

组网及说明

组网描述: 终端 22.223.x.219 —— 防火墙 —— 服务器 10.255.y.7

问题描述

现场22.223.x.219/24网段的SIP流量经过防火墙策略NAT同时转换了源目地址后SIP通信异常

过程分析

1、检查配置: 配置无误

```
#
nat global-policy
rule name P1
source-zone Trust
source-ip host 22.223.x.219
destination-ip host 14.b.4.1
action snat static ip-address 10.a.41.176
action dnat ip-address 10.255.y.7
counting enable
#
nat alg sip
```

2、检查会话: SIP报文收发正常

```
[F1000]dis nat session verbose
Slot 1:
Initiator:
Source IP/port: 22.223.x.219/5060
Destination IP/port: 14.b.4.1/5060
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/
Protocol: UDP(17)
Inbound interface: Ten-GigabitEthernetx/x/x
Source security zone: Trust
Responder:
Source IP/port: 10.255.y.7/5060
Destination IP/port: 10.a.41.176/5060
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/
Protocol: UDP(17)
Inbound interface: Ten-GigabitEthernetx/x/x
Source security zone: Untrust
State: UDP_READY
Application: SIP
Rule ID: -/-/
Rule name:
Start time: 2023-11-16 00:11:54 TTL: 177s
Initiator->Responder: 6 packets 4174 bytes
Responder->Initiator: 12 packets 8322 bytes
```

3、查看抓包: 正常SIP协议交互完成后业务报文应该是RTP报文, 此时发现服务器回应的SIP报文源地址是10.255.y.7但是RTP报文源地址变成了10.255.y.10.

Time	Source	Destination	Protocol	Info
17 7.283514	10.255.7	10.41.176	SIP/SDP	Status: 183 Session Progress, with session description
18 7.543856	10.255.10	10.41.176	RTP	PT=ITU-T G.711 PCMA, SSRC=0xEEEE, Seq=12, Time=1600, Mark
19 7.563967	10.255.10	10.41.176	RTP	PT=ITU-T G.711 PCMA, SSRC=0xEEEE, Seq=13, Time=1760
20 7.583845	10.255.10	10.41.176	RTP	PT=ITU-T G.711 PCMA, SSRC=0xEEEE, Seq=14, Time=1920
21 7.603882	10.255.10	10.41.176	RTP	PT=ITU-T G.711 PCMA, SSRC=0xEEEE, Seq=15, Time=2080
22 7.624317	10.255.7	10.41.176	SIP/SDP	Status: 180 Ringing, with session description
23 7.624480	10.255.10	10.41.176	RTP	PT=ITU-T G.711 PCMA, SSRC=0xEEEE, Seq=16, Time=2240
24 7.643962	10.255.10	10.41.176	RTP	PT=ITU-T G.711 PCMA, SSRC=0xEEEE, Seq=17, Time=2400
25 7.663888	10.255.10	10.41.176	RTP	PT=ITU-T G.711 PCMA, SSRC=0xEEEE, Seq=18, Time=2560
26 7.682931	10.255.10	10.41.176	RTP	PT=ITU-T G.711 PCMA, SSRC=0xEEEE, Seq=19, Time=2720

那么为什么业务报文的源地址会变化呢? 将SIP报文展开可以看到从服务器回包的时候报文携带的Connection Information的IP地址和真实服务器地址不一致:

Filter: sip Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
17	7.283514	10.255.10.7	10.41.176	SIP/SDP	Status: 183 Session Progress, with session description

```

Frame 17: 829 bytes on wire (6632 bits), 829 bytes captured (6632 bits)
Ethernet II, Src: 10:82:3d:95:3c:98 (10:82:3d:95:3c:98), Dst: f4:e9:75:94:da:e6 (f4:e9:75:94:da:e6)
Internet Protocol, Src: 10.255.10.7 (10.255.254.7), Dst: 10.41.176 (10.41.176)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol
  Status-Line: SIP/2.0 183 Session Progress
  Message Header
  Message Body
    Session Description Protocol
      Session Description Protocol Version (v): 0
      Owner/Creator, Session Id (o): - 33312 33312 IN IP4 10.255.254.10
      Session Name (s): VOSS000
      Connection Information (c): IN IP4 10.255.10.10
      Time Description, active time (t): 0 0
      Media Description, name and address (m): audio 44860 RTP/AVP 8 101
      Media Attribute (a): rtpmap:8 PCMA/8000
      Media Attribute (a): rtpmap:101 telephone-event/8000
      Media Attribute (a): fmtp:101 0-15
      Media Attribute (a): sendrecv
  
```

Connection Information的IP地址是后续报文需要交互业务报文的地址，正常情况下Connection Information携带的IP地址在配置NAT ALG后也是需要地址转换的，但是因为现场该参数地址与真实服务器地址不一致，匹配不上NAT转换策略，因此从防火墙回给终端的抓包中Connection Information的地址并不会转换，因此后续业务会出现异常：

Filter: sip Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
13	6.044151	14.4.1	22.223.219	SIP/SDP	Status: 183 Session Progress, with session description

```

Frame 13: 829 bytes on wire (6632 bits), 829 bytes captured (6632 bits)
Ethernet II, Src: f4:e9:75:94:da:e6 (f4:e9:75:94:da:e6), Dst: 10:82:3d:95:3d:d9 (10:82:3d:95:3d:d9)
Internet Protocol, Src: 14.4.1 (14.4.1), Dst: 22.223.219 (22.223.219)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol
  Status-Line: SIP/2.0 183 Session Progress
  Message Header
  Message Body
    Session Description Protocol
      Session Description Protocol Version (v): 0
      Owner/Creator, Session Id (o): - 33246 33246 IN IP4 10.255.10.10
      Session Name (s): VOSS000
      Connection Information (c): IN IP4 10.255.10.10
      Time Description, active time (t): 0 0
      Media Description, name and address (m): audio 15702 RTP/AVP 8 101
      Media Attribute (a): rtpmap:8 PCMA/8000
      Media Attribute (a): rtpmap:101 telephone-event/8000
      Media Attribute (a): fmtp:101 0-15
      Media Attribute (a): sendrecv
  
```

## 解决方法

配置防火墙NAT ALG时，SIP协议请求报文中的request主机部分、to头域会进行NAT转换，应答报文sdp里的Connection Information连接地址和端口、contact头域会进行NAT转换。上述问题有以下两种解决方法：

方法一：因现场问题为服务器回包中Connection Information携带的服务器IP地址有误导致的该问题，因此最根本的解决方法是服务器那边修改Connection Information参数为服务器真实IP地址进行解决；  
方法二：防火墙开启NAT ALG后可以直接对内层的Connection Information地址进行报文匹配和转换，现场可以增加NAT策略，让内层地址转换成公网地址，注意不能是14.b.4.1了：

```

#
source-ip host 10.255.y.10
action snat static ip-address x.x.x.x
#
destination-ip host x.x.x.x
action snat static ip-address xxxxxx %看现场是否需要转源
action dnat ip-address 10.255.y.7
#
参考案例: https://zhiliao.h3c.com/theme/details/222369
  
```