

## HCIA 实验 9 ACL 和 NAT

版本 V1.0

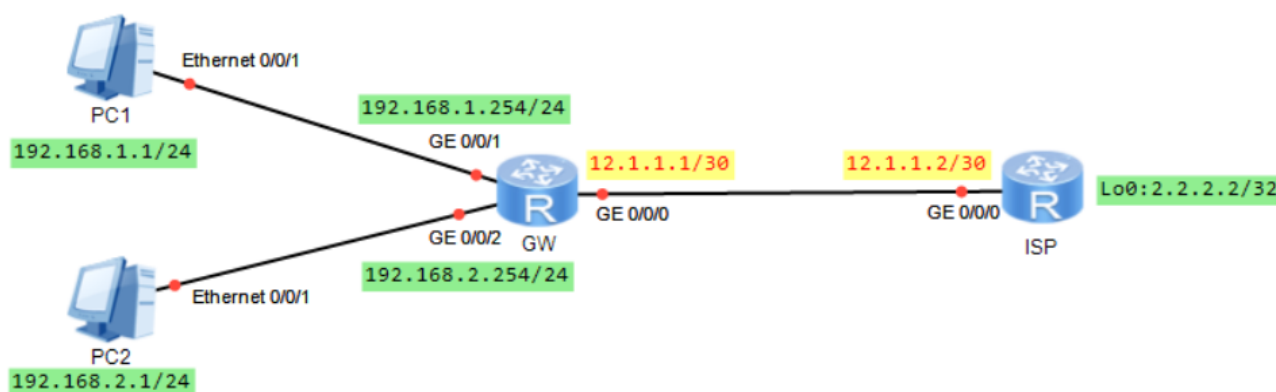
密级 ☒ 开放 ☐ 内部 ☐ 机密

类型 ☐ 讨论版 ☐ 测试版 ☒ 正式版

修订记录

修订日期	修订人	版本号	审核人	修订说明
2019-11-14	Ryan	1.0		
2020-03-01	童驰阳	1.1		增加静态 nat 和 server nat 配置说明

### 1 实验拓扑



### 2 实验需求

- 如图所示，配置设备名称和IP地址。GW为模拟企业网关设备，ISP模拟运营商设备。
- 在GW上使用高级ACL，使得PC1不能访问PC2，满足以下需求：
  - ACL编号为3000
  - 只有一条规则，且序号为5

- c) 仅仅拒绝PC1访问PC2的流量，其他任何流量不得拒绝
  - d) 在入方向上调用该ACL
3. 在GW上部署NAT和默认路由满足以下需求：
- a) NAT使用基础ACL，编号为2000，且只有一条规则，序号为5，仅允许PC1所在的网络号
  - b) PC1访问ISP时会使用GW的G0/0/0地址，并采用端口转换的形式
  - c) 因PC2需要为外网用户提供服务，企业从ISP处购买了新的公网地址100.1.1.1/32
4. 配置静态NAT，使得外网ISP访问100.1.1.1就可以访问到PC2。
- (提示：ISP上没有100.1.1.1/32的路由，企业付费购买公网地址后，ISP需配置静态路由。)

