Risoluzione dei problemi relativi al traffico FMC che causa la perdita di pacchetti stack obsoleti dopo la terminazione di TCP

Sommario

Problema

Questo documento descrive il motivo per cui FTD registra gli eventi acl-drop per il traffico di ritorno da FMC ai sistemi client, in particolare i pacchetti ACK che arrivano dopo che le connessioni TCP sono già state terminate dai pacchetti RST dal client. Le cadute sono il prodotto di una gara di livello al microsecondo tra il comportamento dello stack TCP di Windows e la generazione di ACK conformi allo standard RFC 793 dei FMC. Non si verifica alcun impatto sul servizio e non è necessario alcun rimedio.

Nota: Si tratta di un comportamento normale. Una volta confermato questo modello, gli eventi acl-drop possono essere esclusi dai sistemi di monitoraggio.

Sintomi:

- I registri del firewall FTD mostrano gli eventi di rilascio degli acl per il traffico di ritorno da FMC ai sistemi client (JumpHost nell'esempio)
- Interruzioni sulle connessioni della porta TCP 443 (HTTPS) tra FMC e i sistemi client
- Gli eventi vengono visualizzati negli eventi unificati di FMC come pacchetti bloccati
- Elimina codici motivo nelle clip: tcp-rstfin-ooo, tcp-not-syn, acl-drop
- Non viene osservato alcun impatto effettivo sul servizio nonostante le riduzioni registrate

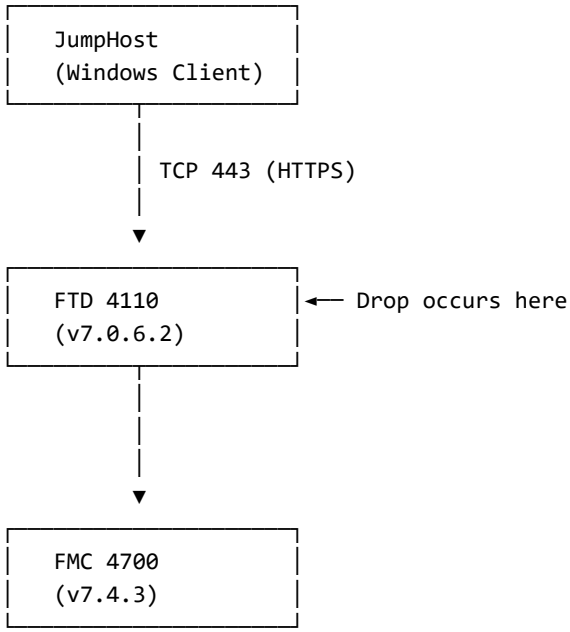
Ambiente

· Firewall Cisco Secure Firewall Threat Defense (FTD) con versione 7.0.x, 7.2.x, 7.4.x o successive (FPR-1000/2100/3100/4100/4200/9300 o FTDv)

· Centro di gestione: Cisco Secure Firewall Management Center (FMC) 4600 / 4700 / FMCv con versione 7.2.x, 7.4.x o successive

· Sistema client: Windows OS (JumpHost, Workstation o Server) con connessione tramite browser/API su HTTPS (TCP 443)

Topologia semplice



Risoluzione

Sequenza pacchetti

Questa sequenza precede in modo coerente le eliminazioni registrate:

```
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

Nota: I passi 5 e 7 sono il punto di collisione. L'RST determina la rimozione immediata dello stato (passaggio 6) e gli ACK obbligatori dei FMC (passaggio 7) arrivano nella finestra tra la rimozione dello stato e il successivo ciclo di valutazione dei pacchetti.

Metodologia di indagine TAC

Per l'analisi dei casi di possibile caduta di stack inattivi, utilizzare il successivo processo di correlazione a tre livelli:

Passaggio 1 - Raccolta dati

- Acquisizione di pacchetti FTD in entrata, interfacce in uscita e cadute asp
- Dump TCP da FMC filtrato sulla porta 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-
```

