使用FlexConfig在FTD上配置DHCP IPv4保留

目录

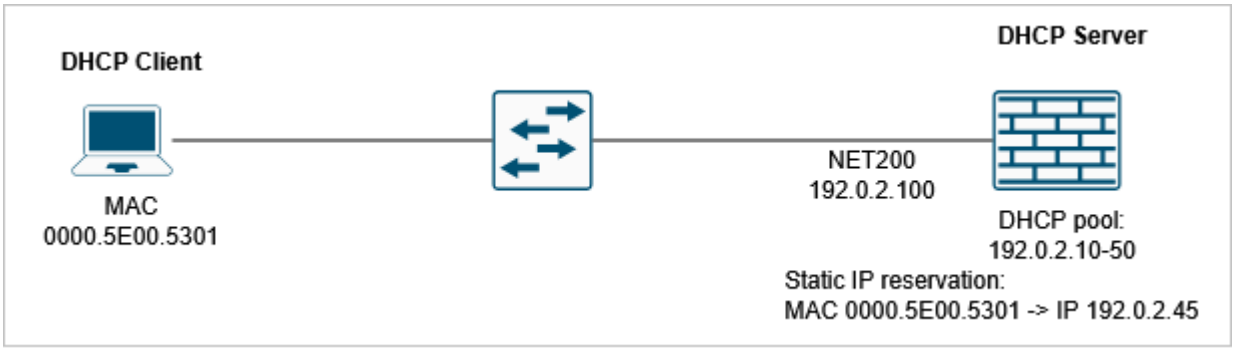
问题

- 管理员希望将防火墙威胁防御(FTD)设备配置为工作站的DHCP服务器，并为终端设备设置DHCP地址保留。
- 配置包括在防火墙管理中心(FMC)本地配置FTD的DHCP服务器，并使用FlexConfig添加DHCP IP保留。

环境

- 防火墙威胁防御(FTD)版本10.x。其他软件版本也会受到影响。
- 防火墙管理中心(FMC)10.x。其他软件版本也会受到影响。

拓扑



特定DHCP环境包括：

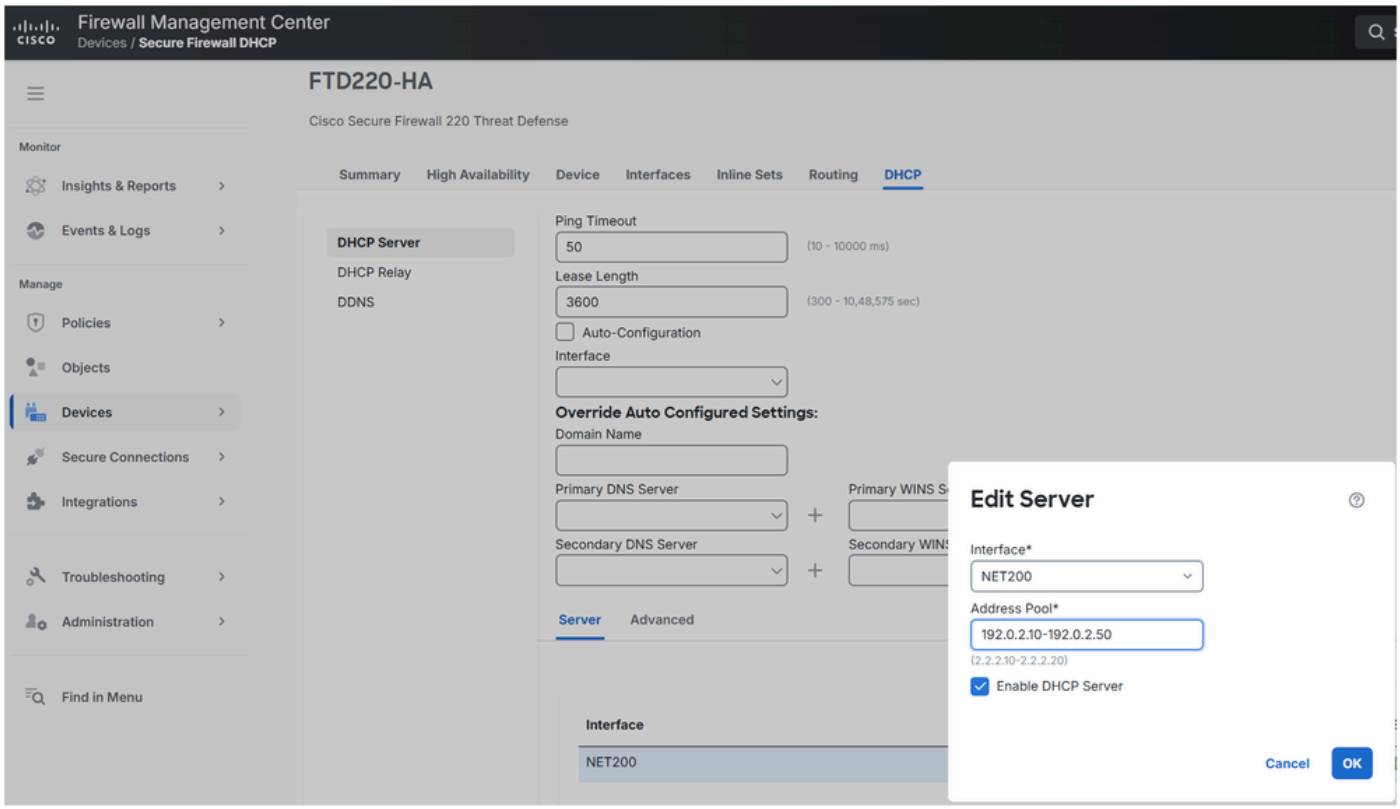
- DHCP服务器接口为NET200。
- DHCP服务器池为192.0.2.10 - 50。

