SR66路由器做NAT出口来回路径不一致导致丢包

NAT 罗梦恺 2023-02-20 发表

组网及说明

内网设备 -----SR66-1（SR66-2）---双链路负载--外网设备

问题描述

两台SR66 做并行的出口nat，两台设备上配置完全一致，外网访问内网做nat static inbound/nat static outbound的源目转换。目前外访内流量两个链路负载，随机到两台SR66上做源目转换，内网回包单链路到我们SR66-1上。测试发现部分流量不通，排查发现不通的流量来回路径为：

外网---》-SR66-2 ---》---内网

内网---》-SR66-1 ---》---外网

流量在从内网回到SR66-1上时在SR66-1上丢弃，来回路径一致的流量测试都正常（外--SR66-1---内，回程：内--SR66-1---外）。

过程分析

SR66 V7版本NAT因为防攻击的考虑，存在首包校验的功能。首次收到icmp replay报文，tcp ack等报文时会检测是否存在已有的首包会话（icmp request，tcp syn等），如果未找到首包会话默认不进行nat转化会导致报文丢弃。

解决方法

升级至8218p22以及之后版本，配置静态NAT转化时配置nat static xxx packet-type-ignore 忽略首包检测