

# Configure Anyconnect VPN Client en FTD: Servidor DHCP para la Asignación de Direcciones

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Paso 1. Configuración del alcance DHCP en el servidor DHCP](#)

[Paso 2. Configurar Anyconnect](#)

[Paso 2.1. Configurar perfil de conexión](#)

[Paso 2.2. Configure la Política de Grupo](#)

[Paso 2.3. Configurar la política de asignación de direcciones](#)

[Escenario de IP Helper](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

## Introducción

Este documento proporciona un ejemplo de configuración para Firepower Threat Defense (FTD) en la versión 6.4, que permite a las sesiones VPN de acceso remoto obtener una dirección IP asignada por un servidor de protocolo de configuración dinámica de host (DHCP) de terceros.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- FTD
- Firepower Management Center (FMC).
- DHCP

### Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- FMC 6.5

- FTD 6.5
- Windows Server 2016

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. If your network is live, make sure that you understand the potential impact of any command.

## Antecedentes

Este documento no describirá toda la configuración de acceso remoto, solamente la configuración requerida en el FTD para cambiar de conjunto de direcciones locales a asignación de dirección DHCP.

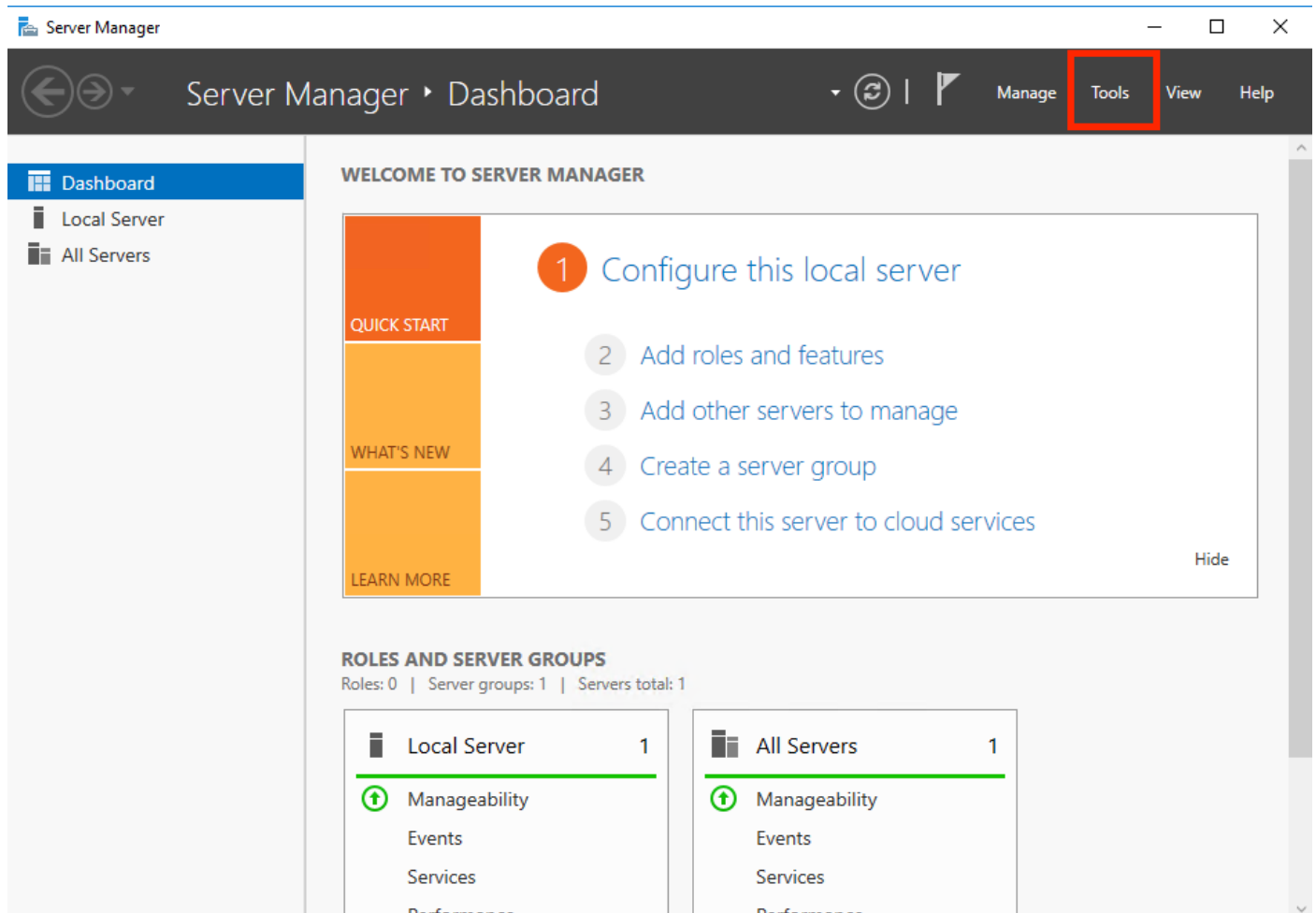
Si está buscando el documento de ejemplo de configuración de Anyconnect, consulte "Configure AnyConnect VPN Client on FTD: Documento Hairpinning y NAT Exemption".

