

## 组网及说明

### 1 配置需求及说明

#### 1.1 适用的产品系列

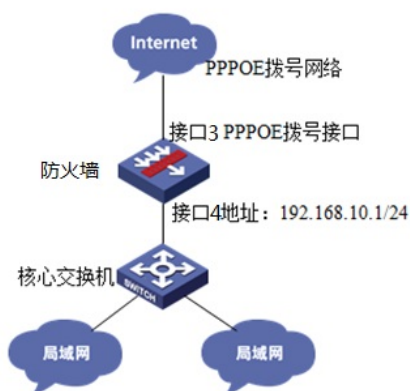
本案例适用于如F5080、F5060、F5030、F5000-M等F5000、F5000-X系列的防火墙。

注：本案例是在F1000-C-G2的Version 7.1.064, Release 9323P1801版本上进行配置和验证的。

#### 1.2 配置需求及实现的效果

将防火墙部署在互联网出口，使用PPPOE拨号方式接入互联网。运营商提供的拨号账号为：hz123456，密码为：123456。初步规划防火墙使用3接口接入运营商，使用4接口连接内部网络，内部网络使用192.168.10.0网段，要求内网终端可以自动获取到地址并可以访问互联网。

### 2 组网图



## 配置步骤

### 3 配置步骤

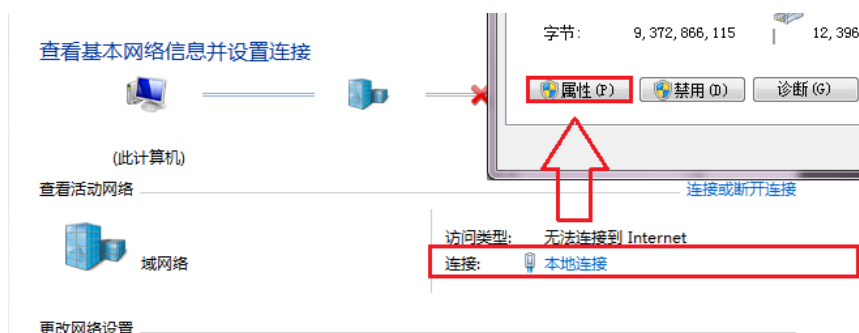
#### 3.1 基本登录

#在防火墙接口面板找到0接口，用网线将电脑和设备的0接口连在一起，电脑配置与设备管理IP相同网段的地址192.168.0.2/24，下面是电脑IP地址配置方法：

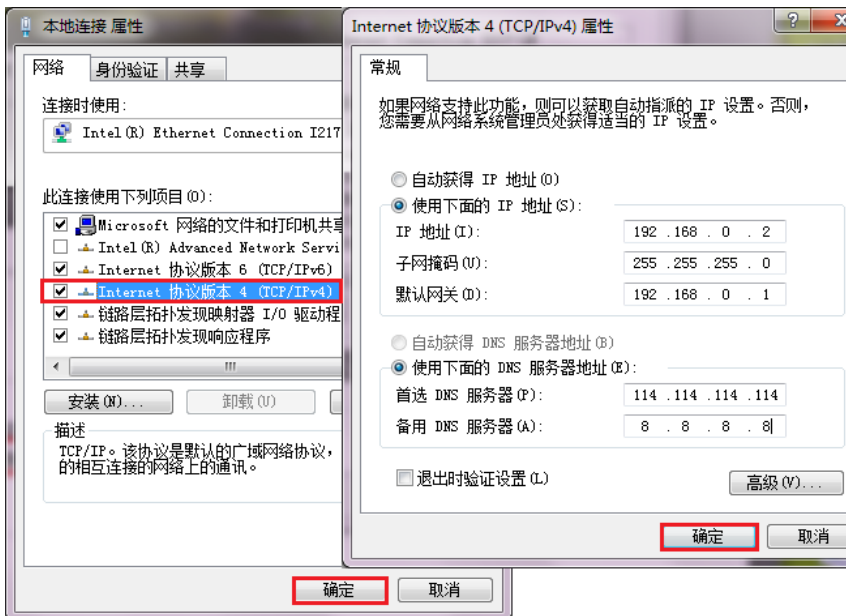
点击电脑右下角电脑图标，选择“打开网络和共享中心”选项。



