أستكشاف أخطاء حركة مرور FMC وإصلاحها عند إنهاء TCP بعد إسقاط حزم ACK القديمة

المحتويات

مسألة

يوضح هذا المستند سبب تسجيل دخول FTD بأحداث قائمة التحكم في الوصول (ACL) التي إسقاط لحركة مرور البيانات العائدة من FMC إلى أنظمة العميل، وخاصة حزم ACK. عمليات الإسقاط هي نتاج حالة سباق من المستوى الثاني المصغر بين سلوك مكدس Windows TCP وإنشاء إتصالات TCP بالفعل بواسطة حزم RST من العميل. تصل بعد إنهاء إتصالات TCP. لا يحدث أي تأثير على الخدمة، ولا يلزم إجراء أي إصلاح. ACK المتوافق مع FMCs RFC 793.

ملاحظة: هذا هو السلوك المتوقع. تكون أحداث قائمة التحكم في الوصول في الإسقاط في أنظمة المراقبة بمجرد تأكيد هذا النمط آمنة للتصفية في أنظمة المراقبة.

الأعراض:

- تظهر سجلات جدار حماية FTD أحداث إسقاط قائمة التحكم في الوصول (ACL) لحركة المرور العائدة من FMC إلى أنظمة العميل (JumpHost في هذا المثال)
- تحدث حالات السقوط على إتصالات منفذ TCP رقم 443 (HTTPS) بين FMC وأنظمة العميل
- تظهر الأحداث في FMC Unified Events كحزم محظورة
- أكواد أسباب الإسقاط التي تم رؤيتها في عمليات الالتقاط: tcp-rstfin-ooo، tcp-not-syn، acl-drop
- لا يلاحظ أي تأثير على الخدمة على الرغم من عمليات السقوط المسجلة

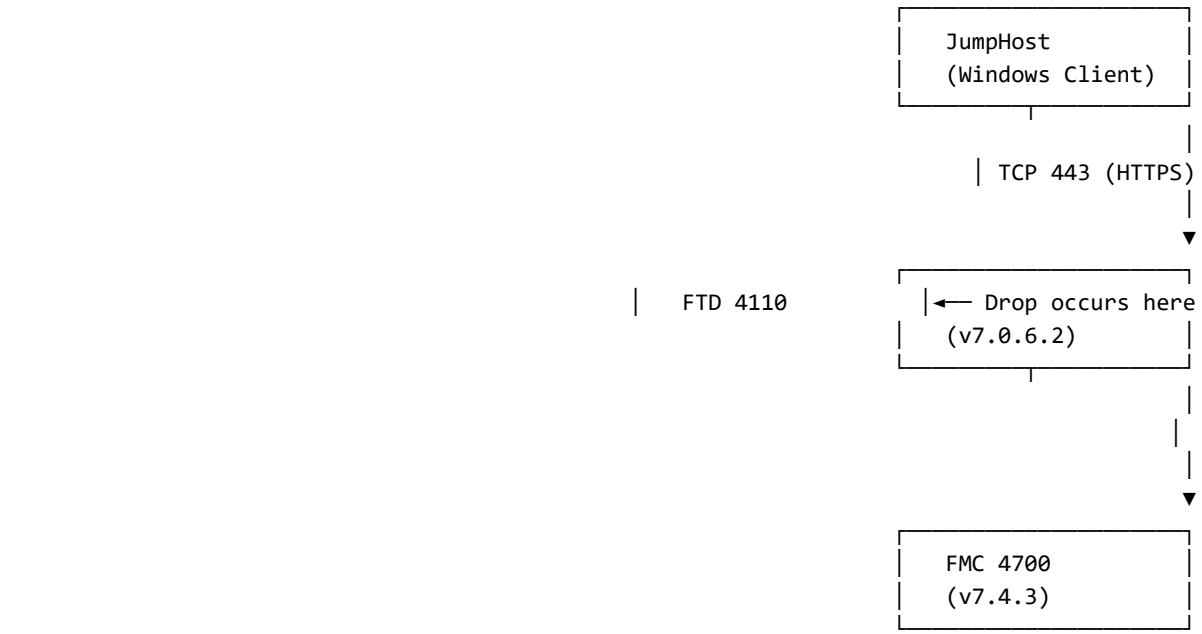
البيئة

· جدار الحماية: الدفاع الآمن عن تهديد جدار الحماية (FTD) من Cisco الذي يشغل الإصدار 7.0.x وأ
FTDv) وأ FPR-1000/2100/3100/4100/4200/9300) إصدار أحدث وأ 7.4.x وأ 7.2.x

