

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

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Licences](#)

[Composants utilisés](#)

[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 VPN RA 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 (RA VPN) sur Firepower Device Manager (FDM).

### Licences

- Firepower Threat Defense (FTD) enregistré sur le portail de licences Smart avec les fonctionnalités d'exportation contrôlée activées (afin de permettre l'activation de l'onglet de configuration VPN RA)

- Toutes les licences AnyConnect activées (APEX, Plus ou VPN uniquement)

## Composants utilisés

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

- Cisco 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.

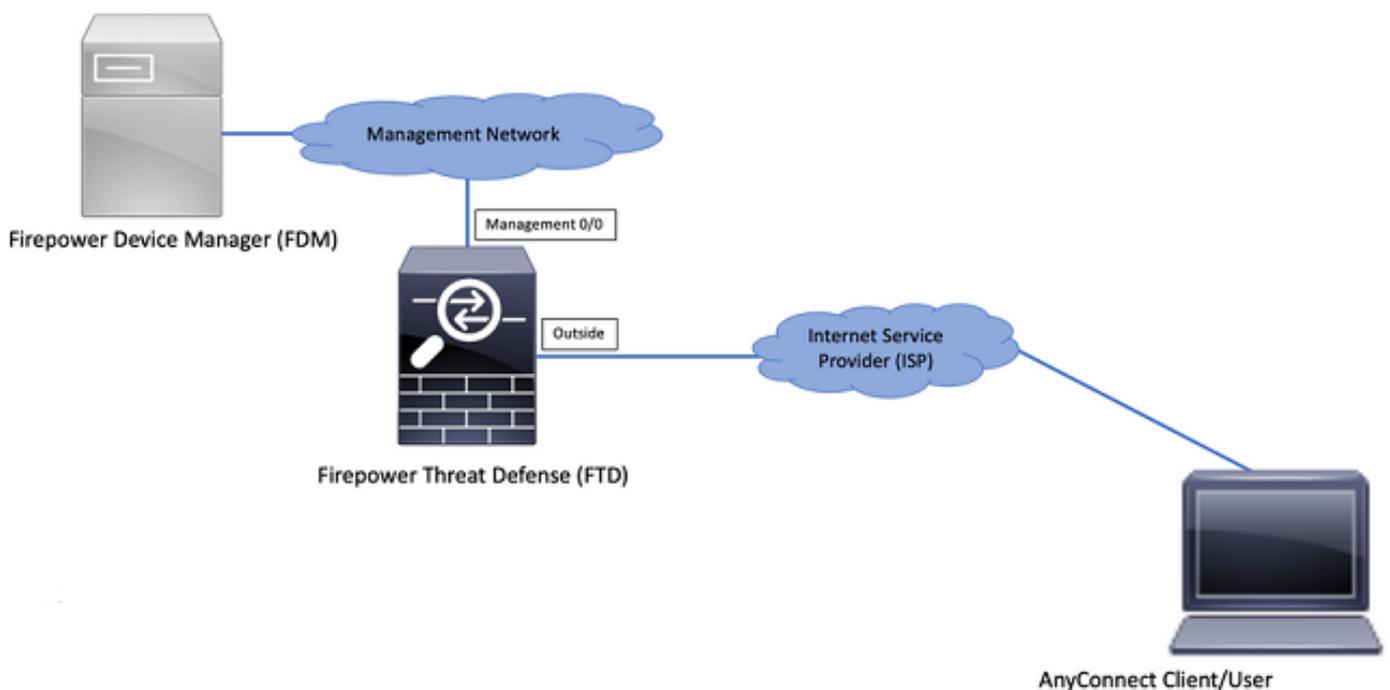
## Informations générales

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. La demande d'amélioration [CSCvm76499](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvm76499) a été déposée pour ce problème.

## Configurer

### Diagramme du réseau

Authentification client AnyConnect avec l'utilisation de Local.

