排除TCP終止後FMC流量丟棄過時的ACK資料包故障

目錄

問題

本檔案將說明為什麼FTD會記錄從FMC到使用者端系統的傳回流量的acl-drop事件，特別是在TCP連線已由使用者端的RST封包終止後到達的ACK封包。丟包是Windows TCP堆疊行為與符合FMC RFC 793的ACK生成之間微秒級競爭條件的產物。不會發生服務影響，無需進行補救。


附註：這是預期行為。確認此模式後，可以在監控系統中安全過濾acl-drop事件。

症狀：

- FTD防火牆記錄顯示從FMC傳回至使用者端系統（在本範例中為JumpHost）的流量的acl-drop事件
- FMC和客戶端系統之間的TCP埠443(HTTPS)連線發生丟棄
- 在FMC統一事件中，事件顯示為阻止的資料包
- 丟棄在捕獲中看到的原因代碼：tcp-rstfin-ooo， tcp-not-syn， acl-drop
- 儘管記錄了丟包，仍然沒有觀察到實際服務影響

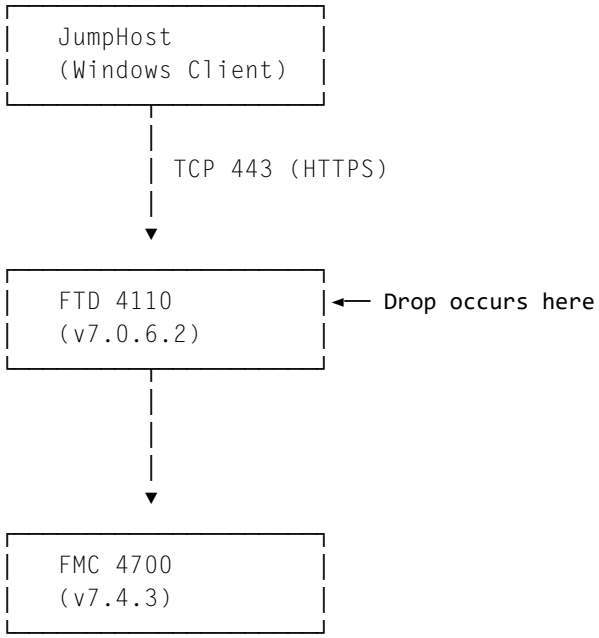
環境

•Firewall:執行7.0.x、7.2.x、7.4.x或更新版本（FPR-1000/2100/3100/4100/4200/9300或FTDv）的Cisco安全防火牆威脅防禦(FTD)

·管理中心：思科安全防火牆管理中心(FMC)4600/4700/FMCv（運行版本7.2.x、7.4.x或更高版本）

·客戶端系統：Windows OS（JumpHost、Workstation或Server）通過瀏覽器/API通過HTTPS(TCP 443)連線

簡單拓撲



解析

資料包序列

此順序始終在記錄的丟棄之前：

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
```

附註：步驟5和7為衝突點。RST導致立即狀態刪除（步驟6），而FMC的強制ACK（步驟7）在狀態刪除和下一個資料包評估週期之間到達視窗。

TAC調查方法

在調查可疑的陳舊ACK丟棄時，請使用下一個三層關聯過程：

步驟1 — 收集資料

- 輸入、輸出介面和asp捨棄時的FTD封包擷取
- 從FMC過濾的TCP轉儲埠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-
```

步驟2 — 提取並關聯

·從asp drop capture中提取5元組顯示丟棄和原因(tcp-rstfin-ooo、tcp-not-syn、acl-drop)

·使用入口和出口捕獲重建連線狀態表：識別SYN、FIN/RST和準確的時間戳

·將丟棄、其輸入/輸出捕獲上的時間戳與會話壽命終止時間戳關聯起來

```
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)
```


附註：FMC ACK序列確認FIN序列號$+ 1$，並確認這是對已終止連線的RFC響應。

步驟3 — 確認圖案

- 確認丟棄僅在處理RST之後發生，而不是在活動會話期間
- 驗證丟棄的資料包是否為序列號為FIN_Seq + 1的ACK（RFC 793強制性響應）
- 驗證沒有應用程式故障與丟棄事件相對應


提示：在參考案例(SR 700468261)中，55個作業階段中有54個將RST顯示為最終封包。一個作業階段(連線埠55137)顯示FMC的ACK在RST後到達0.024ms，直接顯示比賽條件時間。

解析

無需修正。此行為完全符合TCP RFC標準和狀態防火牆設計。沒有缺陷、效能下降或資料丟失。

升級時間


警告：不要僅基於此丟棄模式升級。僅在滿足下一部分中的條件時上報。

- 丟棄在活動會話期間發生 — 而不是在RST或FIN/ACK交換之後
- 觀察到應用程式故障、會話超時或FMC GUI不可訪問性
- 丟棄容量會隨著時間而增加，但連線容量不會相應增加
- 丟棄模式與本文描述的順序不同

原因

滴落是由三個獨立正確行為之間的微秒級競爭條件導致的：

1. Windows TCP堆疊最佳化：當Windows應用程式關閉一個套接字時，該套接字的遠端已經傳送了FIN，Windows將立即傳送FIN-ACK。這是繼RST-ACK之後，在15 - 31s內，即時釋放記憶體和TCP控制塊。
2. FTD狀態連線移除：收到RST封包後，FTD會立即捨棄並清除其狀態表（conn表）中的連線專案，以維持狀態安全完整性。
3. FMC RFC 793合規性：根據RFC 793規範，FMC TCP堆疊生成一個ACK，確認客戶端的FIN（序列$+ 1$）。 由於系統排程和傳播延遲，此ACK達到FTD。
0.06 — RST已刷新連線後2.2毫秒。
4. FTD捨棄評估：由於狀態表中不存在相符的連線，且封包只有ACK旗標（不是SYN），FTD會根據存取控制清單(ACL)評估該連線。 如果沒有外態ACK的明確允許，FTD會以acl-drop / tcp-not-syn形式捨棄封包。

相關內容

- RFC 793 — 傳輸控制通訊協定
- ASP刪除原因
- SR參考：700468261（內部）

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。