

知 F1000-X-G2/F100-X-G2系列防火墙外网使用DHCP方式上网配置方法（WEB界面）

DHCP zhiliao_FO3qD 2018-11-25 发表

组网及说明

1 配置需求及说明

1.1 适用的产品系列

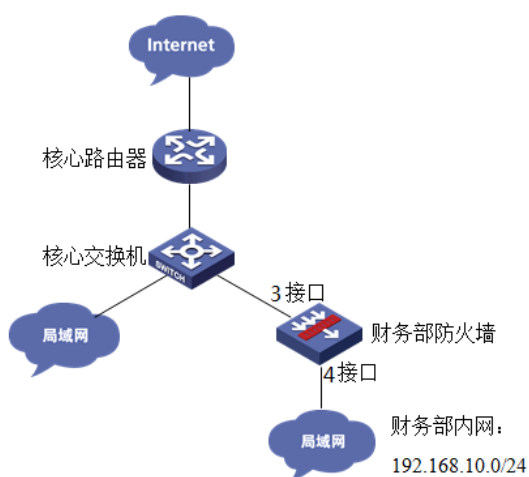
本案例适用于如F1000-A-G2、F1000-S-G2、F100-M-G2、F100-S-G2等F1000-X-G2、F100-X-G2系列的防火墙。

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

将防火墙部署在公司核心网络下为财务部门提供网络安全防护，要求防火墙使用3接口自动获取公司内部网地址，4接口连接财务部为财务部用户动态下发192.168.10.0网段地址。在对公司原有网络影响最小的情况下实现财务部电脑可以访问防火墙以外的网络，防火墙以外的网络不能访问财务部电脑的需求。

