防火墙下接交换机单臂路由配置方法（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

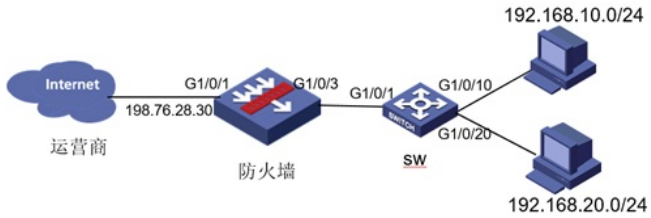
本案例适用于软件平台为Comware V7系列防火墙：如F1000-A-G2、F1000-S-G2、F100-M-G2、F100-S-G2等F1000-X-G2、F100-X-G2系列的防火墙。

注：本案例是在F1000-C-G2的Version 7.1.064, Release 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1接口接入运营商，使用3接口连接内网二层交换机，电脑接到交换机10口可以获取192.168.10.0网段地址上网，接到交换机20口可以获取192.168.20.0网段地址上网。

2 组网图



配置步骤

3 配置步骤

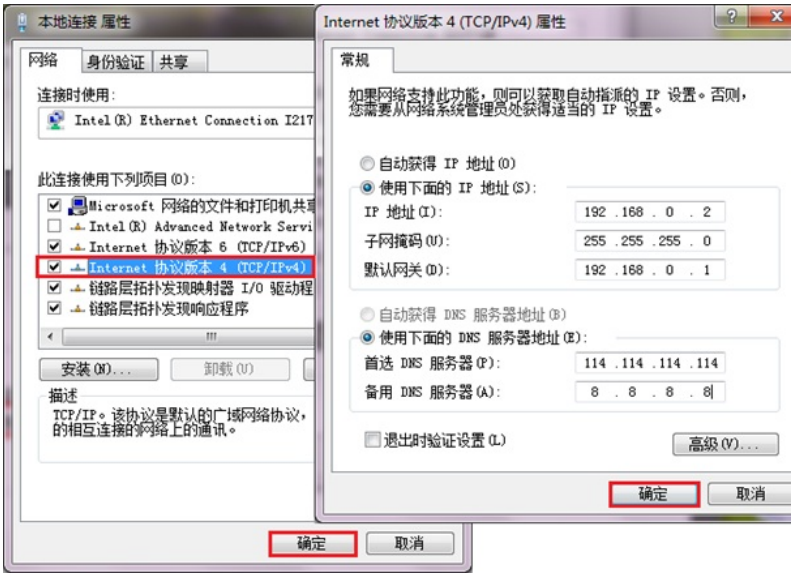
3.1 基本登录

#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1/0/1接口并点击此接口最后面的”编辑”按钮。

#接口加入安全域“untrusrt”，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。

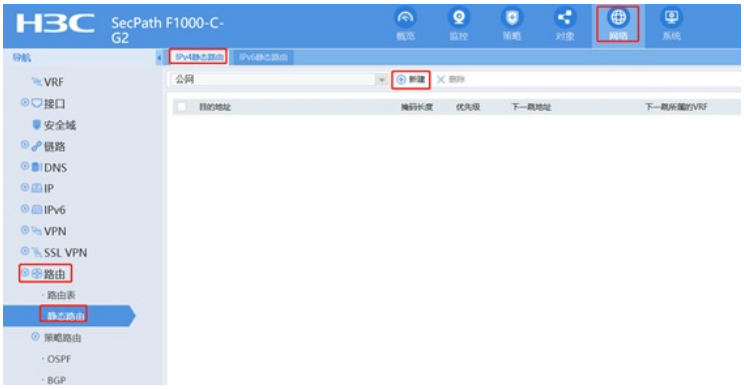
3.3 配置NAT地址转换

#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1/0/1，转换后源地址选择“接口IP地址”并点击“确定”。

