Dépannage des abandons de trafic FMC Paquets ACK obsolètes après l'arrêt TCP

Table des matières

Problème

Ce document décrit pourquoi FTD consigne les événements acl-drop pour le trafic de retour de FMC vers les systèmes clients, en particulier les paquets ACK arrivant après que les connexions TCP ont déjà été terminées par des paquets RST du client. Les abandons sont le produit d'une condition de concurrence de microseconde entre le comportement de la pile TCP de Windows et la génération ACK conforme à la RFC 793 des FMC. Aucun impact sur le service ne se produit et aucune correction n'est requise.

Remarque : C’est un comportement attendu. Les événements acl-drop sont sûrs pour filtrer dans les systèmes de surveillance une fois que ce modèle est confirmé.

Symptômes :

- Les journaux de pare-feu FTD affichent les événements acl-drop pour le trafic de retour de FMC vers les systèmes clients (JumpHost dans cet exemple)
- Des abandons se produisent sur les connexions du port TCP 443 (HTTPS) entre FMC et les systèmes clients
- Les événements apparaissent dans les événements FMC unifiés comme des paquets bloqués
- Abandonner les codes raison visibles dans les captures : tcp-rstfin-ooo, tcp-not-syn, acl-drop
- Aucun impact réel sur le service n'est observé malgré les pertes enregistrées

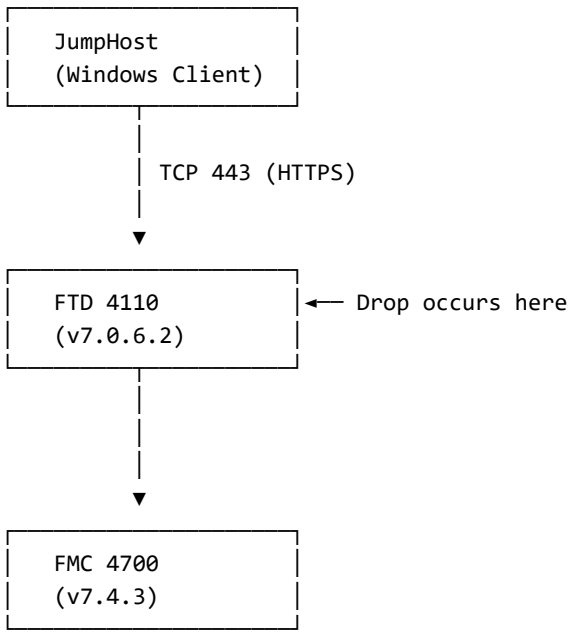
Environnement

· Pare-feu Cisco Secure Firewall Threat Defense (FTD) version 7.0.x, 7.2.x, 7.4.x ou ultérieure (FPR-1000/2100/3100/4100/4200/9300 ou FTDv)

· Centre de gestion : Cisco Secure Firewall Management Center (FMC) 4600 / 4700 / FMCv exécutant la version 7.2.x, 7.4.x ou ultérieure

· Système client : Système d'exploitation Windows (JumpHost, Workstation ou Server) avec connexion via navigateur/API via HTTPS (TCP 443)

Topologie simple



Résolution

Séquence de paquets

Cette séquence précède systématiquement les abandons consignés :

```
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



Remarque : Les étapes 5 et 7 représentent le point de collision. La RST entraîne la suppression immédiate de l'état (étape 6) et la réception obligatoire ACK des FMC (étape 7) arrive dans la fenêtre entre la suppression de l'état et le cycle d'évaluation de paquet suivant.

Méthodologie d'enquête TAC

Utilisez le processus de corrélation à trois niveaux suivant lorsque vous recherchez des pertes ACK suspectées d'être périmées :

Étape 1 : collecte des données

- Captures de paquets FTD en entrée, interfaces de sortie et points d'accès asp
- Vidage TCP depuis FMC filtré sur le 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-
```

Étape 2 — Extraction et corrélation

· Le tuple 5 extrait de la capture asp affiche les abandons et les raisons (tcp-rstfin-ooo, tcp-not-

syn, acl-drop)

· Reconstruisez la table d'état de connexion en utilisant les captures d'entrée et de sortie : identifier SYN, FIN/RST et les horodatages exacts

· Corrélez l'estampille de la perte, de son horodatage sur les captures d'entrée/de sortie avec l'horodatage de fin de vie de la session

```
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)
```


Remarque : La séquence ACK FMC accuse réception du numéro de séquence FIN $+ 1$, confirmant qu'il s'agit d'une réponse RFC à une connexion déjà interrompue.

Étape 3 — Confirmez le modèle

- Confirmer les abandons uniquement après le traitement de la RST et non pendant les sessions actives
- Vérifiez que le paquet abandonné est un ACK avec le numéro de séquence = FIN_Seq + 1 (réponse RFC 793 obligatoire)
- Vérifier qu'aucune défaillance d'application ne correspond aux événements de suppression

---


Conseil : Dans le cas de référence (SR 700468261), 54 sessions sur 55 ont montré RST comme paquet final. Une session (port 55137) a montré que l'ACK de FMC arrivait 0,024 ms après le RST, démontrant directement le timing de la condition de course.

Résolution

Aucune correction n'est requise. Ce comportement est entièrement conforme aux normes TCP RFC et à la conception de pare-feu avec état. Il n'y a aucun défaut, dégradation des performances

ou perte de données.

Quand transférer

Avertissement : Ne pas escalader en fonction de ce modèle de suppression seul. Transférer uniquement si les conditions de la section suivante sont remplies.

- Les abandons se produisent pendant les sessions actives, et non après l'échange RST ou FIN/ACK
- Des pannes d'application, des dépassements de délai de session ou une inaccessibilité de l'interface utilisateur FMC sont observés
- Le volume de chute augmente avec le temps sans augmentation correspondante du volume de connexion
- Le modèle de dépôt diffère de la séquence décrite dans cet article

Motif

Les chutes résultent d'une condition de course à l'échelle de la microseconde entre trois comportements corrects indépendamment :

1. Optimisation de la pile TCP Windows : Lorsqu'une application Windows ferme un socket où l'extrémité distante a déjà envoyé FIN, Windows transmet immédiatement un FIN-ACK. Ceci est après le RST-ACK dans les 15 - 31s pour libérer instantanément la mémoire et les blocs de contrôle TCP.
2. Suppression de la connexion dynamique FTD : À la réception du paquet RST, FTD désactive immédiatement et purge l'entrée de connexion de sa table d'état (table conn) pour maintenir l'intégrité de la sécurité avec état.
3. Conformité FMC RFC 793 : Selon les spécifications RFC 793, la pile TCP FMC génère un accusé de réception accusant réception du FIN du client (séquence $+ 1$). En raison de la planification du système et du délai de propagation, cet ACK atteint le FTD.
   0,06 — 2,2 ms après que la RST a déjà vidé la connexion.
4. Évaluation de la suppression FTD : Étant donné qu'aucune connexion correspondante

n'existe dans la table d'état et que le paquet possède uniquement l'indicateur ACK (et non un SYN), FTD l'évalue par rapport à la liste de contrôle d'accès (ACL). Sans autorisation explicite pour les ACK hors état, FTD abandonne le paquet comme acl-drop / tcp-not-syn.

Autres informations utiles

- RFC 793 - Protocole de contrôle de transmission
- Motif de rejet ASP
- Référence SR : 700468261 (interne)

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.