

Configurar o AnyConnect Remote Access VPN no FTD

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configuração](#)

[1. Prerequisites](#)

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

[c\) Crie um pool de endereços para usuários de VPN](#)

[d\) Criar perfil XML](#)

[e\) Carregar imagens do AnyConnect](#)

[2. Assistente de Acesso Remoto](#)

[Conexão](#)

[Limitações](#)

[Considerações sobre segurança](#)

[a\) Habilitar uRPF](#)

[b\) Ativar a opção de conexão sysopt permit-vpn](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve uma configuração para o AnyConnect Remote Access VPN no FTD.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico de VPN, TLS e IKEv2
- Conhecimento de Autenticação, Autorização e Tarifação Básica (AAA - Basic Authentication, Authorization, and Accounting) e RADIUS
- Experiência com o Firepower Management Center

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- FTD 7.2.0 da Cisco

- Cisco FMC 7.2.1
- AnyConnect 4.10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento fornece um exemplo de configuração para o Firepower Threat Defense (FTD) versão 7.2.0 e posterior, que permite que a VPN de acesso remoto use o Transport Layer Security (TLS) e o Internet Key Exchange versão 2 (IKEv2). Como um cliente, o Cisco AnyConnect pode ser usado, que é suportado em várias plataformas.

Configuração

1. Prerequisites

Para passar pelo assistente de acesso remoto no Firepower Management Center:

- Crie um certificado usado para autenticação de servidor.
- Configure o servidor RADIUS ou LDAP para autenticação de usuário.
- Crie um pool de endereços para usuários VPN.
- Carregue imagens do AnyConnect para plataformas diferentes.

a) Importar o certificado SSL

Os certificados são essenciais ao configurar o AnyConnect. O certificado deve ter a extensão de Nome Alternativo da Entidade com o nome DNS e/ou endereço IP para evitar erros em navegadores da Web.

Observação: somente usuários registrados da Cisco têm acesso a ferramentas internas e informações de bug.

Há limitações para o registro manual de certificados:

- No FTD, você precisa do certificado CA antes de gerar o CSR.
- Se o CSR for gerado externamente, o método manual falhará, um método diferente deverá ser usado (PKCS12).

Há vários métodos para obter um certificado no dispositivo FTD, mas o seguro e fácil é criar uma CSR (Certificate Signing Request, Solicitação de assinatura de certificado), assiná-la com uma CA (Certificate Authority, Autoridade de certificado) e importar o certificado emitido para a chave pública, que estava em CSR. Veja como fazer isso:

- Ir para **Objects > Object Management > PKI > Cert Enrollment** clique em **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
dBiQIQmsBeFz9JkF4..b3l8Bo
GN+qMa56Y
lt8una2gY4l2O//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

- Selecionar Enrollment Type e cole o certificado da Autoridade de Certificação (CA) (o certificado usado para assinar o CSR).
- Em seguida, vá para a segunda guia e selecione Custom FQDN e preencha todos os campos necessários, por exemplo:

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

- Na terceira guia, selecione Key Type, escolha nome e tamanho. Para RSA, 2048 bits são no mínimo.
- Clique em salvar e vá para Devices > Certificates > Add > New Certificate.
- Em seguida selecione Device, e sob Cert Enrollment selecione o ponto confiável que você acabou de criar, clique em 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

- Depois, ao lado do nome do ponto de confiança, clique no  , em seguida Yes, e depois copie CSR para CA e assine-o. O certificado deve ter atributos iguais aos normais de um servidor HTTPS.
- Depois de receber o certificado da CA no formato base64, selecione-o no disco e clique em Import. Quando isso for bem-sucedido, você verá:

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

b) Configurar o servidor RADIUS

- Ir para **Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group**.
- Preencha o nome e adicione o endereço IP junto com o segredo compartilhado, clique em 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

- Depois disso, você verá o servidor na lista:

Name	Value	
RadiusServer	1 Server	

c) Crie um pool de endereços para usuários de VPN

- Ir para **Objects > Object Management > Address Pools > Add IPv4 Pools**.
- Coloque o nome e o intervalo, a máscara não é necessária:

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) Criar perfil XML

- Faça o download do Editor de perfis no site da Cisco e abra-o.
- Ir para **Server List > Add...**
- Coloque o Nome para Exibição e o FQDN. Você verá entradas na 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

- Clique em **File > Save as...**

e) Carregar imagens do AnyConnect

- Faça o download de imagens de pacotes do site da Cisco.
- Ir para Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File.
- Digite o nome e selecione o arquivo PKG no disco. Clique em Save:

Edit AnyConnect File ?

