

知 防火墙通过Vlan实现内网多端口上网配置方法 (WEB界面)

二层转发 张新姿 2020-12-14 发表

组网及说明

1 配置需求及说明

1.1 适用的产品系列

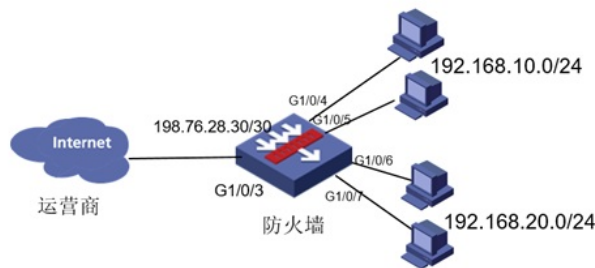
本案例适用于软件平台为Comware V7系列防火墙：如M9006、M9010、M9014等M9K系列的防火墙。

注：本案例是在F1000-C-G2的Version 7.1.064, Release 9333P30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，使用固定IP地址线路接入互联网。运营商提供的IP地址为198.76.28.30/30，网关为198.76.28.29，DNS地址为114.114.114.114。初步规划防火墙使用3接口接入运营商，使用4接口到7接口连接内部网络，4接口和5接口使用192.168.10.0网段，6接口和7接口使用192.168.20.0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：

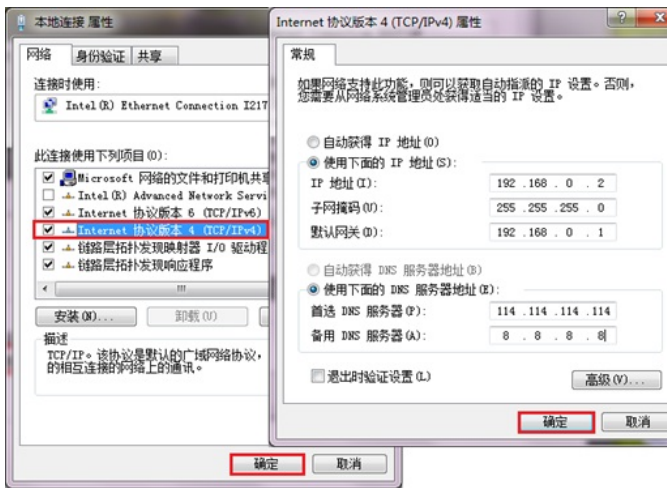
点击电脑右下角电脑图标，选择“打开网络和共享中心”选项。



#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。

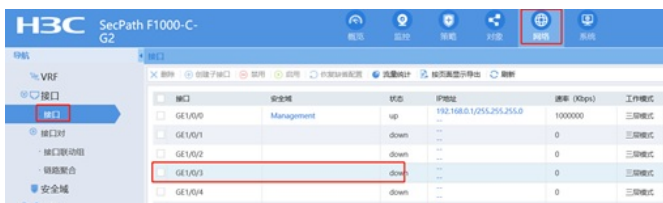


#电脑IP地址配置完成后打开浏览器，在浏览器地址栏中输入<https://192.168.0.1>登录设备管理界面。设备默认用户名密码均为admin。



3.2 配置外网接口

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



#接口加入安全域“untrust”，点击“IP地址/掩码”后面的“编辑”按钮



#“IP地址”填写运营商给的公网地址198.76.28.30，掩码为255.255.255.252。



3.3 配置内网接口G1/0/4和G1/0/5

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



#工作模式选择“二层模式”，选择“是”



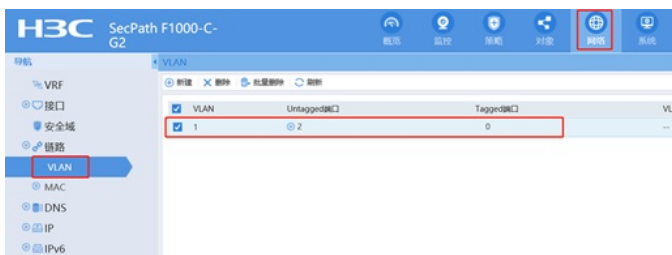
#接口加入安全域“trust”，VLAN填写“1-4094”，点击“确定”



