

# Configurar VPN de acceso remoto en FTD administrado por FDM

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Licencias](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Verificación de licencias en el FTD](#)

[Definición de redes protegidas](#)

[Crear usuarios locales](#)

[Agregar certificado](#)

[Configurar VPN de acceso remoto](#)

[Verificación](#)

[Troubleshoot](#)

[Problemas del cliente AnyConnect](#)

[Problemas de conectividad inicial](#)

[Problemas Específicos Del Tráfico](#)

## Introducción

Este documento describe cómo configurar la implementación de una VPN de RA en FTD administrada por el administrador integrado FDM que ejecuta la versión 6.5.0 y posteriores.

## Prerequisites

## Requirements

Cisco recomienda que conozca la configuración de la red privada virtual de acceso remoto (VPN de RA) en Firepower Device Manager (FDM).

## Licencias

- Firepower Threat Defence (FTD) registrado en el portal de licencias inteligentes con las funciones de exportación controladas habilitadas (para permitir habilitar la ficha de configuración de VPN de RA)
- Cualquiera de las licencias de AnyConnect habilitadas (APEX, Plus o solo VPN)

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco FTD que ejecuta la versión 6.5.0-115
- Versión 4.7.01076 de Cisco AnyConnect Secure Mobility Client

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

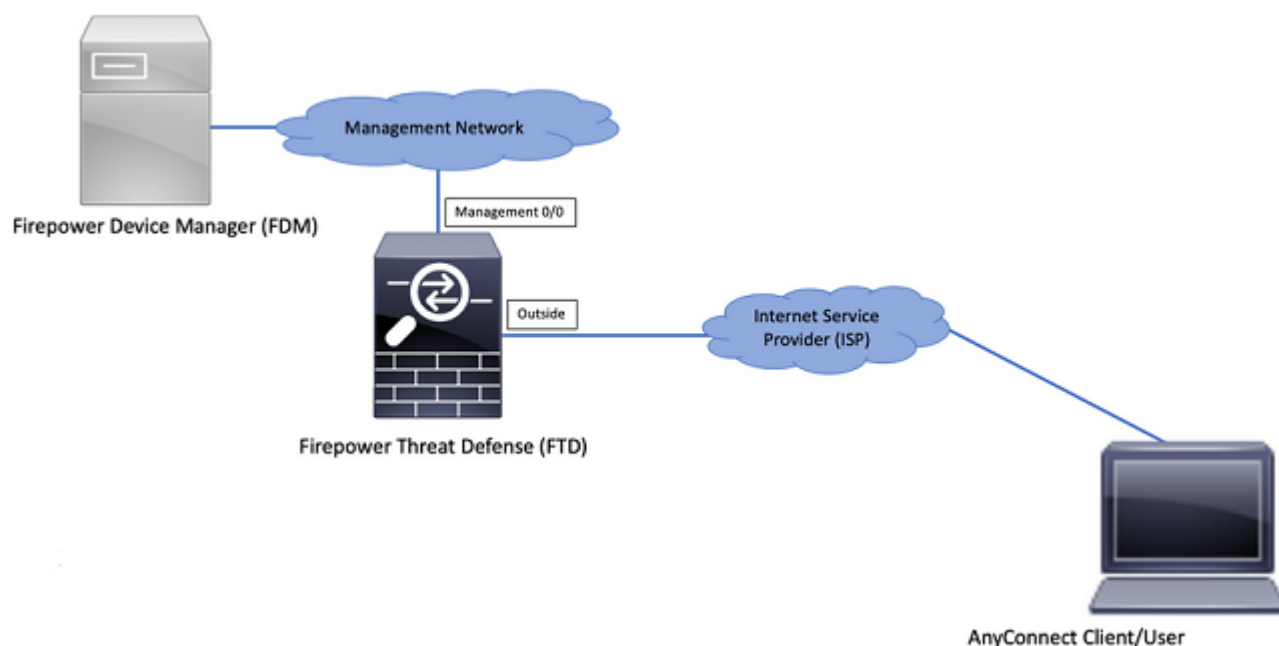
## Antecedentes

La configuración de FTD a través de FDM plantea dificultades cuando se intenta establecer conexiones para los clientes de AnyConnect a través de la interfaz externa mientras se accede a la administración a través de la misma interfaz. Esta es una limitación conocida de FDM. La solicitud de mejora [CSCvm76499](#) se ha presentado para este problema.

