Firepower Threat Defenseトランスペアレントファイアウォールモードの高度な概念とトラブルシューティングのヒント

内容

概要

このドキュメントでは、トランスペアレントファイアウォール(TFW)モードでのFirepower Threat Defense(FTD)の導入の主要な概念と要素を理解するための詳細な説明について説明します。この記事では、トランスペアレントファイアウォールアーキテクチャに関連する最も一般的な問題に対する便利なツールとウォークスルーについても説明します。

著者：Cisco TACエンジニア、Cesar Lopez、編集：Yeraldin Sanchez

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco FTDトランスペアレントファイアウォールモードの知識

- ホットスタンバイルータプロトコル(HSRP)の概念
- アドレス解決プロトコル(ARP)およびインターネット制御メッセージプロトコル(ICMP)プロトコル

このドキュメントで説明されている概念をより理解するために、『Firepower設定ガイドトランスペアレントファイアウォールモードまたはルーテッドファイアウォールモード』セクションを読むことを強くお勧めします。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Firepower 4120 FTDバージョン6.3.0.4
- Cisco Firepower Management Center(FMC)バージョン6.3.0.4
- Cisco ASR1001 IOS-XEバージョン16.3.9
- Cisco Catalyst 3850 IOS-XEバージョン16.9.3

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、初期（デフォルト）設定の状態から起動しています。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。

トランスペアレントファイアウォールの高度な概念

MAC アドレス テーブル

ルーテッドモードのファイアウォールは、出力インターフェイスと必要なデータをルーティングテーブルとARPテーブルに基づいてパケットをネクストホップに転送しますが、TFWモードはMACアドレステーブルを使用して、パケットの宛先への送信に使用される出力インターフェイスを判別します。ファイアウォールは、処理中のパケットの宛先MACアドレスフィールドを参照し、このアドレスとインターフェイスをリンクするエントリを検索します。

MACアドレステーブルには、次のフィールドがあります。

```
> 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：このフィールドには、このMACアドレスが動的に学習または静的に設定された場所からのインターフェイス名が保持されます
- MACアドレス – 保存するMACアドレスレコード
- type – エントリの学習に使用するメソッド。ダイナミックまたはスタティックにすることができます
- Age(min)：ディクリメンタルタイマー（分）。このエントリがdeadとしてマークされるまでの残り時間を表示します。このタイマーは、動的に学習するエントリにのみ適用されます
- bridge-group：インターフェイスが属するブリッジグループID

パケット転送の決定はスイッチに似ていますが、MACテーブルのエントリが欠落していると、非常に重要な違いがあります。スイッチでは、パケットは入力インターフェイスを除くすべてのインターフェイスでブロードキャストされますが、TFWでは、パケットが受信され、宛先MACアド

レスのエントリがない場合、パケットはドロップされます。Accelerated Security Path (ASP)ドロップコード*dst-l2_lookup-failで廃棄されます*。

```
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
```

この状態は、ダイナミックラーニングが有効な環境の最初のパケットで常に発生し、パケット内で以前に送信元MACアドレスとしてMACアドレスが見られなかった場合は、宛先のスタティックエントリが存在しません。

エントリがMACアドレステーブルに追加されると、次のパケットはファイアウォール機能を有効にするよう調整できます。

```
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ルックアップは、ファイアウォールによって実行されるアクションの最初のフェーズです。L2ルックアップの失敗によるドロップが絶えず発生すると、関連するパケット損失や検出エンジン検査が不完全になる可能性があります。この影響は、プロトコルまたはアプリケーションの再送信に依存します。

