IPsec隧道丢包问题非典型案例

ASPF IKE 会话 IPSec VPN 孔凡安 2024-02-24 发表

组网及说明

组网简化为如下，如下两台防火墙作为IPsec网关

H3C防火墙----公网----Huawei防火墙

告警信息

*Jan 23 11:48:26:771 2024 QZAX-EIS-E18C22-PODM-S-CK-F5000-1 IPFW/7/IPFW_INFO: -COntext=1-Chassis=1-Slot=2;

MBUF was intercepted! Phase Num is 9(post routing beforefrag), Service ID is 28(ipsec), Bitmap is 800000000, **return 1(0:continue, 1:dropped, 2:consumed, 3:enqueued, 4:relay)!**Interface is Route-Aggregation2.10,

s= 10.49.233.161, d= 10.244.31.250, protocol= 1, pktid = 52298

问题描述

H3C防火墙带感兴趣流ping对端私网地址无法ping通，查看对应会话显示有发无收。

```
Slot 0 in chassis 1:
Initiator:
  Source      IP/port: 10.49.233.161/23248
  Destination IP/port: 10.244.31.250/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: MGMT/-/-
  Protocol: ICMP(1)
  Inbound interface: InLoopBack0
  Source security zone: Local
Responder:
  Source      IP/port: 10.244.31.250/23248
  Destination IP/port: 10.49.233.161/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: MGMT/-/-
  Protocol: ICMP(1)
  Inbound interface: M-GigabitEthernet1/0/0/0
  Source security zone: Management
State: ICMP_REQUEST
Application: ICMP
Rule ID: -/-/-
Rule name:
Start time: 2024-01-23 14:26:50  TTL: 56s
Initiator->Responder:            1 packets         84 bytes
Responder->Initiator:            0 packets          0 bytes
```

debug显示被IPsec模块丢包：

*Jan 23 11:48:26:771 2024 QZAX-EIS-E18C22-PODM-S-CK-F5000-1 IPFW/7/IPFW_INFO: -COntext=1-Chassis=1-Slot=2;

MBUF was intercepted! Phase Num is 9(post routing beforefrag), Service ID is 28(ipsec), Bitmap is 800000000, **return 1(0:continue, 1:dropped, 2:consumed, 3:enqueued, 4:relay)!**Interface is Route-Aggregation2.10,

s= 10.49.233.161, d= 10.244.31.250, protocol= 1, pktid = 52298

过程分析

感兴趣流配置如下：

```
#
acl advanced 3000
description FOR-quanzhouanxi-EIS-IPSecVPN
rule 5 permit ip source 10.49.233.128 0.0.0.127 destination 10.174.0.0 0.0.255.255
rule 10 permit ip source 10.49.233.128 0.0.0.127 destination 10.234.0.0 0.0.255.255
rule 15 permit ip source 10.49.233.128 0.0.0.127 destination 10.213.0.0 0.0.255.255
rule 20 permit ip source 10.49.233.128 0.0.0.127 destination 10.244.31.250 0
rule 25 permit ip source 10.49.233.128 0.0.0.127 destination 10.246.40.240 0
```

```
rule 30 permit ip source 10.49.233.128 0.0.0.127 destination 10.194.0.0 0.0.255.255
#
```

IPsec策略调用的感兴趣流是包括我们如上测试的IP信息，但是实际测试无法ping到对端。
此类问题排查思路一般就是先查看有无对应的IPsec SA和IKE SA，如果有的话那就需要查看设备是否封装后发出，排查案例可以参考：中低端防火墙点到多点GRE over IPsec模式下Tunnel口无法ping通对端问题
如果没有对应的IPsec SA，那就需要查看是否有对应的IKE SA，隧道是否协商成功。隧道建立失败排查可以参考：IPsec建立失败排查SOP

经过查看，现场的情况属于IKEv2 SA存在，但是对应如上标红的感兴趣流没有建立IPsec SA。这就有点儿奇怪了。
一般来说，标准方式下一条IPsec隧道保护一条数据流。ACL中的每一个规则对应的数据流分别由一条单独创建的IPsec隧道来保护。缺省采用该方式。
那么需要排查为何没有对应的IPsec SA建立，首先值得怀疑的就是两边保护的数据流不匹配，但是核对之后发现是OK的。

对感兴趣流的流量进行debug分析，打印显示IPsec模块丢包：

```
*Jan 23 11:48:26:771 2024 QZAX-EIS-E18C22-PODM-S-CK-F5000-1 IPFW/7/IPFW
_INFO: -COntext=1-Chassis=1-Slot=2;
MBUF was intercepted! Phase Num is 9(post routing beforefrag), Service ID is 28(ips
ec), Bitmap is 800000000, return 1(0:continue, 1:dropped, 2:consumed, 3:enque
ued, 4:relay)! Interface is Route-Aggregation2.10,
s= 10.49.233.161, d= 10.244.31.250, protocol= 1, pktid = 52298
```

想起以往处理过的经典案例，存在感兴趣流冲突的情况。例如：某局点IPsec中心模板方式运行中故障典型分析
检查过后发现没有类似情况。

解决方法

debug ike all remote xxx发现没有触发ike协商，检查设备配置发现IPsec策略下没有调用ikev2 profile。
其他隧道可以正常协商是因为是对端发起协商，本端正常响应建立IPsec SA。本端主动发起的话就歇菜了。
总结：简单配置问题，业务正常的前提是要保证配置正确。