FirePOWER Threat Defense Transparenter Firewall-Modus Erweiterte Konzepte und Tipps zur Fehlerbehebung

Inhalt

Einführung

In diesem Dokument wird eine detaillierte Erläuterung der Kernkonzepte und -elemente einer FirePOWER Threat Defense (FTD)-Bereitstellung im TFW-Modus (Transparent Firewall) beschrieben. Dieser Artikel enthält außerdem nützliche Tools und exemplarische Vorgehensweisen für die häufigsten Probleme im Zusammenhang mit der transparenten Firewall-Architektur.

Verfasst von Cesar Lopez und herausgegeben von Yeraldin Sánchez, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Informationen zum transparenten Firewall-Modus von Cisco FTD
- Hot Standby Router Protocol (HSRP)-Konzepte
- Address Resolution Protocol (ARP)- und Internet Control Message Protocol (ICMP)-Protokolle

Es wird dringend empfohlen, den Abschnitt "FirePOWER Configuration Guide Transparent and Routed Firewall Mode" zu lesen, um die in diesem Dokument beschriebenen Konzepte besser zu verstehen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Erweiterte Konzepte für transparente Firewall

MAC-Adresstabelle

Während eine Firewall im Routing-Modus die Routing-Tabelle und die ARP-Tabelle verwendet, um die Ausgangsschnittstelle und die erforderlichen Daten für die Weiterleitung eines Pakets an den nächsten Hop zu bestimmen, verwendet der TFW-Modus die MAC-Adresstabelle, um die Ausgangsschnittstelle zu bestimmen, die zum Senden eines Pakets an sein Ziel verwendet wird. Die Firewall überprüft das Ziel-MAC-Adressfeld des verarbeiteten Pakets und sucht nach einem Eintrag, der diese Adresse mit einer Schnittstelle verknüpft.

Die MAC-Adresstabelle enthält diese Felder.

```
> 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
```

- Schnittstelle - Dieses Feld enthält den Schnittstellennamen, von dem aus diese MAC-Adresse dynamisch abgerufen oder statisch konfiguriert wurde.
- MAC-Adresse - MAC-Adresseintrag zum Speichern
- type - Methode zum Lernen des Eintrags. Sie kann dynamisch oder statisch sein.
- Age(min) - Timer für dekrementelle Meldungen in Minuten, der die Zeit anzeigt, die noch verbleibt, bevor der Eintrag als "Dead" (Deaktiviert) markiert wird. Dieser Timer gilt nur für dynamisch zu lernende Einträge
- bridge-Group - Bridge-Gruppen-ID, zu der die Schnittstelle gehört

Die Entscheidung für die Paketweiterleitung ist ähnlich wie bei einem Switch, es besteht jedoch

ein sehr wichtiger Unterschied, wenn es um einen fehlenden Eintrag in der MAC-Tabelle geht. In einem Switch wird das Paket über alle Schnittstellen übertragen, mit Ausnahme der Eingangs-Schnittstelle, aber in TFW. Wenn ein Paket empfangen wird und es keinen Eintrag für die MAC-Zieladresse gibt, wird das Paket verworfen. Er wird mit dem Accelerated Security Path (ASP)-Dropdowncode *dst-l2_lookup-fail* verworfen.

```
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
```

Diese Bedingung gilt immer für das erste Paket in einer Umgebung mit aktiviertem dynamischem Lernen und ohne statische Einträge für ein Ziel, wenn die MAC-Adresse zuvor in einem Paket nicht als Quell-MAC-Adresse erkannt wurde.

Sobald der Eintrag der MAC-Adresstabelle hinzugefügt wurde, kann das nächste Paket mit den aktivierten Firewall-Funktionen konditioniert werden.

```
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
```

> **Vorsicht**: Die MAC-Suche ist die erste Phase der von der Firewall durchgeführten Aktionen. Wenn aufgrund von fehlgeschlagenen L2-Suchläufen konstante Verwerfungen auftreten, kann dies zu Paketverlusten und/oder einer unvollständigen Überprüfung der Erkennungs-Engine führen. Die Beeinträchtigung beruht auf der Protokoll- oder Anwendungsfunktion für die erneute Übertragung.