#G1/0/5口配置与G1/0/4相同

3.4 配置内网地址—192.168.10.1

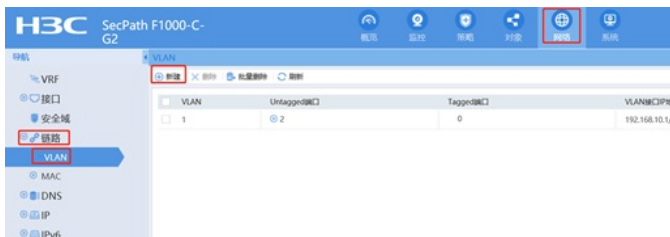
#在“网络”>“链路”>“VLAN”选项中VLAN 1并点击此最后面的“编辑”按钮。



#在“VLAN接口”打上勾，配置接口地址为“192.168.10.1”，掩码为“255.255.255.0”

3.5 创建VLAN 2

#在“网络”>“链路”>“VLAN”选项中点击“新建”按钮。



#VLAN列表写成“2”

#在“网络”>“链路”>“VLAN”选项中VLAN 2并点击此最后面的“编辑”按钮。



#在“VLAN接口”打上勾，配置接口地址为“192.168.20.1”，掩码为“255.255.255.0”

编辑VLAN

VLAN ID: 2

描述: VLAN 0002 (1-255字符)

VLAN接口:

指定IP地址 通过DHCP自动获取IP地址

IPv4地址/掩码: 192.168.20.1 / 255.255.255.0

链路类型: Access

链路类型: Trunk

确定 取消

3.6 配置内网接口G1/0/6和G1/0/7

#在“网络”>“接口”选项中选择1/0/6接口并点击此接口最后面的“编辑”按钮。

接口	安全域	状态	IP地址	速率
<input type="checkbox"/> GE1/0/0	Management	down	192.168.0.1/255.255.255.0	0
<input type="checkbox"/> GE1/0/1		down	...	0
<input type="checkbox"/> GE1/0/2		down	...	0
<input type="checkbox"/> GE1/0/3	Untrust	up	198.76.28.30/255.255.255.252	10000
<input type="checkbox"/> GE1/0/4	Trust	up	...	10000
<input type="checkbox"/> GE1/0/5	Trust	down	...	0
<input checked="" type="checkbox"/> GE1/0/6		down	...	0
<input type="checkbox"/> GE1/0/7		down	...	0

#工作模式选择“二层模式”，选择“是”，接口加入安全域“trust”，VLAN填写“1-4094”，“VLAN相关参数”>“PVID”写成“2”，点击“确定”

修改接口设置

接口: GE1/0/6

加入安全域: Trust

VLAN: 1-4094 (1-4094)

链路状态: Down 禁用

描述: GigabitEthernet1/0/6 Interface (1-255字符)

工作模式: 二层模式 三层模式

MAC地址: D4-61-FE-A4-8E-06

VLAN相关参数

链路类型: Access

PVID: 2

MDIX模式: 自协商

速率: 自协商

确定 取消

#G1/0/7口配置与G1/0/6口配置相同

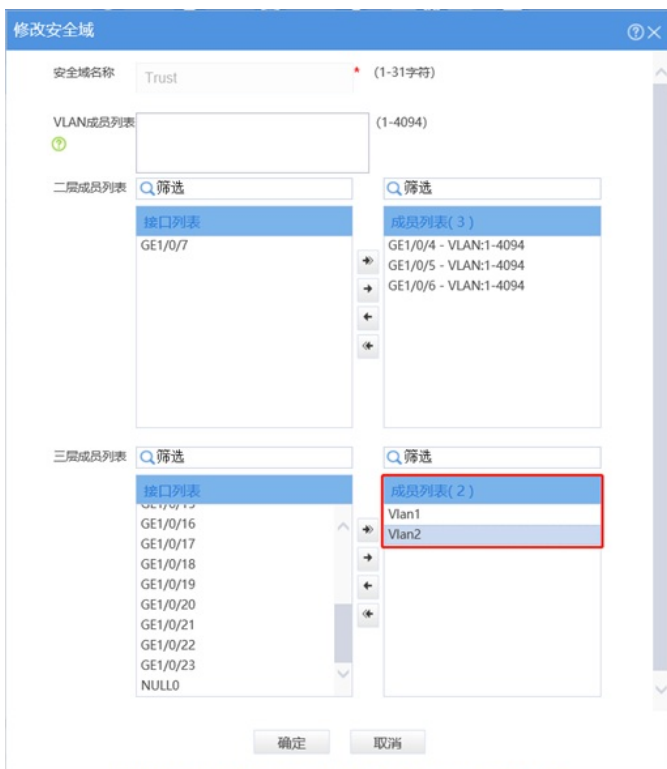


3.7 将虚接口加入安全域

#在“网络”>“安全域”选项中“trust”并点击此最后面的“编辑”按钮。



#将VLAN 1和VLAN 2加入成员列表，点击“确定”

