V7平台防火墙D022版本SSH与ACG1000加密算法不一致导致通过防火墙无法SSH到ACG命令行问题

其他 刘嘉炜 2019-10-16 发表

组网及说明

不涉及

问题描述

现场ACG开启SSH认证，用户通过CRT或者Xshell SSH到ACG1000命令行正常，但是通过内网中一台F5000防火墙命令行却无法SSH到ACG命令行。

过程分析

1、 首先确认ACG配置中是否有限制登录用户，在收集配置分析ACG本没有限制登录用户的配置。

收集命令：display running-config

!

user administrator admin local secret 4wOYmbRjpR5d+FZdz81r/gB1x7Z4nP30jzMANhxZgvZh+SKAeUkFmWeJdzfrle6 authorized-table admin

user administrator admin authorized-address first **0.0.0.0/0**

2、在防火墙访问ACG时在防火墙开启Debug，Debug信息收发现防火墙与ACG加密算法不匹配导致了SSH登录失败问题。

<H3C>debugging ssh client all

<H3C>terminal monitor

<H3C>terminal debugging

<binjiang-ipsec>ssh2 1.2.3.32 9422

Username: admin

Press CTRL+C to abort.

Connecting to 1.2.3.32 port 9422.

*Aug 1 15:38:00:372 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Connection established.

<binjiang-ipsec>*Aug 1 15:38:00:536 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Remote protocol version 2.0, remote software version OpenSSH_7.5

*Aug 1 15:38:00:536 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Enabling compatibility mode for protocol 2.0

*Aug 1 15:38:00:537 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Get self version string Comware-7.1.064

*Aug 1 15:38:00:537 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Local version string SSH-2.0-Comware-7.1.064

*Aug 1 15:38:00:538 2019 binjiang-ipsec SSHC/7/MESSAGE: -COntext=1; Prepare packet[20].

*Aug 1 15:38:00:545 2019 binjiang-ipsec SSHC/7/MESSAGE: -COntext=1; Received packet type 20.

*Aug 1 15:38:00:546 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Received SSH2_MSG_KEXINIT.

*Aug 1 15:38:00:546 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; My proposal kex:

*Aug 1 15:38:00:546 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(0): diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1

*Aug 1 15:38:00:546 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(1): ecdsa-sha2-nistp256,ssh-dss,ssh-rsa

*Aug 1 15:38:00:546 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(2): aes128-cbc,aes256-cbc,3des-cbc,des-cbc

*Aug 1 15:38:00:546 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(3): aes128-cbc,aes256-cbc,3des-cbc,des-cbc

*Aug 1 15:38:00:546 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(4): hmac-sha1,hmac-sha1-96,hmac-md5,hmac-md5-96

*Aug 1 15:38:00:546 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(5): hmac-sha1,hmac-sha1-96,hmac-md5,hmac-md5-96

*Aug 1 15:38:00:546 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(6): none,zlib,zlib@openssh.com

*Aug 1 15:38:00:546 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(7): none,zlib,zlib@openssh.com

*Aug 1 15:38:00:546 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(8):

*Aug 1 15:38:00:546 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(9):

*Aug 1 15:38:00:546 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Peer proposal kex:

*Aug 1 15:38:00:546 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(0): curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1

*Aug 1 15:38:00:546 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(1): ssh-rsa,rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256

*Aug 1 15:38:00:546 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(2): chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com

*Aug 1 15:38:00:546 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(3): chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com

*Aug 1 15:38:00:546 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(4): umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1

*Aug 1 15:38:00:547 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(5): umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1

*Aug 1 15:38:00:547 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(6): none,zlib@openssh.com

*Aug 1 15:38:00:547 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(7): none,zlib@openssh.com

*Aug 1 15:38:00:547 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(8):

*Aug 1 15:38:00:547 2019 binjiang-ipsec SSHC/7/EVENT: -COntext=1; Kex strings(9):

%Aug 1 15:38:00:547 2019 binjiang-ipsec SSHS/6/SSHS_ALGORITHM_MISMATCH: -COntext=1;**SSH client 1.2.3.32 failed to log in because of encryption algorithm mismatch.**

*Aug 1 15:38:00:547 2019 binjiang-ipsec SSHC/7/ERROR: -COntext=1; No matching cipher found: client aes128-cbc,aes256-cbc,3des-cbc,des-cbc server chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com

解决方法

实验室测试与客户现场同版本设备测试，当版本在version 7.1.064, Release 9320P16时会出现和现场一致的现象，将版本升级官网最新版本9333P20时问题解决，判断是防火墙老版本支持的加密算法与ACG不一致导致， 升级软件版本后解决。

注：Release 9320P1对应内部版本**D022**SP16、Release 9333P20对应内部版本**D032**SP20，升级版本确认版本至D032版本即可。