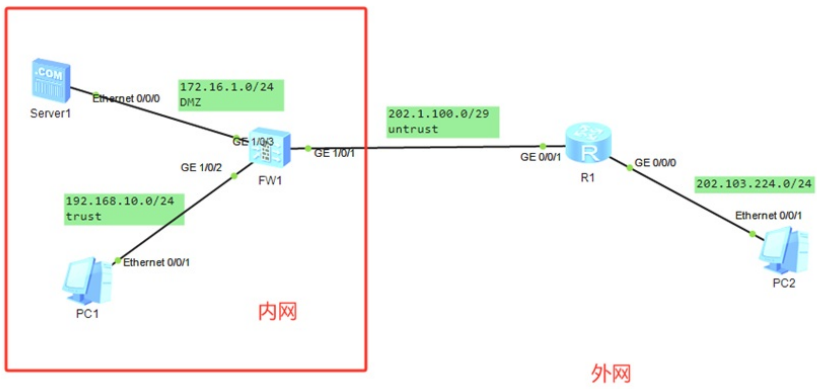
【MVS】华为防火墙NAT Server典型组网配置案例

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NAT Server将内网服务器映射到外网提供服务，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202.1.100.2-202.1.100.5的公网地址，通过Basic NAT的方式，内网的PC转换为202.1.100.3和202.1.100.4的IP地址实现内网访问外网，同时内网服务器映射为202.1.100.5的IP地址为外网提供服务。

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和NAT server。

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]int gi 1/0/3
[FW1-GigabitEthernet1/0/3]ip address 172.16.1.1 24
```

[FW1-GigabitEthernet1/0/3]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]firewall zone dmz
[FW1-zone-dmz]add int gi 1/0/3
[FW1-zone-dmz]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]rule name 2
[FW1-policy-security-rule-2]action permit
[FW1-policy-security-rule-2]source-zone untrust
[FW1-policy-security-rule-2]destination-zone dmz
[FW1-policy-security-rule-2]quit
[FW1-policy-security]rule name 3
[FW1-policy-security-rule-3]action permit
[FW1-policy-security-rule-3]source-zone trust dmz
[FW1-policy-security-rule-3]destination-zone trust dmz
[FW1-policy-security-rule-3]quit
[FW1-policy-security]quit

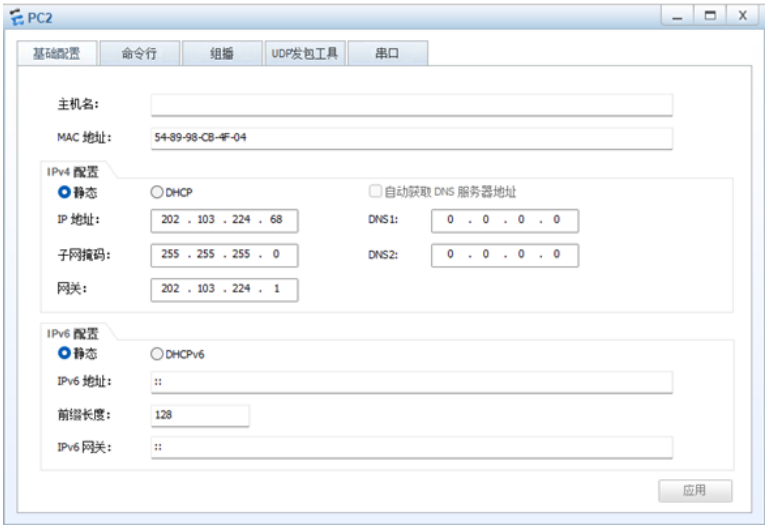
[FW1]nat address-group 1
[FW1-address-group-1]section 202.1.100.3 202.1.100.4
[FW1-address-group-1]quit

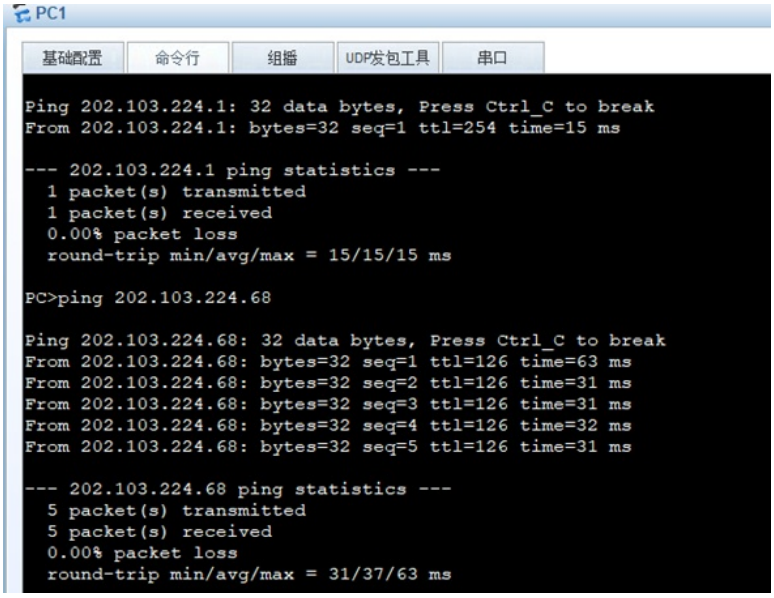
[FW1]nat server 1 global 202.1.100.5 inside 172.16.1.2
[FW1]nat statistics enable

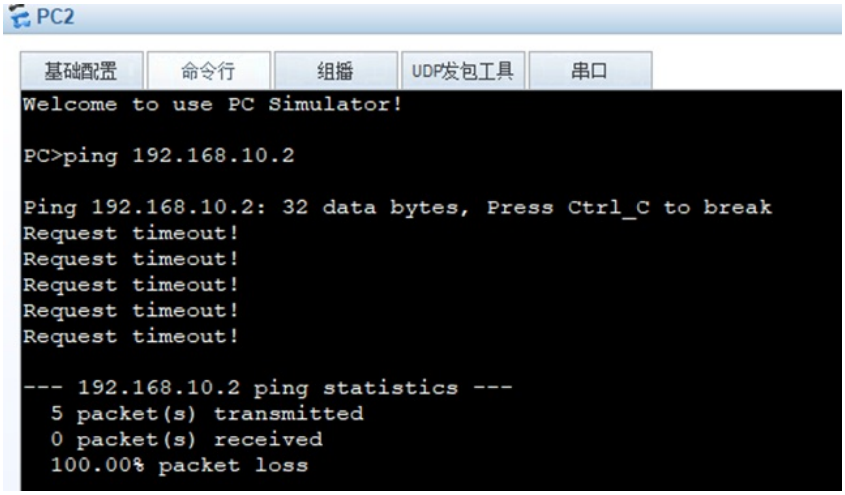