## Configurar

### Diagrama de la red

Autenticación del cliente AnyConnect con el uso de Local.



### Verificación de licencias en el FTD

Paso 1. Verifique que el dispositivo esté registrado en Smart Licensing como se muestra en la imagen:

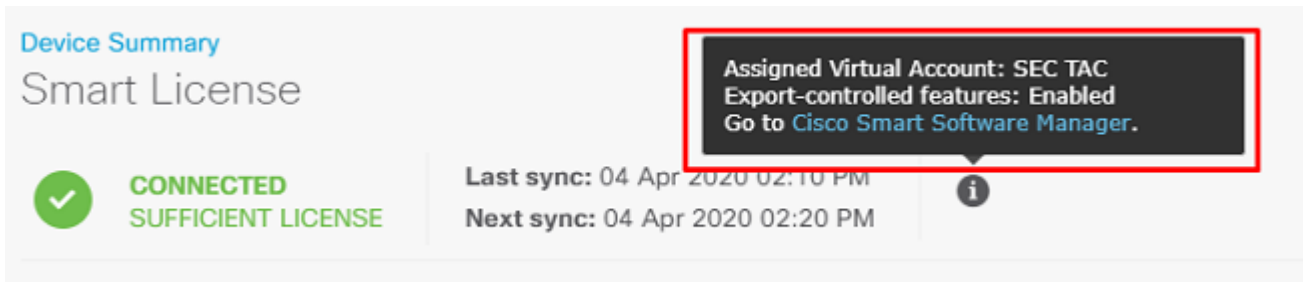
The screenshot shows the Cisco Firepower Device Manager interface for a device named 'firepower'. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: firepower'. The main dashboard displays various configuration sections: Interfaces (3 of 4 enabled), Routing (no routes yet), Updates (Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds), System Settings (Management Access, Logging Settings, DHCP Server, DNS Server, Management Interface, Hostname, NTP, Cloud Services, Reboot/Shutdown, Traffic Settings), Smart License (Registered), Backup and Restore, Troubleshoot, Site-to-Site VPN, Remote Access VPN, Advanced Configuration, and Device Administration. The 'Smart License' section is highlighted with a red box.

Paso 2. Compruebe que las licencias de AnyConnect estn habilitadas en el dispositivo, como se muestra en la imagen.

The screenshot shows the Cisco Firepower Device Manager 'Smart License' configuration page. The page shows the license status as 'CONNECTED SUFFICIENT LICENSE' with a 'Go to Cloud Services' button. Under 'SUBSCRIPTION LICENSES INCLUDED', there are sections for Threat, Malware, URL License, and RA VPN License. The RA VPN License section is highlighted with a red box, showing it is 'Enabled' and includes 'RA-VPN'. Under 'PERPETUAL LICENSES INCLUDED', there is a 'Base License' section which is 'ENABLED ALWAYS'.

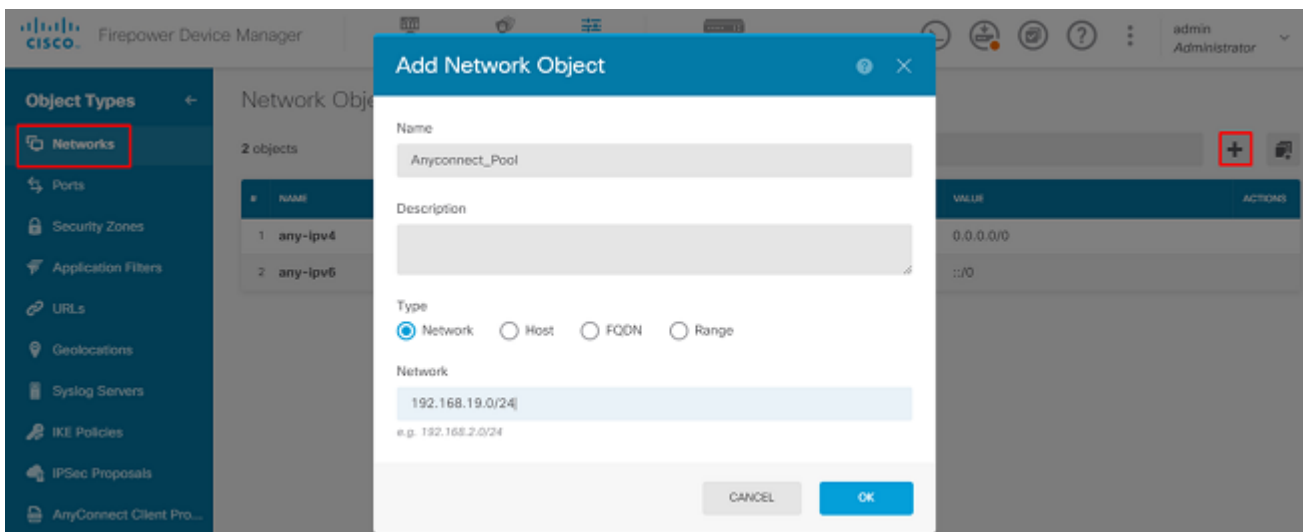
Paso 3. Verifique que las funciones controladas por exportacin estn habilitadas en el token, como se

