某局点在M9000通过SSH远程登录交换机S7600失败案例分析

认证 其他 zhiliao_2TE8Y 2018-09-30 发表

组网及说明

不涉及

问题描述

M9K通过SSH登录交换机7600（，可以进入到用户名阶段，但是不能进入输入密码阶段（M9K可以ping通7600环回口地址）：

```
<GDSG-GZ-NEW-FW-M9014>ping 172.31.230.198
Ping 172.31.230.198 (172.31.230.198): 56 data bytes, press CTRL_C to break
56 bytes from 172.31.230.198: icmp_seq=0 ttl=255 time=2.067 ms
56 bytes from 172.31.230.198: icmp_seq=1 ttl=255 time=1.857 ms
56 bytes from 172.31.230.198: icmp_seq=2 ttl=255 time=1.013 ms
56 bytes from 172.31.230.198: icmp_seq=3 ttl=255 time=1.728 ms
56 bytes from 172.31.230.198: icmp_seq=4 ttl=255 time=6.560 ms

--- Ping statistics for 172.31.230.198 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.013/2.645/6.560/1.989 ms
<GDSG-GZ-NEW-FW-M9014>ssh 172.31.230.198
Username: gcable
Press CTRL+C to abort.
Connecting to 172.31.230.198 port 22.
<GDSG-GZ-NEW-FW-M9014>
```

每次在登录时在M9K上都会显示SSH user （null） disconnected from the server

```
<GDSG-NCK-S7604X-2>dis log re
Log buffer: Enabled
Max buffer size: 1024
Actual buffer size: 512
Dropped messages: 0
Overwritten messages: 83881
Current messages: 512
%Aug 29 16:09:13:662 2018 GDSG-NCK-S7604X-2 SSH5/6/SSH5_DISCONNECT: SSH user (null) (IP: 172.31.236.77) disconnected from the server.
```

过程分析

查看设备是否能够匹配到相应的ACL

ssh server acl 2097

#

acl basic 2097

description TELNET-SSH-control

rule 0 permit source 172.31.229.160 0.0.0.15

rule 10 permit source 172.31.230.0 0.0.0.255

rule 11 permit source 10.184.0.197 0

rule 20 permit source 100.100.100.2 0

rule 30 permit source 172.31.236.0 0.0.0.255

rule 999 deny

带着源去ssh设备，SSH的时候确保源地址在以上范围。

源去ssh情况如图所示，跟不带源ssh情况是一样的

```
<GDSG-GZ-NEW-FW-M9014>ping -a 172.31.236.77 172.31.230.198
Ping 172.31.230.198 (172.31.230.198) from 172.31.236.77: 56 data bytes, press CTRL_C to break
56 bytes from 172.31.230.198: icmp_seq=0 ttl=255 time=1.891 ms
56 bytes from 172.31.230.198: icmp_seq=1 ttl=255 time=1.220 ms
56 bytes from 172.31.230.198: icmp_seq=2 ttl=255 time=2.124 ms
56 bytes from 172.31.230.198: icmp_seq=3 ttl=255 time=5.805 ms
56 bytes from 172.31.230.198: icmp_seq=4 ttl=255 time=1.493 ms

--- Ping statistics for 172.31.230.198 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.220/2.507/5.805/1.679 ms
<GDSG-GZ-NEW-FW-M9014>ssh 172.31.230.198 source ip 172.31.236.77
Username: gcable
Press CTRL+C to abort.
Connecting to 172.31.230.198 port 22.
<GDSG-GZ-NEW-FW-M9014>
```

查看 ACL看见ACL此时有匹配到，

```
<GDSG-NCK-S7604X-2>dis acl 2097
Basic IPv4 ACL 2097, 6 rules,
TELNET-SSH-control
ACL's step is 5, start ID is 0
 rule 0 permit source 172.31.229.160 0.0.0.15 (3373 times matched)
 rule 10 permit source 172.31.230.0 0.0.0.255 (137 times matched)
 rule 11 permit source 10.184.0.197 0
 rule 20 permit source 100.100.100.2 0
 rule 30 permit source 172.31.236.0 0.0.0.255 (294 times matched)
 rule 999 deny (56914 times matched)

<GDSG-NCK-S7604X-2>
```

进一步收集设备诊断信息与设备的debugging信息

1、以下log里server端支持的列表是ssh-rsa,ssh-dss，客户端支持的列表是ecdsa-sha2-nistp256,ssh-dss,ssh-rsa，最终协商使用的是ssh-dss，也就是dsa。登录失败

