

Activer les options d'étendue DHCP sur le serveur DHCP en utilisant FTD comme agent de relais

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration du relais DHCP](#)

[Configuration de l'agent relais DHCP](#)

[Configuration du serveur DHCP externe](#)

[Activer l'option 43 sur le serveur DHCP externe](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment activer les options sur le serveur DHCP en utilisant dans FTD géré par FMC.

Conditions préalables

Exigences

- Connaissance de la technologie Firepower
- Connaissance du serveur DHCP (Dynamic Host Control Protocol) et du relais DHCP.

Composants utilisés

- Les informations contenues dans ce document sont basées sur Virtual Cisco FTD et FMC, version 7.4.0
- Windows Server 2019 est utilisé comme serveur DHCP

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Le périphérique de défense contre les menaces peut transmettre des informations à l'aide des options DHCP spécifiées dans les documents RFC 2132, RFC 2562 et RFC 5510.

Elle prend en charge toutes les options DHCP numérotées de 1 à 255, à l'exception des options 1, 12, 50-54, 58-59, 61, 67 et 82.

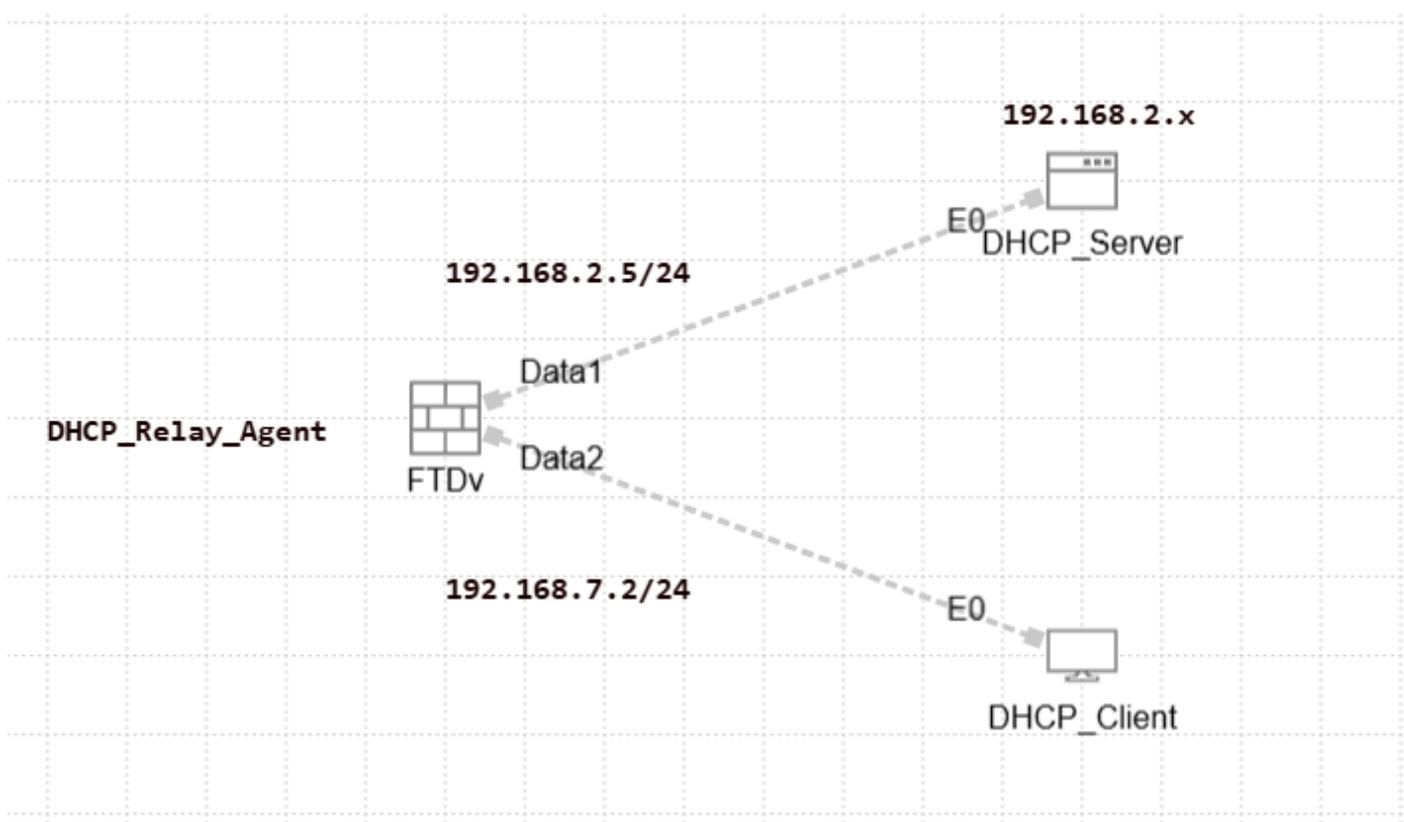
La RFC 2132 spécifie deux options DHCP pertinentes pour les configurations spécifiques au fournisseur : Options 60 et 43.

