Firepower威脅防禦透明防火牆模式高級概念和故障排除提示

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[透明防火牆進階概念](#)
[MAC地址表](#)
[MAC地址表學習選項](#)
[靜態條目](#)
[基於源MAC地址的動態學習](#)
[基於ARP探測的動態學習](#)
[基於ICMP探測的動態學習](#)
[MAC地址表老化計時器](#)
[老化超時第一階段](#)
[老化超時第二階段](#)
[ARP表](#)
[疑難排解提示](#)
[流量方向](#)
[MAC跟蹤](#)
[Mac-address-table Debug](#)
[相關資訊](#)

簡介

本檔案介紹瞭解透明防火牆(TFW)模式下Firepower威脅防禦(FTD)部署的核心概念和要素的詳細說明。針對透明防火牆體系結構最常見的問題，本文還提供有用的工具和一些解決方法。

作者：Cesar Lopez，編輯者：Yeraldin Sánchez，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco FTD透通防火牆模式知識
- 熱待命路由器通訊協定(HSRP)概念
- 位址解析通訊協定(ARP)和網際網路控制訊息通訊協定(ICMP)通訊協定

強烈建議閱讀「Firepower配置指南[透明或路由防火牆模式」一節](#)，以更好地瞭解本文檔中介紹的概念。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

透明防火牆進階概念

MAC地址表

雖然路由模式下的防火牆依賴路由表和ARP表來確定出口介面以及將資料包轉發到下一跳所需的資料，但是TFW模式使用MAC地址表來確定用於將資料包傳送到其目標的出口介面。防火牆會檢視正在處理的封包的目標MAC位址欄位，並搜尋將此位址與介面連結的專案。

MAC地址表包含以下欄位。

```
> 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
```

- Interface — 此欄位保留從中動態獲取或靜態配置此MAC地址的介面名稱
- MAC地址 — 要儲存的MAC地址記錄
- type — 用於學習條目的方法。可以是動態的，也可以是靜態的
- Age(min) — 減少計時器（以分鐘為單位），顯示條目標籤為失效之前剩餘的時間。此計時器僅適用於動態學習條目
- bridge-group — 介面所屬的網橋組ID

封包轉送決定與交換器類似，但若是MAC表中遺失專案，則差別非常重大。在交換機中，資料包通過除入口介面之外的所有介面進行廣播，但在TFW中，如果收到資料包，且沒有目標MAC地址條目，則資料包將被丟棄。使用加速安全路徑(ASP)丟棄代碼*dst-l2_lookup-fail*將其丟棄。

```
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
```

如果在封包中之前未將MAC位址視為來源MAC位址，則會在啟用動態學習且沒有目的地靜態專案的環境中，對第一個封包總是發生這種情況。

一旦將條目新增到MAC地址表中，就允許將下一個資料包調整為已啟用防火牆功能。

```
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
```

> **注意**：MAC查詢是防火牆採取的操作的第一階段。由於L2查詢失敗導致持續丟棄可能導致相關資料包丟失和/或不完全檢測引擎檢查。這種影響依賴於協定或應用功能重新傳輸。

