科来

第 21 章
如何解决支付交易间歇性失败问题

400-6869-069
www.colasoft.com.cn
support@colasoft.com.cn

科来官微　CSNA 公众号

间歇性业务故障往往是运维人员的工作难点之一，随着网络设备日渐增多，网络环境也变得更加复杂，但保障业务性能仍需要各个设备正常运行，因此故障排查难度也越来越大。本案例将通过解决由 WAF 设备异常引发的支付交易故障，为运维人员提供面对间歇性业务故障时的应对思路。

21.1 问题描述

某大学老师、学生在通过手机支付宝在线充值校园卡时，频繁发生显示交易成功但校园卡的充值金额迟迟未到账的现象，这在校园中产生了极其恶劣的影响。故障发生后，网络管理员逐一排查一卡通服务器、防火墙、网络等，均未发现明显异常，无法有效定位问题原因。随后故障又恢复正常，如此往复多次，无法得到解决。

为了定位和解决问题，科来网络分析工程师在相关网络中旁路部署了科来网络回溯分析系统。

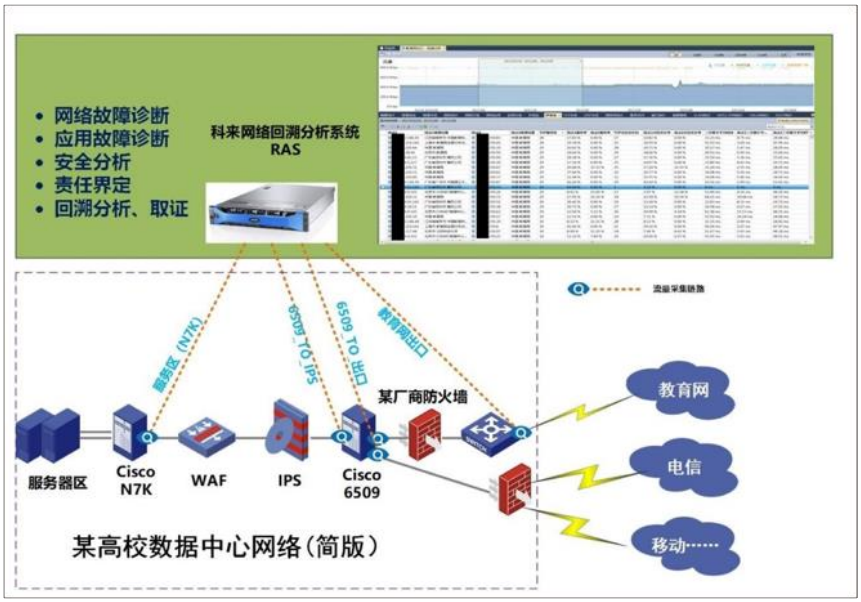


图　21-1

21.2　分析方案设计

21.2.1　分析思路

该充值业务路径为“手机支付宝充值操作→阿里支付宝处理账务交易→支付宝向校园一卡通系统提交充值金额”。由于“手机支付宝充值操作→阿里支付宝处理账务交易”交易流量无法被监控，因此只能根据故障时间重点分析“支付宝向校园一卡通系统提交充值金额”这一环节，通过提取“充值立即到账”与“充值迟迟未到账”的报文比对分析差异。

21.2.2　分析过程

首先在链路：“6509_TO_出口”提取一卡通充值服务器（X.X.194.23）交易流量，如下图在 HTTP 请求日志中我们可以看到支付宝服务器（X.X.0.0/16 网段）向一卡通服务器 POST 的 URL 均同为“/webservices-alipay/getway.ashx”，但是一卡通服务器应答有两种状态：

