FTD를 릴레이 에이전트로 사용하여 DHCP 서버에서 DHCP 범위 옵션 사용

목차

소개

이 문서에서는 FMC에서 관리하는 FTD에서 를 사용하여 DHCP 서버에서 옵션을 활성화하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

- firepower 기술에 대한 지식
- DHCP(Dynamic Host Control Protocol) 서버/DHCP 릴레이에 대한 지식

사용되는 구성 요소

- 이 문서의 정보는 Virtual Cisco FTD 및 FMC, 버전 7.4.0을 기반으로 합니다
- Windows Server 2019가 DHCP 서버로 사용됨

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

위협 방어 디바이스는 RFC 2132, RFC 2562 및 RFC 5510에 지정된 대로 DHCP 옵션을 사용하여 정보를 전송할 수 있습니다.

1, 12, 50-54, 58-59, 61, 67 및 82를 제외하고 1~255로 번호가 지정된 모든 DHCP 옵션을 지원합니다.

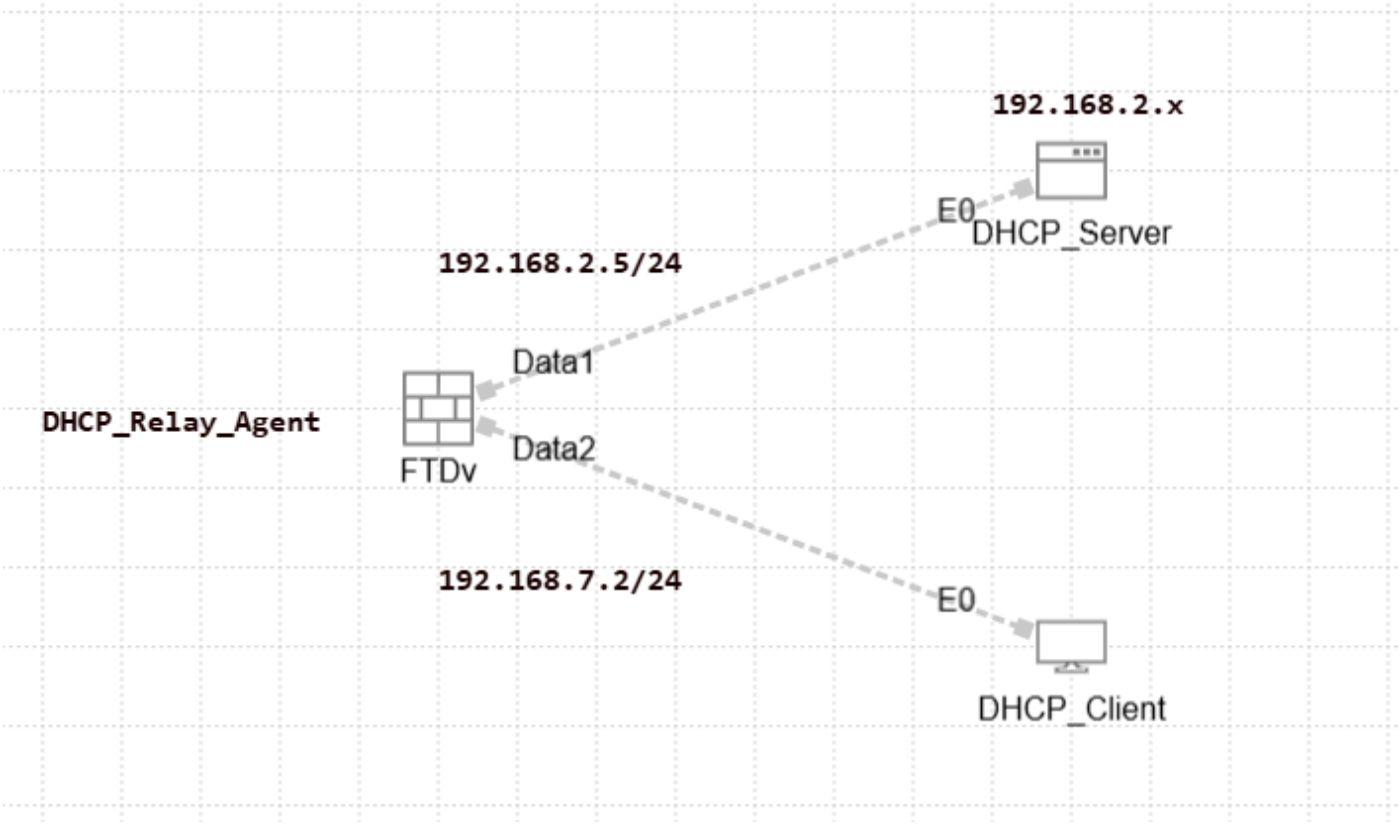
RFC 2132는 공급업체별 구성과 관련된 두 가지 DHCP 옵션을 지정합니다. 옵션 60 및 옵션 43.

