Configuración de VPN de acceso remoto AnyConnect en FTD

Contenido

Introducción

Este documento describe una configuración para AnyConnect Remote Access VPN en FTD.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de VPN, TLS e IKEv2
- Conocimiento básico de autenticación, autorización y contabilidad (AAA) y RADIUS
- Experiencia con Firepower Management Center

Componentes Utilizados

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

- FTD 7.2.0 de Cisco

- Cisco FMC 7.2.1
- AnyConnect 4.10

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

Este documento proporciona un ejemplo de configuración para Firepower Threat Defence (FTD) versión 7.2.0 y posteriores, que permite que la VPN de acceso remoto use Transport Layer Security (TLS) e Internet Key Exchange versión 2 (IKEv2). Como cliente, se puede utilizar Cisco AnyConnect, que es compatible con varias plataformas.

Configuración

1. Prerequisites

Para pasar a través del asistente de acceso remoto en Firepower Management Center:

- Cree un certificado utilizado para la autenticación del servidor.
- Configure el servidor RADIUS o LDAP para la autenticación de usuarios.
- Cree un conjunto de direcciones para los usuarios de VPN.
- Cargue imágenes de AnyConnect para diferentes plataformas.

a) Importar el certificado SSL

Los certificados son esenciales al configurar AnyConnect. El certificado debe tener una extensión de nombre alternativo de sujeto con nombre DNS o dirección IP para evitar errores en los navegadores web.

> **Nota**: Solo los usuarios registrados de Cisco tienen acceso a las herramientas internas y a la información de errores.

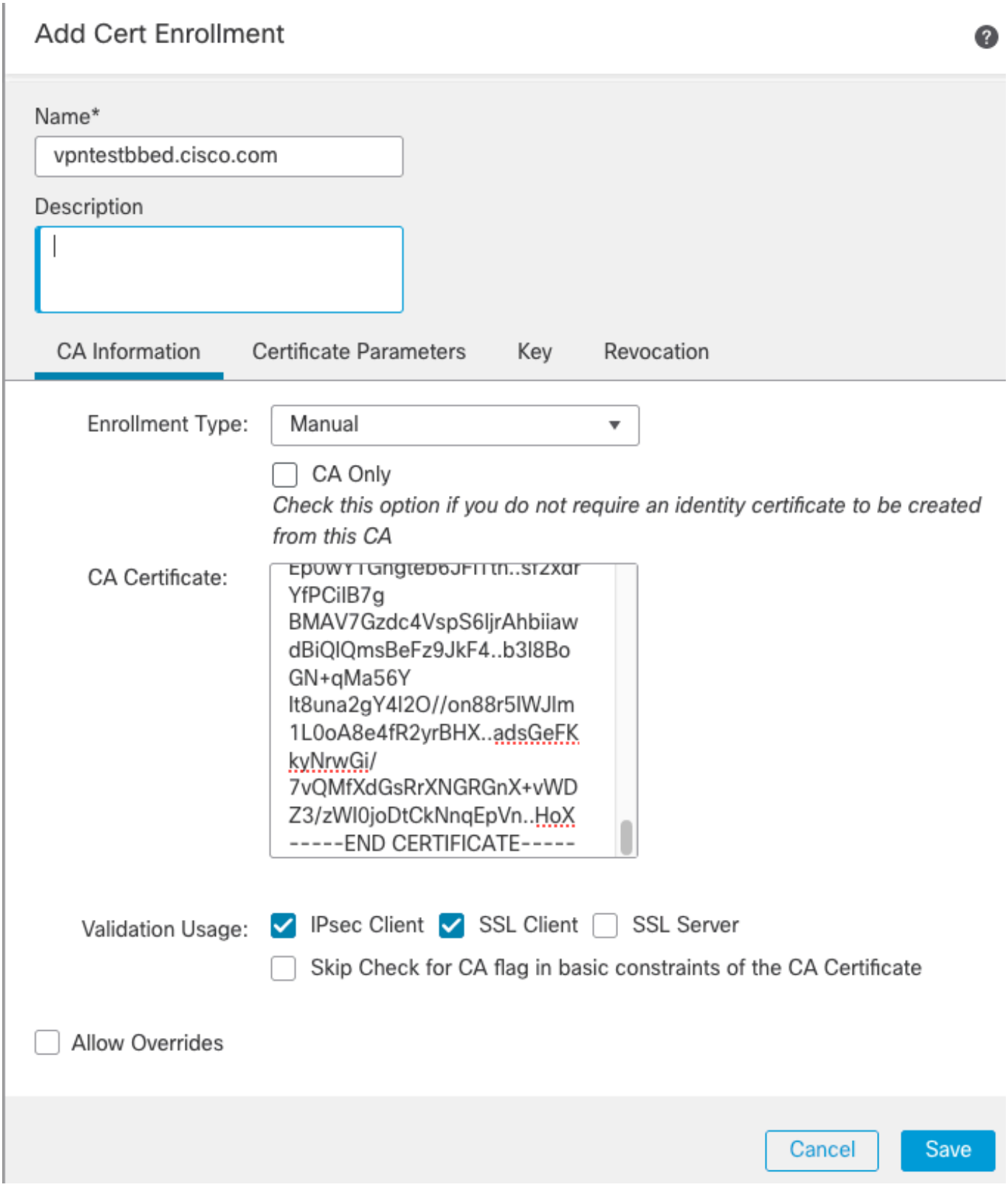
Existen limitaciones para la inscripción manual de certificados:

- En el FTD necesita el certificado de CA antes de generar el CSR.

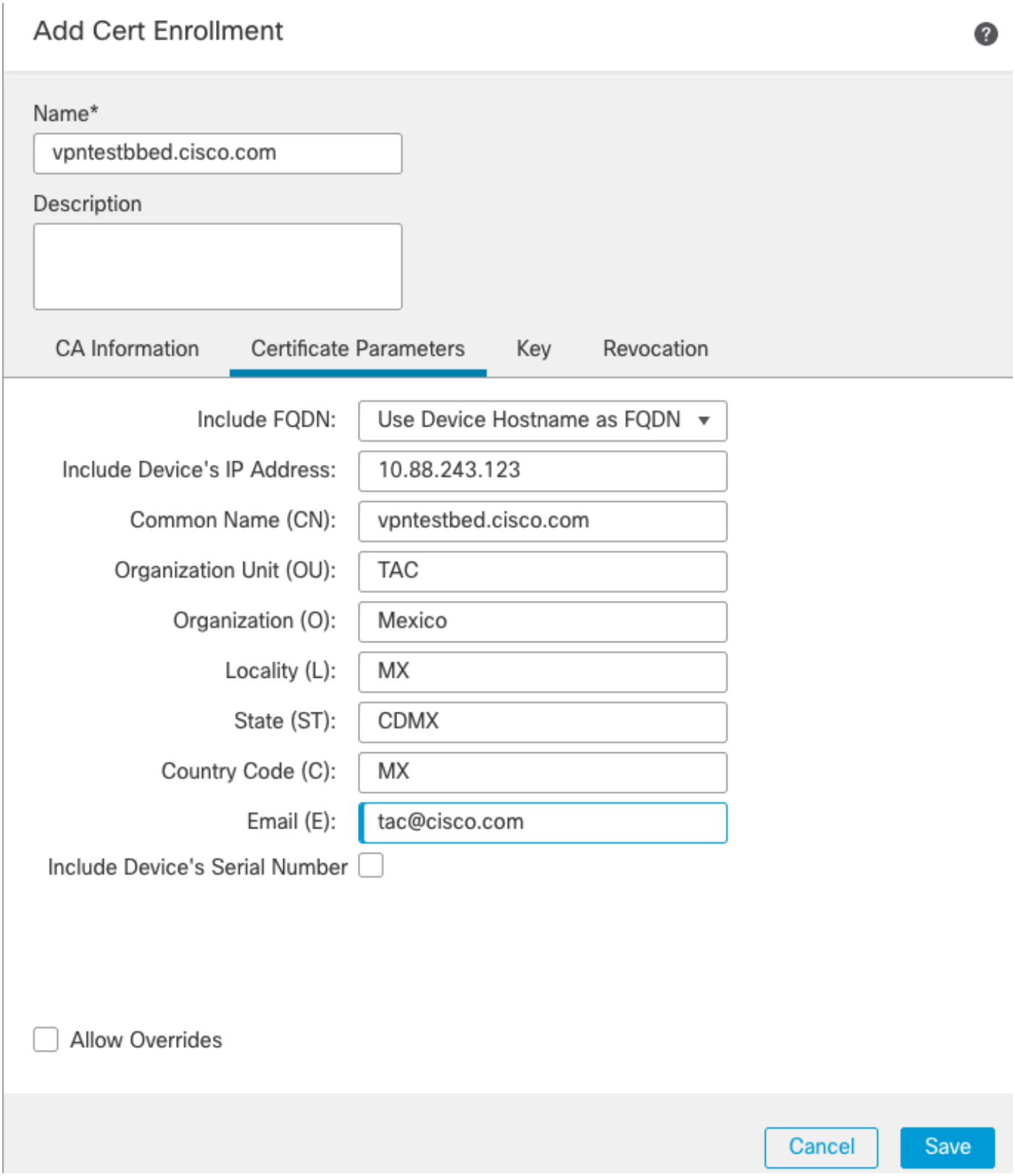
- Si el CSR se genera externamente, el método manual falla, se debe utilizar un método diferente (PKCS12).

