Firepower Threat Defense 투명 방화벽 모드 고급 개념 및 문제 해결 팁

목차

소개

이 문서에서는 TFW(Transparent Firewall) 모드에서 FTD(Firepower Threat Defense) 구축의 핵심 개념과 요소를 이해하기 위한 자세한 설명을 설명합니다.또한 투명 방화벽 아키텍처와 관련된 가장 일반적인 문제에 대한 유용한 툴과 연습도 제공합니다.

기고자: Cesar Lopez, Yeraldin Sánchez, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FTD 투명 방화벽 모드 지식
- HSRP(Hot Standby Router Protocol) 개념
- ARP(Address Resolution Protocol) 및 ICMP(Internet Control Message Protocol) 프로토콜

이 문서에 설명된 개념을 더 잘 이해하기 위해서는 Firepower Configuration Guide [Transparent 또](#)

는 Routed Firewall Mode 섹션을 읽는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Firepower 4120 FTD 버전 6.3.0.4
- Cisco FMC(Firepower Management Center) 버전 6.3.0.4
- Cisco ASR1001 IOS-XE 버전 16.3.9
- Cisco Catalyst 3850 IOS-XE 버전 16.9.3

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

투명 방화벽 고급 개념

MAC 주소 테이블

라우팅 모드의 방화벽은 라우팅 테이블 및 ARP 테이블을 사용하여 이그레스 인터페이스와 패킷을 다음 홉으로 전달하는 데 필요한 데이터를 결정하지만, TFW 모드는 MAC 주소 테이블을 사용하여 패킷을 목적지로 전송하는 데 사용되는 이그레스 인터페이스를 결정합니다.방화벽은 처리 중인 패킷의 대상 MAC 주소 필드를 확인하고 이 주소를 인터페이스와 연결하는 항목을 검색합니다.

MAC 주소 테이블에는 이러한 필드가 있습니다.

```
> show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
Outside 0050.56a5.6d52 dynamic 1 1
Inside 0000.0c9f.f014 dynamic 3 1
```

- 인터페이스 - 이 필드에는 이 MAC 주소가 동적으로 학습되거나 정적으로 구성된 인터페이스 이름이 포함됩니다.
- MAC 주소 - 저장할 MAC 주소 레코드
- type - 항목을 학습하는 데 사용되는 방법입니다.동적 또는 정적
- Age(min) - 해당 항목이 Dead로 표시되기 전의 남은 시간을 표시하는 시간(분)을 줄여 줍니다.이 타이머는 동적으로 학습 항목에만 적용됩니다.
- bridge-group - 인터페이스가 속한 브리지 그룹 ID

패킷 전달 결정은 스위치와 비슷하지만 MAC 테이블에서 누락된 항목이 있을 때 매우 중요한 차이가 있습니다.스위치에서 패킷은 인그레스 인터페이스를 제외한 모든 인터페이스를 통해 브로드캐스트되지만 TFW에서는 패킷이 수신되고 대상 MAC 주소에 대한 항목이 없으면 패킷이 삭제됩니다.ASP(Accelerated Security Path) 삭제 코드 dst-*l2_lookup-fail로 삭제됩니다*.

```
FTD63# show cap icmpin trace pack 1

7 packets captured

1: 00:20:22.338391 802.1Q vlan#20 P0 10.10.10.5 > 20.20.20.5 icmp: echo request
Result:
input-interface: Inside
```

```
input-status: up
input-line-status: up
Action: drop
Drop-reason: (dst-l2_lookup-fail) Dst MAC L2 Lookup Failed
```
이 상태는 항상 동적 학습이 활성화된 환경에서 첫 번째 패킷에 대해 발생하며, MAC 주소가 소스 MAC 주소로 패킷에서 이전에 보이지 않은 경우 대상에 대한 정적 항목이 없습니다.

항목이 MAC 주소 테이블에 추가되면 다음 패킷이 활성화된 방화벽 기능에 맞게 허용됩니다.

```
FTD63# show cap icmpin trace pack 2

7 packets captured

2: 00:20:27.329206 802.1Q vlan#20 P0 10.10.10.5 > 20.20.20.5 icmp: echo request
Phase: 1
Type: L2-EGRESS-IFC-LOOKUP
Subtype: Destination MAC L2 Lookup
Result: ALLOW
Config:
Additional Information:
Destination MAC lookup resulted in egress ifc Outside
```

> **주의:**MAC Lookup은 방화벽에서 수행하는 작업의 첫 번째 단계입니다.Failed L2 lookup으로 인해 상수가 감소하면 관련 패킷 손실 및/또는 불완전한 탐지 엔진 검사가 발생할 수 있습니다.이러한 영향은 프로토콜 또는 애플리케이션 기능에 따라 재전송됩니다.