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：

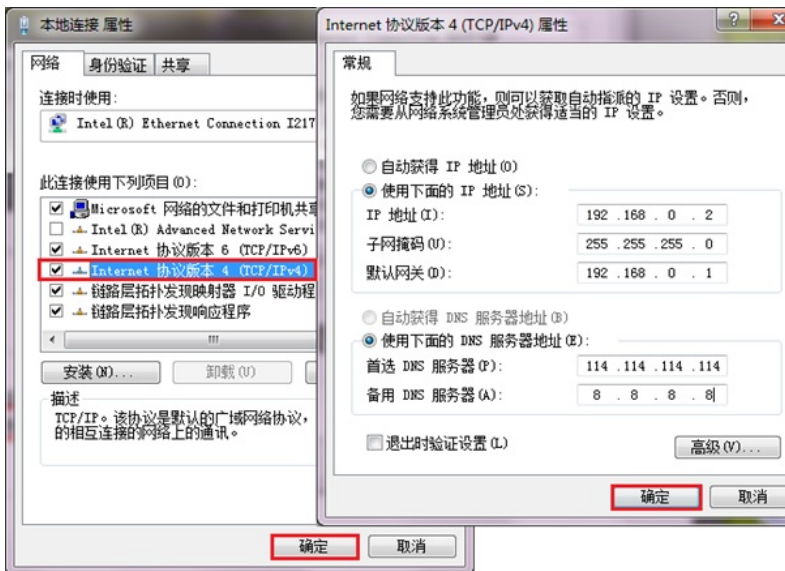
点击电脑右下角电脑图标，选择“打开网络和共享中心”选项。



#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。

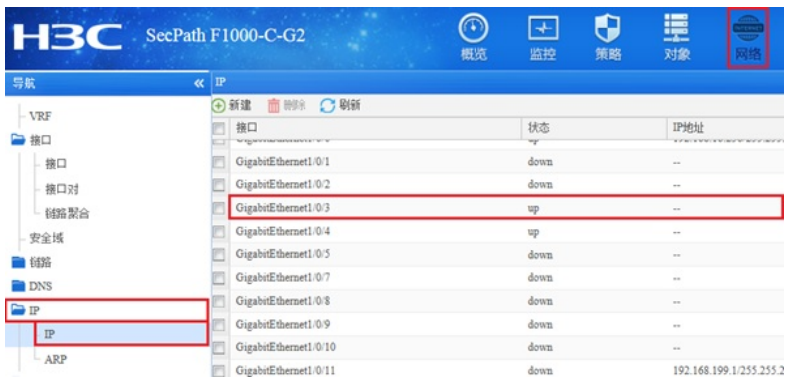


#电脑IP地址配置完成后打开浏览器，在浏览器地址栏中输入<https://192.168.0.1>登录设备管理界面。设备默认用户名密码均为admin。



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。

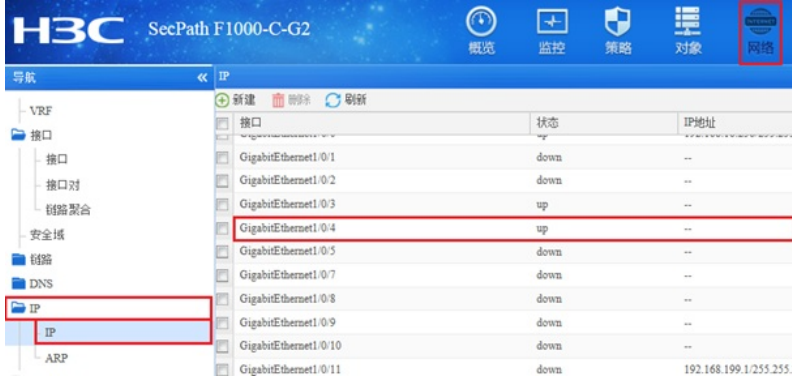


#“IP地址”选择“通过DHCP自动获取IP地址”，并点击“确定”按钮。



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”填写规划的内网地址192.168.10.1，掩码为255.255.255.0。

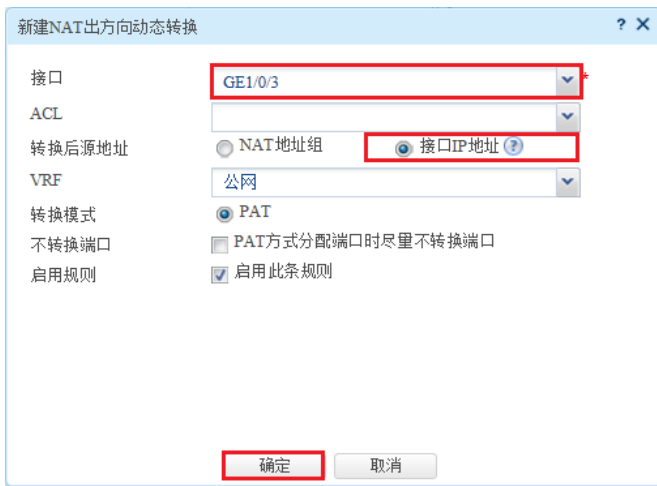


3.4 配置NAT地址转换

#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1/0/3，转换后源地址选择“接口IP地址”并点击“确定”。

