リレーエージェントとしてFTDを使用してDHCPサーバのDHCPスコープオプションを有効にする

内容

はじめに

このドキュメントでは、FMCによって管理されるFTDでを使用してDHCPサーバのオプションを有効にする方法について説明します。

前提条件

要件

- FirePOWER の知識
- Dynamic Host Control Protocol(DHCP)サーバ/DHCPリレーに関する知識

使用するコンポーネント

- このドキュメントの情報は、仮想Cisco FTDおよびFMCバージョン7.4.0に基づいています。
- DHCPサーバとしてWindows Server 2019を使用

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

脅威対策デバイスは、RFC 2132、RFC 2562、およびRFC 5510で指定されているDHCPオプションを使用して情報を送信できます。

1 ~ 255のすべてのDHCPオプション（1、12、50 ~ 54、58 ~ 59、61、67、および82を除く）をサポートします。

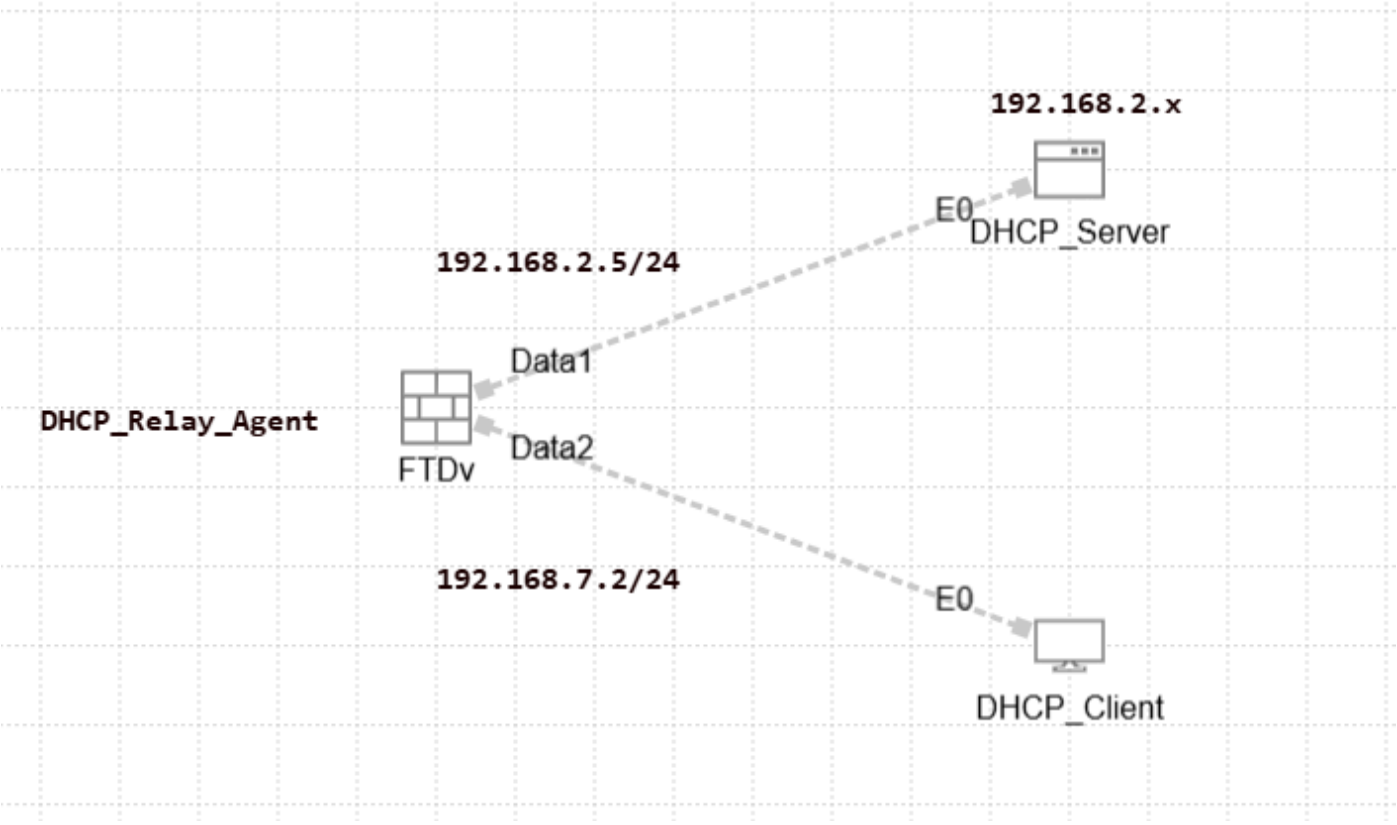
RFC 2132では、ベンダー固有の設定に関する2つのDHCPオプション（オプション60とオプション43）が規定されています。

