Configuração do acesso remoto VPN de AnyConnect em FTD

Índice

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 RAIO
- 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 ldap para a autenticação de usuário,
- crie o conjunto de endereço para usuários VPN,
- transfira arquivos pela rede imagens de AnyConnect para Plataformas diferentes.

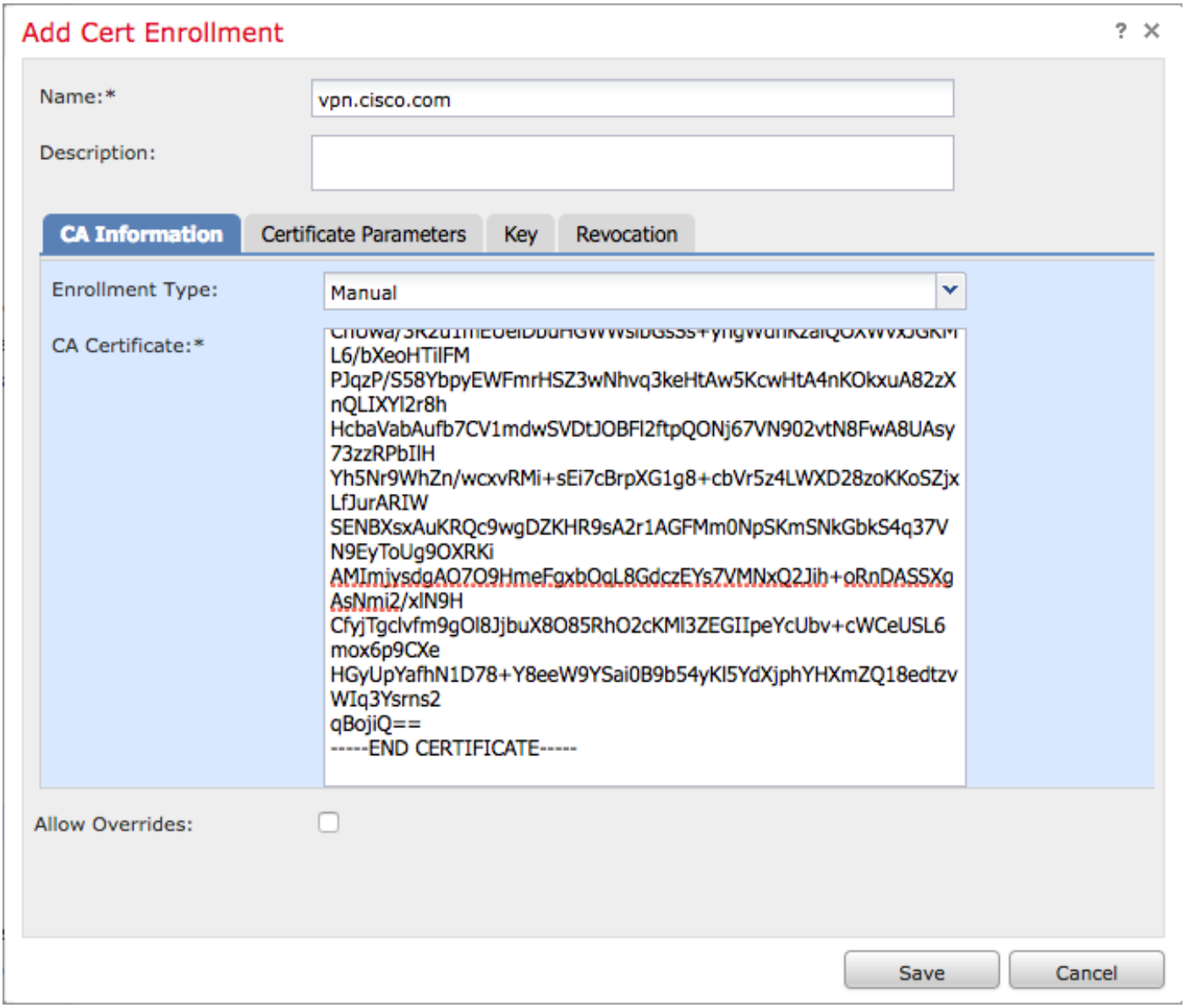
a) importando o certificado SSL

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:

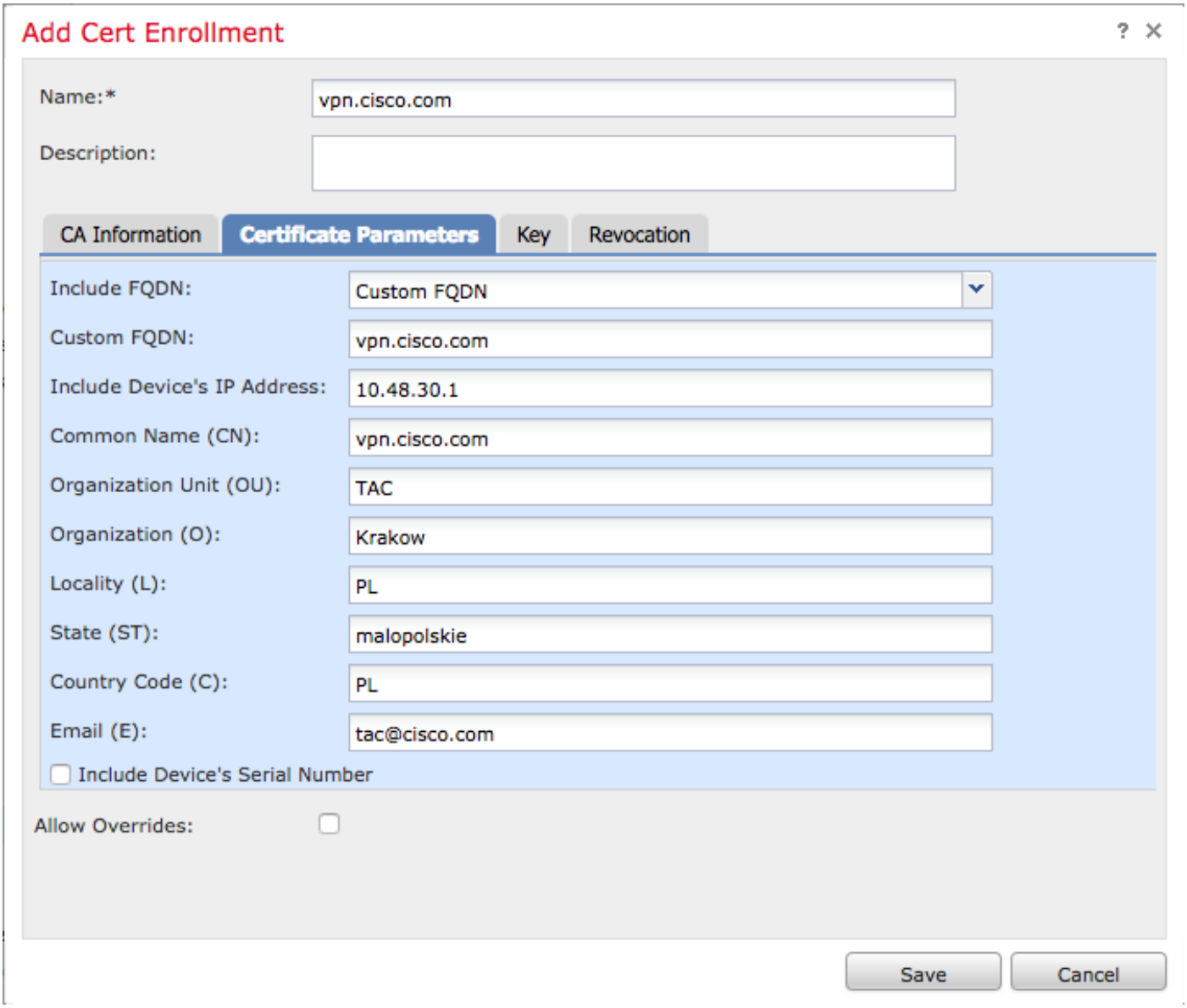
CSCtx42595). Adicionalmente o certificado deve ter a extensão alternativa sujeita do nome com nome e/ou IP address DNS para evitar erros em navegadores da Web.

