

# 知 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。

0x0000 (0)	443 → 64468 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0
0x0c24 (3108)	64468 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
0x0c26 (3110)	Client Hello
0xa0c7 (41159)	443 → 64468 [ACK] Seq=1 Ack=518 Win=15680 Len=0
0xa0c8 (41160)	Server Hello
0xa0c9 (41161)	Certificate, Server Key Exchange, Server Hello Done
0x0c28 (3112)	64468 → 443 [ACK] Seq=518 Ack=2416 Win=65536 Len=0
0x0c29 (3113)	Alert (Level: Fatal, Description: Unknown CA)

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录时验证证书的域名为passport.baidu.com

- > Compression Methods (1 method)
- Extensions Length: 307
- ▼ Extension: server\_name (len=23)
  - Type: server\_name (0)
  - Length: 23
  - ▼ Server Name Indication extension
    - Server Name list length: 21
    - Server Name Type: host\_name (0)
    - Server Name length: 18
    - Server Name: 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

启用	<input checked="" type="checkbox"/>
入接口	any
源地址	https解密 X
目的地址	any X
解密类型	https解密
HTTPS对象	HTTPS
排除站点	passport.baidu.com

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。

