# MSR与第三方设备建立Ipsec隧道业务传输慢问题

IPSec VPN 王科 2022-03-02 发表

## 组网及说明

组网：云端---google---（IPSEC）---MSR56---机房服务器

设备：MSR5620 0605P18

## 问题描述

问题点是与google 建立Ipsec隧道传输业务慢，拓扑如上。从机房两台机器打流到Google云端有问题，大于1184b的IP包有丢包、 从Google打流到机房两台机器没问题。测试结果如下：

1、下行没有问题，上行到 Google 服务器有问题，ping包大小1183字节的IP包没有丢包, 1184字节的IP包开始丢包~5%, 1200字节的IP包丢包率23%, 1300B的IP包丢包50%, 1350字节的IP包丢包70%, 1400字节的IP包完全不通。
2、 不走ipsec vpn，出口默认mtu，Google服务器配置公网地址，走公网没测试问题。
3、 走ipsec vpn，默认mtu，iperf 打流最快是100kbps。
4、 走ipsec vpn，服务器配置mtu=600，iperf 打流最快是400mbps，ping没丢包。

## 过程分析

1. ipsec statistics显示丢包原因是No available SA。同时发现，ipsec MTU check error丢包，怀疑可能是IPSec报文不分片导致的，此类问题建议配置ipsec global-df-bit clear /ipsec fragmentation afer-encryption 尝试。

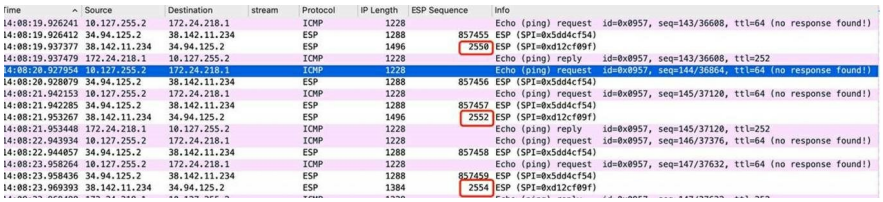
2. 问题复现时，ipsec 隧道上错误信息统计都是0。没业务的时候也是MTU大于1200 就是有丢包，不管业务空不空闲，只要MTU大于1200，上行方向就有丢包。

3. 在云端抓包，云端server的地址是10.127.255.2，本端机房服务器地址172.24.218.1。如下图所示：

1）从上行方向,同样大小的1140字节的ping包，对应的esp封包大小最高可以到1432，最低是1288。而下行方向，发过来的ping包大小是1228字节，对应的esp包大小是稳定的1288字节； 这个esp封包大小上下波动，应该就是造成上行方向丢包的原因了。

2）从上面看推测原因可能是经过vpn设备封装后的ESP报文大小上下波动导致的：mtu=1140的时候，封装后的esp包大小还都能控制在1500字节以内；mtu=1228时，有部分esp包大小超过1500字节了， 从google这边vpn网关的公网抓包看，部分esp包没有到达google。

4. 通过dis ipsec sa 里面看到Traffic Flow Confidentiality enable: Y，而通过dis ipsec policy vpn 7看到的结果是disable。tfc默认情况是关闭的。