上記に基づいて、エントリを送信する前に学習しておくことをお勧めします。TFWには、エントリを学習するための複数のメカニズムがあります。

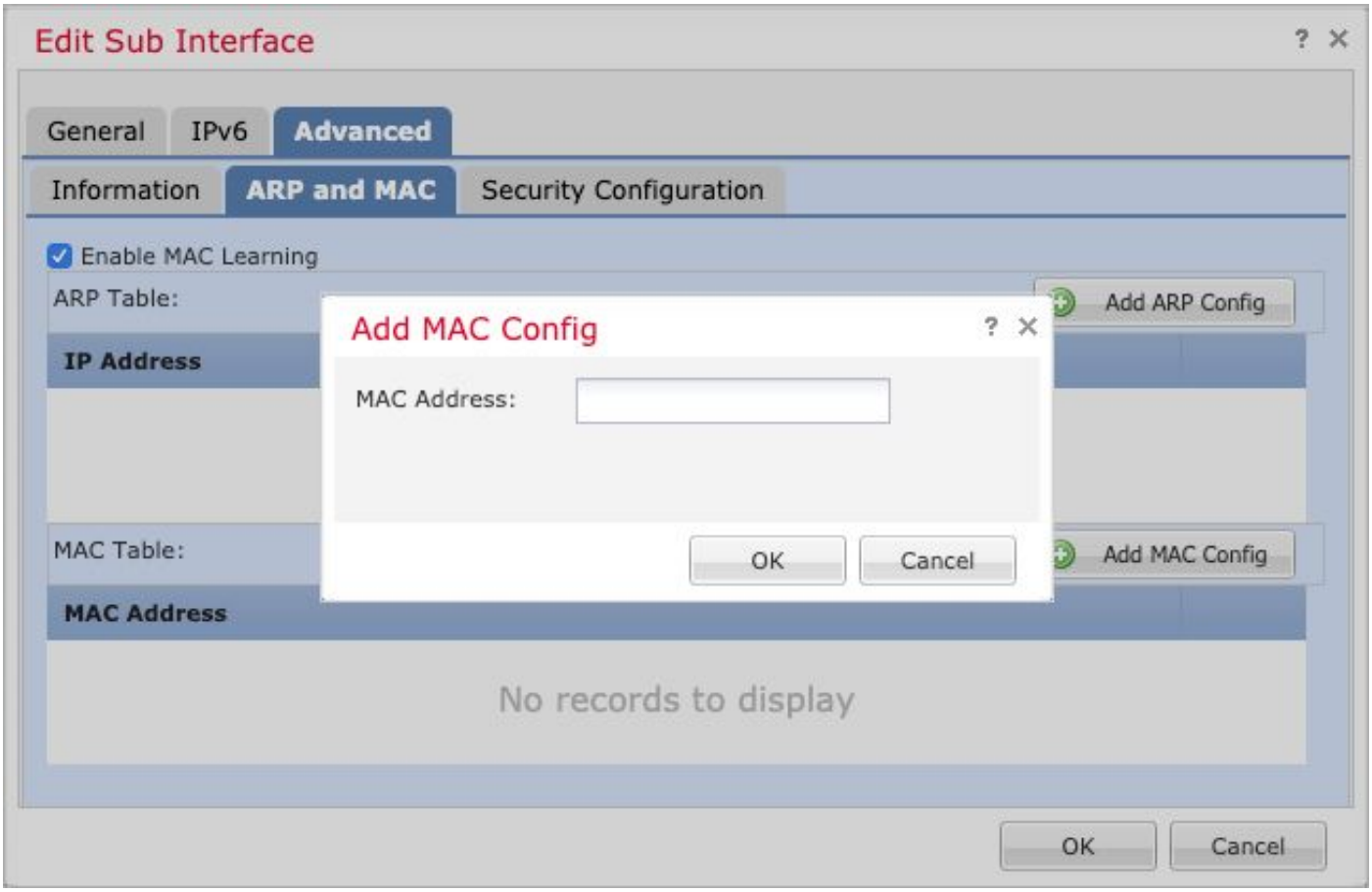
MACアドレステーブルの学習オプション

スタティックエントリ

MACアドレスを手動で追加して、ファイアウォールがその特定のエントリに常に同じインターフェイスを使用するようにできます。これは、変更の可能性がないエントリに対して有効なオプションです。これは、スタティックMACが設定レベルまたはネクストホップの機能によって上書きされる場合の一般的なオプションです。

たとえば、デフォルトゲートウェイのMACアドレスが、設定に手動で追加されたCiscoルータ上で常に同じになるシナリオ、またはHSRP仮想MACアドレスが同じままである場合などです。

FMCによって管理されるFTDのスタティックエントリを設定するには、**[Edit Interface / Subinterface] > [Advanced] > [ARP and MAC]をクリックし、[Add MAC Config]をクリックします**。[デバイス] > [デバイス管理] > [インターフェイス]セクションから編集する特定の**インターフェイスのエントリが追加**されます。



送信元MACアドレスに基づく動的学習

この方法は、スイッチがMACアドレステーブルにデータを入力する方法に似ています。パケットの送信元MACアドレスが、受信したインターフェイスのMACテーブルエントリの一部ではない場合、新しいエントリがテーブルに追加されます。

