

知 F1000-AK系列使用PPPOE拨号方式上网配置方法（WEB）

PPPoE zhiliao_8mkdB 2018-11-24 发表

组网及说明

1 配置需求及说明

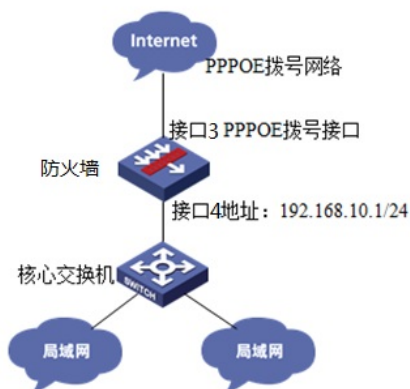
1.1 适用的产品系列

本案例适用于如F1000-AK180、F1000-AK170等F1000-AK系列的防火墙。

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 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：

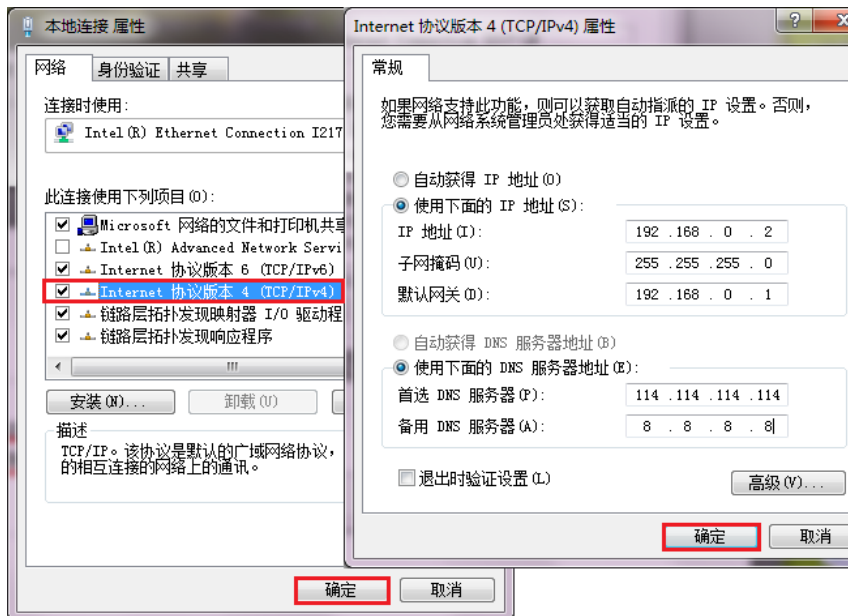
点击电脑右下角电脑图标，选择“打开网络和共享中心”选项。



#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。

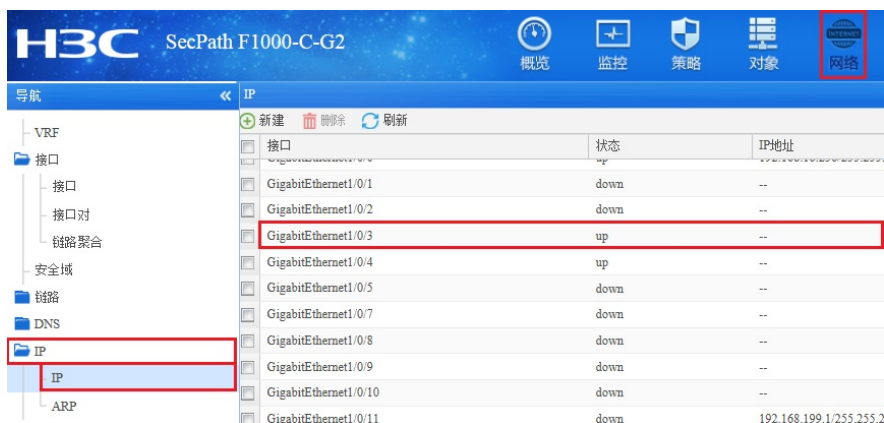


#电脑IP地址配置完成后打开浏览器，在浏览器地址栏中输入<https://192.168.0.1>登录设备管理界面。设备默认用户名密码均为admin。



3.1 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:

3.2 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。

H3C SecPath F1000-C-G2

概览 监控 策略 对象 **网络**

导航: VRF, 接口, 接口对, 链路聚合, 安全域, 策略, DNS, **IP**, ARP

IP配置列表:

