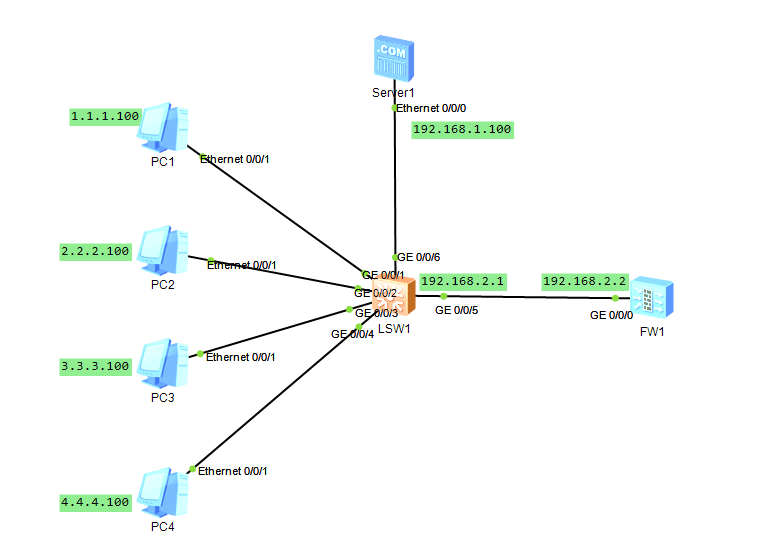
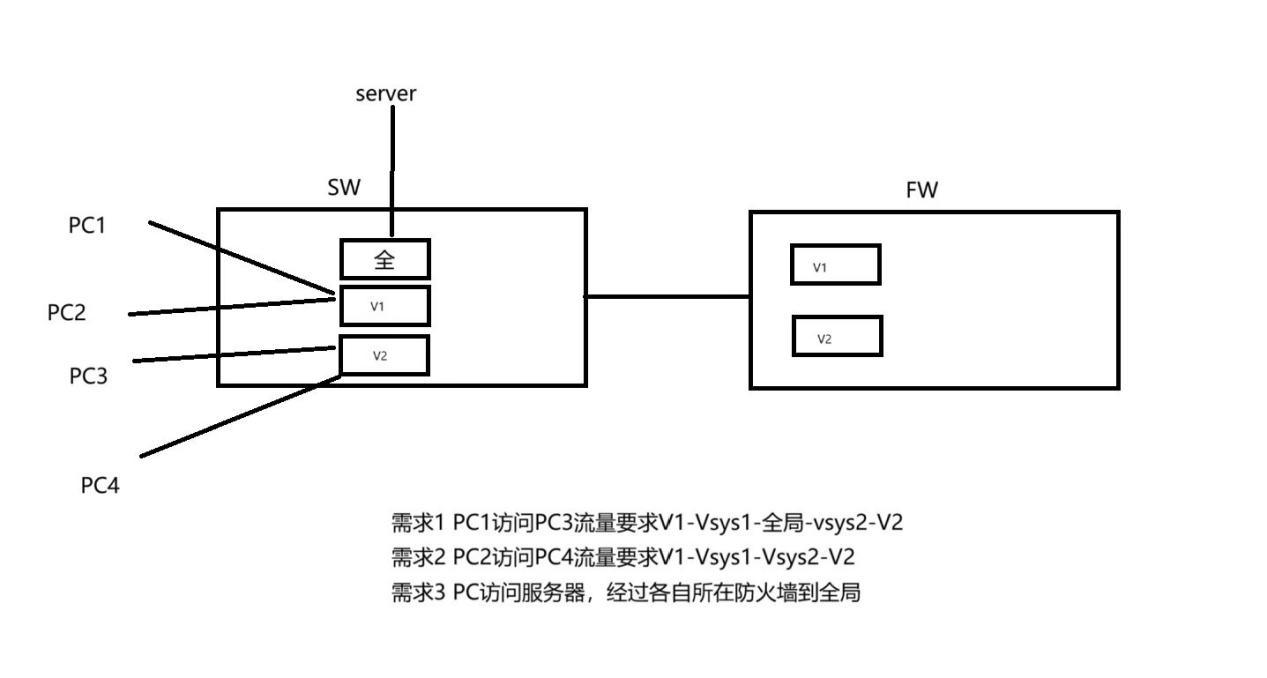
# 防火墙虚拟墙旁挂实验

