Dépannage de l'asymétrie de cluster FTD causant des échecs de connexion TCP

Problème

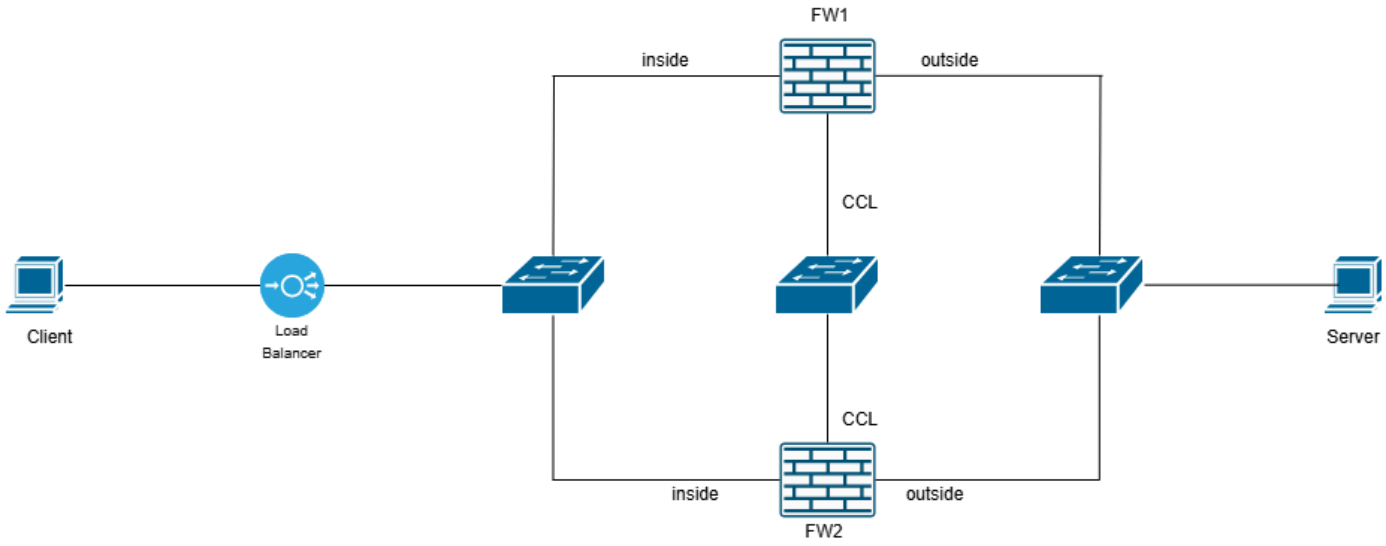
Un ou plusieurs de ces symptômes peuvent apparaître :

- Défaillances de connectivité intermittentes pour les applications traversant un cluster FTD.
- La connexion TCP en trois étapes échoue lors des tentatives de connexion.
- Le client envoie un paquet SYN, mais ne reçoit pas la réponse SYN-ACK attendue.
- Le client envoie un paquet RST après le SYN initial.

Environnement

- Première vue dans Secure Firewall Threat Defense 7.4 : d'autres versions peuvent également être affectées
- Configuration de cluster
- Équilibreur de charge dans le chemin du réseau : facultatif