muestra en la imagen:

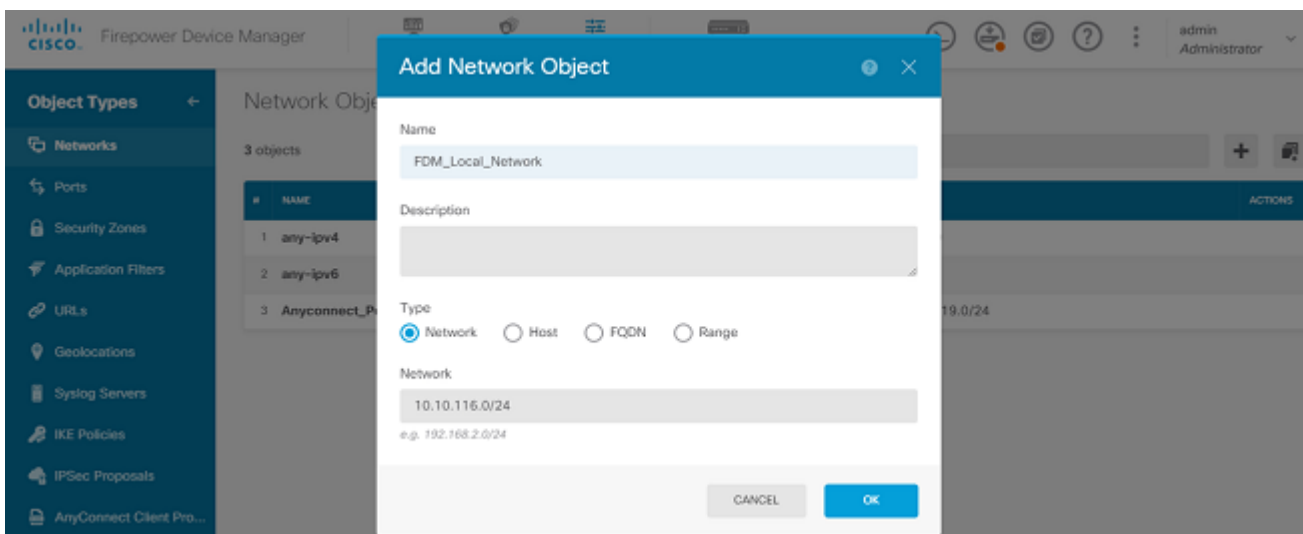


## Definición de redes protegidas

Desplácese hasta **Objects > Networks > Add new Network**. Configure el grupo VPN y las redes LAN desde la GUI de FDM. Cree un conjunto VPN para utilizarlo para la asignación de direcciones locales a los usuarios de AnyConnect, como se muestra en la imagen:

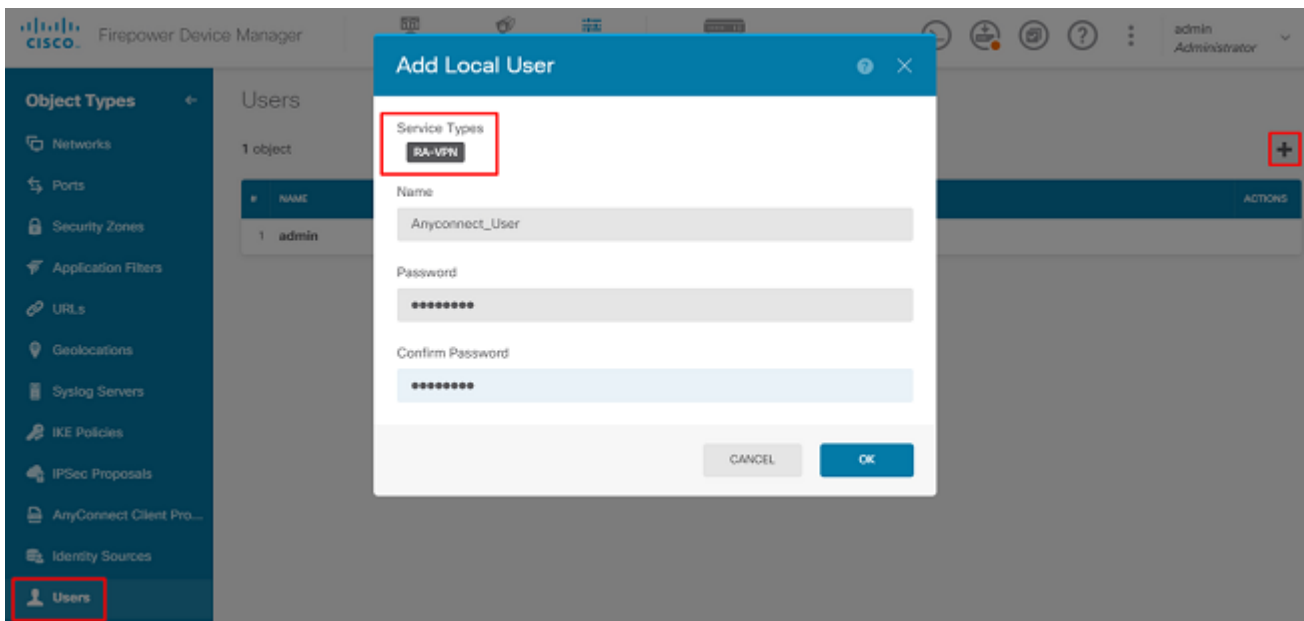


Cree un objeto para la red local detrás del dispositivo FDM como se muestra en la imagen:



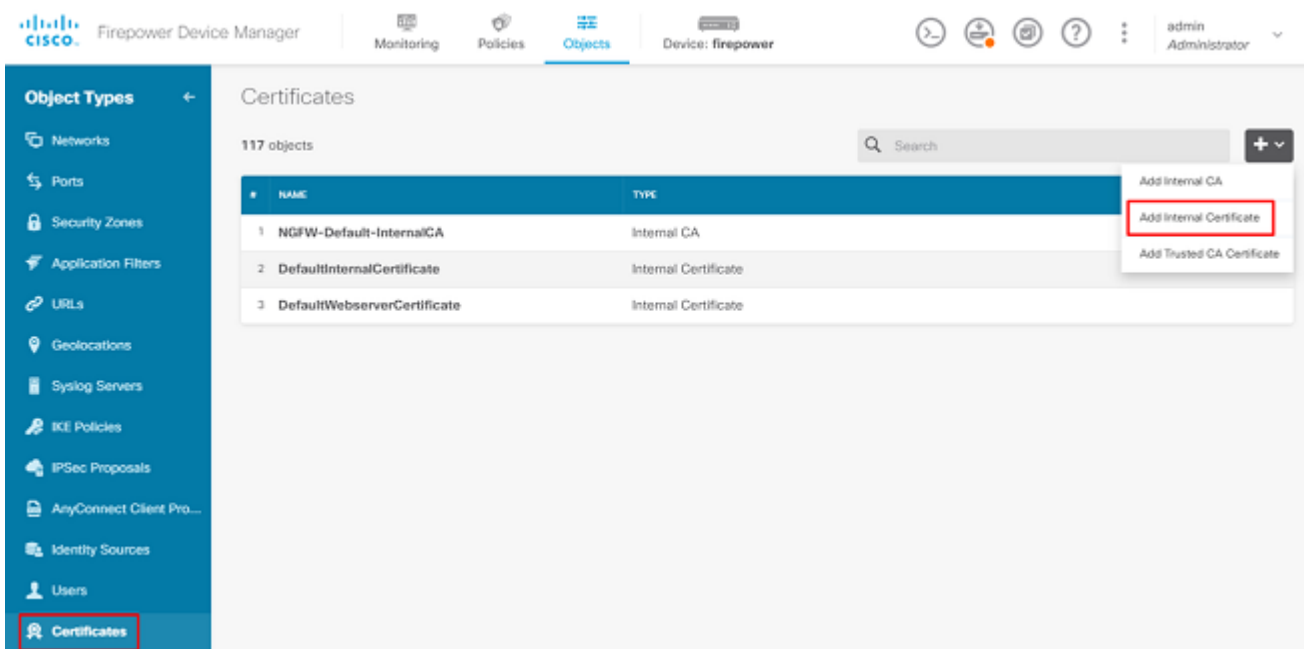
## Crear usuarios locales

Desplácese hasta **Objects > Users > Add User**. Agregue usuarios locales de VPN que se conecten a FTD a través de Anyconnect. Cree los usuarios locales como se muestra en la imagen:



## Agregar certificado

Desplácese hasta Objects > Certificates > Add Internal Certificate. Configure un certificado como se muestra en la imagen:



Cargue el certificado y la clave privada como se muestra en la imagen:

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.

