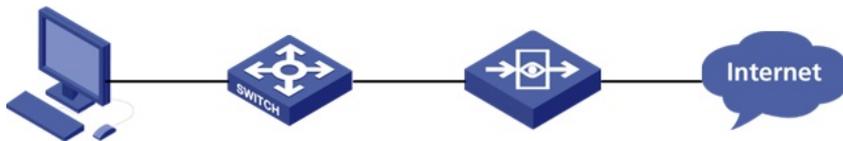


# 某局点ACG1000 HTTPS解密部分网站不生效的经验处理案例

应用审计 孙轶宁 2019-03-10 发表

## 组网及说明

拓扑如下:

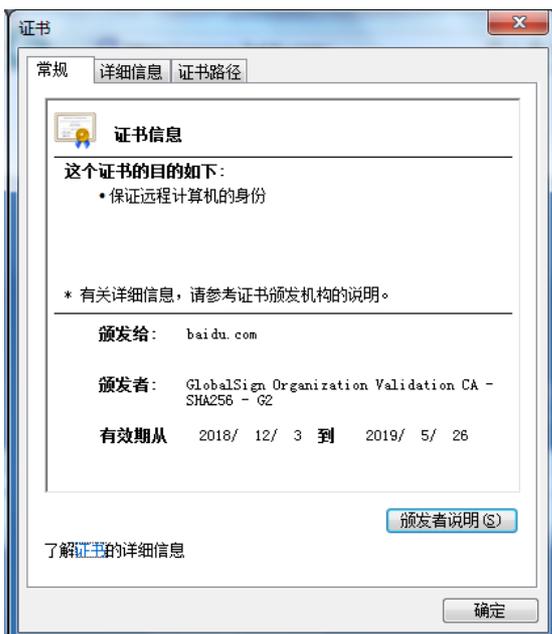
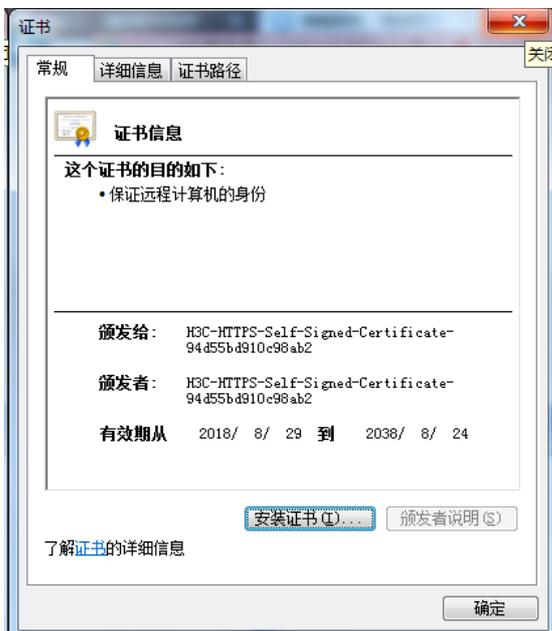


## 问题描述

某局点ACG1000配置https解密用于访问网站审计,配置完成后,发现部分网站能够被正常解密,能够在网站访问日志里面看到,但是部分网站无法被正常解密,看不到相关审计日志。

## 过程分析

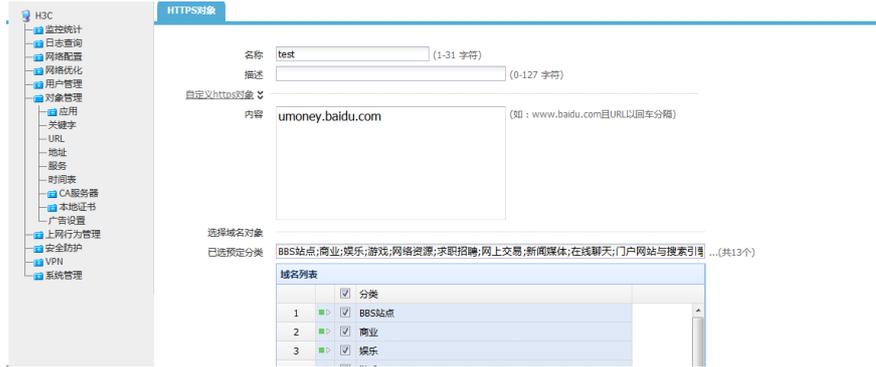
仔细对比正常解密网站与非正常解密网站的证书,发现正常解密网站的证书已经被替换为ACG的解密证书,但是非正常解密网站的证书没有被替换。



经过确认,发现ACG解密策略只会解密HTTPS对象里面的域名,不在对象里面的域名是不会被解密的

## 解决方法

在自定义https对象里面添加希望解密的域名后，问题解决。



The screenshot shows the H3C configuration interface for an HTTPS object. The left sidebar contains a navigation tree with the following items: H3C, 监控统计, 日志查询, 网络配置, 网络优化, 用户管理, 对象管理, 应用, 关键字, URL, 地址, 解密, 时间表, CA服务器, 本地证书, 广告设置, 上网行为管理, 安全防护, VPN, and 系统管理. The main area is titled "HTTPS对象" and contains the following fields:

- 名称: test (1-31 字符)
- 描述: (0-127 字符)
- 自定义https对象: umoney.baidu.com (如: www.baidu.com且URL以回车分隔)
- 选择域名对象: BBS站点;商业;娱乐;游戏;网络资源;求职招聘;网上交易;新闻媒体;在线聊天;门户网站与搜索引擎... (共13个)
- 已选预定分类:

Below the "已选预定分类" section is a table titled "域名列表" (Domain List):

分类	域名	操作
<input checked="" type="checkbox"/>	分类	
<input checked="" type="checkbox"/>	BBS站点	
<input checked="" type="checkbox"/>	商业	
<input checked="" type="checkbox"/>	娱乐	