科来

第 23 章
如何发现由设备机制引发的应用故障

科来官微
CSNA 公众号
400-6869-069
www.colasoft.com.cn
support@colasoft.com.cn

© 2003-2019 科来版权所有

当业务系统中的设备进行切换后，往往业务故障也随即出现。我们通常认为问题的发生是由新旧设备的策略差异导致的。但在实际情况中，往往问题根因在于某些设备自身的机制造成，设备的切换只是让这些潜在的问题展现出来，并对业务产生负面影响，正如本案例所述。

23.1 问题描述

某集团防火墙切换后，堡垒机（X.X.15.15）访问数据库时连接时断时续；当建议清除相关 IP 的防火墙会话表后，出现堡垒机访问延迟较大的异常现象，需要 1-3 秒内才能建立连接。

针对本次故障，我们对防火墙的 outside、inside 接口和堡垒机进行抓包分析，如下方拓扑图所示。

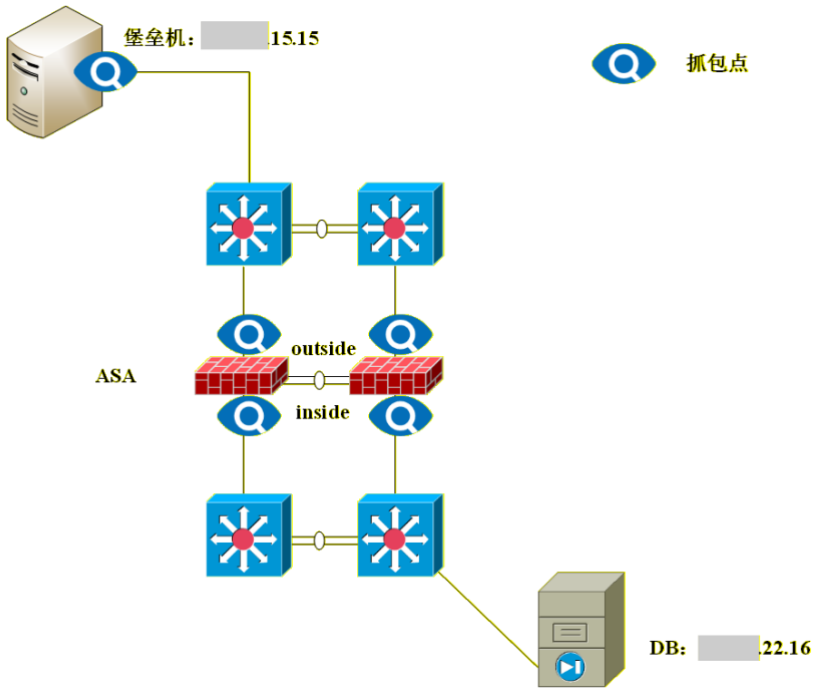

图 23-1

23.2 分析过程

23.2.1 堡垒机访问数据库异常现象分析

针对 inside 接口抓包，只抓到 5 个会话，如下图所示。

节点1->	端口1->	<-节点2	<-端口2	数据包	字节数	字节->	<-字节	数据包 ->	<- 数据包	开始发包时间	最后发包时间
.15.15	45576	.22.16	3306	22	3.66 KB	2.10 KB	1.56 KB	12	10	2017/06/24 13:58:09	2017/06/24 13:58:09
.15.15	43667	.22.16	3306	3	522.00 B	371.00 B	151.00 B	2	1	2017/06/24 13:58:09	2017/06/24 13:58:09
.15.15	45514	.22.16	3306	26	24.68 KB	588.00 B	24.10 KB	8	18	2017/06/24 13:58:09	2017/06/24 13:58:09
.15.15	43653	.22.16	3306	1,234	1.13 MB	302.12 KB	851.41 KB	537	697	2017/06/24 13:58:09	2017/06/24 13:58:11
.15.15	43686	.22.16	3306	1,780	1.66 MB	462.60 KB	1.21 MB	798	982	2017/06/24 13:58:09	2017/06/24 13:58:11

图 23-2

针对 outside 接口抓包，抓到 32 个会话。其中只有 5 个会话是完全建立的（红框部分）且与 inside 方向抓取的会话一致；其余会话都是由堡垒机（X.X.15.15）发起的新建会话，且新建会话数据包内容是 1-3 个 SYN 包。说明数据包是丢弃在防火墙的 outside 接口，如下图所示。

