

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Firepower威胁防御(FTD)的配置示例，该示例允许远程访问VPN会话获取由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

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

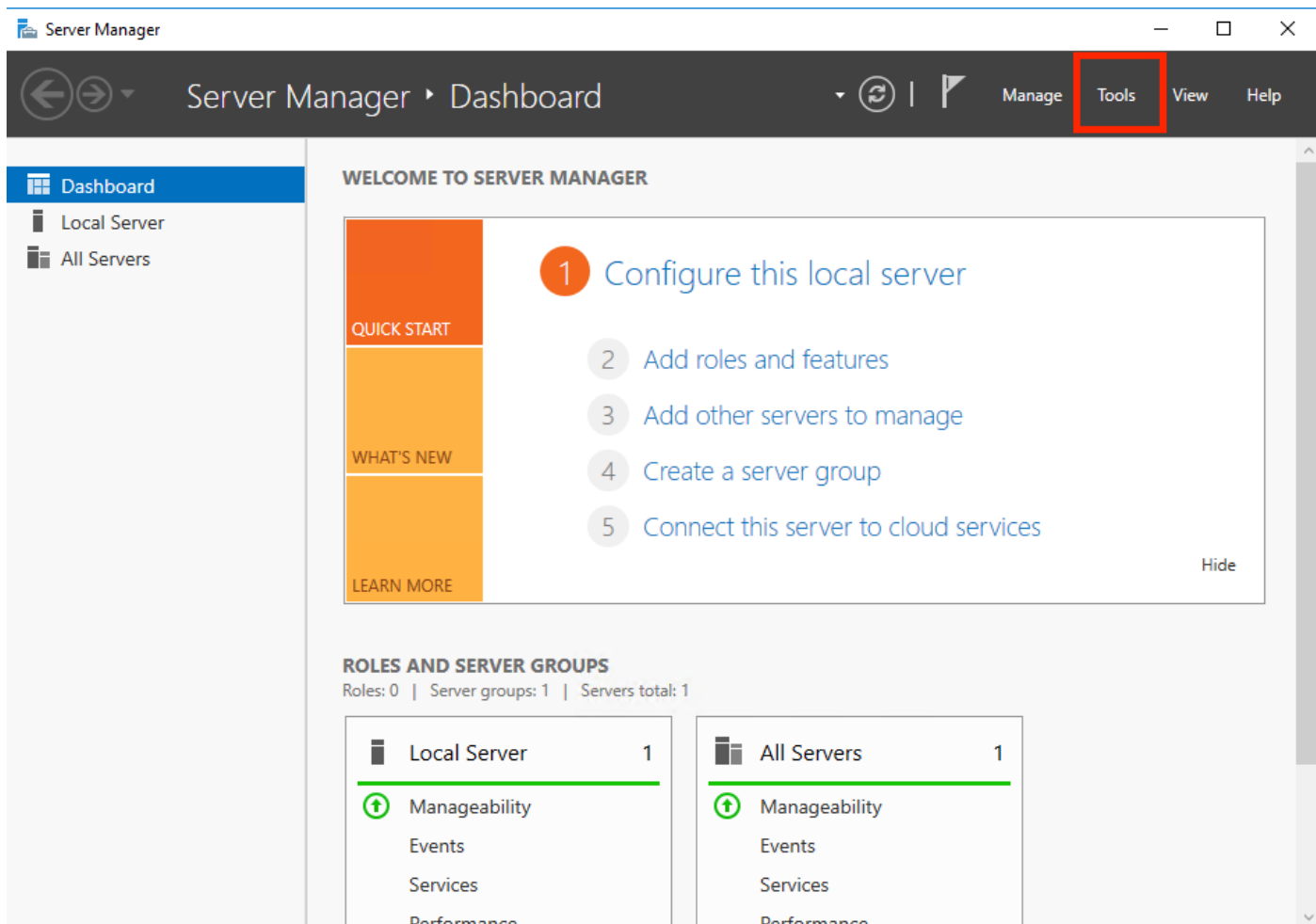
如果您正在查找AnyConnect配置示例文档，请参阅“在FTD上配置AnyConnect VPN客户端：Hairpin and NAT Exemption”文档。