このドキュメントでは、設定例を紹介し、FTDがDHCPリレーエージェントとして機能するWindows Server 2019でDHCPオプション43（ベンダー固有の情報）がどのように動作するかを説明します。

オプション43を使用すると、DHCPサーバはベンダー固有の情報をクライアントに送信できるため、アクセスポイントなどのデバイスが異なるVLANやサブネット上にあっても、コントローラの特定とコントローラへの接続が容易になります。

コンフィギュレーション

ネットワーク図



ネットワーク図

DHCPリレーの設定

FTDインターフェイスはDHCPリレーエージェントとして機能し、クライアントと外部DHCPサーバ間の通信を容易にします。

クライアント要求をリッスンし、クライアントリンク情報などの重要な設定データを追加します。この情報は、DHCPサーバがクライアントにアドレスを割り当てる際に必要です。

DHCPサーバからの応答を受信すると、インターフェイスは応答パケットをDHCPクライアントに転送します。

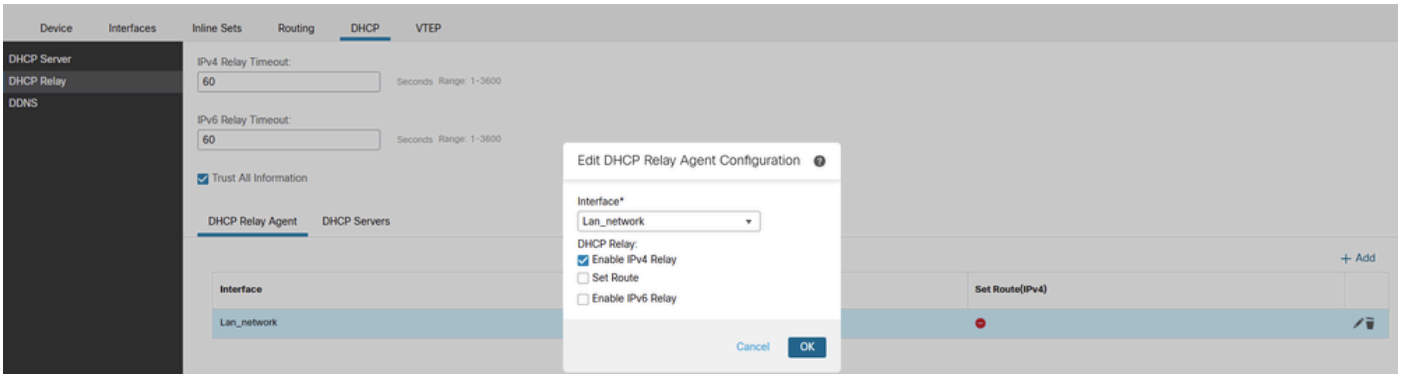
DHCPリレーの設定には、主に次の2つのステップがあります。
1. DHCPリレーエージェントをセットアップします。
2. 外部DHCPサーバーをセットアップします。

DHCPリレーエージェントの設定

DHCPリレーを設定するには、次の手順を確認します。

1. Devices > Device Managementの順に移動します。
2. FTDアプライアンスの編集ボタンをクリックします。
3. DHCP > DHCP Relayオプションに移動します。
4. Addをクリックします。

インターフェイス：ドロップダウンリストから適切なインターフェイスを選択します。ここで、インターフェイスはクライアント要求をリッスンし、DHCPクライアントはIPアドレス要求のためにこのインターフェイスに直接接続できます。
Enable DHCP Relay：このチェックボックスをオンにして、DHCPリレーサービスをアクティブにします。



