对导致TCP连接故障的FTD集群不对称问题进行故障排除

问题

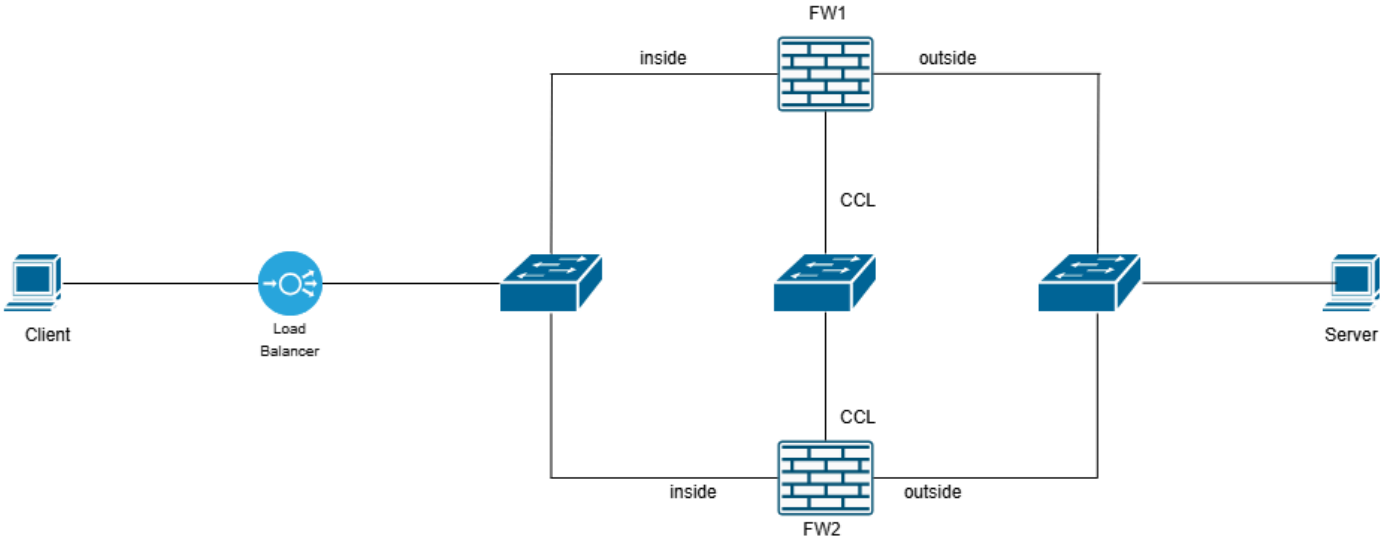
可能出现以下一个或多个症状：

- 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

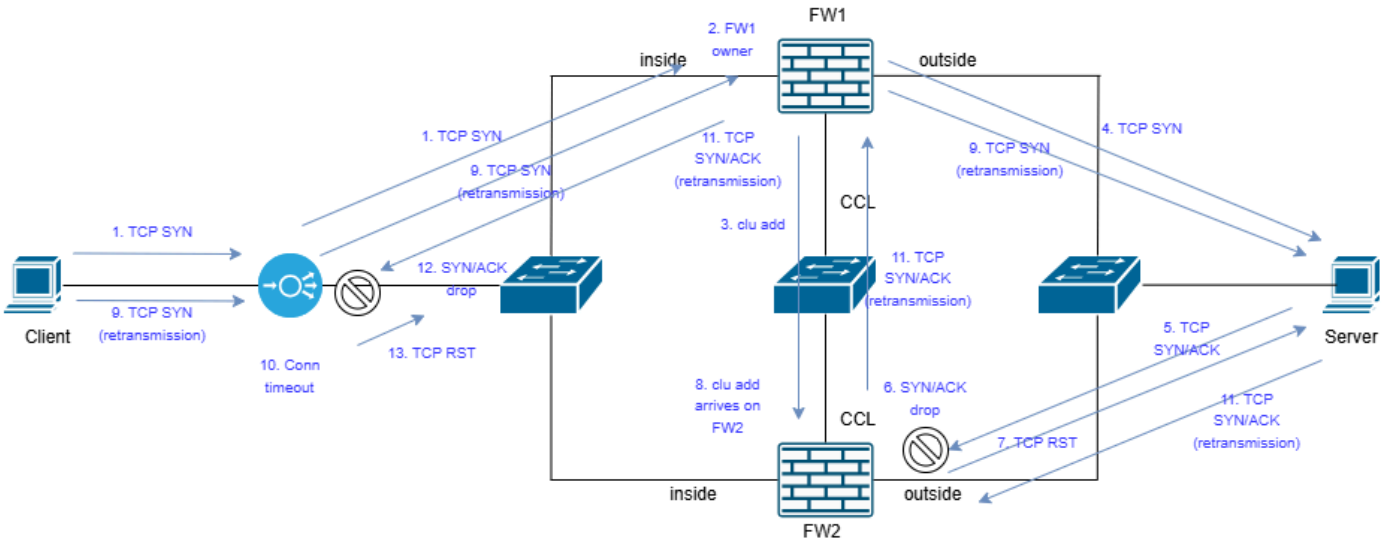
分辨率

为了从根本上解决问题，您需要在以下几点执行同时捕获：

- 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：步骤3和4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。

```
firepower# show capture CCL decode

捕获了3个数据包

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

        群集ASP消息：发件人：1，收件人：0

        添加流程：所有者1、指挥交换机0、备份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：跟踪SYN/ACK数据包并关注时间戳和跟踪结果：

firepower# show capture CAPI packet-number 1 trace

捕获了13个数据包

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>

阶段：1

类型：CAPTURE

子类型：

结果：允许

运行时间：1708纳秒

Config :

其它信息：

MAC访问列表

阶段：2

类型：ACCESS-LIST

子类型：

结果：允许

运行时间：1708纳秒

Config :

隐式规则

其它信息：

MAC访问列表

阶段：3

类型：INPUT-ROUTE-LOOKUP

子类型：解析出口接口

结果：允许

运行时间：13664 ns