위에서 설명한 내용을 기반으로, 전송 전에 항목을 학습하는 것이 좋습니다.TFW에는 항목을 학습하는 여러 메커니즘이 있습니다.

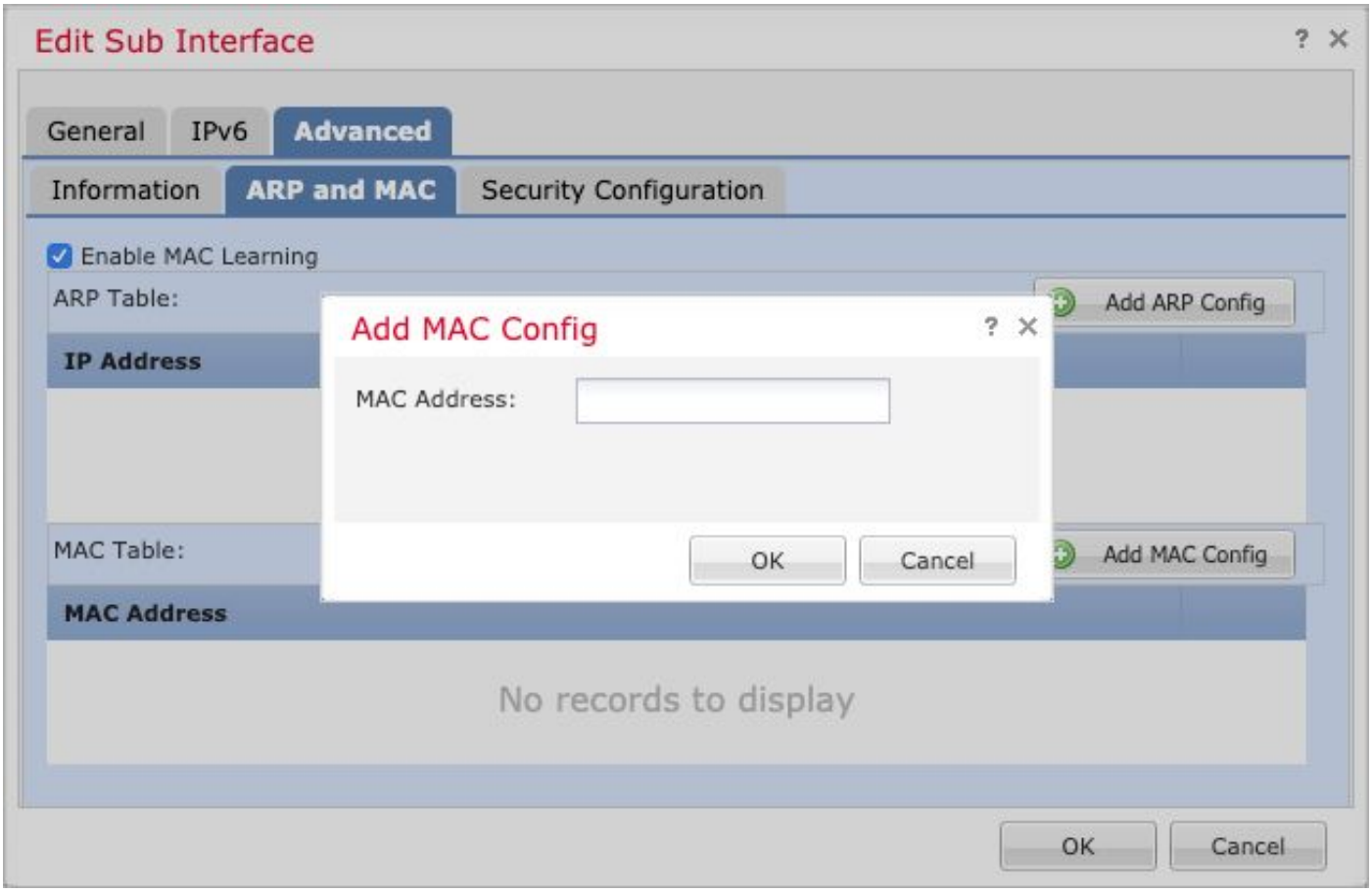
MAC 주소 테이블 학습 옵션

정적 항목

MAC 주소를 수동으로 추가하여 방화벽에서 항상 특정 항목에 동일한 인터페이스를 사용하도록 할 수 있습니다.변경할 수 없는 항목에 대해 유효한 옵션입니다.이 옵션은 컨피그레이션 레벨에서 또는 다음 홉의 기능에 의해 고정 MAC를 덮어쓸 때 일반적으로 사용하는 옵션입니다.

