F1030防火墙SSH因超过会话连接数导致登录失败经验案例

其他 葛松炜 2021-03-29 发表

组网及说明

不涉及

问题描述

SSH登陆防火墙失败，提示SSH会话超过最大数32个

<FW>ssh2 127.0.0.1

Username: admin

Press CTRL+C to abort.

Connecting to 127.0.0.1 port 22.

<FW>%Mar 8 10:49:34:497 2021 FW SSHS/6/SSHS_REACH_SESSION_LIMIT: -COntext=1;**SSH client 127.0.0.1 failed to log in. The current number of SSH sessions is 33. The maximum number allowed is (32).**

过程分析

起初想要通过调整连接数让使其能够连接更多会话查看防火墙支持命令，发现可以通过如下命令设置同时在线的最大SSH用户连接数，但是缺省情况下，同时在线的最大SSH用户连接数已经为最大值32（不同型号设备规格可能存在不同），无法将其调整到更高的数值。

设置同时在线的最大SSH用户连接数。

aaa session-limit ssh max-sessions

缺省情况下，同时在线的最大SSH用户连接数为32。

系统资源有限，当前在线SSH用户数超过设定的最大值时，系统会拒绝新的SSH连接请求。该值的修改不会对已经在线的用户连接造成影响，只会对新的用户连接生效。

后续怀疑SSH会话没有老化所以新的SSH用户无法接入，于是让现场重启SSH服务（undo ssh server enable后ssh server enable）释放无法不老化的会话进行测试，但是重新使能后仍有问题，于是让现场收集如下信息，发现并没有SSH会话和用户在线：

<FW>display ssh user-information

Total ssh users:0

<FW>display ssh server session

UserPid SessID Ver Encrypt State Retries Serv Username Idx

[FW]display users

Idx Line Idle Time Pid Type

+ 4 VTY 0 00:00:00 Mar 08 12:38:43 10505 TEL

Following are more details.

VTY 0 :

User name: admin

Location: 192.168.10.55

\+ : Current operation user.

F : Current operation user works in async mode.

现场因为开启了安全策略日志且流量较大，所以很多日志被冲刷掉。让现场关闭安全策略日志观察，发现了有一个地址为117.2.73.223的终端每隔几秒就会尝试SSH一次设备，且一直在报错SSH会话已达到最大。与现场确认发现该IP并非测试终端IP，于是怀疑设备受到该IP终端攻击，建议现场先通过策略禁掉该IP，后续排查该IP地址来源。现场禁掉该IP后过一段时间就恢复正常，排查后发现确实是设备受到了攻击导致SSH登录不上。

%Mar 8 11:41:55:144 2021 FW SSHS/6/SSHS_REACH_SESSION_LIMIT: SSH client 117.2.76.223 failed to log in. The current number of SSH sessions is 33. The maximum number allowed is (32).

%Mar 8 11:41:58:384 2021 FW SSHS/6/SSHS_REACH_SESSION_LIMIT: SSH client 117.2.76.223 failed to log in. The current number of SSH sessions is 33. The maximum number allowed is (32).

%Mar 8 11:42:04:817 2021 FW SSHS/6/SSHS_REACH_SESSION_LIMIT: SSH client 117.2.76.223 failed to log in. The current number of SSH sessions is 33. The maximum number allowed is (32).

%Mar 8 11:42:13:496 2021 FW SSHS/6/SSHS_REACH_SESSION_LIMIT: SSH client 117.2.76.223 failed to log in. The current number of SSH sessions is 33. The maximum number allowed is (32).

解决方法

后续遇到此类问题，首先通过命令查看一下是否已有大量用户进行SSH连接导致会话连接数超过规格；如果并没有用户导致连接数超规格的话，建议开启信息中心查看是否有IP反复SSH登录设备导致SSH会话连接数被消耗，如果频率较高，很可能是设备收到了攻击，可以将对应IP在安全策略内阻断进行观察。