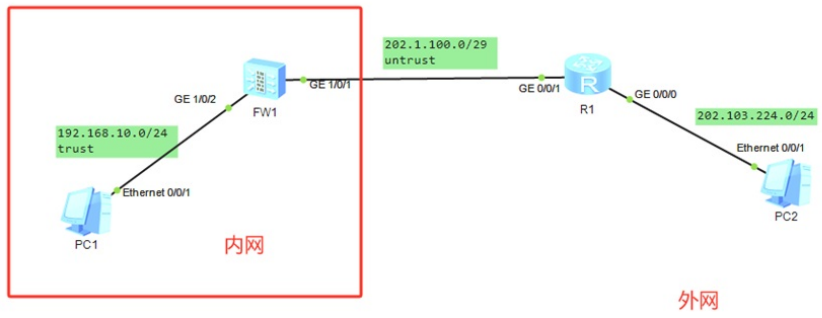
# 【MVS】华为防火墙Basic NAT典型组网配置案例

网络相关 韦家宁 2024-09-14 发表

## 组网及说明




组网说明：
本案例采用ENSP模拟器的防火墙来部署Basic NAT，安全域和内网、外网在网络拓扑图中已经有了明确的标识，FW1作为出口设备与外网连接，某局点申请到了202.1.100.2-202.1.100.4的公网地址，通过Basic NAT的方式，实现内网访问外网。

配置思路：
1、按照网络拓扑图配置IP地址。
2、配置FW1的安全策略。
3、配置FW1的Basic NAT。

## 配置步骤

R1：

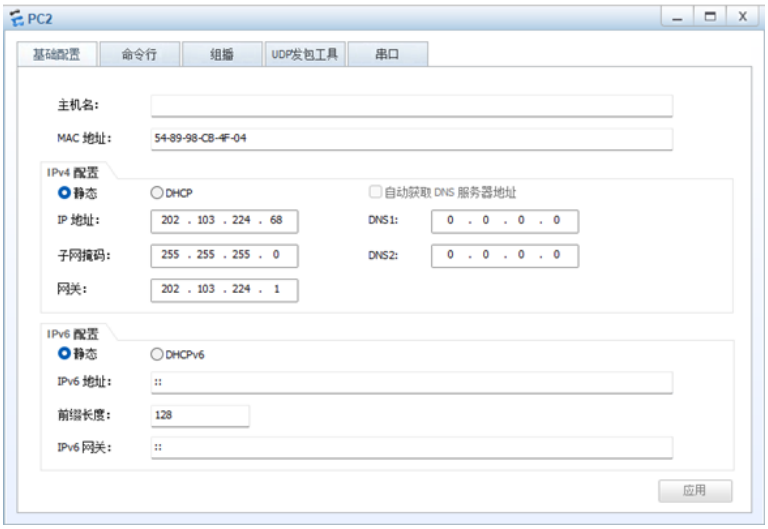
```
<Huawei>u t m
Info: Current terminal monitor is off.
<Huawei>u t d
Info: Current terminal debugging is off.
<Huawei>system
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]int gi 0/0/0
[R1-GigabitEthernet0/0/0]ip address 202.103.224.1 24
[R1-GigabitEthernet0/0/0]quit
[R1]int gi 0/0/1
[R1-GigabitEthernet0/0/1]ip address 202.1.100.1 29
[R1-GigabitEthernet0/0/1]quit
```

