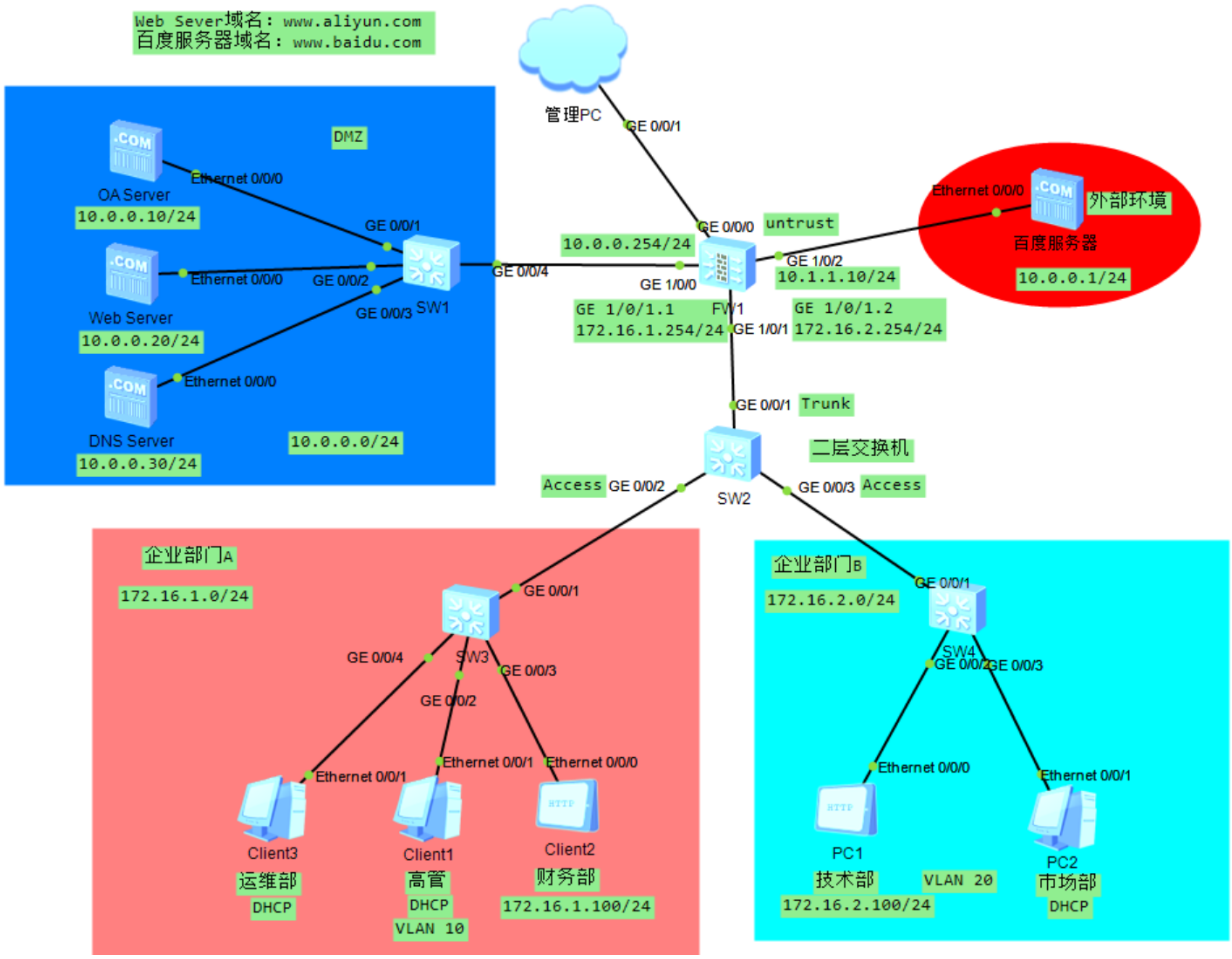
防火墙第二次综合练习

实验拓扑：



需求：

在FW上启动DHCP功能，并配置不同的全局地址池，为接入网络的终端设备分配IP地址。
Client1、Client3和PC2通过DHCP获取地址信息。Client2和PC1手工静态配置。
Client1必须通过DHCP获取172.16.1.90/24地址。

地址池名称	网段/掩码	网关	DNS
dhcp-a	172.16.1.0/24	172.16.1.254	10.0.0.30
dhcp-b	172.16.2.0/24	172.16.2.254	10.0.0.30

设备	接口	安全区域	优先级
FW	GE1/0/1	Trust_A	70
	GE1/0/1.2	Trust_B	80
	GE1/0/0	DMZ	默认
	GE1/0/2	Untrust	默认

设备	地址	地址族	描述信息
OA Server	10.0.0.10/32	DMZ_Server	DMZ区域的OA服务器
Web Server	10.0.0.20/32	DMZ_Server	DMZ区域的Web服务器

设备	地址	地址族	描述信息
DNS Server	10.0.0.30/32	DMZ_Server	DMZ区域的DNS服务器
Client1(高管)	172.16.1.90/32	Trust_A_address	高管
Client2(财务部)	172.16.1.100/32	Trust_A_address	财务部
Client3(运维部)	172.16.1.0/24 需要去除172.16.1.90和172.16.1.100。	Trust_A_address	运维部
PC1(技术部)	172.16.2.100/32	Trust_B_address	技术部
PC2(市场部)	172.16.2.0/24 需要去除172.16.2.100。	Trust_B_address	市场部
管理员	172.16.1.10/32	Trust_A_address	

为FW配置一个配置管理员。要求管理员可以通过Telnet登录到CLI界面对FW进行管理和维护。FW对管理员进行本地认证。

项目	数据	说明
管理员账号密码	账号：vtyadmin 密码：admin@123	
管理员PC的IP地址	172.16.1.10/24	
角色	service-admin	拥有业务配置和设备监控权限。
管理员信任主机	172.16.1.0/24	登录设备的主机IP地址范围
认证类型	本地认证	

管理员角色信息

名称	权限控制项
service-admin	策略、对象、网络：读写操作
	面板、监控、系统：无

1、部门A分为运维部、高层管理、财务部；其中，财务部IP地址为静态IP。高管地址DHCP固定分配。
2、部门B分为研发部和市场部；研发部IP地址为静态IP
3、新建一个认证域，所有用户属于认证域下组织架构
4、根据下表信息，创建企业组织架构
5、用户密码统一为admin@123
6、首次登录必须修改密码

项目	数据
认证域	名称：openlab 认证方案：Portal 接入控制：上网行为管理 新用户认证选项：使用/openlab组权限
用户组信息	
部门A	用户组组名：A 用户组所属组：/openlab
部门B	用户组组名：B 用户组所属组：/openlab
高级管理者	用户组组名：manager 用户组所属组：/openlab/A
运维部	用户组组名：DevOps 用户组所属组：/openlab/A
财务部	用户组组名：FD 用户组所属组：/openlab/A
技术部	用户组组名：TD 用户组所属组：/openlab/B

市场部	用户组组名：MD 用户组所属组：/openlab/B
用户信息	
高管用户	用户登录名：user_001 用户显示名：Super_user 用户所属组：/openlab/A/manager 不允许多人同时使用该账号登录 IP/MAC绑定方式：双向绑定 IP/MAC地址：Client1的MAC

项目	**数据**
运维部用户	用户登录名：DevOps_001 用户显示名：张三 用户所属组：/openlab/A/DevOps 不允许多人同时使用该账号登录
财务部用户	用户登录名：FD_001 用户显示名：李四 用户所属组：/openlab/A/FD IP/MAC绑定方式：双向绑定 IP/MAC地址：172.16.1.100 不允许多人同时使用该账号登录

技术部用户	用户登录名：TD_001...TD_003 用户所属组：/openlab/B/TD 允许多人同时使用该账号登录
市场部用户	用户登录名：MD_001...MD_005 用户所属组：/openlab/B/MD 不允许多人同时使用该账号登录 账号过期时间：10天

1、高级管理者访问任何区域时，需要使用免认证。
2、运维部访问DMZ区域时，需要进行Portal认证。
3、技术部和市场部访问DMZ区域时，需要使用匿名认证。
4、财务部访问DMZ区域时，使用不认证。
5、运维部和市场部访问外网时，使用Portal认证。
6、财务部和技术部不能访问外网环境。故不需要认证策略