1、HTTP 状态码为 0

POST 请求内容长度（Content-Length）为 10180 字节（此类交易会话数量较

多），产生原因可能是 POST 请求数据包未发到一卡通服务器，或是一卡通服务器收到 POST 请求但不回应，或是回应被中间设备阻断。

2、HTTP 状态码为 200（此类交易会话数量较少）

表明一卡通服务器成功回应 POST 请求，此时 POST 请求的内容长度在 800 左右字节。

由于第一种 HTTP 状态为 0 的会话数量较多，怀疑充值金额未到账原因可能与此类会话有关。

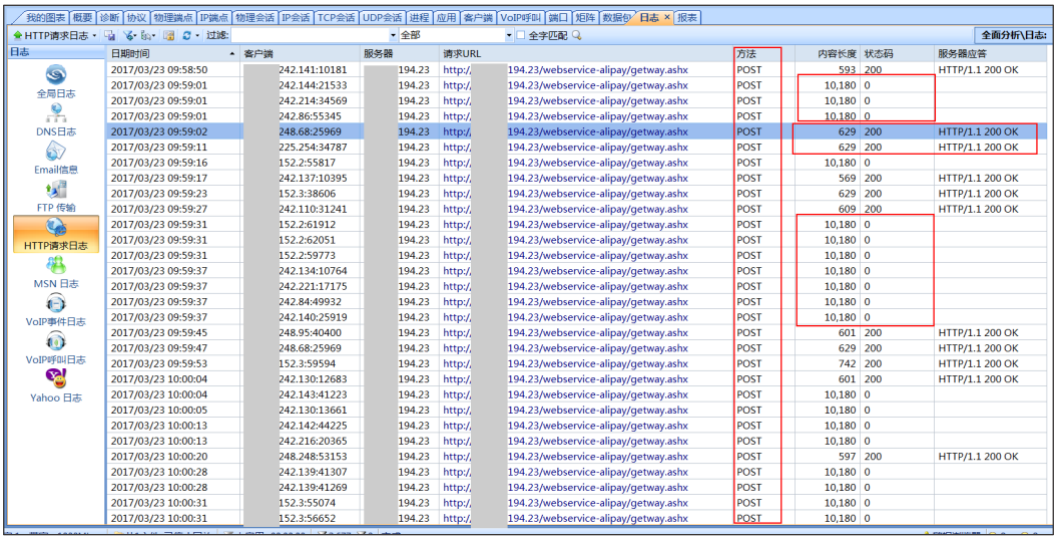


图　21-2

对此，我们抽样分析内容长度为 10180 字节的会话。如下图所示，对数据流重组解码可以看到支付宝 POST 请求的内容以“sign=”开头，其余为加密信息呈现，无法完全判断此类交易信息与充值金额有关。但不妨先看此类会话传输状况。

