# Abilita opzioni ambito DHCP sul server DHCP tramite FTD come agente di inoltro

## Sommario



## Introduzione

In questo documento viene descritto come abilitare le opzioni sul server DHCP utilizzando in FTD gestito da FMC.

## Prerequisiti

### Requisiti

- Conoscenza della tecnologia Firepower
- Conoscenza del server/inoltro DHCP (Dynamic Host Control Protocol).

### Componenti usati

- Il riferimento delle informazioni contenute in questo documento è Virtual Cisco FTD e FMC, versione 7.4.0
- Windows Server 2019 viene utilizzato come server DHCP

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

# Premesse

Il dispositivo di difesa dalle minacce può trasmettere informazioni utilizzando le opzioni DHCP specificate nella RFC 2132, RFC 2562 e RFC 5510.

Supporta tutte le opzioni DHCP con numero da 1 a 255, ad eccezione delle opzioni 1, 12, 50-54, 58-59, 61, 67 e 82.

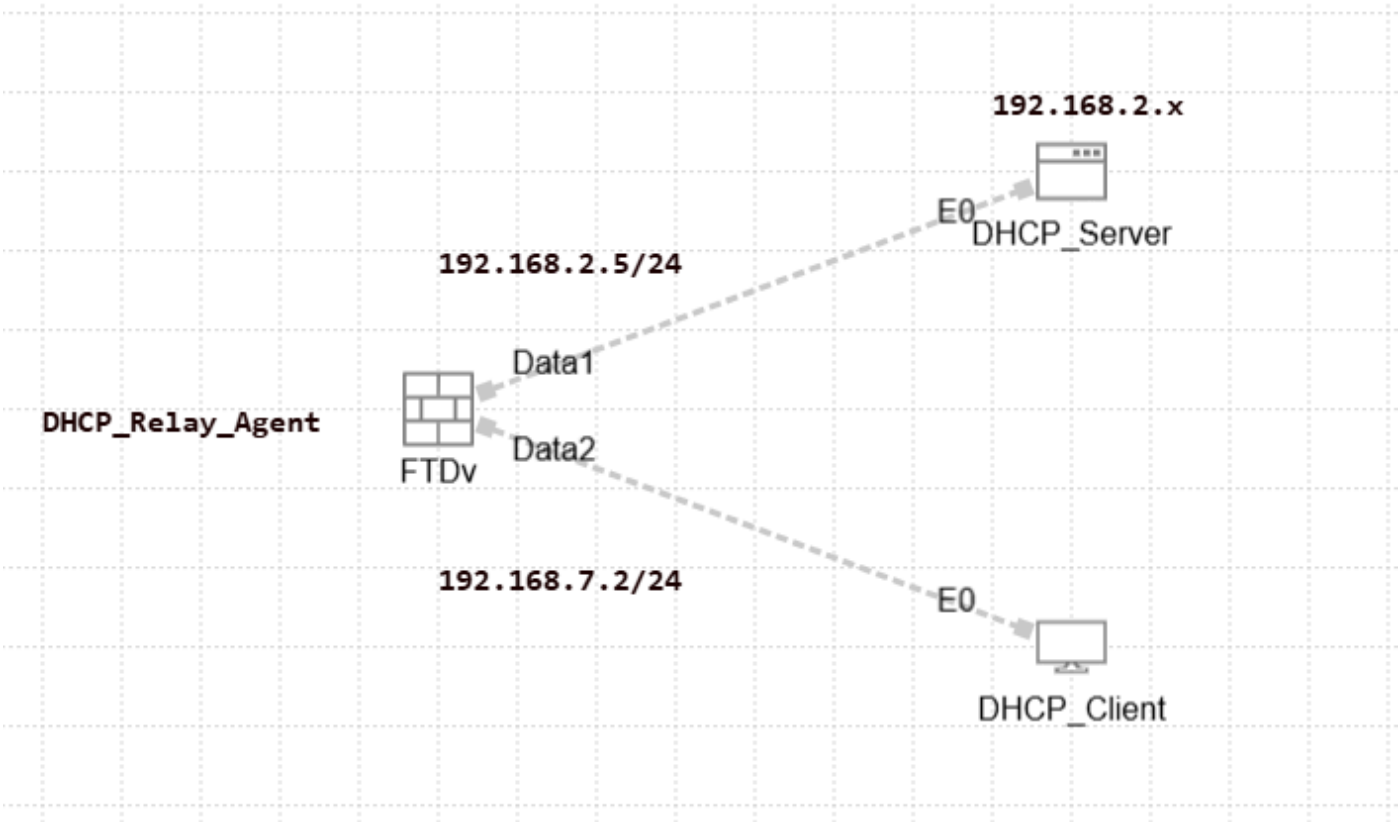
La RFC 2132 specifica due opzioni DHCP utilizzabili dal fornitore: Opzione 60 e opzione 43.