DHCP_リレー_エージェント_設定

5. OKをクリックして、DHCPリレーエージェントの設定を保存します。

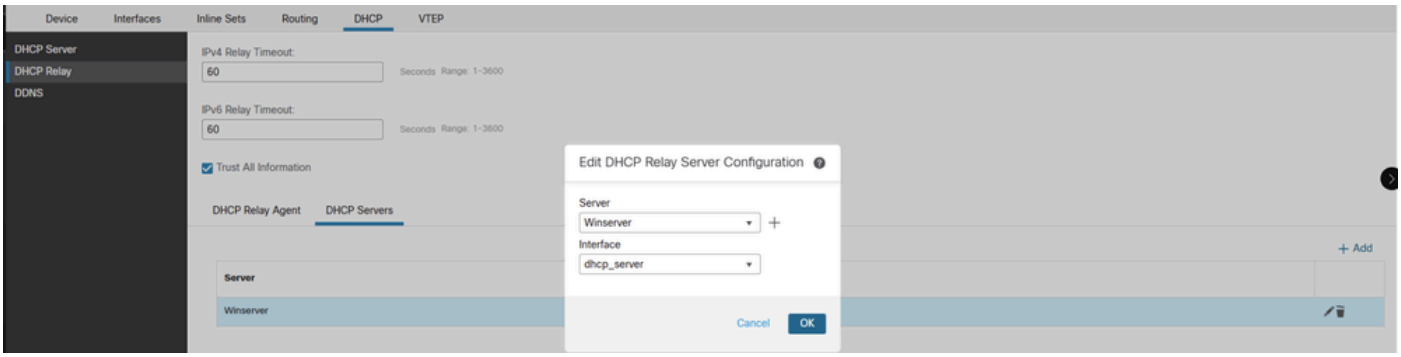
外部DHCPサーバの設定

クライアント要求の転送先となる外部DHCPサーバのIPアドレスを設定するには、次の手順を実

行します。

DHCP Serverセクションに移動し、Addをクリックします。
1. Serverフィールドに、DHCPサーバのIPアドレスを入力します。ドロップダウンメニューから既存のネットワークオブジェクトを選択するか、プラス(+)アイコンをクリックして新しいネットワークオブジェクトを作成できます。
2. Interfaceフィールドで、DHCPサーバに接続するインターフェイスを指定します。

