SR6604路由器和U200防火墙建立IPSec VPN部分网段不通的问题

IPsec 傅昆 2016-01-26 发表

客户这边有8台U200防火墙，作为分支和中心的SR6604路由器做IPSec VPN。在一次运营商链路中断恢复以后，其中一台U200，出现了部分IPSec保护网段从该U200到SR6604路由器不通的问题。具体表现为：IPSec VPN SA和IKE SA正常，U200下的10.26.108.1PING部分网段，如192.168.0.207/24网段不通。

在U200防火墙上，通过debug IP packet 查看防火墙将数据包已经发出，debug ipsec packet 提示已经进入隧道，但是没有收到SR6604路由器的回应报文。在U200上PING 对端192.168.0.207 测试时发现，出方向统计的ACL3000 命中数增长，入方向统计ACL 3010 的命中数不变，这也说明进入了隧道。
从目前的分析情况看，问题可能出在了中间链路或者SR6604路由器设备上。
由于SR6604路由器上打开debug ipsec packet 后cpu100%，长时间收集信息，担心会影响业务，而且信息量非常大，不便于分析，所以只开了一分钟的debug，但是没有抓到相关有用的信息。
通过下面的信息分析，从U200防火墙上PING -c 10 -a 10.26.108.1 192.168.0.207

```
display ipsec statistics
  the security packet statistics:
    input/output security packets: 25172172445/31796989123
    input/output security bytes: 3997629875568/5772012932920
    input/output dropped security packets: 7519790/655691（PING包期间，数值没有增加）
    dropped security packet detail:
      not enough memory: 228
      can't find SA: 3252553
      queue is full: 0
      authentication has failed: 159064
      wrong length: 0
      replay packet: 483429
      packet too long: 639371
      wrong SA: 0
      decrypt/encrypt failed: 0
      ACL check failure: 3640836

PING -c 10 -a 10.26.108.1 192.168.0.207
  PING 192.168.0.207: 56  data bytes, press CTRL_C to break（全部都丢了）
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
Request time out

*Jan 14 12:24:14:953 2016 SR6604-1 DPIPFWD/7/debug_case: -Slot=3;
Receiving, interface = GigabitEthernet3/1/7, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 41917, offset = 0, ttl = 255, protocol = 1,
checksum = 57432, s = 10.26.108.1, d = 192.168.0.207
prompt: Receiving IP packet

*Jan 14 12:24:14:954 2016 SR6604-1 DPIPFWD/7/debug_case: -Slot=3;
Delivering, interface = GigabitEthernet3/1/7, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 41917, offset = 0, ttl = 255, protocol = 1,
checksum = 57432, s = 10.26.108.1, d = 192.168.0.207
prompt: IP packet is delivering up!

*Jan 14 12:24:14:955 2016 SR6604-1 ADDR/7/debug_case: -Slot=3;
Delivering, interface = GigabitEthernet3/1/7, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 41917, offset = 0, ttl = 255, protocol = 1,
checksum = 57432, s = 10.26.108.1, d = 192.168.0.207
```

prompt: IP packet is delivering up!

*Jan 14 12:24:14:955 2016 SR6604-1 DPIPFWD/7/debug_case: -Slot=3;
Sending, interface = GigabitEthernet3/1/7, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 32330, offset = 0, ttl = 255, protocol = 1,
checksum = 57432, s = 192.168.0.207, d = 10.26.108.1
prompt: Sending the packet from local

*Jan 14 12:24:17:155 2016 SR6604-1 DPIPFWD/7/debug_case: -Slot=3;
Receiving, interface = GigabitEthernet3/1/7, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 41929, offset = 0, ttl = 255, protocol = 1,
checksum = 57420, s = 10.26.108.1, d = 192.168.0.207
prompt: Receiving IP packet

*Jan 14 12:24:17:155 2016 SR6604-1 DPIPFWD/7/debug_case: -Slot=3;
Delivering, interface = GigabitEthernet3/1/7, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 41929, offset = 0, ttl = 255, protocol = 1,
checksum = 57420, s = 10.26.108.1, d = 192.168.0.207
prompt: IP packet is delivering up!

*Jan 14 12:24:17:156 2016 SR6604-1 ADDR/7/debug_case: -Slot=3;
Delivering, interface = GigabitEthernet3/1/7, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 41929, offset = 0, ttl = 255, protocol = 1,
checksum = 57420, s = 10.26.108.1, d = 192.168.0.207
prompt: IP packet is delivering up!