예를 들어, 기본 게이트웨이 MAC 주소가 컨피그레이션에 수동으로 추가된 것과 동일한 경우 또는 HSRP 가상 MAC 주소가 동일하게 유지되는 경우 Cisco 라우터에서 항상 동일한 상태가 됩니다.

FMC에서 관리하는 FTD에서 고정 엔트리를 구성하려면 Edit **Interface / Subinterface > Advanced > ARP and MAC를** 클릭하고 **Add MAC Config(MAC 컨피그레이션 추가)를** 클릭합니다.이렇게 하면 Devices(디바이스) > Device **Management**(디바이스 **관리) > Interfaces(인터페이스)** 섹션에서 편집 중인 특정 인터페이스에 대한 항목이 추가됩니다.



소스 MAC 주소를 기반으로 하는 동적 학습

이 방법은 스위치가 MAC 주소 테이블을 채우기 위해 수행하는 방법과 유사합니다.패킷에 수신된 인터페이스에 대한 MAC 테이블 항목의 일부가 아닌 소스 MAC 주소가 있는 경우 새 항목이 테이블에 추가됩니다.

ARP 프로브 기반 동적 학습

패킷이 MAC 테이블에 속하지 않은 대상 MAC 주소를 가지고 도착하고 대상 IP가 BVI(Bridge Virtual Interface)와 동일한 네트워크의 일부인 경우 TFW는 모든 브리지 그룹 인터페이스를 통해 ARP 요청을 전송하는 방법을 알아보려고 시도합니다.브리지 그룹 인터페이스에서 ARP 응답을 수신하면 MAC 테이블에 추가됩니다.위에서 설명한 것처럼 해당 ARP 요청에 대한 회신은 없지만 모든 패킷은 ASP 코드 dst-*l2_lookup-fail*과 함께 *삭제됩니다*.

ICMP 프로브를 기반으로 하는 동적 학습

패킷이 MAC 테이블의 일부가 아닌 대상 MAC 주소와 함께 도착하고 대상 IP가 BVI와 동일한 네트워크의 일부가 아닌 경우 ICMP 에코 요청은 TTL(Time-to-Live) 값이 1과 같은 상태로 전송됩니다. 방화벽은 next-hop MAC 주소를 학습하기 위해 ICMP Time Exceeded 메시지를 예상합니다.

MAC 주소 테이블 사용 기간 타이머

MAC 주소 테이블 Age 타이머는 학습된 각 항목에 대해 5분으로 설정됩니다.이 시간 초과 값은 두 개의 다른 단계를 가집니다.

Age Timeout First Stage

처음 3분 동안 소스 MAC 주소가 있는 방화벽을 통과하는 ARP 응답 패킷이 MAC 주소 테이블의 항목과 동일하지 않으면 MAC 항목 Age 값이 새로 고쳐지지 않습니다.이 조건은 브리지 그룹 IP 주소로 전송되는 ARP 응답을 제외합니다.즉, through-the-box ARP 응답이 아닌 다른 패킷은 처음 3분 동안 무시됩니다.

이 예에서는 IP 주소가 10.10.10.5인 PC가 10.20.20.5으로 ping을 전송합니다. 10.20.20.5의 게이트웨이 IP 주소는 MAC 주소 0000.0c9f.f014인 10.20.20.3입니다.

대상 PC는 25초마다 ARP 업데이트를 생성하여 고정 ARP 패킷이 방화벽을 통과하도록 합니다.

```
FTD63# show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
Inside 00fc.baf3.d680 dynamic 3 1
Outside 0050.56a5.6d52 dynamic 5 1
Inside 0000.0c9f.f014 dynamic 5 1
Outside 40a6.e833.2a05 dynamic 4 1
```