基於上述所述，在任何傳輸之前總是優選地獲知條目。TFW有多個機制來學習條目。

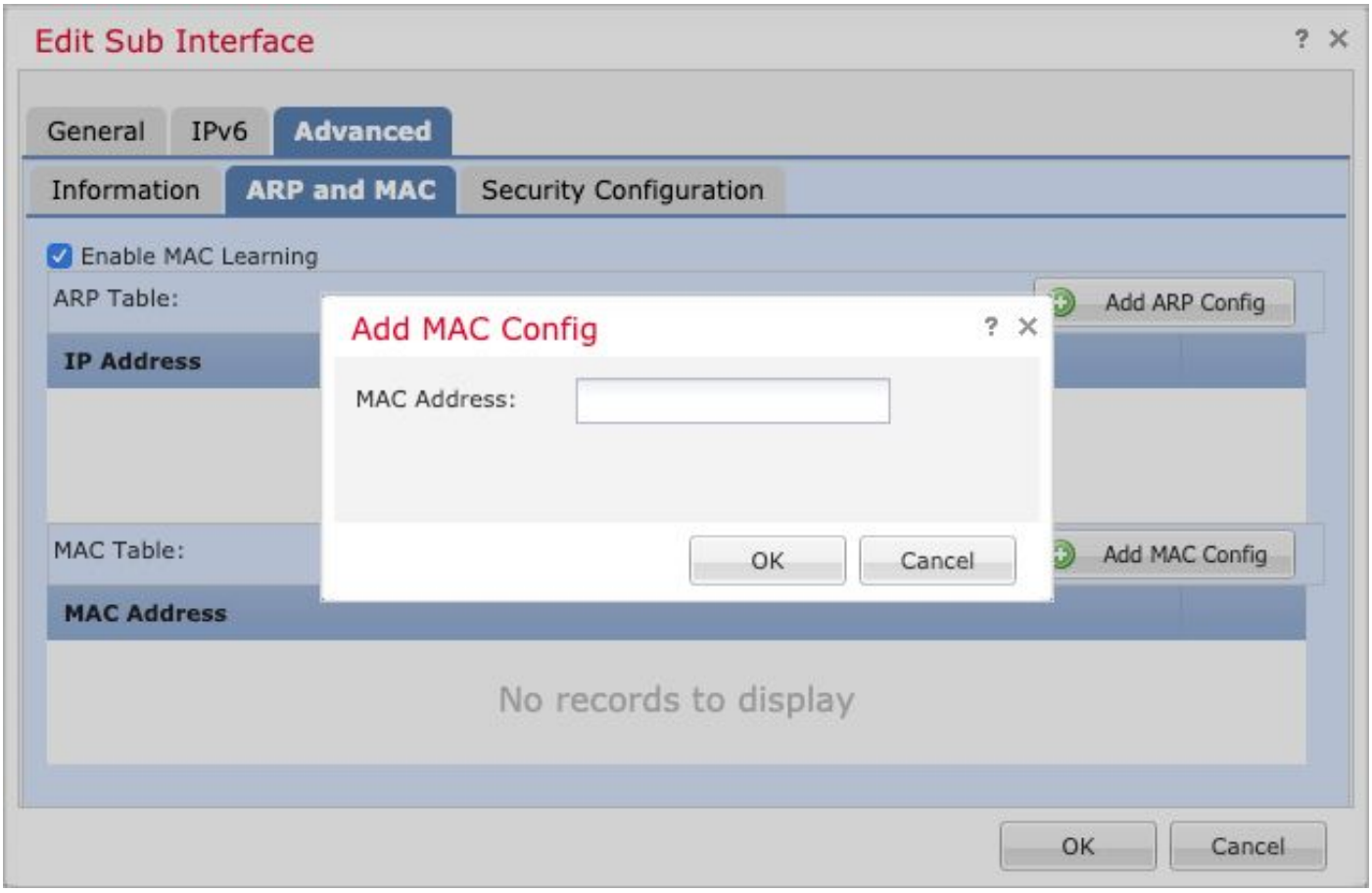
MAC地址表學習選項

靜態條目

可以手動新增MAC地址，使防火牆始終對該特定條目使用相同的介面。對於不易受更改的條目，這是一個有效的選項。當靜態MAC在配置級別被覆蓋或被下一跳的功能覆蓋時，這是一個常見選項。

例如，在以下情況中，Cisco路由器上的預設網關MAC地址始終與手動新增到配置中的相同，或者HSRP虛擬MAC地址將保持不變。

若要在FMC管理的FTD中設定靜態專案，可以按一下「**Edit Interface / Subinterface > Advanced > ARP and MAC**」，然後按一下「**Add MAC Config**」。這將新增從**Devices > Device Management > Interfaces**部分編輯的特定介面的條目。



