

Configurar o AnyConnect VPN Client no FTD: Hairpin e Isenção de NAT

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Etapa 1. Importar um certificado SSL](#)

[Etapa 2. Configurar um servidor RADIUS](#)

[Etapa 3. Criar um pool de IPs](#)

[Etapa 4. Criar um perfil XML](#)

[Etapa 5. Carregar perfil XML do Anyconnect](#)

[Etapa 6. Carregar imagens do AnyConnect](#)

[Passo 7. Assistente de VPN de Acesso Remoto](#)

[Isenção de NAT e Hairpin](#)

[Etapa 1. Configuração de isenção de NAT](#)

[Etapa 2. Configuração Hairpin](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar a solução de VPN de acesso remoto da Cisco (AnyConnect) no Firepower Threat Defense (FTD), v6.3, gerenciado pelo FMC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico de VPN de acesso remoto, Secure Sockets Layer (SSL) e Internet Key Exchange versão 2 (IKEv2)
- Conhecimento de Autenticação, Autorização e Tarifação Básica (AAA - Basic Authentication, Authorization, and Accounting) e RADIUS
- Conhecimentos básicos de CVP
- Conhecimento básico de FTD

Componentes Utilizados

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

- Cisco FMC 6.4
- FTD 6.3 da Cisco
- AnyConnect 4.7

Este documento descreve o procedimento para configurar a solução de VPN de acesso remoto da Cisco (AnyConnect) no Firepower Threat Defense (FTD), versão 6.3, gerenciado pelo Firepower Management Center (FMC).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento destina-se a cobrir a configuração em dispositivos FTD. Se você procurar o exemplo de configuração do ASA, consulte o documento: <https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html>

Limitações:

Atualmente, esses recursos não são suportados no FTD, mas ainda estão disponíveis em dispositivos ASA:

- Autenticação AAA dupla (disponível no FTD versão 6.5)
- Política de acesso dinâmico
- Verificação de host
- postura de ISE
- RADIUS CoA
- Balanceador de carga de VPN
- Autenticação local (disponível no Firepower Device Manager 6.3. ID de bug da Cisco [CSCvf92680](#))
- Mapa de atributos LDAP (disponível via FlexConfig, ID de bug da Cisco [CSCvd64585](#))
- Personalização do AnyConnect
- Scripts do AnyConnect
- Localização do AnyConnect
- VPN por aplicativo
- proxy SCEP
- Integração com WSA
- SAML SSO (ID de bug da Cisco [CSCvq90789](#))
- Mapa de criptografia dinâmica IKEv2 simultâneo para RA e VPN L2L
- Módulos do AnyConnect (NAM, Hostscan, AMP Enabler, SBL, Umbrella, Web Security etc.). O DART é o único módulo instalado por padrão nesta versão.
- TACACS, Kerberos (autenticação KCD e RSA SDI)
- Proxy do navegador

Configurar

Para passar pelo assistente de VPN de acesso remoto no FMC, estas etapas devem ser concluídas:

Etapa 1. Importar um certificado SSL

Os certificados são essenciais ao configurar o AnyConnect. Somente certificados baseados em RSA têm suporte para SSL e IPsec.

Os certificados ECDSA (Elliptic Curve Digital Signature Algorithm) são suportados no IPsec, no entanto, não é possível implantar um novo pacote do AnyConnect ou perfil XML quando o certificado baseado em ECDSA é usado.

Ele pode ser usado para IPsec, mas você deve pré-implantar os pacotes do AnyConnect junto com o perfil XML, todas as atualizações de perfil XML devem ser enviadas manualmente em cada cliente (ID de bug Cisco [CSCtx42595](#)).

Além disso, o certificado deve conter uma extensão de Nome Comum (CN) com nome DNS e/ou endereço

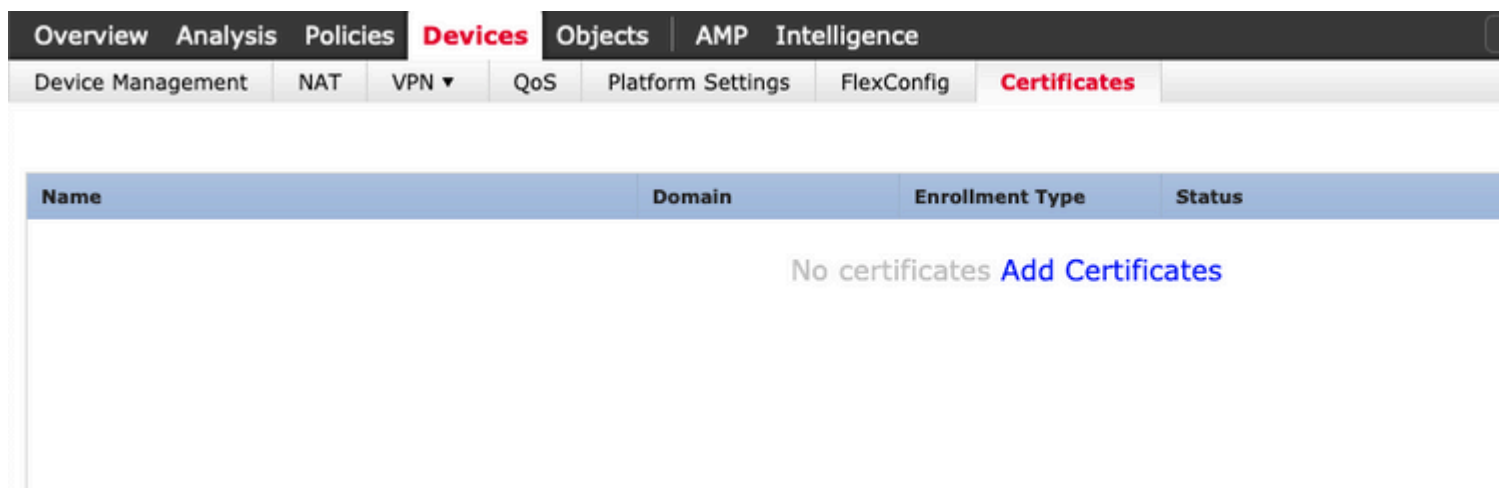
IP para evitar erros de "Certificado de servidor não confiável" em navegadores da Web.