Le document propose des exemples de configurations et illustre le fonctionnement de l'option DHCP 43 (informations spécifiques au constructeur) sur Windows Server 2019, avec FTD fonctionnant comme agent de relais DHCP.

L'option 43 permet aux serveurs DHCP de transmettre des informations spécifiques au fournisseur aux clients, facilitant ainsi la localisation et la connexion des périphériques tels que les points d'accès à leurs contrôleurs, même lorsqu'ils se trouvent sur des VLAN ou des sous-réseaux différents.

Configuration

Diagramme du réseau



Configuration du relais DHCP

L'interface FTD fonctionne comme un agent de relais DHCP, facilitant la communication entre le client et un serveur DHCP externe.

Il écoute les requêtes des clients et ajoute les données de configuration essentielles, telles que les informations de liaison client, dont le serveur DHCP a besoin pour attribuer une adresse au client.

À la réception d'une réponse du serveur DHCP, l'interface renvoie le paquet de réponse au client DHCP.

La configuration du relais DHCP comprend deux étapes principales :

1. Configurez l'agent de relais DHCP.
2. Configurez le serveur DHCP externe.

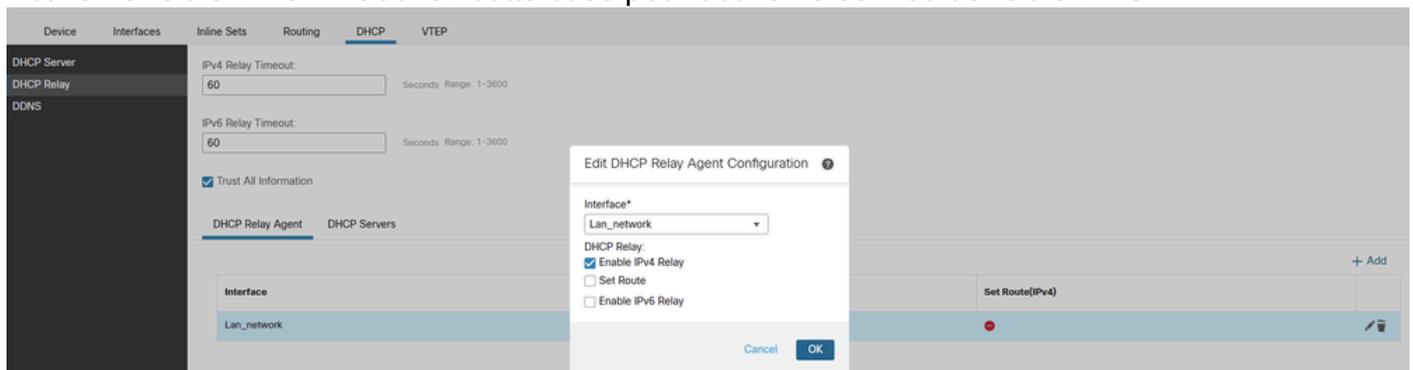
Configuration de l'agent relais DHCP

Pour configurer le relais DHCP, procédez comme suit :

1. Accédez à Périphériques > Gestion des périphériques.
2. Cliquez sur le bouton de modification de l'appareil FTD.
3. Accédez à l'option DHCP > DHCP Relay.
4. Cliquez sur Ajouter.

