تلميحات أستكشاف المشكلات وإصلاحها في وضع جدار الحماية الشفاف الخاص ب Firepower Threat Defense

المحتويات

المقدمة

يوضح هذا المستند شرح مفصل لمفهوم المفاهيم والعناصر الأساسية من نشر برنامج الدفاع عن تهديد الطاقة النارية (FTD) في وضع جدار الحماية الشفاف (TFW). توفر هذه المقالة أيضا أدوات ومهارات مفيدة لمعظم المشاكل الشائعة المتعلقة ببنية جدار الحماية الشفافة.

ساهم به سيزار لوبيز وحرره ياريدين سانشيز، مهندس TAC من Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة وضع جدار الحماية الشفاف ل Cisco FTD

- مفاهيم بروتوكول الموجه الاحتياطي الفعال (HSRP)
- بروتوكولات بروتوكول تحليل العنوان (ARP) وبروتوكول رسائل التحكم في الإنترنت (ICMP)

يوصى بشدة بقراءة قسم وضع جدار الحماية الشفاف أو الموجه الخاص بدليل تكوين Firepower لفهم المفاهيم الموضحة في هذا المستند بشكل أفضل.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco Firepower 4120 FTD، الإصدار 6.3.0.4
- مركز إدارة Cisco Firepower (FMC)، الإصدار 6.3.0.4
- Cisco ASR1001 IOS-XE الإصدار 16.3.9
- Cisco Catalyst 3850 IOS-XE الإصدار 16.9.3

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المفاهيم المتقدمة لجدار الحماية الشفاف

جدول عناوين MAC

بينما يعتمد جدار حماية في الوضع الموجه على جدول التوجيه وجدول ARP لتحديد واجهة المخرج والبيانات الضرورية لإعادة توجيه حزمة إلى الخطوة التالية، يستخدم وضع TFW جدول عنوان MAC للتمكن من تحديد واجهة المخرج التي يتم إستخدامها لإرسال حزمة إلى الوجهة الخاصة بها. ينظر جدار الحماية في حقل عنوان MAC للوجهة للحزمة التي يتم معالجتها ويبحث عن إدخال يربط هذا العنوان بواجهة.

يحتوي جدول عنوان MAC على هذه الحقول.

```
> 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
```

- الواجهة - يحمل هذا الحقل اسم الواجهة من حيث تم التعرف على عنوان MAC هذا ديناميكيا أو تم تكوينه بشكل ثابت
- عنوان MAC - سجل عنوان MAC المراد تخزينه
- النوع - الطريقة المستخدمة لتعلم الإدخال. يمكن أن يكون ديناميكيا أو ساكنا
- العمر(الحد الأدنى) - يتم وضع علامة "ميت" على المؤقت المؤقت المؤقت المؤقت المؤقت المؤقت في الدقائق التي تعرض الوقت المتبقي قبل هذا الإدخال. ينطبق هذا المؤقت على إدخالات التعلم الديناميكي فقط
- مجموعة الجسر - معرف مجموعة الجسر الذي تنتمي إليه الواجهة

يكون قرار إعادة توجيه الحزمة مماثل لمحول ما ولكن هناك أختلاف مهم جدا عندما يتعلق الأمر بإدخال مفقود في جدول MAC. في مفتاح، بثت الربط من خلال كل إطار عادي المدخل إطار لكن في TFW، إذا إستلمت ربط وهناك ما من مدخل للغاية {upper}mac address، الربط سقطت. يتم التخلص منه مع رمز إسقاط مسار الأمان السريع (ASP) *dst-l2_lookup-fail*.

```
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
```

ةتباث تالاخدإ نودبو يكرح ملعت نيكمت عم ةئيب ىلع ىلوألا ةمزحلل ثدحي امئاد طرش اذه ةجولل اذإ مل يظهر عنوان MAC نم لبق يف طبر كمصدر {upper}mac address.

