本电子书由CyberArticle制作。点击这里下载CyberArticle。注册版本不会显示该信息。 删除广告

本电子书由CyberArticle制作。点击这里下载CyberArticle。注册版本不会显示该信息。 删除广告

防火墙L2TP VPN的配置方法（WEB）

目录

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F1060的Version 7.1.064, Release 9333P17版本上进行配置和验证的。

1.2 配置需求及实现的效果

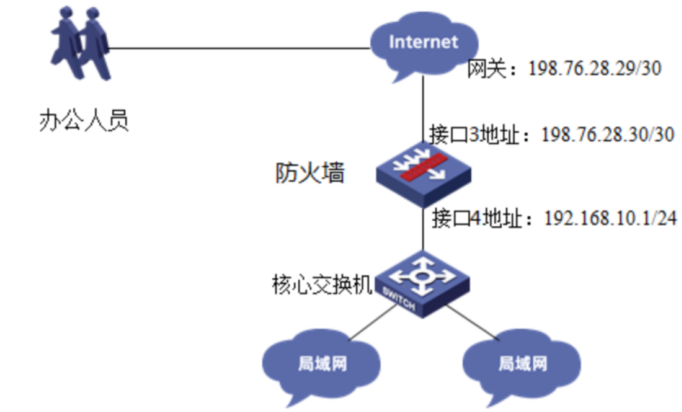
防火墙采用固定IP地址的方式部署在公司互联网出口，运营商提供的IP地址为198.76.28.30/30，网关为198.76.28.29，DNS地址为221.228.255.1。初步规划防火墙使用3接口接入运营商，使用4接口连接内部网络，内部网络使用192.168.10.0网段。

需求：

1）要求内网终端可以自动获取到地址并可以访问互联网。

2）公司外部办公人员需要通过拨号VPN连入公司内网。

2 组网图



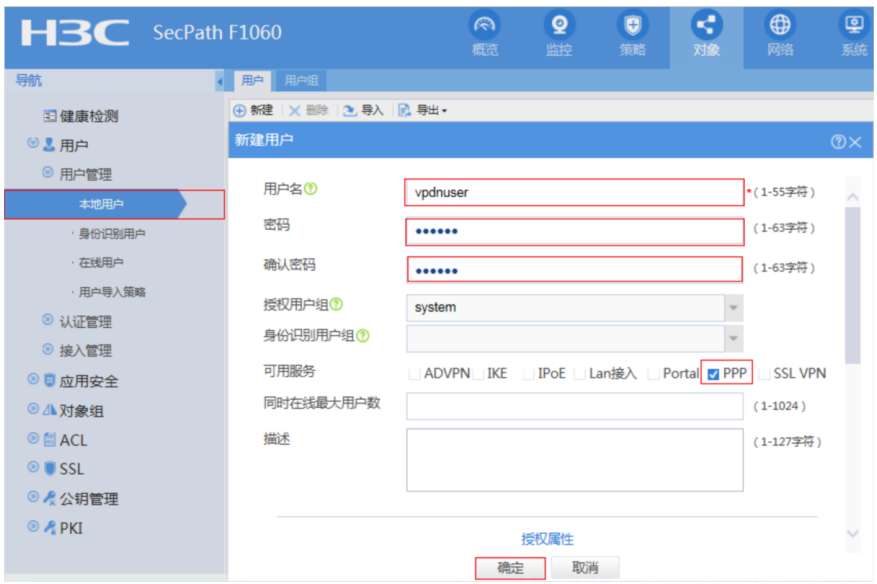
3 配置步骤

3.1 基本网络配置

本章节重点描述VPN配置方法，上网配置略。

3.2 建立VPN拨号账户

#在“对象”>“用户”>“用户管理”>“本地用户”中新建用户，设置用户名为“vpdnuser”、密码为“hello”、服务类型设置为“PPP”，完成后点击确定完成配置。



