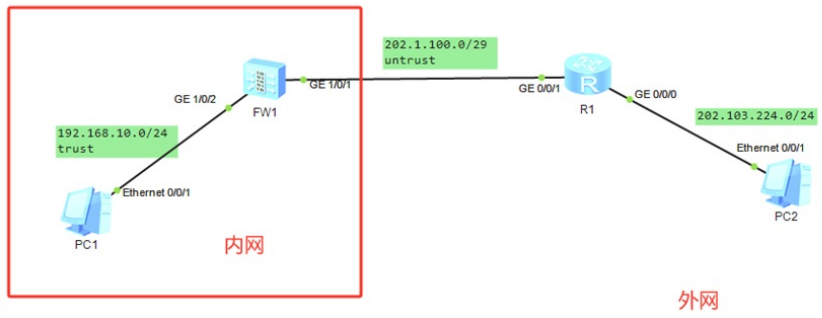
【MVS】华为防火墙NAPT典型组网配置案例

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NAPT，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202.1.100.2-202.1.100.3的公网地址，通过NAPT的方式，实现内网访问外网，因为防火墙的外网接口已经占用了202.1.100.2的一个公网IP，所以内网终端全部通过转换为202.1.100.3的IP地址访问外网。

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NAPT。

配置步骤

R1：

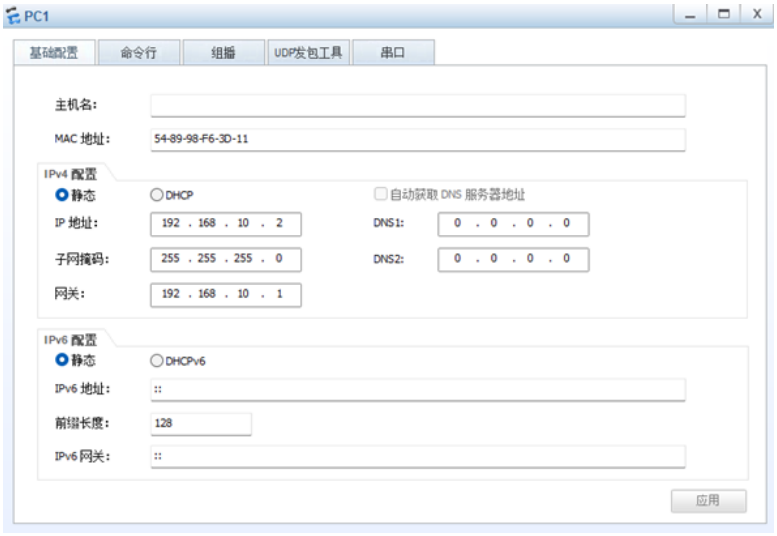
```
<Huawei>u t m
Info: Current terminal monitor is off.
<Huawei>u t d
Info: Current terminal debugging is off.
<Huawei>system
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]int gi 0/0/0
[R1-GigabitEthernet0/0/0]ip address 202.103.224.1 24
[R1-GigabitEthernet0/0/0]quit
[R1]int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

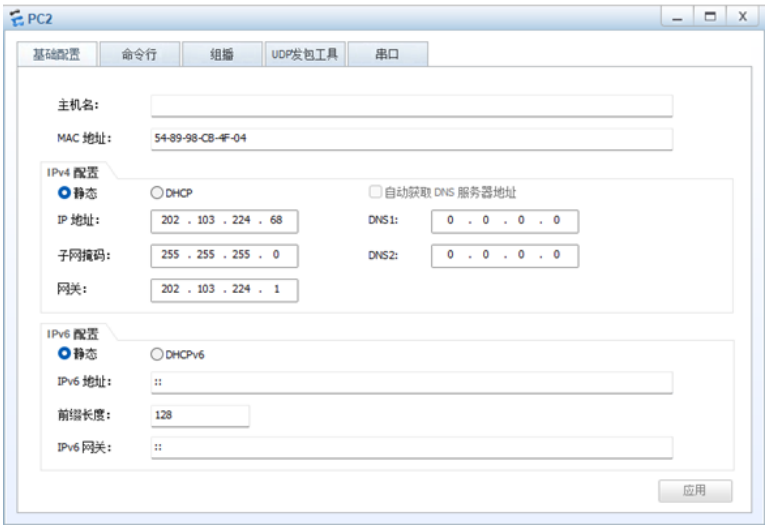
FW1：

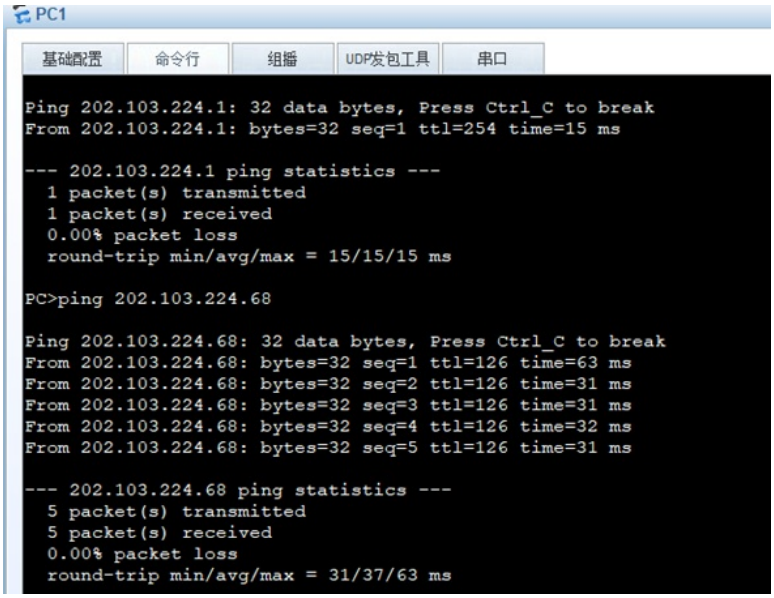
```
<USG6000V1>u t m
Info: Current terminal monitor is off.
<USG6000V1>u t d
Info: Current terminal debugging is off.
<USG6000V1>system
Enter system view, return user view with Ctrl+Z.
[USG6000V1]sysname FW1
[FW1]int gi 1/0/2
[FW1-GigabitEthernet1/0/2]ip address 192.168.10.1 24
[FW1-GigabitEthernet1/0/2]quit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

