

Configuración del VPN de acceso remoto de AnyConnect en FTD

Contenido

[Introducción](#)

[Requisitos](#)

[Componentes usados](#)

[Configuración](#)

1. [Preresiquites](#)

a) [importación del certificado SSL](#)

b) [configure al servidor de RADIUS](#)

c) [crear a la agrupación de direcciones para los usuarios de VPN](#)

d) [crear el perfil XML](#)

e) [imágenes de AnyConnect que cargan por teletratamiento](#)

2. [Asisistente del Acceso Remoto](#)

[Conexión](#)

[Limitaciones](#)

[Observaciones de seguridad](#)

a) [Activación del uRPF](#)

b) [Activación de la opción de permiso-VPN de la conexión del sysopt](#)

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 Asistente 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 **agregar la inscripción CERT**:

Add Cert Enrollment



Name:*

vpn.cisco.com

Description:

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Certificate:*

```
CN0wa/5Kzu1ME0eiD0ungWwSIdGSS5+yngvWuIKZaiQOXVWVXGKRM  
L6/bXeoHTiIFM  
PJqzP/S58YbpyEWFmrHSZ3wNhvq3keHtAw5KcwHtA4nKOkxuA82zX  
nQLIXYI2r8h  
HcbaVabAufb7CV1mdwSVDtJOBFI2ftpQONj67VN902vtN8FwA8UAsy  
73zzRPbIIH  
Yh5Nr9WhZn/wcxvRmi+sEi7cBrpXG1g8+cbVr5z4LWXD28zoKKoSZjx  
LfJurARIW  
SENBXsxAuKRQc9wgDZKHR9sA2r1AGFMm0NpSKmSNkGbkS4q37V  
N9EyToUg9OXRKI  
AMImjysdgAO7O9HmeFgxbOqL8GdczEYs7VMNxQ2Jih+oRnDASSXg  
AsNmi2/xIN9H  
CfyjTgclvfm9gO18JjbuX8O85RhO2cKMI3ZEGIIpeYcUbv+cWCeUSL6  
mox6p9CXe  
HGyUpYafhN1D78+Y8eeW9YSai0B9b54yKI5YdXjphYHXmZQ18edtzv  
WIq3Ysrns2  
qBojiQ==  
-----END CERTIFICATE-----
```

Allow Overrides:

Save

Cancel

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

Add Cert Enrollment



Name:*

Description:

CA Information

Certificate Parameters

Key

Revocation

Include FQDN: ▼

Custom FQDN:

Include Device's IP Address:

Common Name (CN):

Organization Unit (OU):

Organization (O):

Locality (L):

State (ST):

Country Code (C):

Email (E):

Include Device's Serial Number

Allow Overrides:

Save

Cancel

- En la tercera tabulación, seleccione el tipo dominante, elija el nombre y el tamaño. Para el RSA, 2048 bytes son mínimos.
- Haga clic la salvaguarda 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**:

Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

ASA5512-X_FTD

Cert Enrollment*:

vpn.cisco.com

Cert Enrollment Details:

Name:

vpn.cisco.com

Enrollment Type:


Manual


SCEP URL:

NA

Add

Cancel

- 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 firmelo. 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 platform 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 teclado**:

New RADIUS Server

IP Address/Hostname:*
When using hostname, configure DNS using FlexConfig Policy

Authentication Port:* (1-65535)

Key:*

Confirm Key:*

Accounting Port: (1-65535)

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

Name	Value	Override	
ISE	1 Server	✗	 

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:

Edit IPv4 Pool


Name:*

IPv4 Address Range:*
 Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask:

Description:

Allow Overrides:

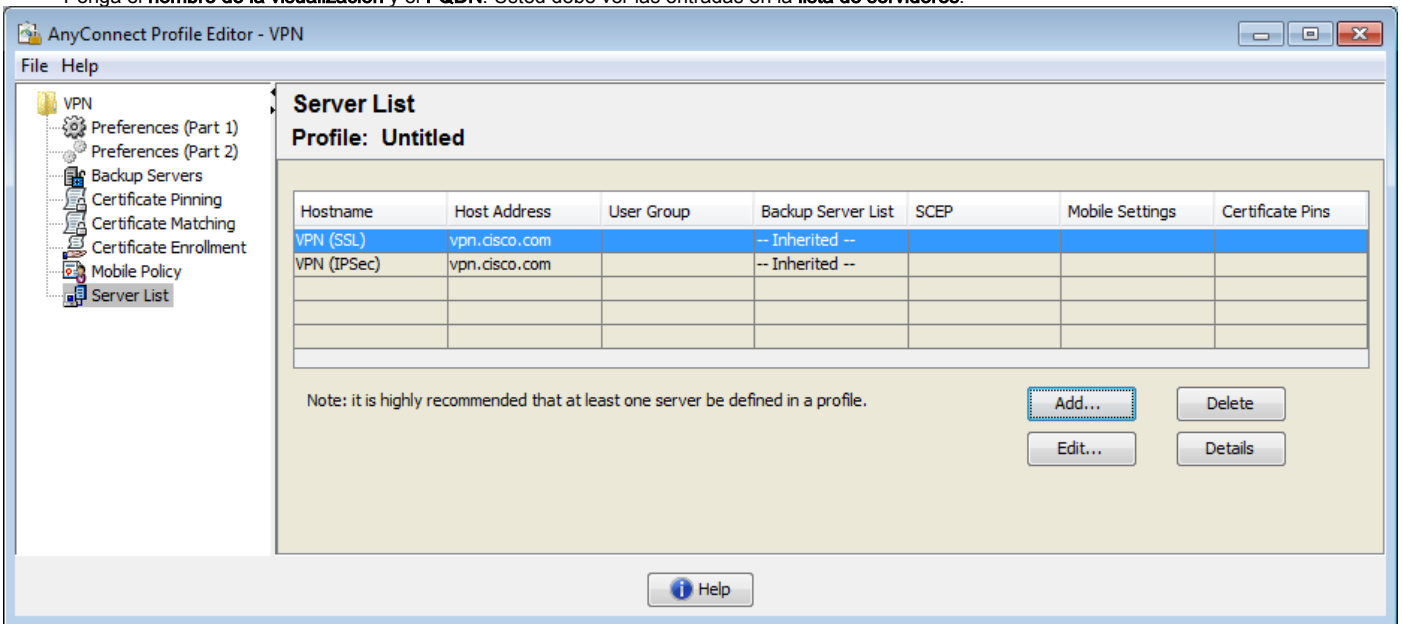
 Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

Override (0)

d) crear el perfil XML

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

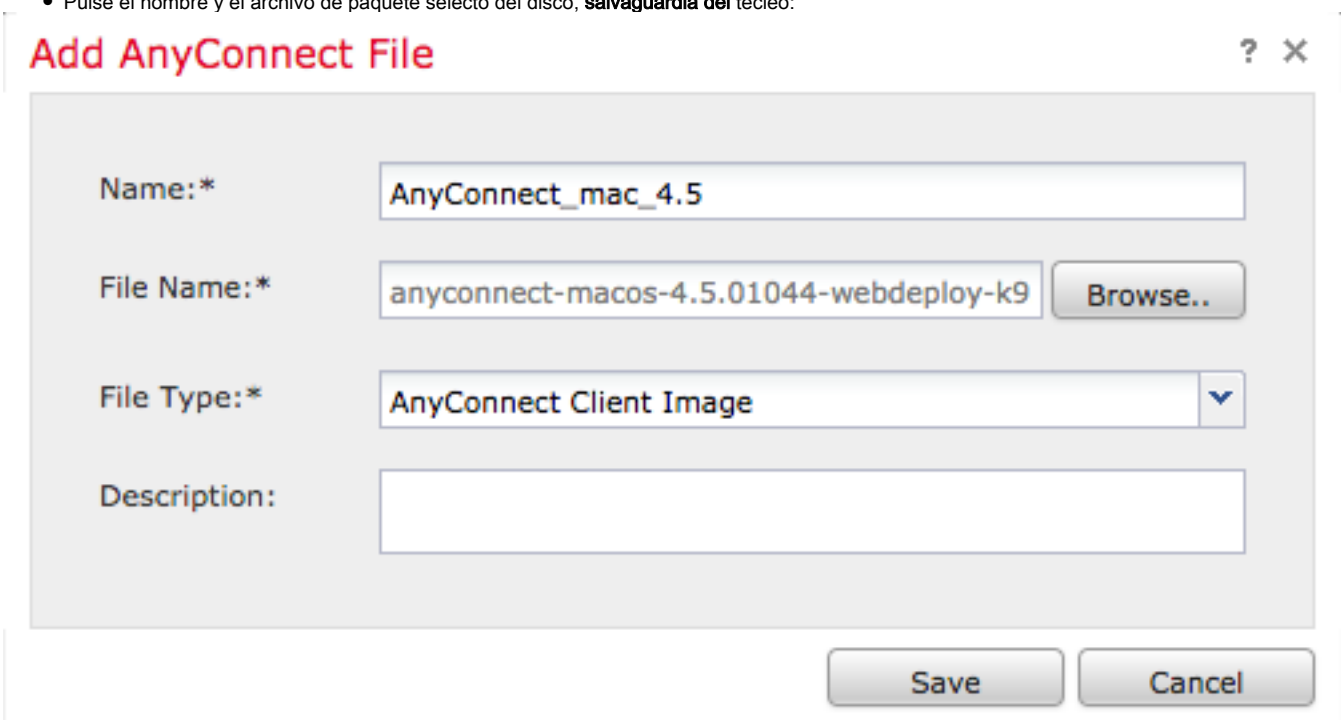
- Ponga el **nombre de la visualización** y el **FQDN**. Usted debe ver las entradas en la **lista de servidores**:



- AUTORIZACIÓN y File (Archivo) > Save as (Guardar como) del teclado...

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 teclado**:



- Agregue más paquetes dependiendo de sus requisitos.

2. Asistente 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:

Name:*

Description:

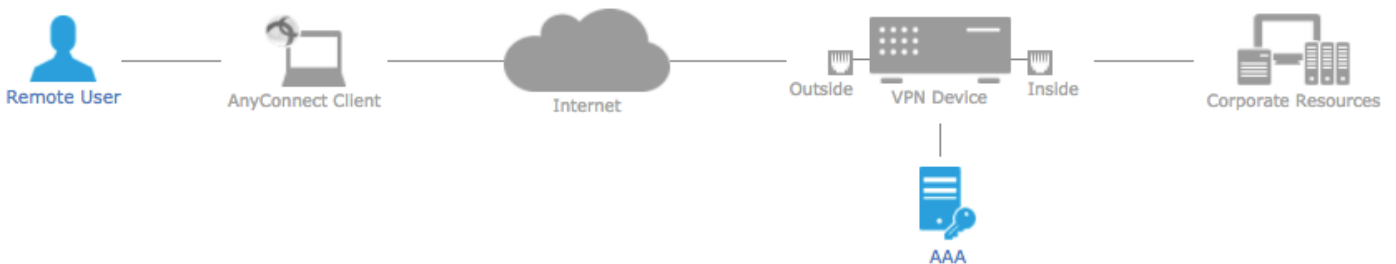
VPN Protocols: SSL IPsec-IKEv2

Targeted Devices: **Available Devices** **Selected Devices**

ASA5512-X_FTD

ASA5512-X_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:



Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:*

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

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method:

Authentication Server:* (+) (Realm or RADIUS)

Authorization Server: (+) (RADIUS)

Accounting Server: (+) (RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (RADIUS only) (i)

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: (edit icon)

IPv6 Address Pools: (edit icon)

Group Policy:

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.

Group Policy:* (+)

[Edit Group Policy](#)

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

Edit Group Policy



Name:*

Description:

General

AnyConnect

Advanced

Profiles

SSL Settings

Connection Settings

AnyConnect profiles contains settings for the VPN client functionality and optional features. FTD deploys the profiles during AnyConnect client connection.

Client Profile:

Standalone profile editor can be used to create a new or modify existing AnyConnect profile. You can download the profile editor from [Cisco Software Download Center](#).

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

<input type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	AnyConnect_mac_4.5	anyconnect-macos-4.5.01044-webdeploy-k9....	Mac OS
<input checked="" type="checkbox"/>	AnyConnect_win_4.5	anyconnect-win-4.5.01044-webdeploy-k9.pkg	Windows

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

Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:*

Enable DTLS on member interfaces

All the devices must have interfaces as part of the Interface Group/Security Zone selected.

