某局点ACG1000产品https流量及邮件无法审计成功的经验案例

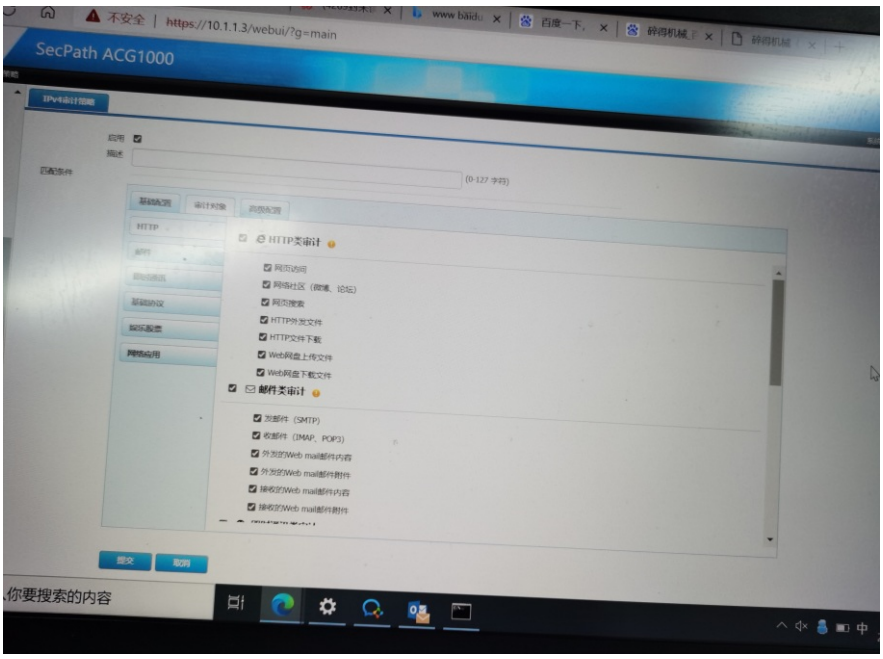
ACG1000 姜霁琛 2021-07-08 发表

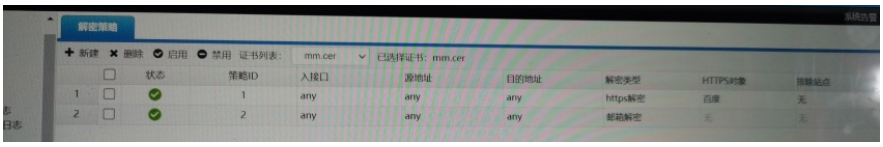
组网及说明

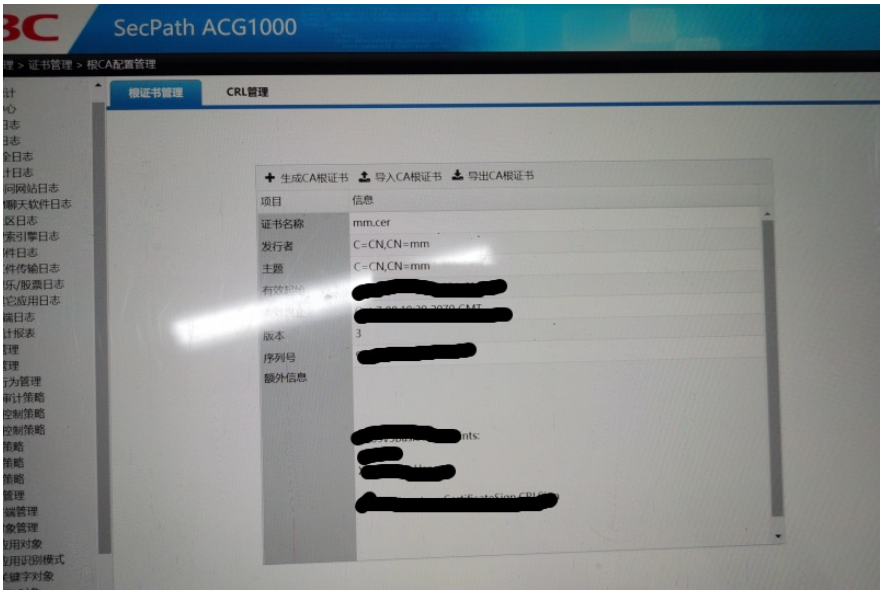
透明桥模式部署，bvi口已配置ip地址

问题描述

现场需要审计https流量以及邮箱，所以需要配置https解密，但是现场配置后，依然看不到审计日志





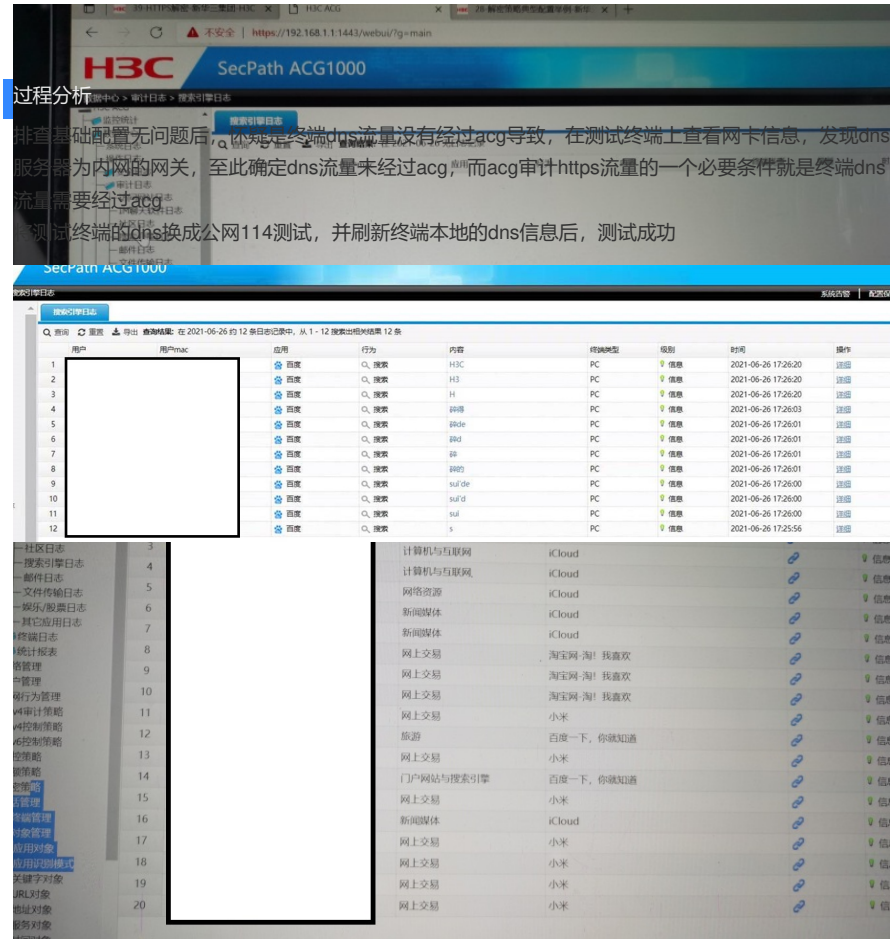


使用百度进行搜索，但是在acg上查看搜索引擎日志为空白

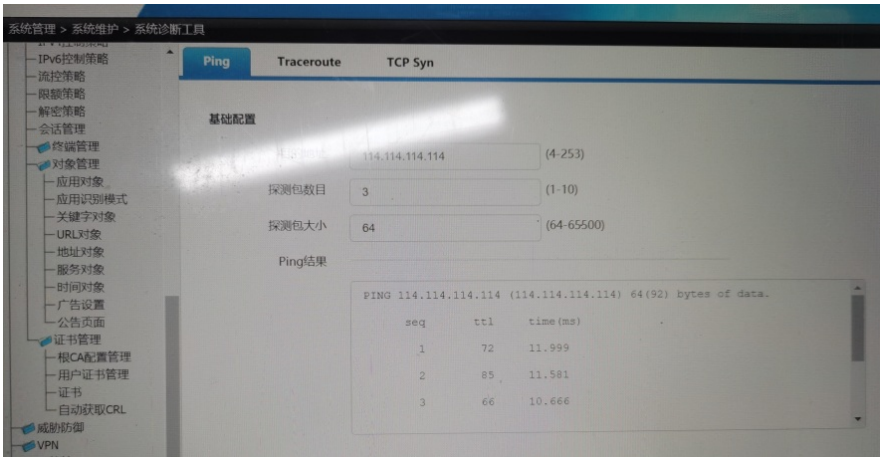
过程分析

排查基础配置无问题后，初始是终端dns流量没有经过acg导致，在测试终端上查看网卡信息，发现dns服务器为内网的网关，至此确定dns流量未经过acg，而acg审计https流量的一个必要条件就是终端dns流量需要经过acg

测试终端的dns换成公网114测试，并刷新终端本地的dns信息后，测试成功



测试ACG本身上外网是没问题的



解决方法

配置https解密时需要注意：

· 当设备DNS设置成全局模式时，用户电脑的DNS需要指向设备的入接口，以保证DNS过设备，解密策略才能生效。若DNS不经过设备的话，解密策略不生效。

· HTTPS解密策略所需证书为CA证书。

· 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。

· 部分HTTPS站点的客户端会进行证书校验，会显示非安全连接。

· 如果是网桥模式组网，配置步骤是一致的，需要注意的是网桥接口下一定要配置IP地址，并且要保证桥接口IP能访问外网。