在FTD上配置Anyconnect VPN客户端：用于地址分配的DHCP服务器

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 步骤1.在DHCP服务器中配置DHCP范围
- 步骤2.配置Anyconnect
  - 步骤2.1.配置连接配置文件
  - 步骤2.2.配置组策略
  - 步骤2.3.配置地址分配策略

IP帮助程序场景

验证

故障排除

相关信息

简介

本文档提供版本6.4上的Firepower威胁防御(FTD)配置示例，允许远程访问VPN会话获取第三方动态主机配置协议(DHCP)服务器分配的IP地址。

先决条件

要求

Cisco 建议您了解以下主题：

- FTD
- Firepower管理中心(FMC)。
- DHCP

使用的组件

本文档中的信息基于以下软件版本：

- FMC 6.5
- FTD 6.5
- Windows Server 2016

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

本文档不会描述整个远程访问配置，而只是在FTD中从本地地址池更改为DHCP地址分配所需的配置。

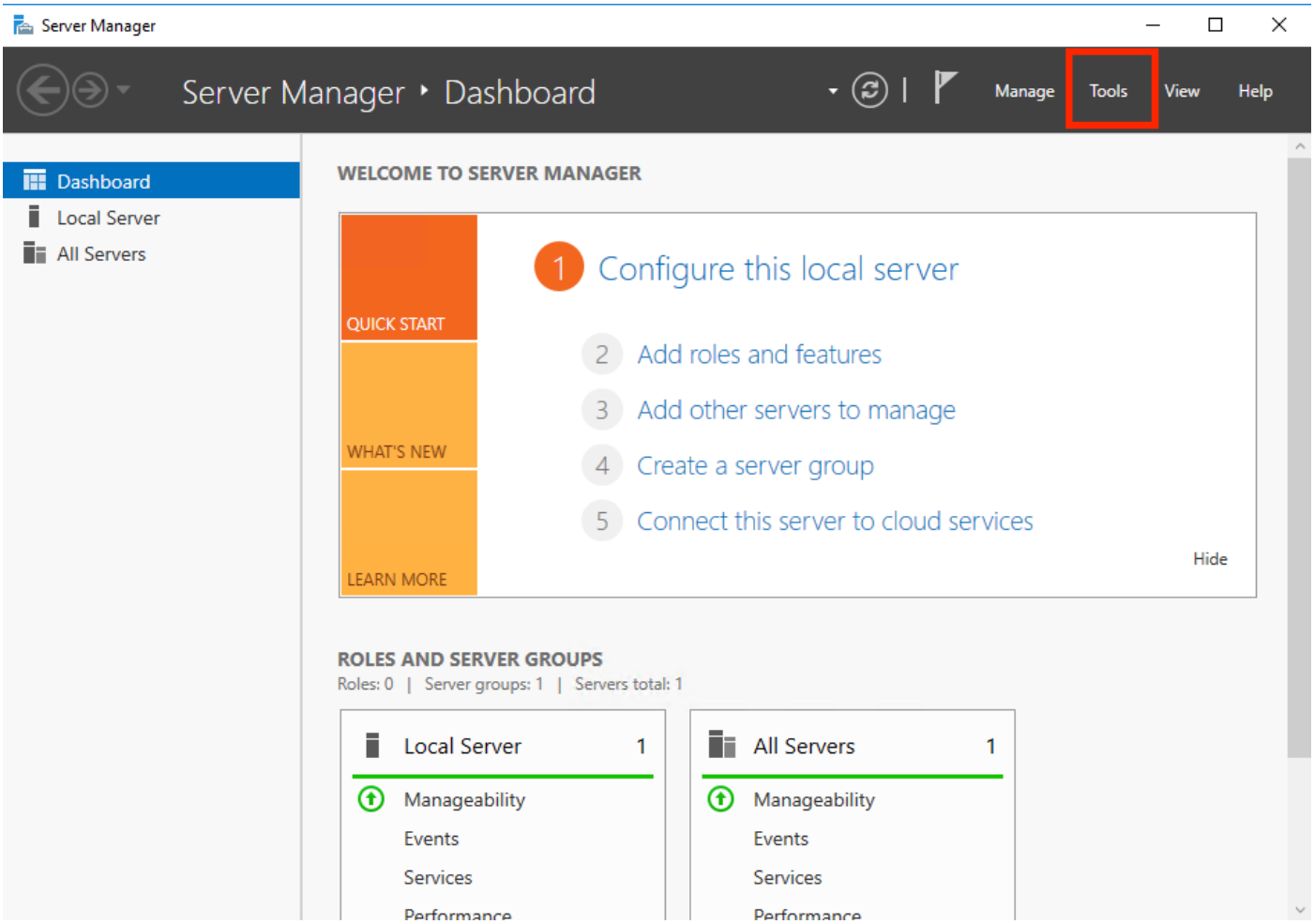
如果您正在查找Anyconnect配置示例文档，请参阅“在FTD上配置AnyConnect VPN客户端：Hairpining and NAT Exemption”文档。