3.4 配置到外网网关的静态路由

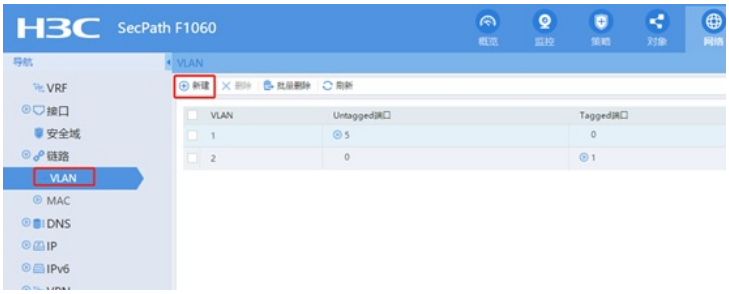
#在“网络”>“路由”>“静态路由”>“IPv4静态路由”中点击”新建”静态路由。



#“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。

3.5 配置内网网段--VLAN10

#在“网络”>“链路”>“VLAN”中点击“新建”，新建VLAN 10

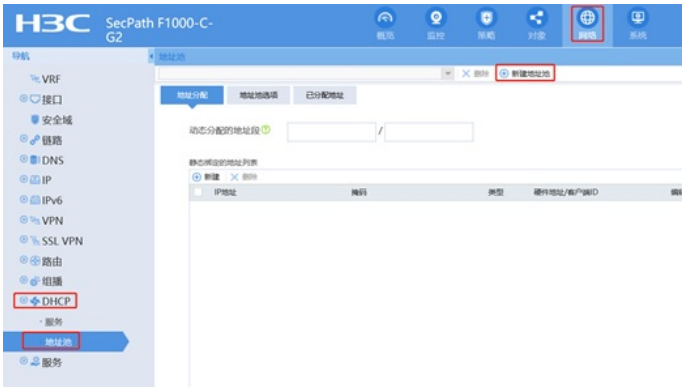


#点击VLAN10后面的“编辑”，勾选“VLAN接口”配置指定IP地址192.168.10.1，掩码是255.255.255.0

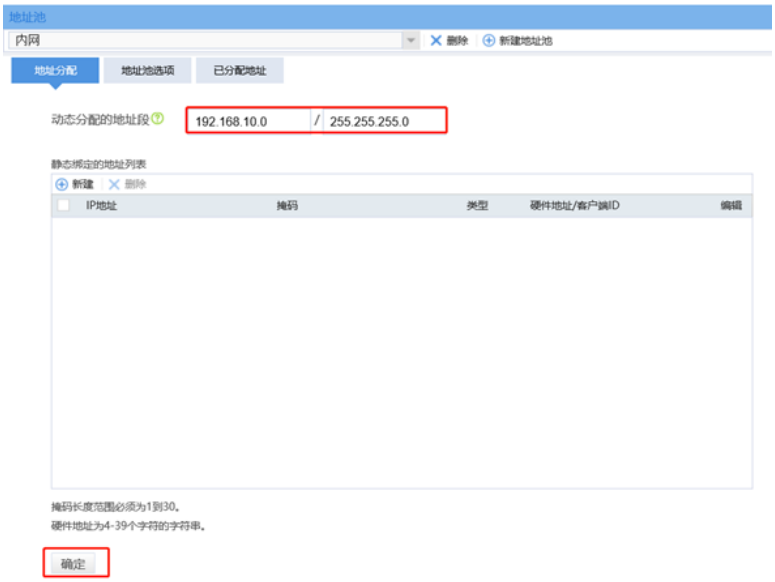
3.6 配置VLAN10的DHCP

#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”。



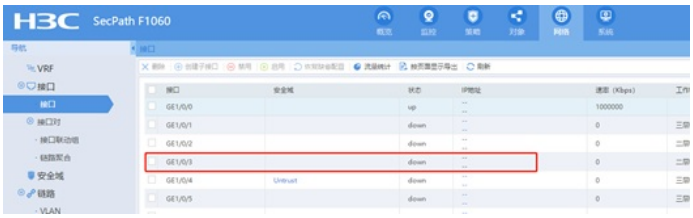
#选择“地址池选项”配置“网关”地址为192.168.10.1点击“确定”按钮，“DNS服务器”地址优先设置当地运营商提供的DNS服务器地址，如果没有提供可以设置114.114.114.114或8.8.8.8等DNS服务器地址，配置完成后点击最下面“确定”。

