ACG上送给综合日志审计平台 的日志没有来源IP

ACG1000　叶红兵　2024-01-31 发表

组网及说明

设备型号和版本：

综合日志审计平台：CSAP-SA-AK640 E6101P08

应用控制网关：ACG1000-AK240 R6616p02

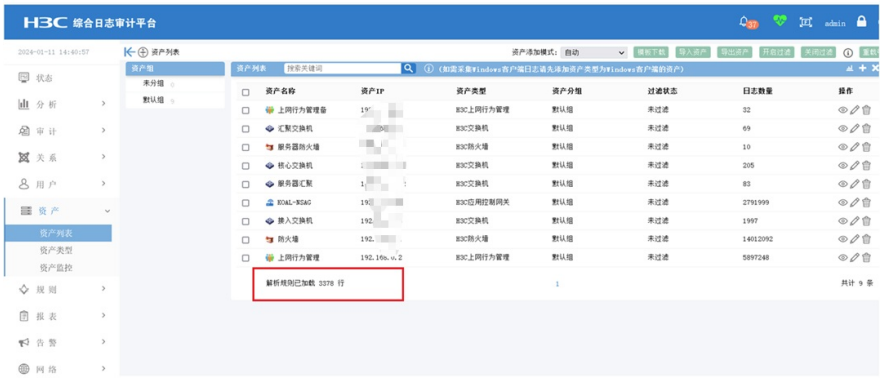
问题描述

综合日志审计平台接收到的ACG的日志没有来源IP，但是防火墙是可以识别到来源IP的

事件名称	事件类型	事件级别	接收时间	资产名称	资产IP	资产类型	来源IP	目的IP
其他事件	其他类型	信息	2024-01-11 12:00:10	上网行为管理	192.1	H3C上网行…		
其他事件	其他类型	信息	2024-01-11 12:00:10	上网行为管理	192.168.	H3C上网行…		
其他事件	其他类型	信息 事件级别:信息	024-01-11 12:00:10	上网行为管理	192.1	H3C上网行…		
其他事件	其他类型	信息	2024-01-11 12:00:10	上网行为管理	192.	H3C上网行…		
其他事件	其他类型	信息	2024-01-11 12:00:10	上网行为管理	192.	H3C上网行…		
其他事件	其他类型	信息	2024-01-11 12:00:10	上网行为管理	192.	H3C上网行…		
其他事件	其他类型	信息	2024-01-11 12:00:10	上网行为管理	192	H3C上网行…		
其他事件	其他类型	信息	2024-01-11 12:00:10	上网行为管理	19	H3C上网行…		
其他事件	其他类型	信息	2024-01-11 12:00:10	上网行为管理	19	H3C上网行…		
策略日志	策略管理	信息	2024-01-11 12:00:10	防火墙	192.	H3C防火墙	172.1	5…
策略日志	策略管理	信息	2024-01-11 12:00:10	防火墙	192.1	H3C防火墙	172. 4	114…
策略日志	策略管理	信息	2024-01-11 12:00:10	防火墙	192.16	H3C防火墙	172.1	121. 7…
策略日志	策略管理	信息	2024-01-11 12:00:10	防火墙	192.168.	H3C防火墙	172.1	

过程分析

1、刚开始怀疑是解析规则超规格导致解析异常，但是反馈解析规则并不多



2、因为综合日志审计平台可以收到并识别为日志，说明日志解析没有问题，因此怀疑是日志解析时匹配的关键字段有问题，导致识别不到，因此看了下详细日志

ACG的详细日志如下：

其他事件	其他类型	信息　2024-01-11 12:… 上网行为管理　192.168.0.2　H3C上网行为管理
原始日志	:	<6>Jan 11 12:07:08 H3C,1101037001231122650131 21,ipv4;3; policy_detail: src_ip=[ ]5;dst_ip=[ ].10;protocol=[ ];src_port=5[ ]1;dst_port=[ ]
资产类型	:	H3C上网行为管理
事件级别	:	信息
事件名称	:	其他事件
发生时间	:	2024-01-11 12:07:11
事件类型	:	其他类型
日志拆解	:	<6>Jan 11 12:07:08 H3C;1101037001231122650131 21;ipv4;3; policy_detail: src_ip=[ ];dst_ip=[ ]0;protocol=TCP; src_port=[ ]1;dst_port=[ ];in_interface=[ ];out_interface=[ ];policyid[ ];action=permit;Content="[ ]7*: The packet pass because the firewall policy is permit"

防火墙的详细日志如下：

源端口	:	57197
件类型	:	策略管理
志拆解	:	<190>Jan 11 14:03:35 2024 FW1000 %%10FILTER/6/FILTER_ZONE_IPV4_EXECUTION: -DevIP=1[ ]1; SrcZoneName(1025)=T[ ]t; DstZoneName(1035)=U[ ]; Type(1067)=[ ]; SecurityPolicy(1072)=[ ] RuleID(1078)=0; Protocol(1001)=TCP; Application(1002)=h[ ]s; SrcIPAddr(1003)=[ ]6 SrcPort(1004)=[ ]7; SrcMacAddr(1021)=[ ] DstIPAddr(1007)=[ ]15 DstPort(1008)=[ ]; MatchCount(1069)=[ ]; Event(1048)=Permit;

解决方法

后经产品线远程发现，我们的ACG1000添加资产的时候要选择 应用控制网关，现场是自定义了一个H3C上网行为管理，导致日志识别不完整，修改资产类型后已正常。

应用控制网关产品

- H3C SecPath ACG1000系列应用控制网关
- H3C SecPath ACG1000-V系列应用控制网关
- H3C SecPath ACG1000 BA用户行为感知平台
- H3C SecBlade ACG插卡
- H3C SecPath ACG1000日志分析与管理平台