

Configuración de AnyConnect VPN Client en FTD: exención de horquilla y NAT

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Paso 1. Importar un certificado SSL](#)

[Paso 2. Configuración de un servidor RADIUS](#)

[Paso 3. Creación de un pool IP](#)

[Paso 4. Crear un perfil XML](#)

[Paso 5. Cargar perfil XML de Anyconnect](#)

[Paso 6. Cargar imágenes de AnyConnect](#)

[Paso 7. Asistente para VPN de acceso remoto](#)

[Exención de NAT y horquilla](#)

[Paso 1. Configuración de exención de NAT](#)

[Paso 2. Configuración Hairpin](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar la solución VPN de acceso remoto de Cisco (AnyConnect) en Firepower Threat Defence (FTD), v6.3, gestionada por FMC.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de VPN de acceso remoto, capa de conexión segura (SSL) e intercambio de claves de Internet versión 2 (IKEv2)
- Conocimiento básico de autenticación, autorización y contabilidad (AAA) y RADIUS
- Conocimientos básicos de FMC
- Conocimientos básicos de FTD

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

Este documento describe el procedimiento para configurar la solución VPN de acceso remoto de Cisco (AnyConnect) en Firepower Threat Defence (FTD), versión 6.3, gestionada por Firepower Management Center (FMC).

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 está pensado para cubrir la configuración en los dispositivos FTD. Si busca el ejemplo de configuración de ASA, consulte el documento: <https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html>

Limitaciones:

Actualmente, estas funciones no son compatibles con FTD, pero siguen estando disponibles en los dispositivos ASA:

- Autenticación AAA doble (disponible en la versión 6.5 del FTD)
- Política de acceso dinámica
- Análisis de host
- postura de ISE
- RADIUS CoA
- balanceador de carga VPN
- Autenticación local (disponible en Firepower Device Manager 6.3. ID de bug de Cisco [CSCvf92680](#))
- Mapa de atributos LDAP (disponible a través de FlexConfig, ID de error de Cisco [CSCvd64585](#))
- Personalización de AnyConnect
- Scripts de AnyConnect
- localización de AnyConnect
- VPN por aplicación
- proxy SCEP
- Integración de WSA
- SSO SAML (Id. de error de Cisco [CSCvq90789](#))
- Mapa criptográfico dinámico IKEv2 simultáneo para VPN RA y L2L
- Módulos de AnyConnect (NAM, Hostscan, AMP Enabler, SBL, Umbrella, Web Security, etc.). DART es el único módulo instalado de forma predeterminada en esta versión.
- TACACS, Kerberos (autenticación KCD y RSA SDI)
- Proxy de explorador

Configurar

Para acceder al asistente para VPN de acceso remoto en el FMC, se deben completar estos pasos:

Paso 1. Importar un certificado SSL

Los certificados son esenciales al configurar AnyConnect. Sólo se admiten certificados basados en RSA para SSL e IPsec.

Los certificados de algoritmo de firma digital de curva elíptica (ECDSA) son compatibles con IPsec; sin embargo, no es posible implementar un nuevo paquete o perfil XML de AnyConnect cuando se utiliza un certificado basado en ECDSA.

Se puede utilizar para IPsec, pero debe implementar previamente los paquetes de AnyConnect junto con el perfil XML. Todas las actualizaciones del perfil XML deben enviarse manualmente en cada cliente (Id. de error de Cisco [CSCtx42595](#)).

Además, el certificado debe contener una extensión de nombre común (CN) con nombre DNS o dirección IP

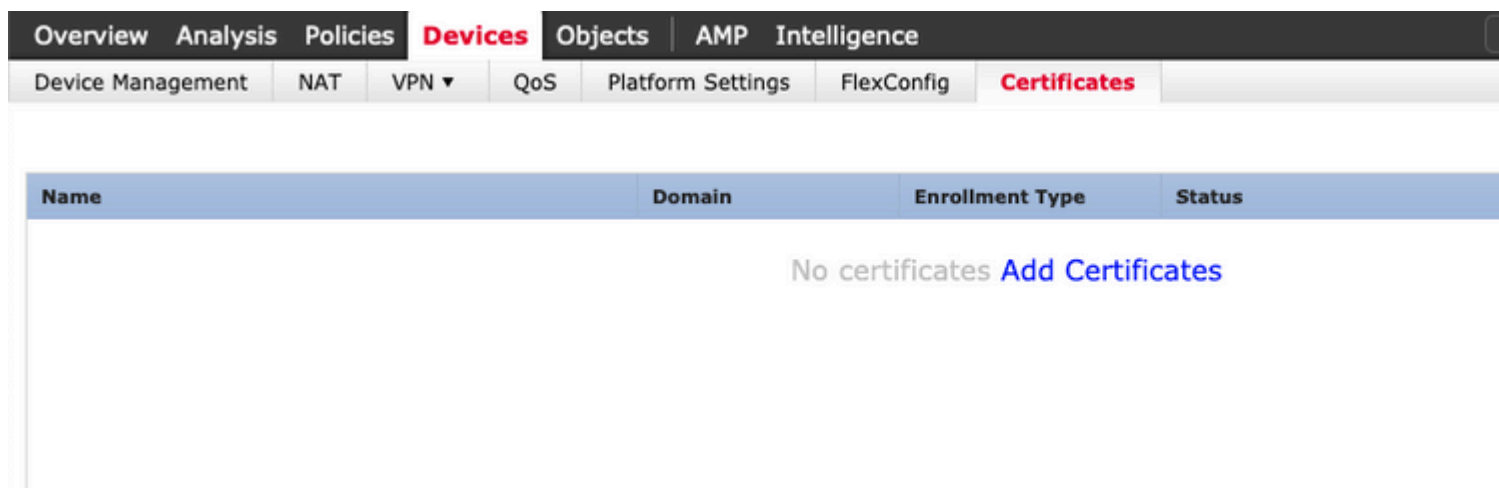
para evitar errores de "certificado de servidor no fiable" en los navegadores web.

Nota: en los dispositivos FTD, se necesita el certificado de la autoridad certificadora (CA) antes de generar la solicitud de firma de certificado (CSR).

- Si el CSR se genera en un servidor externo (como Windows Server o OpenSSL), el **método de inscripción manual** está destinado a fallar, ya que FTD no admite la inscripción manual de claves.
- Se debe utilizar un método diferente, como PKCS12.

Para obtener un certificado para el dispositivo FTD con el método de inscripción manual, debe generarse un CSR, firmarlo con una CA y, a continuación, importar el certificado de identidad.