## 1实验设想

公司有四个部门，在sw1上分配两个vrf，将pc1和pc2的部门加入v1中，pc3和pc4加入v2中，分别进行互访需求，要求经过旁挂防火墙增加业务部门的安全性，同时避免公司内部人员攻击服务器。

## 2.拓扑设计



## 3.配置脚本

**基础配置：**

在SW1上创建两个vrf实例分别为V1和V2，防火墙上创建两个虚拟墙Vsys1和Vsys2

**sysname SW1**

**#**

**vlan batch 10 20 30 40 50 60**

**#**

**ip vpn-instance v1 //创建实例v1**

**ipv4-family**

**route-distinguisher 1:1**

**#**

**ip vpn-instance v2 //创建实例v2**

**ipv4-family**

**route-distinguisher 2:2**

**#**

**interface Vlanif10**

**ip binding vpn-instance v1 //将vlan10划分到实例v1中**

**ip address 1.1.1.1 255.255.255.0**

**#**

**interface Vlanif20**

**ip binding vpn-instance v1 //将vlan20划分到实例v1中**

**ip address 2.2.2.2 255.255.255.0**

**#**

**interface Vlanif30**

**ip binding vpn-instance v2** **//将vlan30划分到实例v2中**

**ip address 3.3.3.3 255.255.255.0**

**#**

**interface Vlanif40**

**ip binding vpn-instance v2 //将vlan40划分到实例v2中**

**ip address 4.4.4.4 255.255.255.0**

**#**

**interface Vlanif50 //sw1全局与fw1的vsys1互联网段**

**ip address 192.168.1.1 255.255.255.0**

**#**

**interface Vlanif60** **//sw1全局与fw1的vsys2互联网段**

**ip address 192.168.2.1 255.255.255.0**

**#**

**interface GigabitEthernet0/0/1**

**port link-type access**

**port default vlan 10**

**#**

**interface GigabitEthernet0/0/2**

**port link-type access**

**port default vlan 20**

**#**

**interface GigabitEthernet0/0/3**

**port link-type access**

**port default vlan 30**

**#**

**interface GigabitEthernet0/0/4**

**port link-type access**

**port default vlan 40**

**#**

**interface GigabitEthernet0/0/5**

**port link-type trunk**

**port trunk allow-pass vlan 10 20 30 40 50 60**

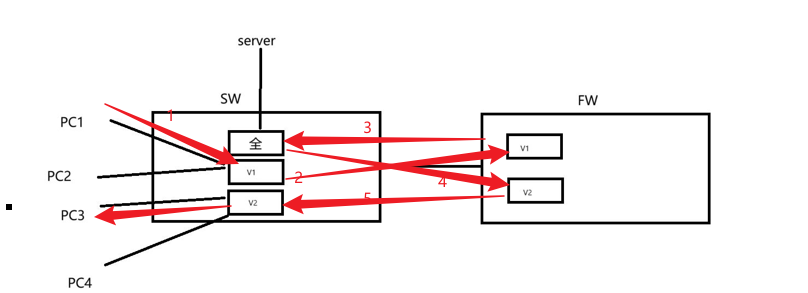
**#**

**interface GigabitEthernet0/0/6**

**port link-type access**

**port default vlan 50 //server 网段**

**#**



**防火墙配置**

**Sys FW**

**vlan batch 10 20 30 40 50 60**

**vsys enable //开启vsys虚拟墙功能**

**#**

**vsys name vsys1 1 //创建虚拟墙vsys1，并将vlan10 20 50划分到vsys1**

**assign vlan 10**

**assign vlan 20**

**assign vlan 50**

**#**

**vsys name vsys2 2 //创建虚拟墙vsys2，并将vlan30 40 60划分到vsys1**

**assign vlan 30**

**assign vlan 40**

**assign vlan 60**

**#**

**interface GigabitEthernet1/0/0**

**portswitch**

**undo shutdown**

**port link-type trunk**

**port trunk allow-pass vlan 10 20 30 40 50 60**

**#**

**interface Virtual-if0 //全局虚拟接口**

**ip address 172.16.0.3 255.255.255.0**

**#**

**firewall zone trust //将全局的虚拟接口划分到trust区域**

**add interface Virtual-if0**

**#**

**switch vsys vsys1**

**interface Vlanif10**

**ip binding vpn-instance vsys1**

**ip address 1.1.1.253 255.255.255.0**

**service-manage ping permit**

**#**

**interface Vlanif20**

**ip binding vpn-instance vsys1**

**ip address 2.2.2.253 255.255.255.0**

**service-manage ping permit**

**#**

**interface Vlanif50**

**ip binding vpn-instance vsys1**

**ip address 192.168.1.253 255.255.255.0**

**service-manage ping permit**

**#**

**interface Virtual-if1 //vsys1虚拟接口**

**ip address 172.16.0.1 255.255.255.0**

**#**

**firewall zone trust**

**set priority 85**

**add interface Vlanif50**

**#**

**firewall zone untrust**

**set