Configurer un VPN d'accès à distance sur FTD géré par FDM

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
  - Licences
- Informations générales
- Configurer
  - Diagramme du réseau
  - Vérification des licences sur le FTD
  - Définition des réseaux protégés
  - Créer des utilisateurs locaux
  - Ajouter un certificat
  - Configuration du VPN d'accès distant
- Vérifier
- Dépannage
  - Problèmes du client AnyConnect
  - Problèmes de connectivité initiaux
  - Problèmes spécifiques au trafic

Introduction

Ce document décrit comment configurer le déploiement d'un RAVPN sur FTD géré par le gestionnaire FDM sur le routeur qui exécute la version 6.5.0 et ultérieure.

Conditions préalables

Exigences

Cisco recommande que vous ayez connaissance de la configuration du réseau privé virtuel d'accès à distance (RAVPN) sur Firepower Device Manager (FDM).

Composants utilisés

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

- Cisco Firepower Threat Defense (FTD) qui exécute la version 6.5.0-115
- Client de mobilité sécurisée Cisco AnyConnect, version 4.7.01076

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.

Licences

- Firepower Threat Defense enregistré sur le portail de licences Smart avec les fonctionnalités d'exportation contrôlée activées (afin de permettre l'activation de l'onglet de configuration RAVPN)
- Toutes les licences AnyConnect activées (APEX, Plus ou VPN uniquement)

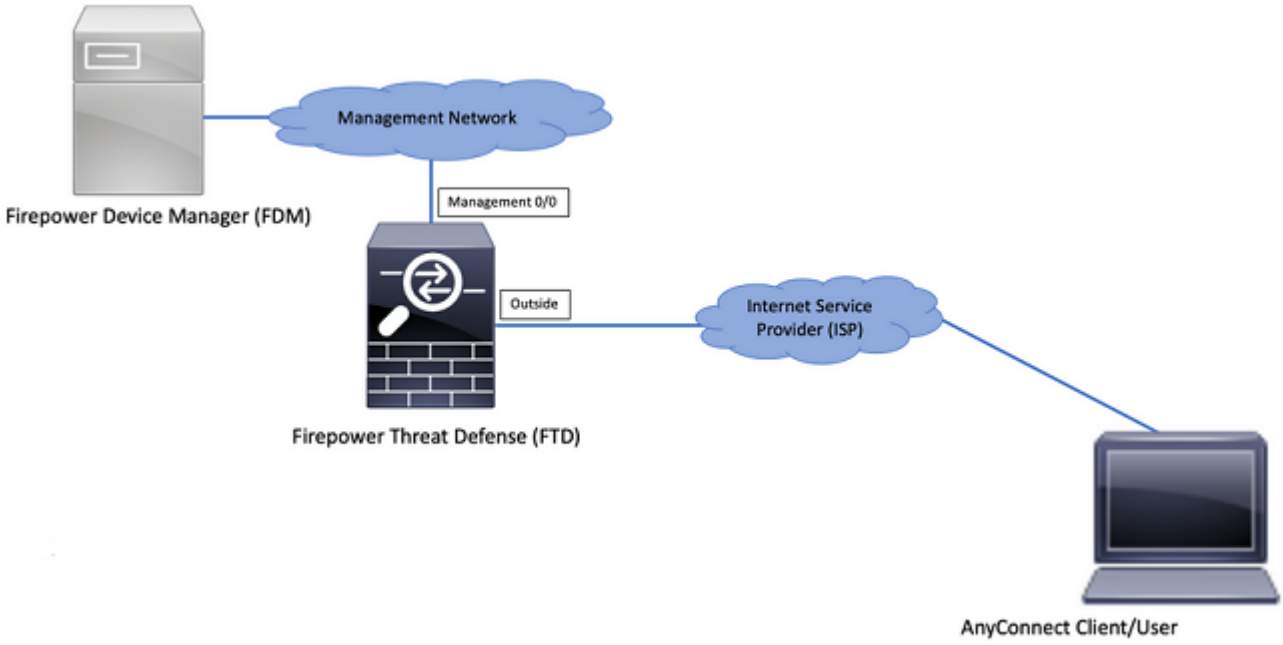
Informations générales

La configuration de FTD via FDM pose des difficultés lorsque vous tentez d'établir des connexions pour des clients AnyConnect via l'interface externe alors que la gestion est accessible via la même interface. Il s'agit d'une limitation connue de la FDM. L'ID de bogue Cisco CSCvm76499 de la demande d'amélioration a été déposé pour ce problème.

Configurer

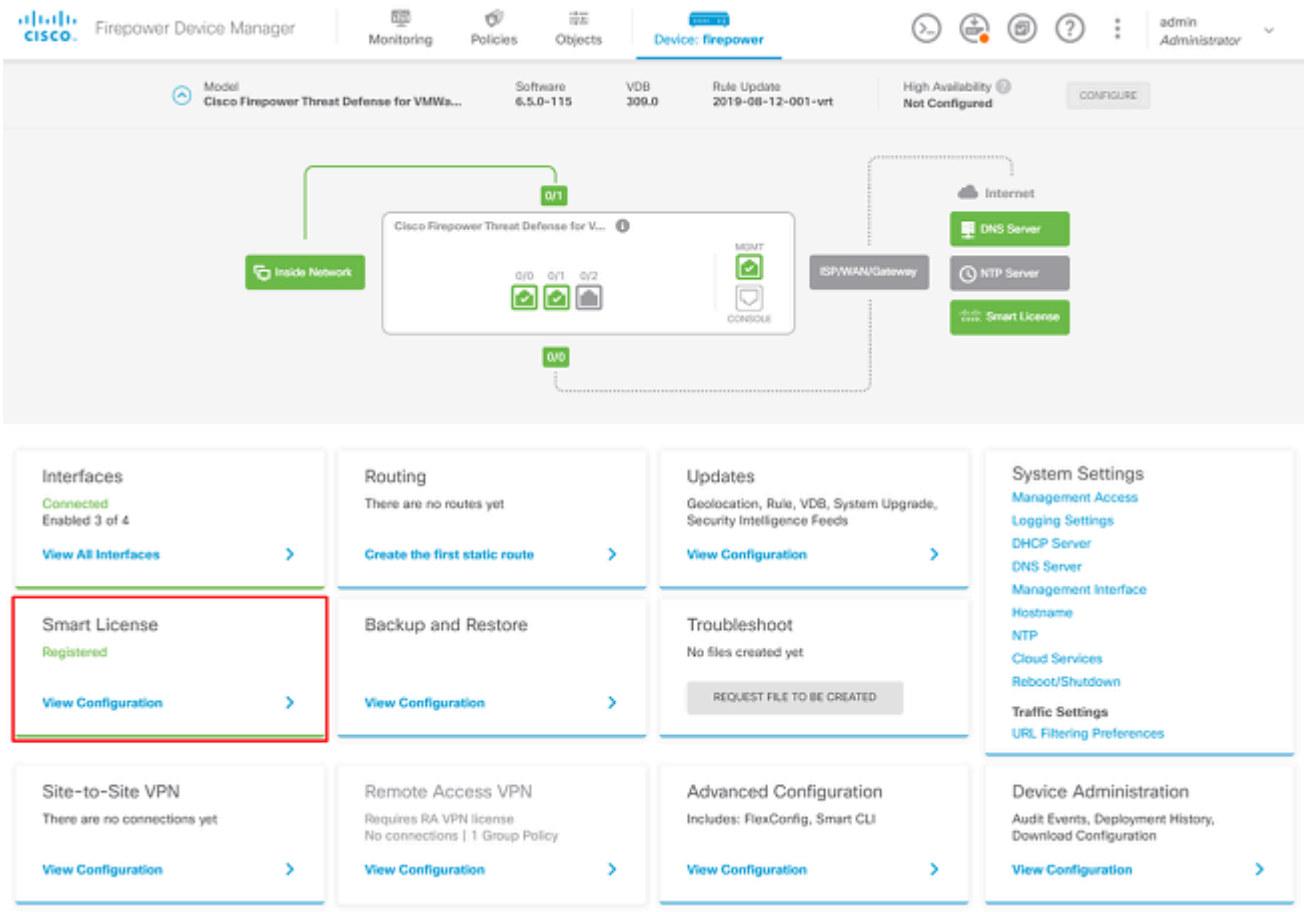
Diagramme du réseau

Authentification client AnyConnect avec l’utilisation de Local.



