科来

第 32 章
如何定位系统大面积无法访问的根源

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

用户访问互联网需要通过很多网络节点，如交换机、防火墙、IPS、防毒墙、流量控制、负载均衡设备等，一旦出现不能上网的情况，每个节点都会是可疑的故障节点，大大增加了维护人员的排查工作量。本案例将详细讲解如何迅速精准定位故障节点。

32.1 问题描述

某单位部分用户通过互联网访问 Web 页面时，可以正常打开两到三个页面，之后再也无法正常打开其它页面，而这些用户在访问单位内部网页时却无此异常现象。

该单位网络结构如下图所示。

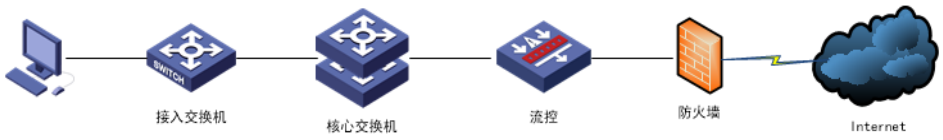

图 32-1

从结构图上可以看出，用户在进行互联网 Web 访问时，数据包除了经过接入层交换机和核心交换机外，中间还经过流控设备和防火墙。

32.2 分析过程

由于用户访问单位内部网页时状态正常，在访问互联网 Web 页面时才出现故障现象。通过对两种情况进行对比分析发现：用户对外网的访问路径只增加了交换机、流控设备和防火墙节点，而交换机只是对数据进行单纯的转发，并未对用户进行策略上的限制。因此，我们初步判断可疑故障点为流控设备节点或防火墙节点。

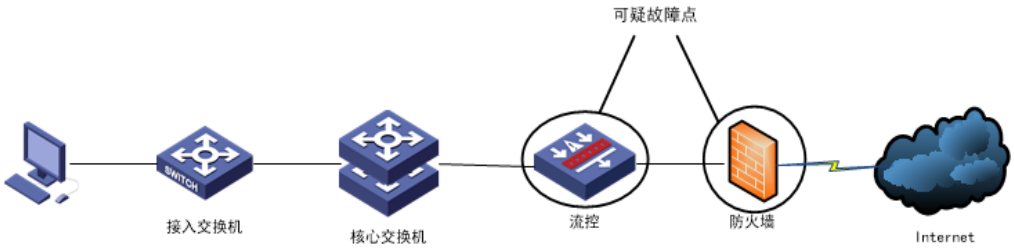

图　32-2

观察故障现象，我们定位了流控设备和防火墙这两个可疑故障点。首先对流控设备可疑故障点进行排查：将核心交换机和防火墙直接相连，使数据包传输跳过流控设备。观察用户进行互联网 Web 页面访问的情况，发现问题依旧存在。那么可以得出结论，故障问题与流控设备无关。

由于防火墙工作处于路由模式下，我们无法将其透明过去，只能通过对数据包抓取和分析，来定位故障产生原因。因此开启防火墙抓包功能，并在防火墙后端利用科来网络回溯分析系统抓取通信的数据包。