Observação: em dispositivos FTD, o certificado da Autoridade de Certificação (CA) é necessário antes que a CSR (Solicitação de Assinatura de Certificado) seja gerada.

- Se o CSR for gerado em um servidor externo (como o Windows Server ou o OpenSSL), o **método de registro manual** falhará, pois o FTD não oferece suporte ao registro manual de chave.
- Um método diferente deve ser usado, como PKCS12.

Para obter um certificado para o dispositivo de FTD com o método de registro manual, é necessário gerar um CSR, assiná-lo com uma CA e importar o certificado de identidade.

1. Navegue até **Devices > Certificates** e selecione **Add** conforme mostrado na imagem.



2. Selecione o **Dispositivo** e adicione um novo objeto **Cert Enrollment** como mostrado na imagem.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates**

Name	Domain	Enrollment Type	Status
No certificates Add Certificates			

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*:

Add Cert Enrollment

Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

Enrollment URL:*

Challenge Password:

Confirm Password:

Retry Period: Minutes (Range 1-60)

Retry Count: (Range 0-100)

Fingerprint:

Allow Overrides

3. Selecione **Tipo de Inscrição** manual e cole o certificado CA (o certificado que deve assinar o CSR).

Add Cert Enrollment ? X

Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate: *

```

/3C4h07uzuR0ygywKEBaMdg4DI/z
4x3nk3tTUhyppmbWqWAXM7GNDRVWG9BZ1svk3shDK2Bogkzou6
RqV66G9IE7Z2
xiVsrJFqhrT795kMb8amBxhb4eXYXUjJmODTPqZ76RSTAT0+v1
VLSP+vHGm8X
g6wEFskuzay27a48e/IJG2LgRDrA0Kt+jwb57DGSK4mfZsZqhFdQP
LhBNFbyBVb9
dOJukmd5vzQDR5qSo+HINEm3E8/q20wrtIzP4MpAabyhr+hEpeP
VMYhIVBOT8h
H8eMJSQjGhhHkuKofVlzQmM0RvGnTB6EKYIvb4CUW8HcgDdDv
mwNgy5mTP9chla
9Or3RIWRzEa11HE3mHO4Rj6DOnmgujfx+TZRYczownSKLL7LcW1
D8ZcLYmfaIdC
W2CZuBR0yVdxCvq4f04ISEIBFOWFSd5rAD/bvk2n6xrJI1SLqABMJ
uslu9KTGH1
bIVKEYACKVYETw==
-----END CERTIFICATE-----

```

Allow Overrides

Save Cancel

4. Seleccione a guia **Parâmetros do Certificado** e seleccione "FQDN Personalizado" para o campo **Incluir FQDN** e preencha os detalhes do certificado conforme mostrado na imagem.

Add Cert Enrollment ? X

Name*

Description

CA Information **Certificate Parameters** Key Revocation

Include FQDN:

Include Device's IP Address:

Common Name (CN):

Organization Unit (OU):

Organization (O):

Locality (L):

State (ST):

Country Code (C):

Email (E):

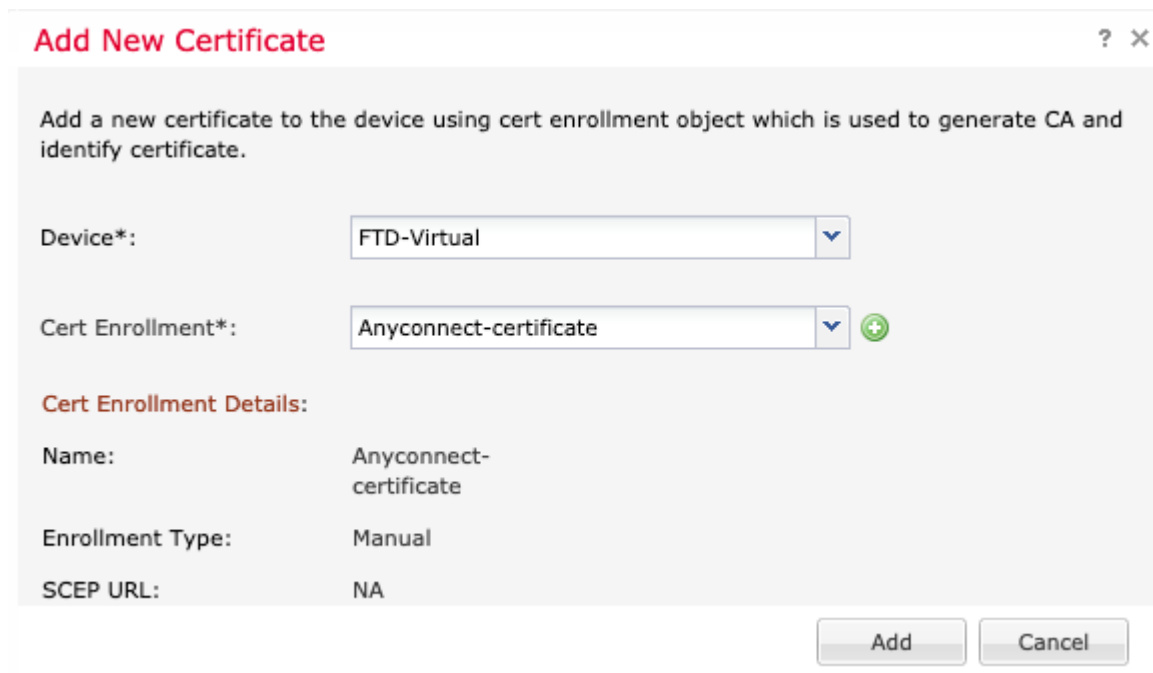
Include Device's Serial Number

Allow Overrides

Save Cancel

5. Selecione a guia **Chave** e selecione o tipo de chave, você pode escolher o nome e o tamanho. Para RSA, 2048 bytes é um requisito mínimo.

6. Selecione salvar, confirme o **dispositivo** e, em **Cert Enrollment**, selecione o ponto confiável que acabou de ser criado, selecione **Add** para implantar o certificado.