[FW1]nat-policy
[FW1-policy-nat]rule name 1
[FW1-policy-nat-rule-1]source-address 192.168.10.0 24
[FW1-policy-nat-rule-1]action source-nat address-group 1
[FW1-policy-nat-rule-1]source-zone trust
[FW1-policy-nat-rule-1]destination-zone untrust
[FW1-policy-nat-rule-1]enable
[FW1-policy-nat-rule-1]quit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


PC1
基础配置
命令行
组播
UDP发包工具
串口
主机名:
MAC 地址: 54-89-98-F6-3D-11
IPv4 配置
静态
DHCP
自动获取 DNS 服务器地址
IP 地址: 192 . 168 . 10 . 2
子网掩码: 255 . 255 . 255 . 0
网关: 192 . 168 . 10 . 1
DNS1: 0 . 0 . 0 . 0
DNS2: 0 . 0 . 0 . 0
IPv6 配置
静态
DHCPv6
IPv6 地址: ::
前缀长度: 128
IPv6 网关: ::
应用

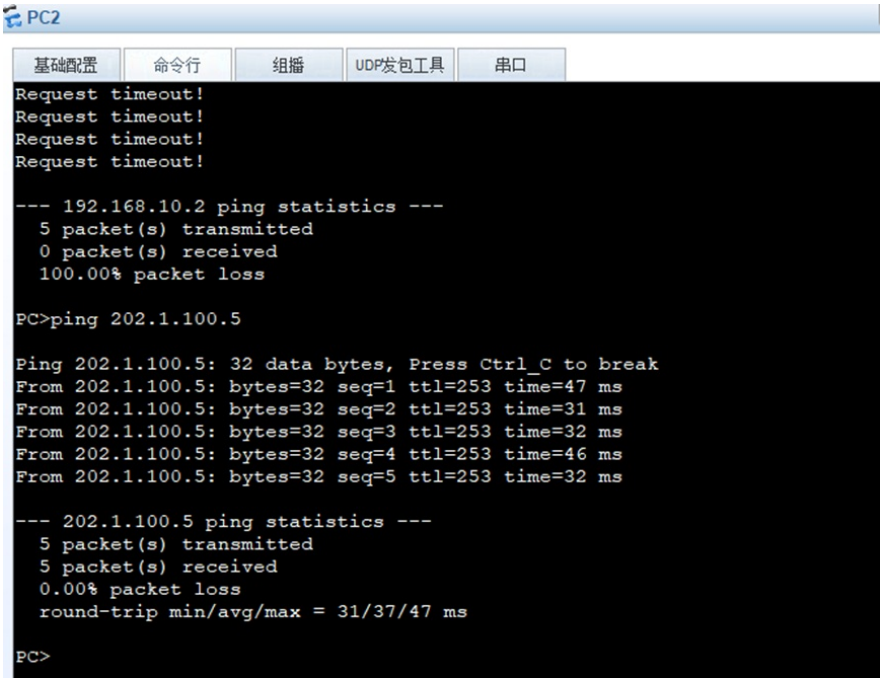

PC2
基础配置
命令行
组播
UDP发包工具
串口
主机名:
MAC 地址: 54-89-98-CB-4F-04
IPv4 配置
静态
DHCP
自动获取 DNS 服务器地址
IP 地址: 202 . 103 . 224 . 68
子网掩码: 255 . 255 . 255 . 0
网关: 202 . 103 . 224 . 1
DNS1: 0 . 0 . 0 . 0
DNS2: 0 . 0 . 0 . 0
IPv6 配置
静态
DHCPv6
IPv6 地址: ::
前缀长度: 128
IPv6 网关: ::
应用


PC1
基础配置
命令行
组播
UDP发包工具
串口
Ping 202.103.224.1: 32 data bytes, Press Ctrl_C to break
From 202.103.224.1: bytes=32 seq=1 ttl=254 time=15 ms
--- 202.103.224.1 ping statistics ---
1 packet(s) transmitted
1 packet(s) received
0.00% packet loss
round-trip min/avg/max = 15/15/15 ms
PC>ping 202.103.224.68
Ping 202.103.224.68: 32 data bytes, Press Ctrl_C to break
From 202.103.224.68: bytes=32 seq=1 ttl=126 time=63 ms
From 202.103.224.68: bytes=32 seq=2 ttl=126 time=31 ms
From 202.103.224.68: bytes=32 seq=3 ttl=126 time=31 ms
