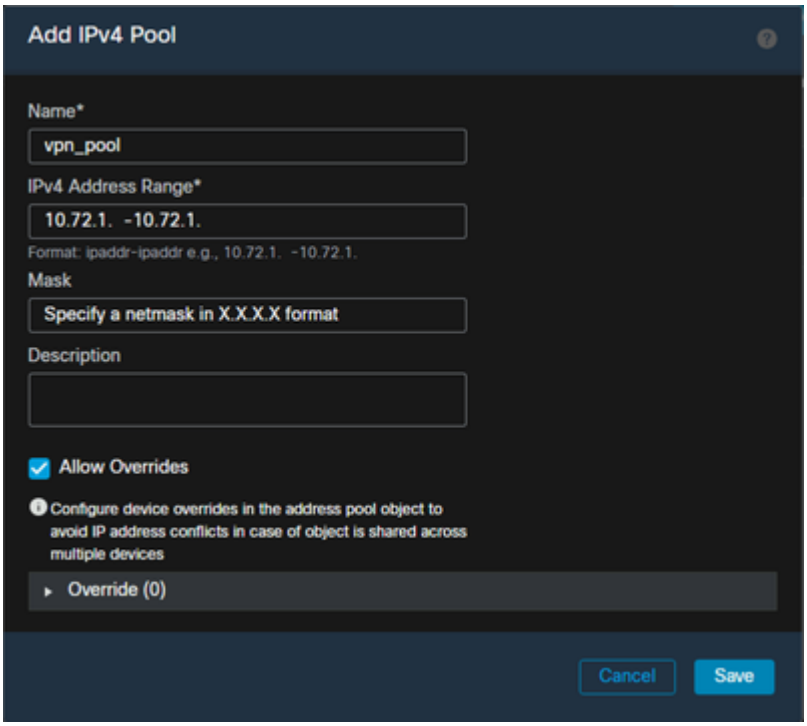


- Après, vous pouvez voir le serveur sur la liste :



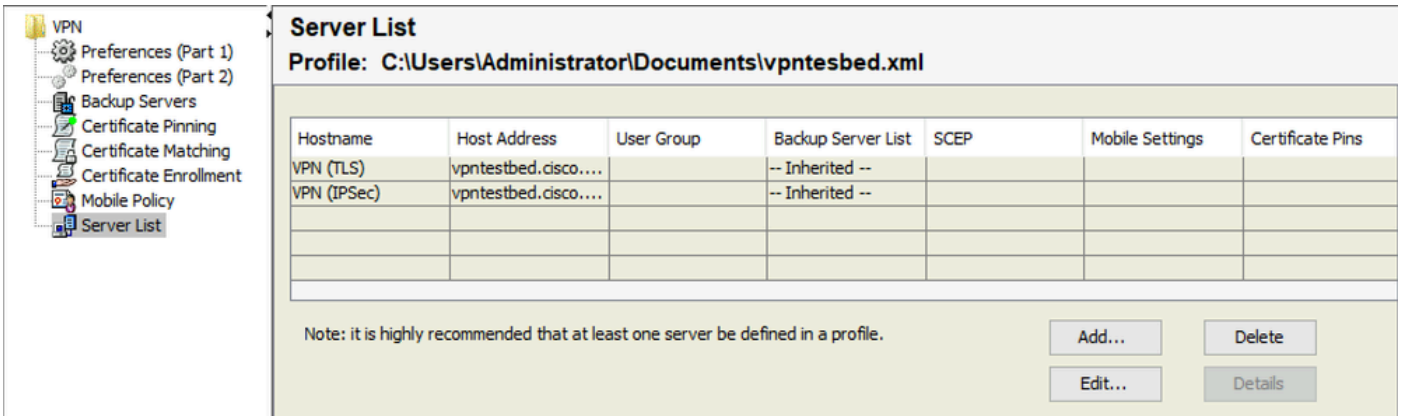
c) Créer un pool d'adresses pour les utilisateurs VPN

