某局点F10X0防火墙多出口链路外网访问内网异常的经验案例

NAT 叶靖 2019-11-29 发表

组网及说明

某局点购买了一台F1010的防火墙设备，设备版本为comvare v7 R9514P28。现在设备作为用户现场的出口设备，防火墙上有两条运营商外网链路，一条是 IP 地址的链路，IP地址为2.2.2.2/24，另一条是PPPOE拨号上网的，IP地址为3.3.3.3/24，客户现场内网有一台内网服务器，在两条外网线路上都配置了NAT server将内网的服务器映射出去。

主要配置如下：

```
interface Dialer1
 description TO_LianTong
 mtu 1450
 ppp pap local-user xxxxxx password cipher xxxxxxxxxxxxxx
 dialer bundle enable
 dialer-group 1
 dialer timer idle 0
 dialer timer autodial 60
 ip address ppp-negotiate
 tcp mss 1200
 nat outbound
 nat server protocol tcp global current-interface 5000 inside 172.16.20.250 5000 reversible
 nat server protocol tcp global current-interface 5978 inside 172.16.10.40 5001
#
interface GigabitEthernet1/0/2
 port link-mode route
 description TO_LianTong
 ip last-hop hold
 pppoe-client dial-bundle-number 1

#
interface GigabitEthernet1/0/3
 port link-mode route
 description TO_DianXin
 mtu 1450
 ip address 2.2.2.2 255.255.255.0
 tcp mss 1200
 ip last-hop hold
 nat outbound
 nat server protocol tcp global current-interface 5000 inside 172.16.20.250 5000 reversible
 nat server protocol tcp global current-interface 5978 inside 172.16.10.40 5001
```

问题描述

现场测试发现，外网通过固定IP地址线路映射出去的地址访问内网服务器，可以正常访问；但是通过拨号线路映射出去的IP地址进行访问，是无法正常访问的。

过程分析

我们后续继续从外网访问内网服务器测试，其中外网终端映射出去的公网地址为1.1.1.1/24，在F1010防火墙设备上通过查看会话如下：

```
<F1010>display session table ipv4 source-ip 1.1.1.1 verbose
Slot 1:
Initiator:
  Source      IP/port: 1.1.1.1/5306
  Destination IP/port: 3.3.3.3/5000
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
```

Inbound interface: Dialer1
Source security zone: Untrust
Responder:
Source IP/port: 172.16.20.250/5000
Destination IP/port: 1.1.1.1/5306
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/4
Source security zone: Trust
State: TCP_SYN_RECV
Application: GENERAL_TCP
Start time: 2019-10-31 19:37:04 TTL: 22s
Initiator->Responder: 3 packets 156 bytes
Responder->Initiator: 6 packets 312 bytes

可以从会话信息看到，会话是有收有发的，但是会话状态卡在TCP_SYN_RECV，之后我们在防火墙的内外网接口上进行抓包发现，内网口试收到了请求的，并且从内网口将请求转发给了服务器，另外服务器也回包了，但是并没有从外网口发出去。感觉是保存上一跳并没有生效。

之后我们确认，保存上一跳只能配在以太口，但是PPPOE拨号口进来的流量创建的快转表项指明的接口是dialer口，所以这种情况下无法配置保存上一跳。

解决方法

当前可以通过下面三种办法规避：
1、内网口做策略路由，指向拨号口，固定口的映射由于配置了保存上一跳，优先于策略路由，所以不受影响。
2、内网服务器配置sub地址，策略路由匹配sub地址。
3、Dialer口配合nat inbound。