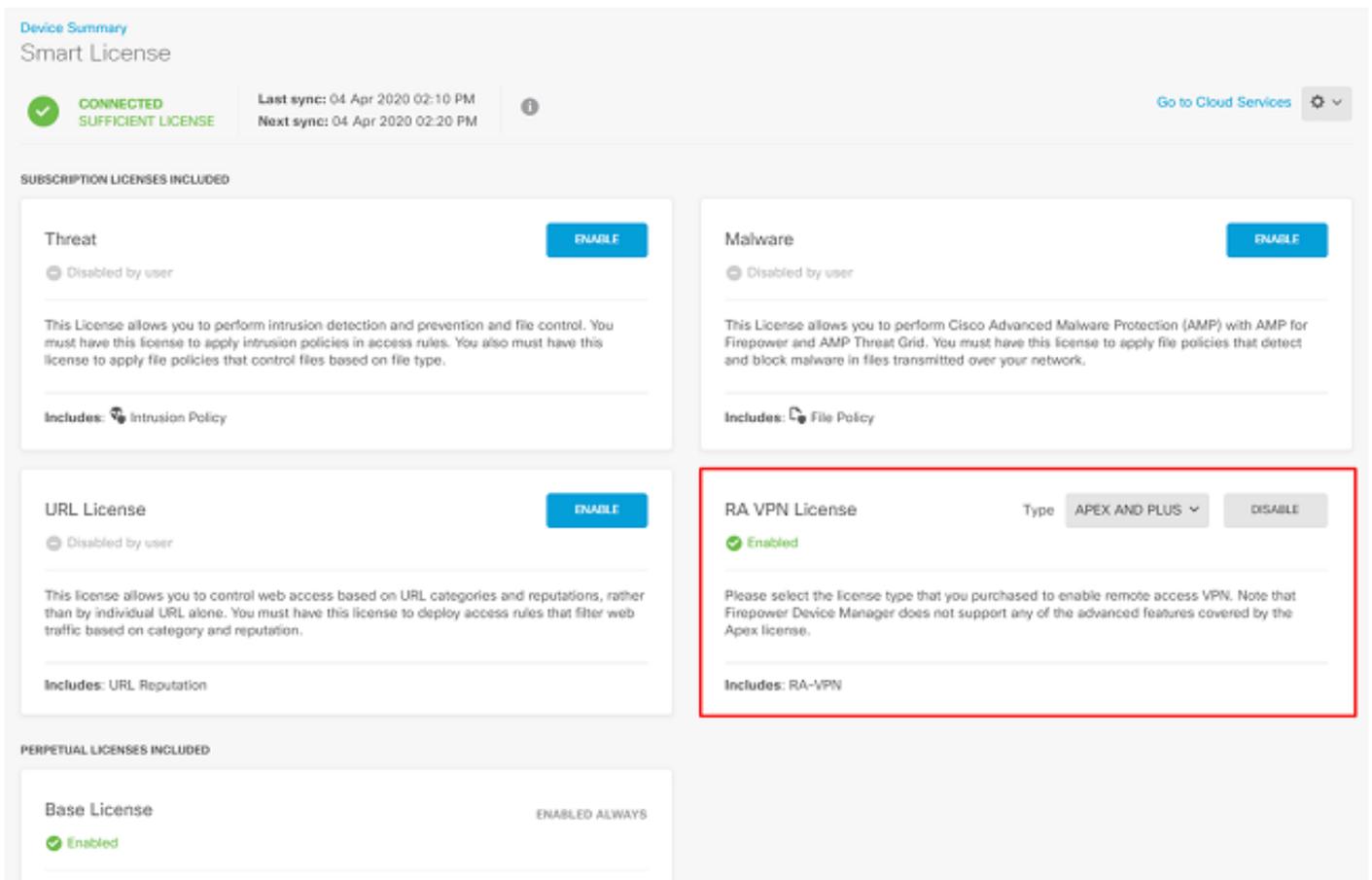


## Vérification des licences sur le FTD

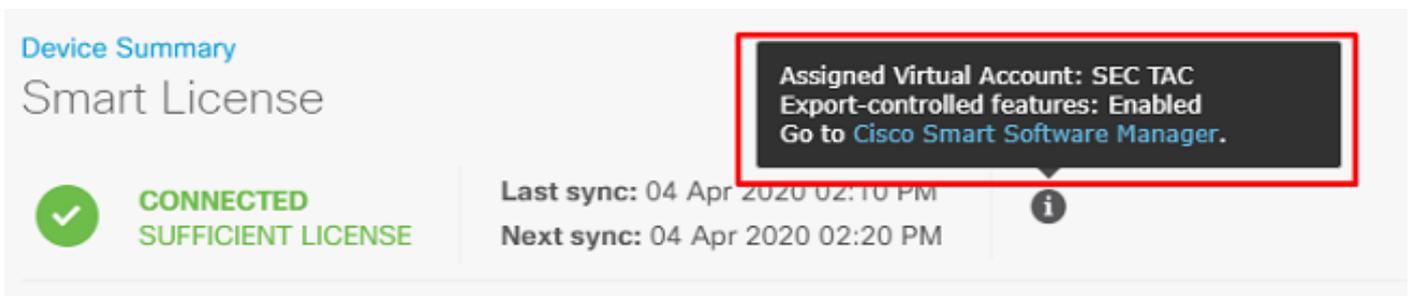
Étape 1. Vérifiez que le périphérique est enregistré dans Smart Licensing, comme indiqué dans l'image :

The screenshot displays the Cisco Firepower Device Manager (FDM) interface for a Cisco Firepower Threat Defense (FTD) device. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: firepower'. The main header shows the device model 'Cisco Firepower Threat Defense for VMWa...', software version '6.5.0-115', VDB '309.0', and rule update '2019-08-12-001-vrt'. The 'High Availability' status is 'Not Configured'. The central diagram illustrates the device's network configuration, showing an 'Inside Network' connected to the device via interface 'o/1', and an 'ISP/WAN/Gateway' connected via interface 'o/0'. The device also has interfaces 'o/2' and 'o/3'. The 'Smart License' status is highlighted as 'Registered'. Below the diagram, a grid of configuration options is visible, including 'Interfaces', 'Routing', 'Updates', 'System Settings', 'Smart License', 'Backup and Restore', 'Troubleshoot', 'Site-to-Site VPN', 'Remote Access VPN', 'Advanced Configuration', and 'Device Administration'. The 'Smart License' option is highlighted with a red box, indicating its status as 'Registered'.