项目	数据
高级管理者认证策略	名称：policy_auth_01 描述：高级管理者认证策略 源安全区域：Trust_A 目的安全区域：any 源地址/地区:Client1 目的地址/地区：any 认证动作：免认证
运维部认证策略	名称：policy_auth_02 描述：运维部_to_DMZ 源安全区域：Trust_A 目的安全区域：dmz 源地址/地区:Client3 目的地址/地区：DMZ_Server 认证动作：Portal认证

项目	数据
	名称：policy_auth_03 描述：运维部_to_Untrust 源安全区域：Trust_A 目的安全区域：untrust 源地址/地区:Client3 目的地址/地区：any 认证动作：Portal认证
技术部认证策略	名称：policy_auth_04 描述：技术部_to_DMZ 源安全区域：Trust_B 目的安全区域：dmz 源地址/地区:PC1 目的地址/地区：DMZ_Server 认证动作：匿名认证
财务部认证策略	名称：policy_auth_05 描述：财务部_to_DMZ 源安全区域：Trust_A 目的安全区域：dmz 源地址/地区:Client2 目的地址/地区：DMZ_Server 认证动作：不认证
市场部认证策略	名称：policy_auth_06 描述：市场部_to_DMZ 源安全区域：Trust_B 目的安全区域：dmz 源地址/地区:PC2 目的地址/地区：DMZ_Server 认证动作：匿名认证
	名称：policy_auth_07 描述：市场部_to_Untrust 源安全区域：Trust_B 目的安全区域：untrust 源地址/地区:PC2 目的地址/地区：any 认证动作：Portal认证

1、配置Telnet策略
2、配置DHCP策略

3、配置DNS策略
4、部门A中分为三个部门，运维部、高管、财务。
a.运维部允许随时随地访问DMZ区域，并对设备进行管理；
b.高管和财务部仅允许访问DMZ区域的OA和web服务器，并且只有HTTP和HTTPS权限。
c.运维部允许在非工作时间访问互联网环境
d.高管允许随时访问互联网环境
e.财务部任何时间都不允许访问互联网环境
5、部门B分为两个部门，技术部和市场部
a.技术部允许访问DMZ区域中的web服务器，并进行管理
b.技术部和市场部允许访问DMZ区域中的OA服务器，并且只有HTTP和HTTPS权限。
c.市场部允许访问互联网环境
6、每周末公司服务器需要检修维护，允许运维部访问；即，每周末拒绝除运维部以外的流量访问DMZ区域。
7、部门A和部门B不允许存在直接访问流量，如果需要传输文件信息，则需要通过OA服务器完成。---依靠默认规则拒绝

分析：

一、基础网络配置

完成核心设备接口与 VLAN 规划，包括交换机 SW2 的 Access 接口（GE0/0/2 对应 VLAN 10、GE0/0/3 对应 VLAN 20）和 Trunk 接口（GE0/0/1 承载 VLAN 10/20）；明确防火墙 FW、服务器（OA、Web、DNS）、客户端（Client1-3、PC1-2）的接口 VLAN 与 IP 地址

二、DHCP 地址分配

在 FW 上部署 DHCP 功能，创建两个全局地址池：（172.16.1.0/24，网关 172.16.1.254，DNS 10.0.0.30）和（172.16.2.0/24，网关 172.16.2.254，DNS 10.0.0.30）。区分终端配置方式：Client1（固定获取 172.16.1.90）、Client3、PC2 通过 DHCP 获取地址；Client2、PC1 采用静态 IP 配置。

三、防火墙安全区域划分

按接口功能划分安全区域及优先级：FW 的 GE1/0/1 对应 Trust_A（优先级 70）、GE1/0/1.2 对应 Trust_B（优先级 80）、GE1/0/0 对应 DMZ（默认优先级）、GE1/0/2 对应 Untrust（默认优先级），通过区域隔离实现基础安全边界。

四、地址组定义

归类关键地址为逻辑组，便于策略调用：

- **DMZ_Server 组：包含 OA Server（10.0.0.10/32）、Web Server（10.0.0.20/32）、DNS Server（10.0.0.30/32）；**
- **Trust_A_address 组：涵盖高管（Client1，172.16.1.90/32）、财务部（Client2，172.16.1.100/32）、管理员（172.16.1.10/32）；**
- **Trust_B_address 组：包含技术部（PC1，172.16.2.100/32）、市场部（172.16.2.0/24 剔除 172.16.2.100）。**

五、管理员权限配置

创建本地认证管理员`vtyadmin`（密码 admin@123），允许通过 Telnet 从 172.16.1.0/24 网段登录，角色为`service-admin`，拥有策略、对象、网络的读写权限，限制非信任主机访问。

六、用户认证策略

基于组织架构（认证域`openlab`，含部门 A/B 及下属子部门）配置差异化认证规则：

- **高管（Client1）免认证访问任何区域；**
- **运维部（Client3）访问 DMZ 和外网需 Portal 认证；**
- **技术部（PC1）、市场部（PC2）访问 DMZ 采用匿名认证，市场部访问外网需 Portal 认证；**
- **财务部（Client2）访问 DMZ 不认证，且禁止访问外网。**

七、安全访问控制策略

覆盖基础服务、部门权限与特殊场景：

- **基础策略：允许 Telnet 管理、DHCP 协议、DNS 解析流量；**
- **部门权限：运维部全时段访问 DMZ、非工作时间访问外网；高管 / 财务部有限访问 DMZ（仅 HTTP/HTTPS），高管可随时访问外网；技术部访问 DMZ 的 Web 和 OA，市场部访问 DMZ 的 OA 和外网；**
- **特殊规则：周末仅允许运维部访问 DMZ，拒绝其他流量；禁止部门 A 与 B 直接互访，需通过 OA 服务器中转。**

