SMP不显示防火墙发送的配置日志

info-center 孔凡安 2022-08-11 发表

组网及说明

不涉及

问题描述

SMP不显示防火墙发送的配置日志

过程分析

首先确保防火墙上配置正确，是否有如下命令：

info-center source CFGLOG loghost level informational

防火墙缺省info-center发送日志级别为：

表1-11 日志信息的缺省输出规则

输出方向	日志信息来源	开关	等级
控制台	所有支持的模块	开	debugging
监视终端	所有支持的模块	关	debugging
日志主机	所有支持的模块	开	informational
日志缓冲区	所有支持的模块	开	informational
日志文件	所有支持的模块	开	informational

在SMP平台底层抓包，查看报文是否发送过来：

```
[root@cyber ~]#
[root@cyber ~]# tcpdump -vv -i eth0 udp and src 11.206.0.34 dst port 514
tcpdump: syntax error
[root@cyber ~]# tcpdump -vv -i eth0 udp and src 11.206.0.34 and dst port 514
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 byt
es
16:38:54.062127 IP (tos 0x0, ttl 251, id 18186, offset 0, flags [none], proto UD
P (17), length 147)
    11.206.0.34.24192 > lcahost.syslog: [udp sum ok] SYSLOG, length: 119
        Facility local7 (23), Severity info (6)
        Msg: Jul 15 16:38:54 2022 ZBJD-F1050 %%10SHELL/6/SHELL_CMD: -Line=vty0-I
PAddr=10.1.110.201-User=admin; Command is save\0x00
        0x0000:  3c31 3930 3e4a 756c 2031 3520 3136 3a33
        0x0010:  383a 3534 2032 3032 3220 5a42 4a44 2d46
        0x0020:  3130 3530 2025 2531 3053 4845 4c4c 2f36
        0x0030:  2f53 4845 4c4c 5f43 4d44 3a20 2d4c 696e
        0x0040:  653d 7674 7930 2d49 5041 6464 723d 3130
        0x0050:  2e31 2e31 3130 2e32 3031 2d55 7365 723d
        0x0060:  6164 6d69 6e3b 2043 6f6d 6d61 6e64 2069
        0x0070:  7320 7361 7665 00
16:38:56.367689 IP (tos 0x0, ttl 251, id 18200, offset 0, flags [none], proto UD
P (17), length 135)
    11.206.0.34.24192 > lcahost.syslog: [udp sum ok] SYSLOG, length: 107
        Facility local7 (23), Severity info (6)
        Msg: Jul 15 16:38:56 2022 ZBJD-F1050 %%10SHELL/6/SHELL_CMD_CONFIRM: Conf
irm option of command save is yes.\0x00
        0x0000:  3c31 3930 3e4a 756c 2031 3520 3136 3a33
        0x0010:  383a 3536 2032 3032 3220 5a42 4a44 2d46
        0x0020:  3130 3530 2025 2531 3053 4845 4c4c 2f36
        0x0030:  2f53 4845 4c4c 5f43 4d44 5f43 4f4e 4649
        0x0040:  524d 3a20 436f 6e66 6972 6d20 6f70 7469
        0x0050:  6f6e 206f 6620 636f 6d6d 616e 6420 7361
        0x0060:  7665 2069 7320 7965 732e 00
16:38:59.376344 IP (tos 0x0, ttl 251, id 18214, offset 0, flags [none], proto UD
P (17), length 146)
```

发现有收到防火墙发送过来的配置日志。

目前SMP收的配置日志都是设备 CFGLOG 模块发的配置日志，也就是会识别报文头部是否有CFGLOG字样，从而针对日志类型进行归类。

解决方法

升级防火墙版本，满足版本说明书中的最低适配版本的要求。