이 문서에서는 샘플 컨피그레이션을 제공하고 FTD가 DHCP 릴레이 에이전트로 작동하는 Windows Server 2019에서 DHCP Option 43(Vendor-Specific Info)이 작동하는 방법을 설명합니다.

옵션 43을 사용하면 DHCP 서버가 공급업체별 정보를 클라이언트에 전송할 수 있으므로 액세스 포인트와 같은 장치가 서로 다른 VLAN 또는 서브넷에 있는 경우에도 컨트롤러를 찾아서 연결할 수 있습니다.

설정

네트워크 다이어그램



네트워크 다이어그램

DHCP 릴레이 구성

FTD 인터페이스는 DHCP 릴레이 에이전트 역할을 하여 클라이언트와 외부 DHCP 서버 간의 통신

을 용이하게 합니다.

클라이언트 요청을 수신하고 DHCP 서버가 클라이언트에 주소를 할당해야 하는 클라이언트 링크 정보와 같은 필수 컨피그레이션 데이터를 추가합니다.

DHCP 서버로부터 응답을 받으면 인터페이스는 회신 패킷을 DHCP 클라이언트로 다시 전달합니다 .

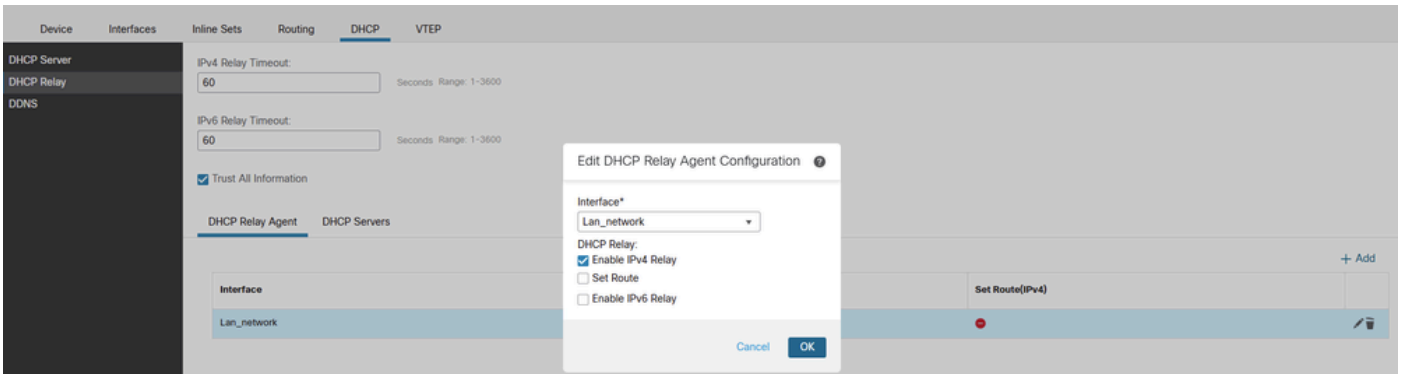
DHCP 릴레이 구성에는 두 가지 기본 단계가 포함됩니다.
1. DHCP 릴레이 에이전트를 설정합니다.
2. 외부 DHCP 서버를 설정합니다.

