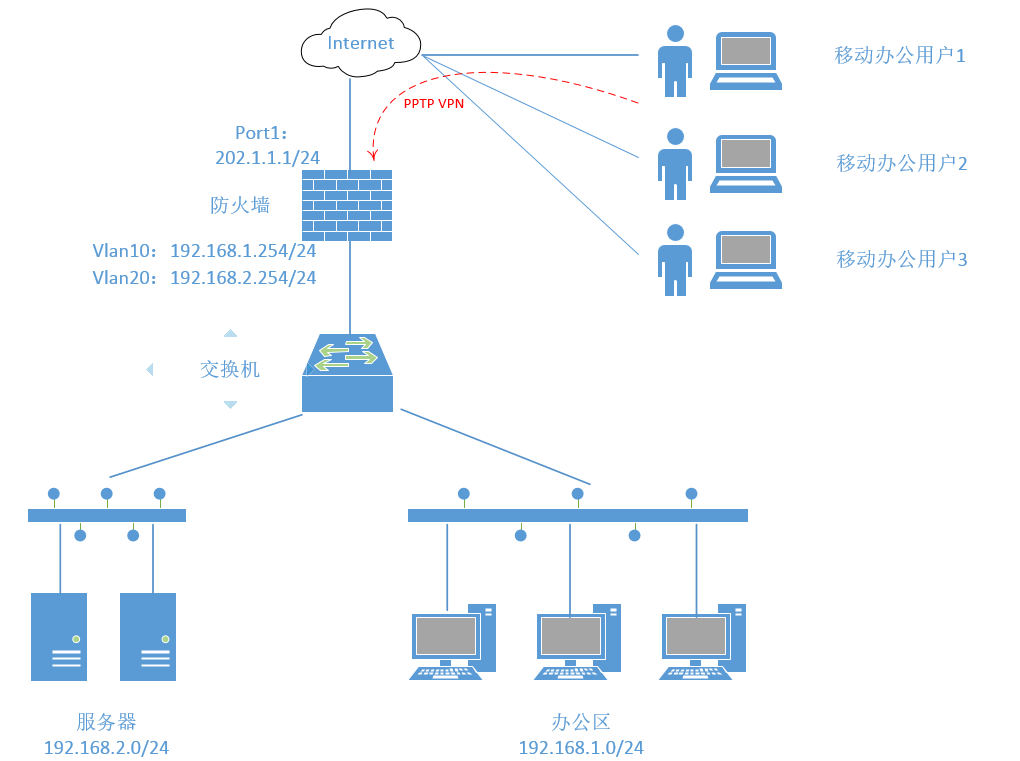
# PPTP VPN配置案例

## 组网需求

* 办公区用户可以正常访问互联网；
* 办公区用户可以正常访问服务器；
* 移动办公用户1需要访问内部服务器；
* 用户2需要VPN进入公司内部，并从内部访问互联网；
* 用户3可以访问内部服务器并从公司内部访问外网。

## 网络拓扑

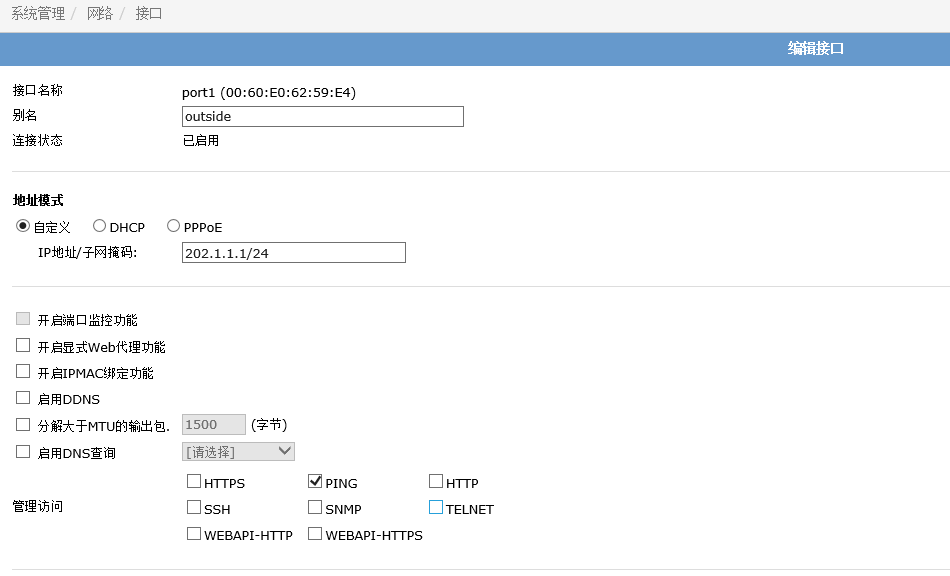
* 办公区使用网段192.168.1.0/24；
* 服务器区使用网段192.1682.0/24；
* 防火墙内网口配置VLAN1和VLAN2，并配置办公区和服务器的网关192.168.1.254/24和192.168.2.254/24；
* 防火墙外网口配置公网地址：202.1.1.1/24；



