

Habilitar las opciones de alcance DHCP en el servidor DHCP mediante FTD como agente de retransmisión

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configuración](#)

[Diagrama de la red](#)

[Configuración de DHCP Relay](#)

[Configuración del Agente de retransmisión DHCP](#)

[Configurar servidor DHCP externo](#)

[Activar la opción 43 en el servidor DHCP externo](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo habilitar las opciones en el servidor DHCP usando en FTD administrado por FMC.

Prerequisites

Requirements

- Conocimiento de la tecnología Firepower
- Conocimiento del servidor de protocolo de control dinámico de host (DHCP)/retransmisión DHCP.

Componentes Utilizados

- La información de este documento se basa en Virtual Cisco FTD and FMC, versión 7.4.0
- Windows Server 2019 se utiliza como servidor DHCP

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

El dispositivo de defensa contra amenazas puede transmitir información mediante las opciones DHCP especificadas en RFC 2132, RFC 2562 y RFC 5510.

Admite todas las opciones DHCP numeradas del 1 al 255, excepto las opciones 1, 12, 50-54, 58-59, 61, 67 y 82.

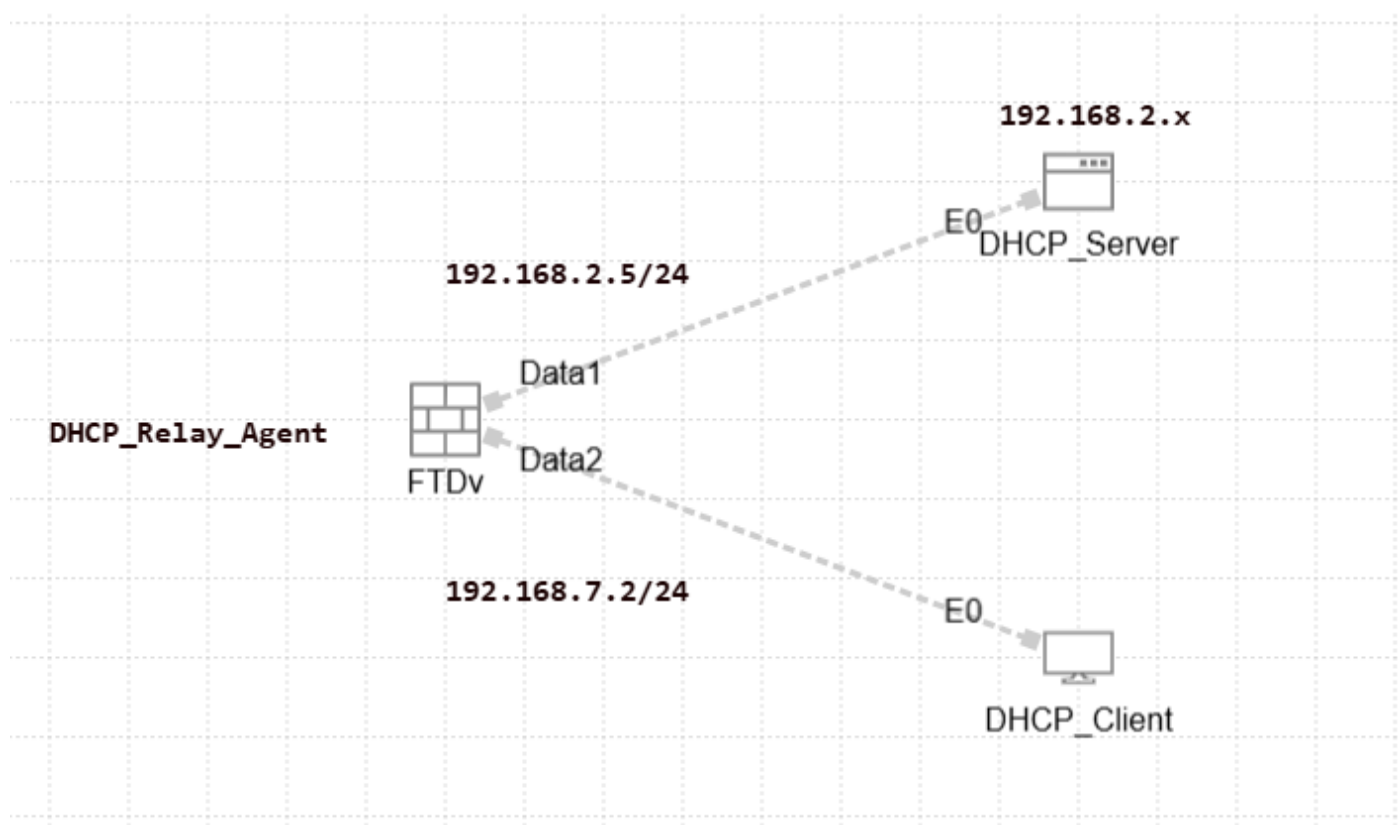
RFC 2132 especifica dos opciones DHCP pertinentes a las configuraciones específicas del proveedor: Opción 60 y opción 43.