## Configurar

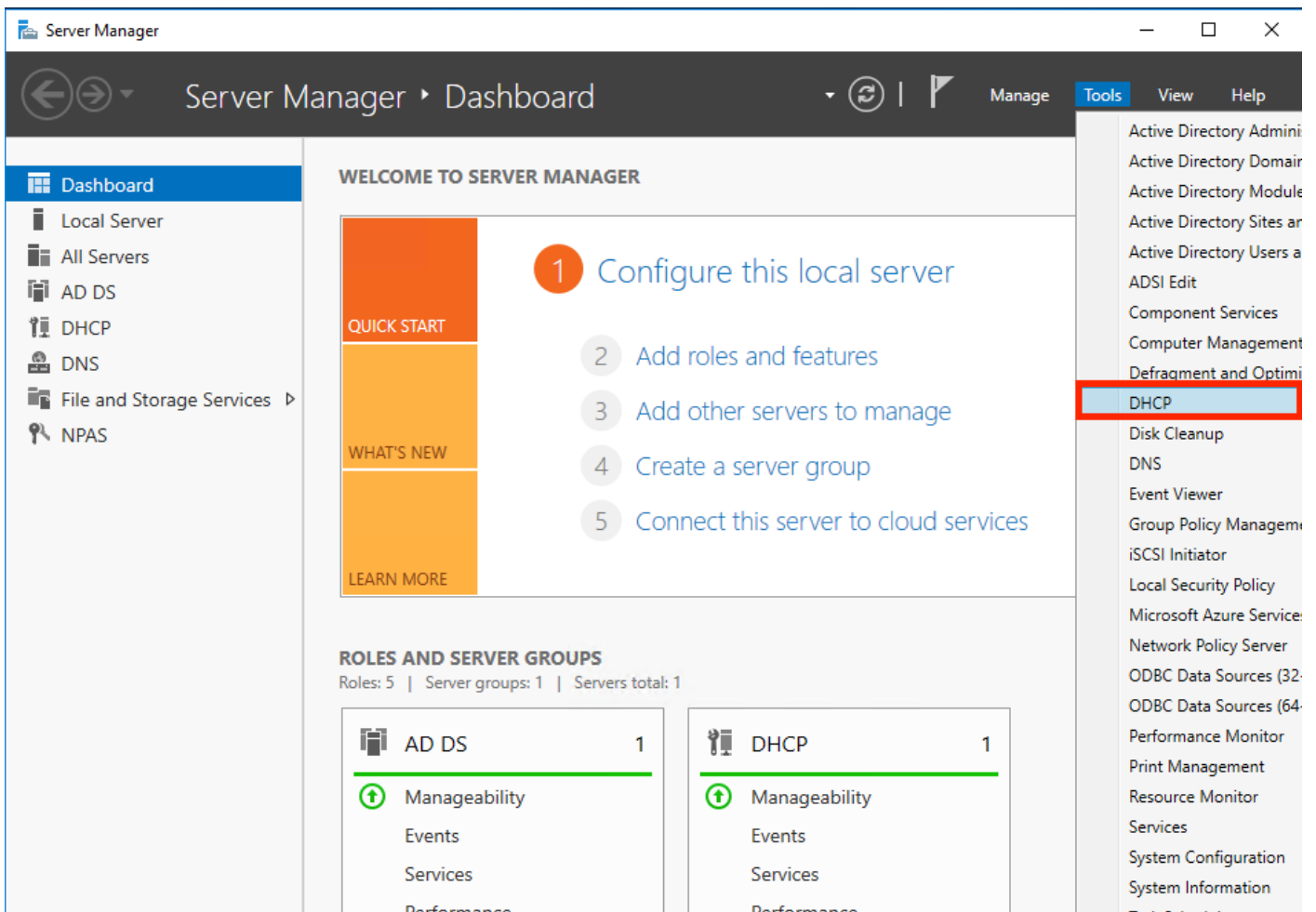
### Paso 1. Configuración del alcance DHCP en el servidor DHCP