Interface: Sélectionnez l'interface appropriée dans la liste déroulante. C'est à ce niveau que l'interface écoute les requêtes des clients et que les clients DHCP peuvent se connecter directement à cette interface pour les requêtes d'adresse IP.

Activer le relais DHCP : Cochez cette case pour activer le service de relais DHCP.



Agent_Relais_DHCP_Config

5. Cliquez sur OK pour enregistrer les paramètres de configuration de l'agent de relais DHCP.

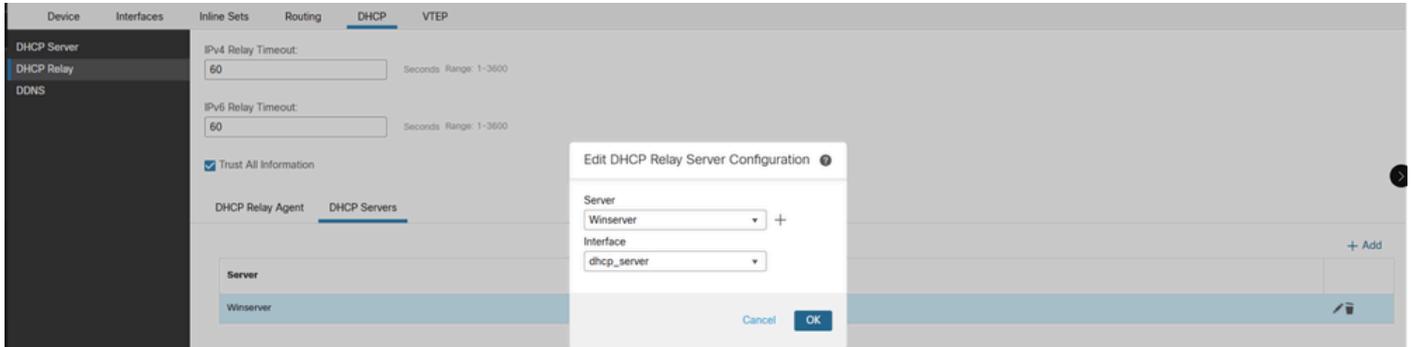
Configuration du serveur DHCP externe

Pour configurer l'adresse IP du serveur DHCP externe vers lequel les requêtes des clients sont transmises, procédez comme suit :

Accédez à la section DHCP Server et cliquez sur Add"

1. Dans le champ Server, saisissez l'adresse IP du serveur DHCP. Vous pouvez choisir un objet réseau existant dans le menu déroulant ou en créer un nouveau en cliquant sur l'icône plus (+).
2. Dans le champ Interface, spécifiez l'interface qui se connecte au serveur DHCP.

3. Pour enregistrer la configuration, cliquez sur OK. Cliquez ensuite sur Save pour enregistrer les paramètres de la plate-forme.



