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

Table des matières

Problème

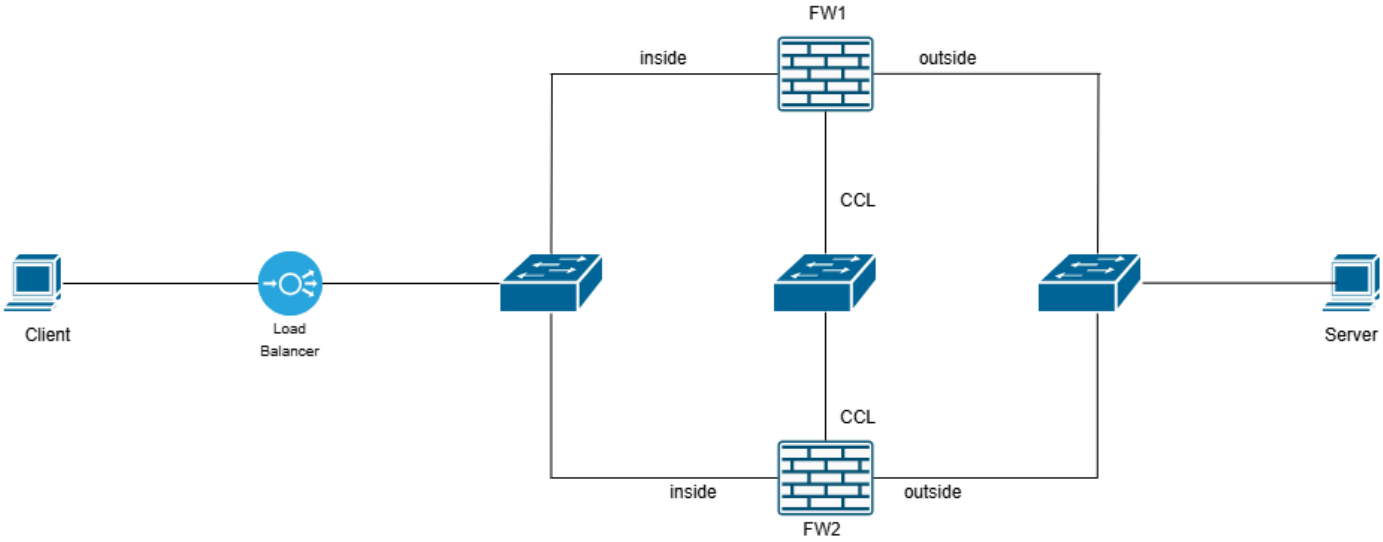
Un ou plusieurs de ces symptômes peuvent apparaître :