· مركز الإدارة: مركز إدارة جدار الحماية الآمن (FMC) من Cisco طراز 4600 / 4700 / FMCv الذي يشغل
الإصدار 7.2.x وأ 7.4.x وأ إصدار أحدث

· نظام العميل: نظام تشغيل Windows (JumpHost، أو محطة العمل، أو الخادم) يتصل عبر
(TCP 443 لبروتوكول HTTPS) عبر بروتوكول تطبيقات البرمجة واجهة/المستعرض

طوبولوجيا بسيطة



قرار

تسلسل الحزمة

:يسبق هذا التسلسل عمليات الإسقاط المسجلة بشكل ثابت

```
Packet Flow & Timing Collision:
```

Step	Packet Direction	TCP Flags	Delta Timing	Description / State
1.	FMC ⟶ Client	[FIN, ACK]	T=0	FMC initiates graceful session close.
2.	Client → FMC	[ACK]	+0.2 ms	Client acknowledges FMC FIN.
3.	Client → FMC	[FIN, ACK]	+3ms - 13s	Application closes its half of socket.
4.	Client → FMC	[RST, ACK]	+15 - 31 µs	Windows immediately destroys socket.
5.	[FTD Firewall Action]	---	Immediate	FTD receives RST, purges connection from st
6.	FMC ⟶ Client	[ACK]	+0.06 - 2.2 ms	RFC 793 mandatory ACK for Step 3 FIN arrives.
7.	[FTD Firewall Action]	[acl-drop]	Immediate	No state table entry found -> Dropped as ac

---

ملاحظة: الخطوات 5 و 7 هي نقطة التصادم. يتسبب إجراء إعادة التوجيه السريع (RST) في الإزالة الفورية للحالة (الخطوة 6)، ويصل ACK إلزامي ل FMCs (الخطوة 7) في النافذة بين إزالة الحالة ودورة تقييم الحزمة التالية.

منهجية تحقيق TAC

أستخدم عملية الارتباط التالية من ثلاث طبقات عند التحقيق في حالات السقوط المفاجئ المفاجئ المشتبه بها:

الخطوة 1 — جمع البيانات

- تلتقط حزمة FTD على نقاط الدخول وواجهات الخروج وعمليات إسقاط ASP
- تصفية تفريغ TCP من FMC على المنفذ 443

```
> system support diagnostic-cli
ciscoasa# capture ASP_DROP type asp-drop acl-drop
ciscoasa# show capture ASP_DROP | include 443
1: 10:14:22.102345 10.10.32.15.443 > 10.10.10.50.55137: Flags [.], ack 3829104, win 501, length 0 (acl-
```

الخطوة 2 — إستخلاص و ربط

· إستخراج 5-tuple من التقاط إسقاط ASP يعرض الإسقاط والأسباب (tcp-rstfin-ooo، tcp-not-syn، acl-drop)

· إعادة بناء جدول حالة الاتصال باستخدام التقاط الدخول والخروج: التعرف على SYN، FIN/RST، والطوابع الزمنية الدقيقة

· ربط الإسقاط، والختم الزمني على المدخل/المخرج مع الطابع الزمني لنهاية العمر للجلسة

```
ciscoasa# show capture CAP_IN | include 10.10.10.50.55137
10:14:22.102110 10.10.10.50.55137 > 10.10.32.15.443: Flags [F.], seq 3829103, ack 1024
10:14:22.102128 10.10.10.50.55137 > 10.10.32.15.443: Flags [R.], seq 3829104, ack 1024
 10:14:22.102345 10.10.32.15.443 > 10.10.10.50.55137: Flags [.], ack 3829104 (DROPPED)
```

ملاحظة: يقر تسلسل FMC ACK برقم تسلسل FIN $+ 1$، ويؤكد أنه إستجابة RFC. تم إنهاؤه بالفعل.

