某局点IPsec中心模板方式运行中故障典型分析

IKE IPSec VPN 孔凡安 2022-11-30 发表

组网及说明

为方便理解组网简化如下：

(a.a.a.a)分支（A.A.A.A）---------(B.B.B.B)总部(b.b.b.b)

故障现象为分支侧感兴趣流a.a.a.a 无法ping通总部b.b.b.b

告警信息

不涉及

问题描述

总部采用IPsec安全策略模板方式与分支建立IPsec隧道，运行过程中有一个分支出现无法访问总部网站的情况，其他分支访问正常。

过程分析

分析历程如下：

1. 首先查看分支到总部的IPsec隧道是否建立成功，IKE SA和IPsec SA是否存在。所幸现场隧道没有问题，于是排查防火墙是否进行IPsec封装并发出报文。

2. 首先在分支侧查看报文是否封装后发出，先看内层报文会话，即a.a.a.a--->b.b.b.b。查看防火墙会话显示未收到回包。此时可以通过抓包或者debug的方式查看防火墙是否有丢包。抓包判断的说明如下：
acl写4条rule，对应a.a.a.a--->b.b.b.b（来回），A.A.A.A--->B.B.B.B（来回）
防火墙web界面全局抓包，只选acl，不选接口。查看封装后的报文是否发出。可以在测试的时候ping固定大小、固定数量的报文，经过IPsec封装后的报文大小是固定的，通过比较数据包长度判断防火墙是否发出报文。

3. 经过第三步的抓包可以判断，分支侧发出报文，但是未收到回程报文，即没有收到B.B.B.B--->A.A.A.A。于是在总部的防火墙上进行排查，首先还是查看会话，发现内层会话（a.a.a.a--->b.b.b.b）有来有回。似乎已经把报文经过IPsec隧道封装后发出了。同样的，在总部的防火墙上web抓包确认，数据包是否封装后发出，参考步骤2描述的方法。

4. 经过总部侧抓包排查，很遗憾，没有抓到IPsec封装后的报文发出。内层会话显示收发正常，但是IPsec封装后没有发出。问题还是出在总部的防火墙上。此时可以通过debug查看防火墙是否在流程处理上有丢包。acl写法如下：
两条rule，对应a.a.a.a--->b.b.b.b（来回）
debug内容如下：

```
<FW>debugging ip packet acl 3XXX      # 查看报文具体从哪个接口，哪个slot上来和发出的情况
<FW>debugging ip info acl 3XXX        # 如果有丢包则会打印信息丢包的具体模块，如果没有丢包则不打印
<FW>debugging aspf packet acl 3XXX    # 如果报文状态不合法，则会显示被aspf丢弃，需检查流量来回是否一致
<FW>debugging security-policy packet ip acl 3XXX      # 如果是对象策略则用object-policy，如果是包过滤则用packet-filter
```

查看debug ip info的打印，发现回包（b.b.b.b--->a.a.a.a）被IPsec模块丢弃,如图所示，return 1（drop）代表丢包。如果返回其他值可不用关注。

5. 排查到这个地步，需要思考IPsec模块为啥会丢包。一般情况下都是走错隧道出口导致的，可能是某些隧道有重复的感兴趣流。于是把所有的IPsec SA打印出来，查看是否有感兴趣流冲突的情况，结果并没有。。。

6. 所谓事出反常必有妖！IPsec模块不会无缘无故丢包。检查总部的IPsec配置，发现IPsec policy下有调用感兴趣流acl，那么很大的概率就是这些acl有重叠的情况。果不其然，其中一条acl最后一条rule是permit ip的配置。而这条acl的调用顺序正好优于出问题的分支。

解决方法

取消acl下rule里面permit ip的配置。