In questo documento vengono fornite configurazioni di esempio e viene illustrato il funzionamento dell'opzione DHCP 43 (Vendor-Specific Info) su Windows Server 2019, con FTD che funziona come agente di inoltro DHCP.

L'opzione 43 consente ai server DHCP di trasmettere ai client informazioni specifiche del fornitore, facilitando l'individuazione e la connessione ai controller da parte di dispositivi quali i punti di accesso, anche quando si trovano su VLAN o subnet diverse.

# Configurazione

## Esempio di rete




Diagramma_rete

## Configura inoltro DHCP

L'interfaccia FTD funziona come agente di inoltro DHCP, facilitando la comunicazione tra il client e un server DHCP esterno.

Ascolta le richieste del client e aggiunge i dati di configurazione essenziali, ad esempio le informazioni sul collegamento del client, necessari al server DHCP per allocare un indirizzo al client.

Dopo aver ricevuto una risposta dal server DHCP, l'interfaccia inoltra il pacchetto di risposta al client DHCP.

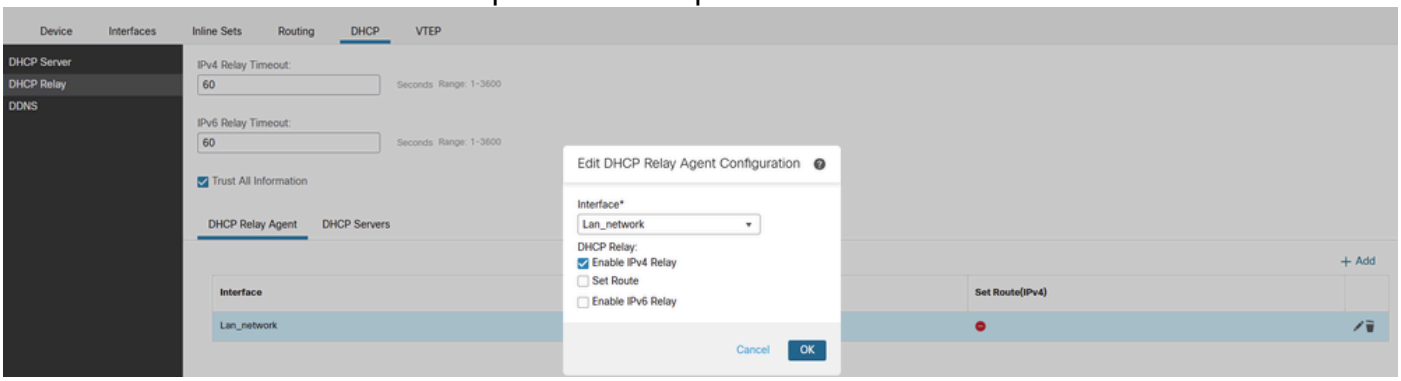
La configurazione dell'inoltro DHCP comporta due passaggi principali:
1. Configurare l'agente di inoltro DHCP.
2. Configurare il server DHCP esterno.