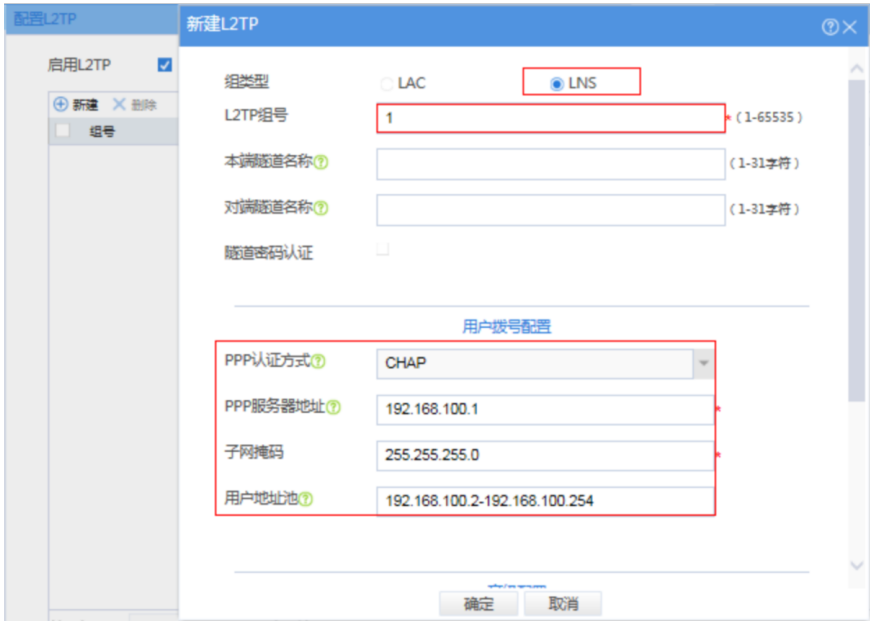
3.3 开启L2TP功能

#在“网络”>“VPN”>“L2TP”选项中启用L2TP VPN功能。

3.4 配置L2TP VPN服务端

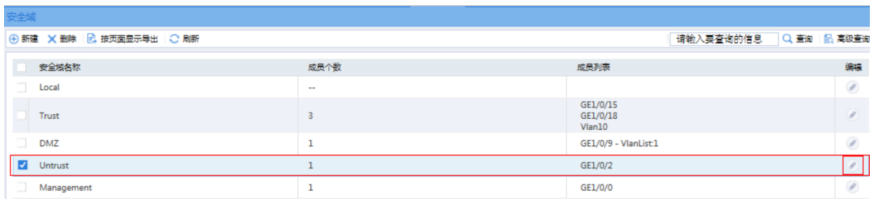
#开启VPN后在“网络”>“VPN”>“L2TP”点击新建L2TP，组类型选择“LNS”、L2TP组号设置为1（若使用Windows客户端则此编号必须为1）、PPP认证方式选择为“CHAP”、PPP服务器地址设置