En este escenario, el servidor DHCP se encuentra detrás de la interfaz interna del FTD.

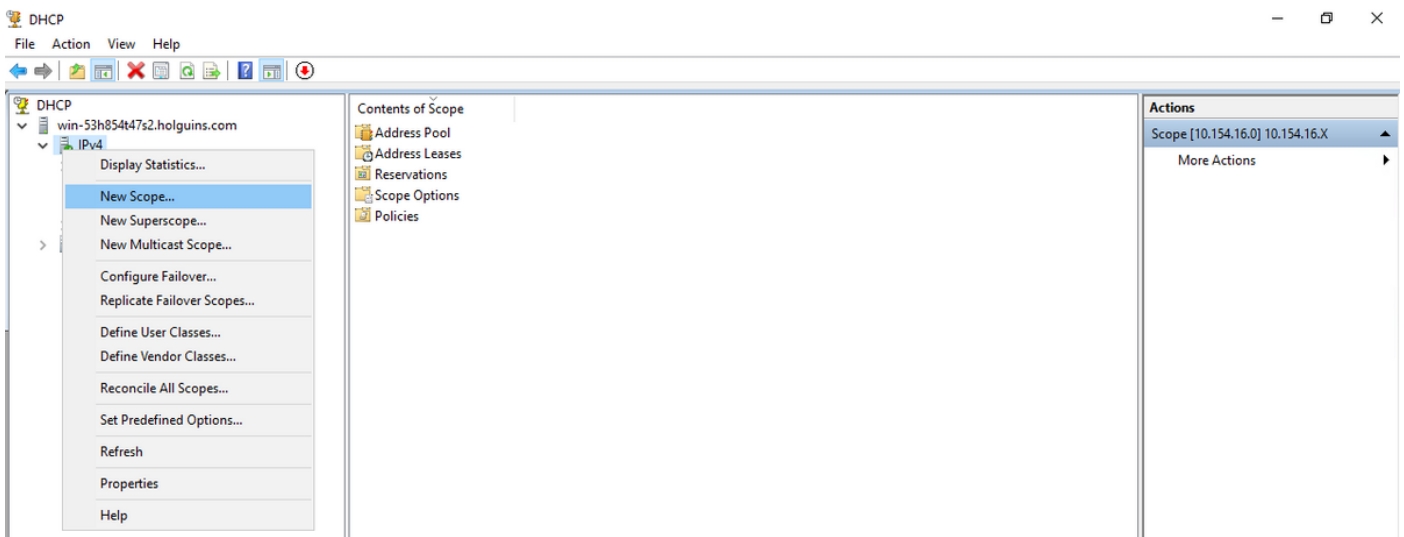
1. Abra el Administrador de servidores en Windows Server y seleccione **Herramientas** como se muestra en la imagen.



## 2. Seleccionar DHCP:



## 3. Seleccione IPv4, haga clic con el botón derecho en él y seleccione **Nuevo alcance** como se muestra en la imagen.



## 4. Siga el **asistente** como se muestra en la imagen.

## New Scope Wizard



### Welcome to the New Scope Wizard

This wizard helps you set up a scope for distributing IP addresses to computers on your network.

To continue, click Next.

< Back

Next >

Cancel

5. Asigne un nombre al ámbito como se muestra en la imagen.

## New Scope Wizard

### Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.



Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

< Back

Next >

Cancel

6. Configure el rango de direcciones como se muestra en la imagen.

## New Scope Wizard

### IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

< Back   Next >   Cancel

7. (Opcional) Configure las exclusiones como se muestra en la imagen.

## New Scope Wizard

### Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.



Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:

End IP address:

Add

Excluded address range:

Remove

Subnet delay in milli second:

< Back

Next >

Cancel

8. Configure la **duración del arrendamiento** como se muestra en la imagen.

## New Scope Wizard

### Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days:  Hours:  Minutes:

< Back

Next >

Cancel

9. (Opcional) Configure las opciones de alcance DHCP:



## New Scope Wizard

### Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.



When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

- Yes, I want to configure these options now
- No, I will configure these options later

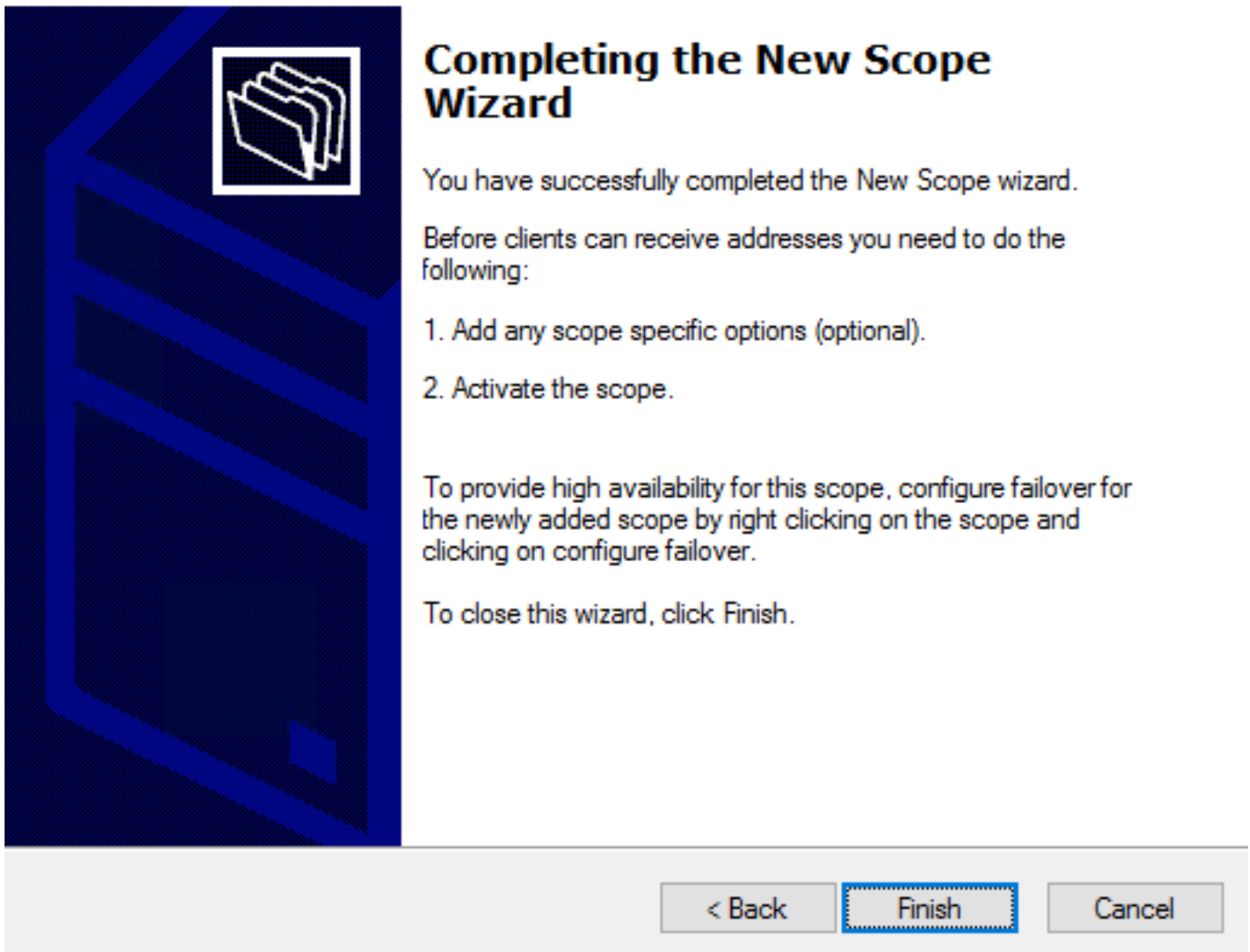
< Back

Next >

Cancel

10: Seleccione **Finalizar** como se muestra en la imagen.