3.7 配置内网网段-VLAN20以及DHCP

配置步骤参考3.5和3.6，修改VLAN的ID和IP地址，配置dhcp的时候，新建一个其他名称的地址池，配置对应的地址段，网关和DNS即可。

3.8 配置内网物理接口

#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。

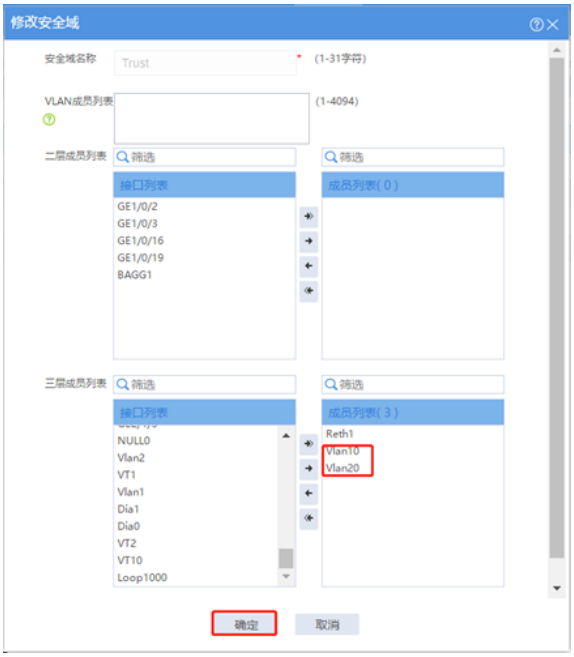


#工作模式先选择二层模式，安全域选择“trust”，VLAN写“1-4094”，链路类型选择“trunk”，permit VLAN填写“10,20”

3.9 VLAN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 10和VLAN 20加入成员列表，点击“确定”

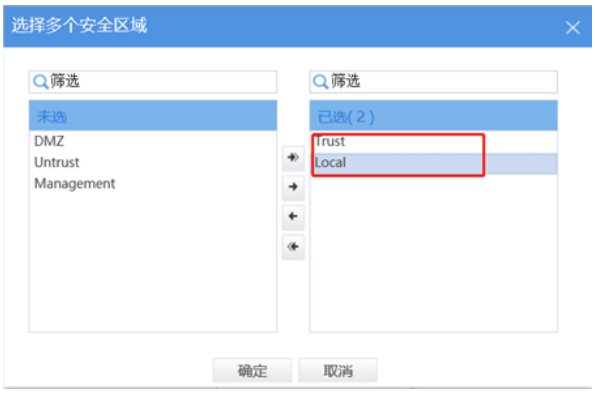


3.10 配置安全策略将Trust到Local域、Local到Trust域数据全放通策略

#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、trust。

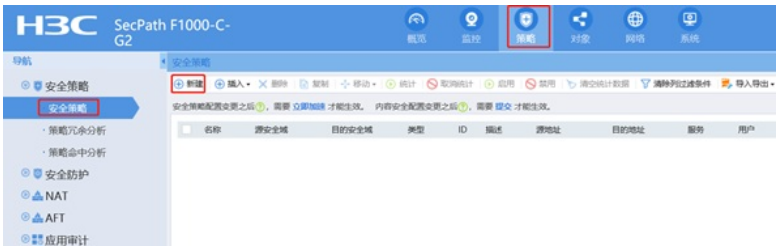
#将“trust”和“local”加入“已选”