Name:*

File Name:*

File Type:*

Description:

- Adicione mais pacotes com base em seus próprios requisitos.

2. Assistente de Acesso Remoto

- Ir para Devices > VPN > Remote Access > Add a new configuration.
- Nomeie o perfil e selecione o 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 

- Na etapa Perfil de Conexão, digite **Connection Profile Name**, selecione a **Authentication Server e Address Pools** que você criou 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](#)

- Clique em **Edit Group Policy** e, na guia AnyConnect, selecione Client Profile e clique em **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](#).

- Na próxima página, selecione as imagens do AnyConnect e clique em 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

- Na próxima tela, selecione **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.

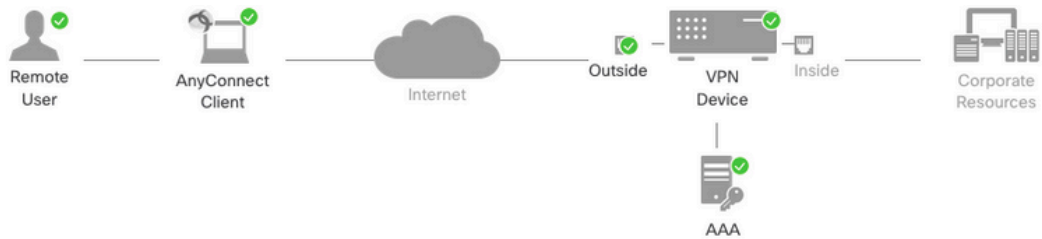
Certificate Enrollment:* +

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.

- Quando tudo estiver configurado corretamente, você poderá clicar em Finish e depois 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'

- Isso copia toda a configuração junto com os certificados e os pacotes do AnyConnect para o dispositivo FTD.

Conexão

Para se conectar ao FTD, você precisa abrir um navegador, digitar o nome DNS ou o endereço IP que aponta para a interface externa. Em seguida, efetue login com as credenciais armazenadas no servidor RADIUS e siga as instruções na tela. Depois que o AnyConnect for instalado, você precisará colocar o mesmo endereço na janela do AnyConnect e clicar em [Connect](#).

Limitações

Atualmente sem suporte no FTD, mas disponível no ASA:

- Não há suporte para a seleção de interface no servidor RADIUS no Firepower Threat Defense 6.2.3 ou em versões anteriores. A opção de interface é ignorada durante a implantação.
- Um servidor RADIUS habilitado para autorização dinâmica requer Firepower Threat Defense 6.3 ou posterior para que a autorização dinâmica funcione.

- A VPN FTDposture não oferece suporte à alteração de política de grupo por meio de autorização dinâmica ou alteração de autorização (CoA) RADIUS.
- Personalização do AnyConnect (Aprimoramento: ID de bug da Cisco [CSCvq87631](#))
- Scripts do AnyConnect
- Localização do AnyConnect
- Integração com WSA
- Mapa de criptografia dinâmica IKEv2 simultâneo para RA e VPN L2L (Aprimoramento: ID de bug Cisco [CSCvr52047](#))
- Módulos do AnyConnect (NAM, Hostscan, AMP Enabler, SBL, Umbrella, Web Security e assim por diante) - O DART é instalado por padrão (Aprimoramentos do AMP Enabler e Umbrella: ID de bug da Cisco [CSCvs03562](#) e ID de bug da Cisco [CSCvs06642](#)).
- TACACS, Kerberos (autenticação KCD e RSA SDI)
- Proxy do navegador

Considerações sobre segurança

Por padrão, o `sysopt connection permit-vpn` está desativada. Isso significa que você precisa permitir o tráfego que vem do pool de endereços na interface externa através da Política de Controle de Acesso. Embora a regra de pré-filtro ou de controle de acesso seja adicionada para permitir somente o tráfego VPN, se o tráfego de texto simples corresponder aos critérios da regra, ele será permitido erroneamente.

