NGFW防火墙映射视频流业务（SIP协议）异常过程分析

ALG NAT 孔凡安 2022-11-30 发表

组网及说明

内网服务器（10.55.0.17）---防火墙（192.100.63.43）---监控台（192.100.161.3）

防火墙上global地址192.100.63.43映射内网服务器inside地址10.55.0.17。对应会话如下：

```
Initiator:
  Source      IP/port: 192.100.161.3/7100
  Destination IP/port: 192.100.63.43/7100
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
  Inbound interface: GigabitEthernet1/0/10
  Source security zone: GA
Responder:
  Source      IP/port: 10.55.0.17/7100
  Destination IP/port: 192.100.161.3/7100
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: UDP(17)
  Inbound interface: Route-Aggregation1
  Source security zone: Trust
State: UDP_READY
Application: SIP
Rule ID: 0
Rule name: 1
Start time: 2022-11-29 23:07:03  TTL: 285s
Initiator->Responder:          15 packets      11970 bytes
Responder->Initiator:          22 packets      12161 bytes
```

告警信息

不涉及

问题描述

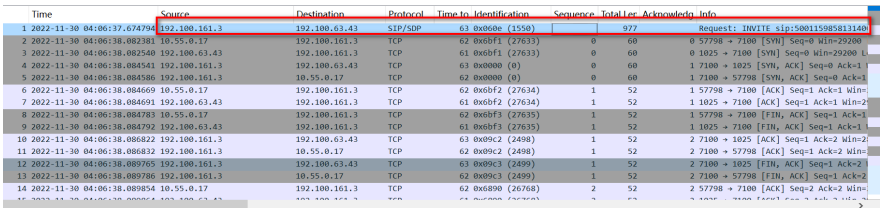
故障现象：监控中心无法获取视频画面，内网服务器的资源无法传递。

关键配置如下：

```
#
port-mapping application sip port 7100
#
 nat alg sip
 nat static inbound 192.100.63.43 10.55.0.17
#
interface GigabitEthernet1/0/10
 port link-mode route
 ip address 192.100.63.43 255.255.255.128
 ip last-hop hold
 nat outbound 2000
 nat static enable
 manage ping inbound
 manage ping outbound
#
acl basic 2000
 rule 0 permit
#
```

过程分析

根据现场反馈访问监控中心侧发起的INVITE报文没有进行NAT转换，No.1报文（192.100.161.3/7100--->192.100.63.43/7100），没有抓到NAT转换后的报文（192.100.161.3/7100--->10.55.0.17/7100）：