## New Scope Wizard



### Completing the New Scope Wizard

You have successfully completed the New Scope wizard.

Before clients can receive addresses you need to do the following:

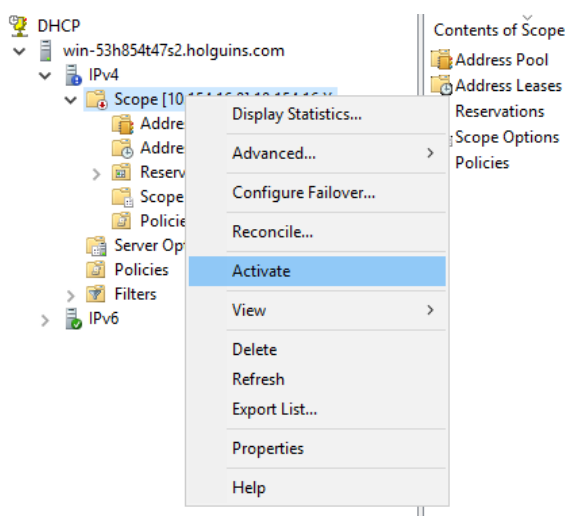
1. Add any scope specific options (optional).
2. Activate the scope.

To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover.

To close this wizard, click Finish.

< Back   Finish   Cancel


11: Haga clic con el botón derecho del ratón en el alcance que acaba de crear y seleccione **Activar** como se muestra en la imagen.



## Paso 2. Configurar Anyconnect

Una vez que se configura y activa el alcance DHCP, el siguiente procedimiento se realiza en el FMC.


## Paso 2.1. Configurar perfil de conexión

1. En la sección Servidores DHCP, seleccione el  y crear un objeto con la dirección IP del servidor DHCP.

2. Seleccione el objeto como servidor DHCP para solicitar una dirección IP de como se muestra en la imagen.


### Edit Connection Profile

Connection Profile:\*


Group Policy:\*   [Edit Group Policy](#)


**Client Address Assignment** AAA Aliases


IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria.

Address Pools: 

Name	IP Address Range
------	------------------

DHCP Servers: 

Name	DHCP Server IP Address
DC-holguins-172.204.206.224	172.204.206.224 

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

## Paso 2.2. Configure la Política de Grupo

1. Dentro del menú Directiva de grupo, navegue hasta **General > DNS/WINS**, hay una sección **Alcance de red DHCP** como se muestra en la imagen.

## Edit Group Policy



Name: \*

Description:

**General** AnyConnect Advanced

VPN Protocols  
IP Address Pools  
Banner  
**DNS/WINS**  
Split Tunneling

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

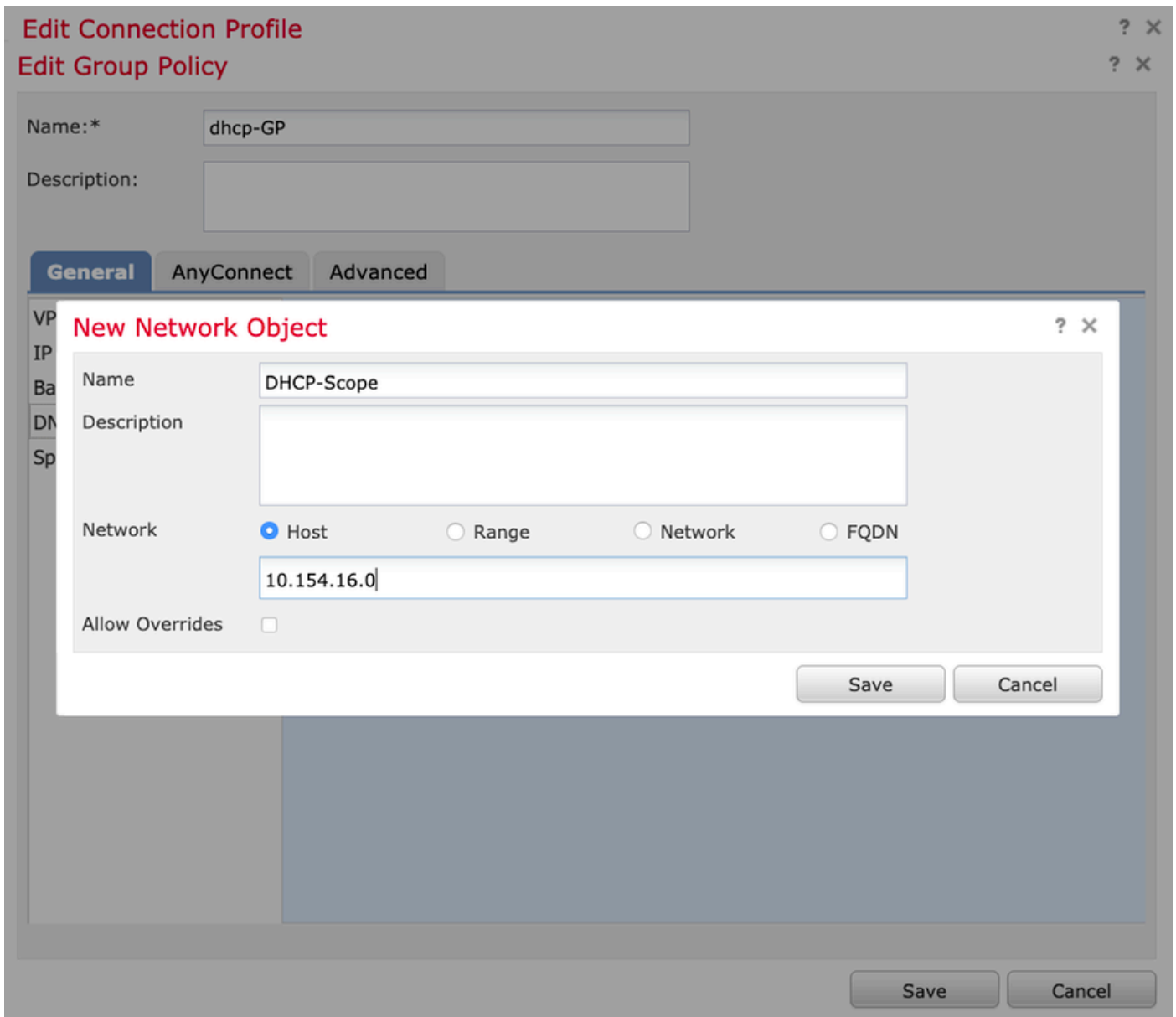
DHCP Network Scope:    
*Only network object with ipv4 address is allowed (Ex: 10.72.3.5)*

Default Domain:

Save Cancel

2. Cree un nuevo objeto, debe tener el mismo alcance de red que el servidor DHCP.

**Nota:** Debe ser un objeto host, no una subred.



3. Seleccione el objeto de alcance DHCP y seleccione **Guardar** como se muestra en la imagen.

## Edit Group Policy



Name:\*

Description:

**General** AnyConnect Advanced

VPN Protocols  
IP Address Pools  
Banner  
DNS/WINS  
Split Tunneling

Primary DNS Server:  +

Secondary DNS Server:  +

Primary WINS Server:  +

Secondary WINS Server:  +

**DHCP Network Scope:**  +

*Only network object with ipv4 address is allowed (Ex: 10.72.3.5)*

Default Domain:

**Save** Cancel

### Paso 2.3. Configurar la política de asignación de direcciones

1. Navegue hasta **Avanzada > Política de Asignación de Direcciones** y asegúrese de que la opción **Usar DHCP** esté alterada como se muestra en la imagen.

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

Anyconnect-FTD

Policy Assignments (1)

**Connection Profile** Access Interfaces **Advanced**

AnyConnect Client Images  
**Address Assignment Policy**  
Certificate Maps  
Group Policies  
IPsec  
Crypto Maps  
IKE Policy  
IPsec/IKEv2 Parameters

**Address Assignment Policy**  
Client address assignment criteria for all connection profiles. For incoming VPN client, the following options are tried in order, until an address is found.