配置

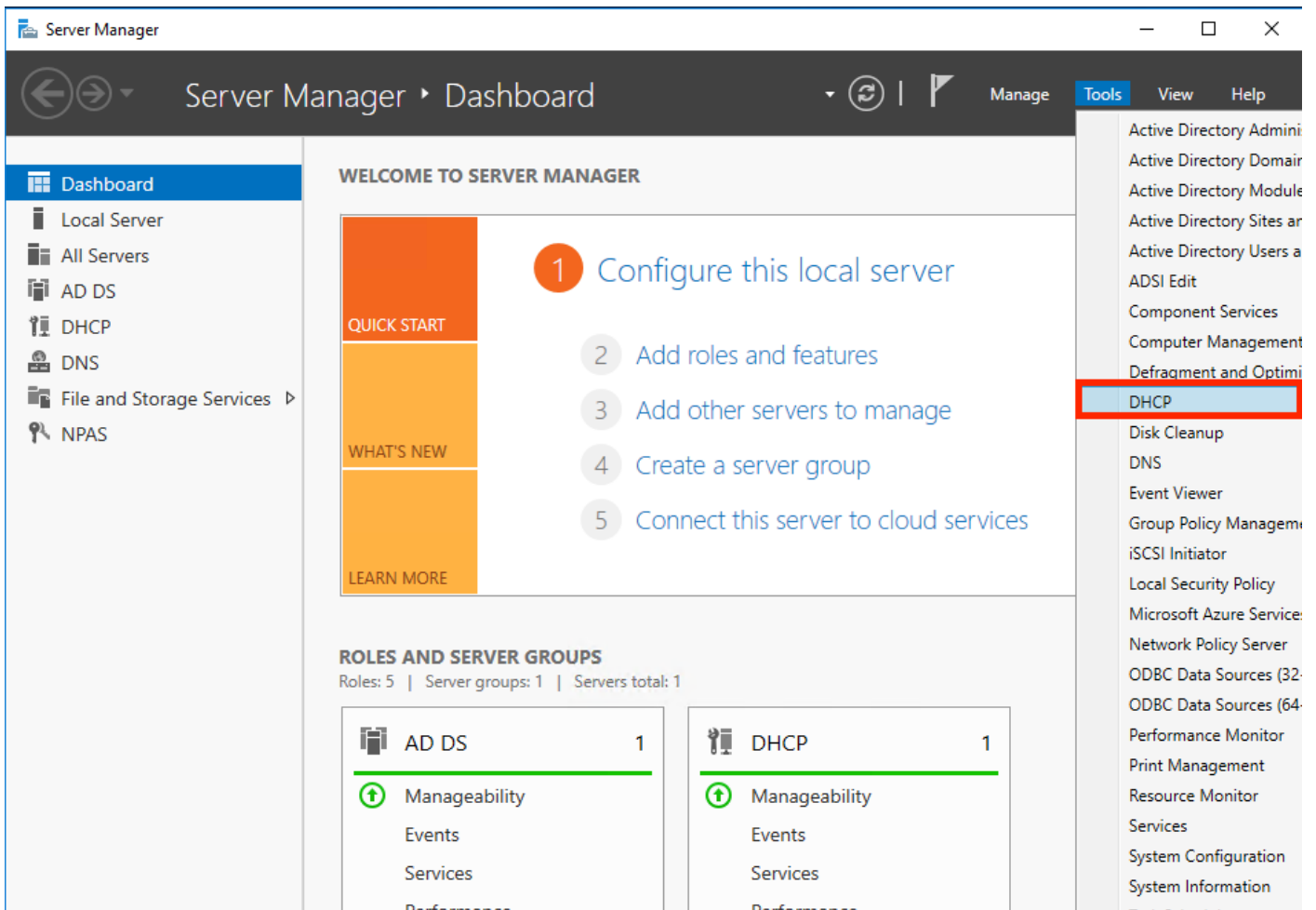
步骤1.在DHCP服务器中配置DHCP范围

在此场景中，DHCP服务器位于FTD的内部接口后面。

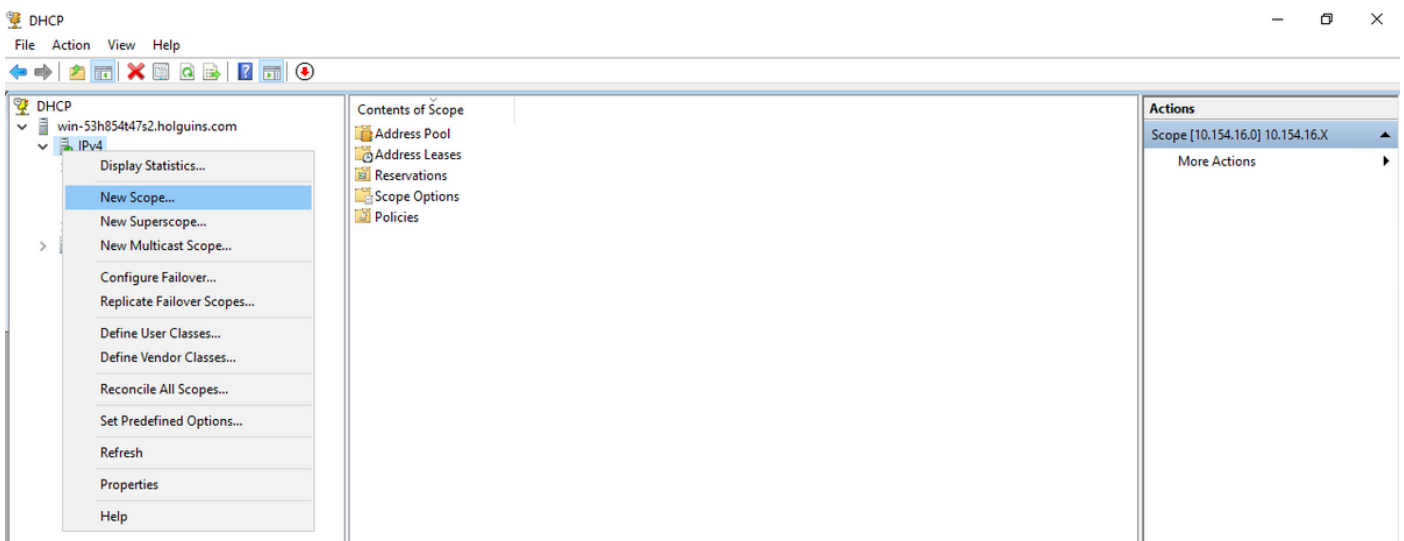
1.在Windows Server中打开Server Manager，然后选择“工具”，如图所示。



2.选择DHCP:



3.选择IPv4，右键单击它，然后选择“新建范围”，如图所示。



4.按照图像所示执行向导。



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.为范围指定名称，如图所示。

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.配置地址范围，如图所示。

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. (可选) 配置如图所示的排除项。

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.如图所示配置租用持续时间。

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. (可选) 配置DHCP范围选项 :

