

Configuración de VPN de acceso remoto AnyConnect en FTD

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configuración](#)

[1. Prerequisites](#)

[a\) Importar el certificado SSL](#)

[c\) Crear un conjunto de direcciones para usuarios de VPN](#)

[d\) Crear perfil XML](#)

[e\) Cargar imágenes de AnyConnect](#)

[2. Asistente para acceso remoto](#)

[Conexión](#)

[Limitaciones](#)

[Observaciones de seguridad](#)

[a\) Habilitar uRPF](#)

[b\) Activar la opción `sysopt connection permit-vpn`](#)

[Información Relacionada](#)

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**.

Add Cert Enrollment



Name*

vpntestbbed.cisco.com

Description

|

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

Manual

CA Only

Check this option if you do not require an identity certificate to be created from this CA

CA Certificate:

```
Ep0WYTGngteb6JFITIn..StZxdr  
YfPCiIB7g  
BMAV7Gzdc4VspS6lJrAhbiiaw  
dBiIQmsBeFz9JkF4..b3l8Bo  
GN+qMa56Y  
It8una2gY4l2O//on88r5IWJlm  
1L0oA8e4fR2yrBHX..adsGeFK  
kyNrwGi/  
7vQMfXdGsRrXNGRGnX+vWD  
Z3/zWI0joDtCkNnqEpVn..HoX  
-----END CERTIFICATE-----
```

Validation Usage: IPsec Client SSL Client SSL Server

Skip Check for CA flag in basic constraints of the CA Certificate

Allow Overrides

Cancel

Save

- 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:

Add Cert Enrollment



Name*

vpntestbbed.cisco.com

Description

CA Information

Certificate Parameters

Key

Revocation

Include FQDN: Use Device Hostname as FQDN ▾

Include Device's IP Address: 10.88.243.123

Common Name (CN): vpntestbed.cisco.com

Organization Unit (OU): TAC

Organization (O): Mexico

Locality (L): MX

State (ST): CDMX

Country Code (C): MX

Email (E): tac@cisco.com

Include Device's Serial Number

Allow Overrides

Cancel

Save

- 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**:

Add New Certificate



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


Device*:



Cert Enrollment*:

 +

Cert Enrollment Details:

Name: vpntestbed.cisco.com

- Más adelante, junto al nombre del punto de confianza, haga clic en el botón  icono, a continuación **Yes**, 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:

Name	Domain	Enrollment Type	Status
FTD			
vpntestbed.cisco.com	Global	Self-Signed	 

b) Configuración del servidor RADIUS

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

Edit RADIUS Server



IP Address/Hostname:*

192.168.20.7

Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* (1-65535)

1812

Key:*

Confirm Key:*

Accounting Port: (1-65535)

1813

Timeout: (1-300) Seconds

10

Connect using:

Routing Specific Interface

Default: Management/Diagnostic ▾



Redirect ACL:



Cancel

Save

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

Name	Value	
RadiusServer	1 Server	

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:

Name*

vpn_pool

IPv4 Address Range*

10.72.1.1-10.72.1.150

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

Specify a netmask in X.X.X.X format

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)

Cancel

OK

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:

AnyConnect Profile Editor - VPN

File Help

Server List
Profile: C:\Users\calo\Documents\Anyconnect_profile.xml

Hostname	Host Address	User Group	Backup Server List	SCEP	Mobile Settings	Certificate Pins
VPN(SSL)	vpntestbed.cisco....		-- Inherited --			
VPN(IPSEC)	vpntestbed.cisco....		-- Inherited --			

Note: it is highly recommended that at least one server be defined in a profile.

Add... Delete Edit... Details

- Haga clic en **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:

Edit AnyConnect File ?

Name:*

File Name:*

File Type:*

Description:

- 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:

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:*

Description:

VPN Protocols:

SSL

IPsec-IKEv2


Targeted Devices:

Available Devices

- FTD

Add

Selected Devices

- FTD 

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

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:*

i 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:* +

(LOCAL or Realm or RADIUS)

Fallback to LOCAL Authentication

Authorization Server: +

(Realm or 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 (Realm or RADIUS only) **i**

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: 

IPv6 Address Pools: 

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

Name:*

DfltGrpPolicy

Description:

General

AnyConnect

Advanced

Profile

Management Profile

Client Modules

SSL Settings

Connection Settings

Custom Attributes

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

Client Profile:

Anyconnect_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, seleccione imágenes de AnyConnect y haga clic en Next.

AnyConnect Client Image

The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#).

Show Re-order buttons +

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	Anyconnectmac4.10	anyconnect-macos-4.10.06079-webdeploy...	Mac OS

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

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.