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:

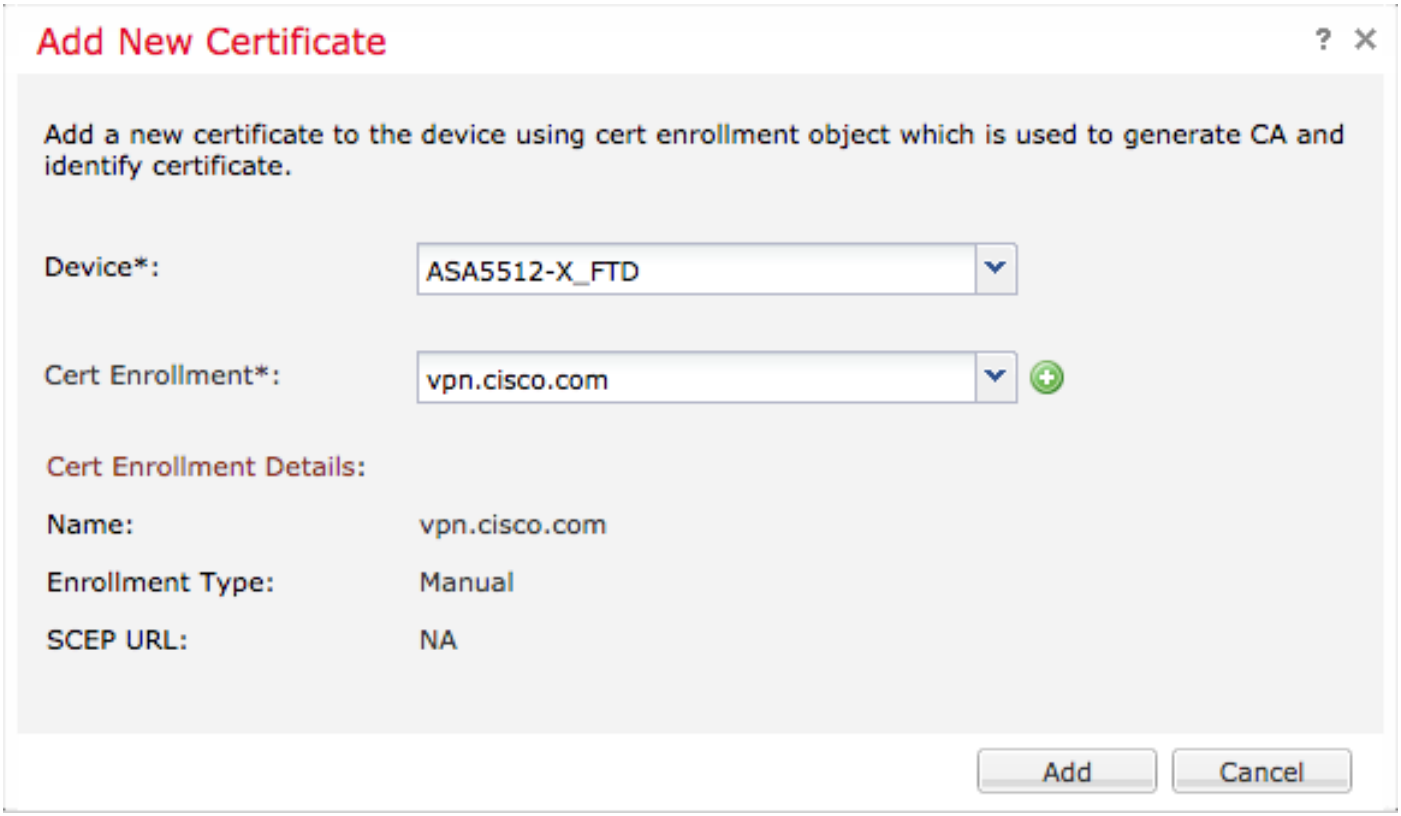
- Vá aos **objetos** > ao **Gerenciamento do objeto** > ao **PKI** > ao **registro CERT**, clique sobre o **registro CERT Add**:



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



- 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**:



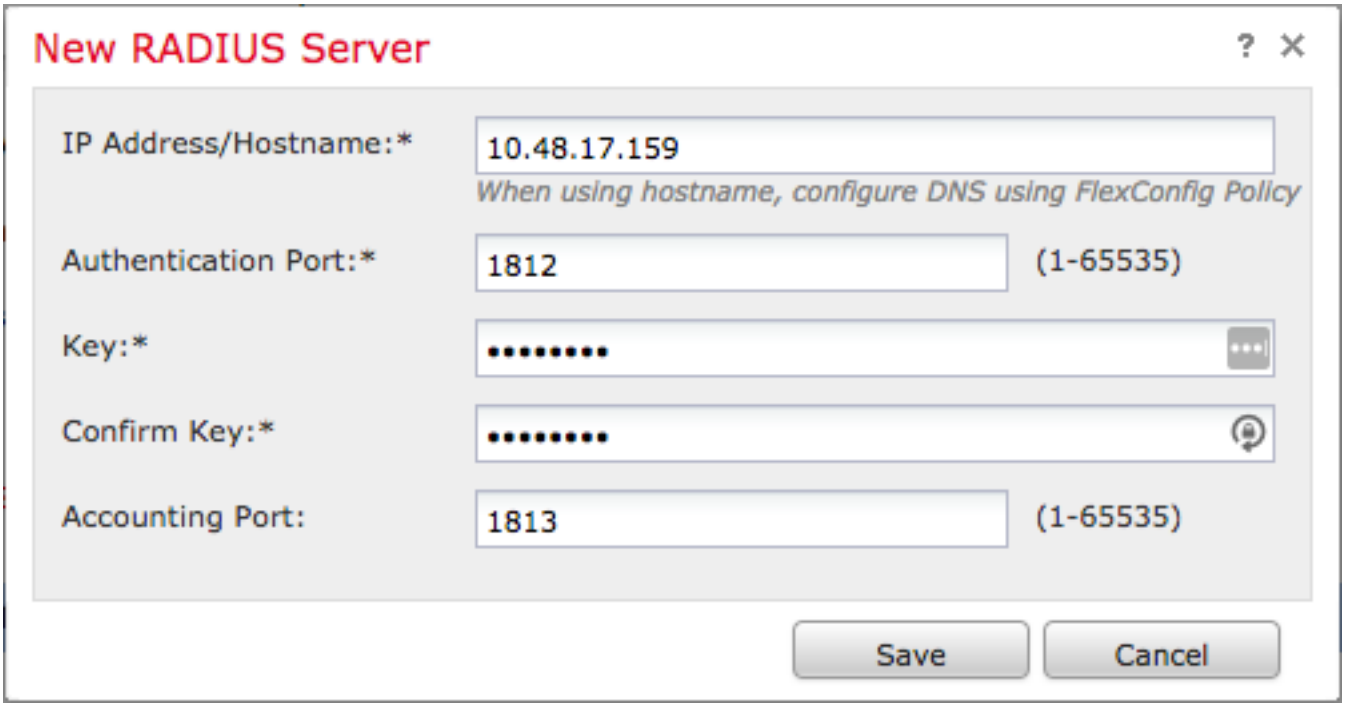
- Mais tarde, ao lado do nome do trustpoint, clique sobre o ícone, então **sim e em seguida essa cópia CSR ao CA e assine-o. O certificado deve ter atributos como o servidor HTTPS normal.**
- Após ter recebido o certificado do CA no formato base64, selecione-o do disco e clique-o a **importação**. Quando 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 platftorm FTD, a base de dados de usuário local não pode ser usada, assim que você precisa o RAIO ou o servidor ldap para a autenticação de usuário. Para configurar o RAIO:

- 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, **salvaguarda do** clique:



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

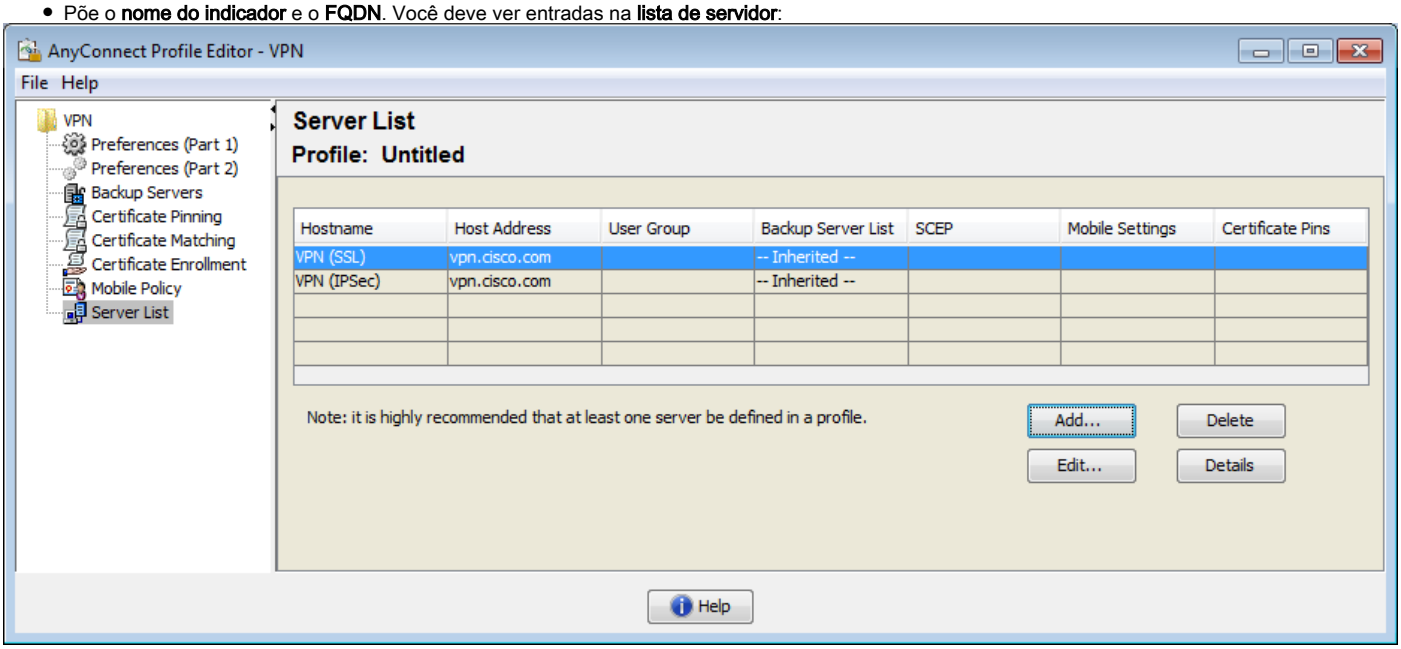
c) criando o conjunto de endereço para usuários VPN