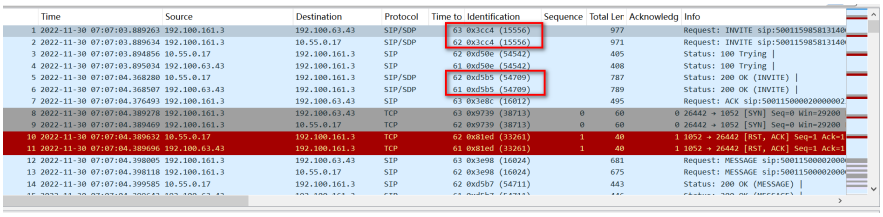
	Time	Source	Destination	Protocol	Time to	Identification	Sequence	Total Ler	Acknowledg	Info
1	2022-11-30 04:06:37.674794	192.100.161.3	192.100.63.43	SIP/SDP	63	0x060e (1550)		977		Request: INVITE sip:500115985813140
2	2022-11-30 04:06:38.082381	10.55.0.17	192.100.161.3	TCP	62	0x6bf1 (27633)	0	60		0 57798 → 7100 [SYN] Seq=0 Win=29200
3	2022-11-30 04:06:38.082540	192.100.63.43	192.100.161.3	TCP	61	0x6bf1 (27633)	0	60		0 1025 → 7100 [SYN] Seq=0 Win=29200 L
4	2022-11-30 04:06:38.084541	192.100.161.3	192.100.63.43	TCP	63	0x0000 (0)	0	60		1 7100 → 1025 [SYN, ACK] Seq=0 Ack=1
5	2022-11-30 04:06:38.084586	192.100.161.3	10.55.0.17	TCP	62	0x0000 (0)	0	60		1 7100 → 57798 [SYN, ACK] Seq=0 Ack=1
6	2022-11-30 04:06:38.084669	10.55.0.17	192.100.161.3	TCP	62	0x6bf2 (27634)	1	52		1 57798 → 7100 [ACK] Seq=1 Ack=1 Win=
7	2022-11-30 04:06:38.084691	192.100.63.43	192.100.161.3	TCP	61	0x6bf2 (27634)	1	52		1 1025 → 7100 [ACK] Seq=1 Ack=1 Win=2
8	2022-11-30 04:06:38.084783	10.55.0.17	192.100.161.3	TCP	62	0x6bf3 (27635)	1	52		1 57798 → 7100 [FIN, ACK] Seq=1 Ack=1
9	2022-11-30 04:06:38.084792	192.100.63.43	192.100.161.3	TCP	61	0x6bf3 (27635)	1	52		1 1025 → 7100 [FIN, ACK] Seq=1 Ack=1
10	2022-11-30 04:06:38.086822	192.100.161.3	192.100.63.43	TCP	63	0x09c2 (2498)	1	52		2 7100 → 1025 [ACK] Seq=1 Ack=2 Win=2
11	2022-11-30 04:06:38.086832	192.100.161.3	10.55.0.17	TCP	62	0x09c2 (2498)	1	52		2 7100 → 57798 [ACK] Seq=1 Ack=2 Win=
12	2022-11-30 04:06:38.089765	192.100.63.43	192.100.161.3	TCP	63	0x09c3 (2499)	1	52		2 7100 → 1025 [FIN, ACK] Seq=1 Ack=2
13	2022-11-30 04:06:38.089786	192.100.161.3	10.55.0.17	TCP	62	0x09c3 (2499)	1	52		2 7100 → 57798 [FIN, ACK] Seq=1 Ack=2
14	2022-11-30 04:06:38.089854	10.55.0.17	192.100.161.3	TCP	62	0x6890 (26768)	2	52		2 57798 → 7100 [ACK] Seq=2 Ack=2 Win=

查看192.100.161.3/7100--->192.100.63.43/7100的会话，发现没有检索到。怀疑是会话冲突导致NAT转换失败，创建的会话被删除掉了。

优化配置如下：

```
#
nat staticoutbound 10.55.0.17 192.100.63.43  //实现双向互转，原来的配置只能外访内实现NAT转换，因为没加reversible参数
#
interface GigabitEthernet1/0/10
 port link-mode route
 ip address 192.100.63.43 255.255.255.128
 ip last-hop hold
 nat outbound 3005
 nat static enable
 manage ping inbound
 manage ping outbound
#
acl advanced 3005
 rule 10 deny ip source 10.55.0.17
 rule 15 permit ip
#
```

