排除TCP终止后FMC流量丢弃过时的ACK数据包故障

目录

问题

本文档说明为什么FTD记录从FMC到客户端系统的返回流量的acl-drop事件，特别是在TCP连接已被来自客户端的RST数据包终止之后到达的ACK数据包。丢弃是Windows TCP堆栈行为与符合FMC RFC 793的ACK生成之间的微秒级竞争条件的产物。不会产生任何服务影响，无需进行补救。

注意：这是预料之中的现象。一旦确认此模式，acl-drop事件在监控系统中可以安全过滤。

症状：

- FTD防火墙日志显示从FMC到客户端系统（本示例中为JumpHost）的返回流量的acl-drop事件
- 丢弃发生在FMC和客户端系统之间的TCP端口443(HTTPS)连接上
- 在FMC统一事件中，事件显示为受阻数据包
- 删除捕获中看到的原因代码：tcp-rstfin-ooo、tcp-not-syn、acl-drop
- 尽管已记录丢弃数据,但并未观察到实际服务影响

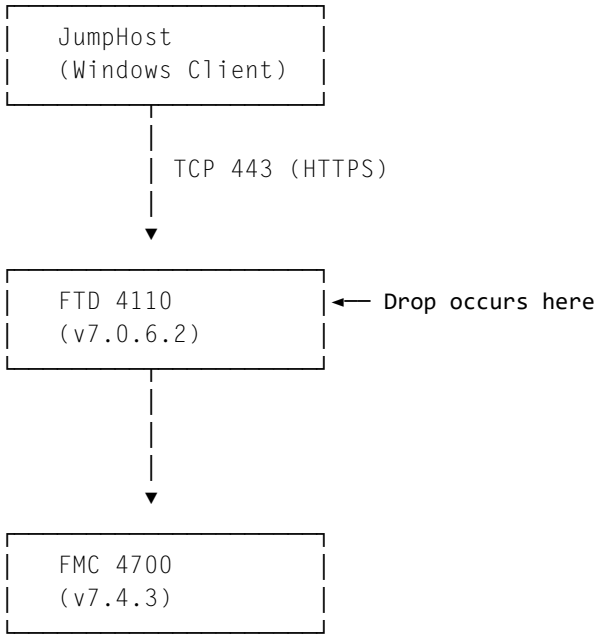
环境

•防火墙：运行版本7.0.x、7.2.x、7.4.x或更高版本的思科安全防火墙威胁防御(FTD)（FPR-1000/2100/3100/4100/4200/9300或FTDv）

·管理中心：运行版本7.2.x、7.4.x或更高版本的思科安全防火墙管理中心(FMC)4600/4700/FMCv

•客户端系统:Windows操作系统（JumpHost、Workstation或Server）通过浏览器/API over HTTPS(TCP 443)连接

简单拓扑



分辨率

数据包序列

此序列始终位于记录的丢弃之前：

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
```

注意：步骤5和步骤7是冲突点。RST导致立即状态删除（第6步），FMC强制确认在状态删除和下一个数据包评估周期之间到达窗口。

TAC调查方法

在调查可疑的陈旧ACK丢弃时，请使用下一个三层关联过程：

步骤1 — 收集数据

- 入口接口、出口接口和asp丢弃上的FTD数据包捕获
- FMC的TCP转储已在端口443上过滤

```
> 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-
```

步骤2 — 提取并关联

·从asp drop capture提取5元组显示丢弃和原因(tcp-rstfin-ooo、tcp-not-syn、acl-drop)

·使用入口和出口捕获重建连接状态表：识别SYN、FIN/RST和准确的时间戳

·将丢弃、其入口/出口捕获的时间戳与会话寿命终止时间戳关联起来

```
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)
```


注意：FMC ACK序列确认FIN序列号$+ 1$，并确认这是对已终止连接的RFC响应。

步骤3 — 确认模式

- 确认丢弃仅在已处理RST之后发生，而不是在活动会话期间
- 验证丢弃的数据包是否为序列号为FIN_Seq + 1的ACK（RFC 793强制性响应）
- 确认没有应用程序故障与丢弃事件相对应


提示：在参考案例(SR 700468261)中，55个会话中有54个将RST显示为最终数据包。一个会话（端口55137）显示FMC的ACK在RST之后到达0.024ms，直接显示竞争条件时间。

分辨率

无需补救。此行为完全符合TCP RFC标准和状态防火墙设计。无缺陷、性能下降或数据丢失。

升级时间


警告：不要仅基于此丢弃模式进行上报。仅在满足下一部分中的条件时上报。

- 丢弃发生在活动会话期间 — 而不是在RST或FIN/ACK交换之后
- 观察到应用故障、会话超时或FMC GUI不可访问
- 丢包量随时间增加，但连接量不会相应增加
- 丢弃模式与本文描述的顺序不同

原因

丢包是由三个独立正确行为之间的微秒级竞争条件导致的：

1. Windows TCP堆栈优化：当Windows应用程序关闭远端已经发送FIN的套接字时，Windows将立即发送FIN-ACK。这是在15 - 31秒内RST-ACK后，即时释放内存和TCP控制块。
2. FTD状态连接删除：收到RST数据包后，FTD立即将其从状态表（连接表）中移除并清除连接条目，以保持状态安全完整性。
3. FMC RFC 793合规性：根据RFC 793规范，FMC TCP协议栈会生成一个确认消息，确认客户端的FIN（序列$+ 1$）。 由于系统调度和传播延迟，此ACK到达FTD。
   0.06 - RST已刷新连接后2.2毫秒。
4. FTD丢弃评估：由于状态表中不存在匹配的连接，并且数据包只有ACK标志（不是SYN），因此FTD根据访问控制列表(ACL)评估该连接。 如果没有状态外ACK的明确许可，FTD会以acl-drop / tcp-not-syn形式丢弃数据包。

相关内容

- RFC 793 — 传输控制协议
- ASP丢弃原因
- SR参考：700468261（内部）

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。