

# Configuração do acesso remoto VPN de AnyConnect em FTD

## Índice

[Introdução](#)

[Requisitos](#)

[Componentes usados](#)

[Configuração](#)

1. [Preresiquites](#)

a) [importando o certificado SSL](#)

b) [configurar o servidor Radius](#)

c) [criando o conjunto de endereço para usuários VPN](#)

d) [criando o perfil XML](#)

e) [imagens transferindo arquivos pela rede de AnyConnect](#)

2. [Assistente do Acesso remoto](#)

[Conexão](#)

[Limitações](#)

[Considerações de segurança](#)

a) [Permitindo o uRPF](#)

b) [Permitindo a opção da conexão licença-VPN do sysopt](#)

## Introdução

Este original fornece um exemplo de configuração para a versão 6.2.2 e mais recente da defesa da ameaça de FirePOWER (FTD), aquele permite que o acesso remoto VPN use a versão 2 do Transport Layer Security (TLS) e do intercâmbio de chave de Internet (IKEv2). Como um cliente, Cisco AnyConnect será usado, que seja apoiado em plataformas múltiplas.

## Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento VPN, TLS e IKEv2 básico
- Conhecimento da autenticação básica, da autorização, e da contabilidade (AAA) e do RAIIO
- Experimente com centro de gerenciamento de FirePOWER

## Componentes usados

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

- Cisco FTD 6.2.2
- AnyConnect 4.5

## Configuração

# 1. Preresiquites

A fim dirigir o assistente do Acesso remoto no centro de gerenciamento de FirePOWER, primeiramente você precisará de seguir estas etapas:

- crie um certificado usado para a autenticação de servidor,
- configurar o RAIO ou o servidor Idap para a autenticação de usuário,
- crie o conjunto de endereço para usuários VPN,
- transfira arquivos pela rede imagens de AnyConnect para Plataformas diferentes.

## a) importando o certificado SSL

Os Certificados são essenciais quando você configura AnyConnect. Somente os Certificados baseados RSA são apoiados no SSL e no IPSec. Os Certificados elípticos do Digital Signature Algorithm da curva (ECDSA) estão apoiados em IPSec, mas nele não são possíveis para distribuir o pacote novo de AnyConnect ou o perfil XML quando o certificado baseado ECDSA é usado. Significa que você pode o usar para IPSec, mas você terá que predeploy o pacote de AnyConnect e o perfil XML a cada usuário e toda a mudança no perfil XML terão que ser refletidos manualmente em cada cliente (erro:

[CSCtx42595](#) ). [Adicionalmente o certificado deve ter a extensão alternativa sujeita do nome com nome e/ou IP address DNS para evitar erros em navegadores da Web.](#)

Há diversos métodos para obter um certificado no dispositivo FTD, mas seguro e fácil é criar uma solicitação de assinatura de certificado (CSR), assina a e então o certificado de importação emitidos para a chave pública, que estava no CSR. É aqui como fazer isso:

- Vá aos **objetos** > ao **Gerenciamento do objeto** > ao **PKI** > ao **registro CERT**, clique sobre o **registro CERT Add**:

## Add Cert Enrollment

Name:\* vpn.cisco.com

Description:

**CA Information** Certificate Parameters Key Revocation

Enrollment Type: Manual

CA Certificate:\*

```

Cf0wa/5Kzu1ME0eiDdunGwWsiDGS5S+yngvWuHkZaiQOXVWVXGKIM
L6/bXeoHTiIFM
PJqzP/S58YbpyEWFmrHSZ3wNhvq3keHtAw5KcwHtA4nKOkxuA82zX
nQLIXYI2r8h
HcbaVabAufb7CV1mdwSVDtJOBFI2ftpQONj67VN902vtN8FwA8UAsy
73zzRPbIIH
Yh5Nr9WhZn/wcxvRmi+sEi7cBrpXG1g8+cbVr5z4LWXD28zoKKoSZjx
LfJurARIW
SENBXsxAuKRQc9wgDZKHR9sA2r1AGFMm0NpSKmSNkGbkS4q37V
N9EyToUg9OXRKI
AMImjysdgAO7O9HmeFgxbOqL8GdczEYs7VMNxQ2Jih+oRnDASSXg
AsNmi2/xIN9H
CfyjTgclvfm9gOI8JjbuX8O85RhO2cKMI3ZEGIIpeYcUbv+cWCeUSL6
mox6p9CXe
HGyUpYafhN1D78+Y8eeW9YSai0B9b54yKI5YdXjphYHXmZQ18edtzv
WIq3Ysrns2
qBojiQ==
-----END CERTIFICATE-----