Auf der Grundlage der oben angeführten Informationen ist es immer vorzuziehen, vor einer Übertragung einen Eintrag zu erlernen. Die TFW verfügt über mehrere Mechanismen, um einen Eintrag zu erlernen.

Lernoptionen für MAC-Adresstabelle

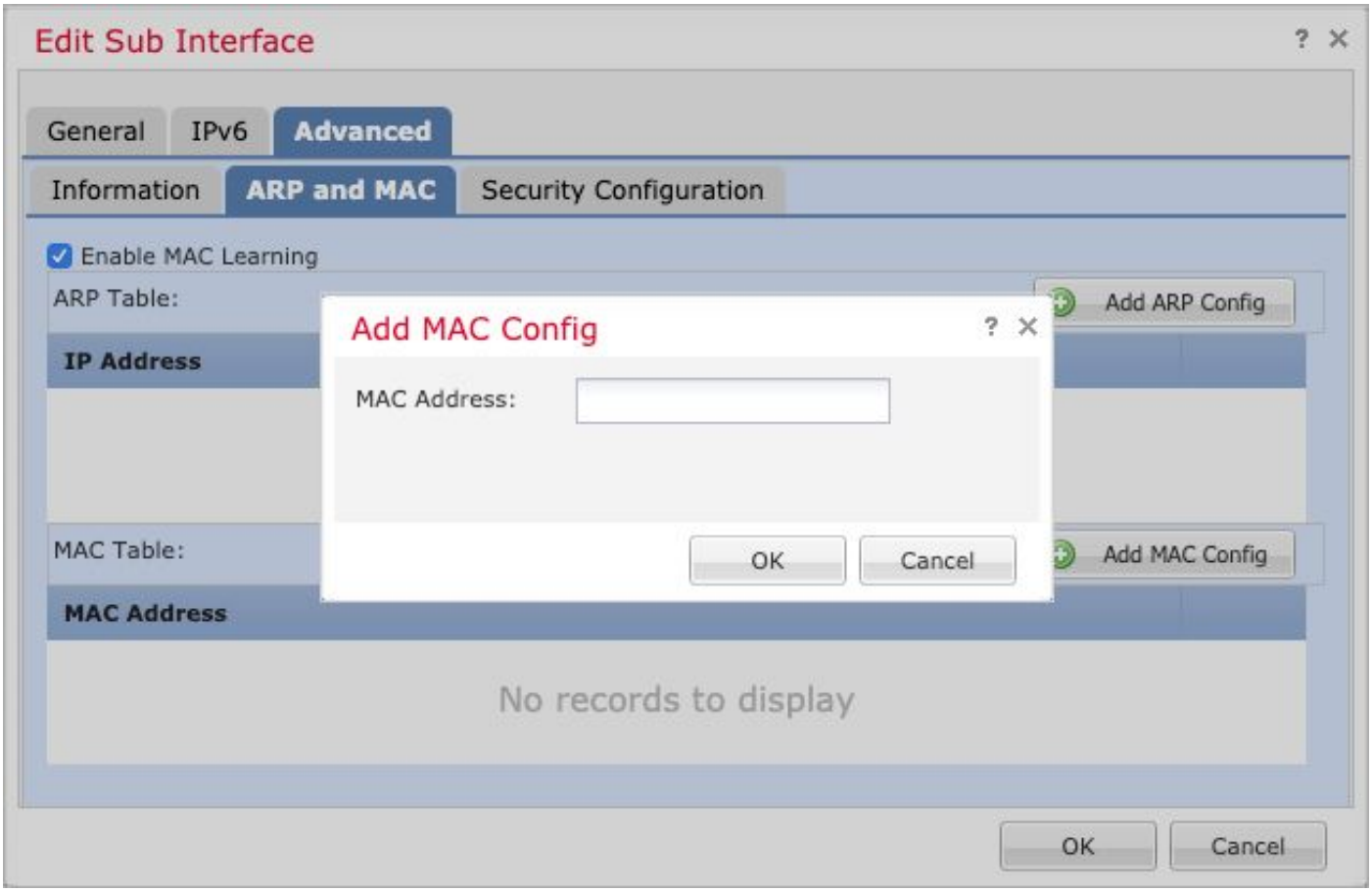
Statische Einträge

MAC-Adressen können manuell hinzugefügt werden, damit die Firewall immer dieselbe Schnittstelle für den jeweiligen Eintrag verwendet. Dies ist eine gültige Option für Einträge, die nicht geändert werden können. Dies ist eine gängige Option, wenn die statische MAC-Adresse auf

Konfigurationsebene oder durch eine Funktion im nächsten Hop überschrieben wird.

Beispiel: In einem Szenario, in dem die MAC-Adresse des Standardgateways auf einem Cisco Router immer die gleiche ist wie die, die der Konfiguration manuell hinzugefügt wurde, oder wenn die virtuelle HSRP-MAC-Adresse die gleiche bleibt.

Um statische Einträge in von FMC verwalteten FTD zu konfigurieren, können Sie auf **Edit Interface/Subinterface > Advanced > ARP and MAC** klicken und auf **Add MAC Config** klicken. Damit wird ein Eintrag für die spezifische Schnittstelle hinzugefügt, die im Abschnitt **Geräte > Geräteverwaltung > Schnittstellen** bearbeitet wird.



Dynamisches Lernen basierend auf Quell-MAC-Adresse