Hay varios métodos para obtener un certificado en un dispositivo FTD, pero el más seguro y fácil es crear una solicitud de firma de certificado (CSR), firmarla con una autoridad de certificación (CA) y luego importar el certificado emitido para una clave pública, que estaba en CSR. A continuación se explica cómo hacerlo:

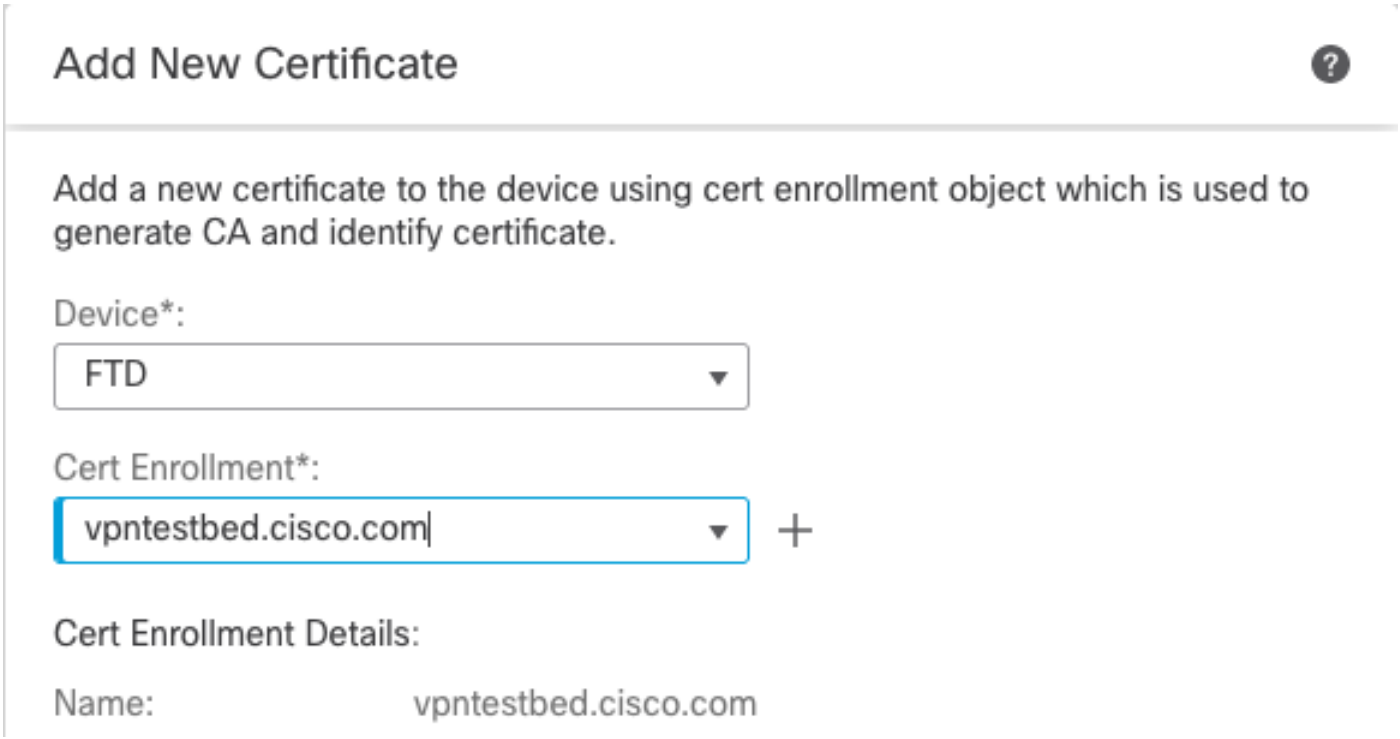
- Vaya a Objects > **Object Management > PKI > Cert Enrollment** Haga clic en **Add Cert Enrollment**.



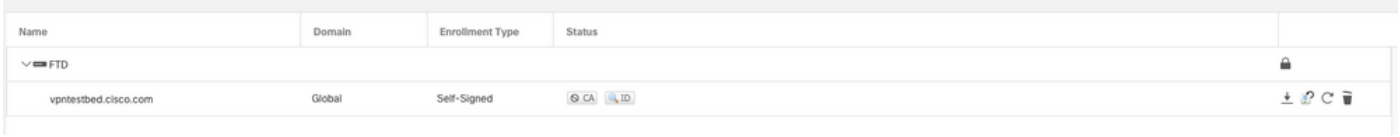
- Seleccionar Enrollment Type y pegue el certificado de la autoridad certificadora (CA) (el certificado que se utiliza para firmar la CSR).
- A continuación, vaya a la segunda pestaña y seleccione Custom FQDN y rellene todos los campos necesarios, por ejemplo:



- En la tercera ficha, seleccione Key Type, elija nombre y tamaño. Para RSA, 2048 bits es mínimo.
- Haga clic en Guardar y vaya a Devices > Certificates > Add > New Certificate.
- A continuación seleccione Device, y en Cert Enrollment seleccione el punto de confianza que acaba de crear y haga clic en Add:

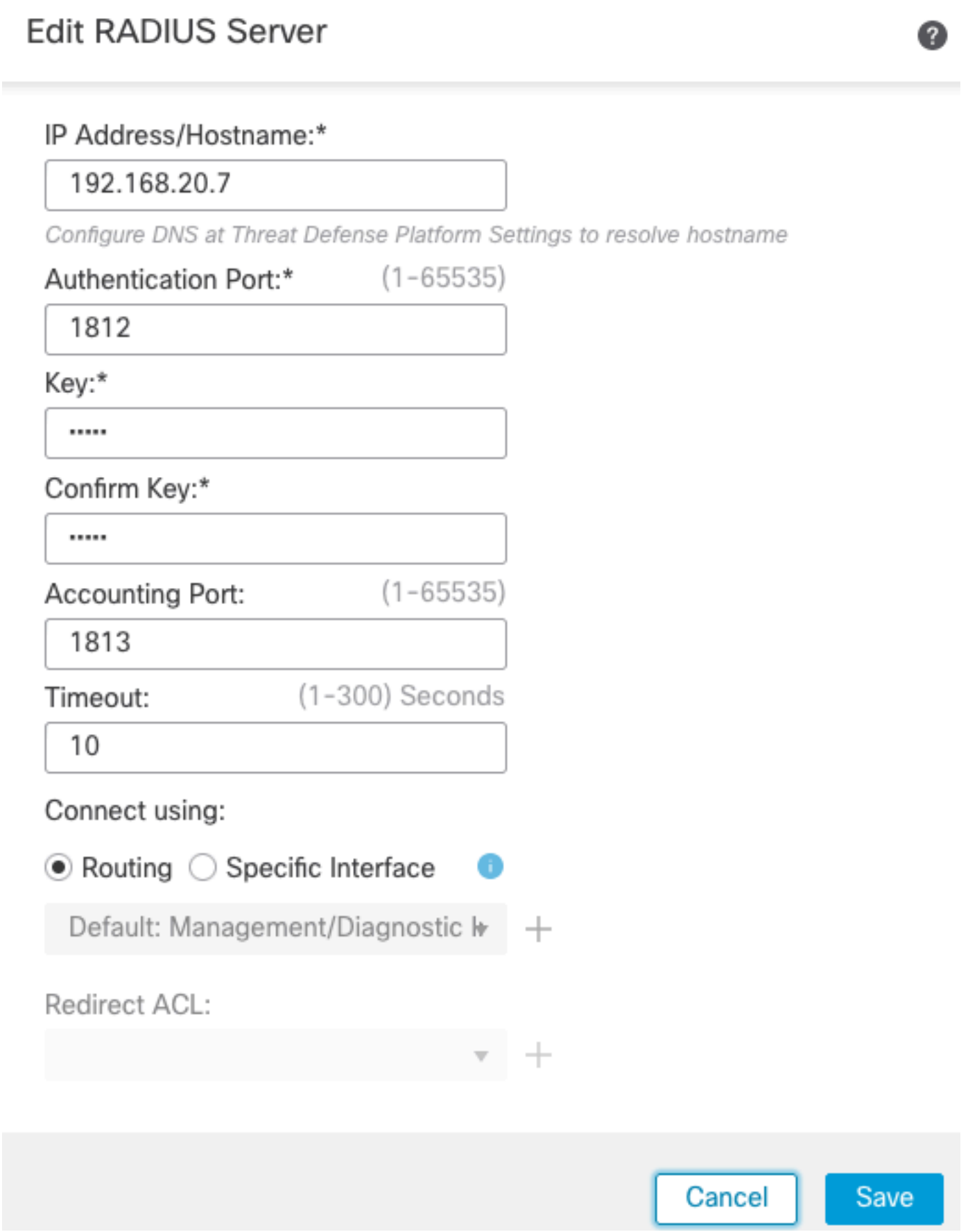


- Más adelante, junto al nombre del punto de confianza, haga clic en el botón icono, a continuación Yesy, a continuación, copie CSR en CA y fírmela. El certificado debe tener los mismos atributos que un servidor HTTPS normal.
- Después de recibir el certificado de CA en formato base64, selecciónelo en el disco y haga clic en Import. Cuando esto tenga éxito, verá:

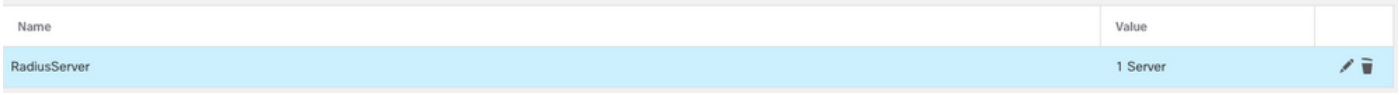


b) Configuración del servidor RADIUS

- Vaya a **Objects > Object Management > RADIUS Server Group > Add RADIUS Server Grou**p.
- Rellene el nombre y agregue la dirección IP junto con el secreto compartido. Haga clic en Save:

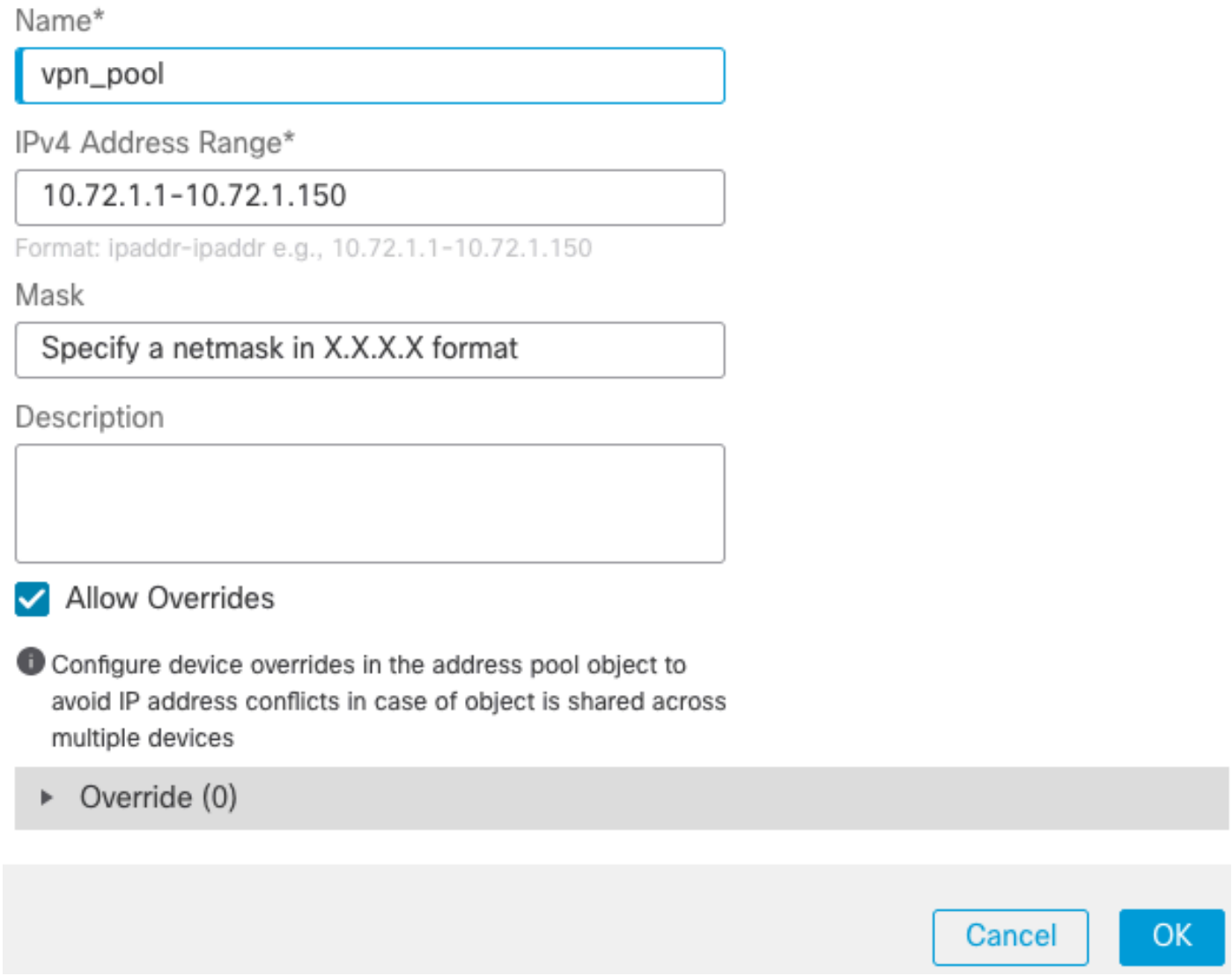


- Después de esto, verá el servidor en la lista:



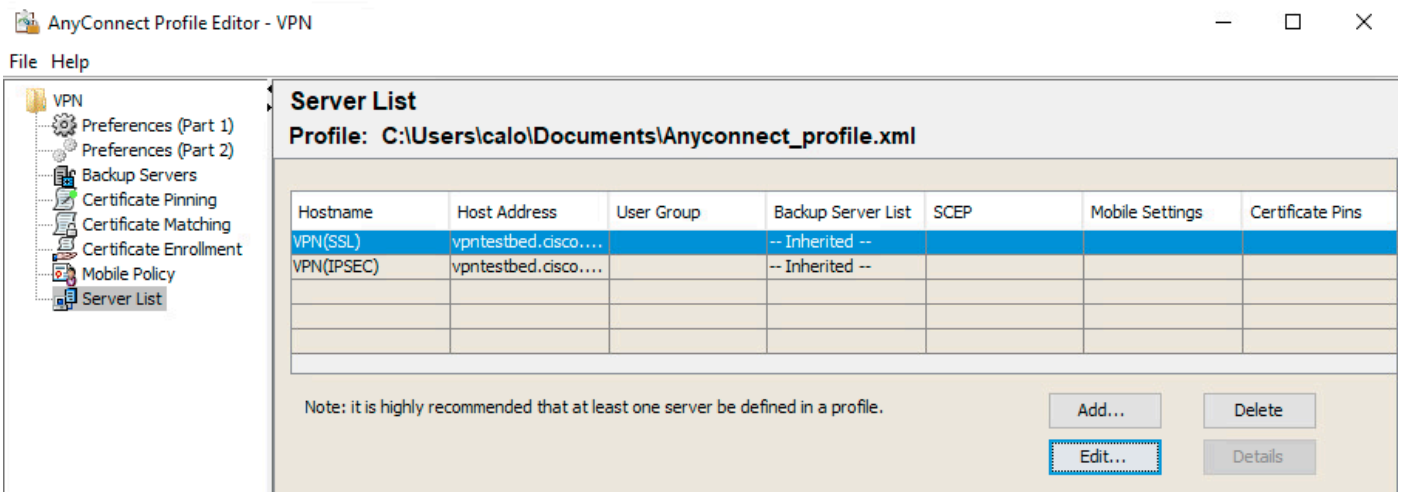
c) Crear un conjunto de direcciones para usuarios de VPN