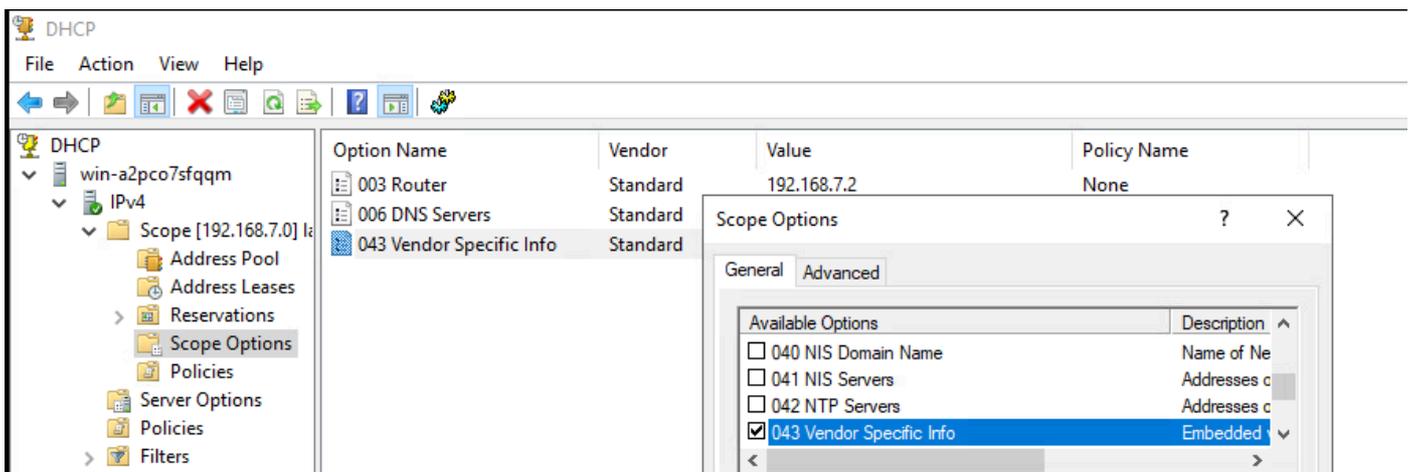
Configuration_Serveur_DHCP

4. Ensuite, allez à l'option Déployer, sélectionnez l'appliance FTD où vous souhaitez appliquer les modifications, et cliquez sur Déployer pour lancer le déploiement des paramètres de la plate-forme.

Activer l'option 43 sur le serveur DHCP externe

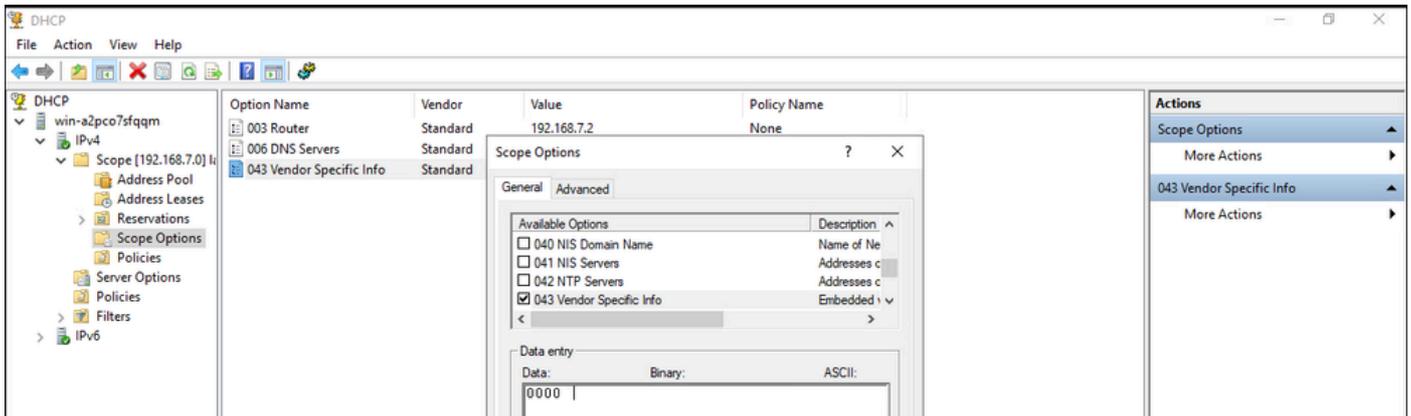
Veillez noter que : Conformément à la RFC 2132 , la longueur minimale de l'option 43 est de 1.