From 202.103.224.68: bytes=32 seq=4 ttl=126 time=32 ms
From 202.103.224.68: bytes=32 seq=5 ttl=126 time=31 ms
--- 202.103.224.68 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 31/37/63 ms



服务器填写IP地址。

外网的PC能PING通服务器映射后的公网IP。



查看NAT地址组的状态是激活的。

```
[FW1]dis nat address-group
2024-09-14 07:03:21.880
NAT address-group information:
  Total 1 address-group(s)
nat address-group 1 0
 reference count: 1
 mode pat
 status active
 section 0 202.1.100.3 202.1.100.4
[FW1]
```

查看NAT server的配置显示信息，确认配置没有问题。

```
[FW1]dis nat server
2024-09-14 07:03:34.060
Server in private network information:
  Total    1 NAT server(s)
 server name    : 1
 id             : 0                    zone           : ---
 global-start-addr : 202.1.100.5       global-end-addr    : 202.1.100.5
 inside-start-addr : 172.16.1.2        inside-end-addr    : 172.16.1.2
 global-start-port : ---               global-end-port    : ---
 inside-start-port : ---               inside-end-port    : ---
 globalvpn      : public               insidevpn      : public
 vsys           : public               protocol       : ---
 no-revers      : 0                    interface      : ---
 unr-route      : 0                    description    : ---
 nat-disable    : 0
```

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 07:04:09.480
 Current Total Sessions : 38
 icmp  VPN: public --> public  202.103.224.68:565 --> 202.1.100.5:2048[172.16.1.