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

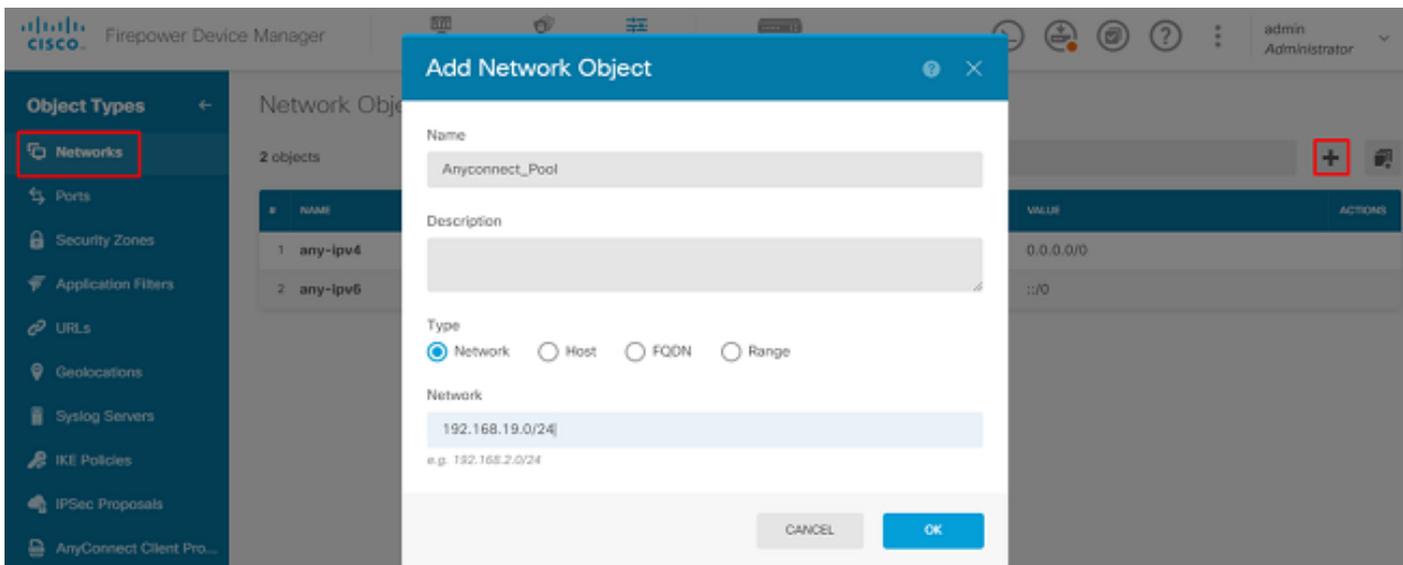


Étape 3. Vérifiez que les fonctionnalités d'exportation contrôlée sont activées dans le jeton, comme indiqué dans l'image :

