## DCFW

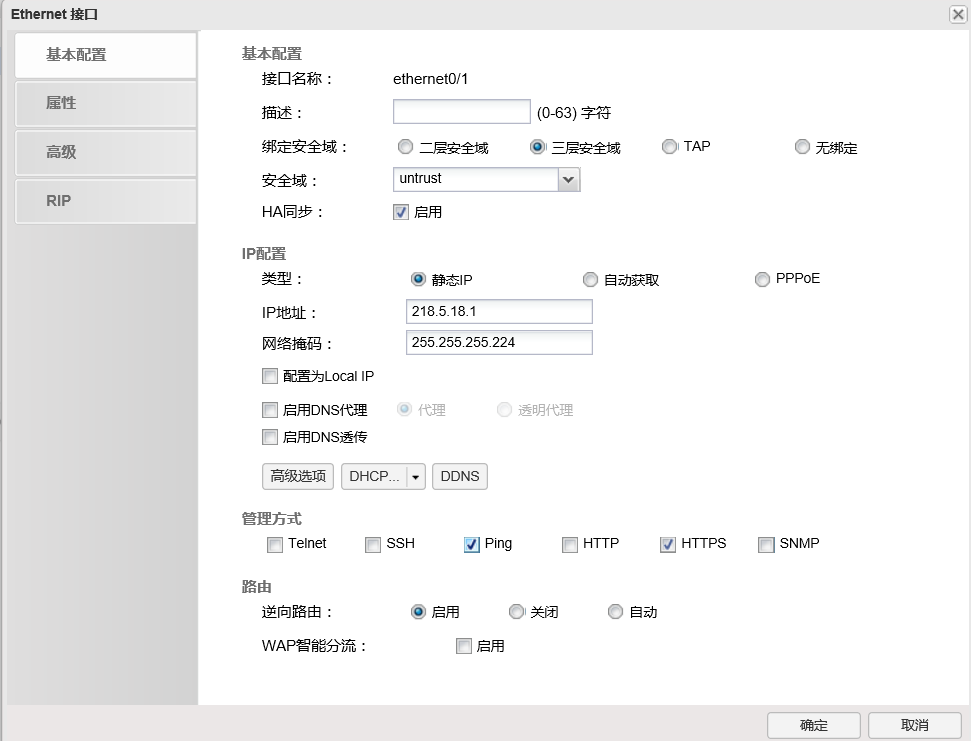
### 第1题

**在 DCFW 上配置，连接 LAN 接口开启 PING,HTTP,HTTPS，telnet 功能，连接Internet 接口开启 PING、HTTPS 功能；连接 netlog 接口为 DMZ 区域，合理配置策略，让内网用户能通过网络管理 netlog**

连接 LAN 接口(设置为turst)