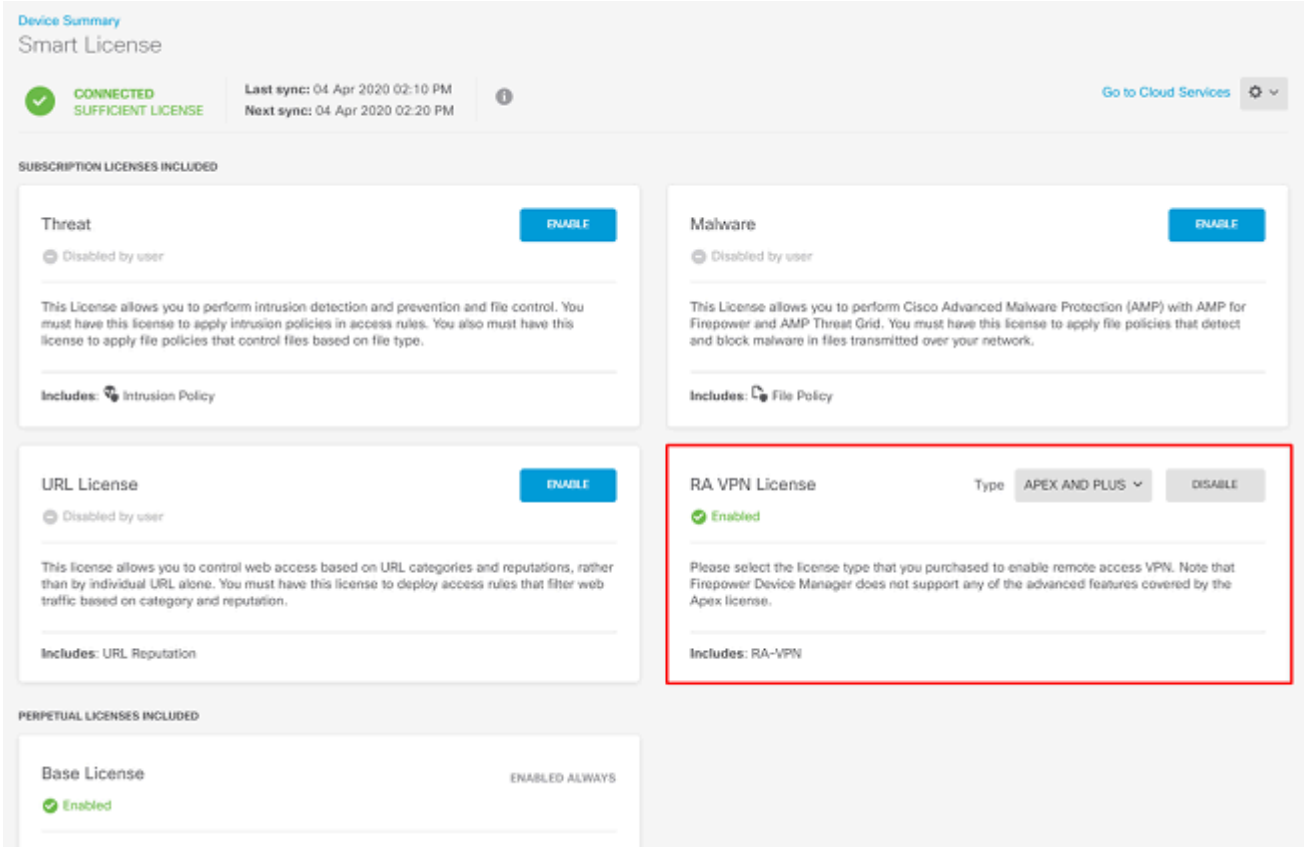
Vérification des licences sur le FTD

Étape 1 : vérification de l'enregistrement du périphérique dans Smart Licensing (voir l'image)

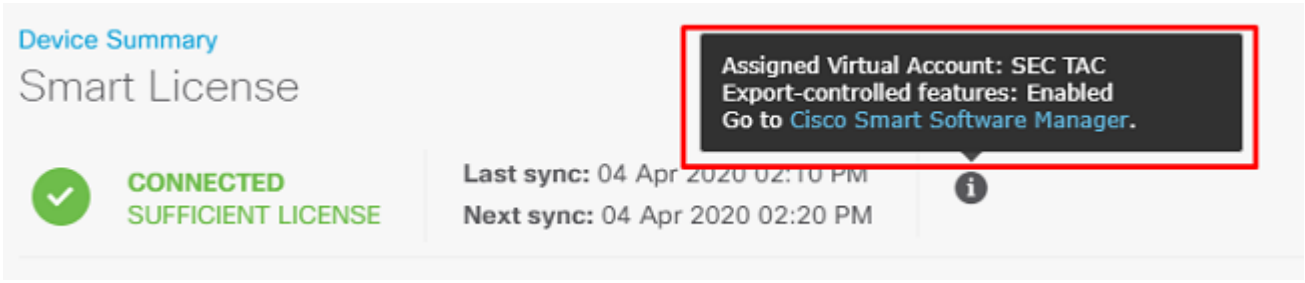


Étape 2. Vérifiez que les licences AnyConnect sont activées sur le périphérique, comme indiqué

dans l'image.

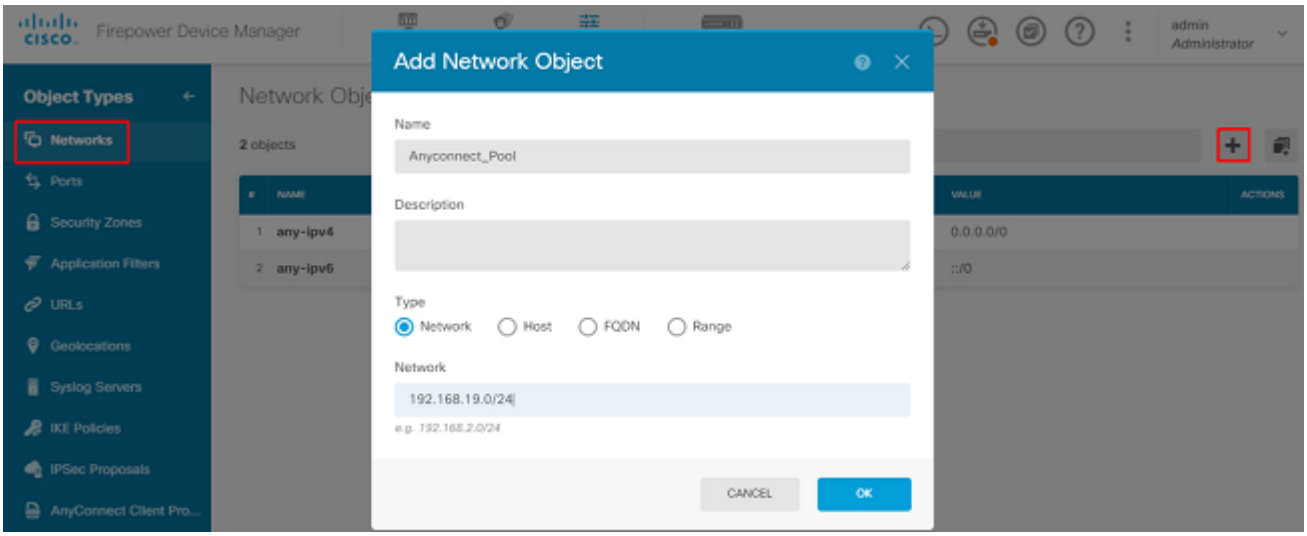


Étape 3. Vérifiez que les fonctionnalités d'exportation contrôlée sont activées dans le jeton, comme indiqué dans l'image.

