Risoluzione dei problemi di asimmetria cluster FTD che causano errori di connessione TCP

Problema

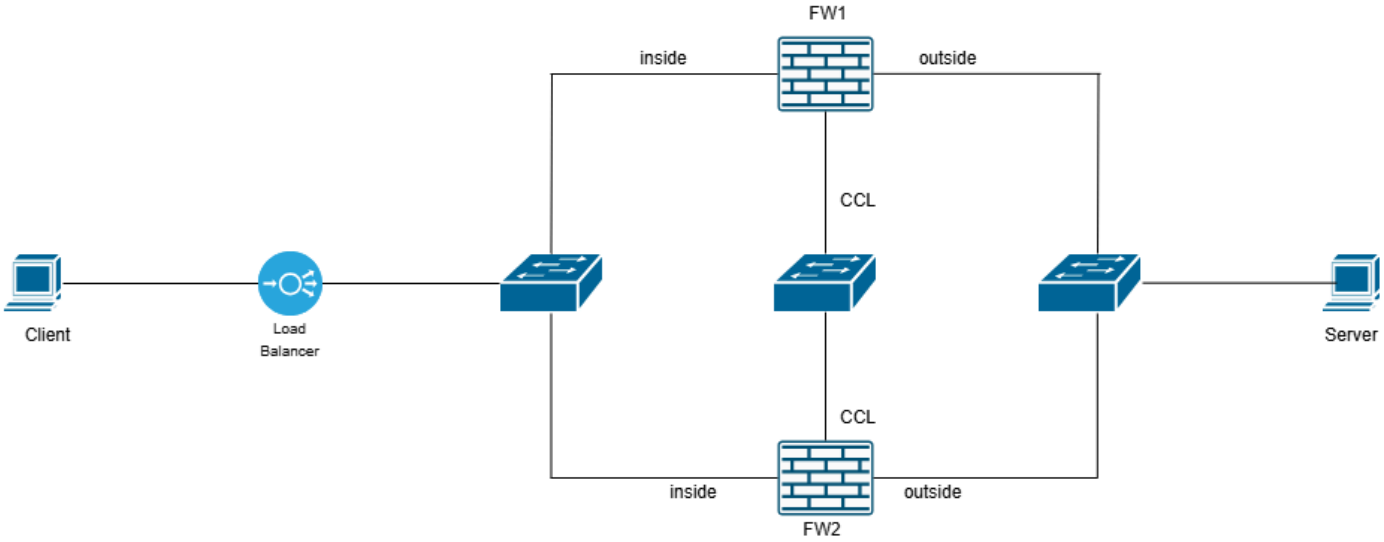
Possono presentarsi uno o più dei seguenti sintomi:

- Errori di connettività intermittenti per le applicazioni che attraversano un cluster FTD.
- Handshake a tre vie TCP non riuscito durante i tentativi di connessione.
- Il client invia un pacchetto SYN, ma non riceve la risposta SYN-ACK prevista.
- Il client invia un pacchetto RST dopo il SYN iniziale.

Ambiente

- Visualizzato per la prima volta in Secure Firewall Threat Defense 7.4 — il problema può riguardare anche altre versioni
- Configurazione cluster
- Bilanciamento del carico nel percorso di rete. Facoltativo