基於源MAC地址的動態學習

此方法類似於交換機填寫MAC地址表的操作。如果資料包的源MAC地址不屬於所接收介面的MAC表條目，則會向表中新增新條目。

基於ARP探測的動態學習

如果封包到達時所用的目的地MAC位址不是MAC表的一部分，且目的地IP與橋接器虛擬介面(BVI)屬於同一網路，則TFW會嘗試得知其透過所有橋接器群組介面傳送ARP要求。如果收到來自任何網橋組介面的ARP應答，則會將其新增到MAC表中。請注意，如上文所述，雖然沒有回覆該ARP請求，但所有資料包都會被ASP代碼*dst-l2_lookup-fail*丟棄。

基於ICMP探測的動態學習

如果封包到達時所用的目的地MAC位址不是MAC表的一部分，且目的地IP不是BVI的同一網路的一部分，則會傳送一個ICMP回應要求，其生存時間(TTL)值等於1。防火牆期望ICMP超出時間訊息來瞭解下一個躍點的MAC位址。

MAC地址表老化計時器

對於每個獲知的條目，MAC地址表老化計時器設定為5分鐘。此超時值有兩個不同的階段。

老化超時第一階段

在前3分鐘內，MAC條目Age值不會刷新，除非ARP應答資料包通過防火牆，且源MAC地址等於MAC地址表中的條目。此條件不包括發往網橋組IP地址的ARP應答。這表示在前3分鐘內，任何不

是機箱內ARP回覆的其他資料包都會被忽略。

在本示例中，IP地址為10.10.10.5的PC正在向10.20.20.5傳送ping。10.20.20.5的網關IP地址為10.20.20.3,MAC地址為000.0c9f.f014。

目的PC每25秒建立一次ARP更新，導致持續的ARP資料包通過防火牆。

```
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
```

資料包捕獲過濾ARP資料包用於匹配這些資料包。

```
> 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的條目始終為5，並且不會低於該數字。

```
> 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
```

老化超時第二階段

在最後2分鐘內，該條目進入被視為地址已過時的時間段。

```
> 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
```

該條目尚未刪除，如果檢測到任何源MAC地址與表條目（包括出廠設定資料包）匹配的資料包，則老化條目將刷新回5分鐘。

在本例中，此2分鐘內會傳送ping，強制防火牆傳送自己的ARP封包。

```
> 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地址條目被重新設定為5分鐘。

```
> 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，必須瞭解MAC地址表完全獨立於ARP表。當防火牆傳送的ARP資料包刷新一個ARP條目時，可以同時刷新MAC地址表，這些刷新過程是單獨的任務，每個過程都有自己的超時和條件。

即使ARP表不是像在路由模式中那樣用於確定出口下一跳，瞭解在透明部署中生成和發往防火牆身份的ARP資料包的影響也很重要。

ARP條目用於管理目的，僅在管理功能或任務需要時才新增到表中。作為管理任務的示例，如果網橋組具有IP地址，則此IP可用於ping目的地。

