Firepower威胁防御透明防火墙模式高级概念和故障排除提示

目录

简介

本文档介绍详细说明，以了解透明防火墙(TFW)模式下Firepower威胁防御(FTD)部署的核心概念和元素。本文还针对与透明防火墙架构相关的最常见问题提供了有用的工具和演练。

作者：Cesar Lopez和Yeraldin Sánchez，Cisco TAC工程师编辑。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科FTD透明防火墙模式知识
- 热备份路由器协议(HSRP)概念
- 地址解析协议(ARP)和Internet控制消息协议(ICMP)协议

强烈建议阅读“Firepower配置指南透明或路由防火墙模式”部分，以更好地理解本文档中描述的概念。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科Firepower 4120 FTD版本6.3.0.4
- 思科Firepower管理中心(FMC)版本6.3.0.4
- 思科ASR1001 IOS-XE版本16.3.9
- 思科Catalyst 3850 IOS-XE版本16.9.3

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

透明防火墙高级概念

MAC 地址表

在路由模式下，防火墙依靠路由表和ARP表来确定出口接口以及将数据包转发到下一跳所需的数据，而TFW模式则使用MAC地址表来确定用于将数据包发送到目的地的出口接口。防火墙会查看正在处理的数据包的目的MAC地址字段，并搜索将此地址与接口链接起来的条目。

MAC地址表包含这些字段。

```
> 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
```

- 接口 — 此字段保留动态获取或静态配置此MAC地址的接口名称
- MAC地址 — 要存储的MAC地址记录
- type — 用于学习条目的方法。它可以是动态的，也可以是静态的
- Age(min) — 以分钟为单位递减计时器，显示该条目标记为失效之前剩余的时间。此计时器仅适用于动态学习条目
- bridge-group — 接口所属的网桥组ID

数据包转发决策类似于交换机，但在MAC表中缺少条目时，有一个非常重要的区别。在交换机中，数据包通过除入口接口之外的所有接口广播，但在TFW中。如果收到数据包，并且没有目的MAC地址的条目，则数据包将被丢弃。它被加速安全路径(ASP)丢弃代码*dst-l2_lookup-fail丢弃*。

```
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
```

如果MAC地址之前在数据包中不被视为源MAC地址，则在启用动态学习且没有目标静态条目的环境中，第一个数据包始终会出现此情况。

将条目添加到MAC地址表后，可以将下一个数据包设置为启用的防火墙功能。

```
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
```

> **警告**：MAC查找是防火墙所执行操作的第一阶段。由于Failed L2查找而不断丢弃可能导致相关数据包丢失和/或检测引擎检查不完整。影响依赖于协议或应用功能来重新传输。