接口	状态	IP地址
GigabitEthernet1/0/1	down	--
GigabitEthernet1/0/2	down	--
GigabitEthernet1/0/3	up	--
GigabitEthernet1/0/4	up	--
GigabitEthernet1/0/5	down	--
GigabitEthernet1/0/7	down	--
GigabitEthernet1/0/8	down	--
GigabitEthernet1/0/9	down	--
GigabitEthernet1/0/10	down	--
GigabitEthernet1/0/11	down	192.168.199.1/255.255.2

#“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。

修改IP配置

接口: GigabitEthernet1/0/4 (GE1/0/4)

状态: up

描述: GigabitEthernet1/0/4 Interface

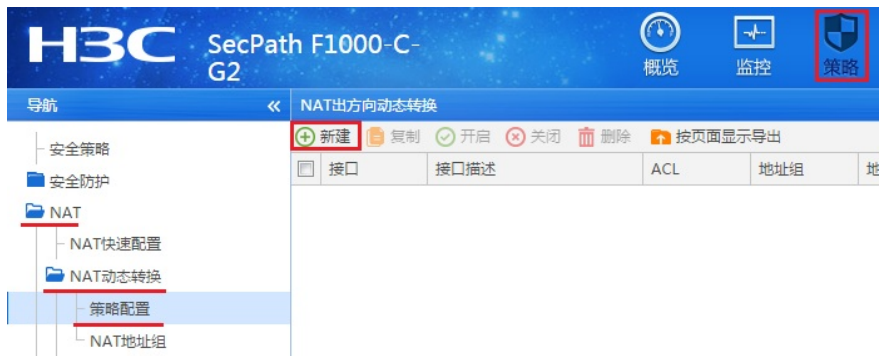
IP地址: ☒ 指定IP地址 ☐ 通过DHCP自动获取IP地址 ☐ PPPoE

IP地址/掩码长度: /

从IP地址	掩码	编辑

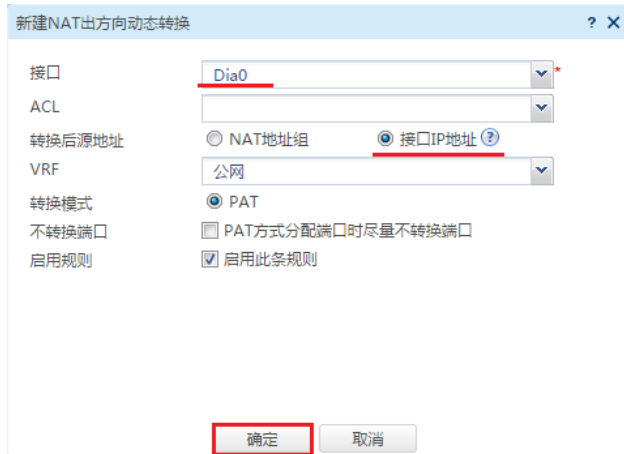
3.3 配置NAT地址转换

#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。

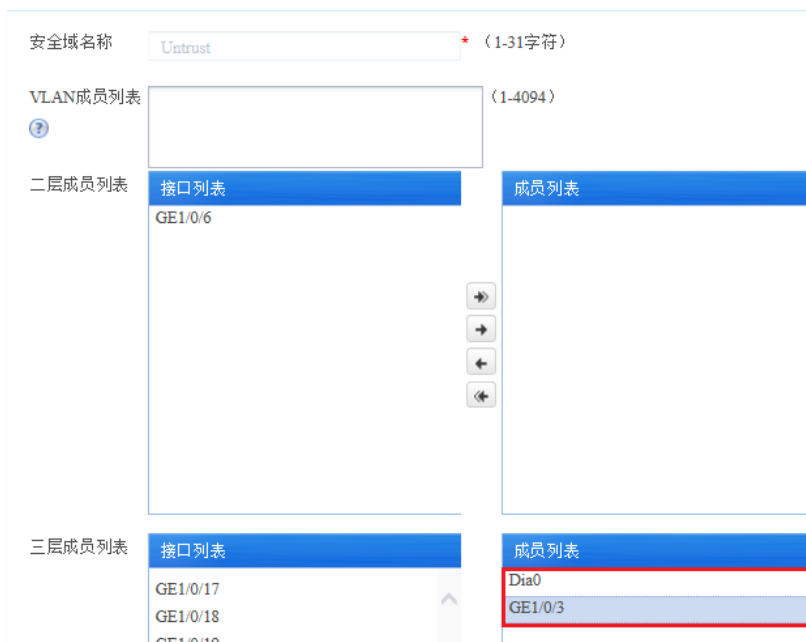


3.4 配置外网接口加入Untrust安全区域

#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。