配置

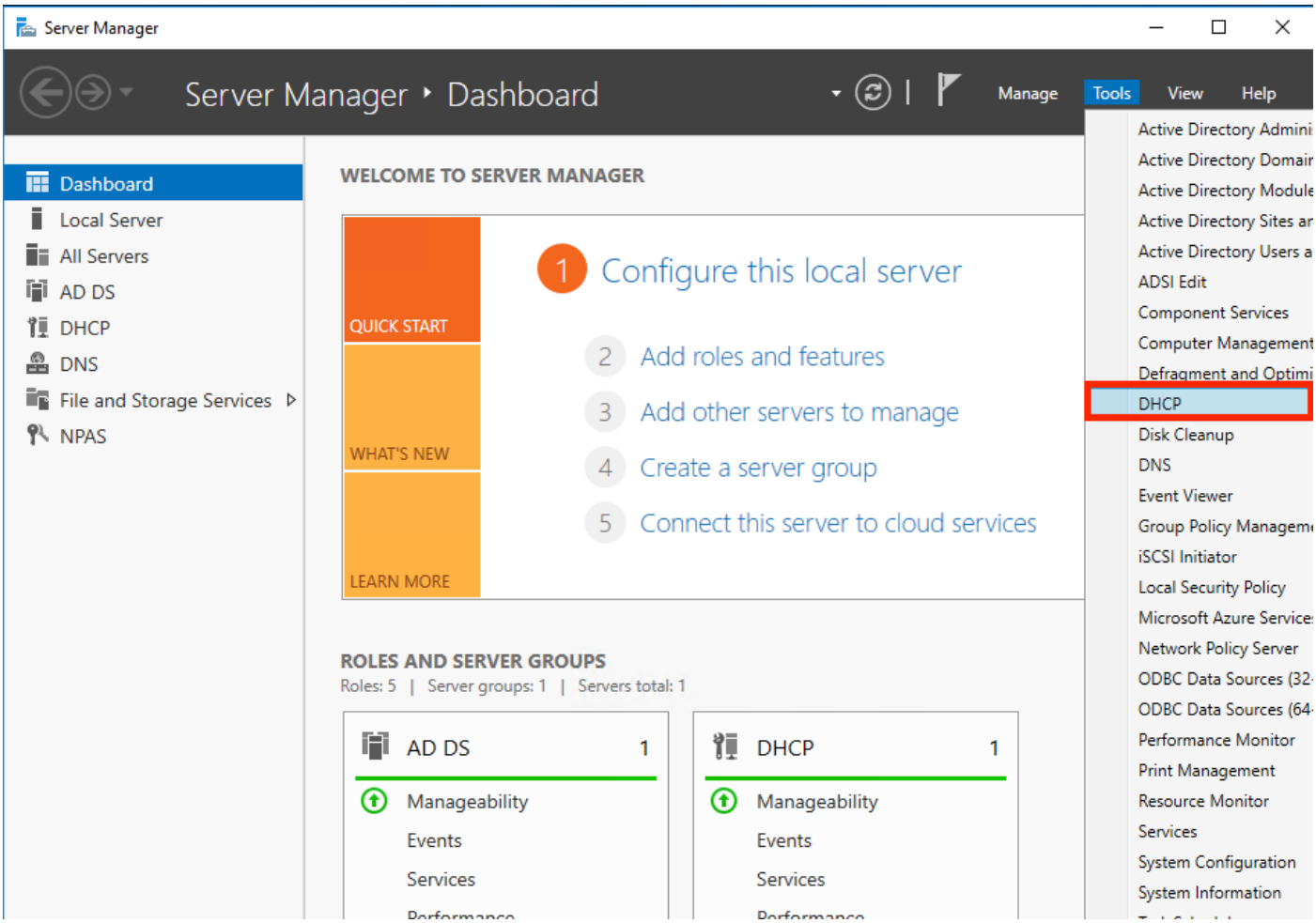
步骤1.在DHCP服务器中配置DHCP范围

在此场景中，DHCP服务器位于FTD的内部接口后面。

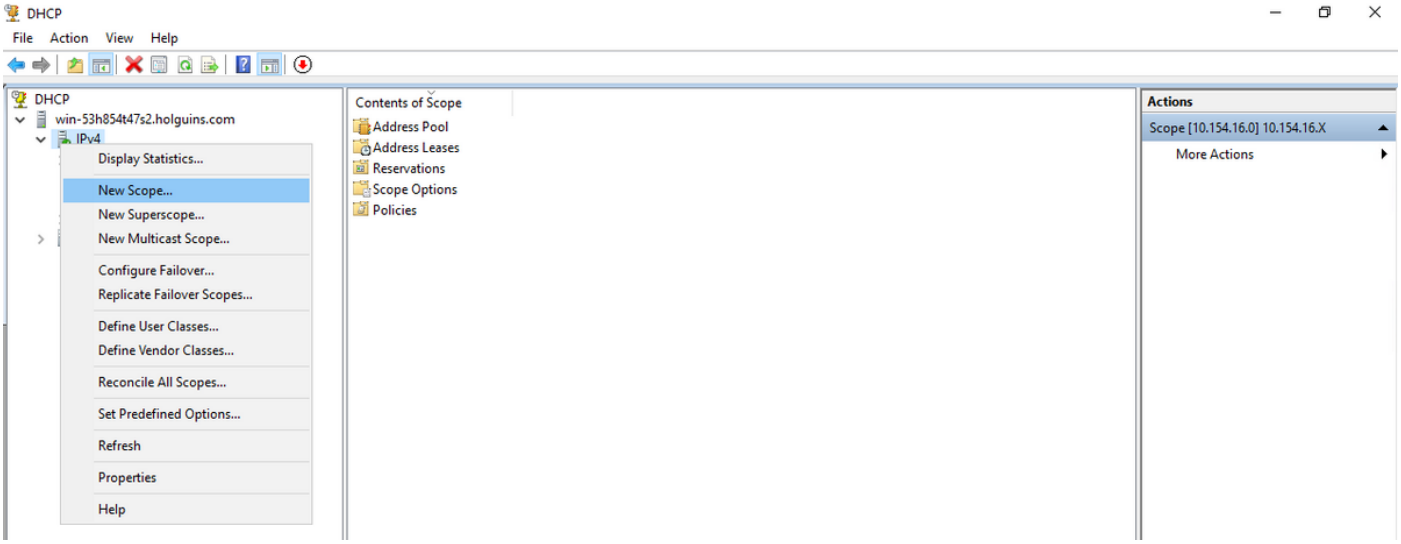
1.在Windows Server中打开“服务器管理器”，然后选择工具，如图所示。



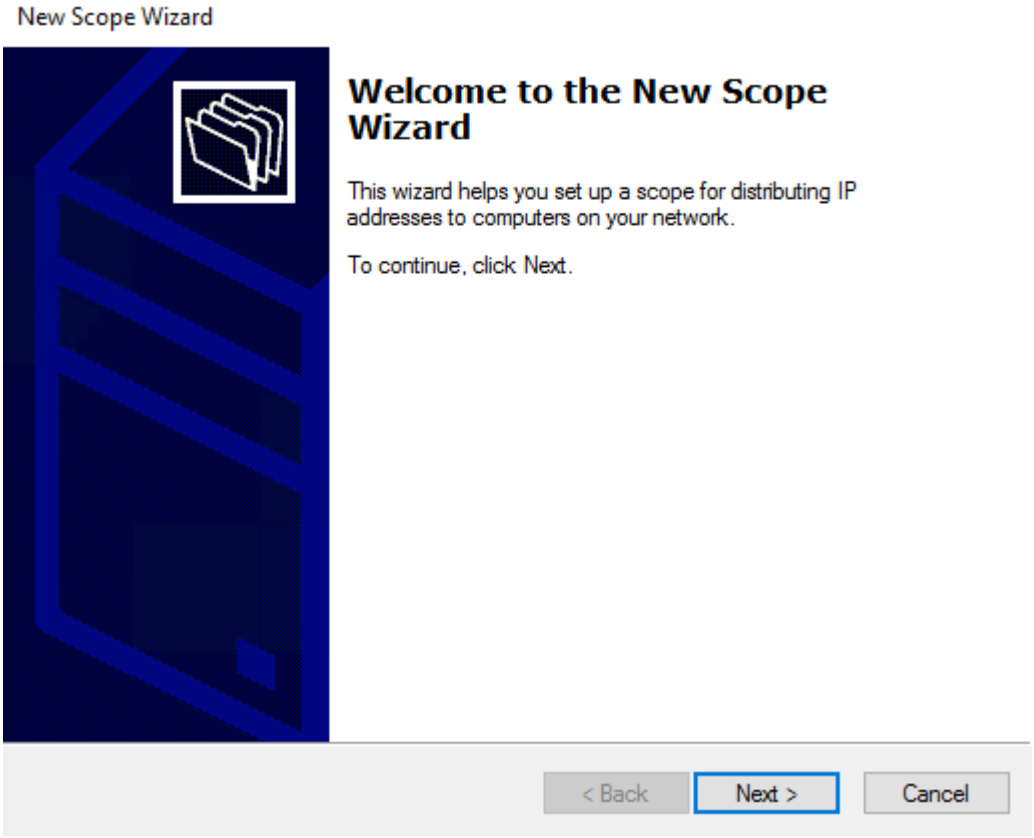
2.选择DHCP:



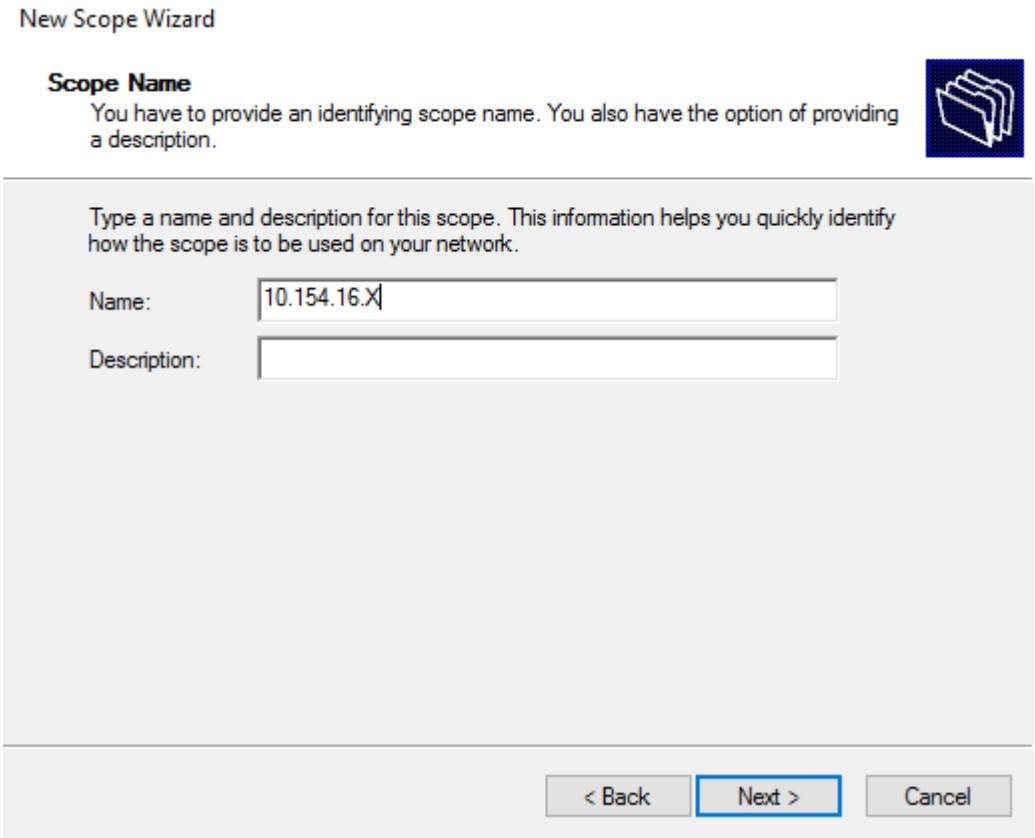
3.选择IPv4，右键单击并选择New Scope，如图所示。



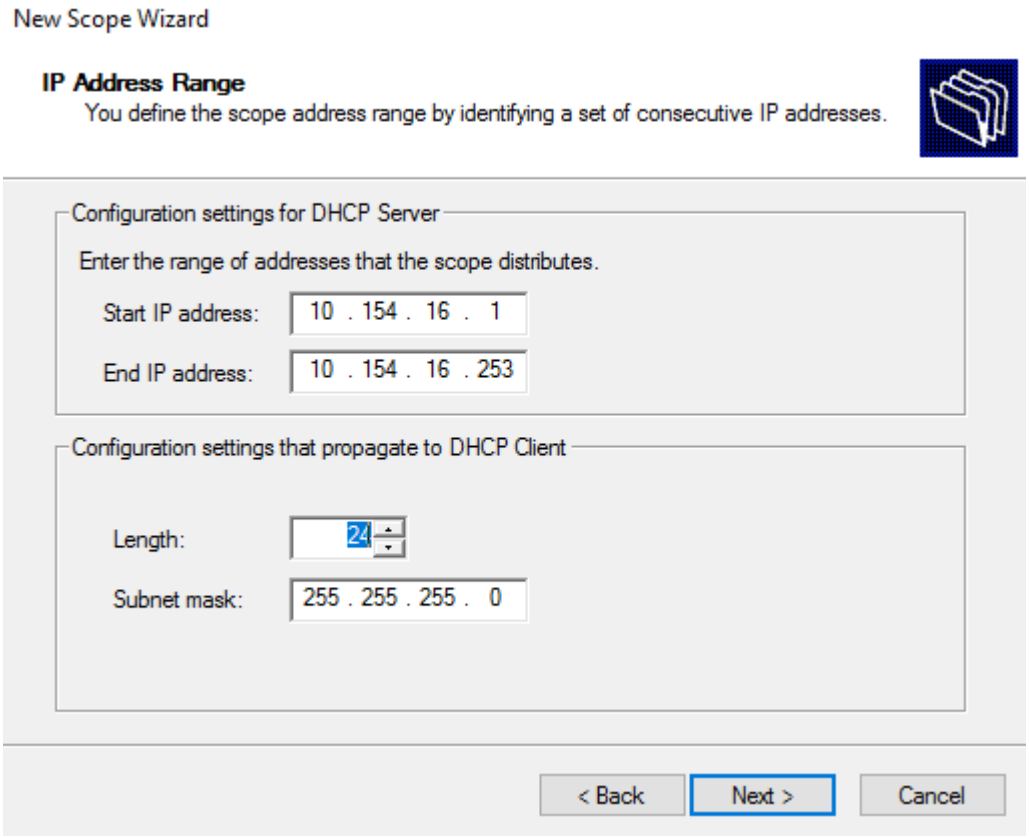
4.按照向导执行操作，如图所示。



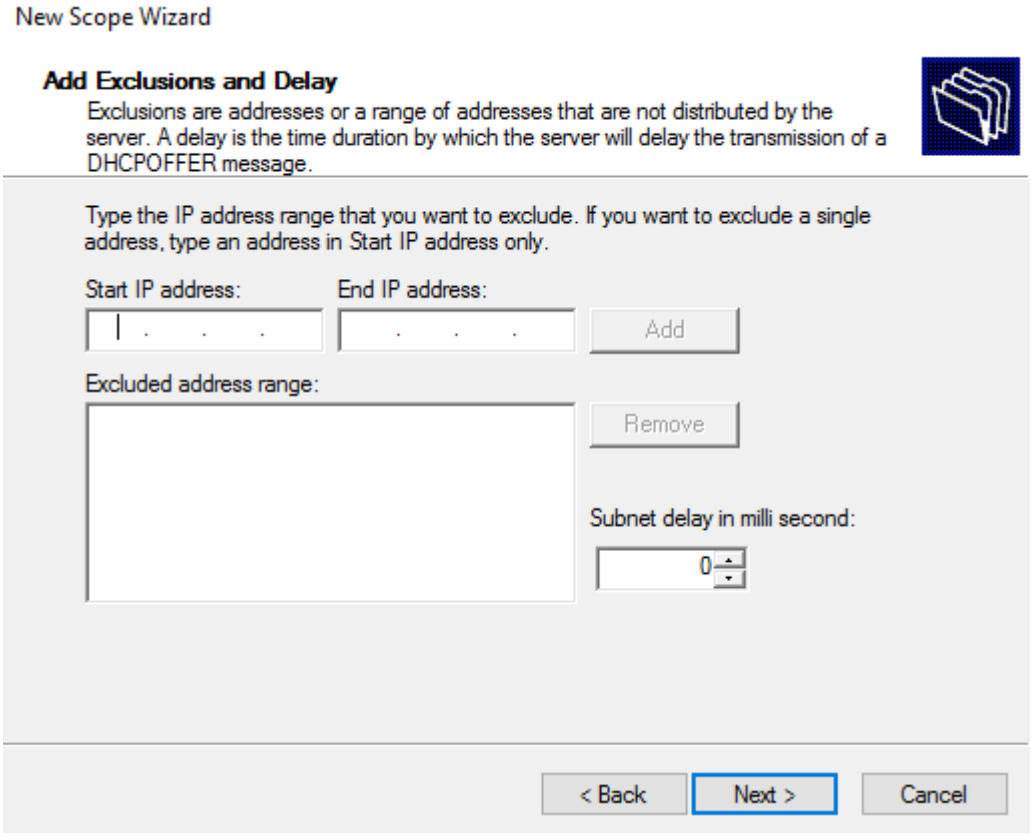
5.如图所示为范围分配名称。



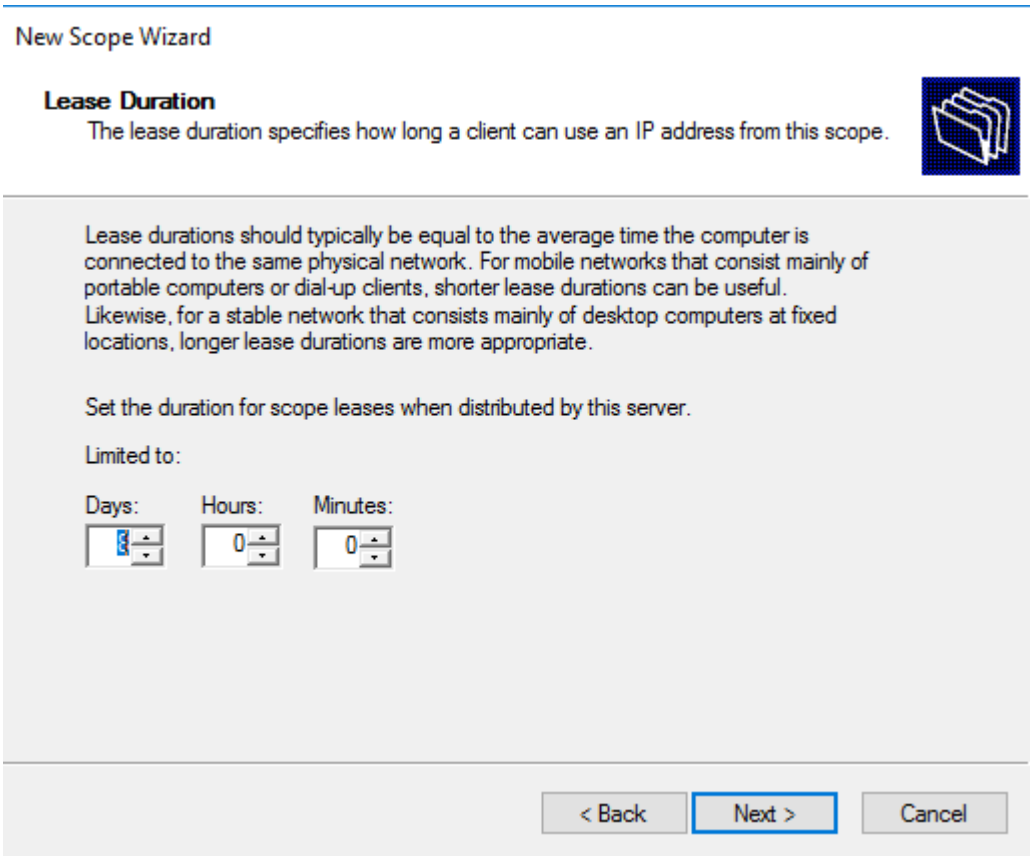