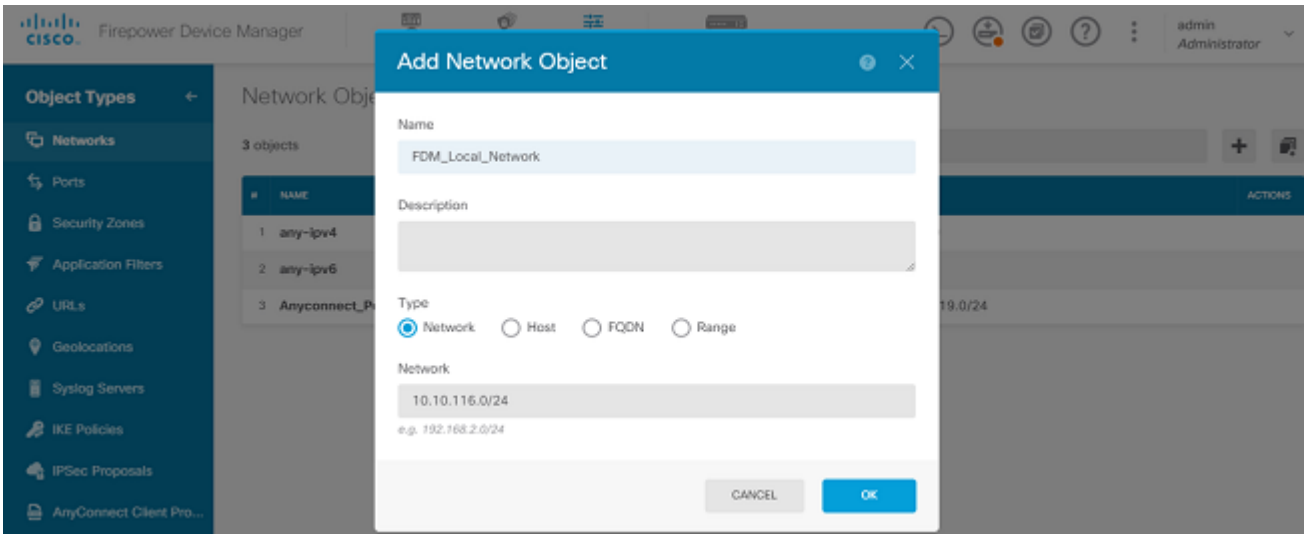


Définition des réseaux protégés

Accédez à Objects > Networks > Add new Network. Configurez le pool VPN et les réseaux LAN à partir de l'interface utilisateur graphique de FDM. Créez un pool VPN afin d'être utilisé pour l'attribution d'adresses locales aux utilisateurs AnyConnect, comme illustré dans l'image.

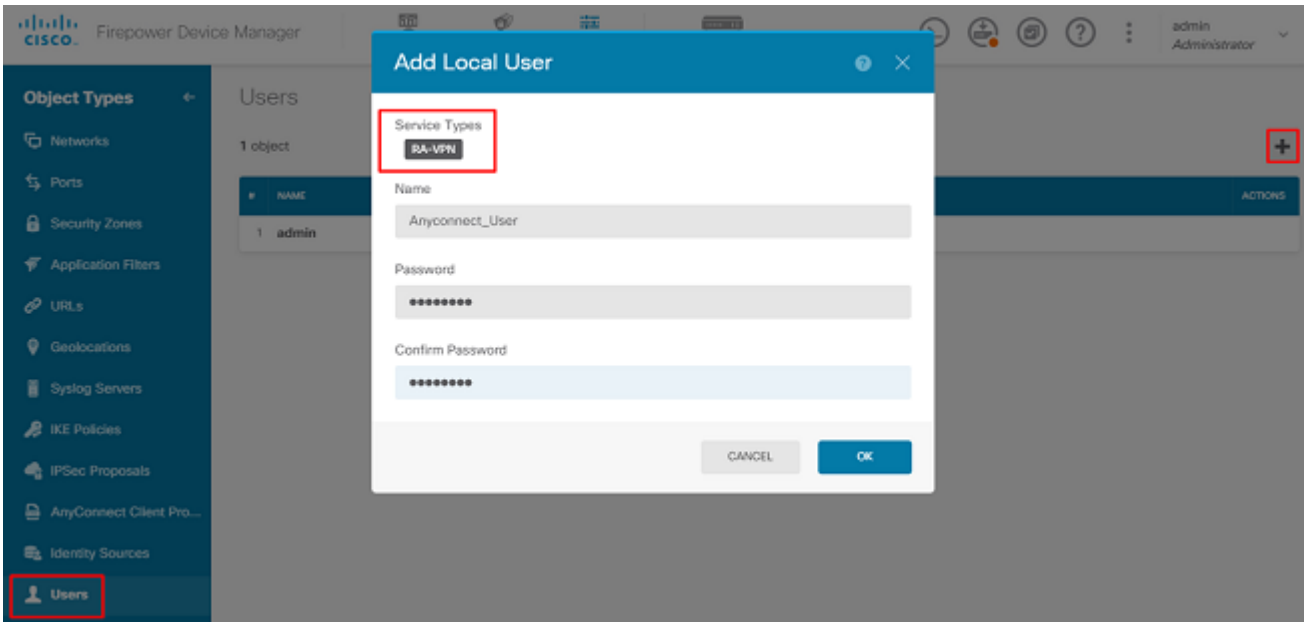


Créez un objet pour le réseau local derrière le périphérique FDM, comme illustré dans l'image.



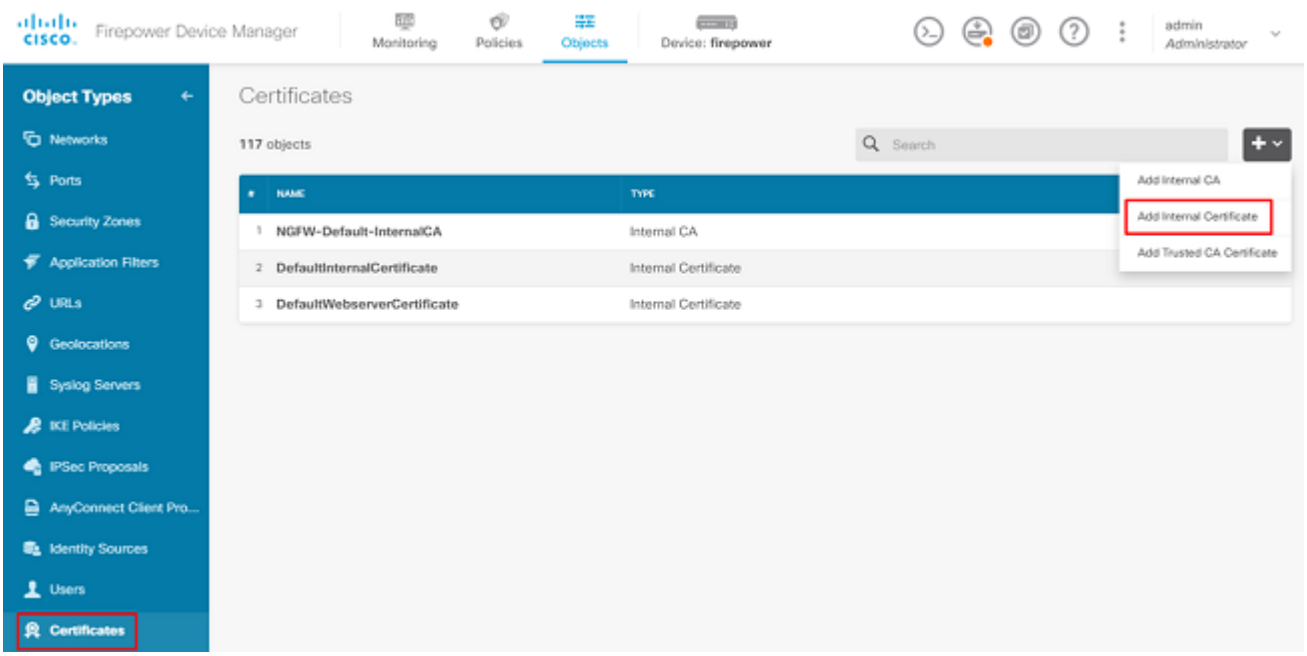
Créer des utilisateurs locaux

Accédez à Objects > Users > Add User. Ajoutez des utilisateurs VPN locaux qui se connectent à FTD via AnyConnect. Créez des utilisateurs locaux comme illustré dans l'image.

