# 某局点NAT配置取消后业务还能通问题处理分享

会话 孔凡安 2023-09-04 发表

## 组网及说明

设备型号：F5030

组网：下行Reth口，上行双出口（Route-Aggregation32和Route-Aggregation42），RAGG32和 RAGG42为单框聚合，路由主备。

关键配置如下，两个接口下其他的NAT配置省略，只列出关键配置如下：

```
#
interface Route-Aggregation32
 description to-liantong-zhu
 ip address 172.26.1.5 255.255.255.252
 ip last-hop hold
。。。。
#
interface Route-Aggregation42
 description to-liantong-bei
 ip address 172.26.1.29 255.255.255.252
 ip last-hop hold
 nat server protocol tcp global 119.X.X.X 9998 inside 10.1.229.140 9999 rule Server Rule_3045
```

## 告警信息

不涉及

## 问题描述

Ro32和Ro42作为设备出口，接口下NAT配置相同。某天接口RAGG32下 NAT Server配置取消后，发现业务依然正常。

## 过程分析

据现场人员反馈，设备出口采取主备路由的方式，接口Ro32下的配置取消后，理论上业务应该直接不通才对。
查看路由，确实如此：

```
#
 ip route-static 0.0.0.0 0 172.26.1.26 preference 100 description
zwdxliantongserver1      ---备用路由，RAGG42接口下一跳
 ip route-static 0.0.0.0 0 172.26.1.2         ---RAGG32下一跳地址
#
```

首先查看设备上会话，发现设备上确实做了NAT转换：

```
<INTERNET-F03-YUNBIANJIE-F5030>display session table ipv4 destination-ip 119.
X.X.X destination-port 9998 interface ro32 v
Slot 1:
Initiator:
  Source      IP/port: 119.4.189.69/21207
  Destination IP/port: 119. X.X.X /9998
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Route-Aggregation32
  Source security zone: Internet
Responder:
  Source      IP/port: 10.1.229.140/9999
  Destination IP/port: 119.4.189.69/21207
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Reth20
  Source security zone: Trust
State: TCP_ESTABLISHED
Application: GENERAL_TCP
Rule ID: 50
Rule name: dsjb_internet
Start time: 2023-08-23 14:26:02  TTL: 2500s
Initiator->Responder:            3 packets        120 bytes
Responder->Initiator:            4 packets        172 bytes

Total sessions found: 1

Slot 2:
Initiator:
  Source      IP/port: 119.4.189.69/21207
  Destination IP/port: 119.X.X.X /9998
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Route-Aggregation32
  Source security zone: Internet
Responder:
  Source      IP/port: 10.1.229.140/9999
  Destination IP/port: 119.4.189.69/21207
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Reth20
  Source security zone: Trust
```

```
State: INACTIVE
Application: GENERAL_TCP
Rule ID: 50
Rule name: dsjb_internet
Start time: 2023-08-23 14:26:02  TTL: 90s
  Initiator->Responder:            2 packets         92 bytes
  Responder->Initiator:            0 packets         0 bytes
```

## 解决方法

调整对端流量走向，保持只走单框即可。

我司设备NAT机制：对于已有NAT会话，只要接口下打开了NAT业务点，就会做NAT。所以后续报文在Ro32接口下也能正常NAT。

小Tips：会话刷新的机制为入方向接口和安全域都会刷，出方向只刷新安全域。

这个现象确实比较诡异，我们都知道防火墙对于首包的处理流程就是首包建立会话。如果设备接口下没有对应的NAT配置，理论上不会做NAT转换。

那么根据经验，要么是软件问题（NAT配置有残留），要么就是流量入接口发生了变化。按照这个思路，先查看写NAT下发内核的情况，对应命令：

```
[H3C-probe]disp system internal nat slot 1
```

发现 RAGG32接口下的NAT配置已经无了，接口 RAGG42下的配置没做删除还是有的。那么此时剩下了第二种可能，那就是流量的入接口变了，开始流量的入接口为 RAGG42，后续的流量入接口变为了RAGG32，接口和安全域被刷新。

那么可以通过debug等信息来查看，常见的debug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
<FW>debugging nat packet acl 3XXX          #查看nat会话情况
如果没有会话，但是debug有报文上来，还需要收集：
<FW>debugging session session-table event acl 3XXX      # 可以查看会话被删除的具体情况
```

现场的打印信息如下，从debug可以看出，首包确实从RAGG42接口上来，并创建了会话。后续报文从 RAGG32上来，刷新了会话的入接口。

```
*Sep  1 17:21:32:697 2023 INTERNET-F03-YUNBIANJIE-F5030 IPFW/7/IPFW_PACKET: -COntext=1-Slot=2;
Receiving, interface = Route-Aggregation42
version = 4, headlen = 20, tos = 0
pktlen = 52, pktid = 54326, offset = 0, ttl = 121, protocol = 6
checksum = 50698, s = 119.4.189.73, d = 119.X.X.X
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
VsysID = 1
prompt: Receiving IP packet from interface Route-Aggregation42.
Payload: TCP
  source port = 30332, destination port = 9998
  sequence num = 0x825fd4cf, acknowledgement num = 0x00000000, flags = 0x2 ---syn置位，TCP首包
  window size = 64240, checksum = 0x17e3, header length = 32.


*Sep  1 17:21:31:800 2023 INTERNET-F03-YUNBIANJIE-F5030 SESSION/7/TABLE: -COntext=1;
 Tuple5(EVENT): 119.4.189.73/30332-->119.X.X.X/9998(TCP(6))
 Session entry was restored.
*Sep  1 17:21:32:697 2023 INTERNET-F03-YUNBIANJIE-F5030 SESSION/7/TABLE: -COntext=1-Slot=2;
 Tuple5(EVENT): 119.4.189.73/30332-->119.X.X.X/9998(TCP(6))
 Session entry was created.
*Sep  1 17:21:32:697 2023 INTERNET-F03-YUNBIANJIE-F5030 NAT/7/COMMON: -COntext=1-Slot=2;
```

PACKET: (Route-Aggregation42-in-config) Protocol: TCP ----匹配接口Ro42下配置进行NAT转换
119.4.189.73:30332 - 119.X.X.X: 9998(VPN: 0)(vsys: 1) ------>
119.4.189.73:30332 - 10.1.229.140: 9999(VPN: 0)(vsys: 1)
*Sep 1 17:21:32:697 2023 INTERNET-F03-YUNBIANJIE-F5030 IPFW/7/IPFW_PACKET: -COntext=1-Slot=2;