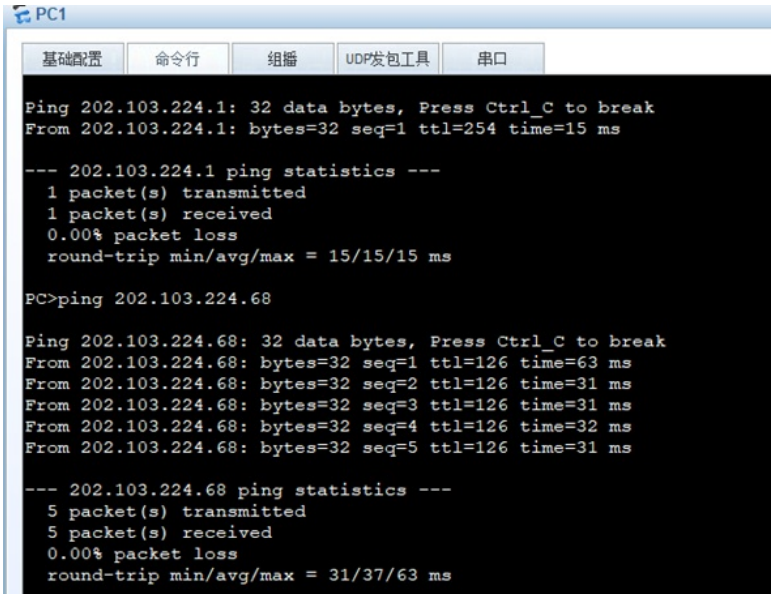
FW1：

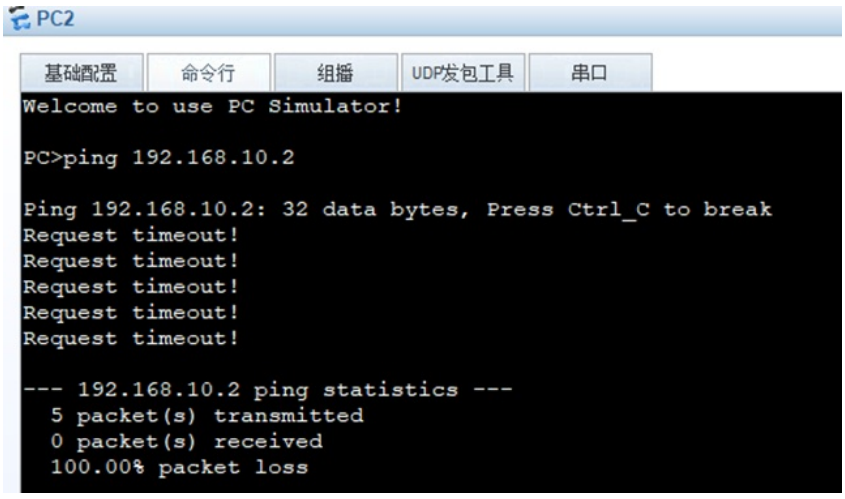
```
<USG6000V1>u t m
Info: Current terminal monitor is off.
<USG6000V1>u t d
Info: Current terminal debugging is off.
<USG6000V1>system
Enter system view, return user view with Ctrl+Z.
[USG6000V1]sysname FW1
[FW1]int gi 1/0/2
[FW1-GigabitEthernet1/0/2]ip address 192.168.10.1 24
[FW1-GigabitEthernet1/0/2]quit
[FW1]int gi 1/0/1
[FW1-GigabitEthernet1/0/1]ip address 202.1.100.2 29
[FW1-GigabitEthernet1/0/1]quit
[FW1]ip route-static 0.0.0.0 0.0.0.0 202.1.100.1

[FW1]firewall zone trust
```

```
[FW1-zone-trust]add int gi 1/0/2
[FW1-zone-trust]quit
[FW1]firewall zone untrust
[FW1-zone-untrust]add int gi 1/0/1
[FW1-zone-untrust]quit

[FW1]security-policy
[FW1-policy-security]rule name 1
[FW1-policy-security-rule-1]action permit
[FW1-policy-security-rule-1]source-address 192.168.10.0 24
[FW1-policy-security-rule-1]source-zone trust
[FW1-policy-security-rule-1]destination-zone untrust
[FW1-policy-security-rule-1]quit
[FW1-policy-security]quit

[FW1]nat address-group 1 10
[FW1-address-group-1]section 202.1.100.3 202.1.100.4
[FW1-address-group-1]quit
[FW1]nat statistics enable

[FW1]nat-policy
[FW1-policy-nat]rule name 1
[FW1-policy-nat-rule-1]source-address 192.168.10.0 24
[FW1-policy-nat-rule-1]action source-nat address-group 1
[FW1-policy-nat-rule-1]source-zone trust
[FW1-policy-nat-rule-1]destination-zone untrust
[FW1-policy-nat-rule-1]enable
```

内网的PC和外网的PC分别填写IP地址，内网的PC能PING通外网的PC，但是外网的PC无法PING通内网的PC，说明NAT已经生效。




查看NAT地址组的状态是激活的。

```
[FW1]dis nat address-group
2024-09-14 04:13:54.020
NAT address-group information:
  Total 1 address-group(s)
nat address-group 1 10
 reference count: 1
 mode pat
 status active
 section 0 202.1.100.3 202.1.100.4
[FW1]
```

查看防火墙的会话表，发现会话表的源地址已经转换后访问外网。

```
[FW1]dis firewall session table
2024-09-14 04:15:31.670
 Current Total Sessions : 19
 icmp  VPN: public --> public  192.168.10.2:53005[202.1.100.4:2556] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:51981[202.1.100.4:2552] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:51725[202.1.100.4:2551] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:48653[202.1.100.4:2540] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:48909[202.1.100.4:2541] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:52493[202.1.100.4:2554] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:50701[202.1.100.4:2547] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:51469[202.1.100.4:2550] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:53261[202.1.100.4:2557] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:49165[202.1.100.4:2542] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:49933[202.1.100.4:2545] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:52237[202.1.100.4:2553] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:49421[202.1.100.4:2543] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:49677[202.1.100.4:2544] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:50445[202.1.100.4:2546] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:53517[202.1.100.4:2558] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:51213[202.1.100.4:2549] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:50957[202.1.100.4:2548] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:52749[202.1.100.4:2555] --> 202.103.
224.68:2048
[FW1]
```

至此，华为防火墙Basic NAT典型组网配置案例已完成！