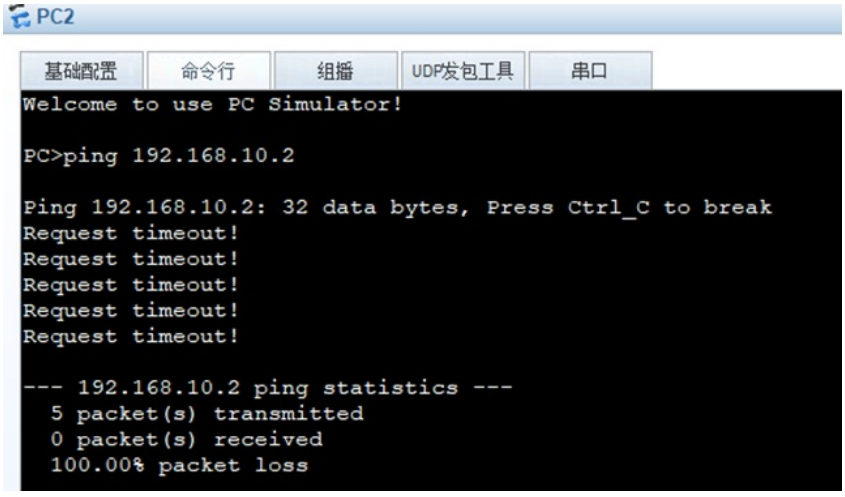
```
[FW1]firewall zone trust
[FW1-zone-trust]add int gi 1/0/2
[FW1-zone-trust]quit
[FW1]firewall zone untrust
[FW1-zone-untrust]add int gi 1/0/1
[FW1-zone-untrust]quit

[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
[FW1-address-group-1]section 202.1.100.3 202.1.100.3
[FW1-address-group-1]quit

[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]source-zone trust
[FW1-policy-nat-rule-1]destination-zone untrust
[FW1-policy-nat-rule-1]action source-nat address-group 1
[FW1-policy-nat-rule-1]quit
[FW1-policy-nat]quit
```

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 06:19:45.940
NAT address-group information:
  Total 1 address-group(s)
nat address-group 1 0
 reference count: 1
 mode pat
 status active
 section 0 202.1.100.3 202.1.100.3
[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 06:20:25.650
 Current Total Sessions : 19
 icmp  VPN: public --> public  192.168.10.2:55594[202.1.100.3:2152] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:55850[202.1.100.3:2153] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:53546[202.1.100.3:2144] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:51754[202.1.100.3:2138] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:54314[202.1.100.3:2147] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:52778[202.1.100.3:2141] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:52266[202.1.100.3:2139] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:55082[202.1.100.3:2150] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:51242[202.1.100.3:2136] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:51498[202.1.100.3:2137] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:52522[202.1.100.3:2140] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:54058[202.1.100.3:2146] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:53290[202.1.100.3:2143] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:54826[202.1.100.3:2149] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:55338[202.1.100.3:2151] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:53034[202.1.100.3:2142] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:53802[202.1.100.3:2145] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:50986[202.1.100.3:2135] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:54570[202.1.100.3:2148] --> 202.103.
224.68:2048
[FW1]
```

至此，华为防火墙NAPT典型组网配置案例已完成！