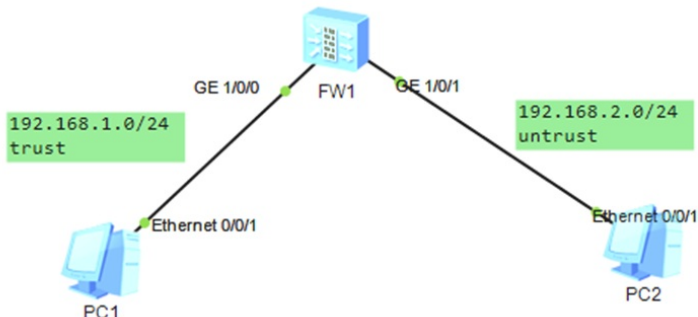


### 组网及说明



#### 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。

PC1

基础配置 命令行 组播 UDP发包工具 串口

主机名:

MAC 地址: 54-89-98-7A-46-9A

IPv4 配置

静态  DHCP  自动获取 DNS 服务器地址

IP 地址: 192.168.1.2 DNS1: 0.0.0.0

子网掩码: 255.255.255.0 DNS2: 0.0.0.0

网关: 192.168.1.1

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-FE-7F-74

IPv4 配置

静态  DHCP  自动获取 DNS 服务器地址

IP 地址: 192.168.2.2 DNS1: 0.0.0.0

子网掩码: 255.255.255.0 DNS2: 0.0.0.0

网关: 192.168.2.1

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

```
From 192.168.2.2: bytes=32 seq=3 ttl=127 time=31 ms
From 192.168.2.2: bytes=32 seq=4 ttl=127 time=31 ms
From 192.168.2.2: bytes=32 seq=5 ttl=127 time=32 ms

--- 192.168.2.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/37/63 ms

PC>ping 192.168.2.2

Ping 192.168.2.2: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 192.168.2.2: bytes=32 seq=2 ttl=127 time=78 ms
From 192.168.2.2: bytes=32 seq=3 ttl=127 time=62 ms
From 192.168.2.2: bytes=32 seq=4 ttl=127 time=94 ms
From 192.168.2.2: bytes=32 seq=5 ttl=127 time=62 ms

--- 192.168.2.2 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
 20.00% packet loss
 round-trip min/avg/max = 0/74/94 ms

PC>
```

```
PC2
基础配置 命令行 组播 UDP发包工具 串口
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 192.168.1.2 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
100.00% packet loss

PC>ping 192.168.1.2

Ping 192.168.1.2: 32 data bytes, Press Ctrl_C to break
From 192.168.1.2: bytes=32 seq=1 ttl=127 time=47 ms
From 192.168.1.2: bytes=32 seq=2 ttl=127 time=47 ms
From 192.168.1.2: bytes=32 seq=3 ttl=127 time=47 ms
From 192.168.1.2: bytes=32 seq=4 ttl=127 time=31 ms
From 192.168.1.2: bytes=32 seq=5 ttl=127 time=62 ms

--- 192.168.1.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/46/62 ms

PC>
```

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！