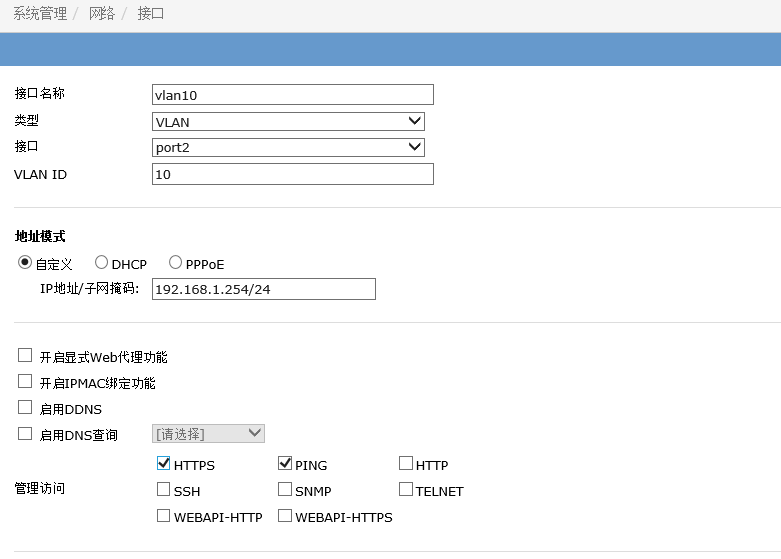
## 配置步骤

### 防火墙配置

1，登陆防火墙，进入“系统管理>网络>接口”页面，配置外网口地址：202.1.1.1/24；



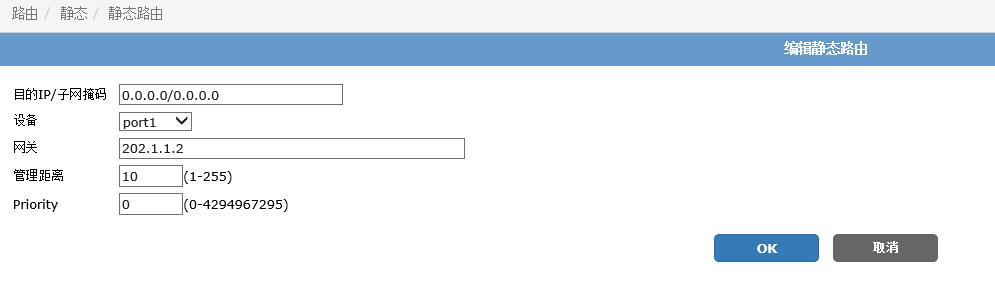
2，在Port2端口下新建VLAN10，并配置地址：192.168.1.254/24；



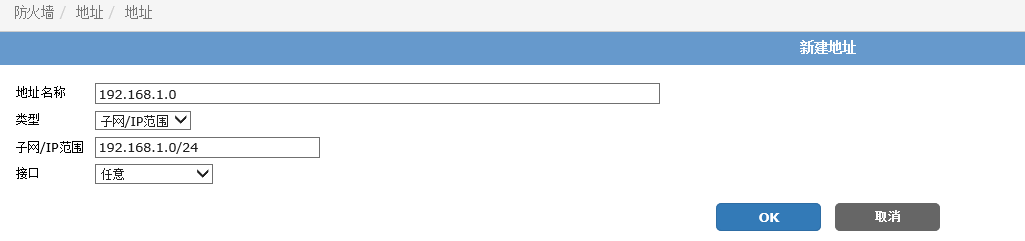
3，在Port2端口下新建VLAN20，并配置地址：192.168.2.254/24；