配置过程：

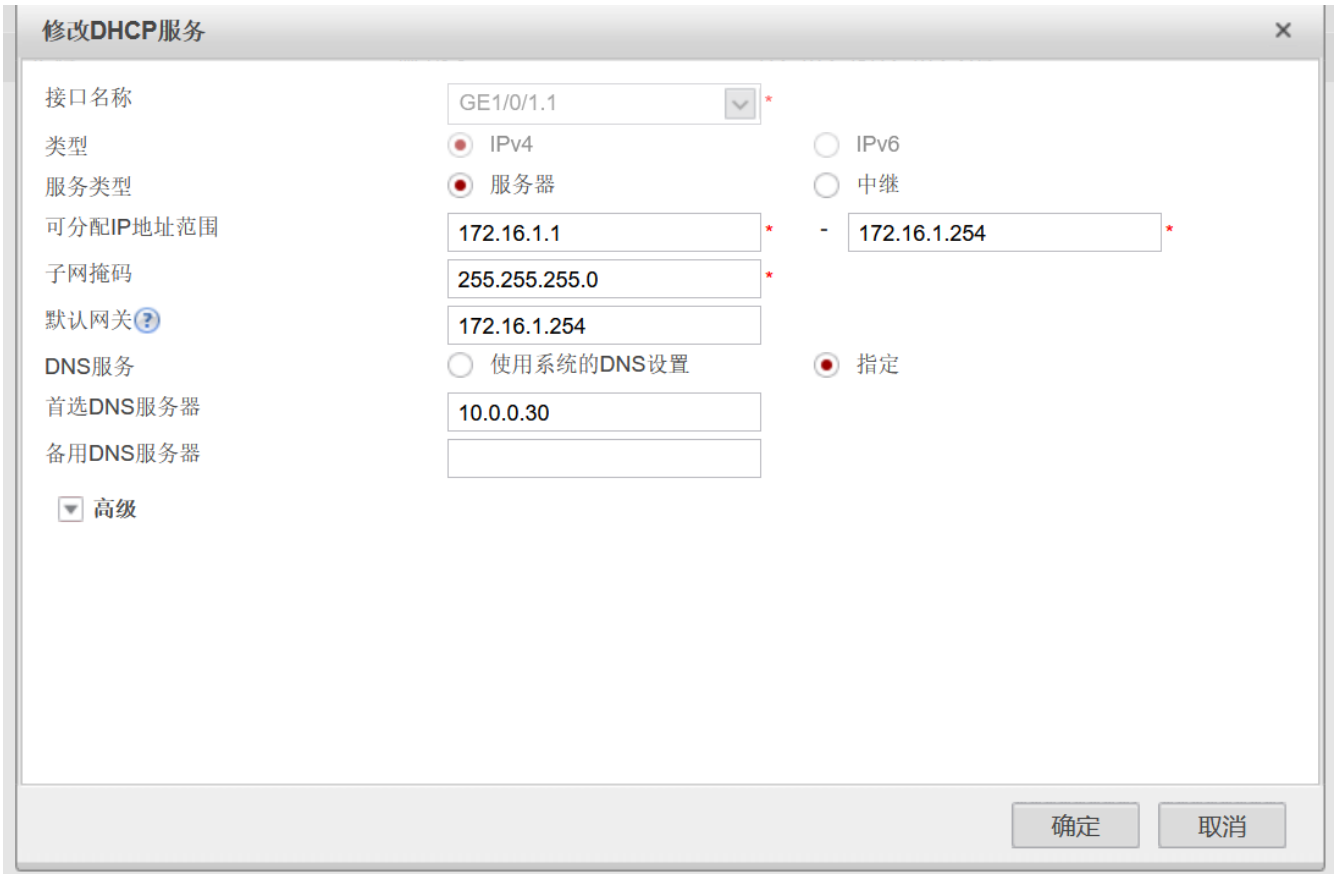
一、根据拓扑图信息完成基础IP配置

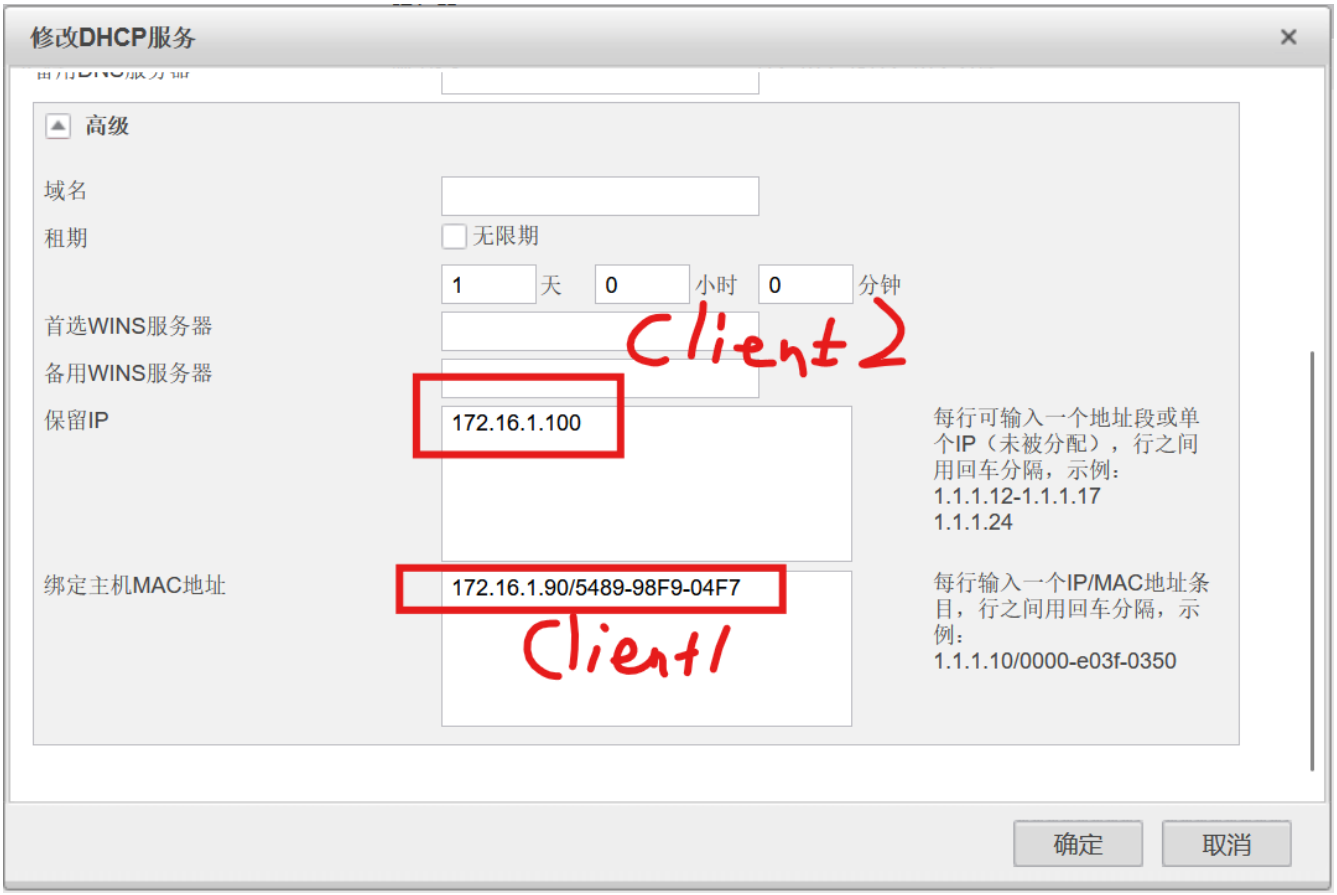
二、配置SW2的VLAN

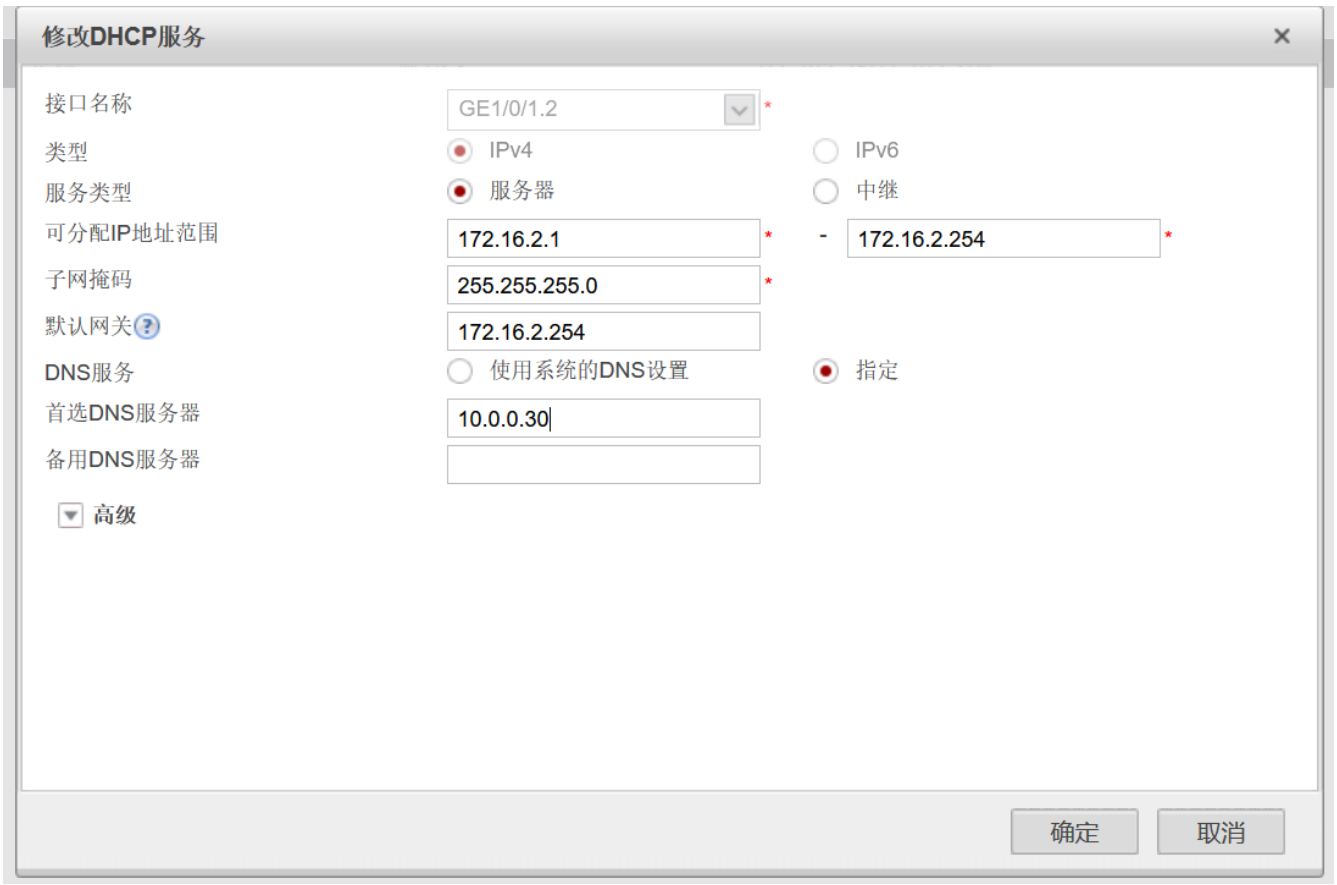
```
[SW2]vlan batch 10 20
[SW2]interface GigabitEthernet 0/0/2
[SW2-GigabitEthernet0/0/2]port link-type access
[SW2-GigabitEthernet0/0/2]port default vlan 10
[SW2]interface GigabitEthernet 0/0/3
[SW2-GigabitEthernet0/0/2]port link-type access
[SW2-GigabitEthernet0/0/2]port default vlan 20
[SW2]interface GigabitEthernet 0/0/1
[SW2-GigabitEthernet0/0/1]port link-type trunk
[SW2-GigabitEthernet0/0/1]port trunk allow-pass vlan 10 20
```