根据上述，总是最好在传输之前先获取条目。TFW具有多种机制来学习条目。

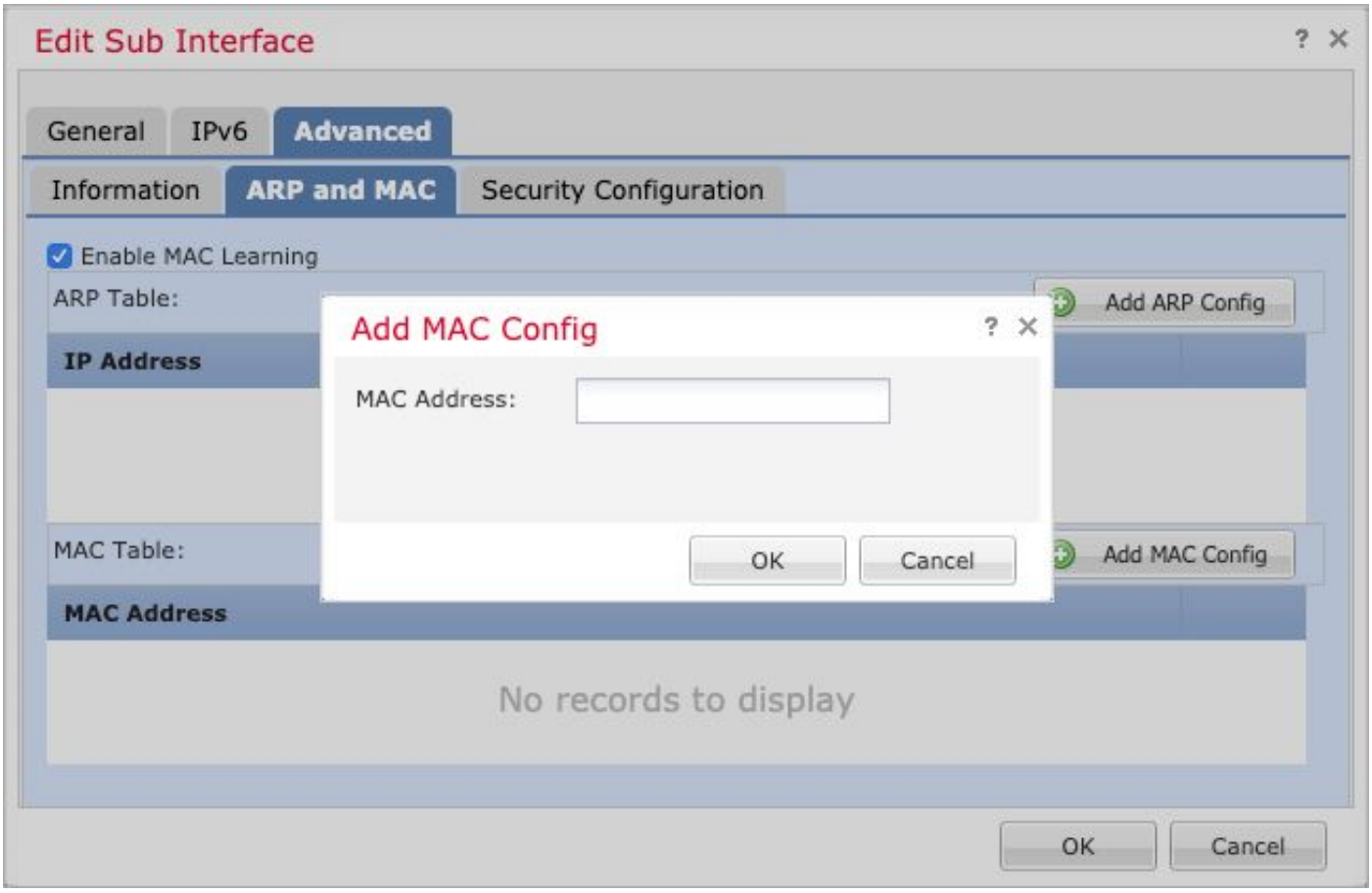
MAC地址表学习选项

静态条目

可以手动添加MAC地址，使防火墙始终使用该特定条目的相同接口。对于不易更改的条目，这是有效选项。当静态MAC在配置级别被覆盖或在下一跳被功能覆盖时，这是常见选项。

例如，在默认网关MAC地址始终与手动添加到配置中的Cisco路由器上的默认网关MAC地址相同或HSRP虚拟MAC地址保持不变的情况下。

要在由FMC管理的FTD中配置静态条目，可以单击**Edit Interface / Subinterface > Advanced > ARP and MAC，然后单**击Add MAC Config**。**这会为正在从Devices > Device Management > Interfaces部分编辑的特**定接口添加一个**条目。



基于源MAC地址的动态学习

此方法类似于交换机填充MAC地址表的操作。如果数据包的源MAC地址不是收到的接口的MAC表条目的一部分，则会向该表中添加新条目。

基于ARP探测的动态学习

如果数据包到达的目的MAC地址不是MAC表的一部分，并且目的IP与网桥虚拟接口(BVI)属于同一网络，则TFW会尝试获知它通过所有网桥组接口发送ARP请求。如果从任何网桥组接口收到ARP应答，则会将其添加到MAC表。请注意，如上所述，当没有对该ARP请求的应答时，所有数据包都会使用ASP代码*dst-l2_lookup-fail丢弃*。