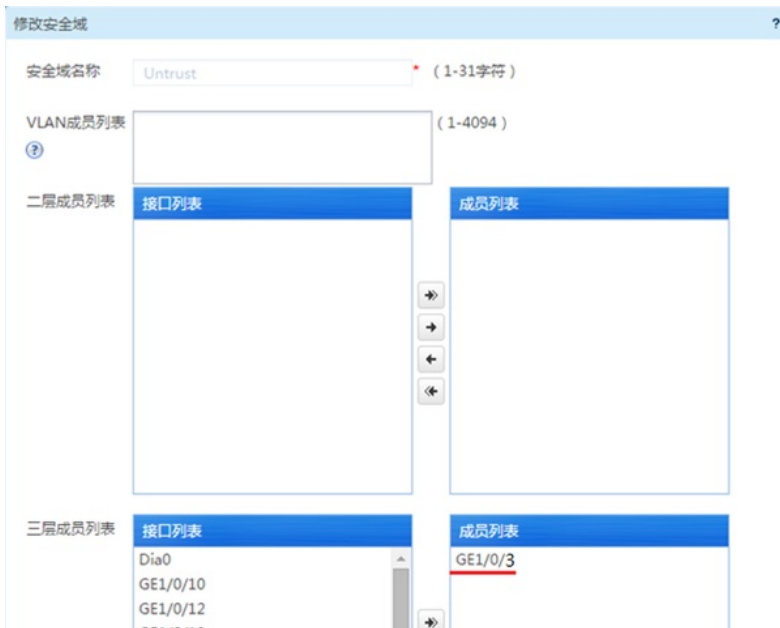


3.5 配置外网接口加入Untrust安全区域

#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1/0/1接口加入成员列表。

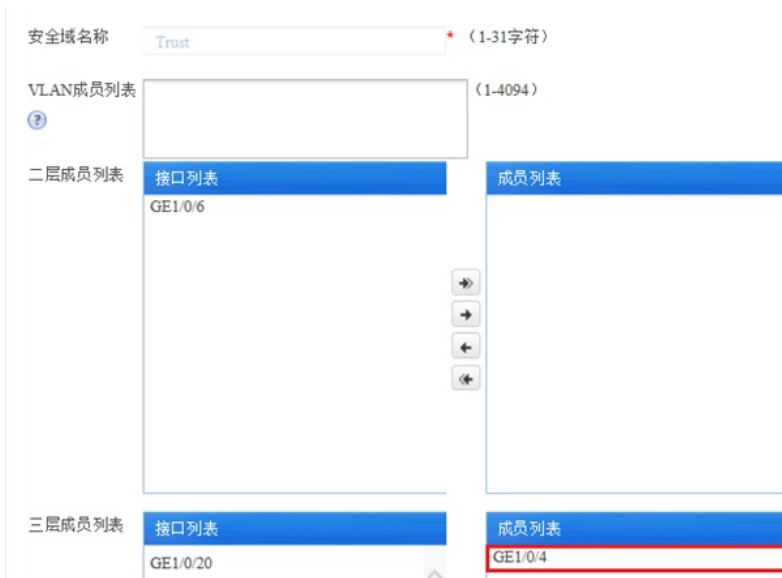


3.6 配置内网接口加入Trust安全区域

#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1/0/4口加入成员列表。

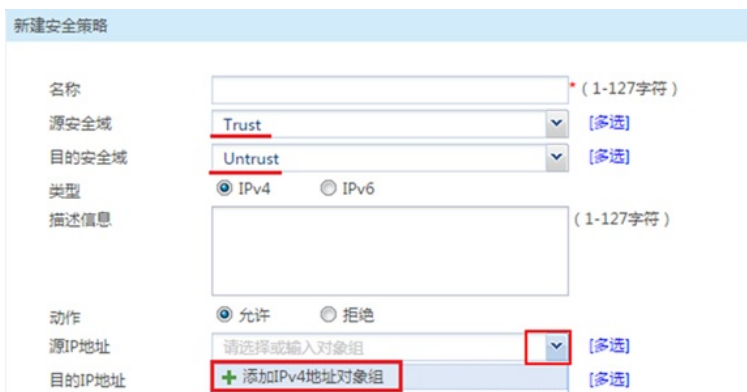


3.7 配置安全策略将Trust到Untrust域内网数据放通

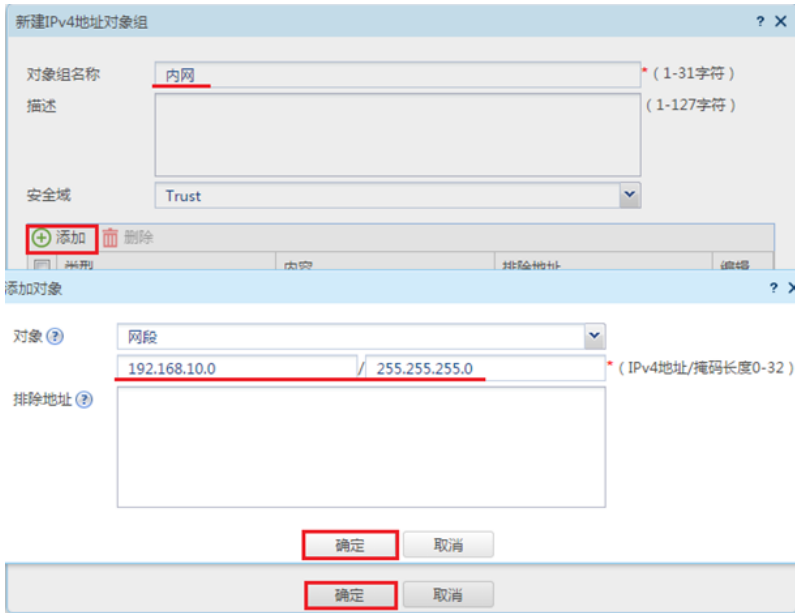
#在“安全策略”中点击“新建”。



#“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。



3.8 配置安全策略将Trust到Local域、Local到Trust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。



#配置成功显示结果，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: Trust, Local [多选]