3. 設定を保存するには、OKをクリックします。次に、Saveをクリックしてプラットフォーム設定を保存します。



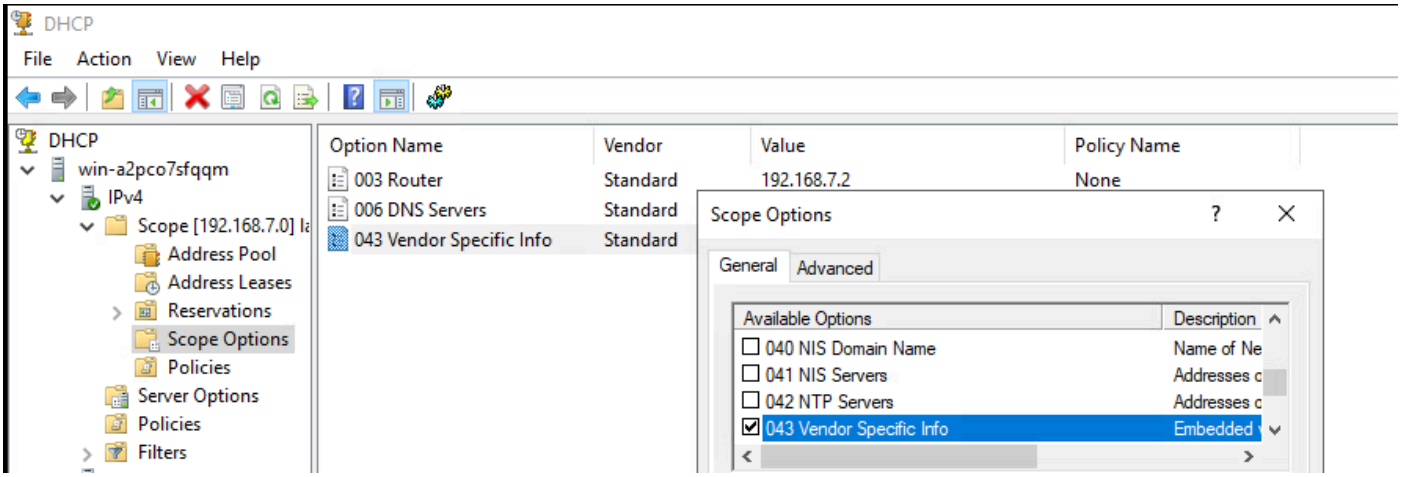
DHCPサーバ設定

4. 次に、Deployオプションに移動し、変更を適用するFTDアプライアンスを選択し、Deployをクリックしてプラットフォーム設定の導入を開始します。

外部DHCPサーバでオプション43を有効にする

注意：RFC 2132によれば、オプション43の最小長は1です。

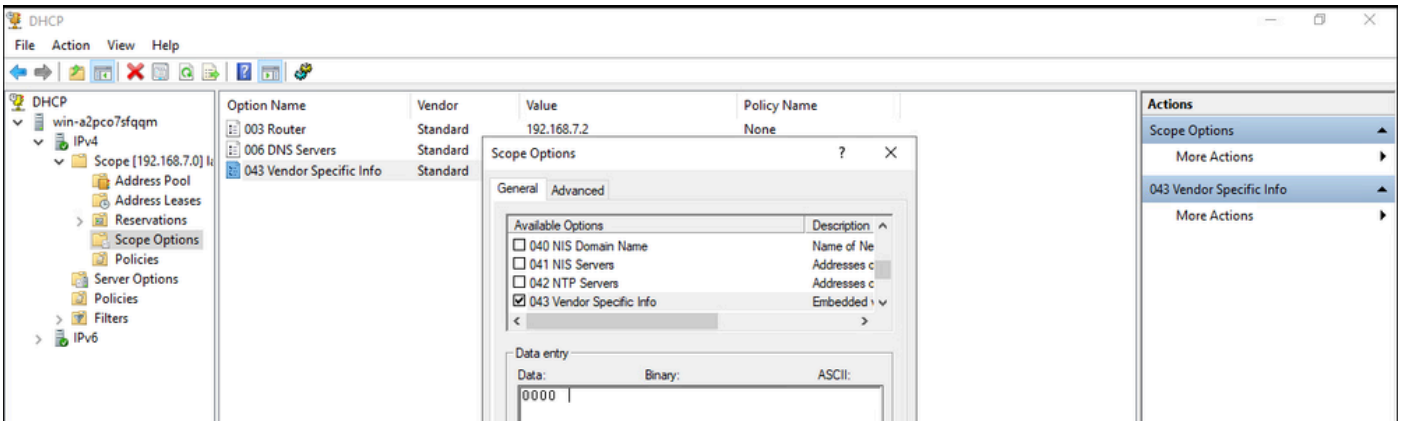
DHCPサーバ設定に移動し、IPv4に移動して、ScopeおよびScope Options >More Actions >Configure Optionsの順に選択し、オプション43をイネーブルにします



Enable_Option_43_On _External_DHCP_サーバ

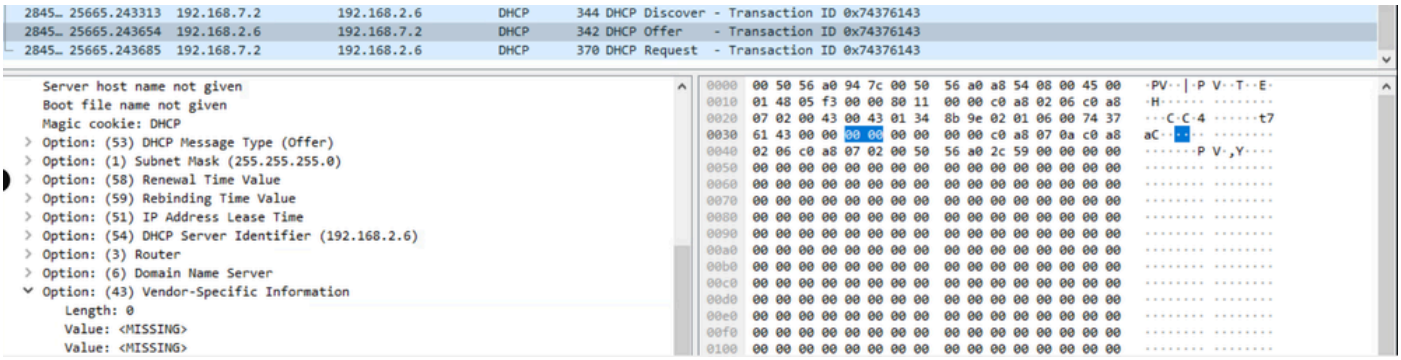
最初は、デフォルト設定ではこの値は空のままであるため、FTDはパケットをドロップし、不正

なパケットとして分類します。



Default_Config_Of_オプション_43

Wiresharkを使用しているサーバ側から、長さが0の場合にOFFERパケットのオプション43の値が欠落していることがわかります。



Non_Working_Server_Side_pcap

パケットの長さが0であり、RFC 2132に違反して不正と見なされるため、パケットはCisco Firepower Threat Defense(FTD)によってドロップされます。

