Configurer la réservation IPv4 DHCP sur FTD à l'aide de FlexConfig

Table des matières

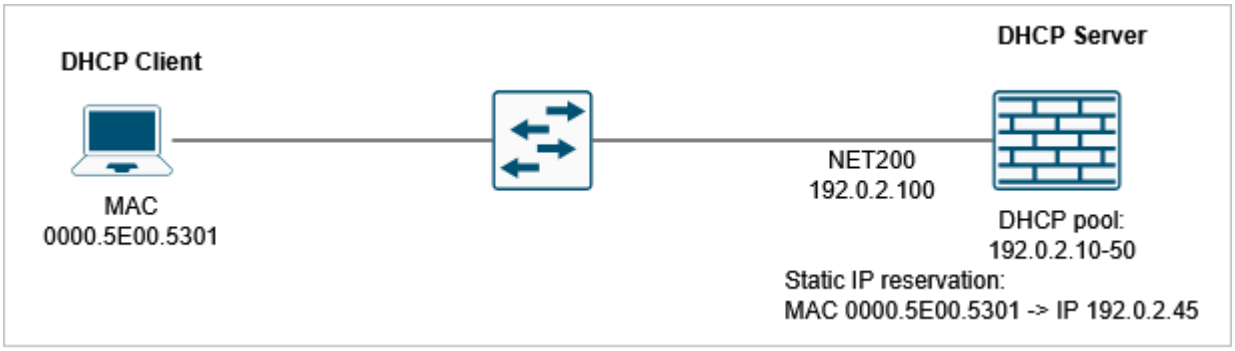
Problème

- Un administrateur souhaite configurer un périphérique Firewall Threat Defense (FTD) en tant que serveur DHCP pour une station de travail et configurer une réservation d'adresse DHCP pour un périphérique d'extrémité.
- La configuration implique la configuration native du serveur DHCP pour le FTD dans le Centre de gestion des pare-feu (FMC) et l'utilisation de FlexConfig pour ajouter la réservation IP DHCP.

Environnement

- Firewall Threat Defense (FTD) version 10.x. D'autres versions logicielles sont également affectées.
- Firewall Management Center (FMC) 10.x. D'autres versions logicielles sont également affectées.

Topologie



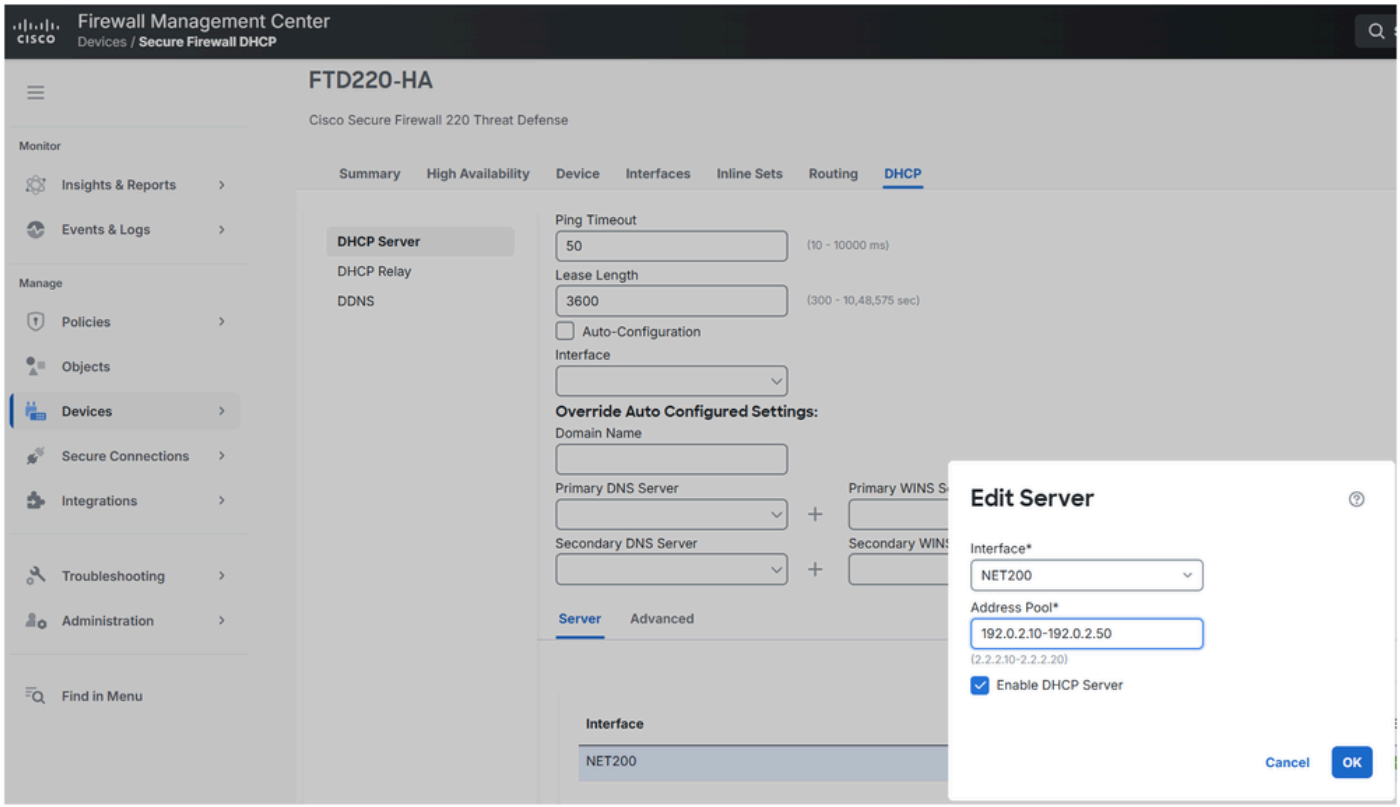
L'environnement DHCP spécifique inclut :

