Problemen met FTD-clusterasymmetrie oplossen die TCP-verbindingsfouten veroorzaken

uitgeven

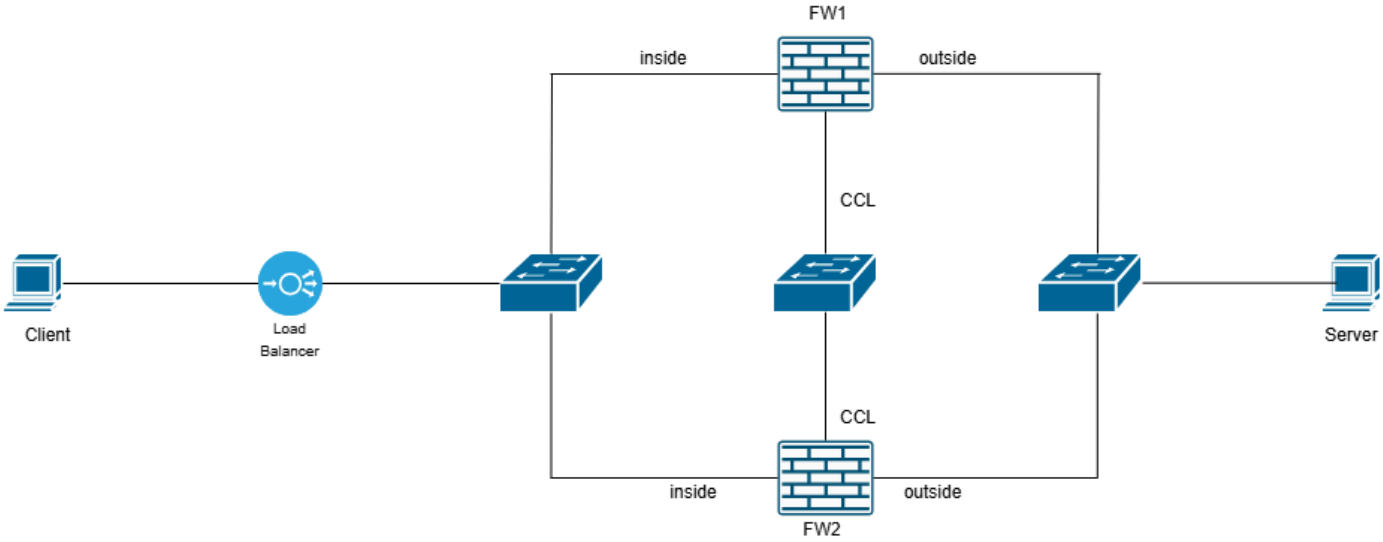
Een of meer van deze symptomen kunnen optreden:

- Intermitterende connectiviteitsfouten voor toepassingen die een FTD-cluster doorkruisen.
- TCP-handshake in drie richtingen mislukt tijdens verbindingspogingen.
- De client verzendt een SYN-pakket, maar ontvangt niet de verwachte SYN-ACK-respons.
- De client verzendt een RST-pakket na de eerste SYN.

milieu

- Voor het eerst gezien in Secure Firewall Threat Defense 7.4 - andere versies kunnen ook worden beïnvloed
- Clusterconfiguratie
- Load balancer in het netwerkpad — optioneel