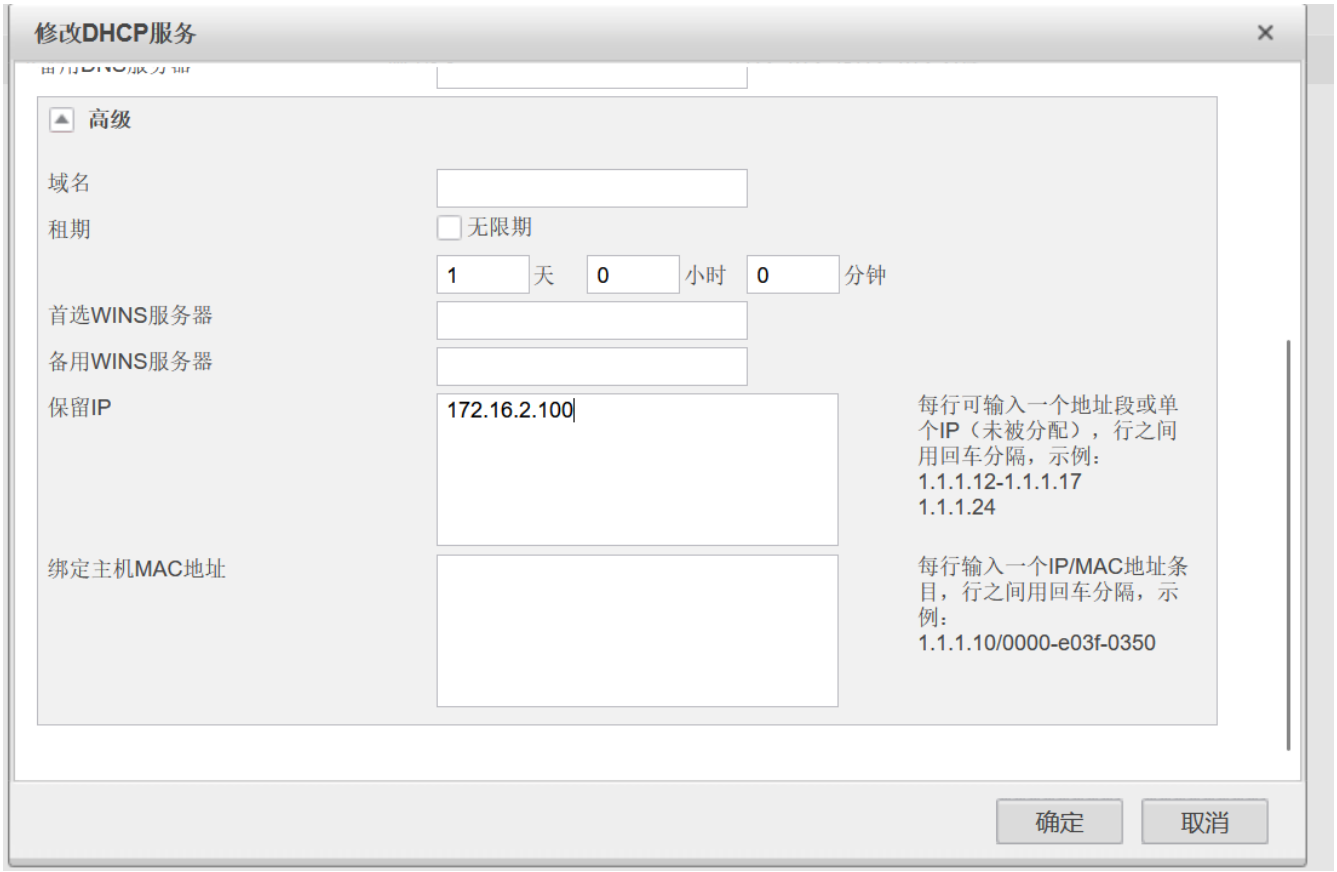
三、配置FW上的DHCP服务

```
[USG6000V1]dhcp enable
[USG6000V1-GigabitEthernet1/0/1.1]dhcp select interface
[USG6000V1-GigabitEthernet1/0/1.2]dhcp select interface
```