El certificado y la clave se pueden cargar mediante copiar y pegar o el botón de carga de cada archivo, como se muestra en la imagen:

## 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++UJSrq777/9NgonwTpLI/8/J  
idGSN0b/ic6iPh2aGpB1Lra3MGCL1pJaRxa3+1vBDsfVFCaKt9wWcnUveQd6LZp  
k+iaN+V24yQj3vCJILlhtxwdllqeSs8F8XdaL4LQObcTfZ/3YNBWqvevV2TL  
-----END CERTIFICATE-----
```

CERTIFICATE KEY

Paste key, or choose file:

UPLOAD KEY

The supported formats are: PEM, DER.

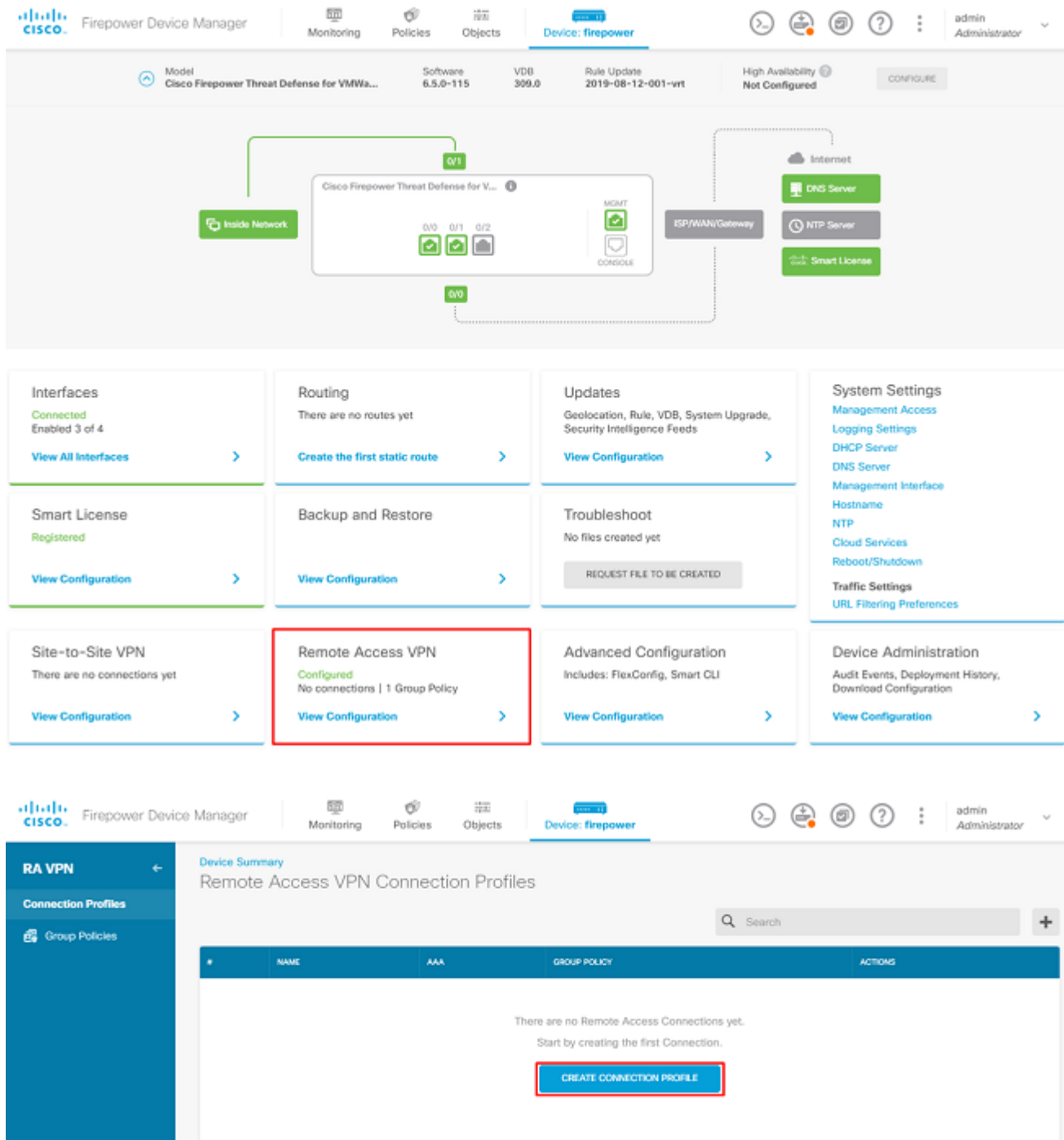
```
QzYPpikCgYEAgJ9nlk8sfPfmotyQwprlBEdwMMDeKLX3KDY58jiv1/8a/wsX+uz  
3A7VQn6gA6iSWHqxHdmgYnD38P6kCuK/hQMUcadiKUITXkh0ZpglQbfW2lJ0VD4M  
gKugRI5t0Zva5j+bO5q0f8D/mtYYTBf8JGggEfSju0Zsy2ifWtsbJrE=  
-----END RSA PRIVATE KEY-----
```

CANCEL

OK

## Configurar VPN de acceso remoto

Desplácese hasta Remote Access VPN > Create Connection Profile. Desplácese por el asistente de VPN de RA en FDM como se muestra en la imagen:



Cree un perfil de conexión e inicie la configuración como se muestra en la imagen:

# 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](#)

Elija los métodos de autenticación como se muestra en la imagen. Esta guía utiliza la autenticación local.

## 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

Elija el Anyconnect\_Pool como se muestra en la imagen:



## 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

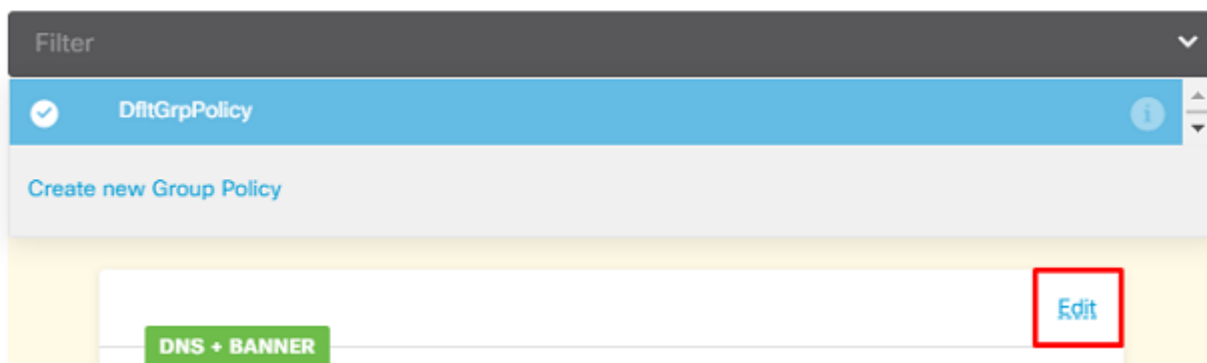
NEXT