节点1->	端口1->	<-节点2	<-端口2	数据包	字节数	字节->	<-字节	数...	<-...	开始发包时间	最后发包时间
.15.15	45526	.22.16	3306	1	70.00 B	70.00 B	0.00 B	1	0	2017/06/24 13:58:05	2017/06/24 13:58:05
.15.15	45557	.22.16	3306	1	70.00 B	70.00 B	0.00 B	1	0	2017/06/24 13:58:05	2017/06/24 13:58:05
.15.15	45559	.22.16	3306	1	70.00 B	70.00 B	0.00 B	1	0	2017/06/24 13:58:05	2017/06/24 13:58:05
.15.15	45560	.22.16	3306	1	70.00 B	70.00 B	0.00 B	1	0	2017/06/24 13:58:05	2017/06/24 13:58:05
.15.15	45561	.22.16	3306	1	70.00 B	70.00 B	0.00 B	1	0	2017/06/24 13:58:05	2017/06/24 13:58:05
.15.15	45547	.22.16	3306	1	70.00 B	70.00 B	0.00 B	1	0	2017/06/24 13:58:06	2017/06/24 13:58:06
.15.15	45529	.22.16	3306	1	70.00 B	70.00 B	0.00 B	1	0	2017/06/24 13:58:06	2017/06/24 13:58:06
.15.15	45562	.22.16	3306	2	140.00 B	140.00 B	0.00 B	2	0	2017/06/24 13:58:05	2017/06/24 13:58:07
.15.15	45563	.22.16	3306	2	140.00 B	140.00 B	0.00 B	2	0	2017/06/24 13:58:06	2017/06/24 13:58:08
.15.15	45531	.22.16	3306	1	70.00 B	70.00 B	0.00 B	1	0	2017/06/24 13:58:08	2017/06/24 13:58:08
.15.15	45564	.22.16	3306	2	140.00 B	140.00 B	0.00 B	2	0	2017/06/24 13:58:06	2017/06/24 13:58:08
.15.15	45565	.22.16	3306	3	210.00 B	210.00 B	0.00 B	3	0	2017/06/24 13:58:05	2017/06/24 13:58:08
.15.15	45566	.22.16	3306	3	210.00 B	210.00 B	0.00 B	3	0	2017/06/24 13:58:05	2017/06/24 13:58:08
.15.15	45567	.22.16	3306	3	210.00 B	210.00 B	0.00 B	3	0	2017/06/24 13:58:05	2017/06/24 13:58:08
.15.15	45568	.22.16	3306	3	210.00 B	210.00 B	0.00 B	3	0	2017/06/24 13:58:05	2017/06/24 13:58:08
.15.15	45570	.22.16	3306	2	140.00 B	140.00 B	0.00 B	2	0	2017/06/24 13:58:08	2017/06/24 13:58:09
.15.15	45571	.22.16	3306	2	140.00 B	140.00 B	0.00 B	2	0	2017/06/24 13:58:08	2017/06/24 13:58:09
.15.15	45572	.22.16	3306	2	140.00 B	140.00 B	0.00 B	2	0	2017/06/24 13:58:08	2017/06/24 13:58:09

图 23-3

15.15	45538	.22.16	3306	1	70.00 B	70.00 B	0.00 B	1	0	2017/06/24 13:58:09	2017/06/24 13:58:09
15.15	45573	.22.16	3306	2	140.00 B	140.00 B	0.00 B	2	0	2017/06/24 13:58:08	2017/06/24 13:58:09
15.15	45496	.22.16	3306	1	70.00 B	70.00 B	0.00 B	1	0	2017/06/24 13:58:09	2017/06/24 13:58:09
15.15	45574	.22.16	3306	2	140.00 B	140.00 B	0.00 B	2	0	2017/06/24 13:58:08	2017/06/24 13:58:09
15.15	45576	.22.16	3306	22	3.66 KB	2.10 KB	1.56 KB	12	10	2017/06/24 13:58:09	2017/06/24 13:58:09
15.15	43667	.22.16	3306	3	522.00 B	371.00 B	151.00 B	2	1	2017/06/24 13:58:09	2017/06/24 13:58:09
15.15	45514	.22.16	3306	26	24.68 KB	588.00 B	24.10 KB	8	18	2017/06/24 13:58:09	2017/06/24 13:58:09
15.15	45577	.22.16	3306	1	70.00 B	70.00 B	0.00 B	1	0	2017/06/24 13:58:10	2017/06/24 13:58:10
15.15	45575	.22.16	3306	2	140.00 B	140.00 B	0.00 B	2	0	2017/06/24 13:58:09	2017/06/24 13:58:10
15.15	45569	.22.16	3306	3	210.00 B	210.00 B	0.00 B	3	0	2017/06/24 13:58:08	2017/06/24 13:58:11
15.15	45578	.22.16	3306	1	70.00 B	70.00 B	0.00 B	1	0	2017/06/24 13:58:11	2017/06/24 13:58:11
15.15	45540	.22.16	3306	1	70.00 B	70.00 B	0.00 B	1	0	2017/06/24 13:58:11	2017/06/24 13:58:11
15.15	43686	.22.16	3306	1,778	1.66 MB	461.99 KB	1.21 MB	797	981	2017/06/24 13:58:09	2017/06/24 13:58:11
15.15	43653	.22.16	3306	1,233	1.13 MB	302.12 KB	850.03 KB	537	696	2017/06/24 13:58:09	2017/06/24 13:58:11

