对导致TCP连接故障的FTD集群不对称问题进行故障排除

目录

问题

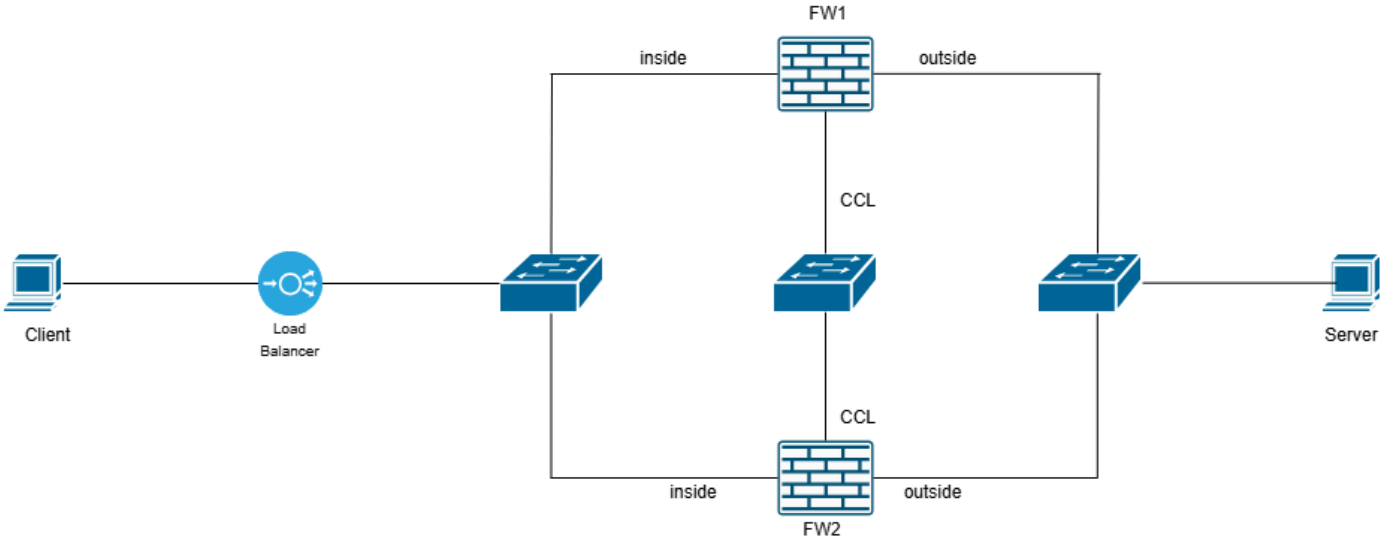
可能出现以下一个或多个症状：

- 通过FTD集群的应用间歇性连接故障
- TCP三次握手在连接尝试期间失败。
- 客户端发送SYN数据包，但是没有收到预期的SYN-ACK响应。
- 客户端在初始SYN后发送RST数据包。

环境

- 首次见于Secure Firewall Threat Defense 7.4 — 其他版本也可能受到影响
- 集群配置
- 网络路径中的负载均衡器 — 这是可选的