## Configura agente di inoltro DHCP

Per configurare l'inoltro DHCP, attenersi alla seguente procedura:

1. Passare a Dispositivi > Gestione dispositivi.
2. Fare clic sul pulsante Modifica relativo all'accessorio FTD.
3. Passare all'opzione DHCP > DHCP Relay (DHCP > Inoltro).
4. Fare clic su Aggiungi.

Interfaccia: Selezionare l'interfaccia appropriata dall'elenco a discesa. In questo punto l'interfaccia resta in ascolto delle richieste dei client e i client DHCP possono connettersi direttamente a questa interfaccia per le richieste di indirizzi IP.
Abilita inoltro DHCP: Selezionare questa casella per attivare il servizio di inoltro DHCP.




Configurazione agente di inoltro DHCP

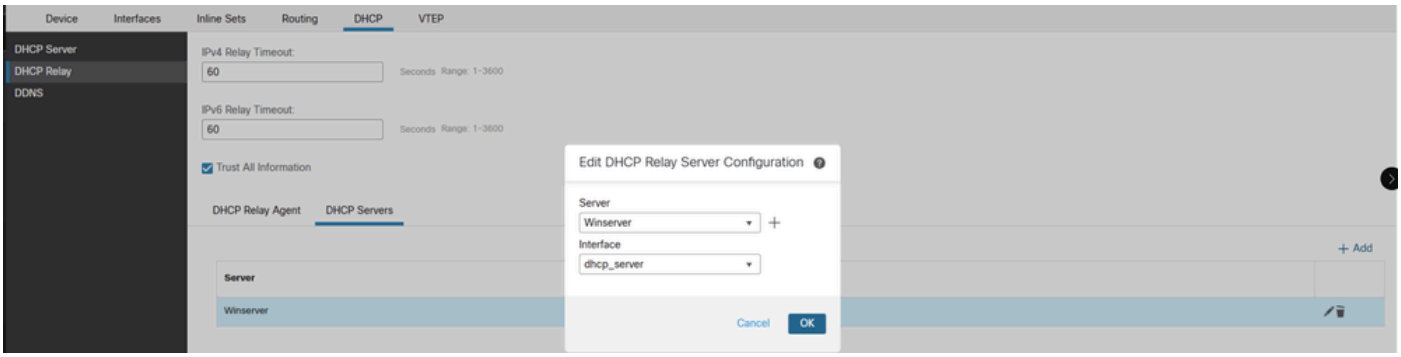
5. Fare clic su OK per salvare le impostazioni di configurazione dell'agente di inoltro DHCP.

## Configura server DHCP esterno

Per configurare l'indirizzo IP del server DHCP esterno a cui vengono inoltrate le richieste client, controllare i passaggi seguenti:

Passare alla sezione Server DHCP e fare clic su Add (Aggiungi)"
1. Nel campo Server, immettere l'indirizzo IP del server DHCP. È possibile scegliere un oggetto di rete esistente dal menu a discesa oppure crearne uno nuovo facendo clic sull'icona più (+).
2.Nel campo Interface (Interfaccia), specificare l'interfaccia che si connette al server DHCP.

3.Per salvare la configurazione, fare clic su OK. Quindi, fare clic su Save (Salva) per memorizzare le impostazioni della piattaforma.



