某局点SR6608和分支MSR路由器建立IPSec后业务不通问题处理经验案例

ACL IP PoS IPsec 张玺 2015-10-22 发表

某局点使用SR6608路由器作为总部路由器，使用MSR路由器作为分支路由器，总部和分支之间的数据通过IPSec进行封装，使用IKE主模式建立IPSec隧道。
该局点共有三个分支，设备开局时，前两个分支已经调通，业务正常。但配置第三个分支时，IKE SA和PSec SA均能正常建立，公、私网路由也配置正确，但业务不通。
总部和第三个分支大致拓扑如下：
L0：192.168.15.254/32------总部SR66-------公网-------分支MSR----L0：172.16.10.254/32
其中，使用Loopback0接口模拟两端的私网地址。两端Loopback0地址互ping不通。

故障现象比较奇怪，此时，我们分以下几个步骤来排查问题原因：
1、从MSR侧带Loopback0 ping 总部SR66的L0，以下结果可见SR66收到了该IPSec报文，但没有回复IPSec报文。

```
dis ipsec statistics tunnel-id 17
 -----------------------------------------------
  Connection ID : 17
 -----------------------------------------------
  the security packet statistics:
    input/output security packets: 7/0       //开始只收到了7个IPSec报文
    input/output security bytes: 616/0
    input/output dropped security packets: 0/0
    dropped security packet detail:
      not enough memory: 0
      queue is full: 0
      authentication has failed: 0
      wrong length: 0
      replay packet: 0
      packet too long: 0
      wrong SA: 0
```

从MSR上ping -a 172.16.10.254 192.168.15.254，5个包：

```
dis ipsec statistics tunnel-id 17
 -----------------------------------------------
  Connection ID : 17
 -----------------------------------------------
  the security packet statistics:
    input/output security packets: 12/0   /输入增加了5个，输出仍为0个
    input/output security bytes: 1056/0
    input/output dropped security packets: 0/0
    dropped security packet detail:
      not enough memory: 0
      queue is full: 0
      authentication has failed: 0
      wrong length: 0
      replay packet: 0
      packet too long: 0
      wrong SA: 0
```

2、在SR66的公网口出方向做Firewall：

```
#
acl number 3999
 rule 0 permit ip source 172.16.10.0 0.0.0.255 destination 192.168.15.0 0.0.0.255
 rule 5 permit ip source 192.168.15.0 0.0.0.255 destination 172.16.10.0 0.0.0.255
#
dis firewall-statistics interface g3/2/6
  Interface: GigabitEthernet3/2/6
  Out-bound Policy: acl 3999
  From 2013-04-11 16:46:58 to 2013-04-11 17:50:58
     27 packets, 2268 bytes, 0% permitted,   //开始统计到27个包
     0 packets, 0 bytes, 0% denied,
     140902 packets, 89998909 bytes, 100% permitted default,
```

```
    0 packets, 0 bytes, 0% denied default,
  Totally 140929 packets, 90001177 bytes, 100% permitted,
  Totally 0 packets, 0 bytes, 0% denied.
```

SR66 ping MSR 端私网地址：

```
ping -a 192.168.15.254 172.16.10.254
  PING 172.16.10.254: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 172.16.10.254 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

从下面的防火墙统计信息可见SR66确实回包了，但从g3/2/6发出去的包没有被IPSec加密：

```
dis firewall-statistics interface g3/2/6
  Interface: GigabitEthernet3/2/6
  Out-bound Policy: acl 3999
  From 2013-04-11 16:46:58 to 2013-04-11 17:51:38
     32 packets, 2688 bytes, 0% permitted, //匹配ACL 3999的包增长了5个
     0 packets, 0 bytes, 0% denied,
     141111 packets, 90051714 bytes, 100% permitted default,
     0 packets, 0 bytes, 0% denied default,
  Totally 141143 packets, 90054402 bytes, 100% permitted,
  Totally 0 packets, 0 bytes, 0% denied.
```

3、为何业务报文匹配了感兴趣流，但没有被SR66的IPSec隧道加密呢？我们继续来看一下设备IPSec相关配置：

```
#
        ipsec policy loncin 1 isakmp
         security acl 3000
         ike-peer gz
         proposal cp1
    #
        ipsec policy loncin 2 isakmp
         security acl 3001
         ike-peer hn
         proposal hn
    #
        ipsec policy loncin 3 isakmp          //第三个分支配置
         security acl 3004
         ike-peer hnlx
         proposal def
    #
acl number 3004
     rule 0 permit ip source 192.168.15.0 0.0.0.255 destination 172.16.10.0 0.0.0.255
     rule 5 permit ip source 192.168.15.0 0.0.0.255 destination 172.16.11.0 0.0.0.255
```

到此，配置都没有问题，但此时，我们发现了acl 3001中有一条奇怪的配置：rule 40

```
acl number 3001
     rule 0 permit ip source 192.168.130.0 0.0.0.255 destination 192.168.17.0 0.0.0.255
     rule 5 permit ip source 192.168.15.0 0.0.0.255 destination 192.168.17.0 0.0.0.255
     rule 15 permit ip source 192.168.192.0 0.0.0.255 destination 192.168.17.0 0.0.0.255
     rule 20 permit ip source 192.168.15.0 0.0.0.255 destination 172.16.2.0 0.0.0.255
     rule 25 permit ip source 192.168.130.0 0.0.0.255 destination 172.16.2.0 0.0.0.255
     rule 30 permit ip source 192.168.192.0 0.0.0.255 destination 172.16.2.0 0.0.0.255
     rule 35 permit ip source 192.168.15.254 0 destination 172.16.2.0 0.0.0.255
     rule 40 deny ip
```

明明是第二个分支引用的ACL，会对第三个分支造成影响么？

答案是肯定的。事实上，H3C Comware V5平台的设备，配置IPSec ACL的时候，通常要保护什么流量，就配置相应的permit；不保护的流量不用配置deny，否则，deny的ACL会影响后面的节点，导致后面节点业务流量无法被IPSec封装。

到此，问题的原因被我们找到了，删除该ACL后，业务恢复正常通信，问题解决 。

H3C Comware V5平台的设备，配置IPSec ACL的时候，通常要保护什么流量，就配置相应的permit；不保护的流量不用配置deny，否则，deny的ACL会影响后面的节点，导致后面节点业务流量无法被IPSec封装。