

DHCP-toepassingsopties op DHCP-server inschakelen met FTD als Relay Agent

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configuratie](#)

[Netwerkdigram](#)

[DHCP-relay configureren](#)

[DHCP Relay Agent configureren](#)

[Externe DHCP-server configureren](#)

[Schakel optie 43 in op externe DHCP-server](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u opties op DHCP-server kunt inschakelen met behulp van in FTD beheerde functies van het FMC.

Voorwaarden

Vereisten

- Kennis van FirePOWER-technologie
- Kennis van Dynamic Host Control Protocol (DHCP) Server/ DHCP Relay.

Gebruikte componenten

- De informatie in dit document is gebaseerd op Virtual Cisco FTD en FMC, versie 7.4.0
- Windows Server 2019 wordt gebruikt als DHCP-server

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Het bedreigingsbeschermingsapparaat kan informatie verzenden met DHCP-opties zoals gespecificeerd in RFC 2132, RFC 2562 en RFC 5510.

Het ondersteunt alle DHCP-opties, genummerd 1 tot en met 255, behalve de opties 1, 12, 50-54, 58-59, 61, 67 en 82.

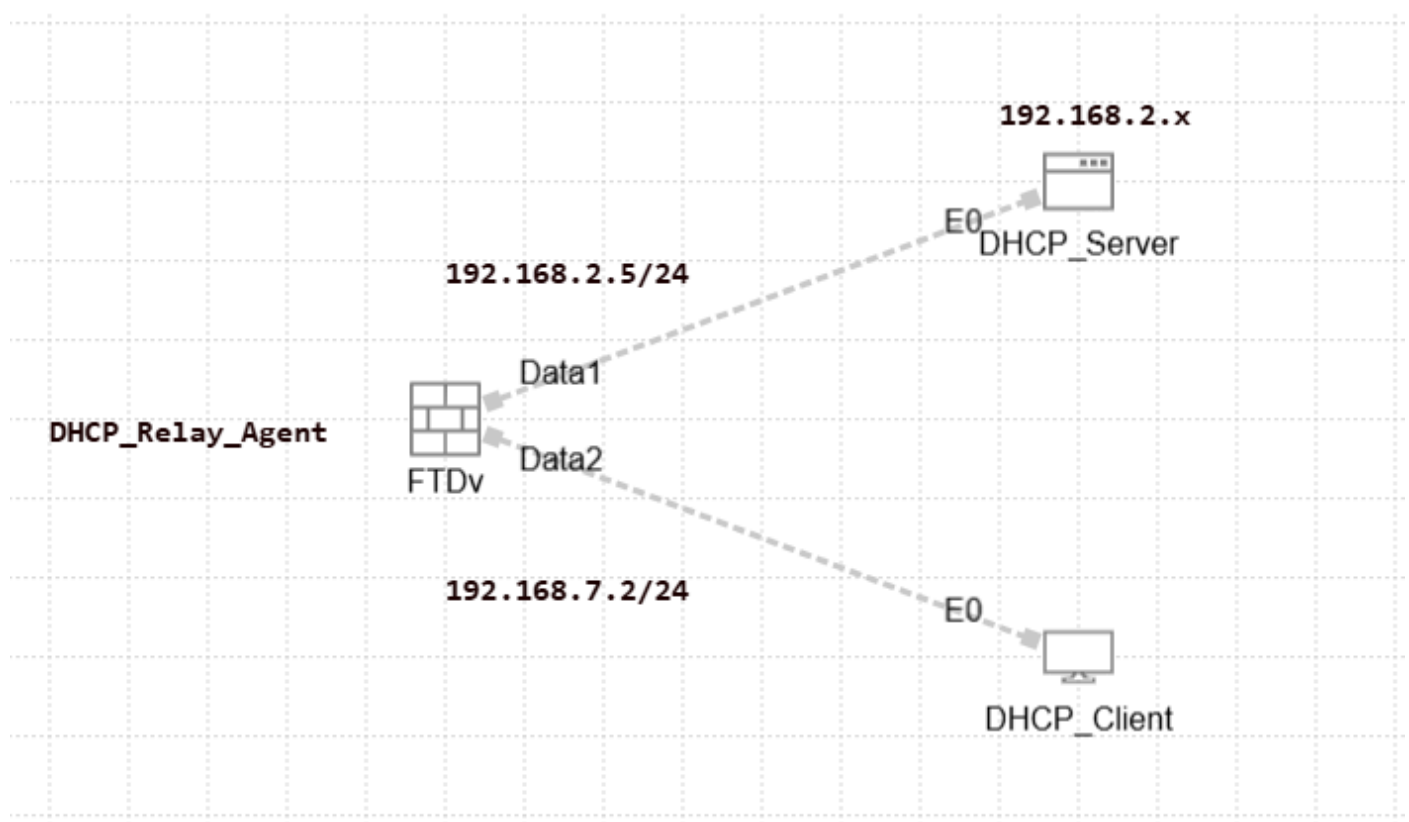
RFC 2132 specificeert twee DHCP-opties voor leverancierspecifieke configuraties: Optie 60 en optie 43.

