使用FTD作为中继代理在DHCP服务器上启用DHCP范围选项

目录

简介

本文档介绍如何在FMC管理的FTD中使用DHCP服务器上启用选项。

先决条件

要求

- Firepower技术知识
- 动态主机控制协议(DHCP)服务器/DHCP中继知识。

使用的组件

- 本文档中的信息基于虚拟思科FTD和FMC 7.4.0版
- Windows Server 2019用作DHCP服务器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

威胁防御设备可以使用RFC 2132、RFC 2562和RFC 5510中指定的DHCP选项传输信息。

它支持编号为1到255的所有DHCP选项，但选项1、12、50-54、58-59、61、67和82除外。

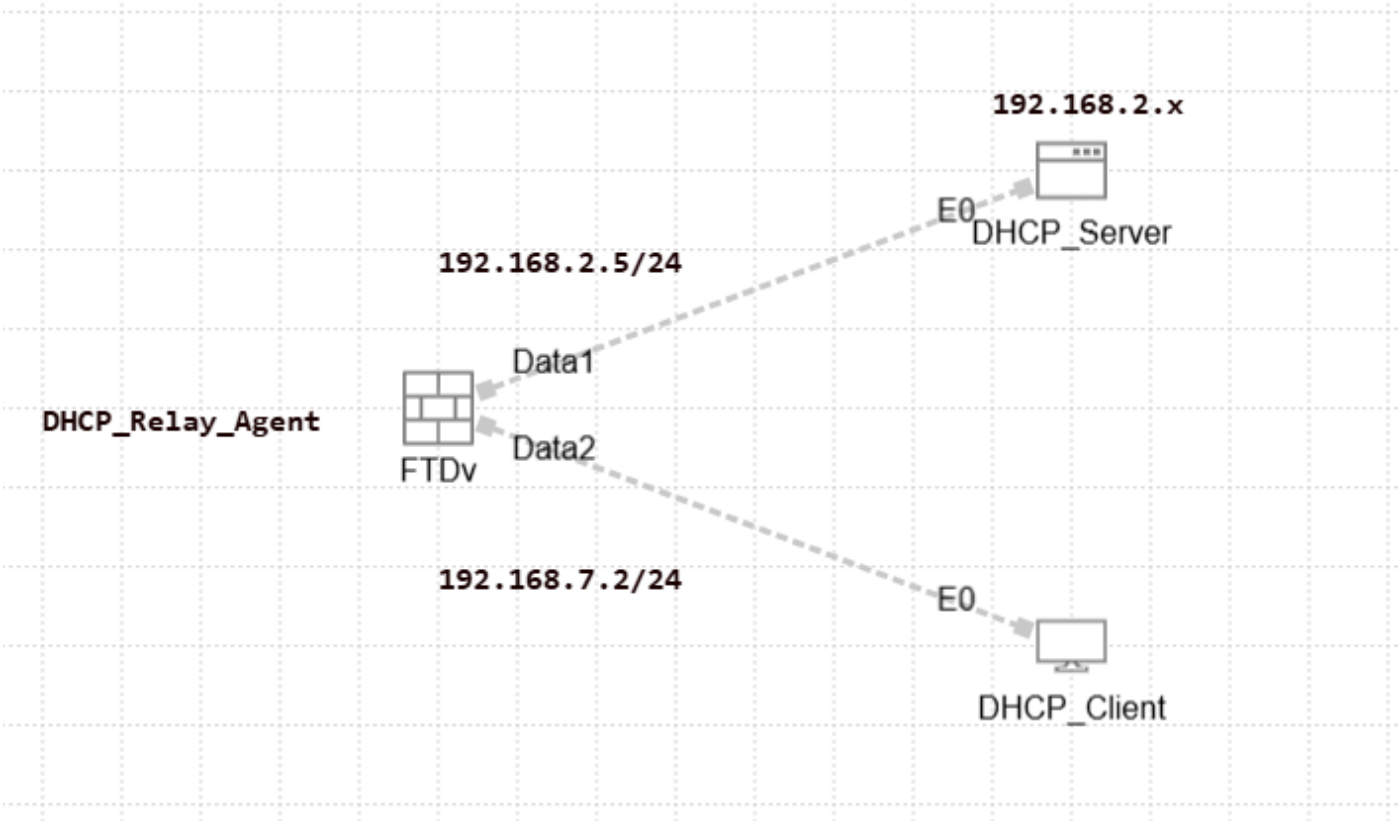
RFC 2132指定了两个与供应商特定配置相关的DHCP选项：第60和第43项。

