Aktivieren der DHCP-Bereichsoptionen auf dem DHCP-Server mithilfe von FTD als Relay Agent

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Optionen auf dem DHCP-Server aktivieren, indem Sie die FTD-Funktion verwenden, die vom FMC verwaltet wird.

Voraussetzungen

Anforderungen

- Kenntnisse der FirePOWER-Technologie
- Kenntnisse des Dynamic Host Control Protocol (DHCP)-Servers/DHCP-Relays

Verwendete Komponenten

- Die Informationen in diesem Dokument basieren auf Virtual Cisco FTD und FMC, Version 7.4.0.
- Windows Server 2019 wird als DHCP-Server verwendet

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Das Threat Defense-Gerät kann Informationen mithilfe der in RFC 2132, RFC 2562 und RFC 5510 angegebenen DHCP-Optionen übertragen.

Es unterstützt alle DHCP-Optionen mit den Nummern 1 bis 255, mit Ausnahme der Optionen 1, 12, 50-54, 58-59, 61, 67 und 82.

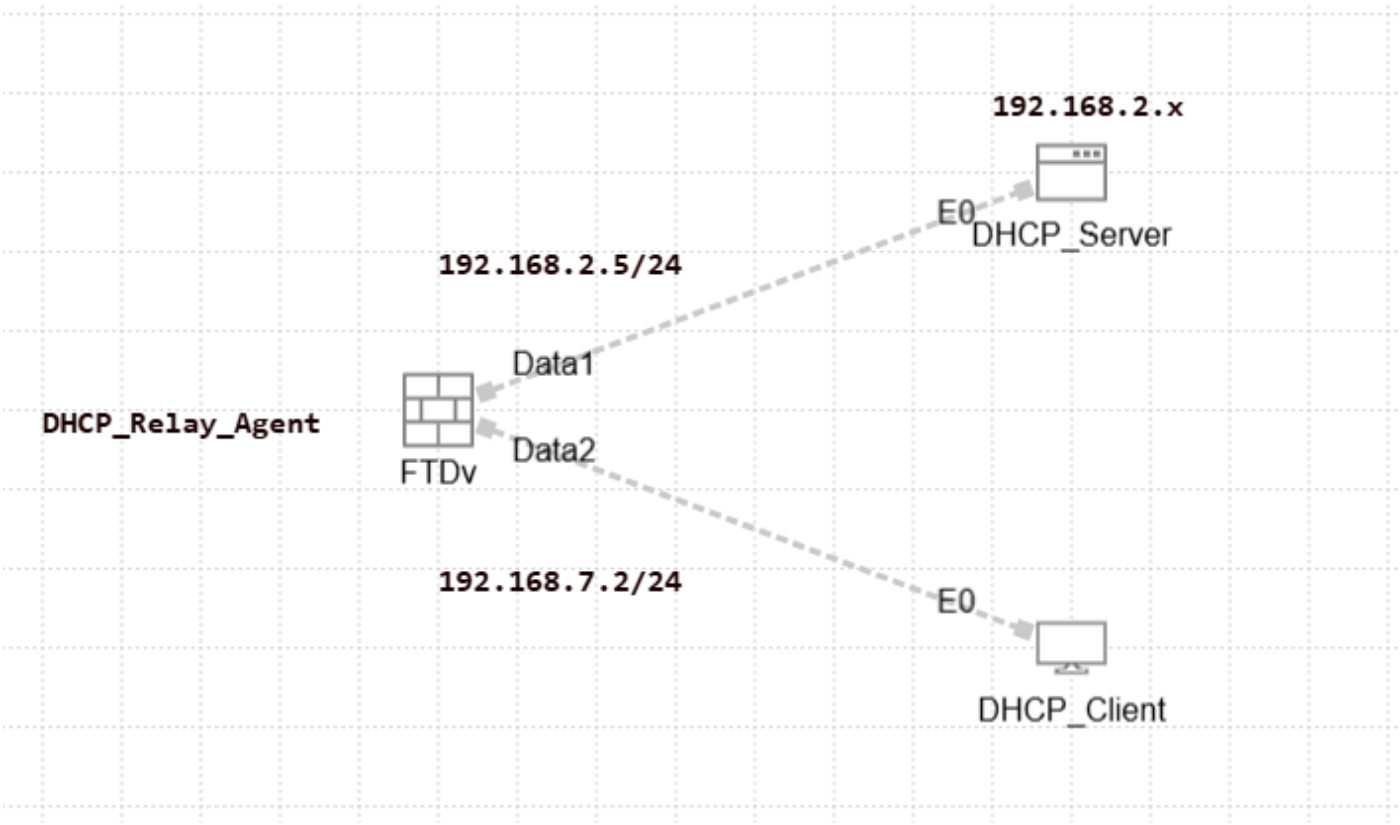
RFC 2132 legt zwei DHCP-Optionen für anbieterspezifische Konfigurationen fest: Die Antworten 60 und 43.

