TCP 종료 후 오래된 ACK 패킷을 삭제하는 FMC 트래픽 문제 해결

목차

문제

이 문서에서는 FTD가 FMC에서 클라이언트 시스템으로의 반환 트래픽, 특히 클라이언트의 RST 패킷에 의해 TCP 연결이 이미 종료된 후에 도착하는 ACK 패킷에 대해 acl-drop 이벤트를 사용하여 로그인하는 이유를 설명합니다. 삭제는 Windows TCP 스택 동작과 FMC RFC 793 호환 ACK 생성 간의 마이크로초 수준 경쟁 조건의 산물입니다. 서비스에 영향을 미치지 않으며 교정이 필요하지 않습니다.

참고: 이는 정상적인 동작입니다. acl-drop 이벤트는 이 패턴이 확인되면 모니터링 시스템에서 필터링할 수 있습니다.

증상:

- FTD 방화벽 로그는 FMC에서 클라이언트 시스템(이 예에서는 JumpHost)으로의 반환 트래픽에 대한 acl-drop 이벤트를 표시합니다
- FMC와 클라이언트 시스템 간의 TCP 포트 443(HTTPS) 연결에서 삭제 발생
- 이벤트는 FMC 통합 이벤트에 차단된 패킷으로 표시됩니다
- 캡처에 표시된 삭제 사유 코드: tcp-rstfin-ooo, tcp-not-syn, acl-drop
- 로그된 삭제에도 불구하고 실제 서비스 영향은 관찰되지 않음

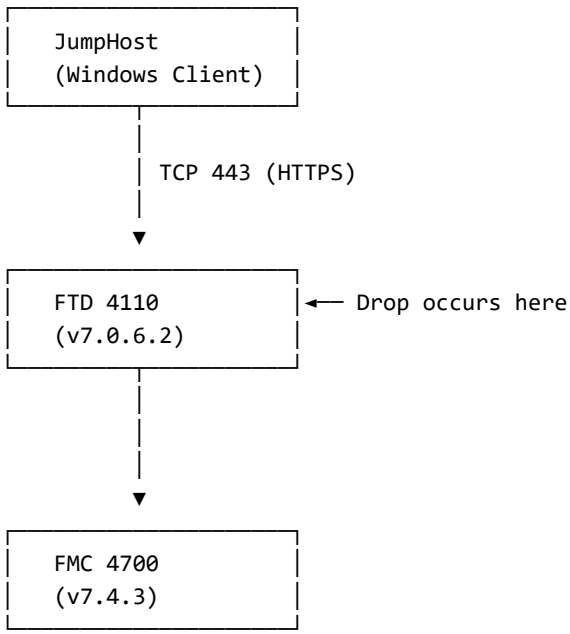
환경

· 방화벽: 버전 7.0.x, 7.2.x, 7.4.x 이상을 실행하는 Cisco FTD(Secure Firewall Threat Defense)(FPR-1000/2100/3100/4100/4200/9300 또는 FTDv)

· 관리 센터: 버전 7.2.x, 7.4.x 이상을 실행하는 Cisco FMC(Secure Firewall Management Center) 4600/4700/FMCv

· 클라이언트 시스템: 브라우저/API를 통해 HTTPS를 통해 연결하는 Windows OS(JumpHost, Workstation 또는 Server)(TCP 443)

단순 토폴로지



해결

패킷 시퀀스

이 시퀀스는 로깅된 삭제 앞에 지속적으로 옵니다.

```
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

참고: 5단계와 7단계는 충돌 지점입니다. RST는 즉각적인 상태 제거를 야기하고(6단계), FMCs 필수 ACK(7단계)는 상태 제거와 다음 패킷 평가 주기 사이의 기간에 도달합니다.

TAC 조사 방법론

의심스러운 부실 ACK 삭제를 조사할 때 다음 3계층 상관관계 프로세스를 사용합니다.

1단계 - 데이터 수집

- 인그레스(ingress), 이그레스(egress) 인터페이스 및 asp 드롭에서 FTD 패킷 캡처
- 포트 443에서 필터링된 FMC의 TCP 덤프