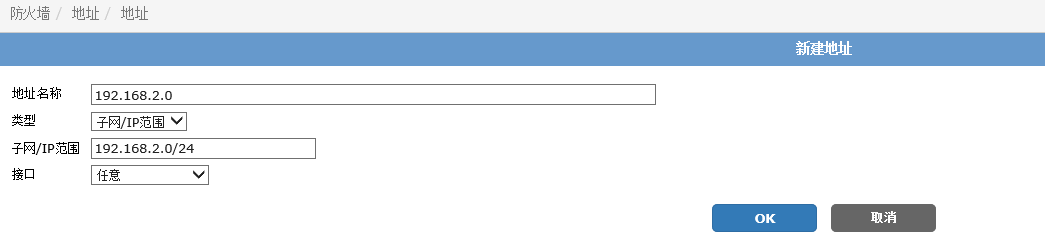


4，进入“路由>静态>静态路由”页面，配置默认路由。

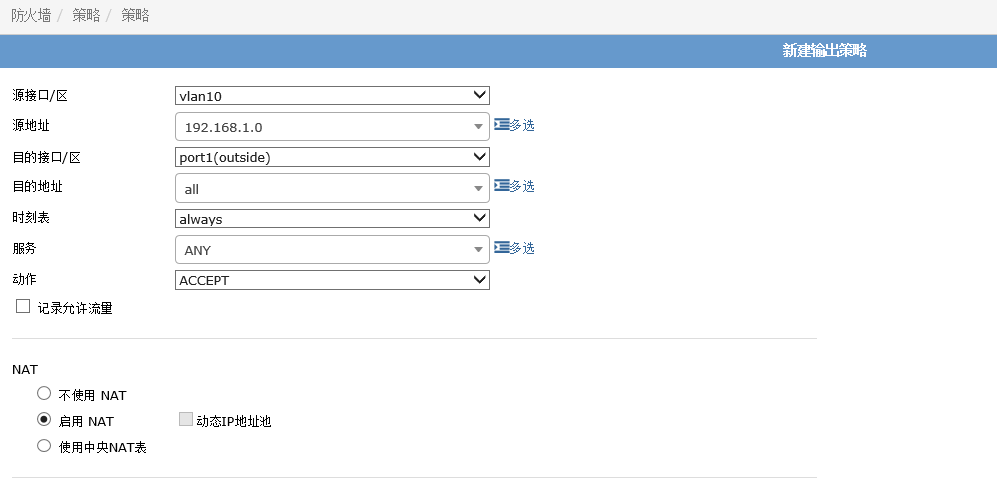


5，进入“防火墙>地址>地址”页面，单击“创建”按钮新建内网地址段。

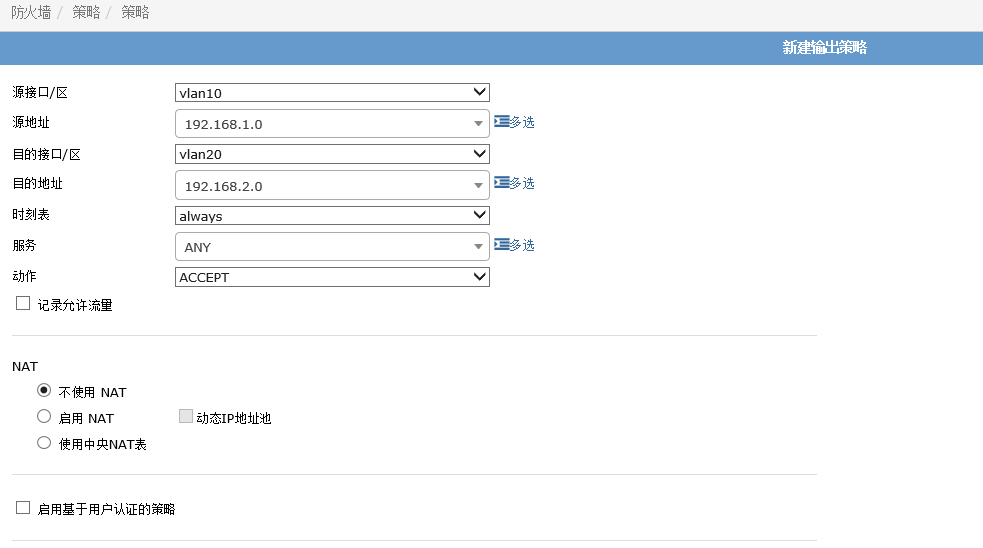




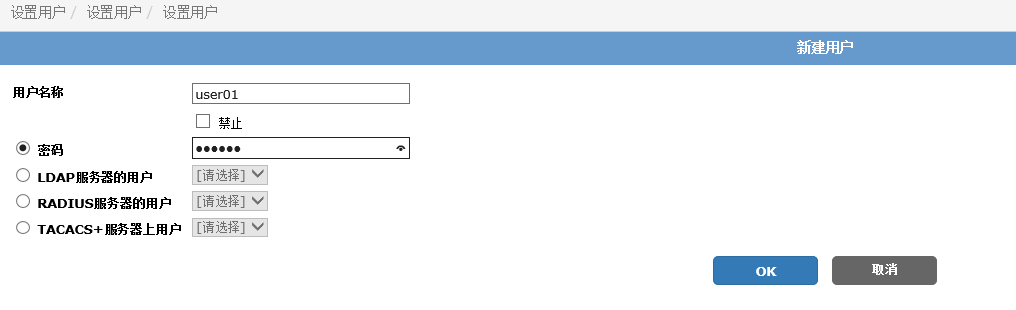
6，进入“防火墙>策略>策略”页面，单击“创建”按钮，新建防火墙策略允许办公区网段访问互联网。

