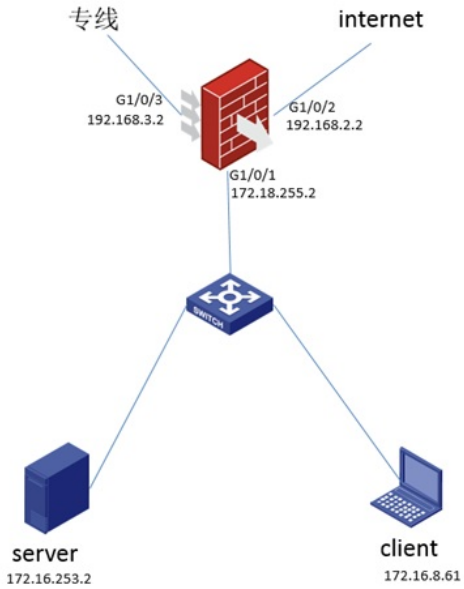
V7防火墙内网口配置策略路由后nat hairpin不生效经验案例

NAT 策略路由 **孙兆强** 2022-10-31 发表

组网及说明

注：此处公网地址用私网地址代替



用户公网有一条internet线路跟一条专线，通过策略路由指定client流量走internet，服务器server到特定网段的流量走专线。

问题描述

用户希望client通过公网地址访问内部服务器，在内网口部署nat hairpin不生效。

过程分析

从fw上分别ping终端及服务器均能通，路由核查无问题。
内网口trust域到trust域已放通，安全策略检查无问题。

```
interface GigabitEthernet1/0/2
 port link-mode route
 combo enable copper
 ip address 192.168.2.2 255.255.255.0
 nat outbound 3001 address-group 1
 nat server protocol tcp global 192.168.2.2 1823 inside 172.16.253.2 23

nat address-group 1
 address 192.168.2.3 192.168.2.3

[FW]dis ip policy-based-route
Policy name: 1
  node 10 permit:
    if-match acl 3002
    apply next-hop 192.168.3.1
  node 20 permit:
    if-match acl 3003
    apply next-hop 192.168.2.1

[FW]dis acl all
Advanced IPv4 ACL 3002, 1 rule,
ACL's step is 5
 rule 5 permit ip source 172.16.253.0 0.0.0.255

Advanced IPv4 ACL 3003, 2 rule,
ACL's step is 5
 rule 5 permit ip source 172.16.8.0 0.0.0.255
rule 10 permit ip
```

查看会话信息没有收到回程的报文。

```
[FW]dis session table ipv4 verbose
Slot 1:
Initiator:
  Source      IP/port: 172.16.8.61/24003
  Destination IP/port: 192.168.2.2/1823
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Trust
Responder:
  Source      IP/port: 172.16.253.2/23
  Destination IP/port: 192.168.2.3/1027
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust
State: TCP_SYN_SENT
Application: GENERAL_TCP
Start time: 2022-10-31 22:00:49  TTL: 27s
Initiator->Responder:            2 packets        120 bytes
Responder->Initiator:            0 packets          0 bytes

Total sessions found: 1
```

在fw内网口抓包发现没有报文发下到服务器，全局抓包发现有到server的目的地址报文。但是源地址是

192.168.2.3。在fw上debug nat packet发现只有单向的nat，没有回程的nat

[FW]dis session table ipv4 verbose

解决方法

将acl 3003中的rule 10去掉，或者在前面增加一个node节点匹配源地址192.168.2.3目的是172.16.253.2动作permit指定内网回不一跳。

Slot 1:

Total sessions found: 0

[FW]dis session table ipv4 verbose

Slot 1:

Total sessions found: 0

[FW]debug nat packet

[FW]Oct 31 22:00:49:251 2022 FW NAT/7/COMMON: -COntext=1;

PACKET: (GigabitEthernet1/0/2-out-config) Protocol: TCP

172.16.8.61:24003 - 192.168.2.2: 1823(VPN: 0) ------>

192.168.2.3: 1027 - 192.168.2.2: 1823(VPN: 0)

Oct 31 22:00:49:251 2022 FW NAT/7/COMMON: -COntext=1;

PACKET: (GigabitEthernet1/0/1-in-config) Protocol: TCP

192.168.2.3: 1027 - 192.168.2.2: 1823(VPN: 0) ------>

192.168.2.3: 1027 - 172.16.253.2: 23(VPN: 0)

Oct 31 22:00:49:251 2022 FW NAT/7/COMMON: -COntext=1;

PACKET: (GigabitEthernet1/0/2-out-config) Protocol: TCP

172.16.8.61:24004 - 192.168.2.2: 1823(VPN: 0) ------>

192.168.2.3: 1028 - 192.168.2.2: 1823(VPN: 0)

*Oct 31 22:38:00:942 2022 FW NAT/7/COMMON: -COntext=1;

PACKET: (GigabitEthernet1/0/1-in-config) Protocol: TCP

192.168.2.3: 1028 - 192.168.2.2: 1823(VPN: 0) ------>

192.168.2.3: 1028 - 172.16.253.2: 23(VPN: 0)

*Oct 31 22:38:00:949 2022 FW NAT/7/COMMON: -COntext=1;

PACKET: (GigabitEthernet1/0/1-in-session) Protocol: TCP

172.16.253.2: 23 - 192.168.2.3: 1028(VPN: 0) ------>

192.168.2.2: 1823 - 192.168.2.3: 1028(VPN: 0)

*Oct 31 22:38:00:949 2022 FW NAT/7/COMMON: -COntext=1;

PACKET: (GigabitEthernet1/0/1-out-session) Protocol: TCP

192.168.2.2: 1823 - 192.168.2.3: 1028(VPN: 0) ------>

192.168.2.2: 1823 - 172.16.8.61:24004(VPN: 0)

Acl number 3003

ACL's step is 5

rule 5 permit ip source 172.16.8.0 0.0.0.255

rule 10 permit ip

fw的流量处理规则

设备接收报文3: 192.168.2.3 -> 172.16.253.2 策略路由 -> 安全策略

服务器的回程报文看抓包结果看得知流量进入后就进行了nat，并且同时做了源及目的地址转换，然后再进行策略路由的匹配，所以4行会到服务器的报文命中策略路由走了Tunnel出口。