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

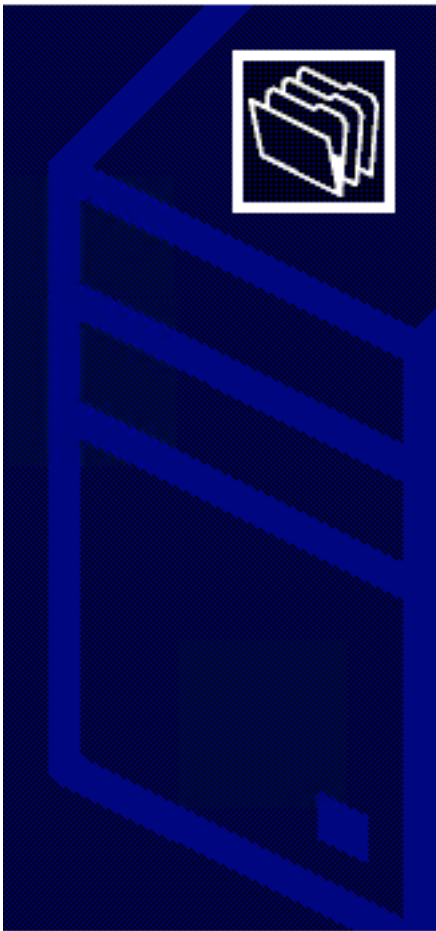
< Back

Next >

Cancel

10:选择“完成”，如图所示。

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.

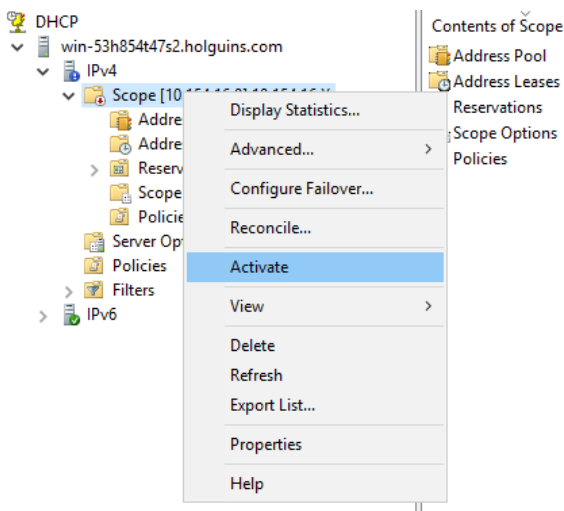
To close this wizard, click Finish.