基于ICMP探测的动态学习

如果数据包到达的目的MAC地址不是MAC表的一部分，并且目的IP不是与BVI属于同一网络的一部分，则会发送ICMP回应请求，其生存时间(TTL)值等于1。防火墙希望ICMP超时消息获取下一跳MAC地址。

MAC地址表老化计时器

MAC地址表老化计时器为每个学习的条目设置为5分钟。此超时值有两个不同的阶段。

老化超时第一阶段

在前3分钟内，除非源MAC地址等于MAC地址表中的条目的ARP应答数据包通过防火墙，否则MAC条目老化时间值不会刷新。此情况不包括发往网桥组IP地址的ARP应答。这意味着在前3分钟

内，将忽略任何其他非直通ARP应答的数据包。

在本例中，IP地址为10.10.10.5的PC向10.20.20.5发送ping命令。10.20.20.5的网关IP地址为10.20.20.3,MAC地址为0000.0cf.f014。

目的PC每25秒创建一次ARP更新，导致持续的ARP数据包通过防火墙。

```
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
```

数据包捕获过滤ARP数据包用于匹配这些数据包。

```
> 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.4014的条目保持为5，且从不低于该数字。

```
> 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
```

老化超时第二阶段

在最近2分钟内，该条目将进入地址视为过期的时间段。

```
> 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
```

该条目尚未删除，如果检测到任何具有与表条目匹配的源MAC地址的数据包（包括到机箱的数据包），则年龄条目将刷新回5分钟。

在本例中，在此2分钟内发送ping命令，以强制防火墙发送自己的ARP数据包。

```
> 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地址条目设置回5分钟。

```
> 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 表

首先，必须了解MAC地址表完全独立于ARP表。虽然防火墙发送的用于刷新ARP条目的ARP数据包可以同时刷新MAC地址表，但这些刷新过程是独立的任务，每个过程都有自己的超时和条件。

即使ARP表不用于确定路由模式下的出口下一跳，也必须了解在透明部署中生成并发往防火墙标识IP的ARP数据包的影响。

ARP条目用于管理目的，仅在管理功能或任务需要时添加到表中。例如，如果网桥组有IP地址，则此IP可用于ping目标。

