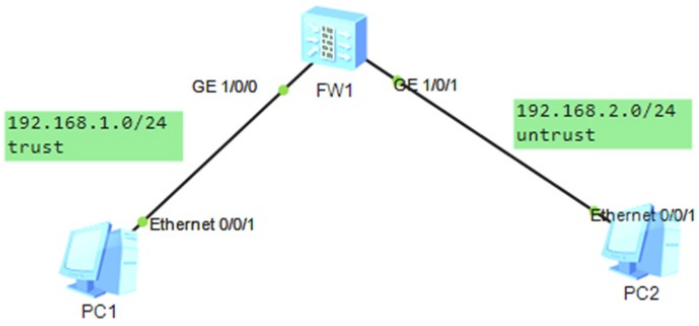
【MVS】华为防火墙不同安全域互通的典型组网配置案例2-安全策略

网络相关 韦家宁 2024-09-12 发表

组网及说明



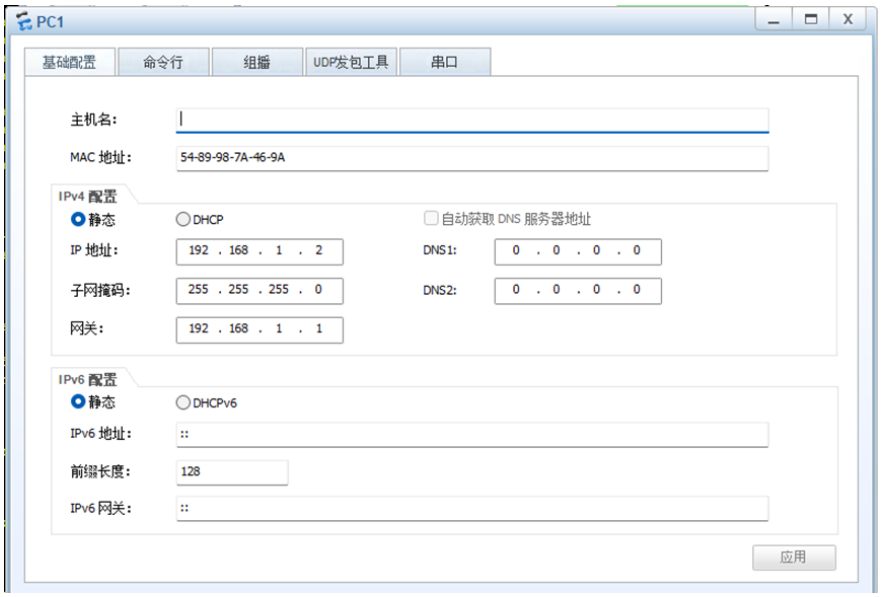
组网说明:
本案例采用ENSP模拟器来部署华为防火墙不同安全域互通的基础典型配置，在网络拓扑图中，已经标识了具体的IP和所属的安全域，需要在防火墙内配置安全策略实现不同安全域的互通。

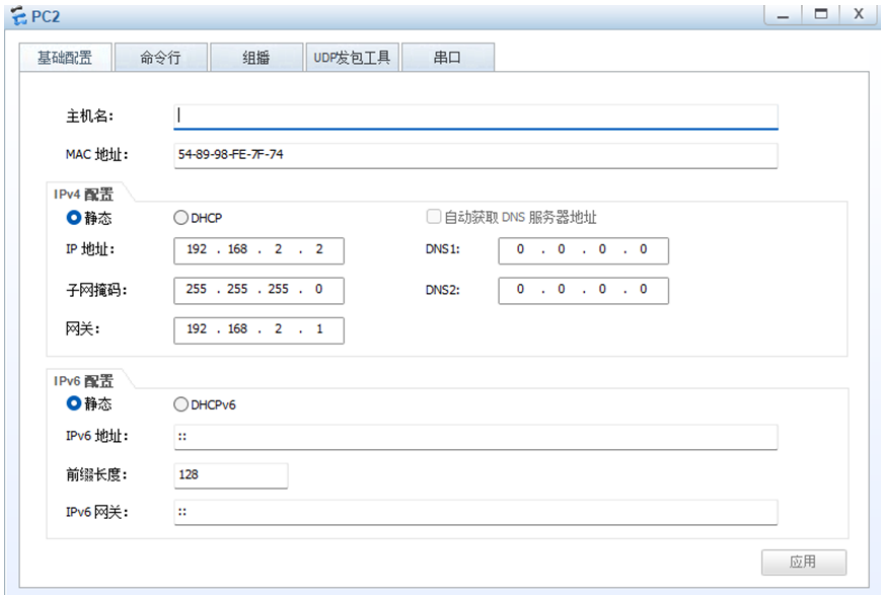
配置思路:
1、按照网络拓扑图配置IP地址。
2、将接口加入安全域并放通安全策略。
3、PC分别填写IP地址，并进行PING测试。