目的安全域: Local, Trust [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 [多选]

时间段: 请选择时间段 [多选]

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--

确定 取消

3.9 配置安全策略将Untrust到Local域、Local到Untrust域DHCP数据放通策略

#在“安全策略”中点击“新建”按钮创建安全策略，“源安全区域”选择Local、Untrust区域，“目的安全域”选择Local、Untrust区域。”服务“选择DHCP-client、DHCP-server。

新建安全策略

名称: 放通DHCP (1-127字符)

源安全域: Local, Untrust [多选]

目的安全域: Local, Untrust [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: dhcp-client, dhcp-server [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 [多选]

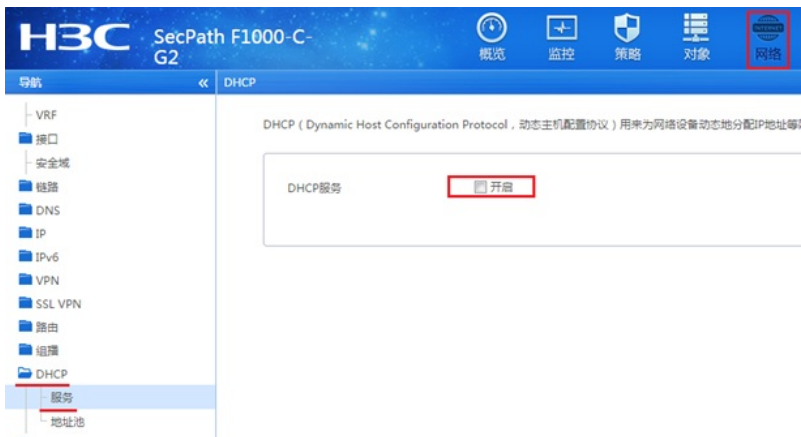
时间段: 请选择时间段 [多选]

