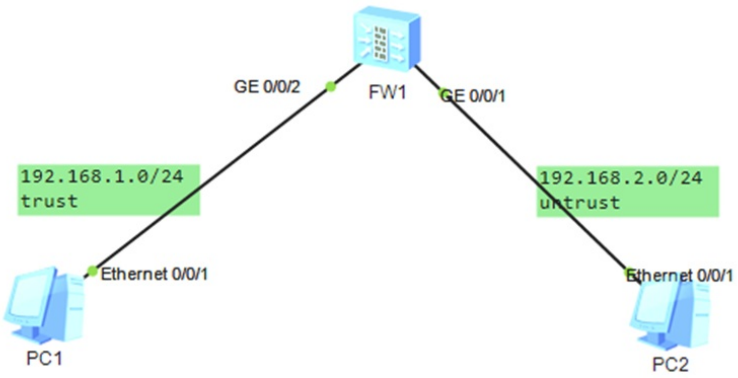
【MVS】华为防火墙不同安全域互通的典型组网配置案例

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域间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域间策略。
3、PC分别填写IP地址，并进行PING测试。

配置步骤

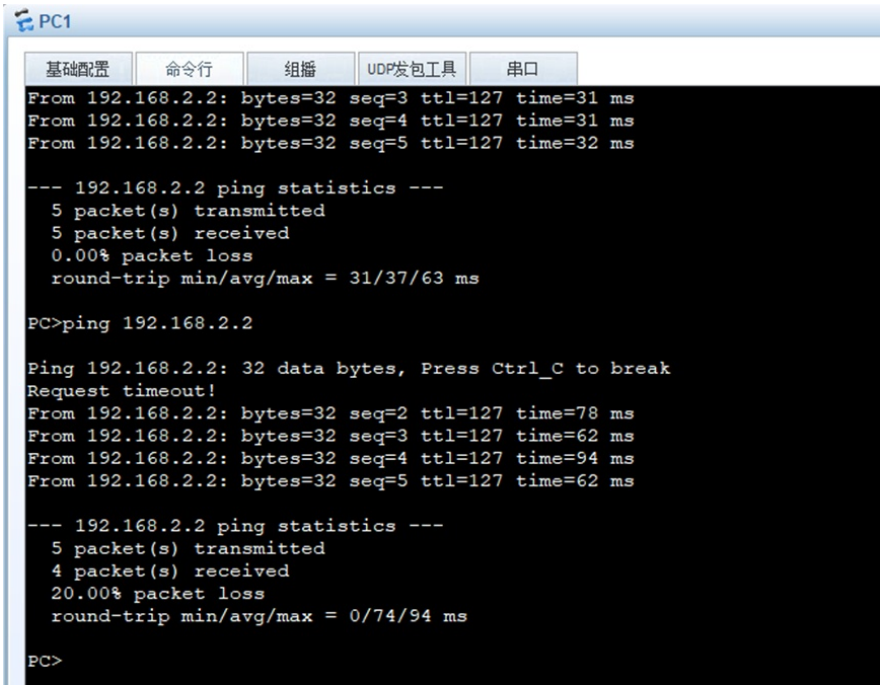
```
<SRG>system
[SRG]sysname FW1
[FW1]int gi 0/0/2
[FW1-GigabitEthernet0/0/2]ip address 192.168.1.1 24
[FW1-GigabitEthernet0/0/2]quit
[FW1]int gi 0/0/1
[FW1-GigabitEthernet0/0/1]ip address 192.168.2.1 24
[FW1-GigabitEthernet0/0/1]quit

[FW1]firewall zone trust
[FW1-zone-trust]add interface GigabitEthernet 0/0/2
[FW1-zone-trust]quit

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

[FW1]firewall packet-filter default permit all
14:56:52  2024/09/12
Warning:Setting the default packet filtering to permit poses security risks. You
 are advised to configure the security policy based on the actual data flows. Ar
e you sure you want to continue?[Y/N]y

[FW1]policy interzone trust untrust outbound
[FW1-policy-interzone-trust-untrust-outbound]policy 1
[FW1-policy-interzone-trust-untrust-outbound-1]action permit
[FW1-policy-interzone-trust-untrust-outbound-1]policy source any
[FW1-policy-interzone-trust-untrust-outbound-1]quit
[FW1-policy-interzone-trust-untrust-outbound]quit
```