DHCP 릴레이 에이전트 구성

DHCP 릴레이를 구성하려면 아래 단계를 확인하십시오.

1. Devices(디바이스) > Device Management(디바이스 관리)로 이동합니다.
2. FTD 어플라이언스에 대한 편집 버튼을 클릭합니다.
3. DHCP > DHCP Relay(DHCP 릴레이) 옵션으로 이동합니다.
4. 추가를 클릭합니다.

인터페이스: 드롭다운 목록에서 적절한 인터페이스를 선택합니다. 여기서 인터페이스가 클라이언트 요청을 수신 대기하며 DHCP 클라이언트가 IP 주소 요청을 위해 이 인터페이스에 직접 연결할 수 있습니다.
DHCP 릴레이 활성화: DHCP 릴레이 서비스를 활성화하려면 이 확인란을 선택합니다.



DHCP_Relay_Agent_Config

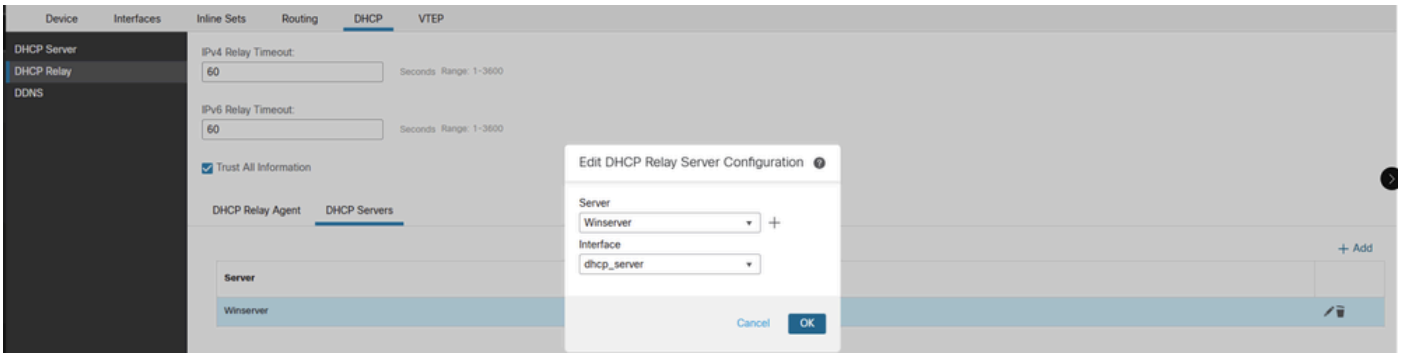
5.OK를 클릭하여 DHCP 릴레이 에이전트의 컨피그레이션 설정을 저장합니다.

외부 DHCP 서버 구성

클라이언트 요청이 전달되는 외부 DHCP 서버의 IP 주소를 구성하려면 아래 단계를 확인하십시오.

DHCP Server(DHCP 서버) 섹션으로 이동하고 Add(추가)를 클릭합니다.
1. Server(서버) 필드에 DHCP 서버의 IP 주소를 입력합니다. 드롭다운 메뉴에서 기존 네트워크 객체를 선택하거나 더하기(+) 아이콘을 클릭하여 새 네트워크 객체를 생성할 수 있습니다.
2. Interface 필드에서 DHCP 서버에 연결하는 인터페이스를 지정합니다.

3. 컨피그레이션을 저장하려면 OK(확인)를 클릭합니다. 그런 다음 Save(저장)를 클릭하여 플랫폼 설정을 저장합니다.