连接 Internet 接口（设置为unturst）

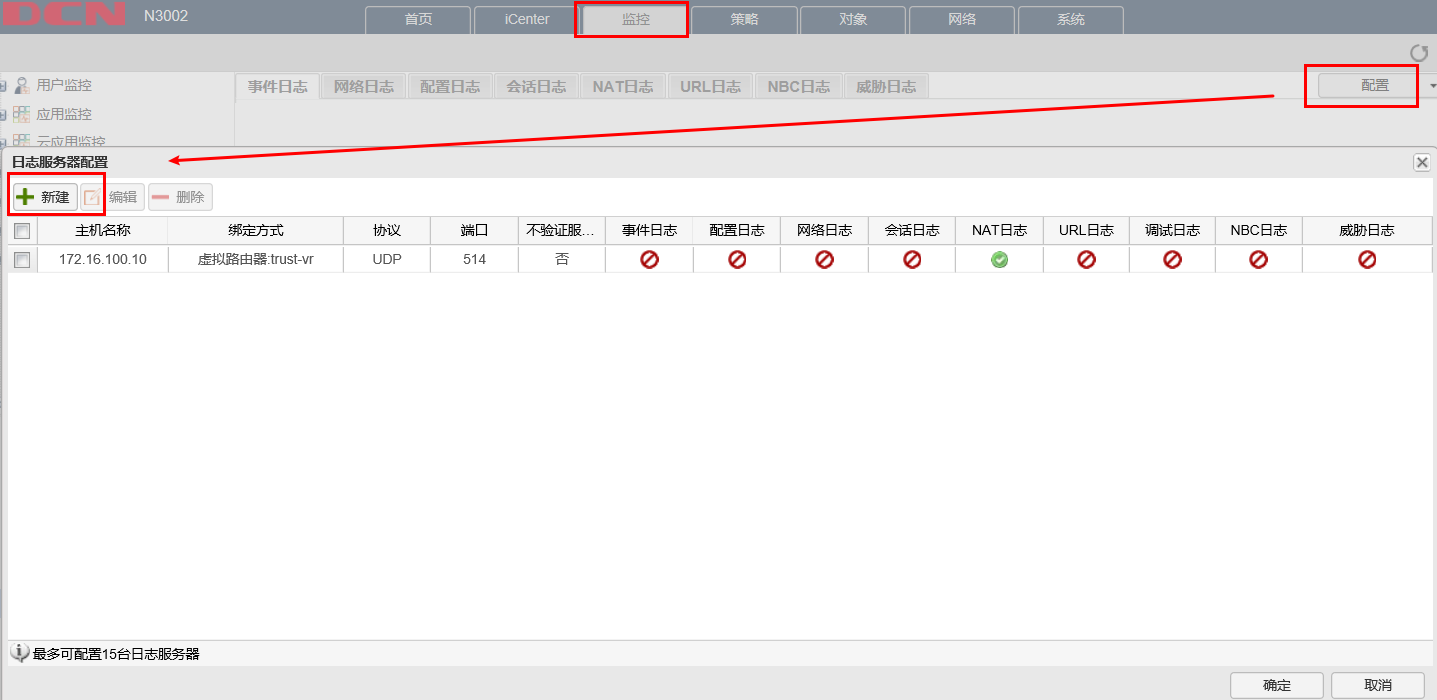


连接 netlog 接口（设置为dmz）

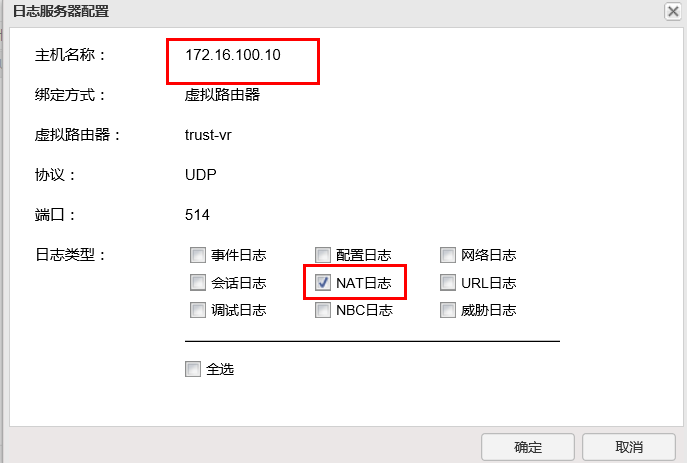


### 第2题

配置日志服务器