- Vaya a **Objects > Object Management > Address Pools > Add IPv4 Pools**.
- Pon el nombre y el rango, la máscara no es necesaria:



d) Crear perfil XML

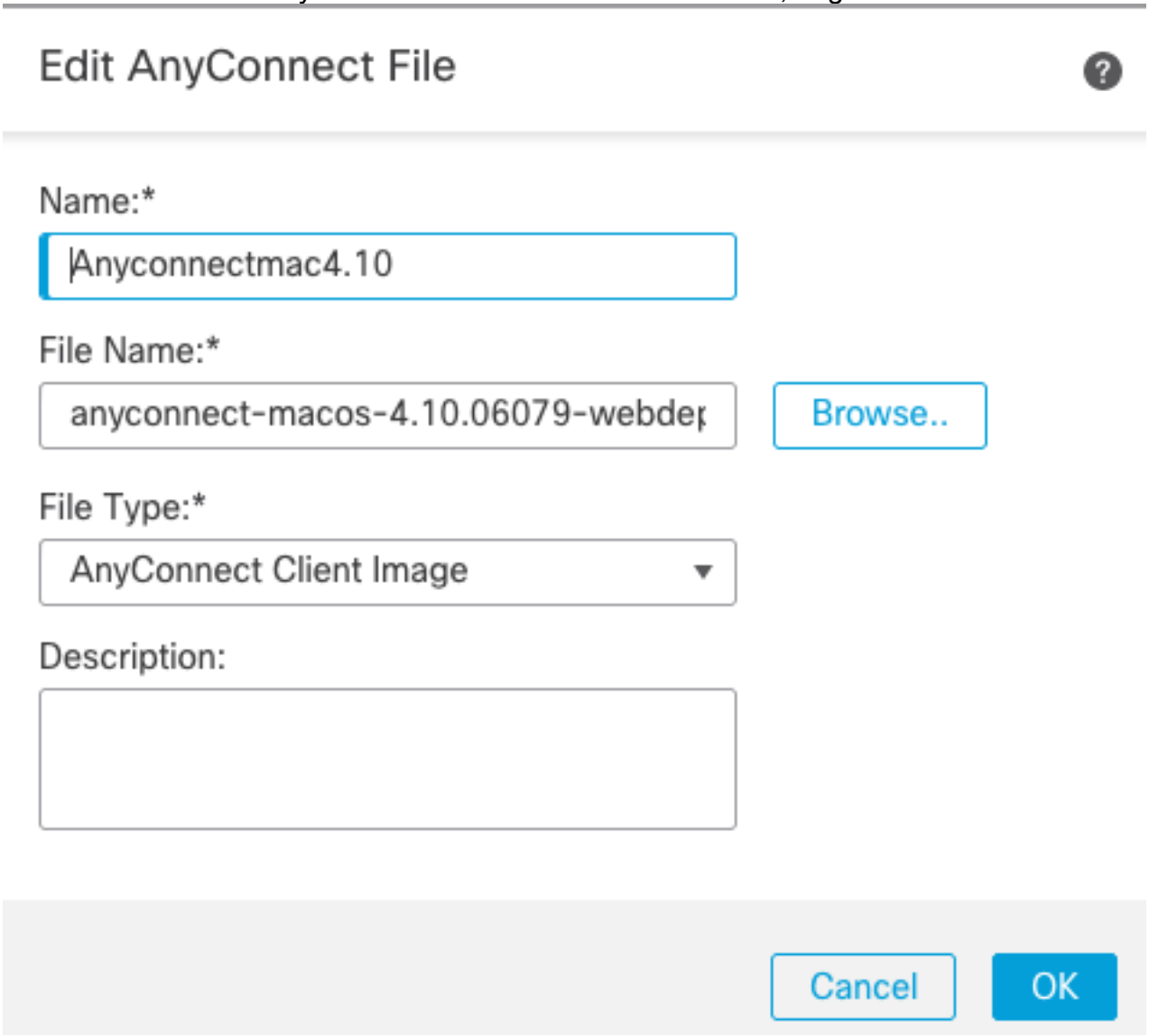
- Descargue el Editor de perfiles del sitio de Cisco y ábralo.
- Vaya a Server List > Add...
- Colocar nombre para mostrar y FQDN. Verá entradas en la Lista de servidores:



- Haga clic en OKy **File** > **Save as...**

e) Cargar imágenes de AnyConnect

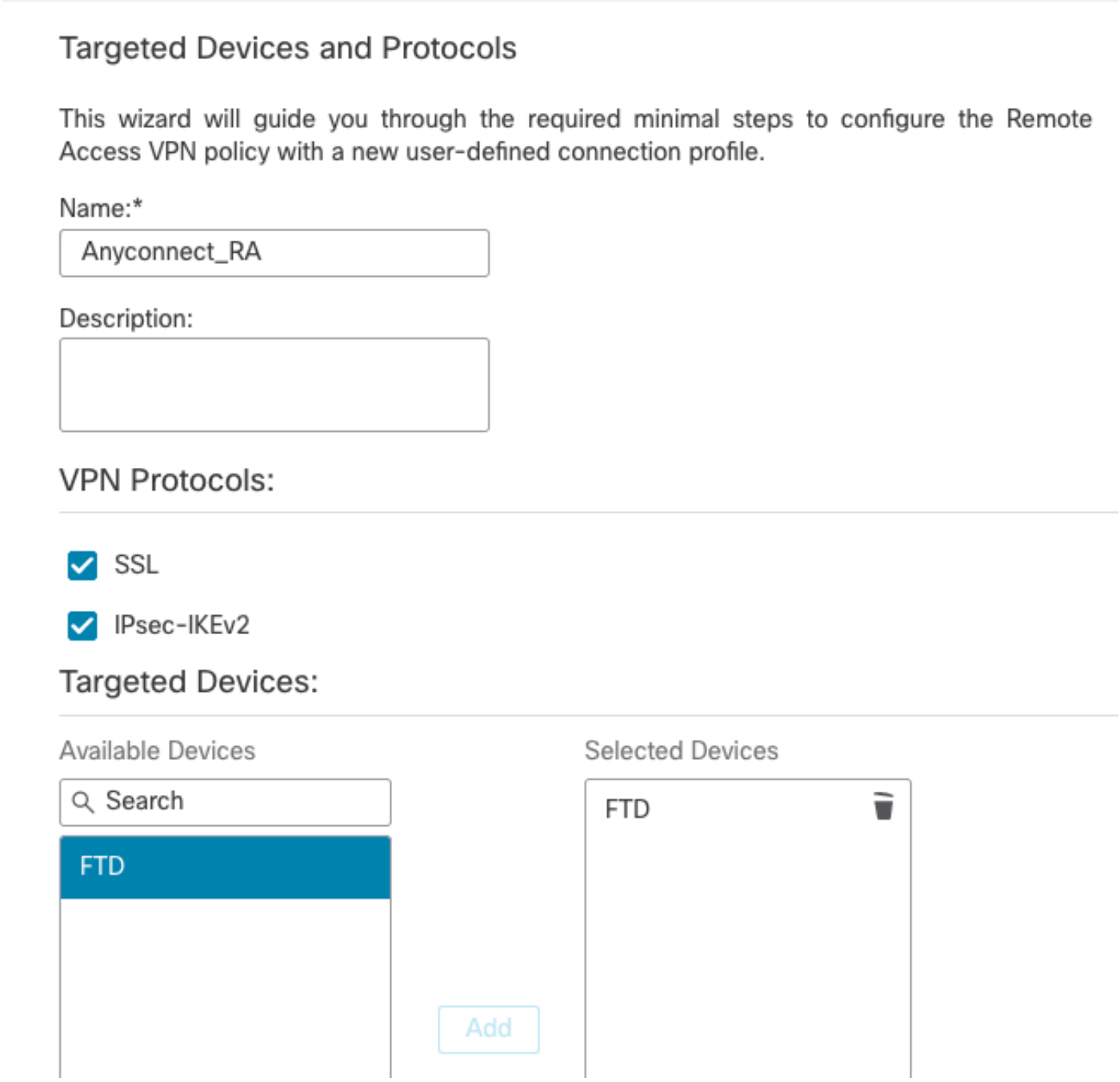
- Descargue imágenes de paquetes del sitio de Cisco.
- Vaya a Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
- Escriba el nombre y seleccione el archivo PKG del disco; haga clic en Save:



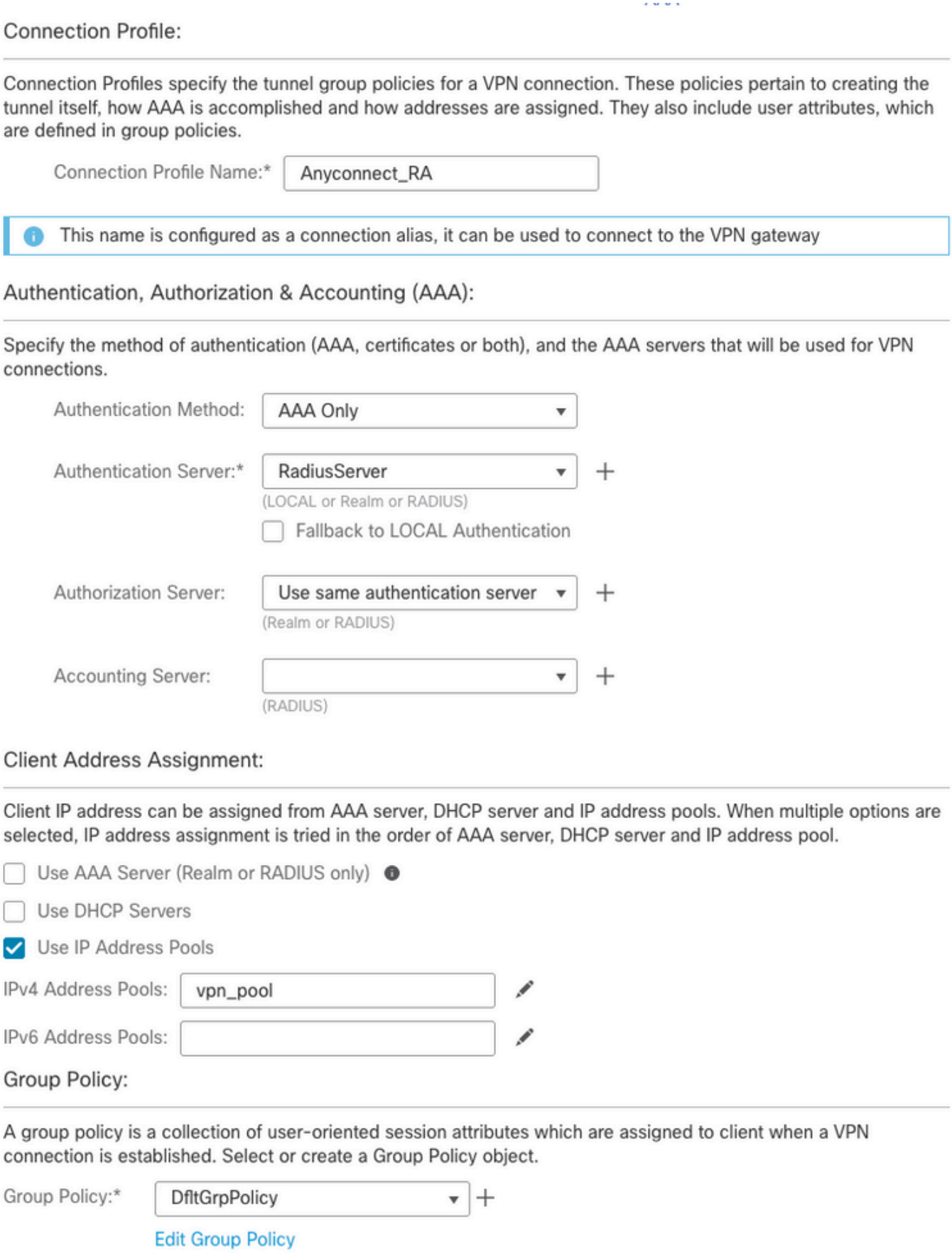
- Agregue más paquetes en función de sus propios requisitos.

2. Asistente para acceso remoto

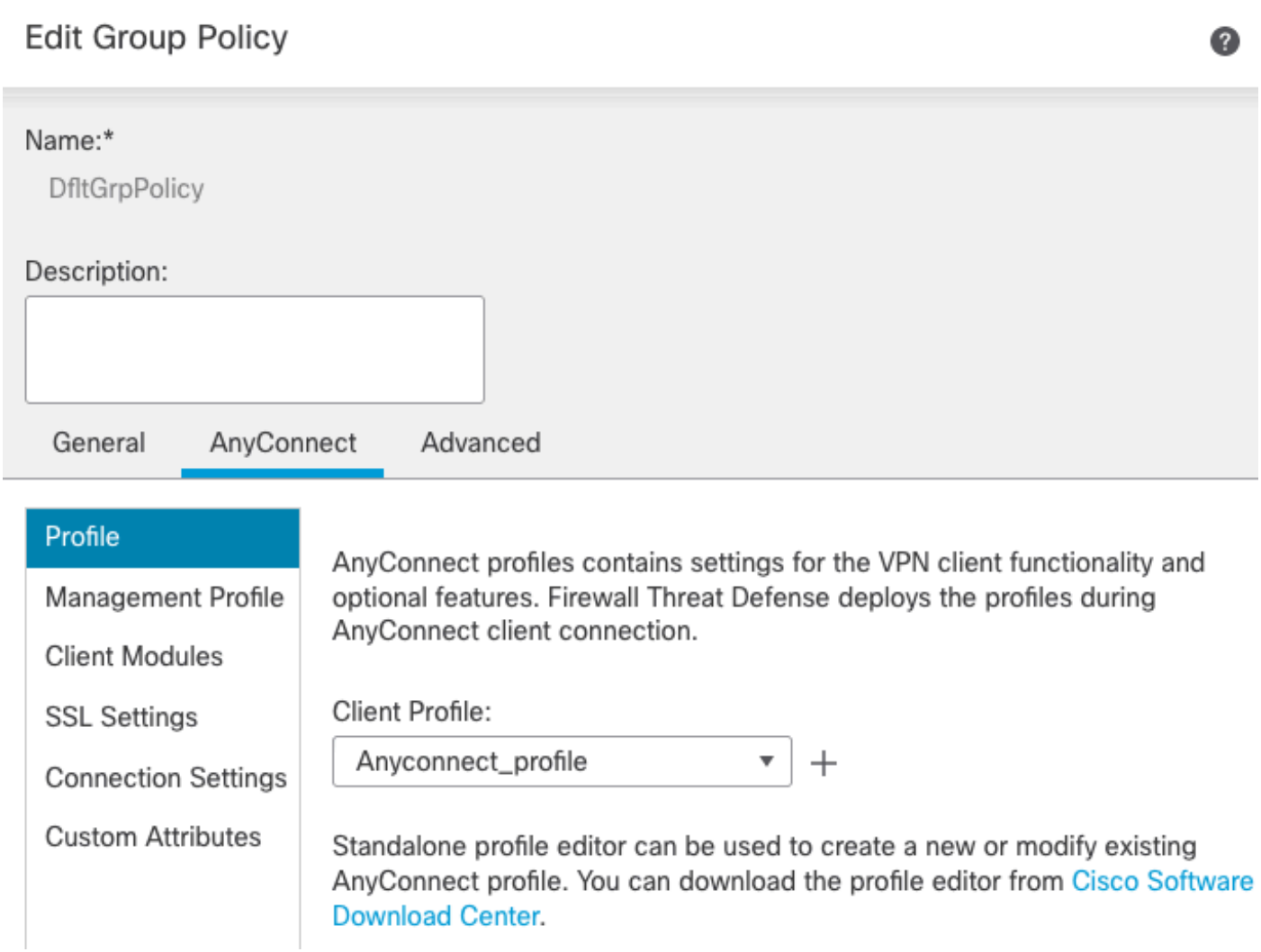
- Vaya a Devices > VPN > Remote Access > Add a new configuration.
- Asigne un nombre al perfil y seleccione el dispositivo FTD:



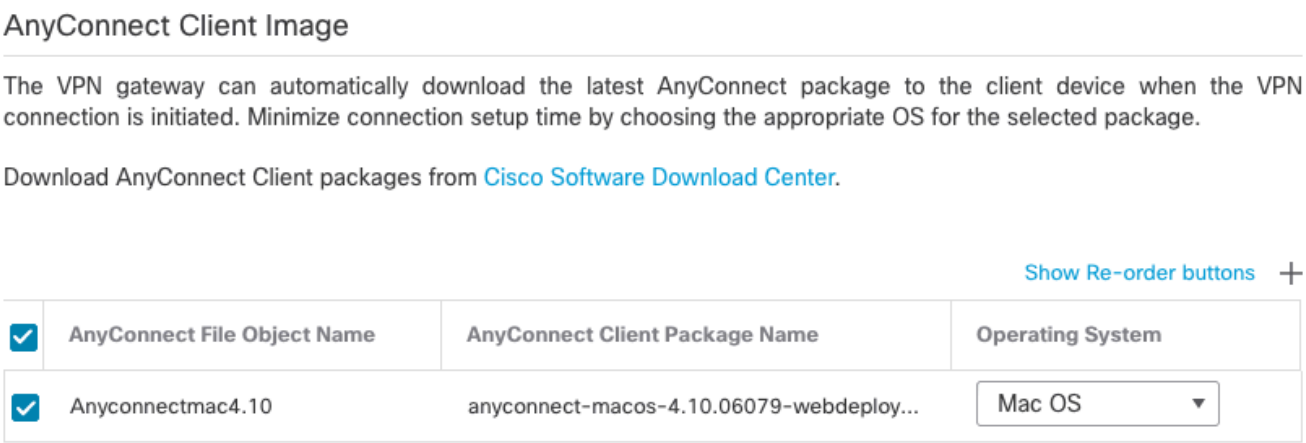
- En el paso Perfil de conexión, escriba **Connection Profile Name**, seleccione la **Authentication Server** y Address Pools que creó anteriormente:



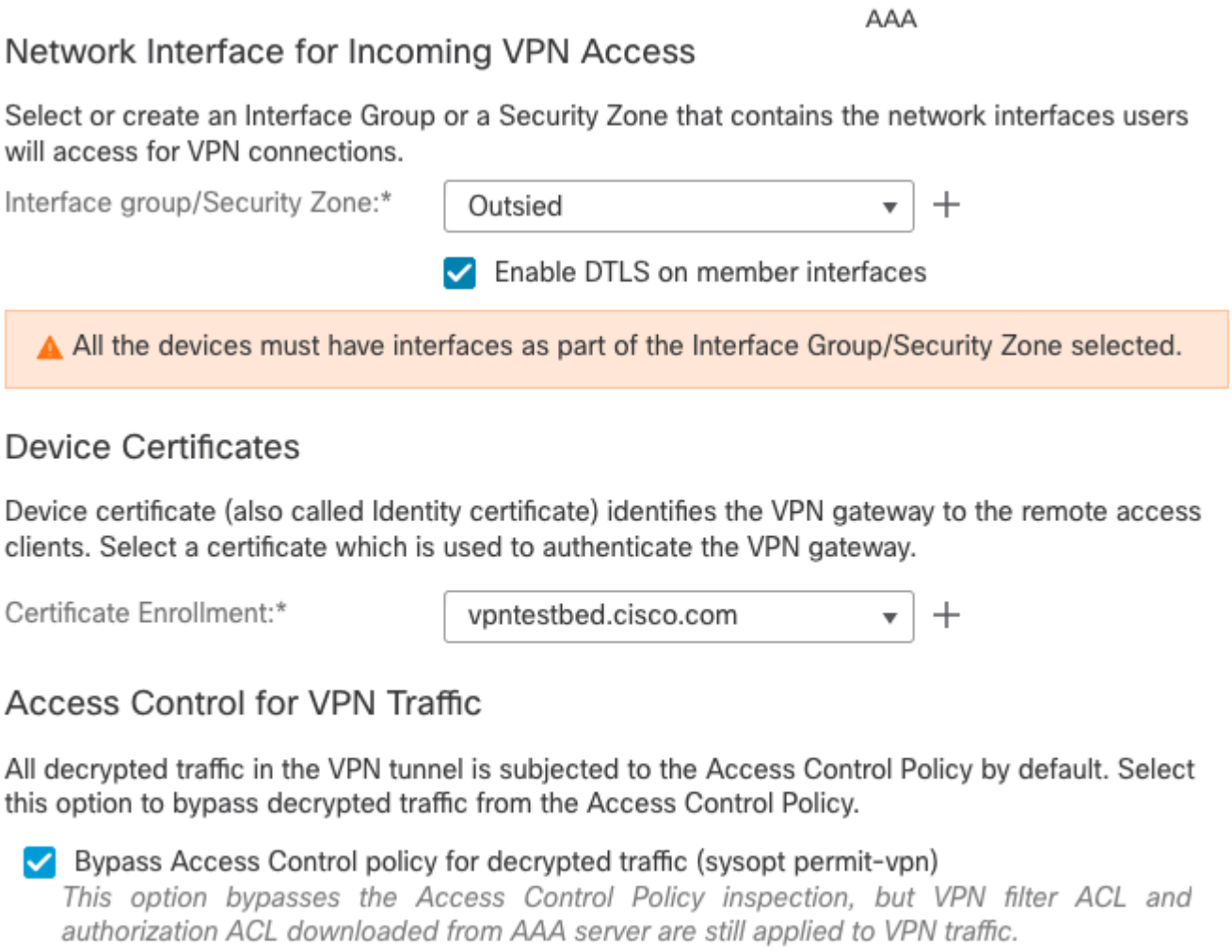
- Haga clic en **Edit Group Policy** y en la ficha AnyConnect, seleccione Client Profile, haga clic en Save:



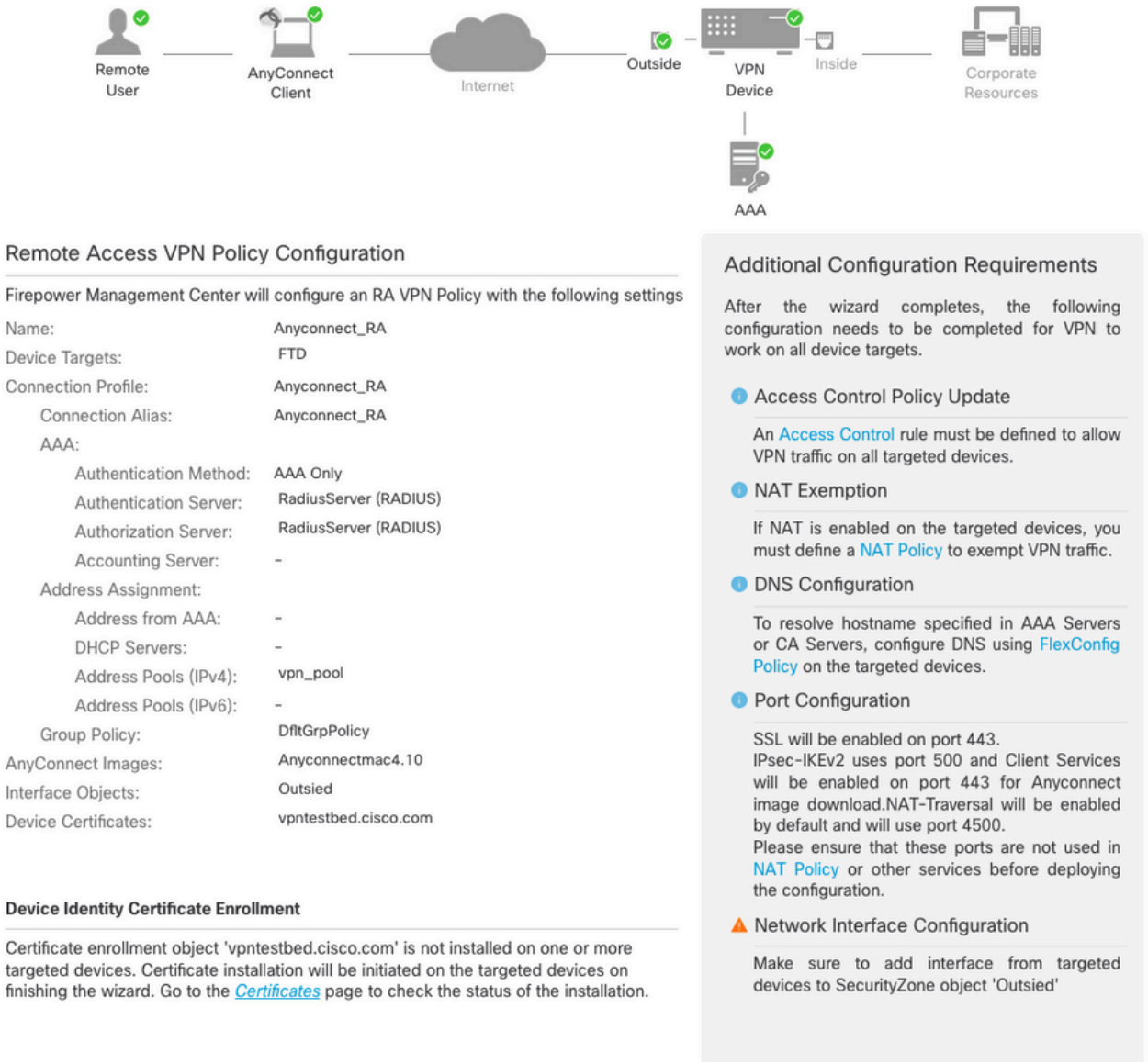
- En la página siguiente, seleccione imágenes de AnyConnect y haga clic en Next.



- En la siguiente pantalla, seleccione **Network Interface and Device Certificates**:



- Cuando todo esté configurado correctamente, puede hacer clic en Finish y luego Deploy:



- Esto copia toda la configuración junto con los certificados y los paquetes de AnyConnect en el dispositivo FTD.

Conexión

Para conectarse al FTD debe abrir un explorador, escribir un nombre DNS o una dirección IP que apunte a la interfaz externa. A continuación, inicie sesión con las credenciales almacenadas en el servidor RADIUS y siga las instrucciones de la pantalla. Una vez que se instala AnyConnect, debe poner la misma dirección en la ventana de AnyConnect y hacer clic en Connect.

Limitaciones

Actualmente no es compatible con FTD, pero está disponible en ASA:

- La selección de interfaz en el servidor RADIUS no se admite en Firepower Threat Defense6.2.3 o versiones anteriores. La opción de interfaz se omite durante la implementación.
- Un servidor RADIUS con autorización dinámica requiere Firepower Threat Defense6.3 o posterior para que funcione la autorización dinámica.