Diese Methode ähnelt der Vorgehensweise eines Switches zum Ausfüllen der MAC-Adresstabelle. Wenn ein Paket über eine Quell-MAC-Adresse verfügt, die nicht Teil der Einträge in der MAC-Tabelle für die Schnittstelle ist, die es empfangen wurde, wird der Tabelle ein neuer Eintrag hinzugefügt.

Dynamisches Lernen basierend auf ARP-Probe

Wenn ein Paket mit einer MAC-Zieladresse eingeht, die nicht Teil der MAC-Tabelle ist und die Ziel-IP Teil desselben Netzwerks ist wie die Bridge Virtual Interface (BVI), versucht die TFW zu erfahren, wie sie eine ARP-Anfrage über alle Bridge Virtual Interface (BVI) sendet. Wenn eine ARP-Antwort von einer der Bridge-Gruppen-Schnittstellen empfangen wird, wird sie der MAC-Tabelle hinzugefügt. Beachten Sie, dass, wie oben erwähnt, alle Pakete mit dem ASP-Code *dst-l2_lookup-fail* verworfen werden, obwohl keine Antwort auf diese ARP-Anforderung vorliegt.

Dynamisches Lernen basierend auf der ICMP-Probe

Wenn ein Paket mit einer MAC-Zieladresse eingeht, die nicht Teil der MAC-Tabelle ist und die Ziel-IP NICHT Teil desselben Netzwerks wie die BVI ist, wird eine ICMP-Echoanfrage mit einem TTL-Wert (Time-to-Live) gleich 1 gesendet. Die Firewall erwartet, dass eine ICMP Time Overceeded-Nachricht die Next-Hop-MAC-Adresse ermittelt.

Zeitgeber der MAC-Adresstabelle

Der Zeitgeber für die MAC-Adresstabelle "Alter" wird für jeden gelernten Eintrag auf 5 Minuten festgelegt. Dieser Timeoutwert umfasst zwei verschiedene Phasen.

