F1000-X-G2/F100-X-G2系列防火墙内网用户通过公网地址访问内部服务器配置方法（WEB界面）

NAT　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

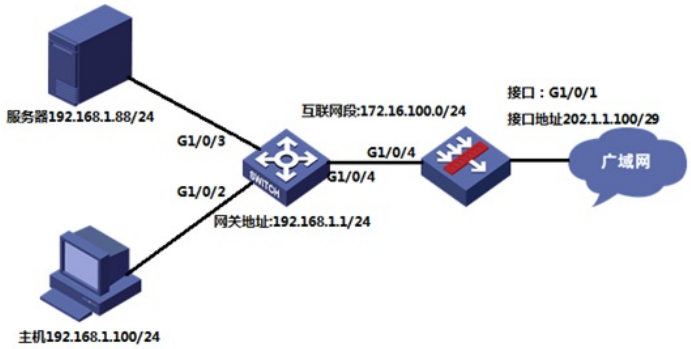
本案例适用于软件平台为Comware V7系列防火墙：F100-X-G2、F1000-X-G2、F100-X-WiNet、F1000-AK、F10X0等。

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

防火墙部署在互联网出口，内网有一台OA服务器通过防火墙发布了8081端口，并且外网用户访问对应服务正常。目前需要实现内网用户也能通过公网地址去访问内部服务器的需求。