Het document biedt voorbeeldconfiguraties en illustreert hoe DHCP-optie 43 (leverancierspecifieke informatie) werkt op Windows Server 2019, met FTD functionerend als de DHCP Relay Agent.

Optie 43 stelt DHCP-servers in staat om leverancierspecifieke informatie naar clients te verzenden, waardoor apparaten zoals toegangspunten worden gefaciliteerd bij het lokaliseren en verbinden met hun controllers, zelfs wanneer ze op verschillende VLAN's of subnetten staan.

Configuratie

Netwerkdigram



Netwerkdigram

DHCP-relay configureren

De FTD-interface functioneert als een DHCP Relay-agent die de communicatie tussen de client en een externe DHCP-server vergemakkelijkt.

Het luistert op cliëntverzoeken en voegt essentiële configuratiegegevens, zoals de informatie van de cliëntverbinding toe, die de server van DHCP vereist om een adres aan de cliënt toe te wijzen.

Op het ontvangen van een reactie van de DHCP-server, stuurt de interface het antwoordpakket terug naar de DHCP-client.

Het configureren van DHCP Relay omvat twee primaire stappen:

1. Stel de DHCP Relay Agent in.
2. Stel de externe DHCP-server in.

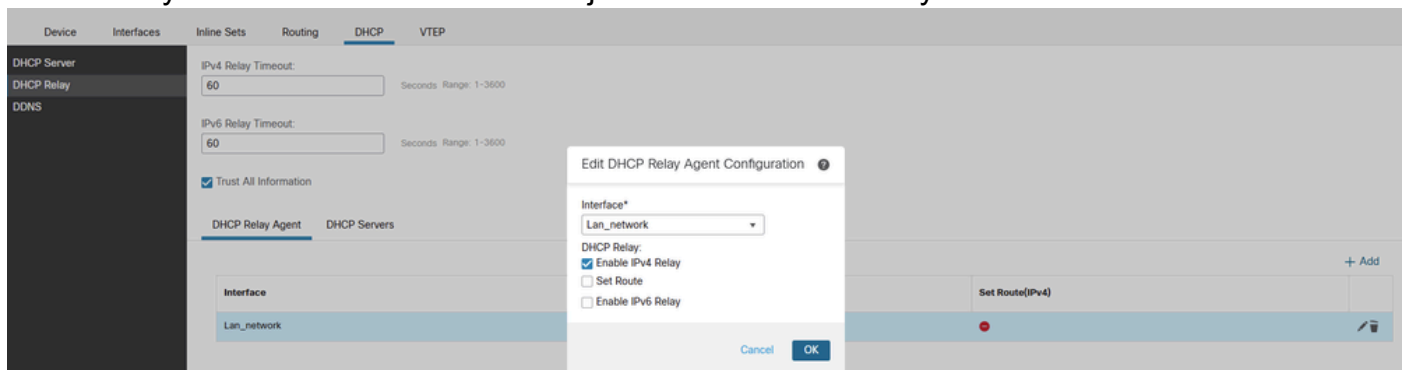
DHCP Relay Agent configureren

Om het DHCP Relay te configureren controleert u de onderstaande stappen:

1. Navigeer naar Apparaten > Apparaatbeheer.
2. Klik op de knop Bewerken voor het FTD-apparaat.
3. Ga naar de optie DHCP > DHCP Relay.
4. Klik op Toevoegen.

Interface: Selecteer de gewenste interface in de vervolgkeuzelijst. Dit is waar de interface op cliëntverzoeken let, en de cliënten van DHCP kunnen rechtstreeks met deze interface voor IP adresverzoeken verbinden.

DHCP-relay inschakelen: Schakel dit vakje in om de DHCP Relay-service te activeren.