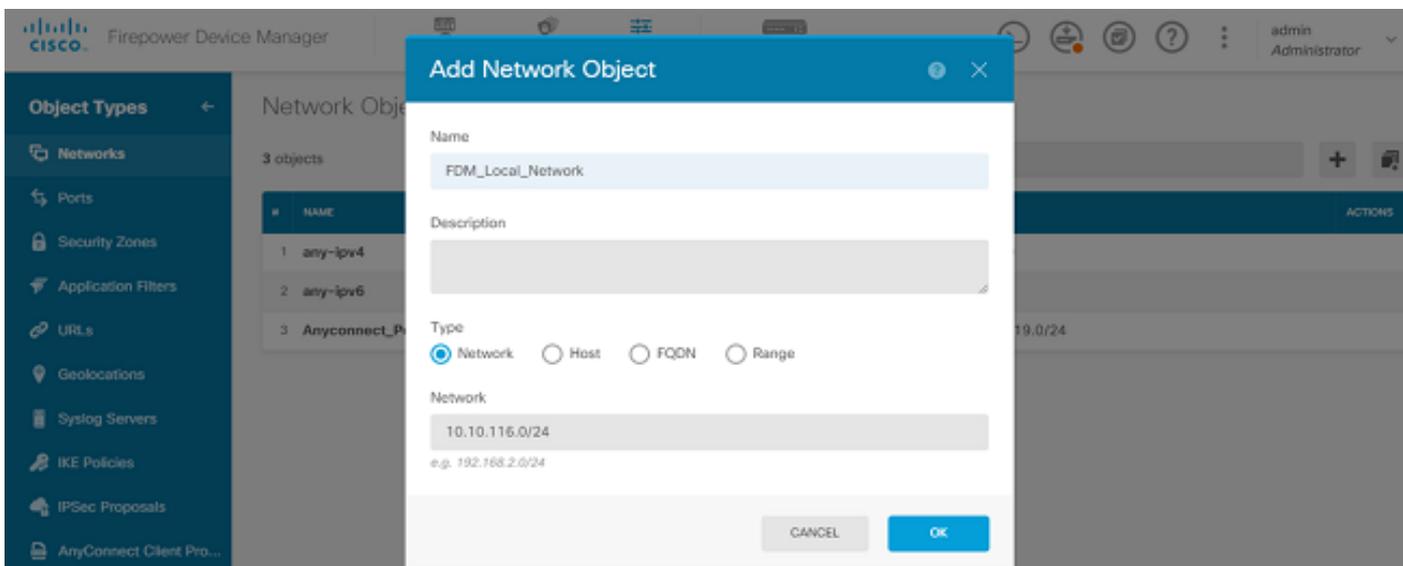


## Définition des réseaux protégés

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

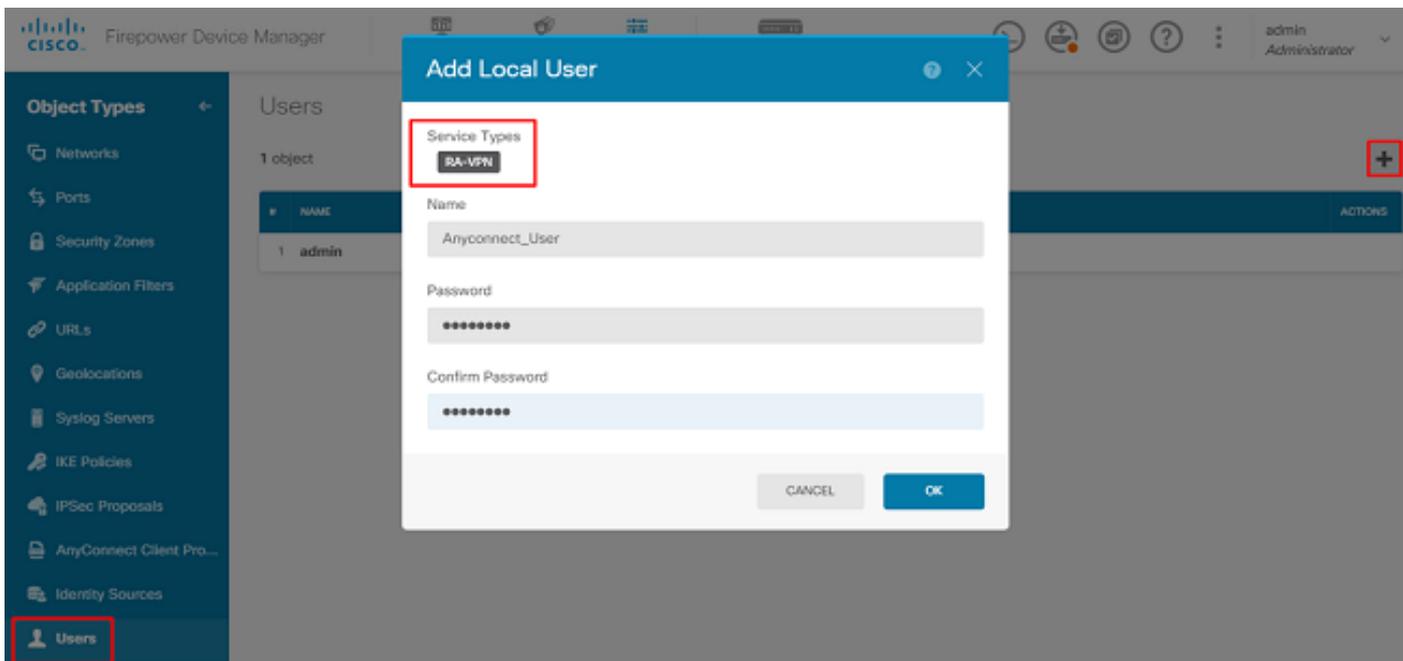


Créez un objet pour le réseau local derrière le périphérique FDM, comme illustré dans l'image :