**IPv4 Policy**

- Use authorization server (RADIUS Only)
- Use DHCP** ←
- Use internal address pools

Reuse an IP address:  minutes until session released. (0 - 480 mins)

**IPv6 Policy**

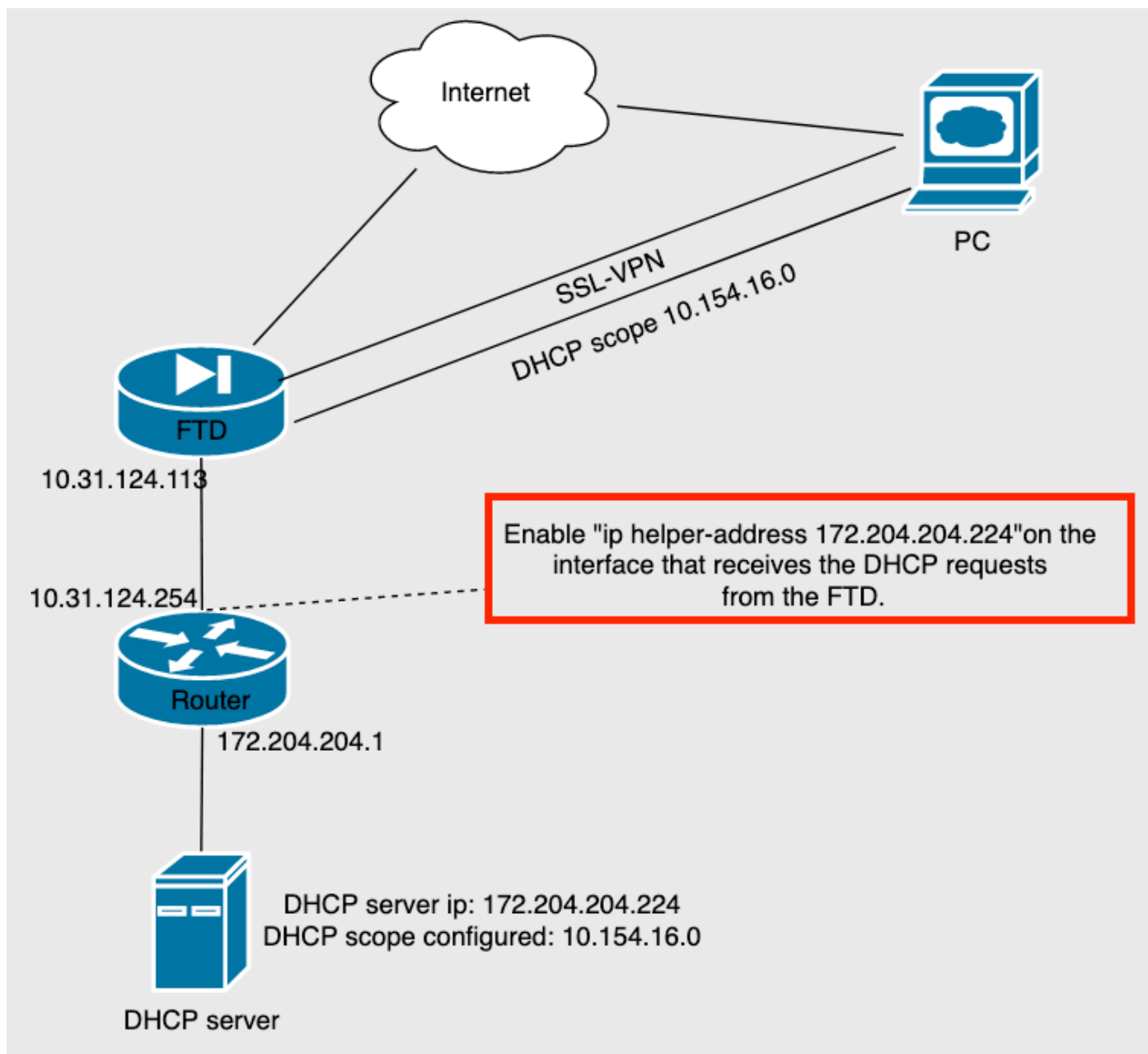
- Use authorization server (RADIUS Only)
- Use internal address pools

2. Guarde los cambios e implemente la configuración.

## Escenario de IP Helper

Cuando el servidor DHCP está detrás de otro router en la red de área local (LAN), se necesita un "ayudante IP" para reenviar las solicitudes al servidor DHCP.