本文档提供示例配置并说明DHCP选项43（供应商特定信息）如何在Windows Server 2019上运行，FTD将充当DHCP中继代理。

选项43使DHCP服务器能够向客户端传输特定于供应商的信息，使接入点等设备更容易定位和连接到其控制器，即使它们位于不同的VLAN或子网中。

配置

网络图



Network_Diagram

配置DHCP中继

FTD接口充当DHCP中继代理，促进客户端和外部DHCP服务器之间的通信。

它会侦听客户端请求并附加基本配置数据，例如DHCP服务器向客户端分配地址所需的客户端链路信息。

当从DHCP服务器收到响应时，接口将应答数据包转发回DHCP客户端。

配置DHCP中继包括两个主要步骤：

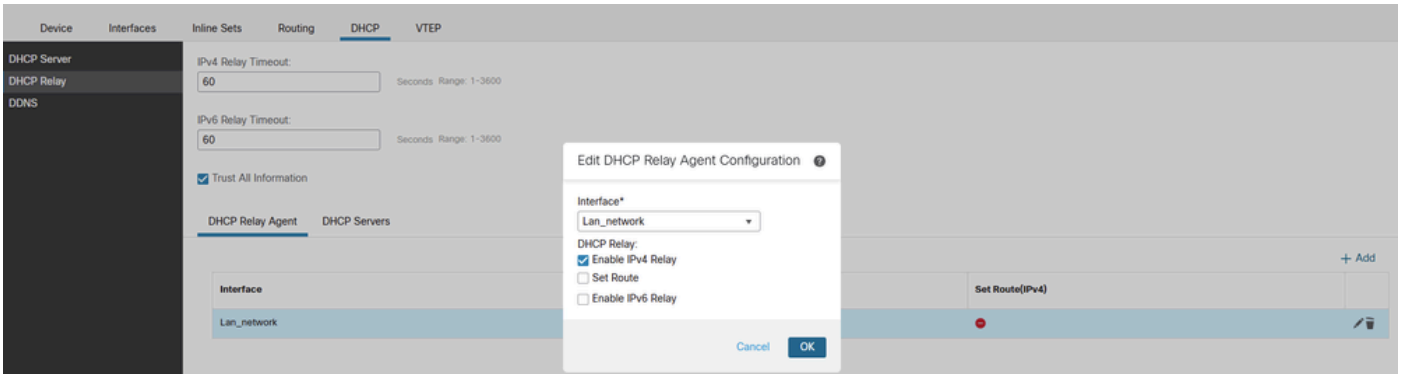
1.设置DHCP中继代理。
2.设置外部DHCP服务器。

配置DHCP中继代理

要配置DHCP中继，请检查以下步骤：

1.导航到设备>设备管理。
2.点击FTD设备的编辑按钮。
3.导航到DHCP > DHCP Relay选项。
4.单击Add。

接口:从下拉列表中选择适当的接口。这是接口侦听客户端请求的位置，并且DHCP客户端可以直接连接到此接口以进行IP地址请求。
启用DHCP中继：选中此框以激活DHCP中继服务。