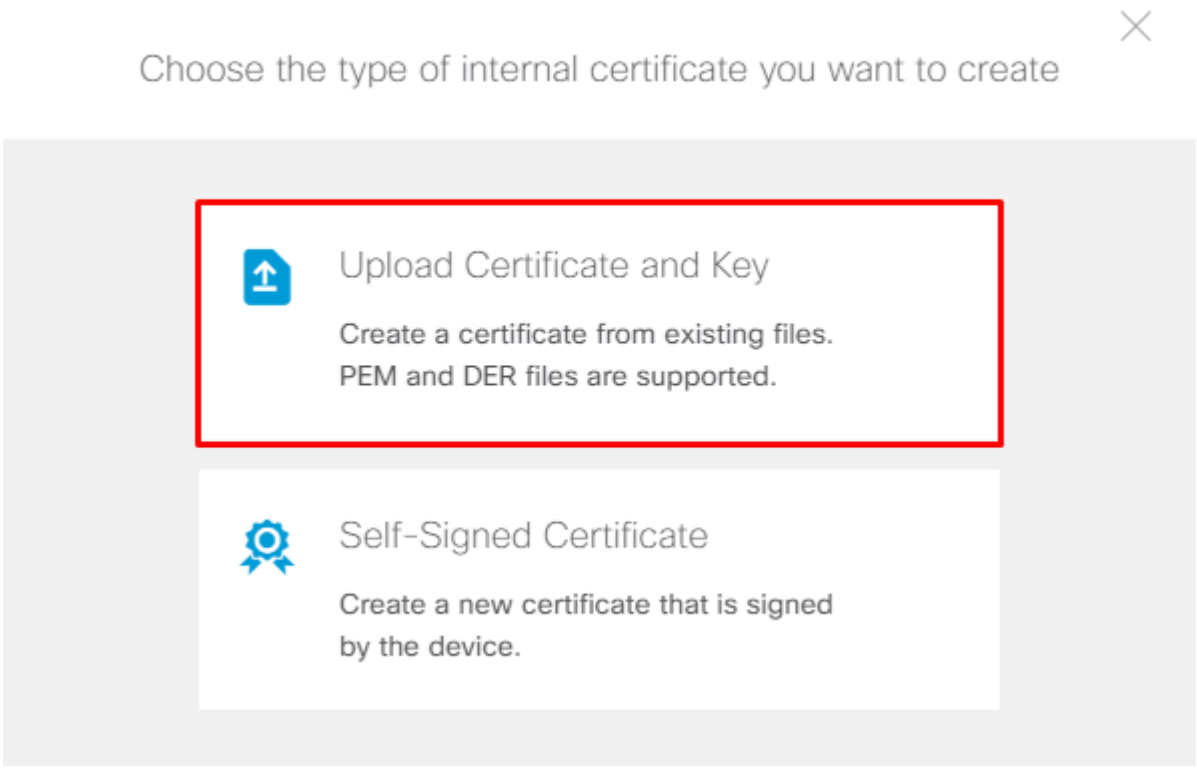


Ajouter un certificat

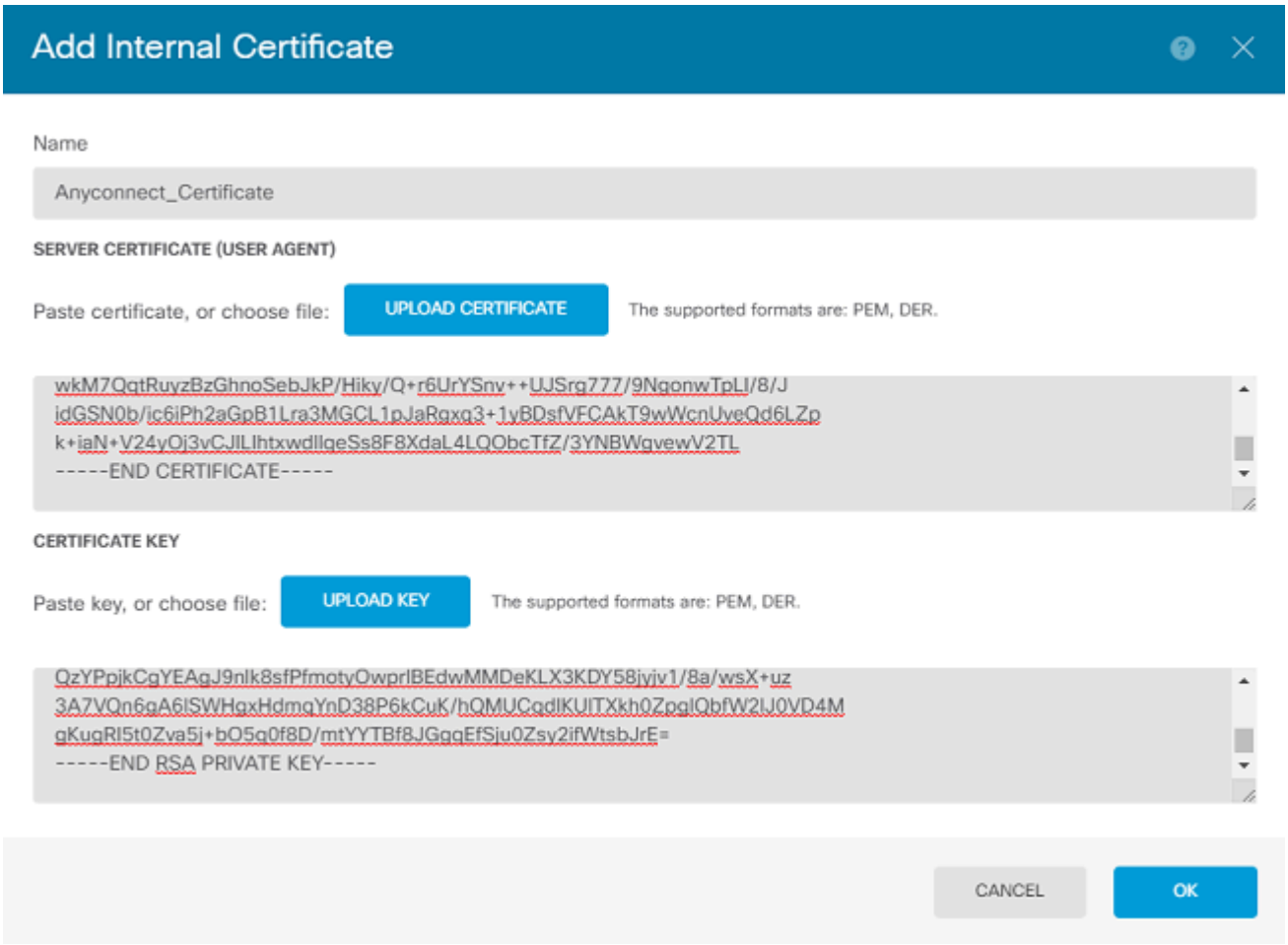
Accédez à Objects > Certificates > Add Internal Certificate. Configurez un certificat comme indiqué dans l'image.



Téléchargez à la fois le certificat et la clé privée comme indiqué dans l'image.