priority 5**

**add interface Virtual-if1**

**add interface Vlanif10**

**add interface Vlanif20**

**#**

**#**

**security-policy**

**rule name ttu**

**source-zone trust**

**destination-zone untrust**

**source-address 192.168.1.0 mask 255.255.255.0**

**service icmp**

**action permit**

**rule name utt**

**source-zone untrust**

**destination-zone trust**

**source-address 1.1.1.0 mask 255.255.255.0**

**source-address 2.2.2.0 mask 255.255.255.0**

**destination-address 192.168.1.0 mask 255.255.255.0**

**service icmp**

**action permit**

**rule name utu**

**source-zone untrust**

**destination-zone untrust**

**source-address 1.1.1.0 mask 255.255.255.0**

**source-address 2.2.2.0 mask 255.255.255.0**

**destination-address 3.3.3.0 mask 255.255.255.0**

**destination-address 4.4.4.0 mask 255.255.255.0**

**service icmp**

**action permit**

**switch vsys vsys2**

**#**

**interface Vlanif30**

**ip binding vpn-instance vsys2**

**ip address 3.3.3.253 255.255.255.0**

**service-manage ping permit**

**#**

**interface Vlanif40**

**ip binding vpn-instance vsys2**

**ip address 4.4.4.253 255.255.255.0**

**service-manage ping permit**

**#**

**interface Vlanif60**

**ip binding vpn-instance vsys2**

**ip address 192.168.2.253 255.255.255.0**

**service-manage ping permit**

**#**

**interface Virtual-if2 //vsys2虚拟接口**

**ip address 172.16.0.2 255.255.255.0**

**#**

**firewall zone trust**

**set priority 85**

**add interface Vlanif60**

**#**

**firewall zone untrust**

**set priority 5**

**add interface Virtual-if2**

**add interface Vlanif30**

**add interface Vlanif40**

**#**

**security-policy**

**rule name ttu**

**source-zone trust**

**destination-zone untrust**

**source-address 192.168.1.0 mask 255.255.255.0**

**service icmp**

**action permit**

**rule name utt**

**source-zone untrust**

**destination-zone trust**

**source-address 3.3.3.0 mask 255.255.255.0**

**source-address 4.4.4.0 mask 255.255.255.0**

**destination-address 192.168.1.0 mask 255.255.255.0**

**destination-address 192.168.2.0 mask 255.255.255.0**

**service icmp**

**action permit**

**rule name utu**

**source-zone untrust**

**destination-zone untrust**

**source-address 3.3.3.0 mask 255.255.255.0**

**source-address 4.4.4.0 mask 255.255.255.0**

**destination-address 1.1.1.0 mask 255.255.255.0**

**destination-address 2.2.2.0 mask 255.255.255.0**

**service icmp**

**action permit**

**需求一：**

PC1访问PC3流量需求V1-Vsys1-全局-Vsys2-V2

交换机配置：

**ip route-static vpn-instance v1 3.3.3.0 255.255.255.0 192.168.1.253**

**//sw1 去往pc3的路由，下一跳是防火墙的fw vsys1**

**ip route-static vpn-instance v1 192.168.1.0 255.255.255.0 1.1.1.253**

**//sw1 v1去往 fw vsys 1与全局互联的路由，下一跳是防火墙的v1 1.1.1.253**

**ip route-static vpn-instance v2 1.1.1.0 255.255.255.0 192.168.2.253**

**//sw1 v2去往1.1.1.1的路由下一跳是fw vsys2 （反向）**

**ip route-static 3.3.3.0 255.255.255.0 vpn-instance v2 192.168.2.253**

**//sw1全局去往pc3的路由，下一跳为fw vsys2**

**防火墙配置：**

**switch vsys1**

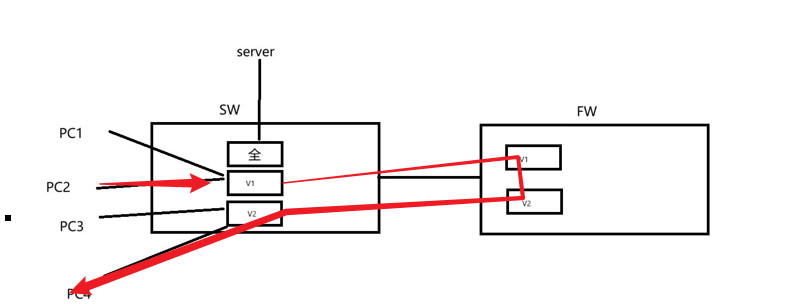
**ip route-static 3.3.3.0 255.255.255.0 192.168.1.1**