DHCP_Relay_Agent_Config

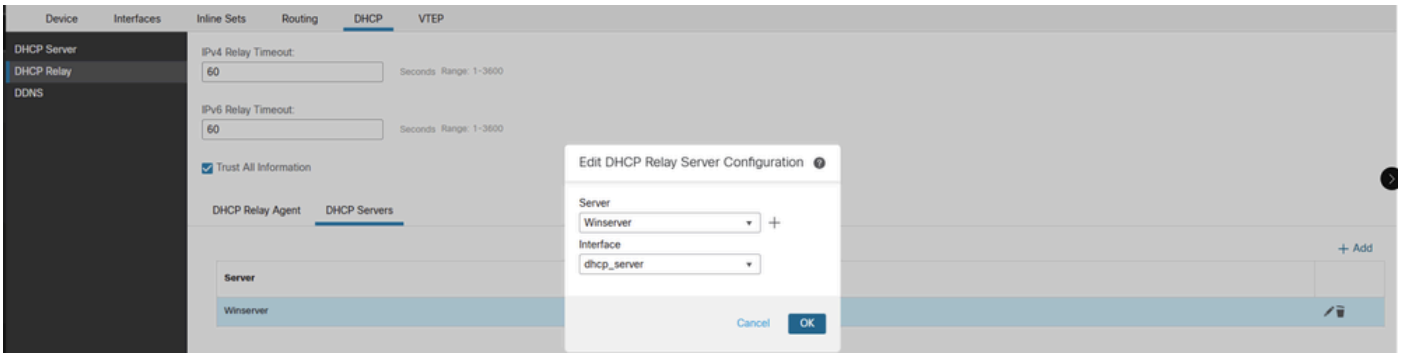
5.单击OK保存DHCP中继代理的配置设置。

配置外部DHCP服务器

要配置客户端请求转发到的外部DHCP服务器的IP地址，请检查以下步骤：

导航到DHCP Server部分，然后单击Add”
1.在Server字段中，输入DHCP服务器的IP地址。您可以从下拉菜单中选择现有网络对象，也可以通过单击加号(+)图标创建一个新网络对象。
2.在Interface字段中，指定连接到DHCP服务器的接口。