- MAC地址为0000.5E00.5301的终端设备。目标是为此终端保留IP地址192.0.2.45。

分辨率

DHCP 服务器配置

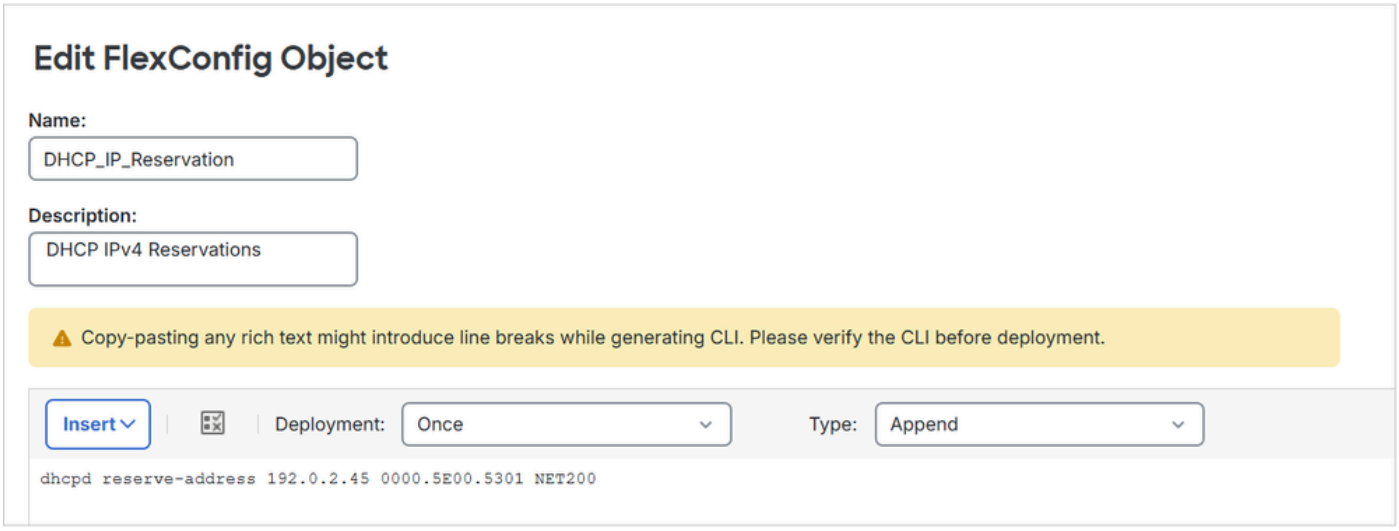
池192.0.2.10 - 50在FTD接口NET200上配置：



FlexConfig配置

对于DHCP IP地址保留，请使用FlexConfig:

- 部署类型:设置为“一次”。
- 配置类型:设置为“Append”（这是默认值）。也可以使用“预置”。



配置验证

已部署的配置：

<#root>

device#

show run dhcpd

dhcpd address 192.0.2.10-192.0.2.50 NET200
dhcpd enable NET200
dhcpd reserve-address 192.0.2.45 0000.5E00.5301 NET200