- 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:

d) criando o perfil XML

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

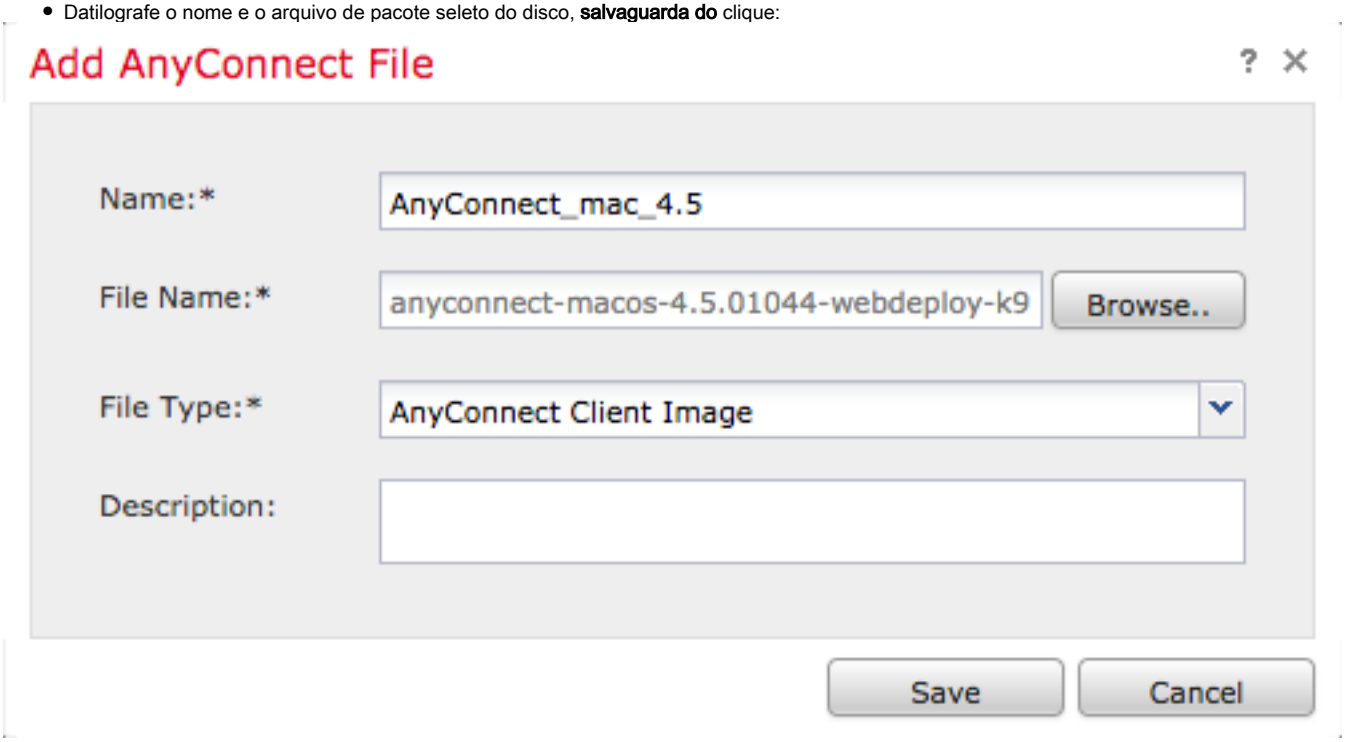
- Põe o **nome do indicador** e o **FQDN**. Você deve ver entradas na **lista de servidor**:



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

e) imagens transferindo arquivos pela rede de AnyConnect

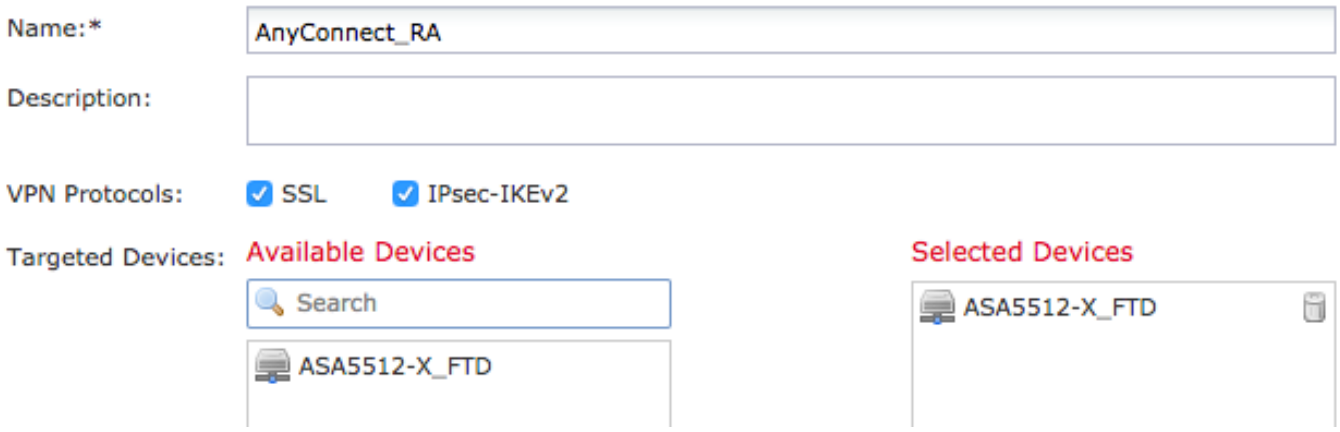
- Imagens do pacote da transferência do local de Cisco.
- Vai aos **objetos** > ao **Gerenciamento do objeto** > ao **arquivo VPN** > de **AnyConnect o arquivo de AnyConnect do** > Add.
- Datilografe o nome e o arquivo de pacote seleto do disco, **salvaguarda do** clique:



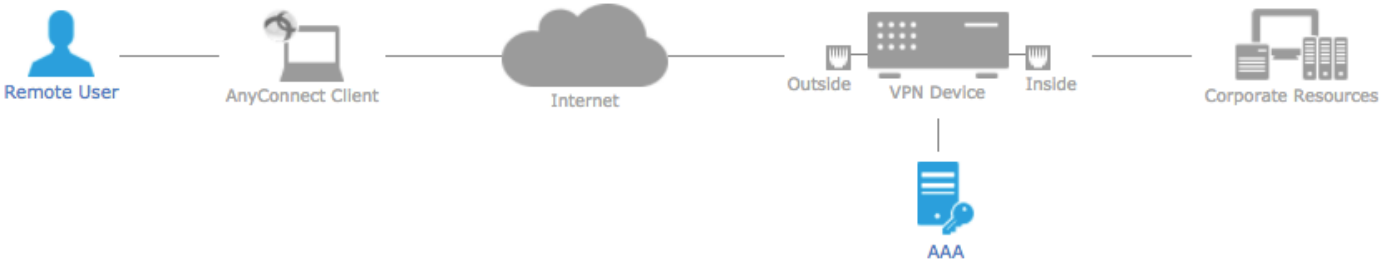
- Adicionar mais pacotes segundo suas exigências.

