

知 某局点ACG1000产品https流量及邮件无法审计成功的经验案例

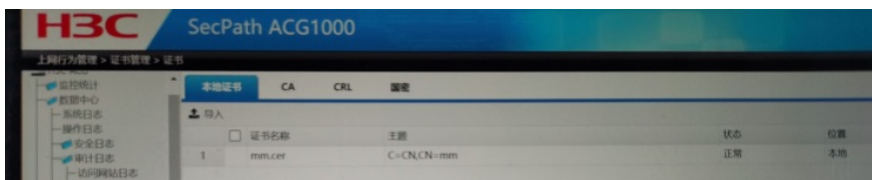
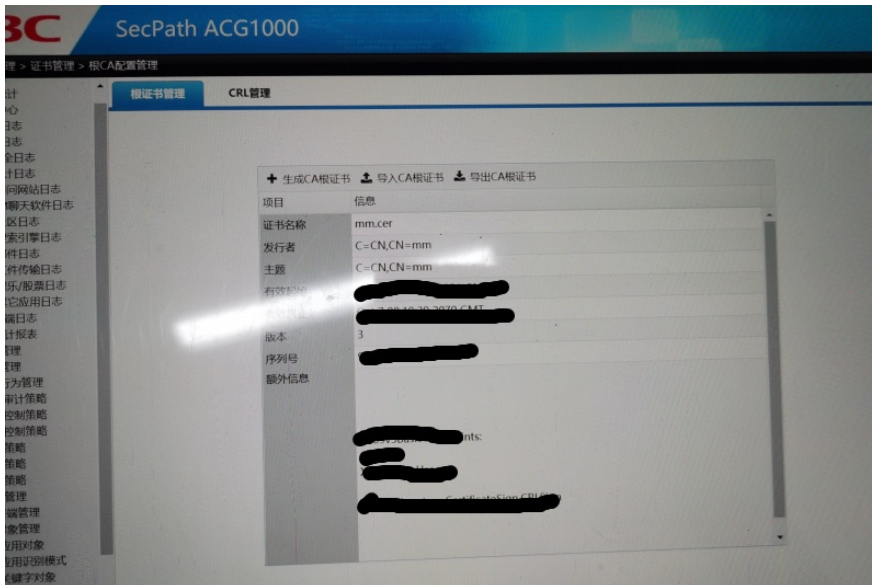
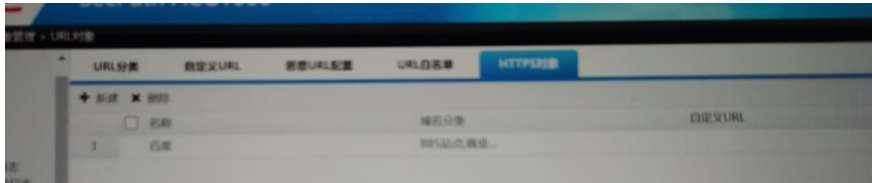
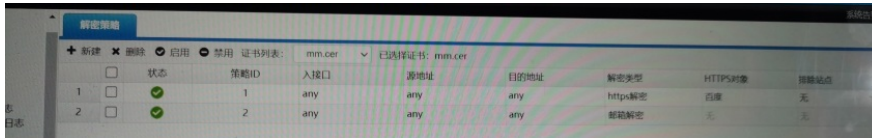
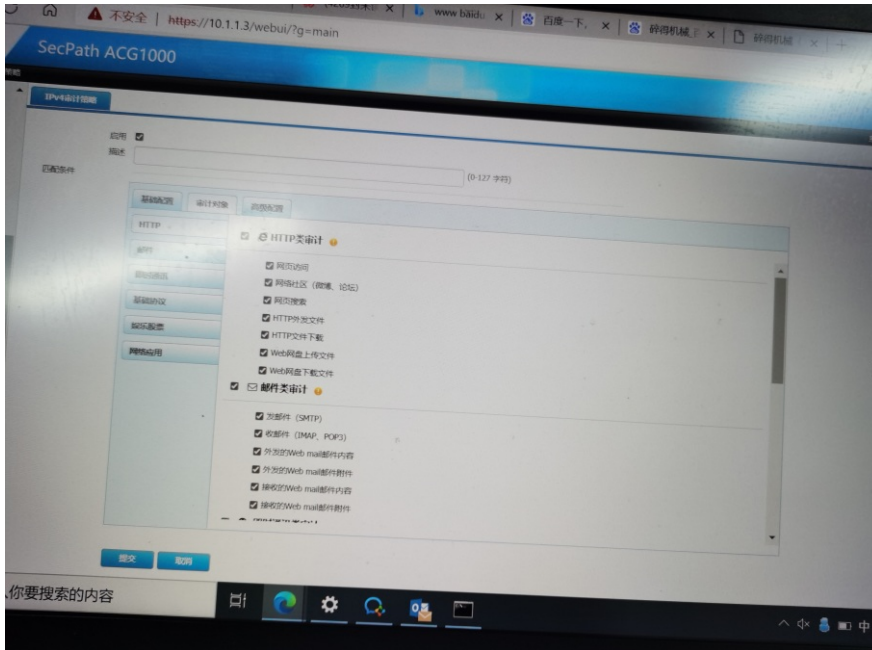
ACG1000 姜霖琛 2021-07-08 发表