- Accédez à Objets > Gestion des objets > Pools d'adresses > Pools IPv4 > Ajouter des pools IPv4.
- Entrez 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.
- Accédez à Liste des serveurs > Ajouter...
- Saisissez le nom d'affichage et le nom de domaine complet. Vous pouvez voir les entrées dans la liste des serveurs :



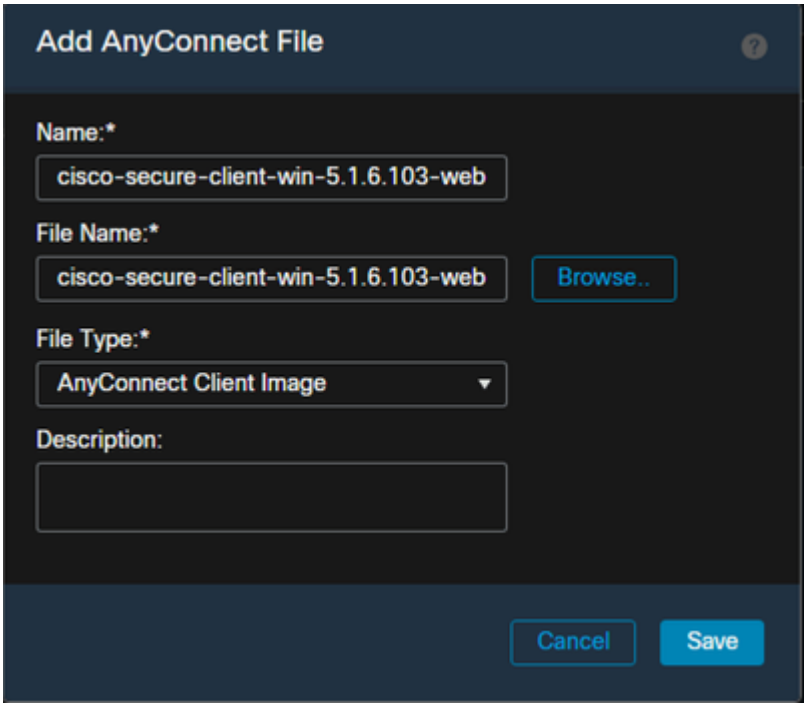
- Cliquez sur OK et File > Save as...

e) Télécharger des images AnyConnect

- Téléchargez des images de pkg depuis le site Cisco.
- Accédez à Objets > Gestion des objets > VPN > Fichier AnyConnect > Ajouter un fichier

AnyConnect.

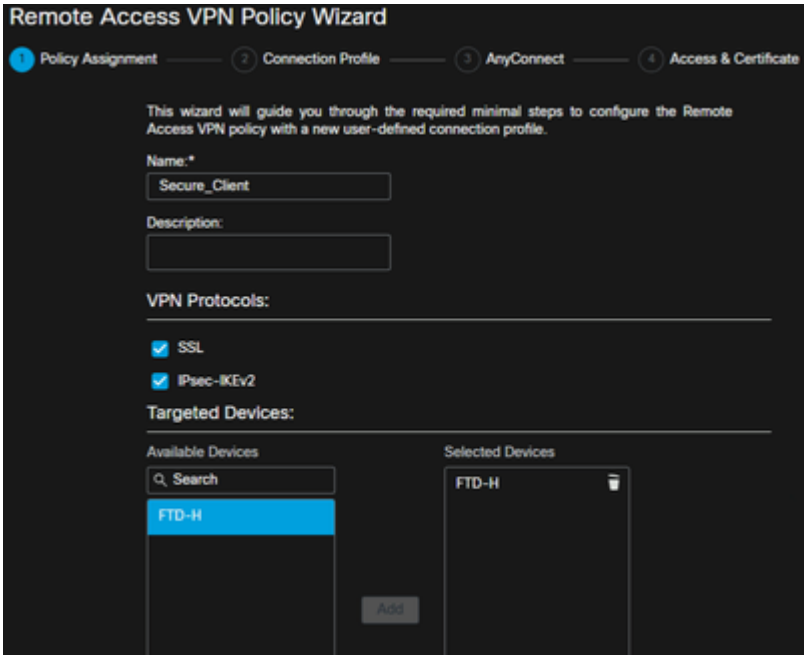
- Tapez le nom et sélectionnez le fichier PKG à partir du disque, cliquez sur Save :



