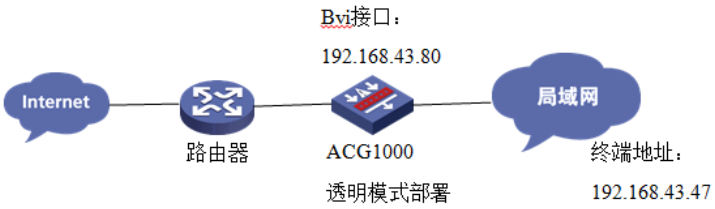
关于ACG1000系列设备F6608版本HTTPS解密过程分析

刘嘉炜 2018-04-13 发表

关于ACG1000系列设备F6608版本HTTPS解密过程分析

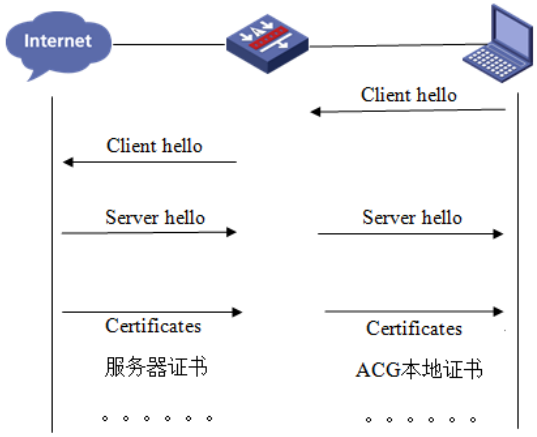
一、组网规划

ACG做透明模式部署



此案例假定您已经了解ACG HTTPS解密配置。

二、解密流程：



三、Wireshark报文分析

1、客户端向服务器提供下列信息：

```
182 10.575889 192.168.43.47 183.232.231.172 TLSv1.2 264 Client Hello
  [SEQ/ACK analysis]
Secure Sockets Layer
  TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 205
    Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 201
      Version: TLS 1.2 (0x0303)
      Random
      Session ID Length: 32
      Session ID: b6b8504ca664fe0452dfdd11d045b6d9848ed6cf792098b3...
      Cipher Suites Length: 48
      Cipher Suites (24 suites)
      Compression Methods Length: 1
      Compression Methods (1 method)
```

ACG在审计到客户端发出的client hello包后，立即仿制一个发向服务器。

No.	Time	Source	Destination	Protocol	Length	Info
11	11.524663	192.168.43.47	183.232.231.173	TLSv1.2	232	Client Hello
15	11.599264	192.168.43.80	183.232.231.173	TLSv1.2	571	Client Hello
17	11.669180	183.232.231.173	192.168.43.80	TLSv1.2	140	Server Hello
21	11.670598	183.232.231.173	192.168.43.80	TLSv1.2	739	Certificate
27	11.681486	183.232.231.173	192.168.43.80	TLSv1.2	392	Server Key Exchange

服务器向ACG回包。

No.	Time	Source	Destination	Protocol	Length	Info
11	11.524663	192.168.43.47	183.232.231.173	TLSv1.2	232	Client Hello
15	11.599264	192.168.43.80	183.232.231.173	TLSv1.2	571	Client Hello
17	11.669180	183.232.231.173	192.168.43.80	TLSv1.2	140	Server Hello
21	11.670598	183.232.231.173	192.168.43.80	TLSv1.2	739	Certificate
27	11.681486	183.232.231.173	192.168.43.80	TLSv1.2	392	Server Key Exchange
28	11.681594	183.232.231.173	192.168.43.80	TLSv1.2	63	Server Hello Done

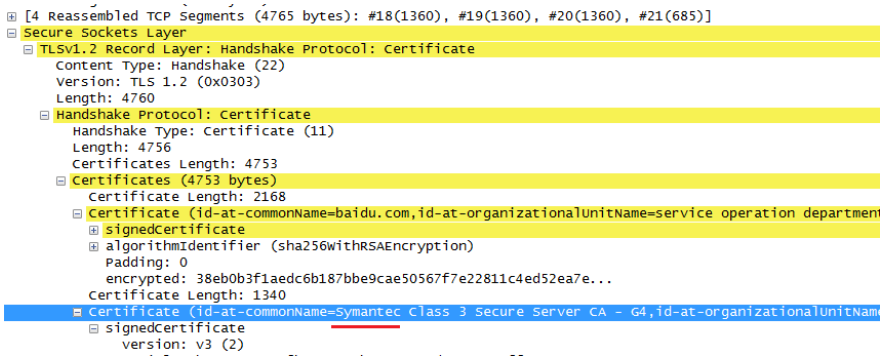
抓包看是服务器向客户端回包，实际上这个包已经被ACG篡改。

182	10.575889	192.168.43.47	183.232.231.172	TLSv1.2	264 Client Hello
187	10.900373	183.232.231.172	192.168.43.47	TLSv1.2	1514 Server Hello
188	10.900389	183.232.231.172	192.168.43.47	TLSv1.2	781 Certificate
191	10.906562	192.168.43.47	183.232.231.172	TLSv1.2	236 Client Key Exchange, Change Cipher Spec