Das Dokument enthält Beispielkonfigurationen und zeigt, wie die DHCP-Option 43 (Herstellerspezifische Informationen) unter Windows Server 2019 funktioniert, wobei FTD als DHCP Relay Agent fungiert.

Option 43 ermöglicht DHCP-Servern die Übertragung anbieterspezifischer Informationen an Clients. So können Geräte wie Access Points ihre Controller leichter finden und eine Verbindung zu ihnen herstellen, selbst wenn sie sich in unterschiedlichen VLANs oder Subnetzen befinden.

Konfiguration

Netzwerkdiagramm



Netzwerkdiagramm

DHCP-Relay konfigurieren

Die FTD-Schnittstelle fungiert als DHCP-Relay-Agent und ermöglicht so die Kommunikation zwischen dem Client und einem externen DHCP-Server.

Er überwacht Client-Anfragen und fügt wichtige Konfigurationsdaten hinzu, z. B. die Client-Link-Informationen, die der DHCP-Server benötigt, um dem Client eine Adresse zuzuweisen.

Wenn die Schnittstelle eine Antwort vom DHCP-Server erhält, leitet sie das Antwortpaket zurück an den DHCP-Client.

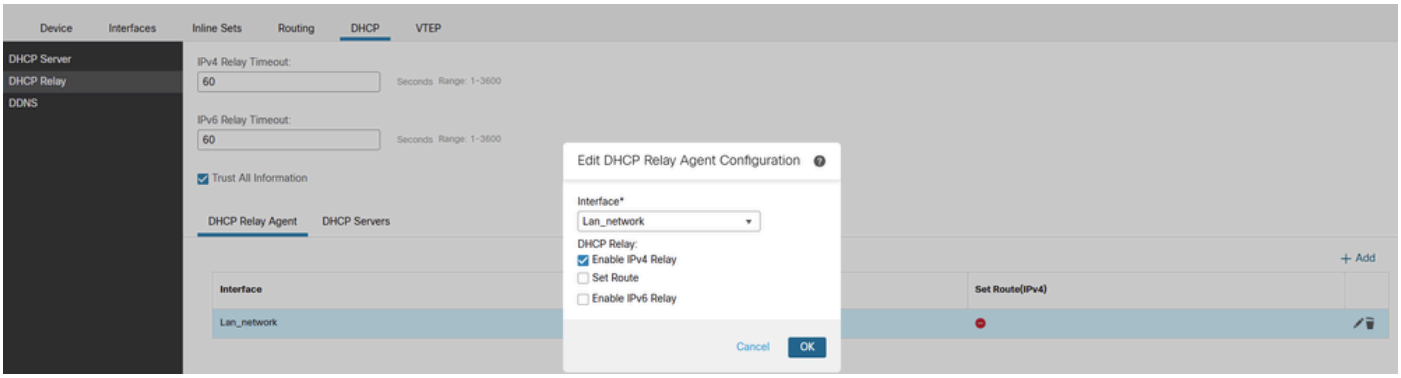
Die Konfiguration von DHCP Relay umfasst zwei primäre Schritte:
1. Richten Sie den DHCP Relay Agent ein.
2. Einrichten des externen DHCP-Servers

DHCP-Relay-Agent konfigurieren

Um das DHCP-Relay zu konfigurieren, gehen Sie wie folgt vor:

1. Navigieren Sie zu Geräte > Geräteverwaltung.
2. Klicken Sie auf die Schaltfläche Bearbeiten für die FTD-Einheit.
3. Navigieren Sie zu DHCP > DHCP Relay (DHCP > DHCP-Relay).
4. Klicken Sie auf Hinzufügen.