3.要保存配置，请单击OK。然后，单击Save以存储平台设置。



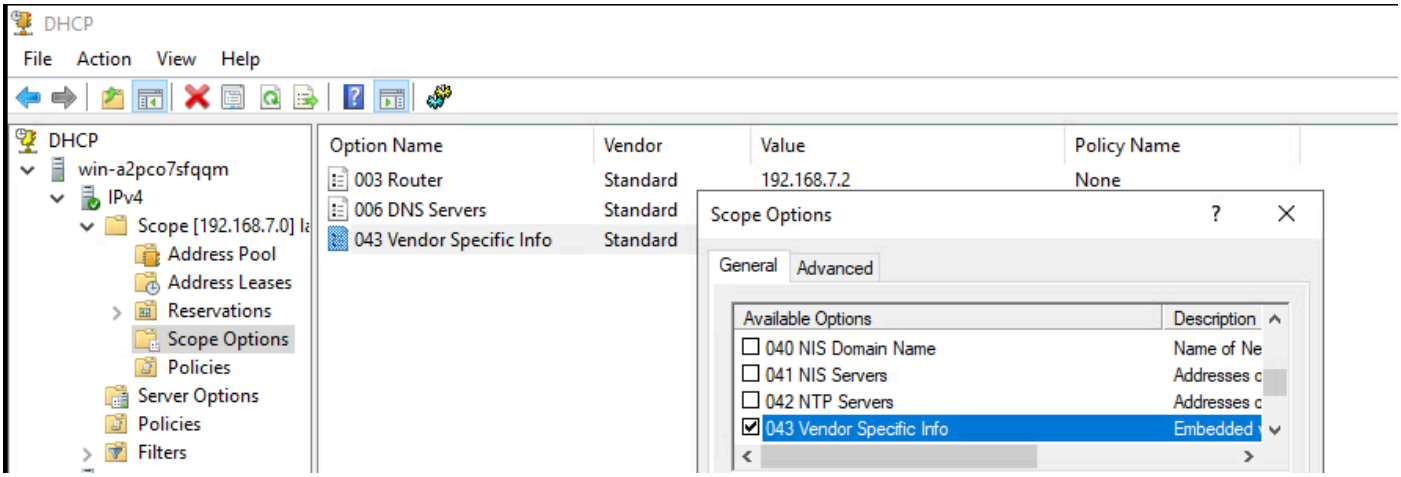
DHCP_Server_Config

4.接下来，转到Deploy选项，选择要应用更改的FTD设备，然后单击Deploy启动平台设置的部署。

在外部DHCP服务器上启用选项43

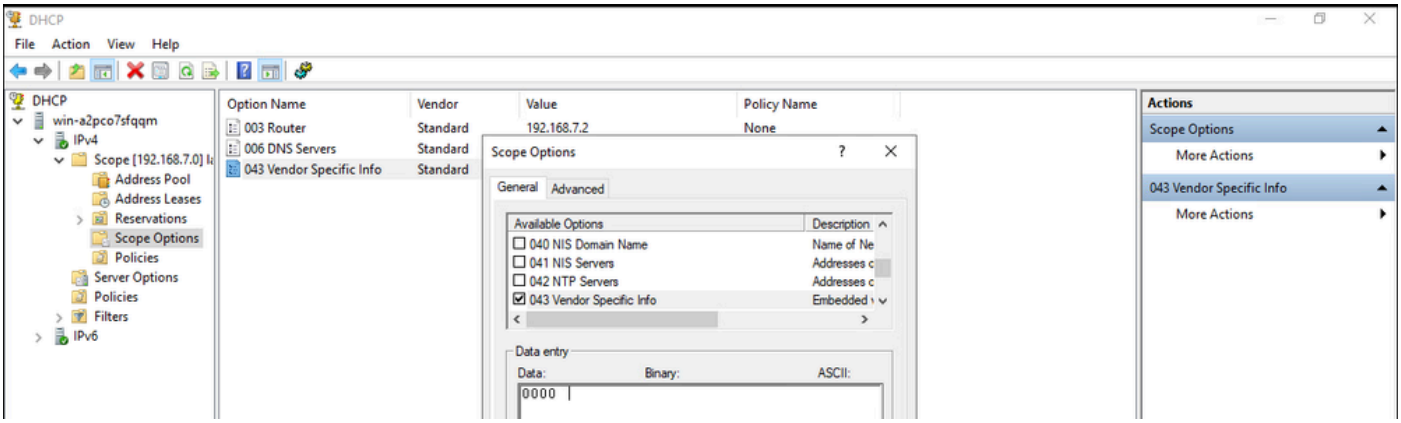
请注意：根据RFC 2132，选项43的最小长度为1。

导航到DHCP服务器设置并转到IPv4，然后选择Scope和Scope选项>更多操作 >配置选项并启用选项43



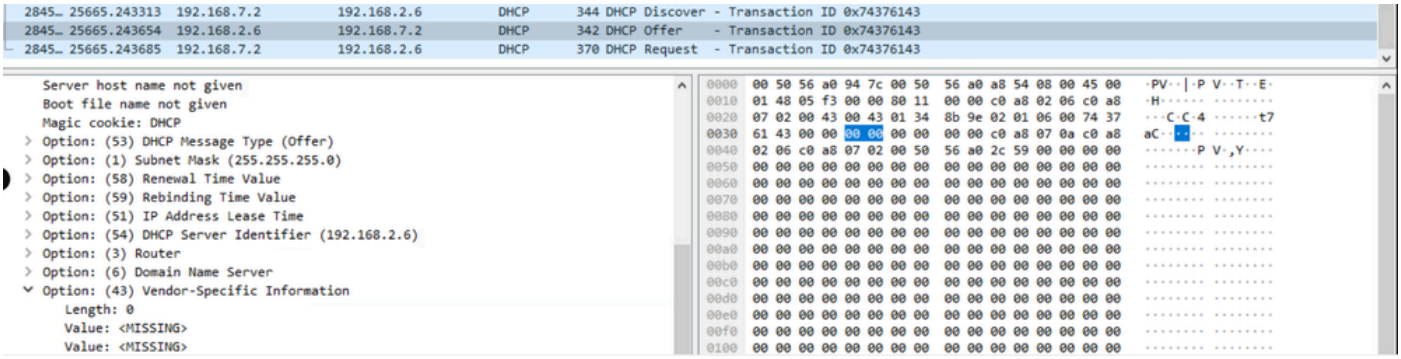
Enable_Option_43_On _External_DHCP_Server

最初，默认设置将值留空，导致FTD丢弃数据包并将其分类为格式不正确。



Default_Config_Of_Option_43

从使用Wireshark的服务器端，我们发现，在OFFER数据包中，当长度为0时，没有选项43的值。



Non_Working_Server_Side_cap

这些数据包被Cisco Firepower威胁防御(FTD)丢弃，因为它们长度为0，被视为格式错误，违反了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
DHCP: 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.