Há duas abordagens para esse problema. Primeiro, a opção recomendada do TAC é ativar o Anti-Spoofing (no ASA, era conhecido como Unicast Reverse Path Forwarding - uRPF) para a interface externa e, segundo, é ativar `sysopt connection permit-vpn` para ignorar completamente a inspeção Snort. A primeira opção permite uma inspeção normal do tráfego que vai para e de usuários de VPN.

a) Habilitar uRPF

- Crie uma rota nula para a rede usada para usuários de acesso remoto, definida na seção C. Vá para `Devices > Device Management > Edit > Routing > Static Route` e selecione `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

- Em seguida, habilite o uRPF na interface onde as conexões VPN terminam. Para localizar isso, navegue até **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

Quando um usuário está conectado, a rota de 32 bits é instalada para esse usuário na tabela de roteamento. Limpe o tráfego de texto originado de outros endereços IP não utilizados do pool que é descartado pelo uRFP. Para ver uma descrição de **Anti-Spoofing** consulte [Definir parâmetros de configuração de segurança no Firepower Threat Defense](#).

b) Habilitar `sysopt connection permit-vpn` Opção

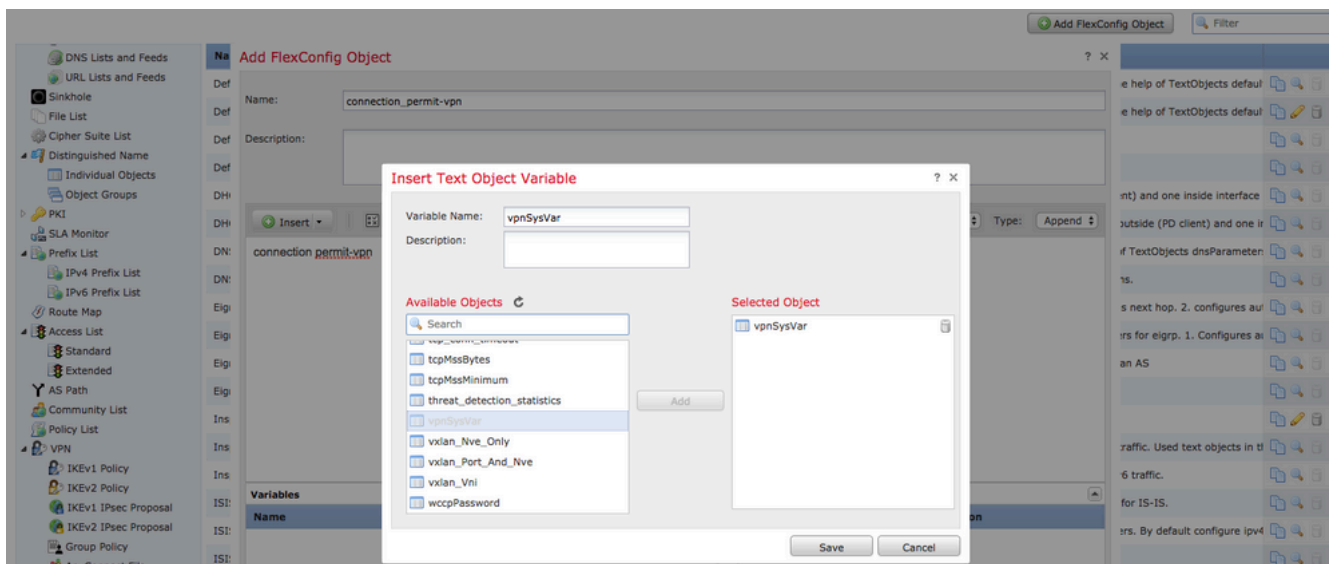
- Se você tiver a versão 6.2.3 ou posterior, há uma opção para fazer isso com o assistente ou `sof` Devices > VPN > Remote Access > VPN Profile > Access Interfaces.