Schnittstelle: Wählen Sie die entsprechende Schnittstelle aus der Dropdown-Liste aus. Hier überwacht die Schnittstelle Client-Anfragen, und DHCP-Clients können sich direkt mit dieser Schnittstelle für IP-Adressen verbinden.
DHCP-Relay aktivieren: Aktivieren Sie dieses Kontrollkästchen, um den DHCP-Relay-Service zu aktivieren.



DHCP-Relay-Agent-Konfiguration

5.Klicken Sie auf OK, um die Konfigurationseinstellungen für den DHCP-Relay-Agenten zu speichern.

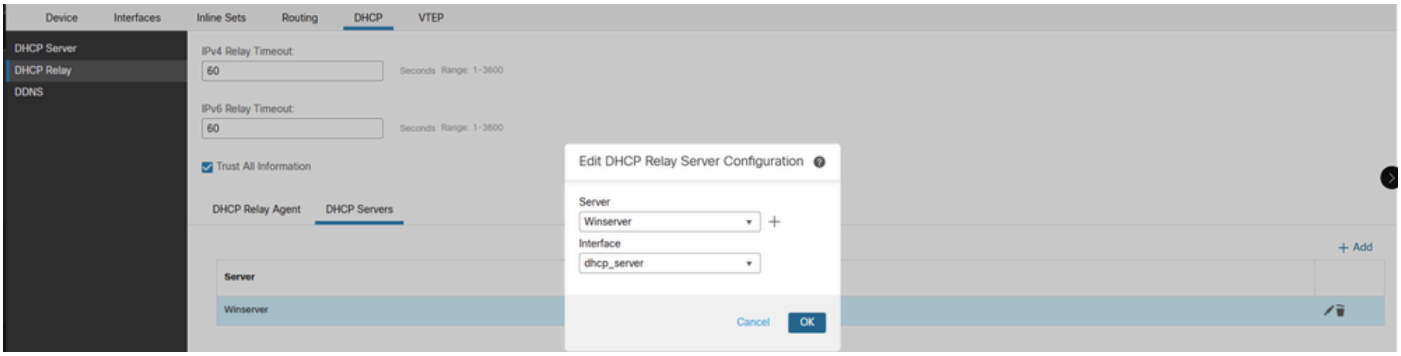
Externen DHCP-Server konfigurieren

Um die IP-Adresse des externen DHCP-Servers zu konfigurieren, an den Client-Anfragen

weitergeleitet werden, gehen Sie wie folgt vor:

Navigieren Sie zum Abschnitt DHCP-Server, und klicken Sie auf Hinzufügen"
1. Geben Sie im Feld Server die IP-Adresse des DHCP-Servers ein. Sie können entweder ein vorhandenes Netzwerkobjekt aus dem Dropdown-Menü auswählen oder ein neues Objekt erstellen, indem Sie auf das Pluszeichen (+) klicken.
2. Geben Sie im Feld Interface (Schnittstelle) die Schnittstelle an, die mit dem DHCP-Server verbunden wird.

3. Klicken Sie auf OK, um die Konfiguration zu speichern. Klicken Sie anschließend auf Speichern, um die Plattformeinstellungen zu speichern.