El documento ofrece configuraciones de ejemplo e ilustra cómo funciona la opción 43 de DHCP (información específica del proveedor) en Windows Server 2019, con FTD funcionando como agente de retransmisión DHCP.

La opción 43 permite que los servidores DHCP transmitan información específica del proveedor a los clientes, lo que facilita que los dispositivos, como los puntos de acceso, se localicen y conecten a sus controladores, incluso cuando se encuentran en diferentes VLAN o subredes.

Configuración

Diagrama de la red



Configuración de DHCP Relay

La interfaz FTD funciona como un agente de retransmisión DHCP, facilitando la comunicación entre el cliente y un servidor DHCP externo.

Presta atención a las solicitudes de los clientes y anexa datos de configuración esenciales, como la información del vínculo del cliente, que el servidor DHCP necesita para asignar una dirección al cliente.

Al recibir una respuesta del servidor DHCP, la interfaz reenvía el paquete de respuesta al cliente DHCP.

La configuración de la retransmisión DHCP implica dos pasos principales:

1. Configure el Agente de retransmisión DHCP.
2. Configure el servidor DHCP externo.

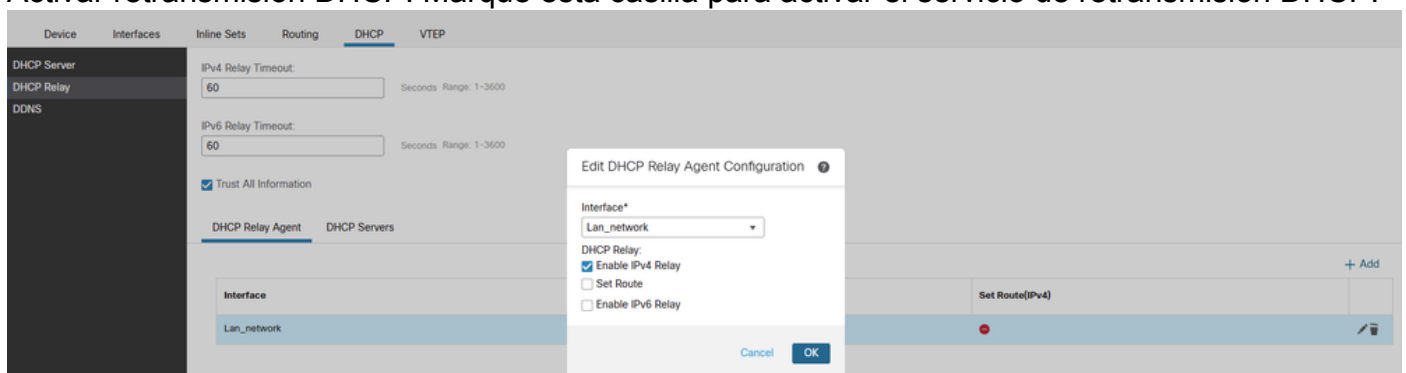
Configuración del Agente de retransmisión DHCP

Para configurar la retransmisión DHCP, verifique los siguientes pasos:

1. Navegue hasta Dispositivos > Administración de dispositivos.
2. Haga clic en el botón Editar del dispositivo FTD.
3. Navegue hasta la opción DHCP > DHCP Relay.
4. Haga clic en Agregar.