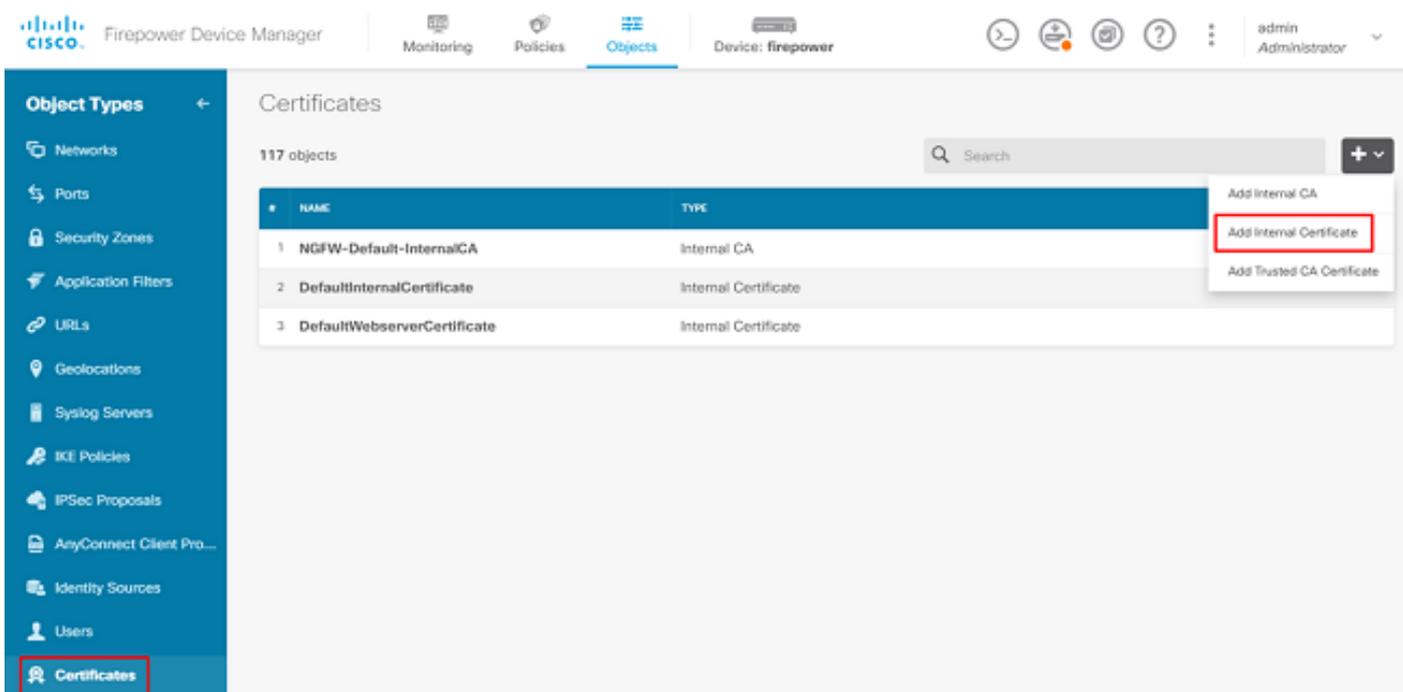
## Créer des utilisateurs locaux

Naviguez jusqu'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

Naviguez jusqu'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 :



Choose the type of internal certificate you want to create



### Upload Certificate and Key

Create a certificate from existing files.  
PEM and DER files are supported.



### Self-Signed Certificate

Create a new certificate that is signed  
by the device.

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

## Add Internal Certificate



Name

Anyconnect\_Certificate

SERVER CERTIFICATE (USER AGENT)

Paste certificate, or choose file:

UPLOAD CERTIFICATE

The supported formats are: PEM, DER.

```
wkM7QqtRuyzBzGhnoSebJkP/Hiky/Q+r6UrYSnv++UJSrg777/9NgonwTpLI/8/J
idGSN0b/ic6iPh2aGpB1Lra3MGCL1pJaRqxq3+1yBDsfVFCaKT9wWcnUveQd6LZp
k+iaN+V24yOj3vCJILihtxwdllqeSs8F8XdaL4LQObcTfZ/3YNBWqvwV2TL
-----END CERTIFICATE-----
```

CERTIFICATE KEY

Paste key, or choose file:

UPLOAD KEY

The supported formats are: PEM, DER.

```
QzYPpjCgYEAqJ9nlk8sfPfmotyOwprlBEdwMMDeKLX3KDY58jviv1/8a/wsX+uz
3A7VQn6gA6ISWHgxHdmqYnD38P6kCuK/hQMUCqdIKUITXkh0ZpglQbfW2lJ0VD4M
gKugRI5t0Zva5j+bO5q0f8D/mtYYTBf8JGqqEfSju0Zsy2ifWtsbJrE=
-----END RSA PRIVATE KEY-----
```

CANCEL

OK

## Configuration du VPN d'accès distant

Naviguez jusqu'à Remote Access VPN > Create Connection Profile. Parcourez l'assistant VPN RA sur FDM comme illustré dans l'image :

Firepower Device Manager

Monitoring Policies Objects Device: firepower

Model Cisco Firepower Threat Defense for VMWa... Software 6.5.0-115 VDB 309.0 Rule Update 2019-08-12-001-vrt High Availability Not Configured CONFIGURE