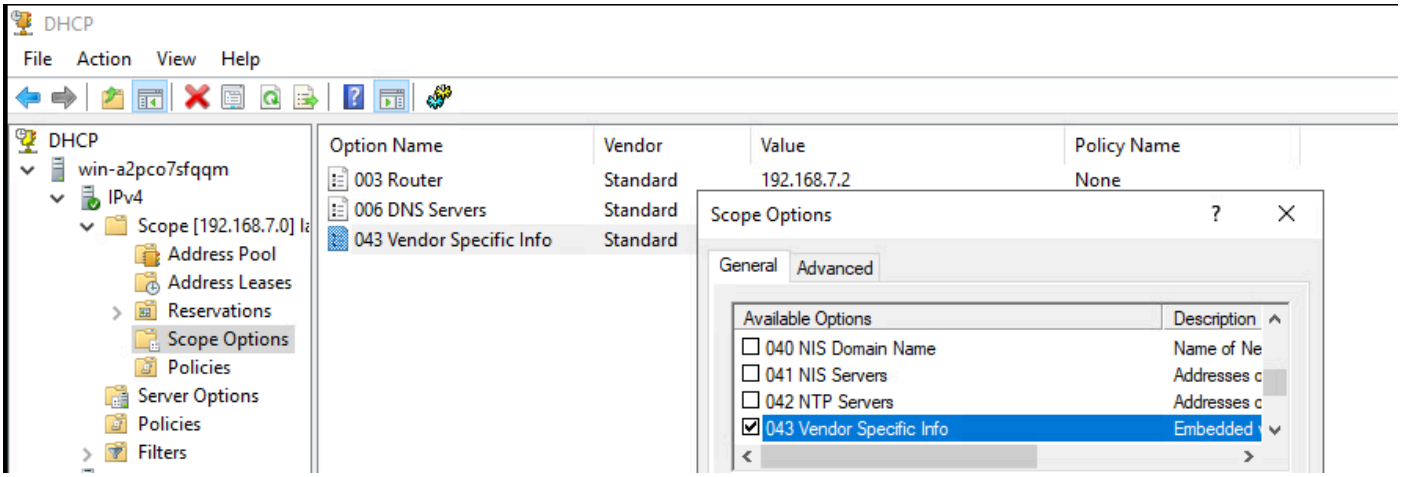
DHCP_Server_Config

4.다음으로, Deploy(구축) 옵션으로 이동하여 변경 사항을 적용하려는 FTD 어플라이언스를 선택하고 Deploy(구축)를 클릭하여 플랫폼 설정 구축을 시작합니다.

외부 DHCP 서버에서 옵션 43 사용

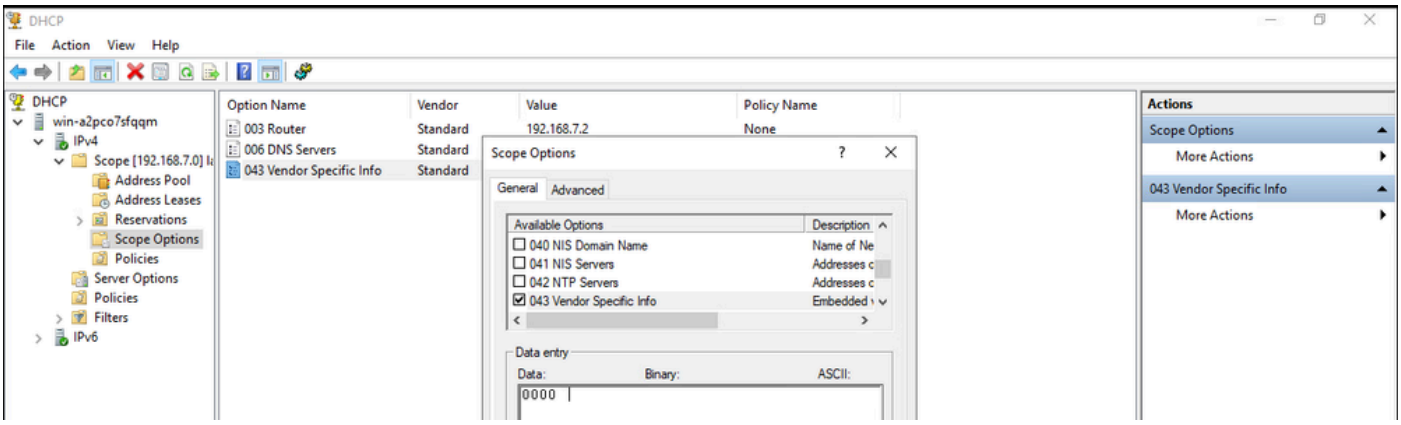
참고: RFC 2132에 따르면 옵션 43의 최소 길이는 1입니다.