为“192.168.100.1”、子网掩码为“255.255.255.0”、用户地址池为“192.168.100.2-192.168.100.254”。

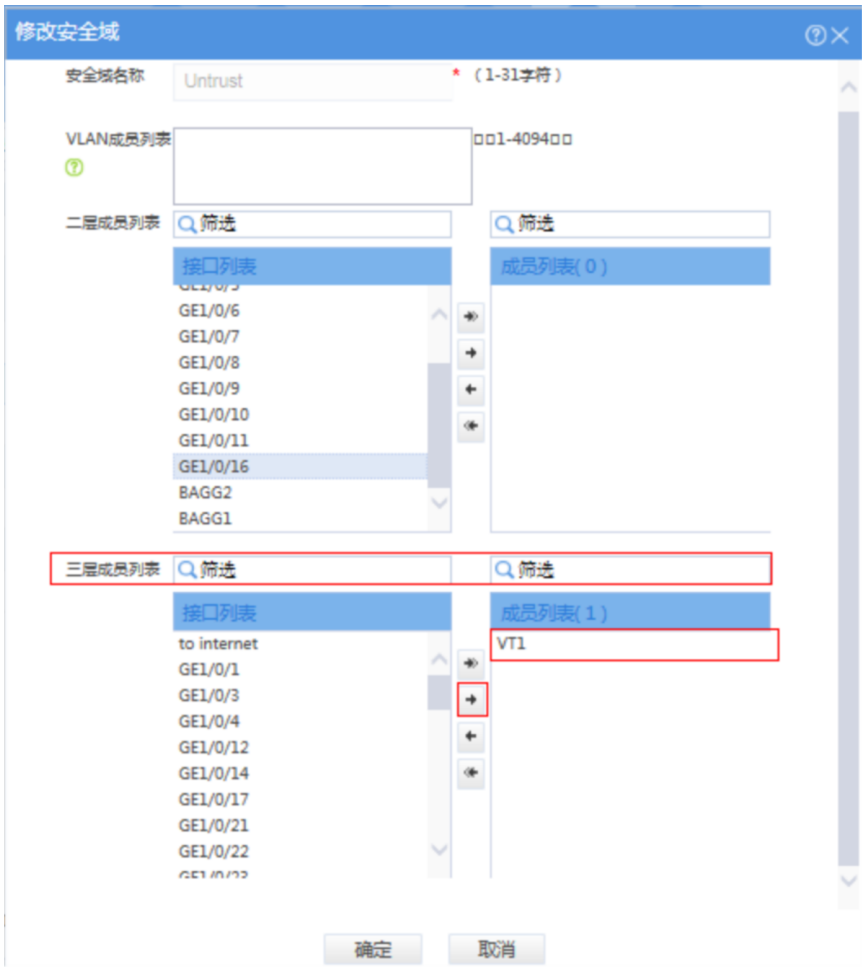


3.5 将L2TP 虚接口加入Untrust安全域

#L2TP默认会生成VT1接口作为L2TP VPN网关，进入“网络”>”安全域”中编辑“Untrust”域。



在三层成员列表中将VT接口移动至成员列表，表示VT1 接口已经加入了“Untrust”安全域。

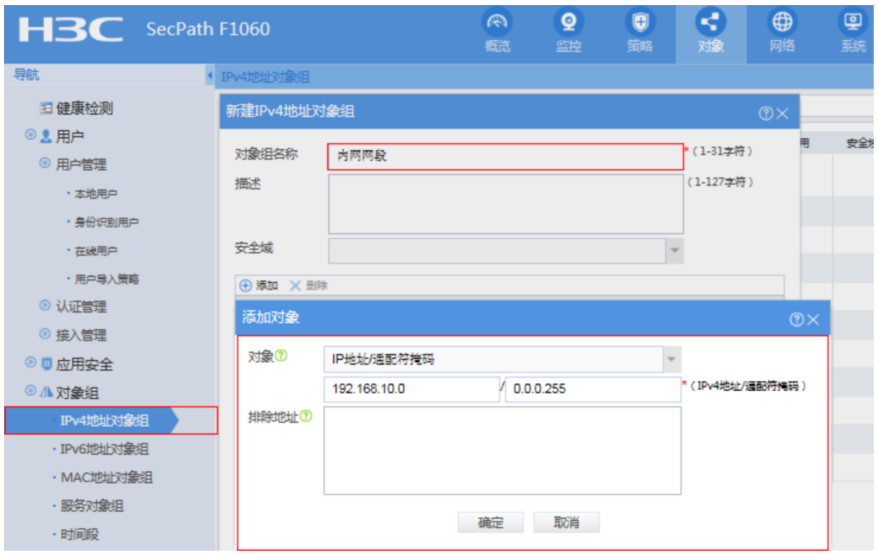


3.6 配置安全策略将Untrust到Local域目的端口为UDP1701端口放通。

#在”策略”>“安全策略”>中添加安全策略，名称定义为“l2tp”、源安全区域选择为”untrust”、目的安全区域选择为”local”、服务选择”l2tp”。

3.7 配置安全策略将Untrust到trust访问内网资源的数据放通

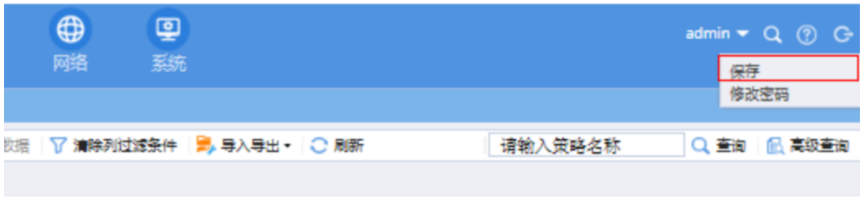
#在”对象”>“对象组”>“IPV4地址对象组”中新建，对象组名称设置为”内网网段”、添加地址对象192.168.10.0网段。



#在”策略”>“安全策略”>中添加安全策略，名称定义为“pass”、源安全区域选择为”untrust”、目的安全区域选择为”trust”、目的IP地址选择之前配置好的地址对象“内网网段”。

3.8 保存配置

#在设备右上角点击“保存”按钮，保存当前配置。



4 VPN客户端配置

4.1 Windows 7电脑拨号配置

#点击电脑右下角电脑图标，选择“打开网络和共享中心”选项。

#点击“设置新的连接或者网络”。

#点击“连接到工作区”。

#选择“使用我的Internet连接（VPN）”。

#点击“我将稍后设置Internet连接”