- FTDposture VPN no admite el cambio de política de grupo a través de la autorización dinámica o el cambio de autorización RADIUS (CoA).
- Personalización de AnyConnect (mejora: ID de error de Cisco CSCvq87631)
- Scripts de AnyConnect
- localización de AnyConnect
- Integración de WSA
- Mapa criptográfico dinámico IKEv2 simultáneo para VPN RA y L2L (Mejora: ID de error de Cisco CSCvr52047)
- Módulos AnyConnect (NAM, Hostscan, AMP Enabler, SBL, Umbrella, Web Security, etc.): DART se instala de forma predeterminada (Mejoras de AMP Enabler y Umbrella: ID de error de Cisco CSCvs03562 e ID de error de Cisco CSCvs06642).
- TACACS, Kerberos (autenticación KCD y RSA SDI)
- Proxy de explorador

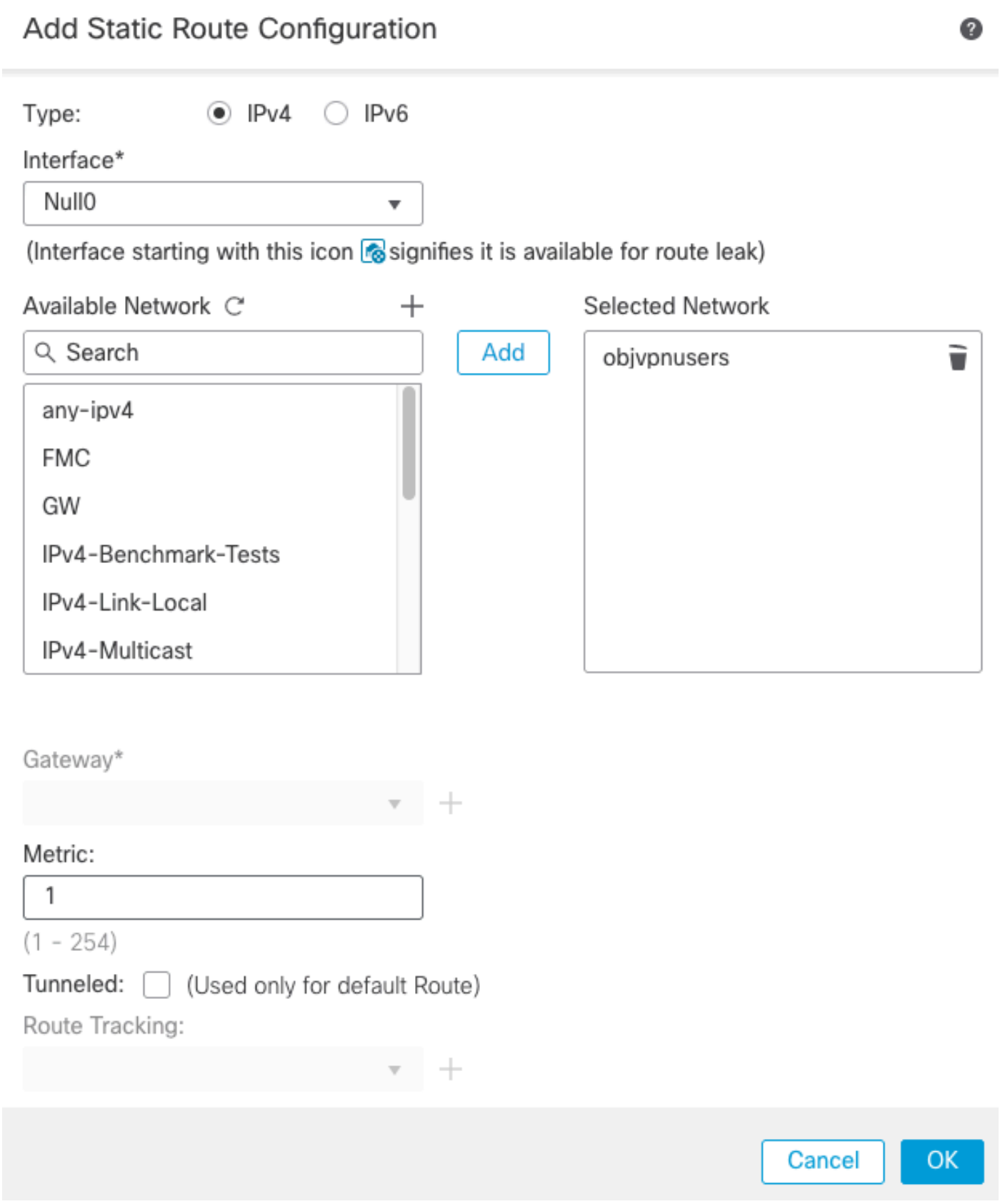
Observaciones de seguridad

De forma predeterminada, el sysopt connection permit-vpnestá desactivada. Esto significa que debe permitir el tráfico que proviene del conjunto de direcciones en la interfaz externa a través de la política de control de acceso. Aunque la regla de prefiltro o control de acceso se agrega para permitir solamente el tráfico VPN, si el tráfico de texto sin cifrar coincide con los criterios de la regla, se permite erróneamente.

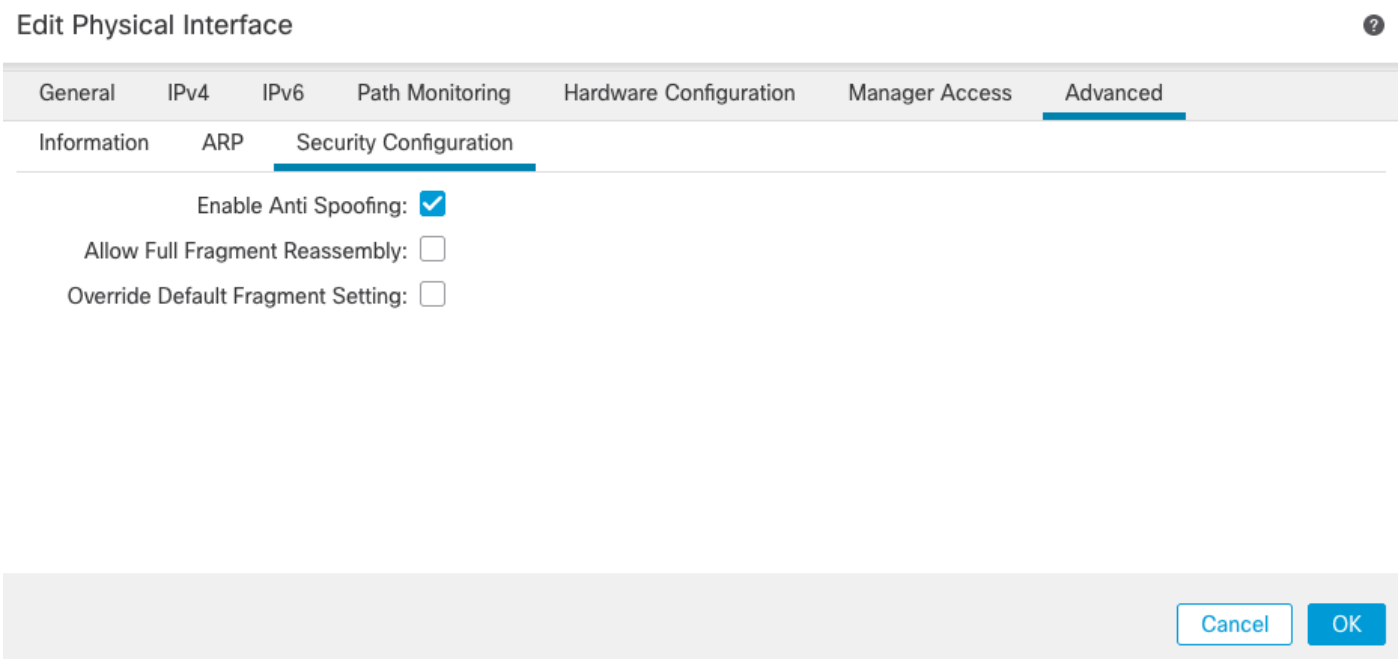
Hay dos enfoques para este problema. En primer lugar, la opción recomendada por el TAC es habilitar la antisimulación (en ASA se la conocía como Unicast Reverse Path Forwarding - uRPF) para la interfaz externa y, en segundo lugar, habilitar sysopt connection permit-vpn para omitir completamente la inspección de Snort. La primera opción permite una inspección normal del tráfico que va hacia y desde los usuarios de VPN.

a) Habilitar uRPF

- Cree una ruta nula para la red utilizada por los usuarios de acceso remoto, definida en la sección C. Vaya a Devices > Device Management > Edit > Routing > Static Route y seleccione Add route



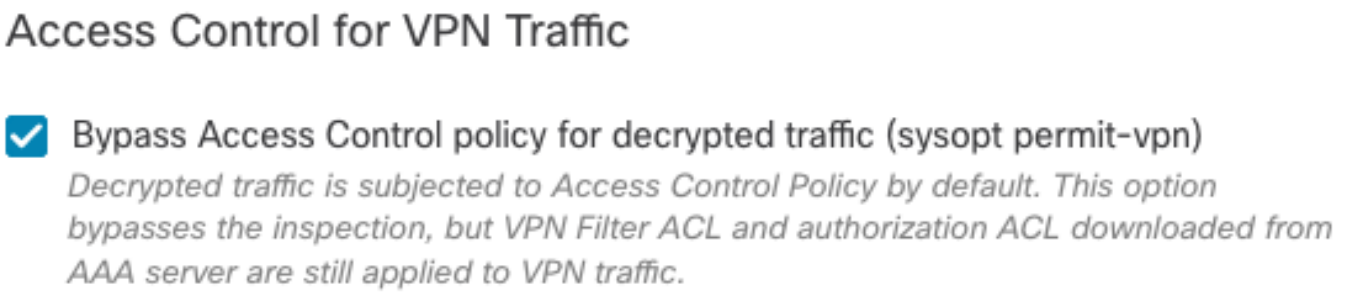
- Luego, habilite uRPF en la interfaz donde terminan las conexiones VPN. Para encontrar esto, navegue hasta **Devices > Device Management > Edit > Interfaces > Edit > Advanced > Security Configuration > Enable Anti Spoofing**.