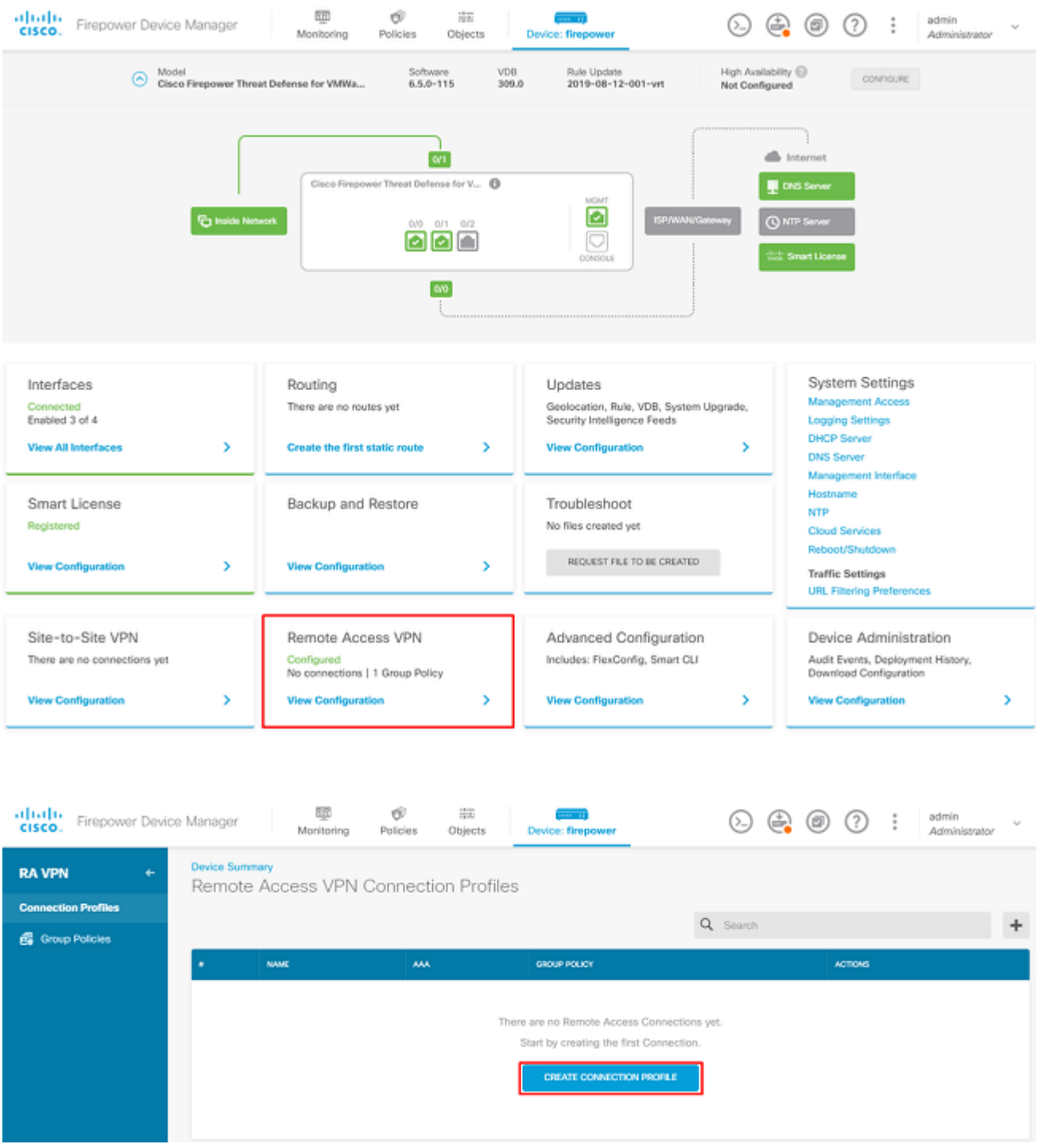


Le certificat et la clé peuvent être téléchargés par copier-coller ou par le bouton de téléchargement de chaque fichier, comme illustré dans l'image.

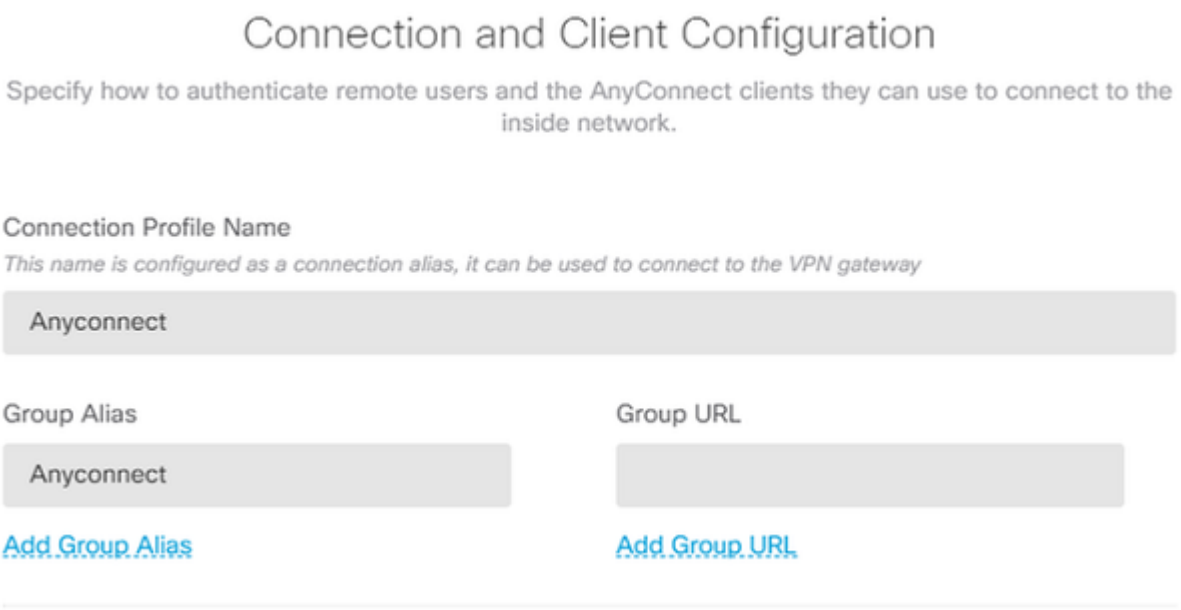


Configuration du VPN d'accès distant

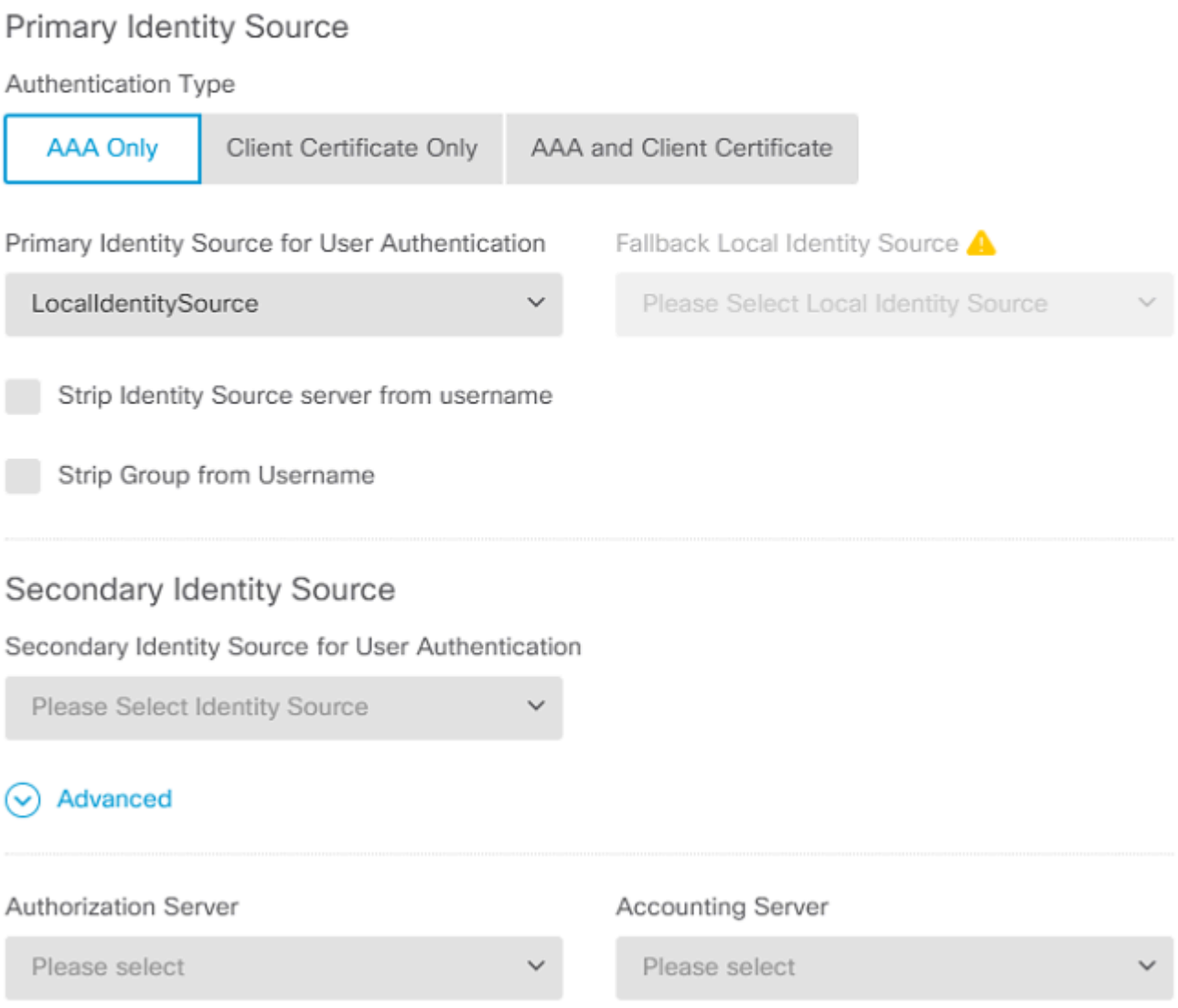
Accédez à Remote Access VPN > Create Connection Profile. Parcourez l'Assistant VPN RA sur FDM, comme illustré dans l'image.