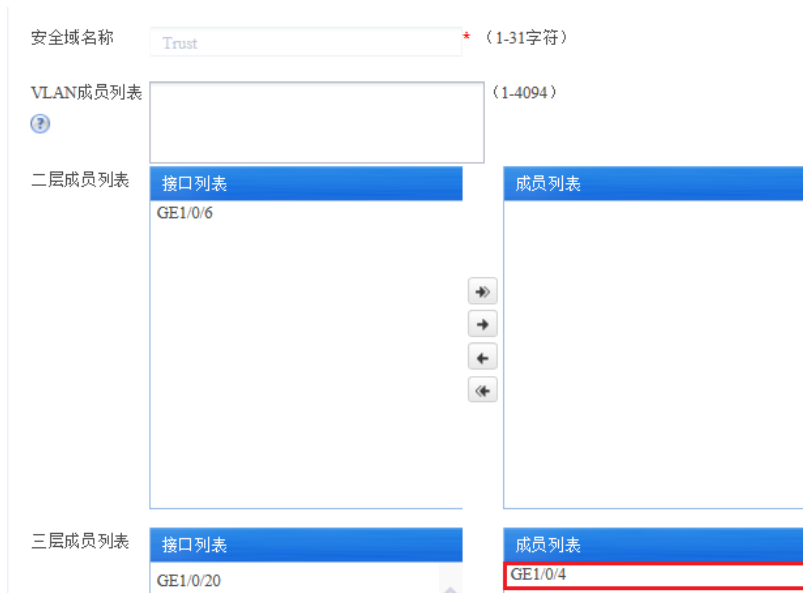


3.5 配置内网接口加入Trust安全区域

#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。

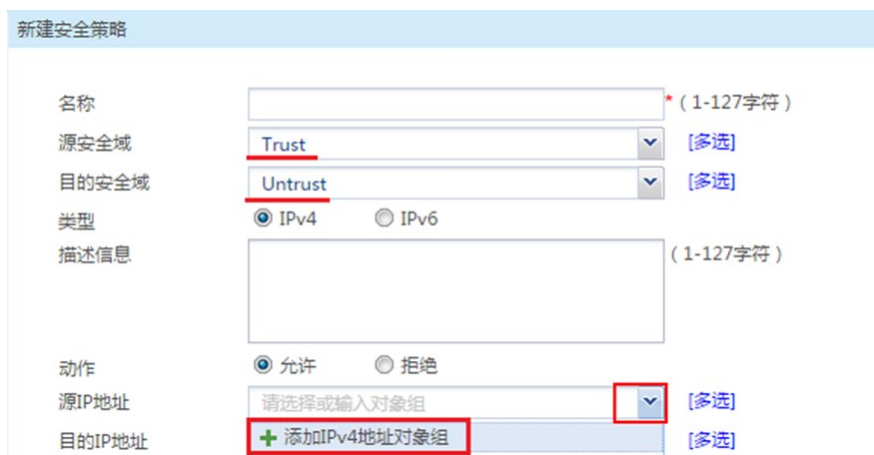


3.6 配置安全策略将Trust到Untrust域内网数据放通

#在“安全策略”中点击“新建”。



#“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”。



#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

+ 添加 删除

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:

确定 取消

确定 取消

3.7 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。

H3C SecPath F1000-C-G2

概览 监控 **策略**

导航 << 安全策略

+ 新建 删除 复制 移动 统计 取消统计 启用 禁用

安全策略配置变更之后(?), 需要 **立即加速** 才能生效。内容安全配置变更之后(?), 需要 **立即加速** 才能生效。

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		

#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 [多选]

目的安全域: 请选择目的安全域 [多选]

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 [多选]