#鼠标单击“本地连接”后在弹出的状态窗口中选择“属性”选项



#鼠标双击“Internet协议版本4”打开属性菜单，按照下面图片内容配置电脑IP地址。

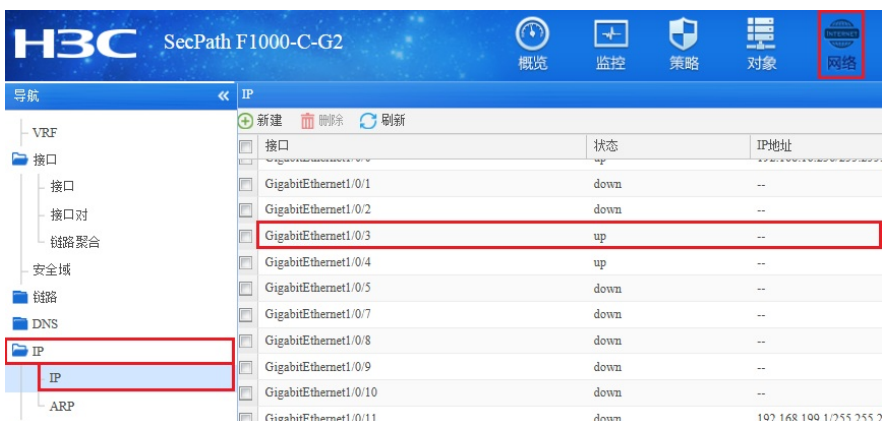


#电脑IP地址配置完成后打开浏览器，在浏览器地址栏中输入<https://192.168.0.1>登录设备管理界面。设备默认用户名密码均为admin。



### 3.2 配置外网接口

#在“网络”>“IP” 选项中选择1/0/3接口并点击此接口最后面的“编辑”按钮。



#“IP地址”处选择PPPOE，用户名密码分别填入运营商分配的账号和密码。

**修改IP配置**

接口: GigabitEthernet1/0/3 (GE1/0/3)

状态: up

描述: GigabitEthernet1/0/3 Interface

IP地址:  指定IP地址  通过DHCP自动获取IP地址  PPPoE

用户名:  (1-80字符)

密码:  (1-255字符)

在线方式:  永久在线  空闲自动断线

自动获取IP地址

使用指定的IP地址

IP地址/掩码长度:  /

自动获取DNS地址

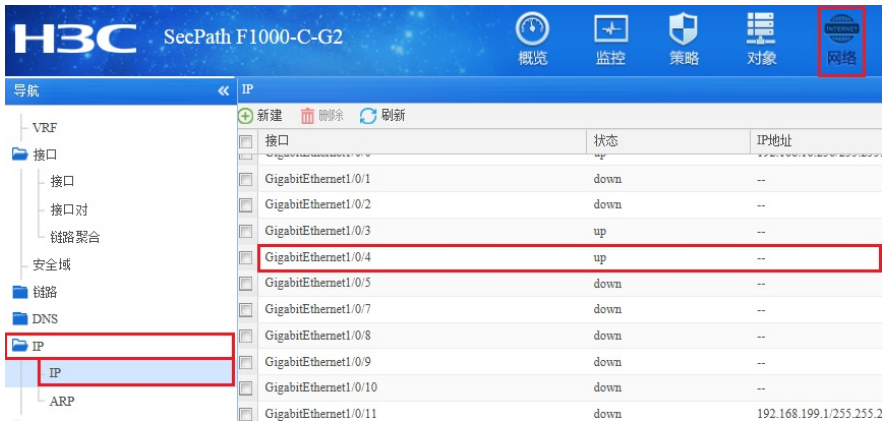
使用指定的DNS地址

首选DNS服务器:

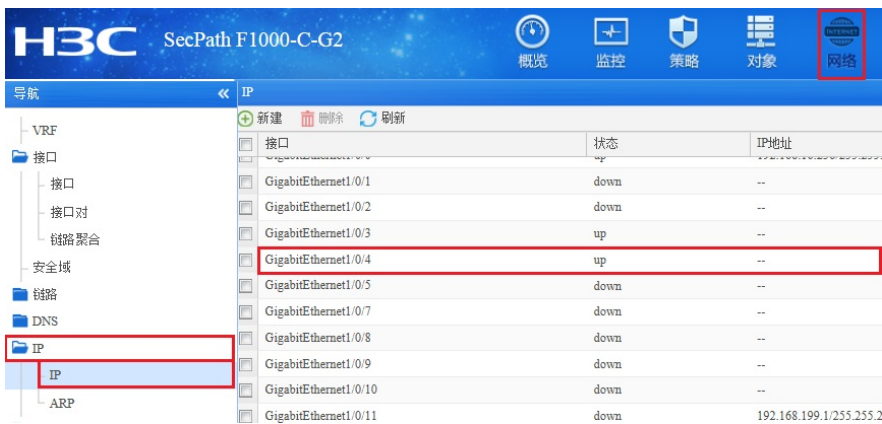
备选DNS服务器:

### 3.3 配置内网接口

#在“网络”>“IP”选项中选择1/0/4接口并点击此接口最后面的“编辑”按钮。

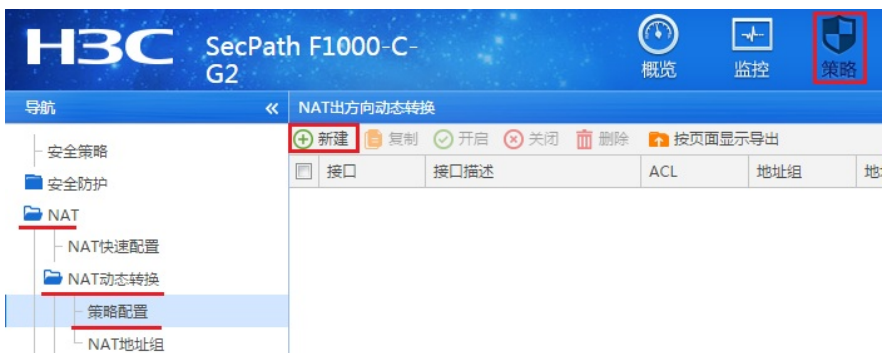


#“IP地址”选择指定IP地址，设置内网网关地址为192.168.10.1，掩码为255.255.255.0。

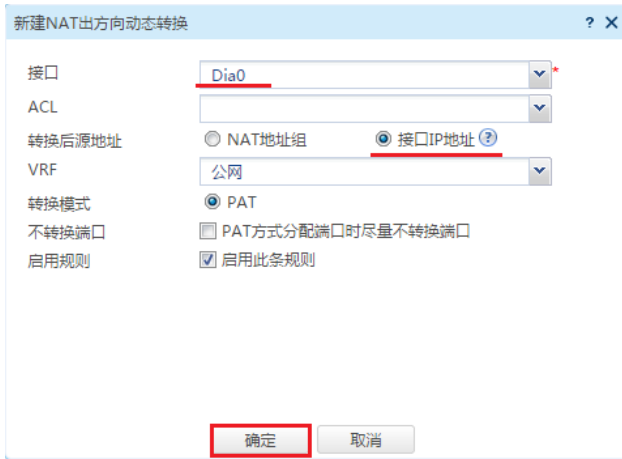


### 3.4 配置NAT地址转换

#在“策略”>“NAT”>“NAT动态转换”>“策略配置”选项中点击新建。



#“接口”选择外网接口“Dia0”接口，转换后源地址选择“接口IP地址”并点击确定。



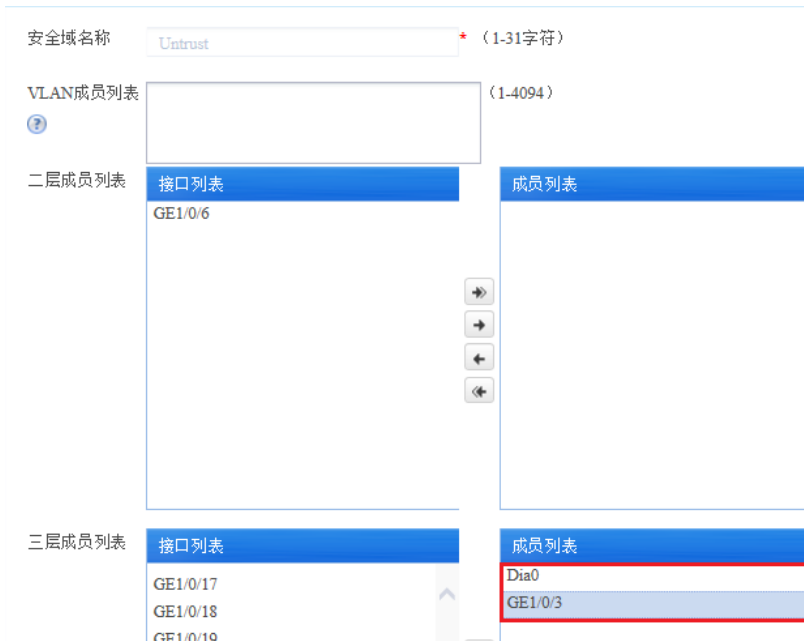
注：外网口1/0/3接口配置为PPPOE时，在接口列表中会生成一个Dia接口，编号默认从0开始。

### 3.5 配置外网接口加入Untrust安全区域

#在“网络”>“接口”>“安全域”中选择“Untrust”区域点击编辑按钮。



#在“三层成员列表”中将1/0/3、Dia0接口加入成员列表。



### 3.6 配置内网接口加入Trust安全区域

#在“网络”>“接口”>“安全域”中选择“Trust”区域点击编辑按钮。



#在“三层成员列表”中将1/0/2接口加入成员列表。

The screenshot shows a configuration window for a security policy named 'Trust'. It is divided into three sections: VLAN member list, two-layer member list, and three-layer member list. In the three-layer member list, the 'Interface List' tab is active, showing 'GE1/0/20'. The 'Member List' tab is also active, and 'GE1/0/4' is highlighted with a red box, indicating it has been added to the list.

### 3.7 配置安全策略将Trust到Untrust域内网数据放通

#在“安全策略”中点击“新建”。

The screenshot shows the H3C management interface for a SecPath F1000-C-G2 device. The 'Security Policy' (安全策略) section is selected in the navigation menu. A table lists existing policies, and a '+ New' (新建) button is highlighted with a red box. The table below shows:

名称	源安全域	目的安全域	类型	ID	描述	源地址
ljs			IPv4	3		
2			IPv4	1		

#“源安全域”选择Trust，“目的安全域”选择Untrust，在“源IP地址”中选择“添加IPv4地址对象组”。

The screenshot shows the 'New Security Policy' (新建安全策略) configuration form. The 'Source Security Domain' (源安全域) is set to 'Trust' and the 'Destination Security Domain' (目的安全域) is set to 'Untrust'. The 'Type' (类型) is set to 'IPv4'. The 'Action' (动作) is set to 'Allow' (允许). The 'Source IP Address' (源IP地址) dropdown menu is open, and the option '+ Add IPv4 Address Object Group' (添加IPv4地址对象组) is highlighted with a red box.

#对象组名称输入内网，点击“添加”按钮添加地址对象，添加内网192.168.10.0网段。点击“确定”完成策略配置。

新建IPv4地址对象组

对象组名称: 内网 \* (1-31字符)

描述: (1-127字符)

安全域: Trust

类型	内容	排除地址	编辑
添加对象			

对象: 网段

192.168.10.0 / 255.255.255.0 \* (IPv4地址/掩码长度0-32)

排除地址: (1-127字符)

3.8 配置安全策略将Trust到Local域、Local到Trust域、Local到Untrust域数据全放通策略  
#在“安全策略”中点击新建。



#创建策略名称为互通，“源安全域”、“目的安全域”选择“多选”，并选中Local、Trust。

新建安全策略

名称: 互通 \* (1-127字符)

源安全域: 请选择源安全域

目的安全域: 请选择目的安全域

类型:  IPv4  IPv6

描述信息: (1-127字符)

