科来

第 30 章
如何解决远程 VPN 连接失败问题

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

科来官微　CSNA 公众号

链路负载均衡设备可解决多链路网络环境中流量分担的问题，提高多链路的带宽利用率，保障了网络通信的稳定性。为用户和应用系统分配最佳的通信线路，使用户获得绝佳的访问体验。但也存在因为策略配置或设备自身问题引起的连接失败。

30.1 问题描述

某证券公司的客户端 PC1 通过互联网远程登录 VPN 时，每次都能够正常访问，但客户端 PC2 在登录远程 VPN 时，经常不能成功连接。针对这一现象，部署科来网络回溯分析系统分别采集客户端 PC1、客户端 PC2 及负载均衡上连防火墙的链路流量。远程 VPN 地址为：X.X.242.94。下图为该证券公司的简易部署图。

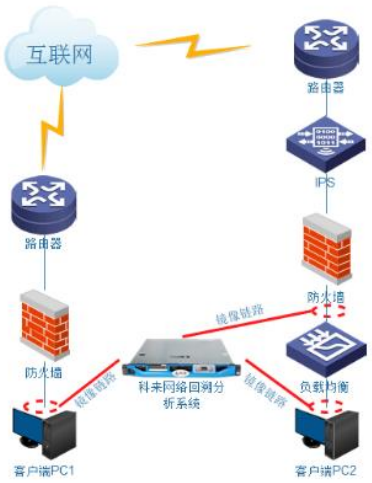

图 30-1

30.2 分析过程

客户端 PC1：

客户端 PC1 在任何时段都能够正常连接远程 VPN，所以首先抓取客户端 PC1 的数据进行分析：（圆框遮挡处为客户端 PC1 地址，方框为 VPN 地址）

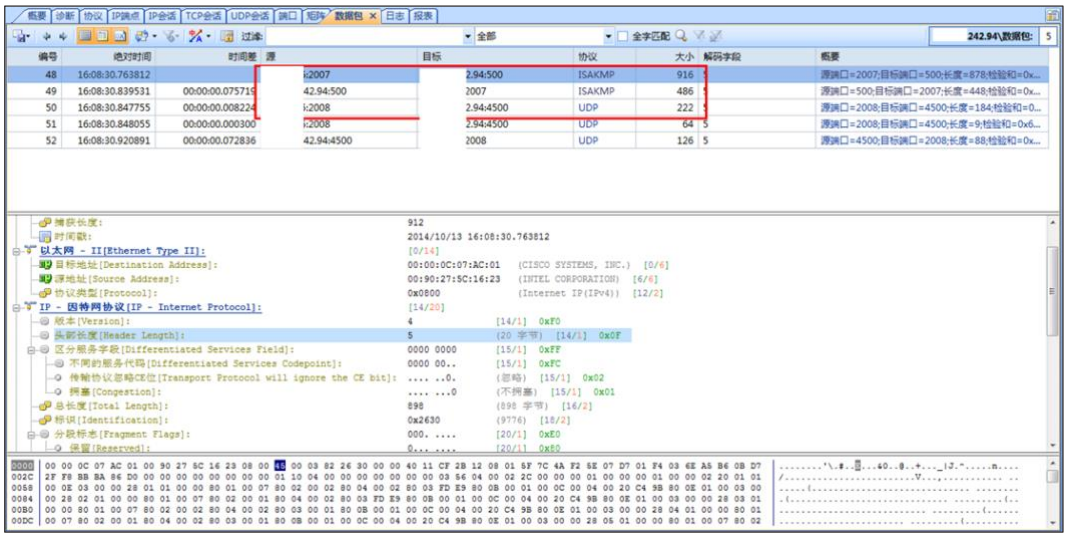

图　30-2

如上图所示，红框处三个包为 ISAKMP 协议，VPN 使用的是主动模式，其主要作用是定义 VPN 封装格式和协商包交换的方式。第一个包为客户端 PC1 向 VPN 地址发起连接，第二个包为 VPN 地址发送给客户端 PC1，第三个包为客户端 PC1 向 VPN 地址发送完成 ISAKMP 协议协商（由于 VPN 使用 NAT Traversal 技术所以第三个包开始就使用 UDP 4500 端口）。