DHCP 서버 설정으로 이동하여 IPv4로 이동한 다음 범위 및 범위 옵션 >추가 작업 >옵션 구성 >을 선택하고 옵션 43을 활성화합니다



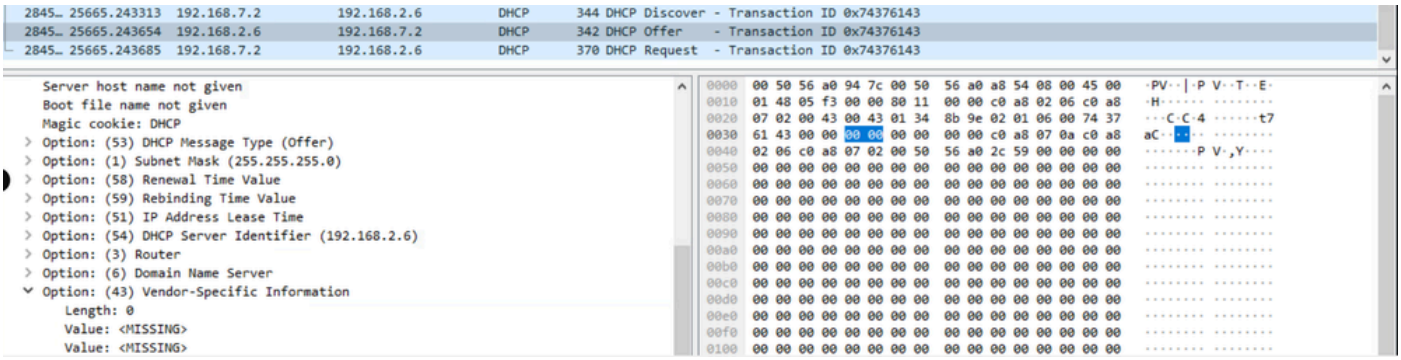
Enable_Option_43_On _External_DHCP_Server

처음에 기본 설정은 값을 비워 두어 FTD가 패킷을 삭제하고 형식이 잘못된 패킷으로 분류하도록 합니다.



Default_Config_Of_Option_43

Wireshark를 사용하는 서버 측에서 OFFER 패킷에서는 길이가 0인 경우 옵션 43에 대한 값이 없음을 확인합니다.



Non_Working_Server_Side_cap

Cisco FTD(Firepower Threat Defense)에서 패킷을 삭제하는 중입니다. 패킷의 길이가 0이고 형식이 잘못되어 RFC 2132를 위반하는 것으로 간주되기 때문입니다.

<#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.