```
> 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
```

如果目的地與網橋組IP位於同一子網中，則會強制執行ARP請求；如果收到有效的ARP應答，則IP/MAC條目將儲存在ARP表中。

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

與MAC地址表不同，介面/IP地址/MAC地址三元組附帶的計時器是一個遞增值。

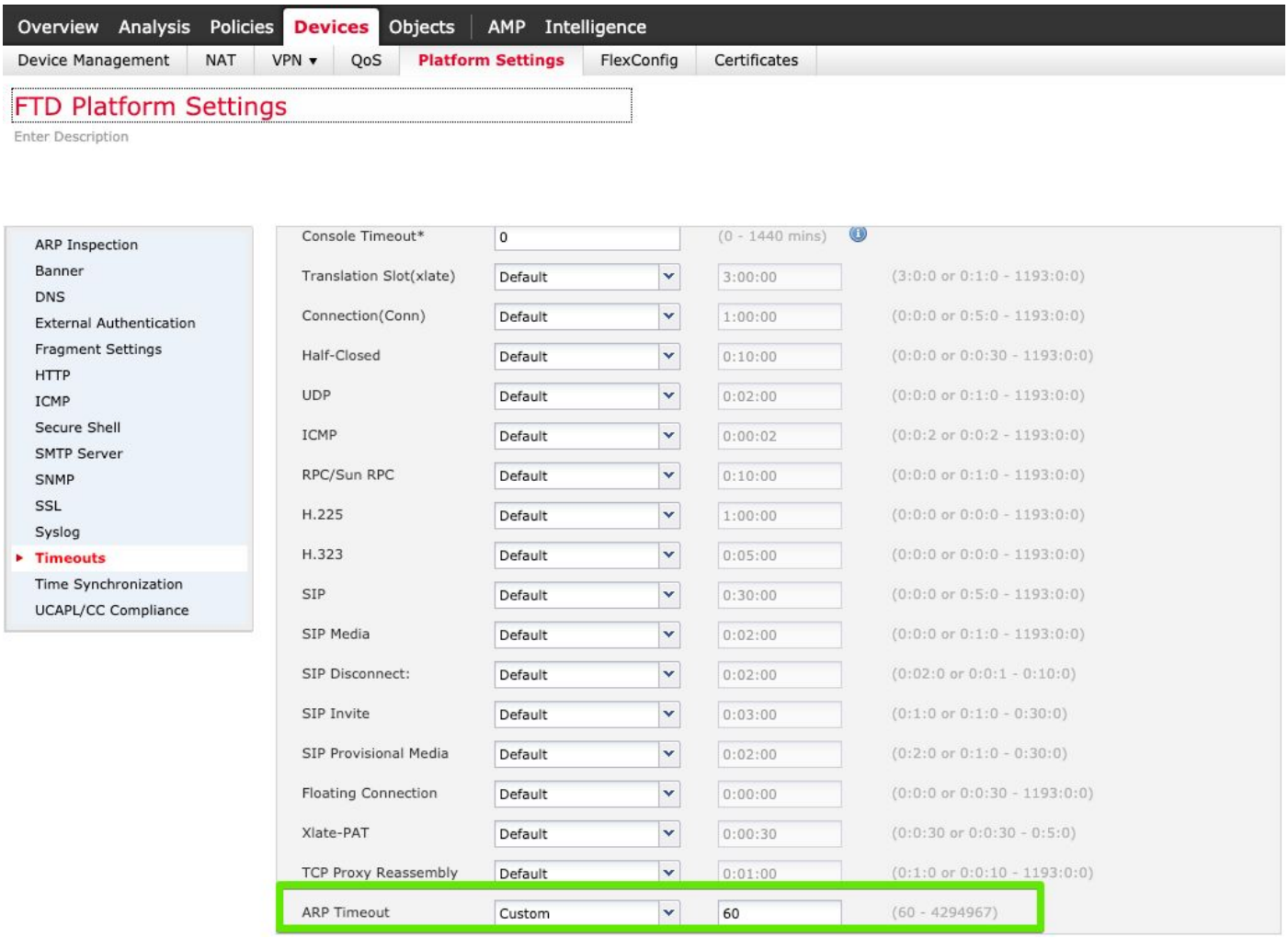
```
> show arp
Inside 10.20.20.3 0000.0c9f.f014 1
>show arp
Inside 10.20.20.3 0000.0c9f.f014 2
>show arp
Inside 10.20.20.3 0000.0c9f.f014 3
>show arp
Inside 10.20.20.3 0000.0c9f.f014 4
```

當計時器達到*n - 30*值(其中*n*是ARP設定的逾時(預設值為14400秒)時，防火牆會傳送一個ARP要求來刷新專案。如果收到有效的ARP應答，則保留條目，計時器返回到0。

在本例中，ARP超時縮短到60秒。

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

可以在FMC中的**Devices > Platform Settings > Timeouts**頁籤中配置此超時，如下圖所示。



由於超時為60秒，因此每30秒傳送一個ARP請求(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
```