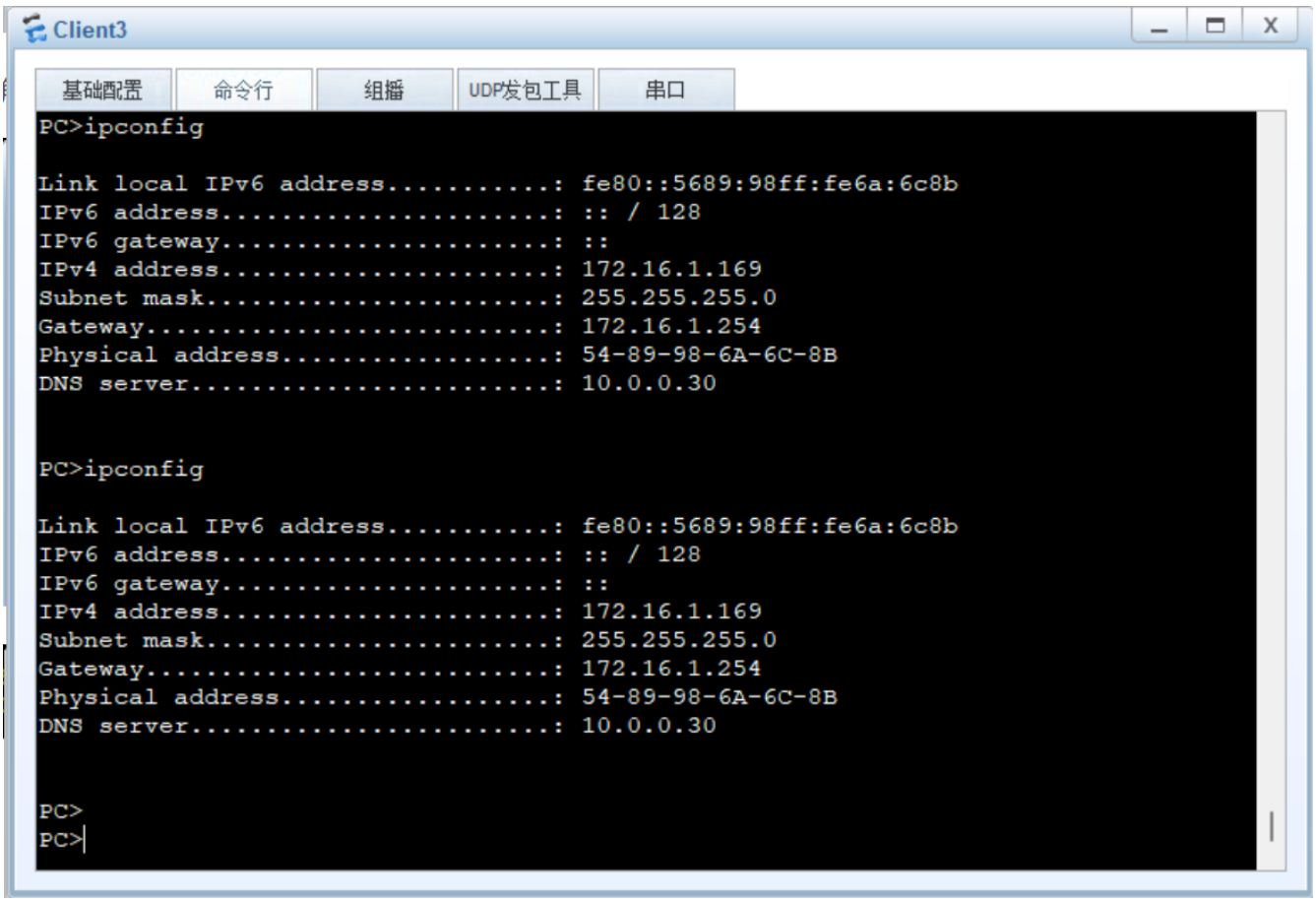


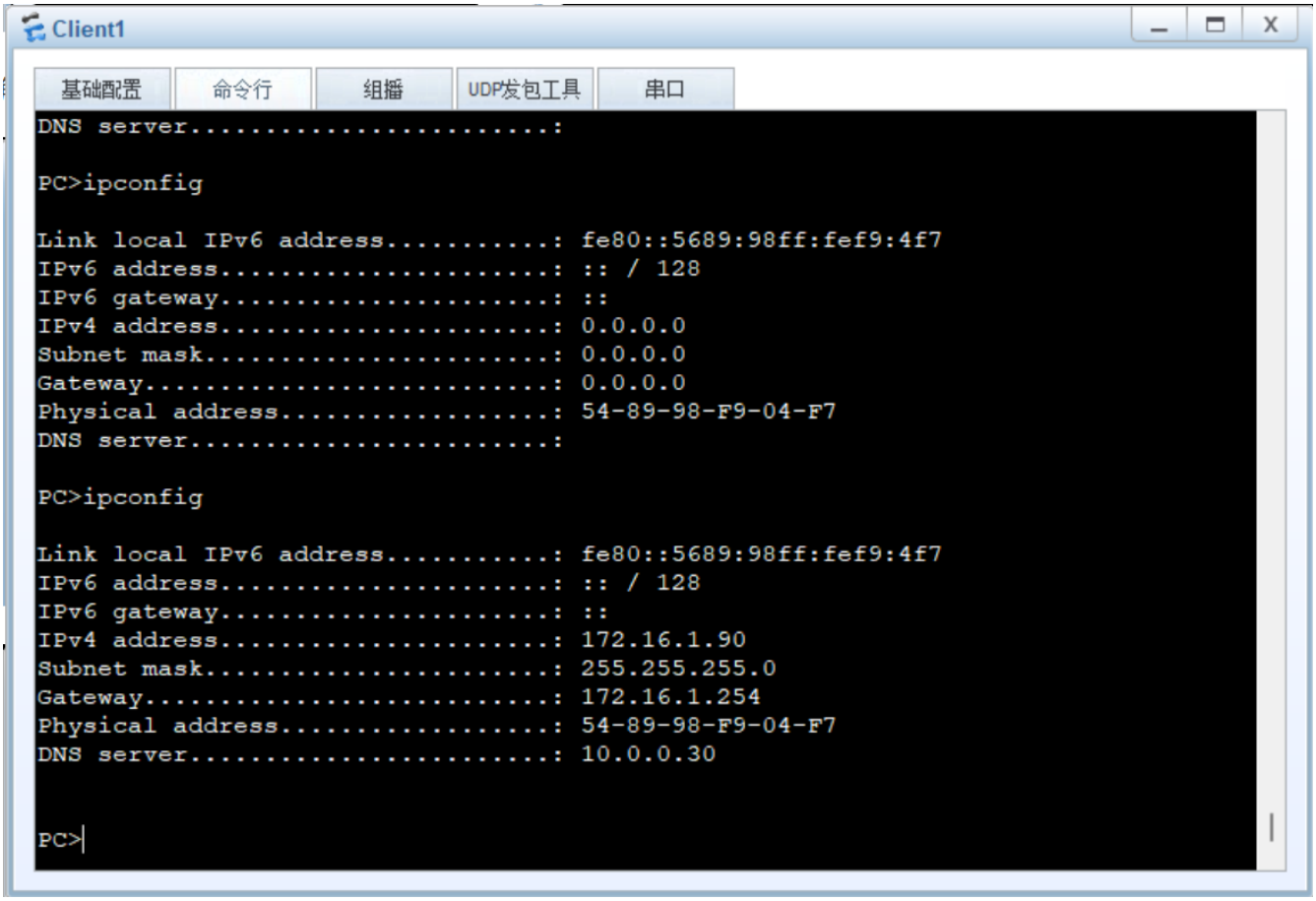

修改DHCP服务
高级
域名
租期
无限期
1
天
0
小时
0
分钟
首选WINS服务器
备用WINS服务器
保留IP
172.16.1.100
client2
每行可输入一个地址段或单个IP（未被分配），行之间用回车分隔，示例：
1.1.1.12-1.1.1.17
1.1.1.24
绑定主机MAC地址
172.16.1.90/5489-98F9-04F7
client1
每行输入一个IP/MAC地址条目，行之间用回车分隔，示例：
1.1.1.10/0000-e03f-0350
确定
取消