Accédez aux paramètres de votre serveur DHCP et accédez à IPv4, puis sélectionnez Scope and Scope Options >More Actions >Configure Options et activez l'option 43



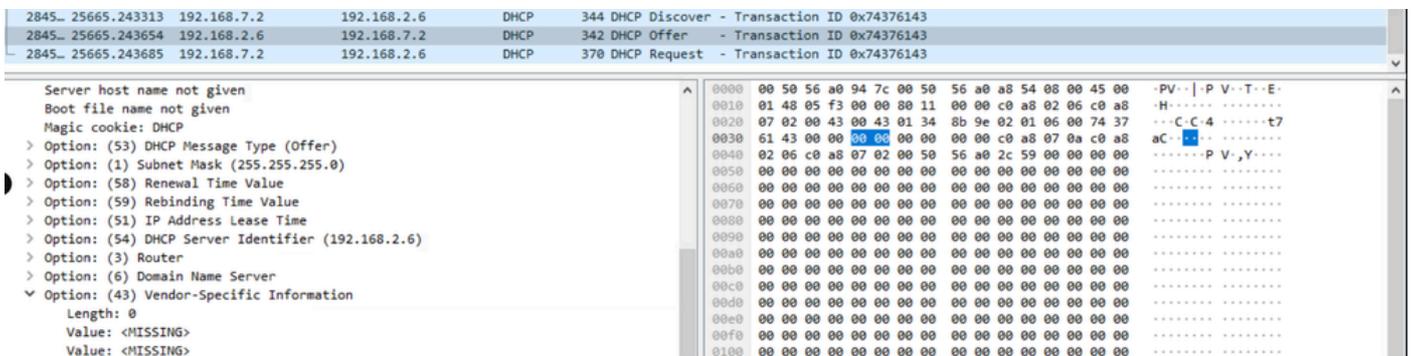
Enable_Option_43_On_External_DHCP_Server

Initialement, le paramètre par défaut laisse la valeur vide, ce qui conduit FTD à abandonner le paquet et à le classer comme malformé.



Default_Config_Of_Option_43

Du côté du serveur utilisant Wireshark, nous observons que dans le paquet OFFER, la valeur est absente pour l'option 43 lorsque la longueur est 0.



Non_Working_Server_Side_pcap

Les paquets sont abandonnés par Cisco Firepower Threat Defense (FTD) car ils ont une longueur de 0 et sont considérés comme malformés, en violation du document RFC 2132.

```
<#root>
```

```
firepower#
```

```
debug dhcprelay packet
```

```
debug dhcprelay packet enabled at level 1
ftd# DHCPD/RA: Relay msg received, fip=ANY, fport=0 on Lan_network interface
DHCP: Received a BOOTREQUEST from interface 3 (size = 302)
DHCPD/RA: Binding successfully added to hash table
DHCPR: relay binding created for client 0050.56a0.2c59.
DHCPR: setting giaddr to 192.168.7.2.
dhcpd_forward_request: request from 0050.56a0.2c59 forwarded to 192.168.2.6.
```

```
DHCPD/RA: option 43 is malformed.
```

```
DHCPD/RA: Unable to load workspace.
```

```
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on Lan_network interface
DHCP: Received a BOOTREQUEST from interface 3 (size = 328)
DHCPR: relay binding found for client 0050.56a0.2c59.
```