패킷 캡처 필터링 ARP 패킷은 이러한 패킷과 일치시키는 데 사용됩니다.

```
> show capture

capture arp type raw-data ethernet-type arp interface Inside [Capturing - 1120 bytes]

>show capture arp

12 packets captured

1: 23:04:52.142524 802.1Q vlan#20 P0 arp who-has 10.20.20.3 (0:0:c:9f:f0:14) tell 10.20.20.5
2: 23:04:52.142952 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
3: 23:04:52.145057 802.1Q vlan#20 P0 arp who-has 10.20.20.3 (0:0:c:9f:f0:14) tell 10.20.20.5
4: 23:04:52.145347 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
5: 23:05:16.644574 802.1Q vlan#20 P0 arp who-has 10.20.20.3 (0:0:c:9f:f0:14) tell 10.20.20.5
6: 23:05:16.644940 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
7: 23:05:16.646756 802.1Q vlan#20 P0 arp who-has 10.20.20.3 (0:0:c:9f:f0:14) tell 10.20.20.5
8: 23:05:16.647015 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
9: 23:05:41.146614 802.1Q vlan#20 P0 arp who-has 10.20.20.3 (0:0:c:9f:f0:14) tell 10.20.20.5
10: 23:05:41.146980 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
11: 23:05:41.148734 802.1Q vlan#20 P0 arp who-has 10.20.20.3 (0:0:c:9f:f0:14) tell 10.20.20.5
12: 23:05:41.149009 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
```

000.0c9f.4014의 엔트리는 5에 유지되며 해당 숫자 이하로 내려가지 않습니다.

```
> show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
Inside 00fc.baf3.d680 dynamic 3 1
Outside 0050.56a5.6d52 dynamic 5 1
Inside 0000.0c9f.f014 dynamic 5 1
Outside 40a6.e833.2a05 dynamic 4 1
```

Age Timeout 2단계

지난 2분 동안 해당 주소가 오래된 것으로 간주되는 기간이 됩니다.

```
> show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
Inside 00fc.baf3.d680 dynamic 5 1
Outside 0050.56a5.6d52 dynamic 3 1
Inside 0000.0c9f.f014 dynamic 2 1
Outside 40a6.e833.2a05 dynamic 3 1
```

항목이 아직 제거되지 않고, 소스 MAC 주소가 테이블 항목과 일치하는 패킷이 to-the-box 패킷을 포함하여 탐지되면 Age 항목이 다시 5분으로 새로 고쳐집니다.

이 예에서는 2분 내에 ping을 전송하여 방화벽에서 고유한 ARP 패킷을 강제로 전송합니다.

```
> ping 10.20.20.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.20.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

MAC 주소 항목이 5분으로 다시 설정됩니다.

```
> show mac-address-table
interface mac address type Age(min) bridge-group
-----------------------------------------------------------------------------------------------
----
Inside 00fc.baf3.d680 dynamic 4 1
Outside 0050.56a5.6d52 dynamic 2 1
Inside 0000.0c9f.f014 dynamic 5 1
Outside 40a6.e833.2a05 dynamic 5 1
```

ARP 테이블

첫째, MAC 주소 테이블이 ARP 테이블과 완전히 독립되어 있음을 이해하는 것이 중요합니다.ARP 항목을 새로 고치기 위해 방화벽에서 보낸 ARP 패킷은 MAC 주소 테이블을 새로 고칠 수 있지만, 이러한 새로 고침 프로세스는 별도의 작업이며 각각 고유한 시간 초과 및 조건이 있습니다.

ARP 테이블이 라우팅 모드에서와 같이 이그레스(egress) next-hop을 결정하는 데 사용되지 않더라도 방화벽 ID IP가 투명 구축에서 가질 수 있는 ARP 패킷의 효과를 이해하는 것이 중요합니다.

ARP 항목은 관리 용도로 사용되며 관리 기능이나 작업에 필요한 경우에만 테이블에 추가됩니다.관리 작업의 예로, 브리지 그룹에 IP 주소가 있는 경우 이 IP를 사용하여 대상을 ping할 수 있습니다.

```
> show ip
Management-only Interface: Ethernet1/4
System IP Address:
no ip address
Current IP Address:
no ip address
Group : 1
Management System IP Address:
ip address 10.20.20.4 255.255.255.0
Management Current IP Address:
ip address 10.20.20.4 255.255.255.0
```

대상이 Bridge Group IP와 동일한 서브넷에 있는 경우 ARP 요청을 강제로 수행하고 유효한 ARP 응답을 수신하면 IP/MAC 항목이 ARP 테이블에 저장됩니다.