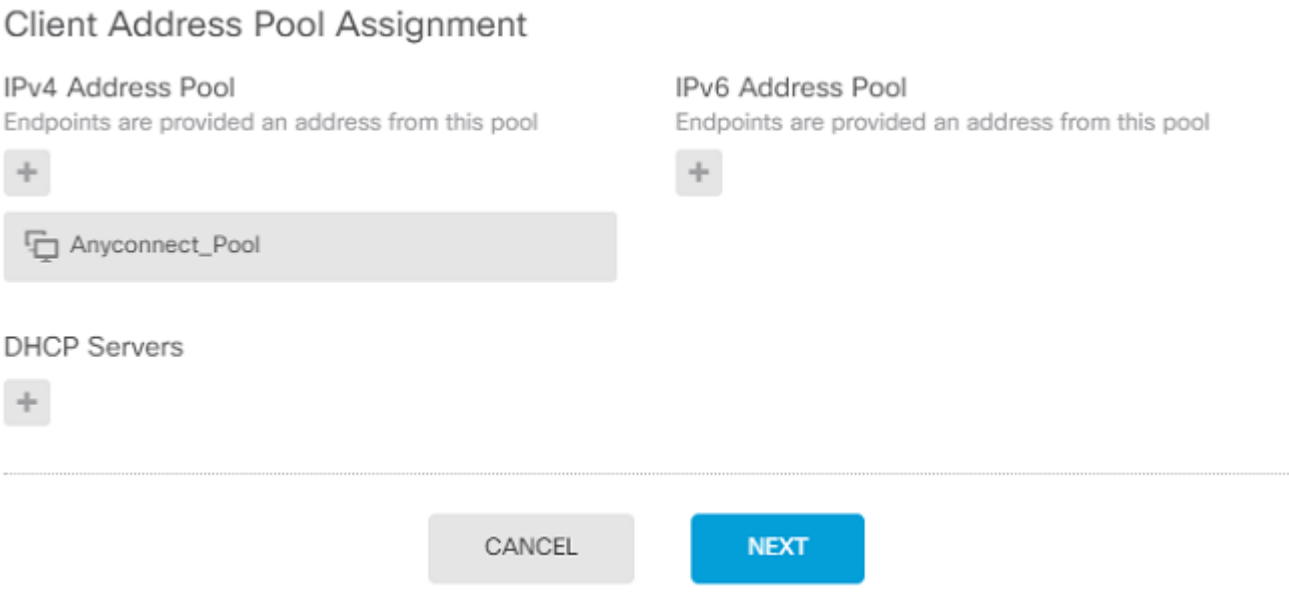
Créez un profil de connexion et démarrez la configuration comme indiqué dans l'image.



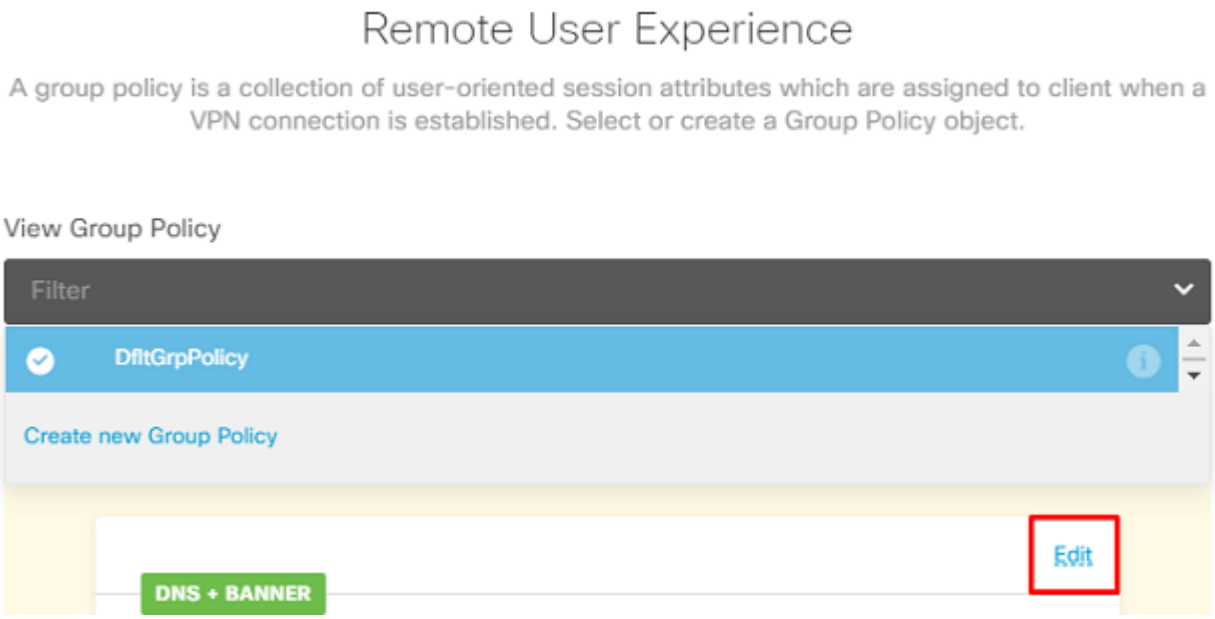
Choisissez les méthodes d'authentification comme indiqué dans l'image. Ce guide utilise l'authentification locale.



Choisissez l'objet Anyconnect_Pool comme illustré dans l'image.



Un résumé de la stratégie de groupe par défaut s'affiche sur la page suivante. Une nouvelle stratégie de groupe peut être créée lorsque vous cliquez sur la liste déroulante et choisissez l'option Create a new Group Policy. Pour ce guide, la stratégie de groupe par défaut est utilisée. Choisissez l'option edit en haut de la politique comme montré dans l'image.

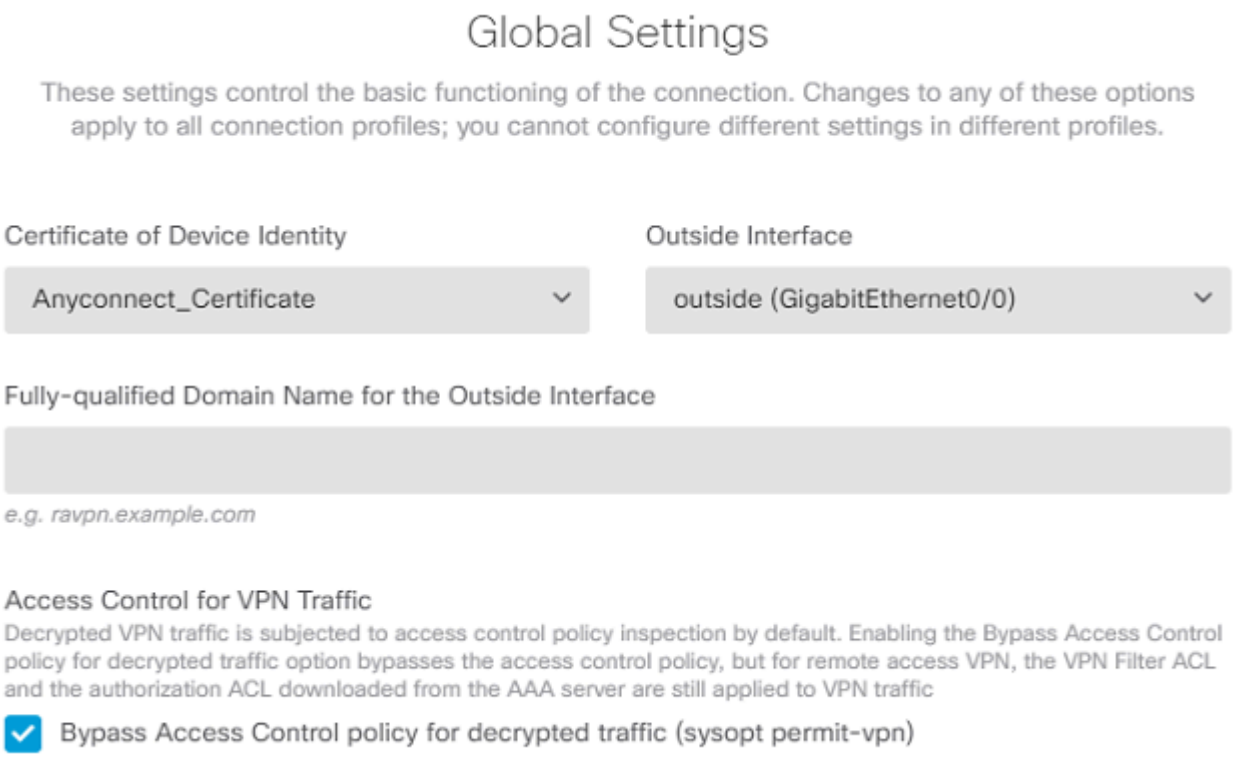


Dans la stratégie de groupe, ajoutez le Split tunneling de sorte que les utilisateurs connectés à AnyConnect envoient uniquement le trafic qui est destiné au réseau FTD interne sur le client AnyConnect tandis que tout autre trafic sort de la connexion FAI de l'utilisateur comme illustré dans l'image.