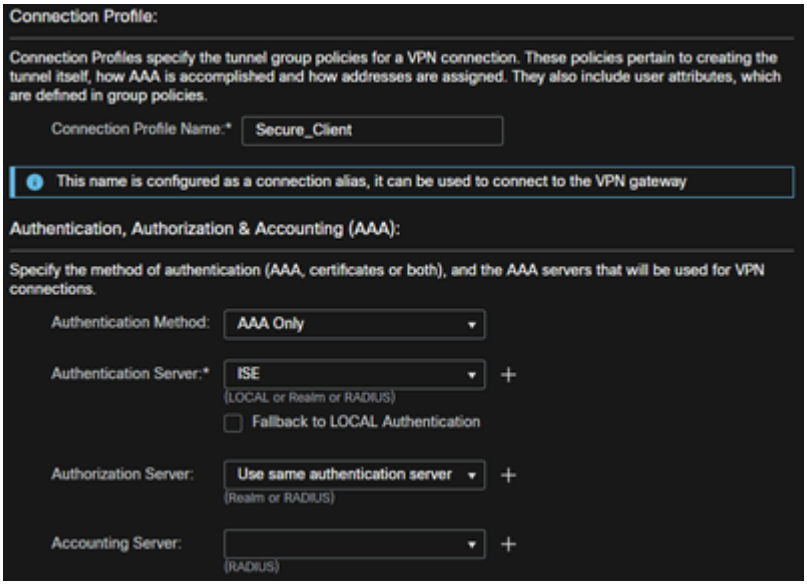
- Ajoutez d'autres packages en fonction de vos propres besoins.