درجمب إضافة الإدخال إلى جدول عناوين MAC، يمكن السماح بتتبع الحزمة التالية مع ميزات جدار الحماية الممكنة.

```
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
```

> **تحذير**: Mac Lookup وه المرحلة الأولى في الإجراءات التي تم إتخاذها بواسطة جدار الحماية. من الممكن أن يؤدي وجود حالات إسقاط مستمرة بسبب عمليات بحث L2 الفاشلة إلى فقدان الحزمة ذات الصلة و/أو حفص محرك الكشف غير المتكامل. دمتعت هذه الميزة على البروتوكول أو قدرة التطبيق لإعادة الإرسال.

واستنادا إلى ام ركذ أعلاه، نم المفضل امئاد ةفرعم الدخول لبق أي عملية نقل. يحتوي TFW على آليات متعددة لتعلم إدخال ام.

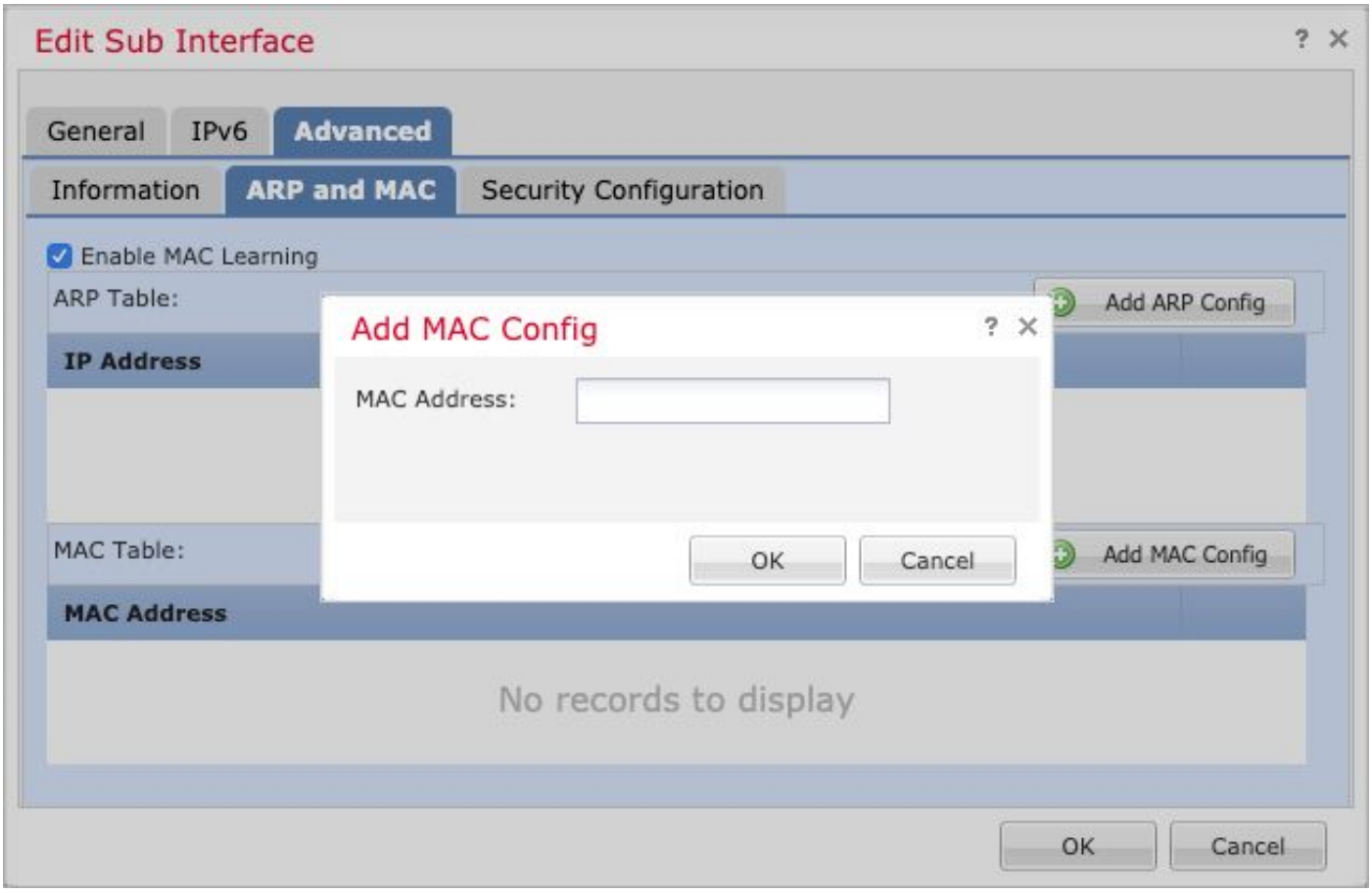
خيارات تعلم جدول عناوين MAC

ةتباث تالاخدإ

يمكن إضافة عناوين MAC يدويا لجعل جدار الحماية يستخدم امئاد سفن الواجهة لذلك الإدخال المحدد. اذه خيار صحيح للإدخالات غير القابلة للتغيير. اذه خيار شائع عندما تتم الكتابة فوق MAC ناكاس إستاتيكي على مستوى التكوين أو بواسطة ميزة في الخطوة التالية.

على سبيل المثال، في سيناريو حيث سيكون عنوان MAC للعبارة الافتراضية امئاد هي نفسها على موجه Cisco حيث تمت إضافته يدويا إلى التكوين أو إذا كان عنوان MAC الظاهري HSRP سيبقى هو نفسه.

in order to تكوين إدخالات ثابتة في FTD يدار ب FMC، أنت يستطيع طقطقت على **حرر قالب / subinterface>متقدم>ARP و MAC** وطقطقت على **إضافة ماك config**. يؤدي هذا إلى إضافة إدخال للواجهة المحددة التي يتم تحريرها من **الأجهزة > إدارة الأجهزة > قسم الواجهات**.