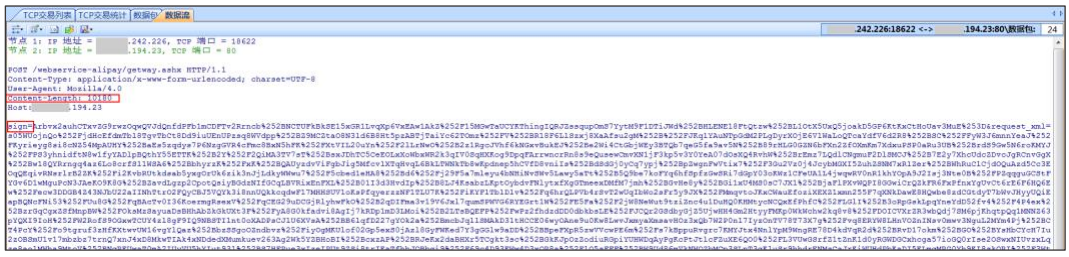


图　21-3

抽取 X.X.242.226：18622-X.X.194.23：80 端到端的分析，详情如下：

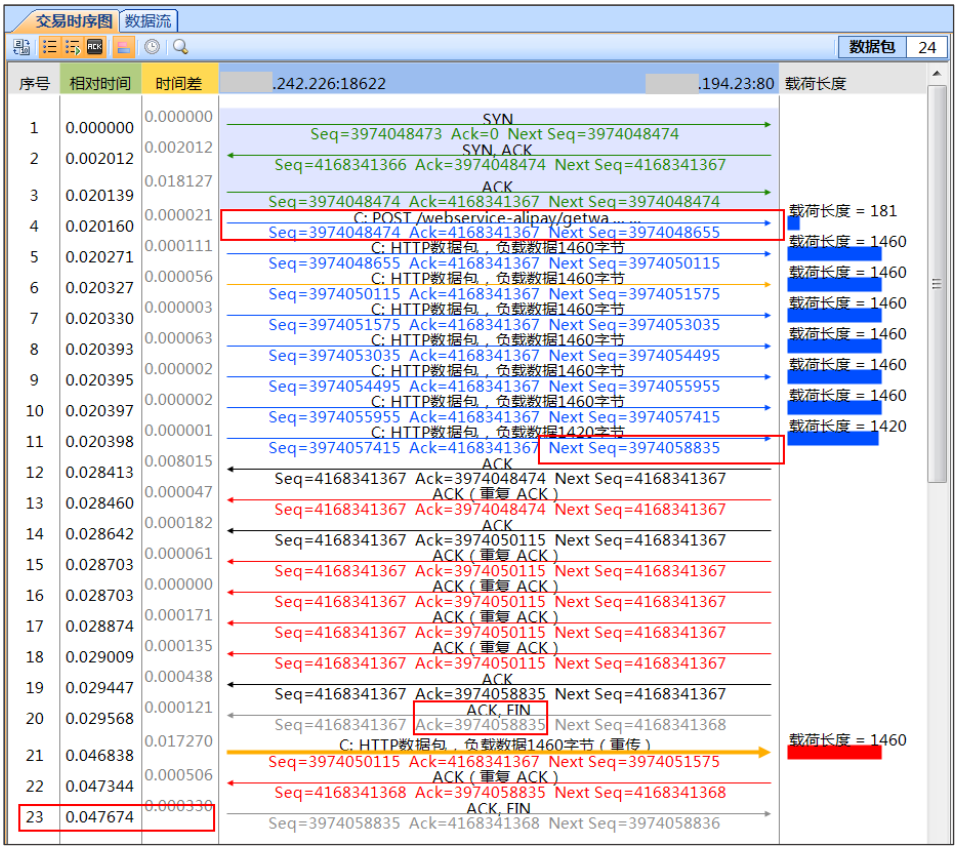


图　21-4

流量采集链路：教育网出口（防火墙外侧）

由于支付宝 POST 请求达 10180 字节，被拆分 8 个数据包（第 4-11 号数据包）且按序传输。同时一卡通服务器多次重传（ACK=3974050115，第 14-18 号数据包），表明第 6 号数据包传输中丢包、或是后期才到服务器。

最后，服务器主动发送“FIN”断开连接（ACK=3974058835，第 20 号数据包），说明一卡通服务器已全部接收到 POST 请求的内容，但为何未应答原因仍需继