ARPプローブに基づく動的学習

MACテーブルの一部ではない宛先MACアドレスを持つパケットが到着し、宛先IPがブリッジ仮想インターフェイス(BVI)と同じネットワークの一部である場合、TFWは、すべてのブリッジグループインターフェイスを介してARP要求を送信しようとします。ARP応答がブリッジグループインターフェイスのいずれかから受信されると、MACテーブルに追加されます。前述したように、このARP要求に対する応答はありませんが、すべてのパケットはASPコード*dst-l2_lookup-fail*で*ドロップされることに注意してください*。

ICMPプローブに基づく動的学習

MACテーブルの一部ではない宛先MACアドレスを持つパケットが到着し、宛先IPがBVIと同じネットワークの一部でない場合、ICMPエコー要求がTime-to-Live(TTL)値で1に送信されます。

MACアドレステーブル経過時間タイマー

MACアドレステーブルのAgeタイマーは、学習したエントリごとに5分に設定されます。このタイムアウト値には2つの異なる段階があります。

Age Timeout First Stage

最初の3分間は、送信元MACアドレスを持つファイアウォールを通過するARP応答パケットがMACアドレステーブルのエントリと等しくない限り、MACエントリの経過時間の値は更新されません。この条件では、ブリッジグループIPアドレス宛てのARP応答は除外されます。これは、through-the-box ARP応答ではない他のパケットは、最初の3分間は無視されることを意味します。

この例では、IPアドレス10.10.10.5のPCが10.20.20.5にpingを送信しています。10.20.20.5のゲートウェイIPアドレスは10.20.20.3で、MACアドレスは0000.0c9f.f014です。

宛先PCは25秒ごとにARPアップデートを作成し、ARPパケットがファイアウォールを通過し続けます。

```
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
```

これらのパケットの照合には、パケットキャプチャフィルタリングARPパケットが使用されます。

```
> 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のエントリは5のままであり、この数値を下回ることはありません。

```
> 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
```

経過時間タイムアウト第2段階

最後の2分間、エントリはアドレスがエージングアウトと見なされる期間に入ります。

```
> 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
```

エントリはまだ削除されておらず、to-the-boxパケットを含むテーブルエントリに一致する送信元MACアドレスを持つパケットが検出されると、Ageエントリが5分に更新されます。

この例では、ファイアウォールが自身のARPパケットを送信するように、この2分以内にpingが送信されます。

```
> 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アドレスエントリは5分に戻されます。

```
> 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テーブル

まず、MACアドレステーブルはARPテーブルから完全に独立していることを理解することが重要です。ARPエントリを更新するためにファイアウォールから送信されるARPパケットは、MACアドレステーブルを同時に更新できますが、これらの更新プロセスは別々のタスクであり、それぞれ独自のタイムアウトと条件があります。

ARPテーブルをルーテッドモードのように出力ネクストホップの決定に使用していない場合でも、トランスペアレント展開でファイアウォールID IP宛てに生成されたARPパケットの影響を理解することが重要です。

ARPエントリは管理目的で使用され、管理機能またはタスクに必要な場合にのみテーブルに追加されます。管理タスクの例として、ブリッジグループにIPアドレスがある場合、このIPを使用して宛先にpingを実行できます。

