

某局点SecPath F1005-GM 国密证书认证失败故障案例

IPSec VPN 单畅 2024-06-27 发表

问题描述

现场IPsec国密证书认证，建立失败。报错如下：

*Apr 29 10:50:10:789 2024 H3C PKI/7/PKI_DEBUG: Get verify result from cache successfully.

*Apr 29 10:50:10:790 2024 H3C PKI/7/PKI_DEBUG: Failed to verify certificate by domain test.

现场FW是使用对端签发的证书，包括CA证书、签名证书、加密证书和私钥，

对端设备厂商为卫士通，使用国密加密算法SM4，认证算法SM3，证书由我们发送请求文件给他们，他们签发给我们。

过程分析

抓包查看证书内容：从ike报文来看，对端ipsec使用的ca证书，和给我们颁发ca证书不一样，两边ca证书不一样，就无法验证证书是否可信

```
signedCertificate
  version: v3 (2)
  serialNumber: 0x14
  > signature (iso.2.156.10197.1.501)
  > issuer: rdnSequence (0)
    > rdnSequence: 7 items (pkcs-9-at-emailAddress=816...@qq.com,id-at-organizationalUnitName=宁德市...主机)
      > RDNSequence item: 1 item (id-at-commonName=宁德市...主机)
      > RDNSequence item: 1 item (id-at-countryName=CN)
      > RDNSequence item: 1 item (id-at-stateOrProvinceName=福建省)
      > RDNSequence item: 1 item (id-at-localityName=宁德市)
      > RDNSequence item: 1 item (id-at-organizationName=福建医...)
      > RDNSequence item: 1 item (id-at-organizationalUnitName=宁德市...)
      > RDNSequence item: 1 item (pkcs-9-at-emailAddress=816...qq.com)
```

让客户重新申请一个证书，导入他们设备的设备证书上。这样对端设备的设备证书和我们设备的证书，ca证书都一样。

debug查看还是有证书相关报错

*Jun 3 18:13:27:054 2024 Dfyy_IPSecVPN_Test PKI/7/PKI_DEBUG: Get verify result from cache successfully.

*Jun 3 18:13:27:055 2024 Dfyy_IPSecVPN_Test PKI/7/PKI_DEBUG: Failed to verify certificate by domain ndyb_domain.

```
18 2024-06-04 02:27:12.943377 18.72.229.251 18.72.229.251 IPv4 68 8x6954 (38484) 68 28 Good Fragmented IP protocol (proto=OP 17, off=1472, ID=9654) [Reassembled in #19]
19 2024-06-04 02:27:12.944088 18.72.229.251 18.72.229.251 ISAKMP 154 8x6954 (38484) 68 1493 Good Identity Protection (Warn Mode)
20 2024-06-04 02:27:12.948898 18.72.231.123 18.72.231.123 ISAKMP 106 8x283a (38298) 255 84 Good Informational
21 2024-06-04 02:27:13.942776 18.72.229.251 18.72.229.251 IPv4 253 8x9754 (38748) 68 231 Good Fragmented IP protocol (proto=OP 17, off=1488, ID=9754) [Reassembled in #23]
```

```
Message ID: 0x00000000
Length: 1683
Payload: Security Association (1)
  > Payload: Certificate (6)
    Next payload: Certificate (6)
    Reserved: 00
    Payload length: 758
    Certificate Encoding: X.509 Certificate - Signature (4)
  > Certificate Data
    > signedCertificate
      > algorithmIdentifier (iso.2.156.10197.1.501)
        Padding: 0
        encrypted: 384502205166d5d1552f5fecbaabf07ce17e6c9e1ca63f98b72ed61e13884429f4...
  > Payload: Certificate (6)
    Next payload: Vendor ID (13)
    Reserved: 00
    Payload length: 758
    Certificate Encoding: X.509 Certificate - Key Exchange (5)
  > Certificate Data
    > signedCertificate
      > algorithmIdentifier (iso.2.156.10197.1.501)
        Padding: 0
        encrypted: 38462910000b0b79c0b15db017930491...f2a...f6d1...c57b3...6e4051...0712b...31
```

看对端证书信息：



本端证书信息：

```

<Dfyy_IPSecVPN_Test>display pki cer domain ndyb_domain ca
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: sm2sign-with-sm3
    Issuer: CN=宁德市, L=宁德市, C=CN
    Validity
      Not Before: May 29 13:11:28 2024 GMT
      Not After : May 28 13:11:28 2034 GMT
    Subject: CN=宁德市电信机房VPN800手机.C=CN.ST=福建省.L=宁德市.
  
```

发现时间不一致。

字段	值	字段	值
版本	V3	版本	V3
序列号	01	序列号	01
签名算法	1.2.156.10197.1.501	签名算法	1.2.156.10197.1.501
颁发者	81675465@qq.com, 宁德...	颁发者	81675465@qq.com, 宁德...
有效期从	2023年8月22日 9:57:23	有效期从	2024年5月29日 21:11:28
到期	2033年8月20日 9:57:23	到期	2034年5月28日 21:11:28
使用者	81675465@qq.com, 宁德...	使用者	81675465@qq.com, 宁德...
公钥	ECC (0 Bits)	公钥	ECC (0 Bits)
公钥参数	1.2.156.10197.1.301	公钥参数	1.2.156.10197.1.301
使用者密钥标识符	b68da471ccf287ca991ed...	使用者密钥标识符	f680a3216706e00120ad9...
授权密钥标识符	KeyID=b68da471ccf287c...	授权密钥标识符	KeyID=f680a3216706e00...
密钥用法	Certificate Signing, Off-lin...	密钥用法	Certificate Signing, Off-lin...
基本约束	Subject Type=CA, Path Le...	基本约束	Subject Type=CA, Path Le...
指纹	4c0feedcd27f81ae40764d...	指纹	21b1466ba69848043f9b2...

进一步查看发现这些信息都是不一样的，就是说其实是两个不同的证书，也就是当前debug报错证书验证失败的原因。

解决方法

- 1、确定下对端使用的证书是不是“设备证书”里面的
 - 2、明确1之后，把“签发证书”里面对应的CA，换成和“设备证书”里面的一致，然后使用一致的证书再签发一份，然后再导入防火墙确保一致。
- 证书内容不一致导致认证失败，虽然名称一样，但已经不是同一个证书了。