Access Control for VPN Traffic

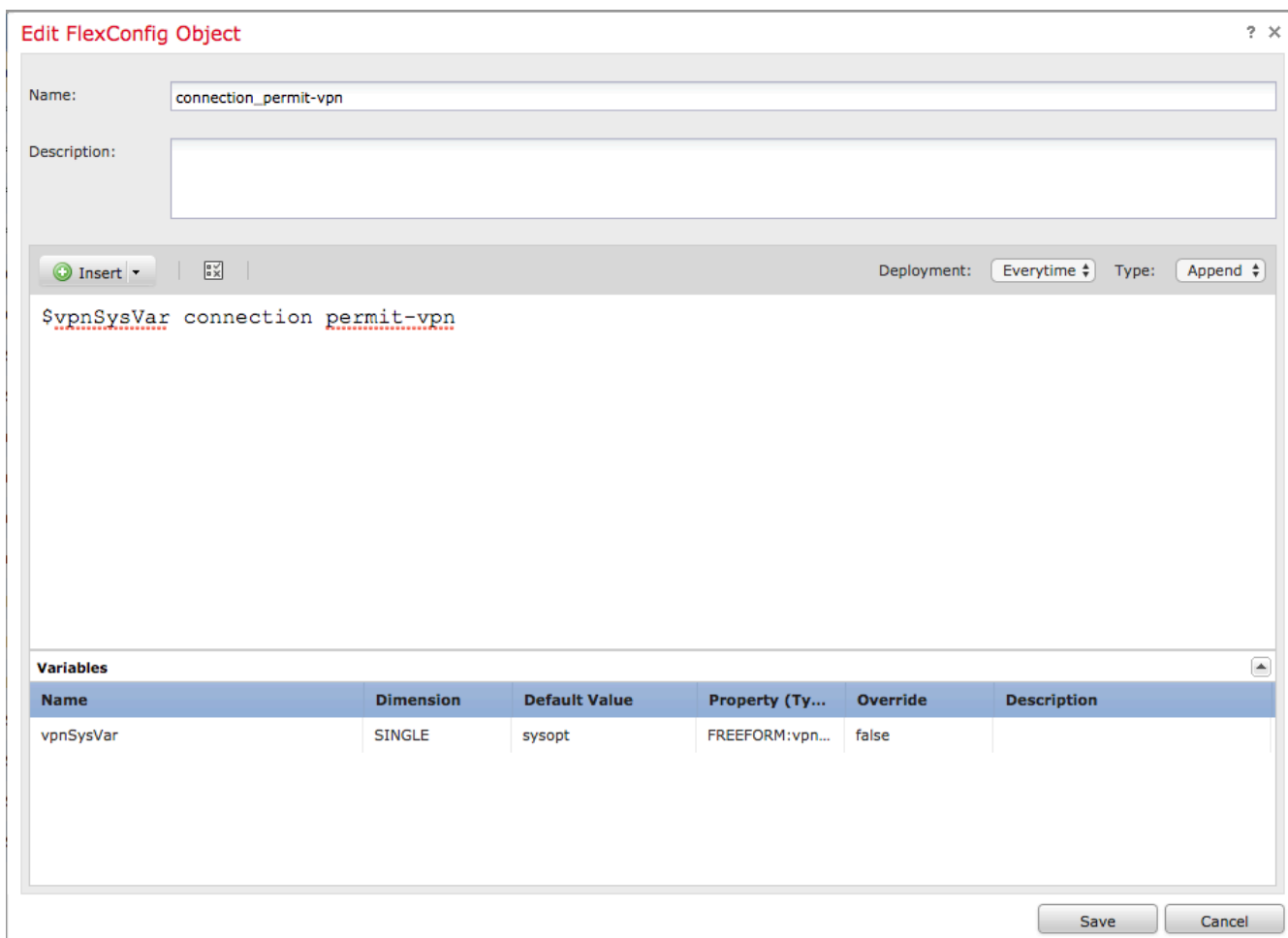
Bypass Access Control policy for decrypted traffic (`sysopt permit-vpn`)

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 versões anteriores à 6.2.3, vá para Objects > Object Management > FlexConfig > Text Object > Add Text Object.
- Crie uma variável de objeto de texto, por exemplo: `vpnSysVar` uma única entrada com valor `sysopt`.
- Ir para Objects > Object Management > FlexConfig > FlexConfig Object > Add FlexConfig Object.
- Crie o FlexConfig objeto com CLI `connection permit-vpn`.
- Insira a variável de objeto de texto no FlexConfig objeto na CLI com `$vpnSysVar connection permit-vpn`. Clique em Save:



- Aplique a FlexConfig objeto como **Append** e selecione a implantação para **Everytime**:



- Ir para **Devices > FlexConfig** e edite a política atual ou crie uma nova com **New Policy** botão.
- Adicionar apenas os FlexConfig, clique em **Save**.
- Implantar a configuração para provisionar **sysopt connection permit-vpn** no dispositivo.

Depois disso, no entanto, você não poderá usar a Política de Controle de Acesso para inspecionar o tráfego que vem dos usuários. Você ainda pode usar o filtro de VPN ou a ACL para download para filtrar o tráfego do usuário.

Se você vir pacotes descartados com o Snort dos usuários VPN, entre em contato com o TAC e

mencione o bug da Cisco ID [CSCvg91399](#).

Informações Relacionadas

- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.