DHCP_Relay_Agent_Config

5. Klik op OK om de configuratie-instellingen voor de DHCP Relay Agent op te slaan.

Externe DHCP-server configureren

Om het IP-adres te configureren van de externe DHCP-server waaraan de clientaanvragen worden doorgestuurd, volgt u de onderstaande stappen:

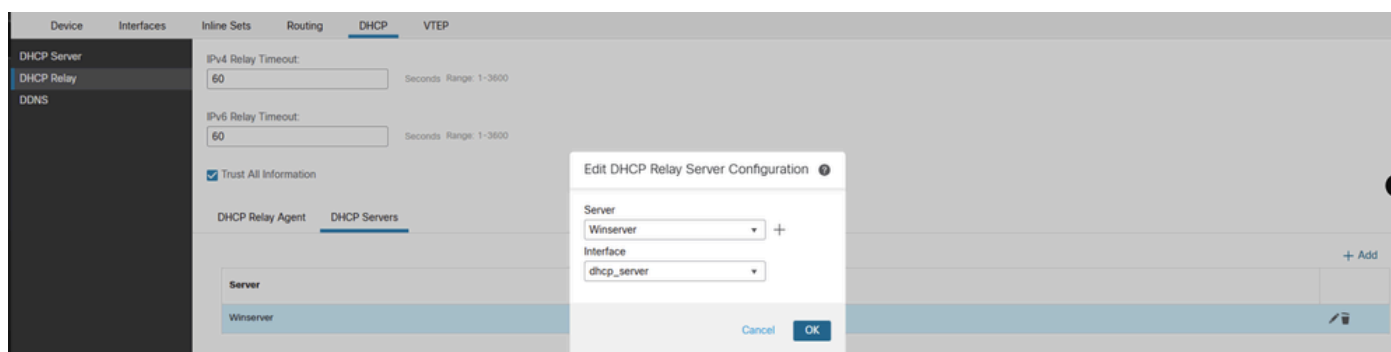
Navigeer naar het gedeelte DHCP Server en klik op Add"

1. Voer in het veld Server het IP-adres van de DHCP-server in. U kunt een bestaand netwerkobject kiezen in het vervolgkeuzemenu of een nieuw object maken door op het plus-pictogram (+) te

klikken.

2. Specificeer in het veld Interface de interface die verbinding maakt met de DHCP-server.

3. Klik op OK om de configuratie op te slaan. Klik vervolgens op Opslaan om de platforminstellingen op te slaan.



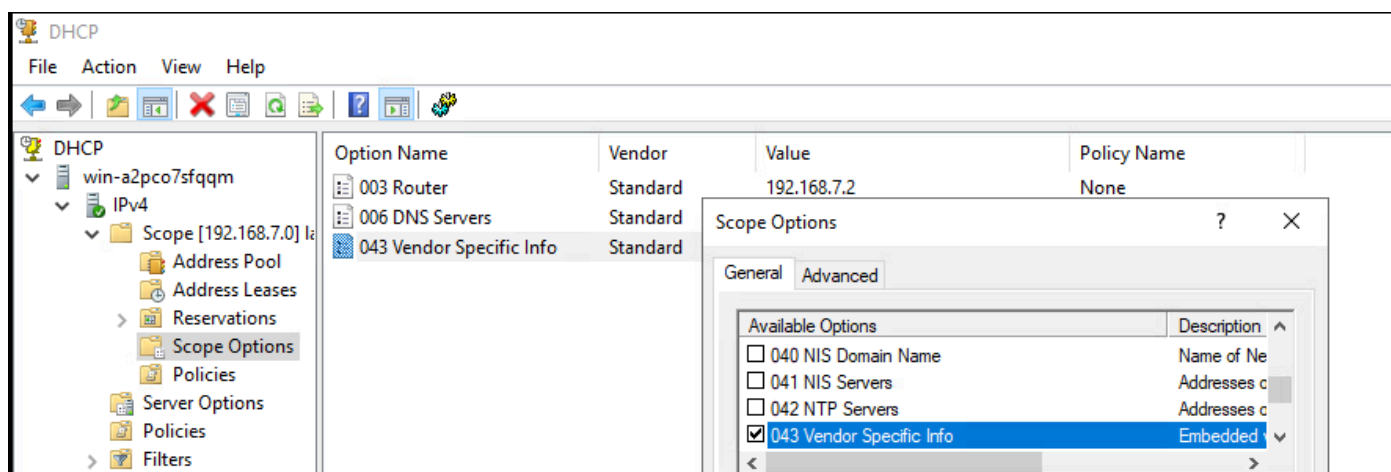
DHCP_Server_Config

4. Next, ga naar de Implementy optie, selecteer het FTD-apparaat waar u de wijzigingen wilt toepassen, en klik op Implementeren om de implementatie van de platforminstellingen te initiëren.