后台操作

要捕获DHCP数据包，请使用以下命令：

<#root>

device#

capture CAPI interface NET200 match udp any any eq bootpc

device#

```
capture CAPI interface NET200 match udp any any eq bootps
```

- DHCP客户端侦听UDP端口68。
- DHCP服务器侦听UDP端口67。

DHCP调试：

<#root>

```
device#
```

```
debug dhcpd event 255
```

```
debug dhcpd event enabled at level 255
device#
```

```
debug dhcpd packet 255
```

```
debug dhcpd packet enabled at level 255
```

注意：请谨慎使用调试！

IP地址分配过程中的调试输出：

<#root>

```
DHCPD/RA:  Server msg received, fip=ANY, fport=0 on NET200 interface
DHCPD:
```

```
 DHCPDISCOVER received from client 0100.5056.885f.d1 on interface NET200.
```

```
DHCPD:IP 248.57.222.26 ARP entry removed from the cache
DHCPD: send ping pkt to 192.0.2.45
DHCPD: ping got no response for ip: 192.0.2.45
DHCPD:
```

```
MAC 0000.5E00.5301 is reserved for IP 192.0.2.45, allocating it
```

```
DHCPD: Add binding 192.0.2.45 to radix tree
DHCPD/RA: Binding successfully added to hash table
dhcpd_create_automatic_binding() adding NP rule for client 192.0.2.45
DHCPD:
```

assigned IP address 192.0.2.45 to client 0100.5056.885f.d1.

DHCPD:

Sending DHCPOFFER to client 0100.5056.885f.d1 (192.0.2.45).

```
DHCPD: Total # of raw options copied to outgoing DHCP message is 0.
DHCPD/RA: creating ARP entry (192.0.2.45, 0000.5E00.5301).
DHCPD: unicasting BOOTREPLY to client 0000.5E00.5301(192.0.2.45).
DHCPD/RA:  Server msg received, fip=ANY, fport=0 on NET200 interface
DHCPD: DHCPDISCOVER received from client 0100.5056.885f.d1 on interface NET200.
DHCPD: Sending DHCPOFFER to client 0100.5056.885f.d1 (192.0.2.45).
DHCPD: Total # of raw options copied to outgoing DHCP message is 0.
DHCPD/RA: creating ARP entry (192.0.2.45, 0000.5E00.5301).
DHCPD: unicasting BOOTREPLY to client 0000.5E00.5301(192.0.2.45).
DHCPD/RA:  Server msg received, fip=ANY, fport=0 on NET200 interface
DHCPD: DHCPDISCOVER received from client 0100.5056.885f.d1 on interface NET200.
DHCPD: Sending DHCPOFFER to client 0100.5056.885f.d1 (192.0.2.45).
DHCPD: Total # of raw options copied to outgoing DHCP message is 0.
DHCPD/RA: creating ARP entry (192.0.2.45, 0000.5E00.5301).
DHCPD: unicasting BOOTREPLY to client 0000.5E00.5301(192.0.2.45).
DHCPD/RA:  Server msg received, fip=ANY, fport=0 on NET200 interface
DHCPD: DHCPREQUEST received from client 0100.5056.885f.d1.
DHCPD: Extracting client address from the message
DHCPD: State = DHCPS_REBOOTING
DHCPD: State = DHCPS_REQUESTING
DHCPD: Client 0100.5056.885f.d1 specified it's address 192.0.2.45
DHCPD: Client is on the correct network
DHCPD:
```

Client accepted our offer

DHCPD:

Client and server agree on address 192.0.2.45

```
DHCPD: Renewing client 0100.5056.885f.d1 lease
DHCPD: Client lease can be renewed
DHCPD: Sending DHCPACK to client 0100.5056.885f.d1 (192.0.2.45).
DHCPD: Including FQDN option name 'DESKTOP-VQ7968K' rcode1=0, rcode2=0 flags=0x0
DHCPD: Total # of raw options copied to outgoing DHCP message is 0.
DHCPD/RA: creating ARP entry (192.0.2.45, 0000.5E00.5301).
DHCPD: unicasting BOOTREPLY to client 0000.5E00.5301(192.0.2.45).
```

DHCP绑定的验证：

<#root>

device#

show dhcpd binding

```
IP address       Client Identifier        Lease expiration        Type

192.0.2.45

0100.005e.0053.01

           3589 seconds    Automatic
```

原因

- FMC本身不支持DHCP IP地址预留的配置。因此，必须使用FlexConfig来配置IP地址保留。
- 相关增强缺陷：思科漏洞ID CSCwn24229。

相关内容

- https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/A-H/asa-command-ref-A-H/m_dh-dm.html#wp1603069952
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwn24229
- 思科技术支持和下载

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）。