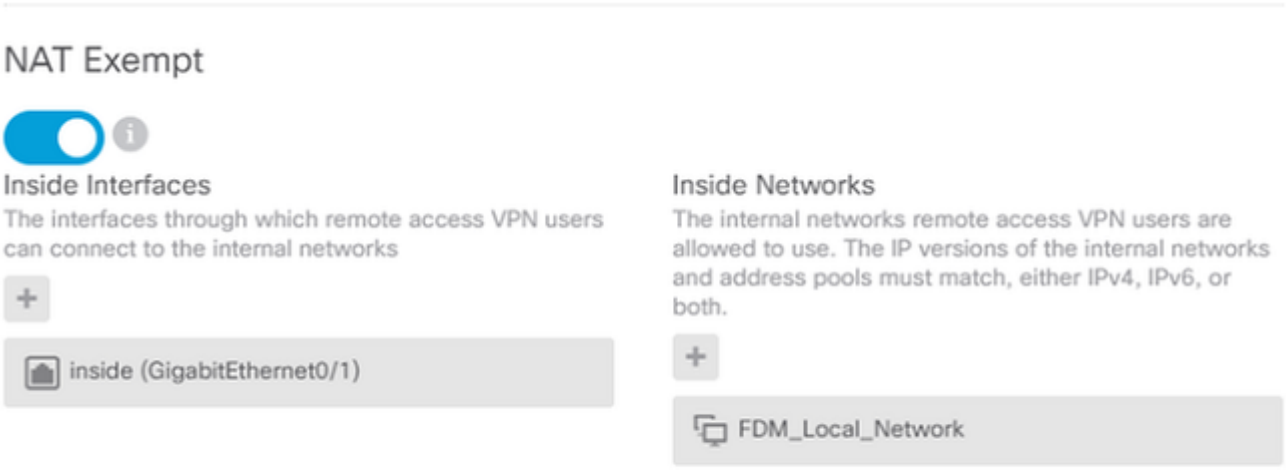


Sur la page suivante, choisissez le Anyconnect_Certificate ajouté dans la section Certificate. Ensuite, choisissez l'interface sur laquelle le FTD écoute les connexions AnyConnect. Choisissez la stratégie Bypass Access Control pour le trafic déchiffré (sysopt permit-vpn). Il s'agit d'une commande facultative si le n' sysopt permit-vpnest pas choisi. Une stratégie de contrôle d'accès doit être créée pour permettre au trafic provenant des clients AnyConnect d'accéder au réseau interne, comme

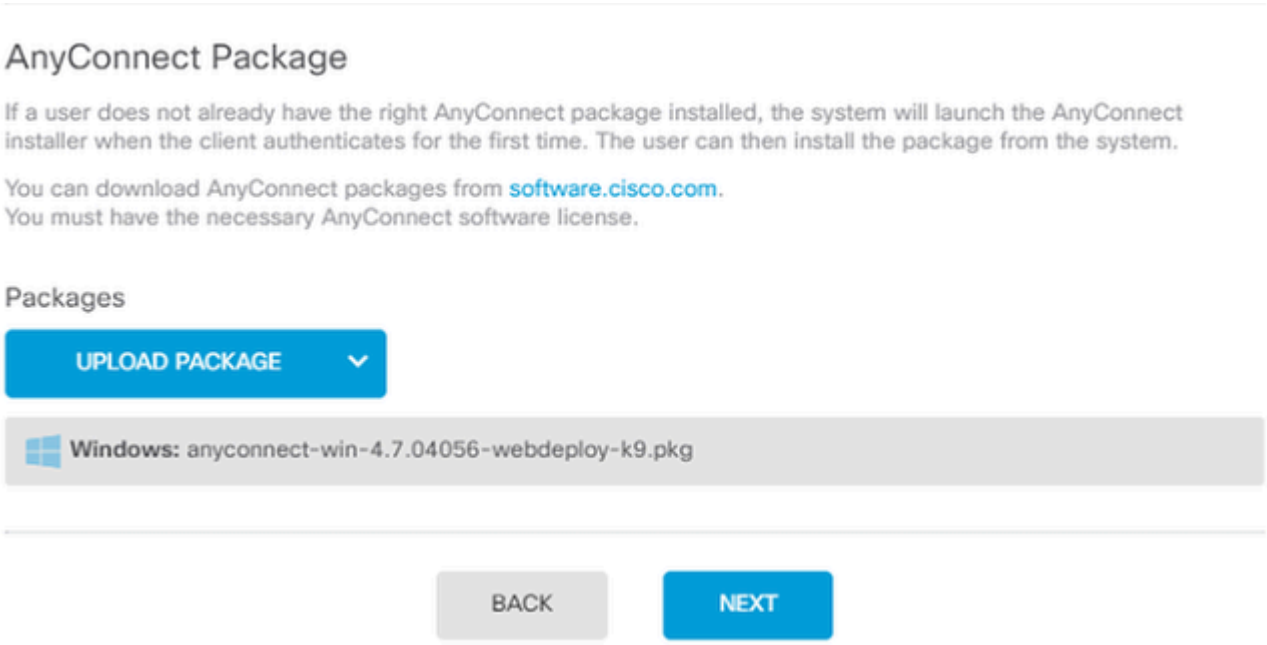
illustré dans l’image.



L'exemption NAT peut être configurée manuellement sous Policies > NAT ou elle peut être configurée automatiquement par l'assistant. Choisissez l’interface interne et les réseaux dont les clients AnyConnect ont besoin pour accéder, comme illustré dans l’image.



Choisissez le package AnyConnect pour chaque système d'exploitation (Windows/Mac/Linux) auquel les utilisateurs peuvent se connecter, comme illustré dans l'image.

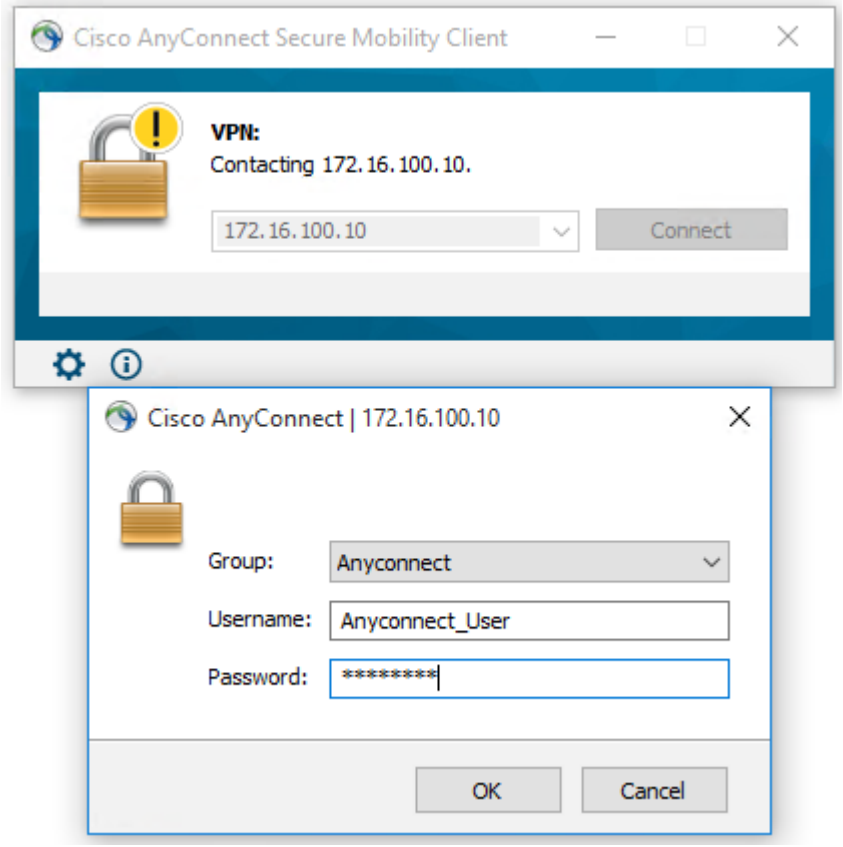


La dernière page donne un résumé de la configuration complète. Vérifiez que les paramètres corrects ont été définis et appuyez sur le bouton Finish et Deploy la nouvelle configuration.