Schakel optie 43 in op externe DHCP-server

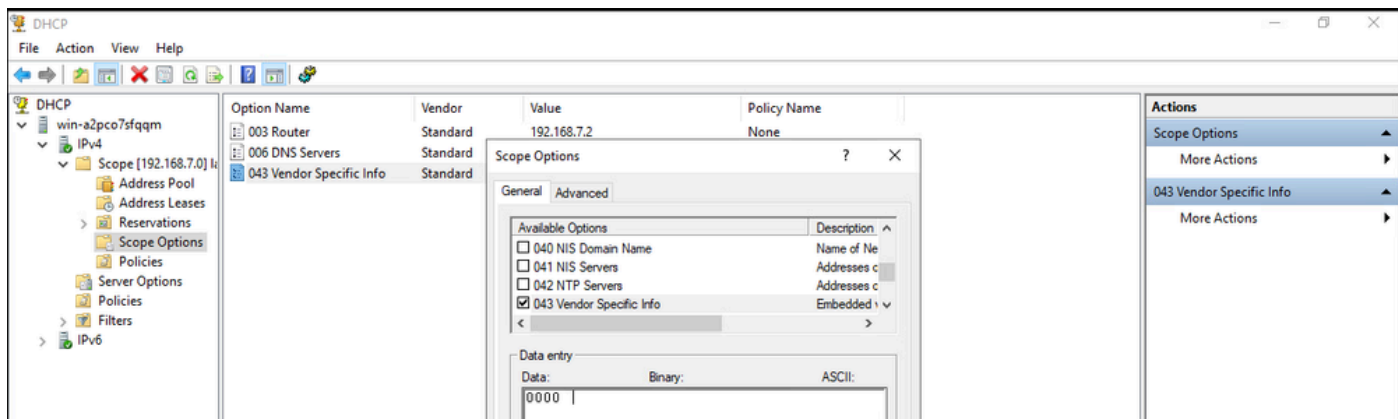
vriendelijke opmerking: Volgens RFC 2132 is de minimumlengte voor optie 43 1.

Navigeer naar uw DHCP-serverinstellingen en ga naar IPv4, selecteer vervolgens Scope and Scope Options >More Actions >Configure Options en schakel optie 43 in



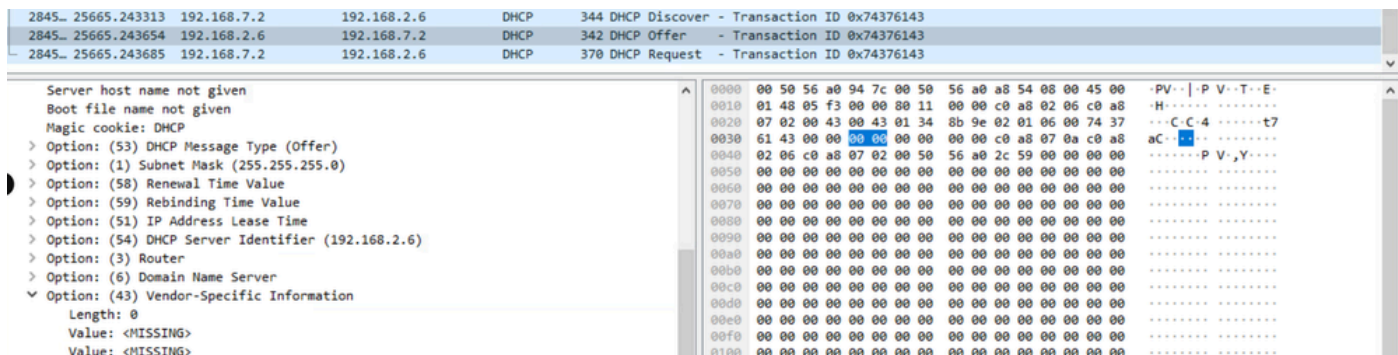
Enable_Option_43_On_external_DHCP_server

Aanvankelijk laat de standaardinstelling de waarde leeg, waardoor FTD het pakket laat vallen en categoriseert als misvormd.