经过上述步骤，一个 VPN 会话连接就能够被正常的建立。所以客户端 PC1 能够一直正常的与远程 VPN 连接。

客户端 PC2：

客户端 PC2 在连接远程 VPN 时，有时能够正常连接，有时很多次连接都会失败，所以在来抓取客户端 PC2 的数据进行分析：（圆框遮挡处为客户端 PC1 地址，方框为 VPN 地址）

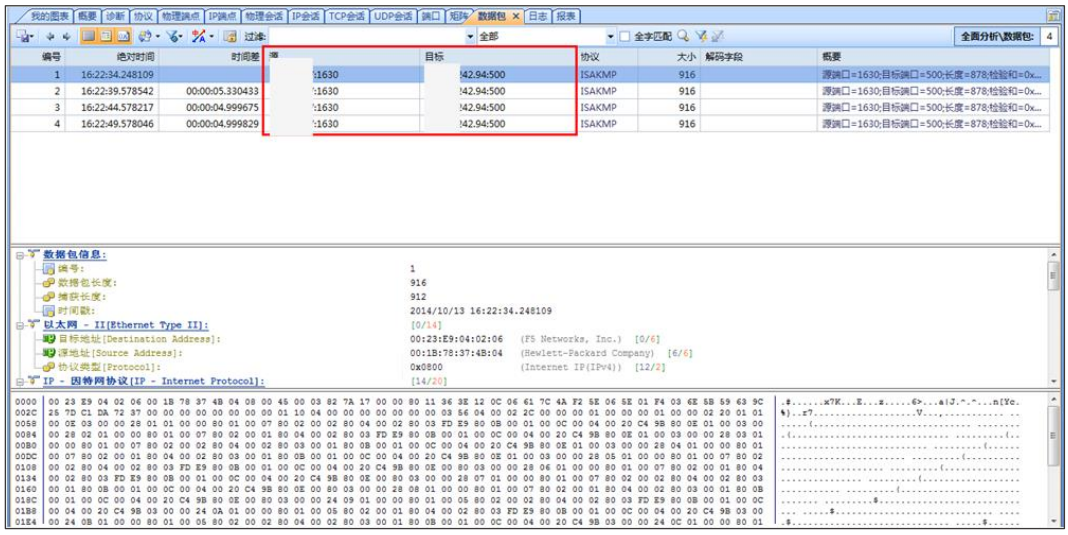

图　30-3

如上图，客户端 PC2 连接不上 VPN 时，数据包全部是有客户端 PC2 向 VPN 地址发起的第一个 ISAKMP 包，每隔 5 秒发送一次，共发送 4 次。

通过该现象分析，怀疑是由于内部网络设备或互联网丢包造成数据包没有到达远程 VPN，另一种可能是远程 VPN 收到数据包并发出回应，但回应数据包丢包。

为了验证分析，在负载均衡上联接口进行抓包分析：

在负载均衡前抓包，正常连接时能够抓包情况与客户端 PC1 一致，但不能连接 VPN 时，从抓包点位置不能抓到 ISAKMP 请求数据包。

结合客户端 PC2 抓包情况来看，客户端 PC2 发送了 ISAKMP 第一个包，但通过了负载均衡之后我们抓不到此包，说明此数据包可能被负载均衡设备丢弃或发送到错误的链路上。

30.3　分析结论

通过上述分析，可以判断在发生 VPN 连接问题时客户端 PC2 正常发送了 VPN 请求包，但通过负载均衡设备后，此包并没有出现在正确的链路上，建议用户对负载均衡设备进行排查，检测是否存在丢包或将此包发送到错误的链路

的情况。

30.4 价值

通过网络流量分析能够掌握网络运行状态，了解不同链路下的网络传输情况，完整追踪数据包的传输路径，迅速定位问题原因，从而解决链路负载均衡、路由等设备造成的丢包、转发错误等情况。

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