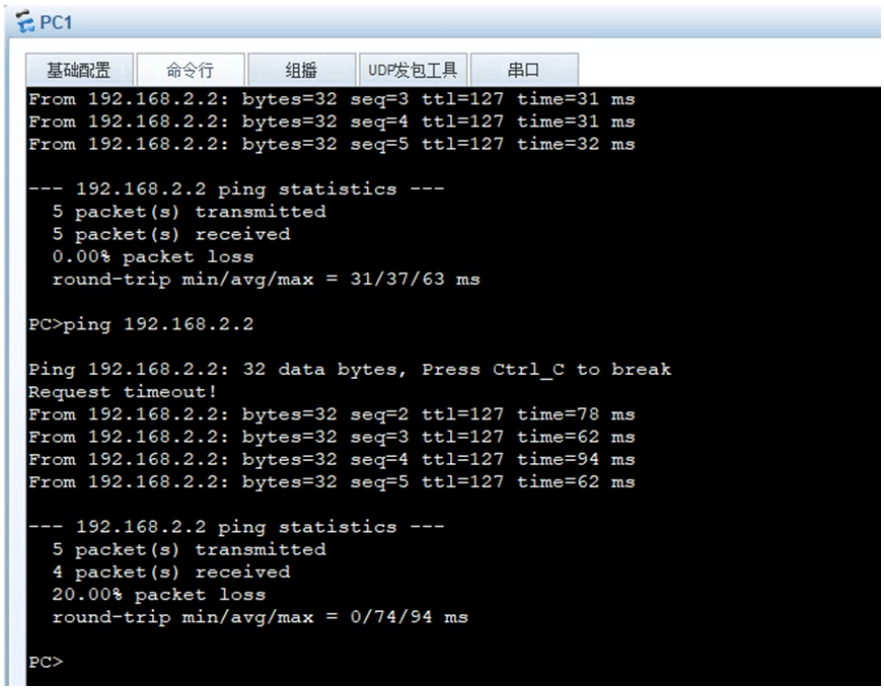
配置步骤

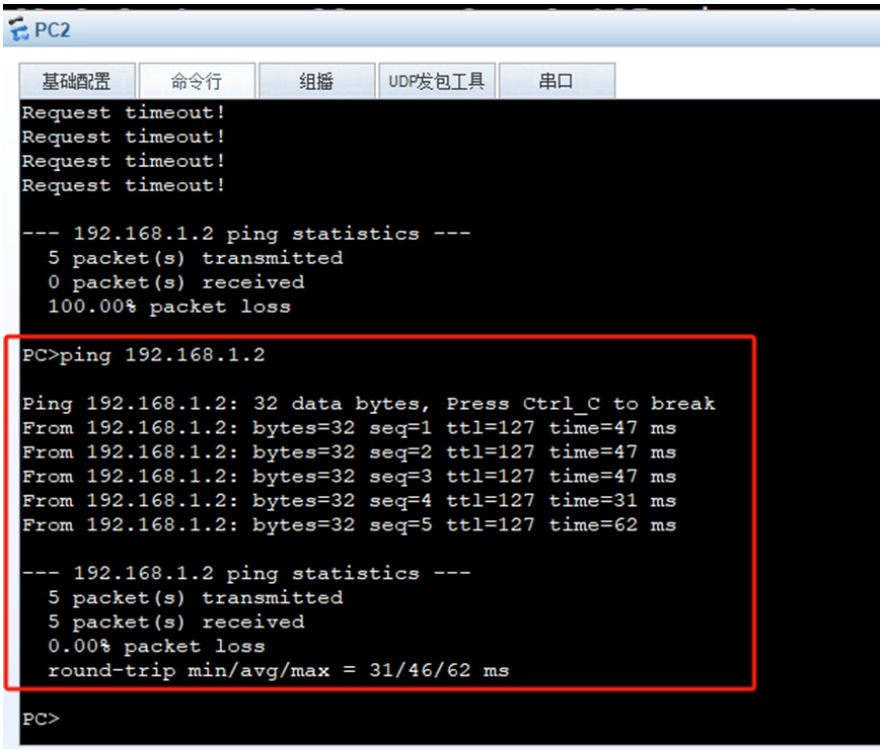
```
[USG6000V1]int gi 1/0/0
[USG6000V1-GigabitEthernet1/0/0]ip address 192.168.1.1 24
[USG6000V1-GigabitEthernet1/0/0]quit

[USG6000V1]int gi 1/0/1
[USG6000V1-GigabitEthernet1/0/1]ip address 192.168.2.1 24
[USG6000V1-GigabitEthernet1/0/1]quit

[USG6000V1]firewall zone trust
[USG6000V1-zone-trust]add int gi 1/0/0
[USG6000V1-zone-trust]quit

[USG6000V1]fire zone untrust
[USG6000V1-zone-untrust]add int gi 1/0/1
[USG6000V1-zone-untrust]quit

[USG6000V1]security-policy
[USG6000V1-policy-security]rule name 1
[USG6000V1-policy-security-rule-1]source-zone trust
[USG6000V1-policy-security-rule-1]destination-zone untrust
[USG6000V1-policy-security-rule-1]action permit
[USG6000V1-policy-security-rule-1]quit

[USG6000V1-policy-security]rule name 2
[USG6000V1-policy-security-rule-2]source-zone untrust
[USG6000V1-policy-security-rule-2]destination-zone trust
[USG6000V1-policy-security-rule-2]action permit
[USG6000V1-policy-security-rule-2]quit
[USG6000V1-policy-security]quit
```