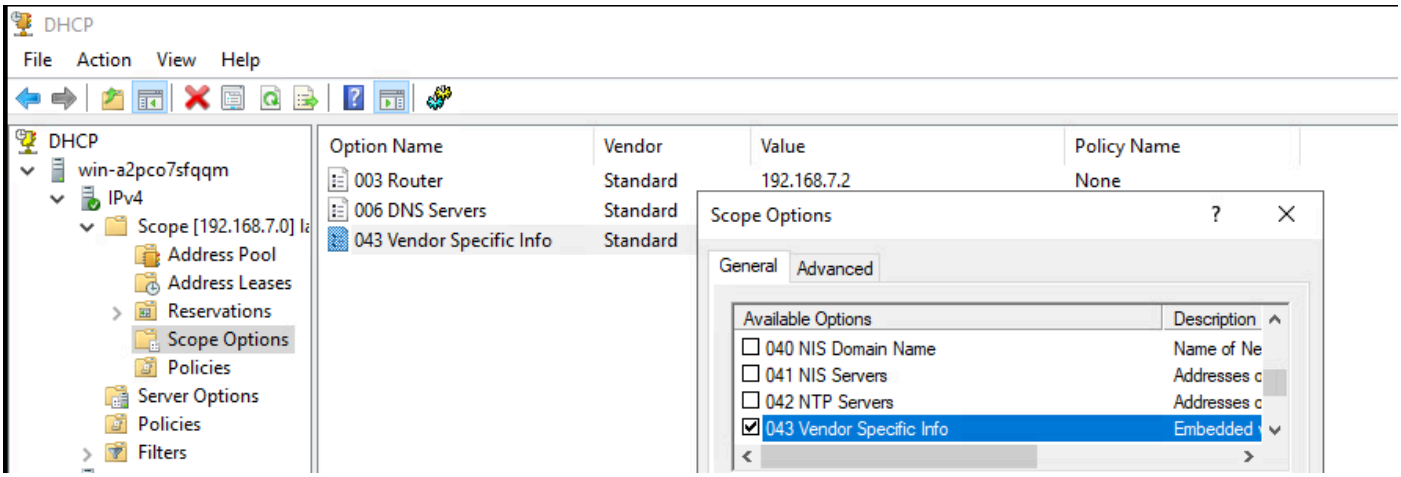
DHCP-Server-Konfiguration

4. Gehen Sie anschließend zur Option Deploy (Bereitstellen), wählen Sie die FTD-Appliance aus, in der die Änderungen angewendet werden sollen, und klicken Sie auf Deploy (Bereitstellen), um die Bereitstellung der Plattformeinstellungen zu initiieren.

Option 43 auf externem DHCP-Server aktivieren

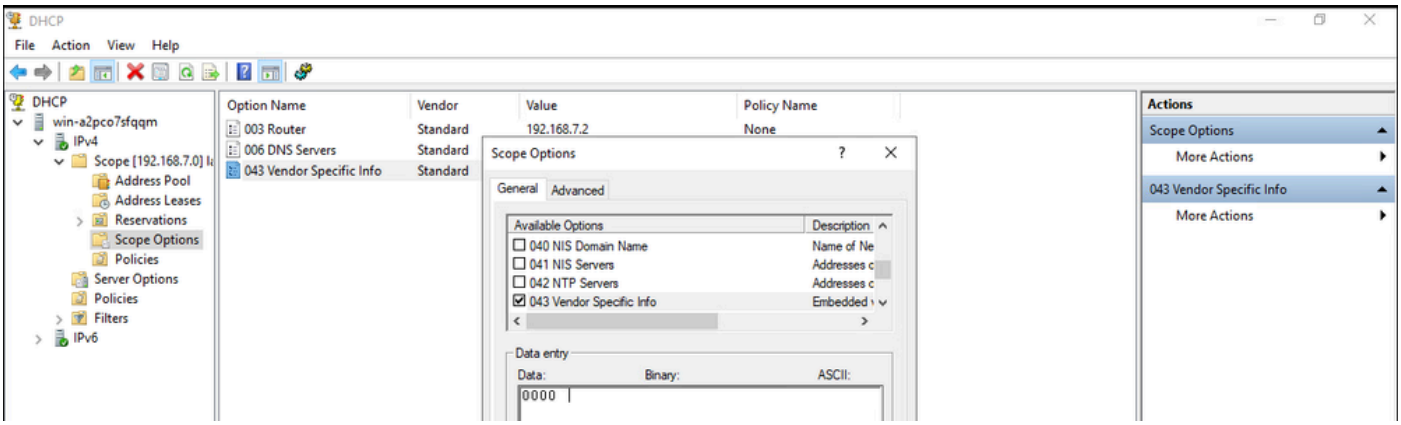
Bitte beachten: Gemäß RFC 2132 muss Option 43 mindestens 1 lang sein.

