内网服务器数据经过我司安全设备后无法上传数据到公网平台

虚拟分片重组 姜霁琛 2019-02-17 发表

组网及说明

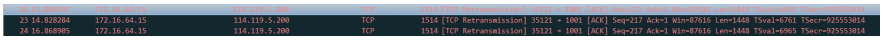
组网如图所示。

问题描述

ACG透明部署，策略全放通，防火墙必要的安全策略也已放通，现场通过无线接入的内网服务器的数据无法传送到公网的平台上，但是内网不论有线用户还是无线用户上网均正常。内网服务器与公网平台之间有两种报文交互，一是心跳报文，二是数据报文，使用的均为1001端口的tcp协议，在公网平台上可看到心跳报文交互正常，但数据报文无法正常接收。且其他局点组网相同未发现此问题。

过程分析

首先检查ACG和防火墙配置没有问题，让现场跳过ACG用核心交换机直连防火墙测试，发现问题现象依旧，所以排除ACG的问题，现场抓包结果发现，服务器与公网平台之间的tcp报文有很多被要求重传，联想到心跳报文可正常传输的故障现象，怀疑和mtu有关



查看报文分片情况，发现分片方式为不允许分片，tcp报文长度为1448字节，帧总长为1514字节，进一步查看mtu发现防火墙出接口mtu配置为1492，由于ip报文经过以太网封装后大小超过了mtu，又不允许分片，所以报文发送失败了

```
Frame 26: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: NewH3CTe_aa:53:b1 (04:d7:a5:aa:53:b1), Dst: 7c:1e:06:cc:2f:ad (7c:1e:06:cc:2f:ad)
Internet Protocol Version 4, Src: 172.16.64.15, Dst: 114.119.5.200
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xcf2c (53036)
  Flags: 0x4000, Don't fragment
    Time to live: 63
    Protocol: TCP (6)
    Header checksum: 0x0291 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.16.64.15
    Destination: 114.119.5.200
Transmission Control Protocol, Src Port: 51073, Dst Port: 1001, Seq: 1096, Ack: 615, Len: 1448
```

解决方法

调小防火墙出接口的tcp mss值后问题解决

interface Dialer0

tcp mss 1024