SecPath ACG1000系列部分邮件账号应用审计不到如何处理

应用审计 ACG1000 王奎银 2019-12-17 发表

问题描述

1、 交换机双向镜像流量镜像到ACG1000的G12接口，旁路部署模式。目前可以审计到上网日志、IM聊天日志都是实时统计的。但是现在邮件日志只能审计到2-3个账号的邮件记录。

2、 ACG1000抓包是可以抓取到的，但是审计不到邮箱日志。

解决方法

邮件日志支持 SMTP 、 POP3 、 IMAP 协议，部分邮箱客户端（网易邮箱大师 闪电邮）的 smtp是使用的 TLS 加密， TLS 加密不支持解密，该部分流量是看不到日志信息的。客户反馈能够审计到的账号使用的客户端为Foxmail，大部分人使用的邮箱客户端为阿里邮箱。通过抓包阿里邮箱都是加密的流量，不支持审计内容。如果要审计的话需要使用串联部署，并且是邮箱解密。