Default_Config_Of_Option_43

Van de serverkant met Wireshark zien we dat in het OFFER-pakket de waarde ontbreekt voor optie 43 wanneer de lengte 0 is.



Non_Working_Server_Side_pcap

De pakketten worden door Cisco Firepower Threat Defence (FTD) gedropt, omdat ze een lengte van 0 hebben en als misvormd worden beschouwd, in strijd met 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.
```

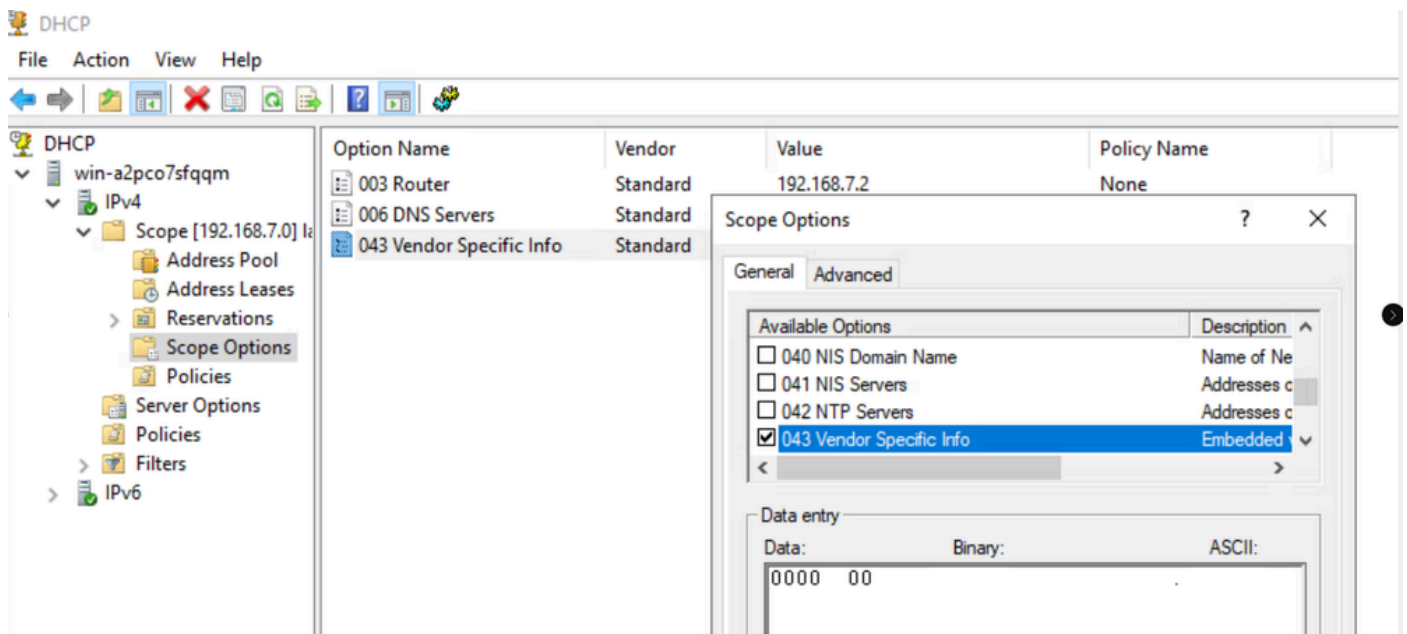
DHCPRA: setting giaddr to 192.168.7.2.

DHCPRA: Server request counter 1

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

Om de binaire waarde aan te passen om groter te zijn dan 0 in overeenstemming met RFC 2132, dubbelklik op het veld 043 leverancier specifieke info en stel de waarde in op 00, zoals in de afbeelding wordt weergegeven.

Deze wijziging zorgt ervoor dat het IP-adres met succes wordt geleased aan de client.



Gewijzigd_Binair_Waarde_aan_1

Server side DORA proces wanneer waarde is ingesteld als 1 op Option 43

2848...	25882.406605	192.168.7.2	192.168.2.6	DHCP	344 DHCP Discover	- Transaction ID 0x9a608024
2848...	25882.406970	192.168.7.2	192.168.7.2	DHCP	342 DHCP Offer	- Transaction ID 0x9a608024
2848...	25882.409264	192.168.7.2	192.168.2.6	DHCP	370 DHCP Request	- Transaction ID 0x9a608024
2848...	25882.409833	192.168.2.6	192.168.7.2	DHCP	342 DHCP ACK	- Transaction ID 0x9a608024

Client hardware address padding: 00000000000000000000	0010 01 48 05 f4 00 00 00 11 00 00 c0 a8 02 06 c0 a8	H.....
Server host name not given	0020 07 02 00 43 00 43 01 34 8b 9e 02 01 06 00 9a 60	..C.C-4.....
Boot file name not given	0030 80 24 00 00 00 00 00 00 00 c0 a8 07 0a c0 a8	.\$.....
Magic cookie: DHCP	0040 02 06 c0 a8 07 02 00 50 56 a0 2c 59 00 00 00 00	P.V.,Y.....
> Option: (53) DHCP Message Type (Offer)	0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
> Option: (1) Subnet Mask (255.255.255.0)	0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
> Option: (58) Renewal Time Value	0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
> Option: (59) Rebinding Time Value	0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
> Option: (51) IP Address Lease Time	0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
> Option: (54) DHCP Server Identifier (192.168.2.6)	00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
> Option: (3) Router	00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
> Option: (6) Domain Name Server	00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
> Option: (43) Vendor-Specific Information	00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
Length: 1	00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
Value: 00	00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
> Option: (255) End	0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
	0110 00 00 00 00 00 00 00 63 82 53 63 35 01 02 01 04 ff	C.Sc5.....
	0120 ff ff 00 3a 04 00 05 46 00 3b 04 00 09 3a 80 33	F.;.....3

Server_Side_Working_pcap

Klantzijde DORA proces wanneer waarde is ingesteld als 1 op Optie 43 en we kunnen zien dat de client wordt geleased met een 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·H·E·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)
DHCPRA: relay binding found for client 0050.56a0.2c59.
DHCPRA: 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
DHCPRA: relay binding found for client 0050.56a0.2c59.
DHCPD/RA: creating ARP entry (192.168.7.10, 0050.56a0.2c59).
DHCPRA: forwarding reply to client 0050.56a0.2c59.
DHCPRA: Client Ip Address :192.168.7.10
DHCPRA: 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)
DHCPRA: relay binding found for client 0050.56a0.2c59.
DHCPRA: Server requested by client 192.168.2.6
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.
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
DHCPRA: relay binding found for client 0050.56a0.2c59.
DHCPRA: 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).
DHCPRA: forwarding reply to client 0050.56a0.2c59.

DHCPRA: Client Ip Address :192.168.7.10

DHCPRA: subnet mask in dhcp options :255.255.255.0