VRF: 公网

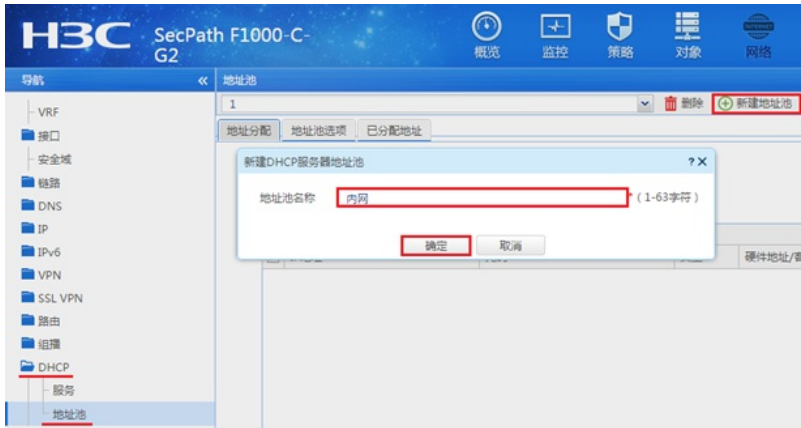
确定 取消

3.10 配置DHCP服务

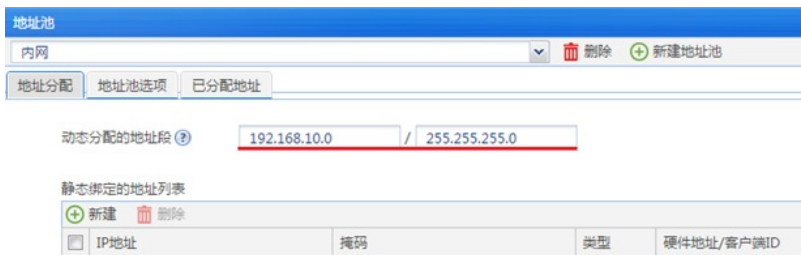
#在“网络”>“DHCP”>“服务”中开启DHCP服务。



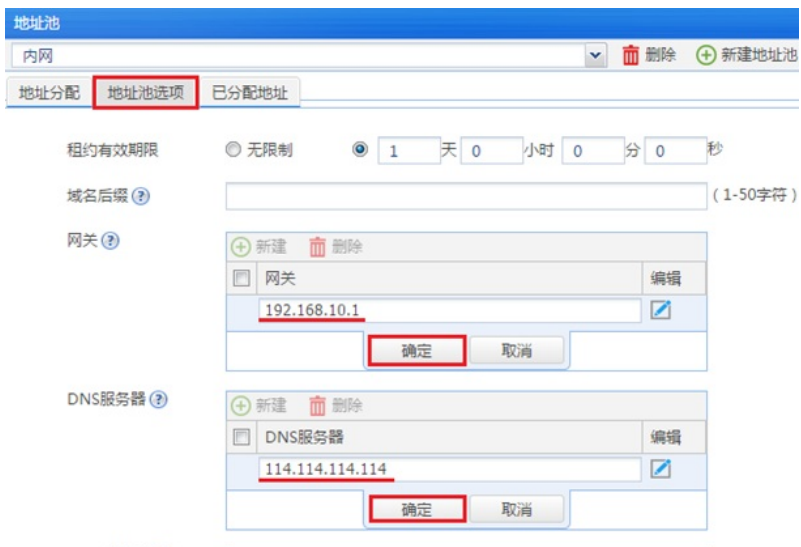
#在“网络”>“DHCP”>“地址池”中新建地址池，名称设定为内网。



#设置“地址分配”的地址段为192.168.10.0后点击“确定”。

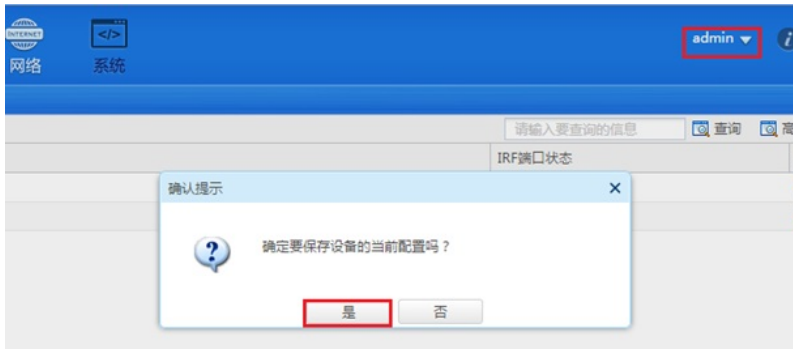


#选择“地址池选项”配置“网关”地址为192.168.10.1点击“确定”按钮，“DNS服务器”地址优先设置当地运营商提供的DNS服务器地址，如果没有提供可以设置114.114.114.114或8.8.8.8等DNS服务器地址，配置完成后点击确定。



3.11 保存配置

在设备右上角选择保存选项，点击“是”按钮完成配置。



3.12 注意事项

防火墙缺省管理地址为192.168.0.0网段，如果核心网下发给防火墙外网接口也是192.168.0.0网段需要防火墙修改0接口管理地址。

配置关键点