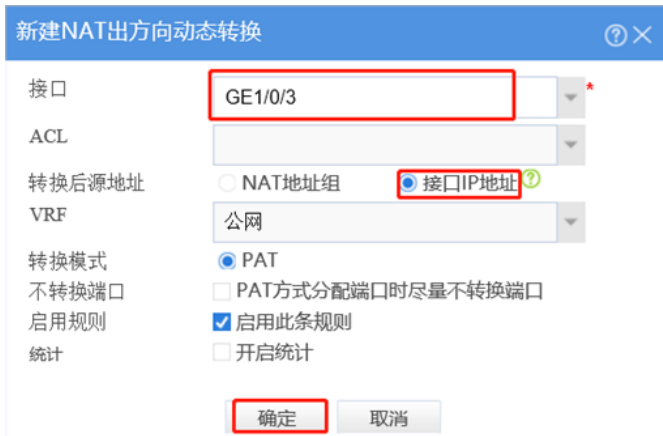


3.8 配置NAT地址转换

#在“策略”>“NAT”>“NAT动态转换”>“NAT出方向动态转换（基于ACL）”选项中点击“新建”。

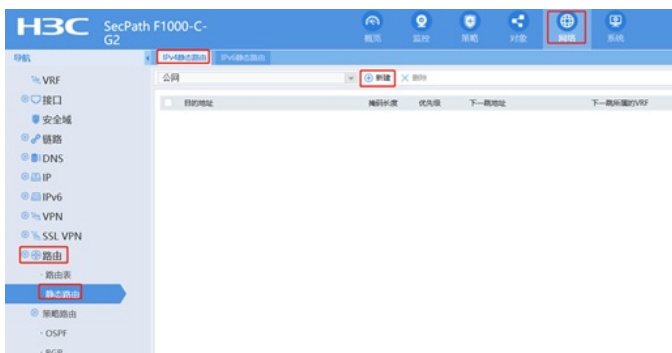


#“接口”选择外网接口1/0/3，转换后源地址选择“接口IP地址”并点击“确定”。



3.9 配置到外网网关的静态路由

#在“网络”>“路由”>“静态路由”>“IPv4静态路由”中点击“新建”静态路由。



#“目的IP地址”配置为0.0.0.0，“掩码长度”选择0，“下一跳”地址填公网网关。

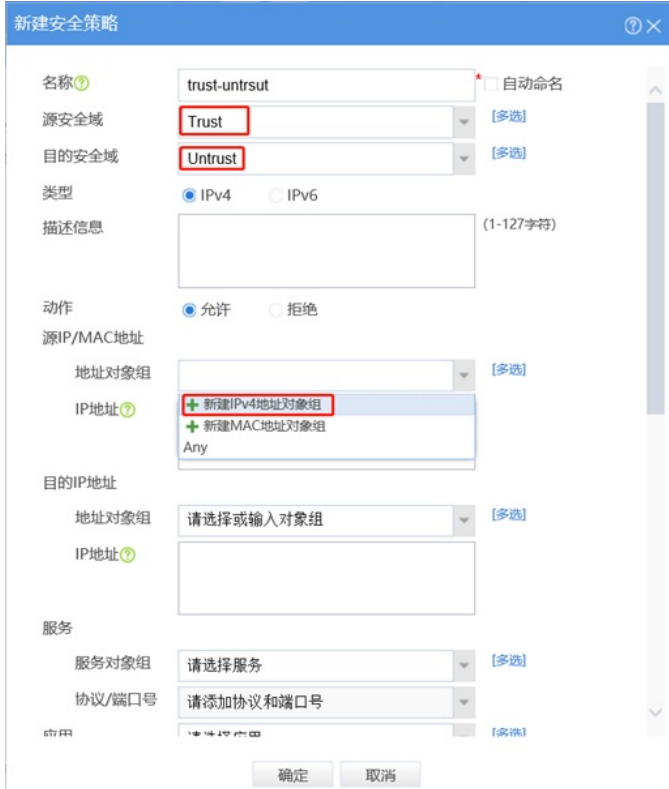