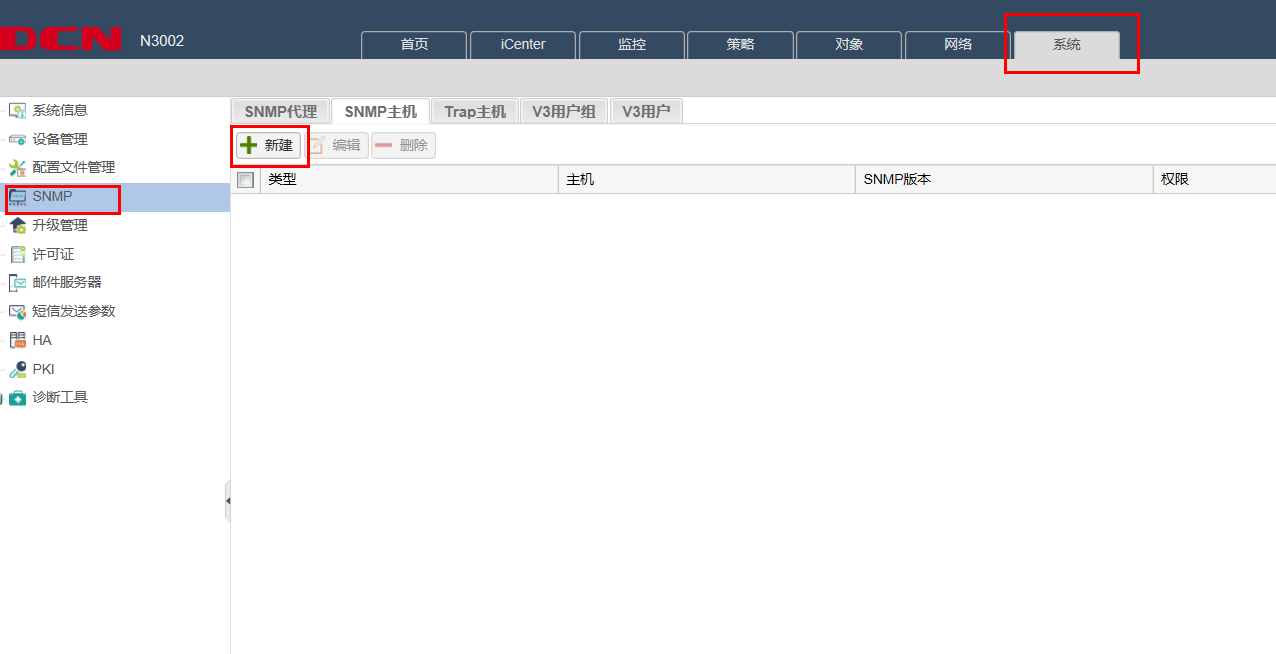
配置其Server IP，并勾选NAT日志

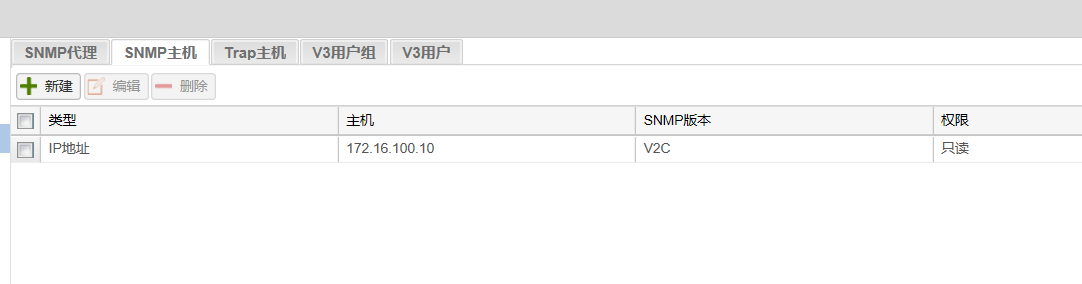


开启日志服务器



**开启 DCFW上 snmp 服务，Server IP 172.16.100.10 团体字符为 public5;**