Add New Certificate ? X

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

Device*: FTD-Virtual

Cert Enrollment*: Anyconnect-certificate

Cert Enrollment Details:

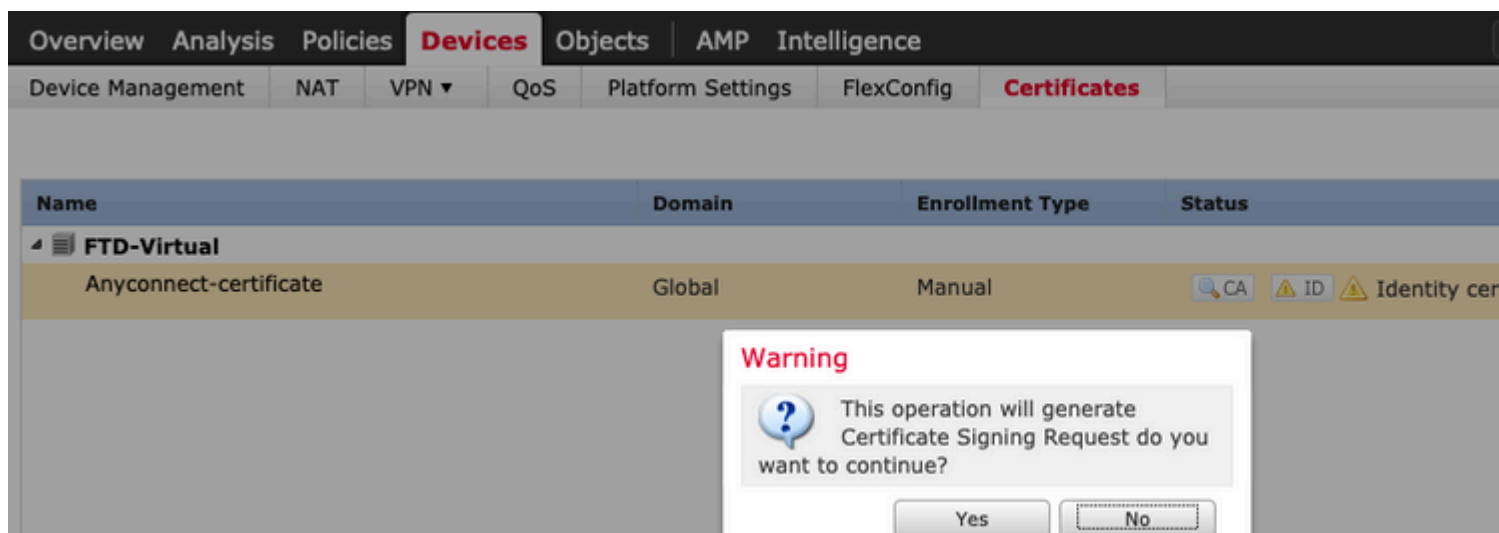
Name: Anyconnect-certificate

Enrollment Type: Manual

SCEP URL: NA

Add Cancel

7. Na coluna **Status**, selecione o ícone **ID** e selecione **Sim** para gerar o CSR como mostrado na imagem.



Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates**

Name	Domain	Enrollment Type	Status
FTD-Virtual			
Anyconnect-certificate	Global	Manual	CA ID Identity cer

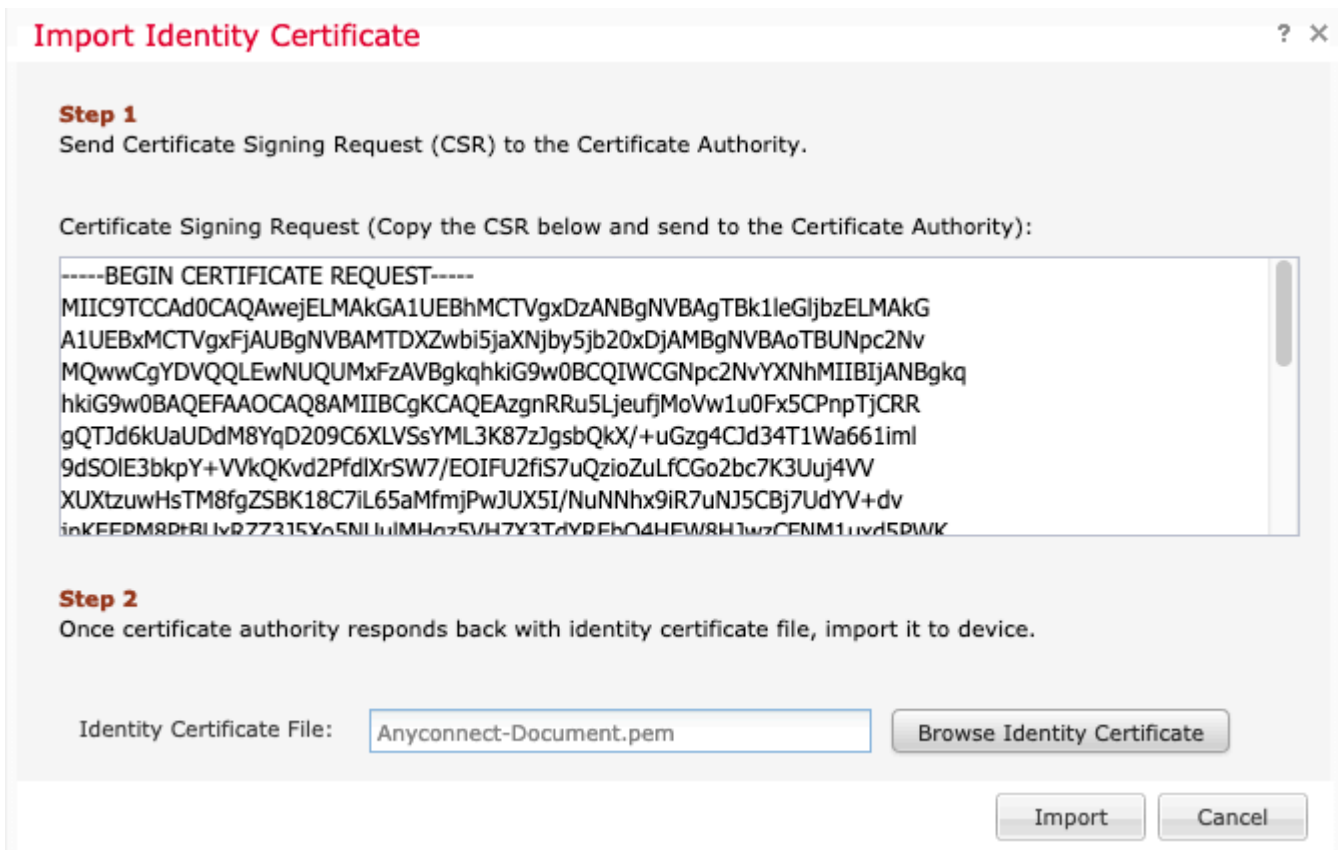
Warning

This operation will generate Certificate Signing Request do you want to continue?

