某局点SR8808-X作为SSH客户端无法登录其它设备故障排查经验案例

SSH　王周华　2021-03-28 发表

组网及说明

本次涉及设备的型号以及版本：SR8808-X　Version 7.1.075, Release 7951P11

问题描述

客户有4台SR8808-X设备，发现将SR8808-X作为SSH客户端时无法登录到SSH服务端；在SSH登陆时，可以输入账号，但之后就停留在连接状态下，无法继续进行输入密码。故障现象如下：

<YN-YJE09-HXLY-SR8808-A>ssh2　　21.112.252.2

Username: admin

Press CTRL+C to abort.

Connecting to 21.112.252.2 port 22.

过程分析

1、检测连通性。用SSH客户端发送SSH报文的源地址PING SSH服务端的地址可以PING通。

```
GE3/2/4                   down      down      --              --
Loop0                     up        up(s)     21.0.5.157      NTP&SNMP
Loop3                     up        up(s)     21.0.5.158      ospf 300 route...
Loop4                     up        up(s)     21.0.5.159      ospf 400 route...
MGE0/0/0                  up        up        21.112.252.1    Link_To_D05_Da...
XGE3/4/1                  up        up        21.112.255.1    to YN-YJE08-HX...
XGE3/4/2                  up        up        21.112.255.5    to YNDZJ-CZW-C...
XGE3/4/3                  up        up        21.112.255.9    to YNDZJ-CZW-C...
XGE3/4/4                  down      down      --              --
<YN-YJE09-HXLY-SR8808-A>
<YN-YJE09-HXLY-SR8808-A>
<YN-YJE09-HXLY-SR8808-A>
<YN-YJE09-HXLY-SR8808-A>
<YN-YJE09-HXLY-SR8808-A>
<YN-YJE09-HXLY-SR8808-A>ping -a 21.112.255.1 21.112.255.2
Ping 21.112.255.2 (21.112.255.2) from 21.112.255.1: 56 data bytes, press CTRL+C
to break
56 bytes from 21.112.255.2: icmp_seq=0 ttl=255 time=0.890 ms
56 bytes from 21.112.255.2: icmp_seq=1 ttl=255 time=0.602 ms
56 bytes from 21.112.255.2: icmp_seq=2 ttl=255 time=0.939 ms
56 bytes from 21.112.255.2: icmp_seq=3 ttl=255 time=0.593 ms
56 bytes from 21.112.255.2: icmp_seq=4 ttl=255 time=0.588 ms

--- Ping statistics for 21.112.255.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.588/0.722/0.939/0.158 ms
```

2、检测SSH服务端的SSH服务是否正常。采用其他的设备作为SSH客户端登陆SSH服务端正常，说明SSH服务正常。

3、检查SSH服务端是否对于SSH登录的客户端进行了限制。如下，限制SSH登录的ACL仅配置了一条PERMIT规则。

ssh server acl 2010

acl basic 2010

description Manager_IP

rule 5 permit

4、检查SSH客户端和服务器间的报文交互。SR8808-A作为客户端，SR8808-B作为服务器端；让现场SSH客户端和服务器均开启如下DEBUG开关后，SSH客户端测试登录SSH服务器，收集下SSH报文的交互过程。

<SR8808-A>debugging ssh client all

<SR8808-A>ter mon

<SR8808-A>ter debugging

开启DEBUG开关测试登录后发现客户端无debug输出，服务器端显示Received packet type 94。

<SR8808-B>*Feb 24 03:14:14:737 2021 SR8808-B SSHS/7/MESSAGE: -MDC=1; Received packet type 94.

服务器端type 94是SSH数据报文，不一定是登录不上的SSH交互打印的。于是怀疑这个问题是TCP没建起来导致的，所以DEBUG没有看到SSH报文的交互。

5、在客户端上发起SSH请求后，查看服务器TCP连接。结果如下，没有看到SR8808-A对应的TCP连接。

```
<YN-YJE08-HXLY-SR8808-B>display  tcp
 *: TCP connection with authentication
 Local Addr:port       Foreign Addr:port     State       Slot  PCB
 0.0.0.0:22            0.0.0.0:0             LISTEN      4     0xfffffffffffffff9
e
*0.0.0.0:179           21.0.5.158:0          LISTEN      4     0xfffffffffffffffa
5
*0.0.0.0:179           21.112.253.16:0       LISTEN      4     0xfffffffffffffffa
7
*21.0.5.161:179        21.112.253.16:63258   ESTABLISHED 4     0xfffffffffffffffd
9
*21.0.5.161:51521      21.0.5.158:179        ESTABLISHED 4     0xfffffffffffffffa
6
 21.112.255.13:22      10.53.233.253:60973   ESTABLISHED 4     0x000000000000004
1
<YN-YJE08-HXLY-SR8808-B>
<YN-YJE08-HXLY-SR8808-B>
<YN-YJE08-HXLY-SR8808-B>display  tcp
 *: TCP connection with authentication
 Local Addr:port       Foreign Addr:port     State       Slot  PCB
 0.0.0.0:22            0.0.0.0:0             LISTEN      4     0xfffffffffffffff9e
*0.0.0.0:179           21.0.5.158:0          LISTEN      4     0xfffffffffffffffa5
*0.0.0.0:179           21.112.253.16:0       LISTEN      4     0xfffffffffffffffa7
*21.0.5.161:179        21.112.253.16:63258   ESTABLISHED 4     0xfffffffffffffffd9
*21.0.5.161:51521      21.0.5.158:179        ESTABLISHED 4     0xfffffffffffffffa6
 21.112.255.13:22      10.53.233.253:60973   ESTABLISHED 4     0x0000000000000041
<YN-YJE08-HXLY-SR8808-B>
```

6、检查TCP相关配置。发现有如下TCP配置。防攻击命令会导致设备丢弃从对端回来的SSH的TCP报文，所以SSH不通。

tcp syn-COOKIE enable

tcp anti-naptha enable

tcp anti-syn-flood flow-based enable

tcp anti-syn-flood interface-based enable

解决方法

去掉tcp anti-syn-flood flow-based enable问题解决。