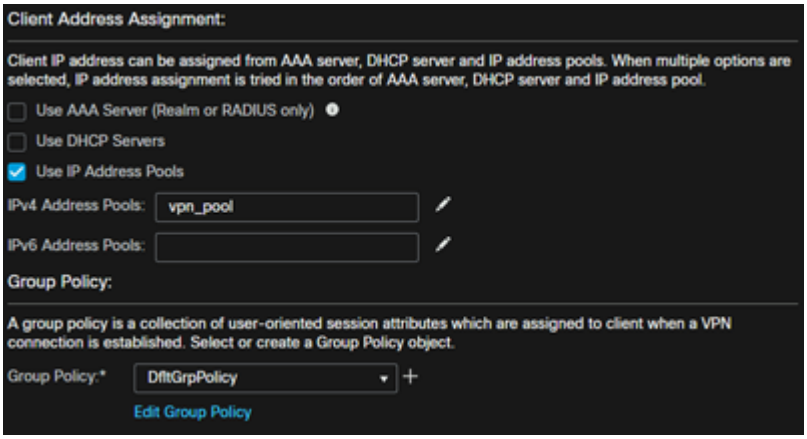
2. Assistant Accès à distance

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

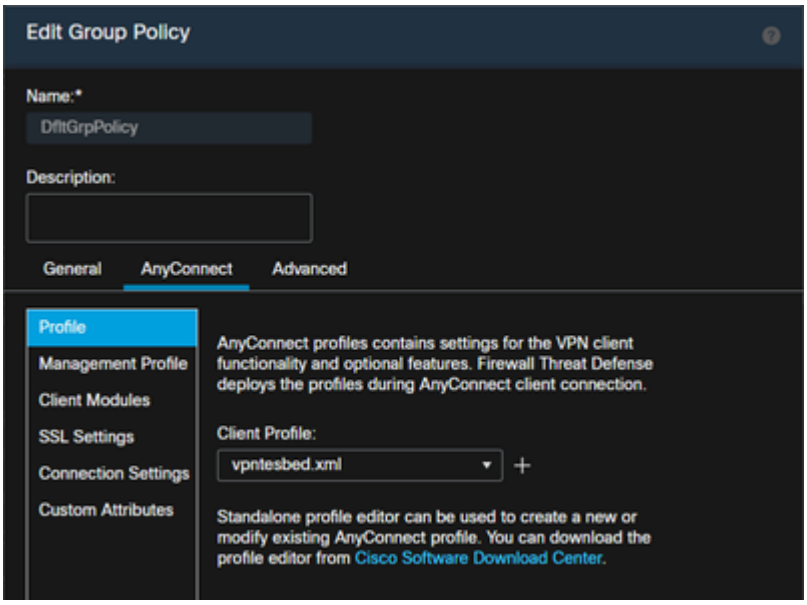


- Dans l'étape Profil de connexion, tapez Nom du profil de connexion, sélectionnez le serveur d'authentification et les pools d'adresses que vous avez créés précédemment :