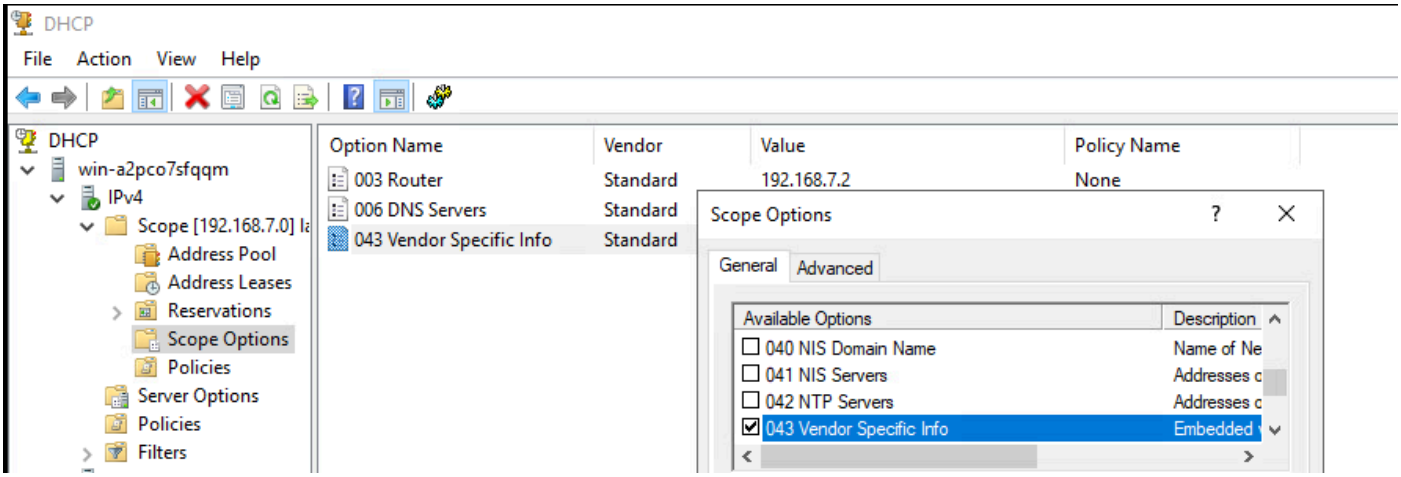

Configurazione server DHCP

4.Passare quindi all'opzione Deploy, selezionare l'accessorio FTD a cui si desidera applicare le modifiche e fare clic su Deploy (Distribuisci) per avviare la distribuzione delle impostazioni della piattaforma.

## Abilitare l'opzione 43 sul server DHCP esterno

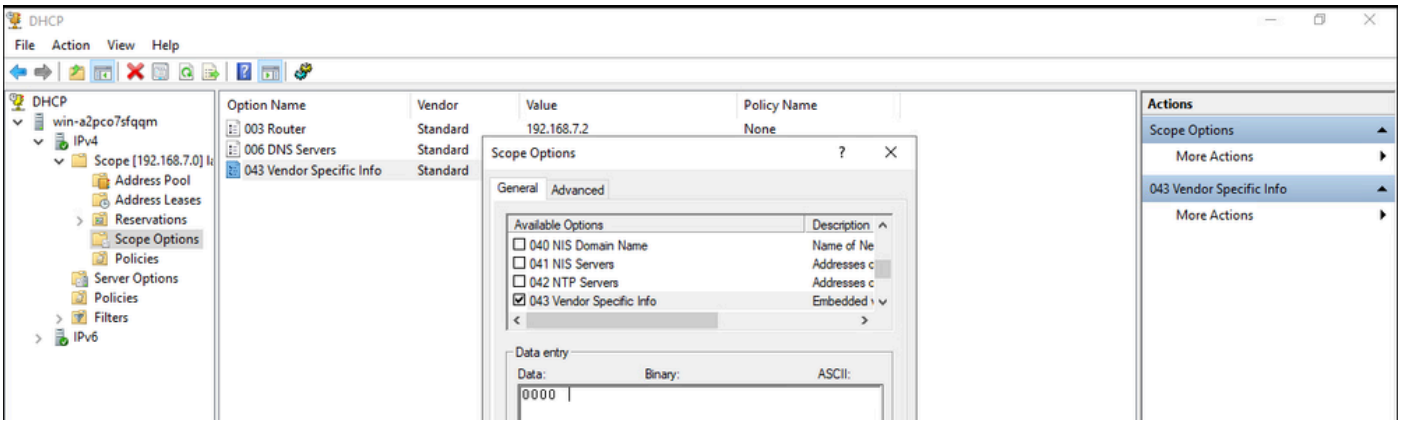
Nota: In base alla RFC 2132, la lunghezza minima per l'opzione 43 è 1.