**//fw1 vsys1去往pc3网段的路由，下一跳是sw1 全局与fw vsys1互联地址**

**switch vsys2**

**ip route-static 1.1.1.0 255.255.255.0 192.168.2.1**

**//fw1 vsys去往pc1网段的路由，下一跳是sw1全局与fw vsys2互联地址（反向）**



**需求二：**

PC2访问PC4流量要求V1-Vsys1-Vsys2-V2

**ip route-static vpn-instance v1 4.4.4.0 255.255.255.0 2.2.2.253**

**//SW1 v1 去往pc4 4.4.4.100网段的路由，下一跳是FW2 vsys1**

**ip route-static vpn-instance vsys1 4.4.4.0 255.255.255.0 vpn-instance vsys2**

**//FW1 vsys1去往vsys2的路由**

**ip route-static vpn-instance vsys2 2.2.2.0 255.255.255.0 vpn-instance vsys1**

**//FW1 vsys2去往vsys1的路由**

**ip route-static vpn-instance v2 2.2.2.0 255.255.255.0 4.4.4.253**

**//SW1 v2 去往pc2 2.2.2.100网段的路由，下一跳是FW2 vsys2**

**需求三：**

pc访问服务器，经过各自所在防火墙到全局

**ip route-static 1.1.1.0 255.255.255.0 vpn-instance v1 192.168.1.253**

**//SW1 全局去往pc1的路由**

**ip route-static 2.2.2.0 255.255.255.0 vpn-instance v1 192.168.1.253**

**//SW1 全局去往pc2的路由**

**ip route-static 3.3.3.0 255.255.255.0 vpn-instance v2 192.168.2.253**

**//SW1 全局去往pc3的路由**

**ip route-static 4.4.4.0 255.255.255.0 vpn-instance v2 192.168.2.253**

**//SW1 全局去往pc4的路由**

**ip route-static vpn-instance v2 192.168.2.0 255.255.255.0 3.3.3.253**

**//SW1 v2去往全局的路由，下一跳是fw vsys2**

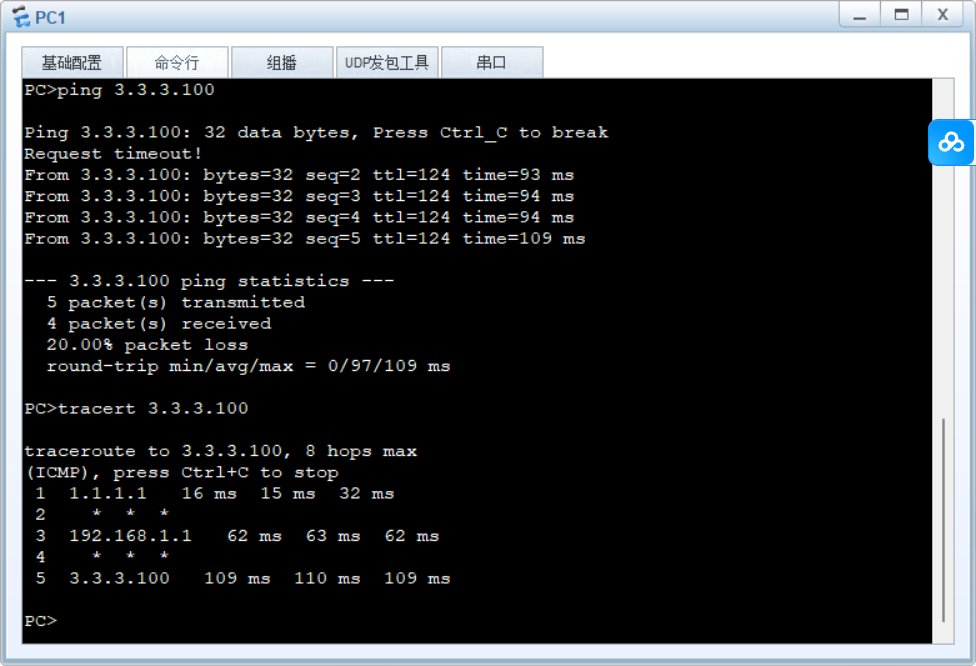
**防火墙配置：**

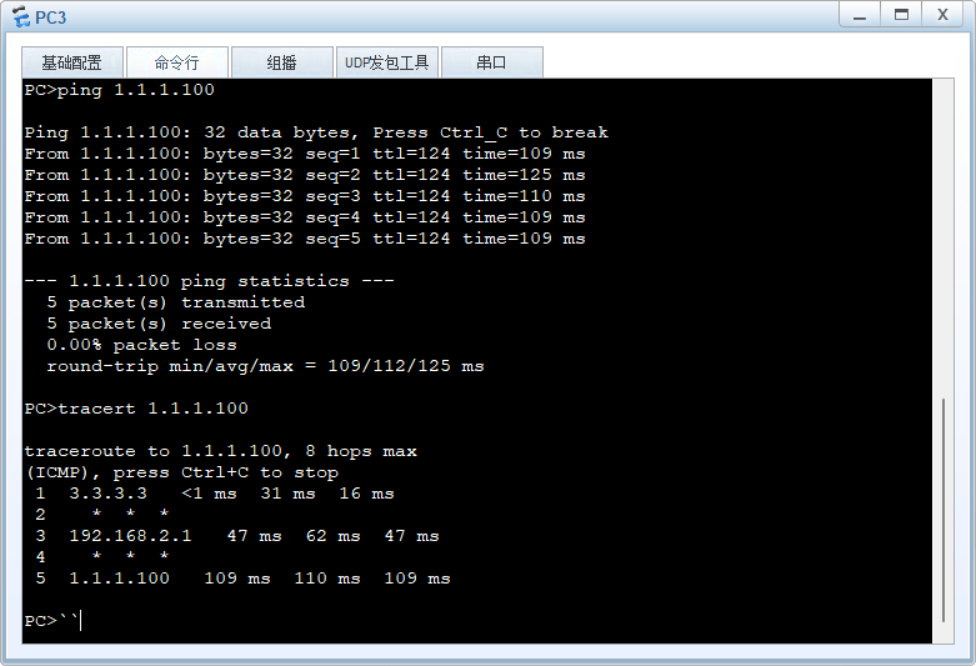
**ip route-static 192.168.1.0 255.255.255.0 192.168.2.1**