Navigieren Sie zu den DHCP-Servereinstellungen, und wechseln Sie zu IPv4. Wählen Sie dann Scope and Scope Options >More Actions >Configure Options aus, und aktivieren Sie Option 43.



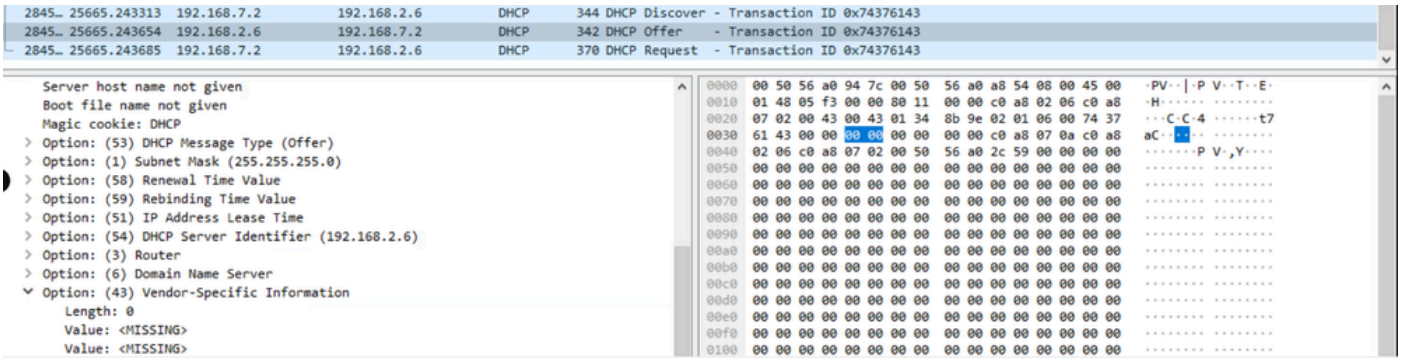
Enable_Option_43_On _External_DHCP_Server

Anfangs lässt die Standardeinstellung den Wert leer, sodass FTD das Paket verwirft und es als fehlerhaft kategorisiert.



default_config_of_option_43

Serverseitig stellen wir mithilfe von Wireshark fest, dass im OFFER-Paket der Wert für Option 43 fehlt, wenn die Länge 0 ist.



Nicht_Working_Server_Side_pcap

Die Pakete werden von Cisco FirePOWER Threat Defense (FTD) verworfen, da sie eine Länge von 0 haben und als fehlerhaft angesehen werden und somit gegen RFC 2132 verstoßen.