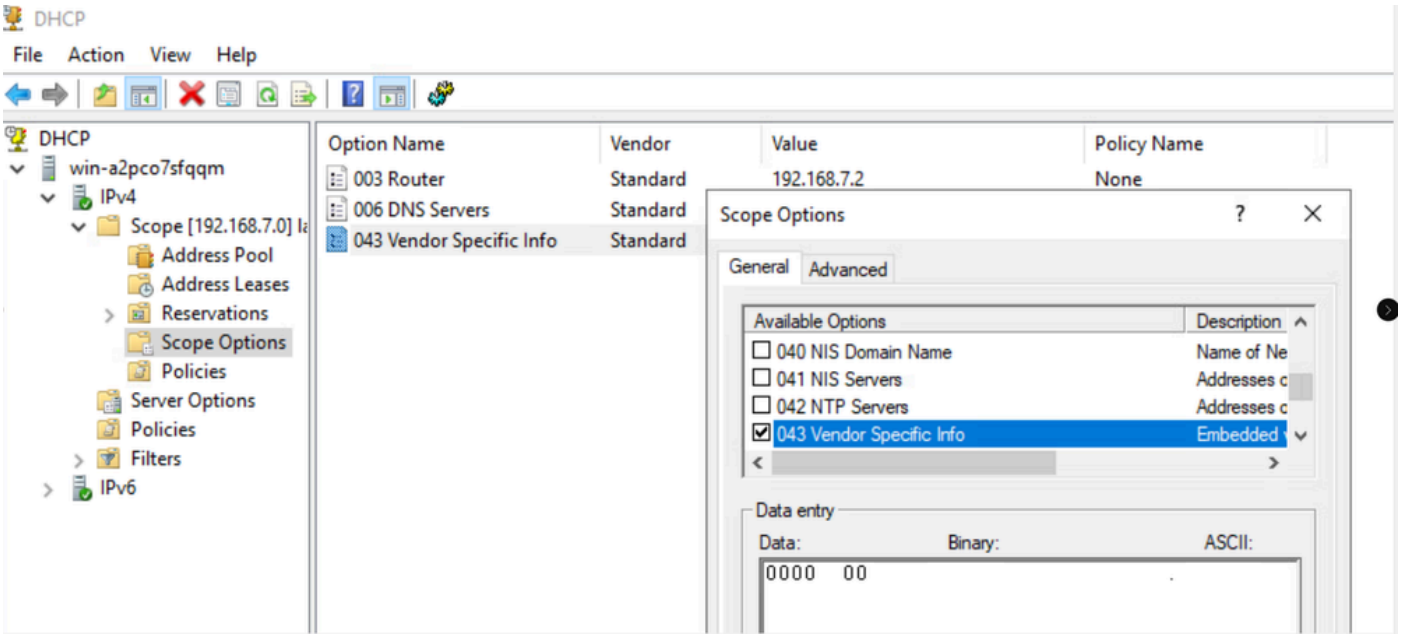
DHCPD/RA: option 43 is malformed.

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.

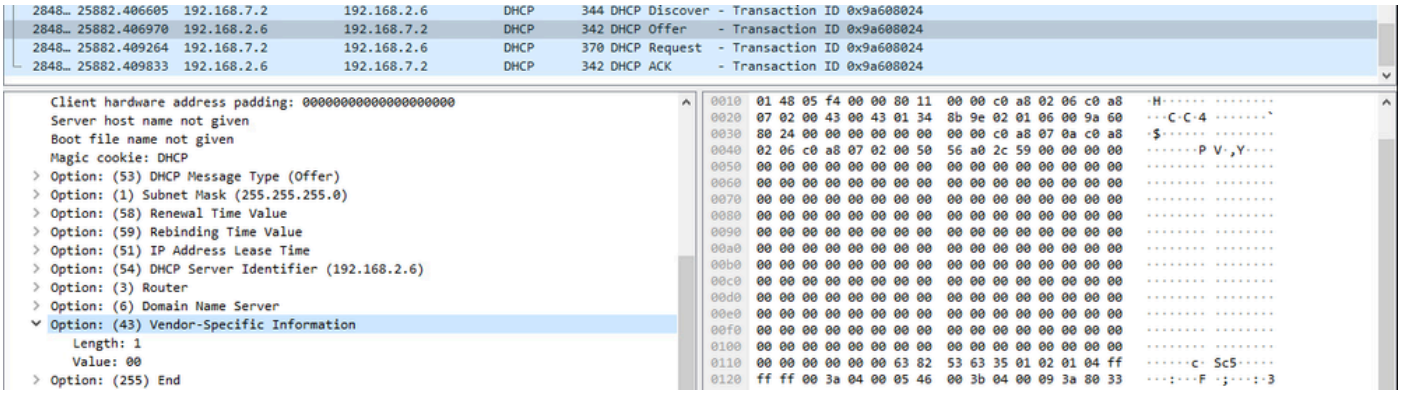
要根据RFC 2132将二进制值调整为大于0，请双击043 Vendor Specific Info字段并将值设置为00，如图所示。

