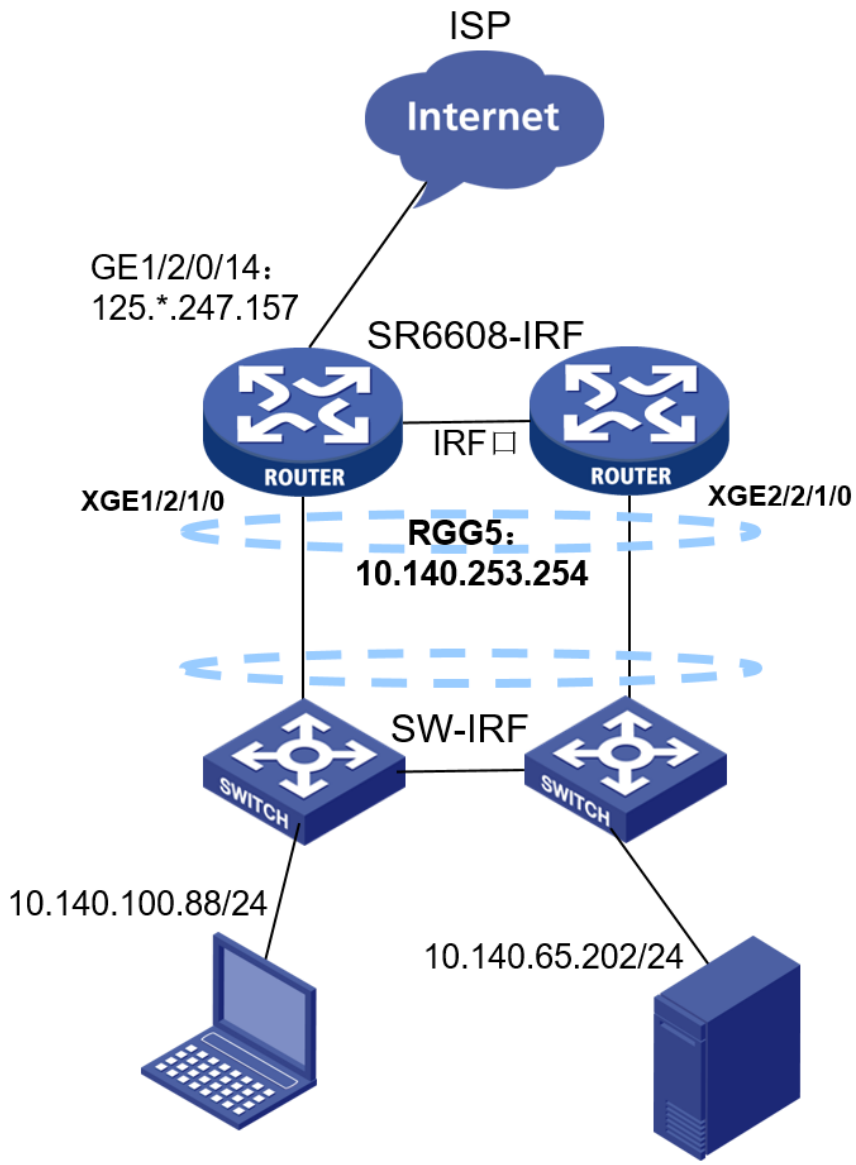
某局点SR6608设备通过nat hairpin实现内网终端通过公网地址访问私网服务器功能异常排查经验案例

NAT 徐猛 2021-11-12 发表

组网及说明

组网拓扑如下：

现场出口为两台SR6608设备做堆叠，且现场只有一根外网出口GE1/2/0/14，该出口地址为：125.*.247.157。现场设备对内使用RGG5三层聚合口对接内网核心交换机，该三层聚合口地址为：10.140.253.254。（为保护隐私，本案例对部分公网地址做了隐藏处理）



