某局点 IPSEC OVER GRE 使用中流量异常问题经验案例

IPSec VPN GRE VPN ACL 林宇阳 2021-10-25 发表

组网及说明

说明：客户现场使用ICG3000作为IPSEC总部设备，本案例同时也适用于其他中低端路由器设备。

组网：

ICG3000F（GRE端点）tunnel0——出口设备——公网1——远端GRE端点设备1——外部网络——大量接入分支

tunnel1——出口设备——公网2——远端GRE端点设备2——外部网络——大量接入分支

组网说明：

ICG3000F外网方向线路不同子接口走到不同的公网链路。并使用不同接口地址作为GRE tunnel source地址与不同的远端设备建立GRE隧道。

在GRE隧道口应用IPSEC 策略模板，大量外部接入分支发起IPsec建立请求。

特点在于，本组网中，GRE隧道仅作为IPSEC VPN公网线路的一部分，而不是直接端点设备建立IPsec。因此实际可以等效看做ICG3000F与两台GRE端点设备直连即可。

问题描述

网络已正常使用数年，近期使用中频繁出现问题，故障时现象为：

1． tunnel1接口业务出现问题时，Tunnel0所承载的ipsec业务依旧正常

2． GRE Tunnel1接口30位直连地址ping不通，但Tunnel1的source-destination地址互通一直正常，没有丢包或中断过。

3. Tunnel1上已建立的ipsec隧道流量能继续正常使用，但新建的ipsec sa流量就无法互通。

4． 虽然gre接口地址互联不通，但新的ipsec sa还是能协商建立。

5． 将gre tunnel1删除ipsec policy后直连互通就恢复，重新应用ipsec policy则新建ipsec sa流量也可以正常使用。

过程分析

一、观察故障时收集的诊断文件：

1、设备CPU、内存、快转等占用量均很小，应该不是路由器性能问题

2、现场驻场反馈业务需要ipsec sa总量在1000+左右，诊断中生效的IPSEC SA数量为1072。查看该款型ipsec tunnel规格是4000，不存在ipsec超规格的情况。

==========display ipsec sa count==========

Total IPsec SAs count: 1072

3、故障仅出现在tunnel1，而两个tunnel配置除了地址外都相同，source地址也是同一个物理接口的不同子接口，理论上本端处理不会有差异。故障大概率是外源性因素导致。

二、debug测试观察：

由于tunnel1的GRE封装源目地址互通正常而接口互联地址不通，需要确定设备是否有发出ICMP echo报文。

故障时debug ip icmp ACL XXX显示本端发起的ping报文已经由icmp进程发出，进入转发流程。

但debug ip packet acl XXX（其中ACL匹配tunnel1接口互联地址源目）发现并没有匹配ACL的IP转发流程的打印。

所以怀疑设备处理直连网段地址的报文时走到异常的流程里了。

三、故障时，tunnel1连接的外部接入终端依旧可以新建ipsec sa，说明IKE协商报文依旧可以正常转发，只是IPSEC封装的流量不通。

结合上述情况推测，tunnel1互联地址交互报文和业务报文可能被IPSEC误匹配了。

再次检查设备诊断中记录的ipsec sa信息，发现有一个异常的SA，其感兴趣流为any-any：

```
Tunnel ID: 193
Status: Active
Perfect forward secrecy:
Inside vpn-instance:
SA's SPI:
  outbound:  3528606412  (0xd25242cc)  [ESP]
  inbound:   4241539002  (0xfcd0bfba)  [ESP]
Tunnel:
  local  address: x.x.x.x
  remote address: y.y.y.y
Flow:
    sour addr: 0.0.0.0/0.0.0.0  port: 0  protocol: ip
    dest addr: 0.0.0.0/0.0.0.0  port: 0  protocol: ip
```

当此SA建立后，接口上新建的ipsec SA流量和非ipsec封装的流量都会被此SA误匹配，直接发送到y.y.y.y的接入终端上。

查看流量不通的SA的统计，收发计数都是0，也证实了流量被误匹配这一情况，如：

```
  Flow:
    sour addr: 0.0.0.0/0.0.0.0  port: 0  protocol: ip
    dest addr: z.z.z.z/255.255.255.248  port: 0  protocol: ip
  [Inbound ESP SAs]
    SPI: 4198228552 (0xfa3be248)
    Connection ID: 144985211011531
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843200/3447
    Max received sequence-number: 0
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active
  [Outbound ESP SAs]
    SPI: 1559474999 (0x5cf3b337)
    Connection ID: 161400576017513
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843200/3447
    Max sent sequence-number: 0
    UDP encapsulation used for NAT traversal: N
    Status: Active
```

解决方法

本端为IPSEC模板配置，未设置感兴趣流。正常使用的IPsec SA都是接入终端在IPsec安全ACL配置明细的source地址段，然后总部侧生成反向的感兴趣流。而any-any的感兴趣流产生是由于y.y.y.y这个终端配置了permit ip的ACL，没有指定明细的source地址段，导致协商出现全匹配流量的SA。
在此SA生成后，除了原先已存在SA按照IPSEC匹配顺序还可以正常匹配流量，后续新建的SA匹配顺序靠后就无法匹配流量。GREtunnel互联地址也被匹配中，进行ipsec封装转发。

解决方案：修改y.y.y.y的安全ACL配置，避免全匹配的感兴趣流出现。