6.如图所示配置地址范围。



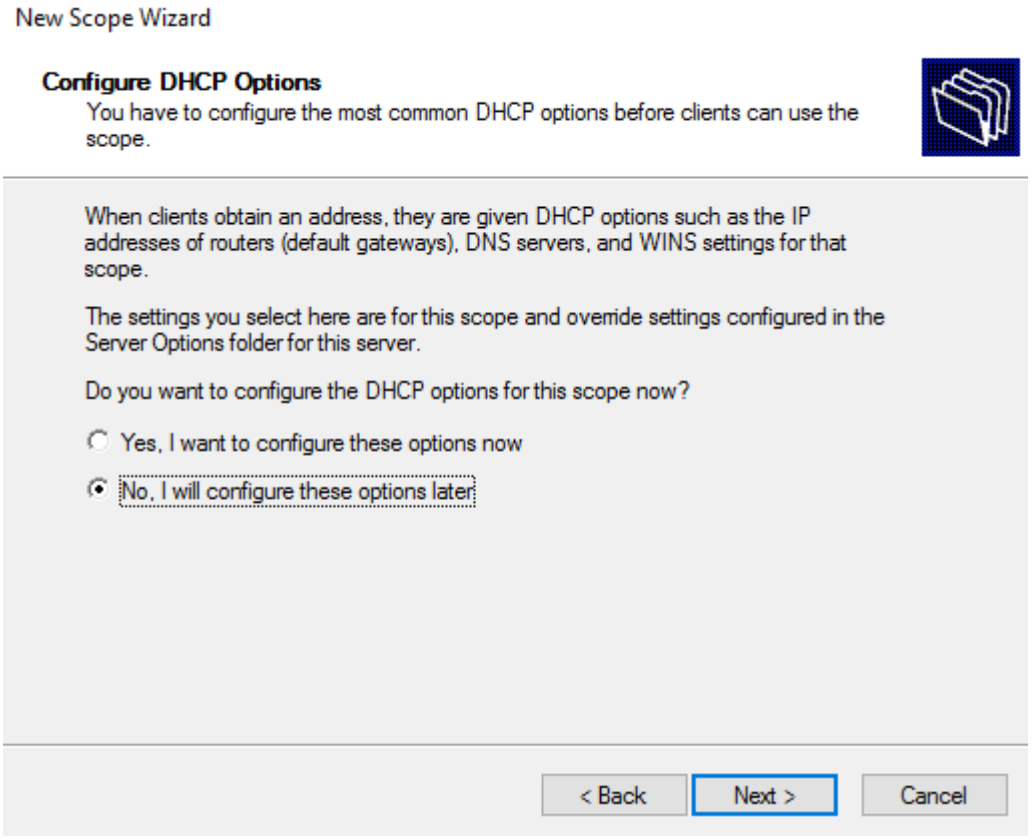
7.（可选）如图所示配置例外项。



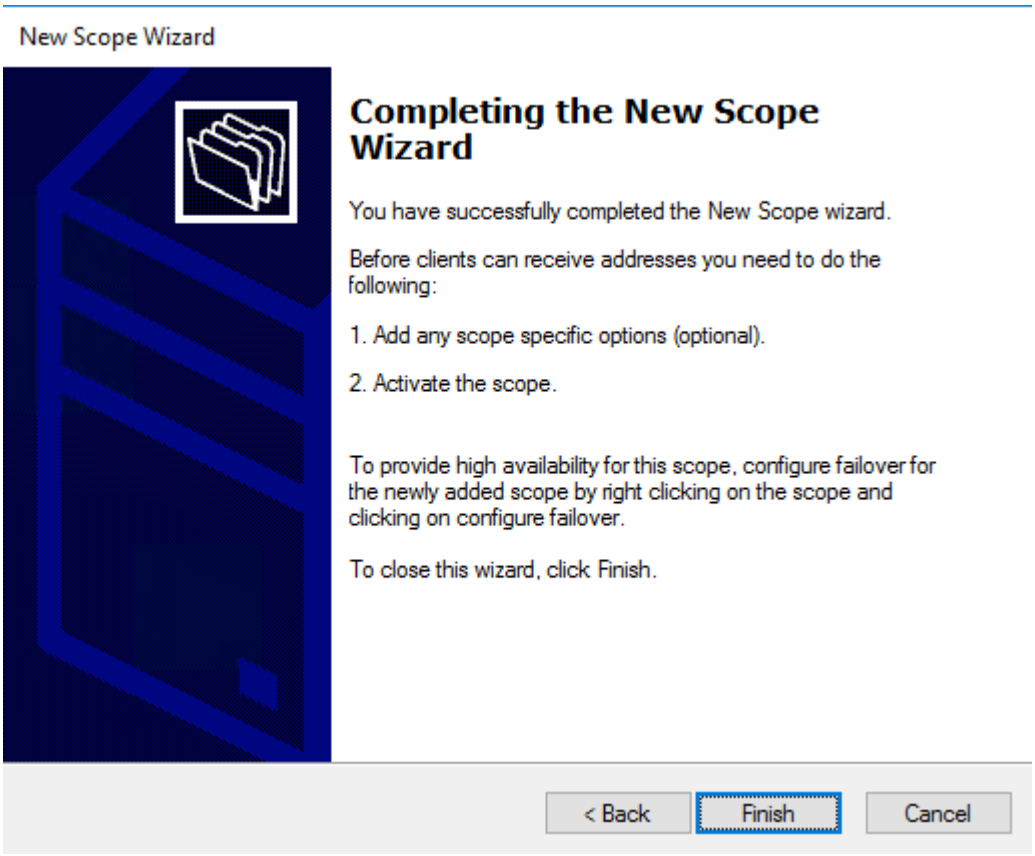
8.配置租用期限，如图所示。



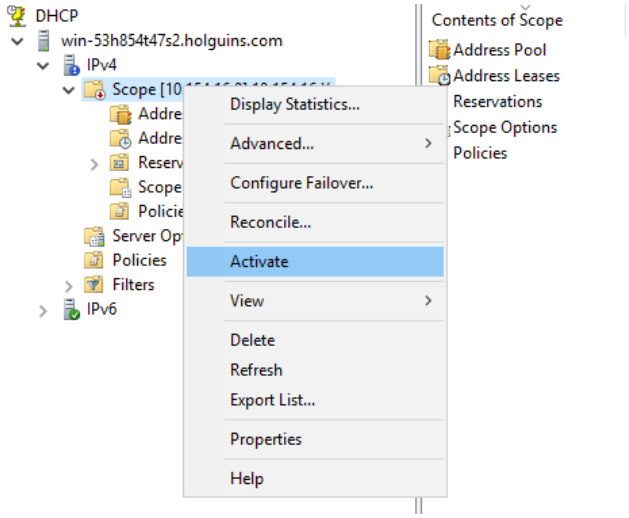
9.（可选）配置DHCP作用域选项：



10:选择完成，如图所示。