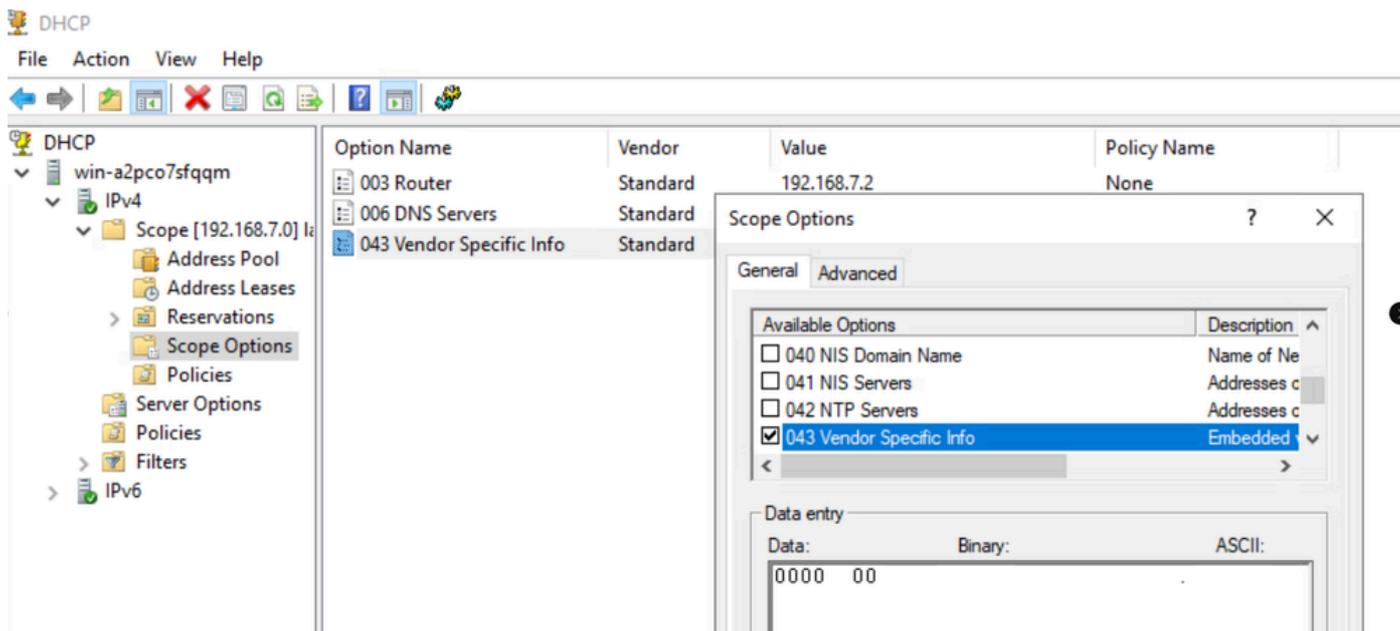
DHCPRA: setting giaddr to 192.168.7.2.

DHCPRA: Server request counter 1

dhcpd_forward_request: request from 0050.56a0.2c59 forwarded to 192.168.2.6.

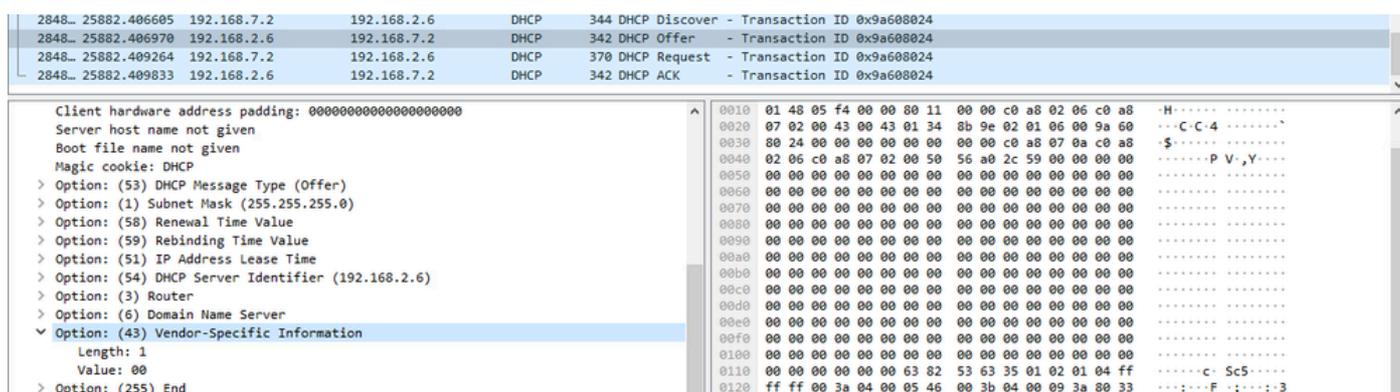
Pour régler la valeur binaire sur une valeur supérieure à 0 conformément à la RFC 2132, double-cliquez sur le champ 043 Vendor Specific Info et définissez la valeur sur 00, comme illustré dans l'image.