التعلم الديناميكي القائم على عنوان MAC للمصدر

هذا أسلوب مماثل لما يفعله مفتاح لمعلم جدول عنوان MAC. إذا كانت الحزمة تحتوي على عنوان MAC مصدر ليس جزءا من إدخالات جدول MAC للواجهة التي تم استقبالها، تتم إضافة إدخال جديد إلى الجدول.

التعلم الديناميكي القائم على تحقيق ARP

إن يصل ربط مع غاية {upper}mac address أن ليس جزء من ال mac طاولة والوجهة ip وه جزء من ال نفسه شبكة بما أن الجسر فعلي قارن (BVI)، ال TFW يحاول أن يتعلمه يرسل طلب ARP من خلال all the bridge-group قارن. إذا تم تلقي رد ARP من أي من واجهات مجموعة الجسر، فإنه تتم إضافته إلى جدول MAC. لاحظ أنه، كما تمت الإشارة إليه أعلاه، بينما ال يوجد رد على طلب ARP هذا، يتم إسقاط جميع الحزم باستخدام رمز ASP *dst-l2_lookup-fail*.

التعلم الديناميكي القائم على تحقيق ICMP

إذا وصلت الحزمة مع عنوان MAC للوجهة الذي ليس جزءا من جدول MAC والوجهة IP ليست جزءا من نفس الشبكة مثل BVI، يتم إرسال طلب صدى ICMP مع قيمة مدة البقاء (TTL) تساوي 1. يتوقع جدار الحماية رسالة تجاوز وقت بروتوكول ICMP للتعرف على عنوان MAC للخطوة التالية.

مؤقت عمر جدول عناوين MAC

تم تعيين مؤقت عمر جدول عناوين MAC على 5 دقائق لكل إدخال تم التعرف عليه. تحتوي قيمة المهلة هذه على مرحلتين مختلفتين.

