ACG1000 日志分析与管理平台下发配置模版失败

ACG1000 曾招维 2023-10-31 发表

组网及说明

ACG1000-AI-10通过ipsec vpn纳管到ACG1000 日志分析与管理平台。

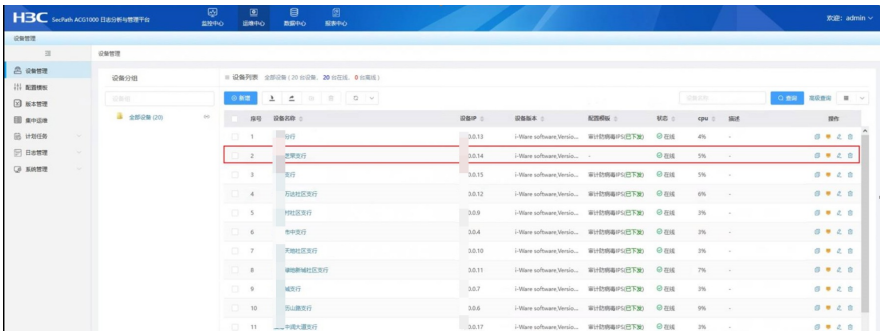
问题描述

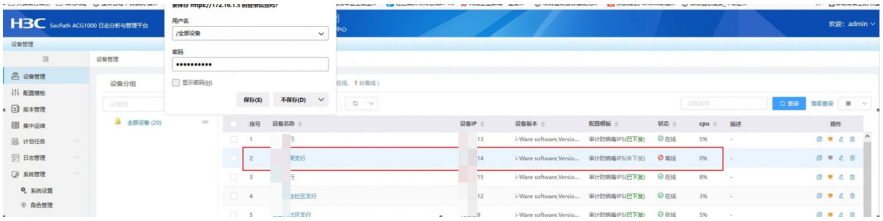
ACG1000 日志分析与管理平台下发配置模版后显示ACG1000-AI-10离线，删除配置模版后重新上线。

同一个配置模版下发到多台ACG1000，现场只有这台有异常。

版本信息：ACG1000-AI-10 R6614P10、平台版本 R0306P01

现象如图：未下发配置时显示正常上线，下发配置后显示“未下发、离线”





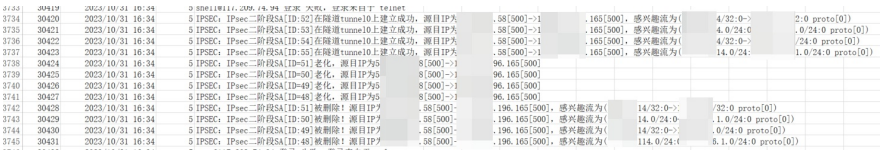
过程分析

1、平台侧信息：配置模版中只有审计策略和安全策略，规则都是全选、对象any，安全策略默认通过；有正常打3000个数量授权、ACG1000-AI-10不属于高端款型。

2、ACG1000-AI-10设备侧显示正常，担心相关策略对纳管有影响，我直接测试下发一个全局白名单，但是故障依旧。

3、ping和tcp syn测试正常。

4、 ACG1000-AI-10通过ipsec vpn纳管到ACG1000 日志分析与管理平，查看系统日志，有IPsec vpn隧道重新建立过程。



解决方法

经确认当 ipsec vpn 断开，相关平台注册流量就会走默认路由，生成一个NAT会话，vpn重新建后nat这条会话还未老化，vpn恢复正常后匹配反向会话，导致平台下发配置模版异常，虽然平台一直显示在线，只是在保活周期内，后面报文序上来，可能底层已经断开了。

解决方法：NAT策略的目的ip里排除一下平台IP地址x.x.1.5 ，还需要命令行ACG# clear ip connection all 配合清除历史会话 使用。