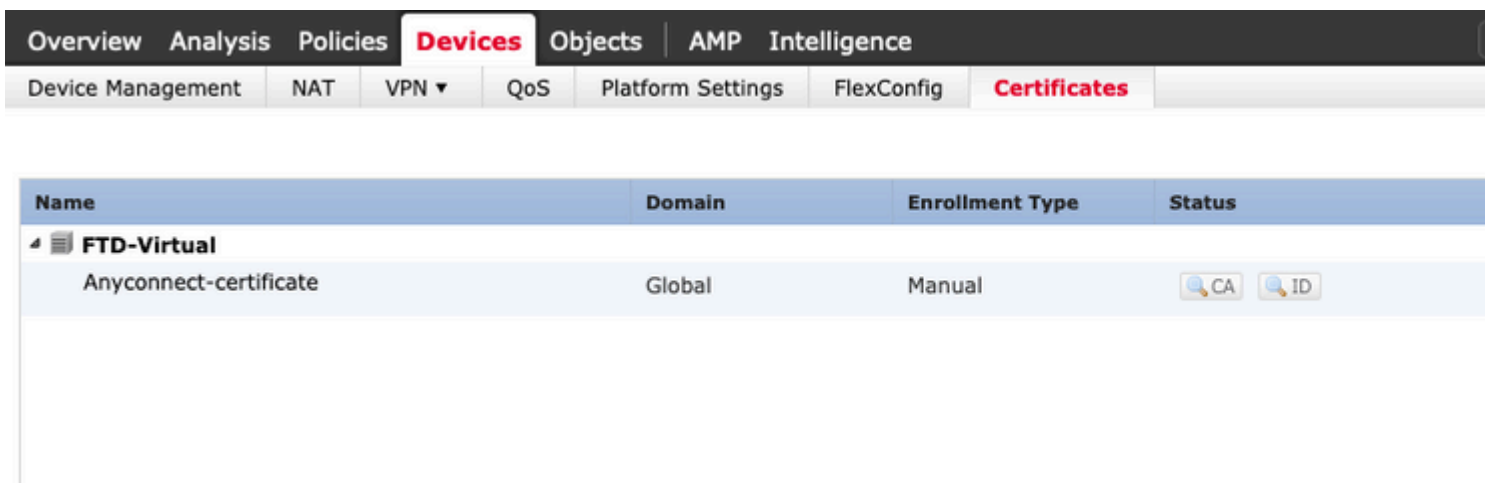
Yes No

8. Copie o CSR e assine-o com o CA de sua preferência (por exemplo, GoDaddy ou DigiCert).

9. Quando o certificado de identidade for recebido da CA (que deve estar no formato base64), selecione **Browse Identity Certificate** e localize o certificado no computador local. Selecione **Importar**.



10. Uma vez importados, os detalhes do certificado de CA e ID estarão disponíveis para exibição.



Etapa 2. Configurar um servidor RADIUS

Em dispositivos FTD gerenciados pelo FMC, o banco de dados de usuário local não é suportado, outro método de autenticação deve ser usado, como RADIUS ou LDAP.

1. Navegue até **Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group** conforme mostrado na imagem.

Add RADIUS Server Group



Name:*

Description:

