某局点F1000-AK115(V7) 没有应用审计日志经验案例

应用审计 info-center 茆新楼 2019-04-05 发表

组网及说明

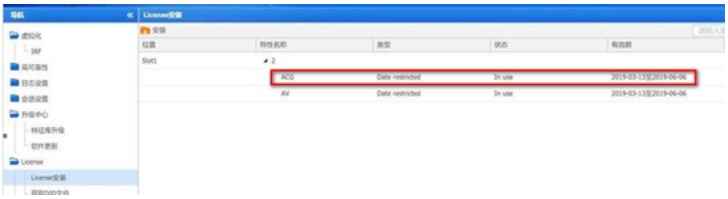
无

问题描述

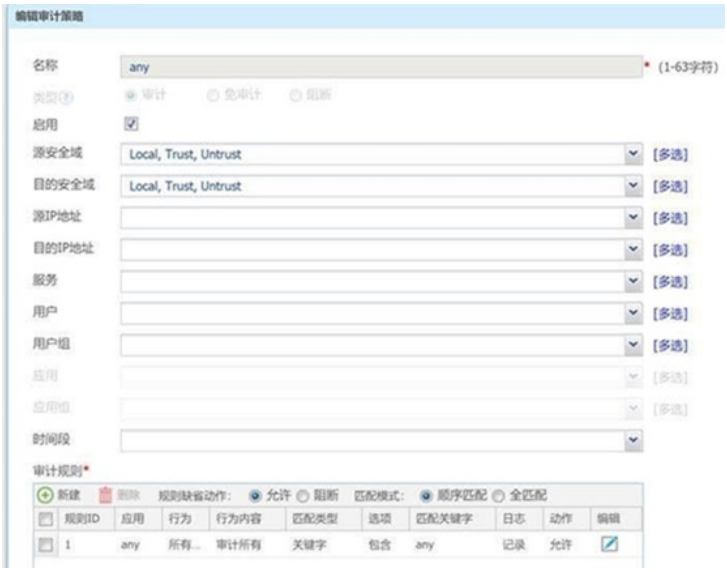
客户现场有台F1000-AK115(V7)作为出口设备，需要使用应用审计功能。相关配置完成后，发现没有任何日志产生。

过程分析

1、检查license和特征库版本：license正常安装，应用特征库也是官网最新。



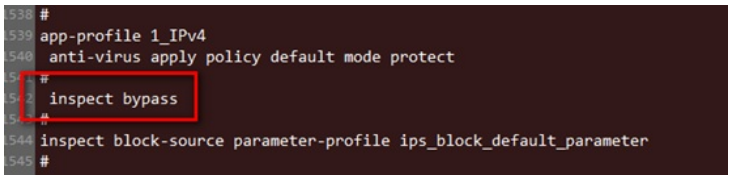
2、应用审计策略配置无异常：



3、在防火墙下行的ACG设备上看审计日志是可以审计到的，在防火墙的下行口抓包有报文收发，说明终端有流量触发并且也确保流量到达了防火墙。

4、在防火墙上配置session statistics enable和inspect activate，依旧无日志产生。

5、检查设备命令行配置发现，除了应用审计的相关配置外，设备的系统视图下还存在一条命令：



6、inspect bypass命令用来关闭应用层检测引擎功能，该功能缺省情况下处于开启状态。关闭应层检测引擎功能后，系统将不会对接收到的报文进行DPI深度安全处理。

解决方法

在设备的系统视图下，用undo inspect bypass命令开启应层检测引擎功能后，应用审计相关日志可以正常显示。