Configuración del VPN de acceso remoto de AnyConnect en FTD

Contenido

Introducción

Este documento proporciona a un ejemplo de la configuración para la versión 6.2.2 y posterior de la defensa de la amenaza de FirePOWER (FTD), ése permite que el VPN de acceso remoto utilice Transport Layer Security (TLS) y el intercambio de las claves de Internet versión 2 (IKEv2). Como cliente, Cisco AnyConnect será utilizado, que se apoya en las plataformas múltiples.

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- VPN básico, TLS y conocimiento IKEv2
- Autenticación básica, autorización, y estadísticas (AAA) y conocimiento RADIUS
- Experimente con el centro de administración de FirePOWER

Componentes usados

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

- Cisco FTD 6.2.2
- AnyConnect 4.5

Configuración

1. Preresiquites

Para pasar a través del Asisitente del Acceso Remoto en el centro de administración de FirePOWER, primero usted necesitará seguir los siguientes pasos:

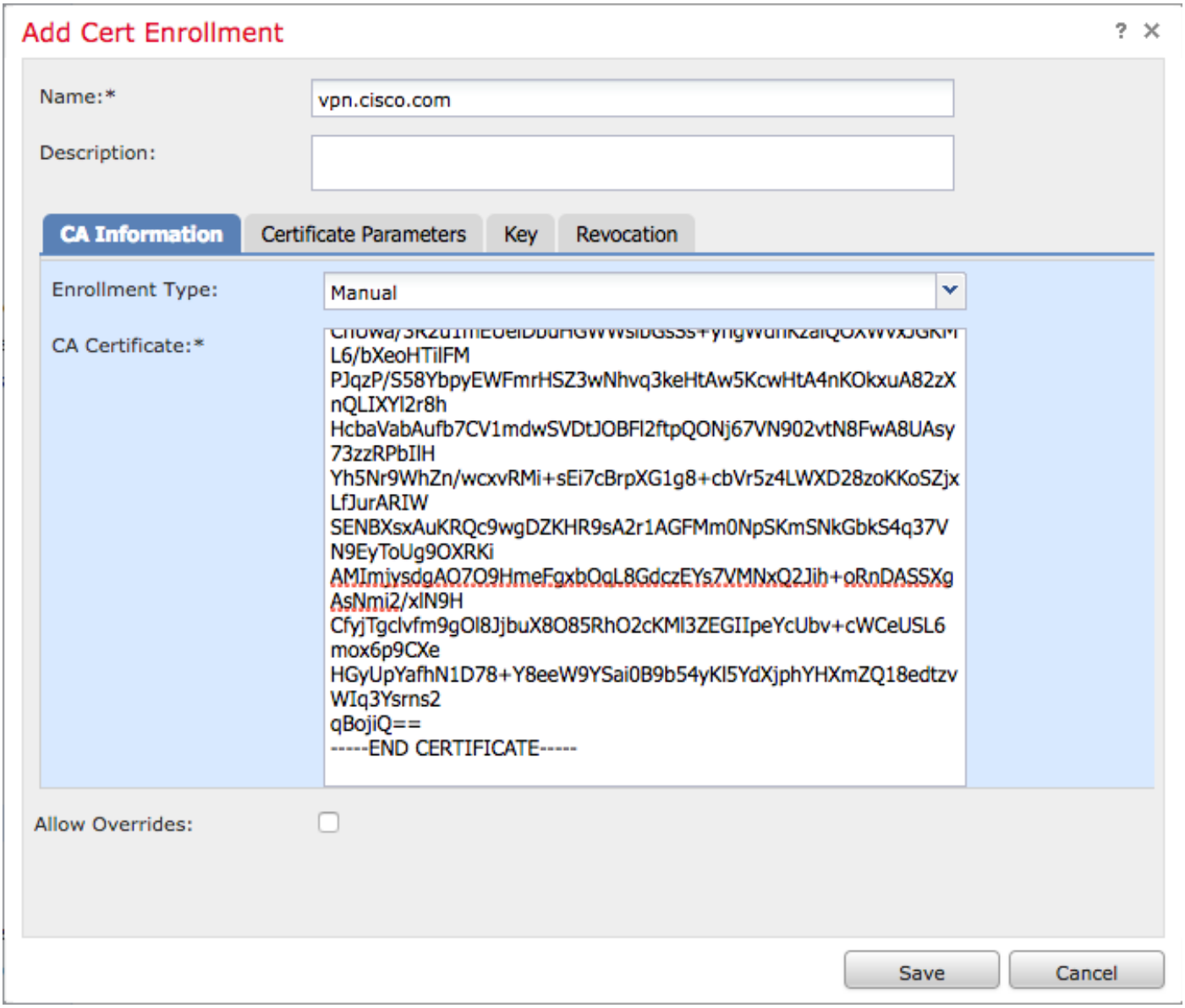
- cree un certificado usado para la autenticación de servidor,
- configure el RADIUS o al servidor LDAP para la autenticación de usuario,
- cree a la agrupación de direcciones para los usuarios de VPN,
- cargue por teletratamiento las imágenes de AnyConnect para diversas Plataformas.

a) importación del certificado SSL

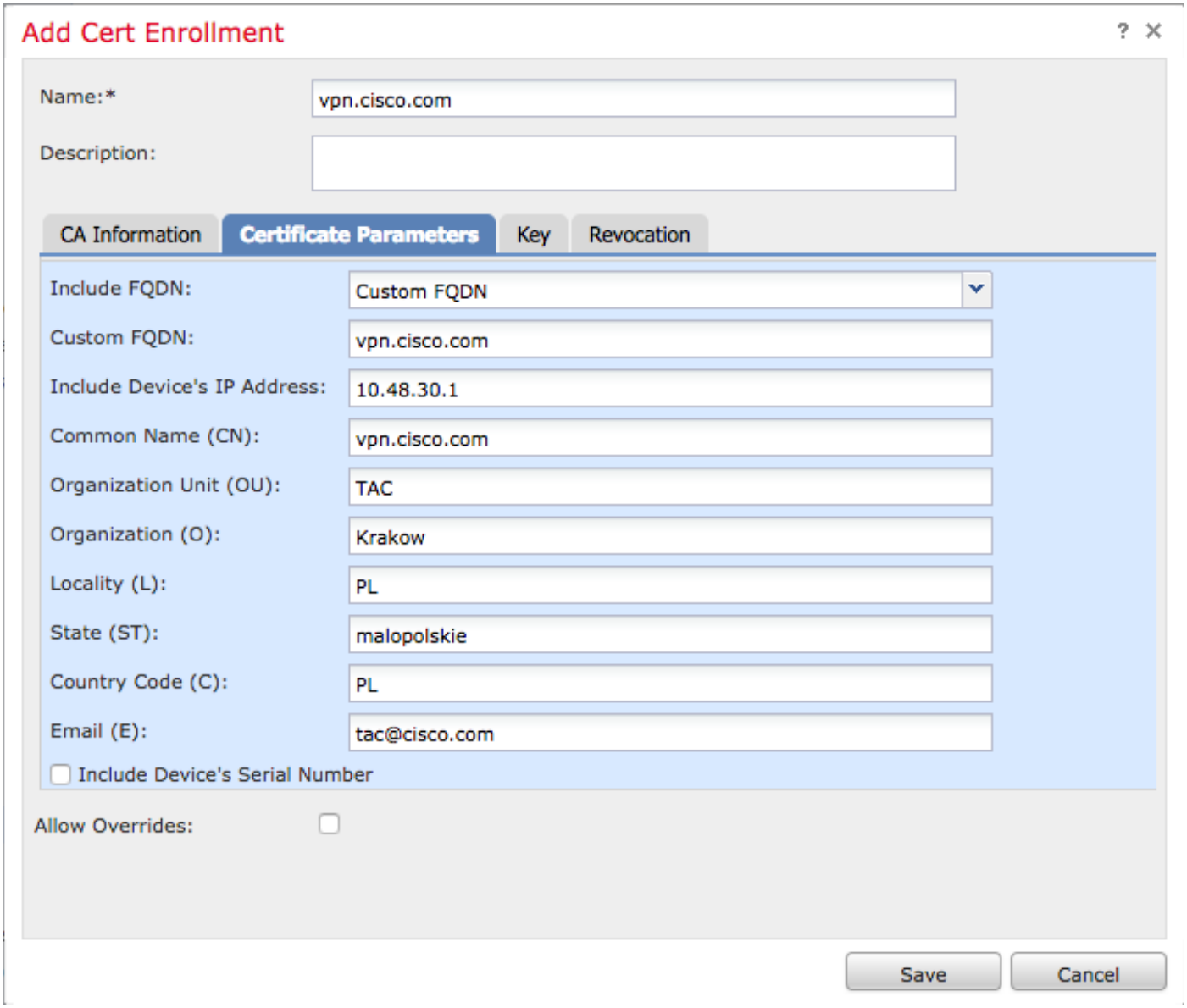
Los Certificados son esenciales cuando usted configura AnyConnect. Solamente los Certificados basados RSA se utilizan en el SSL e IPSec. Los Certificados elípticos del algoritmo de la firma digital de la curva (ECDSA) se utilizan en IPSec, pero él no son posibles desplegar el nuevo paquete de AnyConnect o el perfil XML cuando se utiliza el certificado basado ECDSA. Significa que usted puede utilizarlo para IPSec, pero usted tendrá que predesplegar el paquete de AnyConnect y el perfil XML a cada usuario y cualquier cambio en el perfil XML tendrán que ser reflejados manualmente en cada cliente (bug: CSCtx42595). Además el certificado debe tener extensión alternativa sujeta del nombre con el nombre y/o la dirección IP DNS para evitar los errores en los buscadores Web.