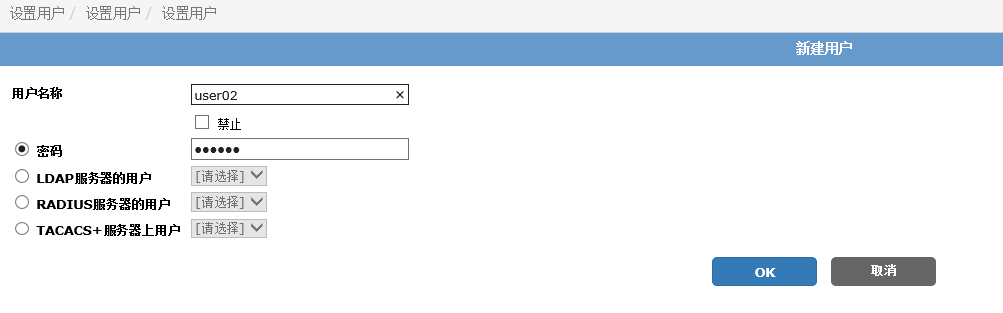


7，单击“创建”按钮，新建防火墙策略允许办公区网段访问服务器。



8，进入“设置用户>设置用户>设置用户”页面，创建不同的用户，user01、user02、user03。







9，进入“设置用户>用户组>用户组”页面，创建不同的用户组。

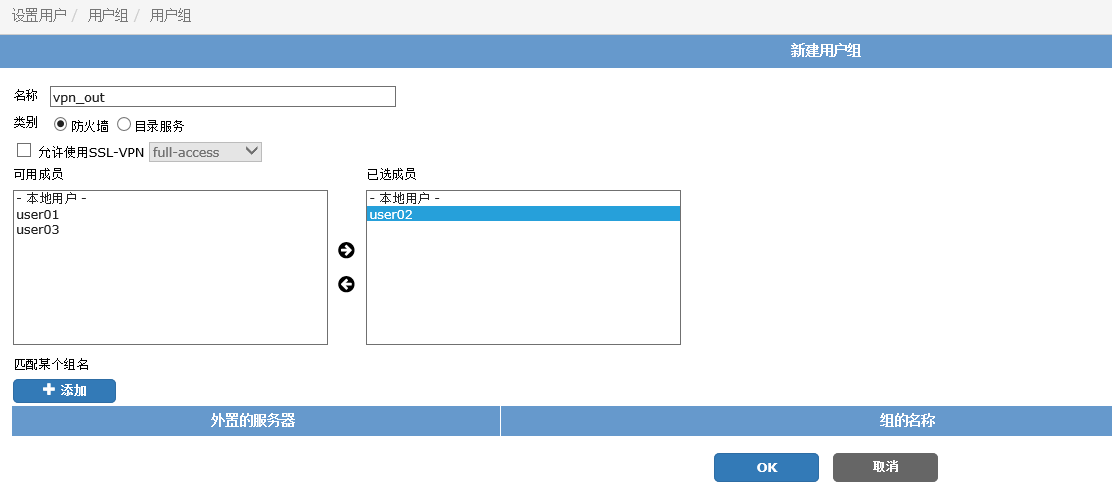
10，“vpnuser”组为登陆VPN时使用，将三个用户均加入。



11，“vpn\_in”组为VPN用户访问内部服务器时使用，将用户“user01”加入。



12，“vpn\_out”组为VPN用户访问外部互联网时使用，将用户“user02”加入。



13，“vpn\_all”组为VPN用户访问内部服务器和互联网时使用，将用户“user03”加入。



14，进入防火墙CLI命令行，创建PPTP VPN。

# define vpn pptp

(pptp) #set status enable //开启PPTP VPN功能

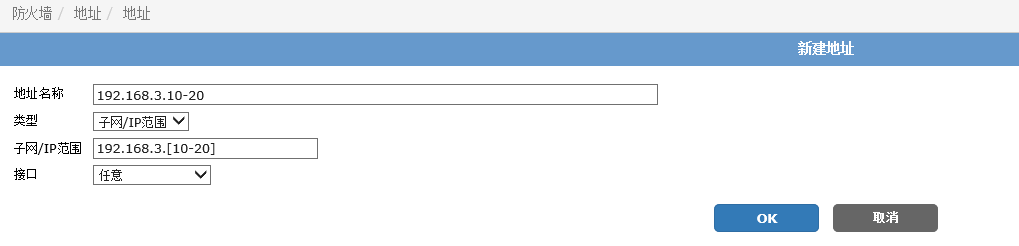
(pptp) #set sip 192.168.3.10 //配置客户端分配的IP范围：开始IP

