某局点S6805设备无法通过ssh登录

SSH 刘倩 2023-12-03 发表

组网及说明

组网不涉及

告警信息

告警信息不涉及

问题描述

现场一台S6805设备无法SSH登录

过程分析

现场一台S6805设备无法SSH登录，debugging ssh相关报文没有任何回显，进一步排查发现 ssh的TCP连接都未建立成功。

流统发现客户端发送TCP报文已经到 故障交换机，但是debugging没有回显，驱动rxtx打印报文也没有回显

进一步排查ssh的TCP报文上送cos 1 队列，而cos 1队列有丢包且在增长

```
========
Acl-Type RX IPv4 Middle, Stage IFP, Pipe 0, Global, Installed, Active
Prio Mjr/Sub 526/23, Group 1 [1], Slice/Idx 9/74, Entry 5596, Triple: 6986/7754/8522
Rule Match --------
      Ports: 0x0000000000000000000000000000000000000000000000001ffffffffffffffe; 0x0000000000
0000000000000000000000000000000000000000000000000000000000
 Lookup: VLAN ID valid[y], STP forwarding, 0x1c, 0x1c
 Dest mac: 0000-0000-0000, 0100-0000-0000
 IP protocol: tcp
 IP Type: Any IPv4 packet
 L4 Source Port: 22, 0xffff
 IP Fragment: 0x3
 Dest Port: CPU
 DropBit: 0x0, Mask : 0x1
 My Station Hit
Actions --------
 CAR cir 0x640, cbs 0x800, pir 0x640, pbs 0x800, pps 1, kbps 0, mode srTCM color blind
 Account mode  packets,  green and non-green
 Redirect and copy to cpu
 L3Switch Cancel L3Switch NextHopIndex 0x1
 Change CPU pkt COS 1
 Red Deny
 Red_Copy_to_cpu : No
 Yel Deny
 Yel_Copy_to_cpu : No
MatchedName:61, TELNET/SSH
 ===============debug rxtx coscar show slot 1===============
 Index      RcvPkt        DisPkt        RcvPkt/s    DisPkt/s    PPS
 0          432221        0             0           0           6000
 1          50068985      8643          2928        0           3000
 2          4684013       0             0           0           8000
 3          119215        0             0           0           6000
 4          19            0             0           0           5500
 5          0             0             0           0           6500
 6          0             0             0           0           20000
```

排查发现上送CPU的ROOT报文比较多，排查发现是syslog，来自一台防火墙的日志，防火墙上指定日志主机错误，导致syslog报文 被错误发送到交换机了，造成TCP报文被挤掉

解决方法

修改防火墙上日志主机配置后解决