Hay varios métodos para obtener un certificado en el dispositivo FTD, pero el seguro y fácil es crear un pedido de firma de certificado (CSR), lo firma y entonces Import Certificate (Importar certificado) publicado para la clave pública, que estaba en el CSR. Aquí es cómo hacer eso:

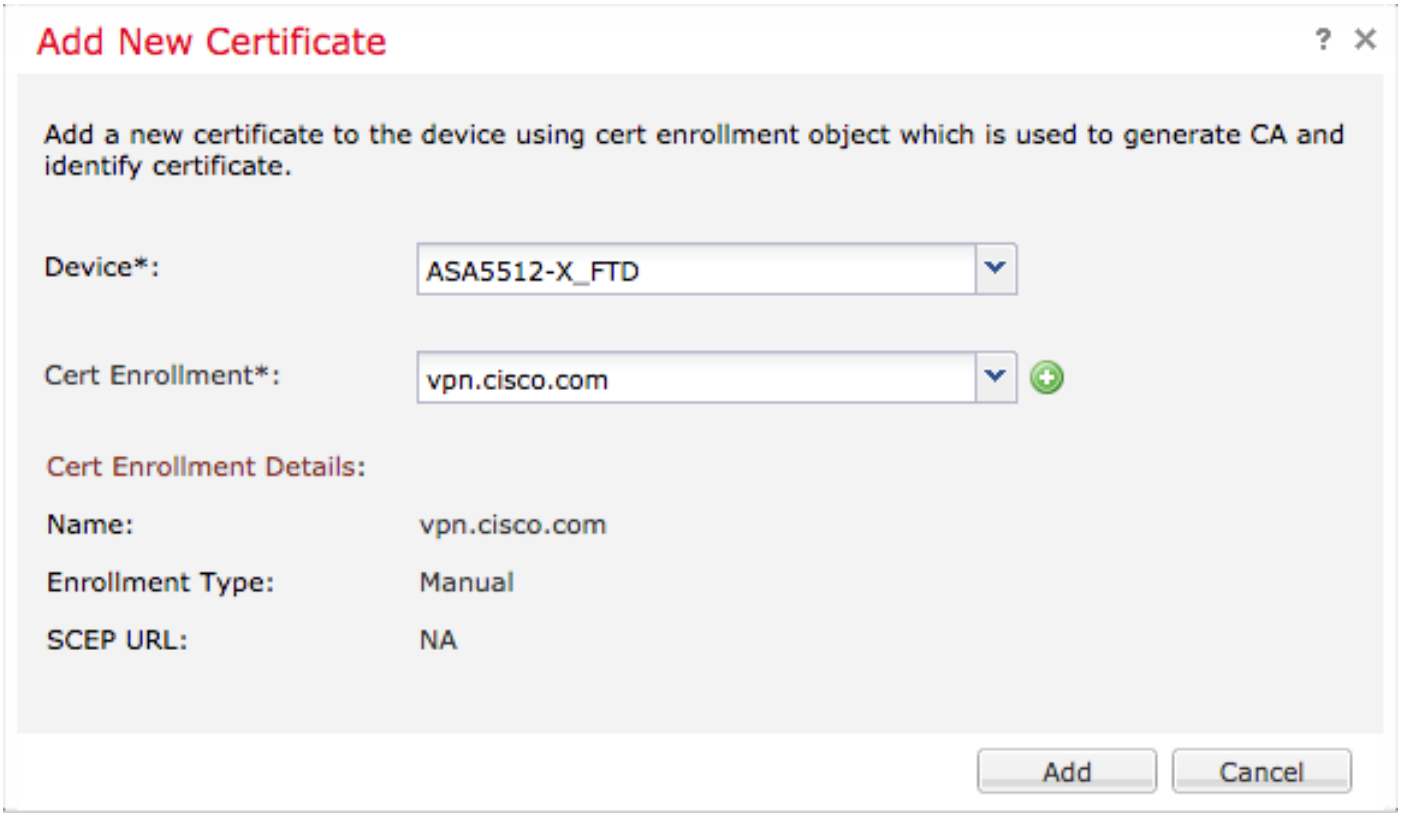
- Vaya a los **objetos** > a la **Administración del objeto** > a **PKI** > a la **inscripción CERT**, haga clic en **agregan la inscripción CERT**:



- Seleccione el **tipo de la inscripción** y pegue el certificado del Certificate Authority (CA),
- Entonces van la segunda tabulación y la **aduana** selecta **FQDN** y llenan todos los campos necesarios, eg.:



- En la tercera tabulación, seleccione el tipo dominante, elija el nombre y el tamaño. Para el RSA, 2048 bytes son mínimos.
- Haga clic la salvaguardia y vaya a los **dispositivos** > a los **Certificados** > **agregan** > **nuevo certificado**. Entonces seleccione el **dispositivo,** y bajo **inscripción CERT** seleccione el trustpoint que usted acaba de crear, tecleo **agregan**:



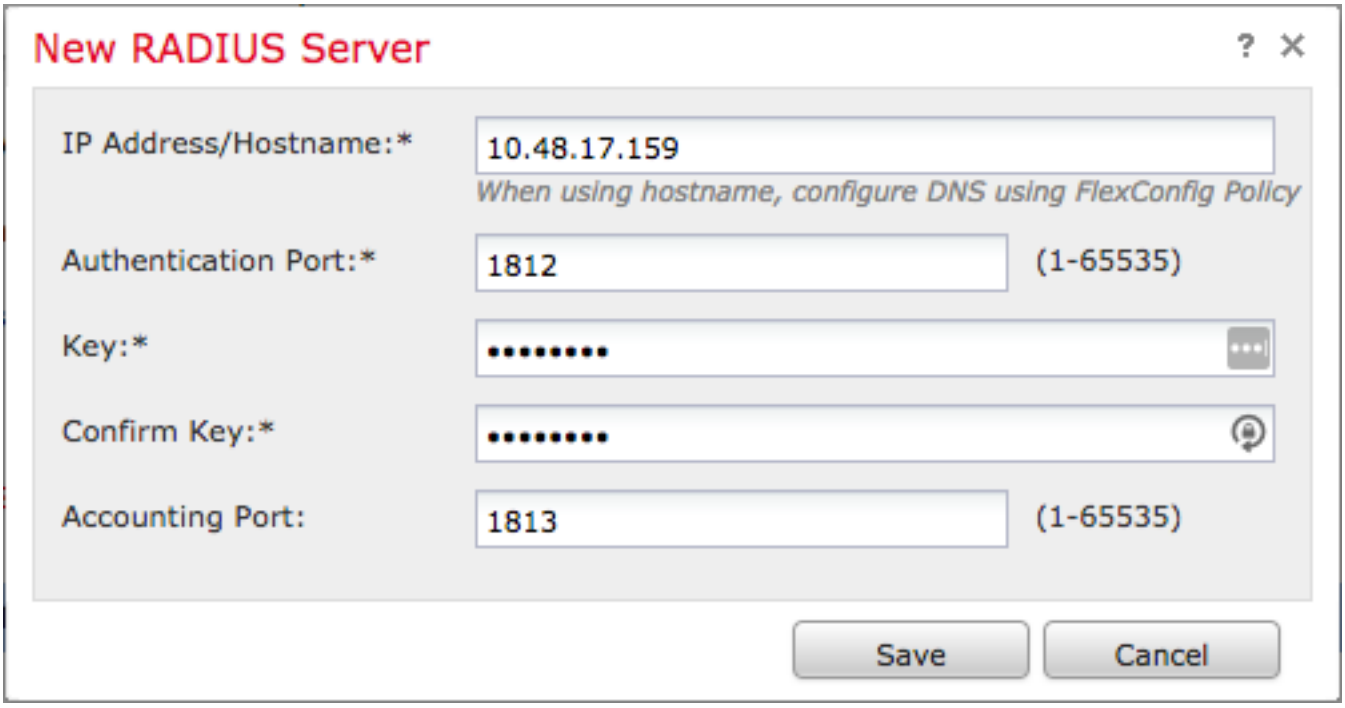
- Más adelante, al lado del nombre del trustpoint, haga clic en el icono, entonces **sí y después ese CSR de la copia al CA y fírmelo. El certificado debe tener atributos como servidor HTTPS normal.**
- Después de recibir el certificado del CA en el formato base64, selecciónelo del disco y haga clic la **importación**. Cuando esto tiene éxito, usted debe ver:

Name	Enrollment Type	CA Certificate	Identity Certificate
ASA5512-X_FTD			
vpn.cisco.com	Manual	Available	Available

b) configure al servidor de RADIUS

En el platftorm FTD, la base de datos de usuarios locales no puede ser utilizada, así que usted necesita el RADIUS o al servidor LDAP para la autenticación de usuario. Para configurar el RADIUS:

- Vaya a los **objetos** > a la **Administración del objeto** > al **grupo de servidor de RADIUS** > **agregan al grupo de servidor de RADIUS**.
- Llene el nombre y agregue la dirección IP junto con el secreto compartido, **salvaguardia del** tecleo:



- Después que usted debe ver el servidor en la lista:

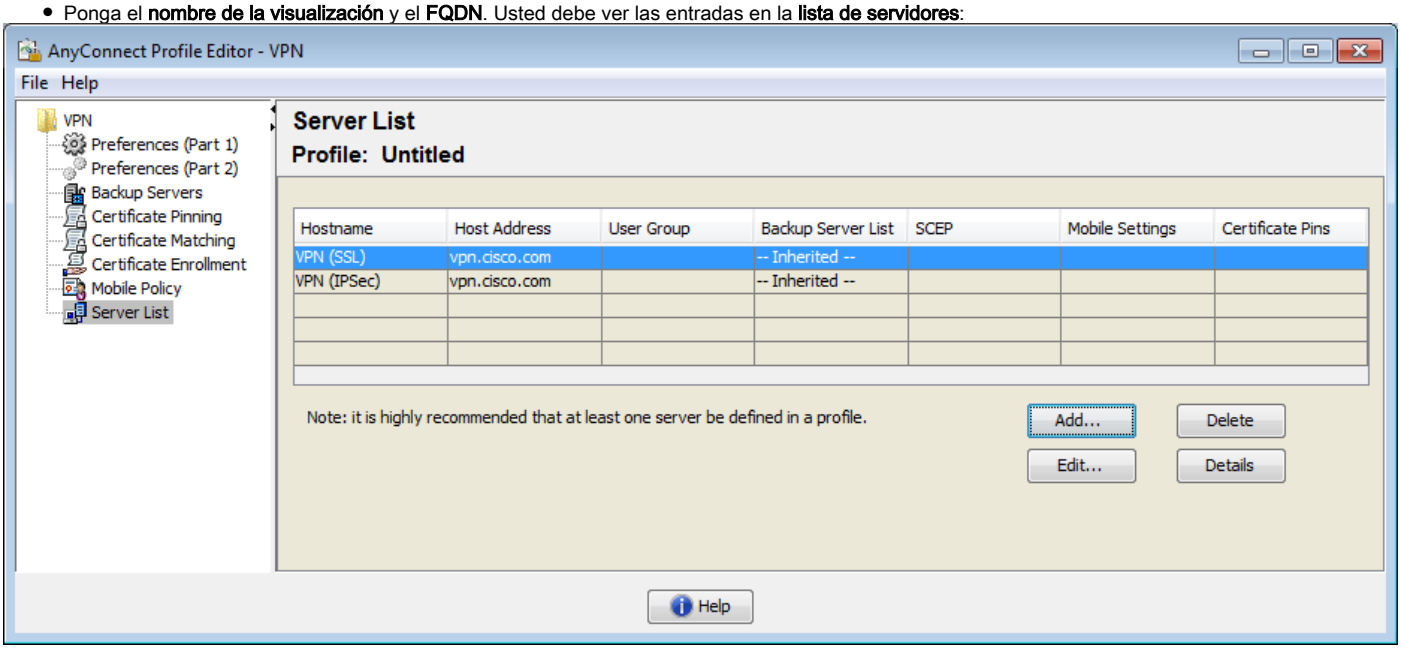
c) crear a la agrupación de direcciones para los usuarios de VPN

- Vaya a las **piscinas de los objetos** > de la **Administración** > del **direccionamiento del objeto** > **agregan las piscinas IPv4**:
- Ponga el nombre y el rango, máscara no es necesario:

d) crear el perfil XML

- Descargue el editor del perfil del sitio de Cisco y ábralo.
- Vaya a la **lista de servidores** > **agregan...**