2 组网图



配置步骤

3 配置步骤

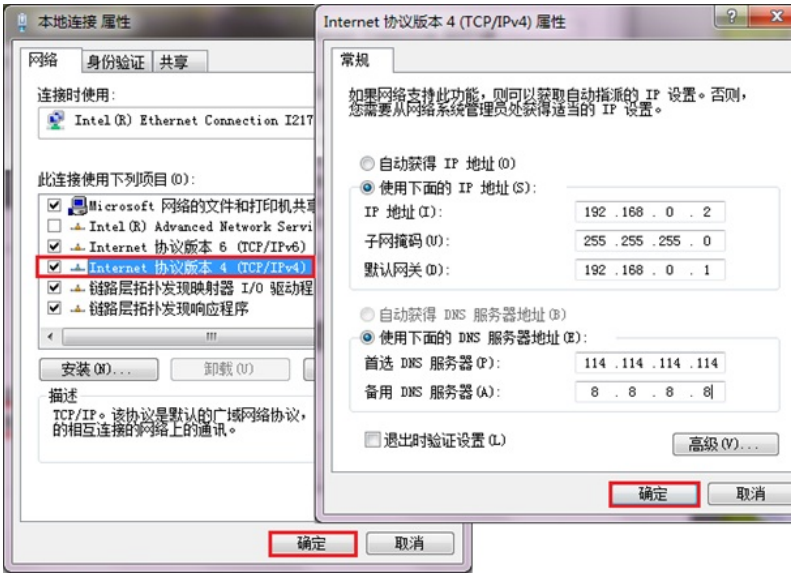
3.1 基本登录

#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。

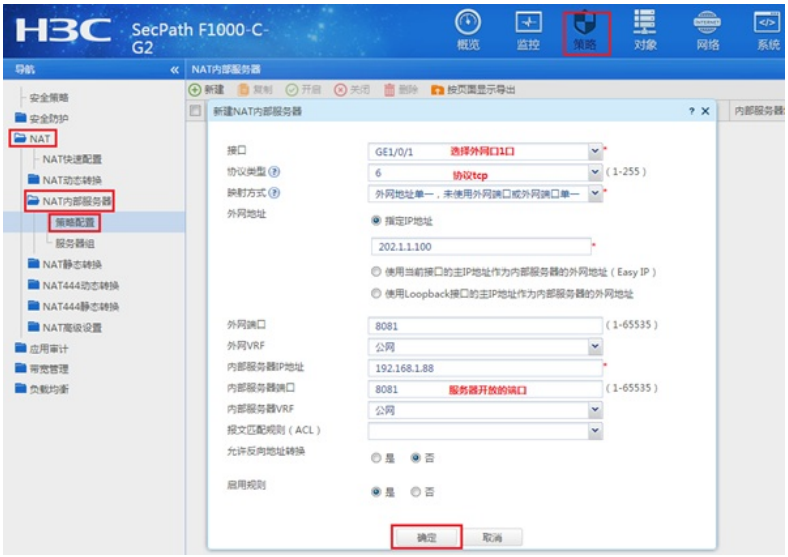


#电脑IP地址配置完成后打开浏览器，在浏览器地址栏中输入https://192.168.0.1登录设备管理界面。设备默认用户名密码均为admin。

3.2 配置内部服务器（端口映射）

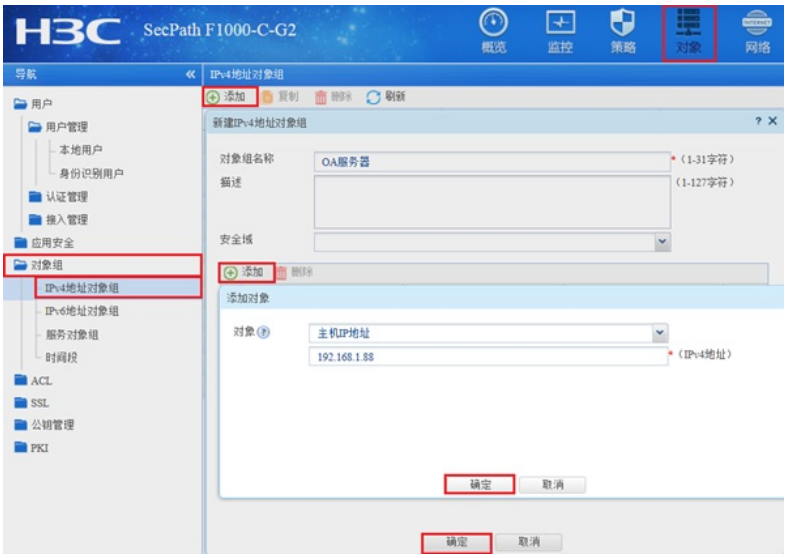
#点击“策略”>“NAT”>“NAT内部服务器”>“策略配置”中新建NAT内部服务器。

“接口”选择外网1/0/1接口，“协议类型”选择6（TCP协议），“外网地址”填写1/0/1接口真实地址，“外网端口”填写要发布的8081端口，“内网服务器IP地址”添加真实服务器地址，“内部服务器端口”填写8081端口。



3.3 创建Untrust到Trust域间策略，放通目的地址为192.168.1.88端口为8081的访问规则。

#创建地址对象：点击“对象”>“对象组”>“IPV4地址对象组”添加IPV4地址对象。“对象”选择“主机IP地址”填入服务器IP地址192.168.1.88。

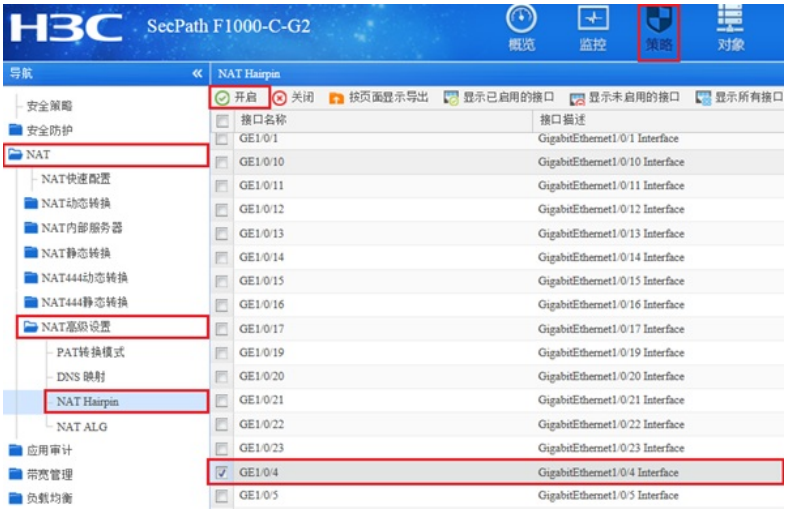


#创建服务器对象：点击“对象”>“对象组”>“服务对象组”添加服务对象。“对象”选择“协议类型”，“目的端口”起始终止端口均选择8081。

#创建安全策略：点击 “策略”>“安全策略”新建安全策略，“源安全域”选择Untrust域，“目的安全域”选择Trust域，“目的IP地址”选择OA服务器地址对象，“服务”选择8081服务对象，点击“确定”完成策略配置。

3.4 内网接口开启NAT Hairpin功能

#点击“策略”>“NAT”>“NAT高级设置”>“NAT Hairpin”中找到1/0/4接口开启NAT Hairpin功能。



3.5 配置安全策略将Trust域和Local域之间的数据全放通

#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。

#策略配置如下图所示，点击“确定”完成策略配置。

3.6 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