防火墙IPSEC VPN对接后视频业务异常问题处理经验

IPSec VPN　刘嘉炜　2018-12-08 发表

组网及说明

无

问题描述

用户反馈使用F1050与F1020防火墙对接IPSEC VPN，访问对端宝利通MCU视频终端时可以到达登陆界面，但是输入用户名和密码后点击确认跳转空白界面。但是在内网的访问是正常的，而且通过VPN去Ping视频终端也正常。

过程分析

正常时在客户端访问服务器的抓包：

可以看到内网客户端发起访问时报文的长度已经是1514了，此时服务器回应正常。

```
263 14.474567  10.56.250.14     10.56.250.150    TCP        54 16854 > http [ACK] Seq=19028 Ack=98574 Win=64464 Len=0
264 14.796072  10.56.250.14     10.56.250.150    HTTP/XM   499 POST http://10.56.250.150:80 HTTP/1.1
265 14.796429  10.56.250.14     10.56.250.150    HTTP/XM  1514 POST http://10.56.250.150:80 HTTP/1.1 POST http://10.56.250.150:80 HTTP/1.1
266 14.796438  10.56.250.14     10.56.250.150    HTTP/XM   115 POST http://10.56.250.150:80 HTTP/1.1
267 14.797450  10.56.250.150    10.56.250.14     TCP       1514 [TCP segment of a reassembled PDU]
268 14.797546  10.56.250.14     10.56.250.150    HTTP/XM   541 POST http://10.56.250.150:80 HTTP/1.1
269 14.797576  10.56.250.150    10.56.250.14     HTTP/XM   141 HTTP/1.1 200 OK
270 14.797618  10.56.250.14     10.56.250.150    TCP        54 16854 > http [ACK] Seq=21481 Ack=100121 Win=65612 Len=0
271 14.797631  10.56.250.150    10.56.250.14     HTTP/XM   811 HTTP/1.1 200 OK
```

通过VPN访问客户端时：

在客户端发起访问时可以看到大量TCP重传包，长度为1254，随即排查配置发现用户将外网接口的TCP MSS修改为1200了，再加公网和IPSEC封装后报文长度达到1254。

```
248 9.361645   10.56.160.2     10.56.250.150    TCP        54 [TCP Window Update] 14170 > http [ACK] Seq=14123 Ack=83279 Win=66000 Len=0
253 9.661768   10.56.160.2     10.56.250.150    HTTP/XM  1254 [TCP Retransmission] POST http://10.56.250.150:80 HTTP/1.1 POST http://10.56.250.150:80 HTTP/1.1
255 10.261746  10.56.160.2     10.56.250.150    HTTP/XM  1254 [TCP Retransmission] POST http://10.56.250.150:80 HTTP/1.1 POST http://10.56.250.150:80 HTTP/1.1
260 11.461658  10.56.160.2     10.56.250.150    HTTP/XM  1254 [TCP Retransmission] POST http://10.56.250.150:80 HTTP/1.1 POST http://10.56.250.150:80 HTTP/1.1
267 13.862398  10.56.160.2     10.56.250.150    HTTP/XM  1254 [TCP Retransmission] POST http://10.56.250.150:80 HTTP/1.1 POST http://10.56.250.150:80 HTTP/1.1
280 18.655098  10.56.160.2     10.56.250.150    HTTP/XM   590 [TCP Retransmission] POST http://10.56.250.150:80 HTTP/1.1
289 23.454972  10.56.160.2     10.56.250.150    HTTP/XM   590 [TCP Retransmission] POST http://10.56.250.150:80 HTTP/1.1
291 23.985827  10.56.250.150   10.56.160.2      TCP        60 http > 14169 [FIN, ACK] Seq=5670 Ack=412 Win=17920 Len=0
292 23.985969  10.56.160.2     10.56.250.150    TCP        54 14169 > http [ACK] Seq=412 Ack=5671 Win=63944 Len=0
```

#

interface GigabitEthernet1/0/15

port link-mode route

ip address X.X.X.X 255.255.255.240

ip address　X.X.X.X　255.255.255.240 sub

ip address　X.X.X.X　255.255.255.240 sub

tcp mss 1200

nat outbound 3000

此时怀疑此问题与接口MTU值有关，进而排查正常和异常抓包发现，

正常客户端发送的数据是带有DF位的，但是经过防火墙后将数据分片了，所以导致报文异常。

```
Internet Protocol Version 4, Src: 10.56.250.14 (10.56.250.14), Dst: 10.56.250.150 (10.56.250.150)
    Version: 4
    Header length: 20 bytes
  ⊟ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
    Total Length: 1500
    Identification: 0x0e1b (3611)
  ⊟ Flags: 0x02 (Don't Fragment)
      0... .... = Reserved bit: Not set
```

解决方法

至此问题已经排查清楚了，是视频客户端报文DF位原因导致的问题。于是让客户逐渐修改TCP MSS值，当修改至1300时业务正常。

结论：

一般报文经过IPSEC封装数据长度会增加，比如客户端发出的报文长度为1300而且有DF置位，那么外网该接口MTU应该调整1300+54（maxMTU）,在此案例中MTU也不应调整太大，若调整太大极有可能被公网丢弃。