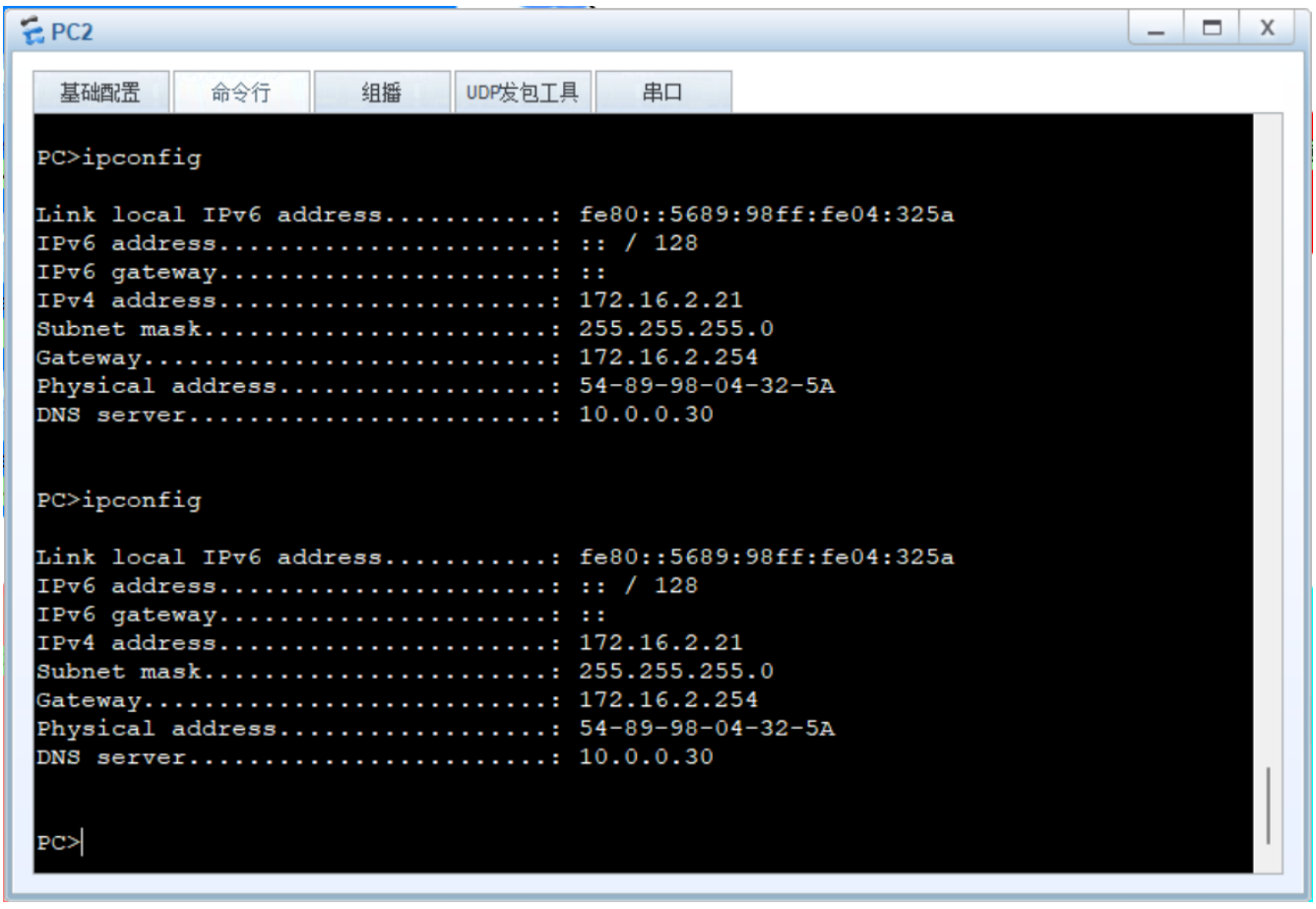

修改DHCP服务
接口名称
GE1/0/1.2
类型
IPv4
IPv6
服务类型
服务器
中继
可分配IP地址范围
172.16.2.1
-
172.16.2.254
子网掩码
255.255.255.0
默认网关
172.16.2.254
DNS服务
使用系统的DNS设置
指定
首选DNS服务器
10.0.0.30
备用DNS服务器
高级
确定
取消



