过防火墙话机语音丢失问题排查案例_SIP协议在防火墙上的实现V1.0

域间策略/安全域 NAT 孔凡安 2024-05-07 发表

组网及说明

不涉及，组网简化为如下：

内网语音服务器172.16.159.10-----防火墙218.X.X.218----外网语音服务器47.X.X.30

告警信息

不涉及

问题描述

故障不定时复现，现象为内网听不到外网的声音。
这个案例比较简单，现场的配置不用提供，单凭报文也能看出问题所在。

过程分析

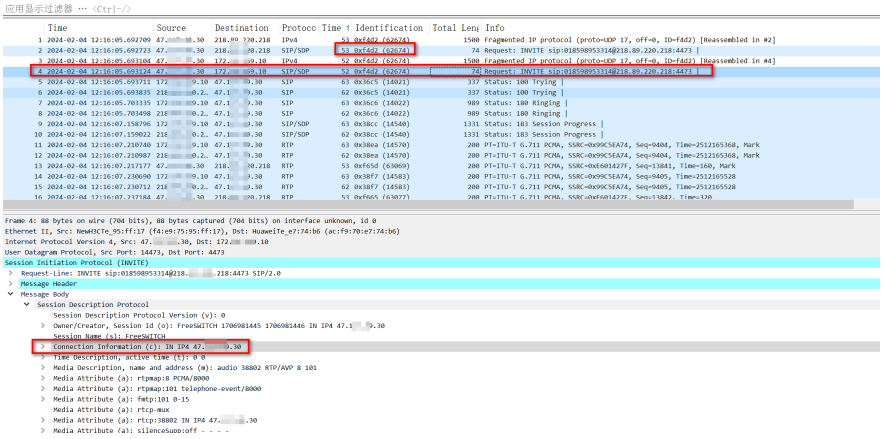
针对涉及SIP协议，防火墙上又做了NAT的场景。抓到故障时候的报文尤为关键，即NAT前后的报文。
抓包可以参考：
H3C防火墙Web界面抓包以及debug总结

以该局点为例，抓包对应的acl如下：

```
acl advanced 3999
rule 0 permit ip source 47.X.X.30 0 destination 218.X.X.218 0
rule 5 permit ip source 218.X.X.218 0 destination 47.X.X.30 0
rule 10 permit ip source 47..X.X.30 0 destination 172..X.X.10 0
rule 15 permit ip source 172..X.X.10 0 destination 47.X.X.30 0
rule 20 permit ip source 218.X.X.218 0 destination 172.X.X.10 0
rule 25 permit ip source 172.X.X.10 0 destination 218..X.X.218 0
```

抓包的原则就是在明细化的前提下多多益善。针对过防火墙前后的报文一定要抓全。方便定位问题。

拿到现场的报文后，先对SIP报文分析。发现设备SDP消息体中携带的连接地址还是公网地址。可以看出不需要设备做ALG转换。
关注如下No.4报文，它是No.2报文经过防火墙DNAT转换后的报文（判断依据ttl-1，以及ip.id一致），报文载荷连接地址还是对应的公网地址47.X.X.30。



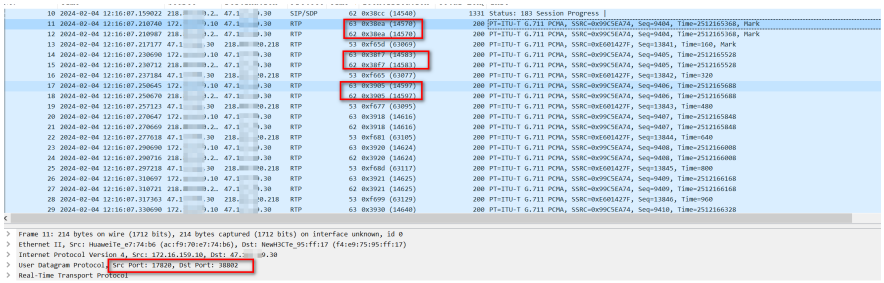
根据以上分析说明设备不需要针对SIP报文进行ALG转换，即针对载荷地址进行NAT转换。对应的不需要设备做ALG的场景可以看一下如下案例：
NGFW防火墙映射视频流业务（SIP协议）异常过程分析

ALG是什么呢，简单解释一下：

> ALG（Application Level Gateway，应用层网关）主要完成对应用层报文的处理。 通常情况下，NAT只对报文头中的IP地址和端口信息进行转换，数据载荷中的IP地址和端口信息不能被NAT进行有效转换，就可能导致问题。ALG主要用来解决在NAT环境中只转换IP地址和端口信息无法有效处理数据载荷的问题。 ALG是解决NAT对应用层