```
> show arp
Inside 10.20.20.3 0000.0c9f.f014 6
```

MAC 주소 테이블과 달리, 인터페이스/IP 주소/MAC 주소 트라이플릿과 함께 제공되는 타이머의 값이 증가합니다.

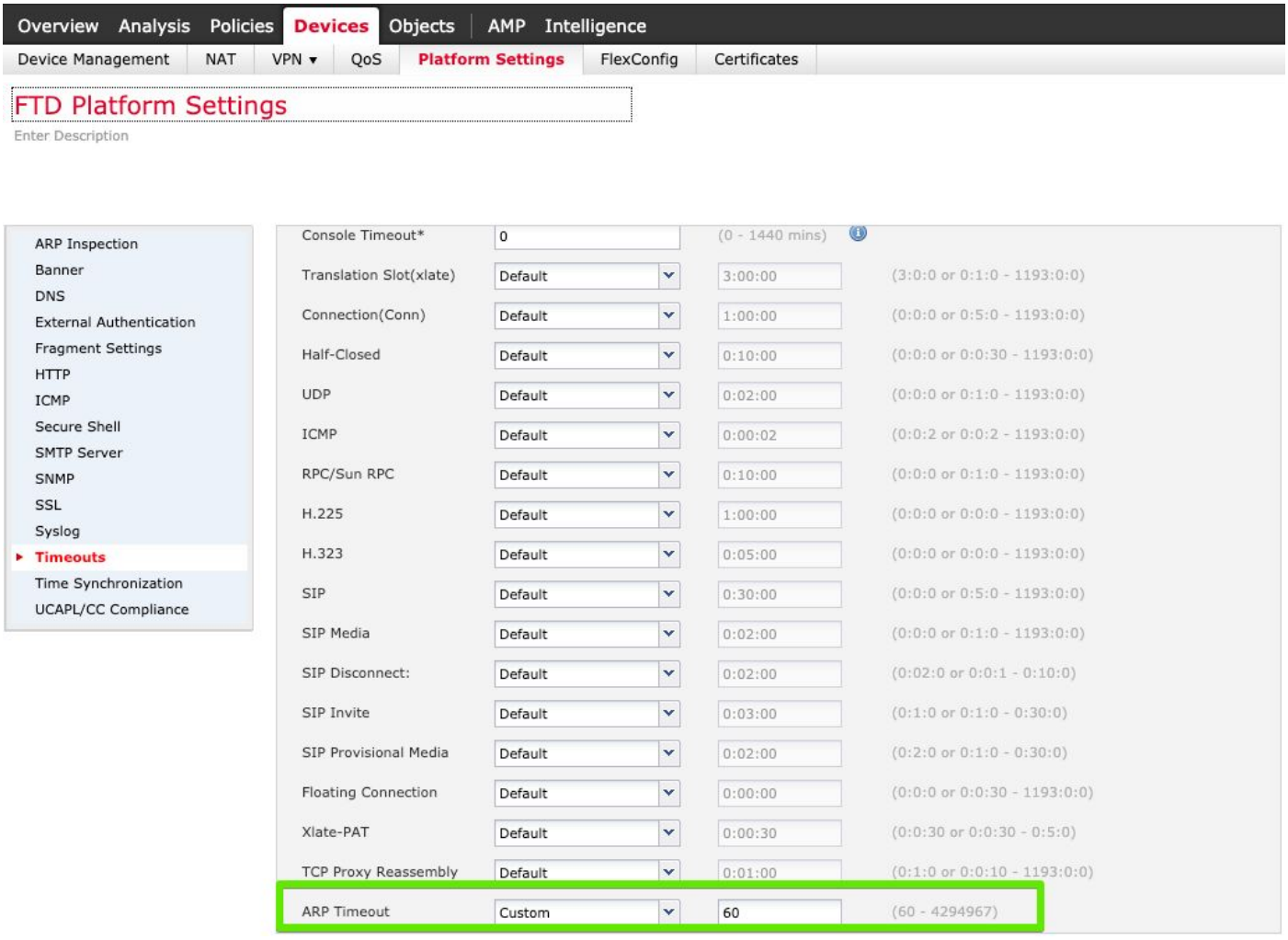
```
> show arp
Inside 10.20.20.3 0000.0c9f.f014 1
>show arp
Inside 10.20.20.3 0000.0c9f.f014 2
>show arp
Inside 10.20.20.3 0000.0c9f.f014 3
>show arp
Inside 10.20.20.3 0000.0c9f.f014 4
```

타이머가 *n - 30 값에* 도달하면 *n*은 ARP 구성 시간 초과(기본값 14,400초)입니다. 방화벽은 ARP 요청을 보내 엔트리를 새로 고칩니다.유효한 ARP 응답이 수신되면 엔트리가 보류되고 타이머가 0으로 돌아갑니다.

이 예에서는 ARP 시간 초과가 60초로 줄었습니다.