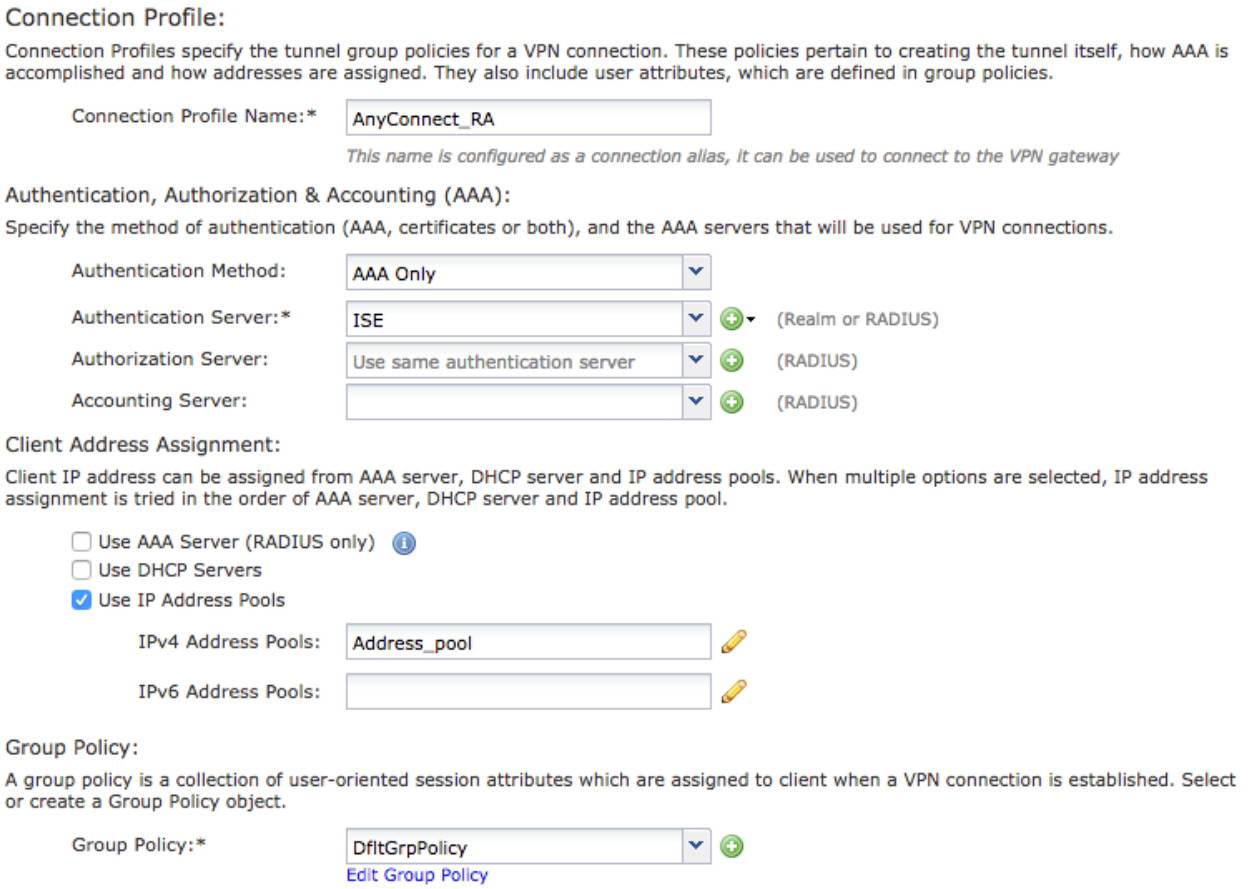
2. Assistente do Acesso remoto

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

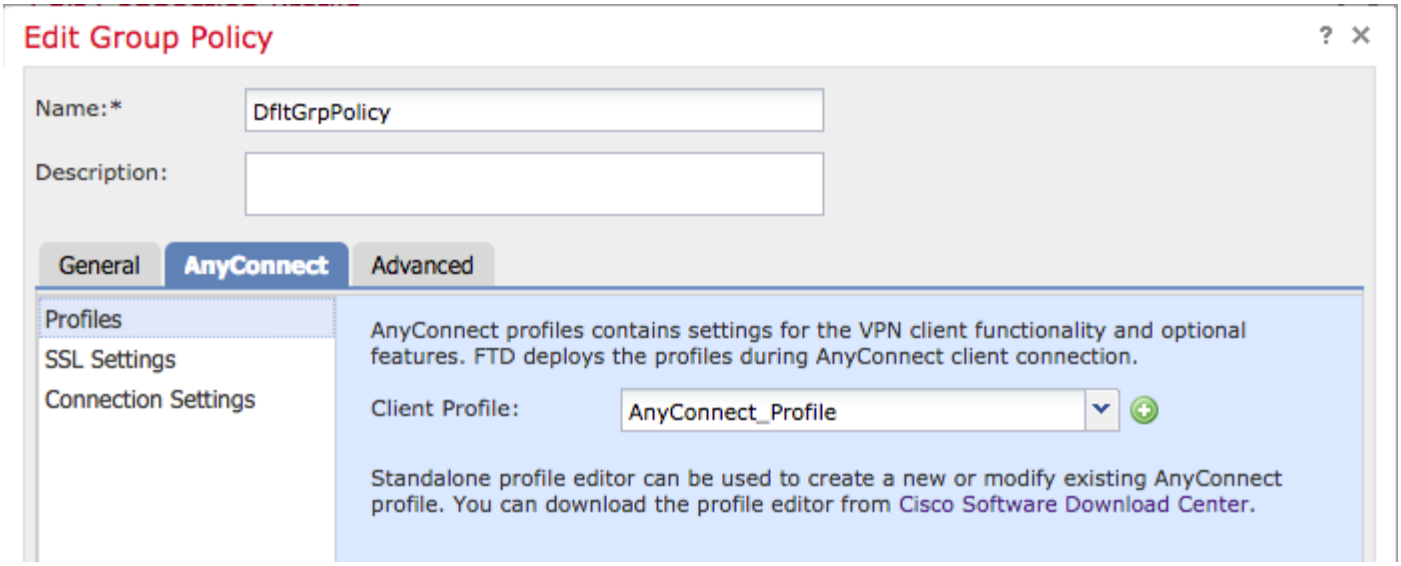


- **No perfil de conexão da etapa, o tipo nome do perfil de conexão, seleciona o Authentication Server e os conjuntos de endereços que você tem criado mais cedo:**