Topologie



image_en_ligne_0.png

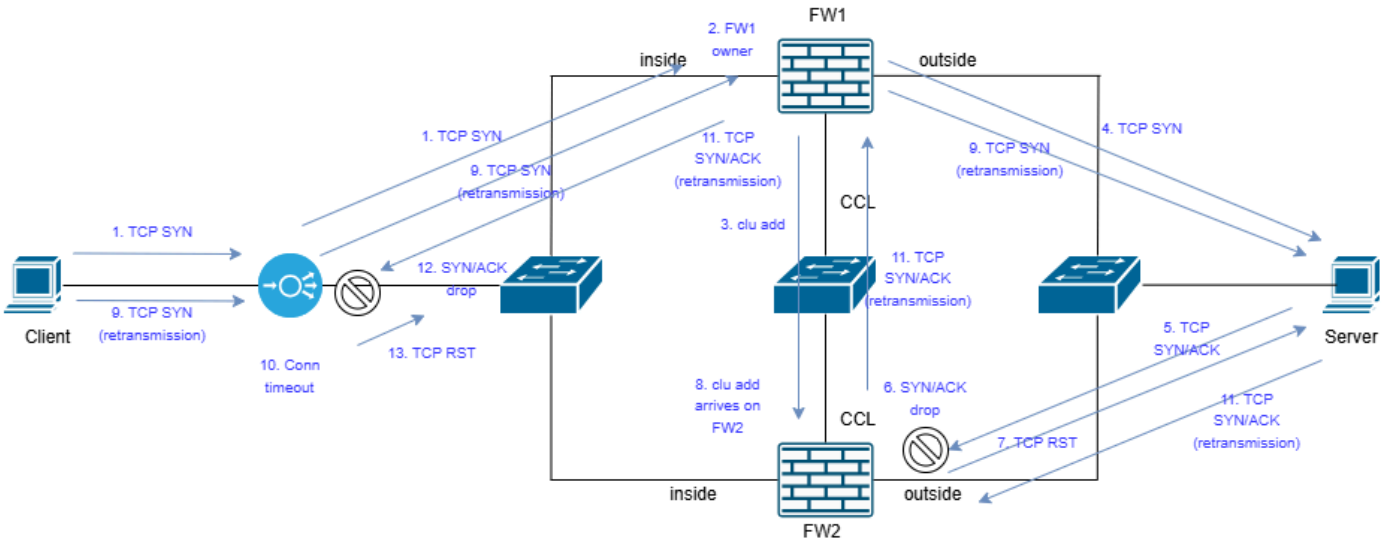
Résolution

Pour déterminer l'origine du problème, vous devez effectuer des captures simultanées à ces points :

- Interface interne FW1 (avec réinjection-masquage)
- Interface externe FW1 (avec reinject-hide)
- Interface de cluster FW1 (CCL)
- Interface interne FW2 (avec reinject-hide)
- Interface externe FW2 (avec reinject-hide)
- Interface de cluster FW2 (CCL)
- Client (ou le plus près possible du client)
- Serveur (ou aussi près que possible du serveur)

Pour plus d'informations sur la configuration de la vérification des captures : Comment activer les captures de cluster.

Les captures effectuées sur les deux pare-feu avec le client et le serveur révèlent cette topologie :



image_en_ligne_0.png

1. Le client envoie TCP SYN. Le paquet arrive à l'équilibreur de charge et est envoyé à FW1.

2. FW1 reçoit le paquet TCP SYN et devient le propriétaire du flux.

3. FW1 informe le directeur (FW2) du propriétaire du flux en envoyant un message de cluster spécial (ajout de cluster).

4. FW1 transfère le SYN TCP au serveur de destination.

Remarque : les étapes 3 et 4 n'ont pas d'ordre spécifique.

5. Le serveur répond avec SYN/ACK. Dans ce cas, nous avons un flux asymétrique puisque le SYN/ACK est envoyé vers FW2 en raison de l'algorithme d'équilibrage de charge du canal de port.

6. SYN/ACK arrive sur FW2 avant le message d'ajout de nuage. Il s'agit d'une condition de concurrence d'accès et elle est purement environnementale (telle que la latence dans CCL). Puisque FW2 ne sait pas qui est le propriétaire du flux, SYN/ACK est abandonné.

7. Un RST TCP est envoyé au serveur.

8. Le message d'ajout de nuage arrive sur FW2.

9. Le client retransmet le paquet TCP SYN. Le paquet TCP SYN est transféré au serveur de destination.

10. Sur le LB, la connexion TCP pour le flux spécifique expire.

11. Le serveur répond avec SYN/ACK (retransmission TCP). Le paquet SYN/ACK arrive sur FW2. Cette fois, FW2 connaît le propriétaire du flux depuis qu'il a reçu le message d'ajout de nuage et le paquet SYN/ACK est transféré au propriétaire du flux via la CCL. Le paquet SYN/ACK est envoyé au client.

12. L'agent de liaison ne connaît pas ce flux et abandonne le SYN/ACK. Par conséquent, le SYN/ACK n'arrive jamais sur le client.

13. L'équilibrage de charge contient un ou plusieurs paquets TCP RST.

Capture de pare-feu avec analyse de trace

Dans ces résultats, les captures ont été collectées à partir du pare-feu sur CCL et les interfaces orientées serveur.

· Sur CCL, la capture se fait sur le port UDP 4193.

· Sur les interfaces de données, la capture fait correspondre le trafic TCP entre les points d'extrémité à l'aide de l'option reinject-hide. La raison en est que nous voulons voir où les paquets arrivent réellement.