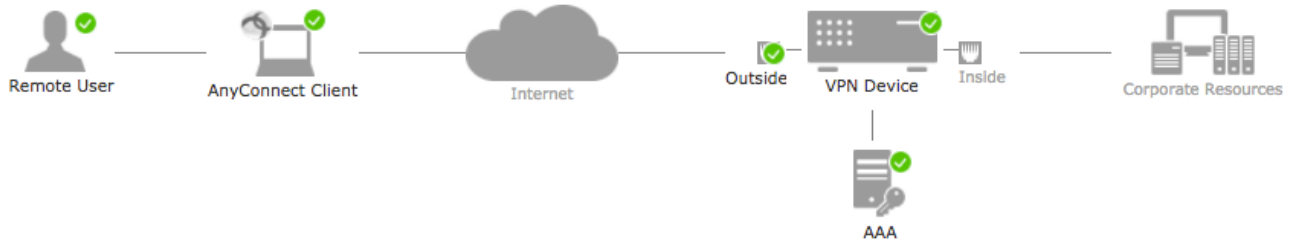
Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:*

Certificate enrollment must be completed before deploying this VPN configuration.

- 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):	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**:

Edit Static Route Configuration

Type: IPv4 IPv6

Interface*: Null0

Available Network

Search

- any-ipv4
- ASAv_inside
- Dflt_GW_30
- DNS_1
- DNS_2
- fake_host
- Inside_network
- IPv4-Benchmark-Tests
- IPv4-Link-Local

Selected Network

obj-192.168.13.0-24

Add

Gateway*:

Metric: (1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

- 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:**

Edit Physical Interface ? X

Mode: ▾

Name: Enabled Management Only

Security Zone: ▾

Description:

General IPv4 IPv6 **Advanced** Hardware Configuration

Information ARP **Security Configuration**

Enable Anti Spoofing:

Allow Full Fragment Reassembly:

Override Default Fragment Setting:

OK Cancel

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](#)

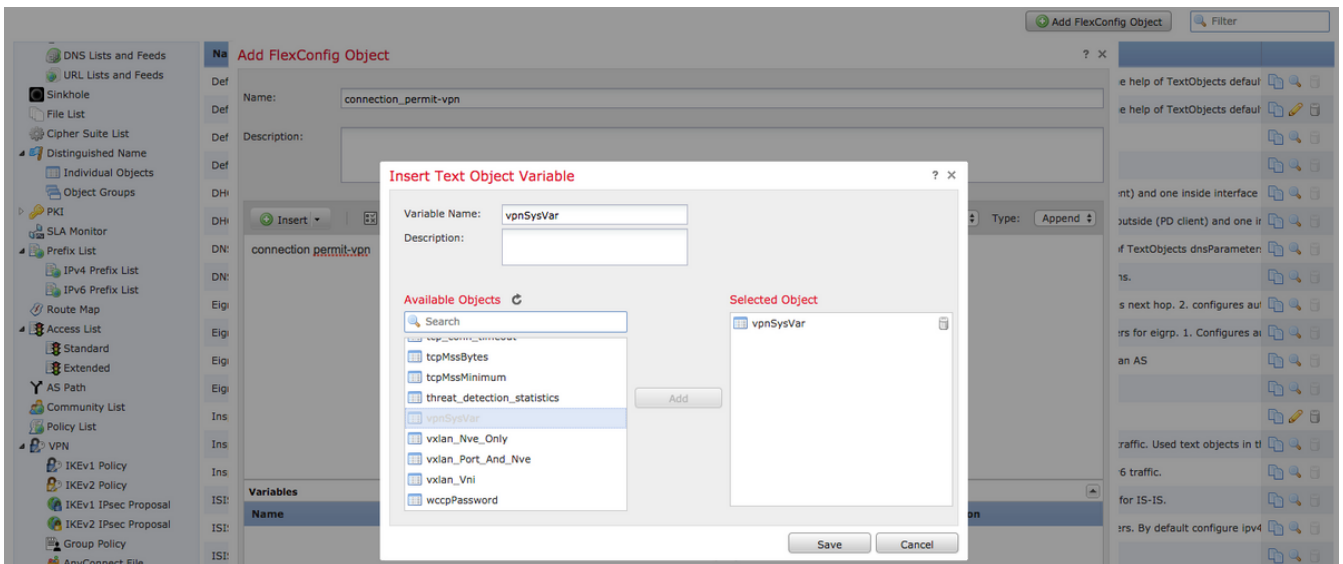
b) Activación de la opción de permiso-VPN de la conexión del sysopt