Group Accounting Mode: ▼

Retry Interval:* (1-10) Seconds

Realms: ▼


Enable authorize only

Enable interim account update

Interval:* (1-120) hours

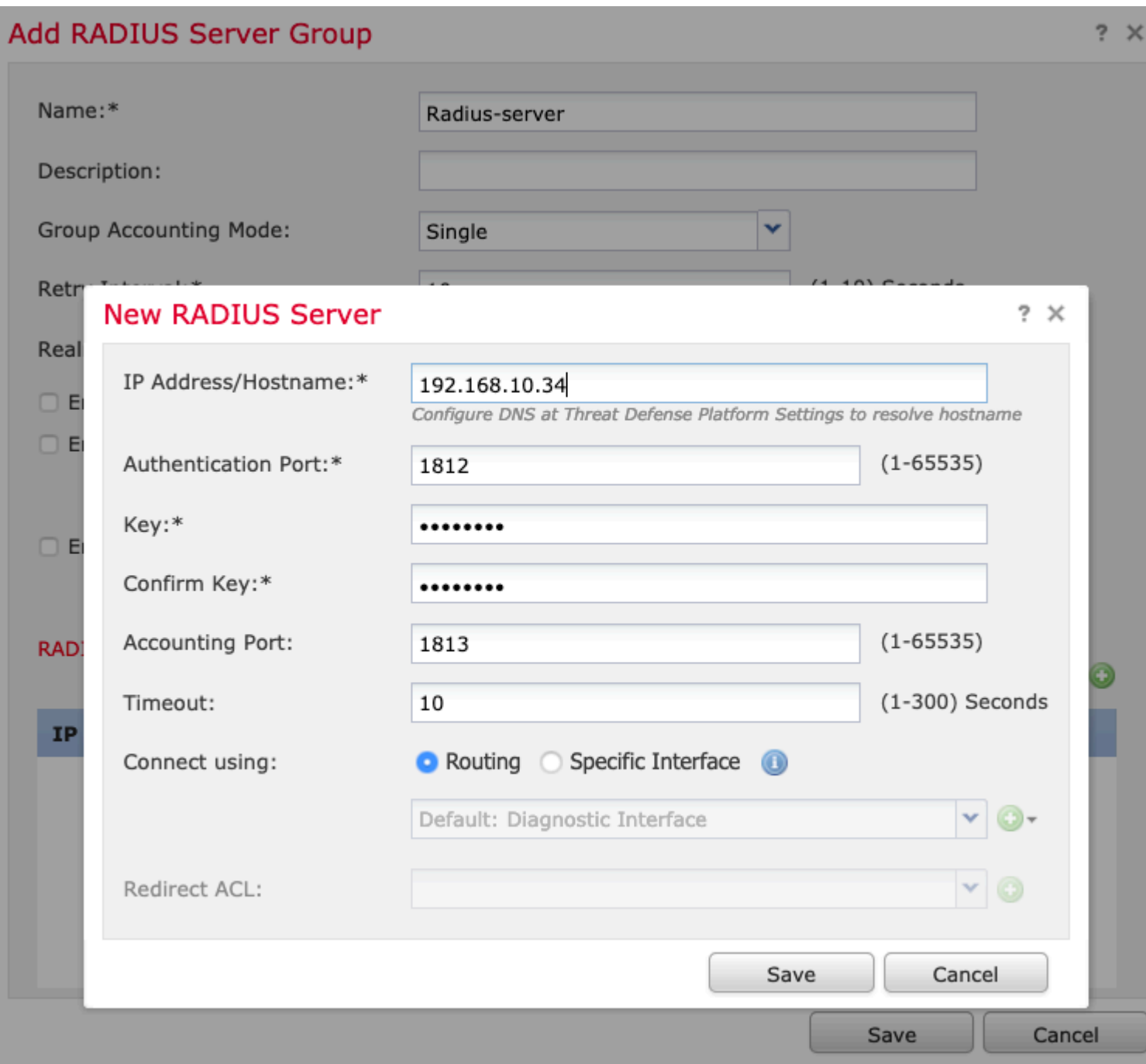
Enable dynamic authorization

Port:* (1024-65535)

RADIUS Servers (Maximum 16 servers) 

IP Address/Hostname
No records to display

2. Atribua um nome ao **Grupo de Servidores Radius** e adicione o endereço IP do servidor Radius juntamente com um segredo compartilhado (o segredo compartilhado é necessário para emparelhar o FTD com o servidor Radius), selecione **Salvar** depois que este formulário for preenchido, como mostrado na imagem.



3. As informações do servidor RADIUS estão agora disponíveis na lista Servidor Radius, conforme mostrado na imagem.

Add RADIUS Server Group



Name:*

Description:

Group Accounting Mode: ▼

Retry Interval:* (1-10) Seconds

Realms: ▼

Enable authorize only

Enable interim account update

Interval:* (1-120) hours

Enable dynamic authorization

Port:* (1024-65535)

RADIUS Servers (Maximum 16 servers)



IP Address/Hostname

192.168.10.34



Save

Cancel

Etapa 3. Criar um pool de IPs

1. Navegue até **Objects > Object Management > Address Pools > Add IPv4 Pools**.
2. Atribua o nome e o intervalo de endereços IP. O campo **Máscara** não é obrigatório, mas pode ser especificado conforme mostrado na imagem.

Add 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

Etapa 4. Criar um perfil XML

1. Baixe a ferramenta **Editor de perfis** de Cisco.com e execute o aplicativo.
2. No aplicativo Editor de perfis, navegue até **Lista de servidores** e selecione **Adicionar** como mostrado na imagem.

VPN

- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Server List

Hostname	Host Address	User Group	Backup Server List	SCEP

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

3. Atribua um **Display Name**, **Fully Qualified Domain Name (FQDN)** ou um **IP Address** e selecione **OK** como mostrado na imagem.

Server List Entry

Server Load Balancing Servers SCEP Mobile Certificate Pinning

Primary Server

Display Name (required) Corporate - FTD (SSL)

FQDN or IP Address User Group

vpn.cisco.com / ssl

Group URL

Connection Information

Primary Protocol SSL

ASA gateway

Auth Method During IKE Negotiation EAP-AnyConnect

IKE Identity (IOS gateway only)

Backup Servers

Host Address

Add

Move Up

Move Down

Delete

OK Cancel

4. A entrada agora está visível no menu **Lista de Servidores**:

VPN

- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Server List

Profile: Untitled

Hostname	Host Address	User Group	Backup Server ...	SCEP	Mobil
Corporate - FTD (SSL)	vpn.cisco.com	ssl	-- Inherited --		

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

Add... Edit...

5. Navegue até **Arquivo > Salvar como**.

Observação: salve o perfil com um nome facilmente identificável com uma extensão **.xml**.

Etapa 5. Carregar perfil XML do Anyconnect

1. No FMC, navegue até Objetos > **Gerenciamento de objetos** > **VPN** > Arquivo do AnyConnect > Adicionar arquivo do AnyConnect.

2. Atribua um **nome** ao objeto e clique em **Procurar**, localize o perfil do cliente no sistema local e selecione **Salvar**.

Cuidado: certifique-se de selecionar **Perfil de cliente do Anyconnect** como o tipo de arquivo.

Add AnyConnect File

Name:* Corporate-profile(SSL)

File Name:* FTD-corp-ssl.xml

File Type:* AnyConnect Client Profile

Description:

Etapa 6. Carregar imagens do AnyConnect

1. Faça download das imagens webdeploy (**.pkg**) da página da Web de downloads da Cisco.

AnyConnect Headend Deployment Package (Mac OS)	26-Jun-2019	51.22 MB	↓
anyconnect-macos-4.7.04056-webdeploy-k9.pkg			

2. Navegue até Objetos > **Gerenciamento de objetos** > **VPN** > Arquivo AnyConnect > Adicionar arquivo AnyConnect.

3. Atribua um nome ao arquivo de pacote do Anyconnect e selecione o arquivo **.pkg** no sistema local, depois que o arquivo for selecionado.

4. Selecione **Salvar**.

Add AnyConnect File ? X

Name:*

File Name:*

File Type:* ▼

Description:

Observação: pacotes adicionais podem ser carregados com base em seus requisitos (Windows, Mac, Linux).

Passo 7. Assistente de VPN de Acesso Remoto

Com base nas etapas anteriores, o Assistente de acesso remoto pode ser seguido de acordo.

1. Navegue até **Devices > VPN > Remote Access**.
2. Atribua o nome da política de Acesso Remoto e selecione um dispositivo FTD em **Dispositivos Disponíveis**.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

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:* TAC

Description:

VPN Protocols: SSL IPsec-IKEv2

Targeted Devices:

Available Devices

Search

FTD-Virtual

Selected Devices

FTD-Virtual

Add

Before You Start

Before you start, configuration elements to complete Remote Access VPN.

Authentication Server

Configure [Realm](#) or to authenticate VPN.

AnyConnect Client

Make sure you have for VPN Client download the relevant Cisco client during the wizard.

