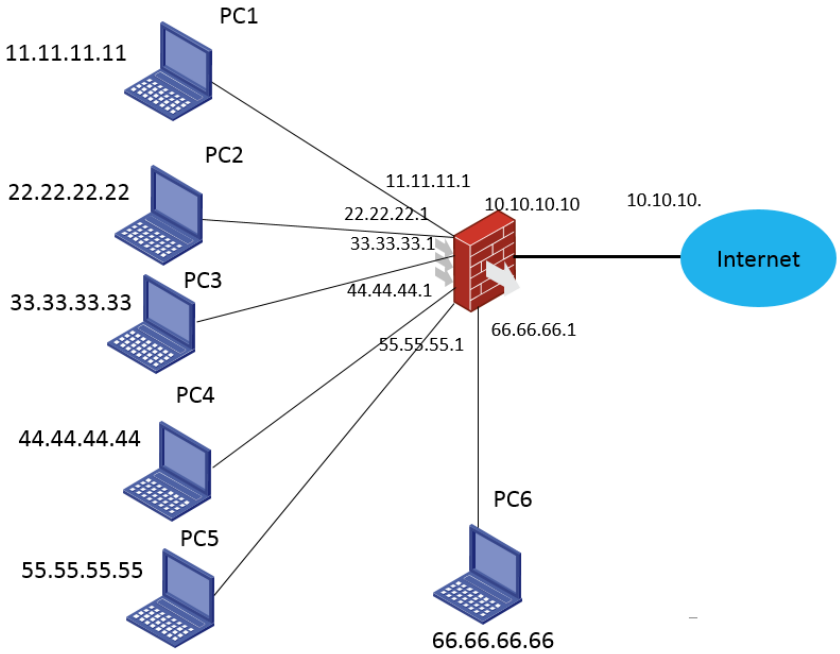
指定内网PC nat转换指定地址出公网，该地址同时可用于其他PC进行地址转换

NAT 郭尧 2020-03-30 发表

组网及说明

PC1进行一对一静态地址转换为1.1.1.1，其他PC进行动态地址转换1.1.1.1-6.6.6.6



配置步骤

防火墙主要配置：

```
#
nat address-group 2
 address 1.1.1.1 1.1.1.1
 address 2.2.2.2 2.2.2.2
 address 3.3.3.3 3.3.3.3
#
 nat static outbound 11.11.11.11 1.1.1.1
#
interface GigabitEthernet1/0/2
 port link-mode route
 combo enable copper
 ip address 10.10.10.10 255.255.255.0
 nat outbound 3099 address-group 2
 nat static enable
#
interface GigabitEthernet1/0/3
 port link-mode route
 combo enable copper
 ip address 11.11.11.1 255.255.255.0
#
interface GigabitEthernet1/0/4
 port link-mode route
 combo enable copper
 ip address 22.22.22.1 255.255.255.0
#
interface GigabitEthernet1/0/5
 port link-mode route
 combo enable copper
 ip address 33.33.33.1 255.255.255.0
#
interface GigabitEthernet1/0/6
```

```
 port link-mode route
 combo enable copper
 ip address 44.44.44.1 255.255.255.0
#
interface GigabitEthernet1/0/7
 port link-mode route
 combo enable copper
 ip address 55.55.55.1 255.255.255.0
#
security-zone name Trust
 import interface GigabitEthernet1/0/3
 import interface GigabitEthernet1/0/4
 import interface GigabitEthernet1/0/5
 import interface GigabitEthernet1/0/6
 import interface GigabitEthernet1/0/7
#
security-zone name DMZ
#
security-zone name Untrust
 import interface GigabitEthernet1/0/2
#
acl advanced 3099
 rule 0 deny ip source 11.11.11.11 0
 rule 5 permit ip
#
#
security-policy ip
 rule 0 name tong
  action pass
#
```

配置关键点

做了nat static enable有转换的会话，没有做就没有相应的会话

```
[H3C-GigabitEthernet1/0/2]dis nat sess v
Slot 1:
Initiator:
  Source      IP/port: 11.11.11.11/156
  Destination IP/port: 10.10.10.11/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/3
  Source security zone: Trust
Responder:
  Source      IP/port: 10.10.10.11/156
  Destination IP/port: 1.1.1.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust
State: ICMP_REPLY
Application: ICMP
Rule ID: 0
Rule name: tong
Start time: 2020-03-25 20:44:59  TTL: 28s
Initiator->Responder:           5 packets       420 bytes
Responder->Initiator:           5 packets       420 bytes

[H3C-GigabitEthernet1/0/2]dis nat sess v
Slot 1:
Total sessions found: 0
```

其他网段的都可以正常转换且也能转换为1.1.1.1：

```
[H3C-GigabitEthernet1/0/2]dis nat sess v
```

Slot 1:
Initiator:
  Source   IP/port: 44.44.44.44/153
  Destination IP/port: 10.10.10.11/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/6
  Source security zone: Trust
Responder:
  Source   IP/port: 10.10.10.11/1
  Destination IP/port: 2.2.2.2/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust
State: ICMP_REPLY
Application: ICMP
Rule ID: 0
Rule name: tong
Start time: 2020-03-25 20:46:58 TTL: 22s
Initiator->Responder: 5 packets   420 bytes
Responder->Initiator: 5 packets   420 bytes