1. Navegue hasta **Dispositivos > Certificados** y seleccione **Agregar** como se muestra en la imagen.



2. Seleccione el **Dispositivo** y agregue un nuevo objeto **Inscripción de Certificados** como se muestra en la imagen.

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. Seleccione el **tipo de inscripción** manual y pegue el certificado de CA (el certificado que está destinado a firmar el CSR).

Add Cert Enrollment ? X

Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate: *

```

/3C4h07uzuRDyggwKEBaMdg4DI/z
4x3nk3tTUhyppmbWqWAXM7GNDRVWG9BZ1svk3shDK2Bogkzou6
RqV66G9IE7Z2
xiVrSrJFqhrT795kMb8amBxhb4eXYXUjJmODtPqZ76RSTAT0+v1
VLSP+vHGm8X
g6wEFsKuZay27a48e/IJG2LgRDrA0Kt+jwb57DGSK4mfZsZqhFdQP
LhBNFbyBVb9
dOJukmd5vzQDR5qSo+HINEm3E8/q20wrtIzP4MpAabyhr+hEpeP
VMYhIVBOT8h
H8eMJSQjGhhHkuKofVlzQmM0RvGnTB6EKYIvb4CUW8HcgDdDv
mwNgy5mTP9chla
9Or3RIWRzEa11HE3mHO4Rj6DOnmgujfx+TZRYczownSKLL7LcW1
D8ZcLYmfaIdC
W2CZuBR0yVDxvCq4f04ISEIBFOWFSd5rAD/bvk2n6xrJI1SLqABMJ
uslu9KTGH1
bIVKEYACKVYETw==
-----END CERTIFICATE-----

```

Allow Overrides

Save Cancel

4. Seleccione la pestaña **Parámetros de certificado** y seleccione "FQDN personalizado" para el campo **Incluir FQDN** y rellene los detalles del certificado como se muestra en la imagen.

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):

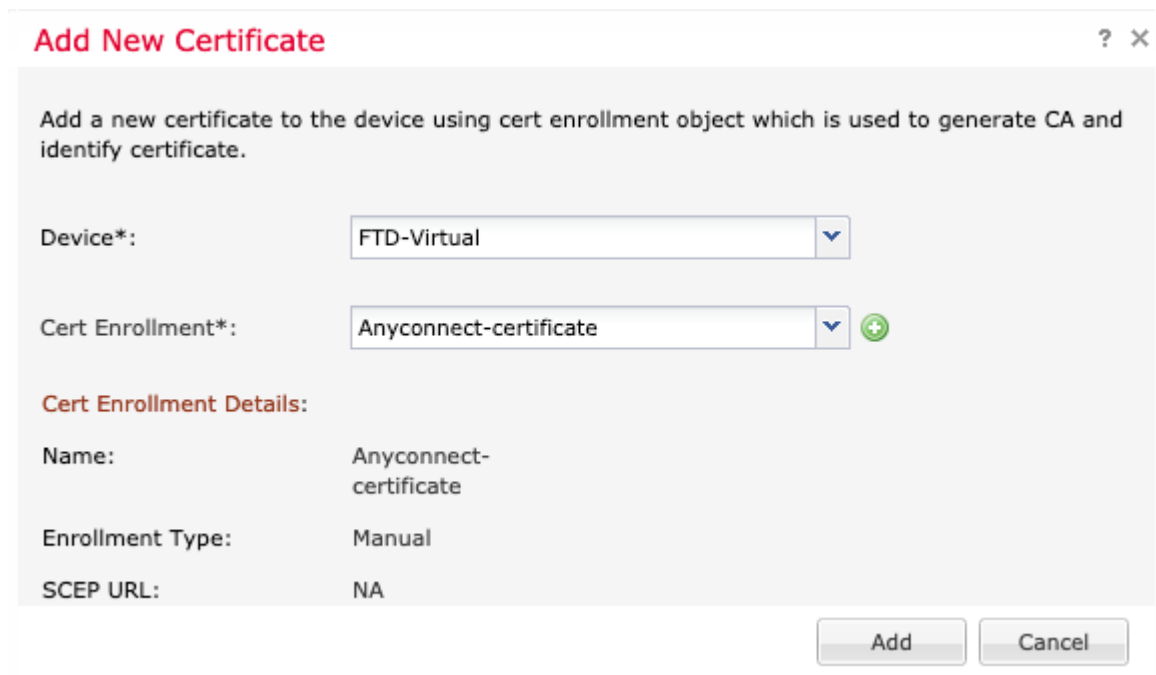
Include Device's Serial Number

Allow Overrides

Save Cancel

5. Seleccione la pestaña **Clave** y seleccione el tipo de clave; puede seleccionar el nombre y el tamaño. Para RSA, 2048 bytes es un requisito mínimo.

6. Seleccione guardar, confirme el **dispositivo** y, en **Inscripción de Certificados**, seleccione el punto de confianza que se acaba de crear y, a continuación, seleccione **Agregar** para implementar el 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:

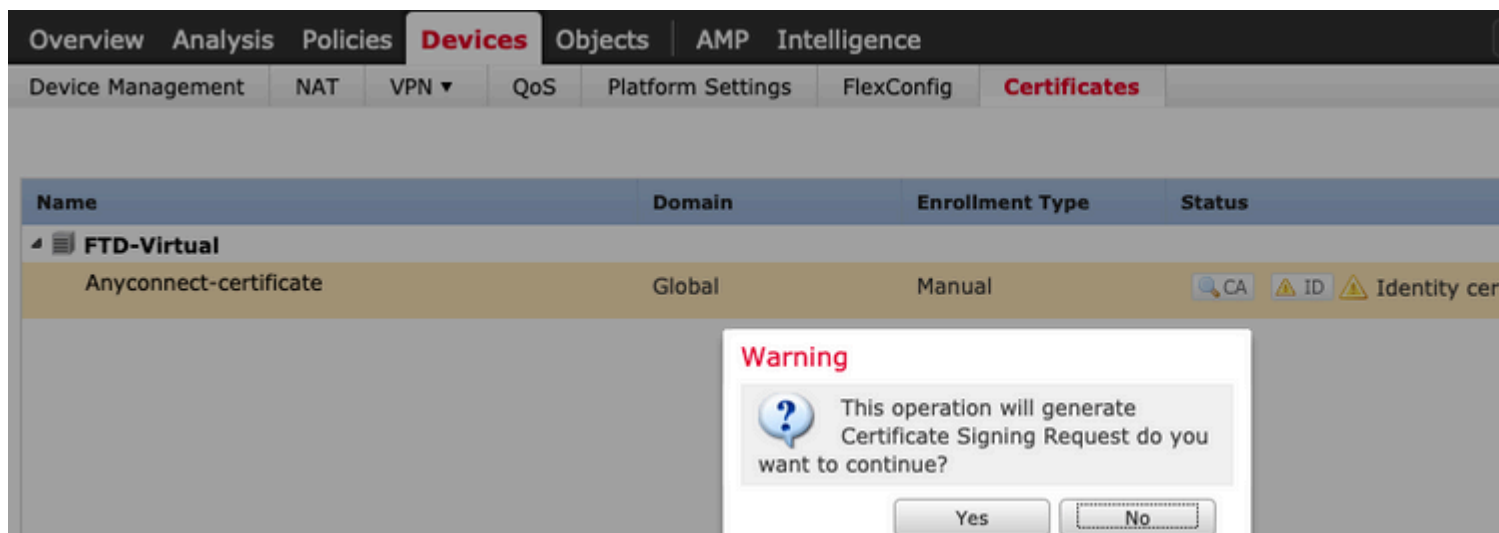
Name: Anyconnect-certificate

Enrollment Type: Manual

SCEP URL: NA

Add Cancel

7. En la columna **Estado**, seleccione el icono **ID** y seleccione **Sí** para generar el CSR como se muestra en la imagen.