Inside Network Cisco Firepower Threat Defense for V... ESP(WAN)Gateway Internet DNS Server NTP Server Smart License

Interfaces Connected Enabled 3 of 4 View All Interfaces

Smart License Registered View Configuration

Routing There are no routes yet Create the first static route

Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration

System Settings Management Access Logging Settings DHCP Server DNS Server Management Interface Hostname NTP Cloud Services Reboot/Shutdown Traffic Settings URL Filtering Preferences

Site-to-Site VPN There are no connections yet View Configuration

Remote Access VPN Configured No connections | 1 Group Policy View Configuration

Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration

Device Administration Audit Events, Deployment History, Download Configuration View Configuration

Firepower Device Manager

Monitoring Policies Objects Device: firepower

RA VPN

Connection Profiles Group Policies

Device Summary Remote Access VPN Connection Profiles

Search

+	NAME	AAA	GROUP POLICY	ACTIONS
There are no Remote Access Connections yet. Start by creating the first Connection.				

CREATE CONNECTION PROFILE

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

## Connection and Client Configuration

Specify how to authenticate remote users and the AnyConnect clients they can use to connect to the inside network.

### Connection Profile Name

*This name is configured as a connection alias, it can be used to connect to the VPN gateway*

Anyconnect

### Group Alias

Anyconnect

[Add Group Alias](#)

### Group URL

[Add Group URL](#)

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

## Primary Identity Source

### Authentication Type

AAA Only  Client Certificate Only  AAA and Client Certificate

### Primary Identity Source for User Authentication

LocalIdentitySource

### Fallback Local Identity Source

Please Select Local Identity Source

Strip Identity Source server from username

Strip Group from Username

---

## Secondary Identity Source

### Secondary Identity Source for User Authentication

Please Select Identity Source

### Advanced

---

### Authorization Server

Please select

### Accounting Server

Please select

Sélectionnez la Anyconnect\_Pool comme l'illustre l'image :

## Client Address Pool Assignment

### IPv4 Address Pool

Endpoints are provided an address from this pool



Anyconnect\_Pool

### IPv6 Address Pool

Endpoints are provided an address from this pool



### DHCP Servers



CANCEL

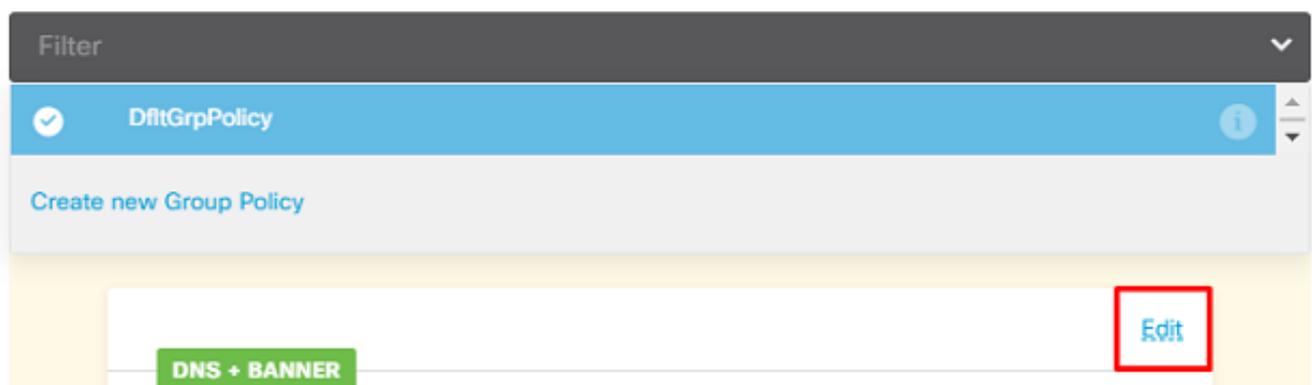
NEXT

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. Sélectionnez l'option de modification en haut de la stratégie, comme illustré dans l'image :

## Remote User Experience

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

### View Group Policy



Dans la stratégie de groupe, ajoutez la transmission tunnel partagée de sorte que les utilisateurs connectés à Anyconnect envoient uniquement le trafic destiné au réseau interne FTD sur le client Anyconnect tandis que tout autre trafic sort de la connexion ISP de l'utilisateur, comme illustré dans l'image :

## Corporate Resources (Split Tunneling)

### IPv4 Split Tunneling

Allow specified traffic over tunnel ▼

### IPv6 Split Tunneling

Allow all traffic over tunnel ▼

### IPv4 Split Tunneling Networks

+

FDM\_Local\_Network

Sur la page suivante, sélectionnez `Anyconnect_Certificate` ajouté dans la section de certificat. Ensuite, choisissez l'interface sur laquelle le FTD écoute les connexions AnyConnect. Sélectionnez la stratégie Contourner le contrôle d'accès pour le trafic déchiffré (`sysopt permit-vpn`). Il s'agit d'une commande facultative si `sysopt permit-vpn` n'est pas choisi. Une stratégie de contrôle d'accès doit être créée pour permettre au trafic des clients Anyconnect d'accéder au réseau interne, comme illustré dans l'image :

## Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

### Certificate of Device Identity

Anyconnect\_Certificate ▼

### Outside Interface

outside (GigabitEthernet0/0) ▼

### Fully-qualified Domain Name for the Outside Interface

e.g. `ravpn.example.com`

### Access Control for VPN Traffic

Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic

Bypass Access Control policy for decrypted traffic (`sysopt permit-vpn`)

L'exemption NAT peut être configurée manuellement sous `Policies > NAT` ou il peut être configuré automatiquement par l'assistant. Choisissez l'interface interne et les réseaux dont les clients Anyconnect ont besoin pour accéder à l'image.

## NAT Exempt



### Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal networks



inside (GigabitEthernet0/1)

### Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.



FDM\_Local\_Network

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

## AnyConnect Package

If a user does not already have the right AnyConnect package installed, the system will launch the AnyConnect installer when the client authenticates for the first time. The user can then install the package from the system.

You can download AnyConnect packages from [software.cisco.com](https://software.cisco.com). You must have the necessary AnyConnect software license.

### Packages

UPLOAD PACKAGE

Windows: anyconnect-win-4.7.04056-webdeploy-k9.pkg

BACK

NEXT

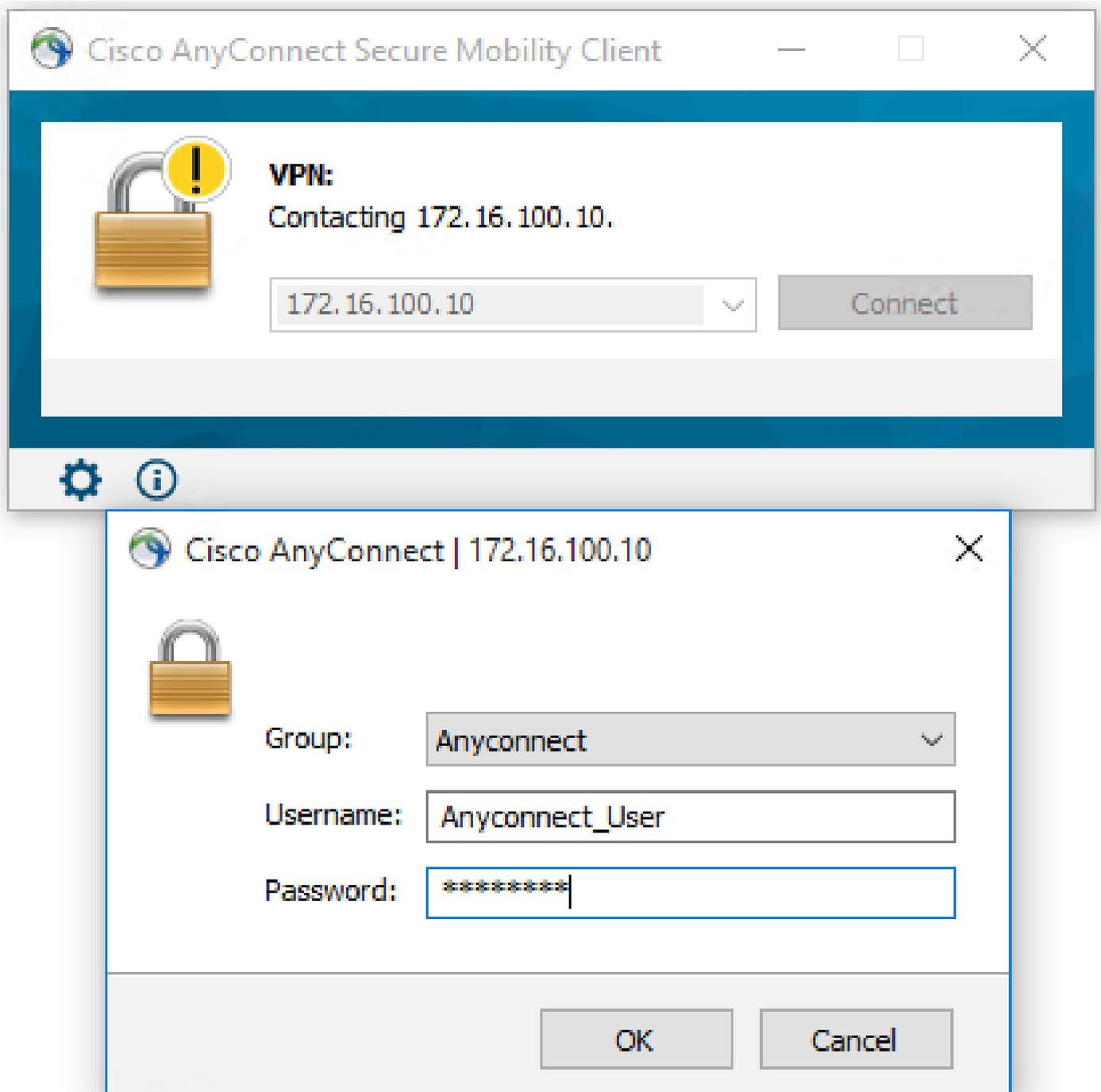
La dernière page donne un résumé de la configuration complète. Vérifiez que les paramètres corrects ont été définis et cliquez sur le bouton Finish (Terminer) et déployez la nouvelle configuration.