拓扑



inline_image_0.png

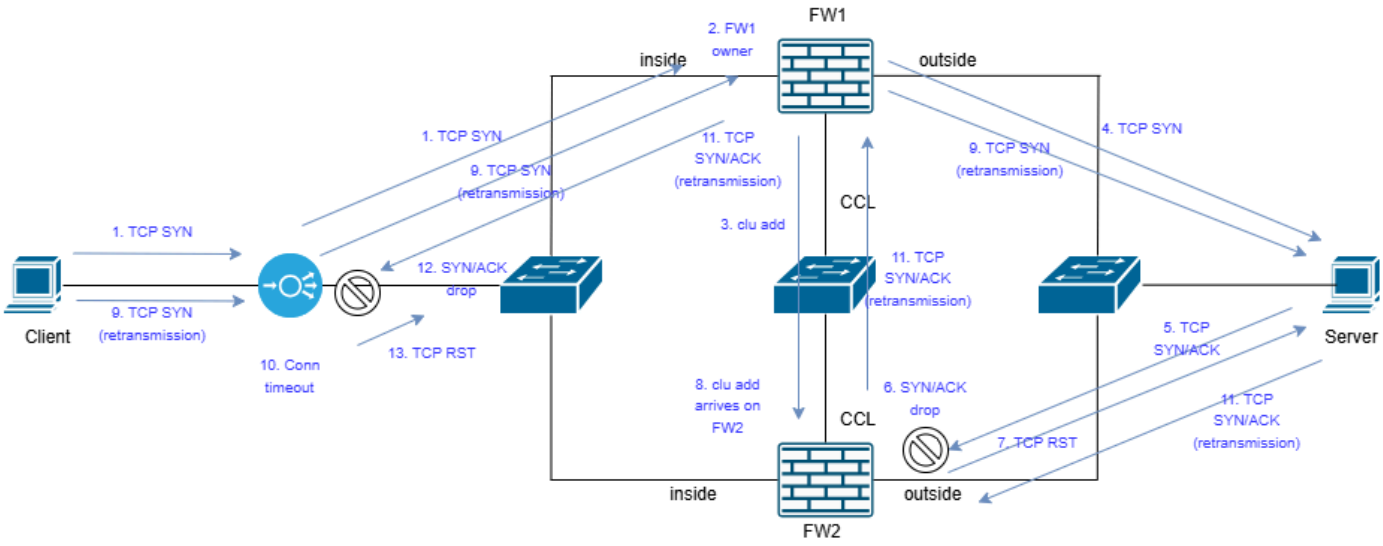
分辨率

要确定问题的根本原因，您需要在以下点同时捕获数据：

- FW1内部接口（带重定义 — 隐藏）
- FW1外部接口（使用重新隐藏）
- FW1集群接口(CCL)
- FW2内部接口（带重定义 — 隐藏）
- FW2外部接口（带重新创建 — 隐藏）
- FW2集群接口(CCL)
- 客户端（或尽可能靠近客户端）
- 服务器（或尽可能靠近服务器）

有关如何配置捕获检查的详细信息：[如何启用集群捕获。]

在防火墙以及客户端和服务器上捕获的捕获显示以下拓扑：



inline_image_0.png

1.客户端发送TCP SYN。数据包到达负载均衡器(LB)并发送到FW1。

2. FW1接收TCP SYN数据包并成为流所有者。

3. FW1通过发送特殊的(clu add)集群消息通知导向器(FW2)有关流所有者信息。

4. FW1将TCP SYN转发到目的服务器。

注意：第3步和第4步没有特定的顺序。

5.服务器以SYN/ACK进行应答。在这种情况下，由于端口通道负载均衡算法，SYN/ACK被发送到FW2，因此我们有一个非对称流。

6. SYN/ACK在clu add消息之前到达FW2。这是竞争条件，纯粹是环境性的（例如CCL中的延迟）。由于FW2不知道流的所有者，因此SYN/ACK被丢弃。

7.向服务器发送TCP RST。

8. clu add消息到达FW2。

9.客户端重新传输TCP SYN数据包。TCP SYN数据包被转发到目的服务器。

10.在LB上，特定流的TCP连接超时。

11.服务器回复SYN/ACK（TCP重新传输）。SYN/ACK数据包到达FW2。这次，FW2知道流所有者，因为它收到clu add消息，并且SYN/ACK通过CCL转发给流所有者。SYN/ACK被发送到客户端。

12. LB不知道此数据流并丢弃SYN/ACK。因此，SYN/ACK永远不会到达客户端。

13. LB一个或多个TCP RST数据包。

通过跟踪分析进行防火墙捕获

在这些输出中，从CCL和面向服务器的接口上的防火墙收集捕获信息：

·在CCL上，捕获在UDP 4193端口上。

·在数据接口上，捕获使用reinject-hide选项匹配终端之间的TCP流量。原因是我们要查看数据包实际到达的位置。

· IP地址192.0.2.65 =客户端

· IP地址192.0.2.6 =服务器

第1步：在获得SYN/ACK的防火墙设备上使用此命令查看clu add消息到达的时间。在CLI输出中，消息显示为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
```

第2步：跟踪SYN/ACK数据包并关注时间戳和跟踪结果：

<#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
```

要点

· Add flow消息到达08:14:20.630521，而SYN/ACK ~2毫秒之前到达08:14:20.628690。这是竞争条件。

·防火墙由于tcp-not-syn ASP原因丢弃了SYN/ACK数据包。请注意，在第4阶段，防火墙尝试识别是否有已知的流所有者，但未找到任何流所有者。因此，它尝试成为流所有者。