Zeitüberschreitung im ersten Stadium

In den ersten drei Minuten wird der Wert für das MAC-Einstiegsalter erst aktualisiert, wenn ein ARP-Antwortpaket, das die Firewall mit der Quell-MAC-Adresse durchläuft, einem Eintrag in der MAC-Adresstabelle entspricht. Diese Bedingung schließt die ARP-Antworten aus, die für die IP-Adressen der Bridge-Gruppe bestimmt sind. Das bedeutet, dass alle anderen Pakete, die keine durchgehende ARP-Antwort sind, in den ersten 3 Minuten ignoriert werden.

In diesem Beispiel gibt es einen PC mit der IP-Adresse 10.10.10.5, der einen Ping an 10.20.20.5 sendet. Die Gateway-IP-Adresse für 10.20.20.5 lautet 10.20.20.3 mit der MAC-Adresse 0000.0c9f.f014.

Der Ziel-PC erstellt alle 25 Sekunden ein ARP-Update, wodurch konstante ARP-Pakete die Firewall passieren.

```
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
```

Diese Pakete werden mithilfe von ARP-Paketen mit Paketerfassungsfilterung abgeglichen.

```
> 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
```

Der Eintrag für 000.0c9f.4014 bleibt bei 5 und fällt nie unter diese Zahl.

```
> 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
```

Zeitüberschreitung in zweiter Phase

In den letzten 2 Minuten fällt der Eingang in einen Zeitraum, in dem die Adresse als veraltet gilt.

```
> 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
```

Der Eintrag wird noch nicht entfernt, und wenn ein Paket mit der Quell-MAC-Adresse, die mit dem Tabelleneintrag übereinstimmt, einschließlich der zu-dem-Paket-Pakete, erkannt wird, wird der Eintrag Alter auf 5 Minuten zurückgesetzt.

In diesem Beispiel wird innerhalb von 2 Minuten ein Ping gesendet, um die Firewall dazu zu zwingen, ihr eigenes ARP-Paket zu senden.

```
> 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
```

Der MAC-Adresseintrag wird auf 5 Minuten zurückgesetzt.

```
> 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-Tabelle

Zunächst ist es wichtig zu verstehen, dass die MAC-Adresstabelle völlig unabhängig von der ARP-Tabelle ist. Während die von der Firewall zur Aktualisierung eines ARP-Eintrags gesendeten ARP-Pakete gleichzeitig die MAC-Adresstabelle aktualisieren können, handelt es sich bei diesen Aktualisierungsvorgängen um eine separate Aufgabe, für die jeweils eigene Zeitüberschreitungen

und Bedingungen gelten.

Auch wenn die ARP-Tabelle nicht verwendet wird, um den Ausgangs-Next-Hop wie im Routing-Modus zu bestimmen, ist es wichtig, die Auswirkungen der generierten und für die Firewall-Identitäts-IPs bestimmten ARP-Pakete in einer transparenten Bereitstellung zu verstehen.

Die ARP-Einträge werden zu Verwaltungszwecken verwendet und der Tabelle nur hinzugefügt, wenn eine Verwaltungsfunktion oder -aufgabe dies erfordert. Wenn eine Bridge-Gruppe beispielsweise über eine IP-Adresse verfügt, kann diese IP zum Pingen des Ziels verwendet werden.