```

Allow Overrides:

Save Cancel

- Selecione o **tipo do registro** e cole o certificado do Certificate Authority (CA),
- Vão então a segunda aba e o **FQDN** seletor do **costume** e enchem todos os campos necessários, por exemplo:

## Add Cert Enrollment



Name:\*

vpn.cisco.com

Description:

CA Information

**Certificate Parameters**

Key

Revocation

Include FQDN:

Custom FQDN

Custom FQDN:

vpn.cisco.com

Include Device's IP Address:

10.48.30.1

Common Name (CN):

vpn.cisco.com

Organization Unit (OU):

TAC

Organization (O):

Krakow

Locality (L):

PL

State (ST):

malopolskie

Country Code (C):

PL

Email (E):

tac@cisco.com

Include Device's Serial Number

Allow Overrides:

Save

Cancel

- Na terceira aba, selecione o tipo chave, escolha o nome e o tamanho. Para o RSA, 2048 bytes são mínimos.
- Clique a salvaguarda e vá ao > Add dos **dispositivos** > dos **Certificados** > **certificado novo**. Selecione então o **dispositivo**, e sob o **registro CERT** selecione o trustpoint que você apenas criou, clique **adicionam**:

## 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

- Mais tarde, ao lado do nome do trustpoint, clique sobre  o ícone, então sim e em seguida essa cópia CSR ao CA e assine-o. O certificado deve ter atributos como o servidor HTTPS normal.
- Após ter recebido o certificado do CA no formato base64, selecione-o do disco e clique-o a **importação**. Quando isto sucede, você deve ver:

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

## b) configurar o servidor Radius

No platform FTD, a base de dados de usuário local não pode ser usada, assim que você precisa o RAI0 ou o servidor Idap para a autenticação de usuário. Para configurar o RAI0:

- Vá aos **objetos** > ao **Gerenciamento do objeto** > ao **grupo de servidor Radius do** > Add do **grupo de servidor Radius**.
- Encha o nome e adicionar o IP address junto com o segredo compartilhado, **salv guarda do** clique:

## 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)

- Em seguida que você deve ver o server na lista:

Name	Value	Override	
ISE	1 Server	<span style="color: red;">✘</span>	 

### c) criando o conjunto de endereço para usuários VPN

- Vá às **associações do > Add IPv4 dos objetos > do Gerenciamento > dos conjuntos de endereços do objeto:**
- Põe o nome e a escala, máscara não é precisada:

## Edit IPv4 Pool

Name:\*

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

Mask:

Description:

Allow Overrides:

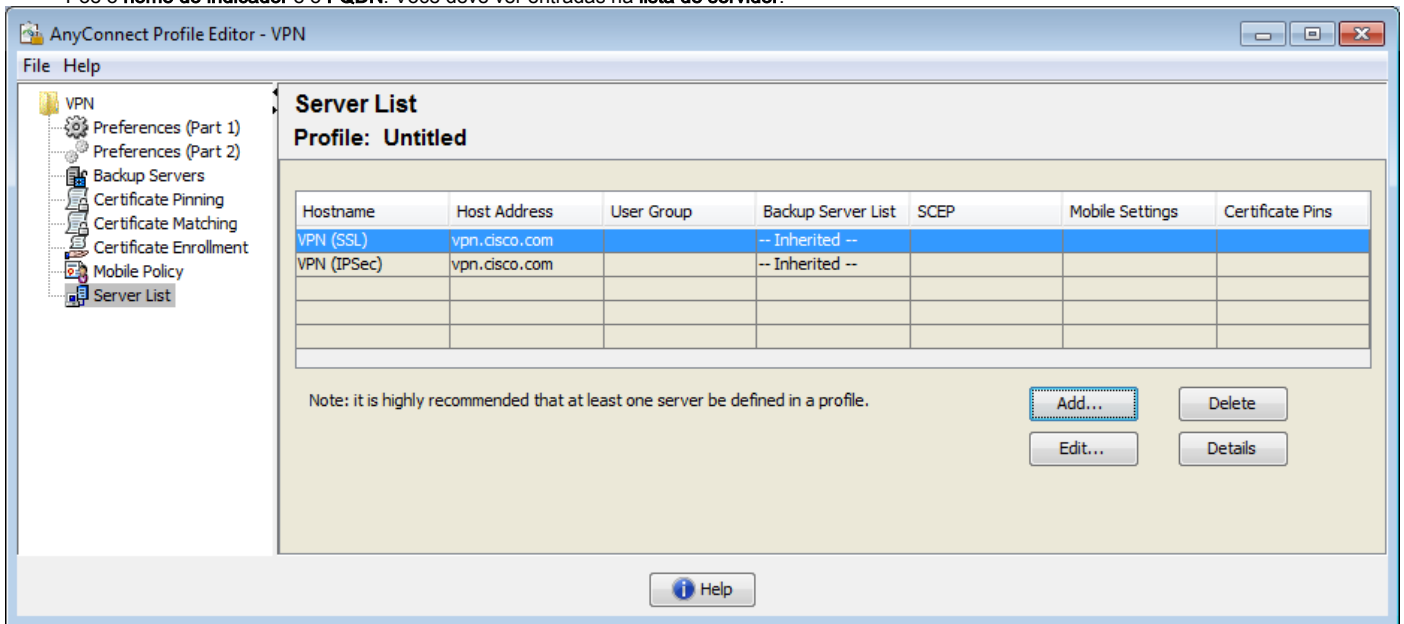
 Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

**Override (0)**

### d) criando o perfil XML

- Transfira o editor do perfil do local de Cisco e abra-o.
- Vá ao > Add da **lista de servidor...**

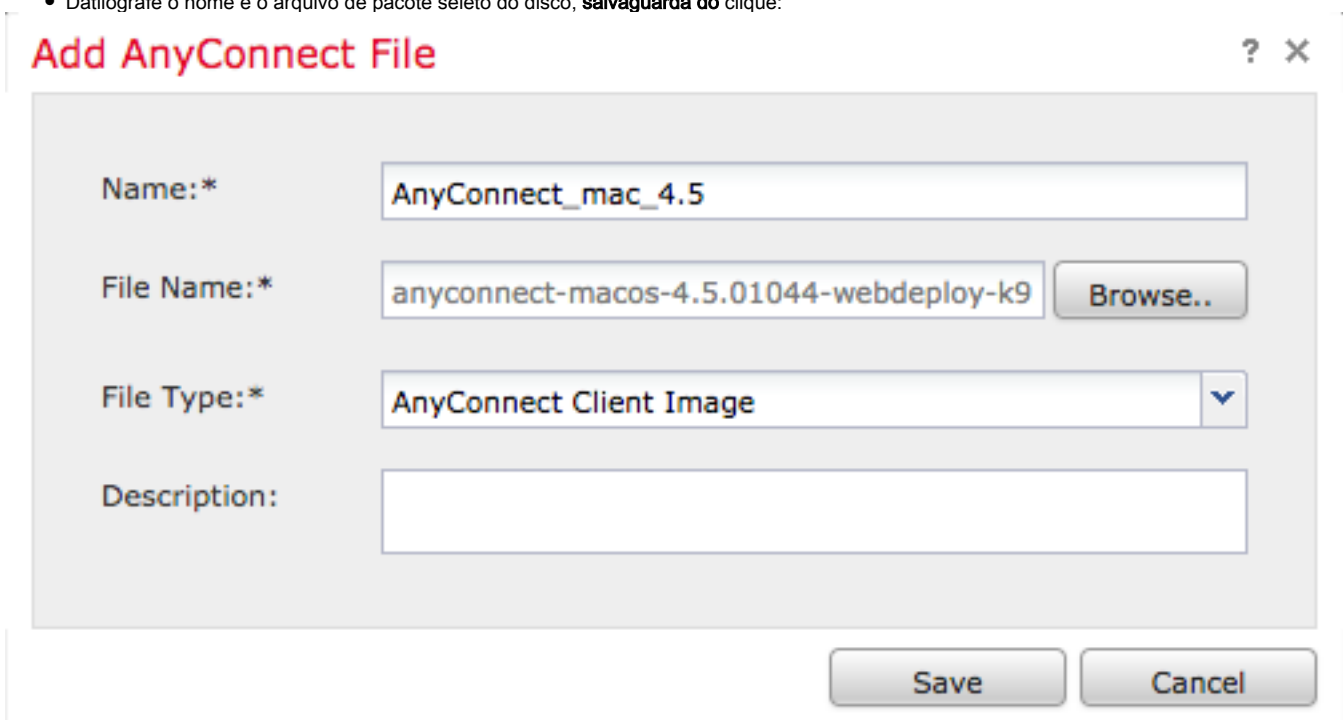
- Põe o **nome do indicador** e o **FQDN**. Você deve ver entradas na **lista de servidor**:



- **APROVAÇÃO** e arquivo > salvaguarda do clique como...

### e) imagens transferindo arquivos pela rede de AnyConnect

- Imagens do pacote da transferência do local de Cisco.
- Vai aos **objetos** > ao **Gerenciamento do objeto** > ao **arquivo VPN** > de **AnyConnect** o **arquivo de AnyConnect** do > Add.
- Datilografe o nome e o arquivo de pacote seletor do disco, **salvaguarda** do clique:



- Adicionar mais pacotes segundo suas exigências.

## 2. Assistente do Acesso remoto

- Vai aos **dispositivos** > ao > Add VPN > de **Acesso remoto uma configuração nova**.
- Nomeie o perfil de acordo com suas necessidades, dispositivo seletor FTD:

Name:\*

Description:

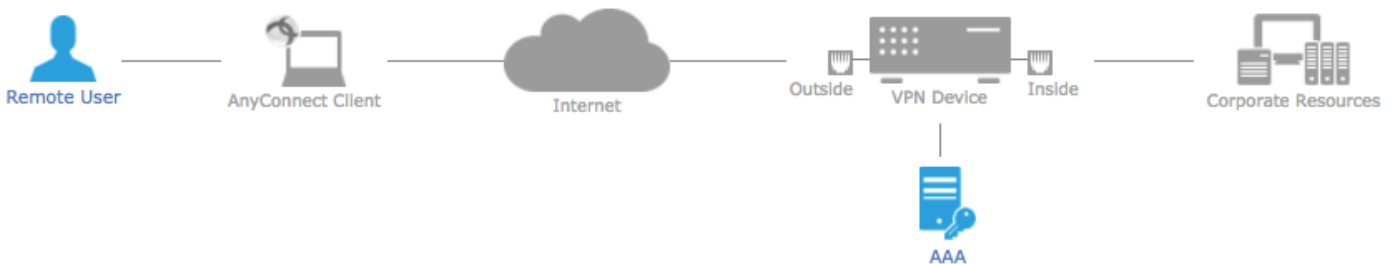
VPN Protocols:  SSL  IPsec-IKEv2

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

ASA5512-X\_FTD

ASA5512-X\_FTD

- No perfil de conexão da etapa, o tipo nome do perfil de conexão, seleciona o Authentication Server e os conjuntos de endereços que você tem criado mais cedo:



### 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:  ✎

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 sobre a política do grupo **Edit** e na aba **AnyConnect**, perfil seletor do cliente, a seguir clique a **salv guarda**:



## 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](#).

- Na página seguinte, nas imagens seletas e no clique de AnyConnect **em seguida**:

<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

- Na tela seguinte, selecione a **interface de rede** e o **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.