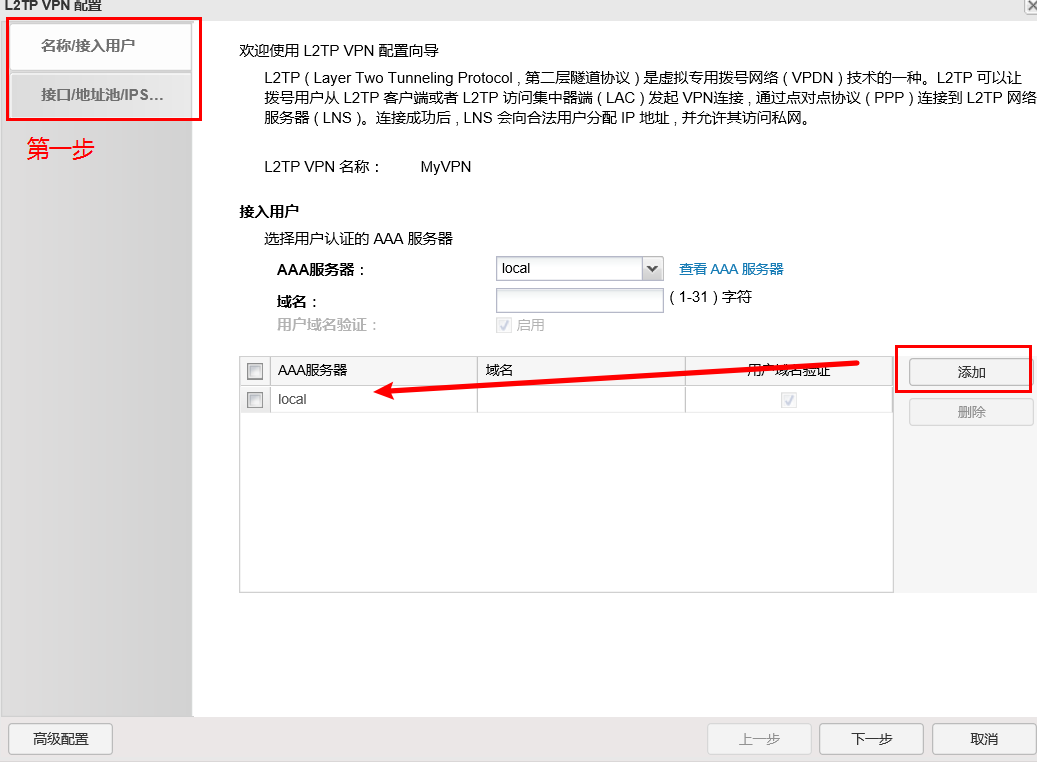


### 第3题

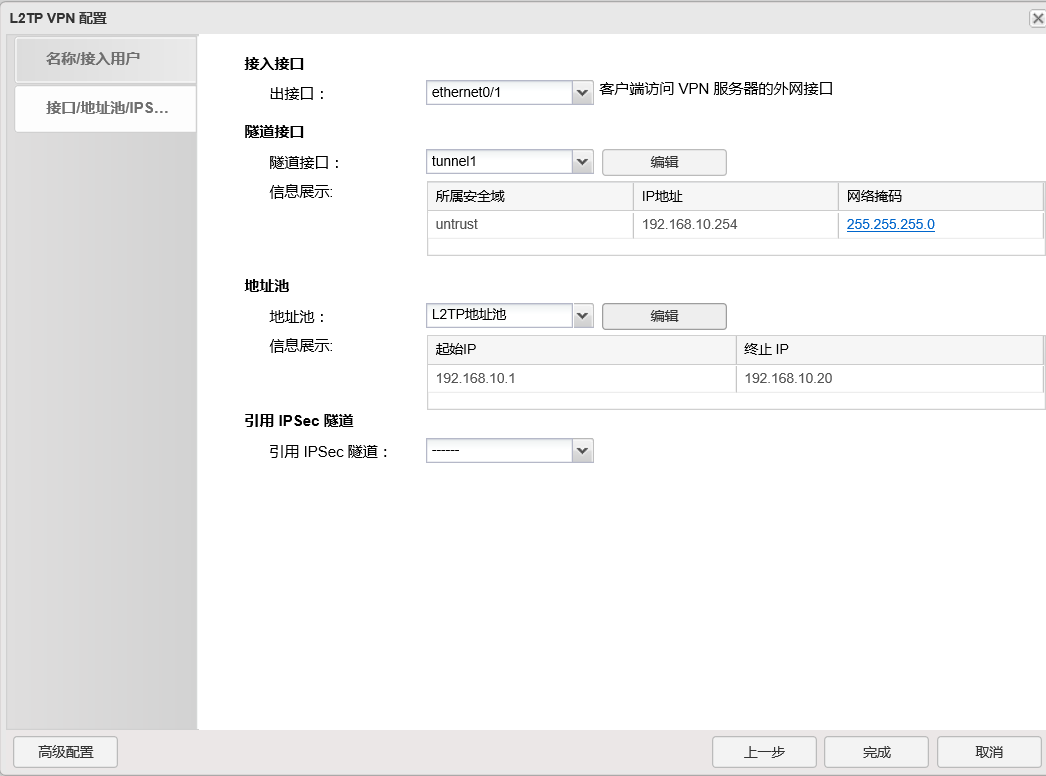
**DCFW 做相应配置，使用 L2TP 方式让外网移动办公用户能够实现对内网的访问，用户名密码为 dcn2015， VPN 地址池参见地址表；**