Topologia



inline_image_0.png

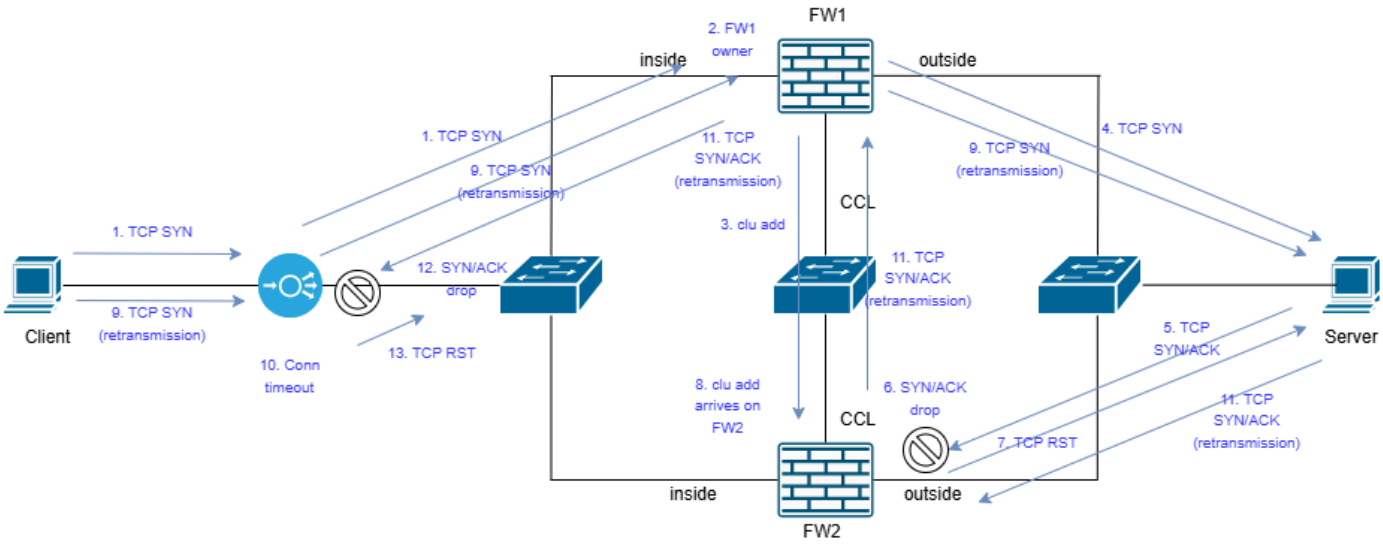
Risoluzione

Per individuare la causa del problema, è necessario eseguire acquisizioni simultanee nei seguenti punti:

- Interfaccia interna FW1 (con nascondiglio a reiezione)
- Interfaccia esterna FW1 (con nascondiglio di reiezione)
- FW1 Cluster Interface (CCL)
- Interfaccia interna FW2 (con nascondiglio a reiezione)
- Interfaccia esterna FW2 (con nascondiglio a reiezione)
- FW2 Cluster Interface (CCL)
- Client (o il più vicino possibile al client)
- Server (o il più vicino possibile al server)

Per i dettagli su come configurare le acquisizioni, controllare: Come abilitare le acquisizioni del cluster.

Le acquisizioni acquisite su entrambi i firewall insieme al client e al server rivelano questa topologia:



inline_image_0.png

1. Il client invia TCP SYN. Il pacchetto arriva al load balancer (LB) e viene inviato all'FW1.

2. FW1 riceve il pacchetto TCP SYN e diventa il proprietario del flusso.

3. FW1 informa il director (FW2) del proprietario del flusso inviando un messaggio speciale (clu add) del cluster.

4. FW1 inoltra il TCP SYN al server di destinazione.

Nota: i passi 3 e 4 non vengono eseguiti in un ordine specifico.

5. Il server risponde con SYN/ACK. In questo caso, il flusso è asimmetrico in quanto SYN/ACK viene inviato verso FW2 a causa dell'algoritmo di bilanciamento del carico del canale della porta.

6. SYN/ACK arriva su FW2 prima del messaggio clu add. Si tratta di una race condition ed è puramente ambientale (come la latenza in CCL). Poiché FW2 non sa chi sia il proprietario del flusso, SYN/ACK viene scartato.

7. Viene inviato TCP RST al server.

8. Il messaggio clu add arriva su FW2.

9. Il client ritrasmette il pacchetto TCP SYN. Il pacchetto TCP SYN viene inoltrato al server di destinazione.

10. Sul bilanciamento carico si verifica il timeout della connessione TCP per il flusso specifico.

11. Il server risponde con SYN/ACK (ritrasmissione TCP). Il pacchetto SYN/ACK arriva su FW2. Questa volta, FW2 conosce il proprietario del flusso dal momento che ha ricevuto il messaggio clu add e il SYN/ACK viene inoltrato al proprietario del flusso tramite CCL. Il SYN/ACK viene inviato al client.

12. Il bilanciamento carico non è a conoscenza di questo flusso e scarta il SYN/ACK. Pertanto, il SYN/ACK non arriva mai sul client.

13. Il bilanciamento del carico è costituito da uno o più pacchetti TCP RST.

Acquisizione del firewall con analisi della traccia

In questi output, le clip sono state raccolte dal firewall su CCL e interfacce rivolte al server.