图 23-4

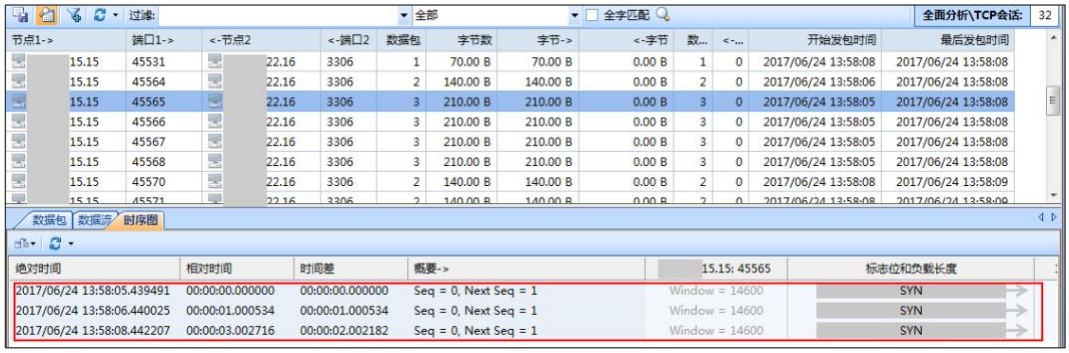

图　23-5

随后观察到堡垒机（X.X.15.15）以源端口 45576 新建的会话连接成功，并且有会话双向传输数据。说明并非所有新建会话都会被拒绝，防火墙策略是没有任何问题的，如下图所示。

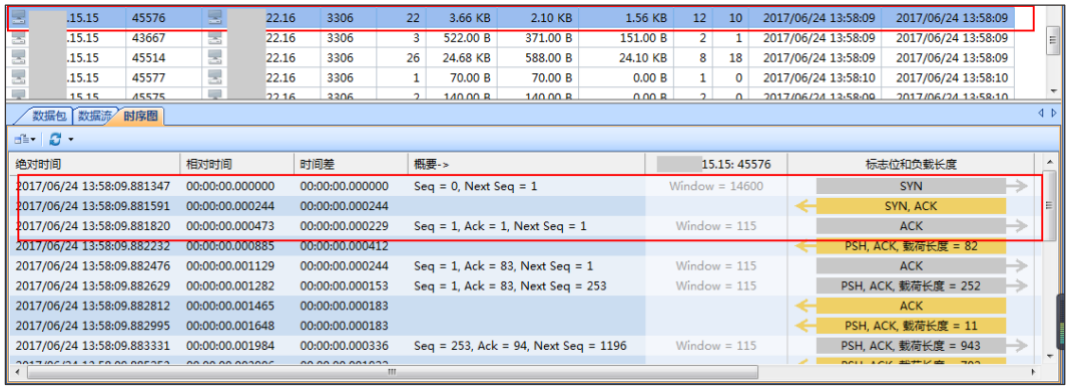

图　23-6

防火墙无论处于何种状态，都会为正常建立连接的 TCP 会话构建一张会话表（Conn 表），在未收到任何断链数据包（FIN、RST）的情况下，该会话表项（源 IP、源端口、目的 IP、目的端口）会一直保持到防火墙内，直到达到超时时间才会删除。到达防火墙的数据包如果匹配该表则放行，如果是 SYN 等包则当做异常流量丢弃。

Cisco 防火墙该表项的默认超时时间是 36 个小时，同时观察到故障期间防火墙上堡垒机到数据库间的会话有 4000 多个。

结合防火墙原理和数据包分析，可以说明：由于防火墙没有收到断链数据包，Conn 表中会话一直保持到超时时间点结束。当堡垒机用这些表项中的源端口发

起建连会话时，因防火墙安全机制会被丢弃。由于堡垒机的并发较高，源端口复用过快，因此会频繁出现建连不成功的现象。这也就是为什么在 outside 口上存在大量 455xx 的源端口建连却只有 45576 建连成功的原因。