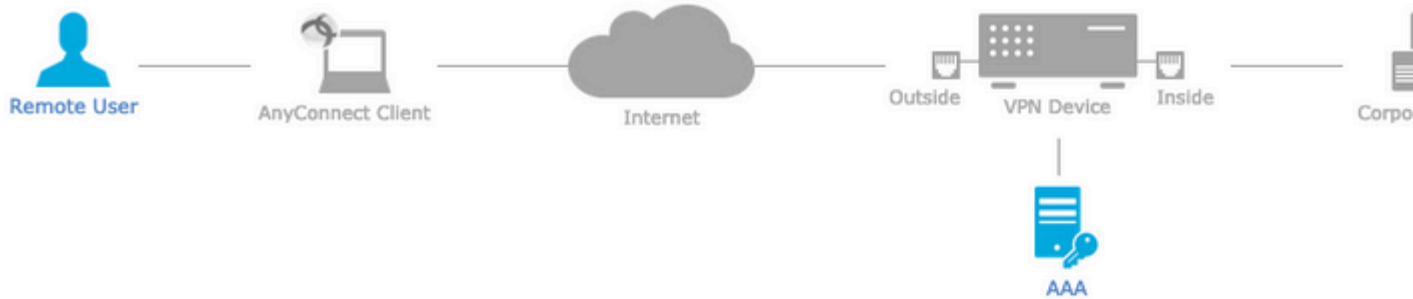
Device Interface

Interfaces should be targeted [devices](#) so as a security zone enable VPN access.

3. Atribua o **Nome do Perfil de Conexão** (o Nome do Perfil de Conexão é o nome do grupo de túneis), selecione **Servidor de Autenticação** e **Pools de Endereços** conforme mostrado na imagem.

Remote Access VPN Policy Wizard

- 1 Policy Assignment 2 **Connection Profile** 3 AnyConnect 4 Access & Certificate 5



Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how 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:

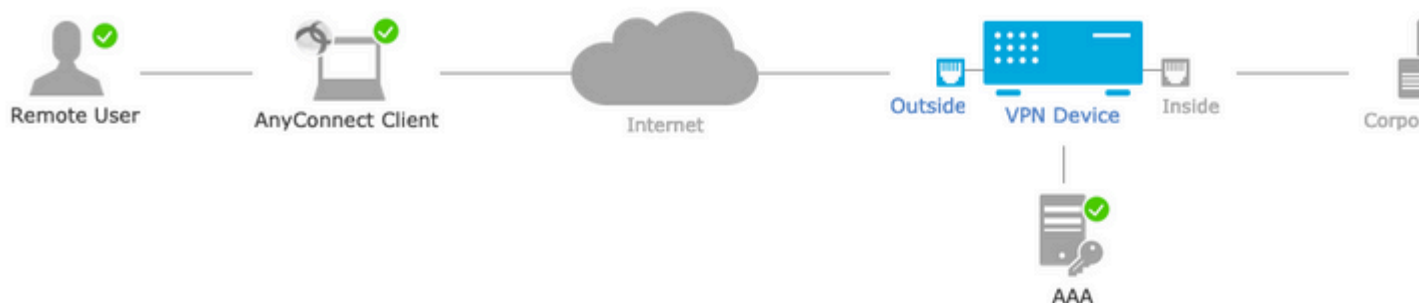
A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. or create a Group Policy object.

Group Policy:* ▼ +
[Edit Group Policy](#)

neste cenário, o FTD é configurado para não inspecionar nenhum tráfego VPN, ignorar a opção Access Control Policies (ACP) é alternado.

Remote Access VPN Policy Wizard

1 Policy Assignment > 2 Connection Profile > 3 AnyConnect > **4 Access & Certificate** > 5



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

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.

Back

Next

10. Seleccione **Finish** e **Deploy** as alterações:

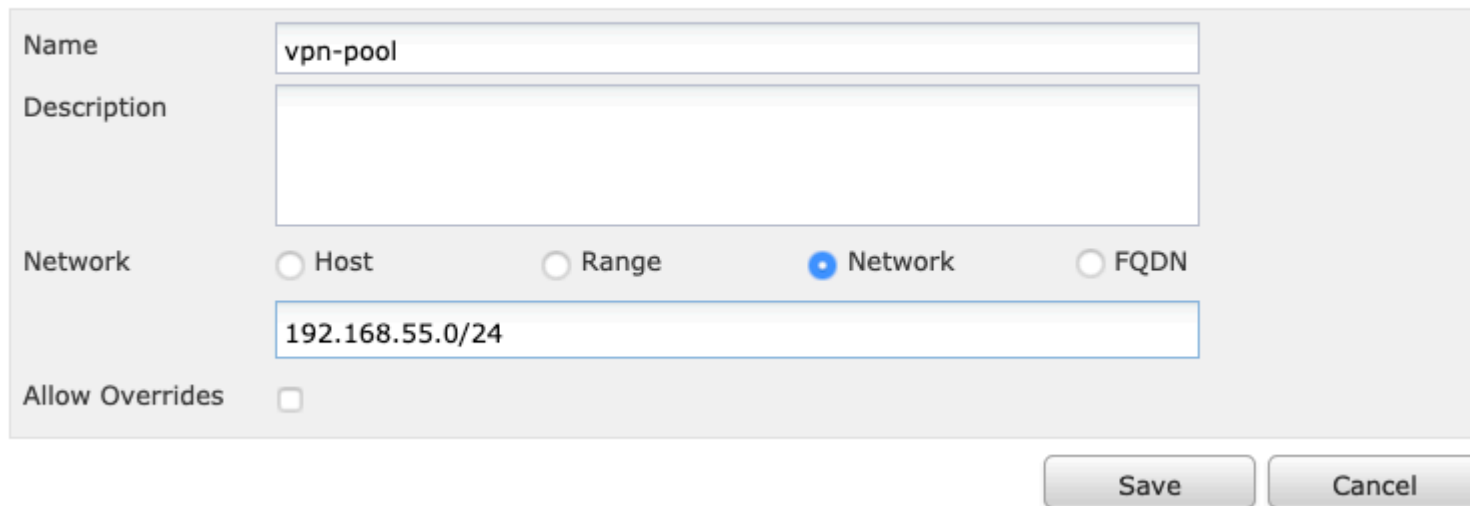
Toda a configuração relacionada a VPN, certificados SSL e pacotes do AnyConnect é enviada por mei

é um método de conversão preferido usado para evitar que o tráfego seja roteado para a Internet quando se pretende que flua por um túnel VPN (acesso remoto ou site a site).