11:在刚创建的范围内右键单击，然后选择激活，如图所示。



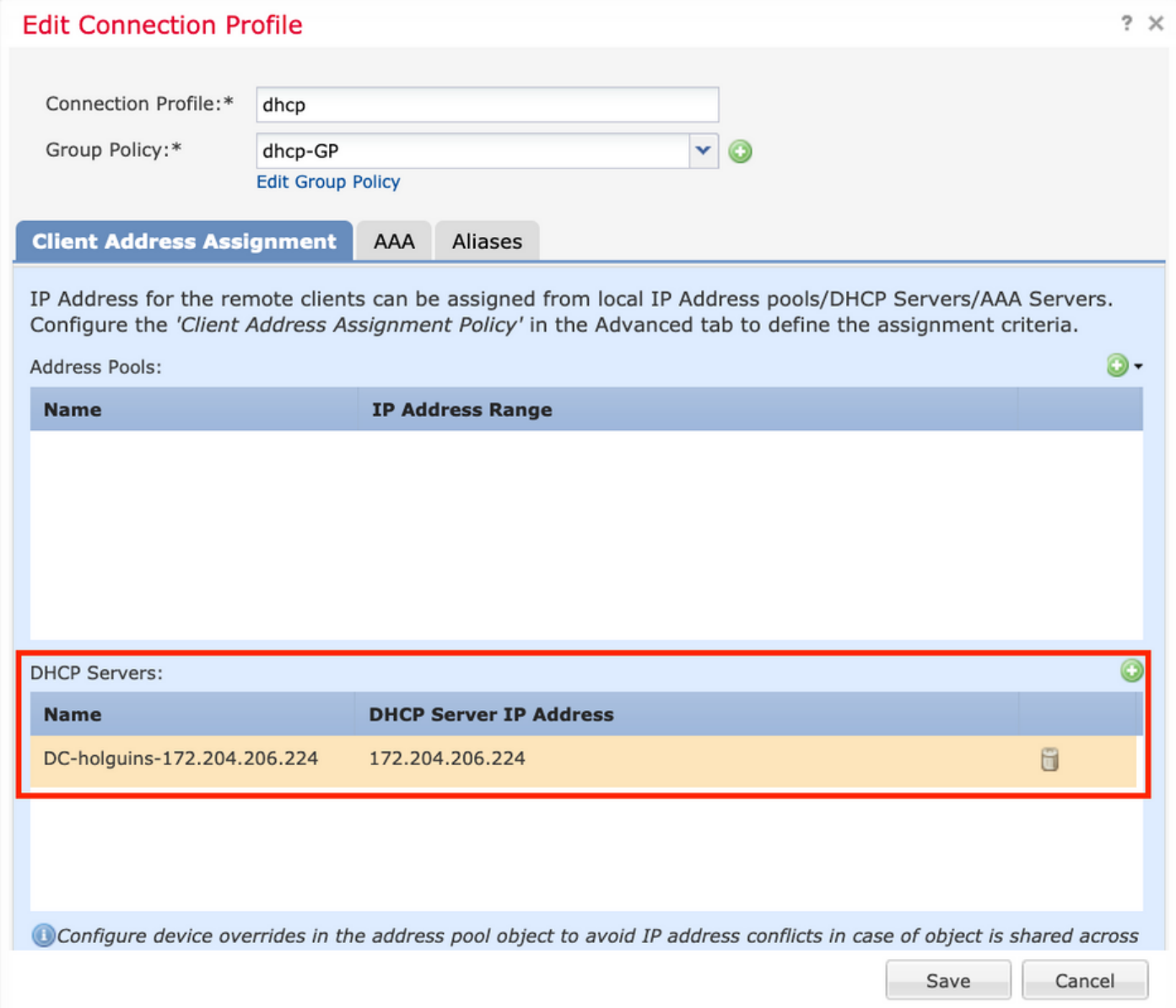
步骤2.配置Anyconnect

配置并激活DHCP作用域后，下一个过程将在FMC中进行。

步骤2.1.配置连接配置文件

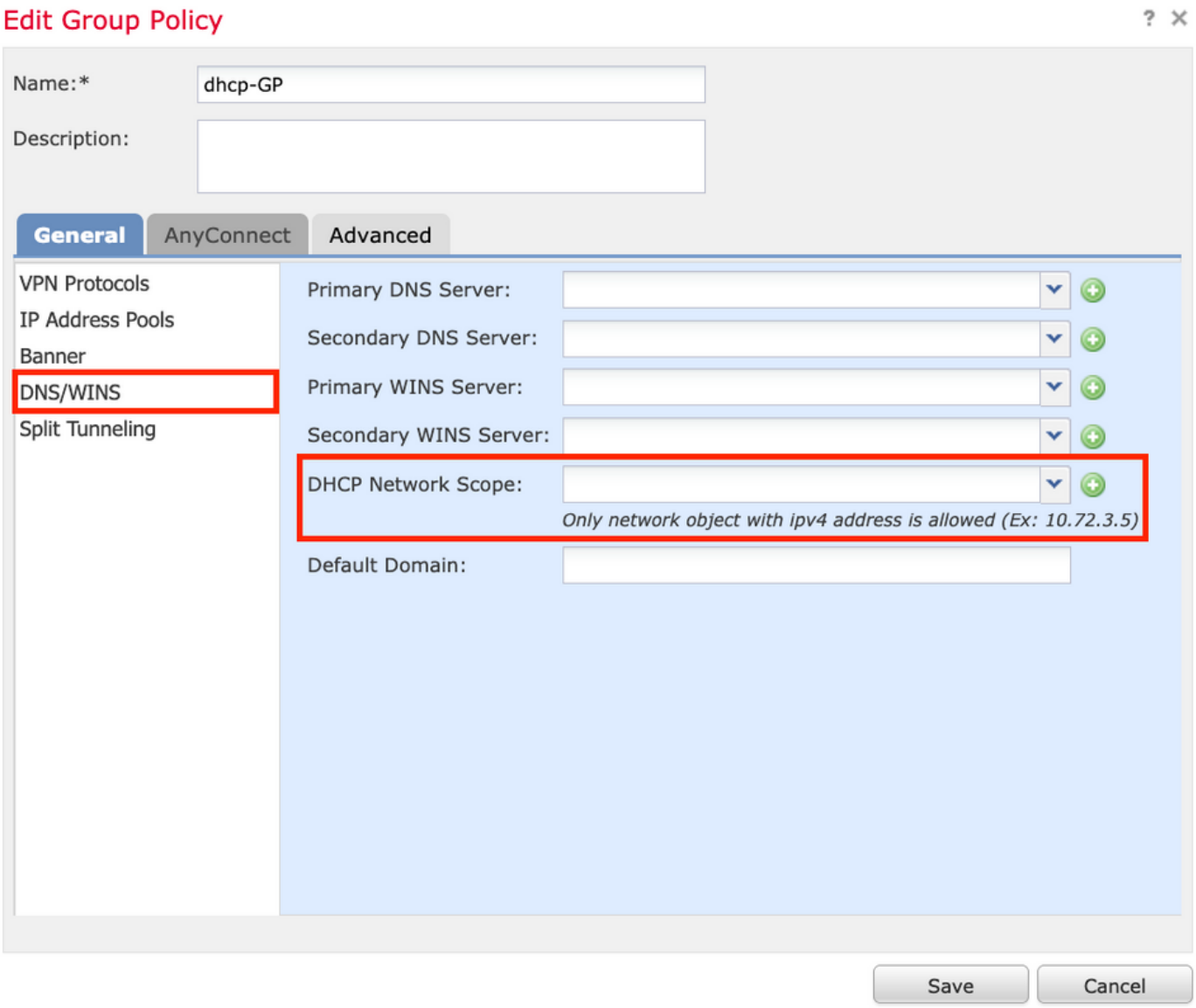
1.在DHCP Servers部分，选择  符号并使用DHCP服务器的IP地址创建一个对象。