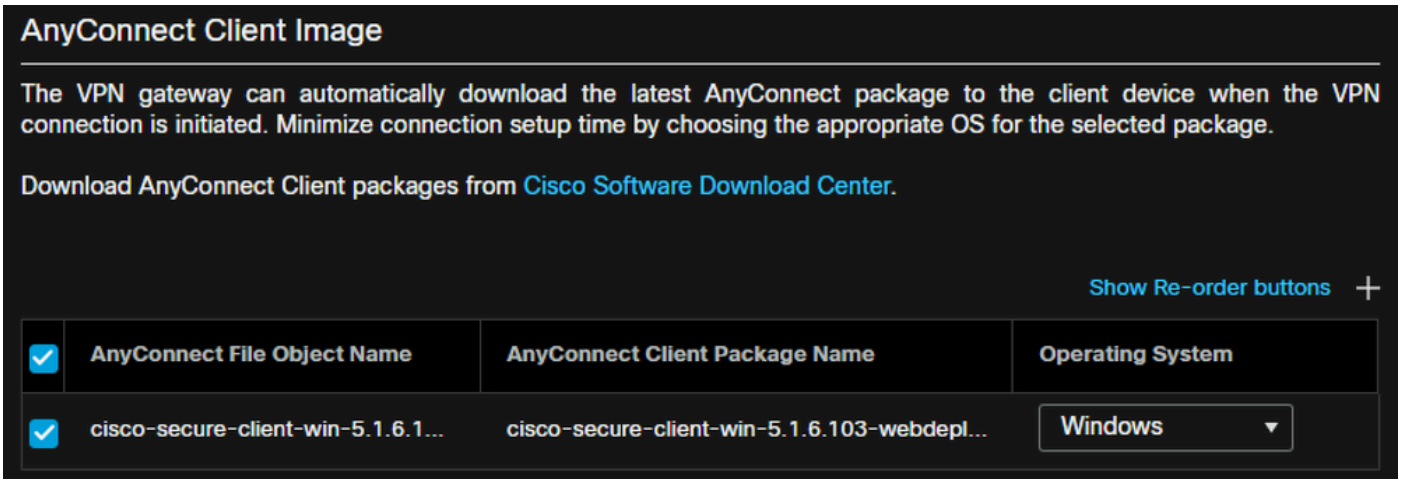




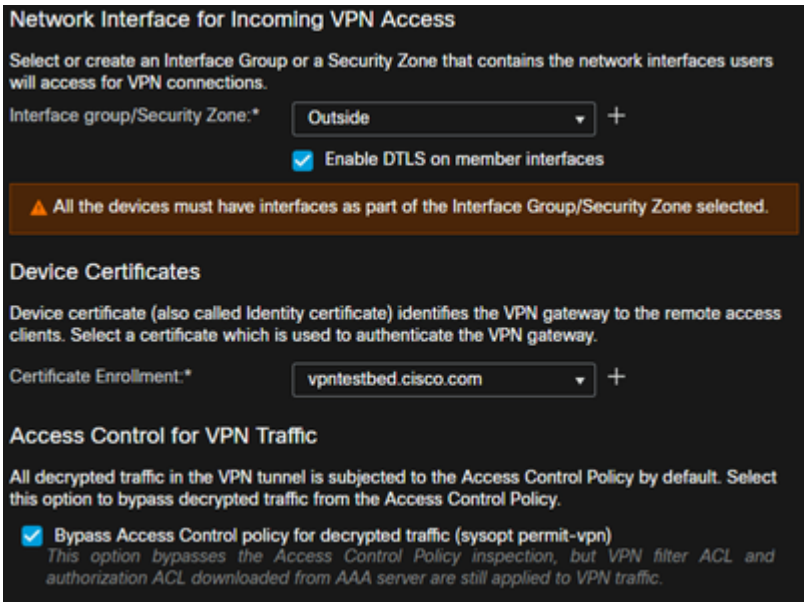
- Cliquez sur Edit Group Policy et dans l'onglet AnyConnect, sélectionnez