Interfaz: Seleccione la interfaz adecuada en la lista desplegable. Aquí es donde la interfaz escucha las solicitudes de los clientes, y los clientes DHCP pueden conectarse directamente a esta interfaz para las solicitudes de dirección IP.

Activar retransmisión DHCP: Marque esta casilla para activar el servicio de retransmisión DHCP.



DHCP_Relay_Agent_Config

5. Haga clic en Aceptar para guardar los ajustes de configuración para el agente de retransmisión DHCP.

Configurar servidor DHCP externo

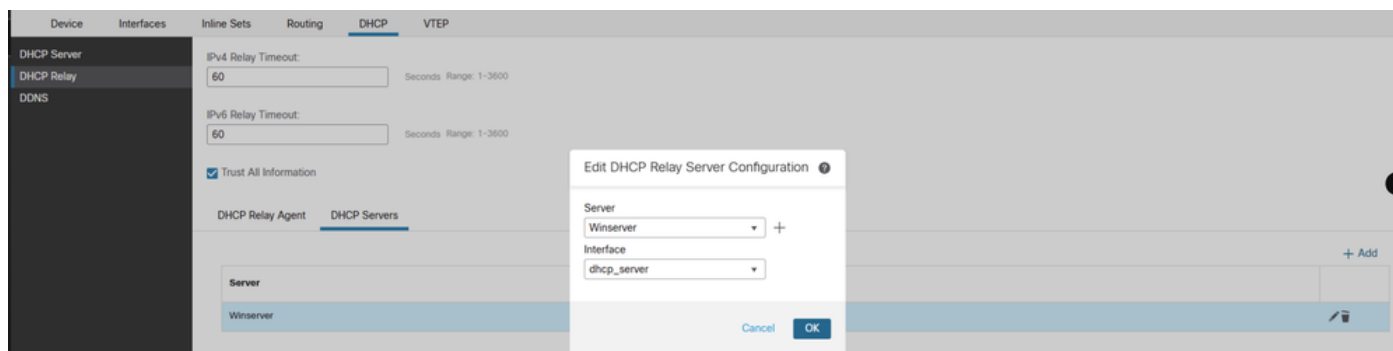
Para configurar la dirección IP del servidor DHCP externo al que se reenvían las solicitudes de los clientes, compruebe los siguientes pasos:

Navegue hasta la sección DHCP Server y haga clic en Add"

1.En el campo Server, ingrese la dirección IP del servidor DHCP. Puede elegir un objeto de red existente del menú desplegable o crear uno nuevo haciendo clic en el icono más (+).

2.En el campo Interface, especifique la interfaz que se conecta al servidor DHCP.

3.Para guardar la configuración, haga clic en OK. A continuación, haga clic en Guardar para almacenar la configuración de la plataforma.