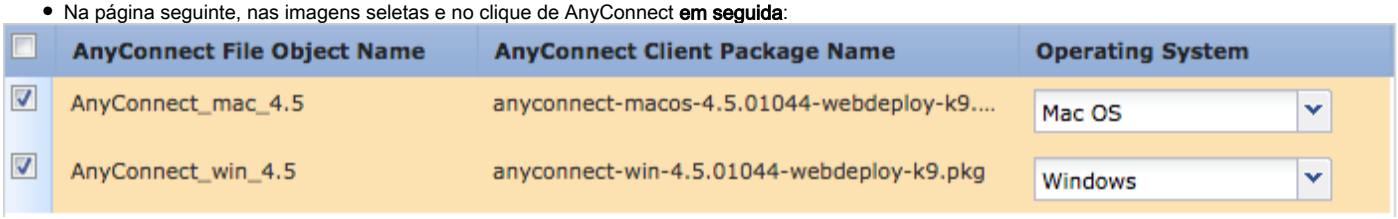




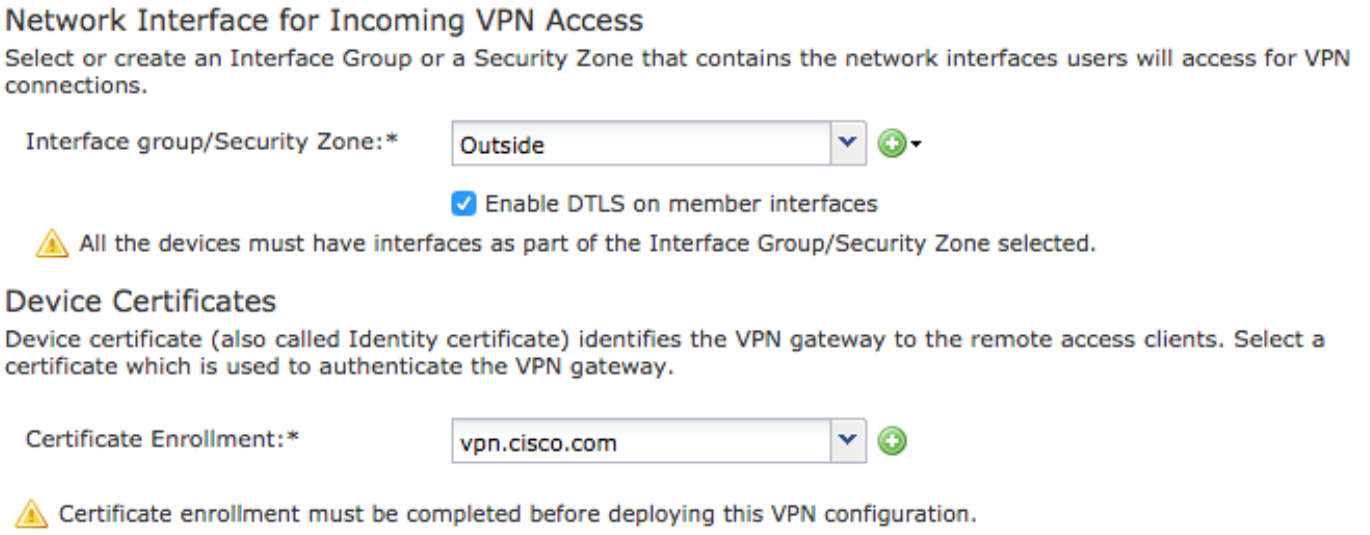
- Clique sobre a **política do grupo Edit** e na aba **AnyConnect**, **perfil** seleto do **cliente**, a seguir clique a **salvaguarda**:



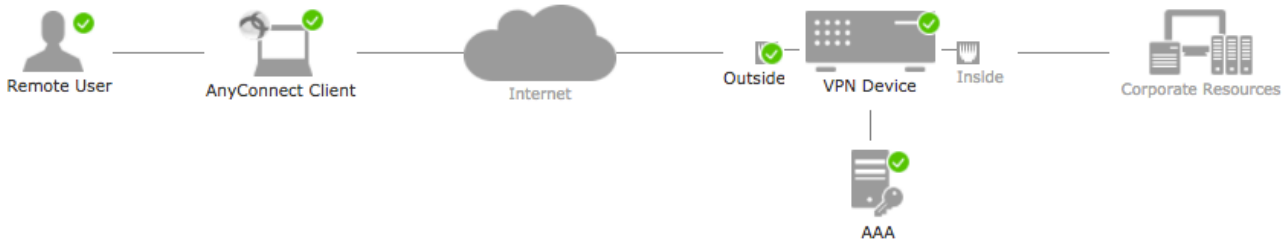
- Na página seguinte, nas imagens seletas e no clique de AnyConnect **em seguida**:



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



- Quando tudo é configurado corretamente, você pode clicar o **revestimento** e então **distribui-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 RAIO
- 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