Client Profile, puis cliquez sur Save :



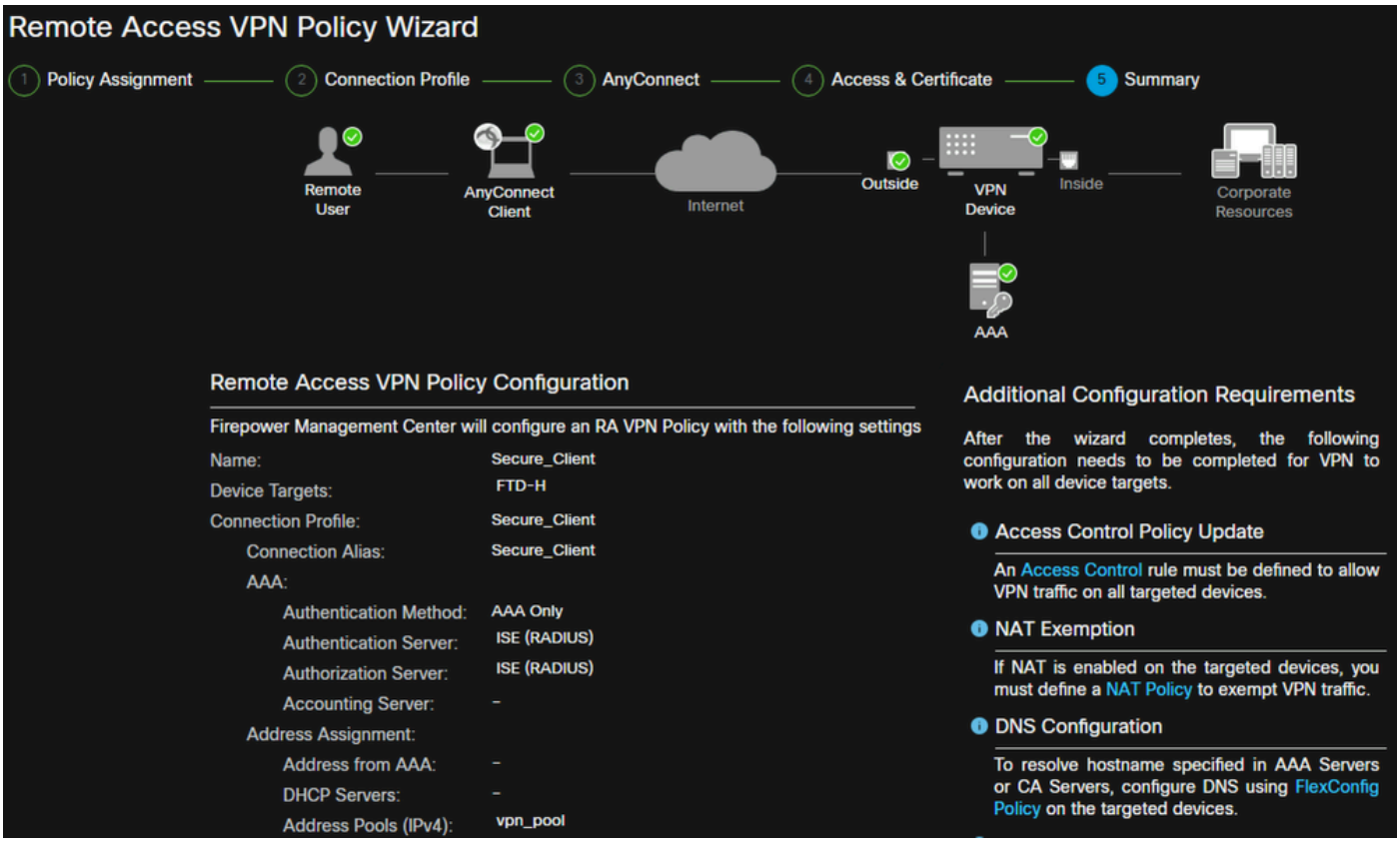
- Sur la page suivante, sélectionnez AnyConnect Images et cliquez sur Next.