```
> 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
```

如果目的地与网桥组IP位于同一子网中，它会强制发出ARP请求，如果收到有效的ARP应答，则IP/MAC条目将存储在ARP表中。

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

与MAC地址表不同，接口/IP地址/MAC地址三连体的计时器值也在增加。

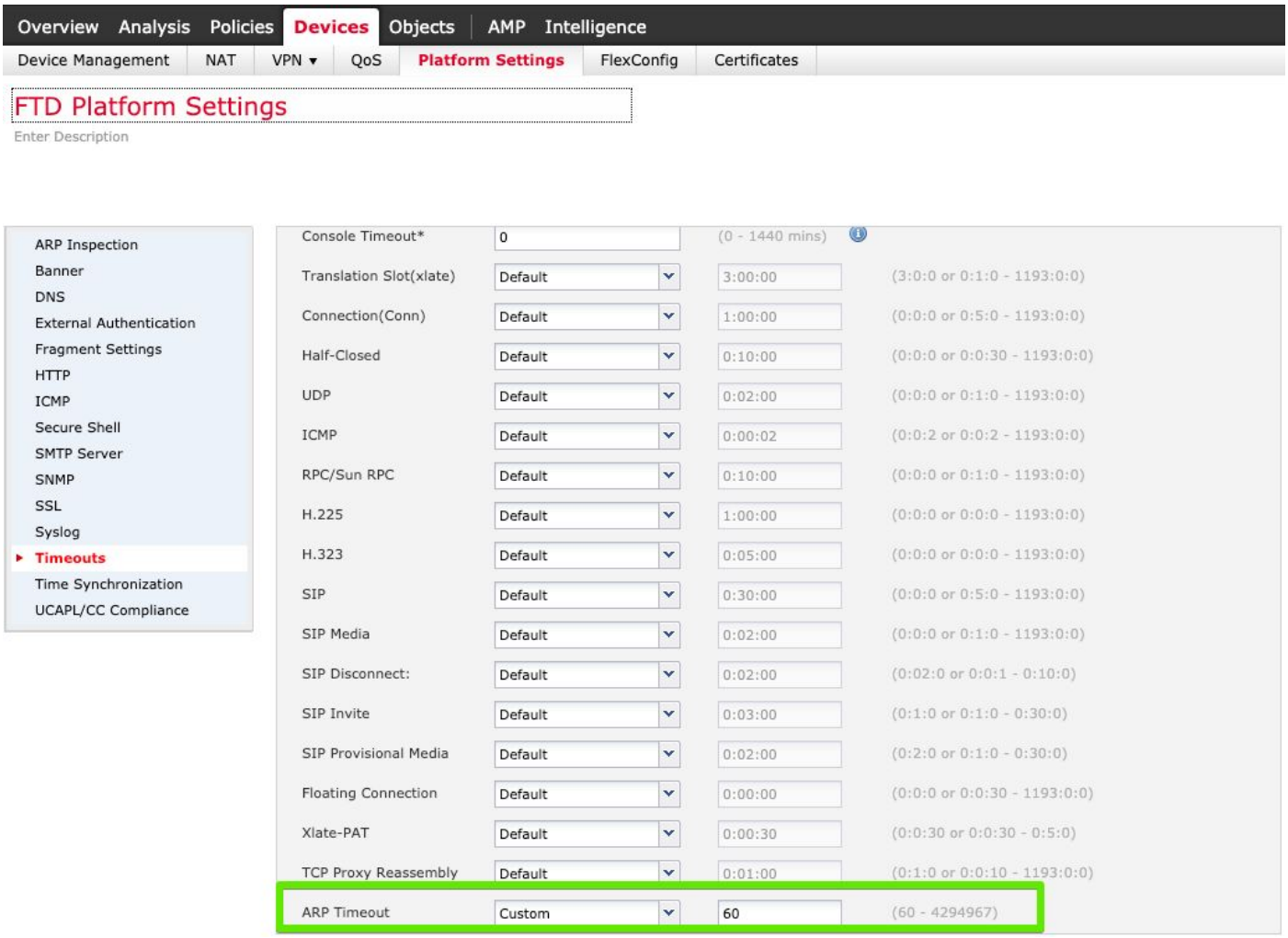
```
> show arp
Inside 10.20.20.3 0000.0c9f.f014 1
>show arp
Inside 10.20.20.3 0000.0c9f.f014 2
>show arp
Inside 10.20.20.3 0000.0c9f.f014 3
>show arp
Inside 10.20.20.3 0000.0c9f.f014 4
```

当计时器达到*n - 30*值(其中*n是ARP配置的超时*(默认为14400秒))时，防火墙会发送ARP请求以刷新条目。如果收到有效的ARP应答，则保留该条目，计时器返回0。

在本例中，ARP超时被缩短到60秒。

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

此超时可在FMC的“设备”**>“平台设置”>“超**时”选项卡上进行配置，如图所示。



由于超时为60秒，因此每30秒发送一次ARP请求(60 - 30 = 30)。

