某局点M9000不同VPN实例NAT映射不通处理经验案例

域间策略/安全域 孙轶宁 2019-06-16 发表

组网及说明

M9K串在两台路由设备之间，与RT1互联口属于VPN实例v1，与RT2互联口属于VPN实例v2。RT2没有去RT1的路由，在M9K上将RT1映射到与RT2的互联口上。

问题描述

RT1能够正常访问RT2，但是RT2无法通过映射的地址访问RT1。

M9K上相关配置如下：

```
ip vpn-instance v1
 #
 address-family ipv4
   route-replicate from vpn-instance v2 protocol direct   //将v2中的直连路由引入v1
#
ip vpn-instance v2
 #
 address-family ipv4
  route-replicate from vpn-instance v1 protocol direct  //将v1中的直连路由引入v2
#
 nat static outbound 192.168.1.2 vpn-instance v1 192.168.2.1 vpn-instance v2
#
interface GigabitEthernet3/0/1
 ip binding vpn-instance v1
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet3/0/2
 ip binding vpn-instance v2
 ip address 192.168.2.1 255.255.255.0
 nat outbound vpn-instance v2
 nat static enable
#
security-zone name Trust
 import interface GigabitEthernet3/0/1
#
security-zone name Untrust
 import interface GigabitEthernet3/0/2
#
security-policy ip
 rule 1 name p1
  action pass
  vrf v1
  source-zone trust
  destination-zone untrust
 rule 2 name p2
  action pass
  vrf v2
  source-zone untrust
  destination-zone trust
```

过程分析

1、在防火墙上面debugging aspf packet，发现报错如下

*Jun 16 19:38:03:514 2019 H3C ASPF/7/PACKET: -COntext=1; The first packet was dropped by packet filter or object-policy. Src-ZOne=**Untrust**, Dst-ZOne=**Trust**;If-In=GigabitEthernet3/0/2(2), If-Out=GigabitEthernet3/0/1(1); Packet Info:Src-IP=192.168.2.2, Dst-IP=192.168.1.2, VPN-Instance=**v2**, Src-Port=195, Dst-Port=2048. Protocol=ICMP(1).

2、检查与VPN实例的配置，发现与p2的配置一致，但是结果是不通的。

rule 2 name p2

action pass
vrf **v2**
source-zone **untrust**
destination-zone **trust**

3、尝试修改配置测试，在RT2上面加上路由，直接通过路由访问RT1，发现能够ping通。查看会话匹配到的是rule 2

Initiator:
Source IP/port: 192.168.2.2/203
Destination IP/port: 192.168.1.2/2048
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: v2/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet3/0/2
Source security zone: Untrust
Responder:
Source IP/port: 192.168.1.2/203
Destination IP/port: 192.168.2.2/0
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: v1/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet3/0/1
Source security zone: Trust
State: ICMP_REPLY
Application: ICMP
Rule ID: 2
Rule name: p2
Start time: 2019-06-16 19:47:14 TTL: 22s
Initiator->Responder: 5 packets 420 bytes
Responder->Initiator: 5 packets 420 bytes

4、经过确认，在涉及nat server以及nat outbound转化报文目的地址的时候，安全策略里面配置的vpn实例写的是目的vpn实例，而不是源vpn实例。

配置下面策略后，发现RT2能够通过映射后的地址访问RT1。

rule 3 name p3
action pass
vrf v1
source-zone untrust
destination-zone trust

能够看到会话匹配的是该策略

Initiator:
Source IP/port: 192.168.2.2/206
Destination IP/port: 192.168.2.1/2048
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: v2/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet3/0/2
Source security zone: Untrust
Responder:
Source IP/port: 192.168.1.2/206
Destination IP/port: 192.168.2.2/0
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: v1/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet3/0/1
Source security zone: Trust
State: ICMP_REPLY
Application: ICMP
Rule ID: 3
Rule name: p3
Start time: 2019-06-16 19:52:11 TTL: 25s
Initiator->Responder: 5 packets 420 bytes
Responder->Initiator: 5 packets 420 bytes

解决方法

在涉及nat server以及nat outbound转化报文目的地址的时候，安全策略里面配置的vpn实例写的是目的vpn实例，而不是源vpn实例。

```
security-policy ip
 rule 1 name p2  //RT1直接通过路由访问RT2，即1.2 ping 2.2的时候，需要这一条安全策略
  action pass
  vrf v1
  source-zone trust
  destination-zone untrust
 rule 2 name p2  //RT2直接通过路由访问RT1，即2.2 ping 1.2的时候，需要这一条安全策略
  action pass
  vrf v2
  source-zone trust
  destination-zone untrust
 rule 3 name p3  //RT2通过nat映射访问RT1 ，即2.2 ping 2.1的时候，需要这一条安全策略
  action pass
  vrf v1
  source-zone untrust
  destination-zone trust
```