排查導致TCP連線失敗的FTD群集不對稱問題

問題

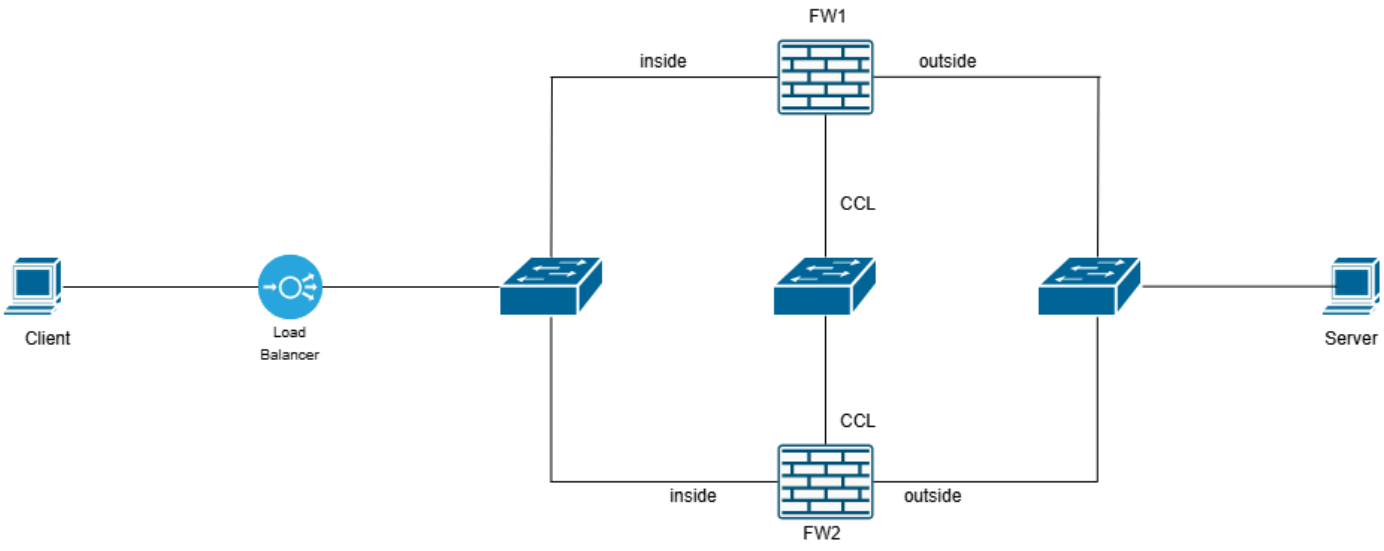
可能出現以下一個或多個症狀：

- 通過FTD集群的應用的間歇性連線故障。
- TCP三次握手在連線嘗試期間失敗。
- 客戶端傳送一個SYN資料包，但沒有收到預期的SYN-ACK響應。
- 使用者端在初始SYN之後傳送RST封包。