<#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.
```

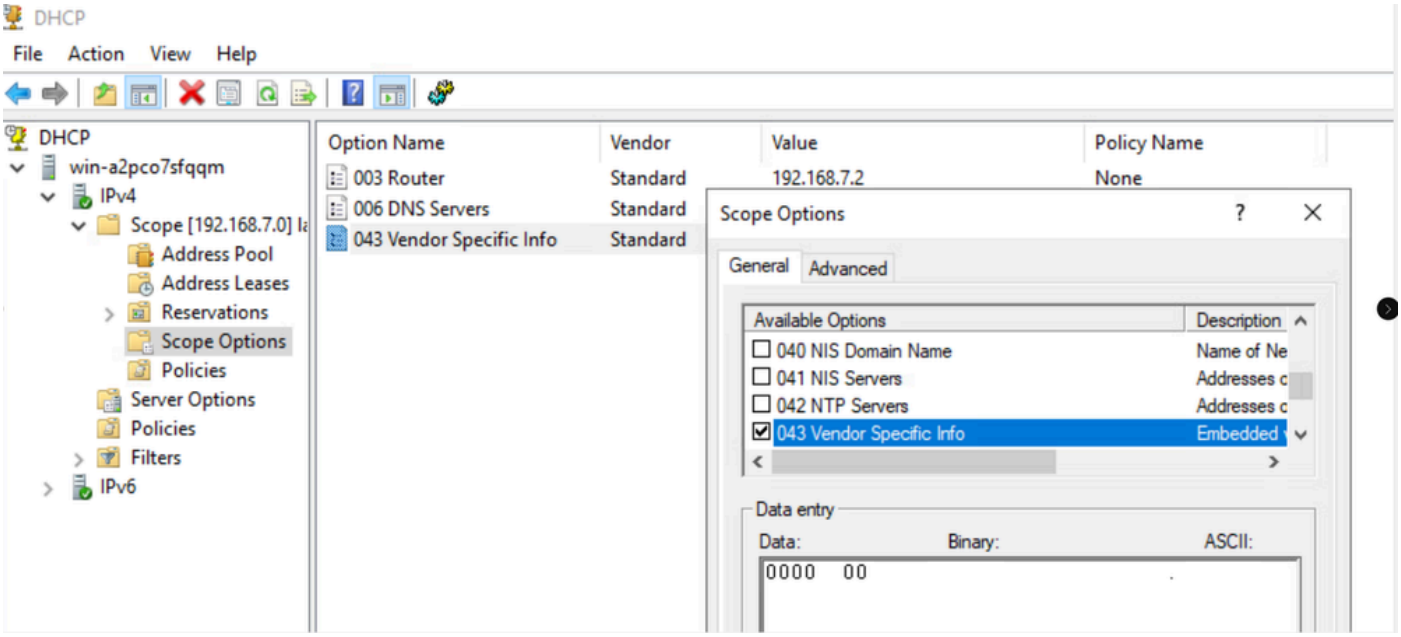
DHCPD/RA: option 43 is malformed.

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.
```

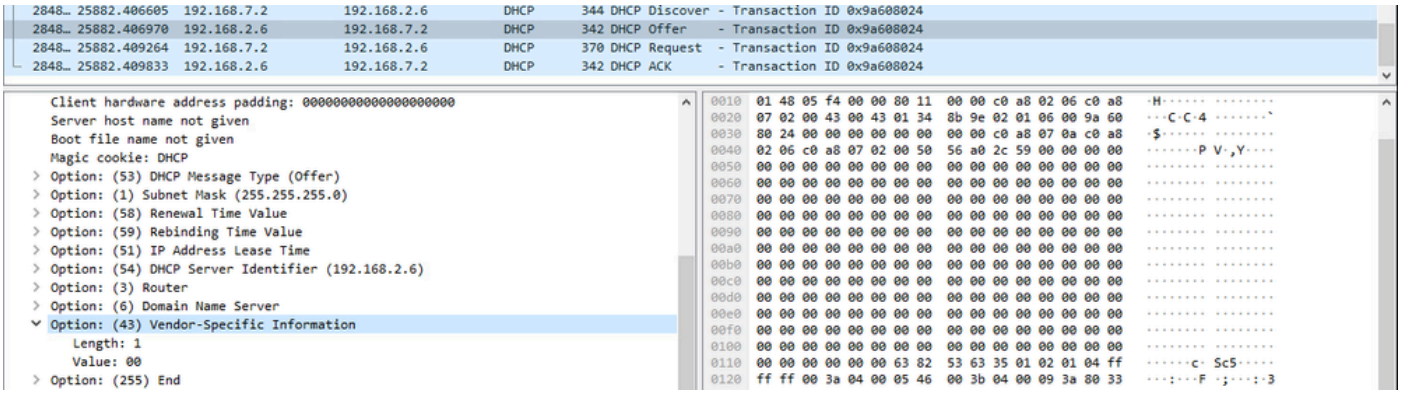
Um den Binärwert gemäß RFC 2132 auf größer als 0 einzustellen, doppelklicken Sie auf das Feld 043 Vendor Specific Info (Herstellerspezifische Informationen), und legen Sie den Wert auf 00 fest, wie im Bild dargestellt.

Diese Änderung stellt sicher, dass die IP-Adresse erfolgreich an den Client geleast wird.