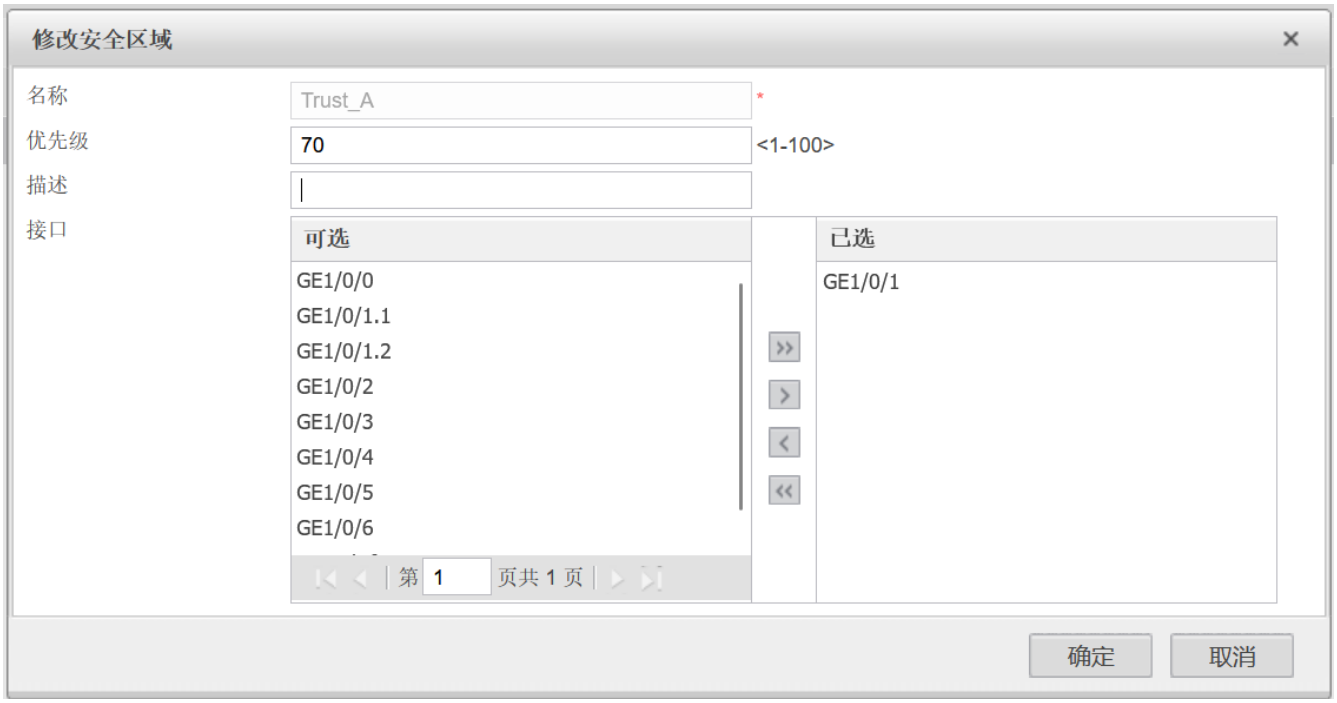
若配置完成后无法正常获取IP，可尝试给主接口配置一个IP

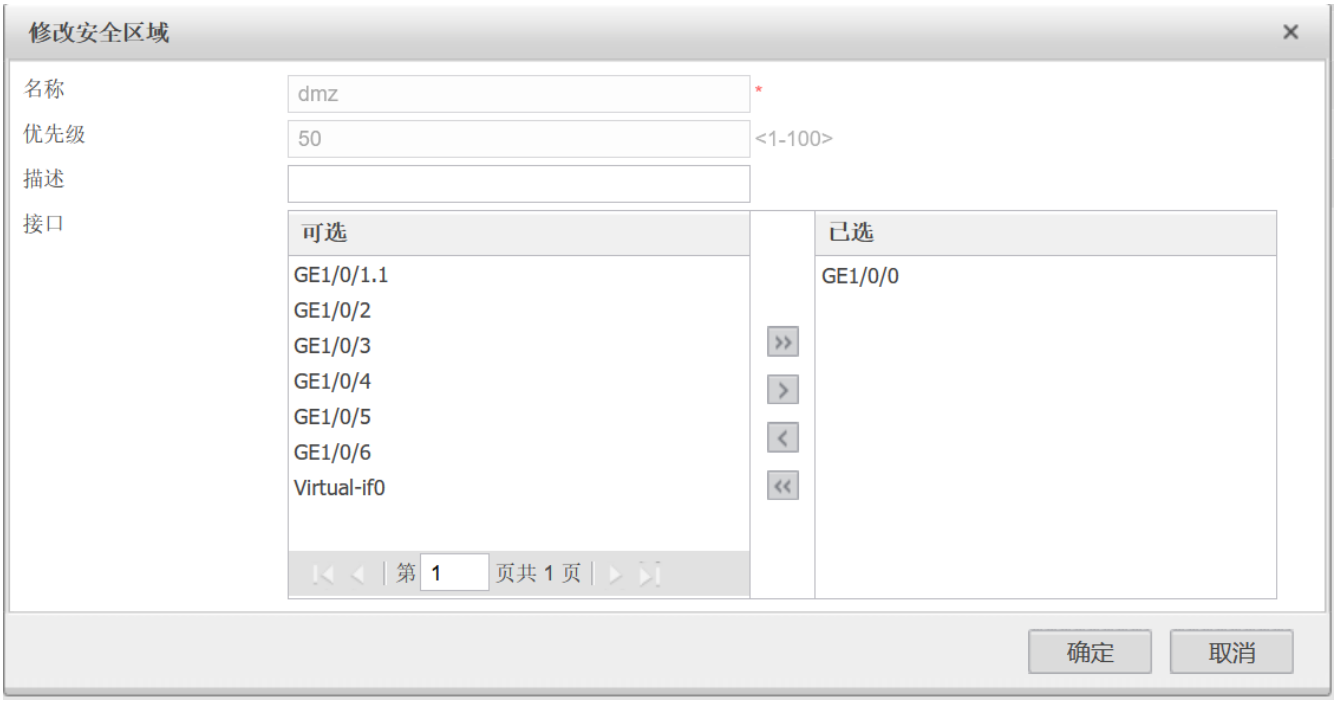


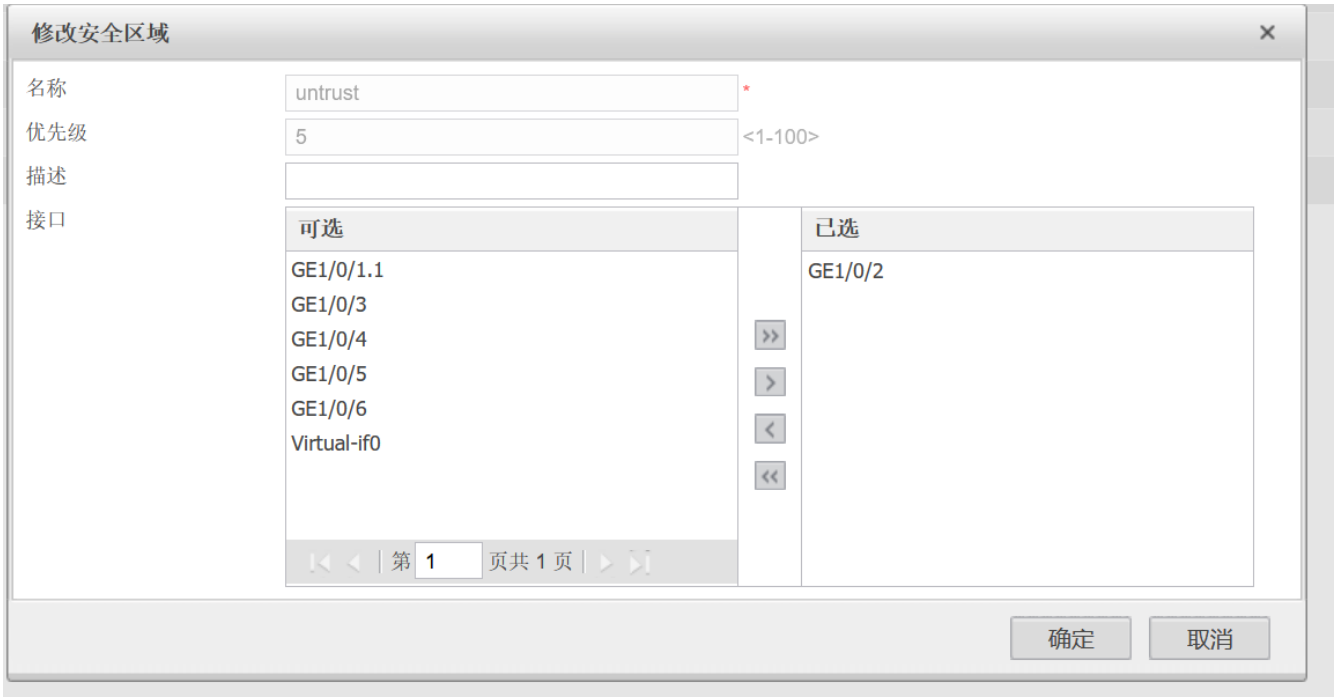

Client1
基础配置
命令行
组播
UDP发包工具
串口
DNS server.....:
PC>ipconfig
Link local IPv6 address.....: fe80::5689:98ff:fef9:4f7
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 0.0.0.0
Subnet mask.....: 0.0.0.0
Gateway.....: 0.0.0.0
Physical address.....: 54-89-98-F9-04-F7
DNS server.....:
PC>ipconfig
Link local IPv6 address.....: fe80::5689:98ff:fef9:4f7
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 172.16.1.90
Subnet mask.....: 255.255.255.0
Gateway.....: 172.16.1.254
Physical address.....: 54-89-98-F9-04-F7
DNS server.....: 10.0.0.30
PC>


PC2
基础配置
命令行
组播
UDP发包工具
串口
PC>ipconfig
Link local IPv6 address.....: fe80::5689:98ff:fe04:325a
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 172.16.2.21
Subnet mask.....: 255.255.255.0
Gateway.....: 172.16.2.254
Physical address.....: 54-89-98-04-32-5A
DNS server.....: 10.0.0.30
PC>ipconfig
Link local IPv6 address.....: fe80::5689:98ff:fe04:325a
IPv6 address.....: :: / 128
IPv6 gateway.....: ::
IPv4 address.....: 172.16.2.21
Subnet mask.....: 255.255.255.0
Gateway.....: 172.16.2.254
Physical address.....: 54-89-98-04-32-5A
DNS server.....: 10.0.0.30
PC>

四、防火墙安全区域配置


修改安全区域
名称
Trust_A
*
优先级
70
<1-100>
描述
接口
可选
GE1/0/0
GE1/0/1.1
GE1/0/1.2
GE1/0/2
GE1/0/3
GE1/0/4
GE1/0/5
GE1/0/6
第 1 页共 1 页
已选
GE1/0/1
确定
取消


修改安全区域
名称
dmz
*
优先级
50
<1-100>
描述
接口
可选
GE1/0/1.1
GE1/0/2
GE1/0/3
GE1/0/4
GE1/0/5
GE1/0/6
Virtual-if0
第 1 页共 1 页
已选
GE1/0/0
确定
取消