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

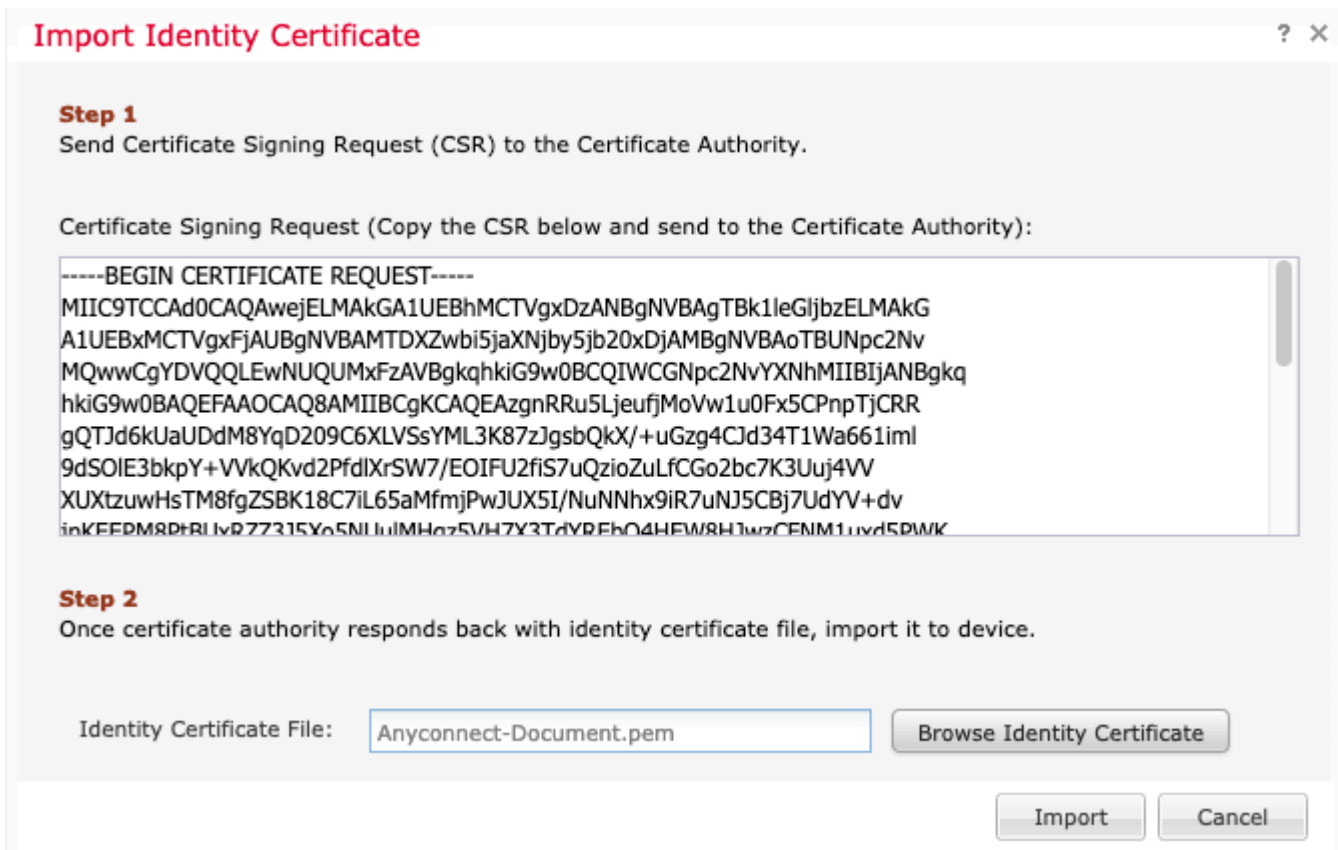
Warning

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

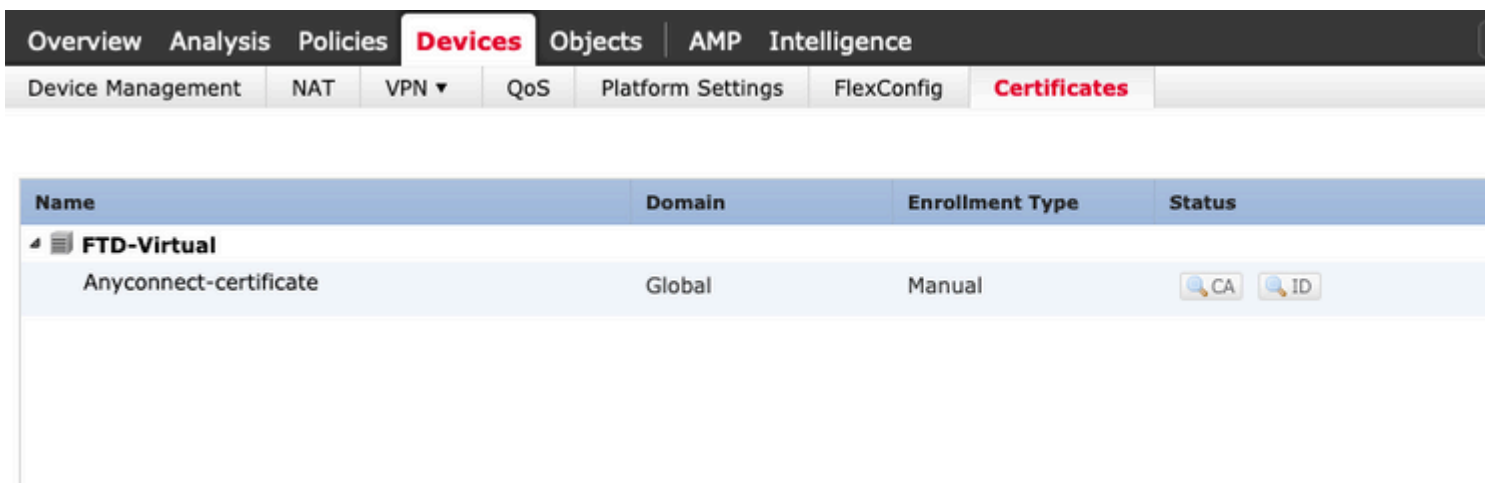
Yes No

8. Copie CSR y fírmela con su CA preferida (por ejemplo, GoDaddy o DigiCert).

9. Una vez recibido el certificado de identidad de la CA (que debe estar en formato base64), seleccione **Examinar certificado de identidad** y localice el certificado en el equipo local. Seleccione **Importar**.



10. Una vez importados, los detalles del certificado de CA e ID estarán disponibles para su visualización.



Paso 2. Configuración de un servidor RADIUS

En los dispositivos FTD gestionados por FMC, la base de datos de usuario local no es compatible. Se debe utilizar otro método de autenticación, como RADIUS o LDAP.

1. Navegue hasta **Objetos > Administración de Objetos > Grupo de Servidores RADIUS > Agregar Grupo de Servidores RADIUS** como se muestra en la imagen.

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

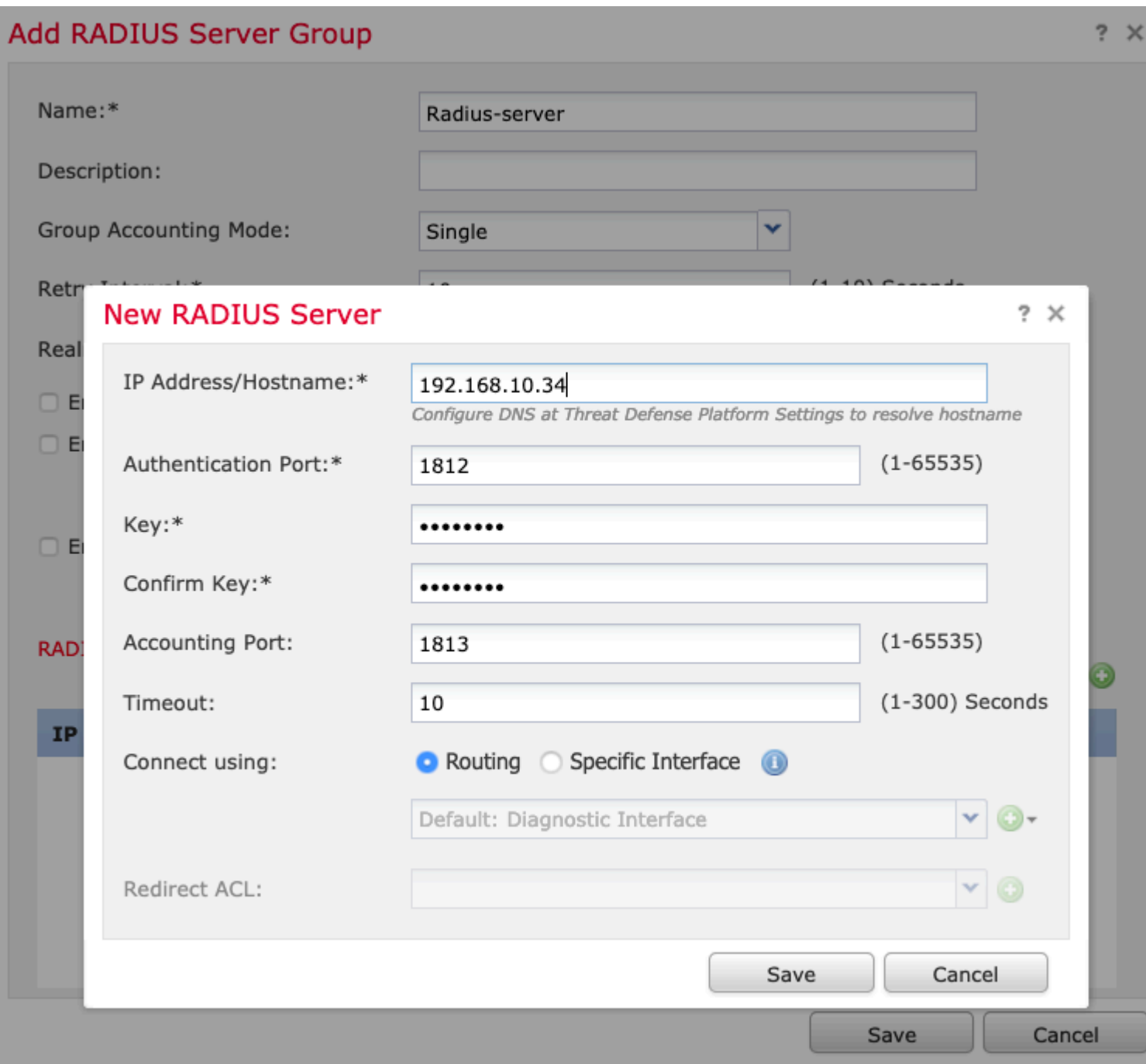
Enable dynamic authorization

Port:* (1024-65535)

RADIUS Servers (Maximum 16 servers) 

IP Address/Hostname
No records to display

2. Asigne un nombre al **grupo de servidores Radius** y agregue la dirección IP del servidor Radius junto con un secreto compartido (el secreto compartido es necesario para emparejar el FTD con el servidor Radius), seleccione **Guardar** una vez que se complete este formulario como se muestra en la imagen.



3. La información del servidor RADIUS ahora está disponible en la lista del servidor RADIUS como se muestra en la imagen.

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

Paso 3. Creación de un pool IP

1. Vaya a **Objetos > Gestión de Objetos > Pools de Direcciones > Agregar Pools IPv4**.
2. Asigne el nombre y el rango de direcciones IP, el campo **Máscara** no es necesario, pero se puede especificar como se muestra en la imagen.