针对上述情况，科来网络分析工程师建议该集团相关负责人清理防火墙、数据库 X.X.15.15 和 X.X.22.16 相关的 TCP 会话表。在清理结束后，经过 1 个小时的观察，没有发现连接、建连不成功的现象，如下图所示。

图　23-7

23.2.2　针对堡垒机访问延迟现象分析过程

清除相关 IP 的防火墙会话表后，所有的连接成功建立时间在 3 秒左右，同堡垒机所报的日志时间相吻合，如下图所示。

图　23-8

但此时发现新的情况，大量会话在建立时发生异常。以下图会话为例：由堡垒机 X.X.15.15 端口 57098 发起 TCP 连接，发起的 SYN 包序列号为 2763703735，数据库 X.X.22.16 回应的数据包应为序列号 2763703736 的 SYN+ACK，然而数据库回应的却是 PUSH+ACK，并且序列号是 3748899045。堡垒机认为此现象是异常情况，所以发送 reset 包重置。由于连接建立不成功，在 1 秒钟后，堡垒机重新用该序列号发起连接。此时回应收到的数据包依旧不是 SYN+ACK，因此堡垒机重复之前的重置动作。直至第三次，得到正确回应后建连成功，如下图所示。

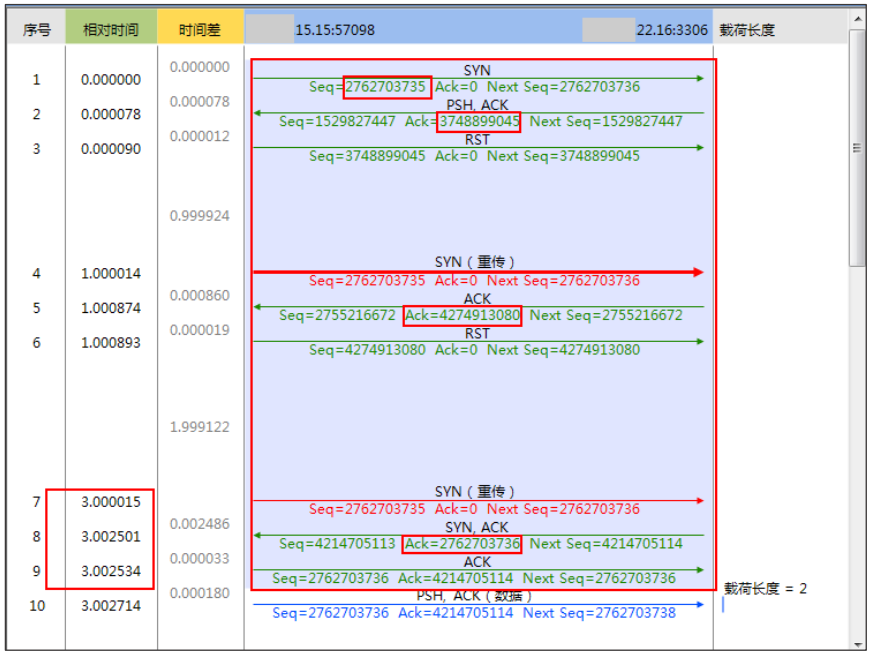

图　23-9

通过分析发现原因：由于数据库端有堡垒机关于该端口的会话列表，数据库端认为发过去的数据包是原有会话。因此按照原有的会话进行回复，直到堡垒机重置掉此会话后建连才恢复正常。

因此，科来网络分析工程师建议维护人员同时清理相关堡垒机、数据库及防火墙的会话。在维护人员操作后，发现该情况仍存在，说明数据库上相关会话并没有清理掉。在确保堡垒机清除的情况下，通过对查看数据库，发现有大量已持续很长时间的会话。该现象从侧面说明堡垒机和数据库的这种会话回收机制有