此输出显示当防火墙知道流时对SYN/ACK的跟踪：

<#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

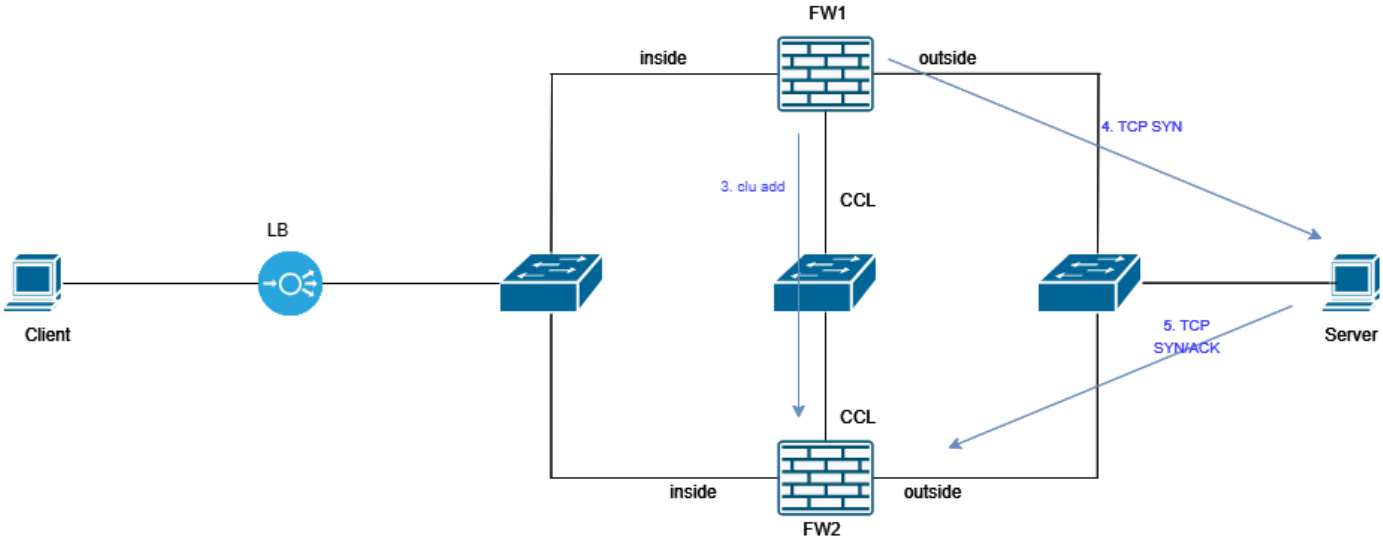
1 packet shown
firepower#
```

关键点位于阶段3。防火墙确定集群设备1是流所有者。您可以使用show cluster info命令查看哪个设备是设备0，哪个设备是1。

常见问题解答

问：为什么会出现间歇性的TCP连接问题？

答：由于这是竞争条件，因此是随机发生的。竞争条件可按以下方式可视化：

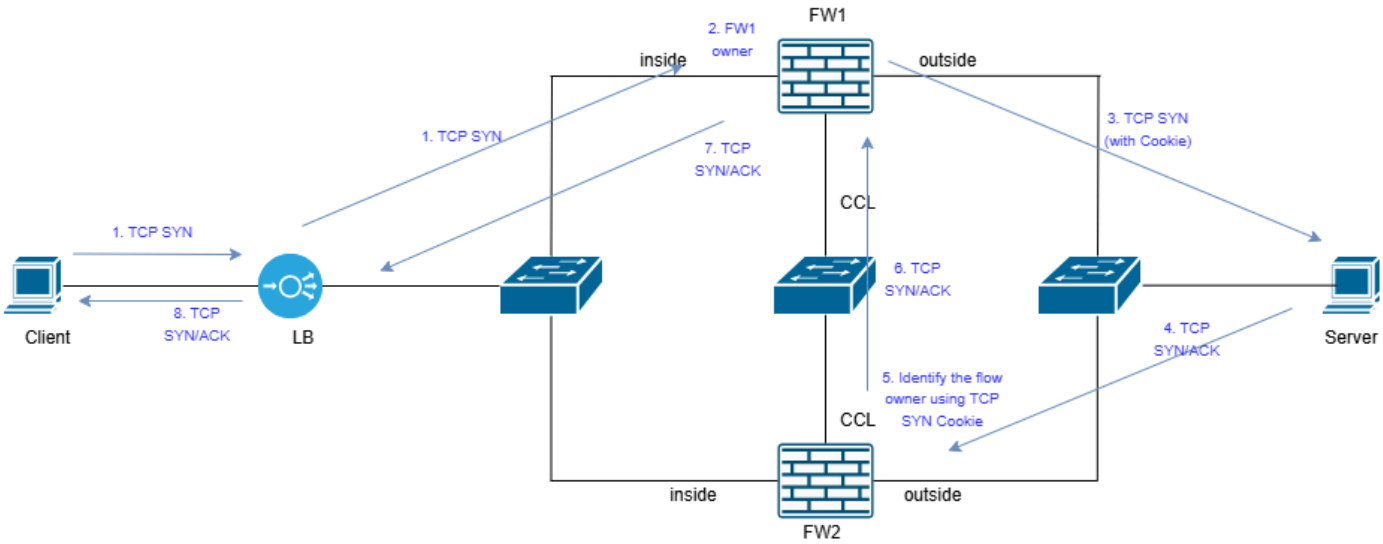


inline_image_0.png

能避免出现这种种族情况吗？

A.

解决方案1：启用TCP序列号随机化，以利用TCP SYN Cookie机制。在这种情况下，通信的结构如下：



inline_image_1.png

解决方案2：消除网络中的不对称。首先，您需要确定不对称的原因。这可能需要调整端口通道负载均衡算法，按不同顺序重新连接端口通道电缆等。

原因

根本原因是由于FTD集群部署中的集群不对称而导致出现竞争情况。来自服务器的SYN-ACK数据包由不同于处理初始SYN数据包的FTD集群节点进行处理，从而阻止正确建立TCP会话。

相关内容

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。