续分析。

小结：支付宝发送的 POST 请求被拆分成 8 个数据包，按序进入防火墙。

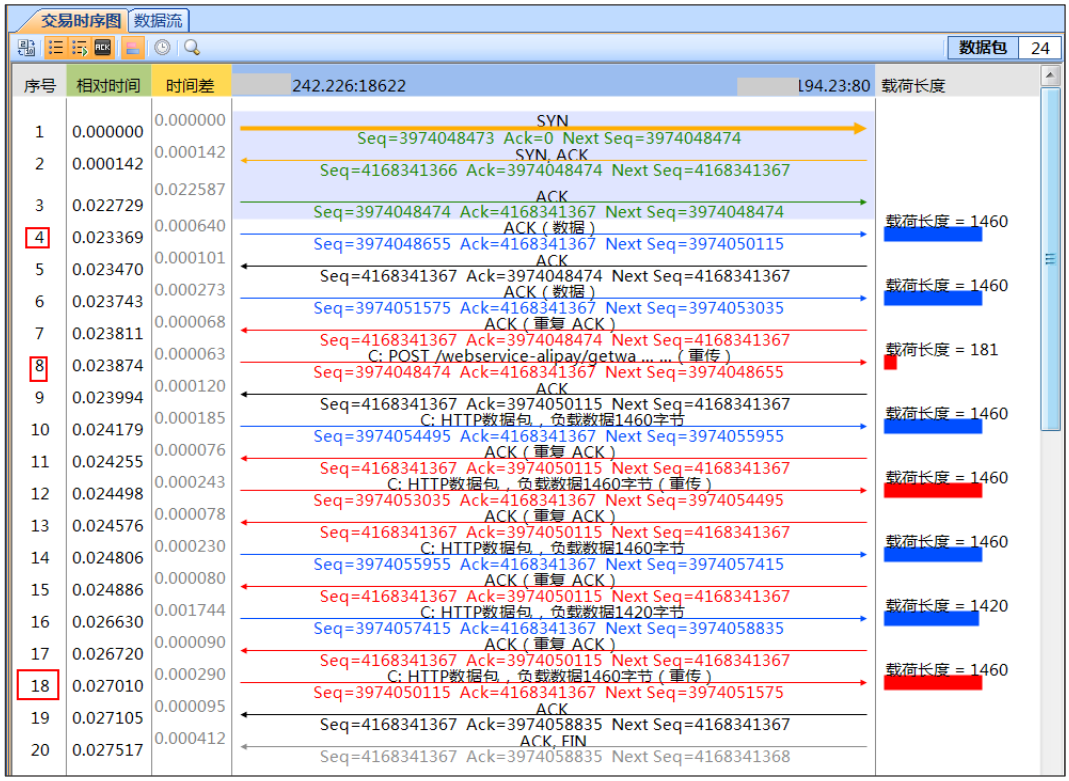


图　21-5

流量采集链路：6509_TO_出口（防火墙内侧）

根据 TCP 协议传输规范要求，每一个 TCP 数据包均携带有序列号（Seq），根据载荷偏移量可计算出下一序列值（Next Seq），在对端确认好 ACK 的值为 Next Seq 后本端向对端发送的下一个数据包的 Seq 值为上一个数据包的 Next Seq 。

可以看到第 4 号与第 8 号数据包失序，第 18 号更是失序到最后才发送，才导致一卡通服务器一直重复 ACK（ACK=3974050115）。最终一卡通服务器也接收了全部请求数据（第 20 号数据包），但仍未见到一卡通服务器应答。