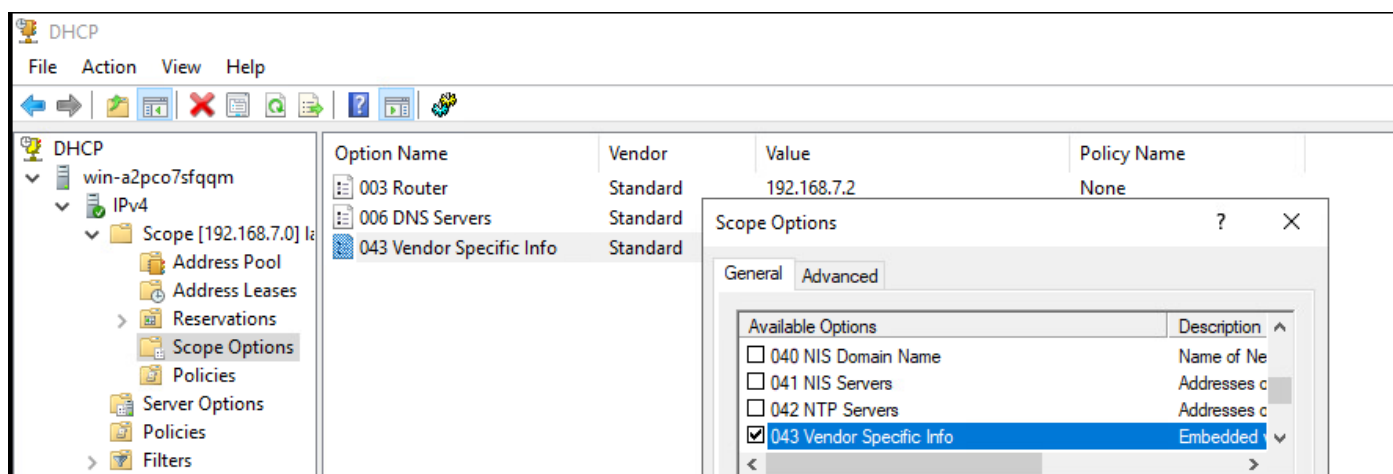
DHCP_Server_Config

4.A continuación, vaya a la opción Deploy, seleccione el dispositivo FTD donde desea aplicar los cambios y haga clic en Deploy para iniciar la implementación de la configuración de la plataforma.

Activar la opción 43 en el servidor DHCP externo

Tenga en cuenta: Según RFC 2132 , la longitud mínima para la opción 43 es 1.

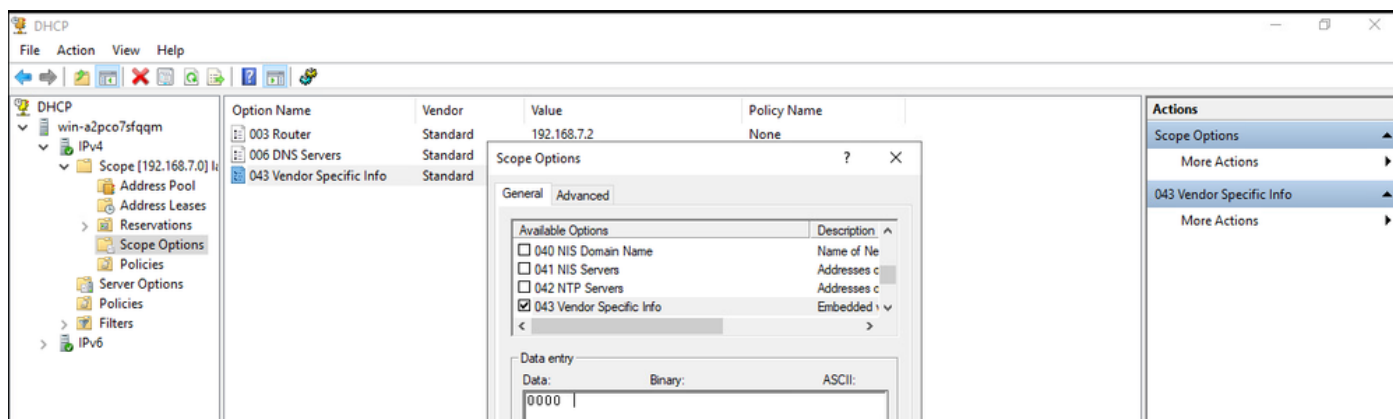
Navegue hasta los parámetros del servidor DHCP y vaya a IPv4, luego seleccione Scope y Scope Options >More Actions >Configure Options y habilite la opción 43