<#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.
```

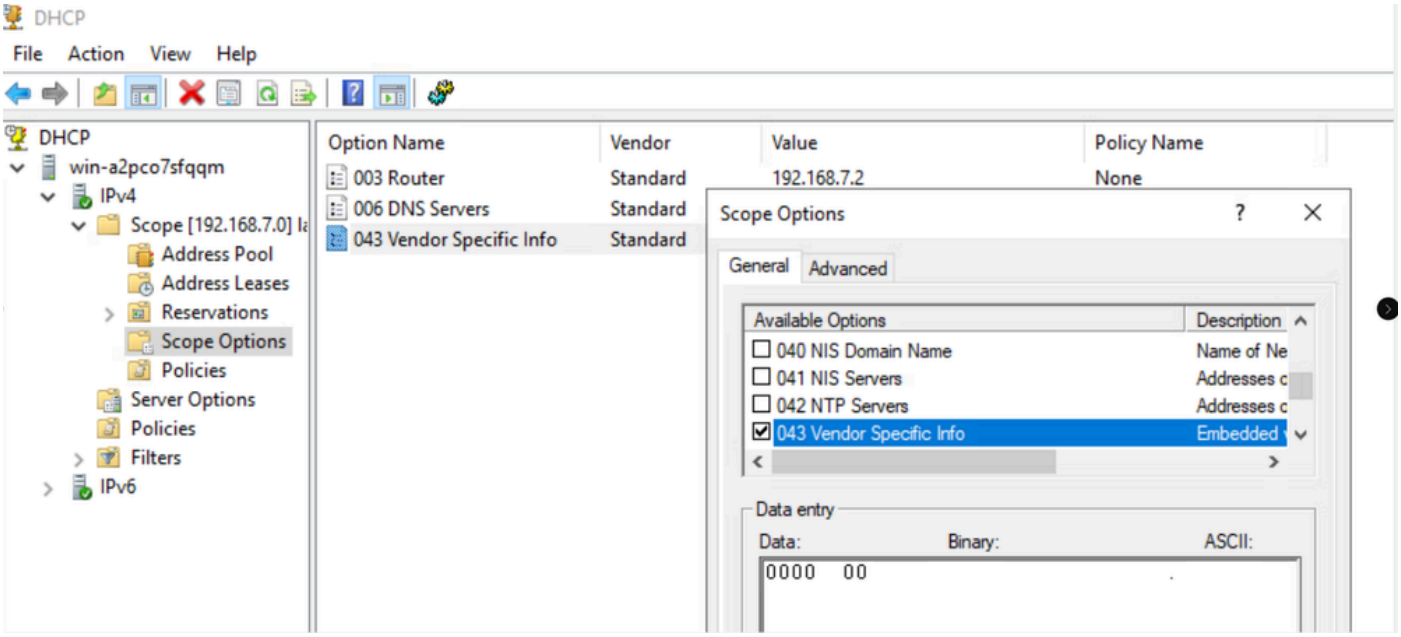
DHCPD/RA: option 43 is malformed.

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.
```

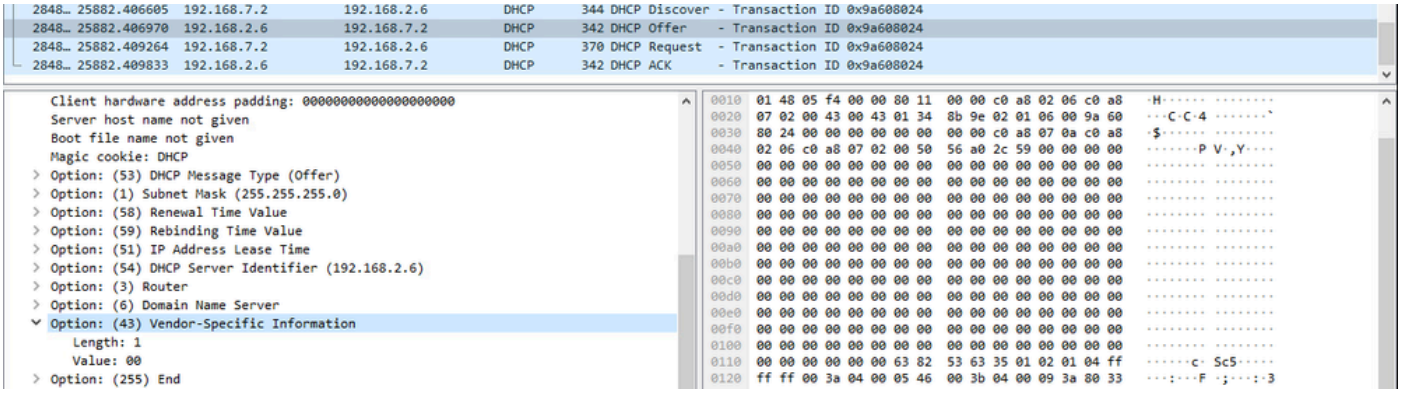
RFC 2132に従ってバイナリ値を0より大きくなるように調整するには、図に示すように、043 Vendor Specific Infoフィールドをダブルクリックし、値を00に設定します。

