Resolución de problemas de tráfico FMC descarta paquetes ACK obsoletos después de la terminación TCP

Contenido

Problema

Este documento describe por qué el FTD registra con los eventos acl-drop para el tráfico de retorno de FMC a los sistemas cliente, específicamente los paquetes ACK que llegan después de que las conexiones TCP ya han sido terminadas por los paquetes RST del cliente. Las caídas son producto de una condición de carrera de microsegundos entre el comportamiento de la pila TCP de Windows y la generación de ACK conforme a RFC 793 de FMCs. No se produce ningún impacto en el servicio y no es necesario remediarlo.


Nota: Debe ocurrir lo siguiente. Los eventos acl-drop son seguros para filtrar en los sistemas de monitoreo una vez que se confirma este patrón.

Síntomas:

- Los registros del firewall FTD muestran eventos acl-drop para el tráfico de retorno desde FMC a los sistemas cliente (JumpHost en este ejemplo)
- Se producen caídas en las conexiones del puerto TCP 443 (HTTPS) entre FMC y los sistemas cliente
- Los eventos aparecen en los eventos unificados de FMC como paquetes bloqueados
- Descartar códigos de motivo vistos en capturas: tcp-rstfin-ooo, tcp-not-syn, acl-drop
- No se observa ningún impacto real en el servicio a pesar de las caídas registradas

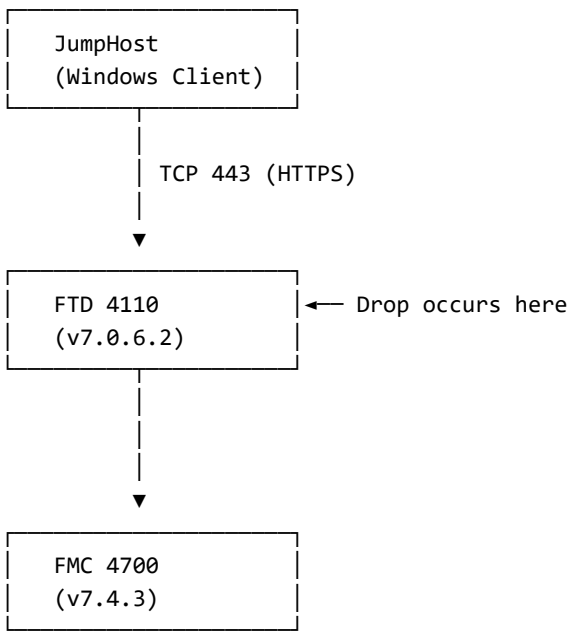
Entorno

•Firewall: Cisco Secure Firewall Threat Defence (FTD) con versión 7.0.x, 7.2.x, 7.4.x o posterior (FPR-1000/2100/3100/4100/4200/9300 o FTDv)

· Centro de gestión: Cisco Secure Firewall Management Center (FMC) 4600 / 4700 / FMCv con la versión 7.2.x, 7.4.x o posterior

· Sistema cliente: Sistema operativo Windows (JumpHost, Workstation o Server) conectado a través del navegador/API sobre HTTPS (TCP 443)

Topología sencilla



Resolución

Secuencia de paquetes

Esta secuencia precede consistentemente a las caídas registradas:

```
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: Los pasos 5 y 7 son el punto de colisión. El RST provoca la eliminación inmediata del estado (paso 6), y el ACK obligatorio de los FMC (paso 7) llega en la ventana entre la eliminación del estado y el siguiente ciclo de evaluación de paquetes.

Metodología de investigación del TAC

Utilice el siguiente proceso de correlación de tres niveles cuando investigue caídas ACK sospechosas de obsolescencia:

Paso 1: Recopilación de datos

- Capturas de paquetes FTD en interfaces de entrada, salida y caídas de asp
- Volcado de TCP desde FMC filtrado en el puerto 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-
```

Paso 2: Extracción y correlación

· Extraer 5 tuplas de la captura de caídas asp muestra las caídas y las razones (tcp-rstfin-ooo, tcp-not-syn, acl-drop)

· Reconstruya la tabla de estado de conexión mediante capturas de ingreso y egreso: identificar SYN, FIN/RST y las marcas de tiempo exactas

· Correlacionar la caída, su marca de tiempo en las capturas de ingreso/egreso con la marca de tiempo de fin de vida de la sesión

```
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 secuencia ACK de FMC reconoce el número de secuencia FIN $+ 1$, lo que confirma que se trata de una respuesta RFC a una conexión que ya ha finalizado.

Paso 3: Confirmar patrón

- La confirmación de caídas ocurre solamente después de que el RST ha sido procesado y no durante las sesiones activas
- Verifique que el paquete descartado sea un ACK con el número de secuencia = FIN_Seq + 1 (respuesta obligatoria RFC 793)
- Verifique que ningún error de aplicación se corresponda con los eventos de descarte

---



Consejo: En el caso de referencia (SR 700468261), 54 de las 55 sesiones mostraron RST como el paquete final. Una sesión (puerto 55137) mostró que el ACK de FMC llegaba 0,024 ms después del RST, demostrando directamente el tiempo de condición de carrera.

Resolución

No es necesario remediar el problema. Este comportamiento es totalmente compatible con los estándares RFC de TCP y el diseño de firewall con estado. No hay ningún defecto, degradación del rendimiento o pérdida de datos.

Cuándo escalar

Advertencia: NO escalar basándose únicamente en este patrón de caída. Derivar sólo si se cumplen las condiciones de la sección siguiente.

- Las caídas se producen durante las sesiones activas, no después del intercambio RST o FIN/ACK
- Se observan fallos de aplicaciones, tiempos de espera de sesiones o inaccesibilidad de la GUI de FMC
- Descartar los aumentos de volumen con el tiempo sin un aumento correspondiente del volumen de conexión
- El patrón de descarte se desvía de la secuencia descrita en este artículo

Causa

Las caídas son el resultado de una condición de carrera en una escala temporal de microsegundos entre tres comportamientos correctos independientemente:

1. Optimización de pila TCP de Windows: Cuando una aplicación para Windows cierra un socket en el que el extremo remoto ya ha enviado FIN, Windows transmite un FIN-ACK inmediatamente. Esto es después del RST-ACK dentro de 15 - 31s para liberar instantáneamente la memoria y los bloques de control TCP.
2. Eliminación de conexión stateful FTD: Al recibir el paquete RST, el FTD elimina inmediatamente y purga la entrada de conexión de su tabla de estados (tabla conn) para mantener la integridad de la seguridad con estado.

3. Cumplimiento de RFC 793 de FMC: Según las especificaciones RFC 793, la pila TCP de FMC genera un ACK que reconoce el FIN del cliente (secuencia $+ 1$). Debido a la programación del sistema y al retraso en la propagación, este ACK alcanza el FTD. 0,06 - 2,2 ms después de que el RST ya haya vaciado la conexión.

4. Evaluación de descarte de FTD: Dado que no existe ninguna conexión coincidente en la tabla de estados y que el paquete sólo tiene el indicador ACK (no un SYN), FTD lo evalúa en la lista de control de acceso (ACL). Sin un permiso explícito para las ACK fuera del estado, FTD descarta el paquete como acl-drop / tcp-not-syn.

Contenido relacionado

- RFC 793: protocolo de control de transmisión
- Motivo del descarte de ASP
- Referencia SR: 700468261 (Interna)

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).