2.选择对象作为DHCP服务器，以便从中请求IP地址，如图所示。



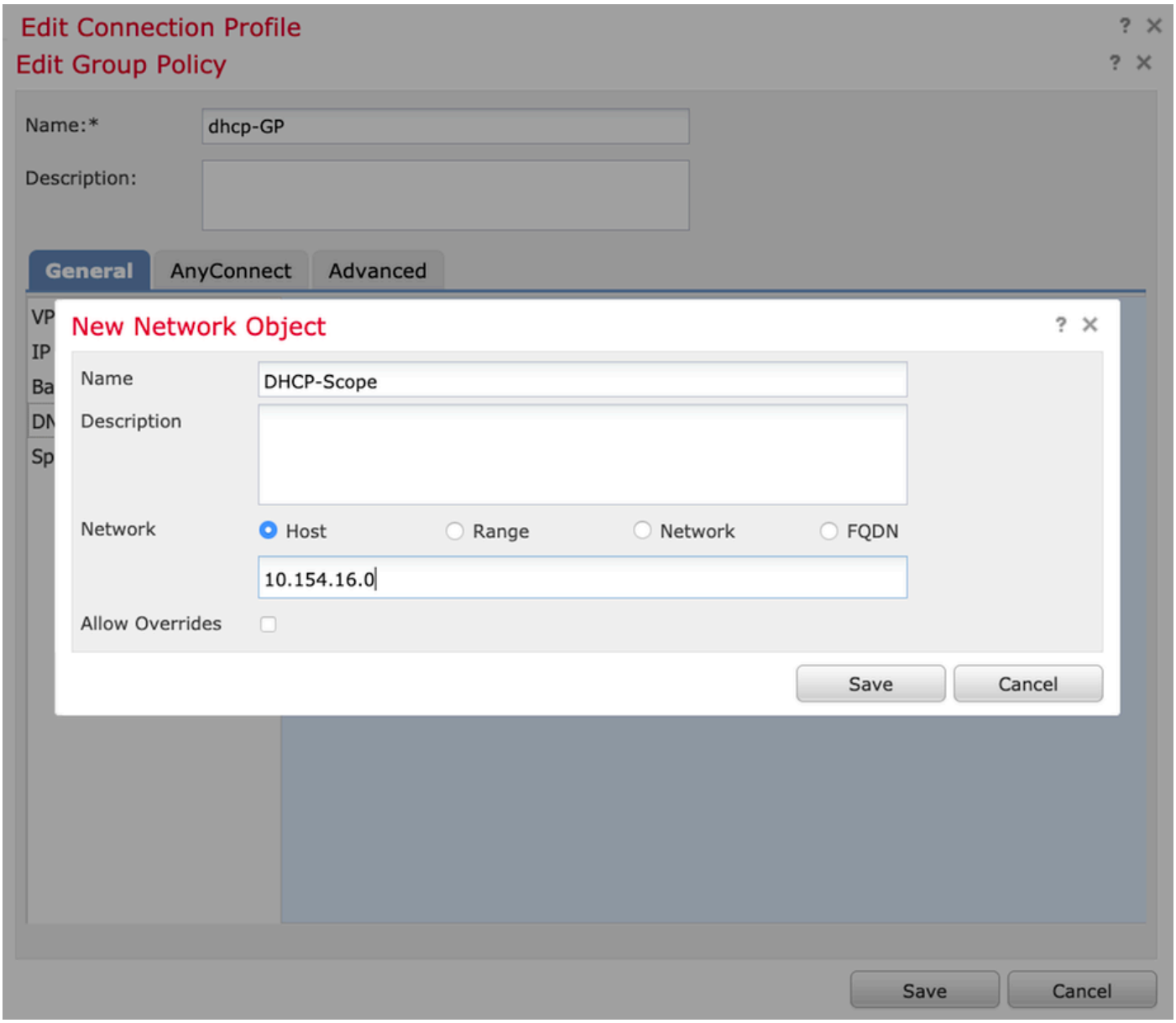
步骤2.2.配置组策略

1.在Group Policy菜单内，导航到General > DNS/WINS，有一个DHCP Network Scope部分，如图所示。

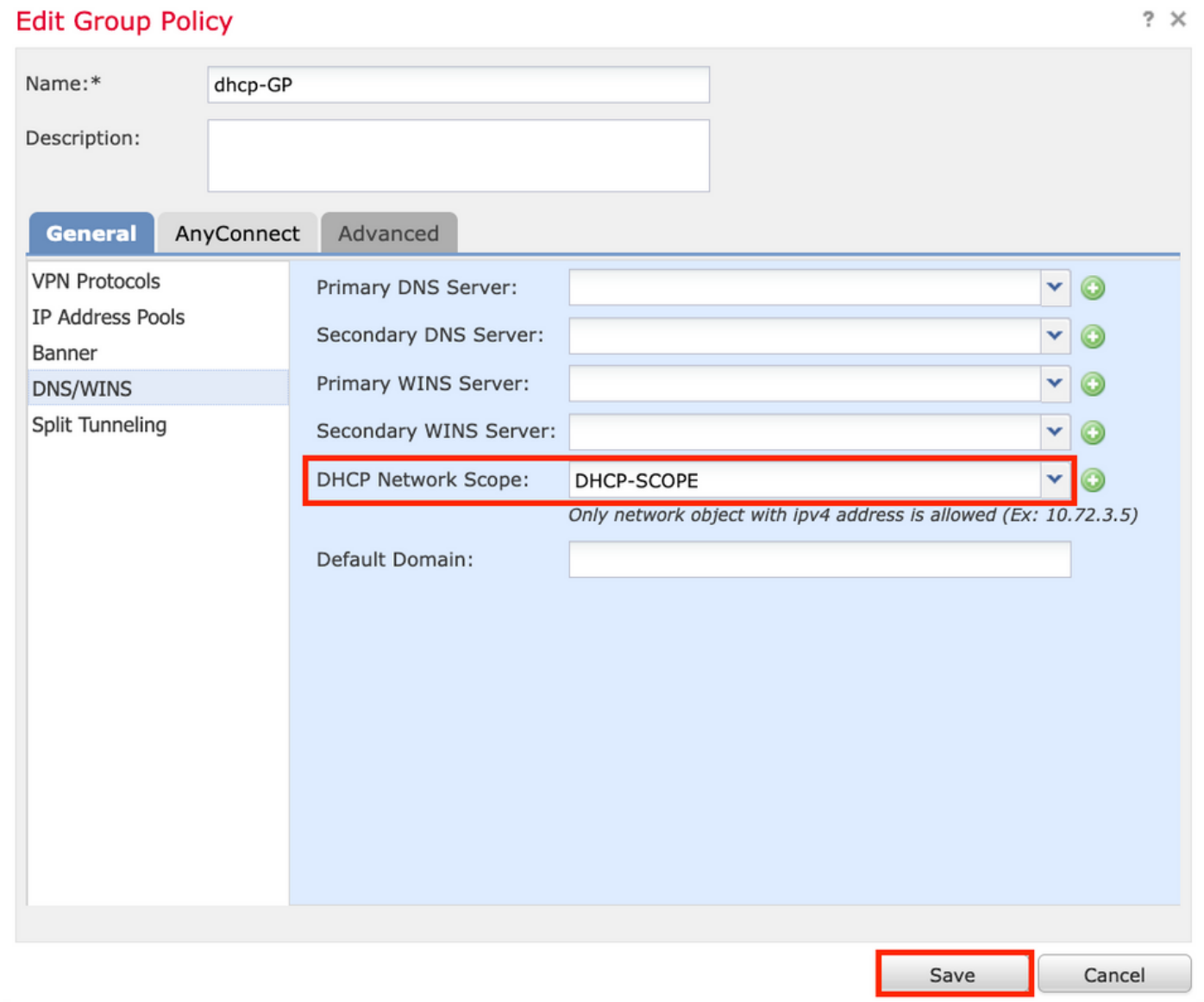


2.创建新对象，该对象必须与DHCP服务器具有相同的网络范围。

注意：这必须是主机对象，而不是子网。

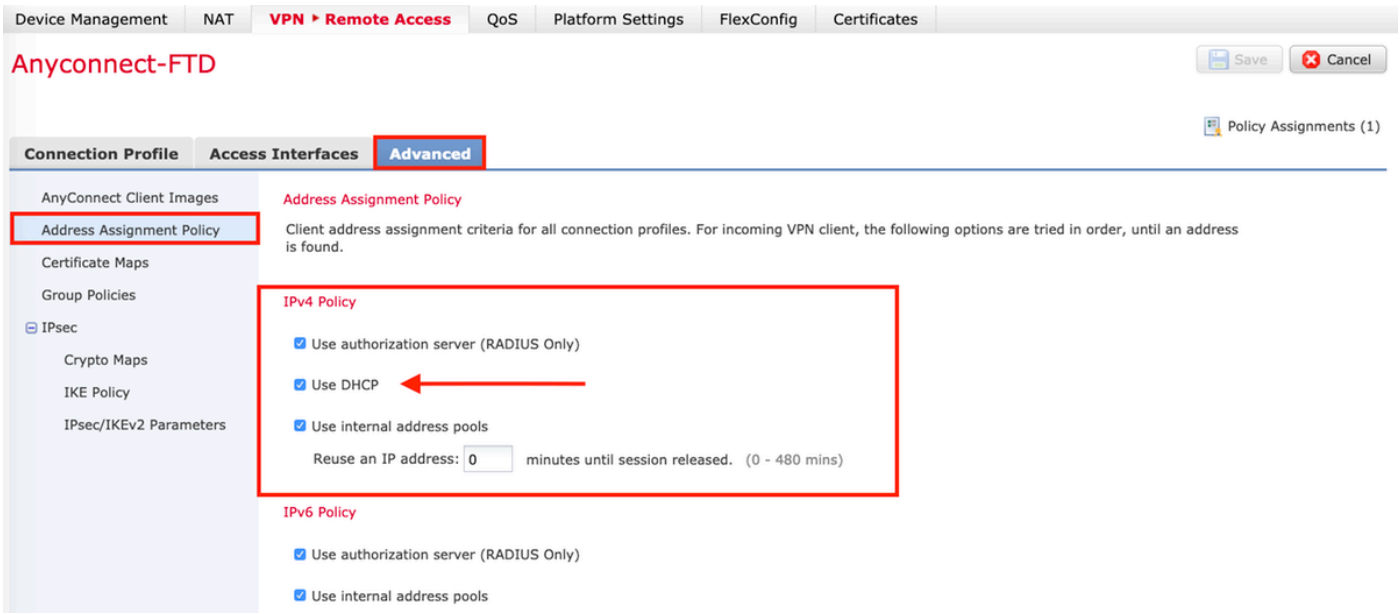


3.选择DHCP作用域对象，然后选择保存，如图所示。



步骤2.3.配置地址分配策略

1.导航到高级 > 地址分配策略，确保使用DHCP选项已切换，如图所示。

