Fehlerbehebung: FMC-Datenverkehr bricht veraltete ACK-Pakete nach TCP-Terminierung ab

Inhalt

Problem

In diesem Dokument wird erläutert, warum FTD ACL-Drop-Ereignisse protokolliert, um Datenrückverkehr von FMC zu Client-Systemen zu ermöglichen. Dies betrifft insbesondere ACK-Pakete, die eintreffen, nachdem TCP-Verbindungen bereits durch RST-Pakete vom Client beendet wurden. Die Drops sind das Produkt eines Race-Condition im Mikrosekundenbereich zwischen dem TCP-Stack-Verhalten von Windows und der RFC 793-konformen ACK-Erzeugung von FMCs. Beeinträchtigungen des Service sind nicht möglich, und eine Behebung ist nicht erforderlich.


Anmerkung: Dies ist ein erwartungsgemäßes Verhalten. Die acl-drop-Ereignisse können in Überwachungssystemen gefiltert werden, sobald dieses Muster bestätigt wurde.

Symptome:

- FTD-Firewall-Protokolle zeigen acl-drop-Ereignisse für den Rückverkehr von FMC zu Client-Systemen an (in diesem Beispiel JumpHost)
- Unterbrechungen treten bei TCP-Port 443 (HTTPS)-Verbindungen zwischen FMC und Client-Systemen auf.
- Ereignisse werden in FMC Unified Events als blockierte Pakete angezeigt
- Ursachencodes in Aufzeichnungen löschen: tcp-rstfin-ooo, tcp-not-syn, acl-drop
- Trotz der protokollierten Drops wurden keine tatsächlichen Auswirkungen auf den Service festgestellt.

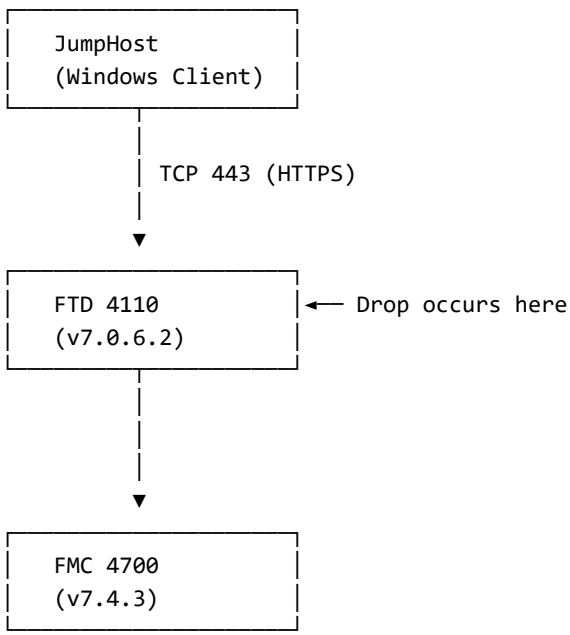
Umwelt

- Firewall: Cisco Secure Firewall Threat Defense (FTD) mit Version 7.0.x, 7.2.x, 7.4.x oder höher (FPR-1000/2100/3100/4100/4200/9300 oder FTDv)

- Management Center: Cisco Secure Firewall Management Center (FMC) 4600/4700/FMCv mit Version 7.2.x, 7.4.x oder höher

- Client-System: Windows-Betriebssystem (JumpHost, Workstation oder Server), Verbindung über Browser/API über HTTPS (TCP 443)

Einfache Topologie



Auflösung

Paketsequenz

Diese Sequenz geht konsistent vor den protokollierten Drops:

```
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

---

Anmerkung: Die Schritte 5 und 7 sind der Kollisionspunkt. Die RST bewirkt die sofortige Entfernung des Zustands (Schritt 6), und die FMCs erfordern eine ACK (Schritt 7), die im Zeitfenster zwischen der Entfernung des Zustands und dem nächsten Paketbewertungszyklus eingeht.

TAC-Untersuchungsmethode

Verwenden Sie den nächsten dreistufigen Korrelationsprozess, wenn Sie vermutete veraltete ACK-Drops untersuchen:

Schritt 1 - Sammeln von Daten

- FTD-Paketerfassung an Eingangs- und Ausgangsschnittstellen und bei asp-drops
- TCP-Dump von FMC gefiltert auf Port 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-
```