Passare alle impostazioni del server DHCP e andare su IPv4, quindi selezionare Scope and Scope Options > More Actions >Configure Options (Opzioni di ambito e ambito) e abilitare l'opzione 43



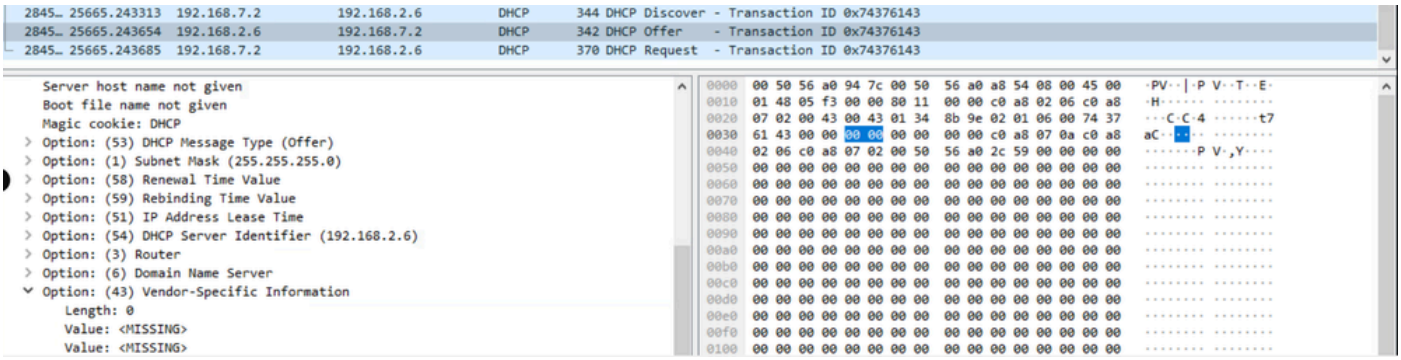

Enable_Option_43_On _External_DHCP_Server

Inizialmente, l'impostazione predefinita lascia il valore vuoto, portando FTD a eliminare il pacchetto e a classificarlo come non valido.




Default_Config_Of_Option_43

Dal lato server, utilizzando Wireshark, si osserva che nel pacchetto offer, il valore per l'opzione 43 è assente quando la lunghezza è 0.




Server_non_funzionante_side_pcap

I pacchetti vengono scartati da Cisco Firepower Threat Defense (FTD) perché hanno una lunghezza di 0 e sono considerati in formato non corretto, violando la 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
DHCPRA: relay binding created 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: option 43 is malformed.**