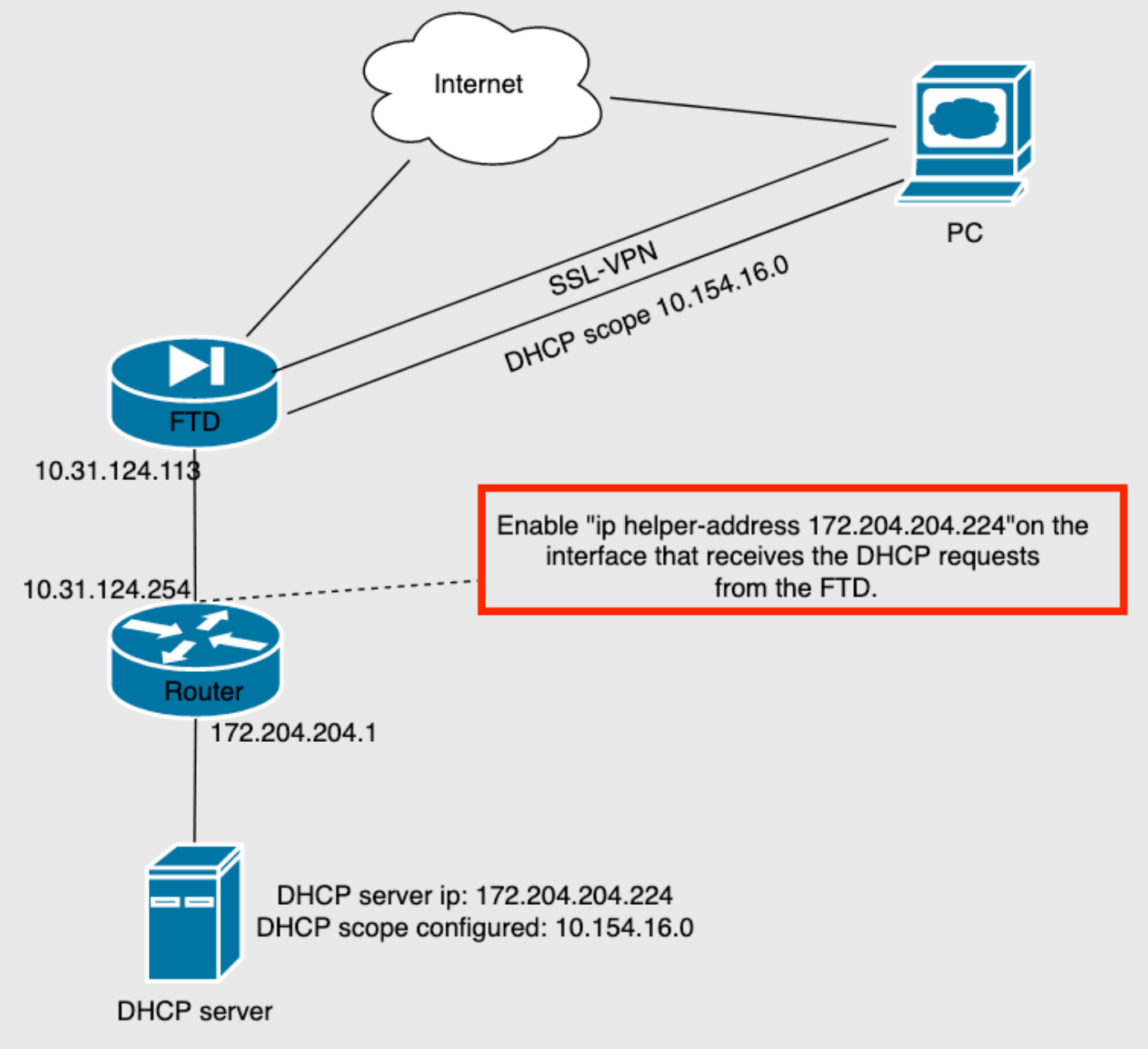


2.保存更改并部署配置。

IP帮助程序场景

当DHCP服务器位于局域网(LAN)中的另一台路由器后面时，需要使用“IP帮助程序”将请求转发到DHCP服务器。

如图所示，拓扑图说明了场景以及网络中的必要更改。

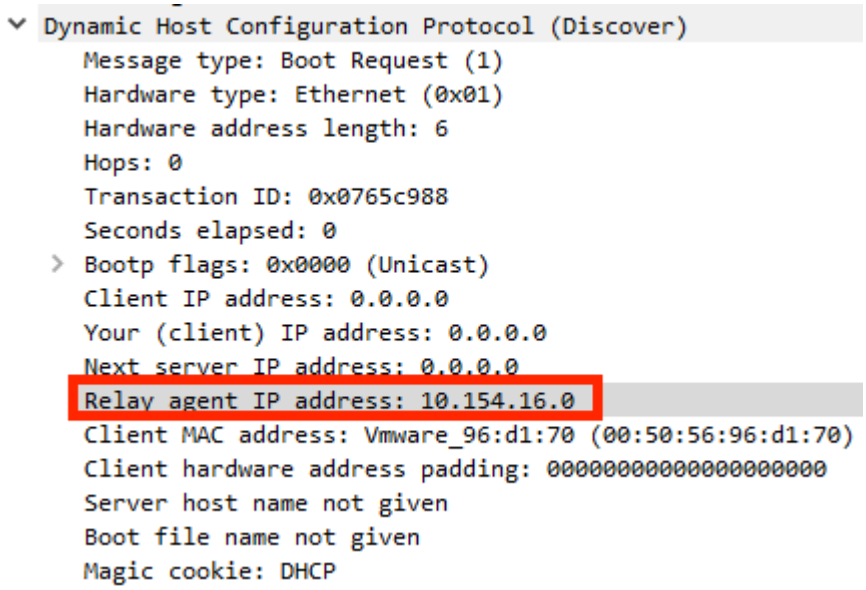


验证

使用本部分可确认配置能否正常运行。

本节介绍FTD和DHCP服务器之间交换的DHCP数据包。

- 发现：这是从FTD的内部接口发送到DHCP服务器的单播数据包。
    - 在负载中，中继代理IP地址指定DHCP服务器的范围，如图所示。



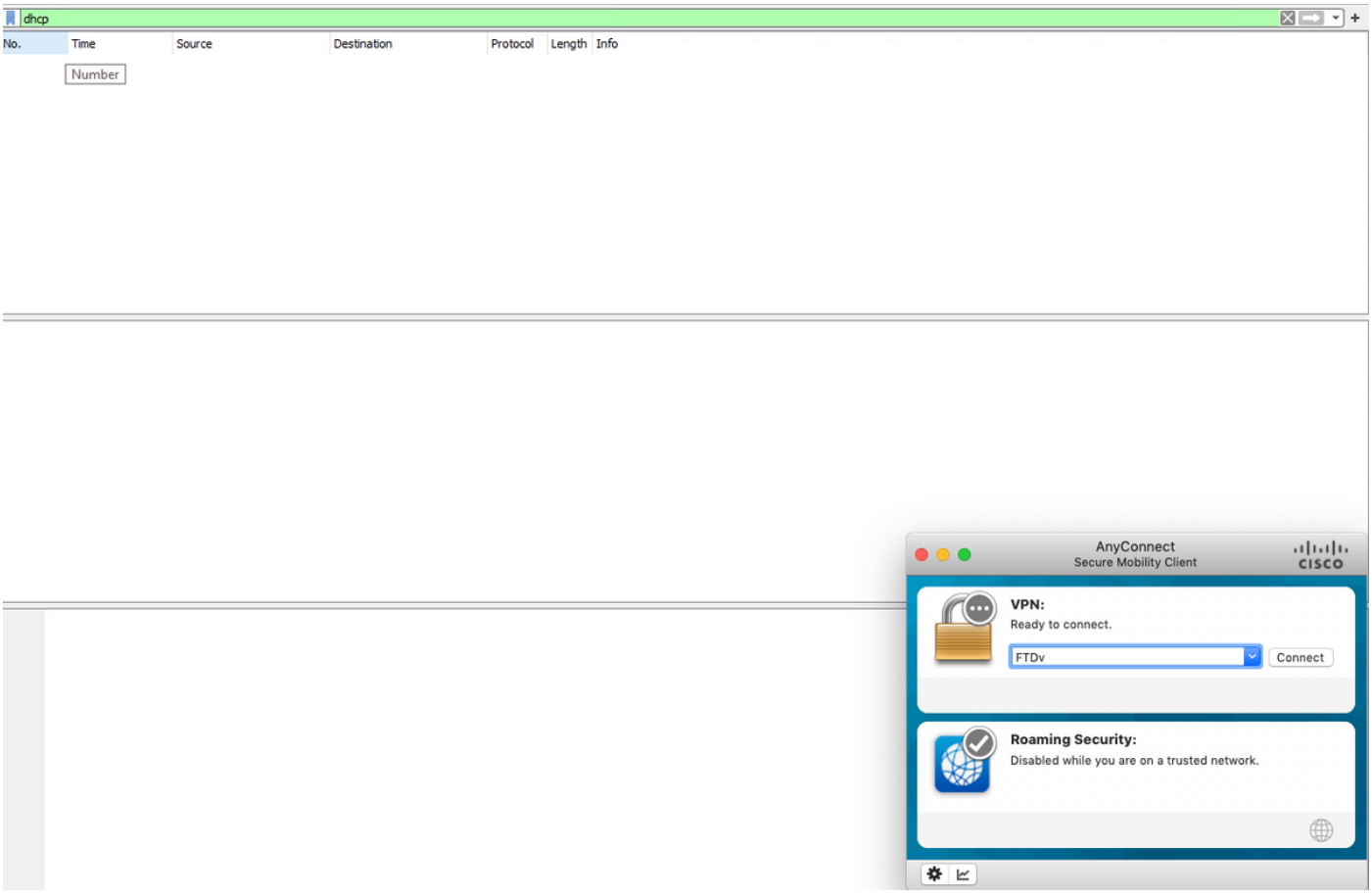
- 产品：此数据包是来自DHCP服务器的响应，它随DHCP服务器源和FTD中DHCP作用域的目标一起提供。