Isso é necessário quando o tráfego da rede interna deve fluir pelos túneis sem nenhuma conversão.

1. Navegue até **Objetos > Rede > Adicionar Rede > Adicionar Objeto** conforme mostrado na imagem.

New Network Object



Name: vpn-pool

Description:

Network: Host Range Network FQDN

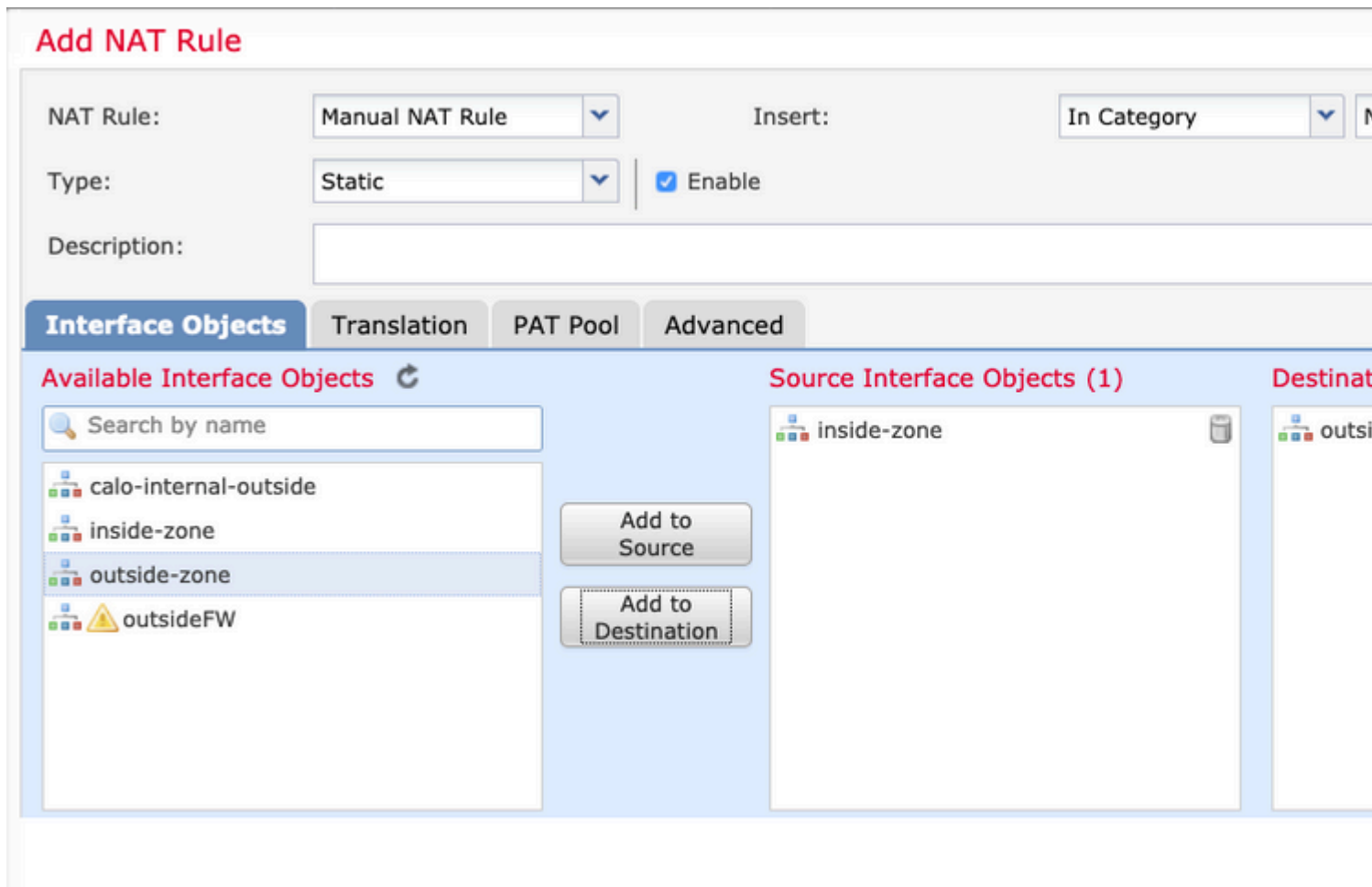
192.168.55.0/24

Allow Overrides:

Save Cancel

2. Navegue até **Device > NAT**, selecione a política NAT que é usada pelo dispositivo em questão e crie uma nova instrução.

Observação: o fluxo de tráfego vai de dentro para fora.



3. Selecione os recursos internos atrás do FTD (**origem original** e **origem convertida**) e o destino como o pool local ip para os usuários do Anyconnect (**destino original** e **destino convertido**), conforme mostrado na imagem.

Add NAT Rule

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects **Translation** PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* <input type="text" value="FTDv-Inside-SUPERNE"/>	Translated Source: <input type="text" value="Address"/>
Original Destination: <input type="text" value="Address"/> <input type="text" value="vpn-pool"/>	Translated Destination: <input type="text" value="vpn-po"/>
Original Source Port: <input type="text"/>	Translated Source Port: <input type="text"/>
Original Destination Port: <input type="text"/>	Translated Destination Port: <input type="text"/>

4. Certifique-se de alternar as opções (conforme mostrado na imagem), para habilitar **"no-proxy-arp"** e **"route-lookup"** na regra NAT, selecione **OK** como mostrado na imagem.

Edit NAT Rule

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

- Translate DNS replies that match this rule
- Fallthrough to Interface PAT(Destination Interface)
- IPv6
- Net to Net Mapping
- Do not proxy ARP on Destination Interface
- Perform Route Lookup for Destination Interface
- Unidirectional

5. Este é o resultado da configuração de isenção de NAT.

1 Static inside-zone outside-zone FTDv-Inside-SUPERNE vpn-pool FTDv-Inside-SUPERNE vpn-pool

Os objetos usados na seção anterior são os descritos abaixo.