| Time | Source | Destination | stream | Protocol | IP Length | ESP Sequence | Info |
|---|---|---|---|---|---|---|---|
| 14:08:19.926241 | 10.127.255.2 | 172.24.218.1 | | ICMP | 1228 | | Echo (ping) request id=0x0957, seq=143/36608, ttl=64 (no response found!) |
| 14:08:19.926412 | 34.94.125.2 | 38.142.11.234 | | ESP | 1288 | 857455 | ESP (SPI=0x5dd4cf54) |
| 14:08:19.937377 | 38.142.11.234 | 34.94.125.2 | | ESP | 1496 | 2550 | ESP (SPI=0xd12cf09f) |
| 14:08:19.937479 | 172.24.218.1 | 10.127.255.2 | | ICMP | 1228 | | Echo (ping) reply id=0x0957, seq=143/36608, ttl=252 |
| 14:08:20.927954 | 10.127.255.2 | 172.24.218.1 | | ICMP | 1228 | | Echo (ping) request id=0x0957, seq=144/36864, ttl=64 (no response found!) |
| 14:08:20.928079 | 34.94.125.2 | 38.142.11.234 | | ESP | 1288 | 857456 | ESP (SPI=0x5dd4cf54) |
| 14:08:21.942153 | 10.127.255.2 | 172.24.218.1 | | ICMP | 1228 | | Echo (ping) request id=0x0957, seq=145/37120, ttl=64 (no response found!) |
| 14:08:21.942285 | 34.94.125.2 | 38.142.11.234 | | ESP | 1288 | 857457 | ESP (SPI=0x5dd4cf54) |
| 14:08:21.953267 | 38.142.11.234 | 34.94.125.2 | | ESP | 1496 | 2552 | ESP (SPI=0xd12cf09f) |
| 14:08:21.953448 | 172.24.218.1 | 10.127.255.2 | | ICMP | 1228 | | Echo (ping) reply id=0x0957, seq=145/37120, ttl=252 |
| 14:08:22.943934 | 10.127.255.2 | 172.24.218.1 | | ICMP | 1228 | | Echo (ping) request id=0x0957, seq=146/37376, ttl=64 (no response found!) |
| 14:08:22.944057 | 34.94.125.2 | 38.142.11.234 | | ESP | 1288 | 857458 | ESP (SPI=0x5dd4cf54) |
| 14:08:23.958264 | 10.127.255.2 | 172.24.218.1 | | ICMP | 1228 | | Echo (ping) request id=0x0957, seq=147/37632, ttl=64 (no response found!) |
| 14:08:23.958436 | 34.94.125.2 | 38.142.11.234 | | ESP | 1288 | 857459 | ESP (SPI=0x5dd4cf54) |
| 14:08:23.969393 | 38.142.11.234 | 34.94.125.2 | | ESP | 1384 | 2554 | ESP (SPI=0xd12cf09f) |

## 解决方法

丢包是因为已知问题导致（ikev2/esp tfc填充加密后超接口mtu丢包问），解决方案如下：

1）需要对端关闭TFC功能（ display ipsec sa看到TFC enable 是因为对方要求我们TFC，我们默认功能是关闭的,所以对方给我们发送报文没有TFC功能)。

2）升级版本解决 ( R07XX以上版本)

如需要tfc相关证明，可使用如下方法：打开ip unreachables enable、并打开debug ip icmp，能够看到自己给自己发送 icmp差错包。

接口mtu1500协商ipsec隧道pmtu为1424。

对端没有携带禁止tfc选项时，我方随机填充0~255填充后加密超接口mtu自己给自己发icmp-df-unreach差错报文。

```
<79-2-CE>ping -c 10 -s 1200 -f 192.168.67.31
Ping 192.168.67.31 (192.168.67.31): 1200 data bytes, press CTRL_C to break
1200 bytes from 192.168.67.31: icmp_seq=0 ttl=254 time=2.765 ms
Request time out
Request time out
Request time out
Request time out
Request time out
1200 bytes from 192.168.67.31: icmp_seq=6 ttl=254 time=2.559 ms
Request time out
Request time out
1200 bytes from 192.168.67.31: icmp_seq=9 ttl=254 time=2.443 ms

--- Ping statistics for 192.168.67.31 ---
10 packet(s) transmitted, 3 packet(s) received, 70.0% packet loss
round-trip min/avg/max/std-dev = 2.443/2.589/2.765/0.133 ms

<MSR3044-PE>*Sep 25 10:40:23:606 2018 MSR3044-PE SOCKET/7/ICMP:
ICMP Output:
 ICMP Packet: src = 172.31.255.253, dst = 193.150.64.8
         type = 3, code = 4 (need fragment-DF set)
 Original IP: src = 193.150.64.8, dst = 178.27.183.27
         proto = 50, first 8 bytes = 12D38C90 0000082C

*Sep 25 10:40:23:606 2018 MSR3044-PE SOCKET/7/ICMP:
ICMP Input:
 ICMP Packet: src = 172.31.255.253, dst = 193.150.64.8
         type = 3, code = 4 (need fragment-DF set)
 Original IP: src = 193.150.64.8, dst = 178.27.183.27
         proto = 50, first 8 bytes = 12D38C90 0000082C
```