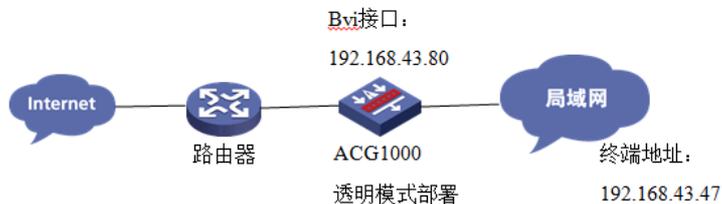


关于ACG1000系列设备F6608版本HTTPS解密过程分析

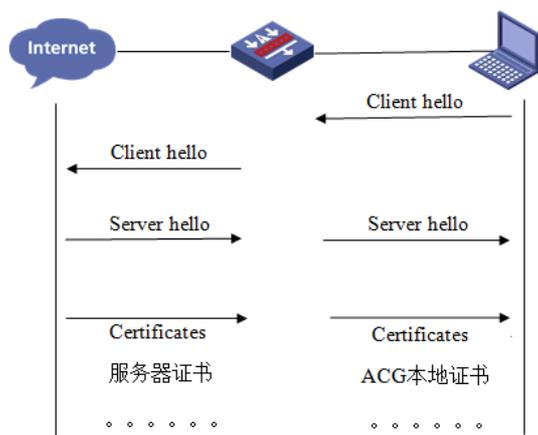
一、组网规划

ACG做透明模式部署



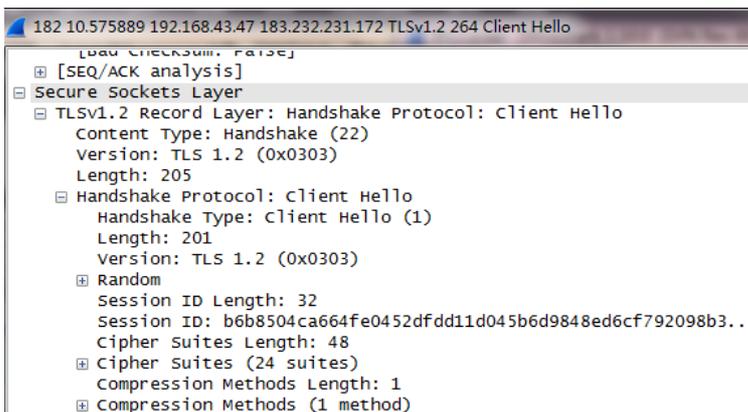
此案例假定您已经了解ACG HTTPS解密配置。

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:



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。

No.	Time	Source	Destination	Protocol	Length	Info
182	10.575889	192.168.43.47	183.232.231.172	TLSv1.2	264	Client Hello
183	10.900839	183.232.231.172	192.168.43.47	TLSv1.2	194	Server Hello
188	10.900839	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。

```

Secure Sockets Layer
  TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 81
  Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 77
    Version: TLS 1.2 (0x0303)
  Random
    gmtime: Apr 12, 2018 21:38:10.000000000 [XXXXXXXXXX]
    random_bytes: 3d91181f81c4ad69fcca51a840c958fe3d96cf918217aa...
    Session ID Length: 32
    Session ID: 3329e372b9519ece794b9883fcd1accad2e4060fa2be89...
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Compression Method: null (0)
    Extensions Length: 5
  Extension: renegotiation_info
    Type: renegotiation_info (0xff01)
    Length: 1
  Renegotiation Info extension
    Renegotiation info extension Length: 0
  Secure Sockets Layer
    TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 93
    Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 89
      Version: TLS 1.2 (0x0303)
    Random
      gmtime: Nov 24, 2023 06:20:24.000000000 [XXXXXXXXXX]
      random_bytes: 41e181fdbbf2a4ef88369ebbc9791c73228e27f28b7b1...
      Session ID Length: 32
      Session ID: 912dcf5befc404a079c9611f107f0467051a17a5a57c5610...
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc028)
      Compression Method: null (0)
      Extensions Length: 17
    Extension: server_name
      Type: server_name (0x0000)
      Length: 0
    Extension: renegotiation_info
      Type: renegotiation_info (0xff01)

```

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)

```

[4 Reassembled TCP Segments (4765 bytes): #18(1360), #19(1360), #20(1360), #21(685)]
Secure Sockets Layer
  TLSv1.2 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 4760
  Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 4756
    Certificates Length: 4753
  Certificates (4753 bytes)
    Certificate Length: 2168
  Certificate (id-at-commonName=baidu.com,id-at-organizationalUnitName=service operation department)
    signedCertificate
      algorithmIdentifier (sha256withRSAEncryption)
      Padding: 0
      encrypted: 38eb0b3f1aedc6b187bbe9cae50567f7e22811c4ed52ea7e...
      Certificate Length: 1340
  Certificate (id-at-commonName=Symantec Class 3 Secure Server CA - G4,id-at-organizationalUnitName=Symantec Corporation)
    signedCertificate
      version: v3 (2)

```

而客户端拿到的证书是由ACG下发的 (证书主题: liujiawei)

```

[2 Reassembled TCP Segments (1870 bytes): #187(1362), #188(508)]
Secure Sockets Layer
  TLSv1.2 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 1865
  Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 1861
    Certificates Length: 1858
  Certificates (1858 bytes)
    Certificate Length: 1363
  Certificate (id-at-commonName=baidu.com,id-at-organizationalUnitName=service operation department)
    Certificate Length: 489
  Certificate (id-at-commonName=liujiawei,id-at-countryName=CN)
Secure Sockets Layer

```

在服务器回应客户端时, 发现服务器采用短暂RSA。

```

Source port: https (443)
Destination port: 48922 (48922)
[Stream index: 5]
Sequence number: 4852 (relative sequence number)
[Next sequence number: 5190 (relative sequence number)]
Acknowledgment number: 518 (relative ack number)
Header length: 20 bytes
Flags: 0x018 (PSH, ACK)
window size value: 812
[Calculated window size: 25984]
[window size scaling factor: 32]
Checksum: 0xe087 [validation disabled]
[SEQ/ACK analysis]
Secure Sockets Layer
  TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 333
  Handshake Protocol: Server Key Exchange
    Handshake Type: Server Key Exchange (12)
    Length: 329

```

而在ACG发给客户端时却使用常规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