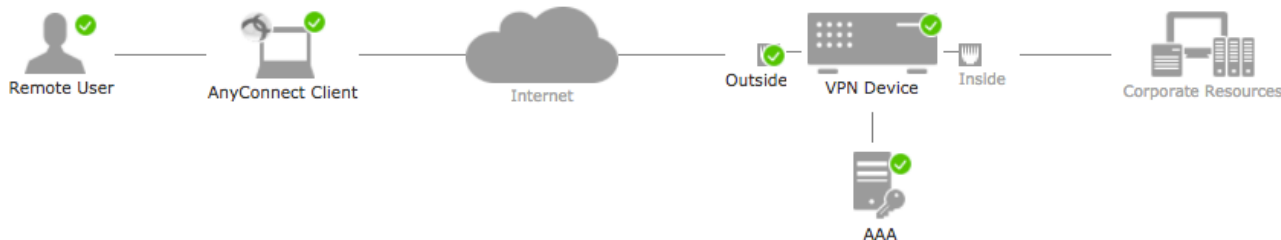
### Device Certificates

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.

- Quando tudo é configurado corretamente, você pode clicar o **revestimento** e então **distribuí-lo**:



### 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'

- Isto copiará a configuração inteira junto com Certificados e pacotes de AnyConnect ao dispositivo FTD.

## Conexão

Para conectar a FTD que você precisa de abrir um navegador, a tipo nome DNS ou a IP address apontando à interface externa, neste exemplo <https://vpn.cisco.com>. Você terá que então entrar usando as credenciais armazenadas no servidor Radius e seguir instruções na tela. Uma vez que AnyConnect instala, você precisa então de pôr o mesmo endereço no indicador de AnyConnect e o clique **conecta**.

## Limitações

Atualmente unsupported em FTD, mas disponível no ASA:

- Autenticação de AAA dobro
- Política do acesso dinâmico
- Varredura do host
- Postura ISE
- CoA do RAIIO
- Carga-equilibrador VPN
- Autenticação local (realce: [CSCvf92680](#) )
- Mapa do atributo LDAP
- Personalização de AnyConnect
- Scripts de AnyConnect

- Localização de AnyConnect
- Por-APP VPN
- Proxy SCEP
- Integração WSA
- SAML SSO
- Mapa cripto dinâmico IKEv2 simultâneo para o RA e o L2L VPN
- Os módulos de AnyConnect (NAM, Hostscan, AMP Habilitador etc.) – DARDO são instalados à revelia
- TACACS, Kerberos (autenticação KCD e RSA SDI)
- Proxy do navegador

## Considerações de segurança

Você precisa de recordar à revelia aquele, opção da conexão licença-VPN do sysopt é desabilitado. Este meios, isso que você precisa de permitir o tráfego que vem do conjunto de endereço na interface externa através da política do controle de acesso. Embora a regra do PRE-filtro ou do controle de acesso seja pretensão adicionada permitir o tráfego VPN somente, se o tráfego da minuta acontece combinar os critérios da regra, está permitido erroneamente.

Há duas aproximações a este problema. Primeiramente, o TAC recomendou a opção, é permitir anti-falsificação (no ASA conhecido como o Unicast Reverse Path Forwarding - uRPF) para a interface externa, e o segundo é permitir a conexão licença-VPN do sysopt de contornar completamente a inspeção do Snort. A primeira opção reserva inspecionar normalmente o tráfego que vai a e dos usuários VPN.

### a) Permitindo o uRPF

- crie uma rota nula para a rede usada para usuários de acesso remotos, definido na seção C. Apenas vai aos **dispositivos** > ao **Gerenciamento de dispositivos** > **edita** > a **rota do** > **Add do roteamento** > da **rota estática**:

### 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 (1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:

OK Cancel

- em segundo lugar, você precisa de permitir o uRPF na relação que está terminando conexões de VPN. Você pode encontrar que nos **dispositivos > no Gerenciamento de dispositivos > para editar > relações > edita > avançou a configuração do > segurança > permite a anti falsificação:**

Quando o usuário é conectado, a rota de 32 bits está instalada para esse usuário na tabela de roteamento. O tráfego do texto claro originado de outro, IP address não utilizados do pool é deixado cair pelo uRFP. Anti-falsificação foi descrito nesta página:

[Ajuste parâmetros da configuração de segurança na defesa da ameaça de FirePOWER](#)