Initiator:
  Source   IP/port: 33.33.33.33/153
  Destination IP/port: 10.10.10.11/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/5
  Source security zone: Trust
Responder:
  Source   IP/port: 10.10.10.11/1
  Destination IP/port: 1.1.1.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust
State: ICMP_REPLY
Application: ICMP
Rule ID: 0
Rule name: tong
Start time: 2020-03-25 20:46:54 TTL: 18s
Initiator->Responder: 5 packets   420 bytes
Responder->Initiator: 5 packets   420 bytes

Initiator:
  Source   IP/port: 22.22.22.22/153
  Destination IP/port: 10.10.10.11/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/4
  Source security zone: Trust
Responder:
  Source   IP/port: 10.10.10.11/1
  Destination IP/port: 3.3.3.3/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2

```
  Source security zone: Untrust
State: ICMP_REPLY
Application: ICMP
Rule ID: 0
Rule name: tong
Start time: 2020-03-25 20:46:51  TTL: 15s
Initiator->Responder:            5 packets        420 bytes
Responder->Initiator:            5 packets        420 bytes

Initiator:
  Source      IP/port: 55.55.55.55/153
  Destination IP/port: 10.10.10.11/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/7
  Source security zone: Trust
Responder:
  Source      IP/port: 10.10.10.11/2
  Destination IP/port: 2.2.2.2/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust
State: ICMP_REPLY
Application: ICMP
Rule ID: 0
Rule name: tong
Start time: 2020-03-25 20:47:02  TTL: 26s
Initiator->Responder:            5 packets        420 bytes
Responder->Initiator:            5 packets        420 bytes

Total sessions found: 4
```

使用TCP协议进行测试：

```
dis sess tab ipv4 v
Slot 1:
Initiator:
  Source      IP/port: 1.1.1.1/61890
  Destination IP/port: 10.10.10.11/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Trust
Responder:
  Source      IP/port: 10.10.10.11/22
  Destination IP/port: 1.1.1.1/61890
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: TCP_ESTABLISHED
Application: SSH
Rule ID: 0
Rule name: tong
Start time: 2020-03-26 20:19:11  TTL: 1179s
Initiator->Responder:           32 packets       3349 bytes
Responder->Initiator:           31 packets       3717 bytes

Initiator:
```

```
  Source      IP/port: 2.2.2.2/1025
  Destination IP/port: 10.10.10.11/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Trust
Responder:
  Source      IP/port: 10.10.10.11/22
  Destination IP/port: 2.2.2.2/1025
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: TCP_ESTABLISHED
Application: SSH
Rule ID: 0
Rule name: tong
Start time: 2020-03-26 20:24:36  TTL: 1194s
Initiator->Responder:          29 packets       3277 bytes
Responder->Initiator:          28 packets       3817 bytes

Initiator:
  Source      IP/port: 1.1.1.1/1024
  Destination IP/port: 10.10.10.11/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Trust
Responder:
  Source      IP/port: 10.10.10.11/22
  Destination IP/port: 1.1.1.1/1024
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: TCP_ESTABLISHED
Application: SSH
Rule ID: 0
Rule name: tong
Start time: 2020-03-26 20:21:32  TTL: 1183s
Initiator->Responder:          34 packets       3553 bytes
Responder->Initiator:          33 packets       4077 bytes

Initiator:
  Source      IP/port: 2.2.2.2/1024
  Destination IP/port: 10.10.10.11/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Trust
Responder:
  Source      IP/port: 10.10.10.11/22
  Destination IP/port: 2.2.2.2/1024
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: TCP_ESTABLISHED
```

Application: SSH
Rule ID: 0
Rule name: tong
Start time: 2020-03-26 20:22:58 TTL: 1184s
Initiator->Responder: 31 packets 3357 bytes
Responder->Initiator: 30 packets 3921 bytes

Initiator:
  Source IP/port: 3.3.3.3/1024
  Destination IP/port: 10.10.10.11/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Trust
Responder:
  Source IP/port: 10.10.10.11/22
  Destination IP/port: 3.3.3.3/1024
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: TCP_ESTABLISHED
Application: SSH
Rule ID: 0
Rule name: tong
Start time: 2020-03-26 20:19:03 TTL: 1180s
Initiator->Responder: 38 packets 3713 bytes
Responder->Initiator: 37 packets 4285 bytes

Total sessions found: 5
根据会话情况来看，静态地址转换和动态地址转换都已经生效，该限制功能能够实现对内网某个PC指定地址出公网，由于一个地址只能加入一个地址组，无法通过配置多个NAT+不同地址组的方式实现，由于静态NAT的优先级高于动态NAT，所以可通过一对一静态地址转换来实现
另外由于测试环境现场流量业务并不大，没有出现静态nat和动态nat端口冲突的情况，在实际生产环境中，由于业务量大，涉及的地址转换情况比较多，有可能会出现静态地址转换和动态地址转换出现端口冲突的情况，在实际环境下要考虑端口冲突，避免影响业务