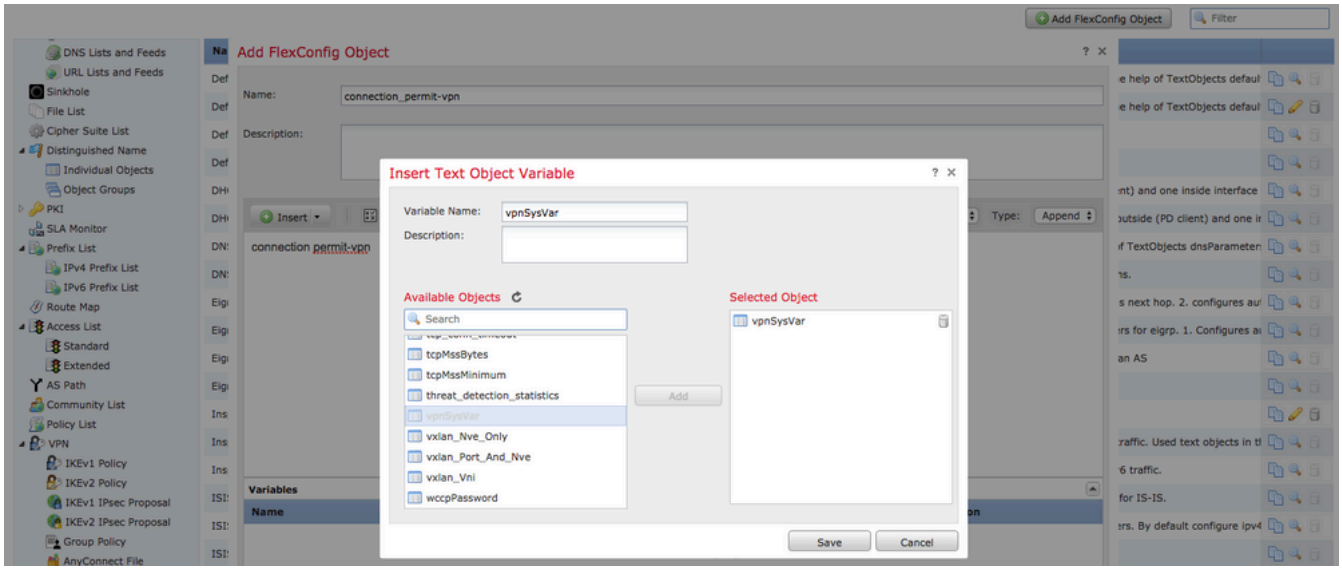
Cuando un usuario está conectado, la ruta de 32 bits se instala para ese usuario en la tabla de ruteo. Borre el tráfico de texto originado en las otras direcciones IP no utilizadas del conjunto que son descartadas por uRFP. Para ver una descripción de **Anti-Spoofing**consulte Establecer parámetros de configuración de seguridad en Firepower Threat Defence.

b) Habilitar Sysopt connection permit-vpn Opción

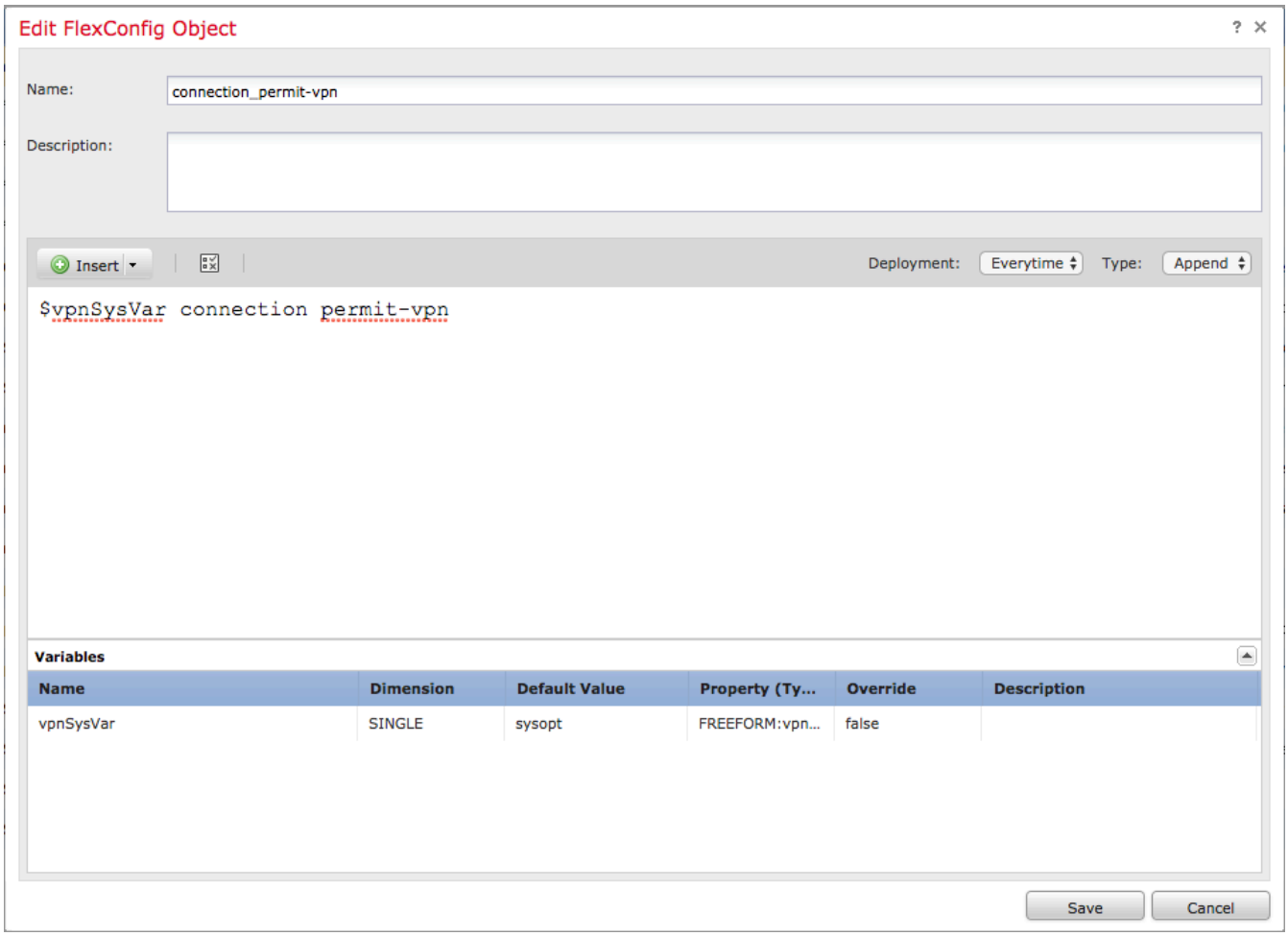
- Si tiene la versión 6.2.3 o posterior, existe la opción de hacerlo con el asistente o en Devices > VPN > Remote Access > VPN Profile > Access Interfaces.



- Para las versiones anteriores a la 6.2.3, vaya a Objects > Object Management > FlexConfig > Text Object > Add Text Object.
- Cree una variable de objeto de texto, por ejemplo: vpnSysVar una sola entrada con valor sysopt.
- Vaya a Objects**> Object Management > FlexConfig > FlexConfig Object > Add FlexConfig Object.**
- Cree el FlexConfig objeto con CLI connection permit-vpn.
- Inserte la variable de objeto de texto en el FlexConfig en la CLI con **$vpnSysVar connection permit-vpn**. Haga clic en Save:



- Aplique el FlexConfigobjeto como **Append** y seleccione implementación para Everytime:



- Vaya a**Devices > FlexConfig** y editar la directiva actual o crear una nueva con New Policy botón.
- Agregue solo los elementos creados FlexConfig, haga clic en Save.
- Implementar la configuración para aprovisionar**sysopt connection permit-vpn**en el dispositivo.

Después de esto, sin embargo, no puede utilizar la política de control de acceso para inspeccionar el tráfico que proviene de los usuarios. Aún puede utilizar el filtro VPN o ACL descargable para filtrar el tráfico de usuario.

Si ve paquetes descartados con Snort de los usuarios de VPN, comuníquese con TAC y haga

referencia al Id. de bug de Cisco CSCvg91399.

Información Relacionada

- Asistencia técnica y descargas de Cisco

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).