Add IPv4 Pool

Name*

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

Mask

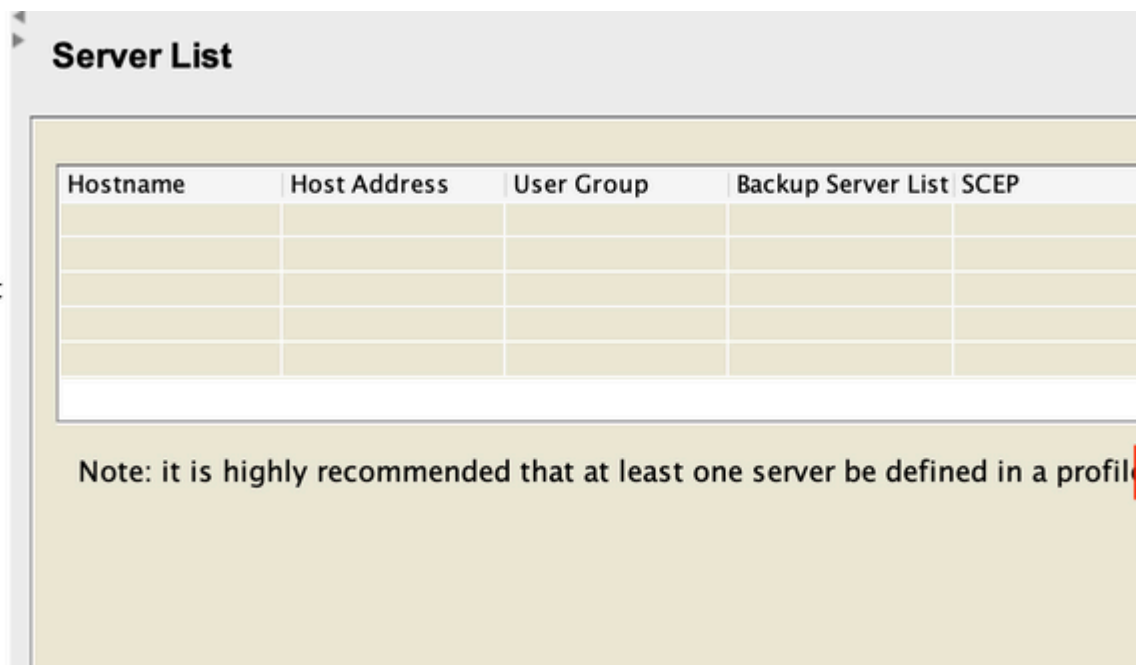
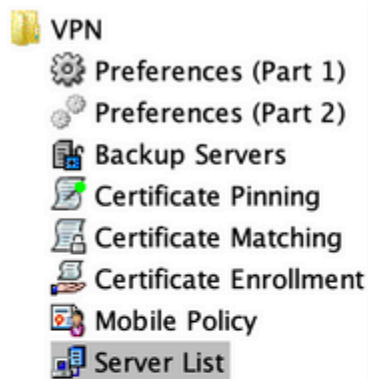
Description

Allow Overrides

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

Paso 4. Crear un perfil XML

1. Descargue la herramienta **Profile Editor** desde Cisco.com y ejecute la aplicación.
2. En la aplicación Profile Editor, navegue hasta **Server List** y seleccione **Add** como se muestra en la imagen.



3. Asigne un **nombre para mostrar**, un **nombre de dominio completo (FQDN)** o una **dirección IP** y seleccione **Aceptar** como se muestra en la imagen.

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. La entrada ahora está visible en el menú **Server List**:

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 hasta **Archivo > Guardar como**.

Nota: Guarde el perfil con un nombre fácilmente identificable con una extensión **.xml**.

Paso 5. Cargar perfil XML de Anyconnect

1. En el FMC, navegue hasta Objetos > **Administración de objetos** > **VPN** > **Archivo AnyConnect** > Agregar archivo AnyConnect.
2. Asigne un **nombre** al objeto y haga clic en **Examinar**, busque el perfil de cliente en el sistema local y seleccione **Guardar**.

Precaución: asegúrese de seleccionar **Perfil del cliente de Anyconnect** como tipo de archivo.

Add AnyConnect File

Name:* Corporate-profile(SSL)

File Name:* FTD-corp-ssl.xml

File Type:* AnyConnect Client Profile

Description:

Paso 6. Cargar imágenes de AnyConnect

1. Descargue las imágenes webdeploy (**.pkg**) desde la página web de descargas de Cisco.

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

2. Vaya a Objetos > **Administración de objetos** > **VPN** > **Archivo AnyConnect** > Agregar archivo AnyConnect.
3. Asigne un nombre al archivo de paquete Anyconnect y seleccione el archivo **.pkg** del sistema local, una vez seleccionado el archivo.
4. Seleccione **Guardar**.

Add AnyConnect File ? X

Name:*

File Name:*

File Type:* ▼

Description:

Nota: Se pueden cargar paquetes adicionales en función de sus requisitos (Windows, Mac, Linux).

Paso 7. Asistente para VPN de acceso remoto

En función de los pasos anteriores, se puede seguir el asistente de acceso remoto según corresponda.

1. Navegue hasta **Dispositivos > VPN > Acceso remoto**.
2. Asigne el nombre de la directiva de acceso remoto y seleccione un dispositivo FTD de **Dispositivos disponibles**.

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

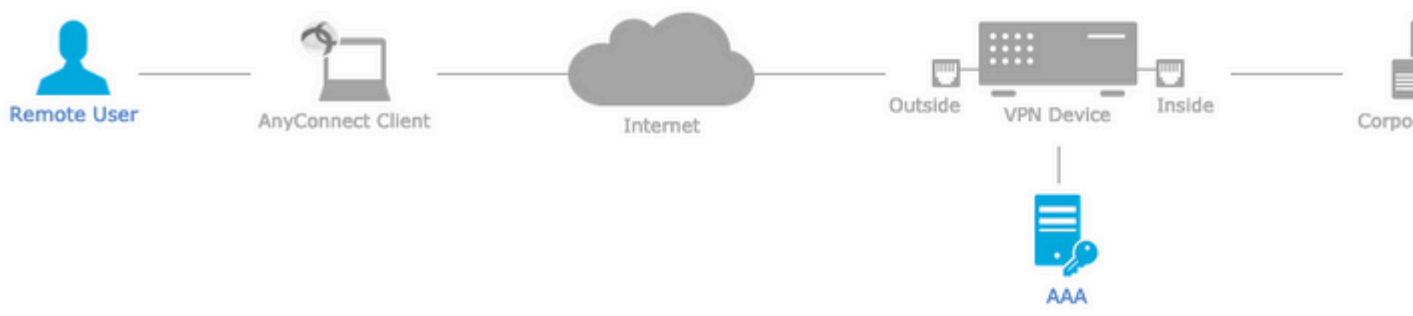
Make sure you have for VPN Client download the relevant Cisco client during the wizard.