```
> 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
```

然后，ARP条目每30秒刷新一次。

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

故障排除提示

流量方向

在TFW上要跟踪的最困难之一是流量方向。了解流量如何有助于确保防火墙将数据包正确转发到目的地。

在路由模式下，确定正确的入口和出口接口是比较容易的任务，因为存在多个防火墙参与的指标，例如源和目的MAC地址修改以及从一个接口到另一个接口的生存时间(TTL)值减少。

这些差异在TFW设置中不可用。在大多数情况下，通过入口接口的数据包看起来与离开防火墙时相同。

在不知道数据包进入何处以及何时离开防火墙的情况下，跟踪特定问题（如网络中的MAC抖动或流量环路）可能会更加困难。

为了帮助区分入口和出口数据包，可以在数据包捕获中使用trace关键字。

```
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 — 增加捕获缓冲区（以字节为单位）。33554432是最大可用值。在5500-X、Firepower设备或虚拟机等型号中，只要尚未配置数十个捕获，使用此大小值是安全的。

trace — 为指定捕获的启用跟踪选项。

trace-count — 允许更多跟踪。1000是允许的最大值，128是默认值。按照与缓冲区大小选项相同的建议，这也是安全的。

> **提示：**如果忘记添加其中一个选项，则无需通过引用捕获名称和选项重新编写整个捕获，即可添加该选项。但是，新选项仅影响新捕获的数据包，因此，必须使用**clear capture *capname***来产生自数据包编号1以来的新效果。示例：**跟踪捕获**

捕获数据包后，命令**show capture *cap_name* trace**将显示被侵入数据包的前1000（如果增加了跟踪编号）跟踪。

```
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
```

此输出是外部接口数据包捕获跟踪的示例。这意味着数据包编号1和3将外部接口压缩，数据包编号2将压缩接口。

在此跟踪中可以找到其他信息，如对该数据包采取的操作和丢弃原因（如果数据包被丢弃）。

对于较长的跟踪，如果您要关注单个数据包，show capture *cap_name* trace packet-number *packet_*number命令可用于显示该特定数据包的跟踪。

这是允许的数据包编号10的示例。

```
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跟踪

TFW根据MAC地址做出所有转发决策。在流量分析过程中，必须确保每个数据包上用作源地址和目的地址的MAC地址根据网络拓扑正确无误。

数据包捕获功能允许您显示使用show capture命令中的detail选*项所*使用的MAC地址。

```
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)
```

找到需要特定跟踪的相关MAC地址后，捕获过滤器将允许您对其进行匹配。

```
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)
```

当有MAC摆动的痕迹并且您想要找到问题时，此过滤器非常有用。

Mac地址表调试

可以启用MAC地址表调试来检查每个阶段。此调试提供的信息有助于了解何时从表中学习、刷新和删除MAC地址。

本节显示每个阶段的示例以及如何阅读此信息。要在FTD上启用debug命令，必须访问诊断CLI。

> **警告：**如果网络太忙，调试可能会消耗相关资源。建议在受控环境或低高峰时段使用它们。如果这些调试过于冗长，建议将这些调试发送到系统日志服务器。

```
> 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
```

步骤1.获取MAC地址。当MAC表中已未找到条目时，此地址将添加到表中。调试消息会通知地址和接收地址的接口。

```
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.
!!!!
```

如果通过ICMP方法获知MAC，则显示下一条消息。该条目进入超时周期的第一阶段，在该阶段不会根据MAC地址表老化时间计时器中列出的条件刷新其计时器。

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

步骤2.如果某个条目已知，调试会通知该条目。调试还显示独立设置或HA设置中不相关的集群消息。

```
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
```

步骤3.一旦条目到达第二阶段（在绝对超时之前2分钟）。

```
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
```

步骤4.防火墙现在希望使用该地址生成的新数据包刷新表。如果在这2分钟内没有使用该条目的数据包，则删除该地址。

```
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.
```

相关信息

- Firepower管理中心指南，版本6.3 — 第3章：用于Firepower威胁防御的透明或路由防火墙模式
- 技术支持和文档 - Cisco Systems