```
> show running-config arp
arp timeout 60
arp rate-limit 32768
```

이 시간 초과는 이미지에 표시된 대로 FMC의 **Devices > Platform Settings > Timeouts** 탭에서 구성할 수 있습니다.



시간 제한은 60초이므로 ARP 요청은 30초(60 - 30 = 30)마다 전송됩니다.

```
> show capture arp

8 packets captured

1: 21:18:16.779729 802.1Q vlan#20 P0 arp who-has 10.20.20.3 tell 10.20.20.4
2: 21:18:16.780111 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
3: 21:18:46.779744 802.1Q vlan#20 P0 arp who-has 10.20.20.3 tell 10.20.20.4
4: 21:18:46.780126 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
5: 21:19:16.779744 802.1Q vlan#20 P0 arp who-has 10.20.20.3 tell 10.20.20.4
6: 21:19:16.780111 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
7: 21:19:46.779729 802.1Q vlan#20 P0 arp who-has 10.20.20.3 tell 10.20.20.4
8: 21:19:46.780126 802.1Q vlan#20 P0 arp reply 10.20.20.3 is-at 0:0:c:9f:f0:14
```

그런 다음 ARP 항목이 30초마다 새로 고쳐집니다.

```
> show arp
Inside 10.20.20.3 0000.0c9f.f014 29
>show arp
Inside 10.20.20.3 0000.0c9f.f014 0
```

문제 해결 팁

트래픽 방향

TFW에서 추적하기 가장 어려운 것 중 하나는 트래픽 흐름 방향입니다.트래픽 플로우가 방화벽에서 목적지로 패킷을 올바르게 전달하는 데 어떤 도움이 되는지 이해

소스 및 목적지 MAC 주소 수정 및 TTL(Time-To-Live) 값 감소 등과 같은 방화벽 개입의 여러 지표가 있기 때문에 라우팅된 모드에서는 올바른 인그레스 및 이그레스 인터페이스를 확인하는 것이 더 쉽습니다.

이러한 차이점은 TFW 설정에서 사용할 수 없습니다.인그레스 인터페이스를 통해 들어오는 패킷은 대부분의 경우 방화벽을 벗어날 때와 동일하게 보입니다.

네트워크의 MAC 플랩 또는 트래픽 루프와 같은 특정 문제는 패킷이 어디에서, 언제 방화벽을 떠났는지 알지 못하고 추적하기가 더 어려울 수 있습니다.

인그레스 패킷과 이그레스 패킷을 구분하기 위해 trace 키워드를 패킷 캡처에서 사용할 수 있습니다.

```
capture in interface inside buffer 33554432 trace trace-count 1000 match tcp host 10.10.220.42 host 10.10.241.225
capture out interface outside buffer 33554432 trace trace-count 1000 match tcp host 10.10.220.42 host 10.10.241.225
```

buffer - 캡처 버퍼를 바이트 단위로 늘립니다.33554432는 사용 가능한 최대값입니다.5500-X, Firepower 어플라이언스 또는 가상 머신 같은 모델에서는 이미 구성된 캡처가 수십 개가 아니면 이 크기 값을 사용하는 것이 안전합니다.

trace - 지정된 캡처에 대한 trace 옵션을 활성화합니다.

trace-count - 더 많은 추적 수를 허용합니다.1000은 최대 허용이고 128은 기본값입니다.이는 버퍼 크기 옵션과 동일한 권장 사항에 따라 안전합니다.

팁:옵션 중 하나를 추가하지 않은 경우 캡처 이름과 옵션을 참조하여 전체 캡처를 다시 쓸 필요 없이 추가할 수 있습니다.그러나 새 옵션은 새로 캡처된 패킷에만 영향을 미치므로 **clear capture capname을 사용하여** 패킷 번호 1 이후 새로운 효과를 가져와야 합니다. 예:**추적에 캡처**

패킷이 캡처되면 **show capture *cap_name* trace** 명령은 인그링된 패킷의 처음 1000(추적 번호가 증가된 경우) 추적을 표시합니다.