(pptp) #set eip 192.168.3.20 //配置客户端分配的IP范围：结束IP

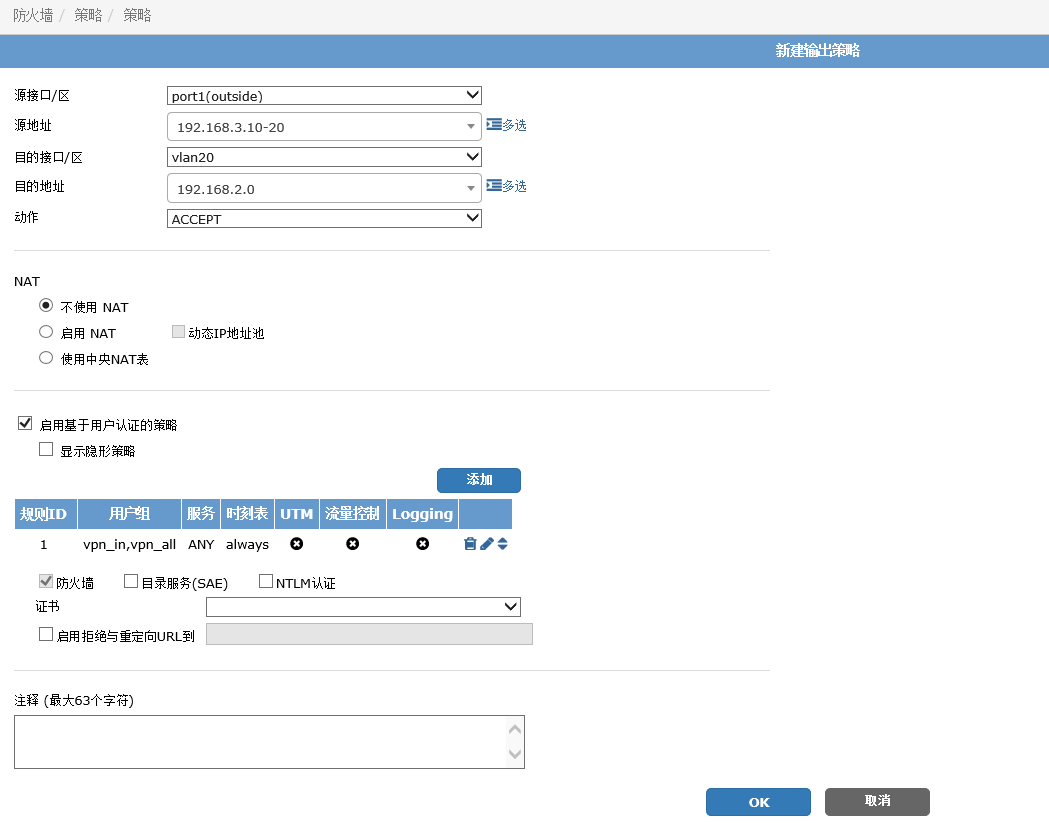
(pptp) #set usrgrp vpnuser //调用VPN用户组

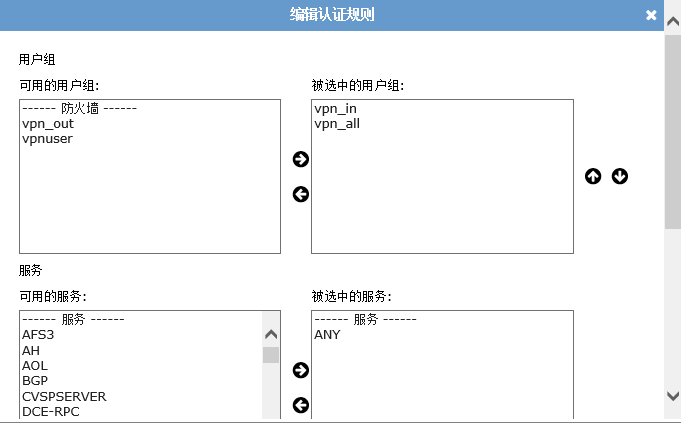
(pptp) #end