进行配置优化后，现场反馈业务还是不正常。进一步抓包定位问题，首先看NAT转换已经没有问题了，报文都是成对出现。



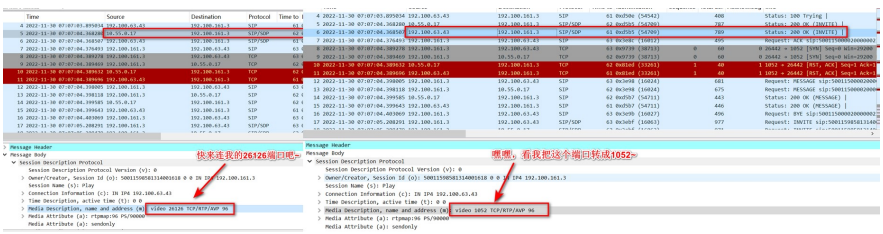
	Time	Source	Destination	Protocol	Time to	Identification	Sequence	Total Ler	Acknowledg	Info
1	2022-11-30 07:07:03.889263	192.100.161.3	192.100.63.43	SIP/SDP	63	0x3cc4 (15556)		977		Request: INVITE sip:500115985813140
2	2022-11-30 07:07:03.889634	192.100.161.3	10.55.0.17	SIP/SDP	62	0x3cc4 (15556)		971		Request: INVITE sip:500115985813140
3	2022-11-30 07:07:03.894856	10.55.0.17	192.100.161.3	SIP	62	0xd50e (54542)		405		Status: 100 Trying |
4	2022-11-30 07:07:03.895034	192.100.161.3	192.100.63.43	SIP	61	0xd50e (54542)		408		Status: 100 Trying |
5	2022-11-30 07:07:04.368280	10.55.0.17	192.100.161.3	SIP/SDP	62	0xd5b5 (54709)		787		Status: 200 OK (INVITE) |
6	2022-11-30 07:07:04.368507	192.100.161.3	192.100.63.43	SIP/SDP	61	0xd5b5 (54709)		789		Status: 200 OK (INVITE) |
7	2022-11-30 07:07:04.376493	192.100.161.3	192.100.63.43	SIP	63	0x3e8c (16012)		495		Request: ACK sip:500115000020000002
8	2022-11-30 07:07:04.389278	192.100.161.3	192.100.63.43	TCP	63	0x9739 (38713)	0	60		0 26442 → 1052 [SYN] Seq=0 Win=29200
9	2022-11-30 07:07:04.389469	192.100.161.3	10.55.0.17	TCP	62	0x9739 (38713)	0	60		0 26442 → 1052 [SYN] Seq=0 Win=29200
10	2022-11-30 07:07:04.389632	10.55.0.17	192.100.161.3	TCP	62	0x81ed (33261)	1	40		1 1052 → 26442 [RST, ACK] Seq=1 Ack=1
11	2022-11-30 07:07:04.389696	192.100.63.43	192.100.161.3	TCP	61	0x81ed (33261)	1	40		1 1052 → 26442 [RST, ACK] Seq=1 Ack=1
12	2022-11-30 07:07:04.398005	192.100.161.3	192.100.63.43	SIP	63	0x3e98 (16024)		681		Request: MESSAGE sip:500115000020000
13	2022-11-30 07:07:04.398118	192.100.161.3	10.55.0.17	SIP	62	0x3e98 (16024)		675		Request: MESSAGE sip:500115000020000
14	2022-11-30 07:07:04.399585	10.55.0.17	192.100.161.3	SIP	62	0xd5b7 (54711)		443		Status: 200 OK (MESSAGE) |

问题显而易见出现在No.8和No.9报文，监控中心连接服务器的1052端口，连接被重置了，导致获取视频信息失败。

对于TCP连接来说，连接被重置的原因有很多，最可能的原因是请求了一个不存在的端口，即服务器的1052端口并没有提供服务。

那么，为什么监控中心会去连接服务器的1052端口呢，问题可以从服务器回给监控中心的200 OK报文中（No.5和No.6）找到答案。

很显然，服务器回应给监控中心的报文中，打开端口由26126变成了1052。



原因在于防火墙开启了NAT SIP ALG功能，会对应用层的IP地址和端口进行转换，并建立对应的关联表项。但是对于现场的业务模型来说，内网服务器做了B2BUA，把自己插入到了后续sip信令的路径上，实际是不需要防火墙开启ALG功能的。

解决方法

关闭NAT SIP ALG功能。

建议：针对SIP的问题，建议在防火墙上抓取NAT前后的报文进行分析，同时把正向的报文和反向的报文都打印出来（打印会话添加verbose参数！！），关联表（disp session relation-table ipv4）作为辅助，一起分析吧~