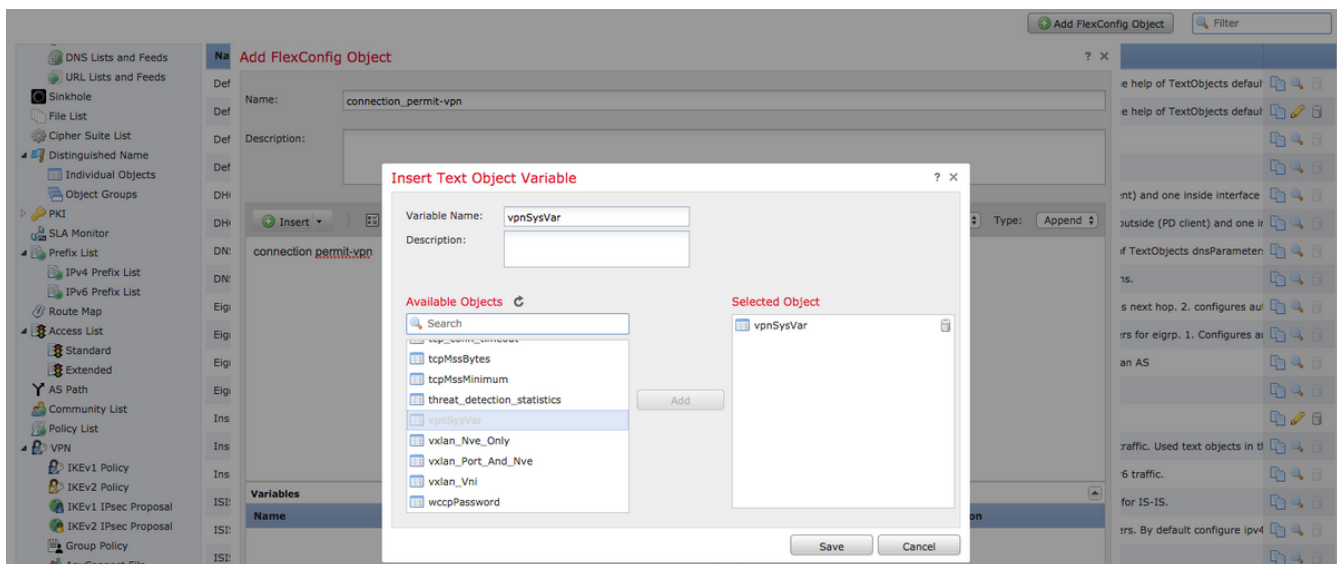
#### b) Permitindo a opção da conexão licença-VPN do sysopt

- Se você tem a versão 6.2.3 ou mais recente, há uma opção para fazê-la durante o assistente ou sob **dispositivos > VPN > Acesso remoto > perfil > interfaces de acesso VPN:**