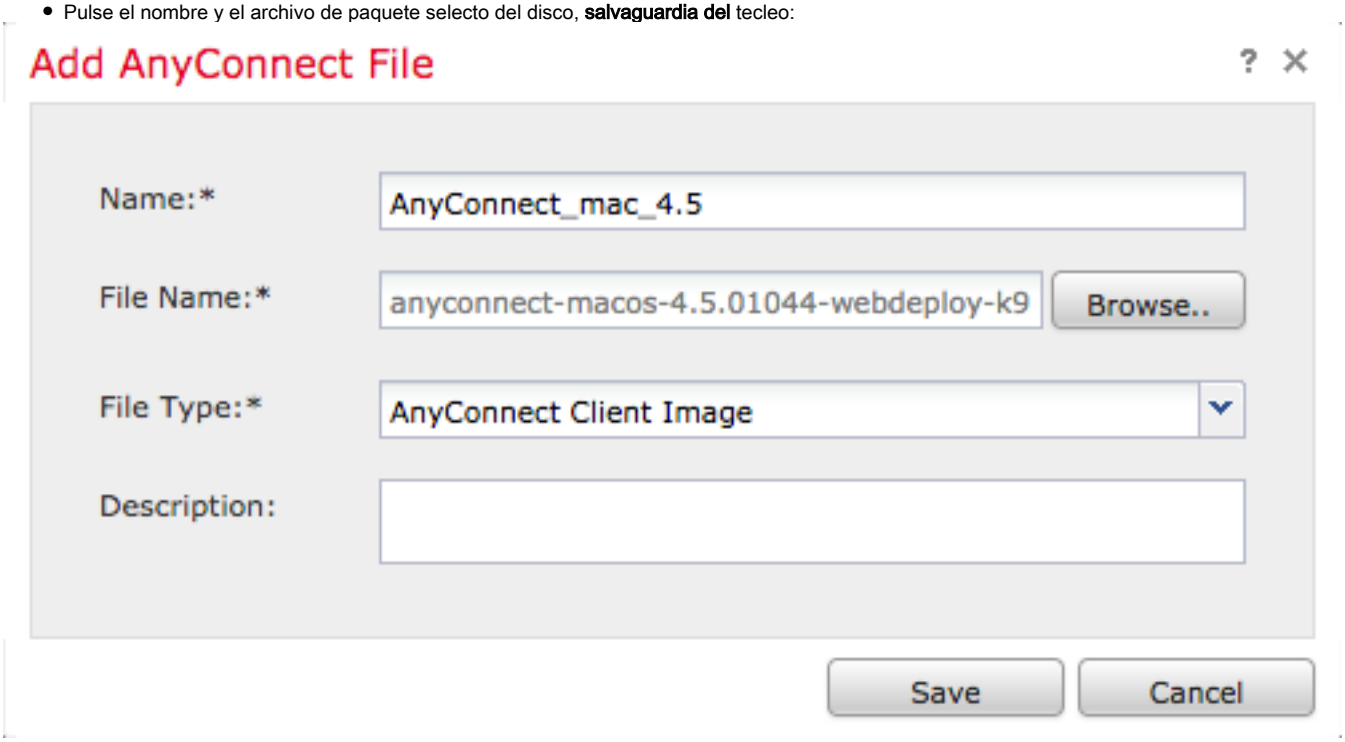
- Ponga el **nombre de la visualización** y el **FQDN**. Usted debe ver las entradas en la **lista de servidores**:



- **AUTORIZACIÓN y File (Archivo) > Save as (Guardar como) del tecleo…**

e) imágenes de AnyConnect que cargan por teletratamiento

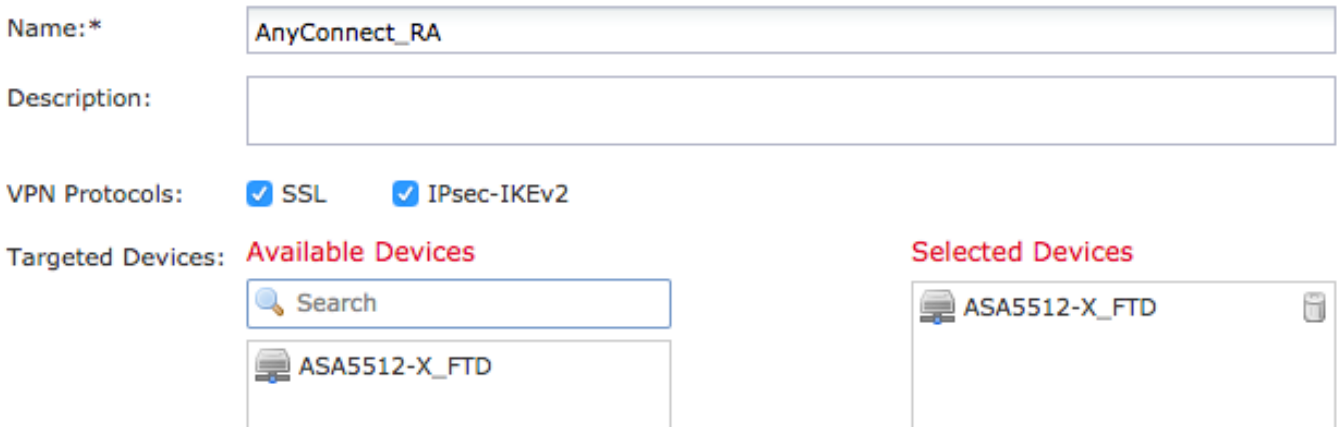
- Imágenes del paquete de la transferencia directa del sitio de Cisco.
- Vaya a los **objetos** > a la **Administración del objeto** > al **fichero VPN** > de **AnyConnect** > **agregan el fichero de AnyConnect**.
- Pulse el nombre y el archivo de paquete selecto del disco, **salvaguardia del** tecleo:



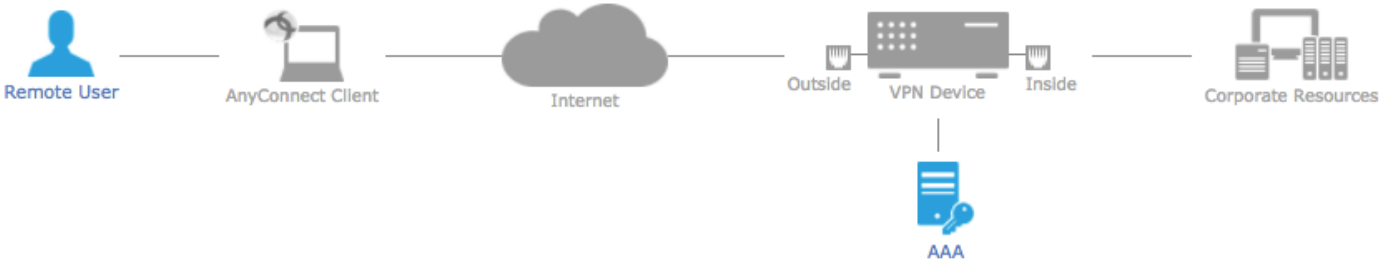
- Agregue más paquetes dependiendo de sus requisitos.