- 请求：这是从FTD的内部接口发送到DHCP服务器的单播数据包。
- 确认：此数据包是来自DHCP服务器的响应，它随DHCP服务器源和FTD中DHCP作用域的目标一起提供。

故障排除

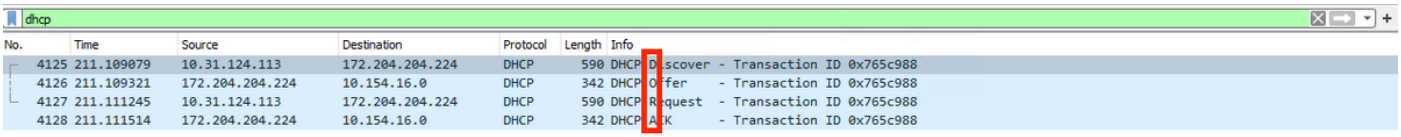
本部分提供的信息可用于对配置进行故障排除。

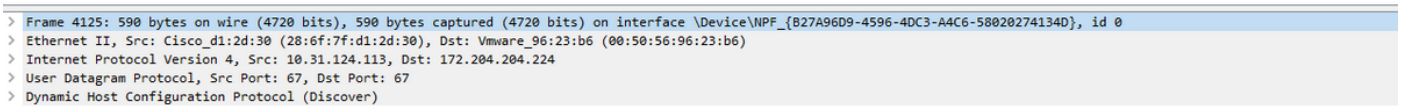
步骤1.在DHCP服务器中下载并启用wireshark。

步骤2.应用DHCP作为捕获过滤器，如图所示。



步骤3.登录到Anyconnect，DHCP协商应如图所示。







相关信息

- 此视频提供了FTD的配置示例，允许远程访问VPN会话获取由第三方DHCP服务器分配的IP地址。
- 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）。