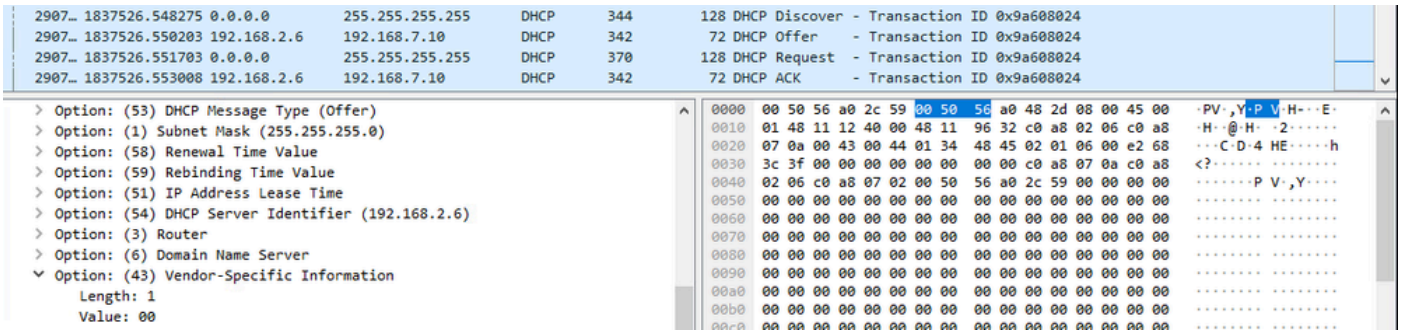
Changed_Binary_Value_to_1

Serverseitiger DORA-Prozess, wenn für Option 43 der Wert 1 festgelegt wird



Server_Seite_Working_pcap

Client-seitiger DORA-Prozess, wenn der Wert für Option 43 auf 1 gesetzt wird und wir sehen, dass der Client mit einer IP geleast wird.



Client_Seite_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

Überprüfung

Stellen Sie vor der Einrichtung des DHCP-Servers oder Relay sicher, dass der FTD beim FMC registriert ist. Überprüfen Sie außerdem, ob in der DHCP-Relay-Konfiguration eine Verbindung zum DHCP-Server besteht.

<#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

Zur Verifizierung der Konfiguration des DHCP Relay Agents über die 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
```

Fehlerbehebung

Um das Problem zu beheben, bedenken Sie folgende Punkte:
1.Überprüfen Sie das Routing zwischen FTD und DHCP-Server, um sicherzustellen, dass der DHCP-Server erreichbar ist.
2. Stellen Sie sicher, dass der DHCP-Server über eine Route für den Zugriff auf die DHCP Relay Agent-Schnittstelle verfügt.
3. Um das Problem zu beheben, dass der Client keine IP-Adresse empfängt, können Sie eine Paketerfassung über die FTD-geroutete Schnittstelle durchführen.

Dadurch können Sie den DORA-Prozess des DHCP-Servers innerhalb der Paketerfassungen untersuchen.

Sie können die Funktionen FirePOWER Threat Defense Captures und Packet Tracer nutzen, um die Paketerfassung effektiv durchzuführen.

Führen Sie den folgenden Befehl aus, um eine bestimmte zuvor gestartete Paketerfassungssitzung zu beenden und zu löschen.
keine Erfassung <capture_name>

4.To überprüfen Sie den Zustand und sammeln Sie die dhcprelay debug, führen Sie unten Befehle

Melden Sie sich dazu bei der FTD CLI an.

<#root>

system support diagnostic-cli

enable

Drücken Sie die Eingabetaste.

<#root>

show dhcprelay statistic

show dhcprelay state

Um zu überprüfen, ob ein Debugging bereits aktiviert ist, führen Sie den folgenden Befehl aus.

<#root>

show debug

<#root>

To capture debug excute below commands

debug dhcprelay packet

```
debug dhcprelay event
```

```
<#root>
```

```
To disable debug
```

```
undebug all
```

Zugehörige Informationen

DHCP-Server und Relay auf FTD mit FMC konfigurieren

DHCP und DDNS

Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.