```
FTD63# show capture out trace
1: 16:34:56.940960 802.1Q vlan#7 P0 10.10.241.225 > 10.10.220.38 icmp: time exceeded in-transit
Result: input-interface: outside input-status: up input-line-status: up Action: drop Drop-
reason: (dst-l2_lookup-fail) Dst MAC L2 Lookup Failed 2: 16:34:57.143959 802.1Q vlan#7 P0
10.10.220.42 > 10.10.241.225 icmp: echo request 3: 16:34:57.146476 802.1Q vlan#7 P0
10.10.241.225 > 10.10.220.42 icmp: echo reply Result: input-interface: outside input-status: up
input-line-status: up Action: drop Drop-reason: (dst-l2_lookup-fail) Dst MAC L2 Lookup Failed
```

이 출력은 외부 인터페이스 패킷 캡처 추적의 예입니다.즉, 패킷 번호 1과 3이 외부 인터페이스와 패킷 번호 2가 인터페이스를 피싱했음을 의미합니다.

이 추적에서는 해당 패킷에 대해 수행한 작업 및 패킷이 삭제될 경우 삭제 사유와 같은 추가 정보를 찾을 수 있습니다.

더 긴 추적을 위해 단일 패킷에 포커스를 두려면 **show capture *cap_name* trace packet-number packet-number *packet*_**number 명령을 사용하여 해당 패킷의 추적을 표시할 수 있습니다.

허용되는 패킷 번호 10의 예입니다.

```
FTD63# show capture in detail trace packet-number 10

10: 20:55:31.118218 0000.0c9f.f014 0100.5e00.0066 0x8100 Length: 98 802.1Q vlan#20 P0
10.20.20.1.1985 > 224.0.0.102.1985: [udp sum ok] udp 52 [tos 0xc0] [ttl 1] (id 0) Phase: 1 Type:
L2-EGRESS-IFC-LOOKUP Subtype: Destination MAC L2 Lookup Result: ALLOW Config: Additional
Information: Destination MAC lookup resulted in egress ifc Outside Phase: 2 Type: CAPTURE
Subtype: Result: ALLOW Config: Additional Information: MAC Access list Phase: 3 Type: ACCESS-
LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC Access list Phase:
4 Type: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information: Found flow with id
2562905, using existing flow Phase: 5 Type: SNORT Subtype: Result: ALLOW Config: Additional
Information: Snort Verdict: (fast-forward) fast forward this flow Phase: 6 Type: CAPTURE
Subtype: Result: ALLOW Config: Additional Information: MAC Access list Result: input-interface:
Inside input-status: up input-line-status: up Action: allow
```

MAC 추적

TFW는 MAC 주소를 기반으로 모든 전달 결정을 수행합니다.트래픽 흐름 분석 중에 각 패킷에서 소스 및 대상으로 사용되는 MAC 주소가 네트워크 토폴로지를 기반으로 정확한지 확인해야 합니다.

패킷 캡처 기능을 사용하면 show capture 명령에서 ***detail*** 옵션을 사용하여 사용된 MAC 주소를 표시할 수 있습니다.

```
FTD63# show cap i detail

98 packets captured

   1: 20:55:06.938473 0000.0c9f.f014 0100.5e00.0066 0x8100 Length: 98
      802.1Q vlan#20 P0 10.20.20.1.1985 > 224.0.0.102.1985:  [udp sum ok] udp 52 [tos 0xc0]
```

```
[ttl 1] (id 0)
   2: 20:55:09.805561 0000.0c9f.f014 0100.5e00.0066 0x8100 Length: 98
      802.1Q vlan#20 P0 10.20.20.1.1985 > 224.0.0.102.1985:  [udp sum ok] udp 52 [tos 0xc0]
[ttl 1] (id 0)
```

특정 추적을 필요로 하는 흥미로운 MAC 주소를 찾은 후에는 캡처 필터를 통해 확인할 수 있습니다 .

```
FTD63# capture in type raw-data trace interface inside match mac 0000.0c9f.f014 ffff.ffff.ffff
any

FTD63# show capture

capture in type raw-data trace interface inside [Capturing - 114 bytes] match mac 0000.0c9f.f014
ffff.ffff.ffff any