问题描述

现场客户在内网有一台服务器，地址为10.140.65.202，需要对外提供服务，同时内网终端有上网需求。现场在设备外网口GE1/2/0/14上配置了nat server和nat outbound后，内网的终端上网正常，外网通过global地址访问内网服务器的业务也正常。外网口配置如下:

```
interface GigabitEthernet1/2/0/14
port link-mode route
ip address 125.*.247.157 255.255.255.0
nat outbound
nat server protocol tcp global 125.64.247.157 18073 inside 10.140.65.202 18073
```

现客户新增业务需求，要求内网的终端能够通过公网地址访问内网服务器，对于该需求，在设备内网口上配置nat hairpin enable后，发现终端无法通过公网地址访问内网服务器。内网口配置如下:

```
interface Route-Aggregation5
service standby chassis 2 slot 2        //分布式设备上逻辑口上需要指定处理流量的板卡槽位。
 ip address 10.140.253.254 255.255.255.252
nat hairpin enable            //使能nat hairpin功能。
```

测试说明:

内网终端地址为：10.140.100.88/24

访问的global地址为：125.*.247.157/24

内网目的地地址为：10.140.65.202/24

过程分析

（1）针对现场配置检查发现，内网三层聚合口上未指定逻辑口上主用的流量处理板卡，建议客户进行了完善。

interface Route-Aggregation5
service chassis 1 slot 1　　//增加该命令指定分布式设备上逻辑口上处理流量的主用板卡槽位。
service standby chassis 2 slot 2　　//分布式设备上逻辑口上指定处理流量的备用板卡槽位。
 ip address 10.140.253.254 255.255.255.252
nat hairpin enable　　//使能nat hairpin功能。

（2）发现完善上述配置后，依旧需求无法实现，通过display nat session查看是否有该业务流量的会话记录。发现并没有源地址为10.140.100.88, 目的地址为125.64.247.157的会话记录。

（3）遂采集了debug ip packet和debug nat packet的记录来查看，发现设备的RGG5口下有收到该流量，但是并未进行nat处理，没有nat的debug记录，设备直接异常处理了。

*Nov 11 17:07:22:190 2021 HLW-R1 IPFW/7/IPFW_PACKET: -MDC=1-Chassis=2-Slot=2;
Receiving, interface = Route-Aggregation5
version = 4, headlen = 20, tos = 0
pktlen = 60, pktid = 16873, offset = 0, ttl = 127, protocol = 6
checksum = 54800, s = 10.140.100.88, d = 125.64.247.157
channelID = 0, vpn-instanceIn = 0, vpn-instanceOut = 0.
prompt: Receiving IP packet from interface Route-Aggregation5.
Payload: TCP
  source port = 52532, destination port = 18073
  sequence num = 0xfcce7629, acknowledgement num = 0x00000000, flags = 0x2
  window size = 8192, checksum = 0xde2a, header length = 40.

*Nov 11 17:07:22:190 2021 HLW-R1 IPFW/7/IPFW_PACKET: -MDC=1-Chassis=2-Slot=2;
Delivering, interface = Route-Aggregation5
version = 4, headlen = 20, tos = 0
pktlen = 60, pktid = 16873, offset = 0, ttl = 127, protocol = 6
checksum = 54800, s = 10.140.100.88, d = 125.64.247.157
channelID = 0, vpn-instanceIn = 0, vpn-instanceOut = 0.
prompt: Forwarding IP packet to upper layer.
Payload: TCP
  source port = 52532, destination port = 18073
  sequence num = 0xfcce7629, acknowledgement num = 0x00000000, flags = 0x2
  window size = 8192, checksum = 0xde2a, header length = 40.