環境

- 首次見於安全防火牆威脅防禦7.4中 — 其他版本也可能受到影響
- 群集配置
- 網路路徑中的負載平衡器 — 這是可選的

拓撲



inline_image_0.png

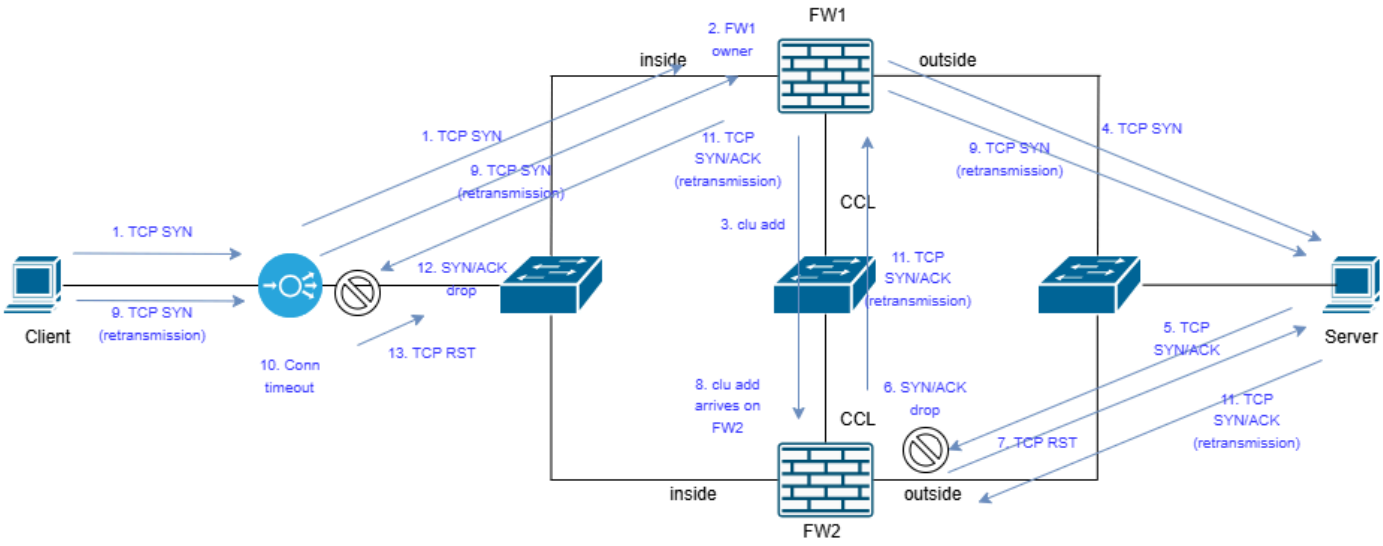
解析

要確定問題的根本原因，您需要在以下幾點執行同步捕獲：

- FW1內部介面（使用reinject-hide）
- FW1外部介面（使用reinject-hide）
- FW1叢集介面(CCL)
- FW2內部介面（使用reinject-hide）
- FW2外部介面（使用reinject-hide）
- FW2叢集介面(CCL)
- 客戶端（或儘可能靠近客戶端）
- 伺服器（或儘可能靠近伺服器）

有關如何配置捕獲檢查的詳細資訊：[如何啟用群集捕獲。]

在防火牆以及客戶端和伺服器上捕獲的捕獲顯示以下拓撲：



inline_image_0.png

1.客戶端傳送TCP SYN。資料包到達負載均衡器(LB)並傳送到FW1。

2. FW1收到TCP SYN資料包並成為流所有者。

3. FW1通過傳送特殊的(clu add)群集消息，將流所有者資訊通知導向器(FW2)。

4. FW1將TCP SYN轉發到目的伺服器。

注意：步驟3和4沒有特定的順序。

5.伺服器使用SYN/ACK進行應答。在這種情況下，由於埠通道負載均衡演算法，SYN/ACK被傳送到FW2，因此出現了非對稱流。

6. SYN/ACK在clu add消息之前到達FW2。這是一個競爭條件，純粹是環境性的（如CCL中的延遲）。由於FW2不知道流的所有者是誰，因此SYN/ACK被丟棄。

7.向伺服器傳送TCP RST。

8. clu add消息到達FW2。

9.客戶端重新傳輸TCP SYN資料包。TCP SYN資料包被轉發到目的伺服器。

10.在LB上，特定流量的TCP連線逾時。

11.伺服器以SYN/ACK（TCP重新傳輸）回覆。SYN/ACK資料包到達FW2。這一次，FW2知道流所有者，因為它收到clu add消息，並且SYN/ACK通過CCL轉發給流所有者。SYN/ACK被傳送到客戶端。

12. LB不知道此流量並捨棄SYN/ACK。因此，SYN/ACK永遠不會到達使用者端。

13. LB一個或多個TCP RST封包。

使用追蹤分析的防火牆擷取

在這些輸出中，捕獲是從防火牆的CCL和面向伺服器的介面上收集的。

·在CCL上，捕獲在UDP 4193埠上。

·在資料介面上，捕獲使用reinject-hide選項匹配端點之間的TCP流量。原因是我們希望檢視資料包實際到達的位置。

· IP地址192.0.2.65 =客戶端

· IP地址192.0.2.6 =伺服器

第1步：在獲得SYN/ACK的防火牆裝置上使用此命令檢視clu add消息到達的時間。在CLI輸出中，消息顯示為Add flow。

```
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

        集群ASP消息：發件人：1，接收器：0

        新增流：所有者1、控制器0、備份0、

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

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

第2步：跟蹤SYN/ACK資料包並關注時間戳和跟蹤結果：

```
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(0)ack 2881263901 win 65160 <mss 1460,sackOK，timestamp 611712900
970937593,nop，wscale 7>

階段：1

型別：CAPTURE

Subtype:

Result: ALLOW
```

運行時間：1708納秒

Config:

Additional Information:

MAC Access list

階段：2

型別：ACCESS-LIST

Subtype:

Result: ALLOW

運行時間：1708納秒

Config:

Implicit Rule

Additional Information:

MAC Access list

階段：3

型別：INPUT-ROUTE-LOOKUP

Subtype：解析輸出介面

Result: ALLOW

運行時間：13664 ns

Config:

Additional Information:

使用輸出ifc INSIDE(vrfid:0)找到下一跳192.168.200.140

階段：4

型別：CLUSTER-EVENT

Subtype:

Result: ALLOW

運行時間：16104 ns

Config:

Additional Information:

輸入介面：「INSIDE」

流型別：無流

我(0)將成為所有者

階段：5

型別：OBJECT_GROUP_SEARCH

Subtype:

Result: ALLOW

運行時間：19520 ns

Config:

Additional Information:

源對象組匹配計數： 0

源NSG匹配計數：0

目標NSG匹配計數： 0

分類表查詢計數：1

總查詢計數：1

重複金鑰對計數： 0

分類表匹配計數：4

階段：6

型別：ACCESS-LIST

Subtype:

Result: ALLOW

運行時間：366納秒

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 - 預設

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

Additional Information:

此封包將傳送到snort以進行進一步的處理，在此過程中將得出判定結果

階段：7

型別：CONN-SETTINGS

Subtype:

Result: ALLOW

運行時間：366納秒

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:

階段：8

型別：NAT

Subtype：每個會話

Result: ALLOW

運行時間：366納秒

Config:

Additional Information:

階段：9

型別：IP-OPTIONS

Subtype:

Result: ALLOW

運行時間：366納秒

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

所用時間：54168 ns

Drop-reason:(tcp-not-syn)First TCP packet not SYN， Drop-location: frame snp_sp:7459 flow(NA)/NA

要點

· Add flow消息到達時間為08:14:20.630521，而SYN/ACK ~2毫秒之前的時間為08:14:20.628690。這是競爭條件。