```
> 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
```

Befindet sich das Ziel im gleichen Subnetz wie die Bridge Group IP, wird eine ARP-Anfrage erzwungen, und wird eine gültige ARP-Antwort empfangen, wird der IP/MAC-Eintrag in der ARP-Tabelle gespeichert.

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

Anders als bei der MAC-Adresstabelle ist der Timer für das Schnittstellentriplet/die IP-Adresse/MAC-Adresse ein wachsender Wert.

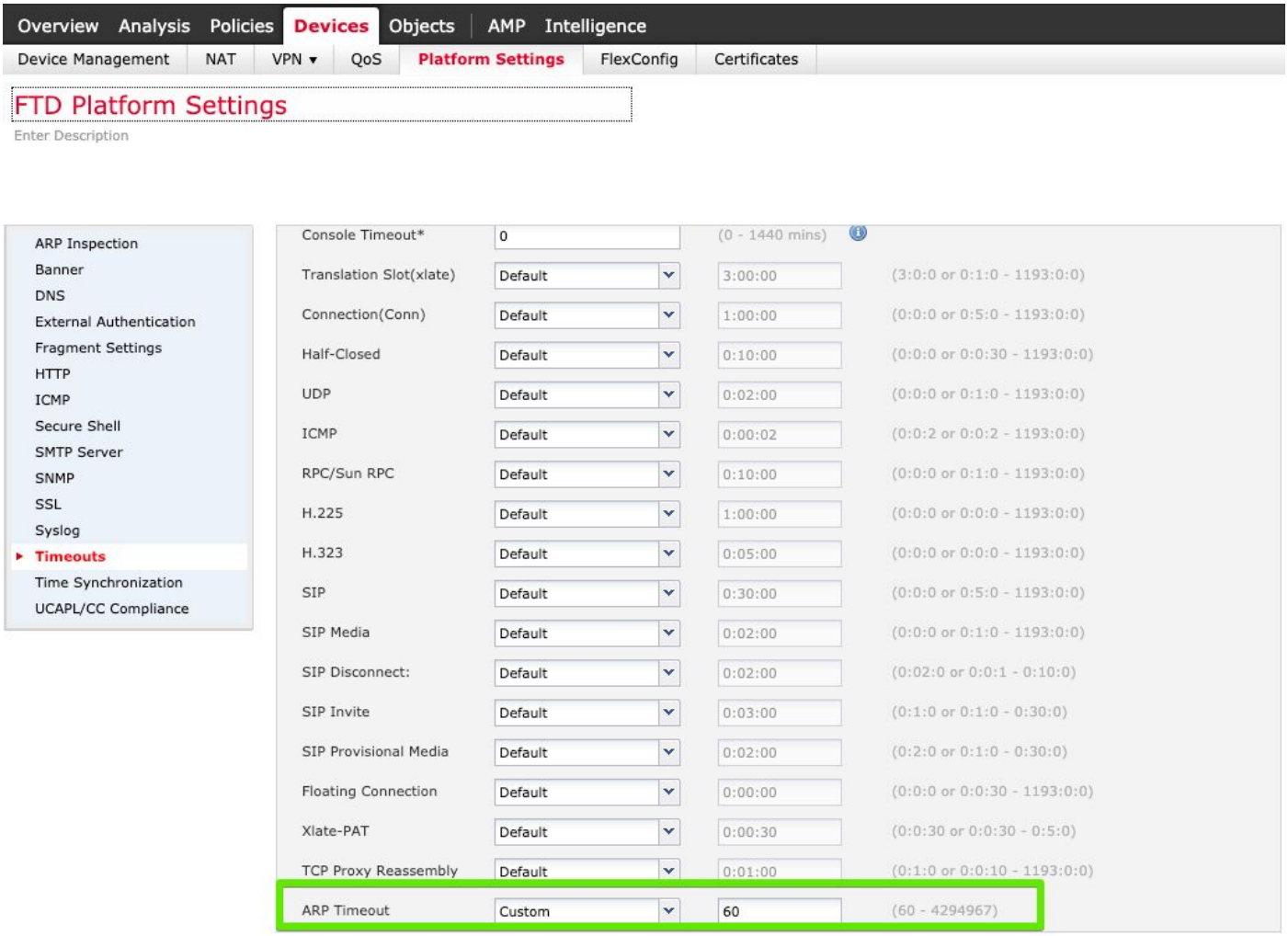
```
> show arp
Inside 10.20.20.3 0000.0c9f.f014 1
>show arp
Inside 10.20.20.3 0000.0c9f.f014 2
>show arp
Inside 10.20.20.3 0000.0c9f.f014 3
>show arp
Inside 10.20.20.3 0000.0c9f.f014 4
```

Wenn der Timer einen *n - 30*-Wert erreicht, wobei *n* der für den ARP konfigurierte Timeout ist (mit einem Standardwert von 14400 Sekunden), sendet die Firewall eine ARP-Anforderung, um den Eintrag zu aktualisieren. Wenn eine gültige ARP-Antwort eingeht, wird der Eintrag gehalten, und der Timer kehrt auf 0 zurück.

In diesem Beispiel wurde das ARP-Timeout auf 60 Sekunden reduziert.

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

Dieses Timeout kann auf der Registerkarte **Devices (Geräte) > Platform Settings (Plattformeinstellungen) > Timeouts (Zeitüberschreitungen)** im FMC konfiguriert werden, wie im Bild gezeigt.



Da das Timeout 60 Sekunden beträgt, wird alle 30 Sekunden eine ARP-Anfrage gesendet (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
```

