某局点 S7606 TELNET acl异常

Telnet　**苏亚东**　2023-10-05 发表

问题描述

现场通过如下acl来限制telnet登陆设备的用户，但是当前发现如下acl配置后，终端10.3.26.33就无法登陆了，理论上该终端的ip能够命中rule 2中的permit规则，但是实际上终端的访问受到限制，将对应acl删除后终端可正常登陆。

```
[BJ-BJ-CYM_ZaiBei-C-S-1.OA]display acl 2001
Basic IPv4 ACL 2001, 7 rules,
ACL's step is 5, start ID is 0
rule 1 permit source 10.3.27.0 0.0.0.255
rule 2 permit source 10.3.26.0 0.0.0.255          //测试终端10.3.26.33能匹配上这条
rule 3 permit source 10.3.0.0 0.0.0.255
rule 4 permit source 10.3.56.248 0
rule 5 permit source 10.143.19.83 0
rule 6 permit source 10.143.19.84 0
rule 70 permit source 10.3.134.0 0.0.0.255
telnet server acl 2001
ssh server acl 2001
```

过程分析

（1）让现场测试了下，不配置acl限制登陆时，终端10.3.26.33可以正常telnet登陆，并且debug能debug到信息；但是如果配置上该acl后，就无法登陆了，设备上也debug不到信息。

[BJ-BJ-CYM_ZaiBei-C-S-1.OA]%Jul 27 22:32:47:283 2023 BJ-BJ-CYM_ZaiBei-C-S-1.OA SHELL/5/SHELL_LOGOUT: -MDC=1; oaroot logged out from 10.3.26.33.
*Jul 27 22:32:47:291 2023 BJ-BJ-CYM_ZaiBei-C-S-1.OA TELNETD/7/RUN: -MDC=1; Successfully closed PTY.
*Jul 27 22:32:47:295 2023 BJ-BJ-CYM_ZaiBei-C-S-1.OA TELNETD/7/RUN: -MDC=1; Received the SIGCHLD signal.
*Jul 27 22:32:47:296 2023 BJ-BJ-CYM_ZaiBei-C-S-1.OA TELNETD/7/RUN: -MDC=1; Successfully cleared the user information.
[BJ-BJ-CYM_ZaiBei-C-S-1.OA]telnet server acl 2001 //配置acl限制登陆后
[BJ-BJ-CYM_ZaiBei-C-S-1.OA]dis
[BJ-BJ-CYM_ZaiBei-C-S-1.OA]display acl 2001 //规则里也都是permit的规则
Basic IPv4 ACL 2001, 7 rules,
ACL's step is 5, start ID is 0
rule 1 permit source 10.3.27.0 0.0.0.255
rule 2 permit source 10.3.26.0 0.0.0.255
rule 3 permit source 10.3.0.0 0.0.0.255
rule 4 permit source 10.3.56.248 0
rule 5 permit source 10.143.19.83 0
rule 6 permit source 10.143.19.84 0
rule 70 permit source 10.3.134.0 0.0.0.255

[BJ-BJ-CYM_ZaiBei-C-S-1.OA]quit
<BJ-BJ-CYM_ZaiBei-C-S-1.OA>%Jul 27 22:33:45:887 2023 BJ-BJ-CYM_ZaiBei-C-S-1.OA CFGMAN/5/CFGMAN_EXIT_FROM_CONFIGURE: -MDC=1; -Line=aux1/0-IPAddr=**-User=**; Exit from the system view or a feature view to the user view.

<BJ-BJ-CYM_ZaiBei-C-S-1.OA> //此时无法登陆，也无debug打印了

（2）经初步分析，telnet中调用的acl是软件acl，和常规的包过滤、PBR、MQC等硬件acl不同，需要考虑telnet访问地址是否携带vpn，如果有vpn的话，需要在对应acl中添加相关参数。而现场实际登陆时使用的是带外网管口，配置了vpn，修改rule规则后恢复。

rule 2 permit vpn-instance mgmt source 10.3.26.0 0.0.0.255

解决方法

1、修改rule规则携带vpn参数解决。