Enable_Option_43_On_External_DHCP_Server

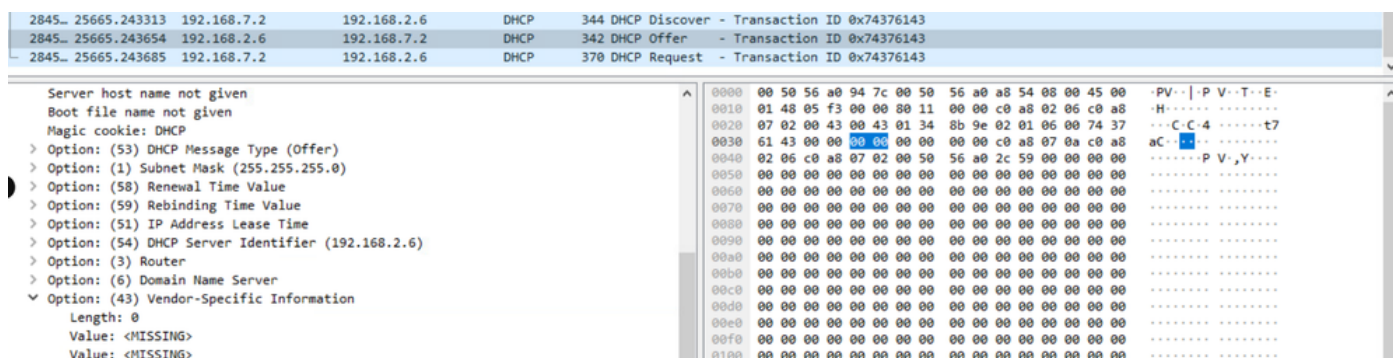
Inicialmente, la configuración predeterminada deja el valor vacío, lo que lleva al FTD a descartar

el paquete y categorizarlo como mal formado.



Default_Config_Of_Option_43

Desde el lado del servidor usando Wireshark, observamos que en el paquete OFFER, el valor está ausente para la opción 43 cuando la longitud es 0.



Non_Working_Server_Side_pcap

Cisco Firepower Threat Defence (FTD) descarta los paquetes porque tienen una longitud de 0 y se consideran malformados, lo que infringe el RFC 2132.

<#root>

firepower#

debug dhcprelay packet

```
debug dhcprelay packet enabled at level 1
ftd# DHCPD/RA: Relay msg received, fip=ANY, fport=0 on Lan_network interface
DHCPD/RA: Received a BOOTREQUEST from interface 3 (size = 302)
DHCPD/RA: Binding successfully added to hash table
DHCPRA: relay binding created for client 0050.56a0.2c59.
DHCPRA: setting giaddr to 192.168.7.2.
dhcpd_forward_request: request from 0050.56a0.2c59 forwarded to 192.168.2.6.
```