·防火牆由於tcp-not-syn ASP原因丟棄了SYN/ACK資料包。請注意，在第4階段，防火牆嘗試識別是否有已知的流所有者，但沒有找到任何流所有者。因此，它嘗試成為流所有者。

此輸出顯示防火牆獲知流量時SYN/ACK的追蹤軌跡：

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(0)ack 2881263901 win 65160 <mss 1460,sackOK，timestamp 611713901 970938595,nop，wscale 7>

階段：1

型別：CAPTURE

Subtype:

Result: ALLOW

運行時間：1708納秒

Config:

Additional Information:

MAC Access list

階段：2

型別：ACCESS-LIST

Subtype:

Result: ALLOW

運行時間：1708納秒

Config:

Implicit Rule

Additional Information:

MAC Access list

階段：3

型別：CLUSTER-EVENT

Subtype:

Result: ALLOW

運行時間：3416納秒

Config:

Additional Information:

輸入介面：「INSIDE」

流型別：STUB

I(0)具有流，有效所有者(1)。

階段：4

型別：CAPTURE

Subtype:

Result: ALLOW

運行時間：7808納秒

Config:

Additional Information:

MAC Access list

Result:

input-interface: INSIDE(vrfid:0)

input-status:up

input-line-status: up

Action: allow

所用時間：14640 ns

1 packet shown

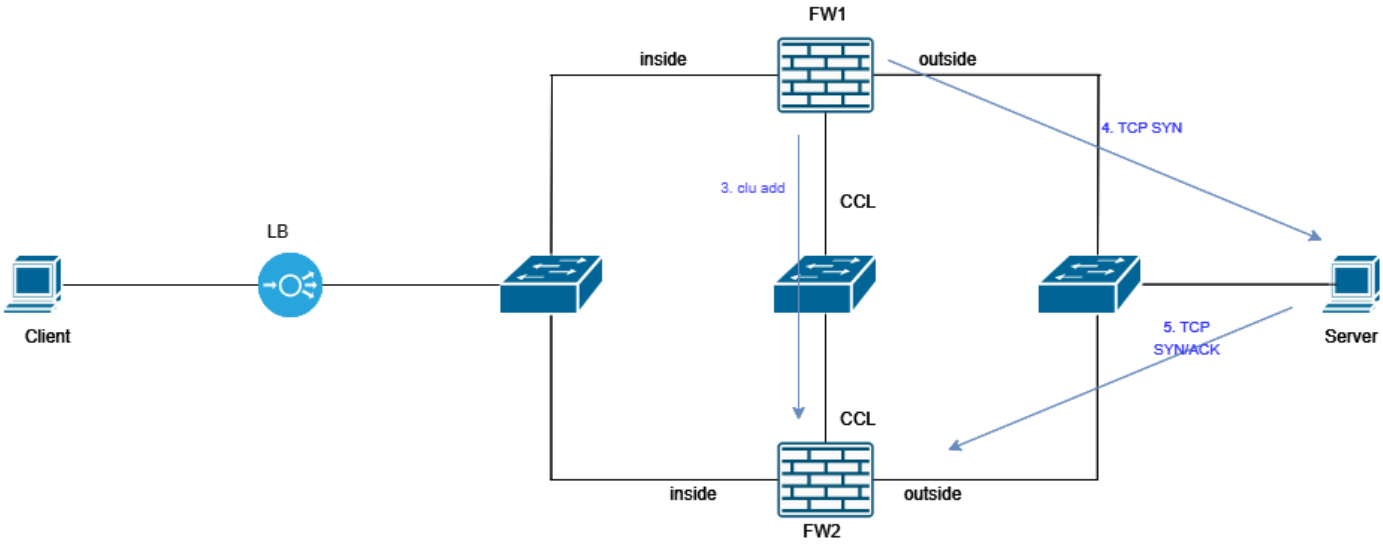
```
firepower#
```

關鍵點位於階段3。防火牆知道集群裝置1是流所有者。可以使用show cluster info命令檢視哪個裝置是裝置0，哪個是1。

常見問題

問：為什麼我們會看到間歇性的TCP連線問題？

A.由於這是一個競爭條件，因此是隨機發生的。競爭條件可以相應地視覺化：

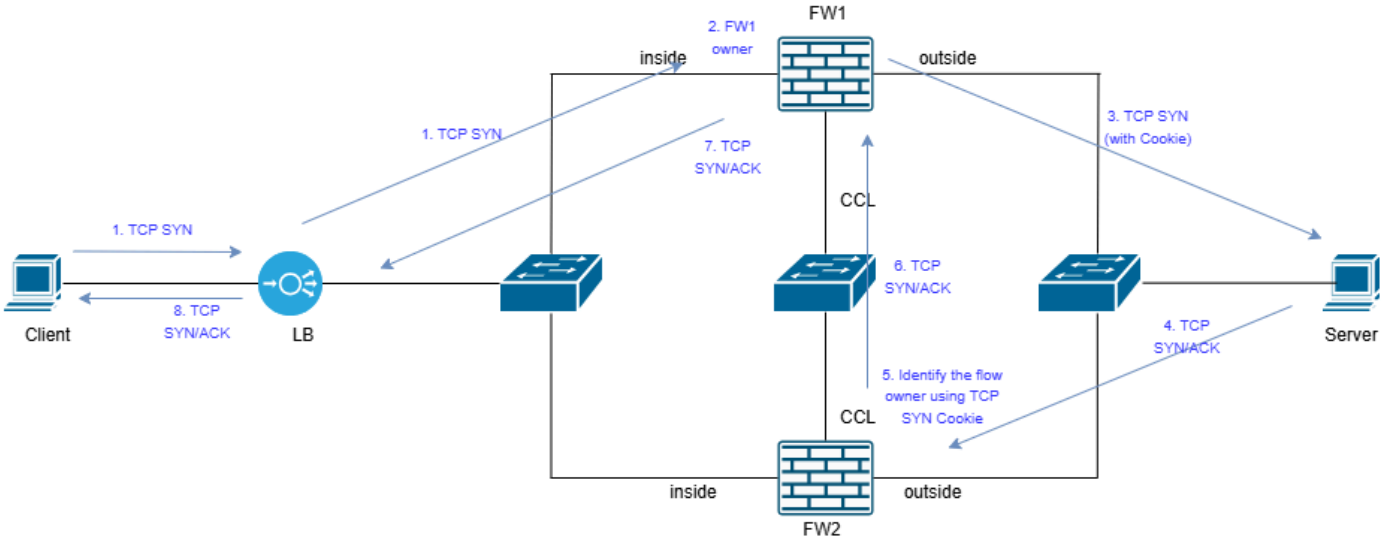


inline_image_0.png

避免這種種族情況的可能方案是什麼？

A.

解決方案1：啟用TCP序列號隨機化以利用TCP SYN Cookie機制。在這種情況下，通訊的結構如下：



inline_image_1.png

解決方案2：消除網路中的非對稱性。首先，您需要確定非對稱性的原因。這需要調整埠通道負載平衡演算法，按不同順序重新連線埠通道電纜等。

原因

根本原因是由於FTD集群部署中的集群非對稱性導致的競爭條件。來自伺服器的SYN-ACK資料包由與處理初始SYN資料包的FTD集群節點不同的節點處理，從而阻止了正確的TCP會話建立。

相關內容

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。