En la página siguiente se muestra un resumen de la directiva de grupo predeterminada. Se puede crear una nueva política de grupo al pulsar el menú desplegable y elegir la opción para *Create a new Group Policy*. Para esta guía, se utiliza la directiva de grupo predeterminada. Elija la opción de edición en la parte superior de la política como se muestra en la imagen:

## 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



En la política de grupo, agregue la tunelización dividida para que los usuarios conectados a Anyconnect envíen solamente el tráfico que está destinado a la red FTD interna a través del cliente Anyconnect mientras que el resto del tráfico sale de la conexión ISP del usuario como se muestra en la imagen:

## 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

En la página siguiente, seleccione la opción `Anyconnect_Certificate` agregado en la sección de certificados. A continuación, elija la interfaz en la que el FTD escucha las conexiones de AnyConnect. Elija la directiva Omitir control de acceso para el tráfico descifrado (`sysopt permit-vpn`). Este es un comando opcional si el `sysopt permit-vpn` no se ha elegido. Se debe crear una política de control de acceso que permita que el tráfico de los clientes de Anyconnect acceda a la red interna como se muestra en la imagen:

## 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`)

La exención de NAT se puede configurar manualmente en `Policías > NAT` o el asistente puede configurarlo automáticamente. Elija la interfaz interna y las redes que los clientes de Anyconnect necesitan para acceder como se muestra en la imagen.

