某局点F10X0 NAT server无法拉流视频流故障案例

NAT 单畅 2022-01-29 发表

组网及说明

现场防火墙作为出口，做了nat server和nat outbound。

问题描述

现场的故障情况是，外网用户经过防火墙拉取内网摄像头的数据流量无法拉取，但是ping内网摄像头能通；内网用户访问外网没有问题。

海康视频流取流失败，协议使用的是SIP协议，故障截图如下：

过程分析

分析现场的抓包及配置

接口下的NAT映射：

interface GigabitEthernet1/0/3

port link-mode route

flow-control

ip address 113.x.x.x 255.255.255.192

nat outbound 3000

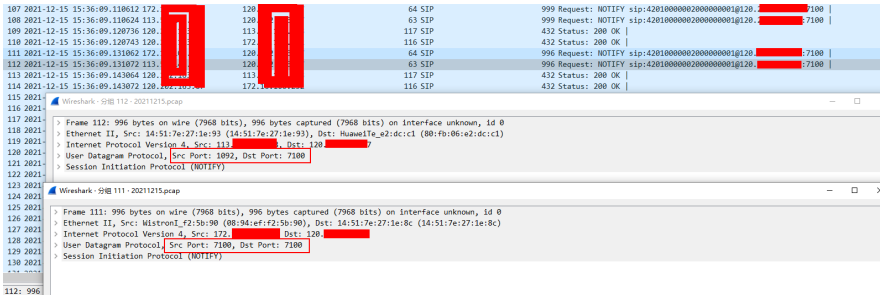
nat server protocol tcp global 113.x.x.x 7100 inside 172.x.x.x 7100

nat server protocol udp global 113.x.x.x 7100 inside 172.x.x.x 7100 rule xx

#

从配置来看，该局点的从外访问内做了7100端口的映射，内到外走的是nat outbound的映射。现场公网通过以上映射访问内部服务器，但是同时内部服务器会向公网的服务器发送心跳报文，源目端口均为7100。

在设备上开启报文捕获抓包后可以看到报文交互如下：



此时，从公网服务器通过公网映射访问的时候，nat转换关系如下，转换之后的源为120.x.x.x:7100，目的为113.x.x.x:7100，协议为udp，这条流与上面内网发起的心跳报文一样，导致会话冲突创建失败。

进一步分析，抓取设备debug：

Tuple5(EVENT): 172.x.x.x/33472-->120.x.x.x/7100(TCP(6))

Session entry was deleted.

*Dec 16 14:42:21:906 2021 J&T-湖北省监控防火墙 SESSION/7/TABLE:

Tuple5(EVENT): 172.x.x.x/7100-->120.x.x.x/7100(UDP(17))

Session entry was deleted.

所以，产生此故障的根本原因是：nat outbound形成的会话和nat server形成的会话出现了冲突。

解决办法是：在nat server 加了reversible 参数之后，这样心跳报文就不会命中出接口的nat outbound转换源端口，从而公网访问内网的会话直接命令该心跳报文转出去了，就不会出现上述问题。

nat server protocol tcp global 113.x.x.x 7100 inside 172.x.x.x 7100 reversible

nat server protocol udp global 113.x.x.x 7100 inside 172.x.x.x 7100 reversible

解决方法

在nat server 加了reversible 参数，这样心跳报文就不会命中出接口的nat outbound转换源端口，从而公网访问内网的会话直接命令该心跳报文转出去了，就不会出现上述问题。配置如下：

nat server protocol tcp global 113.x.x.x 7100 inside 172.x.x.x 7100 reversible

nat server protocol udp global 113.x.x.x 7100 inside 172.x.x.x 7100 reversible

最终优化建议：

1) 取流失败问题优化建议

现场有7100端口作为SIP业务映射的情况下，且现场的视频业务有双向访问的需求（内访问外的心跳业务，外访问内的取流业务），建议现场配置NAT server的反向映射。并且配置port-mapping，因为7100端口不是SIP协议的知名端口，通过port-mapping将7100端口映射成SIP协议，配置如下：

nat server protocol tcp global x.x.x.x 7100 inside y.y.y.y 7100 reversible （接口视图下配置）

nat server protocol udp global x.x.x.x 7100 inside y.y.y.y 7100 reversible （接口视图下配置）

port-mapping application sip port 7100 （系统视图下配置）

2) 内部访问异常问题（根据现场实际情况处理，如果未出现则无须考虑）

与现场了解，内部访问的视频流业务不过防火墙，但是有一个信令业务会通过防火墙的公网映射进行转发，如下：

nat server protocol tcp global 113.x.x.x 7660 inside 172.x.x.x 7660

nat server protocol udp global 113.x.x.x 7660 inside 172.x.x.x 7660

过防火墙的信令业务转发异常，被防火墙的ALG转换成了其他地址和端口，视频流业务比较特殊，需要开启如下两条命令进行测试，看业务是否正常。

[H3C] undo nat alg sip (先开这一条，如果还是不行，就开启下一条)

[H3C]inspect bypass