ACG1000无审计日志经验案例

应用审计 曹圣琪 2024-09-30 发表

组网及说明

ACG网桥模式二层部署在网络中

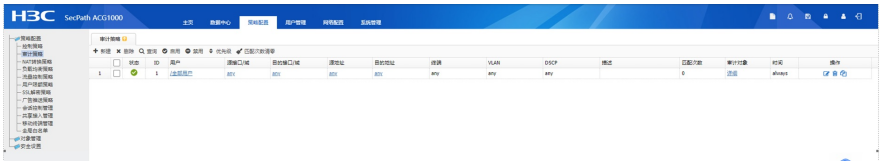
问题描述

现场配置应用审计后发现无审计日志

过程分析

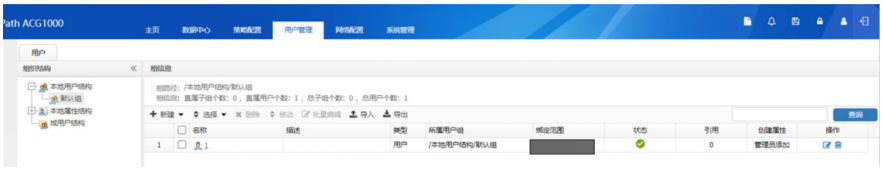
1、检查配置：

检查配置发现源目接口和源目地址匹配条件均为ANY，但是有个明显的问题是匹配次数没有增加



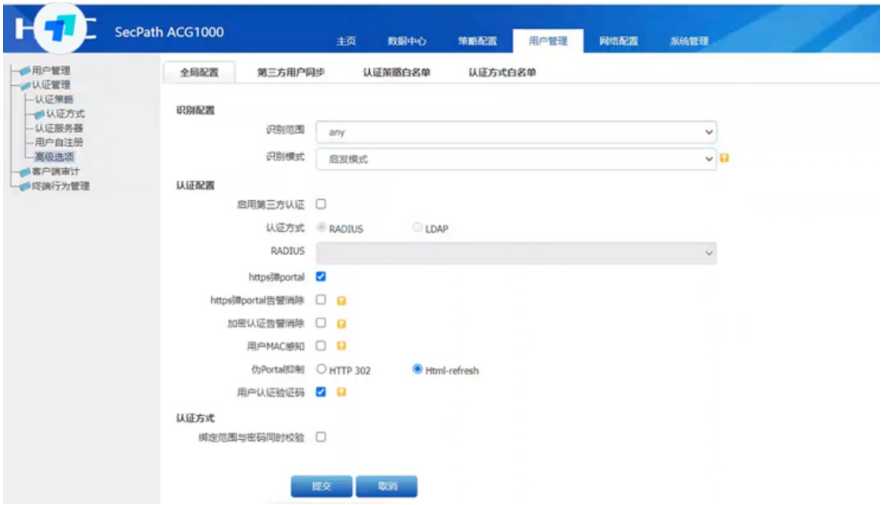
2、检查测试终端是否识别为用户

检查用户匹配条件为全部用户，查看用户管理中该用户已在用户组织结构下



3、检查识别范围和识别模式

用户管理高级选项下的识别范围应该配置为ANY，识别模式应该配置为启发模式，检查现场配置发现识别范围配置有误，修改为以下配置后策略匹配次数有增长，也能正常产生审计日志。



解决方法

现场修改用户识别范围为ANY、识别模式为启发模式后恢复正常。

对于ACG审计策略匹配次数为0的问题除了检查来回流量是否上到ACG上外，可以重点检查匹配条件限制、测试终端是否识别为用户、用户识别范围以及识别模式是否配置有误。