15，进入“防火墙>地址>地址”页面，单击“创建”按钮新建VPN地址段。

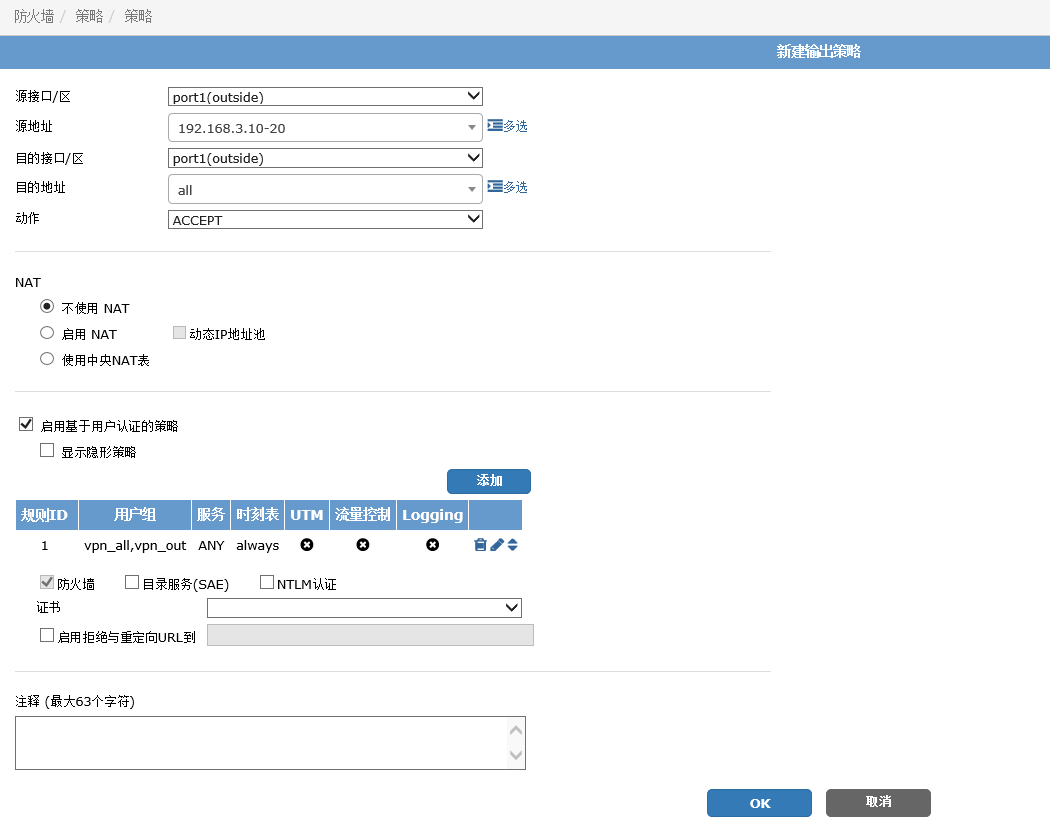


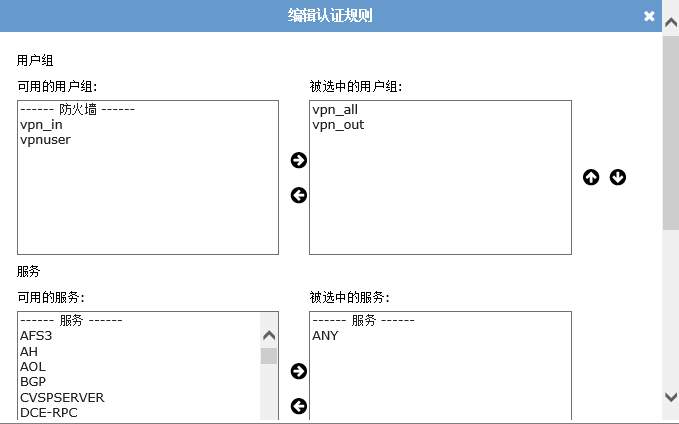
16，进入“防火墙>策略>策略”页面，创建基于用户的策略允许用户组“vpn\_in”和“vpn\_all”访问服务器。