- L'interface du serveur DHCP est NET200.
- Le pool de serveurs DHCP est 192.0.2.10 - 50.
- Périphérique de point d'extrémité avec l'adresse MAC 0000.5E00.5301. L'objectif est de réserver l'adresse IP 192.0.2.45 pour ce point d'extrémité.

Résolution

Configuration du serveur DHCP

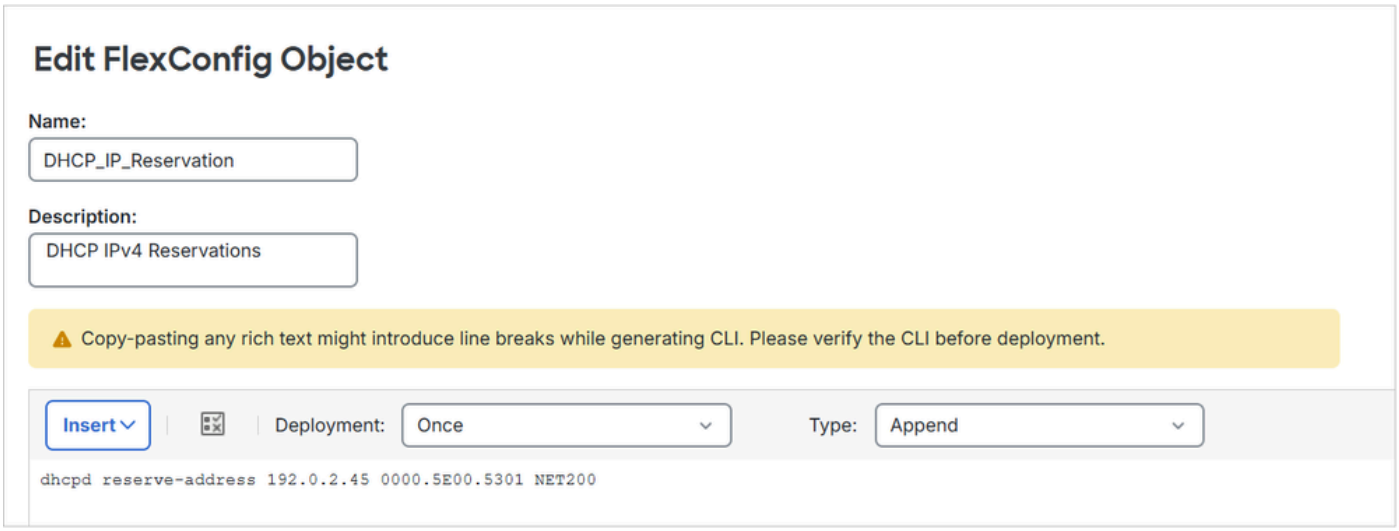
Le pool 192.0.2.10 - 50 est configuré sur l'interface FTD NET200 :



Configuration FlexConfig

Pour la réservation d'adresse IP DHCP, utilisez FlexConfig :

- Type de déploiement : Définissez sur « Une fois ».
- Type de configuration : Réglez sur "Ajouter" (il s'agit de la valeur par défaut). Vous pouvez également utiliser la fonction "Préfixer".



Validation de configuration

La configuration déployée :

<#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
```

Opération De Fond

Pour capturer les paquets DHCP, utilisez ces commandes :

<#root>

device#

capture CAPI interface NET200 match udp any any eq bootpc

device#

capture CAPI interface NET200 match udp any any eq bootps

- Le client DHCP écoute sur le port UDP 68.
- Le serveur DHCP écoute sur le port UDP 67.

Débogages DHCP :

<#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

Remarque : Utilisez les débogages avec prudence !

Sortie de débogage pendant l'attribution d'adresse IP :

<#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).
```

Vérification de la liaison DHCP :

<#root>

```
device#

show dhcpd binding

IP address       Client Identifier        Lease expiration        Type

192.0.2.45

0100.005e.0053.01

            3589 seconds    Automatic
```

Motif

- FMC ne prend pas en charge de manière native la configuration de la réservation d'adresses IP DHCP. Par conséquent, FlexConfig doit être utilisé pour configurer la réservation d'adresse IP.
- Défaut d'amélioration connexe : ID de bogue Cisco CSCwn24229.

Autres informations utiles

- 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
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.