3.10 配置安全策略将Trust到Untrust域内网数据放通

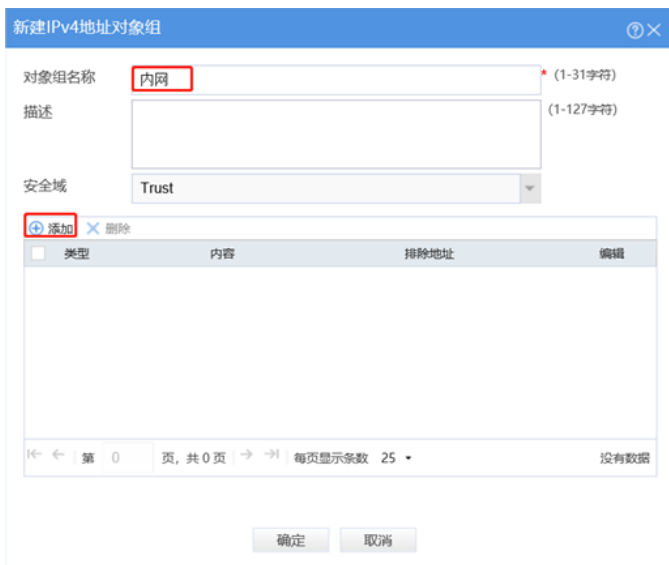
#在“策略”>“安全策略”中点击“新建”。

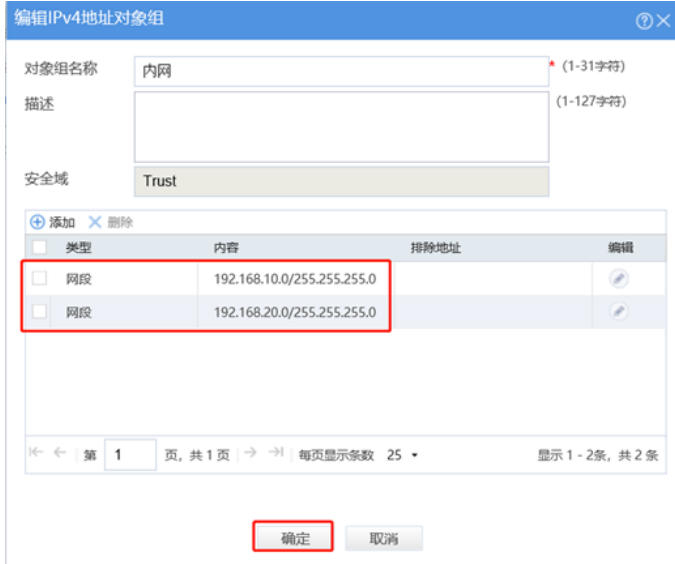
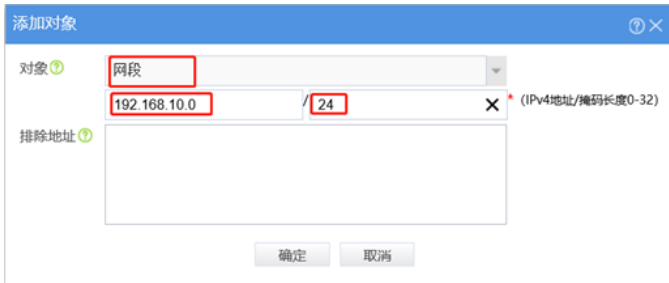


#“源安全域”选择Trust，“目的安全域”选择Untrust，在“源IP/MAC地址”>“IP地址”选择“新建 IPv4地址对象组”。



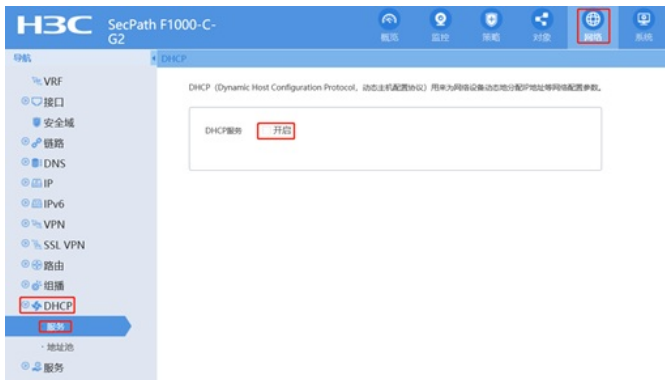
#对象组名称输入内网，点击“添加按钮”添加地址对象，添加内网192.168.10.0和192.168.20.0网段。点击“确定”完成策略配置。