小结：支付宝发送的 POST 请求被拆分成 8 个数据包，乱序从防火墙发出。

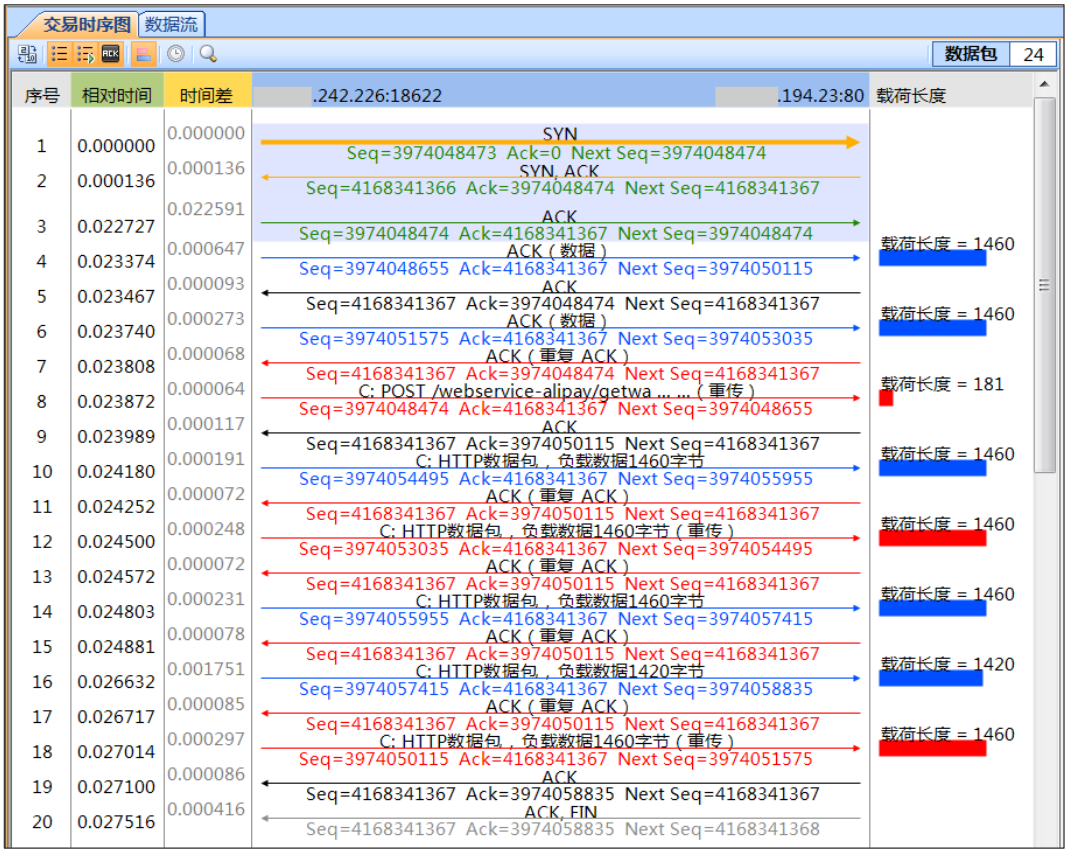


图　21-6

流量采集链路：6509_TO_NIPS（WAF 外侧）

传输状况与在链路：6509_TO_出口一致，结论一致。

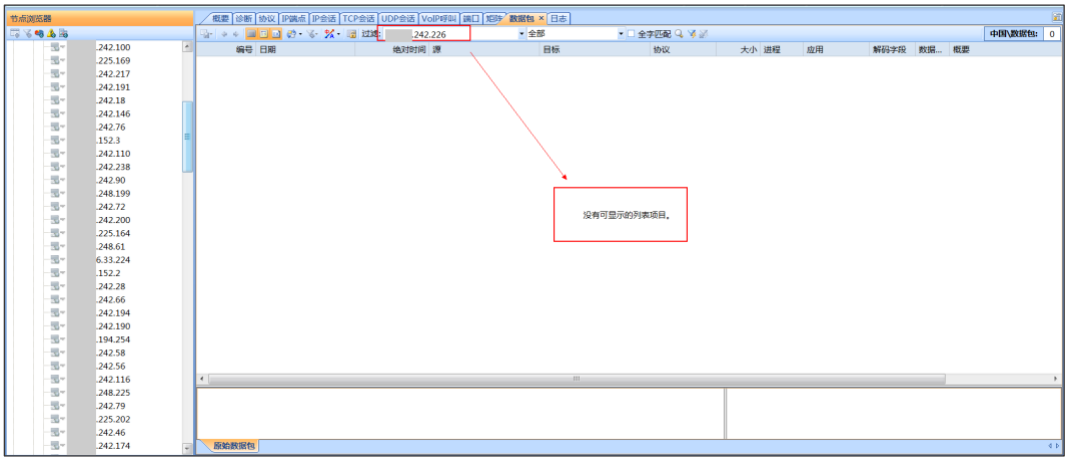


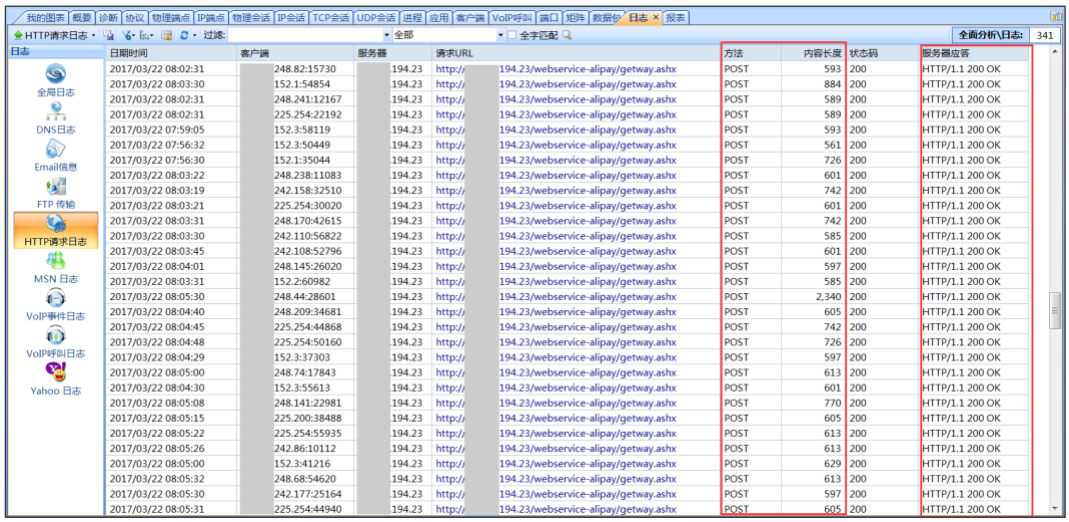
图　21-7

流量采集链路：服务器区（N7K）（WAF 内侧）

WAF 内侧，即 WAF 与一卡通服务器中间采集点。未能检索同一时间段内支付宝服务器 X.X.242.226 会话，表明 WAF 未把支付宝 POST 请求发送给一卡