Fase 2 — Estrazione e correlazione

· L'estrazione di 5 tuple dall'acquisizione con drop dell'asp visualizza le cadute e i motivi (tcp-rstfin-ooo, tcp-not-syn, acl-drop)

· Ricostruire la tabella dello stato di connessione utilizzando le acquisizioni in entrata e in uscita: identificare SYN, FIN/RST e i timestamp esatti

· Correlazione tra la caduta, il relativo timestamp sulle immagini in entrata/uscita e il timestamp di fine sessione

```
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)
```


Nota: La sequenza ACK del CCP riconosce il numero di sequenza FIN $+ 1$, confermando che si tratta di una risposta RFC a una connessione già terminata.

Passaggio 3 - Conferma modello

- Le eliminazioni di conferma si verificano solo dopo l'elaborazione di RST e non durante le sessioni attive
- Verificare che il pacchetto scartato sia un ACK con numero di sequenza = FIN_Seq + 1 (risposta obbligatoria RFC 793)
- Verificare che nessun errore dell'applicazione corrisponda agli eventi di rilascio

---


Suggerimento: Nel caso di riferimento (SR 700468261), 54 sessioni su 55 mostravano RST come pacchetto finale. Una sessione (porta 55137) ha mostrato che l'ACK della FMC arrivava 0,024 ms dopo l'RST, dimostrando direttamente i tempi delle condizioni di gara.

Risoluzione

Non è necessario alcun rimedio. Questo comportamento è pienamente conforme agli standard RFC TCP e alla progettazione del firewall con stato. Non si verificano difetti, peggioramento delle prestazioni o perdita di dati.

Quando effettuare l'escalation

Avviso: NON eseguire l'escalation solo in base a questo modello di rilascio. Escala solo se vengono soddisfatte le condizioni della sezione successiva.

- Cadute durante le sessioni attive, non dopo lo scambio di RST o FIN/ACK
- Sono stati osservati errori delle applicazioni, timeout delle sessioni o inaccessibilità dell'interfaccia utente di FMC
- Il volume di destinazione aumenta nel tempo senza un corrispondente aumento del volume di connessione
- Il motivo di rilascio si discosta dalla sequenza descritta in questo articolo

Causa

Le cadute derivano da una condizione di razza sulla scala cronologica dei microsecondi tra tre comportamenti corretti indipendentemente:

1. Ottimizzazione stack TCP Windows: Quando un'applicazione Windows chiude un socket a cui l'estremità remota ha già inviato un messaggio FIN, Windows trasmette immediatamente un messaggio FIN-ACK. Ciò avviene dopo il RST-ACK entro 15 - 31s per liberare istantaneamente la memoria e i blocchi di controllo TCP.
2. Rimozione connessione stateful FTD: Alla ricezione del pacchetto RST, FTD interrompe immediatamente la connessione e rimuove la voce di connessione dalla relativa tabella di stato (conn table) per mantenere l'integrità della sicurezza con conservazione dello stato.
3. Conformità RFC 793: In base alle specifiche della RFC 793, lo stack TCP del CCP genera un ACK che riconosce l'indirizzo FIN (Sequence $+ 1$) del client. A causa della pianificazione del sistema e del ritardo di propagazione, questo ACK raggiunge l'FTD. 0,06 — 2,2 ms dopo che l'RST ha già scaricato la connessione.
4. Valutazione rilascio FTD: Poiché nella tabella degli stati non esiste una connessione corrispondente e il pacchetto ha solo il flag ACK (non un SYN), FTD lo valuta in base all'Access Control List (ACL). Senza un permesso esplicito per gli ACK fuori stato, FTD scarta il pacchetto come acl-drop / tcp-not-syn.

Contenuto correlato

- RFC 793 - Protocollo di controllo della trasmissione
- Motivo rilascio ASP
- Riferimento SR: 700468261 (interna)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).