## 3 配置思路及验证结果

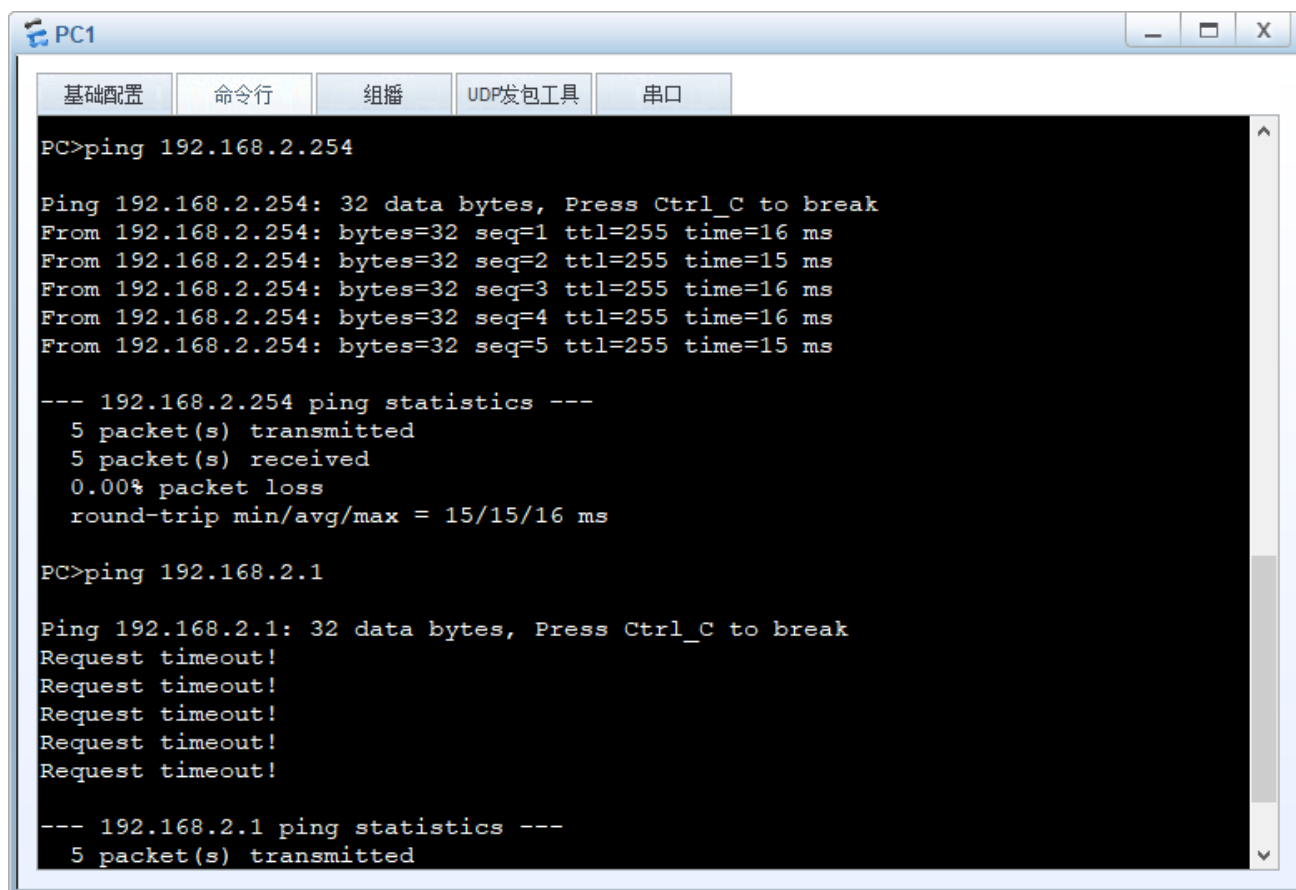
### 3.1 在网关配置高级 ACL

GW

```
[Huawei] sysname GW
[GW] interface g0/0/1
[GW-GigabitEthernet0/0/1] ip address 192.168.1.254 24
[GW-GigabitEthernet0/0/1] interface g0/0/2
[GW-GigabitEthernet0/0/2] ip address 192.168.2.254 24
[GW] acl 3000
[GW-acl-adv-3000] rule 5 deny ip source 192.168.1.1 0 destination 192.168.2.1 0
[GW-acl-adv-3000] interface g0/0/01
[GW-GigabitEthernet0/0/1] traffic-filter inbound acl 3000
```

### 3.2 验证实验部分现象

PC1 到 PC2 的网关能通，但是不能与 PC2 通信



The screenshot shows a PC terminal window with the following output:

```
PC>ping 192.168.2.254

Ping 192.168.2.254: 32 data bytes, Press Ctrl_C to break
From 192.168.2.254: bytes=32 seq=1 ttl=255 time=16 ms
From 192.168.2.254: bytes=32 seq=2 ttl=255 time=15 ms
From 192.168.2.254: bytes=32 seq=3 ttl=255 time=16 ms
From 192.168.2.254: bytes=32 seq=4 ttl=255 time=16 ms
From 192.168.2.254: bytes=32 seq=5 ttl=255 time=15 ms

--- 192.168.2.254 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 15/15/16 ms

PC>ping 192.168.2.1

Ping 192.168.2.1: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 192.168.2.1 ping statistics ---
 5 packet(s) transmitted
```

### 3.3 在网关部署 NAT 和默认路由

GW

[GW] acl 2000

[GW-acl-basic-2000] rule 5 permit source 192.168.1.0 0.0.0.255

[GW] interface g0/0/0

[GW-GigabitEthernet0/0/0] IP address 12.1.1.1 30

[GW-GigabitEthernet0/0/0] Nat outbound 2000

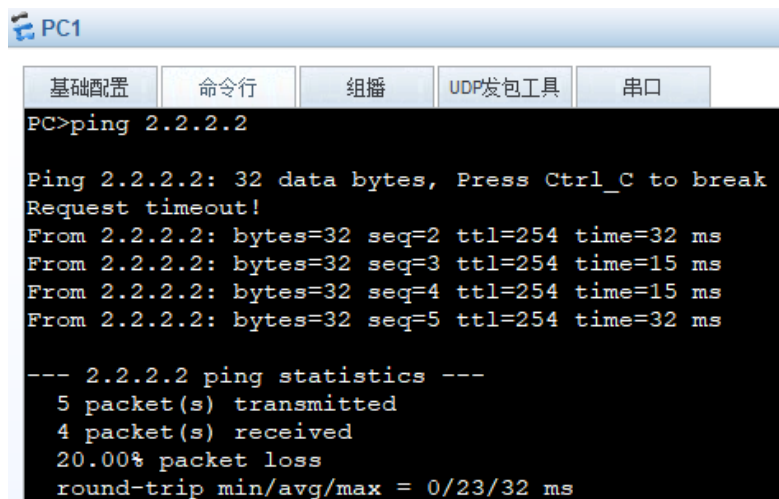
[GW-GigabitEthernet0/0/0] Nat static global 100.1.1.1 inside 192.168.2.1