通服务器，所以服务器一直无法收到支付宝的 POST 请求，也就无法应答。其他 POST 无应答会话也均未能在 N7K 链路上的流量检索到，所以此现象是共性问题。

回查之前可成功充值的交易会话，内容长度均未达到 10180 字节，所有 POST 请求均得到一卡通服务器的应答，如下图所示。



日期时间	客户端	服务器	请求URL	方法	内容长度	状态码	服务器应答
2017/03/22 08:02:31	248.82:15730	194.23	http://	POST	593	200	HTTP/1.1 200 OK
2017/03/22 08:03:30	152.1:54854	194.23	http://	POST	884	200	HTTP/1.1 200 OK
2017/03/22 08:02:31	248.241:12167	194.23	http://	POST	589	200	HTTP/1.1 200 OK
2017/03/22 08:02:31	225.254:22192	194.23	http://	POST	589	200	HTTP/1.1 200 OK
2017/03/22 07:59:05	152.3:58119	194.23	http://	POST	593	200	HTTP/1.1 200 OK
2017/03/22 07:56:32	152.3:50449	194.23	http://	POST	561	200	HTTP/1.1 200 OK
2017/03/22 07:56:30	152.1:35044	194.23	http://	POST	726	200	HTTP/1.1 200 OK
2017/03/22 08:03:22	248.238:11083	194.23	http://	POST	601	200	HTTP/1.1 200 OK
2017/03/22 08:03:19	242.158:32510	194.23	http://	POST	742	200	HTTP/1.1 200 OK
2017/03/22 08:03:21	225.254:30020	194.23	http://	POST	601	200	HTTP/1.1 200 OK
2017/03/22 08:03:31	248.170:42615	194.23	http://	POST	742	200	HTTP/1.1 200 OK
2017/03/22 08:03:30	242.110:56822	194.23	http://	POST	585	200	HTTP/1.1 200 OK
2017/03/22 08:03:45	242.108:52796	194.23	http://	POST	601	200	HTTP/1.1 200 OK
2017/03/22 08:04:01	248.145:26020	194.23	http://	POST	597	200	HTTP/1.1 200 OK
2017/03/22 08:03:31	152.2:60982	194.23	http://	POST	585	200	HTTP/1.1 200 OK
2017/03/22 08:05:30	248.44:28601	194.23	http://	POST	2,340	200	HTTP/1.1 200 OK
2017/03/22 08:04:40	248.209:34681	194.23	http://	POST	605	200	HTTP/1.1 200 OK
2017/03/22 08:04:45	225.254:44868	194.23	http://	POST	742	200	HTTP/1.1 200 OK
2017/03/22 08:04:48	225.254:50160	194.23	http://	POST	726	200	HTTP/1.1 200 OK
2017/03/22 08:04:29	152.3:37303	194.23	http://	POST	597	200	HTTP/1.1 200 OK
2017/03/22 08:05:00	248.74:17843	194.23	http://	POST	613	200	HTTP/1.1 200 OK
2017/03/22 08:04:30	152.3:55613	194.23	http://	POST	601	200	HTTP/1.1 200 OK
2017/03/22 08:05:08	248.141:22981	194.23	http://	POST	770	200	HTTP/1.1 200 OK
2017/03/22 08:05:15	225.200:38488	194.23	http://	POST	605	200	HTTP/1.1 200 OK
2017/03/22 08:05:22	225.254:55935	194.23	http://	POST	613	200	HTTP/1.1 200 OK
2017/03/22 08:05:26	242.86:10112	194.23	http://	POST	613	200	HTTP/1.1 200 OK
2017/03/22 08:05:00	152.3:41216	194.23	http://	POST	629	200	HTTP/1.1 200 OK
2017/03/22 08:05:32	248.68:54620	194.23	http://	POST	613	200	HTTP/1.1 200 OK
2017/03/22 08:05:30	242.177:25164	194.23	http://	POST	597	200	HTTP/1.1 200 OK
2017/03/22 08:05:31	225.254:44940	194.23	http://	POST	605	200	HTTP/1.1 200 OK