PC分别填写IP地址，且能相互PING通。









查看安全策略的显示信息，已开启。

```
[USG6000V1]dis security-policy rule all
2024-09-12 08:17:49.920
Total:3
RULE ID  RULE NAME                       STATE      ACTION       HITS
------------------------------------------------------------------------------
1        1                               enable     permit       5
2        2                               enable     permit       5
0        default                         enable     deny         0
------------------------------------------------------------------------------
[USG6000V1]
```

查看防火墙的会话，能看到两台主机相互PING通的会话记录。

```
[USG6000V1]dis  firewall session table
2024-09-12 08:19:07.550
 Current Total Sessions : 19
 icmp  VPN: public --> public  192.168.1.2:59811 --> 192.168.2.2:2048
 icmp  VPN: public --> public  192.168.1.2:61347 --> 192.168.2.2:2048
 icmp  VPN: public --> public  192.168.1.2:62883 --> 192.168.2.2:2048
 icmp  VPN: public --> public  192.168.1.2:59299 --> 192.168.2.2:2048
 icmp  VPN: public --> public  192.168.1.2:61091 --> 192.168.2.2:2048
 icmp  VPN: public --> public  192.168.1.2:59555 --> 192.168.2.2:2048
 icmp  VPN: public --> public  192.168.1.2:61603 --> 192.168.2.2:2048
 icmp  VPN: public --> public  192.168.1.2:60323 --> 192.168.2.2:2048
 icmp  VPN: public --> public  192.168.1.2:62115 --> 192.168.2.2:2048
 icmp  VPN: public --> public  192.168.1.2:62371 --> 192.168.2.2:2048
 icmp  VPN: public --> public  192.168.1.2:63139 --> 192.168.2.2:2048
 icmp  VPN: public --> public  192.168.1.2:59043 --> 192.168.2.2:2048
 icmp  VPN: public --> public  192.168.1.2:61859 --> 192.168.2.2:2048
 icmp  VPN: public --> public  192.168.1.2:62627 --> 192.168.2.2:2048
 icmp  VPN: public --> public  192.168.1.2:58787 --> 192.168.2.2:2048
 icmp  VPN: public --> public  192.168.1.2:60835 --> 192.168.2.2:2048
 icmp  VPN: public --> public  192.168.1.2:60579 --> 192.168.2.2:2048
 icmp  VPN: public --> public  192.168.1.2:58531 --> 192.168.2.2:2048
 icmp  VPN: public --> public  192.168.1.2:60067 --> 192.168.2.2:2048
[USG6000V1]
```

至此，华为防火墙不同安全域互通的典型组网配置案例已完成！