```
> 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-
```

2단계 — 추출 및 상관관계 분석

· asp drop capture에서 5-tuple을 추출하면 삭제 및 이유(tcp-rstfin-ooo, tcp-not-syn, acl-drop)가 표시됩니다.

· 인그레스(ingress) 및 이그레스(egress) 캡처를 사용하여 연결 상태 테이블을 재구성합니다. SYN, FIN/RST 및 정확한 타임스탬프 식별

· 삭제, 인그레스/이그레스 캡처의 타임스탬프를 세션 end-of-life 타임스탬프와 상호 연결

```
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)
```

참고: FMC ACK 시퀀스는 FIN 시퀀스 번호 $+ 1$을(를) 승인하며, 이미 종료된 연결에 대한 RFC 응답임을 확인합니다.

3단계 - 패턴 확인

- 삭제 확인은 RST가 처리된 후에만 발생하며 활성 세션 중에는 발생하지 않습니다
- 삭제된 패킷이 시퀀스 번호 = FIN_Seq + 1의 ACK인지 확인합니다(RFC 793 필수 응답).
- 애플리케이션 오류가 삭제 이벤트에 해당되지 않는지 확인합니다.

팁: 참조 케이스(SR 700468261)에서는 55개 세션 중 54개 세션이 최종 패킷으로 RST를 보였다. 한 세션(포트 55137)에서는 RST 후 FMC의 ACK가 0.024ms에 도달하는 것을 보여주며, 직접 레이스 상태 타이밍을 입증했습니다.

해결

교정이 필요하지 않습니다. 이 동작은 TCP RFC 표준 및 스테이트풀 방화벽 설계를 완벽하게 준수합니다. 결함, 성능 저하 또는 데이터 손실이 없습니다.

에스컬레이션 시기

경고: 이 삭제 패턴만 기준으로 에스컬레이션하지 마십시오. 다음 섹션의 조건이 충족되는 경우에만 에스컬레이션합니다.

- RST 또는 FIN/ACK 교환 후가 아닌 활성 세션 중에 삭제 발생
- 애플리케이션 장애, 세션 시간 초과 또는 FMC GUI 액세스 불가
- 연결 볼륨이 증가하지 않고 시간이 지남에 따라 드롭 볼륨 증가
- 낙하 패턴은 이 기사에 기술된 순서를 벗어난다

원인

이 삭제는 독립적으로 올바른 동작 3개 사이의 마이크로초 단위의 경합 상태에서 발생합니다.

1. Windows TCP 스택 최적화: Windows 응용 프로그램이 원격 끝에서 이미 FIN을 보낸 소켓을 닫으면 Windows는 FIN-ACK을 즉시 전송합니다. 이는 RST-ACK가 15-31s에 발생한 후 메모리 및 TCP 제어 블록을 즉시 해제하기 위한 것입니다.
2. FTD 상태 저장 연결 제거: FTD는 RST 패킷을 수신하면 즉시 해제하여 상태 기반 보안 무결성을 유지하기 위해 상태 테이블(conn 테이블)에서 연결 항목을 제거합니다.
3. FMC RFC 793 규정 준수: RFC 793 사양에 따라 FMC TCP 스택은 클라이언트의 FIN을 승인하는 ACK를 생성합니다(시퀀스 $+ 1$). 시스템 스케줄링 및 전파 지연으로 인해 이 ACK는 FTD에 도달합니다.
   0.06 — RST에서 연결을 이미 플러시한 후 2.2ms.
4. FTD 삭제 평가: 상태 테이블에 일치하는 연결이 없고 패킷에 ACK 플래그(SYN 아님)만 있으므로 FTD는 ACL(Access Control List)을 기준으로 평가합니다. 상태 외 ACK에 대한 명시적 허가가 없으면 FTD는 패킷을 acl-drop / tcp-not-syn으로 삭제합니다.

관련 콘텐츠

- RFC 793 — 전송 제어 프로토콜
- ASP 삭제 사유
- SR 참조: 700468261(내부)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.