المرحلة الأولى لانتهاء مهلة العمر

أثناء أول 3 دقائق، لا يتم تحديث قيمة سن إدخال MAC إلا إذا كانت حزمة الرد على ARP تمر عبر جدار الحماية باستخدام عنوان MAC المصدر تساوي إدخال في جدول عناوين MAC. هذا يعني أنه يستثني هذا الشرط ردود ARP الموجهة إلى عناوين IP الخاصة بمجموعة الجسر. وهذا يعني أن أي ردود ARP تسير داخل حزمة أخرى أي حزمة ARP تصل أثناء الدقائق الثلاث الأولى.

في هذا المثال، هناك كمبيوتر شخصي بعنوان IP 10.10.10.5 يرسل إختبار اتصال إلى 10.20.20.5. عنوان IP للعبارة ل 10.20.20.5 هو 10.20.20.3 مع عنوان MAC 0000.0c9f.f014.

يقوم كمبيوتر الوجهة بإنشاء تحديث ARP كل 25 ثانية مما يؤدي إلى انتقال حزم ARP من خلال جدار الحماية.

```
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
```

يتم إستخدام حزم التقاط تصفية حزم ARP بمطابقة هذه الحزم.

```
> 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
```

يبقى المدخل ل 000.0c9f.4014 عند 5 ولا يقل أبدا عن ذلك الرقم.

```
> 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
```

المرحلة الثانية لانتهاء مهلة العمر

خالل الدقيقتين الأخيرتين، يقع الإدخال في فترة زمنية تم فيها إعتبار العنوان قديما.

```
> 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
```

لم تتم إزالة الإدخال بعد وإذا تم الكشف عن أي حزمة ذات عنوان MAC للمصدر تطابق إدخال الجدول، بما في ذلك حزم إلى المربع، يتم تحديث إدخال العمر مرة أخرى لمدة 5 دقائق.

في هذا المثال، يتم إرسال إختبار اتصال في غضون دقيقتين لإجبار جدار الحماية على إرسال حزمة ARP الخاصة به.

```
> 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
```

تم تعيين إدخال عنوان MAC مرة أخرى إلى 5 دقائق.

```
> 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
```

جدول ARP

أوال، من الضروري أن نفهم أن جدول عناوين MAC مستقل تماما عن جدول ARP. بينما يمكن لحزم ARP التي تم إرسالها بواسطة جدار الحماية لتحديث إدخال ARP، تحديث جدول عناوين MAC في الوقت نفسه، فإن عمليات التحديث هذه هي مهام منفصلة ولكل منها مهامه وشروطه الخاصة.

حتى إذا لم يتم إستخدام جدول ARP لتحديد المرحلة التالية من المخرج كما هو الحال في حزم ARP التي تم إنشاؤها وتخصيصها إلى هوية جدار الوضع الموجه، فمن المهم فهم أثر حزم ARP التي يمكن أن تحتوي عليها عناوين IP في نشر شفاف.

يتم إستخدام إدخالات ARP أل غراض الإدارة ويتم إضافتها فقط إلى الجدول إذا كانت ميزة الإدارة أو المهمة تتطلب ذلك. على سبيل المثال، إذا كان لمجموعة جسر عنوان IP، يمكن إستخدام IP هذا الختبار اتصال الوجهة.

```
> 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
```

إذا كانت الوجهة في الشبكة الفرعية نفسها الخاصة ب Bridge Group IP، فإنها تفرض طلب ARP وإذا تم تلقي رد ARP صالح، يتم تخزين إدخال IP/MAC في جدول ARP.

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

بخلاف جدول عنوان MAC، فإن المؤقت المصاحب للواجهة/عنوان IP/عنوان MAC ثالثي قيمة متزايدة.

