某局点MSR G2 IPSEC 有packet too long报错经验案例

吕甲南 2017-05-21 发表

MSR G2设备与友商建立IPSEC，IKE SA和IPSEC SA都正常建立，业务也可以正常使用。debugging ipsec error时有报错，提示：The reason of dropping packet is packet too long, sent icmp error。

1. 在设备上查看IKE SA

```
<H3C>dis ike sa
   Connection-ID   Remote              Flag        DOI
-------------------------------------------------------------------------
   9676            2.2.2.2             RD          IPsec
```

2. 在设备上查看IPSEC SA

```
<H3C>dis ipsec sa
-------------------------------
Interface: GigabitEthernet2/3/1
-------------------------------

  ----------------------------
  IPsec policy: vpn
  Sequence number: 1
  Mode: ISAKMP
  ----------------------------
    Tunnel id: 7
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1444
    Tunnel:
        local  address: 1.1.1.1
        remote address: 2.2.2.2
    Flow:
        sour addr: 10.60.0.0/255.255.255.0  port: 0  protocol: ip
        dest addr: 10.255.0.0/255.255.255.0  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 3515913859 (0xd1909683)
      Connection ID: 27973121998852
      Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1833675/2671
      Max received sequence-number: 152906
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active

    [Outbound ESP SAs]
      SPI: 2396010810 (0x8ed0393a)
      Connection ID: 25026774433793
      Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1833701/2671
      Max sent sequence-number: 150697
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

3. debugging ipsec all 发现有报文超过了MTU大小，MTU 为1444，报文大小为1446。该报文强制不让分片导致报文被丢弃。

```
Outbound IPsec processing: src IP = 10.60.0.64, dst IP = 10.255.0.18, SPI = 256915770.
*Apr 26 19:41:32:852 2017 SZHH-RT IPSEC/7/PACKET: -Slot=2;
```

Packet oversize, mtu=1444, packet len=1446.
*Apr 26 19:41:32:852 2017 SZHH-RT IPSEC/7/PACKET: -Slot=2;
Failed to prepare packet.
*Apr 26 19:41:32:852 2017 SZHH-RT IPSEC/7/ERROR: -Slot=2;
The reason of dropping packet is packet too long, sent icmp error.

4.修改MTU与TCP MSS无效果，怀疑客户环境中有部分UDP大包强制不让分片，超过了PATH MTU 1444。
V7设备解决方法：
ipsec global-df-bit clear
ipsec fragmentation after-encryption

ipsec global-df-bit clear表示清除外层IP头的DF位，IPsec封装后的报文可被分片。
ipsec fragmentation after-encryption 表示开启IPsec封装后分片功能。

V5设备解决方法：
undo ipsec fragmentation before-encryption enable
该命令表示使能加密后分片功能，对待封装报文先进行封装，封装后的报文尺寸如果超过接口MTU值，则再进行分片。
V5设备ipsec fragmentation before-encryption enable命令用来使能加密前分片功能，如果满足分片要求的待封装报文被设置了DF位，则丢弃该报文，并发送ICMP差错控制报文。