Der ARP-Eintrag wird dann alle 30 Sekunden aktualisiert.

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

Tipps zur Fehlerbehebung

Richtung des Datenverkehrs

Eine der schwierigsten Aufgaben bei der Verfolgung einer TFW ist die Richtung des Datenverkehrsflusses. Wenn Sie wissen, wie der Datenverkehr fließt, kann die Firewall sicherstellen, dass die Pakete ordnungsgemäß an das Ziel weitergeleitet werden.

Die Auswahl der richtigen Eingangs- und Ausgangsschnittstelle ist im Routed-Modus einfacher, da es mehrere Indikatoren für die Beteiligung der Firewall gibt, z. B. die Änderung der Quell- und Ziel-MAC-Adressen und die Reduzierung des TTL-Werts (Time-To-Live) von einer Schnittstelle zur anderen.

Diese Unterschiede sind in einem TFW-Setup nicht verfügbar. Das Paket, das über die Eingangs-Schnittstelle eingeht, sieht in den meisten Fällen aus, als ob es die Firewall verlässt.

Bestimmte Probleme, wie MAC-Flaps im Netzwerk oder Datenverkehrsschleifen, lassen sich nur schwer nachverfolgen, ohne zu wissen, wo das eingegebene Paket eingeht und wann es die Firewall verlassen hat.

Um die Unterscheidung zwischen Eingangs- und Ausgangspaketen zu erleichtern, kann das trace-Schlüsselwort in der Paketerfassung verwendet werden.

```
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 - Erhöht den Capture-Puffer in Byte. Der maximal verfügbare Wert ist 33554432. Bei Modellen wie 5500-X, FirePOWER Appliances oder virtuellen Systemen ist es sicher, diesen Größenwert zu verwenden, solange noch keine Dutzende von Captures konfiguriert sind.

trace: Aktiviert die Ablaufverfolgungsoption für die angegebene erfasste Ablaufverfolgungsoption.

trace-count: Ermöglicht eine höhere Anzahl von Traces. 1000 ist der maximal zulässige Wert, 128 ist der Standardwert. Dies ist auch sicher, wenn Sie dieselbe Empfehlung für die Option Puffergröße befolgen.

> **Tipp**: Wenn Sie eine der Optionen vergessen, können Sie sie hinzufügen, ohne die gesamte Erfassung erneut schreiben zu müssen, indem Sie auf den Namen der Erfassung und die Option verweisen. Die neue Option betrifft jedoch nur die neu erfassten Pakete. Daher muss ein **klarer *Erfassungsname*** verwendet werden, um die neue Wirkung seit Paket-Nummer 1 zu erzielen. Beispiel: **Erfassung in Spur**

Nach der Paketerfassung zeigt der Befehl **show capture *cap_name* trace** die ersten 1000 (wenn die Trace-Nummer erhöht wurde) Traces der empfangenen Pakete an.