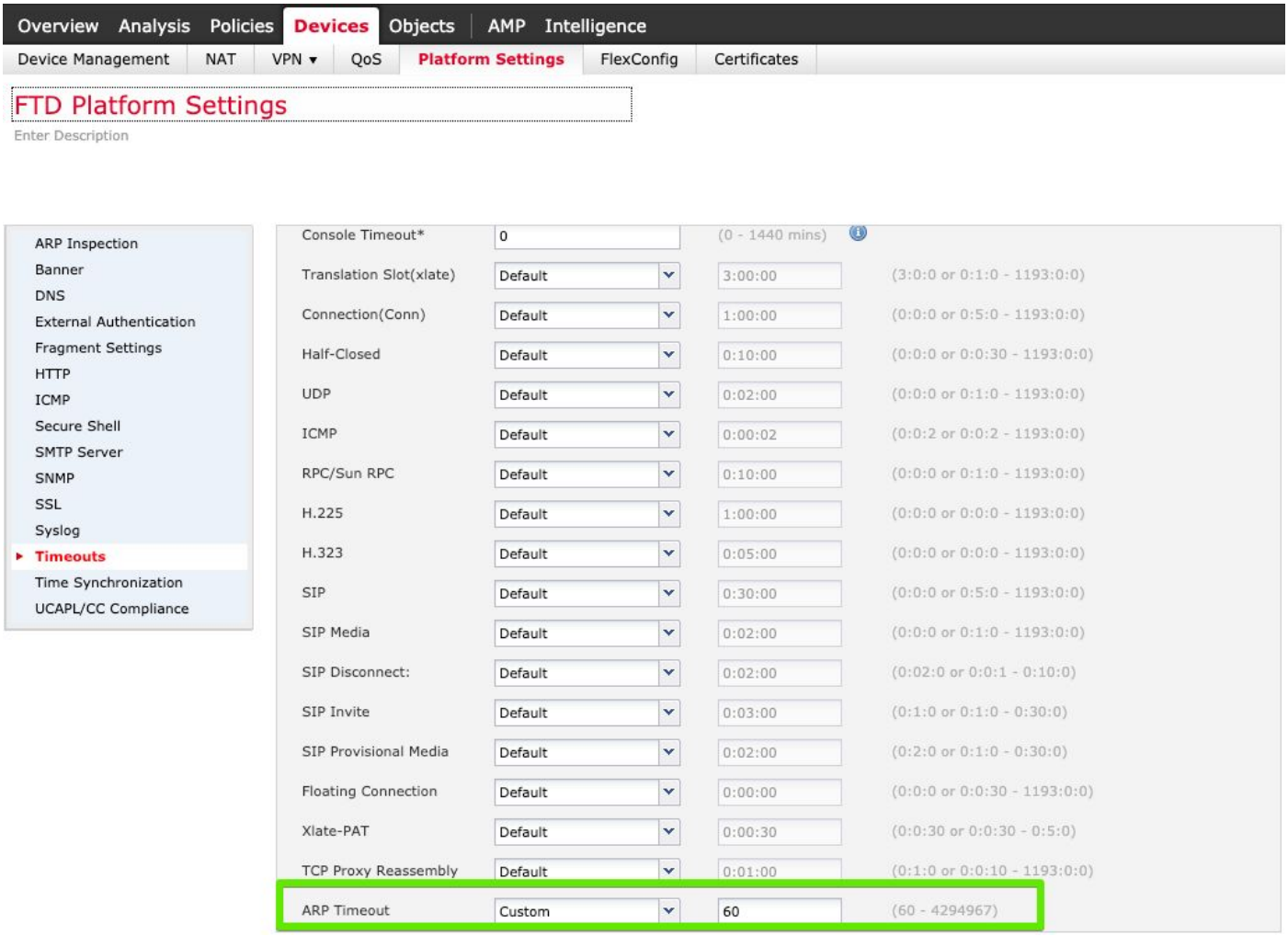
```
> show arp
Inside 10.20.20.3 0000.0c9f.f014 1
>show arp
Inside 10.20.20.3 0000.0c9f.f014 2
>show arp
Inside 10.20.20.3 0000.0c9f.f014 3
>show arp
Inside 10.20.20.3 0000.0c9f.f014 4
```

عندما يصل المؤقت إلى قيمة *N - 30* حيث *n* هي مهلة ARP التي تم تكوينها (مع إعداد افتراضي مدته 14400 ثانية)، يرسل جدار الحماية طلب ARP لتحديث الإدخال. إذا تم تلقي رد ARP صالح، يتم الاحتفاظ بالدخول ويعود المؤقت إلى 0.