· Adresse IP 192.0.2.65 = client

· Adresse IP 192.0.2.6 = serveur

Étape 1 : Utilisez cette commande sur le périphérique pare-feu qui obtient le SYN/ACK pour voir quand le message clu add est arrivé. Dans le résultat CLI est message is show as Add flow.

```
firepower# show capture CCL decode

3 paquets capturés

   1: 08:14:20.630521 127.2.1.1.51475 > 127.2.2.1.4193 : udp 820

        Message ASP de cluster : expéditeur : 1, destinataire : 0
```

```
        Ajouter un flux : propriétaire 1, directeur 0, sauvegarde 0,

                ifc_in INSIDE(7020a7), ifc_out INSIDE(7020a7)

                TCP src 192.0.2.65/37468, dest 192.0.2.6/80
```

Étape 2 : Suivez le paquet SYN/ACK et concentrez-vous sur l'horodatage et le résultat du suivi :

```
firepower# show capture CAPI packet-number 1 trace

13 paquets capturés

   1: 08:14:20.628690 802.1Q vlan#200 P0 192.0.2.6.80 > 192.0.2.65.37468: S
2524735158:2524735158(0) ack 2881263901 win 65160 <mss 1460, sackOK, timestamp 611712900
970937593, nop, wscale 7>

Phase : 1

Type : CAPTURE

Sous-type :

Résultat : ALLOW

Temps écoulé : 1 708 ns

Config :

Informations complémentaires :

Liste d'accès MAC




Phase : 2

Type : ACCESS-LIST
```

Sous-type :

Résultat : ALLOW

Temps écoulé : 1 708 ns

Config :

Règle Implicite

Informations complémentaires :

Liste d'accès MAC

Phase : 3

Type : INPUT-ROUTE-LOOKUP

Sous-type : Résoudre l'interface de sortie

Résultat : ALLOW

Temps écoulé : 13664 ns

Config :

Informations complémentaires :

192.168.200.140 de tronçon suivant trouvé à l'aide de la commande de sortie ifc INSIDE(vrfid:0)

Phase : 4

Type : CLUSTER-EVENT

Sous-type :

Résultat : ALLOW

```
Temps écoulé : 16104 ns

Config :

Informations complémentaires :

Interface d'entrée : 'INSIDE'

Type de flux : NO FLOW

Je (0) deviens propriétaire

Phase : 5

Type : OBJECT_GROUP_SEARCH

Sous-type :

Résultat : ALLOW

Temps écoulé : 19520 ns

Config :

Informations complémentaires :

 Nombre de correspondances de groupe d'objets source : 0

 Nombre de correspondances NSG source : 0

 Nombre de correspondances NSG de destination : 0

 Nombre de recherches dans la table de classification : 1

 Nombre total de recherches : 1

 Nombre de paires de clés dupliquées : 0
```

Nombre de correspondances de la table de classification : 4

Phase : 6

Type : ACCESS-LIST

Sous-type :

Résultat : ALLOW

Temps écoulé : 366 ns

Config :

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit ip any rule-id 268436480

access-list CSM_FW_ACL_ remark rule-id 268436480 : POLITIQUE D'ACCÈS : mzafeiro_empty - Valeur par défaut

access-list CSM_FW_ACL_ remark rule-id 268436480 : L4 RULE : DEFAULT ACTION RULE

Informations complémentaires :

Ce paquet sera envoyé à snort pour un traitement supplémentaire où un verdict sera atteint

Phase : 7

Type : CONN-SETTINGS

Sous-type :

Résultat : ALLOW

Temps écoulé : 366 ns

Config :

class-map tcp

 match access-list tcp

policy-map global_policy

 class tcp

  set connection conn-max 0 embryonic-conn-max 0 random-sequence-number disable syn-cookie-mss 1380

service-policy global_policy global

Informations complémentaires :

Phase : 8

Type : NAT

Sous-type : par session

Résultat : ALLOW

Temps écoulé : 366 ns

Config :

Informations complémentaires :

Phase : 9

Type : IP-OPTIONS

Sous-type :

Résultat : ALLOW

Temps écoulé : 366 ns

Config :

Informations complémentaires :

Résultat :

input-interface : INSIDE(vrfid:0)

input-status : up

input-line-status : up

output-interface : INSIDE(vrfid:0)

output-status : actif

output-line-status : actif

Action : abandonner

Durée : 54168 ns

Raison de la suppression : (tcp-not-syn) Premier paquet TCP non SYN, emplacement de la suppression : frame snp_sp : 7459 flow (NA)/NA

Points clés

· Le message Add flow est arrivé à 08:14:20.630521 alors que le message SYN/ACK ~2 ms plus tôt à 08:14:20.628690. Il s’agit de la condition de concurrence.