Topologie



inline_image_0.png

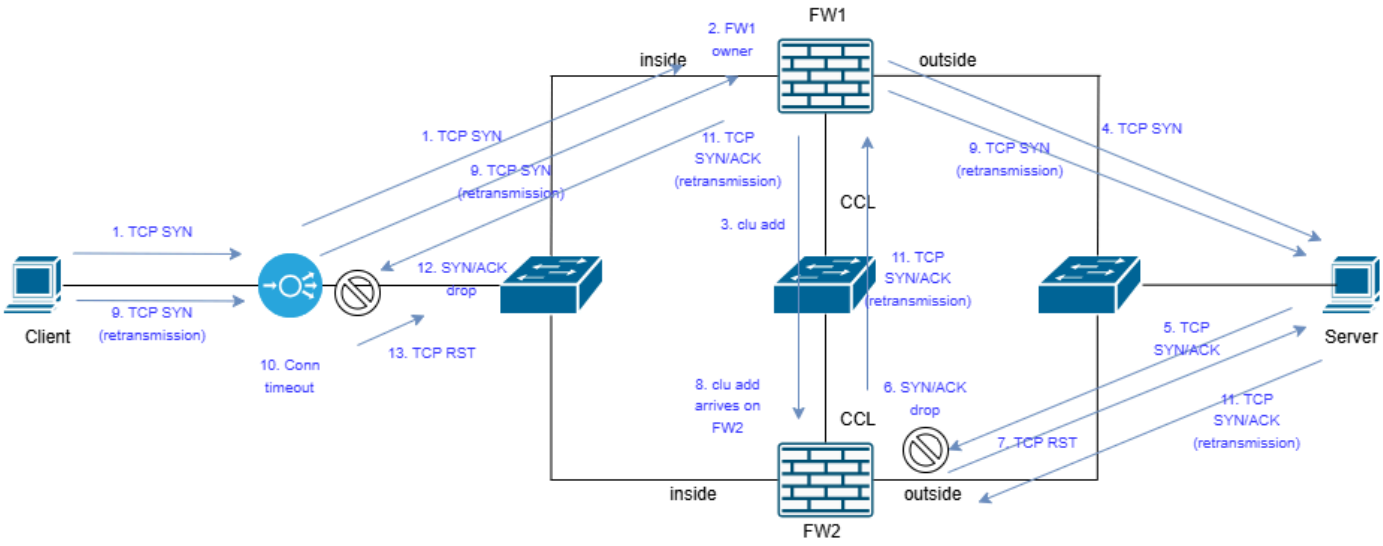
resolutie

Om het probleem bij de wortel te veroorzaken, moet u op deze punten tegelijkertijd vastleggen:

- FW1-binneninterface (met opnieuw injecteren-verbergen)
- FW1-buiteninterface (met opnieuw injecteren-verbergen)
- FW1-clusterinterface (CCL)
- FW2-binneninterface (met opnieuw injecteren-verbergen)
- FW2-buiteninterface (met opnieuw injecteren-verbergen)
- FW2-clusterinterface (CCL)
- De klant (of zo dicht mogelijk bij de klant)
- Server (of zo dicht mogelijk bij de server)

Voor meer informatie over het configureren van de vastgelegde bestanden, controleert u: [Hoe kunt u de vastgelegde clusters inschakelen.]

Opnamen die op beide firewalls samen met client en server zijn gemaakt, onthullen deze topologie:



inline_image_0.png

1. De client verzendt TCP SYN. Het pakket komt aan bij de load balancer (LB) en wordt verzonden naar FW1.

2. FW1 ontvangt het TCP SYN-pakket en wordt eigenaar van de stroom.

3. FW1 informeert de regisseur (FW2) over de eigenaar van de stroom door een speciaal (clu add) clusterbericht te verzenden.

4. FW1 stuurt het TCP-SYN door naar de bestemmingsserver.

Let op: stap 3 en 4 gebeuren in willekeurige volgorde.

5. De server antwoordt met SYN/ACK. In dit geval hebben we een asymmetrische stroom omdat de SYN / ACK naar FW2 wordt verzonden vanwege het algoritme voor load-balancing van het poortkanaal.

6. SYN/ACK arriveert op FW2 voordat het clu-bericht wordt toegevoegd. Dit is een raciale conditie en is puur omgevingsgebonden (zoals latentie in CCL). Aangezien FW2 niet weet wie de eigenaar van de stroom is, wordt de SYN/ACK verwijderd.

7. Er wordt een TCP RST naar de server verzonden.

8. Het clu-add-bericht komt binnen op FW2.

9. De client verzendt het TCP SYN-pakket opnieuw. Het TCP SYN-pakket wordt doorgestuurd naar de bestemmingsserver.

10. Op de LB, de TCP-verbinding voor de specifieke doorstroomtijden uit.

11. De server antwoordt met SYN/ACK (TCP-hertransmissie). Het SYN/ACK-pakket komt binnen op FW2. Deze keer weet FW2 van de eigenaar van de stroom, omdat deze het clu add-bericht heeft gekregen en de SYN / ACK wordt doorgestuurd naar de eigenaar van de stroom via de CCL. De SYN/ACK wordt naar de client verzonden.

12. De LB is niet op de hoogte van deze stroom en laat de SYN/ACK vallen. De SYN/ACK komt dus nooit aan bij de klant.

13. De LB één of meer TCP RST-pakketten.

Firewall vastleggen met sporenanalyse

In deze uitgangen werden opnames verzameld van de firewall op CCL en server-facing interfaces.