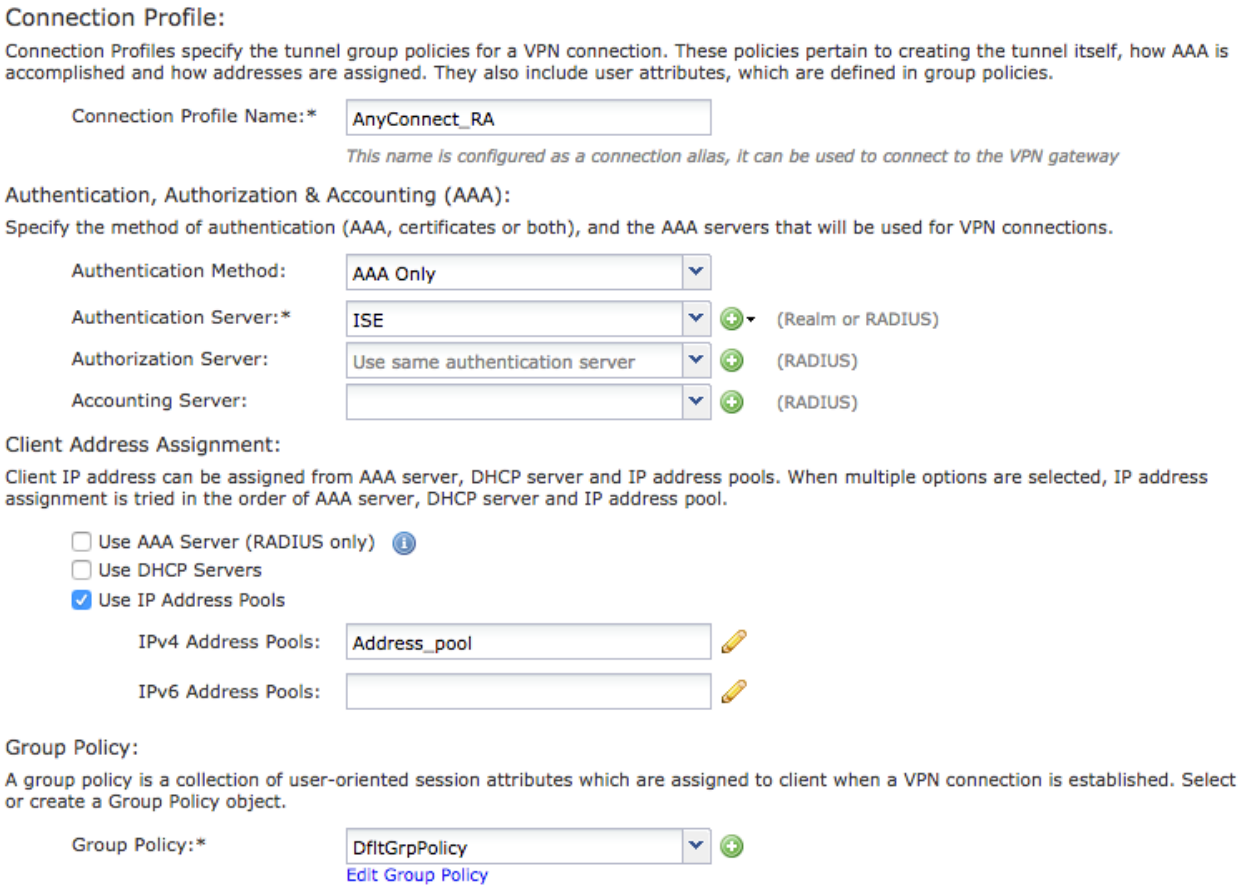
2. Asisitente del Acceso Remoto

- Vaya a los **dispositivos** > al **VPN** > al **Acceso Remoto** > **agregan una nueva configuración**.
- Nombre el perfil según sus necesidades, dispositivo selecto FTD:

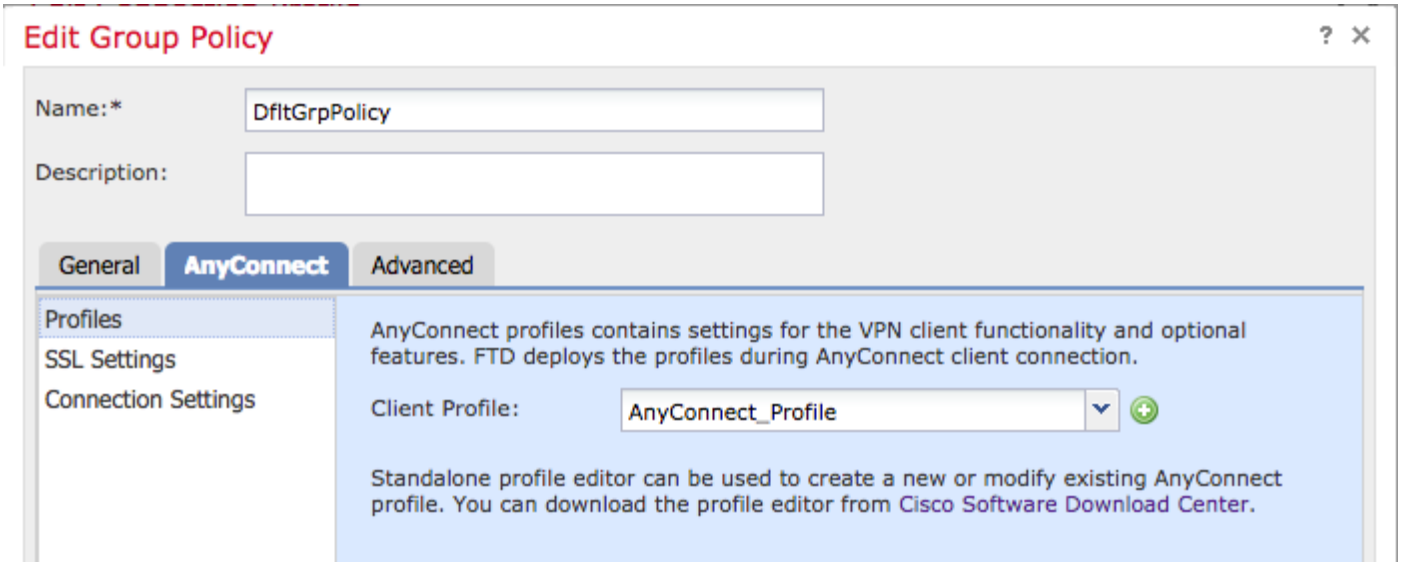


- En el **perfil de la conexión del** paso, pulse el **nombre del perfil de la conexión**, el **servidor** selecto de la **autenticación** y las **piscinas del direccionamiento** que usted ha creado anterior:

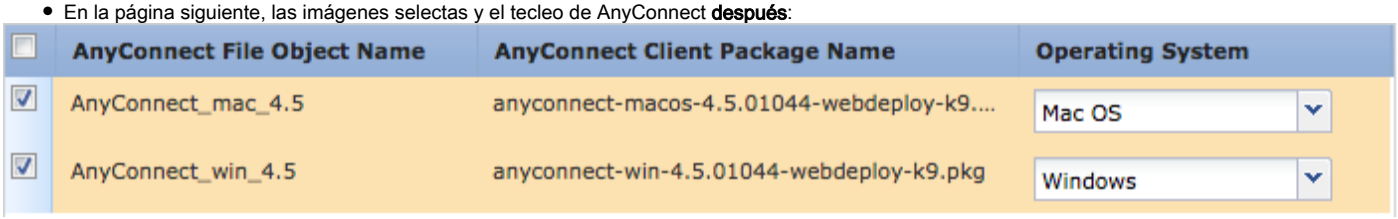




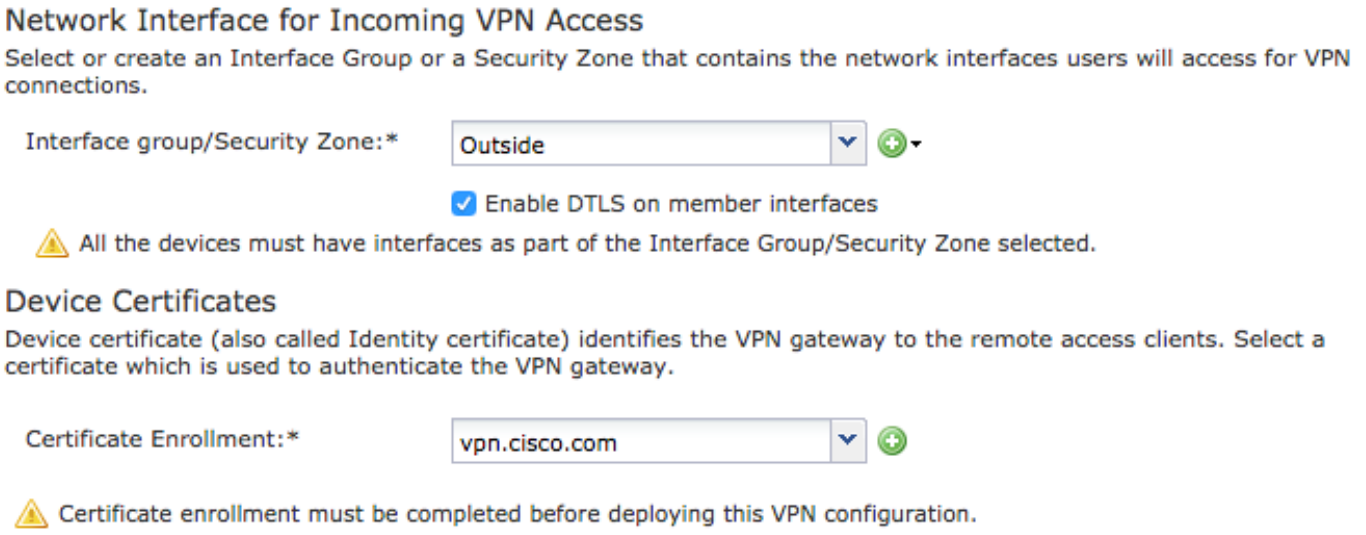
- Haga clic en **corrigen la directiva del grupo** y en la tabulación **AnyConnect**, **perfil** selecto del **cliente**, después hacen clic la **salvaguardia**:



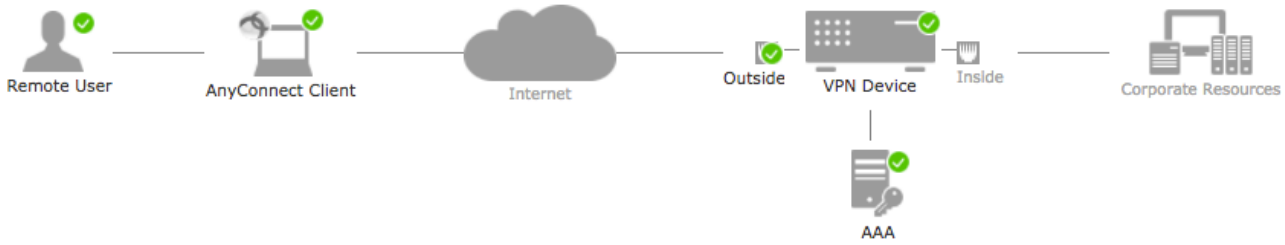
- En la página siguiente, las imágenes selectas y el tecleo de AnyConnect **después**:



- En la siguiente pantalla, seleccione el **interfaz de red** y **DeviceCertificates**:



- Cuando todo se configura correctamente, usted puede clic en Finalizar y entonces **desplegar**:



Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name:	AnyConnect_RA
Device Targets:	ASA5512-X_FTD
Connection Profile:	AnyConnect_RA
Connection Alias:	AnyConnect_RA
AAA:	
Authentication Method:	AAA Only
Authentication Server:	ISE
Authorization Server:	ISE
Accounting Server:	–
Address Assignment:	
Address from AAA:	–
DHCP Servers:	–
Address Pools (IPv4):	Address_pool
Address Pools (IPv6):	–
Group Policy:	DfltGrpPolicy
AnyConnect Images:	AnyConnect_mac_4.5 AnyConnect_win_4.5
Interface Objects:	Outside
Device Certificates:	vpn.cisco.com

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

Access Control Policy Update
An *Access Control* rule must be defined to allow VPN traffic on all targeted devices.

NAT Exemption
If NAT is enabled on the targeted devices, you must define a *NAT rule* to exempt VPN traffic.

DNS Configuration
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using *FlexConfig Policy* on the targeted devices.

Network Interface Configuration
Make sure to add interface from targeted devices to SecurityZone object 'Outside'

Device Identity Certificate Enrollment
Make sure to install identity certificate on targeted devices using PKI Cert object 'vpn.cisco.com'

- Esto copiará la configuración entera junto con los Certificados y los paquetes de AnyConnect al dispositivo FTD.

Conexión

Para conectar con FTD que usted necesita abrir a un navegador, el tipo nombre DNS o la dirección IP señalando a la interfaz exterior, en este ejemplo *https://vpn.cisco.com*. Usted entonces tendrá que abrirse una sesión usando las credenciales salvadas en el servidor de RADIUS y seguir las instrucciones en la pantalla. Una vez que AnyConnect instala, usted entonces necesita poner el mismo direccionamiento en la ventana de AnyConnect y el tecleo **conecta**.

Limitaciones

Actualmente sin apoyo en FTD, pero disponible en el ASA:

- Autenticación doble AAA
- Directiva del acceso dinámico
- Exploración del host
- Postura ISE
- CoA RADIUS
- Carga-balanceador VPN
- Autenticación local (mejora: CSCvf92680)
- Correspondencia del atributo LDAP
- Arreglo para requisitos particulares de AnyConnect
- Scripts de AnyConnect

- Localización de AnyConnect
- Por-app VPN
- Proxy SCEP
- Integración WSA
- SAML SSO
- Correspondencia crypto dinámica simultánea IKEv2 para el RA y L2L VPN
- Los módulos de AnyConnect (NAM, Hostscan, Enabler etc. AMP) – DARDO están instalados por abandono
- TACACS, Kerberos (autenticación y RSA SDI KCD)
- Proxy del navegador