动作:  允许  拒绝

源IP地址: 请选择或输入对象组

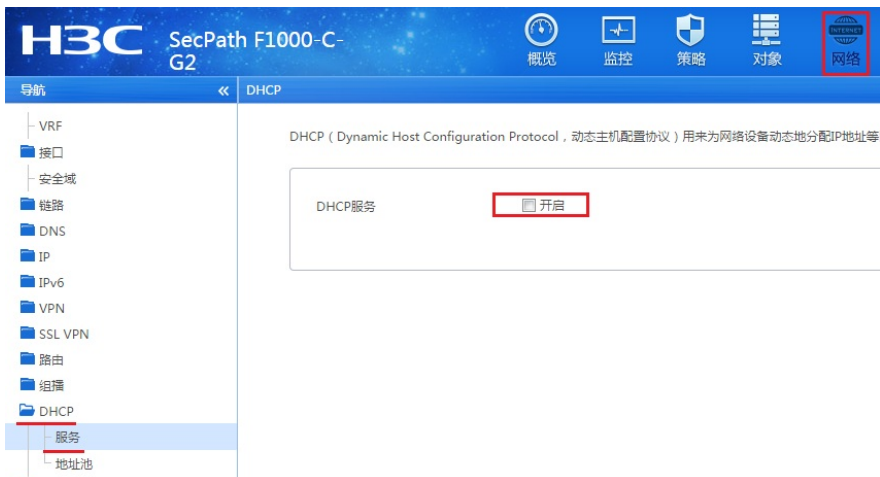
#策略配置如下图所示，点击确定完成策略配置。

## 新建安全策略

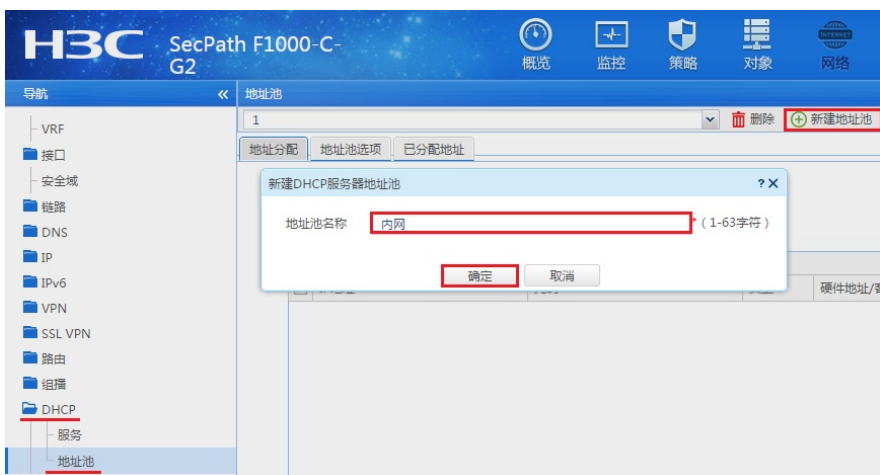
名称	<input type="text" value="互通"/> * (1-127字符)
源安全域	<input type="text" value="Local, Trust"/> [多选]
目的安全域	<input type="text" value="Trust, Untrust, Local"/> [多选]
类型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
描述信息	<input type="text"/> (1-127字符)
动作	<input checked="" type="radio"/> 允许 <input type="radio"/> 拒绝
源IP地址	<input type="text" value="请选择或输入对象组"/> [多选]
目的IP地址	<input type="text" value="请选择或输入对象组"/> [多选]
服务	<input type="text" value="请选择服务"/> [多选]
应用	<input type="text" value="请选择应用"/> [多选]
应用组	<input type="text" value="请选择应用组"/> [多选]
用户	<input type="text" value="请选择用户"/>
时间段	<input type="text" value="请选择时间段"/>
VRF	<input type="text" value="公网"/>
内容安全	
IPS策略	<input type="text" value="--NONE--"/>
数据过滤策略	<input type="text" value="--NONE--"/>
文件过滤策略	<input type="text" value="--NONE--"/>
防病毒策略	<input type="text" value="--NONE--"/>
URL过滤策略	<input type="text" value="--NONE--"/>