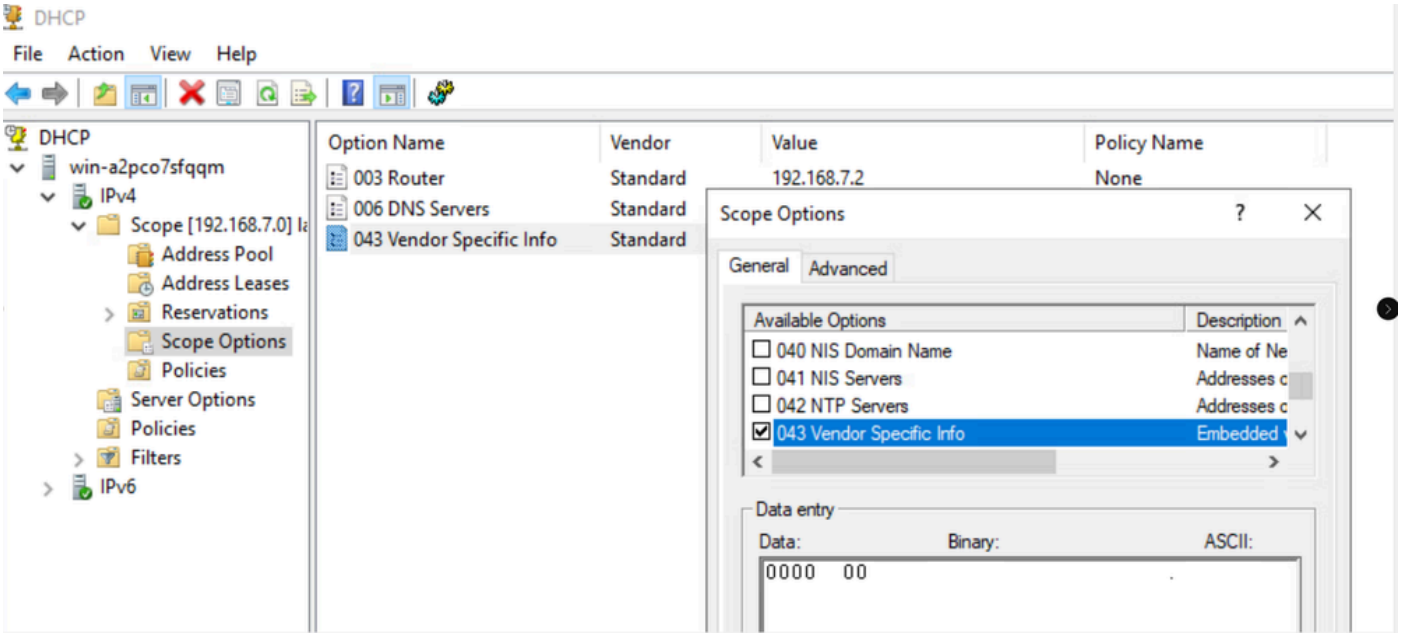
DHCPD/RA: Unable to load workspace.