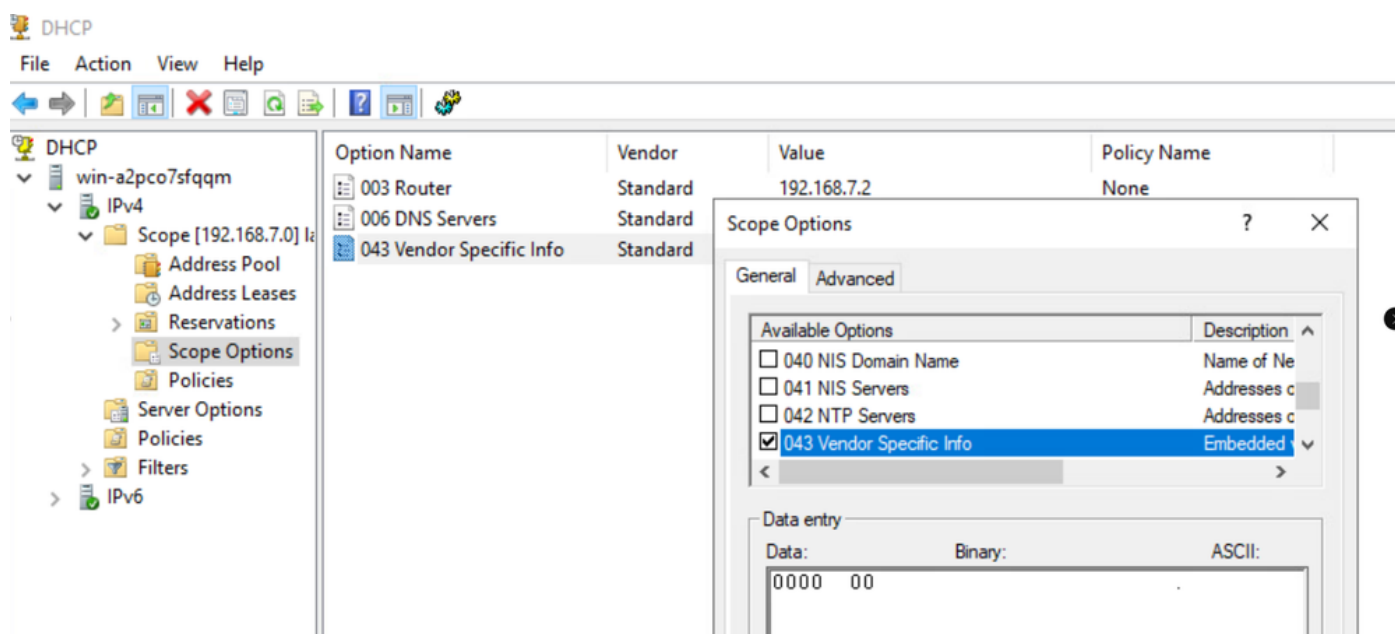
DHCPD/RA: option 43 is malformed.

DHCPD/RA: Unable to load workspace.

DHCPD/RA: Relay msg received, fip=ANY, fport=0 on Lan_network interface
 DHCP: Received a BOOTREQUEST from interface 3 (size = 328)
 DHCPRA: relay binding found for client 0050.56a0.2c59.
 DHCPRA: setting giaddr to 192.168.7.2.
 DHCPRA: Server request counter 1
 dhcpd_forward_request: request from 0050.56a0.2c59 forwarded to 192.168.2.6.

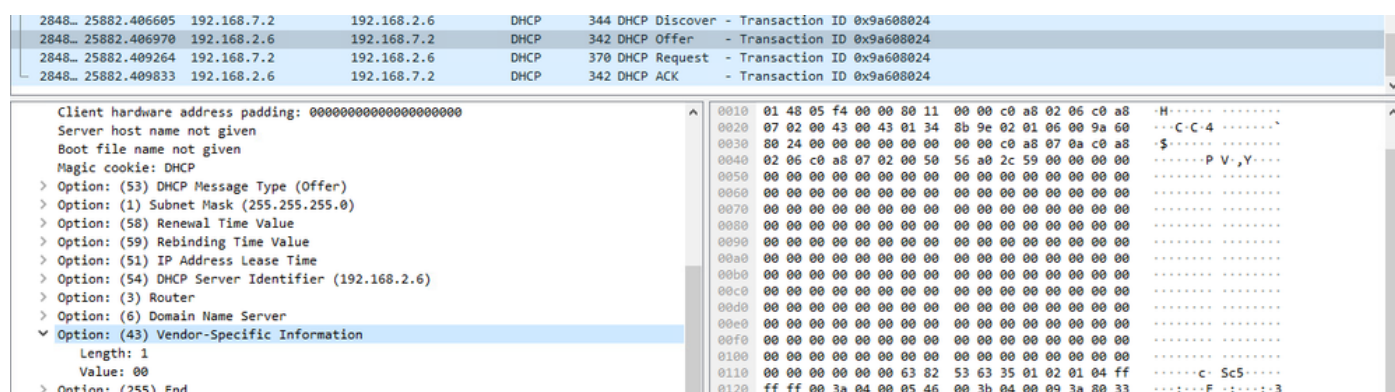
Para ajustar el valor binario para que sea mayor que 0 de acuerdo con RFC 2132, haga doble clic en el campo 043 Vendor Specific Info (Información específica del proveedor 043) y establezca el valor en 00, como se muestra en la imagen.