· Le paquet SYN/ACK est abandonné par le pare-feu avec la raison tcp-not-syn ASP. Notez qu'au cours de la phase 4, le pare-feu a essayé d'identifier s'il y avait un propriétaire de flux connu mais n'en a trouvé aucun. Il a donc essayé de devenir un propriétaire de flux.

Ce résultat montre une trace du SYN/ACK quand le pare-feu connaît le flux :

```
firepower# show capture CAPI packet-number 3 trace

13 paquets capturés

   3: 08:14:21.629560 802.1Q vlan#200 P0 192.0.2.6.80 > 192.0.2.65.37468: S
2540375172:2540375172(0) ack 2881263901 win 65160 <mss 1460, sackOK, timestamp 611713901
970938595, nop, wscale 7>

Phase : 1

Type : CAPTURE

Sous-type :

Résultat : ALLOW

Temps écoulé : 1 708 ns

Config :

Informations complémentaires :

Liste d'accès MAC

Phase : 2

Type : ACCESS-LIST
```

Sous-type :

Résultat : ALLOW

Temps écoulé : 1 708 ns

Config :

Règle Implicite

Informations complémentaires :

Liste d'accès MAC

Phase : 3

Type : CLUSTER-EVENT

Sous-type :

Résultat : ALLOW

Temps écoulé : 3 416 ns

Config :

Informations complémentaires :

Interface d'entrée : 'INSIDE'

Type de flux : STUB

J'ai (0) un flux, un propriétaire valide (1).

Phase : 4

Type : CAPTURE

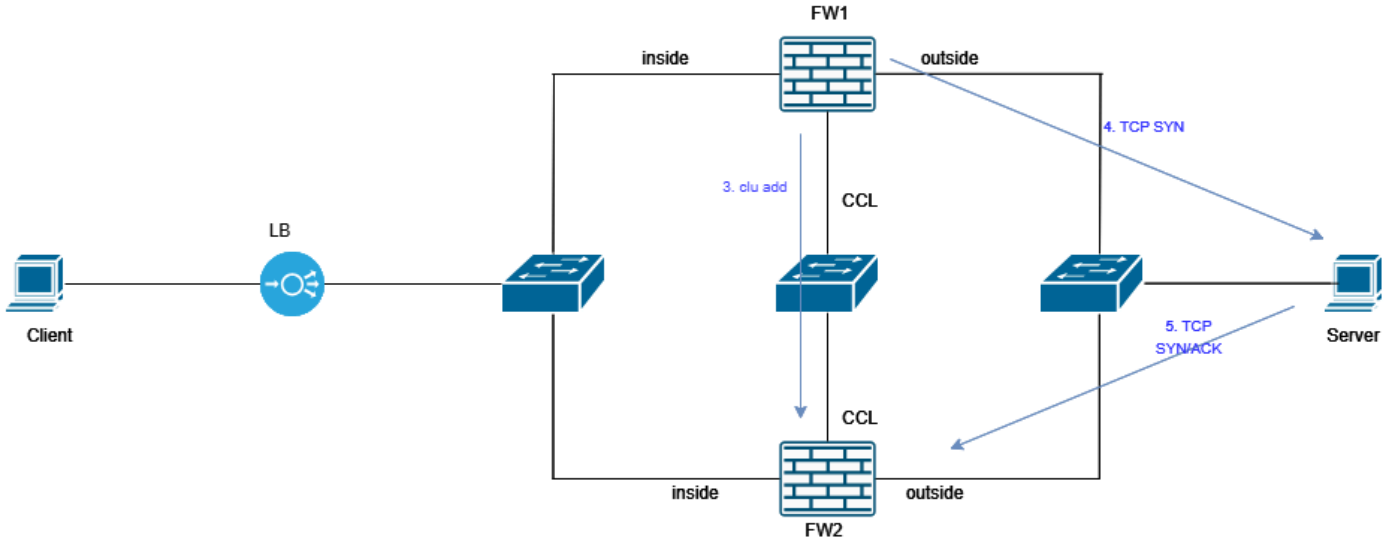
```
Sous-type :

Résultat : ALLOW

Temps écoulé : 7 808 ns

Config :

Informations complémentaires :

Liste d'accès MAC

Résultat :

input-interface : INSIDE(vrfid:0)

input-status : up

input-line-status : up

Action : autoriser

Durée : 14640 ns



1 paquet affiché

firepower#
```

Le point clé est dans la Phase 3. Le pare-feu sait que l'unité de cluster 1 est le propriétaire du flux. Vous pouvez utiliser la commande show cluster info pour voir quel périphérique est l'unité 0 et lequel est 1.