## 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

Elija el paquete Anyconnect para cada sistema operativo (Windows/Mac/Linux) con el que los usuarios pueden conectarse, como se muestra en la imagen.

## 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

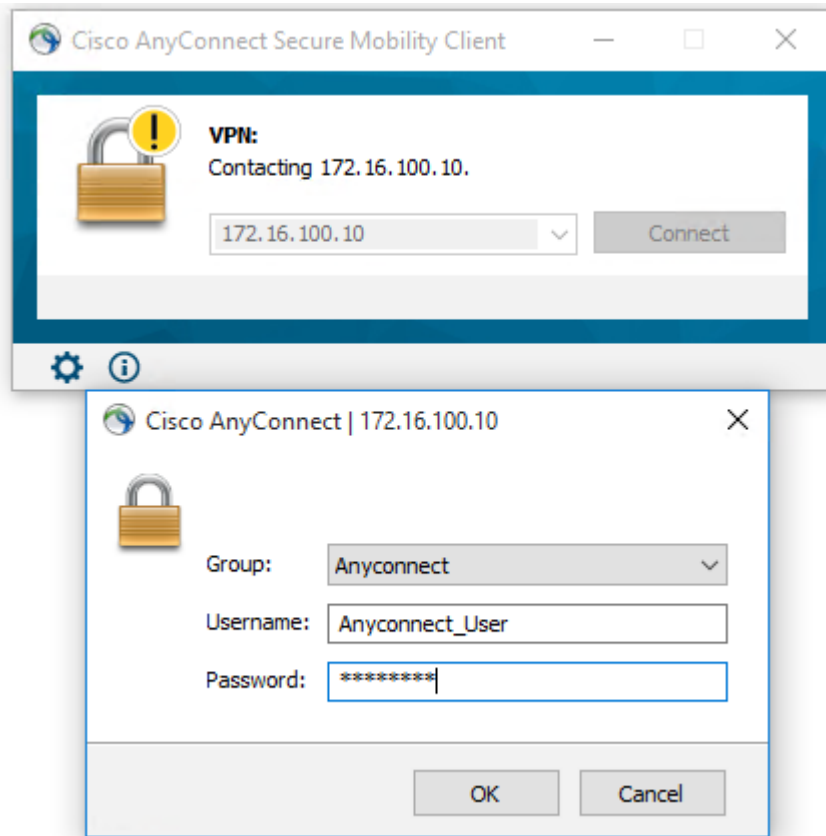
NEXT

La última página ofrece un resumen de toda la configuración. Confirme que se han establecido los parámetros correctos y pulse el botón Finalizar e Implemente la nueva configuración.

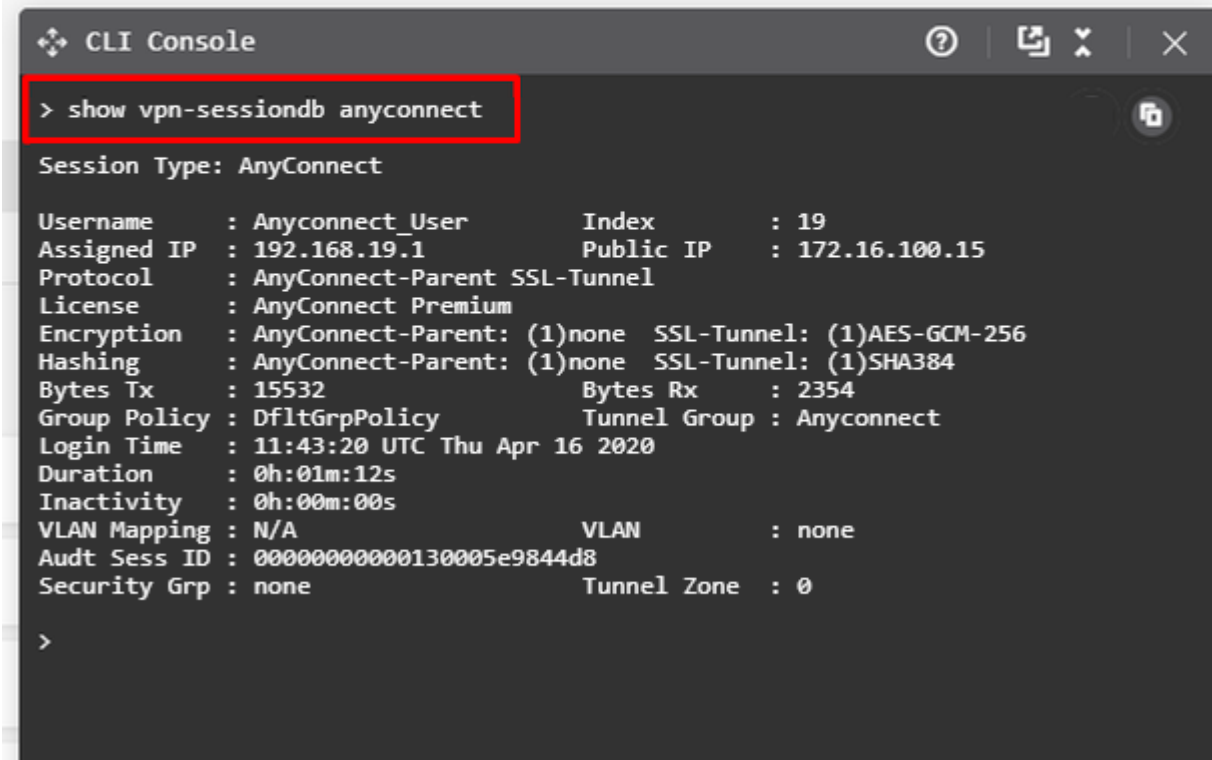
## Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Una vez implementada la configuración, intente conectarse. Si tiene un FQDN que se resuelve en la IP externa del FTD, ingréselo en el cuadro Conexión de Anyconnect. En este ejemplo, se utiliza la dirección IP externa del FTD. Utilice el nombre de usuario y la contraseña creados en la sección de objetos de FDM, como se muestra en la imagen.



A partir de FDM 6.5.0, no hay forma de supervisar a los usuarios de Anyconnect a través de la GUI de FDM. La única opción es supervisar a los usuarios de Anyconnect a través de CLI. También se puede utilizar la consola CLI de la GUI de FDM para comprobar que los usuarios están conectados. Utilice este comando: `Show vpn-sessiondb anyconnect`.



El mismo comando se puede ejecutar directamente desde la CLI.