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.
```

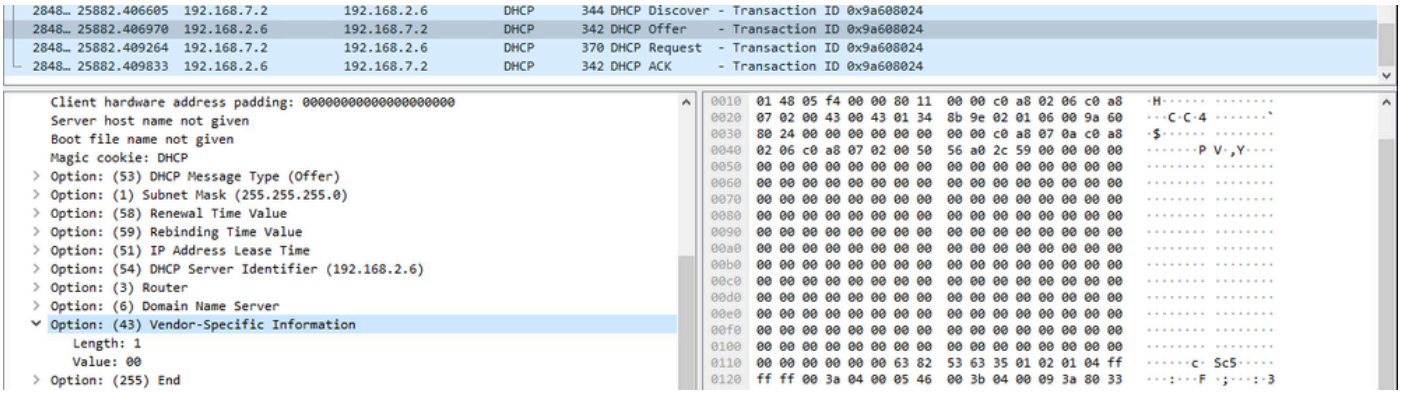
RFC 2132에 따라 이진 값을 0보다 크게 조정하려면 이미지에 표시된 대로 043 Vendor Specific Info(043 공급업체 관련 정보) 필드를 두 번 클릭하고 값을 00으로 설정합니다.

이렇게 변경하면 IP 주소가 클라이언트에 성공적으로 임대됩니다.



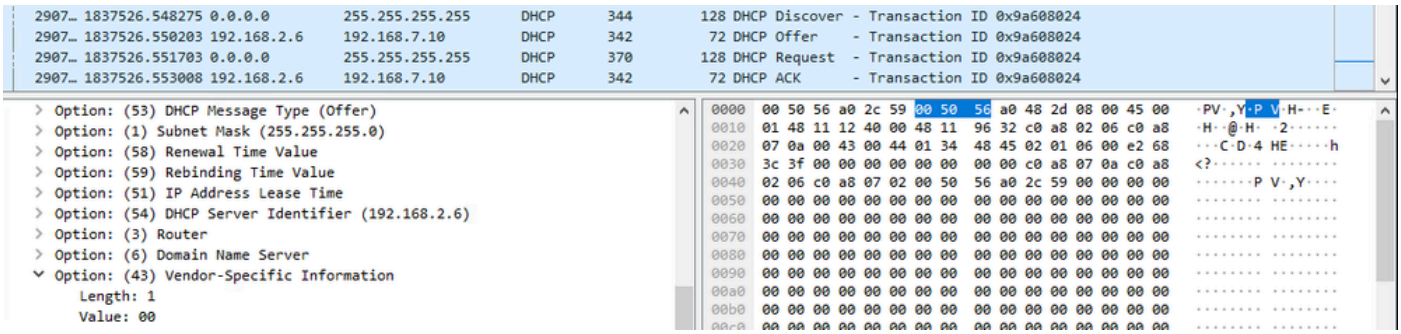
Changed_Binary_Value_to_1

옵션 43에서 값이 1로 설정된 경우 서버측 DORA 프로세스



서버_사이드_워킹_캡

옵션 43에서 값이 1로 설정되어 있고 클라이언트가 IP를 사용하여 임대가 된 것을 볼 수 있는 경우 클라이언트 측 DORA 프로세스.



클라이언트_사이드_작업_캡

<#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

다음을 확인합니다.

DHCP 서버 또는 릴레이를 설정하기 전에 FTD가 FMC에 등록되어 있는지 확인합니다. 또한 DHCP 릴레이 컨피그레이션에서 DHCP 서버에 연결되어 있는지 확인합니다.

```
<#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 CLI에서 DHCP 릴레이 에이전트 컨피그레이션을 확인합니다.

```
<#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
```

문제 해결

문제를 해결하려면 다음 사항을 고려하십시오.
1. DHCP 서버에서 연결할 수 있도록 FTD와 DHCP 서버 간의 라우팅을 확인합니다.
2. DHCP 서버에 DHCP 릴레이 에이전트 인터페이스에 액세스할 수 있는 경로가 있는지 확인합니다.
3. 클라이언트가 IP 주소를 수신하지 못하는 문제를 해결하려면 FTD 라우팅 인터페이스에서 패킷 캡처를 수행할 수 있습니다.

그러면 패킷 캡처 내에서 DHCP 서버의 DORA 프로세스를 검토할 수 있습니다.

Use Firepower Threat Defense Captures and Packet Tracer를 활용하여 패킷 캡처를 효과적으로 수행할 수 있습니다.

이전에 시작한 특정 패킷 캡처 세션을 중지하고 삭제하려면 below 명령을 실행합니다.
<capture_name> 캡처 없음

4.상태를 검토하고 dhcprelay debug를 수집하려면 아래 명령을 실행합니다

이렇게 하려면 FTD CLI에 로그인합니다.

<#root>

system support diagnostic-cli

enable

Enter를 누릅니다.

<#root>

show dhcprelay statistic

show dhcprelay state

디버그가 이미 활성화되었는지 확인하려면 below 명령을 실행합니다.

<#root>

show debug

<#root>

To capture debug excute below commands

debug dhcprelay packet
debug dhcprelay event

<#root>

To disable debug

undebug all

관련 정보

FMC를 사용하여 FTD에서 DHCP 서버 및 릴레이 구성

DHCP 및 DDNS

기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.