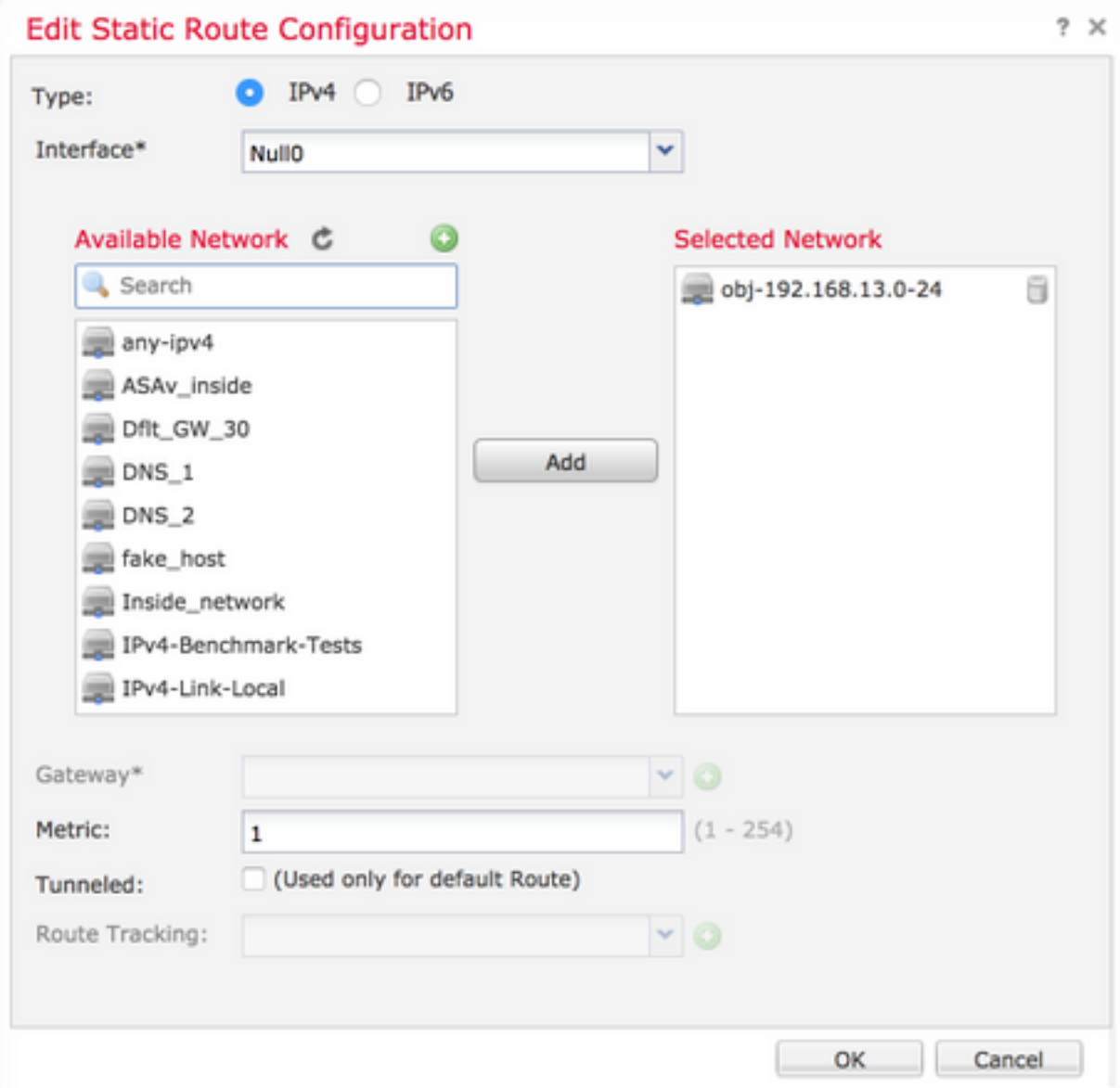
Considerações de segurança

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.

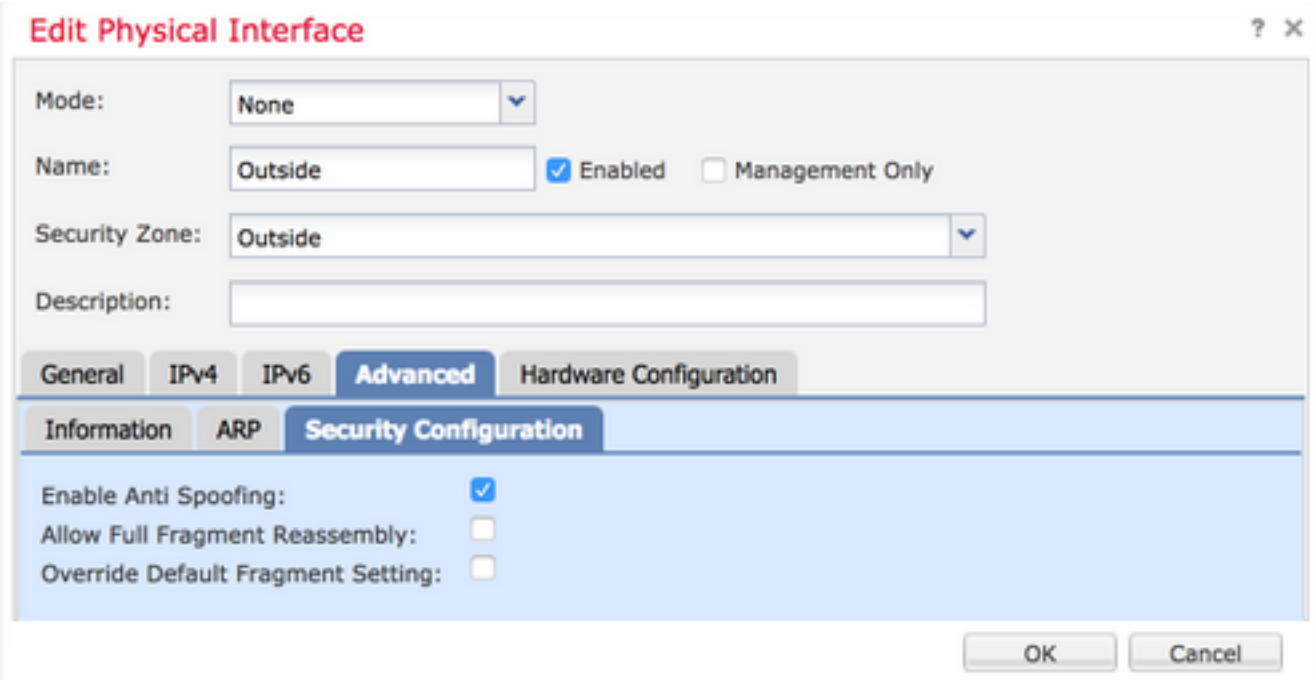
Há duas aproximações a este problema. Primeiramente, o TAC recomendou a opção, é permitir anti-falsificação (no ASA conhecido como o Unicast Reverse Path Forwarding - uRPF) para a interface externa, e o segundo é permitir a conexão licença-VPN do sysopt de contornear completamente a inspeção do Snort. 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**:



- 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**:

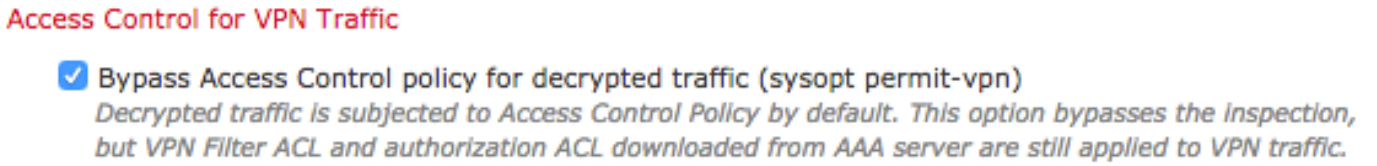


Quando o usuário é conectado, a rota de 32 bits está instalada para esse usuário na tabela de roteamento. O tráfego do texto claro originado de outro, IP address não utilizados do pool é deixado cair pelo uRFP. Anti-falsificação foi descrito nesta página:

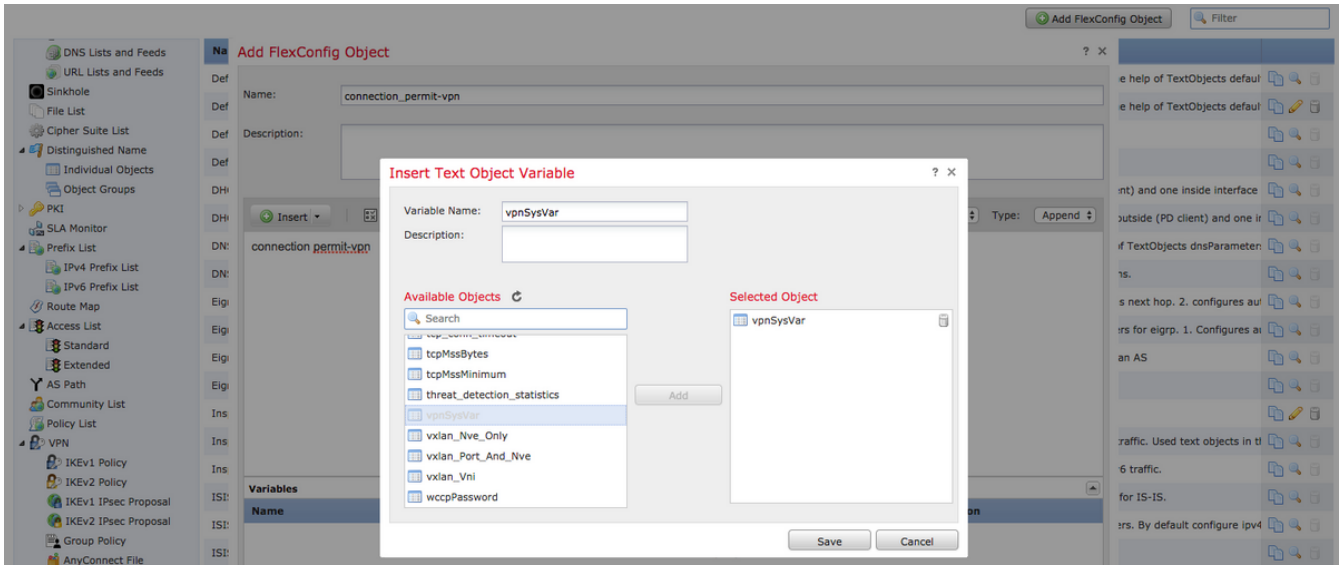
Ajuste parâmetros da configuração de segurança na defesa da ameaça de FirePOWER

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

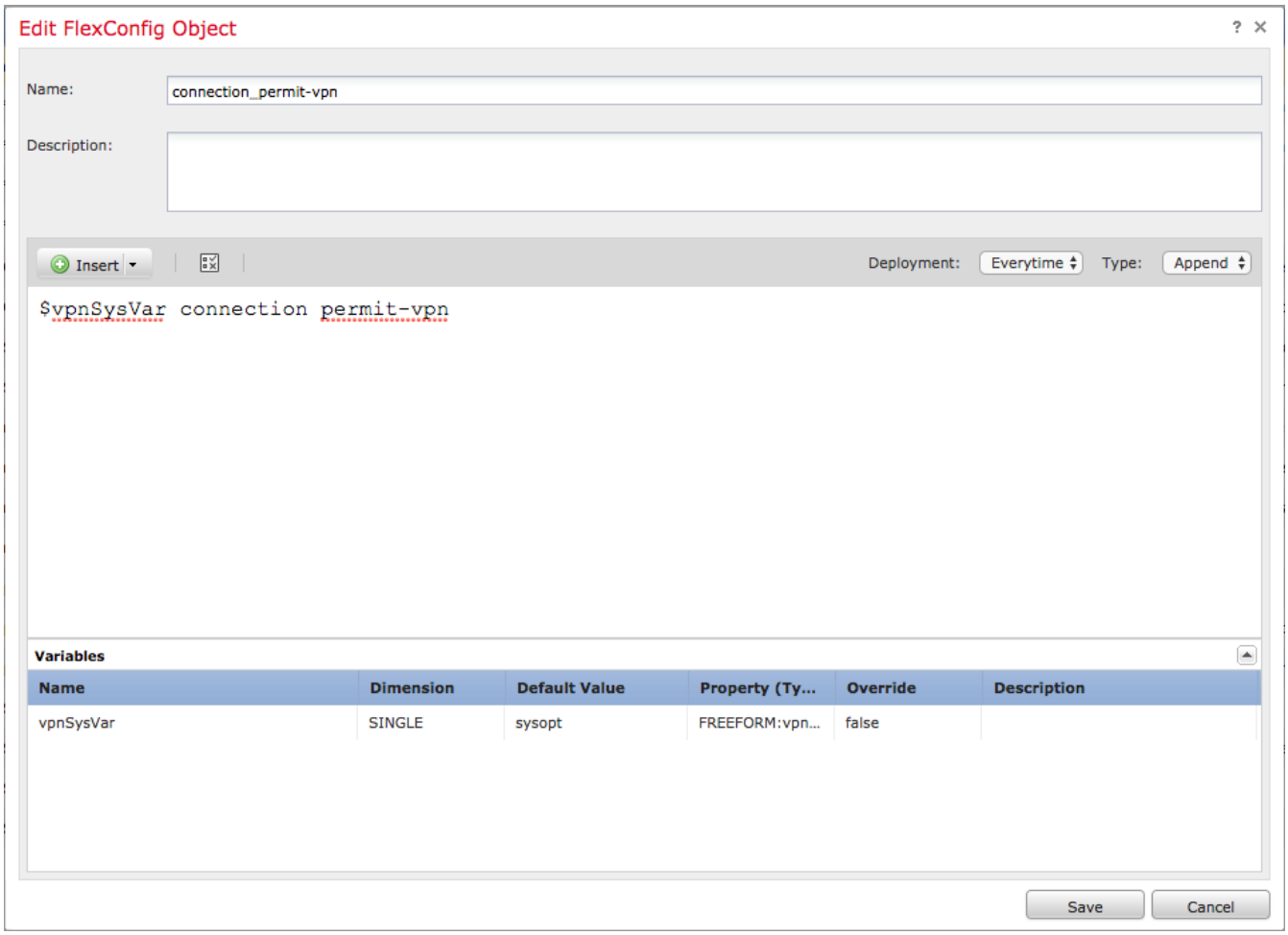
- Se você tem a versão 6.2.3 ou mais recente, há uma opção para fazê-la durante o assistente ou sob **dispositivos > VPN > Acesso remoto >** *perfil* **> interfaces de acesso** *VPN*:



- 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`", **salvaguarda 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, **salvaguarda 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 .