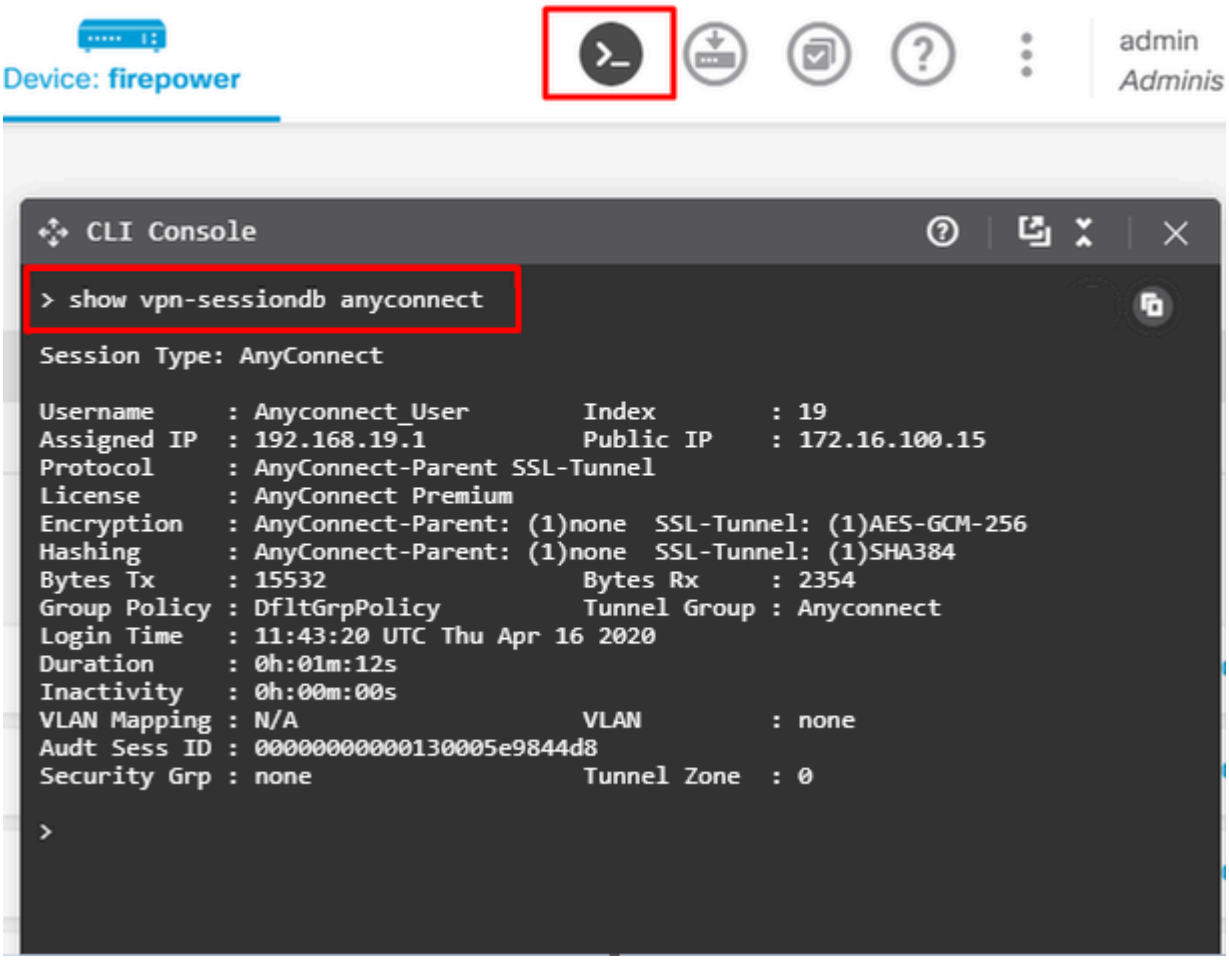
Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Une fois la configuration déployée, essayez de vous connecter. Si vous disposez d'un nom de domaine complet (FQDN) qui correspond à l'adresse IP externe du FTD, entrez-le dans la zone Connexion AnyConnect. Dans cet exemple, l'adresse IP externe du FTD est utilisée. Utilisez le nom d'utilisateur/mot de passe créé dans la section des objets de FDM, comme illustré dans l'image.



Depuis la version 6.5.0 de FDM, il n'existe aucun moyen de surveiller les utilisateurs AnyConnect via l'interface utilisateur graphique de FDM. La seule option consiste à surveiller les utilisateurs AnyConnect via l'interface de ligne de commande. La console CLI de l'interface utilisateur graphique de FDM peut également être utilisée pour vérifier que les utilisateurs sont connectés. Utilisez cette commande, Show vpn-sessiondb anyconnect.



La même commande peut être exécutée directement à partir de l'interface de ligne de commande.

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : Anyconnect_User        Index        : 15
Assigned IP  : 192.168.19.1           Public IP    : 172.16.100.15
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384
Bytes Tx     : 38830                  Bytes Rx     : 172
Group Policy : DfltGrpPolicy          Tunnel Group : Anyconnect
Login Time   : 01:08:10 UTC Thu Apr 9 2020
Duration     : 0h:00m:53s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 000000000000f0005e8e757a
Security Grp : none                   Tunnel Zone  : 0
```

Dépannage

Cette section fournit les informations que vous pouvez utiliser pour dépanner votre configuration.

Si un utilisateur ne parvient pas à se connecter au FTD avec SSL, procédez comme suit afin d'isoler les problèmes de négociation SSL :

1. Vérifiez que l'adresse IP en dehors de FTD peut faire l'objet d'une requête ping sur l'ordinateur de l'utilisateur.
2. Utilisez un analyseur externe afin de vérifier si la connexion TCP en trois étapes est réussie.

Problèmes du client AnyConnect

Cette section fournit des directives pour dépanner les deux problèmes de client VPN AnyConnect les plus courants. Un guide de dépannage pour le client AnyConnect est disponible ici : Guide de dépannage du client VPN AnyConnect.

Problèmes de connectivité initiaux

Si un utilisateur rencontre des problèmes de connectivité initiaux, activez debug webvpn AnyConnect sur le FTD et analysez les messages de débogage. Les débogages doivent être exécutés sur l'interface de ligne de commande du FTD. Utilisez la commande debug webvpn anyconnect 255. Collectez un bundle DART à partir de la machine client afin d'obtenir les journaux d'AnyConnect. Les instructions relatives à la collecte d'un bundle DART sont disponibles ici : Collecte des bundles DART.

Problèmes spécifiques au trafic

Si une connexion réussit mais que le trafic échoue sur le tunnel VPN SSL, examinez les statistiques de trafic sur le client pour vérifier que le trafic est reçu et transmis par le client. Des statistiques client détaillées sont disponibles dans toutes les versions d'AnyConnect. Si le client indique que du trafic est en cours d'envoi et de réception, recherchez le trafic reçu et transmis dans le FTD. Si le FTD applique un filtre, le nom du filtre s'affiche et vous pouvez consulter les entrées de la liste de contrôle d'accès afin de vérifier si votre trafic est abandonné. Les problèmes de trafic courants rencontrés par les utilisateurs sont les suivants :

- Problèmes de routage derrière le FTD : le réseau interne ne parvient pas à router les paquets vers les adresses IP et les clients VPN attribués.
- Listes de contrôle d'accès bloquant le trafic.
- Traduction d'adresses réseau non contournée pour le trafic VPN.

Pour plus d'informations sur les VPN d'accès à distance sur le FTD géré par FDM, consultez le

guide de configuration complet ici : Remote Access FTD géré par FDM.

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.