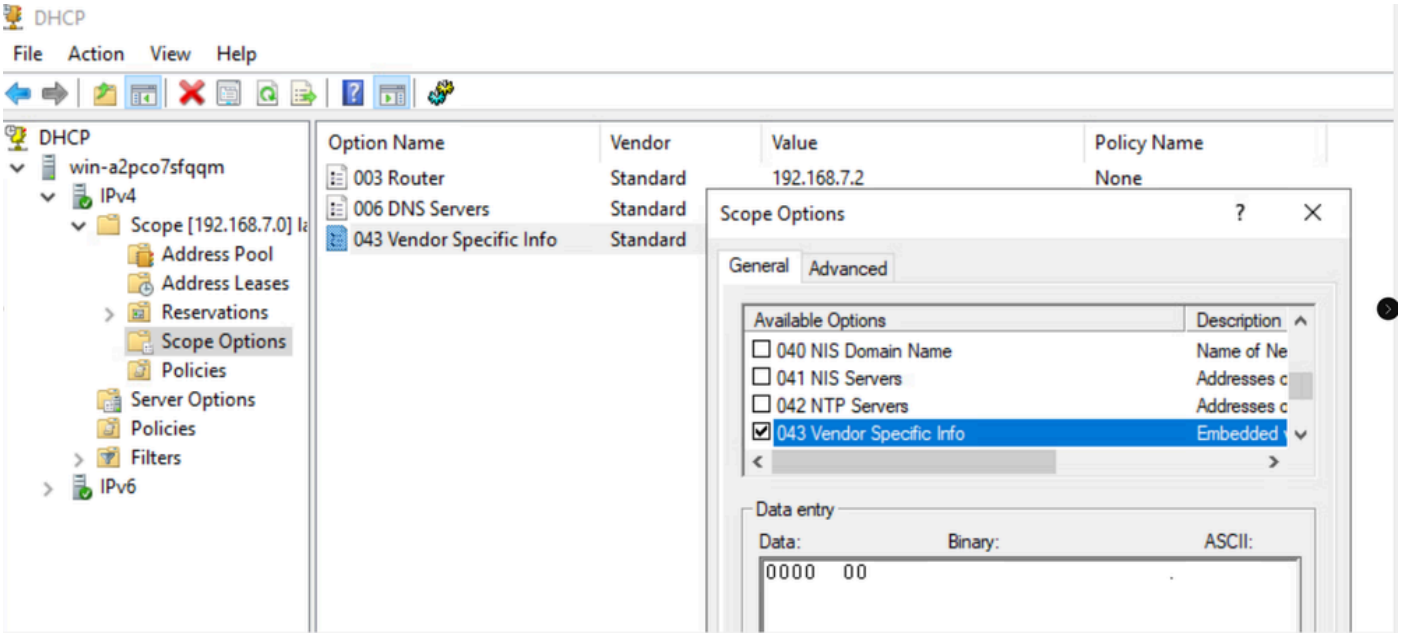
**DHCPD/RA: Unable to load workspace.**

DHCPD/RA: Relay msg received, fip=ANY, fport=0 on Lan_network interface
DHCP: Received a BOOTREQUEST from interface 3 (size = 328)
DHCPRA: 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.
```

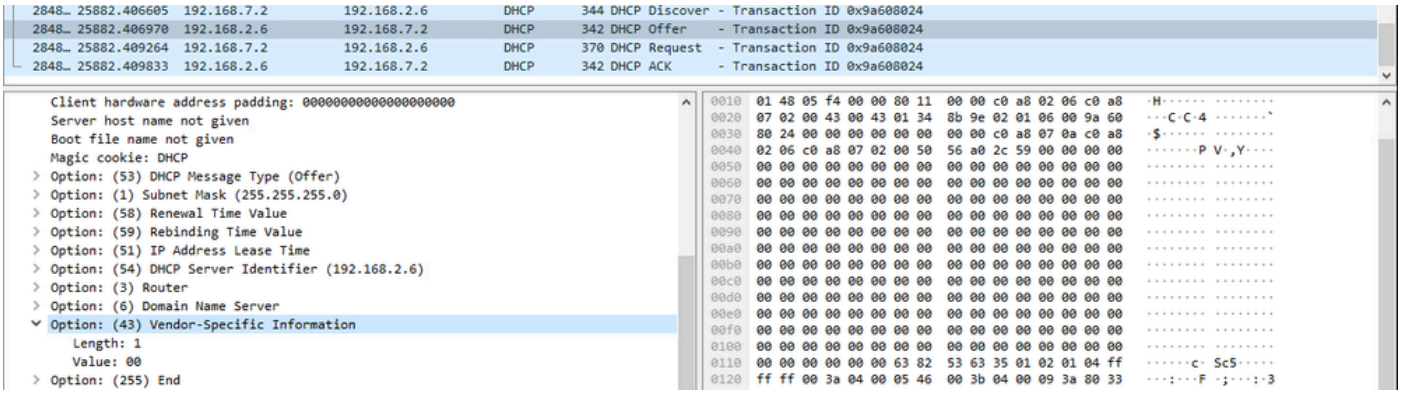
Per impostare un valore binario maggiore di 0 in conformità alla RFC 2132, fare doppio clic sul campo 043 Vendor Specific Info (Informazioni specifiche del fornitore) e impostare il valore su 00, come mostrato nell'immagine.

Questa modifica garantisce che l'indirizzo IP sia assegnato correttamente in lease al client.



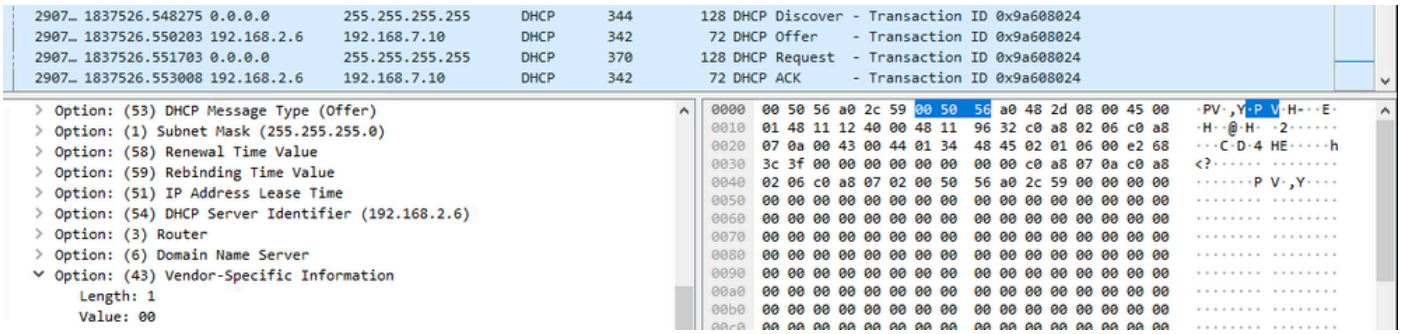

Valore_binario_modificato_in_1

Processo DORA sul lato server quando il valore è impostato su 1 sull'opzione 43




Server_Side_Working_pcap

Il processo DORA sul lato client viene eseguito quando il valore è impostato su 1 sull'opzione 43 e il client viene concesso in leasing con un indirizzo IP.




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**

# Verifica

Prima di configurare il server DHCP o il relay, accertarsi che l'FTD sia registrato nel FMC. Verificare inoltre che esista una connettività al server DHCP nella configurazione dell'inoltro 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**

Per verificare la configurazione dell'agente di inoltro DHCP dalla CLI 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
```

# Risoluzione dei problemi

Per risolvere il problema, considerare i seguenti punti:
1. Verificare il routing tra l'FTD e il server DHCP per accertarsi che sia raggiungibile dal server DHCP.
2.Verificare che il server DHCP disponga di una route per accedere all'interfaccia dell'agente di inoltro DHCP.
3. Per risolvere il problema del client che non riceve un indirizzo IP, è possibile eseguire un'acquisizione pacchetto sull'interfaccia di routing FTD.

In questo modo sarà possibile esaminare il processo DORA del server DHCP all'interno delle acquisizioni dei pacchetti.

Per acquisire i pacchetti in modo efficace, è possibile usare Use Firepower Threat Defense Capture e Packet Tracer.

Per interrompere ed eliminare una sessione di acquisizione pacchetti specifica avviata in precedenza, eseguire il comando seguente.
no capture <nome_acquisizione>

4. Per esaminare lo stato e raccogliere i comandi dhcprelay debug, eseguire i comandi seguenti

A tale scopo, effettuare il login alla CLI FTD.

<#root>

**system support diagnostic-cli**

**enable**

Premere Invio.

<#root>

**show dhcprelay statistic**

**show dhcprelay state**

Per verificare se il debug è già abilitato, eseguire il comando seguente.

<#root>

**show debug**

<#root>

To capture debug excute below commands

**debug dhcprelay packet**

```
debug dhcprelay event
```

```
<#root>
```

```
To disable debug
```

```
undebug all
```

## Informazioni correlate

Configurazione del server DHCP e dell'inoltro su FTD con FMC

DHCP e DNS

Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).