某局点 S7506E 6616p01 ssh登入不上

SSH 软件问题 **许鹏鹏** 2024-03-28 发表

问题描述

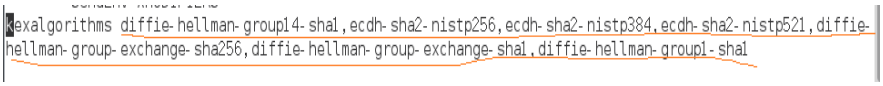
问题描述：客户使用第三方设备使用ssh登入我们设备失败
可以正常登录6708p05的设备，但是无法登录 6616p01 的设备
登录不上提示：incorrect signature

debug3: receive packet: type 33
debug1: got SSH2_MSG_KEX_DH_GEX_REPLY
debug1: Server host key: ssh-rsa SHA256:o5+/cjEKNcxQqAga6QkOMDzR8jUfqBs8TK66ZGzCK5w
debug3: hostkeys_foreach: reading file "/home/eccnet/.ssh/known_hosts"
debug3: record_hostkey: found key type RSA in file /home/eccnet/.ssh/known_hosts:1959
debug3: load_hostkeys: loaded 1 keys from 11.44.11.63
debug1: Host '11.44.11.63' is known and matches the RSA host key.
debug1: Found key in /home/eccnet/.ssh/known_hosts:1959
debug2: bits set: 2060/4096
ssh_dispatch_run_fatal: Connection to 11.44.11.63 port 22: incorrect signature
[eccnet@T-NMP-ZJ-PROBE ~]$

过程分析

问题定位：
有两种可能：
可能一：
在客户端清除保存的我司设备对应公钥（一般放在~/.ssh/ known_hosts，已ip地址作为索引），重新登录试试

可能二：
还有一种可能是和算法有关



现场堡垒机是linux系统，需要确认客户端支持的算法类型是否有diffie-hellman-group14-sha1算法，如果有将该算法写在最前边，没有则添加该算法，修改方式如下：
修改/etc/ssh/ssh_config，添加下面一行：
kexalgorithms diffie-hellman-group14-sha1，
在修改完算法以后如果还不能登录可以删除 /root/.ssh/known_hosts文件后在尝试登录

解决方法

问题解决；
现场按照方案二操作解决了，另外也可以升级6710P03，后续新版本也解决了该问题