## Vérifier

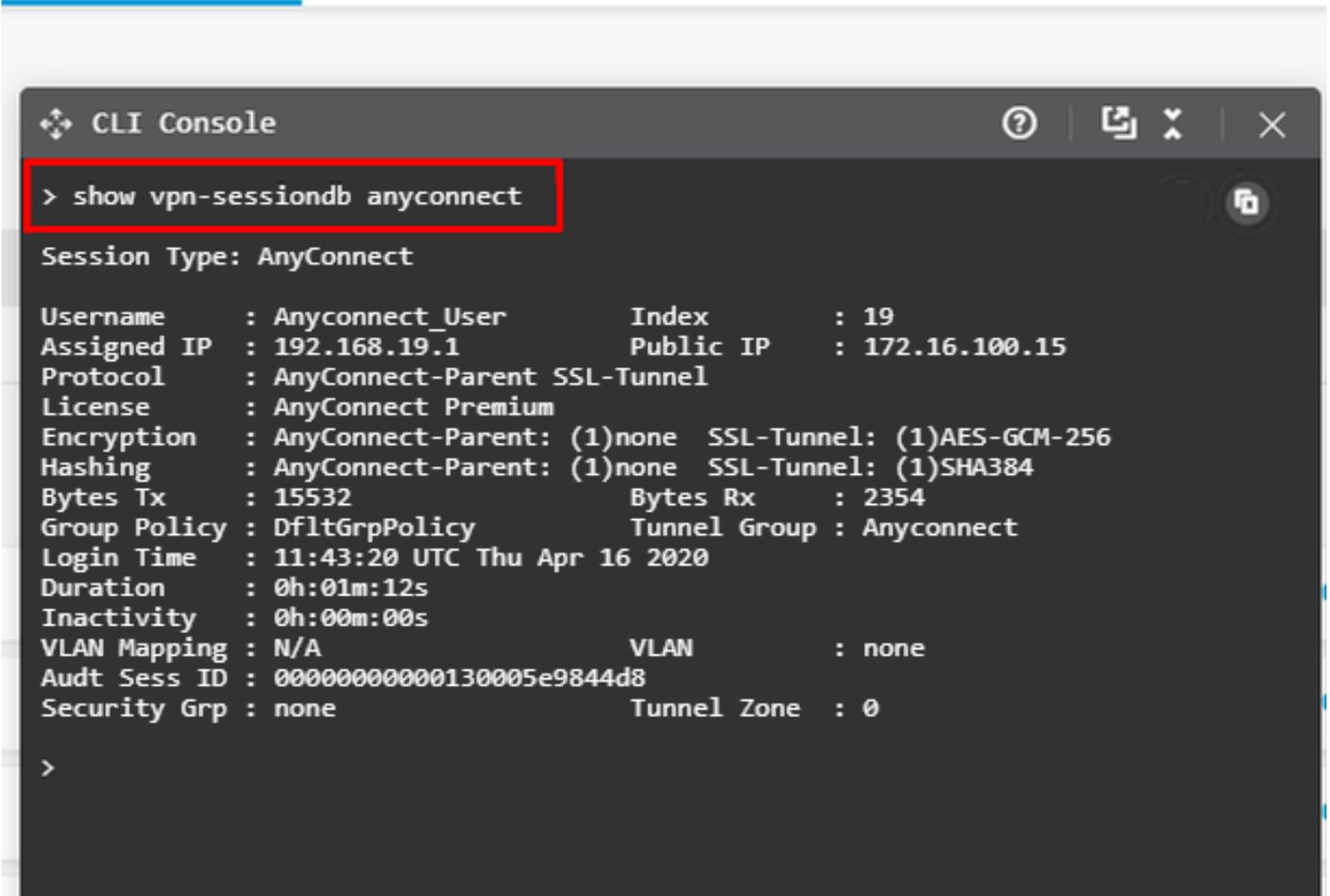
Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

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 FDM 6.5.0, 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 le débogage `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 l'ordinateur client afin d'obtenir les journaux d'AnyConnect. Des instructions sur la collecte d'un bundle DART sont disponibles ici : [Collecte de 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 peut pas 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.