ACG解密配置后无法使用百度网盘

ACG1000 聂骋 2021-05-26 发表

组网及说明

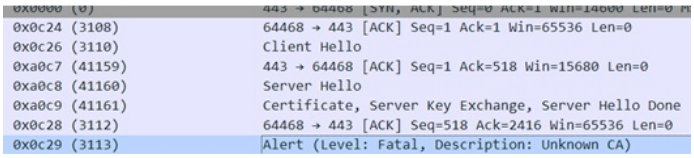
不涉及

问题描述

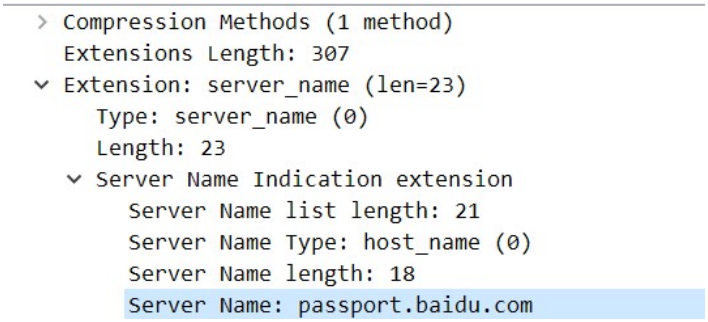
现场配置解密策略后，无法登陆百度网盘。

过程分析

进入ACG抓包发现在百度网盘报文交互中，有验证证书的操作。



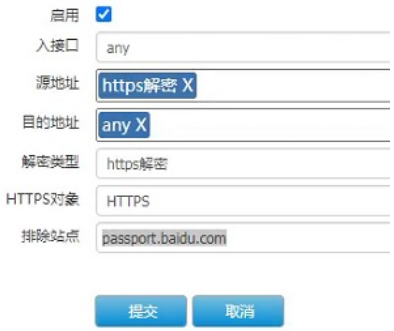
最后一个报文正好是百度网盘认为设备证书CA不可信因此不允许访问。同时在抓包中得到百度网盘登陆时验证证书的域名为passport.baidu.com



由此证明是百度网盘会验证证书，而设备CA证书是本地证书，非专业CA颁发导致百度网盘不予通过。

解决方法

1.解密策略中添加例外站点



2.找专业CA机构获取正式证书做HTTPS解密。

3.升级最新版特征库，默认排除该站点，并且不影响审计操作。