```
> 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
```

宛先がブリッジグループIPと同じサブネットにある場合は、ARP要求を強制し、有効なARP応答を受信すると、IP/MACエントリがARPテーブルに保存されます。

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

MACアドレステーブルとは異なり、インターフェイス/IPアドレス/MACアドレスのトリプレットに付随するタイマーは増加する値です。

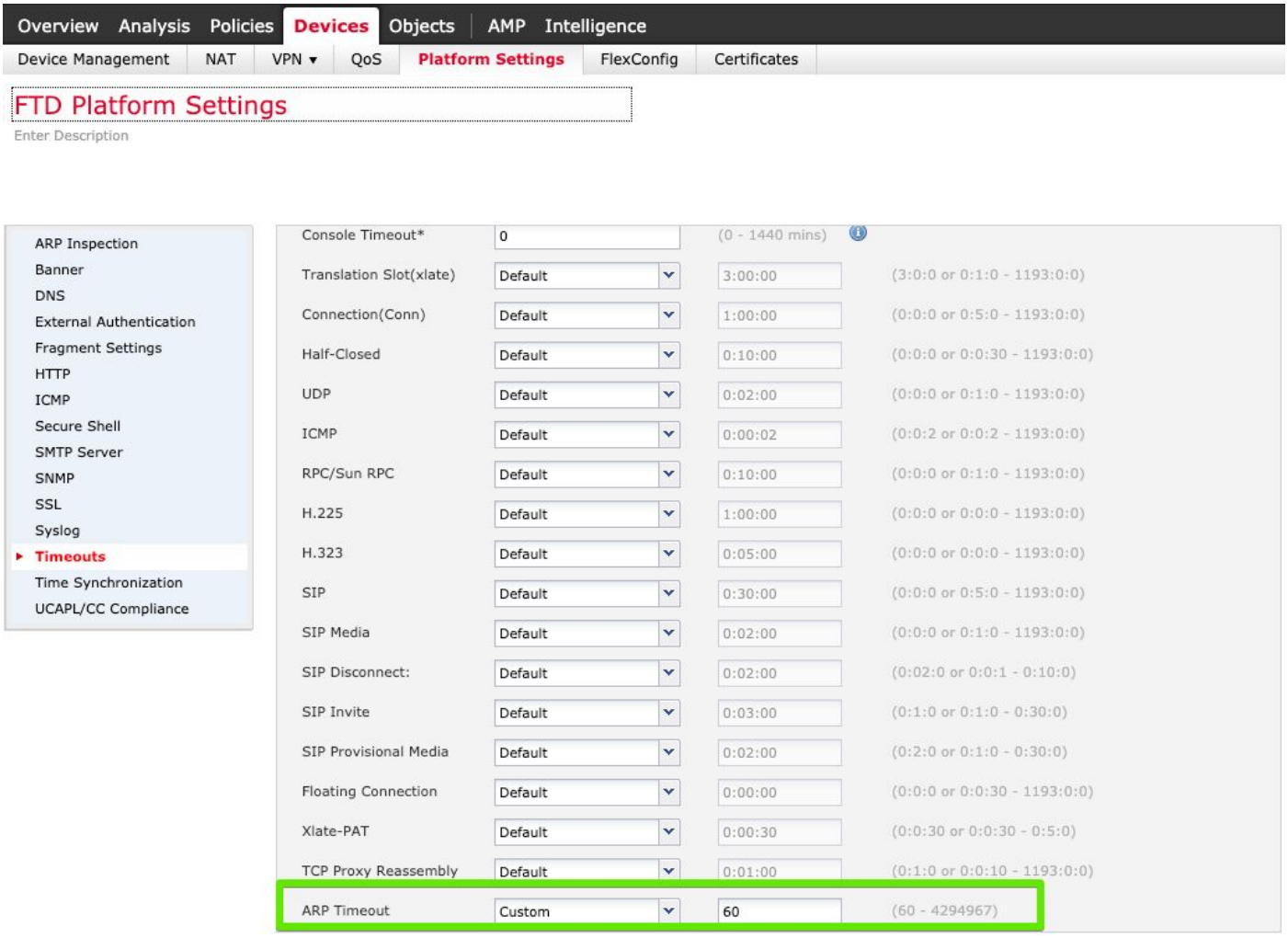
```
> show arp
Inside 10.20.20.3 0000.0c9f.f014 1
>show arp
Inside 10.20.20.3 0000.0c9f.f014 2
>show arp
Inside 10.20.20.3 0000.0c9f.f014 3
>show arp
Inside 10.20.20.3 0000.0c9f.f014 4
```

タイマーが*n - 30の値に達した*場合、*n*はARP設定のタイムアウト（デフォルトは14400秒）で、ファイアウォールはエントリを更新するためのARP要求を送信します。有効なARP応答を受信すると、エントリが保持され、タイマーは0に戻ります。

この例では、ARPタイムアウトが60秒に短縮されています。

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

このタイムアウトは、図に示すように、FMCの[Devices] > [Platform Settings] > [Timeouts]タブで設定できます。



タイムアウトは60秒であるため、ARP要求は30秒(60 - 30 = 30)ごとに送信されます。

```
> 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
```

その後、ARPエントリは30秒ごとに更新されます。

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

トラブルシュートのヒント

トラフィック方向

TFWで追跡する最も困難な事項の1つは、トラフィックフローの方向です。トラフィックフロー

が、ファイアウォールが宛先にパケットを正しく転送していることを確認する方法を理解する。

発信元と宛先のMACアドレスの変更やTime-To-Live（TTL；存続可能時間）値の削減など、ファイアウォールの関与を示す複数のインジケータが存在するため、正しい入力インターフェイスと出力インターフェイスを決定することは、ルーテッドモードでの作業です。

これらの違いは、TFWセットアップでは利用できません。入力インターフェイスを通過するパケットは、ほとんどの場合、ファイアウォールを離れる場合と同じように見えます。

ネットワーク内のMACフラップやトラフィックループなどの特定の問題は、パケットが入力された場所やファイアウォールから出たタイミングを知らなくても、追跡が困難になる可能性があります。

入力パケットと出力パケットを区別するために、パケットキャプチャでtraceキーワードを使用できます。