- 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**:

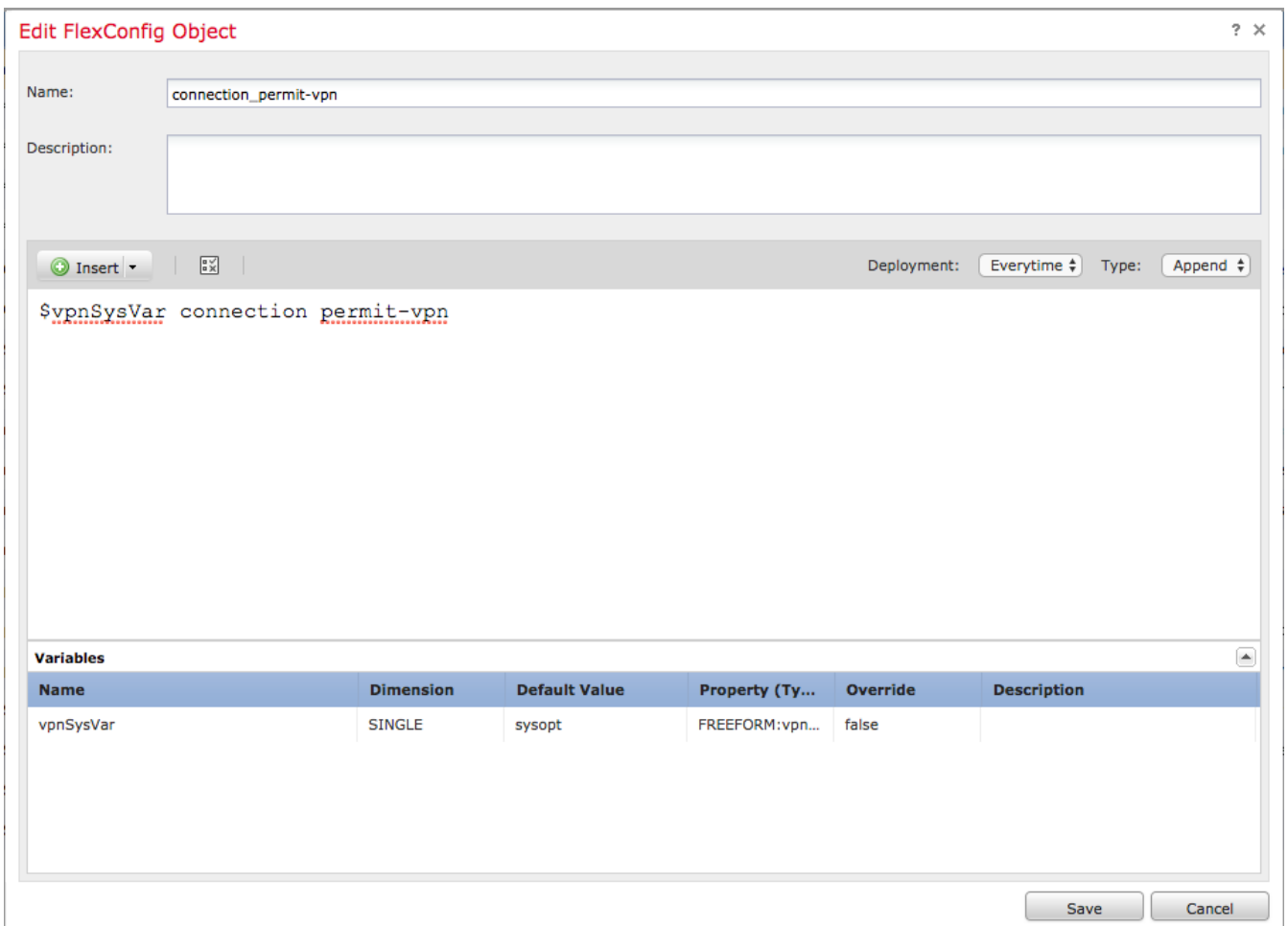
Access Control for VPN Traffic

- Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)**
Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

- 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 teclado**.
- 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](https://support.cisco.com/servlet/JSP?url=ft_jsp pages/JSPContent.jsp) .