Cette modification garantit que l'adresse IP est correctement louée au client.



Valeur_binaire_changée_en_1

Processus DORA côté serveur lorsque la valeur est définie sur 1 dans Option 43



Pcap_Travail_Côté_Serveur

Processus DORA côté client lorsque la valeur est définie sur 1 dans l'option 43 et que nous pouvons voir que le client est loué avec une adresse IP.

2907_	1837526.548275	0.0.0.0	255.255.255.255	DHCP	344	128	DHCP Discover	-	Transaction ID 0x9a608024
2907_	1837526.550203	192.168.2.6	192.168.7.10	DHCP	342	72	DHCP Offer	-	Transaction ID 0x9a608024
2907_	1837526.551703	0.0.0.0	255.255.255.255	DHCP	370	128	DHCP Request	-	Transaction ID 0x9a608024
2907_	1837526.553008	192.168.2.6	192.168.7.10	DHCP	342	72	DHCP ACK	-	Transaction ID 0x9a608024

> Option: (53) DHCP Message Type (Offer)	0000	00 50 56 a0 2c 59 00 50 56 a0 48 2d 08 00 45 00	·P·V·,·Y·P·V·H·-·E·
> Option: (1) Subnet Mask (255.255.255.0)	0010	01 48 11 12 40 00 48 11 96 32 c0 a8 02 06 c0 a8	·H··@·H· 2·-·-·-·
> Option: (58) Renewal Time Value	0020	07 0a 00 43 00 44 01 34 48 45 02 01 06 00 e2 68	·-·-·C·D·4·HE·-·-·-·h
> Option: (59) Rebinding Time Value	0030	3c 3f 00 00 00 00 00 00 00 00 c0 a8 07 0a c0 a8	<?·-·-·-·-·-·-·-·-·
> Option: (51) IP Address Lease Time	0040	02 06 c0 a8 07 02 00 50 56 a0 2c 59 00 00 00 00	·-·-·-·-·P·V·,·Y·-·-·-·
> Option: (54) DHCP Server Identifier (192.168.2.6)	0050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	·-·-·-·-·-·-·-·-·-·-·-·
> Option: (3) Router	0060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	·-·-·-·-·-·-·-·-·-·-·-·
> Option: (6) Domain Name Server	0070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	·-·-·-·-·-·-·-·-·-·-·-·
> Option: (43) Vendor-Specific Information	0080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	·-·-·-·-·-·-·-·-·-·-·-·
Length: 1	0090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	·-·-·-·-·-·-·-·-·-·-·-·
Value: 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	·-·-·-·-·-·-·-·-·-·-·-·