**//fw vsys2去往服务器网段的路由，下一跳为sw1全局与fw2 vsys2互联网段**

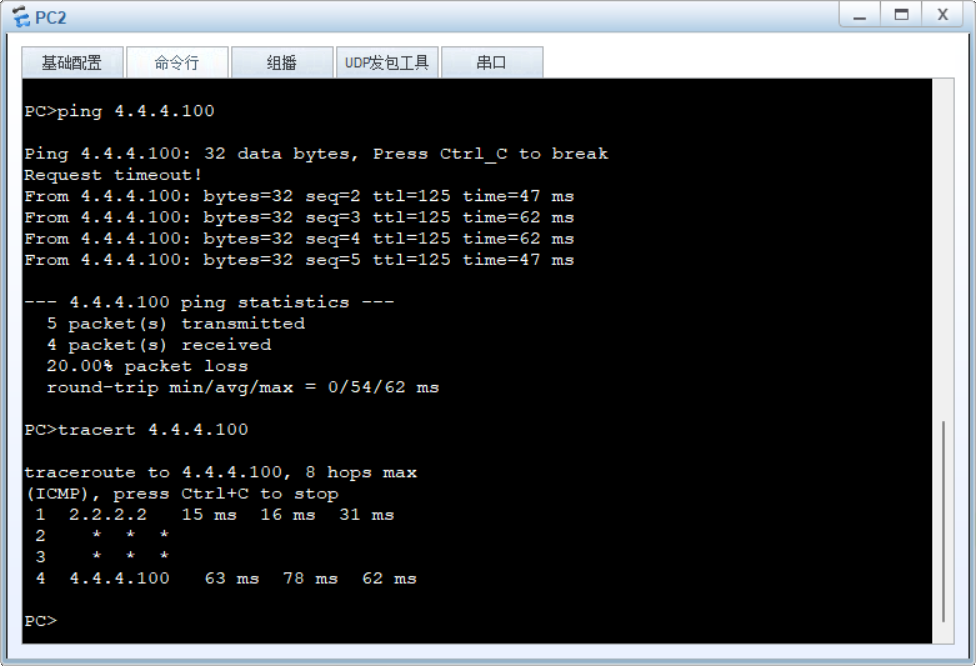
## 4.总结

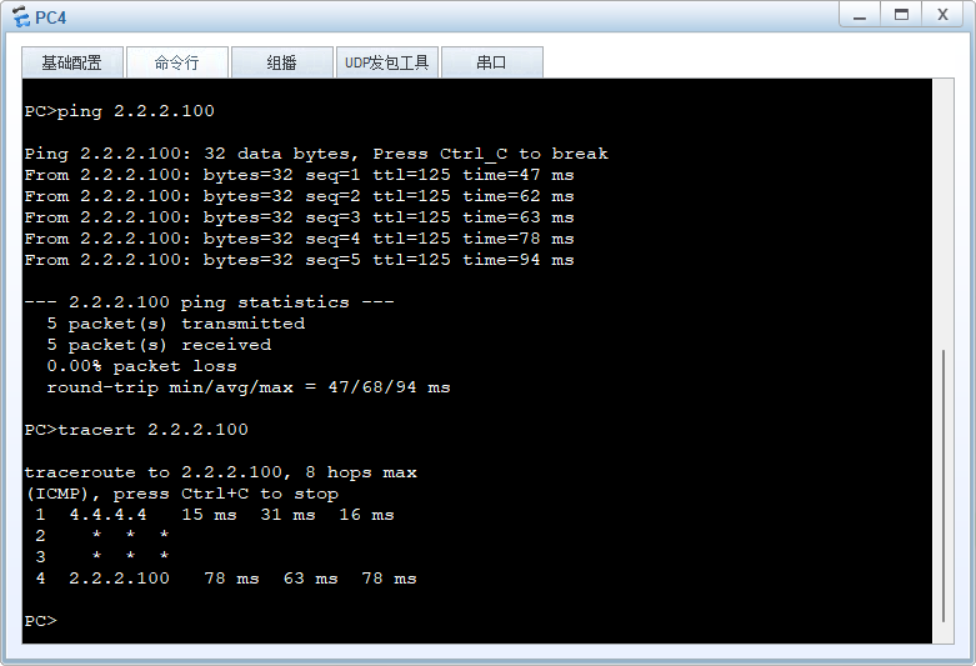
测试pc1与pc3互通以及路径



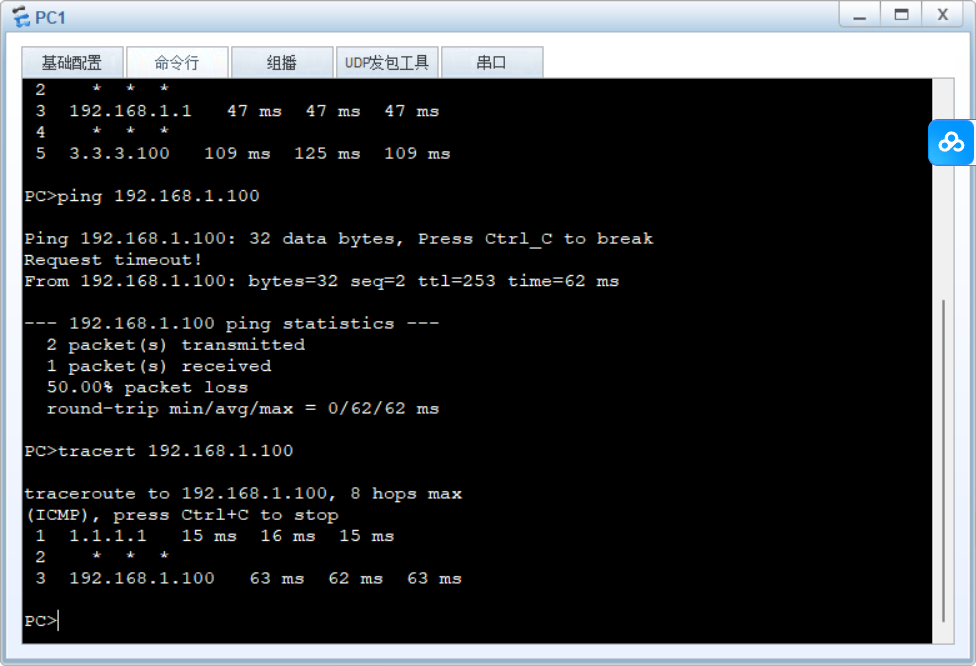