この変更により、IPアドレスがクライアントに正常にリースされます。



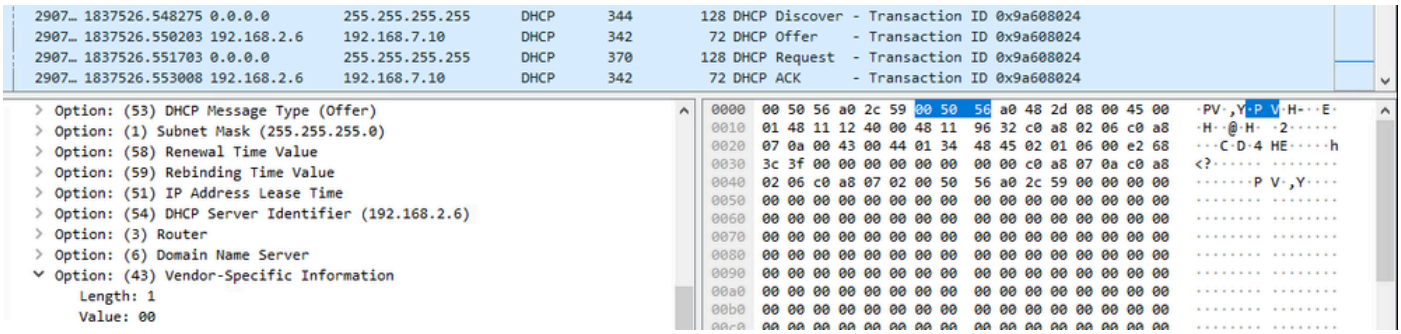
変更されたバイナリ値1へ

オプション43で値が1に設定されている場合のサーバー側のDORAプロセス



サーバ_サイド_作業_pcap

オプション43で値が1に設定されている場合、クライアント側のDORAプロセスにより、クライアントがIPを使用してリースされていることが確認できます。



クライアント_サイド_作業_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

確認

DHCPサーバまたはリレーを設定する前に、FTDがFMCに登録されていることを確認します。また、DHCPリレー設定にDHCPサーバへの接続があることを確認します。

```
<#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
```

FTD CLIからDHCPリレーエージェントの設定を確認します。

```
<#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
```

トラブルシュート

この問題をトラブルシューティングするには、次の点を考慮します。
1. FTDとDHCPサーバ間のルーティングを確認し、DHCPサーバから到達可能であることを確認します。
2. DHCPサーバにDHCPリレーエージェントインターフェイスにアクセスするルートがあることを確認します。
3. クライアントがIPアドレスを受信しない問題のトラブルシューティングを行うには、FTDルーテッドインターフェイスでパケットキャプチャを実行できます。

これにより、パケットキャプチャ内のDHCPサーバのDORAプロセスを調べることができます。

Firepower Threat Defense(FTD)のキャプチャとパケットトレーサの使用を利用して、パケットキャプチャを効果的に実行できます。

以前に開始した特定のパケットキャプチャセッションを停止および削除するには、次のコマンドを実行します。
キャプチャなし<capture_name>

4. 状態を確認してdhcprelay debugを収集するには、次のコマンドを実行します。

これを行うには、FTD CLIにログインします。

<#root>

system support diagnostic-cli

enable

Enter キーを押します。

<#root>

show dhcprelay statistic

show dhcprelay state

デバッグがすでに有効になっているかどうかを確認するには、次のコマンドを実行します。

<#root>

show debug

<#root>

To capture debug excute below commands

debug dhcprelay packet
debug dhcprelay event

<#root>

To disable debug

undebug all

関連情報

FMCを使用したFTDでのDHCPサーバとリレーの設定

DHCPおよびDDNS

テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。