

知 MSR3640 SSL连接建立失败

SSL VPN 张志潮 2019-06-10 发表

组网及说明

不涉及

问题描述

SSLVPN web接入，打开可浏览器后无法弹出ssl登录页面。提示此网站无法提供安全连接



过程分析

1.debugging sslvpn all有如下会话:

```
*May 6 14:19:43:776 2019 ROUTER SSLVPNK/7/SSLVPN_DEBUG_KSSL_HANDSHAKE: Send:TL  
S 1.0 Alert [length 0002], level: fatal, reason: handshake_failure.
```

发现终端与MSR3640建立SSL连接时握手失败

2.设备侧抓包检查ssl报文交互过程:

```
Secure Sockets Layer  
  TLSv1 Record Layer: Handshake Protocol: Client Hello  
    Content Type: Handshake (22)  
    Version: TLS 1.0 (0x0301)  
    Length: 512  
  Handshake Protocol: Client Hello  
    Handshake Type: Client Hello (1)  
    Length: 508  
    Version: TLS 1.2 (0x0303)  
    Random: 381f3ff409b42f4616df3068b249ec560da630b247ff8894...  
    Session ID Length: 32  
    Session ID: fc7fc88352a1a8b1515636e68d7abee017d66fd41d115815...  
    Cipher Suites Length: 34  
    Cipher Suites (17 suites)  
    Compression Methods Length: 1  
    Compression Methods (1 method)  
    Extensions Length: 401  
    Extension: Reserved (GREASE) (len=0)
```

发现只收到了client hello报文，没有响应报文

3.display sslvpn context发现对应的访问实例下引用了ssl server策略,检查配置sslgateway配置:

```
#  
sslvpn gateway gw  
ip address 172.16.100.100 port 2019  
ssl server-policy ssl  
service enable  
#
```

询问现场采用缺省证书方式，怀疑问题和证书相关，让现场删除ssl server策略测试，恢复正常

解决方法

1. 缺省证书方式不要配置ssl server-policy和ssl client-policy，避免影响ssl协商
2. sslvpn gateway下更改配置需要undo service enable再重新service enable后才能生效

