使用FlexConfig在FTD上設定DHCP IPv4保留

目錄

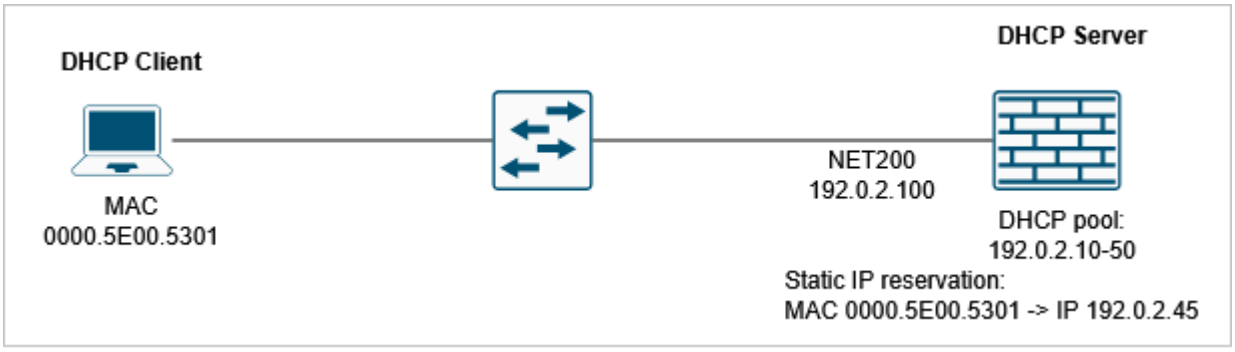
問題

- 管理員希望將防火牆威脅防禦(FTD)裝置配置為工作站的DHCP伺服器，並為終端裝置設定DHCP地址保留。
- 此組態涉及在防火牆管理中心(FMC)內為FTD原生設定DHCP伺服器，並使用FlexConfig來新增DHCP IP保留。

環境

- 防火牆威脅防禦(FTD)版本10.x。其他軟體版本也會受到影響。
- 防火牆管理中心(FMC)10.x。其他軟體版本也會受到影響。

拓撲



特定的DHCP環境包括：

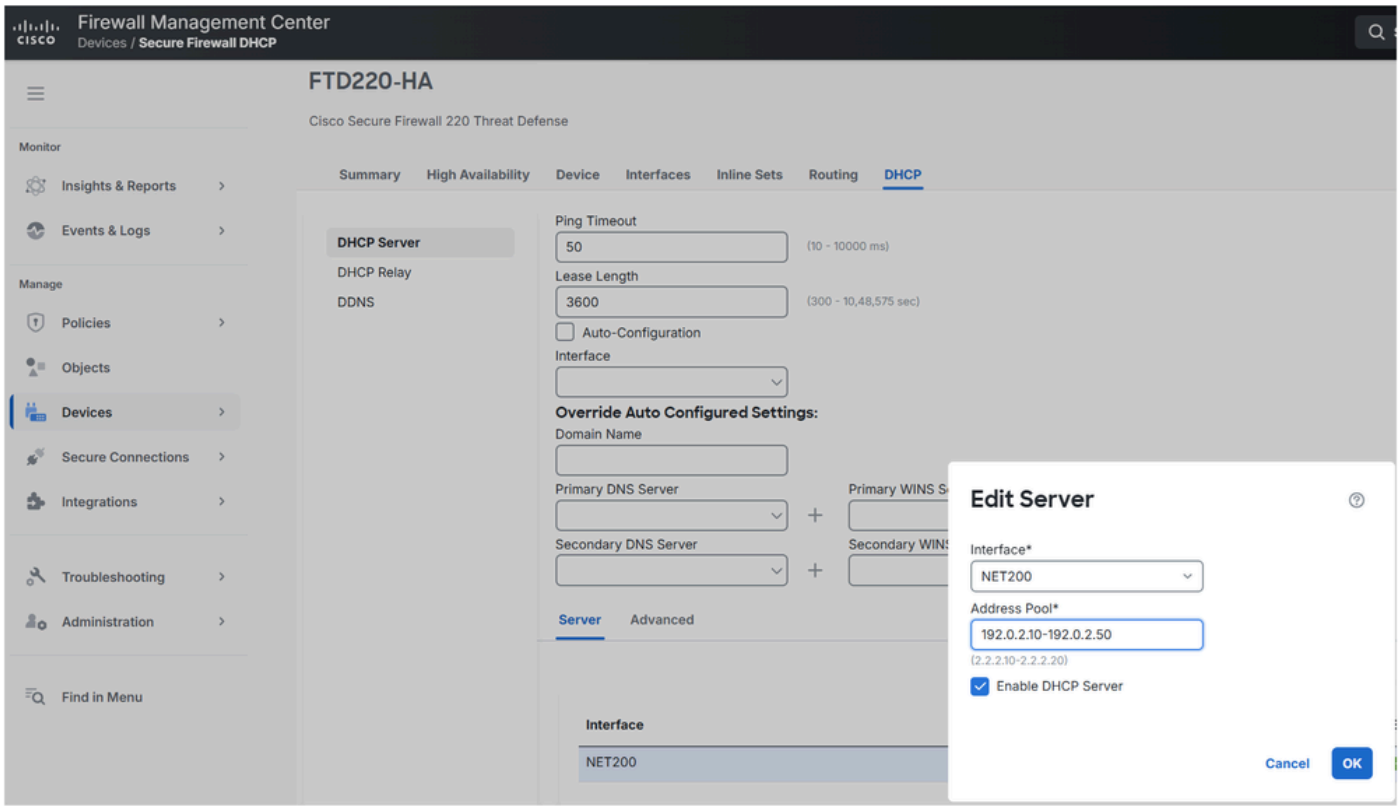
- DHCP伺服器介面為NET200。
- DHCP伺服器池為192.0.2.10 - 50。