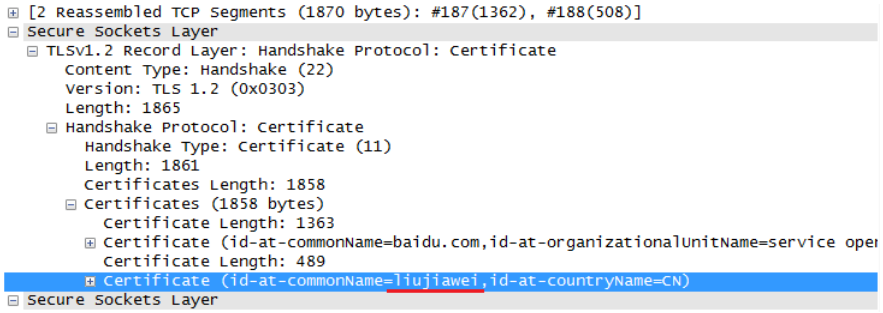
对比两份数据包完全不同。

在接下来的证书下发环节可见一斑

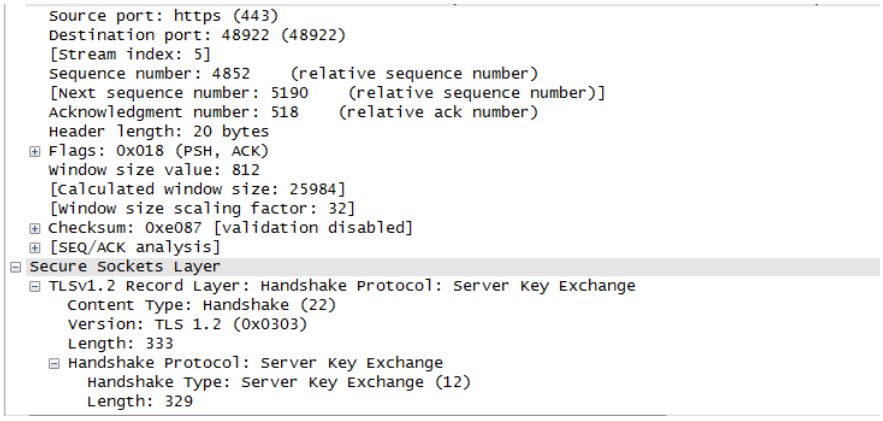
ACG拿到的客户端证书是百度下发的（证书主题：赛门铁克）



而客户端拿到的证书是由ACG下发的（证书主题：liujiawei）



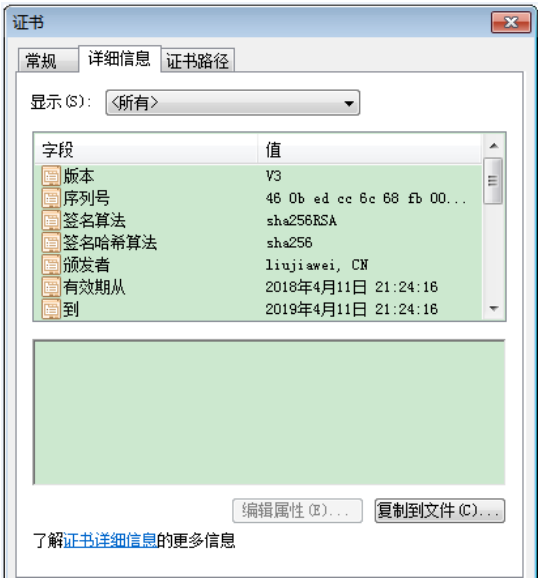
在服务器回应客户端时，发现服务器采用短暂RSA。



而在ACG发给客户时却使用常规RSA，说明访问数据其实是分成两段的，一段是ACG与服务器，另一段是ACG到客户端。下面密钥交互部分暂时省略。

四、测试结果：

客户端打开网页使用的证书


证书
常规
详细信息
证书路径
显示(S): <所有>
字段
值
版本
V3
序列号
46 0b ed cc 6c 68 fb 00...
签名算法
sha256RSA
签名哈希算法
sha256
颁发者
liujiawei, CN
有效期从
2018年4月11日 21:24:16
到
2019年4月11日 21:24:16
编辑属性(E)...
复制到文件(C)...
了解证书详细信息的更多信息