Device Interface

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

3. Asigne el **Nombre del Perfil de Conexión** (el Nombre del Perfil de Conexión es el nombre del grupo de túnel), seleccione **Servidor de Autenticación** y **Pools de Direcciones** como se muestra en la imagen.

Remote Access VPN Policy Wizard



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) ⓘ

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.

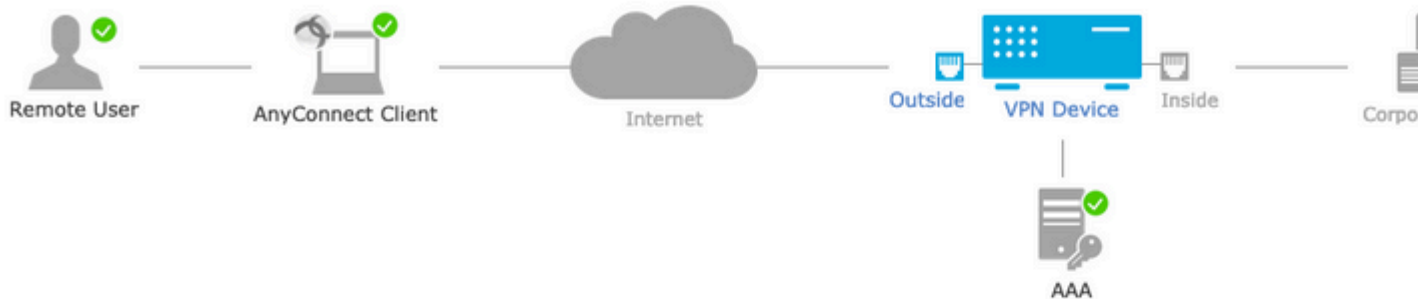
Group Policy:* ▾ +
[Edit Group Policy](#)

4. Seleccione el símbolo + para crear la **política de grupo**.

En este escenario, el FTD se configura para no inspeccionar ningún tráfico VPN, omitir la opción de políticas de control de acceso (ACP) se alterna.

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 **Finalizar** e **Implementar** los cambios:

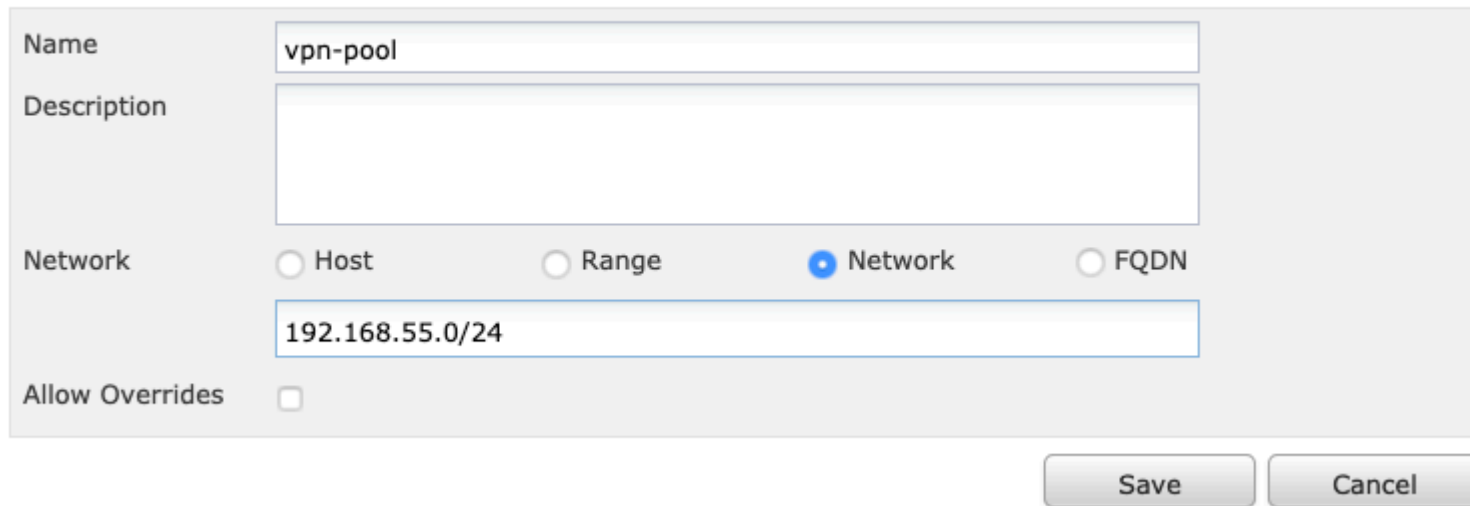
Toda la configuración relacionada con VPN, certificados SSL y paquetes AnyConnect se envía a través

es un método de traducción preferido que se utiliza para evitar que el tráfico se enrute a Internet cuando se pretende que fluya a través de un túnel VPN (acceso remoto o sitio a sitio).

Esto es necesario cuando el tráfico de su red interna está destinado a fluir a través de los túneles sin ninguna traducción.

