Troubleshoot FMC Traffic Drops Stale ACK Packets After TCP Termination

Contents

Issue

This document describes why FTD logs with **acl-drop** events for return traffic from FMC to client systems, specifically ACK packets arriving after TCP connections have already been terminated by RST packets from the client. The drops are a product of a microsecond-level race condition between Windows TCP stack behavior and FMCs RFC 793-compliant ACK generation. No service impact occurs, and no remediation is required.



Note: This is expected behavior. The **acl-drop** events are safe to filter out in monitoring systems once this pattern is confirmed.

Symptoms:

- FTD firewall logs show **acl-drop** events for return traffic from FMC to client systems (JumpHost in this example)
- Drops occur on TCP port 443 (HTTPS) connections between FMC and client systems
- Events appear in FMC unified events as blocked packets
- Drop reason codes seen in captures: tcp-rstfin-ooo, tcp-not-syn, acl-drop
- No actual service impact is observed despite the logged drops

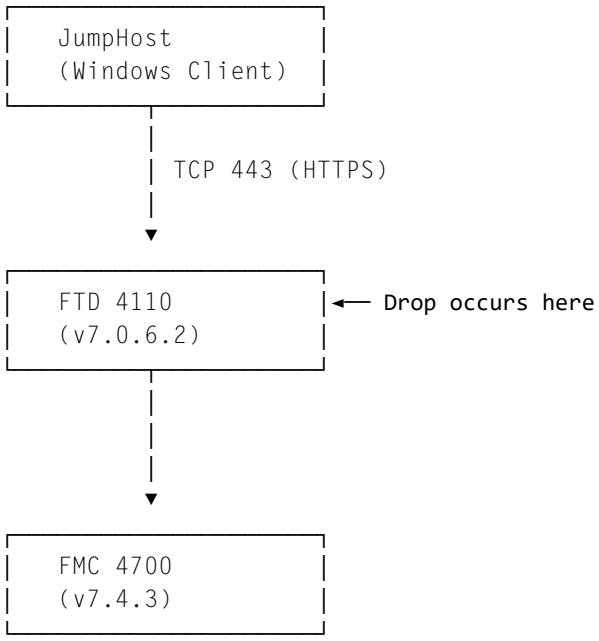
Environment

• **Firewall:** Cisco Secure Firewall Threat Defense (FTD) running version 7.0.x, 7.2.x, 7.4.x, or later (FPR-1000/2100/3100/4100/4200/9300 or FTDv)

• **Management Center:** Cisco Secure Firewall Management Center (FMC) 4600 / 4700 / FMCv running version 7.2.x, 7.4.x, or later

• **Client System:** Windows OS (JumpHost, Workstation, or Server) connecting via browser/API over HTTPS (TCP 443)

Simple Topology



Resolution

Packet Sequence

This sequence consistently precedes the logged 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
```

Note: Steps 5 and 7 are the collision point. The RST causes immediate state removal (Step 6), and FMCs mandatory ACK (Step 7) arrives in the window between state removal and the next packet evaluation cycle.

TAC Investigation Methodology

Use the next three-tier correlation process when investigating suspected stale ACK drops:

Step 1 — Collect Data

- FTD packet captures on ingress, egress interfaces and asp drops
- TCP dump from FMC filtered on 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-
```

Step 2 — Extract and Correlate

• Extract 5-tuple from the asp drop capture displays the drops and reasons (tcp-rstfin-ooo, tcp-not-syn, acl-drop)

• Reconstruct the connection state table using ingress and egress captures: identify SYN, FIN/RST, and the exact timestamps

• Correlate the drop, its timestamp on the ingress/egress captures against the session end-of-life timestamp

```
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)
```

Note: *The FMC ACK sequence acknowledges the FIN sequence number $+ 1$, confirming it is an RFC response to an already terminated connection.*

Step 3 — Confirm Pattern

- Confirm drops occur only after RST has been processed and not during active sessions
- Verify the dropped packet is an ACK with sequence number = FIN_Seq + 1 (RFC 793 mandatory response)
- Verify that no application failures correspond to the drop events

---

Tip: In the reference case (SR 700468261), 54 out of 55 sessions showed RST as the final packet. One session (port 55137) showed FMC's ACK arriving 0.024ms after the RST, directly demonstrating the race condition timing.

Resolution

No remediation is required. This behavior is fully compliant with TCP RFC standards and stateful firewall design. There is no defect, performance degradation, or data loss.

When to Escalate

Warning: Do NOT escalate based on this drop pattern alone. Escalate only if the conditions in the next section are met.

- Drops occur during active sessions — not after RST or FIN/ACK exchange
- Application failures, session timeouts, or FMC GUI inaccessibility are observed

- Drop volume increases over time without a corresponding increase in connection volume
- The drop pattern deviates from the sequence described in this article

Cause

The drops result from a race condition at microsecond timescale between three independently correct behaviors:

1. **Windows TCP Stack Optimization:** When a Windows application closes a socket where the remote end already sent FIN, Windows transmits a FIN-ACK immediately. This is after the RST-ACK within **15 - 31s** to instantly free memory and TCP control blocks.
2. **FTD Stateful Connection Removal:** Upon receiving the RST packet, FTD immediately tears down and purges the connection entry from its state table (conn table) to maintain stateful security integrity.
3. **FMC RFC 793 Compliance:** Per RFC 793 specifications, the FMC TCP stack generates an ACK acknowledging the client's FIN (Sequence $+ 1$). Because of system scheduling and propagation delay, this ACK reaches the FTD.
   0.06 -- 2.2ms after the RST has already flushed the connection.
4. **FTD Drop Evaluation:** Since no matching connection exists in the state table and the packet has only the ACK flag (not a SYN), FTD evaluates it against the Access Control List (ACL). Without an explicit permit for out-of-state ACKs, FTD drops the packet as acl-drop / tcp-not-syn.

Related Content

- RFC 793 — Transmission Control Protocol
- ASP Drop Reason
- SR Reference: 700468261 (Internal)