#策略配置如下图所示，点击“确定”完成策略配置。

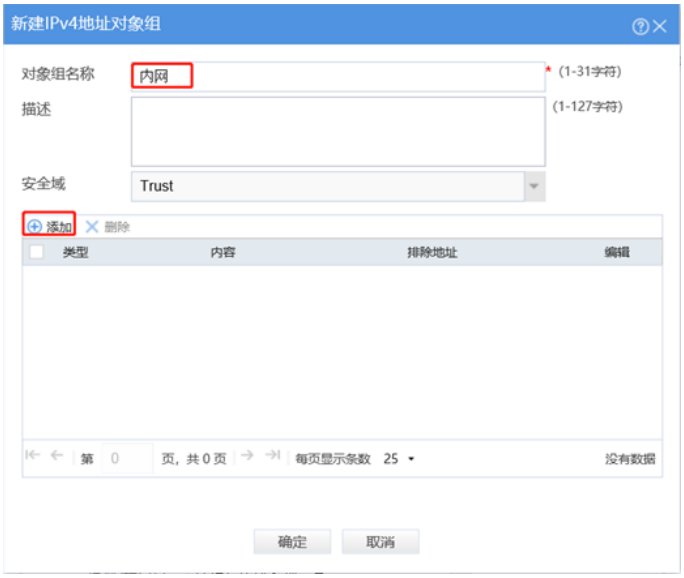
3.11 配置安全策略将Trust到Untrust域内网数据放通

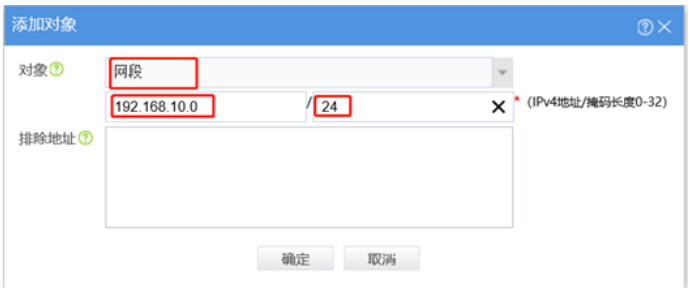
#在“策略”>“安全策略”中点击“新建”。

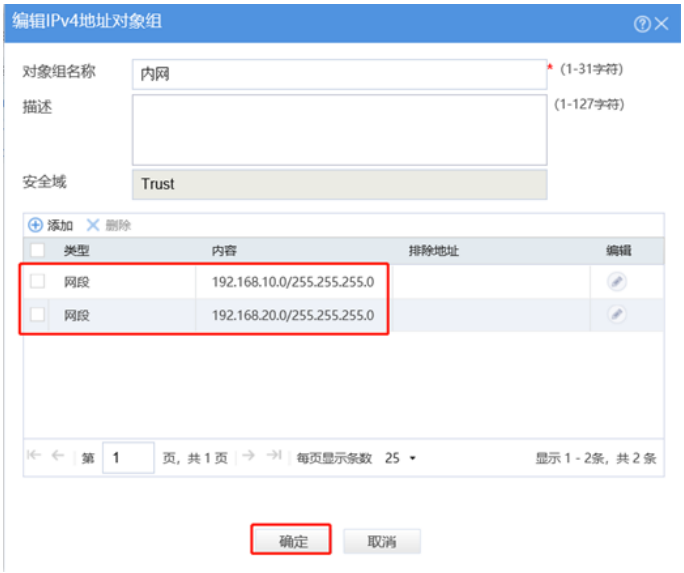


#“源安全域”选择Trust，“目的安全域”选择Untrust，在“源IP/MAC地址”>“IP地址”选择“新建 IPV4地址对象组”。

#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。

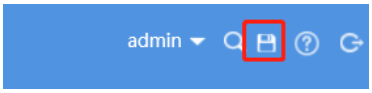






3.12 保存配置

在设备右上角选择“保存”选项，点击”是”完成配置。



3.13 交换机端配置

#创建vlan

<H3C>system-view

[H3C]vlan 10

[H3C-vlan10]quit

[H3C]vlan 20

[H3C-vlan20]quit

#将连接路由器的接口切换成trunk口，并放通所有vlan

[H3C]interface GigabitEthernet 1/0/1

[H3C-GigabitEthernet1/0/1]port link-type trunk

[H3C-GigabitEthernet1/0/1]port trunk permit vlan all

[H3C-GigabitEthernet1/0/1]quit

#将连接PC1和PC2接口划分到相应的vlan中
[H3C]interface GigabitEthernet 1/0/10
[H3C-GigabitEthernet1/0/10] port access vlan 10
[H3C-GigabitEthernet1/0/10] interface GigabitEthernet 1/0/20
[H3C-GigabitEthernet1/0/20] port access vlan 20
#保存配置
[H3C]save force

配置关键点

无