1. Navegue hasta **Objetos > Red > Agregar red > Agregar objeto** como se muestra en la imagen.

New Network Object



Name

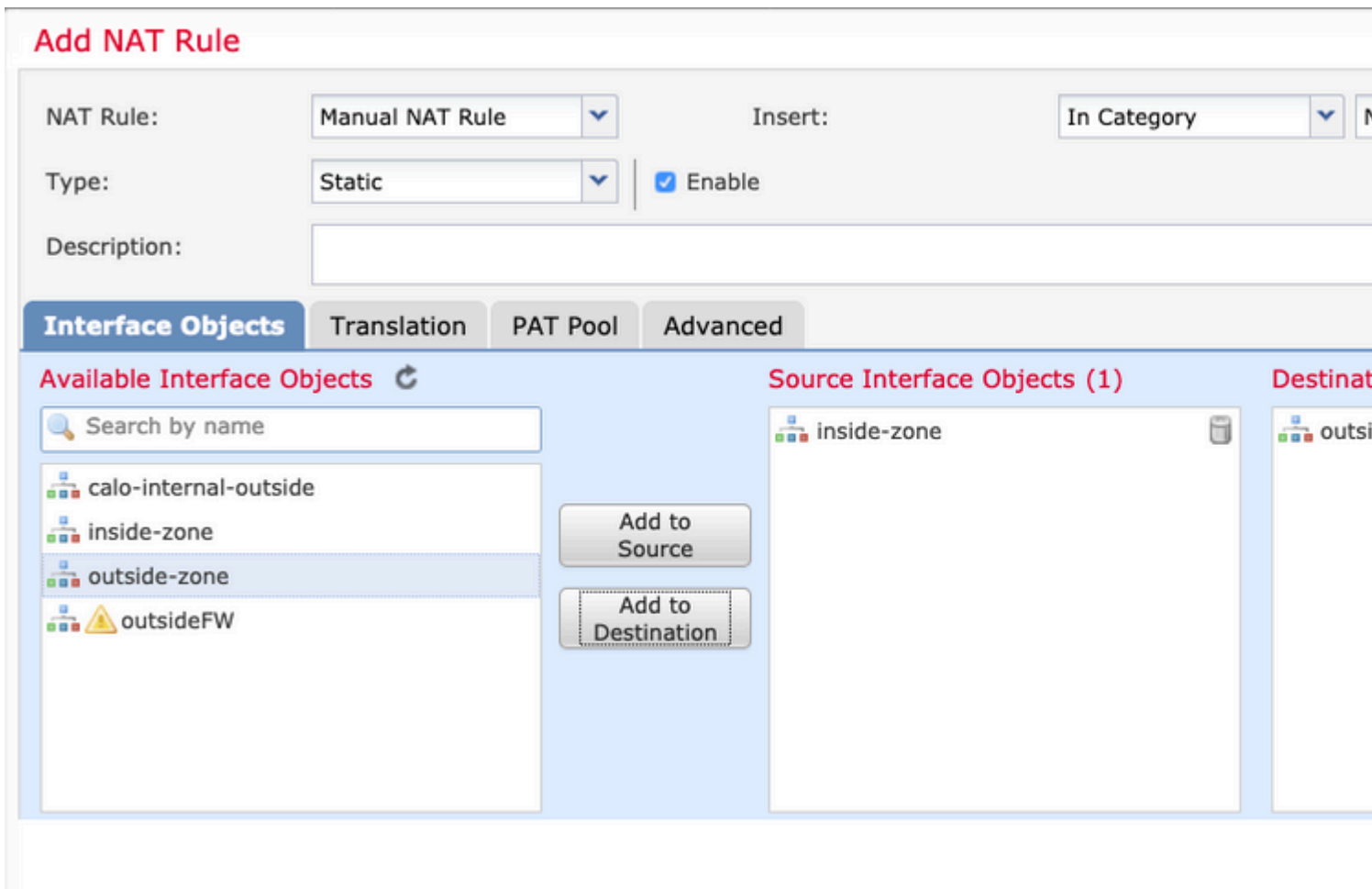
Description

Network Host Range Network FQDN

Allow Overrides

2. Vaya a **Device > NAT**, seleccione la política NAT que utiliza el dispositivo en cuestión y cree una nueva sentencia.

Nota: El flujo de tráfico va de adentro hacia afuera.



3. Seleccione los recursos internos detrás del FTD (**origen original** y **origen traducido**) y el destino como el pool local de IP para los usuarios de Anyconnect (**Destino original** y **destino traducido**) como se muestra en la imagen.

Add NAT Rule

NAT Rule:

Manual NAT Rule

Insert:

In Category

Type:

Static

Enable

Description:

Interface Objects

Translation

PAT Pool

Advanced

Original Packet

Original Source:*

FTDv-Inside-SUPERNE

Original Destination:

Address

vpn-pool

Original Source Port:

Original Destination Port:

Translated Packet

Translated Source:

Translated Destination:

Translated Source Port:

Translated Destination Port:

4. Asegúrese de alternar las opciones (como se muestra en la imagen), para habilitar **"no-proxy-arp"** y **"route-lookup"** en la regla NAT, seleccione **OK** como se muestra en la imagen.

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 es el resultado de la configuración de la exención de NAT.

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

Los objetos utilizados en la sección anterior son los que se describen a continuación.

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"/>

Paso 2. Configuración Hairpin

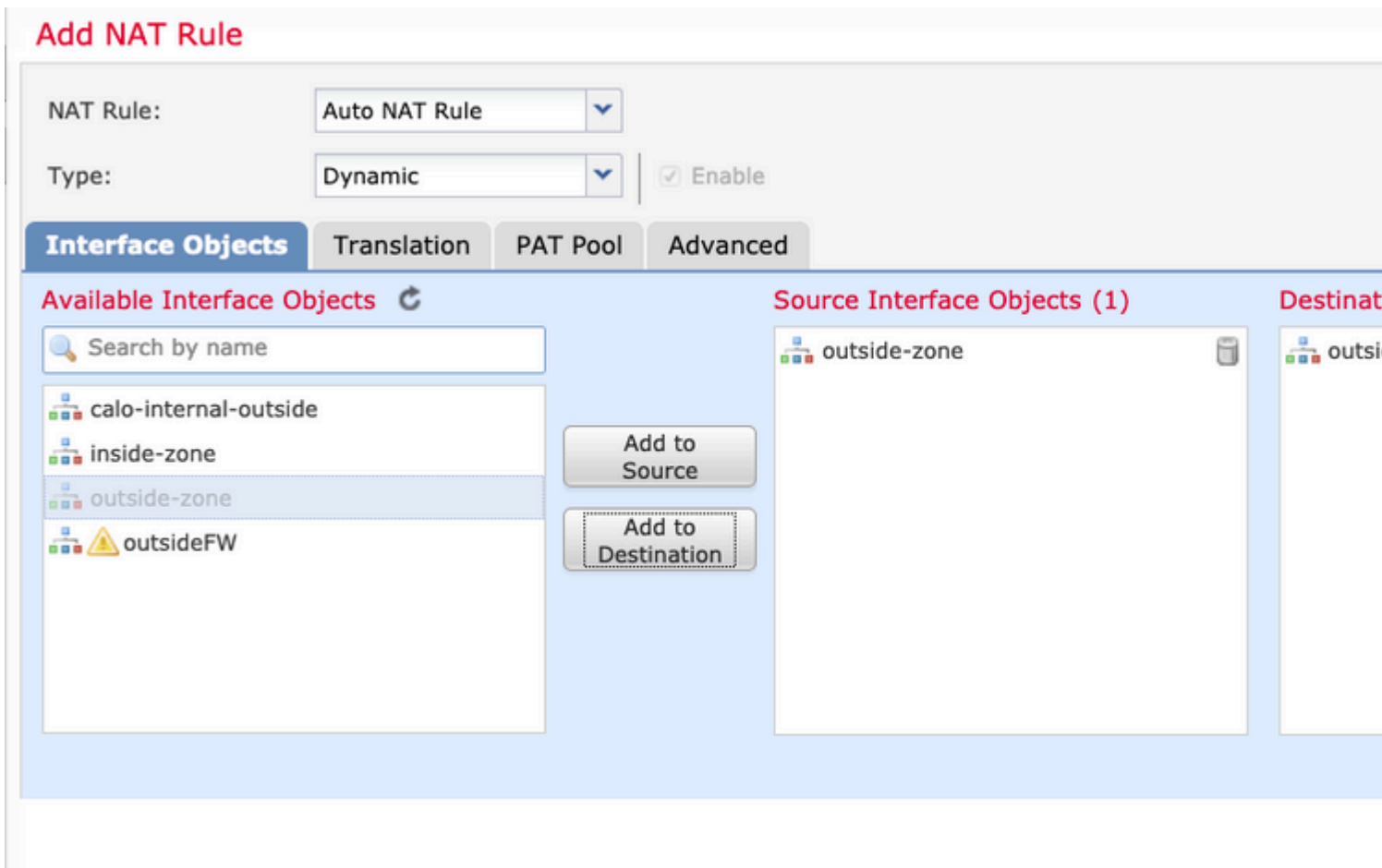
También conocido como **U-turn**, este es un método de traducción que permite que el tráfico fluya sobre la misma interfaz en la que se recibe el tráfico.