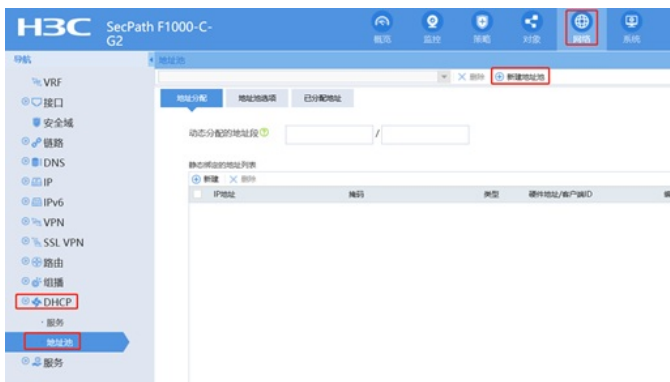


3.11 配置DHCP服务

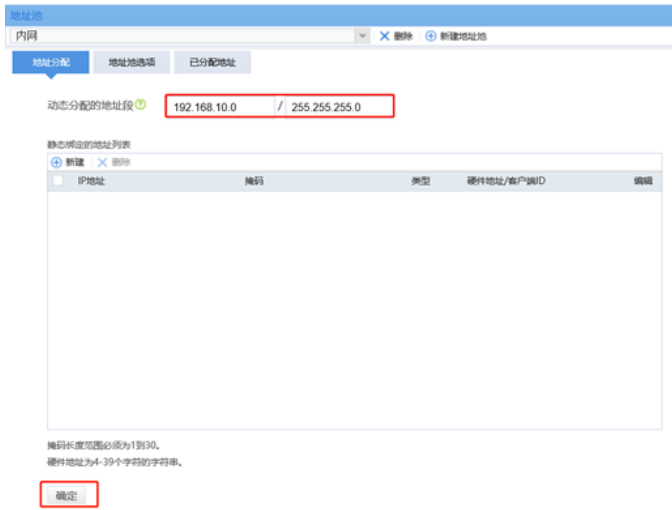
#在“网络”>“DHCP”>“服务”中开启DHCP服务。



#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”。



#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，配置完成后点击最下面“确定”。



#192.168.20.0对应的地址池配置与192.168.10.0网段相同，只需要修改“动态分配的地址段”为192.168.20.0/255.255.255.0，修改“网关”为192.168.20.1

3.12 配置安全策略将Trust到Local域、Local到Trust域数据全放通策略

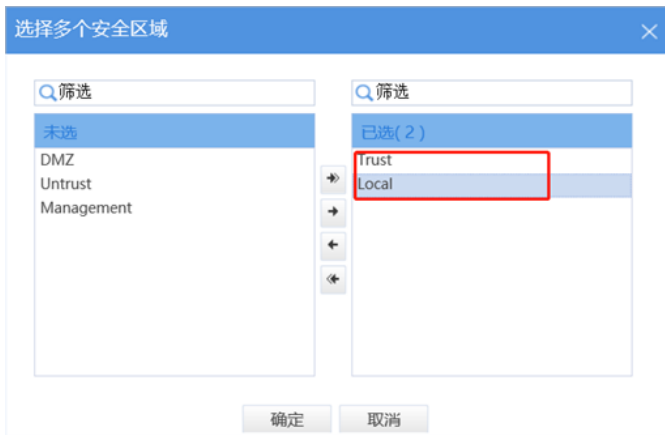
#在“策略”>“安全策略”中点击“新建”。



#创建策略名称为DHCP，源安全域、目的安全域选择多选，并选中Local、Ttrust。



#将“trust”和“local”加入“已选”



#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 自动命名

源安全域 [多选]

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/MAC地址

地址对象组 [多选]

IP地址

目的IP地址

地址对象组 [多选]

IP地址

服务

服务对象组 [多选]

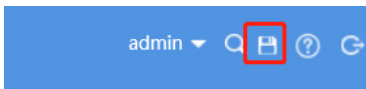
协议/端口号 [多选]

应用 [多选]

确定 取消

3.13 保存配置

在设备右上角选择“保存”选项，点击“是”完成配置。



配置关键点

无