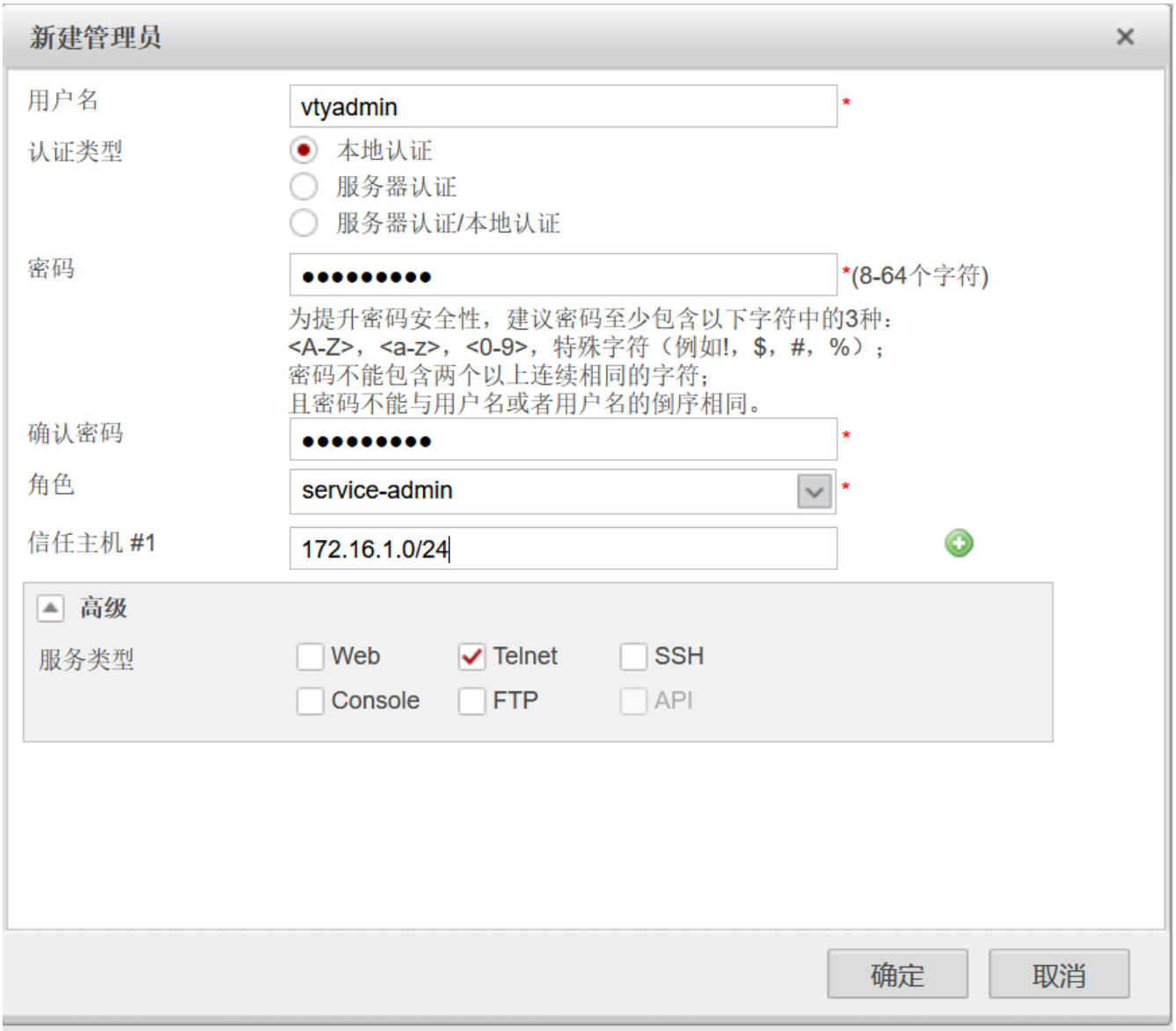
五、防火墙地址组配置

六、管理员配置

启用Telent

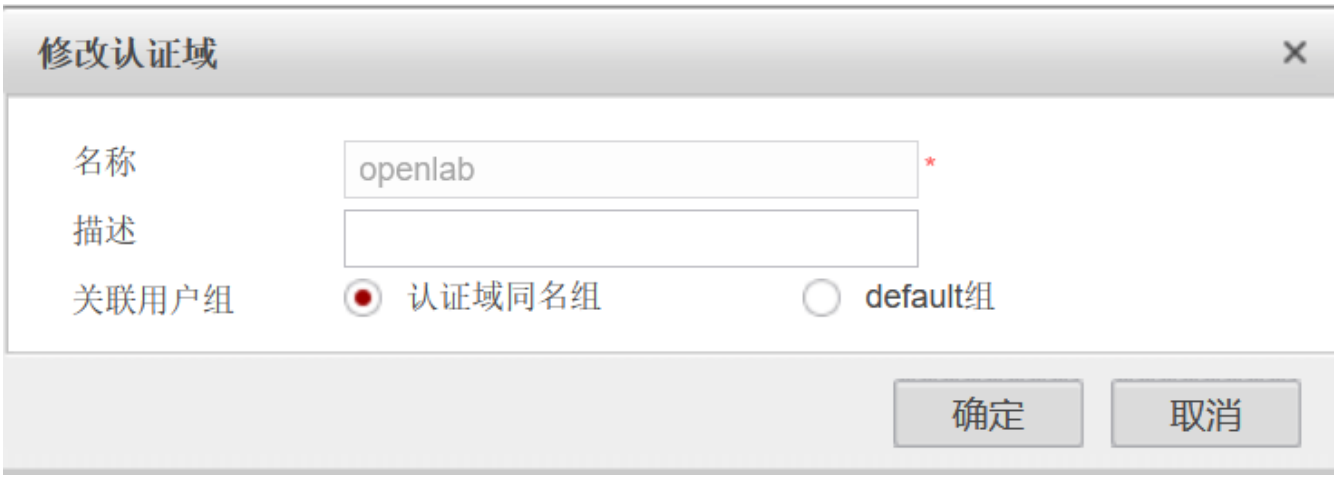
```
[USG6000V1-GigabitEthernet1/0/1.1]service-manage telnet permit
```


新建角色
名称
service-admin
*
描述
拥有业务配置和设备监控权限。
权限控制项
读写
只读
无
面板
监控
策略
对象
网络
系统
确定
取消




```
[USG6000V1]telnet server enable
[USG6000V1]user-interface vty 0 4
[USG6000V1-ui-vty0-4]protocol inbound telnet
```

七、用户认证配置



新建 删除 批量修改 复制 导出 基于组织结构管理用户 最大化显示 刷新 请输入名称 查询

名称	描述	所属组	来源	绑定信息	账号过期时间	激活
a	部门A	/openlab	本地	--	--	--
b	部门B	/openlab	本地	--	--	--
manager	高级管理者	/openlab/a	本地	--	--	--
devops	运维部	/openlab/a	本地	--	--	--
fd	财务部	/openlab/a	本地	--	--	--
td	技术部	/openlab/b	本地	--	--	--
md	市场部	/openlab/b	本地	--	--	--
user_001@openlab(Super_user)	高管用户	/openlab/a/manager	本地	5489-98f9-04f7	永不过期	☑
devops_001@openlab(张三)	运维部用户	/openlab/a/devops	本地	无	永不过期	☑
fd_001@openlab(李四)	财务部用户	/openlab/a/fd	本地	无	永不过期	☑
td_001@openlab	技术部用户	/openlab/b/td	本地	无	永不过期	☑
td_002@openlab	技术部用户	/openlab/b/td	本地	无	永不过期	☑
td_003@openlab	技术部用户	/openlab/b/td	本地	无	永不过期	☑
md_001@openlab	市场部用户	/openlab/b/md	本地	无	2025/08/14 00:00:00	☑
md_001@openlab	市场部用户	/openlab/b/md	本地	无	2025/08/14 00:00:00	☑
md_002@openlab	市场部用户	/openlab/b/md	本地	无	2025/08/14 00:00:00	☑
md_003@openlab	市场部用户	/openlab/b/md	本地	无	2025/08/14 00:00:00	☑
md_004@openlab	市场部用户	/openlab/b/md	本地	无	2025/08/14 00:00:00	☑
md_005@openlab	市场部用户	/openlab/b/md	本地	无	2025/08/14 00:00:00	☑

认证策略列表

新建 删除 复制 插入 移动 清除全部命中次数 启用 禁用

请输入要查询的内容 添加查询项

名称	描述	标签	源安全区域	目的安全区域	源地址/地区	目的地址/地区	服务	认证动作	Portal
policy_auth_01	高级管理者认证策略		Trust_A	any	Client1(高管)	any	any	免认证	
policy_auth_02	运维部_to_DMZ		Trust_A	dmz	Client3(运维部)	DMZ_Server	any	Portal认证	
policy_auth_03	运维部_to_Untrust		Trust_A	untrust	Client3(运维部)	any	any	Portal认证	
policy_auth_04	技术部_to_DMZ		Trust_B	dmz	PC1(技术部)	DMZ_Server	any	匿名认证	
policy_auth_05	财务部_to_DMZ		Trust_A	dmz	Client2(财务部)	DMZ_Server	any	不认证	
policy_auth_06	市场部_to_DMZ		Trust_B	dmz	PC2(市场部)	DMZ_Server	any	匿名认证	
policy_auth_07	市场部_to_Untrust		Trust_B	untrust	PC2(市场部)	any	any	Portal认证	
default	This is the default rule		any	any	any	any	any	不认证	

八、安全策略配置

安全策略列表

新建安全策略 新建安全策略组 删除 复制 移动 插入 导出 清除全部命中次数 启用 禁用 列定制 展开 收缩 刷新 命中查询 清除

请输入要查询的内容 添加查询项

序号	名称	描述	标签	VLAN ID	源安全区域	目的安全...	源地址/地区	目的地址/...	用户	服务	应用	时间段	动作	内容安全	命中次数	启用	编辑
1	policy_01	防火墙tel...		any	Trust_A	local	any	any	any	telnet	any	any	允许		0 清除	☑	
2	policy_02	DHCP协议		any	Trust_A Trust_B	local	any	any	any	DHCP	any	any	允许		0 清除	☑	
3	policy_03	DNS协议		any	Trust_A Trust_B	dmz	Trust... Trust...	DNS ...	any	dns	any	any	允许		0 清除	☑	
4	policy_04	运维部_t...		any	Trust_A	dmz	Client...	DMZ_...	any	any	any	any	允许		0 清除	☑	
5	policy_05	高管和财...		any	Trust_A	dmz	Client... Client...	OA S... Web ...	any	http https	any	any	允许		0 清除	☑	
6	policy_06	运维部_t...		any	Trust_A	untrust	Client...	any	any	any	any	No_workt...	允许		0 清除	☑	
7	policy_07	高管_to_...		any	Trust_A	untrust	Client...	any	any	any	any	any	允许		0 清除	☑	
8	policy_08	技术部_t...		any	Trust_B	dmz	PC1(...	Web ...	any	any	any	any	允许		0 清除	☑	
9	policy_09	技术部和...		any	Trust_B	dmz	PC1(... PC2(...	OA S...	any	http https	any	any	允许		0 清除	☑	
10	policy_10	市场部_t...		any	Trust_B	untrust	PC2(...	any	any	any	any	any	允许		0 清除	☑	
11	policy_11	运维检修		any	Trust_A Trust_B	dmz	Client... Client... PC1(... PC2(...	any	any	any	any	weekend	禁止		0 清除	☑	
12	default	This is th...		any	any	any	any	any	any	any	any	any	允许		65 清除	☑	