Este cambio garantiza que la dirección IP se conceda correctamente al cliente.



Valor_binario_cambiado_a_1

Proceso DORA del servidor cuando el valor se establece en 1 en la opción 43



Server_Side_Working_pcap

Proceso DORA del lado del cliente cuando el valor se establece como 1 en la opción 43 y podemos ver que el cliente es arrendado con una IP.

2907...	1837526.548275	0.0.0.0	255.255.255.255	DHCP	344	128 DHCP Discover	- Transaction ID 0x9a608024	
2907...	1837526.550203	192.168.2.6	192.168.7.10	DHCP	342	72 DHCP Offer	- Transaction ID 0x9a608024	
2907...	1837526.551703	0.0.0.0	255.255.255.255	DHCP	370	128 DHCP Request	- Transaction ID 0x9a608024	
2907...	1837526.553008	192.168.2.6	192.168.7.10	DHCP	342	72 DHCP ACK	- Transaction ID 0x9a608024	

> Option: (53) DHCP Message Type (Offer)	0000	00 50 56 a0 2c 59 00 50 56 a0 48 2d 08 00 45 00	·P·V·,·Y·P·,·V·H·...E·
> Option: (1) Subnet Mask (255.255.255.0)	0010	01 48 11 12 40 00 48 11 96 32 c0 a8 02 06 c0 a8	·H·...@·H·...2·...·
> Option: (58) Renewal Time Value	0020	07 0a 00 43 00 44 01 34 48 45 02 01 06 00 e2 68	...·C·D·4·HE·...·h·
> Option: (59) Rebinding Time Value	0030	3c 3f 00 00 00 00 00 00 00 00 c0 a8 07 0a c0 a8	<?·...·...·...·
> Option: (51) IP Address Lease Time	0040	02 06 c0 a8 07 02 00 50 56 a0 2c 59 00 00 00 00	...·...·P·V·,·Y·...·
> Option: (54) DHCP Server Identifier (192.168.2.6)	0050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...·...·...·...·
> Option: (3) Router	0060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...·...·...·...·
> Option: (6) Domain Name Server	0070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...·...·...·...·
> Option: (43) Vendor-Specific Information	0080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...·...·...·...·
Length: 1	0090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...·...·...·...·
Value: 00	00a0	00 00 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 00 00	...·...·...·...·
	00c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...·...·...·...·