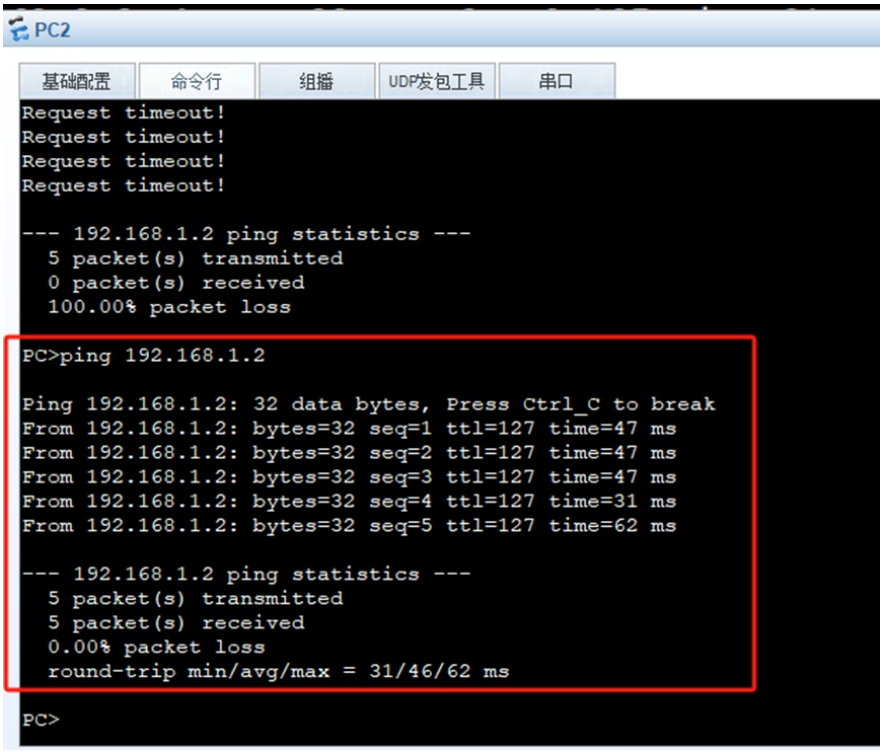
[FW1]policy interzone untrust trust outbound
[FW1-policy-interzone-trust-untrust-outbound]policy 1
[FW1-policy-interzone-trust-untrust-outbound-1]action permit
[FW1-policy-interzone-trust-untrust-outbound-1]policy source any
[FW1-policy-interzone-trust-untrust-outbound-1]quit
[FW1-policy-interzone-trust-untrust-outbound]quit

[FW1]policy interzone trust untrust inbound
[FW1-policy-interzone-trust-untrust-inbound]policy 1
[FW1-policy-interzone-trust-untrust-inbound-1]action permit
[FW1-policy-interzone-trust-untrust-inbound-1]policy source any
[FW1-policy-interzone-trust-untrust-inbound-1]quit
[FW1-policy-interzone-trust-untrust-inbound]quit

[FW1]policy interzone untrust trust inbound
[FW1-policy-interzone-trust-untrust-inbound]policy 1
[FW1-policy-interzone-trust-untrust-inbound-1]action permit
[FW1-policy-interzone-trust-untrust-inbound-1]policy source any
[FW1-policy-interzone-trust-untrust-inbound-1]quit
[FW1-policy-interzone-trust-untrust-inbound]quit

PC分别填写IP地址，且能相互PING通。





分别查看域间策略匹配的情况，能匹配上。

```
[FW1]dis policy interzone trust untrust outbound
15:11:12  2024/09/12
policy interzone trust untrust outbound
 firewall default packet-filter is permit
 policy 1 (10 times matched)
  action permit
  policy service service-set ip
  policy source any
  policy destination any

[FW1]display policy interzone trust untrust in
[FW1]display policy interzone trust untrust inbound
15:11:19  2024/09/12
policy interzone trust untrust inbound
 firewall default packet-filter is permit
 policy 1 (10 times matched)
  action permit
  policy service service-set ip
  policy source any
  policy destination any

[FW1]display policy interzone untrust trust in
15:11:30  2024/09/12
policy interzone trust untrust inbound
 firewall default packet-filter is permit
 policy 1 (10 times matched)
  action permit
  policy service service-set ip
  policy source any
  policy destination any

[FW1]display policy interzone untrust trust out
15:11:37  2024/09/12
policy interzone trust untrust outbound
 firewall default packet-filter is permit
 policy 1 (10 times matched)
  action permit
  policy service service-set ip
  policy source any
  policy destination any

[FW1]
```

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！