

# 知 SMP综合日志审计平台看不到防火墙的审计日志

Syslog日志 王昕宇 2024-01-04 发表

## 组网及说明

不涉及

## 告警信息

不涉及

## 问题描述

Fw 侧抓包，看抓包飞书的审计日志已经发给 smp 了

```
01c0 34 2c 31 30 33 2c 31 30 30 30 30 01 0c 03 03 79 44:103:10 0;Policy
01d0 4e 61 6d 65 28 31 30 37 39 29 3d e6 b5 8b e8 af ..;Application(10
01e0 95 3b 41 70 70 6c 69 63 61 74 69 6f 6e 28 31 30 02)=FeiS hu;Behav
01f0 30 32 29 3d 46 65 69 53 68 75 3b 42 65 68 61 76 0r(1101)=Browse
0200 69 6f 72 28 31 31 30 31 29 3d 42 72 6f 77 73 65 r;Behavi orConten
0210 72 3b 42 65 68 61 76 69 6f 72 43 6f 6e 74 65 6e t(1102)= {Account
0220 74 28 31 31 30 32 29 3d 7b 41 63 63 6f 75 6e 74 (1103)= Password
022a 28 31 31 30 33 29 3d 2c 50 61 73 73 77 6f 72 64
```

```
Syslog 633 LOCAL7.INFO: Jan 04 12:32:44 2024 FW2 %10 VsysId:1 AUDIT/6/AUDIT_RULE #
```

smp侧tcpdump抓包，能收到飞书审计日志

```
0x0180: 3034 3029 3044 656e f930
13:03:30.734107 IP (tos 0x0, ttl 251, id 51257, offset 0, flags [none], proto UDP (17), length 620)
  192.168.0.103 >> 192.168.0.100: Syslog (6) [Len: 592]
  Facility local7 (23), Severity info (6)
  #0x0185: 0x0185 (0x0185) offset 0x00: Application(1100)=FeiShu;Behavior(1101)=Browser;BehaviorContent(1102)=Account(1103)=Password(1112)=Content(1104)=;Client(1110)=ME#;SoftVersion(1111)=
0x0000: 4c18 3030 3020 4a03 6a20 3034 2034 3158
0x0010: 3033 3a32 3020 3230 3234 2046 5732 2025
0x0020: 2331 3020 4072 7073 206d 3a31 2031 3525
```

## 过程分析

- [SMP不显示防火墙发送的配置日志 - 知了社区 \(h3c.com\)](#)
- [某局点SecPath F1000-AK165\(V7\)在SMP平台上显示不全日志 - 知了社区 \(h3c.com\)](#)
- [某局点 SecCenter SMP 安全业务管理平台 \(原SSM-G2\) 无法显示ips日志 - 知了社区 \(h3c.com\)](#)

## 解决方法

现场配置了vrrp，fw发出日志报文时，使用了接口下实际地址，smp上 业务ip 修改为fw发出的源地址后正常显示审计日志

