Solucionar problemas de queda de tráfego de FMC de pacotes ACK obsoletos após a terminação de TCP

Contents

Problema

Este documento descreve por que o FTD registra com eventos acl-drop o tráfego de retorno do FMC para os sistemas cliente, especificamente os pacotes ACK que chegam depois que as conexões TCP já foram terminadas por pacotes RST do cliente. As quedas são um produto de uma condição de corrida de nível de microssegundo entre o comportamento da pilha TCP do Windows e a geração ACK compatível com RFC 793 dos FMCs. Nenhum impacto no serviço ocorre e nenhuma correção é necessária.


Note: Este é um comportamento esperado. Os eventos acl-drop são seguros para filtrar nos sistemas de monitoramento depois que esse padrão é confirmado.

Sintomas:

- Os registros de firewall FTD mostram eventos acl-drop para tráfego de retorno do FMC para sistemas cliente (JumpHost neste exemplo)
- Quedas ocorrem nas conexões da porta TCP 443 (HTTPS) entre o FMC e os sistemas cliente
- Os eventos aparecem em eventos unificados do FMC como pacotes bloqueados
- Códigos de razão de queda vistos em capturas: tcp-rstfin-ooo, tcp-not-syn, acl-drop
- Nenhum impacto real no serviço é observado, apesar dos descartes registrados

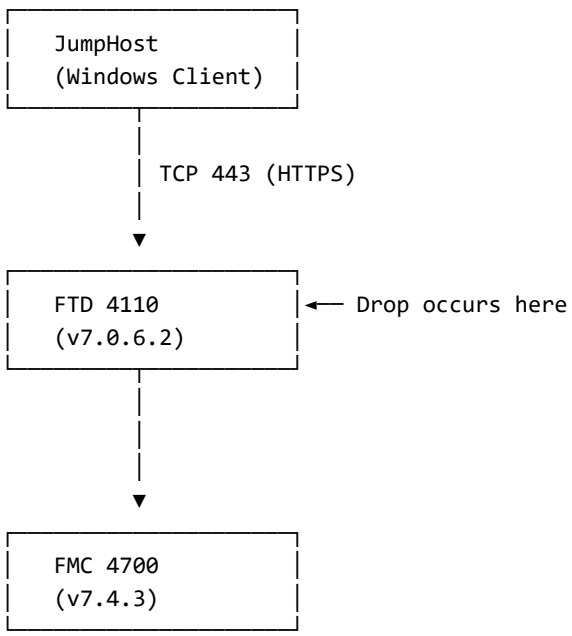
Ambiente

•Firewall: Cisco Secure Firewall Threat Defense (FTD) executando a versão 7.0.x, 7.2.x, 7.4.x ou posterior (FPR-1000/2100/3100/4100/4200/9300 ou FTDv)

· Centro de gerenciamento: Cisco Secure Firewall Management Center (FMC) 4600 / 4700 / FMCv executando a versão 7.2.x, 7.4.x ou posterior

· Sistema cliente: SO Windows (JumpHost, Estação de trabalho ou Servidor) conectando via navegador/API por HTTPS (TCP 443)

Topologia simples



Resolução

Sequência de pacotes

Esta sequência antecede consistentemente os descartes registrados:

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: As etapas 5 e 7 são o ponto de colisão. O RST provoca a remoção imediata do estado (Etapa 6) e o ACK obrigatório dos FMCs (Etapa 7) chega à janela entre a remoção do estado e o próximo ciclo de avaliação do pacote.

Metodologia de investigação do TAC

Use o próximo processo de correlação de três camadas ao investigar quedas ACK obsoletas suspeitas:

Etapa 1 — Coletar dados

- Capturas de pacotes FTD em quedas de entrada, saída e asp
- Despejo TCP do FMC filtrado na 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-
```

Etapa 2 — Extrair e correlacionar

· Extract 5-tuple from the asp drop capture exibe os drops e motivos (tcp-rstfin-ooo, tcp-not-syn, acl-drop)

· Reconstruir a tabela de estados de conexão usando capturas de ingresso e saída: identificar SYN, FIN/RST e os timestamps exatos

· Correlacionar o descarte, seu carimbo de data/hora nas capturas de ingresso/saída com o carimbo de data/hora de fim de vida da sessão

```
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: A sequência ACK do FMC confirma o número de sequência FIN $+ 1$, confirmando que é uma resposta RFC para uma conexão já terminada.

Etapa 3 — Confirmar padrão

- Confirme se os descartes ocorrem somente depois que o RST tiver sido processado e não durante as sessões ativas
- Verifique se o pacote descartado é um ACK com número de sequência = FIN_Seq + 1 (resposta obrigatória do RFC 793)
- Verifique se nenhuma falha de aplicativo corresponde aos eventos de queda

---


Tip: No caso de referência (SR 700468261), 54 das 55 sessões mostraram RST como o pacote final. Uma sessão (porta 55137) mostrou o ACK do FMC chegando 0,024ms após o RST, demonstrando diretamente o tempo da condição da corrida.

Resolução

Nenhuma correção é necessária. Esse comportamento é totalmente compatível com os padrões TCP RFC e o projeto de firewall stateful. Não há defeitos, degradação de desempenho ou perda de dados.

Quando encaminhar

---

aviso: NÃO escale com base apenas nesse padrão de queda. Escalonar somente se as condições na próxima seção forem atendidas.

- Quedas ocorrem durante as sessões ativas — não após a troca de RST ou FIN/ACK
- Falhas de aplicativos, tempos limite de sessão ou inacessibilidade da GUI do FMC são observados
- O volume de queda aumenta com o tempo sem um aumento correspondente no volume de conexão
- O padrão de queda se desvia da sequência descrita neste artigo

Causa

As quedas resultam de uma condição de corrida em uma escala de tempo de microssegundos entre três comportamentos independentemente corretos:

1. Otimização da pilha TCP do Windows: Quando um aplicativo do Windows fecha um soquete onde a extremidade remota já enviou FIN, o Windows transmite um FIN-ACK imediatamente. Isso ocorre após o RST-ACK dentro de 15 - 31s para liberar instantaneamente a memória e os blocos de controle TCP.
2. Remoção de conexão stateful de FTD: Ao receber o pacote RST, o FTD descarta imediatamente e elimina a entrada de conexão de sua tabela de estado (tabela conn) para manter a integridade da segurança stateful.
3. Conformidade com FMC RFC 793: De acordo com as especificações RFC 793, a pilha TCP

do FMC gera um ACK confirmando o FIN do cliente (Sequência $+ 1$). Devido à programação do sistema e ao atraso da propagação, este ACK chega ao FTD. 0,06 — 2,2 ms depois que o RST já tiver liberado a conexão.

4. Avaliação de Queda de FTD: Como não existe conexão correspondente na tabela de estados e o pacote tem apenas a flag ACK (não um SYN), o FTD a avalia em relação à ACL (Access Control List, Lista de controle de acesso). Sem uma permissão explícita para ACKs fora de estado, o FTD descarta o pacote como acl-drop / tcp-not-syn.

Conteúdo relacionado

- RFC 793 — Protocolo de controle de transmissão
- Motivo de Descarte do ASP
- Referência da SS: 700468261 (interno)

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.