< Back

Finish

Cancel


11:在刚创建的范围中右键单击，然后选择激活（如图所示）。



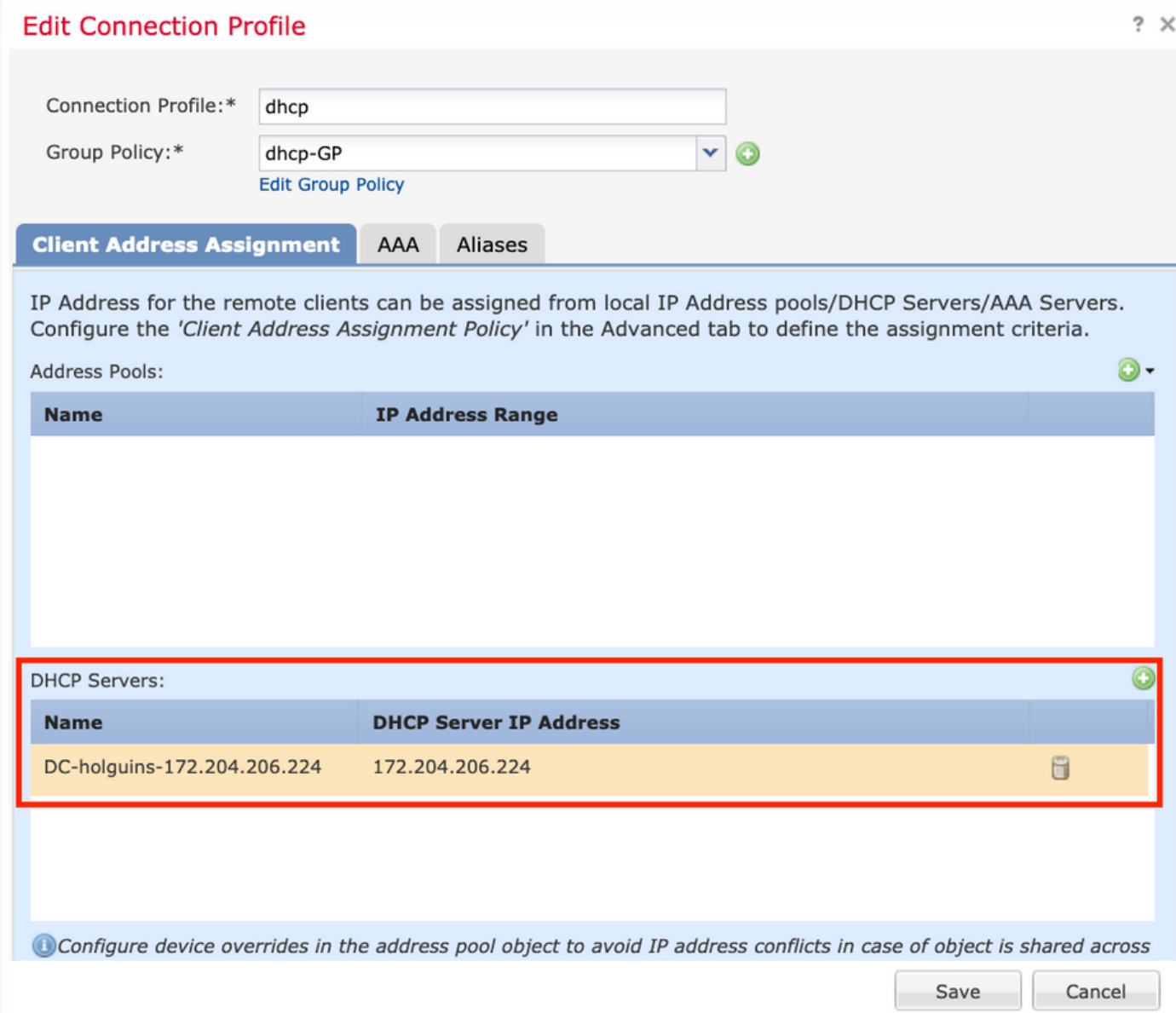
步骤2.配置AnyConnect

配置并激活DHCP范围后，FMC中将执行下一个步骤。

步骤2.1.配置连接配置文件


1.在“DHCP服务器”部分，选择  符号，并使用DHCP服务器的IP地址创建对象。

2.选择对象作为DHCP服务器，以便从请求IP地址，如图所示。




Edit Connection Profile ? X

Connection Profile:* dhcp


Group Policy:* dhcp-GP  [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

Save Cancel

步骤2.2.配置组策略

1.在“组策略”菜单中，导航到“常规”>“DNS/WINS”，其中有DHCP网络范围部分，如图所示。

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:

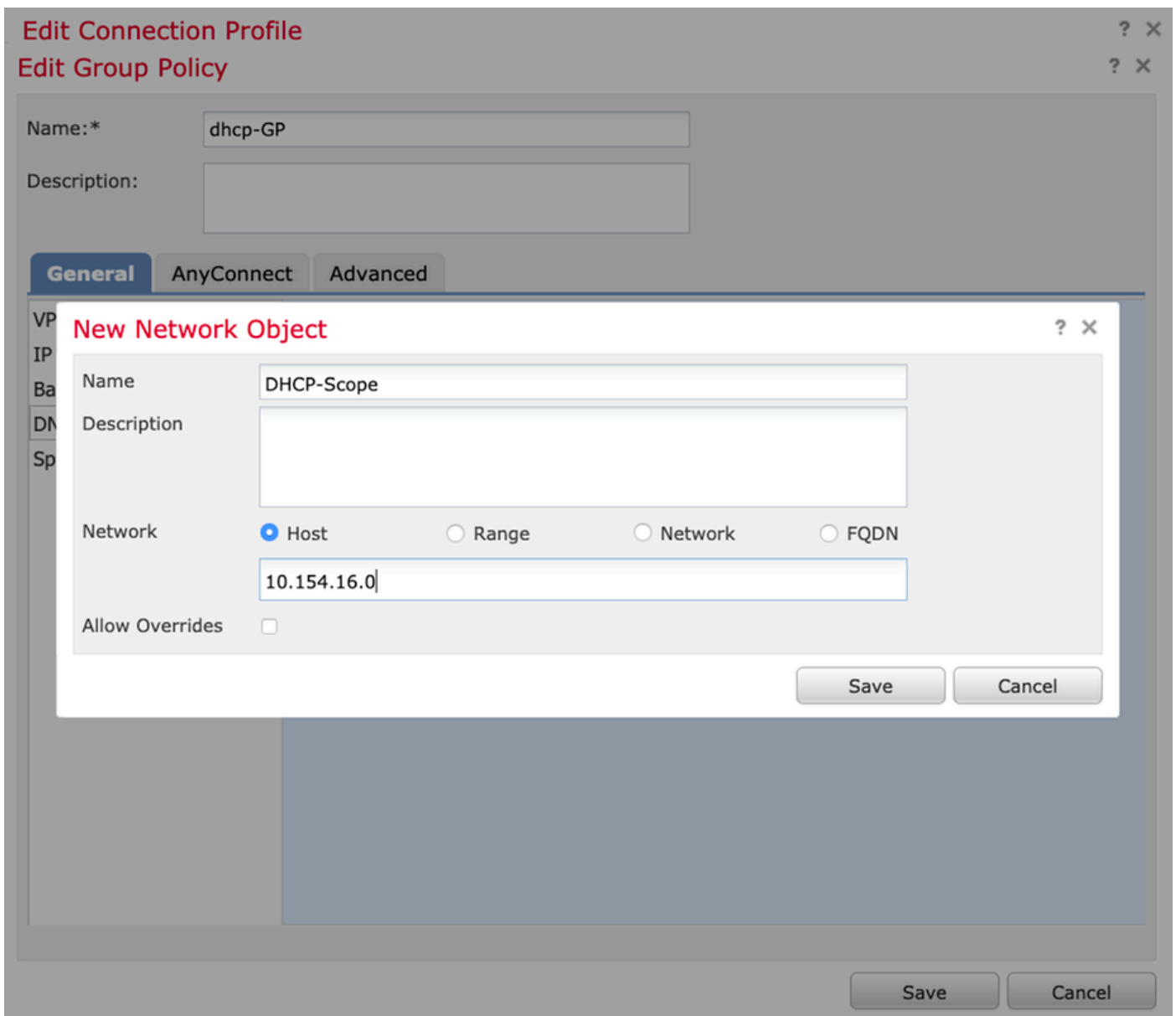
DHCP Network Scope:
Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