في هذا المثال، تم تقليل مهلة ARP إلى 60 ثانية.

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

توفر هذه المهلة ليتم تكوينها في **الأجهزة > إعدادات النظام الأساسي > عام التوبيخ** في FMC، كما هو موضح في الصورة.



بما أن المهلة هي 60 ثانية، يتم إرسال طلب ARP كل 30 ثانية (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
```

يتم بعد ذلك تحديث إدخال ARP كل 30 ثانية.

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

تلميحات أستكشاف المشكلات وإصلاحها

إتجاه حركة المرور

أحد أصعب الأشياء لمتابعة مسار حركة مرور البيانات هو إتجاه تدفق حركة المرور. يفهم

كيف حرك ةكرم روري دعاسي تدفق أن يضمن جادر الحماية بشكل صحيح forwarding الربط إلى الغاية.

تارشؤم دوجول ارظن هجوملا عضولا ىلع لهسأ ةمهم ىنميلا جرخملاو لخدملا ةهجاو ديدحت دعي (MAC) طئاسولل لوصولا يف مكحتلا نيوانع ليدعت لثم ةيامحلا رادج ةكراشمل ةددعتم للرصملاو ةهجولاو ضفخو ةميق ةدم ءاقبلا (TTL) نم ةهجاو إلى أخرى.

ال رفوتت هذه الاختلافات على إعداد TFW. ودبت ةمزحلا ةدراولا نم لالخ ةهجاو لخدلا سفنب الشكل عندما تترك جادر الحماية في مظعم الحالات.

دق نوكي نم الصعب تعقب لكاشم ةنيعم لثم ةفرفر MAC يف الشبكة وأ تاقلح حرك ةكرم رورم البيانات دون معرفة ماكن إدخال ةمزحلا وقوت مغادرتها جادر الحماية.

للمساعدة في التمييز بين المدخل ومزح الخروج، يمكن إستخدام الكلمة الأساسية التتبع في التقاط المزح.

```
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
```

المخزن المؤقت - يزيد من مخزن الالتقاط المؤقت بالبايت. 33554432 وه الحد الأقصى للقيمة المتوفرة. في الطرز مثل 5500-X أو أجهزة FirePOWER أو الأجهزة الافتراضية، نم الآمن إستخدام قيمة الحجم هذه طالما لا توجد عشرات من عمليات الالتقاط التي تم تكوينها بالفعل.

التتبع - تمكين خيار التتبع للأسر المحدد.

عدد التتبع - يسمح بعدد أكبر من عمليات التتبع. 1000 وه الحد الأقصى المسموح به و 128 وه الافتراضي. ويكون هذا الخيار آمنا أيضا بعد التوصية نفسها الخاصة بخيار حجم المخزن المؤقت.

> **تلميح**: إذا نسيت إضافة أحد الخيارات، فيمكنك إضافته دون الاضطرار إلى كتابة الالتقاط بأكمله مرة أخرى بالإشارة إلى اسم الالتقاط والخيار. ومع ذلك، أي خيار جديد لا يؤثر إلا على الالتقاطات التي يتم تكوينها بعد ذلك الحين. ينبغي أن يحتوي الالتقاط على جعل الرقم 1 معنى **الالتقاطات في التتبع**. مثال: 1. رقم ربط منذ جديد التأثير تلقي

لعرض التقاط الحزم، يعرض الأمر **show capture *cap_name*** trace أول 1000 (إذا تم زيادة رقم التتبع) للحزم التي تم تجاوزها.

