某局点静态NAT一对一不通

outbound链路负载均衡 NAT **陈阳** 2021-09-29 发表

组网及说明

不涉及

问题描述

一台LB作为出口设备，配置了静态NAT将内网一台服务器映射到公网上，映射后发现在公网无法访问该服务器。

过程分析

首先检查LB设备的NAT配置，没有发现问题：

```
nat static outbound 192.168.18.165 115.238.159.27 counting
interface GigabitEthernet1/0/2
 port link-mode route
 description dianxin
 ip address 115.238.159.27 255.255.255.248 sub
 nat static enable
```

不配置NAT时，在公网访问LB设备公网接口sub地址能通

```
ping 115.238.159.27

正在 Ping 115.238.159.27 具有 32 字节的数据:
来自 115.238.159.27 的回复: 字节=32 时间=7ms TTL=249
来自 115.238.159.27 的回复: 字节=32 时间=7ms TTL=249
来自 115.238.159.27 的回复: 字节=32 时间=7ms TTL=249
来自 115.238.159.27 的回复: 字节=32 时间=6ms TTL=249

115.238.159.27 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
最短 = 6ms，最长 = 7ms，平均 = 6ms
```

在LB上带公网口sub地址ping内网服务器能通

```
ping -a 115.238.159.27 192.168.18.165

Ping 192.168.18.165 (192.168.18.165) from 115.238.159.27: 56 data bytes, press CTRL_C to break
56 bytes from 192.168.18.165: icmp_seq=0 ttl=127 time=1.737 ms
56 bytes from 192.168.18.165: icmp_seq=1 ttl=127 time=0.649 ms
56 bytes from 192.168.18.165: icmp_seq=2 ttl=127 time=0.594 ms
56 bytes from 192.168.18.165: icmp_seq=3 ttl=127 time=0.614 ms
56 bytes from 192.168.18.165: icmp_seq=4 ttl=127 time=0.589 ms

--- Ping statistics for 192.168.18.165 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.589/0.837/1.737/0.451 ms
```

在设备上收集debug nat packet、debug ip packet，看到如下输出

```
*Sep 26 14:46:43:979 2021 LB_H3C_AK310 IPFW/7/IPFW_PACKET: -COntext=1;
Receiving, interface = GigabitEthernet1/0/2
version = 4, headlen = 20, tos = 0
pktlen = 52, pktid = 30404, offset = 0, ttl = 58, protocol = 6
checksum = 47093, s = 115.238.139.18, d = 115.238.159.27
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: Receiving IP packet from interface GigabitEthernet1/0/2.
Payload: TCP
  source port = 57326, destination port = 443
  sequence num = 0xd785d4ae, acknowledgement num = 0x00000000, flags = 0x2
  window size = 64240, checksum = 0xd436, header length = 32.

*Sep 26 14:46:43:979 2021 LB_H3C_AK310 NAT/7/COMMON: -COntext=1;
 PACKET: (GigabitEthernet1/0/2-in-config) Protocol: TCP
  115.238.139.18:57326 -  115.238.159.27:  443(VPN:    0) ------>
  115.238.139.18:57326 -  192.168.18.165:  443(VPN:    0)
*Sep 26 14:46:43:980 2021 LB_H3C_AK310 NAT/7/COMMON: -COntext=1;
 PACKET: (GigabitEthernet1/0/2-out-config) Protocol: TCP
  115.238.139.18:57326 -  192.168.18.165:  443(VPN:    0) ------>
   61.130.98.122:23135 -  192.168.18.165:  443(VPN:    0)
```

从上面的debug输出可以看到，设备收到了访问sub地址的报文，然后做了入方向的nat转换，但是紧接着又做了出方向的地址转换。

检查配置发现有做出方向的链路负载均衡，所以怀疑流量进入设备后匹配了负载均衡服务被转发到公网上，导致访问不了服务器。

针对NAT的流量单独配置负载均衡动作为forward all进行测试，发现可以正常访问，说明和负载均衡配置有关。

解决方法

创建负载均衡类匹配NAT的流量，配置动作为forward all。