此更改可确保将IP地址成功租借给客户端。



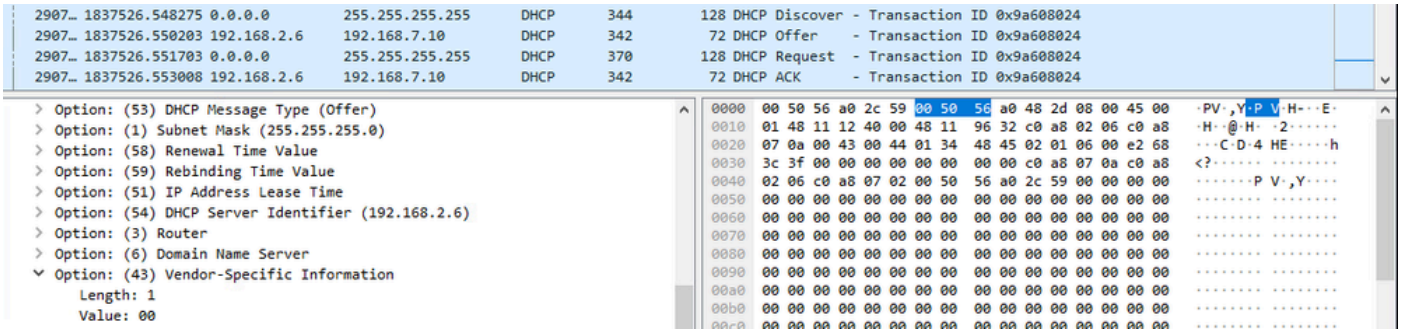
已更改_二进制值_to_1

当选项43上的值设置为1时，服务器端DORA进程



服务器端_工作_pcap

当选项43上的值设置为1时，客户端DORA进程，我们可以看到客户端使用IP租用。



客户端_工作_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

验证

在设置DHCP服务器或中继之前，请确保FTD已向FMC注册。此外，在DHCP中继配置中验证是否存在与DHCP服务器的连接。

<#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
```

从FTD CLI检验DHCP中继代理配置。

```
<#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
```

故障排除

要解决此问题，请考虑以下几点：
1.检验FTD和DHCP服务器之间的路由，确保可以从DHCP服务器访问它。
2.确保DHCP服务器具有访问DHCP中继代理接口的路由。
3.要解决客户端无法接收IP地址的问题，您可以在FTD路由接口上执行数据包捕获。

这将允许您检查数据包捕获中的DHCP服务器的DORA进程。

您可以使用Use Firepower Threat Defense Captures和Packet Tracer有效地执行数据包捕获。

要停止和删除之前启动的特定数据包捕获会话，请执行以下命令。
no capture <capture_name>

4.要查看状态和收集dhcprelay debug，请执行以下命令

为此，请登录FTD CLI 。

```
<#root>
system support diagnostic-cli


enable
```

按 Enter。

<#root>

show dhcprelay statistic

show dhcprelay state

要检查调试是否已启用，请执行以下命令。

<#root>

show debug

<#root>

To capture debug excute below commands

debug dhcprelay packet
debug dhcprelay event

<#root>

To disable debug

undebug all

相关信息

使用FMC在FTD上配置DHCP服务器和中继

DHCP和DDNS

技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。