```
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
```

Diese Ausgabe ist ein Beispiel für die externen Schnittstellen-Paketerfassungsspuren. Dies bedeutet, dass die Paketnummern 1 und 3 die externe Schnittstelle eingaben und die

Paketnummer 2 die Schnittstelle ausweitete.

Weitere Informationen finden Sie in dieser Spur, z. B. die für dieses Paket getroffene Aktion und der Drop-GRÜNDE, falls das Paket verworfen wird.

Für längere Ablaufverfolgungen und wenn Sie sich auf ein einzelnes Paket konzentrieren möchten, kann der Befehl **show capture** *cap_name* **trace packet-number** *paket_*numberverwendet werden, um die Ablaufverfolgung für dieses spezifische Paket anzuzeigen.

Dies ist ein Beispiel für eine zulässige Paketnummer 10.

```
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-Verfolgung

Die TFW trifft alle ihre Weiterleitungsentscheidungen auf der Grundlage von MAC-Adressen. Bei der Analyse des Datenverkehrsflusses muss unbedingt sichergestellt werden, dass die für jedes Paket als Quelle und Ziel verwendeten MAC-Adressen auf Basis der Netzwerktopologie korrekt sind.

Mit der Paketerfassungsfunktion können Sie die verwendeten MAC-Adressen mithilfe der ***Detail-*** Option im Befehl **show capture** anzeigen.

```
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)
```

Sobald Sie eine interessante MAC-Adresse gefunden haben, die eine spezifische Nachverfolgung erfordert, können Sie diese mithilfe der Erfassungsfilter abgleichen.

```
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)
```

Dieser Filter ist äußerst nützlich, wenn es Spuren von MAC-Flaps gibt und Sie die Schuldigen finden möchten.

Debuggen der MAC-Adresstabelle

Das Debuggen von MAC-Adresstabellen kann aktiviert werden, um jede Phase zu überprüfen. Die Informationen, die von diesem Debuggen bereitgestellt werden, helfen zu verstehen, wann eine MAC-Adresse erlernt, aktualisiert und aus der Tabelle entfernt wird.

Dieser Abschnitt zeigt Beispiele für jede Phase und wie diese Informationen gelesen werden. Um Debug-Befehle in FTD zu aktivieren, müssen Sie auf die Diagnose-CLI zugreifen.

> **Warnung**: Debugger können relevante Ressourcen verwenden, wenn das Netzwerk zu ausgelastet ist. Es wird empfohlen, diese in kontrollierten Umgebungen oder zu Zeiten geringer Spitzenzeiten zu verwenden. Es wird empfohlen, diese Debugger an einen Syslog-Server zu senden, wenn diese zu ausführlich sind.

```
> 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
```

Schritt 1: Die MAC-Adresse wird abgerufen. Wenn in der MAC-Tabelle noch kein Eintrag gefunden wurde, wird diese Adresse der Tabelle hinzugefügt. Die Debug-Meldung informiert die Adresse und die Schnittstelle, an der sie empfangen wurde.

```
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.
!!!!
```

Wenn die MAC-Adresse über die ICMP-Methode abgerufen wird, wird die nächste Meldung angezeigt. Der Eintrag tritt in die erste Phase des Timeout-Zyklus ein, in der er seinen Timer nicht entsprechend den Bedingungen aktualisiert, die im Age Timer der MAC-Adresstabelle angegeben sind.

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

Schritt 2: Wenn ein Eintrag bereits bekannt ist, informiert das Debuggen darüber. Beim Debuggen werden auch Clustering-Meldungen angezeigt, die in Standalone- oder HA-Konfigurationen irrelevant sind.

```
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
```

Schritt 3: Sobald der Eintrag die zweite Stufe erreicht hat (2 Minuten vor dem absoluten Timeout).

```
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
```

Schritt 4: Die Firewall geht nun davon aus, dass neue Pakete mit dieser Adresse die Tabelle aktualisieren. Wenn dieser Eintrag in diesen 2 Minuten nicht mehr Pakete enthält, wird die Adresse entfernt.

```
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.
```

Zugehörige Informationen

- Leitfaden zum FirePOWER Management Center, Version 6.3 - Kapitel 3: Transparenter oder gerouteter Firewall-Modus zum Schutz vor Bedrohungen durch Firepower
- Technischer Support und Dokumentation - Cisco Systems