Como se muestra en la imagen, una topología ilustra el escenario y los cambios necesarios en la red.



## Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Esta sección describe los paquetes DHCP intercambiados entre el FTD y el servidor DHCP.

- Descubrimiento: Este es un paquete de unidifusión enviado desde la interfaz interna del FTD

al servidor DHCP. En la carga útil, una **dirección IP del agente Relay** especifica el alcance del servidor DHCP como se muestra en la imagen.

```
Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x0765c988
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 10.154.16.0
  Client MAC address: Vmware_96:d1:70 (00:50:56:96:d1:70)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
```

- Oferta: Este paquete es una respuesta del servidor DHCP, viene con el origen del servidor DHCP y el destino del alcance DHCP en el FTD.
- Solicitud: Este es un paquete de unidifusión enviado desde la interfaz interna de FTD al servidor DHCP.
- ACK: Este paquete es una respuesta del servidor DHCP, viene con el origen del servidor DHCP y el destino del alcance DHCP en el FTD.

## Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Paso 1. Descargue y active el Wireshark en el servidor DHCP.

Paso 2. Aplique DHCP como el filtro de captura como se muestra en la imagen.



No.	Time	Source	Destination	Protocol	Length	Info
						Number

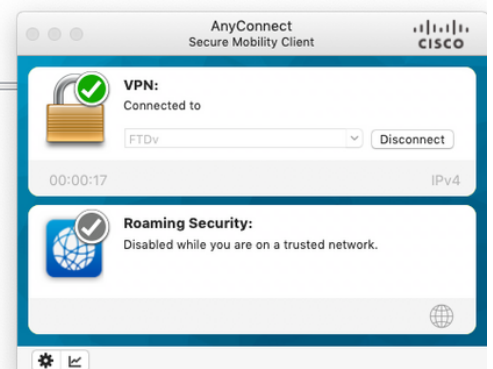


Paso 3. Inicie sesión en Anyconnect, la negociación DHCP debe verse como se muestra en la imagen.

No.	Time	Source	Destination	Protocol	Length	Info
4125	211.109079	10.31.124.113	172.204.204.224	DHCP	590	DHCP Discover - Transaction ID 0x765c988
4126	211.109321	172.204.204.224	10.154.16.0	DHCP	342	DHCP Offer - Transaction ID 0x765c988
4127	211.111245	10.31.124.113	172.204.204.224	DHCP	590	DHCP Request - Transaction ID 0x765c988
4128	211.111514	172.204.204.224	10.154.16.0	DHCP	342	DHCP ACK - Transaction ID 0x765c988

```
> Frame 4125: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{B27A96D9-4596-4DC3-A4C6-58020274134D}, id 0
> Ethernet II, Src: Cisco_d1:2d:30 (28:6f:7f:d1:2d:30), Dst: Vmware_96:23:b6 (00:50:56:96:23:b6)
> Internet Protocol Version 4, Src: 10.31.124.113, Dst: 172.204.204.224
> User Datagram Protocol, Src Port: 67, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

```
0000 00 50 56 96 23 b6 28 6f 7f d1 2d 30 08 00 45 00  .PV.#:(o...-E
0010 02 40 1f 99 00 00 00 11 18 d7 0a 1f 7c 71 ac cc  @.....|q.
0020 cc e0 00 43 00 43 02 2c cb e4 01 01 06 00 07 65  .C.C.....e
0030 c9 88 00 00 00 00 00 00 00 00 00 00 00 00 00  .C.C.....
0040 00 00 0a 9a 10 00 00 50 56 96 d1 70 00 00 00  .P.V.p...
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .
```



## Información Relacionada

- Este vídeo proporciona el ejemplo de configuración para FTD, que permite a las sesiones VPN de acceso remoto obtener una dirección IP asignada por un servidor DHCP de terceros.
- [Soporte Técnico y Documentación - Cisco Systems](#)