- MAC地址為0000.5E00.5301的終端裝置。目標是為此終端保留IP地址192.0.2.45。

解析

DHCP伺服器配置

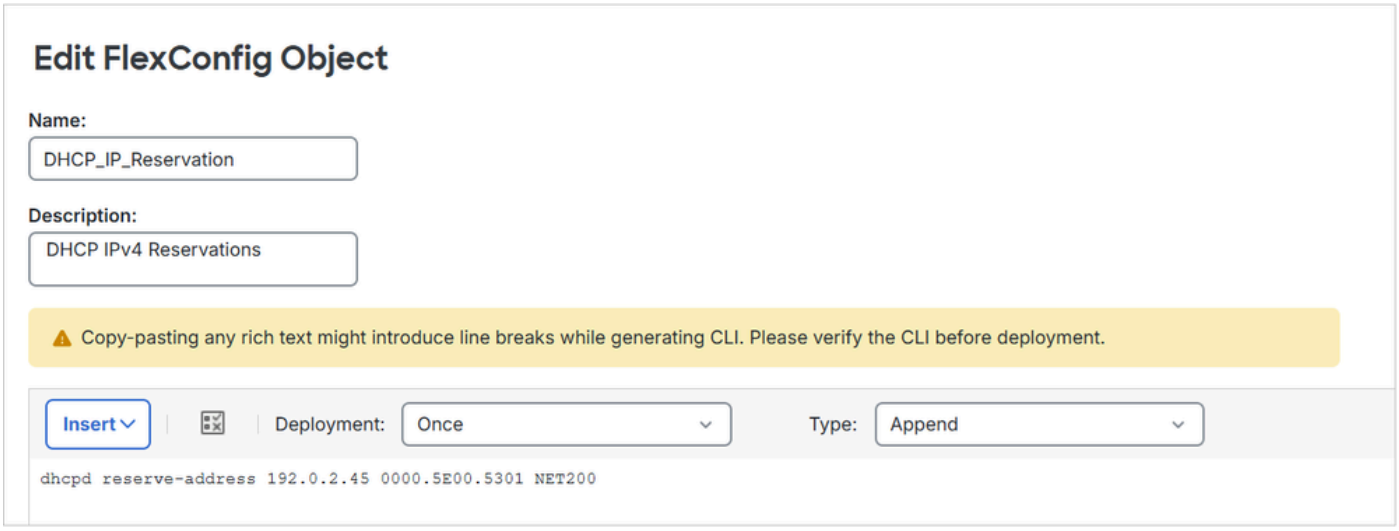
池192.0.2.10 - 50在FTD介面NET200上設定：



FlexConfig配置

對於DHCP IP地址保留，請使用FlexConfig:

- 部署型別：設定為「一次」。
- 配置型別：設定為「Append」（這是預設值）。還可以使用「Prepend」。



組態驗證

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
```

後台操作

要捕獲DHCP資料包，請使用以下命令：

<#root>

device#

capture CAPI interface NET200 match udp any any eq bootpc

device#

capture CAPI interface NET200 match udp any any eq bootps

- DHCP客戶端偵聽UDP埠68。
- DHCP伺服器監聽UDP埠67。

DHCP調試：

<#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

附註：請謹慎使用debug!

在IP地址分配期間調試輸出：

<#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).
```

驗證DHCP繫結：

<#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本地不支援配置DHCP IP地址保留。因此，必須使用FlexConfig來配置IP地址保留。
- 相關增強缺陷：思科錯誤ID CSCwn24229。

相關內容

- 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
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。