Schritt 2 - Extrahieren und Korrelieren

· Extrahieren Sie 5 Tupel aus dem asp drop capture zeigt die Tropfen und Gründe (tcp-rstfin-ooo, tcp-not-syn, acl-drop)

· Die Verbindungsstatustabelle mithilfe von Eingangs- und Ausgangserfassungen rekonstruieren: SYN, FIN/RST und die genauen Zeitstempel identifizieren

· Korrelieren des Drop, seines Zeitstempels auf den Eingangs-/Ausgangserfassungen mit dem Zeitstempel des Sitzungsendes

```
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)
```


Anmerkung: Die FMC ACK-Sequenz bestätigt die FIN-Sequenznummer $+ 1$ und bestätigt, dass es sich um eine RFC-Antwort auf eine bereits terminierte Verbindung handelt.

Schritt 3 - Muster bestätigen

- Vergewissern Sie sich, dass das Verwerfen nur nach der Verarbeitung der RST und nicht während aktiver Sitzungen erfolgt.
- Vergewissern Sie sich, dass es sich bei dem verworfenen Paket um eine ACK mit der Sequenznummer = FIN_Seq + 1 handelt (erforderliche RFC 793-Antwort).
- Überprüfen, ob keine Anwendungsfehler den Ereignissen zum Löschen entsprechen

---


Tipp: Im Referenzfall (SR 700468261) wiesen 54 von 55 Sitzungen RST als letztes Paket auf. Eine Session (Port 55137) zeigte, dass der ACK des FMC 0,024 ms nach dem RST eintraf und direkt den Rennzustand zeigte.

Auflösung

Es sind keine Korrekturen erforderlich. Dieses Verhalten entspricht vollständig den TCP-RFC-Standards und dem Stateful-Firewall-Design. Es treten keine Fehler, Leistungseinbußen oder Datenverluste auf.

Wann eskalieren

Warnung: Eskalieren Sie NICHT allein aufgrund dieses Abwurfmusters. Eskalieren Sie diese nur, wenn die Bedingungen im nächsten Abschnitt erfüllt sind.

- Drops treten während aktiver Sitzungen auf, nicht nach RST- oder FIN/ACK-Austausch.
- Anwendungsfehler, Sitzungszeitüberschreitungen oder Unzugänglichkeit der FMC-GUI wurden beobachtet.
- Die Abwurfmenge nimmt mit der Zeit zu, ohne dass sich die Verbindungsmenge entsprechend erhöht.
- Das Tropfenmuster weicht von der in diesem Artikel beschriebenen Reihenfolge ab

Ursache

Die Verluste resultieren aus einem Wettlauf in Mikrosekunden zwischen drei unabhängig korrekten Verhaltensweisen:

1. Windows TCP-Stack-Optimierung: Wenn eine Windows-Anwendung einen Socket schließt, bei dem das Remote-Ende bereits FIN gesendet hat, überträgt Windows sofort ein FIN-ACK. Nach der RST-ACK innerhalb von 15 - 31 s werden Speicher und TCP-Kontrollblöcke sofort freigegeben.
2. FTD Stateful Connection-Entfernung: Beim Empfang des RST-Pakets beendet FTD sofort den Verbindungseintrag und löscht ihn aus seiner Statustabelle (conn-Tabelle), um die zustandsbehaftete Sicherheitsintegrität aufrechtzuerhalten.
3. FMC RFC 793-Konformität: Gemäß RFC 793-Spezifikationen generiert der FMC TCP-Stack

eine ACK, die die FIN des Clients bestätigt (Sequenz $+ 1$). Aufgrund von Systemplanungs- und Weiterleitungsverzögerungen erreicht dieser ACK den FTD.
0,06 - 2,2 ms, nachdem die RST die Verbindung bereits geleert hat.

4. FTD-Verlustbewertung: Da keine passende Verbindung in der Statustabelle vorhanden ist und das Paket nur das ACK-Flag (kein SYN) enthält, wird es von FTD anhand der Zugriffskontrollliste (ACL) ausgewertet. Ohne ausdrückliche Genehmigung für Out-of-State-ACKs verwirft FTD das Paket als acl-drop/tcp-not-syn.

Verwandte Inhalte

- RFC 793 — Transmission Control Protocol
- ASP-Ablehnungsgrund
- SR-Referenz: 700468261 (intern)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.