\\此处使用nat server global 100.1.1.1 inside 192.168.2.1 亦可。区别在于static可以配置inside地址的掩码，server默认掩码32位。

[GW] ip route-static 0.0.0.0 0.0.0.0 12.1.1.2

### 3.4 验证部分实验现象

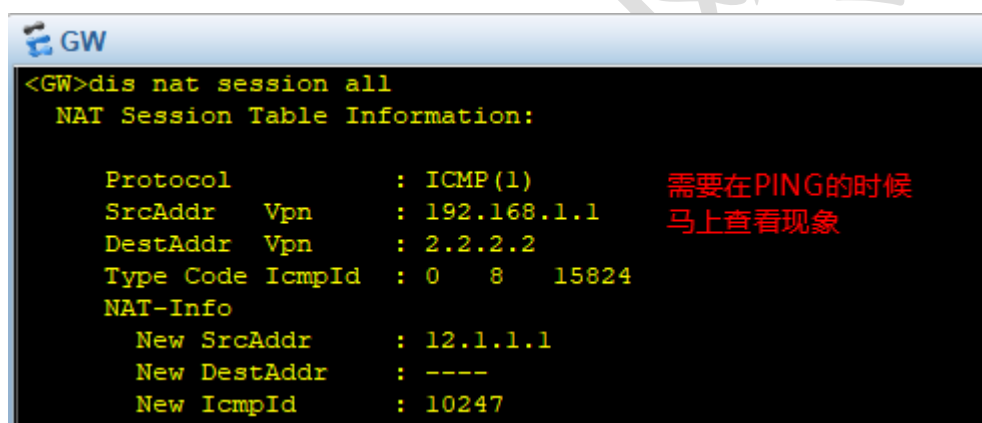
PC1 可以 ISP 互通



```
PC1
基础配置 命令行 组播 UDP发包工具 串口
PC>ping 2.2.2.2

Ping 2.2.2.2: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 2.2.2.2: bytes=32 seq=2 ttl=254 time=32 ms
From 2.2.2.2: bytes=32 seq=3 ttl=254 time=15 ms
From 2.2.2.2: bytes=32 seq=4 ttl=254 time=15 ms
From 2.2.2.2: bytes=32 seq=5 ttl=254 time=32 ms

--- 2.2.2.2 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
20.00% packet loss
round-trip min/avg/max = 0/23/32 ms
```



```
<GW>dis nat session all
NAT Session Table Information:

Protocol      : ICMP(1)
SrcAddr Vpn   : 192.168.1.1
DestAddr Vpn  : 2.2.2.2
Type Code IcmpId : 0 8 15824
NAT-Info
New SrcAddr   : 12.1.1.1
New DestAddr  : ----
New IcmpId    : 10247
```

需要在PING的时候  
马上查看现象

### 3.5 ISP 配置 IP 和静态路由

ISP

```
[Huawei] sysname ISP
[ISP] ip route-static 100.1.1.1 255.255.255.255 12.1.1.1
[ISP] interface g0/0/0
[ISP-GigabitEthernet0/0/0] IP address 12.1.1.2 30
```

### 3.6 验证部分实验现象

ISP 设备 ping 100.1.1.1 这个公网地址，GW 设备看 NAT 的情况

```
<ISP>ping 100.1.1.1
PING 100.1.1.1: 56 data bytes, press CTRL_C to break
Request time out
Reply from 100.1.1.1: bytes=56 Sequence=2 ttl=127 time=20 ms
Reply from 100.1.1.1: bytes=56 Sequence=3 ttl=127 time=20 ms
Reply from 100.1.1.1: bytes=56 Sequence=4 ttl=127 time=20 ms
Reply from 100.1.1.1: bytes=56 Sequence=5 ttl=127 time=20 ms

--- 100.1.1.1 ping statistics ---
5 packet(s) transmitted
4 packet(s) received
20.00% packet loss
round-trip min/avg/max = 20/20/20 ms
```

```
<GW>dis nat session all
NAT Session Table Information:

Protocol      : ICMP(1)
SrcAddr Vpn   : 12.1.1.2
DestAddr Vpn  : 100.1.1.1
Type Code IcmpId : 0 8 43983
NAT-Info
  New SrcAddr   : ----
  New DestAddr  : 192.168.2.1
  New IcmpId    : ----

Total : 1
```