### 3.9 配置DHCP服务

#在“网络”>“DHCP”>“服务”中开启DHCP服务。

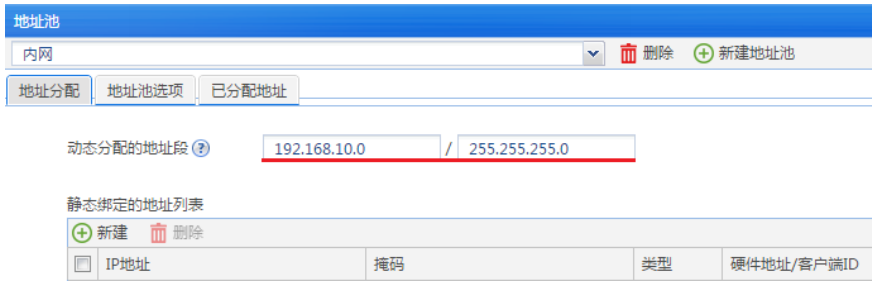


#在“网络”>“DHCP”>“地址池”中新建地址池，名称设定为内网。

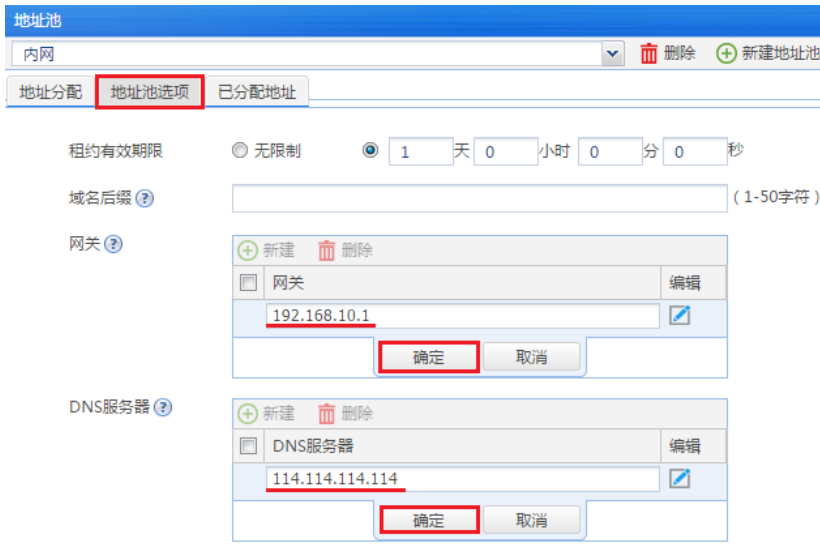


#设置“动态分配的地址段”为192.168.10.0后点击“确定”。



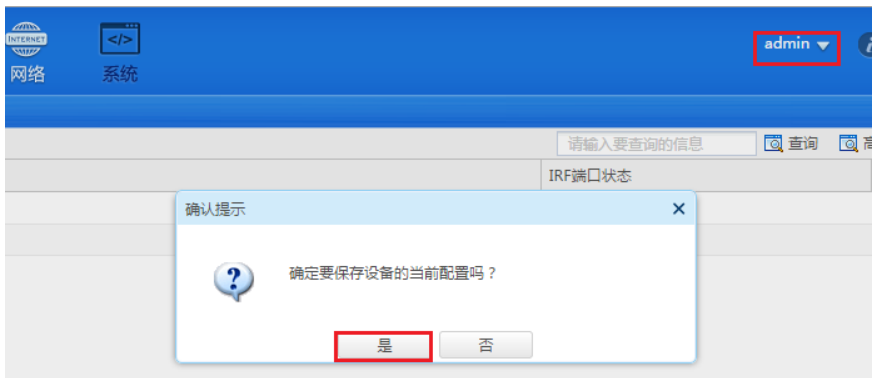


#在“地址池选项”配置“网关”地址为192.168.10.1点击确定按钮，“DNS服务器”地址优先设置当地运营商提供的DNS服务器地址，如果没有提供可以设置114.114.114.114或8.8.8.8等DNS服务器地址，配置完成后点击“确定”。



### 3.10 保存配置

在设备右上角选择“保存”选项，点击确定按钮完成配置。



### 配置关键点