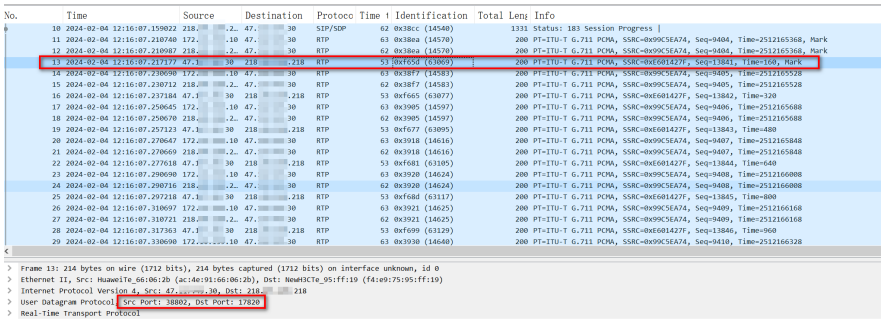
> 协议无感知的一个最常用方法，已经被NAT设备厂商广泛采用，成为NAT设备的一个必需功能。因为NAT不感知应用协议，所以有必要额外为每个应用协议定制协议分析功能，这样NAT网关就能理解并支持特定的协议。

当然以上的分析与故障无关，我们重点关注SIP协议报文协商后的RTP码流。可以看到内网先向外发起呼叫，且报文经过NAT转换后发出。



从No.11报文开始，即是RTP码流的传输阶段，对应客户所谓的呼叫听不到声音的故障过程。故障就出现在外网码流传递到内网期间（例如No.13，No.16以及后续的外到内的单个报文），可以看出没有NAT后的报文，即没有47.X.X.30----172.16.159.10的报文，判断这就是内网听不到声音的原因。

那么为什么防火墙没有转发这个报文呢?
我们进一步对报文分析可以发现，外网主动访问内网的码流端口是38802--17820。结合上面的内网到外网的RTP码流对应的端口可以看出是发生了端口冲突。



分析如下：
内网发起的码流：172.X.X.10：17820---47.X.X.30：38802
经过防火墙NAT转换之后：218.X.X.218：16780----47.X.X.30：38802
内网发起的RTP码流到达设备之后，会建立如上的会话。后续外网发起的RTP码流到达设备之后，根据源目地址+端口是匹配不到会话的。因此会走新建会话流程
外网主动发起的码流：47.X.X.30：38802----218.X.X.218：17820
命中防火墙NAT配置会变为：47.X.X.30：38802----172.X.X.10：17820
事实上，这条会话会因为会话冲突导致会话建立失败，因为和开始建立的会话五元组冲突了。可以对比一下标红部分。所以外网发起的RTP码流无法转发到内网。自然也就听不到声音了。

解决方法

基于以上分析可以判断问题原因为内网发起的RTP码流先到设备，命中snat全局策略转换了端口转发出去。外网侧的码流到达设备后因端口冲突导致dnat转换失败，对应流量没有转发到内网侧。

解决方案就是针对语音流业务配置一对一的静态NAT，避免端口冲突问题。
如果是接口NAT，可以使用nat static配置：

> **nat static outbound**命令用来配置出方向一对一静态地址转换映射。
> **undo nat static outbound**命令用来删除出方向一对一静态地址转换映射。
> 【命令】
> **nat static outbound** *local-ip* [**vpn-instance** *local-vpn-instance-name*] *global-ip* [**vpn-instance** *global-vpn-instance-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**vrrp** *virtual-router-id*] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**] [**packet-type-ignore**] [**description** *text*]
> **undo nat static outbound** *local-ip* [**vpn-instance** *local-vpn-instance-name*] *global-ip* [**vpn-instance** *global-vpn-instance-name*]

如果是全局NAT，需要配置两条配置：

> 静态地址转换方式：
> **action snat static** { **ip-address** *global-address* | **object-group** *object-group-name* | **subnet** *subnet-ip-address mask-length* } [**vrrp** *virtual-router-id*] [**vrf** *vrf-name*]
> 服务器映射方式：
> **action dnat** { **ip-address** *local-address* | **object-group** *ipv4-object-group-name* } [**local-port** { *local-port1* [**to** *local-port2*] }&<1-32>] [**vrrp** *virtual-router-id*] [**vrf** *vrf-name*]