图　21-8

下图会话是从链路“6509_TO_出口”下载的数据包，按序传输且未出现重传等情况；同时 POST 请求内容以“sign=”开头，得到一卡通服务器成功应答。通过对比发现：充值故障发生时一卡通服务器应答 http/1.1 200 OK 的会话都是只有个单个 POST 请求包（POST 请求数据较少），并且 POST 请求内容以“service_type=”开头。再结合故障时间及故障现象，基本上可以判定支付宝如果通过 POST 内容以“sign=”开头的会话提交充值金额，那么该笔充值可立刻到账。

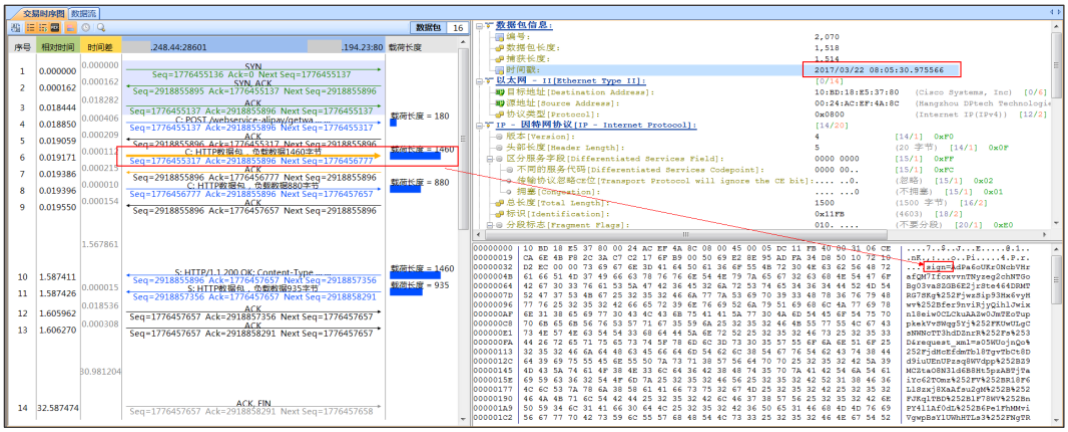


图　21-9

21.3　分析总结及建议

当支付宝充值的 POST 请求数据量较小时（如内容长度在 2300 字节及以下），经过防火墙的请求数据包会按序传输给 WAF 设备，WAF 设备也会将这些请求正常发送给一卡通服务器，充值金额立刻到账。当支付宝充值的 POST 请求数据量较大时（如本例内容长度达 10180 字节），经过防火墙的请求数据包会乱序传输（POST 请求被拆分成 8 个数据包）给 WAF 设备，但 WAF 并未将请求发送给一卡通服务器，直接造成一卡通服务器无法记账，因此出现充值无法及时到账现象。

综上可知充值无法及时到账是因为支付宝的充值请求终结在 WAF 防火墙，请求无法到达一卡通服务器造成。

科来网络分析工程师建议该校运维负责人联系 WAF 厂家进行详细检查，通过排查发现 WAF 设备异常是由其安全防护机制引发的，部分充值请求数据包被 WAF 设备认为是“加密攻击”而被丢弃，当关闭 WAF 设备的相关策略后，充值无法及时到账现象不再出现。

21.4　价值

传统排查方式很定位间歇性业务故障的根源，在问题发生时，仅凭经验排查

安全防护策略、服务器等节点，未必能有效查明原因。对比传统排查方式，科来网络回溯分析系统拥有对间歇性业务故障强悍的解决能力。正如本例所示故障所示，虽然 WAF 设备没有相关告警日志，但是通过流量分析和回溯分析等技术手段，可以准确定位故障原因，为解决故障提参考。

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