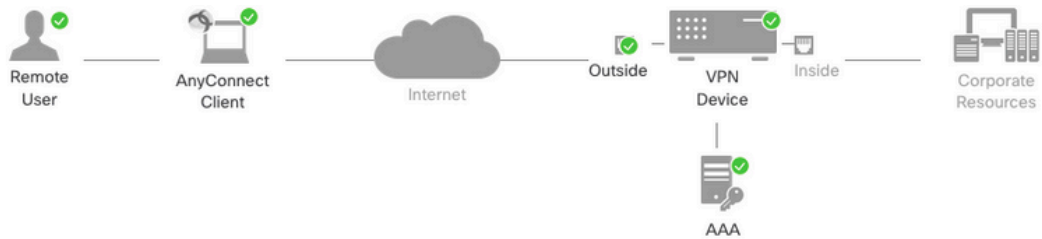
Certificate Enrollment:* +

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

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

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



Remote Access VPN Policy Configuration

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

Name:	Anyconnect_RA
Device Targets:	FTD
Connection Profile:	Anyconnect_RA
Connection Alias:	Anyconnect_RA
AAA:	
Authentication Method:	AAA Only
Authentication Server:	RadiusServer (RADIUS)
Authorization Server:	RadiusServer (RADIUS)
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	vpn_pool
Address Pools (IPv6):	-
Group Policy:	DfltGrpPolicy
AnyConnect Images:	Anyconnectmac4.10
Interface Objects:	Outsied
Device Certificates:	vpntestbed.cisco.com

Device Identity Certificate Enrollment

Certificate enrollment object 'vpntestbed.cisco.com' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the [Certificates](#) page to check the status of the installation.

Additional Configuration Requirements

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

1 Access Control Policy Update

An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.

2 NAT Exemption

If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.

3 DNS Configuration

To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.

4 Port Configuration

SSL will be enabled on port 443. IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Anyconnect image download. NAT-Traversal will be enabled by default and will use port 4500. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.

▲ Network Interface Configuration

Make sure to add interface from targeted devices to SecurityZone object 'Outsied'

- 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 Defense 6.2.3 o versiones anteriores. La opción de interfaz se omite durante la implementación.
- Un servidor RADIUS con autorización dinámica requiere Firepower Threat Defense 6.3 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-vpn` está 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`

Add Static Route Configuration



Type: IPv4 IPv6

Interface*

Null0

(Interface starting with this icon  signifies it is available for route leak)

Available Network  +

Search

Add

any-ipv4
FMC
GW
IPv4-Benchmark-Tests
IPv4-Link-Local
IPv4-Multicast

Selected Network

objvpnusers 

Gateway*

Metric:

1

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

Cancel

OK

- 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**.

General	IPv4	IPv6	Path Monitoring	Hardware Configuration	Manager Access	Advanced
Information	ARP	Security Configuration				

Enable Anti Spoofing:

Allow Full Fragment Reassembly:

Override Default Fragment Setting:

Cancel OK

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](#).

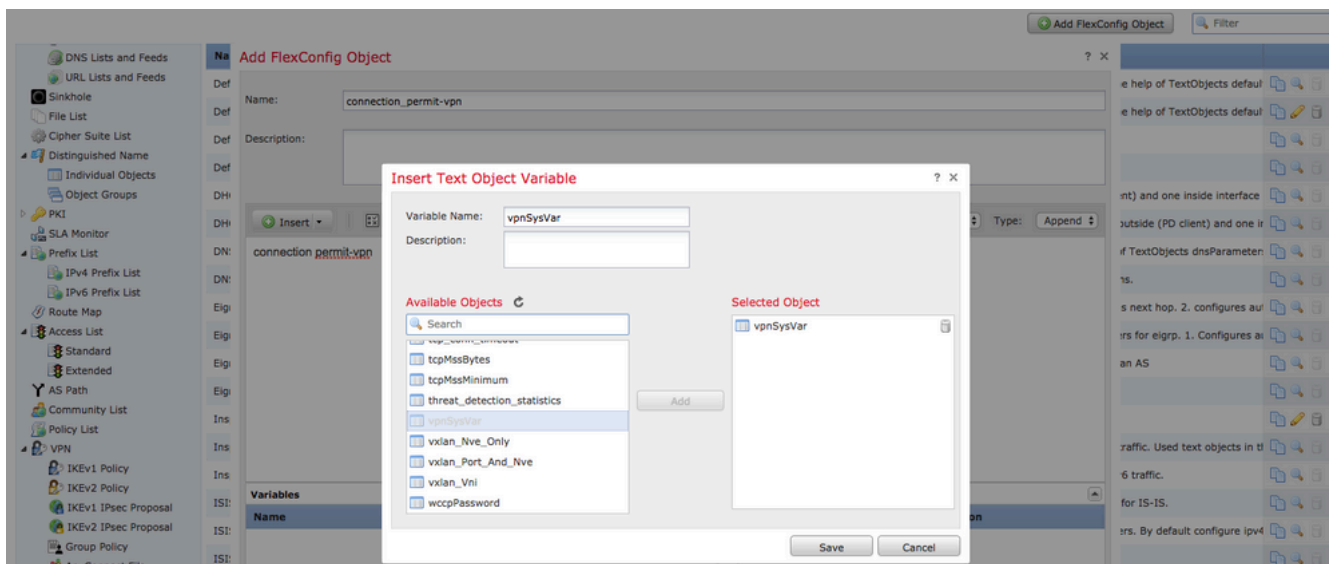
b) Habilitar `sysopt connection permit-vpn` Opción