· Su CCL, l'acquisizione avviene sulla porta UDP 4193.

· Sulle interfacce dati, l'acquisizione associa il traffico TCP tra gli endpoint utilizzando l'opzione reject-hide. Il motivo è che vogliamo vedere dove arrivano effettivamente i pacchetti.

· Indirizzo IP 192.0.2.65 = client

· Indirizzo IP 192.0.2.6 = server

Passaggio 1: utilizzare questo comando sul dispositivo firewall che ottiene il SYN/ACK per verificare quando è arrivato il messaggio clu add. Nell'output CLI il messaggio viene visualizzato come Add flow.

```
firepower# show capture decodifica CCL

3 pacchetti acquisiti

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

        Messaggio ASP del cluster: mittente: 1, destinatario: 0

        Aggiungi flusso: proprietario 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
```

Passaggio 2: Tracciare il pacchetto SYN/ACK e concentrarsi sul timestamp e sul risultato della traccia:

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

13 pacchetti acquisiti

   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

Tipo: ACQUISIZIONE

Sottotipo:

Risultato: ALLOW

Tempo trascorso: 1708 ns

Config:

Ulteriori informazioni:

Elenco accessi MAC




Fase: 2

Tipo: ACCESS-LIST

Sottotipo:

Risultato: ALLOW
```

Tempo trascorso: 1708 ns

Config:

Regola implicita

Ulteriori informazioni:

Elenco accessi MAC

Fase: 3

Tipo: RICERCA INPUT-ROUTE

Sottotipo: Interfaccia Resolve Egress

Risultato: ALLOW

Tempo trascorso: 1364 ns

Config:

Ulteriori informazioni:

Trovato l'hop successivo 192.168.200.140 che usa l'indirizzo ifc INSIDE(vrfid:0)

Fase: 4

Tipo: CLUSTER-EVENT

Sottotipo:

Risultato: ALLOW

Tempo trascorso: 16104 ns

Config:

Ulteriori informazioni:

Interfaccia di input: 'INSIDE'

Tipo di flusso: NESSUN FLUSSO

Sto (0) diventando proprietario

Fase: 5

Tipo: OBJECT_GROUP_SEARCH

Sottotipo:

Risultato: ALLOW

Tempo trascorso: 19520 ns

Config:

Ulteriori informazioni:

 Conteggio corrispondenze oggetto-gruppo di origine: 0

 Conteggio corrispondenze NSG di origine: 0

 Conteggio corrispondenze NSG di destinazione: 0

 Classifica conteggio ricerche tabella: 1

 Conteggio ricerche totali: 1

 Conteggio coppie di chiavi duplicate: 0

 Classifica conteggio corrispondenze tabella: 4

Fase: 6

Tipo: ACCESS-LIST

Sottotipo:

Risultato: ALLOW

Tempo trascorso: 366 ns

Config:

access-group CSM_FW_ACL_ globale

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

access-list CSM_FW_ACL_ note rule-id 268436480: CRITERI DI ACCESSO: mzafeiro_empty - Default

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

Ulteriori informazioni:

Questo pacchetto verrà inviato all'utente corrente per un'ulteriore elaborazione in caso di verdetto

Fase: 7

Tipo: CONN-SETTINGS

Sottotipo:

Risultato: ALLOW

Tempo trascorso: 366 ns

Config:

```
class-map tcp

 match access-list tcp

policy-map criteri_globali

 class tcp

  set connection conn-max 0 embrio-conn-max 0 numero di sequenza casuale disable syn-cookie-mss
1380

criteri-servizio globali_criteri_globali

Ulteriori informazioni:




Fase 8

Tipo: NAT

Sottotipo: per sessione

Risultato: ALLOW

Tempo trascorso: 366 ns

Config:

Ulteriori informazioni:




Fase 9

Tipo: OPZIONI IP
```

```
Sottotipo:

Risultato: ALLOW

Tempo trascorso: 366 ns

Config:

Ulteriori informazioni:



Risultato:

interfaccia di ingresso: INSIDE(vrfid:0)

input-status: attivo

stato della linea di ingresso: su

output-interface: INSIDE (vrfid:0)

stato-output: attivo

output-line-status: attivo

Azione: eliminare

Tempo impiegato: 54168 ns

Drop-reason: (tcp-not-syn) Primo pacchetto TCP non SYN, Drop-location: frame snp_sp:7459 flusso (NA)/NA
```

Punti chiave

· Il messaggio Add flow è arrivato alle 08:14:20.630521 mentre il SYN/ACK è arrivato circa 2 msec prima alle 08:14:20.628690. Questa è la condizione di gara.

· Il pacchetto SYN/ACK viene scartato dal firewall con il motivo ASP tcp-not-syn. Si noti che nella fase 4 il firewall ha tentato di identificare se esiste un proprietario del flusso noto ma non ne ha trovato alcuno. Pertanto, ha tentato di diventare un proprietario del flusso.

Questo output mostra una traccia del SYN/ACK quando il firewall è a conoscenza del flusso:

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

13 pacchetti acquisiti

   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

Tipo: ACQUISIZIONE

Sottotipo:

Risultato: ALLOW

Tempo trascorso: 1708 ns

Config:

Ulteriori informazioni:

Elenco accessi MAC

Fase: 2

Tipo: ACCESS-LIST

Sottotipo:

Risultato: ALLOW
```

Tempo trascorso: 1708 ns

Config:

Regola implicita

Ulteriori informazioni:

Elenco accessi MAC

Fase: 3

Tipo: CLUSTER-EVENT

Sottotipo:

Risultato: ALLOW

Tempo trascorso: 3416 ns

Config:

Ulteriori informazioni:

Interfaccia di input: 'INSIDE'

Tipo di flusso: STUB

I (0) hanno un flusso, un proprietario valido (1).

Fase: 4

Tipo: ACQUISIZIONE

Sottotipo:

Risultato: ALLOW

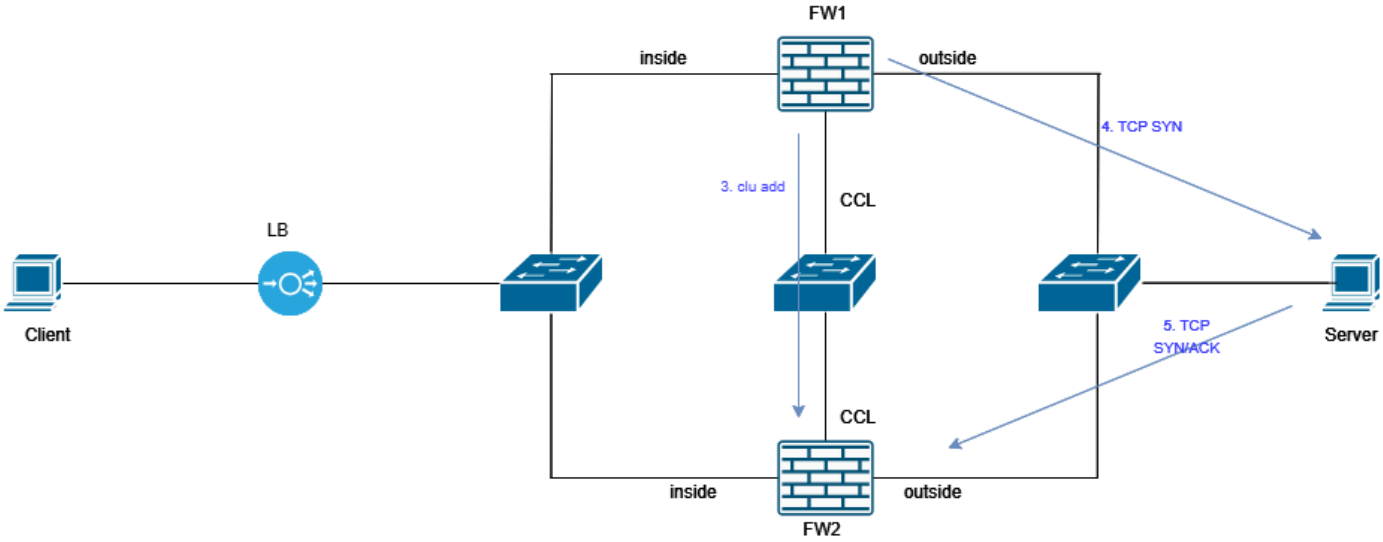
```
Tempo trascorso: 7808 ns

Config:

Ulteriori informazioni:

Elenco accessi MAC

Risultato:

interfaccia di ingresso: INSIDE(vrfid:0)

input-status: attivo

stato della linea di ingresso: su

Azione: consenti

Tempo impiegato: 14640 ns



1 pacchetto visualizzato

firepower#
```

Il punto chiave si trova nella Fase 3. Il firewall sa che l'unità cluster 1 è il proprietario del flusso. È possibile utilizzare il comando show cluster info per verificare quale dispositivo è l'unità 0 e quale è 1.

