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

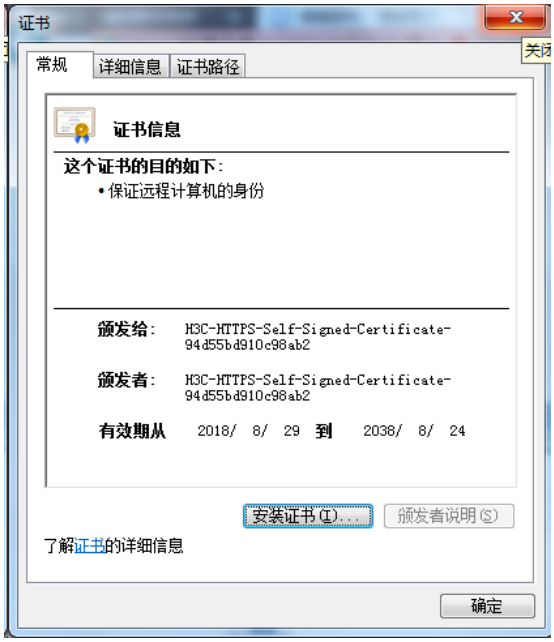
拓扑如下：

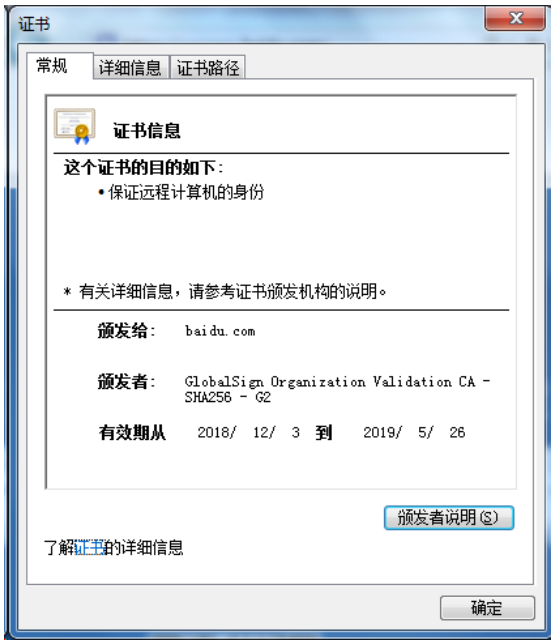
问题描述

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。