- Pannes 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

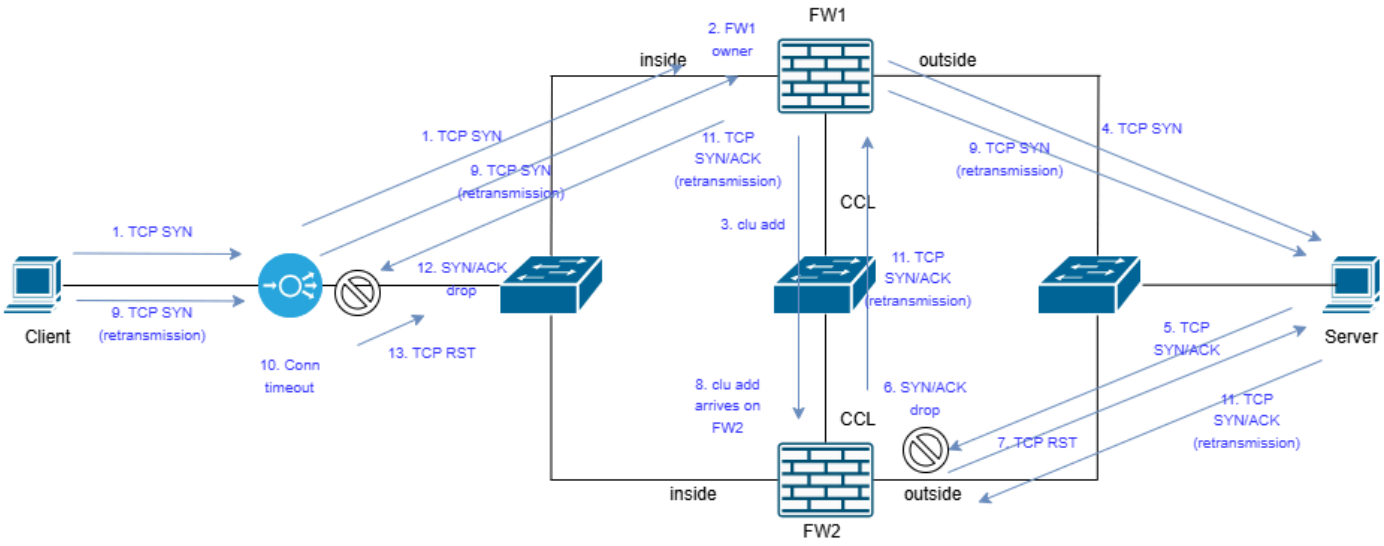
Résolution

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

- 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'apparaissent pas dans un 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.

<#root>

```
firepower#
```

show capture CCL decode

```
3 packets captured
   1: 08:14:20.630521       127.2.1.1.51475 > 127.2.2.1.4193:  udp 820
        Cluster ASP message: sender: 1, receiver: 0
        Add flow: owner 1, director 0, backup 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 :

<#root>

```
firepower#

 show capture CAPI packet-number 1 trace


13 packets captured
   1: 08:14:20.628690       802.1Q vlan#200 P0 192.0.2.6.80 > 192.0.2.65.37468: S 2524735158:2524735158
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 1708 ns
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 1708 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 13664 ns
Config:
Additional Information:
Found next-hop 192.168.200.140 using egress ifc  INSIDE(vrfid:0)

Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Elapsed time: 16104 ns
Config:
Additional Information:
Input interface: 'INSIDE'
```

Flow type: NO FLOW

I (0) am becoming owner

```
Phase: 5
Type: OBJECT_GROUP_SEARCH
Subtype:
Result: ALLOW
Elapsed time: 19520 ns
Config:
Additional Information:
 Source object-group match count:          0
 Source NSG match count:                   0
 Destination NSG match count:              0
 Classify table lookup count:              1
 Total lookup count:                       1
 Duplicate key pair count:                 0
 Classify table match count:               4

Phase: 6
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 366 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268436480
access-list CSM_FW_ACL_ remark rule-id 268436480: ACCESS POLICY: mzafeiro_empty - Default
access-list CSM_FW_ACL_ remark rule-id 268436480: L4 RULE: DEFAULT ACTION RULE
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 7
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Elapsed time: 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
Additional Information:

Phase: 8
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 366 ns
Config:
Additional Information:

Phase: 9
Type: IP-OPTIONS
Subtype:
```

```
Result: ALLOW
Elapsed time: 366 ns
Config:
Additional Information:

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: INSIDE(vrfid:0)
output-status: up
output-line-status: up

Action: drop


Time Taken: 54168 ns

Drop-reason: (tcp-not-syn) First TCP packet not SYN, Drop-location: 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 :