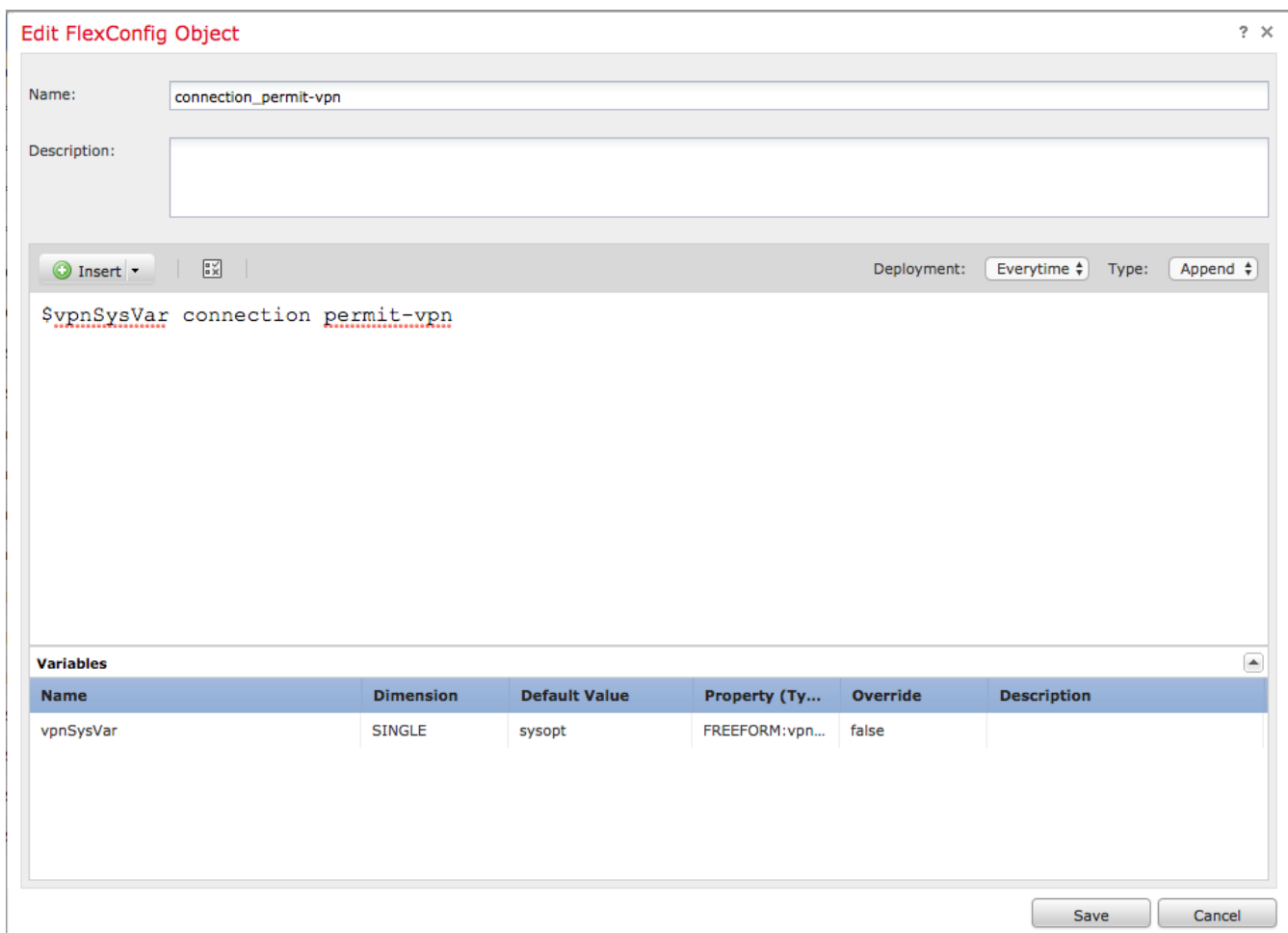
##### Access Control for VPN Traffic

- 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 versões antes de 6.2.3, vá aos **objetos > ao Gerenciamento do objeto > ao FlexConfig > ao objeto do texto do > Add do objeto do texto.**
- Crie uma variável do objeto do texto, por exemplo: `vpnSysVar` uma única entrada com valor "sysopt"
- Vá ao **objeto de FlexConfig do > Add dos objetos > do Gerenciamento > do FlexConfig > de FlexConfig do objeto do objeto.**
- Crie o objeto de FlexConfig com o CLI "conexão licença-VPN":
- Introduza a variável do objeto do texto no objeto do flexconfig no início do CLI como "a conexão licença-VPN `$vpnSysVar`", **salv guarda do clique:**



- Aplique o objeto de FlexConfig como **adicionam** e selecione o desenvolvimento a **todas as vezes**:



- Vá aos **dispositivos** > ao **FlexConfig** e edite a política existente ou crie um novo com o botão **novo da política**.
- Adicionar apenas FlexConfig criado, **salv guarda do clique**.
- Distribua a configuração para provision "sysopt o comando da conexão licença-VPN" no dispositivo.

Isto contudo, removerá a possibilidade para usar a política do controle de acesso para inspecionar o tráfego que vem dos usuários. Você pode ainda usar o filtro VPN ou ACL baixável para filtrar o tráfego de usuário.

Se você vê problemas com os pacotes deixando cair do Snort dos usuários VPN, contacte o TAC que provê [CSCVg91399](mailto:CSCVg91399).