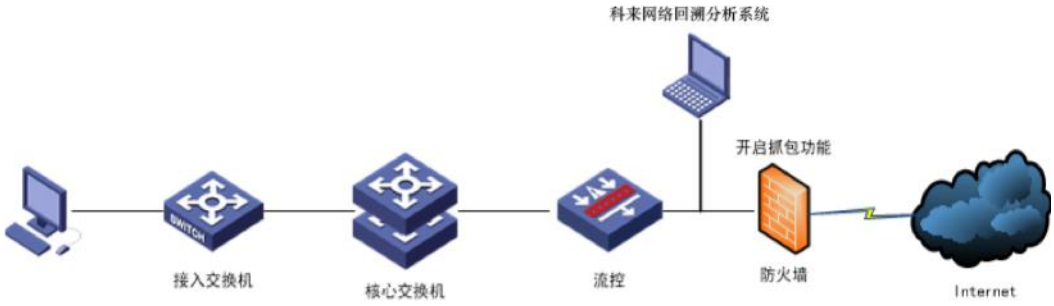

图　32-3

从防火墙后端抓取访问异常现象的数据包，如下图。

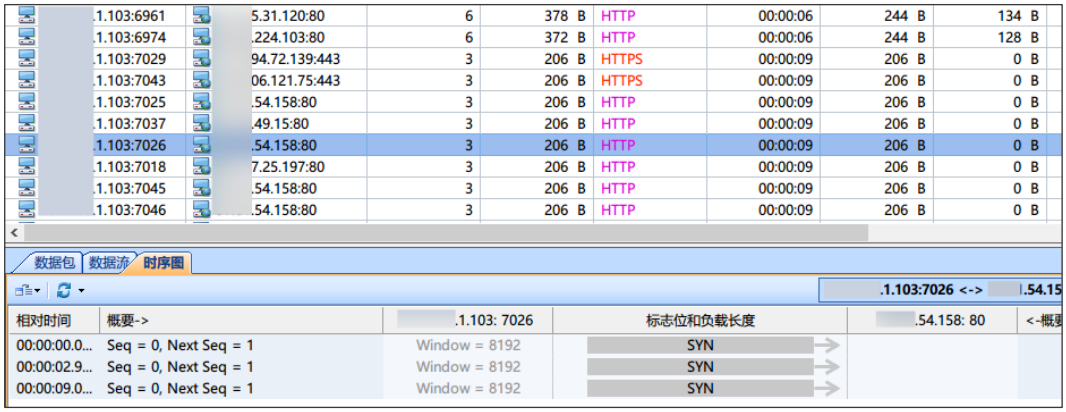

图 32-4

观察上图可以发现：用户在访问 Web 页面时，主机向外网地址发送了 SYN 同步请求数据包，但是没有外网地址发给主机的 SYN/ACK 回应数据包，TCP 会话的三次握手未能建立成功，导致页面出现无法打开的故障现象。

抓取防火墙产生的数据包，如下图。

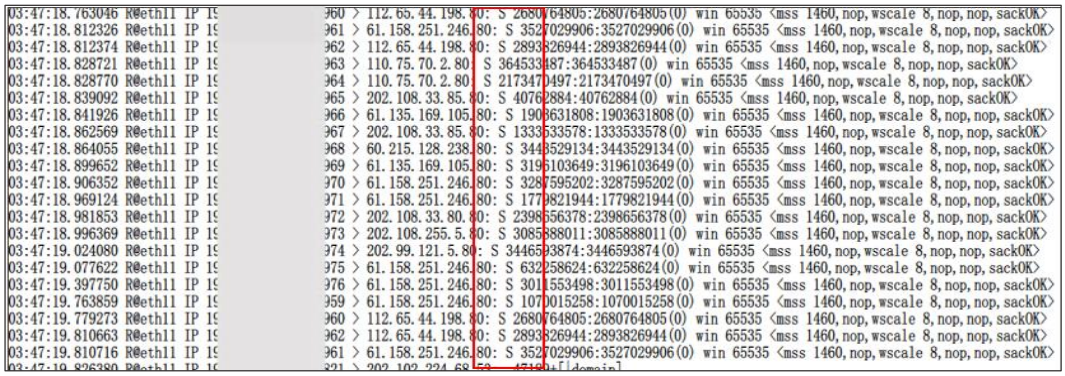

图 32-5

观察上图发现：防火墙能收到内网主机访问外网的 SYN 同步请求数据包（图中 S 代表 SYN 数据包），同样没有 SYN/ACK 的回应数据包，TCP 三次握手没有建立成功。

32.3 分析结论

通过数据包的分析，可以得出结论：由于防火墙性能异常或者配置不当，将所有外网地址对内网主机的回应数据包，进而导致访问出发生故障。通过联系防

火墙厂商对设备进行检测调试后，成功解决该故障。下图是问题解决后在防火墙上抓取的数据包。

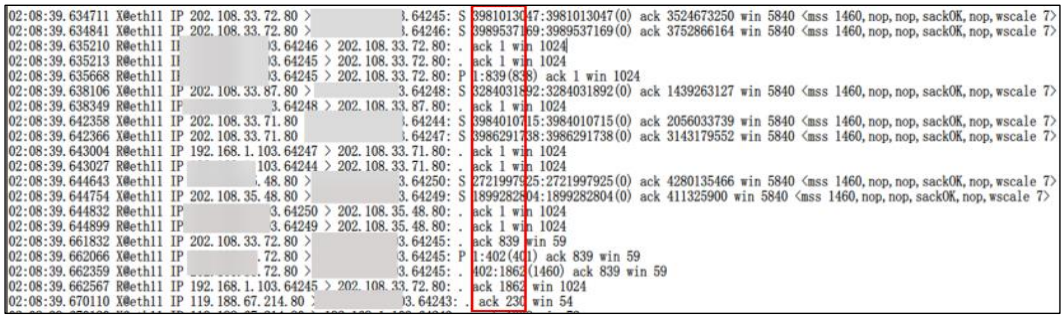

图　32-6

32.4　价值

科来网络回溯分析系统拥有对数据包强大的采集、分析能力，面对此类具有不定时、难复现的业务故障，可通过多点监控方式，快速掌握各关键节点的数据流动情况，迅速发现网络丢包异常，准确定位丢包节点，从而大大节省了排障时间。

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