Client_Side_Working_pcap

<#root>

firepower#

debug dhcprelay packet

debug dhcprelay packet enabled at level 1
ftd# DHCPD/RA: Relay msg received, fip=ANY, fport=0 on Lan_network interface
DHCP: Received a BOOTREQUEST from interface 3 (size = 302)
DHCPRA: relay binding found for client 0050.56a0.2c59.
DHCPRA: setting giaddr to 192.168.7.2.
dhcpd_forward_request: request from 0050.56a0.2c59 forwarded to 192.168.2.6.
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on dhcp_server interface
DHCP: Received a BOOTREPLY from relay interface 2 (size = 300, xid = 0x81f5dddc) at 06:55:25 UTC Tue Ma
DHCPRA: relay binding found for client 0050.56a0.2c59.
DHCPD/RA: creating ARP entry (192.168.7.10, 0050.56a0.2c59).
DHCPRA: forwarding reply to client 0050.56a0.2c59.
DHCPRA: Client Ip Address :192.168.7.10
DHCPRA: subnet mask in dhcp options :255.255.255.0
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on Lan_network interface
DHCP: Received a BOOTREQUEST from interface 3 (size = 328)
DHCPRA: relay binding found for client 0050.56a0.2c59.
DHCPRA: Server requested by client 192.168.2.6
DHCPRA: setting giaddr to 192.168.7.2.
DHCPRA: Server request counter 1
dhcpd_forward_request: request from 0050.56a0.2c59 forwarded to 192.168.2.6.
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on dhcp_server interface
DHCP: Received a BOOTREPLY from relay interface 2 (size = 300, xid = 0x81f5dddc) at 06:55:25 UTC Tue Ma
DHCPRA: relay binding found for client 0050.56a0.2c59.
DHCPRA: exchange complete - relay binding deleted for client 0050.56a0.2c59.
DHCPD/RA: Binding successfully deactivated
dhcpd_destroy_binding() removing NP rule for client 192.168.7.2
DHCPD/RA: free ddns info and binding
DHCPD/RA: creating ARP entry (192.168.7.10, 0050.56a0.2c59).
DHCPRA: forwarding reply to client 0050.56a0.2c59.

DHCPRA: Client Ip Address :192.168.7.10

DHCPRA: subnet mask in dhcp options :255.255.255.0

Verificación

Antes de configurar el servidor DHCP o la retransmisión, asegúrese de que el FTD está registrado en el FMC. Además, verifique que haya conectividad con el servidor DHCP en la configuración de retransmisión DHCP.

```
<#root>
```

```
>
```

```
system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.  
Type help or '?' for a list of available commands.
```

```
<#root>
```

```
><Press Enter>  
firepower#
```

```
ping
```

Para comprobar la configuración del Agente de retransmisión DHCP desde la CLI de FTD.

```
<#root>
```

```
firepower#
```

```
show running-config dhcprelay
```

```
dhcprelay server 192.168.2.6 dhcp_server  
dhcprelay enable Lan_network  
dhcprelay timeout 60  
dhcprelay information trust-all
```

Troubleshoot

Para solucionar el problema, tenga en cuenta los siguientes puntos:

1. Verifique el ruteo entre el FTD y el servidor DHCP para asegurarse de que es accesible desde el servidor DHCP.
2. Asegúrese de que el servidor DHCP tiene una ruta para acceder a la interfaz del agente de retransmisión DHCP.
3. Para resolver el problema de que el cliente no reciba una dirección IP, puede realizar una captura de paquetes en la interfaz enrutada de FTD.

Esto le permitirá examinar el proceso DORA del servidor DHCP dentro de las capturas de paquetes.

Puede utilizar [Use Firepower Threat Defence Captures y Packet Tracer](#) para realizar la captura de paquetes de forma eficaz.

Para detener y eliminar una sesión de captura de paquetes específica que haya iniciado previamente, ejecute el siguiente comando.

```
no capture <capture_name>
```

4. Para revisar el estado y recopilar los comandos dhcprelay debug , ejecute a continuación

Para ello, inicie sesión en la CLI de FTD .

```
<#root>
```

```
system support diagnostic-cli
```

```
enable
```

Press Enter.

```
<#root>
```

```
show dhcprelay statistic
```

```
show dhcprelay state
```

Para verificar si una depuración ya está habilitada, ejecute el siguiente comando.

```
<#root>
```

```
show debug
```

```
<#root>
```

To capture debug excute below commands

```
debug dhcprelay packet
```

```
debug dhcprelay event
```

```
<#root>
```

```
To disable debug
```

```
undebug all
```

Información Relacionada

[Configuración del servidor DHCP y la retransmisión en FTD con FMC](#)

[DHCP y DDNS](#)

[Soporte Técnico y Documentación - Cisco Systems](#)

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).