问题，如下图所示。

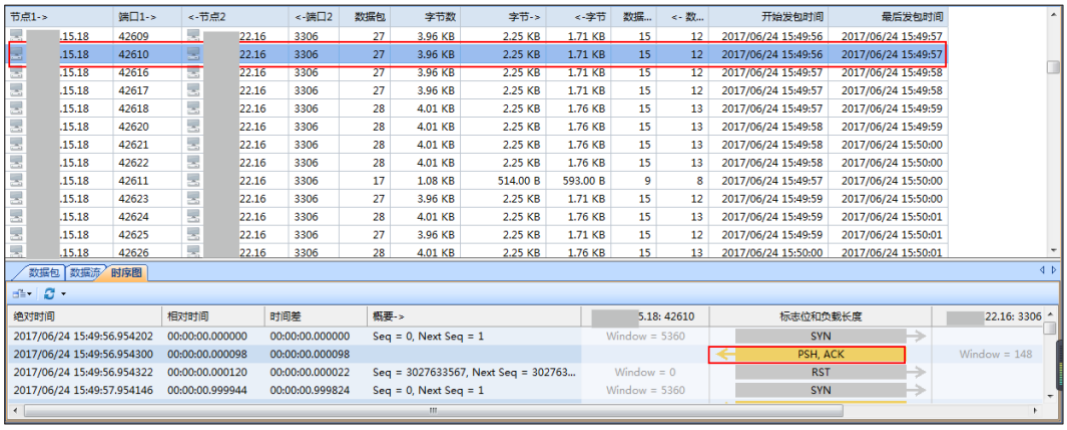

图　23-10

23.3　分析结论及建议

23.3.1　结论

诱因：由于堡垒机的并发较高，端口轮询（堡垒机使用的源端口）过快。在防火墙主备切换时，防火墙上的大量会话没有得到正确释放。当安全机制轮询到会话中的记录的源端口后，该部分源端口新建的连接都被拒绝。

数据库中存在大量的会话记录，并且远多于防火墙记录，说明该应用的会话回收机制存在缺陷。之前应该也存在相关现象，只是不明显，防火墙的切换，仅是在平时的基础上加剧了这种情况，放大问题现象。这也说明为什么切换后只有这个应用有问题，其余应用没有影响。

潜在风险：大量的会话没有得到释放，占用会话资源，这种回收机制会造成数据性能问题。

23.3.2　建议

建议优化应用会话资源回收机制，放开源端口的范围。

建议将调整应用的架构，将 APP 与 DB 放入同一个安全区域。

在该区域建立具备数据包回溯功能和路径梳理实时告警功能的系统，通过

梳理分析便可以发现潜在问题并解决，从而降低故障发生概率。

23.4 价值

通过网络回溯分析技术，能够实现对完整的对应用数据进行全方位监控。通过故障表象，深入挖掘关键设备对相关数据处理的过程，深层次的展现出产生问题的根本原因。快速定位产生故障的源头，帮助运维人员节省了大量的排障工作事件，更加有效率的解决各种疑难故障。更好的保证业务系统的稳定运行。

科来网络流量分析解决方案

科来业务性能解决方案

- 科来业务性能管理系统(UPM)
- 科来网络回溯分析系统(RAS)
- 科来网络分析系统(CSNAS)

科来网络安全分析解决方案

- 科来大数据安全态势感知平台(BAP)
- 科来网络全流量安全分析系统(TSA)
- 科来APT攻击检测系统(APT)

CSNA 网络分析认证培训

课程介绍

培训报名

科来网络流量分析技术资料

网络攻击与防范图谱

科来网络通讯协议图

科来网络故障诊断图

CSNA 网络分析经典实战案例

数据包样本

网络分析过滤器

术语表

科来网络流量分析产品下载(免费版)

科来网络分析系统

科来 MAC 地址扫描器

科来 Ping 工具

科来数据包播放器

科来数据包生成器

科来介绍

科来成立于 2003 年，是专注于网络流量分析技术研究与产品开发的高新技术企业，在这一领域有着几十项专利技术和完全独立的自主知识产权。科来研发的产品广泛应用于国内外用户的网络安全分析及网络智能运维等关键领域。科来连续入围 GartnerNPMD 魔力象限，并荣获“远见者”称号，是唯一入选“远见者”象限的中国企业。科来产品还曾被美国权威评测机构 PC Magazine 评选为《全球最佳科技产品》。

科来专业的技术服务在用户的业务保障上起到关键作用，已经成为对网络时效性高要求的企业的最佳选择，得到了社会各界的广泛认可。同时，科来创办的《CSNA 网络分析认证培训》是我国广具影响力的网络分析认证体系，为国家培养了大量的网络分析技术高级人才。

由于科来公司在网络安全领域的技术优势，受邀为青岛“上合峰会”、多届“两会”、“十九大”、杭州“G20 峰会”、“九三”阅兵、“世界田径锦标赛”、多届“数博会”等重大国家级活动做网络安保工作，做出突出贡献。

- 100 余家世界 500 强企业选择科来
- 为全球 10000 余家商业客户提供网络分析解决方案
- 全球 90 余万用户正在使用科来的产品
- 科来的技术服务于世界 110 个国家和地区