```

Verifiëren

Zorg ervoor dat de FTD is geregistreerd bij het FMC voordat u de DHCP-server of het relay installeert. Controleer bovendien of er connectiviteit is met de DHCP-server in de DHCP Relay-configuratie.

```
<#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
```

Om de configuratie van de DHCP Relay Agent te verifiëren vanuit de FTD CLI.

```
<#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
```

Problemen oplossen

U kunt het probleem als volgt oplossen:

1. Controleer de routing tussen de FTD en de DHCP-server om er zeker van te zijn dat deze vanaf de DHCP-server bereikbaar is.
2. Zorg ervoor dat de DHCP-server een route heeft om toegang te krijgen tot de DHCP Relay Agent-interface.
3. Om het probleem op te lossen dat de client geen IP-adres ontvangt, kunt u een pakketopname op de FTD routed interface uitvoeren.

Hierdoor kunt u het DORA-proces van de DHCP-server in het pakket onderzoeken.

U kunt de [Use Firepower Threat Defence Captures en Packet Tracer](#) gebruiken om de pakketopname effectief uit te voeren.

Om een specifieke pakketopnamesessie die u eerder bent gestart, af te sluiten en te verwijderen, voert u deze onder de opdracht uit.

geen opname <Capture_name>

4. Om de staat te herzien en het DHCP te verzamelen debug, voer hieronder bevelen uit

Hiervoor inloggen op FTD CLI .

```
<#root>
```

```
system support diagnostic-cli
```

```
enable
```

Druk op ENTER.

```
<#root>
```

```
show dhcprelay statistic
```

```
show dhcprelay state
```

Om te controleren als debug reeds toelaat, voer onder bevel uit.

```
<#root>
```

```
show debug
```

```
<#root>
```

To capture debug excute below commands

```
debug dhcprelay packet
```

```
debug dhcprelay event
```

```
<#root>
```

To disable debug

```
undebug all
```

Gerelateerde informatie

[DHCP-server en relay op FTD met FMC configureren](#)

[DHCP en DNS](#)

[Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.