Config :

其它信息：

使用出口ifc INSIDE(vrfid:0)找到下一跳192.168.200.140

阶段：4

类型：CLUSTER-EVENT

子类型：

结果：允许

运行时间：16104 ns

Config :

其它信息：

输入接口：“INSIDE”

流类型：无流

我(0)将成为所有者

阶段：5

类型：OBJECT_GROUP_SEARCH

子类型：

结果：允许

运行时间：19520 ns

Config :

其它信息：

源对象组匹配计数：0

源NSG匹配计数：0

目标NSG匹配计数：0

分类表查找计数：1

总查找计数：1

重复密钥对计数：0

分类表匹配计数：4

阶段：6

类型：ACCESS-LIST

子类型：

结果：允许

运行时间：366纳秒

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 - 默认

access-list CSM_FW_ACL_ remark rule-id 268436480: L4规则：默认操作规则

其它信息：

此数据包将发送到snort以进行其他处理，然后做出判定

阶段：7

类型：CONN-SETTINGS

子类型：

结果：允许

运行时间：366纳秒

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

其它信息：

阶段：8

类型：NAT

子类型：每个会话

结果：允许

运行时间：366纳秒

Config :

其它信息：

阶段：9

类型：IP选项

子类型：

结果：允许

运行时间：366纳秒

Config :

其它信息：

结果：

input-interface: INSIDE(vrfid:0)

input-status: up

input-line-status: up

output-interface:INSIDE(vrfid:0)

output-status: up

output-line-status: up

操作：丢弃