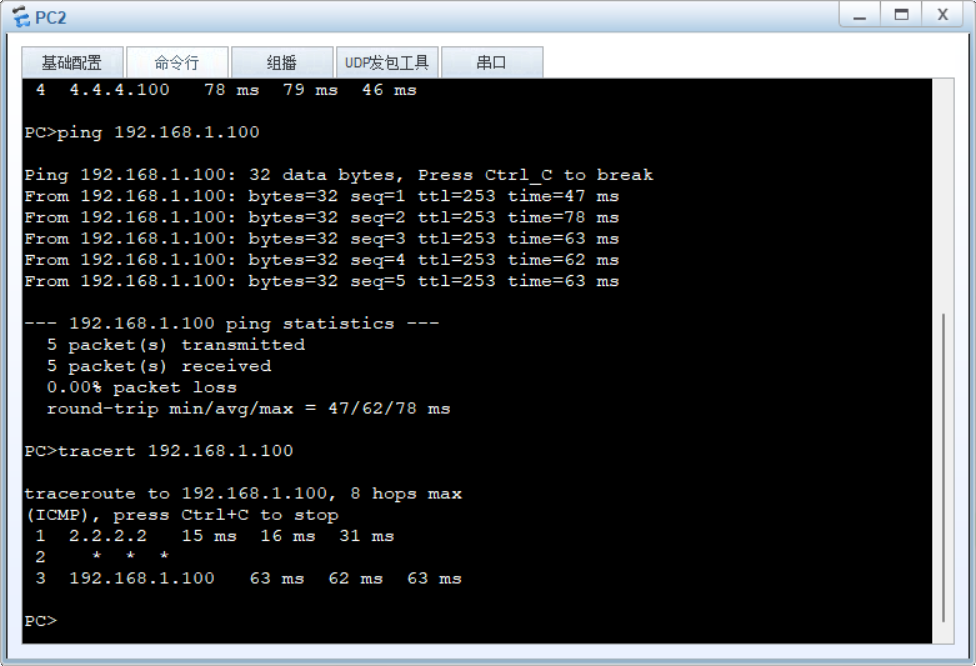
测试pc2与pc4互通以及路径

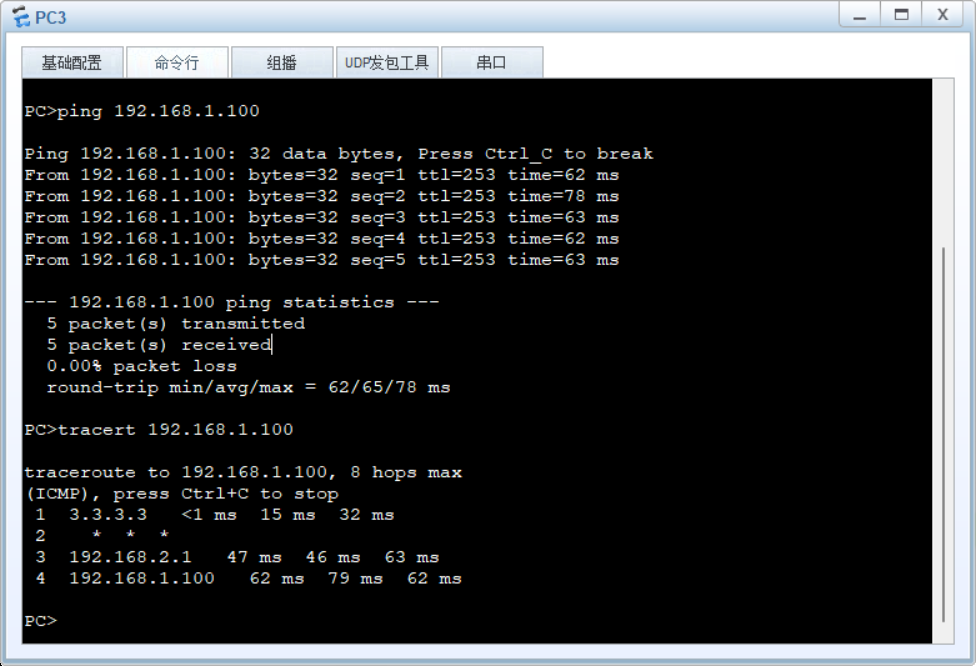


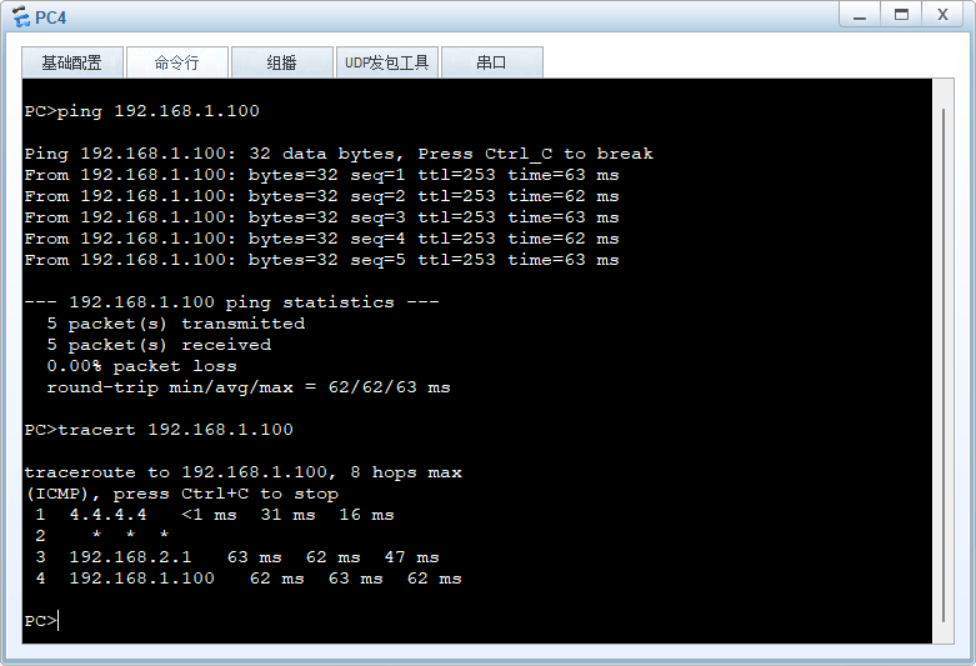


测试pc1，pc2，pc3，pc4与服务器互通以及路径









1. tracert在测试路由所经过的路径时，如果经过防火墙则不会显示路径
2. 防火墙记得加安全策略五元组，经常忘了配置服务的安全策略。一开始做的时候可以用any to any放通全部，等确保路由能够通信后再做安全策略
3. 每个需要用到的接口都要划分zone，包括Virtual-if
4. 需要测试ping的接口记得service-manage ping permit，防火墙主要先确保区域，策略，接口划分再去做路由，后面出错了就比较好排错。