Name

Description

Network Host Range Network

Allow Overrides

Name	<input type="text" value="vpn-pool"/>
Description	<input type="text"/>
Network	<input type="radio"/> Host <input type="radio"/> Range <input checked="" type="radio"/> Network <input type="radio"/>
	<input type="text" value="192.168.55.0/24"/>
Allow Overrides	<input type="checkbox"/>

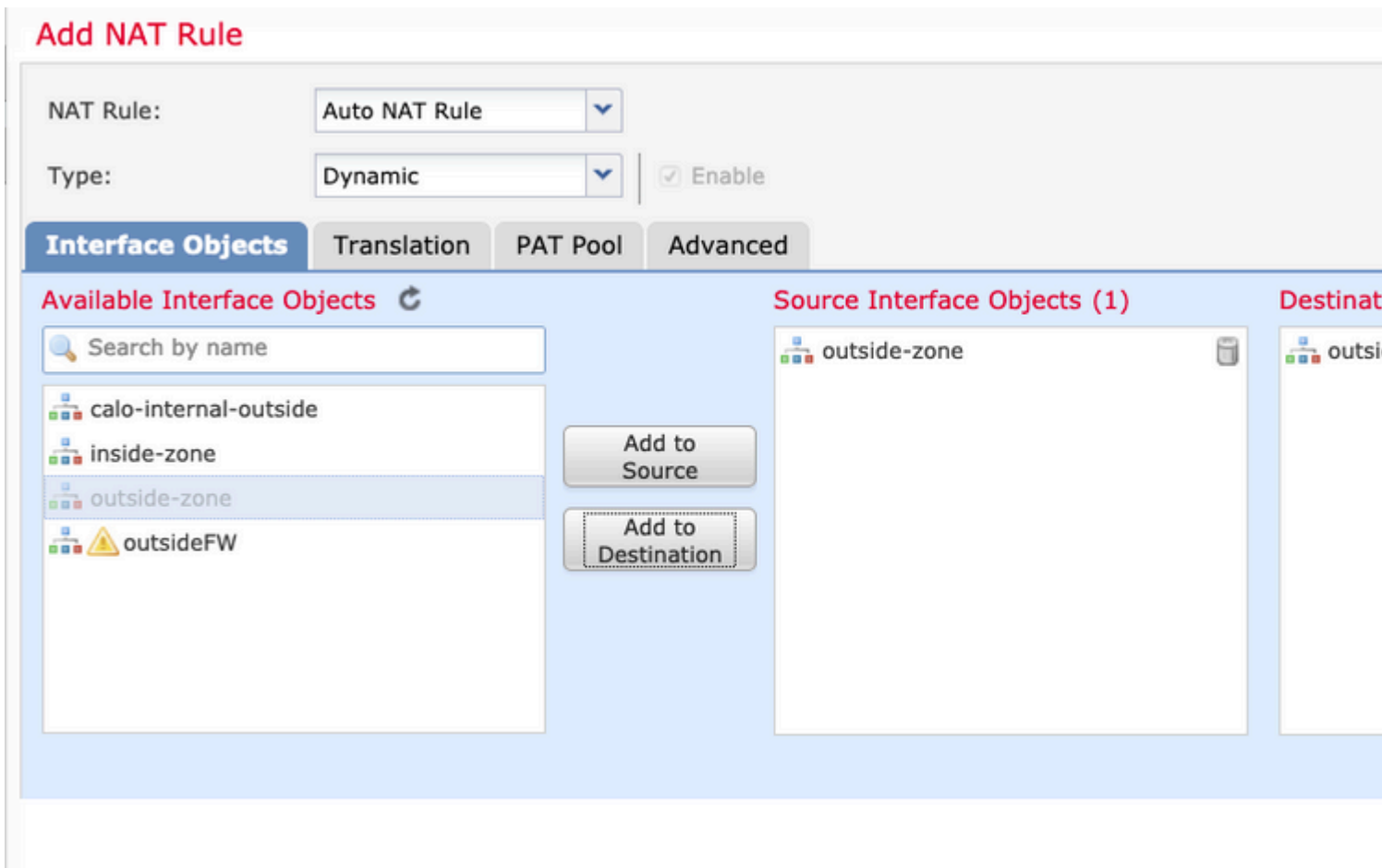
Etapa 2. Configuração Hairpin

Também conhecido como **U-turn**, esse é um método de conversão que permite que o tráfego flua pela mesma interface em que o tráfego é recebido.

Por exemplo, quando o Anyconnect é configurado com uma política **Full tunnel** split-tunnel, os recursos internos são acessados de acordo com a política de Isenção de NAT. Se o tráfego do cliente Anyconnect tiver a intenção de alcançar um site externo na Internet, o hairpin NAT (ou U-turn) é responsável por rotear o tráfego de fora para fora.

Um objeto de pool de VPN deve ser criado antes da configuração de NAT.

1. Crie uma nova instrução NAT, selecione **Auto NAT Rule** no campo **NAT Rule** e selecione **Dynamic** como o **NAT Type**.
2. Selecione a mesma interface para os objetos de interface de **origem** e de destino (externo):



3. Na guia Tradução, selecione como a **Origem Original** o objeto vpn-pool e selecione **IP da Interface de Destino** como a Origem Traduzida, selecione OK como mostrado na imagem.

Add NAT Rule

NAT Rule: ▼

Type: ▼ Enable

Interface Objects **Translation** PAT Pool Advanced

Original Packet

Original Source:* ▼ +

Original Port: ▼

Translated Packet

Translated Source: ▼ i The va Object

Translated Port:

4. Este é o resumo da configuração do NAT como mostrado na imagem.

Rules									
Filter by Device Filter Rules									
#	Direction	Type	Source Interface Obje...	Destination Interface Obje...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destination
▼ NAT Rules Before									
1	↔	Static	inside-zone	outside-zone	FTDv-Inside-SUPERNE	vpn-pool		FTDv-Inside-SUPERNE	vpn-pool
▼ Auto NAT Rules									
#	→	Dyna...	outside-zone	outside-zone	vpn-pool			Interface	
▼ NAT Rules After									

5. Clique em **Salvar** e **Implantar** as alterações.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Execute esses comandos na linha de comando do FTD.

- **sh crypto ca certificates**
- **show running-config ip local pool**
- **show running-config webvpn**
- **show running-config tunnel-group**

- **show running-config group-policy**
- **show running-config ssl**
- **show running-config nat**

Troubleshooting

No momento, não há informações específicas de solução de problemas disponíveis para esta configuração.</>

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.