Foire aux questions

Q. Pourquoi des problèmes de connectivité TCP intermittents apparaissent-ils ?

R. Comme il s'agit d'une condition de course, elle se produit de façon aléatoire. La condition de course peut être visualisée en conséquence :

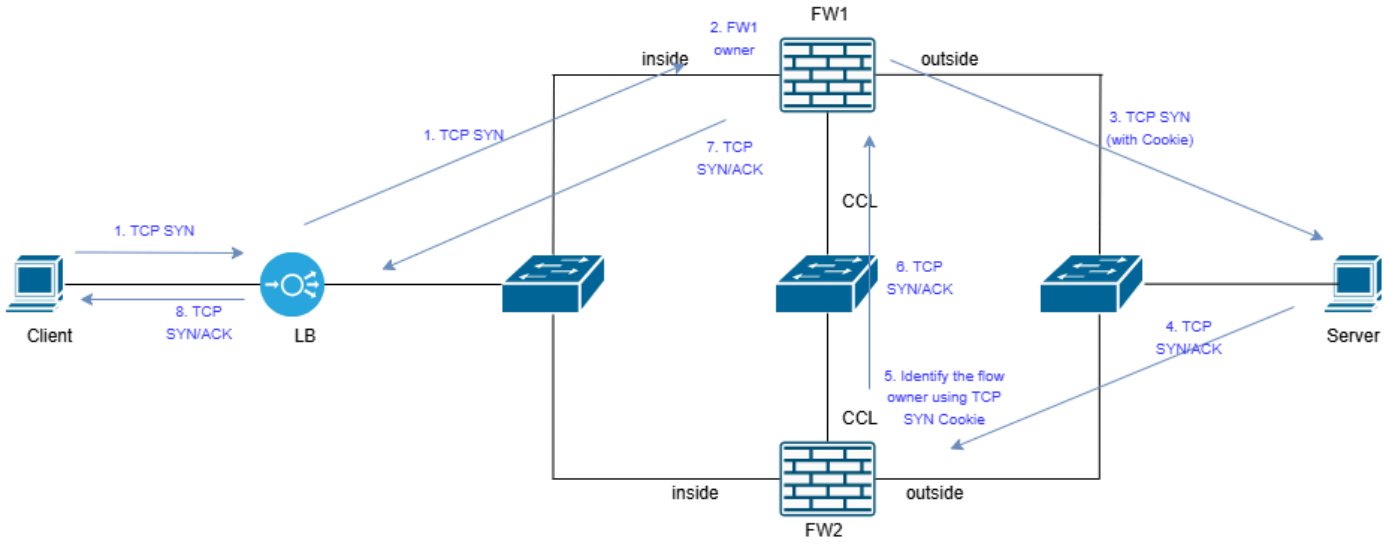


image_en_ligne_0.png

Q. Quelles sont les solutions possibles pour éviter la condition de course ?

A.

Solution 1 : activez la randomisation des numéros de séquence TCP pour tirer parti du mécanisme des cookies SYN TCP. Dans ce cas, la communication est structurée en conséquence :



image_inline_1.png

Solution 2 : supprimez l'asymétrie sur le réseau. Vous devez d'abord identifier la raison de l'asymétrie. Cela peut nécessiter le réglage de l'algorithme d'équilibrage de charge port-channel, le recâblage des câbles port-channel dans un ordre différent, entre autres.

Motif

La cause principale est une condition de concurrence d'accès due à une asymétrie de cluster dans le déploiement du cluster FTD. Les paquets SYN-ACK du serveur sont traités par un noeud de cluster FTD différent de celui qui a traité le paquet SYN initial, ce qui empêche l'établissement correct de la session TCP.

Autres informations utiles

- Assistance technique de Cisco et téléchargements

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.