17，创建基于用户的策略允许用户组“vpn\_out”和“vpn\_all”访问互联网。





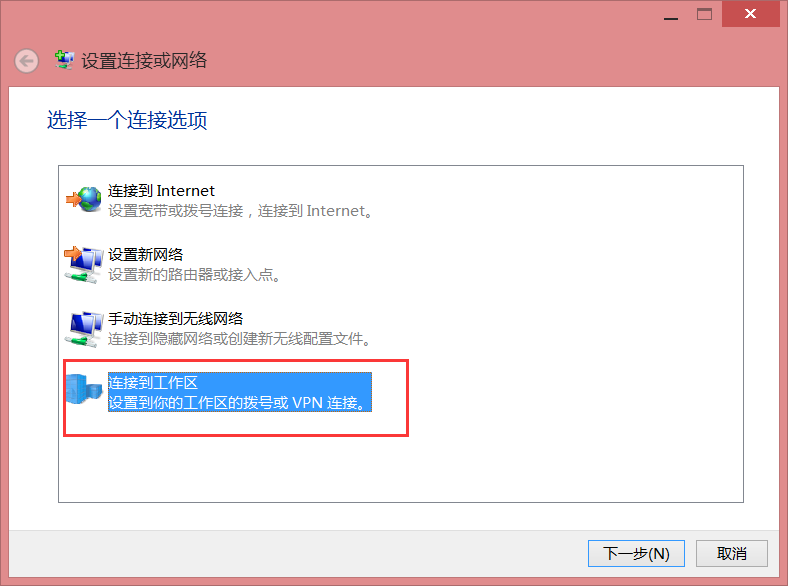
### 用户终端配置

用户需先通过VPN接入公司，这里以Windows8操作系统为例。

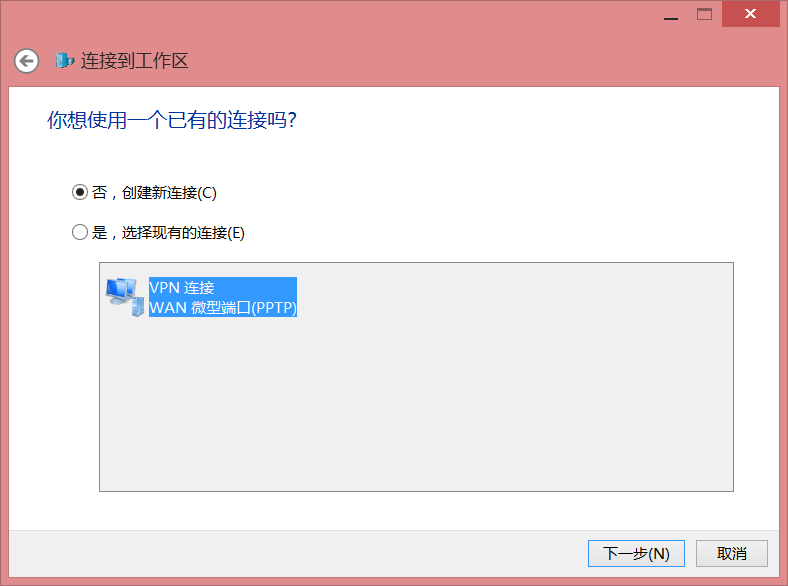
1，打开“控制面板>网络和共享中心”，点击“设置新的链接或网络”。



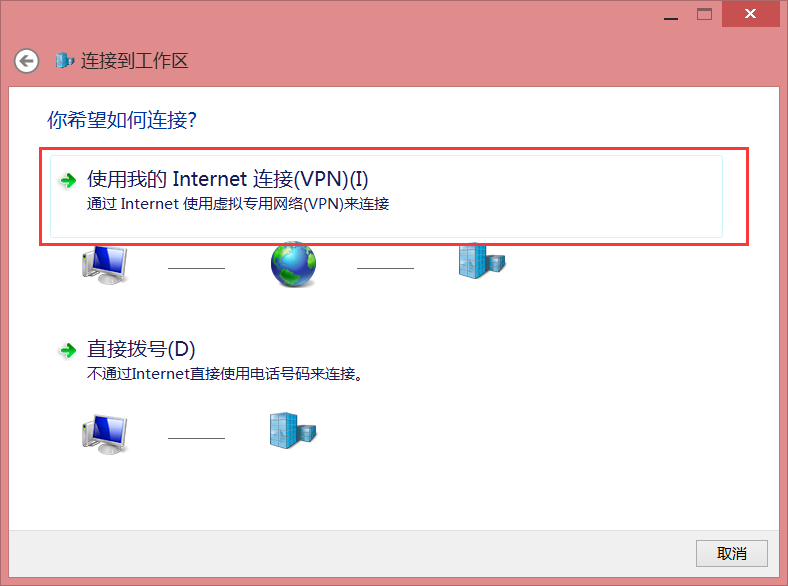
2，在弹出的“选择一个连接选项”窗口中选择“连接到工作区”，并单击“下一步”。



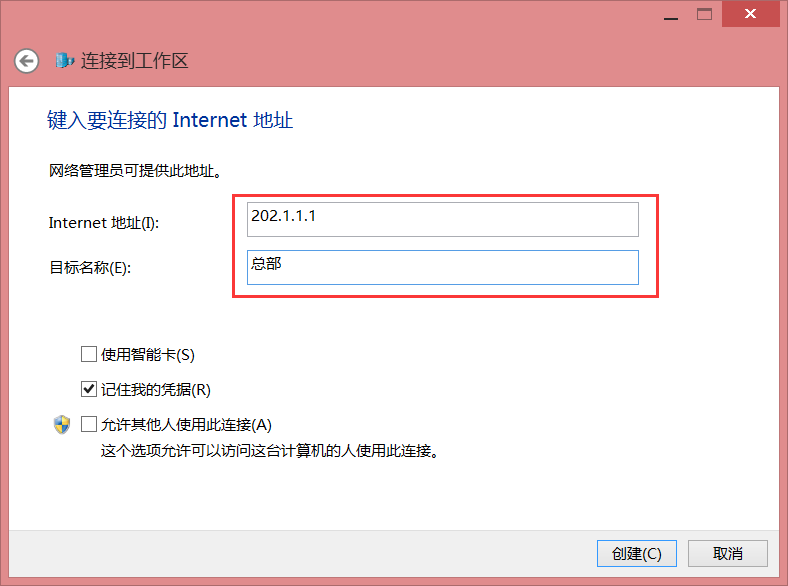
3，选择“否，创建新连接”，单击“下一步”。



4，在弹出的“你希望如何连接？”窗口中选择“使用我的Internet连接(VPN)”，单击“下一步”。



5，在弹出的“键入要连接的Internet地址”窗口中，输入Internet地址，目标名称，其中“Internet地址”为防火墙外网口地址，名称可随便输入，单击“创建”按钮创建该VPN。



6，创建VPN网络后，可在网络选项中看到该VPN，单击“连接”。



7，在弹出的认证窗口中输入用户名和密码，单击“确定”。



8，打开浏览器，在弹出的用户认证页面，输入用户名和密码，即可正常访问内部服务器。



9，如果需要通过VPN访问Internet，则需要使用具有上网权限的账号。