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



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



- La configuration complète, ainsi que les certificats et les packages AnyConnect, sont copiés sur le périphérique FTD.

Connexion

Pour vous connecter à FTD, vous devez ouvrir un navigateur, taper le nom DNS ou l'adresse IP qui pointe vers l'interface externe. Connectez-vous ensuite avec les informations d'identification stockées sur le serveur RADIUS et effectuez les étapes à l'écran. Une fois AnyConnect installé, vous devez entrer la même adresse dans la fenêtre AnyConnect, puis cliquez sur Connect.

Limites

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

- FTDposture VPN 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 (amélioration : ID de bogue Cisco CSCvt58044)
- Localisation AnyConnect
- Intégration WSA
- Carte de cryptage dynamique IKEv2 simultanée pour les VPN RA et L2L (amélioration : ID de bogue Cisco CSCvr52047)
- TACACS, Kerberos - Authentification KCD et RSA SDI (amélioration : ID de bogue Cisco CSCvx55859)
- Proxy du navigateur

Considérations de sécurité

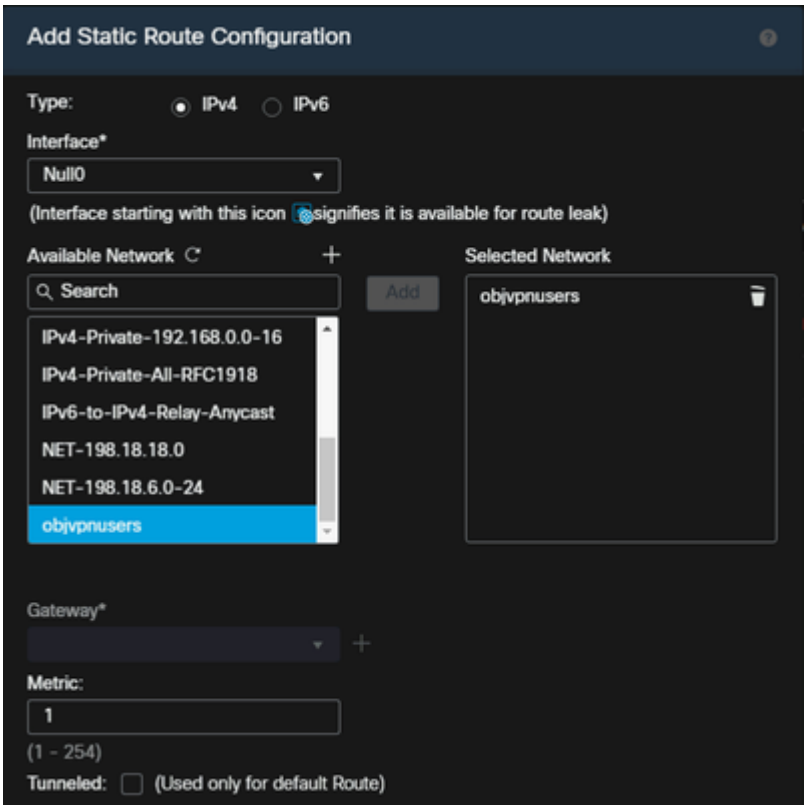
Par défaut, la connexion sysopt permit-vpnoption est désactivée. Cela signifie que vous devez autoriser le trafic provenant du pool d'adresses sur une interface externe via la politique de contrôle d'accès. Bien que la règle de préfiltrage ou de contrôle d'accès soit ajoutée pour autoriser uniquement 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-Spoofing (sur ASA, il était connu sous le nom de Unicast Reverse Path Forwarding - uRPF) pour l'interface externe, et deuxièmement, est d'activer la connexion sysopt 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.

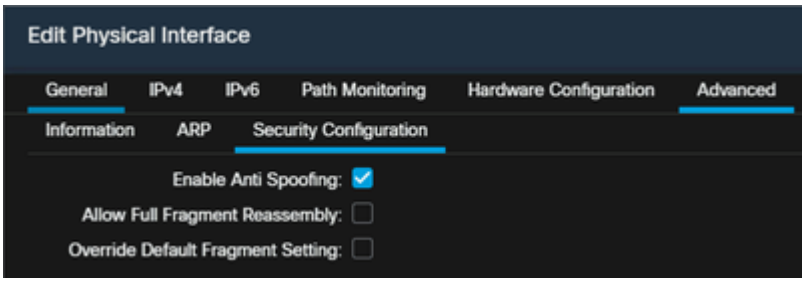
a) Activer uRPF

- Créez une route Null pour le réseau utilisé pour les utilisateurs d'accès à distance, défini dans la section C. Accédez à Périphériques > Gestion des périphériques > Modifier >

Routage > Route statique et sélectionnez Ajouter une route.



- Activez ensuite uRPF sur l'interface où se terminent les connexions VPN. Pour le trouver, accédez à Périphériques > Gestion des périphériques > Modifier > Interfaces > Modifier > Avancé > Configuration de la sécurité > Activer l'anti-usurpation.

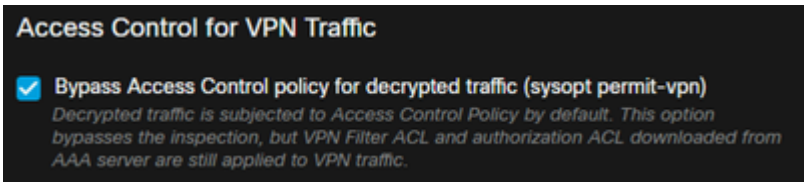


Lorsqu'un utilisateur est connecté, la route 32 bits est installée pour cet utilisateur dans la table de routage. Trafic en texte clair provenant des autres adresses IP inutilisées du pool qui est abandonné par uRFP. Pour afficher une description de l'anti-usurpation, référez-vous à Définir les paramètres de configuration de sécurité sur la défense contre les menaces de pare-feu.

b) Activez l'option de connexion sysopt permit-vpn

- Vous pouvez utiliser l'assistant ou sélectionner Périphériques > VPN > Accès à distance >

Profil VPN > Interfaces d'accès.



Informations connexes

- Assistance technique de Cisco et téléchargements

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.