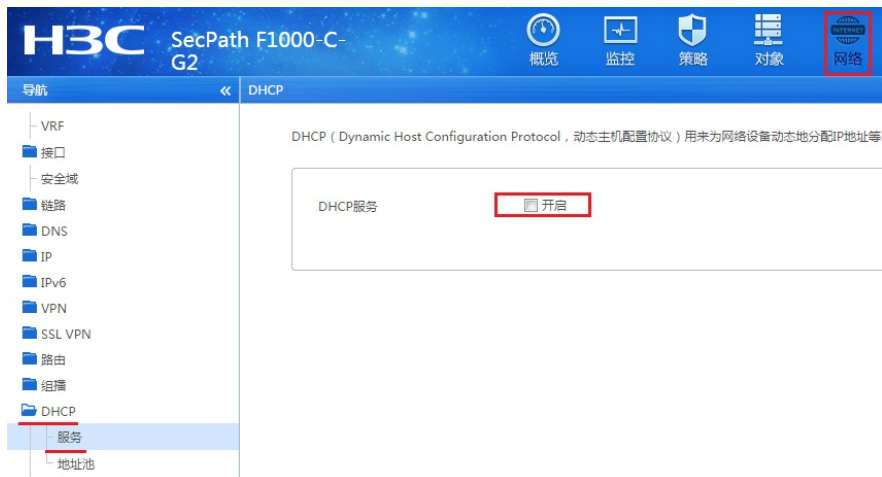
#策略配置如下图所示，点击确定完成策略配置。

新建安全策略

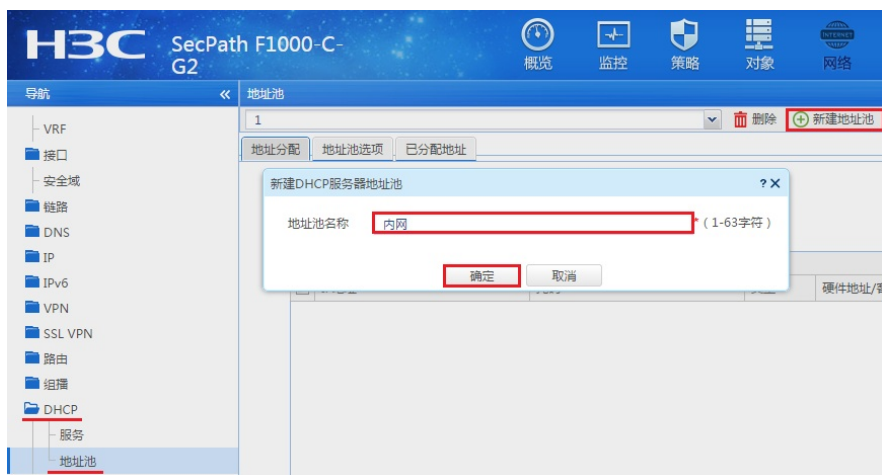
名称	互通	* (1-127字符)
源安全域	Local, Trust	[多选]
目的安全域	Trust, Untrust, Local	[多选]
类型	☒ IPv4 ☐ IPv6	
描述信息		(1-127字符)
动作	☒ 允许 ☐ 拒绝	
源IP地址	请选择或输入对象组	[多选]
目的IP地址	请选择或输入对象组	[多选]
服务	请选择服务	[多选]
应用	请选择应用	[多选]
应用组	请选择应用组	[多选]
用户	请选择用户	
时间段	请选择时间段	
VRF	公网	
内容安全		
IPS策略	--NONE--	
数据过滤策略	--NONE--	
文件过滤策略	--NONE--	
防病毒策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

3.8 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”。

地址池

内网

删除 新建地址池

地址分配 地址池选项 已分配地址

动态分配的地址段 192.168.10.0 / 255.255.255.0

静态绑定的地址列表

IP地址	掩码	类型	硬件地址/客户端ID

#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”。

地址池

内网

删除 新建地址池

地址分配 地址池选项 已分配地址

租约有效期限 无限制 1 天 0 小时 0 分 0 秒

域名后缀 (1-50字符)

网关

网关	编辑
192.168.10.1	

确定 取消

DNS服务器

DNS服务器	编辑
114.114.114.114	

确定 取消

3.9 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。

网络 系统

admin

请输入要查询的信息 查询 高

IRF端口状态

确认提示

确定要保存设备的当前配置吗？

是 否

配置关键点