2:2048]
 icmp  VPN: public --> public  192.168.10.2:64052[202.1.100.4:9522] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  202.103.224.68:53 --> 202.1.100.5:2048[172.16.1.2
:2048]
 icmp  VPN: public --> public  192.168.10.2:63028[202.1.100.4:9518] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  202.103.224.68:821 --> 202.1.100.5:2048[172.16.1.
2:2048]
 icmp  VPN: public --> public  202.103.224.68:1333 --> 202.1.100.5:2048[172.16.1
.2:2048]
 icmp  VPN: public --> public  202.103.224.68:309 --> 202.1.100.5:2048[172.16.1.
2:2048]
 icmp  VPN: public --> public  202.103.224.68:65332 --> 202.1.100.5:2048[172.16.
1.2:2048]
 icmp  VPN: public --> public  192.168.10.2:62260[202.1.100.4:9515] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:821[202.1.100.4:9531] --> 202.103.22
4.68:2048
 icmp  VPN: public --> public  192.168.10.2:62772[202.1.100.4:9517] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  202.103.224.68:63540 --> 202.1.100.5:2048[172.16.
1.2:2048]
 icmp  VPN: public --> public  192.168.10.2:65076[202.1.100.4:9526] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  202.103.224.68:64564 --> 202.1.100.5:2048[172.16.
1.2:2048]
 icmp  VPN: public --> public  192.168.10.2:63540[202.1.100.4:9520] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:62516[202.1.100.4:9516] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  202.103.224.68:64308 --> 202.1.100.5:2048[172.16.
1.2:2048]
 icmp  VPN: public --> public  202.103.224.68:1077 --> 202.1.100.5:2048[172.16.1
.2:2048]
 icmp  VPN: public --> public  192.168.10.2:65332[202.1.100.4:9527] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:63796[202.1.100.4:9521] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  202.103.224.68:63284 --> 202.1.100.5:2048[172.16.
1.2:2048]
 icmp  VPN: public --> public  202.103.224.68:62516 --> 202.1.100.5:2048[172.16.
1.2:2048]
 icmp  VPN: public --> public  192.168.10.2:64308[202.1.100.4:9523] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  202.103.224.68:64820 --> 202.1.100.5:2048[172.16.
1.2:2048]
 icmp  VPN: public --> public  192.168.10.2:63284[202.1.100.4:9519] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  192.168.10.2:64564[202.1.100.4:9524] --> 202.103.
224.68:2048
 icmp  VPN: public --> public  202.103.224.68:63028 --> 202.1.100.5:2048[172.16.
1.2:2048]
 icmp  VPN: public --> public  192.168.10.2:1077[202.1.100.4:9532] --> 202.103.2
24.68:2048
 icmp  VPN: public --> public  202.103.224.68:63796 --> 202.1.100.5:2048[172.16.
1.2:2048]
 icmp  VPN: public --> public  192.168.10.2:309[202.1.100.4:9529] --> 202.103.22
4.68:2048
 icmp  VPN: public --> public  202.103.224.68:64052 --> 202.1.100.5:2048[172.16.
1.2:2048]
```

至此，华为防火墙NAT Server典型组网配置案例已完成！