FTD63# show cap in detail 98 packets captured 1: 20:55:06.938473 0000.0c9f.f014 0100.5e00.0066
0x8100 Length: 98 802.1Q vlan#20 P0 10.20.20.1.1985 > 224.0.0.102.1985: [udp sum ok] udp 52 [tos
0xc0] [ttl 1] (id 0) 2: 20:55:09.805561 0000.0c9f.f014 0100.5e00.0066 0x8100 Length: 98 802.1Q
vlan#20 P0 10.20.20.1.1985 > 224.0.0.102.1985: [udp sum ok] udp 52 [tos 0xc0] [ttl 1] (id 0)
```

이 필터는 MAC 플랩의 추적이 있고 범인을 찾으려는 경우에 매우 유용합니다.

Mac-address-table 디버그

MAC 주소 테이블 디버그를 활성화하여 각 단계를 검토할 수 있습니다.이 디버그에 의해 제공되는 정보는 MAC 주소가 테이블에서 학습, 새로 고침 및 제거되는 시기를 이해하는 데 도움이 됩니다.

이 섹션에서는 각 단계의 예와 이 정보를 읽는 방법을 보여줍니다.FTD에서 디버그 명령을 활성화하려면 진단 CLI에 액세스해야 합니다.

> **경고:**네트워크가 너무 사용 중일 경우 디버그는 관련 리소스를 사용할 수 있습니다.제어 환경이나 사용량이 적은 시간에 사용하는 것이 좋습니다.이러한 디버그가 너무 자세한 경우 Syslog 서버에 전송하는 것이 좋습니다.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

FTD63# debug mac-address-table
debug mac-address-table enabled at level 1
```

1단계. MAC 주소가 학습됩니다.MAC 테이블에서 항목을 이미 찾을 수 없으면 이 주소가 테이블에 추가됩니다.디버그 메시지는 주소 및 수신 인터페이스를 알립니다.

```
FTD63# ping 10.20.20.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.20.3, timeout is 2 seconds:
add_l2fwd_entry: Going to add MAC 0000.0c9f.f014.
add_l2fwd_entry: Added MAC 0000.0c9f.f014 into bridge table thru Inside.
set_l2: Found MAC entry 0000.0c9f.f014 on Inside.
!add_l2fwd_entry: Going to add MAC 00fc.baf3.d680.
add_l2fwd_entry: Added MAC 00fc.baf3.d680 into bridge table thru Inside.
!!!!
```

ICMP 방법을 통해 MAC을 학습하면 다음 메시지가 표시됩니다.이 항목은 MAC 주소 테이블 사용

기간 타이머에 나열된 조건에 따라 타이머를 새로 고치지 않는 시간 초과 주기의 첫 번째 단계에 들어갑니다.

```
learn_from_icmp_error: Learning from icmp error.
```

2단계. 항목이 이미 알려진 경우 디버그가 이에 대해 알립니다.디버그는 독립형 또는 HA 설정과 관련이 없는 클러스터링 메시지도 표시합니다.

```
set_l2: Found MAC entry 0000.0c9f.f014 on Inside.
l2fwd_refresh: Sending clustering LU to refresh MAC 0000.0c9f.f014.
l2fwd_refresh: Failed to send clustering LU to refresh MAC 0000.0c9f.f014
```

3단계. 항목이 두 번째 단계(절대 시간 초과 2분 전)에 도달하면

```
FTD63# show mac-add
interface                  mac  address          type       Age(min)    bridge-group
-------------------------------------------------------------------------------------------
----
Inside                     00fc.baf3.d700        dynamic      3           1
Outside                    0050.56a5.6d52        dynamic      4           1
Inside                     0000.0c9f.f014        dynamic      2           1
Outside                    40a6.e833.2a05        dynamic      3           1

FTD63# l2fwd_clean:MAC 0000.0c9f.f014 entry aged out.
l2fwd_timeout:MAC entry timed out
```

4단계. 이제 방화벽은 해당 주소로 제공된 새 패킷이 테이블을 새로 고칠 것으로 예상합니다.이 2분 동안 해당 항목을 사용하는 패킷이 더 이상 없으면 주소가 제거됩니다.

```
FTD63# show mac-address-table
interface mac address type Age(min) bridge-group
-------------------------------------------------------------------------------------------
----
Inside 0000.0c9f.f014 dynamic 1 1
Outside 40a6.e833.2a05 dynamic 3 1
FTD63# l2fwd_clean:Deleting MAC 0000.0c9f.f014 entry due to timeout.
delete_l2_fromPC: Deleting MAC 0000.0c9f.f014 due to freeing up of entry
l2fwd_clean:Deleted MAC 0000.0c9f.f014 from NP.
```

관련 정보

- Firepower Management Center 가이드, 버전 6.3 - 3장:Firepower Threat Defense를 위한 투명 또는 라우팅된 방화벽 모드
- 기술 지원 및 문서 – Cisco Systems