```
> 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
```

## Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

Si un usuario no puede conectarse al FTD con SSL, realice estos pasos para aislar los problemas de negociación SSL:

1. Verifique que la dirección IP fuera del FTD se pueda hacer ping a través del equipo del usuario.
2. Utilice un sniffer externo para verificar si el intercambio de señales de tres vías TCP es exitoso.

## Problemas del cliente AnyConnect

Esta sección proporciona pautas para resolver los dos problemas más comunes del cliente AnyConnect VPN. Una guía de troubleshooting para el cliente AnyConnect se puede encontrar aquí: [Guía de Troubleshooting de AnyConnect VPN Client](#).

## Problemas de conectividad inicial

Si un usuario tiene problemas de conectividad iniciales, habilite `debug webvpn` AnyConnect en el FTD y analice los mensajes de depuración. Las depuraciones deben ejecutarse en la CLI del FTD. Use el comando `debug webvpn anyconnect 255`.

Recopile un paquete DART de la máquina cliente para obtener los registros de AnyConnect. Puede encontrar instrucciones sobre cómo recopilar un paquete DART aquí: [Recopilación de paquetes DART](#).

## Problemas Específicos Del Tráfico

Si una conexión es exitosa pero el tráfico falla sobre el túnel SSL VPN, observe las estadísticas de tráfico en el cliente para verificar que el tráfico está siendo recibido y transmitido por el cliente. Las estadísticas detalladas del cliente están disponibles en todas las versiones de AnyConnect. Si el cliente muestra que el tráfico se está enviando y recibiendo, verifique el FTD para el tráfico recibido y transmitido. Si el FTD aplica un filtro, se muestra el nombre del filtro y puede observar las entradas de ACL para verificar si su tráfico está siendo descartado. Los problemas comunes de tráfico que experimentan los usuarios son:

- Problemas de ruteo detrás del FTD - la red interna no puede rutear paquetes de vuelta a las direcciones IP asignadas y a los clientes VPN
- Listas de control de acceso que bloquean el tráfico
- Traducción de direcciones de red que no se omite para el tráfico VPN

Para obtener más información sobre las VPN de acceso remoto en el FTD gestionado por FDM, consulte la guía de configuración completa aquí: [FTD de acceso remoto gestionado por FDM](#).

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).