某局点IPsec隧道正常建立，但是感兴趣流不通问题分析

IPSec VPN　孔凡安　2022-06-25 发表

组网及说明

内网----FW1----公网----FW2----内网

问题描述

客户反馈之前隧道一切正常，FW2更换专线后，新隧道可以正常建立，但是业务不通。

过程分析

在FW1上debug显示感兴趣流被IPsec模块丢弃，如下：

<H3C-F1000-A-G2>*Jun 21 15:34:34:557 2022 H3C-F1000-A-G2 IPFW/7/IPFW_INFO: -COntext=1-Slot=2; MBUF was intercepted! Phase Num is 8(post routing beforefrag), Service ID is 22(ipsec), Bit map is 20000000000, return 1(0:continue, 1:dropped, 2:consumed, 3:enqueued, 4:relay)! Interface is Route-Aggregation2, s= 10.26.66.21, d= 10.26.210.188, protocol= 1, pktid = 23140.

web抓包显示FW1没有发往FW2的ESP报文，说明FW1并没有把封装后的报文发出去。

查看隧道的统计，确实如此：

<H3C-F1000-A-G2>disp ipsec statistics tunnel-id 28

IPsec packet statistics:

Received/sent packets: 21/0

Received/sent bytes: 1200/0

Dropped packets (received/sent): 0/0

Dropped packets statistics

No available SA: 0

Wrong SA: 0

Invalid length: 0

Authentication failure: 0

Encapsulation failure: 0

Decapsulation failure: 0

Replayed packets: 0

ACL check failure: 0

MTU check failure: 0

Loopback limit exceeded: 0

Crypto speed limit exceeded: 0

通过隧道统计看该隧道并没有丢包，怀疑是感兴趣流重叠导致走了其他的隧道出去了。

但是查看IPsec SA的情况，没有发现其他的隧道和该隧道感兴趣流重叠。

进一步查看IPsec策略，发现在该策略前面还有一条策略，引用了同样的感兴趣流：

Sequence number: 7

Mode: ISAKMP

Description: ycgs

Traffic Flow Confidentiality: Disabled

Security data flow: 3010

Selector mode: standard

Local address: 61.183.195.237

Remote address: 58.51.41.30

Transform set: GE1/0/2_IPv4_7

IKE profile: GE1/0/2_IPv4_7

IKEv2 profile:

SA duration(time based): 3600 seconds

SA duration(traffic based): 1843200 kilobytes

SA idle time:

解决方法

现场存在相同的策略名不同的序号，引用了相同的ACL，导致出现匹配错误，把前面的策略引用的感兴趣流配置删除，业务正常。