组网及说明

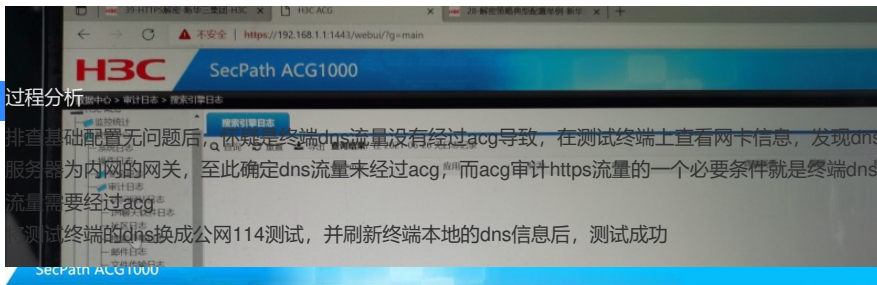
透明桥模式部署，bvi口已配置ip地址

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



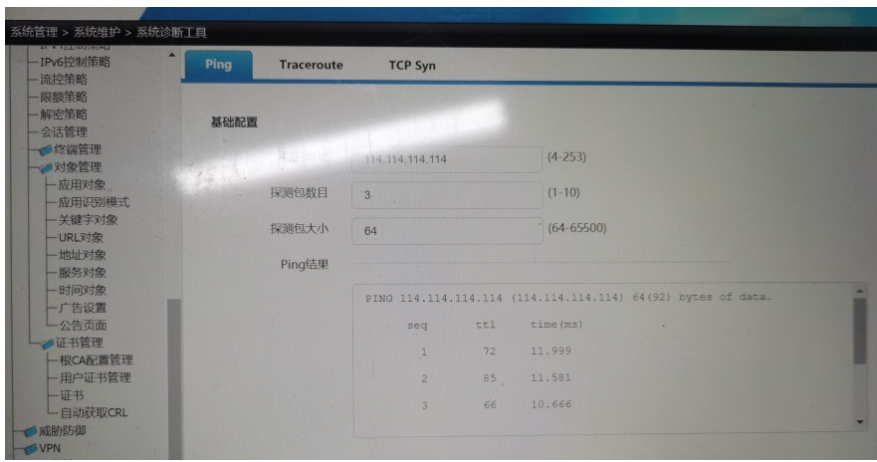
SecPath ACG1000

搜索引擎日志

在 2021-06-26 的 12 条日志记录中, 从 1 - 12 搜索出匹配结果 12 条

序号	用户	应用	行为	内容	终端类型	级别	时间	操作
1		百度	访问	H3C	PC	信息	2021-06-26 17:26:20	查看详情
2		百度	访问	H3	PC	信息	2021-06-26 17:26:20	查看详情
3		百度	访问	H	PC	信息	2021-06-26 17:26:20	查看详情
4		百度	访问	百度	PC	信息	2021-06-26 17:26:03	查看详情
5		百度	访问	百度	PC	信息	2021-06-26 17:26:01	查看详情
6		百度	访问	百度	PC	信息	2021-06-26 17:26:01	查看详情
7		百度	访问	百度	PC	信息	2021-06-26 17:26:01	查看详情
8		百度	访问	百度	PC	信息	2021-06-26 17:26:01	查看详情
9		百度	访问	百度	PC	信息	2021-06-26 17:26:00	查看详情
10		百度	访问	百度	PC	信息	2021-06-26 17:26:00	查看详情
11		百度	访问	百度	PC	信息	2021-06-26 17:26:00	查看详情
12		百度	访问	s	PC	信息	2021-06-26 17:25:56	查看详情

测试ACG本身上下网是没问题的



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。