（4）怀疑是触发了设备的某个限制导致的，遂查看了官网关于nat hairpin功能的限制。发现如下说明：

2.8 配置NAT hairpin功能

1. 功能简介

NAT hairpin功能用于满足位于内网侧的用户之间或用户与服务器之间通过NAT地址进行访问的需求。开启NAT hairpin的内网侧接口上会对报文同时进行源地址和目的地址的转换。

2. 配置限制和指导

NAT hairpin功能需要与内部服务器（nat server）、出方向动态地址转换（nat outbound）或出方向静态地址转换（nat static outbound）配合工作，且这些配置所在的接口必须在同一个接口板，否则NAT hairpin功能无法正常工作。

（5）对设备当前业务涉及端口进行分析：

聚合口5的主用端口为1框2槽位1号子卡上的端口。

Aggregate Interface: Route-Aggregation5
Aggregation Mode: Static
Loadsharing Type: Shar
  Port　　Status Priority Oper-Key

XGE1/2/1/0　　S　　32768　　1
XGE2/2/1/0　　S　　32768　　1

外网口为1框2槽位面板上的端口。

interface GigabitEthernet1/2/0/14

port link-mode route

结合设备当前device所插板卡的情况来分析：

解决方法

==========display device verbose==========

由于设备上对于nat hairpin的使用存在如下限制：

NAT hairpin功能需要与内部服务器（nat server）、出方向动态地址转换（nat outbound）或出方向静态地址转换（nat static outbound）配合工作，且这些配置所在的接口必须在同一个接口板，否则NAT hairpin功能无法正常工作。

Slot Board Type Status Primary SubSlots

1/0 RT-FIP-380 Normal N/A 2

1/1 RT-MIC-X-XP4 Normal N/A 0

1/2 RT-FIP-380 Normal N/A 2

2/0 RT-FIP-E-X5 Normal Standby 0

2/1 RT-FIP-E-X5 Normal Standby 0

2/2 RT-FIP-380 Normal N/A 2

2/3 N/A Absent N/A N/A

2/4 N/A Absent N/A N/A

2/5 N/A Absent N/A N/A

Slot 1/2 : RT-FIP-380(2 Subslots)

Subslot 1 : RT-MIC-X-XP4

Slot 2/2 : RT-FIP-380(2 Subslots)

Subslot 1 : RT-MIC-X-XP4

设备1框2槽位的板卡外观情况如下，设备存在两个子卡槽位，以及面板上还有14个固定端口。

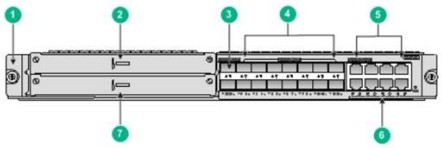
而三层聚合口5的主用端口来自于1框2槽位的1号子卡，而外网口来自于1框2槽上的面板口，不满足官网对于nat hairpin的使用限制。

A.8.9 FIP-380规格

FIP-380（Flexible Interface Platform Module FIP-380，灵活接口平台模块FIP-380）能够提供高速的业务处理能力，提供2个10GBASE-R SFP+接口、14个1000BASE-X SFP接口和8个100/1000BASE-T电口，支持MIC-X接口模块。

1. FIP-380正视图

图A-36 FIP-380正视图



1: 松不脱螺钉	2: slot 2
3: 10GBASE-R以太网光口SFP+22、SFP+23	4: 1000BASE-X以太网光口SFP0～SFP13
5: 100/1000 BASE-T以太网电口GE14～GE21	6: 拉手
7: slot 1	

由于设备上对于nat hairpin的使用存在如下限制：

NAT hairpin功能需要与内部服务器（nat server）、出方向动态地址转换（nat outbound）或出方向静态地址转换（nat static outbound）配合工作，且这些配置所在的接口必须在同一个接口板，否则NAT hairpin功能无法正常工作。

这需要将三层聚合口5指定主用板卡。另外将nat hairpin删除掉，修改为nat outbound + nat server使用即可

#

interface Route-Aggregation5

service chassis 1 slot 1 //指定下主用板卡

service standby chassis 2 slot 2

ip address 10.140.253.254 255.255.255.252

nat hairpin enable //删除

nat outbound //内网口上直接添加nat outbound以及需要的nat server条目。

nat server protocol tcp global 125.64.247.157 18073 inside 10.140.65.202 18073