· Op CCL is de opname op de UDP 4193-poort.

· Op de data-interfaces komt het vastleggen overeen met TCP-verkeer tussen de eindpunten met behulp van de optie opnieuw injecteren-verbergen. De reden is dat we willen zien waar de pakketten daadwerkelijk aankomen.

· IP-adres 192.0.2.65 = client

· IP-adres 192.0.2.6 = server

Stap 1: Gebruik deze opdracht op het firewall-apparaat dat de SYN/ACK krijgt om te zien wanneer het clu-add-bericht is aangekomen. In de CLI-uitvoer wordt het bericht weergegeven als stroom toevoegen.

```
firepower# tonen vastleggen CCL-decodering

3 pakketten vastgelegd

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

        ASP-bericht cluster: afzender: 1, ontvanger: 0
```

```
        Flow toevoegen: eigenaar 1, directeur 0, back-up 0,

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

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

Stap 2: Traceer het SYN/ACK-pakket en focus op de tijdstempel en het traceresultaat:

```
firepower# toont CAPI-pakketnummer 1-tracering vastleggen

13 pakketten vastgelegd

   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>

Fase: 1

Type: CAPTURE

Subtype:

RESULTAAT: TOESTAAN

Verstreken tijd: 1708 ns

Config:

Aanvullende informatie:

MAC-toegangslijst



Fase: 2

Type: ACCESS-LIST
```

Subtype:

RESULTAAT: TOESTAAN

Verstreken tijd: 1708 ns

Config:

impliciete regel

Aanvullende informatie:

MAC-toegangslijst

Fase: 3

Type: INPUT-ROUTE-OPZOEKEN

Subtype: Uitgangs-interface oplossen

RESULTAAT: TOESTAAN

Verstreken tijd: 13664 ns

Config:

Aanvullende informatie:

Gevonden next-hop 192.168.200.140 met egress ifc INSIDE(vrfid:0)

Fase: 4

Type: CLUSTER-EVENT

Subtype:

RESULTAAT: TOESTAAN

```
Verstreken tijd: 16104 ns

Config:

Aanvullende informatie:

Invoerinterface: 'INSIDE'

Stroomtype: GEEN STROOM

Ik (0) ben eigenaar geworden

Fase: 5

Type: OBJECT_GROUP_SEARCH

Subtype:

RESULTAAT: TOESTAAN

Verstreken tijd: 19520 ns

Config:

Aanvullende informatie:

 Aantal overeenkomende bronobjecten-groepen: 0

 Bron NSG-matchtelling: 0

 Aantal NSG-matches op bestemming: 0

 Aantal opgezochte tabellen classificeren: 1

 Totaal aantal zoekopdrachten: 1

 Aantal dubbele sleutelparen: 0
```

Aantal overeenkomende tabellen classificeren: 4

Fase: 6

Type: ACCESS-LIST

Subtype:

RESULTAAT: TOESTAAN

Verstreken tijd: 366 ns

Config:

toegangsgroep CSM_FW_ACL_ global

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

toegangslijst CSM_FW_ACL_ opmerking regel-id 268436480: TOEGANGSBELEID: mazafeiro_empty - Standaard

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

Aanvullende informatie:

Dit pakket wordt verzonden naar snort voor aanvullende verwerking waar een vonnis zal worden bereikt

Fase: 7

Type: CONN-INSTELLINGEN

Subtype:

RESULTAAT: TOESTAAN

Verstreken tijd: 366 ns

Config:

Class-Map TCP

 Match Access-List TCP

policy-map_global_policy

 klasse-TCP

  Verbinding instellen Conn-max 0 Embryonic-Conn-Max 0 Random-Sequence-Number Syn-Cookie-MSS 1380 uitschakelen

service-policy_global_policy global

Aanvullende informatie:

Fase: 8

Type: NAT

Subtype: per sessie

RESULTAAT: TOESTAAN

Verstreken tijd: 366 ns

Config:

Aanvullende informatie:

Fase: 9

Type: IP-OPTIONS

Subtype:

RESULTAAT: TOESTAAN

Verstreken tijd: 366 ns

Config:

Aanvullende informatie:

Resultaat:

invoer-interface: INSIDE(vrfid:0)

Invoerstatus: omhoog

Invoerlijnstatus: omhoog

uitvoer-interface: INSIDE (vrfid:0)

uitvoerstatus: omhoog

uitvoerlijnstatus: omhoog

Actie: laten vallen

Tijd in beslag genomen: 54168 ns

Drop-reason: (tcp-not-syn) Eerste TCP-pakket niet SYN, Drop-location: frame snp_sp:7459 flow (NA)/NA

Belangrijkste punten

· Het bericht Add flow arriveerde om 08:14:20.630521 terwijl de SYN/ACK ~2 msec eerder om 08:14:20.628690 arriveerde. Dit is de conditie van het ras.

· Het SYN/ACK-pakket wordt door de firewall gedropt met tcp-not-syn ASP-reden. Merk op dat in fase 4 de firewall probeerde te identificeren of er een bekende eigenaar van de stroom was, maar er geen vond. Het probeerde een flow-eigenaar te worden.

Deze uitvoer toont een spoor van de SYN/ACK wanneer de firewall weet van de stroom:

```
firepower# toont CAPI-pakketnummer 3-tracering vastleggen

13 pakketten vastgelegd

   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>

Fase: 1

Type: CAPTURE

Subtype:

RESULTAAT: TOESTAAN

Verstreken tijd: 1708 ns

Config:

Aanvullende informatie:

MAC-toegangslijst

Fase: 2

Type: ACCESS-LIST
```

Subtype:

RESULTAAT: TOESTAAN

Verstreken tijd: 1708 ns

Config:

impliciete regel

Aanvullende informatie:

MAC-toegangslijst

Fase: 3

Type: CLUSTER-EVENT

Subtype:

RESULTAAT: TOESTAAN

Verstreken tijd: 3416 ns

Config:

Aanvullende informatie:

Invoerinterface: 'INSIDE'

Stroomtype: STUB

Ik (0) heb flow, geldige eigenaar (1).

Fase: 4

Type: CAPTURE

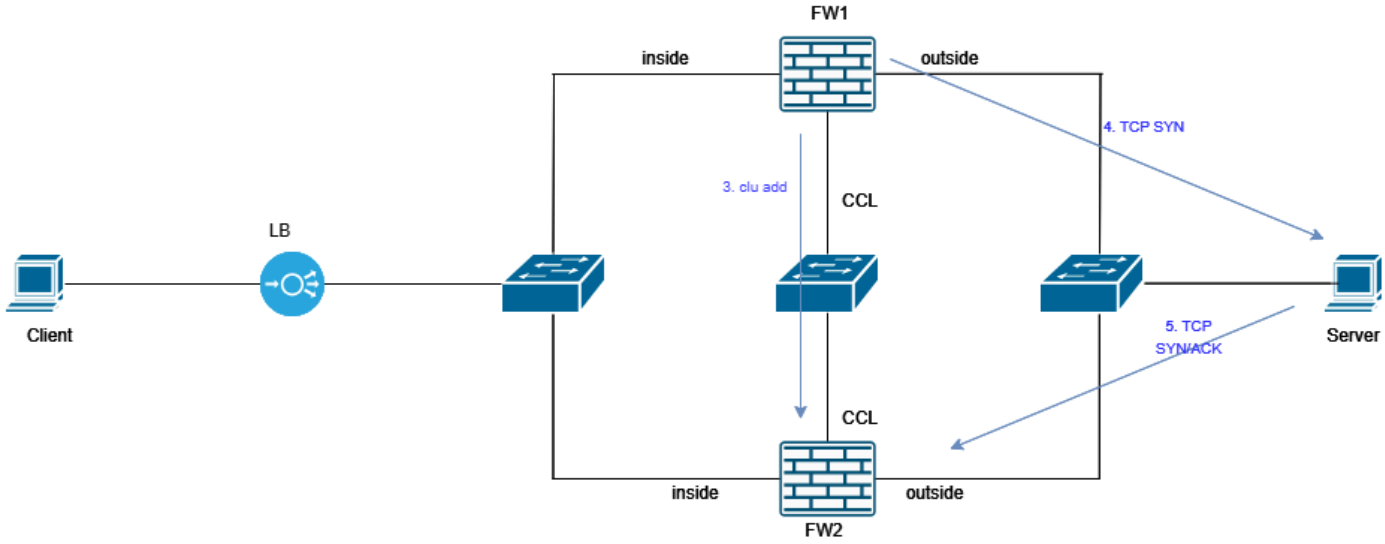
```
Subtype:

RESULTAAT: TOESTAAN

Verstreken tijd: 7808 ns

Config:

Aanvullende informatie:

MAC-toegangslijst

Resultaat:

invoer-interface: INSIDE(vrfid:0)

Invoerstatus: omhoog

Invoerlijnstatus: omhoog

Actie: toestaan

Tijd: 14640 ns



1 pakket weergegeven

Vuurkracht#
```

Het belangrijkste punt is fase 3. De firewall weet dat de clustereenheid 1 de eigenaar van de stroom is. U kunt de opdracht Clusterinfo weergeven gebruiken om te zien welk apparaat eenheid 0 is en welk apparaat eenheid 1 is.

Veelgestelde vragen

V. Waarom zien we intermitterende TCP-connectiviteitsproblemen?

A. Aangezien dit een racetoestand is, gebeurt dit willekeurig. De conditie van het ras kan dienovereenkomstig worden gevisualiseerd:

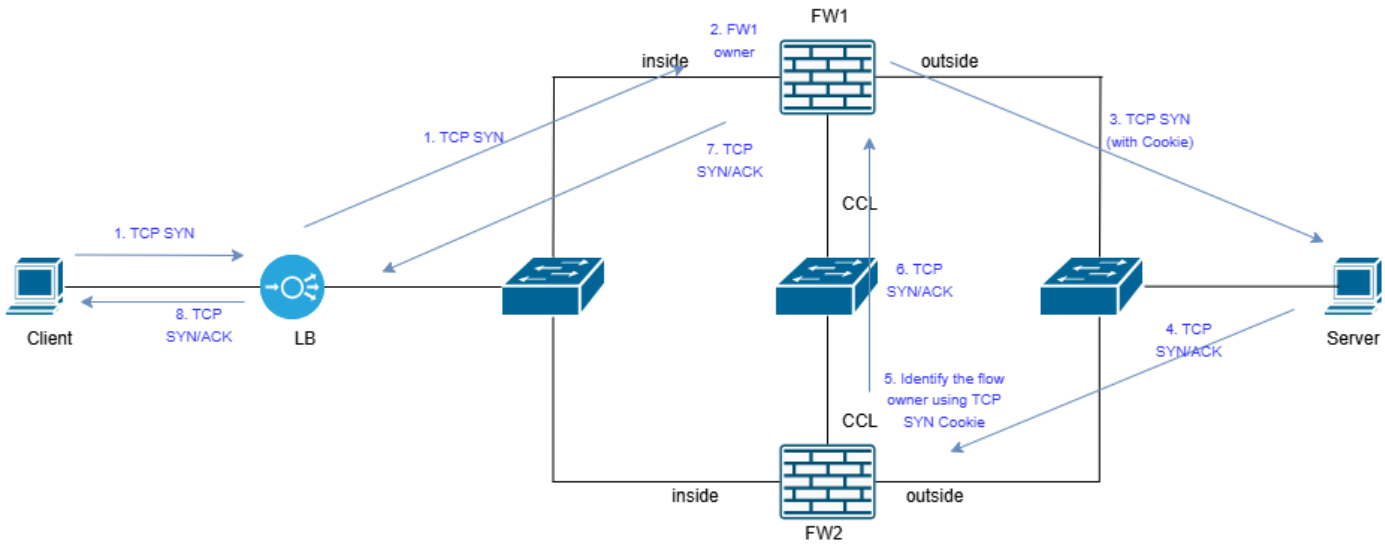


inline_image_0.png

V. Wat zijn mogelijke oplossingen om de race conditie te voorkomen?

A.

Oplossing 1: Schakel de TCP-volgnummerrandomisatie in om te profiteren van het TCP SYN-cookiemechanisme. In dat geval is de communicatie dienovereenkomstig gestructureerd:



inline_image_1.png

Oplossing 2: Elimineer de asymmetrie in het netwerk. Eerst moet je de oorzaak van de

asymmetrie achterhalen. Dit kan onder andere vereisen dat het algoritme voor de load-balancing van het poortkanaal wordt afgestemd, dat de kabels van het poortkanaal in verschillende volgorde worden herbekabeld.

Oorzaak

De hoofdoorzaak is een racetoestand die wordt veroorzaakt door clusterasymmetrie binnen de FTD-clusterimplementatie. De SYN-ACK-pakketten van de server worden verwerkt door een andere FTD-clusternode dan degene die het eerste SYN-pakket heeft verwerkt, waardoor de juiste instelling van TCP-sessies wordt voorkomen.

Verwante inhoud

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.