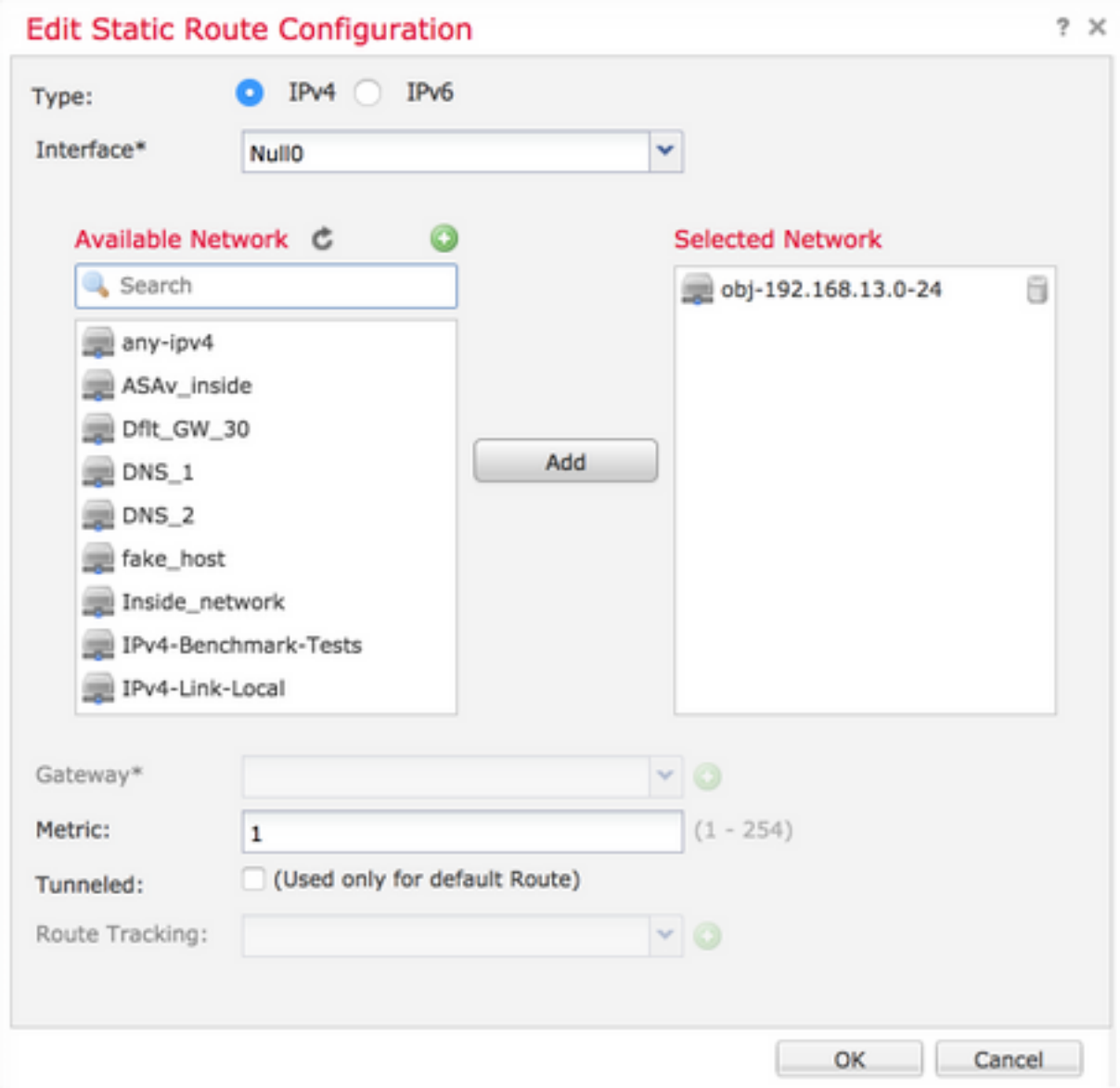
Observaciones de seguridad

Usted necesita recordar eso por abandono, opción de permiso-VPN de la conexión del sysopt se inhabilita. Este medios, eso que usted necesita permitir el tráfico que viene de la agrupación de direcciones en la interfaz exterior vía la directiva del control de acceso. Aunque la regla del pre-filtro o del control de acceso sea el preponerse agregado permitir el tráfico VPN solamente, si el tráfico del texto claro sucede hacer juego los criterios de regla, se permite erróneamente.

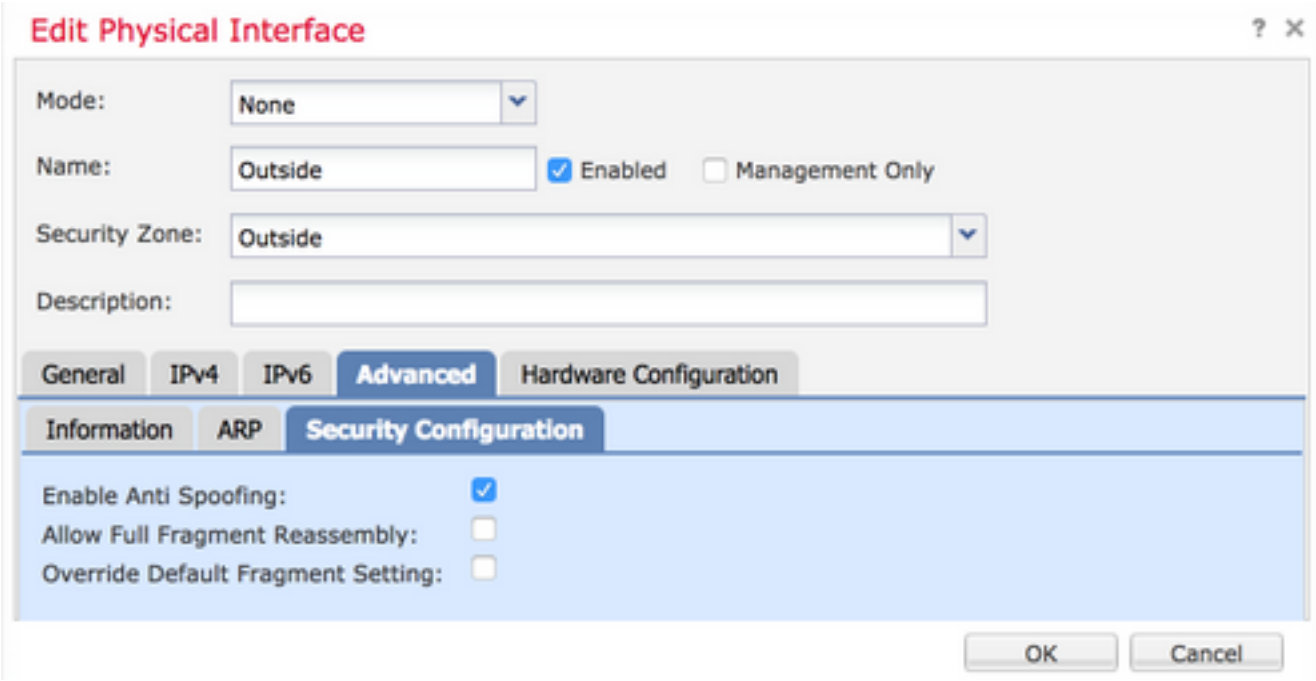
Hay dos acercamientos a este problema. Primero, TAC recomendó la opción, está activar la Anti-falsificación (en el ASA conocido como reenvío de trayecto inverso del unicast - uRPF) para la interfaz exterior, y la segunda es permitir a la conexión permiso-VPN del sysopt desviar el examen del Snort totalmente. La primera opción permite examinar normalmente el tráfico que va a y desde los usuarios de VPN.

a) Activación del uRPF

- cree una ruta nula para la red usada para los usuarios de acceso remoto, definido en la sección C. Apenas van a los **dispositivos >** a la **Administración de dispositivos > corrigen >** la **encaminamiento >** la **Static ruta > agregan la ruta**:



- en segundo lugar, usted necesita activar el uRPF en el interfaz que está terminando las conexiones VPN. Usted puede encontrar que en los **dispositivos > Administración de dispositivos > corregir >** los **interfaces > corrige >** que **avanzó la configuración del >** Security (Seguridad) > la **falsificación anti del permiso**:

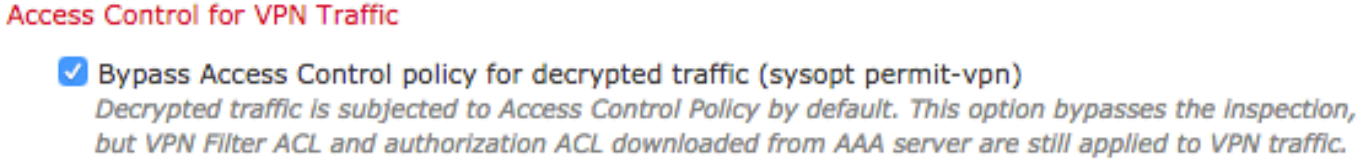


Cuando el usuario está conectado, la ruta de 32 bits está instalada para ese usuario en la tabla de encaminamiento. El tráfico del texto claro originario de otro, los IP Addresses inusitados del pool es caído por el uRFP. La Anti-falsificación se ha descrito en esta página:

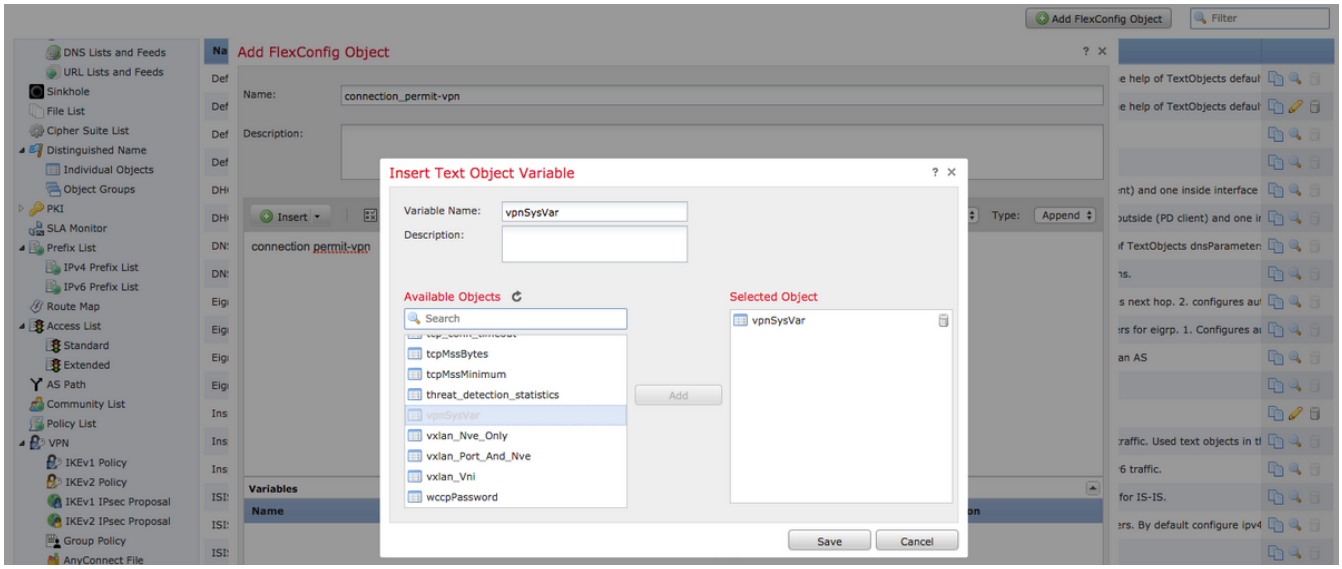
[Fije los parámetros de la configuración de Seguridad en la defensa de la amenaza de FirePOWER]

b) Activación de la opción de permiso-VPN de la conexión del sysopt

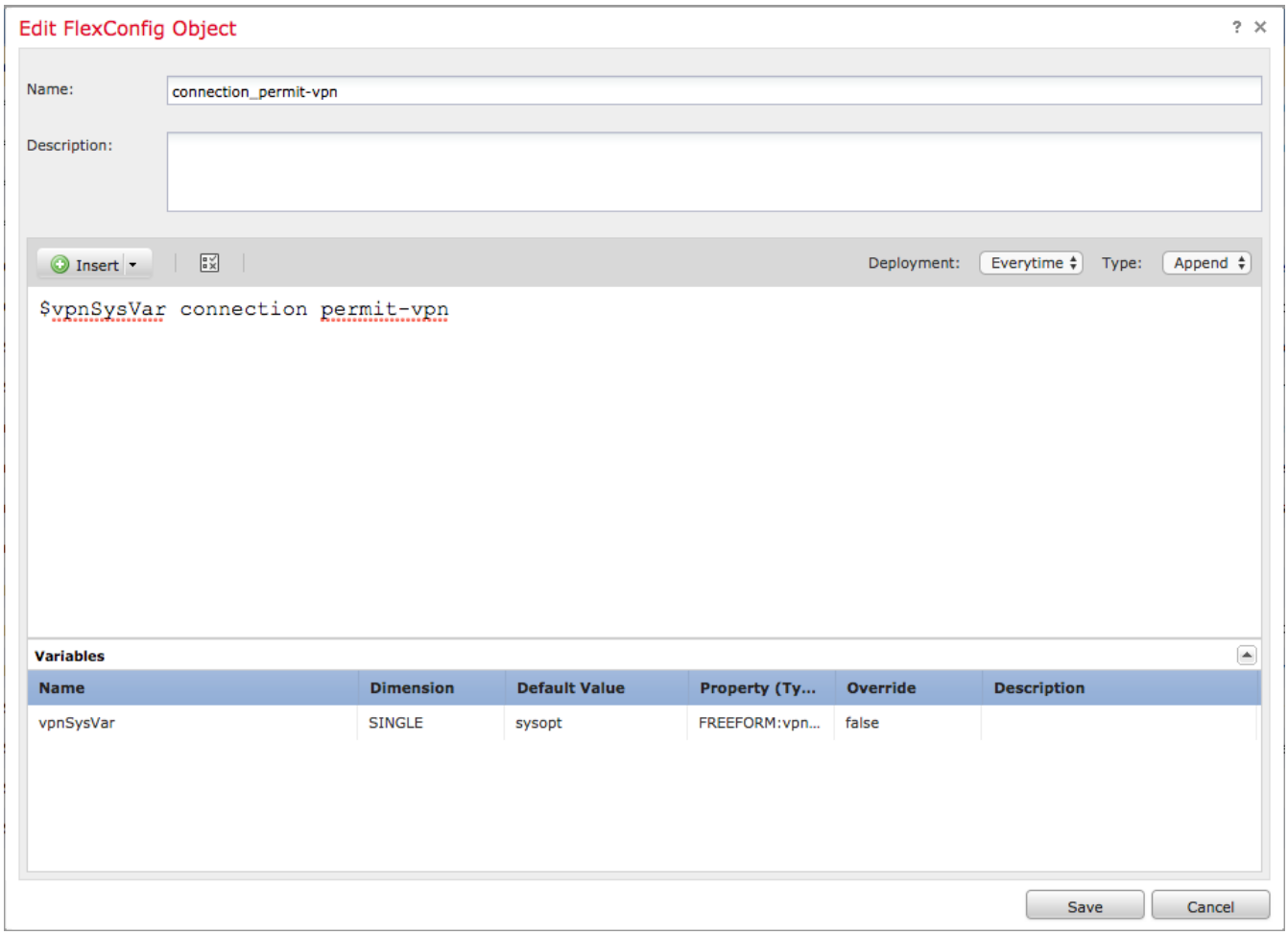
- Si usted tiene versión 6.2.3 o posterior, hay una opción para hacerla durante el Asisitente o bajo los **dispositivos** > el **VPN** > el **Acceso Remoto** > el *perfil* > **interfaces de acceso** *VPN*:



- Para las versiones antes de 6.2.3, vaya a los **objetos** > a la **Administración del objeto** > a **FlexConfig** > al **objeto del texto** > **agregan el objeto del texto**.
- Cree un variable object del texto, por ejemplo: `vpnSysVar` una sola entrada con el valor "`sysopt`"
- Vaya a los **objetos** > a la **Administración del objeto** > a **FlexConfig** > al **objeto de FlexConfig** > **agregan el objeto de FlexConfig**.
- Cree el objeto de FlexConfig con CLI "`conexión permiso-VPN`":
- Inserte el variable object del texto en el objeto del flexconfig al inicio del CLI como "`conexión permiso-VPN $vpnSysVar`", **salvaguardia del** tecleo:



- Aplique el objeto de FlexConfig como **añaden al final del fichero** y seleccione el despliegue a **cada vez**:



- Vaya a los **dispositivos** > a **FlexConfig** y corrija la política existente o cree un nuevo con el **nuevo** botón de la **directiva**.
- Agregue apenas FlexConfig creado, **salvaguardia del** tecleo.
- Despliegue la configuración para provision “el comando de permiso-VPN de la conexión del sysopt” en el dispositivo.

Esto sin embargo, quitará la posibilidad para utilizar la directiva del control de acceso para examinar el tráfico que viene de los usuarios. Usted puede todavía utilizar el filtro VPN o ACL descargable filtrar el tráfico de usuarios.

Si usted ve los problemas con los paquetes de caída del Snort de los usuarios de VPN, entre en contacto con TAC que se refiere a CSCvg91399 .