Domande frequenti

D. Perché vediamo problemi di connettività TCP intermittenti?

R. Poiché si tratta di una race condition, si verifica in modo casuale. La race condition può essere visualizzata di conseguenza:

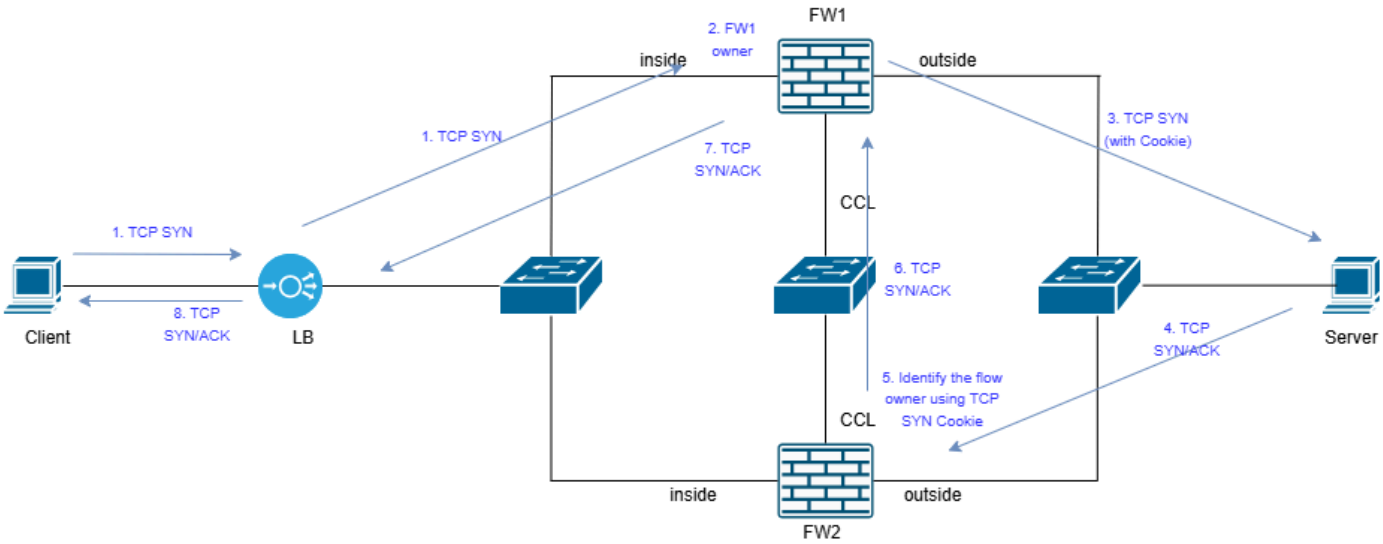


inline_image_0.png

D. Quali sono le possibili soluzioni per evitare la condizione di gara?

R.

Soluzione 1: abilitare la randomizzazione dei numeri di sequenza TCP per sfruttare il meccanismo dei cookie SYN di TCP. In tal caso, la comunicazione è strutturata in modo appropriato:



inline_image_1.png

Soluzione 2: eliminare l'asimmetria nella rete. Innanzitutto, è necessario identificare la causa dell'asimmetria. Può essere necessario regolare l'algoritmo di bilanciamento del carico del canale della porta, ricablare i cavi del canale della porta in un ordine diverso, tra le altre cose.

Causa

La causa principale è una race condition causata dall'asimmetria del cluster all'interno della distribuzione del cluster FTD. I pacchetti SYN-ACK provenienti dal server vengono elaborati da un nodo cluster FTD diverso da quello che ha gestito il pacchetto SYN iniziale, impedendo la corretta definizione della sessione TCP.

Contenuto correlato

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).