```
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
```

هذا الإخراج هو مثال على مسارات تتبع حزمة الواجهة الخارجية. هذا يعني أن رقم ربط 1 و 3 قد دخلت القارن الخارجي ورقم ربط 2 غادرت القارن.

يمكن العثور على معلومات إضافية في هذا التتبع مثل الإجراء المتخذ لتلك الحزمة وسبب إسقاط الحزمة في حالة الإسقاط.

لوطأ راثآل اذإو تنك تريد التركيز على حزمة واحدة، فإن الأمر **show capture** *cap_name* **trace packet-number** packet_number يمكنك استخدام عرض التتبع لتلك الحزمة المحددة.

اذه مثال على حزمة رقم 10 مسموح بها.

```
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
```

تعقب MAC

يقوم TFW باتخاذ جميع قرارات إعادة التوجيه الخاصة به استنادا إلى عناوين MAC. أثناء تحليل تدفق حركة المرور، من الضروري التأكد من صحة عناوين MAC المستخدمة كمصدر ووجهة على كل حزمة استنادا إلى مخطط الشبكة.

تتيح لك ميزة التقاط الحزمة عرض عناوين MAC المستخدمة باستخدام خيار ***التفاصيل*** من الأمر **show capture**.

```
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)
```

بمجرد أن تقوم بتحديد موقع عنوان MAC المثير للاهتمام الذي يتطلب تعقب معين، فإن مرشحات التقاط تتيح لك أن تطابق العنوان.

```
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)
```

يكون هذا المرشح مفيدا للغاية عندما يكون هناك آثار ولصالت MAC وتريد العثور على السبب (الأسباب).

تصحيح أخطاء جدول عناوين MAC

يمكن تمكين تصحيح أخطاء جدول عناوين MAC لمراجعة كل مرحلة. تساعد المعلومات المقدمة من تصحيح الأخطاء هذه على فهم متى يتم التعرف على عنوان MAC، وتحديثه، وإزالته من الجدول.

يوضح هذا القسم أمثلة على كل مرحلة وكيفية قراءة هذه المعلومات. لتمكين أوامر تصحيح الأخطاء على FTD، يجب عليك الوصول إلى CLI التشخيصي.

> **تحذير**: يمكن أن يستهلك تصحيح الأخطاء الموارد ذات الصلة إذا كانت الشبكة مشغولة للغاية. ومن المستحسن استخدامها في البيئات الخاضعة للتحكم أو خلال ساعات الذروة المنخفضة. من المستحسن إرسال هذه الأخطاء إلى خادم syslog إذا كانت هذه مفصلة جدا.

```
> 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
```

الخطوة 1. تم التعرف على عنوان MAC. عند عدم العثور على إدخال في جدول MAC بالفعل، تتم إضافة هذا العنوان إلى الجدول. تقوم رسالة تصحيح الأخطاء بإعلام العنوان والواجهة التي تم تلقيها فيها.

```
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.
!!!!
```

إذا تم التعرف على MAC من خلال طريقة ICMP، يتم عرض الرسالة التالية. يدخل الإدخال المرحلة الأولى من دورة المهلة حيث لا يقوم موقت بتحديث المؤقت الخاص به استنادا إلى الشروط المدرجة في مؤقت عمر جدول عناوين MAC.

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

الخطوة 2. إذا كان أحد الإدخالات معروفا بالفعل، فيعلم تصحيح الأخطاء عنه. يعرض تصحيح الأخطاء أيضا رسائل التجميع غير ذات الصلة بالمواقع المستقلة أو HA.

```
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
```

الخطوة 3. بمجرد وصول الإدخال إلى المرحلة الثانية (قبل دقيقتين من المهلة المطلقة).

```
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
```

الخطوة 4. يتوقع جدار الحماية الآن أن تقوم الحزم الجديدة التي تم الحصول عليها من هذه العنوان بتحديث الجدول. إذا لم يعد هناك حزم أخرى تستخدم هذا الإدخال خلال هاتين الدقيقتين، فسيتم إزالة العنوان.

```
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.
```

معلومات ذات صلة

- دليل مركز إدارة Firepower، الإصدار 6.3 - الفصل 3: وضع جدار الحماية الشفاف أو الموجه للدفاع عن تهديد الطاقة النارية
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).