- 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`.

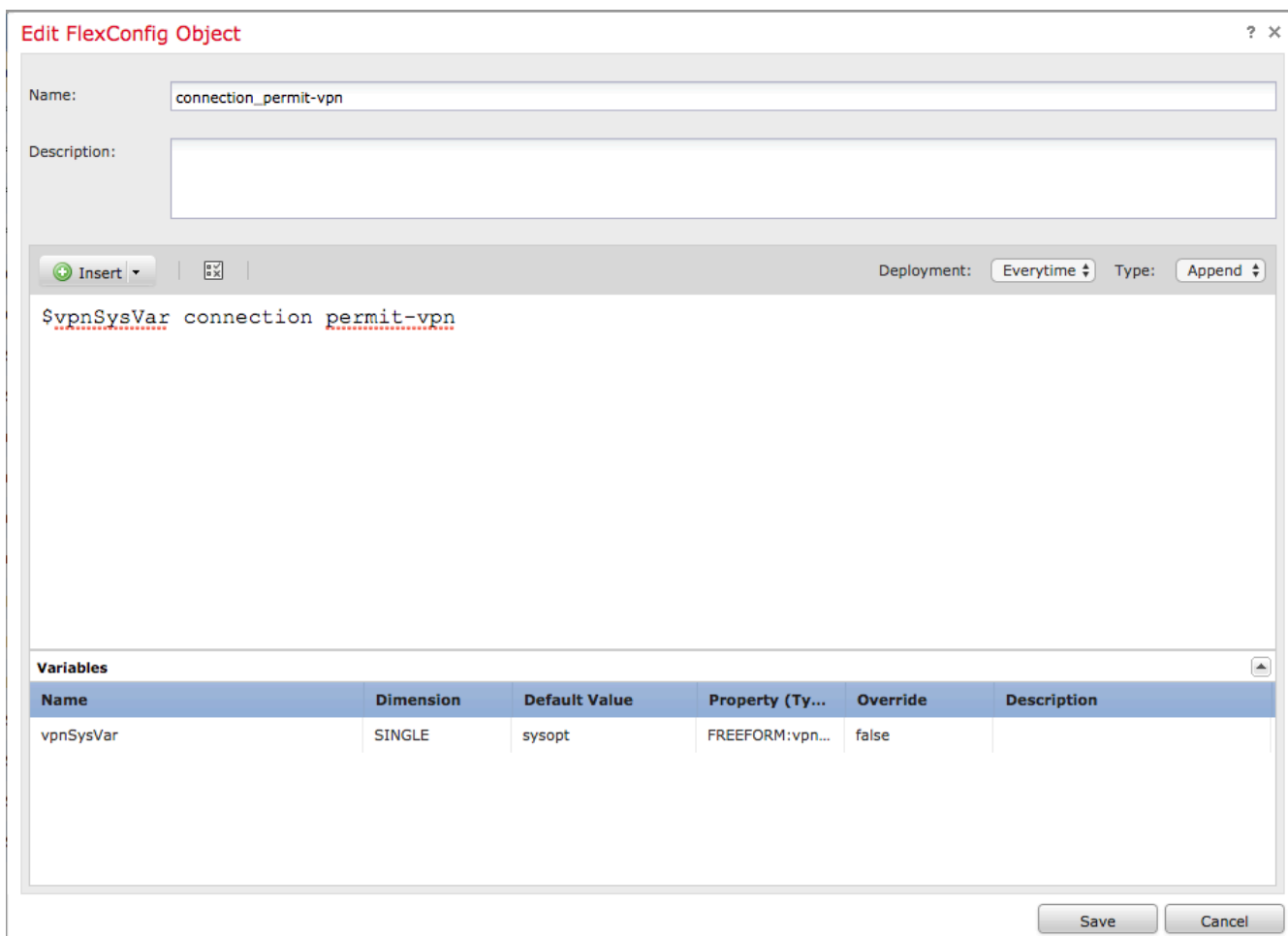
Access Control for VPN Traffic

- 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 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 FlexConfig objeto 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).