Client_Side_Working_pcap

<#root>

firepower#

debug dhcprelay packet

```

debug dhcprelay packet enabled at level 1
ftd# DHCPD/RA: Relay msg received, fip=ANY, fport=0 on Lan_network interface
DHCP: Received a BOOTREQUEST from interface 3 (size = 302)
DHCPR: relay binding found for client 0050.56a0.2c59.
DHCPR: setting giaddr to 192.168.7.2.
dhcpd_forward_request: request from 0050.56a0.2c59 forwarded to 192.168.2.6.
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on dhcp_server interface
DHCP: Received a BOOTREPLY from relay interface 2 (size = 300, xid = 0x81f5dddc) at 06:55:25 UTC Tue Ma
DHCPR: relay binding found for client 0050.56a0.2c59.
DHCPD/RA: creating ARP entry (192.168.7.10, 0050.56a0.2c59).
DHCPR: forwarding reply to client 0050.56a0.2c59.
DHCPR: Client Ip Address :192.168.7.10
DHCPR: subnet mask in dhcp options :255.255.255.0
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on Lan_network interface
DHCP: Received a BOOTREQUEST from interface 3 (size = 328)
DHCPR: relay binding found for client 0050.56a0.2c59.
DHCPR: Server requested by client 192.168.2.6
DHCPR: setting giaddr to 192.168.7.2.
DHCPR: Server request counter 1
dhcpd_forward_request: request from 0050.56a0.2c59 forwarded to 192.168.2.6.
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on dhcp_server interface
DHCP: Received a BOOTREPLY from relay interface 2 (size = 300, xid = 0x81f5dddc) at 06:55:25 UTC Tue Ma
DHCPR: relay binding found for client 0050.56a0.2c59.
DHCPR: exchange complete - relay binding deleted for client 0050.56a0.2c59.
DHCPD/RA: Binding successfully deactivated
dhcpd_destroy_binding() removing NP rule for client 192.168.7.2
DHCPD/RA: free ddns info and binding
DHCPD/RA: creating ARP entry (192.168.7.10, 0050.56a0.2c59).
DHCPR: forwarding reply to client 0050.56a0.2c59.

DHCPR: Client Ip Address :192.168.7.10

DHCPR: subnet mask in dhcp options :255.255.255.0

```

Vérifier

Avant de configurer le serveur DHCP ou le relais, assurez-vous que le FTD est enregistré auprès du FMC. Vérifiez également que la configuration du relais DHCP permet d'établir une connectivité avec le serveur DHCP.

```
<#root>
```

```
>
```

```
system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.  
Type help or '?' for a list of available commands.
```

```
<#root>
```

```
><Press Enter>  
firepower#
```

```
ping
```

Pour vérifier la configuration de l'agent relais DHCP à partir de l'interface de ligne de commande FTD.

```
<#root>
```

```
firepower#
```

```
show running-config dhcprelay
```

```
dhcprelay server 192.168.2.6 dhcp_server  
dhcprelay enable Lan_network  
dhcprelay timeout 60  
dhcprelay information trust-all
```

Dépannage

Pour résoudre le problème, tenez compte des points suivants :

1. Vérifiez le routage entre le FTD et le serveur DHCP pour vous assurer qu'il est accessible à partir du serveur DHCP.
2. Assurez-vous que le serveur DHCP dispose d'une route pour accéder à l'interface de l'agent de relais DHCP.
3. Pour résoudre le problème du client ne recevant pas d'adresse IP, vous pouvez effectuer une capture de paquets sur l'interface routée FTD.

Cela vous permettra d'examiner le processus DORA du serveur DHCP dans les captures de paquets.

Vous pouvez utiliser [Use Firepower Threat Defense Captures et Packet Tracer](#) pour effectuer la capture de paquets de manière efficace.

Pour arrêter et supprimer une session de capture de paquets spécifique que vous avez précédemment démarrée, exécutez la commande ci-dessous.

```
no capture <nom_capture>
```

4. Pour vérifier l'état et collecter le débogage dhcprelay, exécutez les commandes ci-dessous

Pour ce faire, connectez-vous à FTD CLI .

```
<#root>
```

```
system support diagnostic-cli
```

```
enable
```

Appuyez sur Entrée.

```
<#root>
```

```
show dhcprelay statistic
```

```
show dhcprelay state
```

Pour vérifier si un débogage est déjà activé, exécutez la commande ci-dessous.

```
<#root>
```

```
show debug
```

```
<#root>
```

To capture debug excute below commands

```
debug dhcprelay packet
```

```
debug dhcprelay event
```

```
<#root>
```

```
To disable debug
```

```
undebug all
```

Informations connexes

[Configuration du serveur DHCP et du relais sur FTD avec FMC](#)

[DHCP et DDNS](#)

[Assistance et documentation techniques - Cisco Systems](#)

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.