*Sep 3 13:15:36:505 2018 GDSG-NCK-S7604X-2 SSHS/7/EVENT: -MDC=1; Kex strings(0): ecdh-sha2-nistp256,ecdh-sha2-nistp384,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
*Sep 3 13:15:36:505 2018 GDSG-NCK-S7604X-2 SSHS/7/EVENT: -MDC=1; Kex strings(1): ssh-rsa,ssh-dss
*Sep 3 13:15:36:507 2018 GDSG-NCK-S7604X-2 SSHS/7/EVENT: -MDC=1; Peer proposal kex:
*Sep 3 13:15:36:507 2018 GDSG-NCK-S7604X-2 SSHS/7/EVENT: -MDC=1; Kex strings(0): diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
*Sep 3 13:15:36:507 2018 GDSG-NCK-S7604X-2 SSHS/7/EVENT: -MDC=1; Kex strings(1): ecdsa-sha2-nistp256,ssh-dss,ssh-rsa
*Sep 3 13:15:36:512 2018 GDSG-NCK-S7604X-2 SSHS/7/EVENT: -MDC=1; Received SSH2_MSG_KEX_DH_GEX_REQUEST.
*Sep 3 13:15:36:513 2018 GDSG-NCK-S7604X-2 SSHS/7/MESSAGE: -MDC=1; Prepare packet[31].
*Sep 3 13:15:36:530 2018 GDSG-NCK-S7604X-2 SSHS/7/EVENT: -MDC=1; Expecting packet type 32.
*Sep 3 13:15:36:530 2018 GDSG-NCK-S7604X-2 SSHS/7/MESSAGE: -MDC=1; Received packet type 32.
*Sep 3 13:15:36:556 2018 GDSG-NCK-S7604X-2 SSHS/7/ERROR: -MDC=1; Fatal error occurs: unexpected internal error.

2、以下log里server端支持的列表是ssh-rsa，客户端支持的列表是ecdsa-sha2-nistp256,ssh-dss,ssh-rsa，最终协商使用的是ssh-rsa，登录成功。
*Sep 3 13:13:45:501 2018 GDSG-NCK-S7604X-1 SSHS/7/EVENT: -MDC=1; My proposal kex:
*Sep 3 13:13:45:501 2018 GDSG-NCK-S7604X-1 SSHS/7/EVENT: -MDC=1; Kex strings(0): ecdh-sha2-nistp256,ecdh-sha2-nistp384,diffie-hell
an-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
*Sep 3 13:13:45:501 2018 GDSG-NCK-S7604X-1 SSHS/7/EVENT: -MDC=1; Kex strings(1): ssh-rsa
*Sep 3 13:13:45:502 2018 GDSG-NCK-S7604X-1 SSHS/7/EVENT: -MDC=1; Peer proposal kex:
*Sep 3 13:13:45:502 2018 GDSG-NCK-S7604X-1 SSHS/7/EVENT: -MDC=1; Kex strings(0): diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
*Sep 3 13:13:45:502 2018 GDSG-NCK-S7604X-1 SSHS/7/EVENT: -MDC=1; Kex strings(1): ecdsa-sha2-nistp256,ssh-dss,ssh-rsa

解决方法

经确认，存在下述两种可能：
1. dsa配置错误，如果客户端和服务器端的dsa都有配置的话，服务器端或者客户端中有dsa的长度不对。
配置限制和指导
SSH仅支持默认名称的本地DSA、ECDSA或RSA密钥对，不支持指定名称的本地DSA、ECDSA或RSA密钥对。关于密钥对生成命令的相关介绍请参见“安全命令参考”中的“公钥管理”。
生成DSA密钥对时，要求输入的密钥模数的长度必须小于2048比特。
SSH服务器支持secp256r1和secp384r1类型的ECDSA密钥对。
如果服务器端不存在默认名称的本地RSA密钥对，则在服务器端执行SSH服务器相关命令行时（包括开启Stelnet/SFTP/SCP/NETCONF over SSH服务器、配置SSH用户、以及配置SSH服务器端的管理功能），系统会自动生成一个默认名称的本地RSA密钥对。
设备运行于FIPS模式时，服务器端仅支持ECDSA、RSA密钥对，因此请不要生成本地的DSA密钥对，否则会导致用户认证失败。

即使客户端都优先使用dsa，也需要看服务器是否支持dsa，像下面这种情况服务器只支持rsa，此时即使客户端优先使用dsa，协商结果依然是rsa。
*Sep 3 13:13:45:501 2018 GDSG-NCK-S7604X-1 SSHS/7/EVENT: -MDC=1; My proposal kex:
*Sep 3 13:13:45:501 2018 GDSG-NCK-S7604X-1 SSHS/7/EVENT: -MDC=1; Kex strings(0): ecdh-sha2-nist

p256,ecdh-sha2-nistp384,diffie-hellman-group-exchange-sha1,diffie-hellma-group14-sha1,diffie-hellman-group1-sha1
*Sep 3 13:13:45:501 2018 GDSG-NCK-S7604X-1 SSHS/7/EVENT: -MDC=1; Kex strings(1): ssh-rsa
*Sep 3 13:13:45:502 2018 GDSG-NCK-S7604X-1 SSHS/7/EVENT: -MDC=1; Peer proposal kex:
*Sep 3 13:13:45:502 2018 GDSG-NCK-S7604X-1 SSHS/7/EVENT: -MDC=1; Kex strings(0): diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
*Sep 3 13:13:45:502 2018 GDSG-NCK-S7604X-1 SSHS/7/EVENT: -MDC=1; Kex strings(1): ecdsa-sha2-nistp256,ssh-dss,ssh-rsa

修改ssh2 algorithm public-key rsa dsa，优先使用rsa后，设备登录正常