الخطوة 3 — تأكيد النمط

- تأكيد حالات السقوط تحدث فقط بعد معالجة RST وليس أثناء جلسات العمل النشطة
- التحقق من أن الحزمة التي تم إسقاطها هي ACK برقم تسلسلي = FIN_SEQ + 1 (الاستجابة الإلزامية ل RFC 793)
- تحقق من عدم تطابق أي حالات فشل للتطبيق مع أحداث الإسقاط

تلميح: في الحالة المرجعية (SR 700468261)، أظهرت 54 جلسة من 55 جلسة RST على ثانية واحدة (ميناء 55137) ووصول FMC 0.024 ملي. أظهرت جلسة واحدة أن الحزمة النهائية. بعد RST، موضحة مباشرة توقيت حالة السباق.

رارق

ة الحماية جدار وتصميم TCP RFC ير معايي مع تماما متوافق السلوك هذا .إصلاح إلى حاجة توجد ال
.المعبر عن الحالة .ال يوجد أي عيب أو انخفاض في الأداء أو فقد للبيانات

متى يتصاعد

تحذير: لا تقم بالتصعيد استنادا إلى نمط الإسقاط هذا فقط. التصعيد فقط في حالة استيفاء الشروط الواردة في القسم التالي.

- تحدث عمليات السقوط أثناء الجلسات النشطة - وليس بعد تبادل RST أو FIN/ACK
- تتم ملاحظة حالات فشل التطبيقات أو حالات انتهاء المهلة الزمنية للجلسة أو عدم إمكانية الوصول إلى واجهة المستخدم الرسومية (GUI) ل FMC
- قم بإسقاط الزيادة في مستوى الصوت بمرور الوقت دون حدوث زيادة مقابلة في مستوى صوت الاتصال
- يختلف نمط الإسقاط عن التسلسل الموصوف في هذه المقالة

السبب

تنتج حالات الهبوط من حالة السباق في مقياس ميكروثانية بين ثلاثة سلوكيات صحيحة بشكل مستقل:

1. تحسين مكدس Windows TCP: عندما يقوم تطبيق Windows بإغلاق مأخذ توصيل حيث يقوم Windows بإرسال FIN بالفعل، يقوم الطرف البعيد بإرسال FIN-ACK على الفور. هذا بعد وضع RST في وضع التشغيل من 15 إلى 31s لتحرير الذاكرة ووحدات التحكم في بروتوكول TCP على الفور.

2. إزالة اتصال FTD المعبر عن الحالة: عند إستلام حزمة RST، يعمل FTD على إزالة إدخال الاتصال فورا من جدول الحالة الخاص به (جدول conn) للحفاظ على سلامة الأمان المعبرة.

3. التوافق مع معيار FMC RFC 793: وفقا لمواصفات RFC 793، تقوم مكدس بروتوكول TCP الخاص بالعميل (التسلسل $+ 1$). ونظرا لتأخر جدولة النظام وتوسعه، يصل هذا ACK إلى FTD.
تم مسح الاتصال بالفعل بعد أن يكون قد مر ثانية 2.2 — 0.06 مللي.

4. تقييم الإسقاط في برنامج الإرسال فائق السرعة (FTD): ونظرا لعدم وجود اتصال FTD، يقيم (وليس SYN) فقط ACK العامة عليه وتحتوي الحزمة على حالة الجدول في مطابقة ACL). بدون تصريح صريح لسجلات خارج ذلك مقابل قائمة التحكم في الوصول (ACL. الحالة، يقوم FTD بإسقاط الحزمة على هيئة acl-drop / tcp-not-syn.

المحتوى ذي الصلة

- المعيار RFC 793 — بروتوكول التحكم في الإرسال
- سبب إسقاط ASP
- مرجع SR: 700468261 (داخلي)

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).