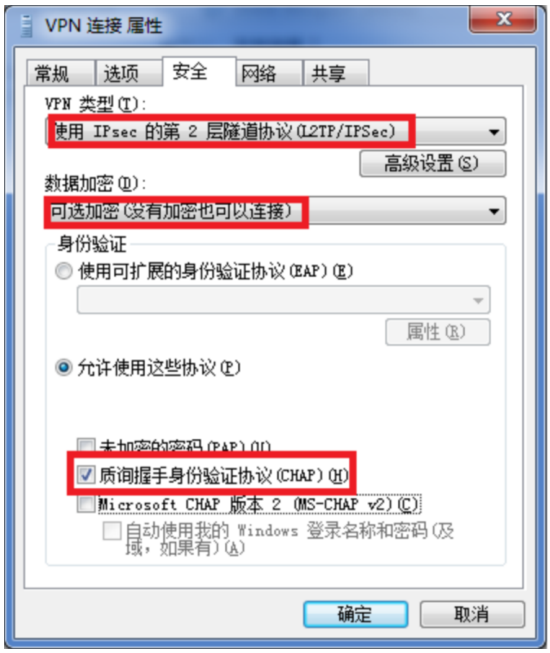
#“Internet地址”置防火墙外网接口的IP地址。

#设置用于VPN拨号的用户名和密码

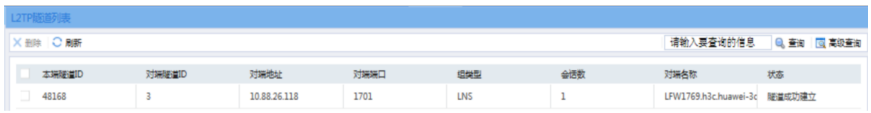
#再次单击电脑桌面右下角的电脑图标，鼠标右击点击“属性”按钮。

#在“安全”页签中选择VPN类型为“使用IPsec的第2层隧道协议

（L2TP/IPSEC）”,数据加密选择“可选加密”，允许协议选择“质询握手身份验证协议（CHAP）”。



拨号成功后设备侧提示：

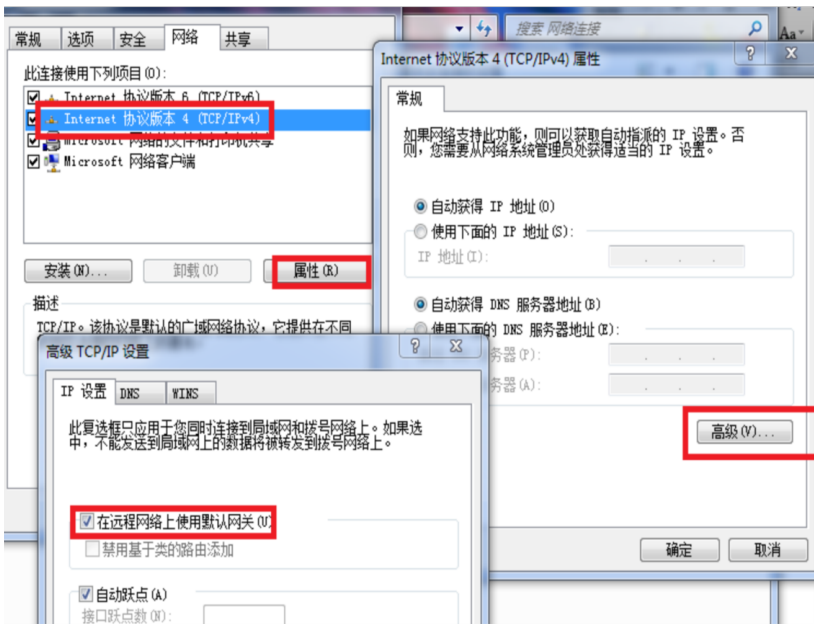


4.2 Windows 7电脑拨号常见问题

4.2.1 连接VPN后无法连接外网

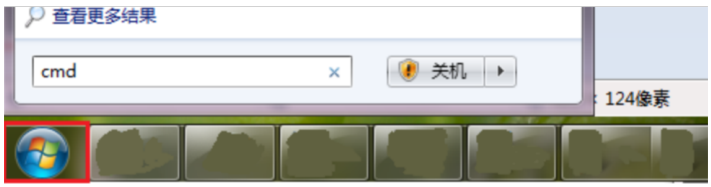
#VPN拨号成功后会在电脑路由表中生成一条到VPN网关的默认路由，其优先级高于电脑自身网关的默认路由。如果即想访问VPN又想上网请参考下面配置。

去掉“在远程网络上使用默认的网关”勾选。



#在电脑添加到对端内网的明细路由。

#打开电脑命令提示图窗口，输入CMD命令。



#增加目的地址为192.168.10.0（防火墙内网地址段），掩码为255.255.255.0，网关地址为192.168.100.1的路由。