Save Cancel

2. 创建新对象，此对象必须具有与DHCP服务器相同的网络范围。

注意：



3.选择DHCP范围对象，然后选择“保存”，如图所示。

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

步骤2.3.配置地址分配策略

1. 导航至Advanced > Address Assignment Policy，并确保Use DHCP 选项已切换，如图所示。

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

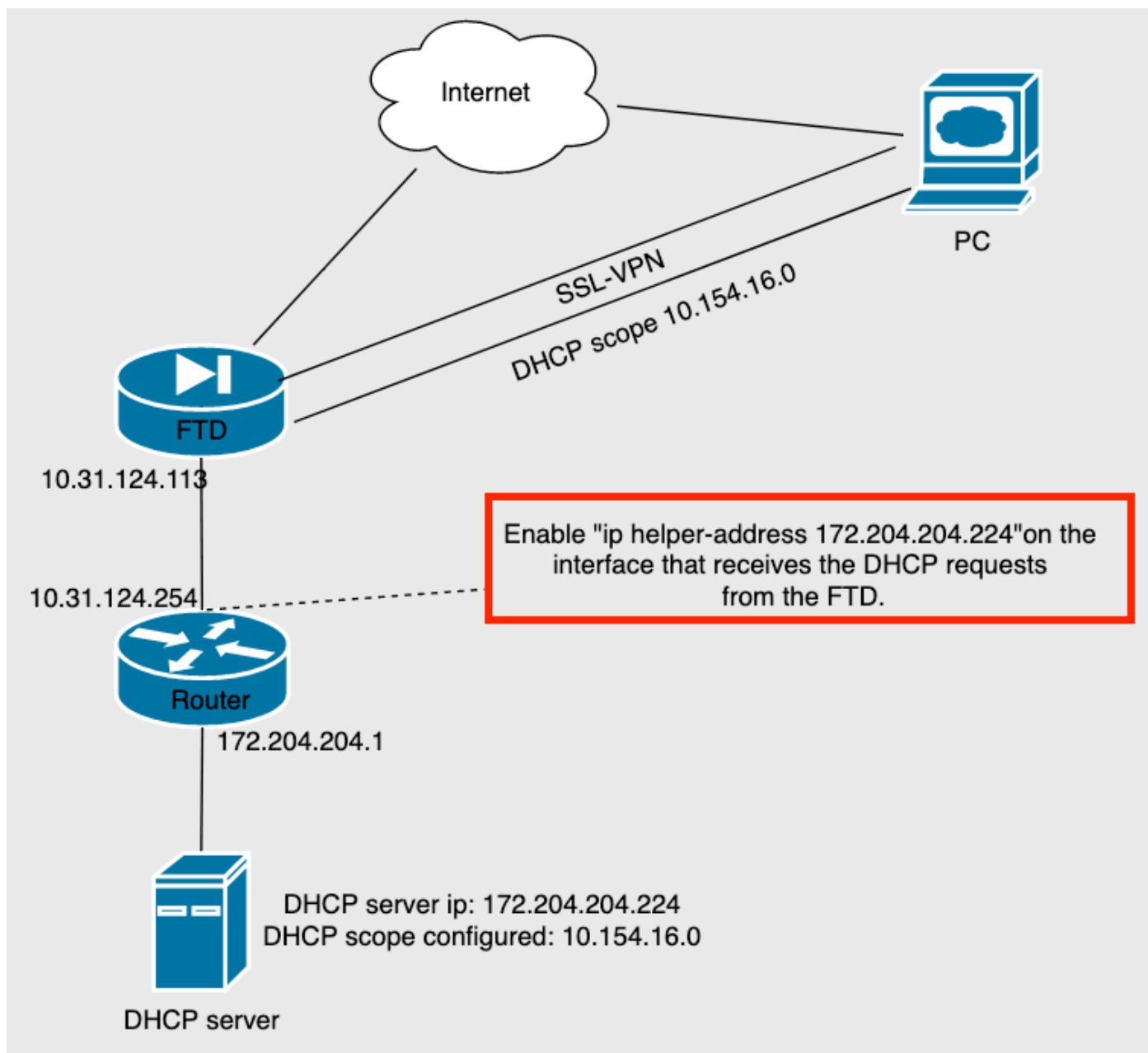
- Use authorization server (RADIUS Only)
- Use internal address pools

2.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“IP助手”才能将请求转发到DHCP服务器。

如图所示，拓扑说明了场景和网络中的必要更改。



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。

```
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: 0000000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
```

- 优惠：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范围的目的地一起提供。
- 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范围的目的地一起提供。

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。

No.	Time	Source	Destination	Protocol	Length	Info
						Number

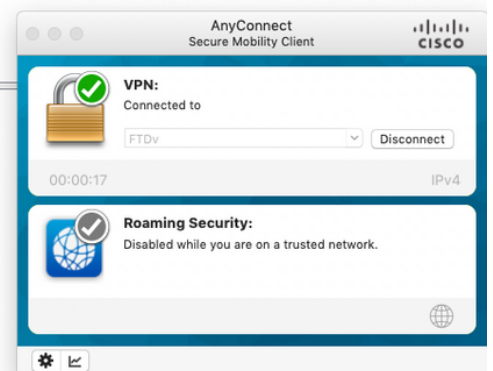


步骤3.登录Anyconnect时，DHCP协商应如图所示。

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---0--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	00P.V.-p...
0040	00	00	0a	9a	10	00	00	50	56	96	d1	70	00	00	00	00
0050	00	00	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	00	00
0070	00	00	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	00	00
0090	00	00	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	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
00d0	00	00	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	00	00
00f0	00	00	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	00	00



相关信息

- 此视频提供了FTD的配置示例，该示例允许远程访问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](#)