Por ejemplo, cuando Anyconnect se configura con una política de túnel dividido **completo**, se accede a los recursos internos según la política de exención de NAT. Si el tráfico del cliente Anyconnect está destinado a alcanzar un sitio externo en Internet, la horquilla NAT (o giro en U) es responsable de rutear el tráfico desde afuera hacia afuera.

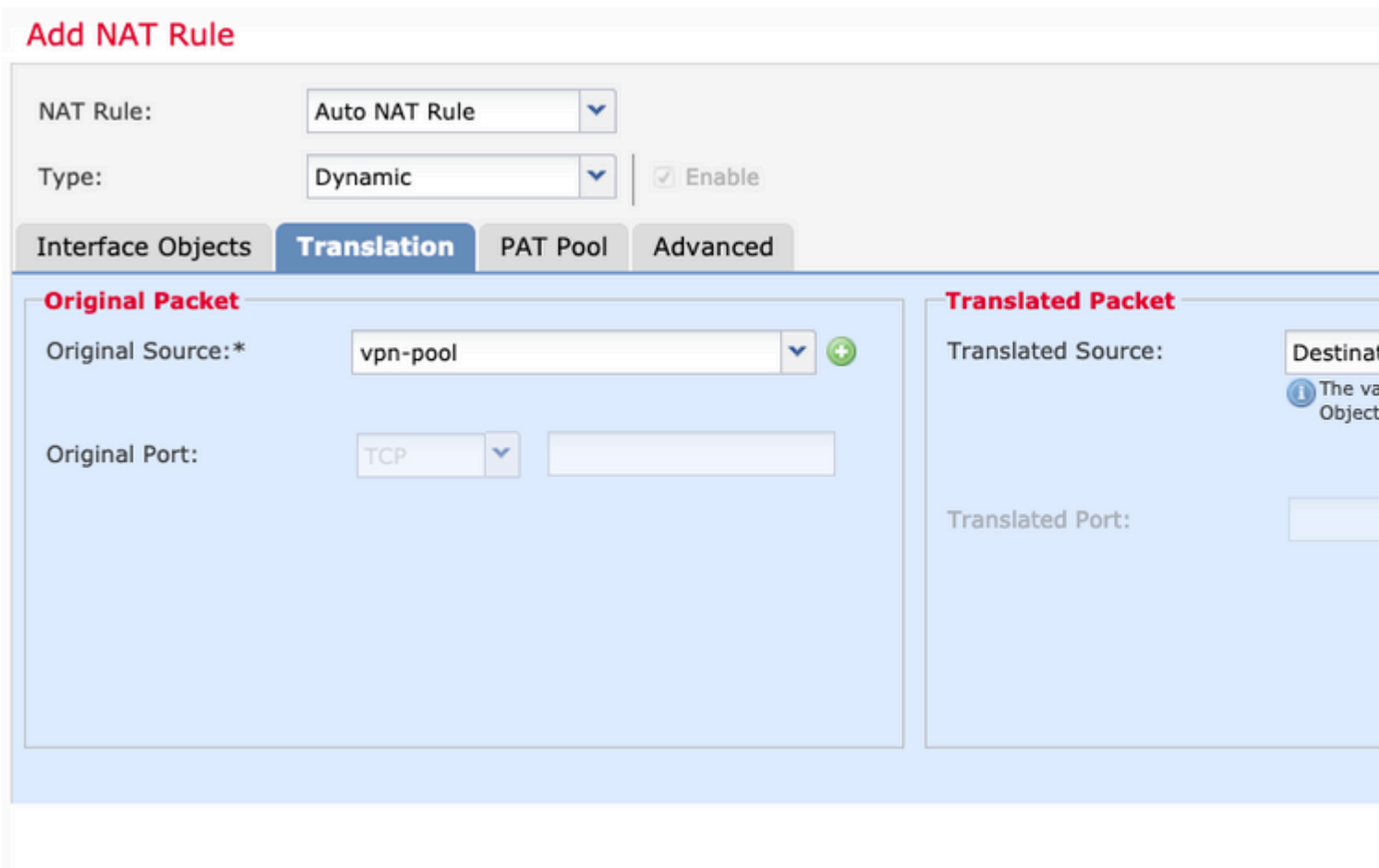
Se debe crear un objeto de conjunto VPN antes de la configuración NAT.

1. Cree una nueva sentencia NAT, seleccione **Auto NAT Rule** en el campo **NAT Rule** y seleccione **Dynamic** como el **tipo de NAT**.

2. Seleccione la misma interfaz para los objetos de interfaz de **origen** y destino (externos):



3. En la pestaña Traducción, seleccione como **Origen Original** el objeto vpn-pool y seleccione **IP de Interfaz de Destino** como **Origen Traducido**, seleccione **Aceptar** como se muestra en la imagen.



4. Este es el resumen de la configuración de NAT como se muestra en la imagen.

#	Direction	Type	Source Interface	Destination Interface	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations
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. Haga clic en **Guardar** e **Implementar** los cambios.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Ejecute estos comandos en la línea de comandos de 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**

Troubleshoot

Actualmente no hay información específica de solución de problemas disponible para esta configuración.</>

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).