然後，ARP專案每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
```

疑難排解提示

流量方向

在TFW上跟蹤最困難的事情之一是流量方向。瞭解流量如何流動有助於確保防火牆正確地將封包轉送到目的地。

在路由模式下，確定正確的入口和出口介面是一項更輕鬆的任務，因為存在多個防火牆參與的指標，例如源和目標MAC地址修改和從一個介面到另一個介面的生存時間(TTL)值減少。

這些差異在TFW設定中不可用。大多數情況下，通過輸入介面的封包看起來與離開防火牆時相同。

如果不瞭解資料包進入何處以及何時離開防火牆，跟蹤網路中的MAC擺動或流量環路等特定問題會更加困難。

為了幫助區分輸入和輸出資料包，可以在資料包捕獲中使用trace關鍵字。

```
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 — 增加捕獲緩衝區（以位元組為單位）。33554432是最大可用值。在5500-X、Firepower裝置或虛擬機器等型號中，只要尚未配置數十個捕獲，即可安全地使用此大小值。

trace — 為指定的捕獲啟用跟蹤選項。

trace-count — 允許更多跟蹤。1000是允許的最大值，128是預設值。這同樣適用於按照與緩衝區大小選項相同的建議操作。

> **提示：**如果您忘記新增其中一個選項，您可以通過引用捕獲名稱和選項來新增該選項，而不必再次寫入整個捕獲。但是，新選項僅影響新捕獲的資料包，因此，必須使用**clear capture** ***capname*** 來產生自資料包編號1以來的新效果。示例：**在跟蹤中捕獲**

擷取封包後，**show capture** ***cap_name*** trace指令會顯示傳入封包的前1000個追蹤（如果追蹤數量增加）。

```
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
```

以下輸出是外部介面資料包捕獲跟蹤的示例。這表示封包1和3進入外部介面，封包2離開介面。

可以在此追蹤軌跡中找到其他資訊，例如對該封包執行的行動以及封包遭捨棄情況下的捨棄原因。

對於較長的跟蹤，如果要集中處理單個資料包，可以使用**show capture** ***cap_name*** trace packet-number packet_number 命令顯示該特定資料包的跟蹤。

以下是允許資料包編號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跟蹤

TFW根據MAC地址做出其所有轉發決策。在流量分析過程中，必須根據網路拓撲確保每個資料包上用作源和目標的MAC地址正確。

封包擷取功能可讓您顯示使用**show capture** 指令的***detail*** 選項所使用的MAC位址。

```
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)
```

找到需要特定追蹤的感興趣MAC位址後，擷取過濾器會允許您將其相符。

```
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)
```

此過濾器在存在MAC翻動的痕跡且您想要找到肇事者時非常有用。

Mac-address-table Debug

可以啟用MAC地址表調試以檢視每個階段。此調試提供的資訊有助於瞭解何時從表中獲取、刷新和刪除MAC地址。

本節顯示每個階段的示例以及如何閱讀此資訊。若要在FTD上啟用debug指令，您必須存取診斷CLI。

> **警告：**如果網路太忙，調試可能會消耗相關資源。建議在受控環境或低峰值時間使用它們。如果系統日誌伺服器的調試過於詳細，建議將這些調試傳送到系統日誌伺服器。

```
> 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
```

步驟1.獲取MAC地址。如果在MAC表中找不到條目，則此地址將新增到表中。偵錯訊息會通知接收該訊息的地址和介面。

```
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.
!!!!
```

如果透過ICMP方法得知MAC，則顯示下一個訊息。該條目進入超時週期的第一階段，在該階段不會根據MAC地址表老化計時器中列出的條件刷新其計時器。

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

步驟2.如果專案已知，則偵錯會通知該專案。調試還會顯示與獨立或HA設定無關的集群消息。

```
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
```

步驟3.輸入內容到達第二階段後（絕對超時前2分鐘）。

```
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
```

步驟4.防火牆現在要求源自該地址的新封包刷新該表。如果在這2分鐘內沒有其它資料包使用該條目，則該地址將被刪除。

```
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.
```

相關資訊

- Firepower管理中心指南6.3版 — 第3章：適用於Firepower威脅防禦的透明或路由防火牆模式
- 技術支援與文件 - Cisco Systems