<#root>

```
firepower#

show capture CAPI packet-number 3 trace



13 packets captured

   3: 08:14:21.629560       802.1Q vlan#200 P0 192.0.2.6.80 > 192.0.2.65.37468: S 2540375172:2540375172
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 1708 ns
```

```
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 1708 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Elapsed time: 3416 ns
Config:
Additional Information:
Input interface: 'INSIDE'
Flow type: STUB

I (0) have flow, valid owner (1).



Phase: 4
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 7808 ns
Config:
Additional Information:
MAC Access list

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
Action: allow
Time Taken: 14640 ns

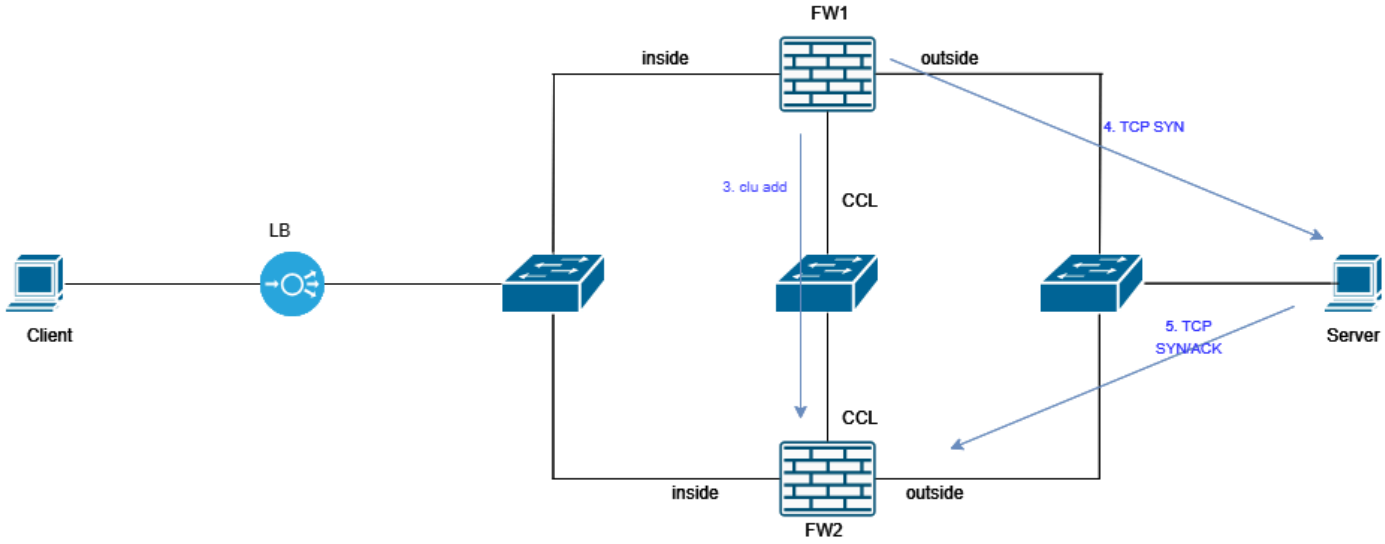
1 packet shown
firepower#
```

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 :

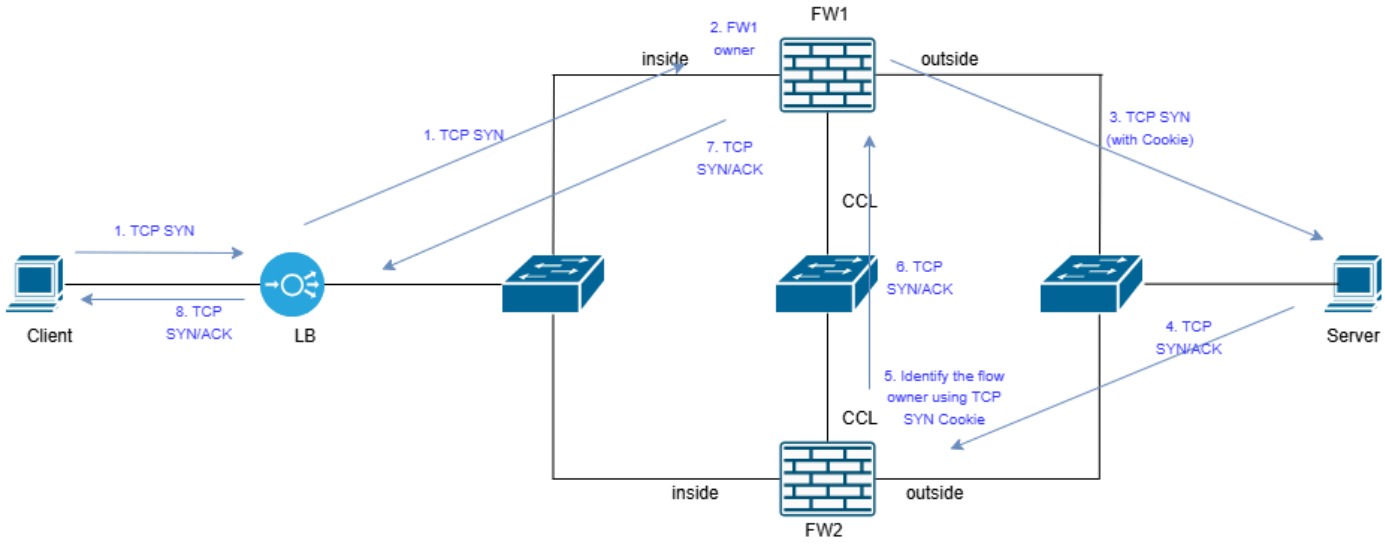


image_en_ligne_0.png

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.