

知 防火墙web界面无法登录典型案例分析

证书 SSL 孔凡安 2022-04-12 发表

组网及说明

不涉及

问题描述

登录防火墙web界面提示“SSL_ERROR_NO_CYPHER_OVERLAP”,更换电脑与浏览器无果。

建立安全连接失败

连接到 11.11.11.11:8443 时发生错误。无法安全地与对等端通信：没有双方共用的加密算法。

错误代码：SSL_ERROR_NO_CYPHER_OVERLAP

- 由于不能验证所收到的数据是否可信，无法显示您想要查看的页面。
- 建议向此网站的管理员反馈这个问题。

[详细了解...](#)

重试

过程分析

查看配置，现场配置了ssl服务器端策略：

关键配置如下：

```
ip https ssl-server-policy fxm
#
ssl server-policy test
pki-domain test
ciphersuite ecdhe_rsa_aes_128_cbc_sha256 ecdhe_ecdsa_aes_128_cbc_sha256 ecdhe_ecdsa_ae
s_256_cbc_sha384 ecdhe_ecdsa_aes_128_gcm_sha256
```

抓包查看，客户端发送“Server Hello”后，服务器侧直接回应握手失败。

Time	Source	Destination	Protocol	Time to Live	Identification	ID	Sequence	Fragment	Offset	Info
332.26.441160	10.10.10.10	10.10.10.10	TCP	64	0x0000 (0)					0 65814 - 8443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 Window=0
333.26.473774	10.10.10.10	10.10.10.10	TCP	245	0x1895 (4184)					0 8443 - 65814 [SYN, ACK] Seq=0 Ack=1 Win=65512 Len=0 MSS=1460 Window=0
334.26.473894	10.10.10.10	10.10.10.10	TCP	64	0x0000 (0)					0 65814 - 8443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=3483324310 T
335.26.478114	10.10.10.10	10.10.10.10	TLSv1.2	64	0x0000 (0)					0 Client Hello
336.26.584263	10.10.10.10	10.10.10.10	TCP	245	0x1895 (4187)					0 8443 - 65814 [ACK] Seq=1 Ack=518 Win=64640 Len=0 TSval=2761783784
337.26.584264	10.10.10.10	10.10.10.10	TLSv1.2	245	0x1895 (4188)					0 Alert (Level: Fatal, Description: Handshake Failure)
338.26.584264	10.10.10.10	10.10.10.10	TCP	244	0x1895 (4189)					0 8443 - 65814 [FIN, ACK] Seq=518 Ack=0 Win=0 Len=0 TSval=2761783784
339.26.584321	10.10.10.10	10.10.10.10	TCP	64	0x0000 (0)					0 65814 - 8443 [ACK] Seq=518 Ack=0 Win=131712 Len=0 TSval=3483324421
340.26.584367	10.10.10.10	10.10.10.10	TCP	64	0x0000 (0)					0 65814 - 8443 [ACK] Seq=518 Ack=0 Win=131712 Len=0 TSval=3483324421
341.26.584551	10.10.10.10	10.10.10.10	TCP	64	0x0000 (0)					0 65814 - 8443 [FIN, ACK] Seq=518 Ack=0 Win=131712 Len=0 TSval=3483324421

Cipher Suites Length: 34

▼ Cipher Suites (17 suites)

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)

Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0ca9)

Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0ca8)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)

Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)

Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)

Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

Compression Methods Length: 1

查看防火墙本地证书的情况，发现为RSA签名证书。

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 0 (0x0)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=HTTPS-Self-Signed-Certificate-893300432ba7ef33

Validity

Not Before: Aug 24 07:07:03 2020 GMT

Not After : Aug 19 07:07:03 2040 GMT

Subject: CN=HTTPS-Self-Signed-Certificate-893300432ba7ef33

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

分析：RSA签名证书无法使用DSA的加密算法，现场的ssl服务器端策略内大部分都是DSA的算法，无法和客户端提供的算法列表匹配，导致协商失败。

解决方法

ssl服务器端策略中添加RSA算法。