*Jan 14 12:24:17:156 2016 SR6604-1 DPIPFWD/7/debug_case: -Slot=3;
Sending, interface = GigabitEthernet3/1/7, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 32392, offset = 0, ttl = 255, protocol = 1,
checksum = 57420, s = 192.168.0.207, d = 10.26.108.1
prompt: Sending the packet from local

从IP层面看SR6604路由器都回复了，现在重点排查SR6604路由器IPSec模块处理是否正常。
排查过程如下：
为了避免其他报文影响，内部测试使用字节1400报文。
从SR6604路由器 ping -s 1400 -c 100 -t 0 -a 192.168.0.207 10.26.108.1（192.168.0.207为SR6604路由器LOPBACK接口地址， 10.26.108.1为对端U200 防火墙LOOPBACK地址）。
PING 之前：
sa remaining duration (kilobytes/sec): 1837640/2978
PING之后：
sa remaining duration(kilobytes/sec):1837500/2949
1837640-1837500=140*1000=140000 正好对应100个 ----说明IPSEC加密正常

PFS: N, DH group: none
tunnel:
local address: 202.107.222.153
remote address: 122.228.178.206
flow:
sour addr: 192.168.0.0/255.255.0.0 port: 0 protocol: IP
dest addr: 10.26.0.0/255.255.0.0 port: 0 protocol: IP
[outbound ESP SAs]
spi: 0xC7F64900(3354806528)
transform: ESP-ENCRYPT-DES ESP-AUTH-MD5
in use setting: Tunnel
connection id: 6366922
sa duration (kilobytes/sec): 1843200/3600
sa remaining duration (kilobytes/sec): 1837640/2978
anti-replay detection: Enabled
anti-replay window size(counter based): 32
udp encapsulation used for nat traversal: N

原始IP报--------原始ICMP报文发送正常
*Jan 15 17:50:36:208 2016 SR6604-1 DPIPFWD/7/debug_case: -Slot=3;
Sending, interface = GigabitEthernet3/1/7, version = 4, headlen = 20, tos

pktlen = 1428, pktid = 5524, offset = 0, ttl = 255, protocol = 1,
checksum = 0, s = 192.168.0.207, d = 10.26.108.1
prompt: Sending the packet from local

IPSec加密后报文----------加密后封装隧道头ICMP发送正常

*Jan 15 17:50:36:208 2016 SR6604-1 DPIPFWD/7/debug_case: -Slot=3;
Sending, interface = GigabitEthernet3/1/7, version = 4, headlen = 20, tos
pktlen = 1480, pktid = 30552, offset = 0, ttl = 255, protocol = 50,
checksum = 0, s = 202.107.222.153, d = 122.228.178.206
prompt: Sending the packet from local

驱动----------驱动正确发送

*Jan 15 17:50:42:444 2016 SR6604-1 DRVDBG/7/debugging: -Slot=3;
(GigabitEthernet3/1/7)PHY/PKT:
Packet Output, Packet Len =1494,Partial data as follows:

----------加上12字节以太头以及2字节前导码

00 E0 FC A4 B0 CD 70 F9 6D 1A 6B 4F 08 00 45 00
05 C8 92 64 00 00 FF 32 4C E7 CA 6B DE 99 7A E4
B2 CE CB 7C B6 3F 00 00 1B AD 86 BA 48 42 90 C5
72 85 9C FB D0 90 68 67 24 6C 8A 01 CD 32 07 D3
DIP： CA 6B DE 99 SIP：7A E4 B2 CE

从SR6604路由器上查看，加密数据的sa的remote address 是122.228.178.206，并非是U200上的任何接口地址。也就是说，从U200PING -c 10 -a 10.26.108.1 192.168.0.207 的回报文是转发给了122.228.178.206这个设备，经过确认，为Juniper路由器。

display ipsec tunnel | begin 10.26.
Dest addr :10.26.0.0/255.255.0.0 port:0 protocol: IP
Current Encrypt-card:
Connection id :139432
Perfect forward secrecy:
SA's SPI:
inbound: 187199087 (0xb286e6f) [ESP]
outbound: 3562274487 (0xd453feb7) [ESP]
tunnel:
local address: 202.107.222.153
remote address : 122.228.178.206
flow:
sour addr : 192.168.0.0/255.255.0.0 port: 0 protocol : IP
dest addr : 10.26.0.0/255.255.0.0 port: 0 protocol : IP
current Encrypt-card:

至此问题似乎已经比较明确了，但是，为什么到U200的流量，转发到了122.228.178.206 这台设备呢？再次确认后发现：

sour addr : 192.168.0.0/255.255.0.0 port: 0 protocol : IP
dest addr : 10.26.0.0/255.255.0.0 port: 0 protocol : IP------16位掩码，应该是32位才对。SR6604路由器IPSec采用的是模板方式，掩码信息是由IKE PEER协商出来的，也就是说，应该是Juniper发送的掩码信息是错误的。
最终确认是客户更改了Juniper设备的IPSec 安全ACL的网段掩码导致这次故障。

修改Juniper设备的IPSec安全ACL的网段掩码配置。