所用时间：54168 ns

丢弃原因：(tcp-not-syn)第一个TCP数据包不是SYN，丢弃位置：帧snp_sp:7459流量(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：

firepower# show capture CAPI packet-number 3 trace

捕获了13个数据包

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>

阶段：1

类型：CAPTURE

子类型：

结果：允许

运行时间：1708纳秒

Config :

其它信息：

MAC访问列表

阶段：2

类型：ACCESS-LIST

子类型：

结果：允许

运行时间：1708纳秒

Config :

隐式规则

其它信息：

MAC访问列表

阶段：3

类型：CLUSTER-EVENT

子类型：

结果：允许

运行时间：3416纳秒

Config ：

其它信息：

输入接口：“INSIDE”

流类型：STUB

I(0)具有流，有效所有者(1)。

阶段：4

类型：CAPTURE

子类型：

结果：允许

运行时间：7808纳秒

Config ：

其它信息：

MAC访问列表

结果：

input-interface: INSIDE(vrfid:0)

input-status: up

input-line-status: up

操作：允许

所用时间：14640 ns

1个数据包显示

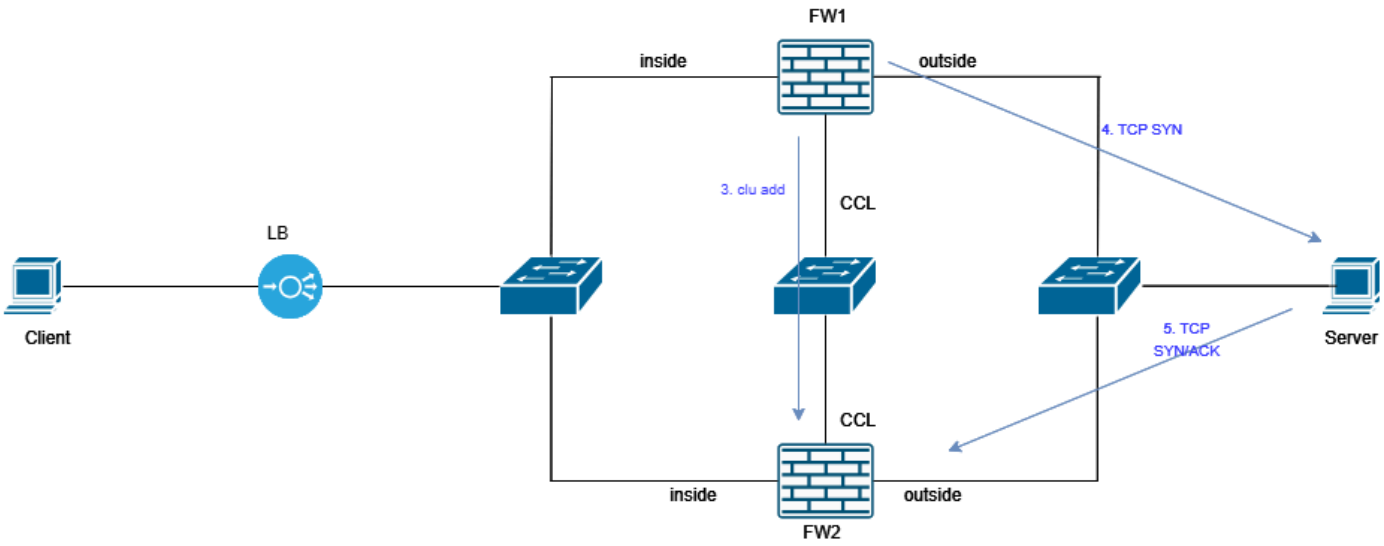
firepower#

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：

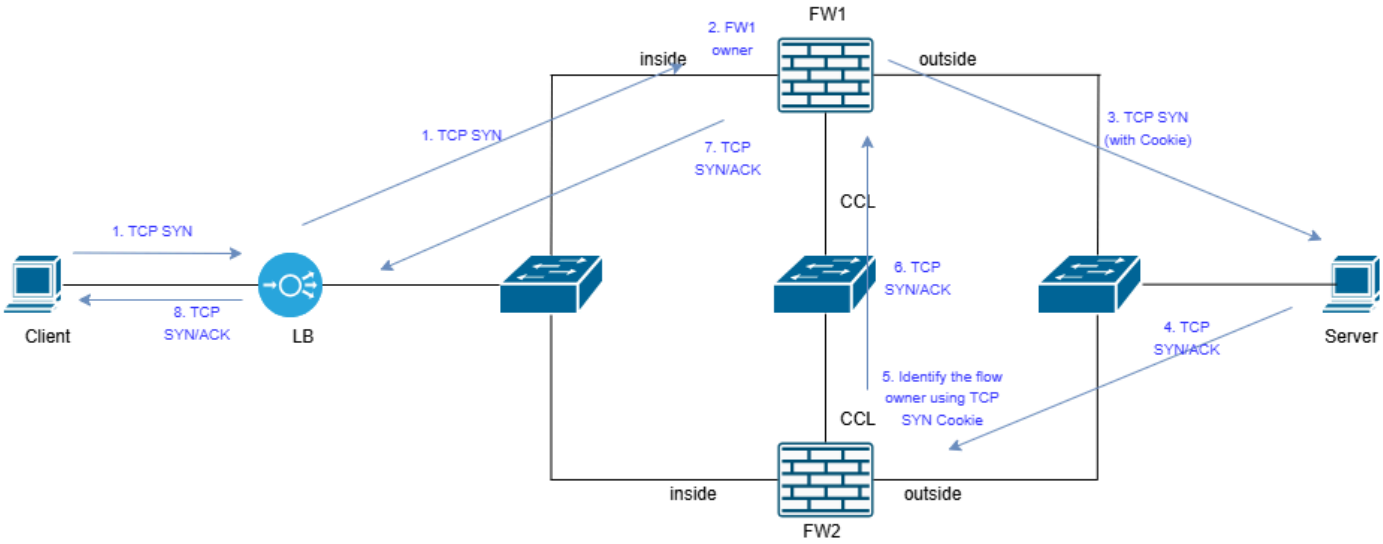


inline_image_0.png

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）。