```
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：キャプチャバッファをバイト単位で増やします。33554432が使用可能な最大値です。5500-X、Firepowerアプライアンス、または仮想マシンなどのモデルでは、すでに設定されているキャプチャ数が少ない限り、このサイズ値を使用しても安全です。

trace：指定したキャプチャのトレースオプションを有効にします。

trace-count：より多くのトレースを許可します。1000が最大許容され、128がデフォルトです。これは、バッファサイズオプションと同じ推奨事項に従っても安全です。

> **ヒント**：オプションの1つを追加し忘れた場合は、キャプチャ名とオプションを参照してキャプチャ全体を再度書き込まなくても追加できます。ただし、新しいオプションは新しくキャプチャされたパケットにのみ影響を与えるため、パケット番号1以降の新しい効果を得るには、clear capture capnameを使用する必要があります。例：**トレースでのキャプチャ**

パケットがキャプチャされると、**show capture *cap_name trace***コマンドは、入力されたパケットの最初の1000（トレース番号が増加している場合）トレースを表示します。

```
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
```

次の出力は、外部インターフェイスのパケットキャプチャトレースの例です。これは、パケット番号1と3が外部インターフェイスに入り、パケット番号2がインターフェイスに出たことを意味します。

このトレースには、そのパケットに対して実行されたアクションや、パケットがドロップされた場合のドロップの理由などの追加情報があります。

より長いトレースや、1つのパケットに焦点を当てる場合は、**show capture *cap_name* trace packet-number *packet*_number**コマンドを使用して、その特定のパケットのトレースを表示できます。

これは、許可されたパケット番号10の例です。

```
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トラッキング

TFWはMACアドレスに基づいてすべての転送を決定します。トラフィックフロー分析では、各パケットの送信元および宛先として使用されるMACアドレスがネットワークトポロジに基づいて正しいことを確認することが不可欠です。

パケットキャプチャ機能を使用すると、**show capture**コマンドの***detail***オプションを使用して使用***するMACア***ドレスを表示できます。

```
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)
```

特定のトラッキングが必要な対象MACアドレスを見つけたら、キャプチャフィルタを使用して一致させることができます。

```
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)
```

このフィルタは、MACフラップのトレースがあり、原因を特定する場合に非常に便利です。

Mac-address-tableのデバッグ

MACアドレステーブルのデバッグを有効にして、各フェーズを確認できます。このデバッグで提供される情報は、MACアドレスがテーブルから学習、更新、および削除されるタイミングを理解するのに役立ちます。

このセクションでは、各フェーズの例とこの情報の読み方を示します。FTDでdebugコマンドを有効にするには、診断CLIにアクセスする必要があります。

> **警告**：ネットワークがビジー状態の場合、デバッグは関連リソースを消費する可能性があります。制御された環境または低ピーク時間帯に使用することを推奨します。これらのデバッグが冗長すぎる場合は、syslogサーバにこれらのデバッグを送信することを推奨します。

```
> 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
```

ステップ1:MACアドレスが学習されます。MACテーブルにエントリが見つからない場合、このアドレスがテーブルに追加されます。デバッグメッセージは、アドレスと、それが受信されたインターフェイスに通知します。

```
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.
!!!!
```

MACがICMP方式で学習されると、次のメッセージが表示されます。エントリは、MACアドレステーブル経過時間タイマーにリストされている条件に基づいてタイマーを更新しない、タイムアウトサイクルの最初の段階に入ります。

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

ステップ2：エントリが既に認識されている場合、デバッグはそのエントリについて通知します。このデバッグでは、スタンドアロンまたはHAの設定に関係のないクラスタリングメッセージも表示されます。

```
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
```

ステップ3：エントリが2番目のステージに達したら（絶対タイムアウトの2分前）。

```
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
```

ステップ4：ファイアウォールは、そのアドレスを送信元とする新しいパケットがテーブルを更新することを想定するようになりました。この2分間に、その エントリを使用するパケットがこれ以上存在しない場合、アドレスは削除されます。

```
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.
```

関連情報

- Firepower Management Centerガイドバージョン6.3 – 第3章：Firepower Threat Defenseのトランスペアレントまたはルーテッドファイアウォールモード
- テクニカル サポートとドキュメント – Cisco Systems