进入L2TP配置向导

添加AAA服务器



配置隧道接口、地址池信息。（隧道接口应该配置为untrust，毕竟该VPN是给外网用户提供的）



这时候，在网络接口就可以看到我们的VPN路由

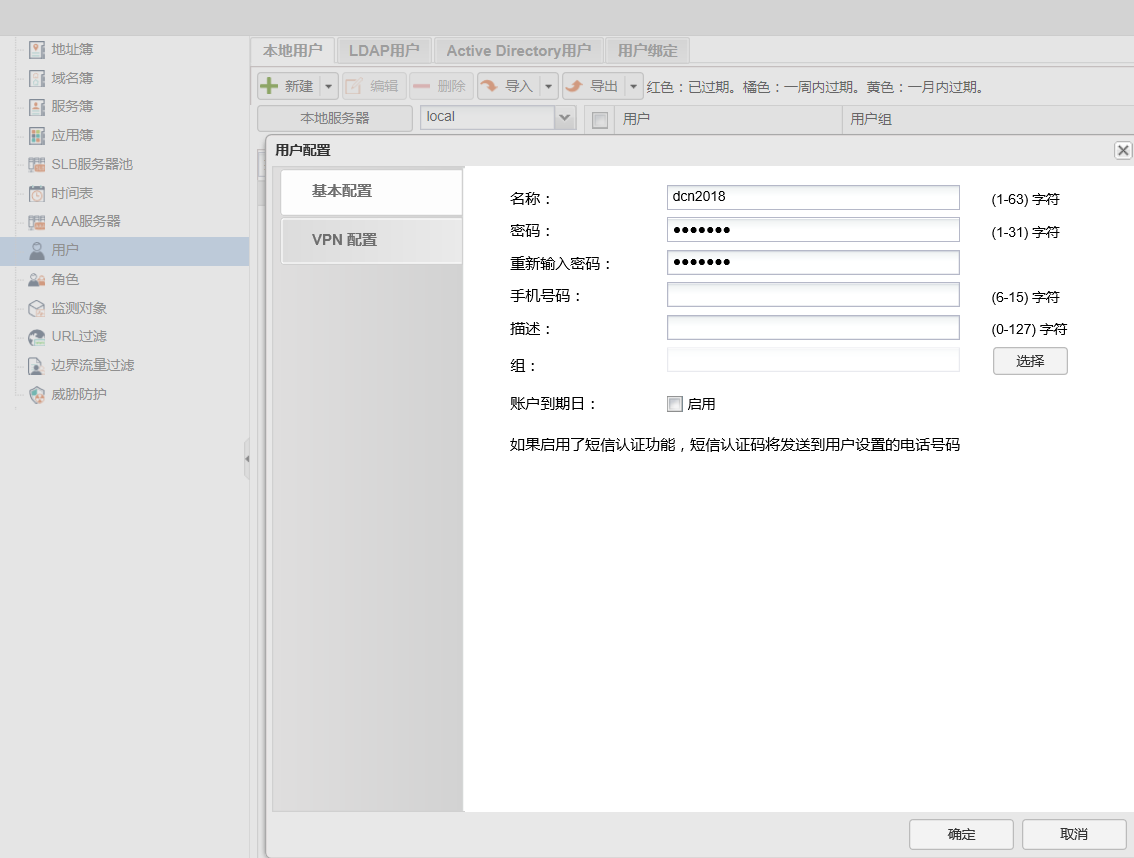


**合理配置安全策略**

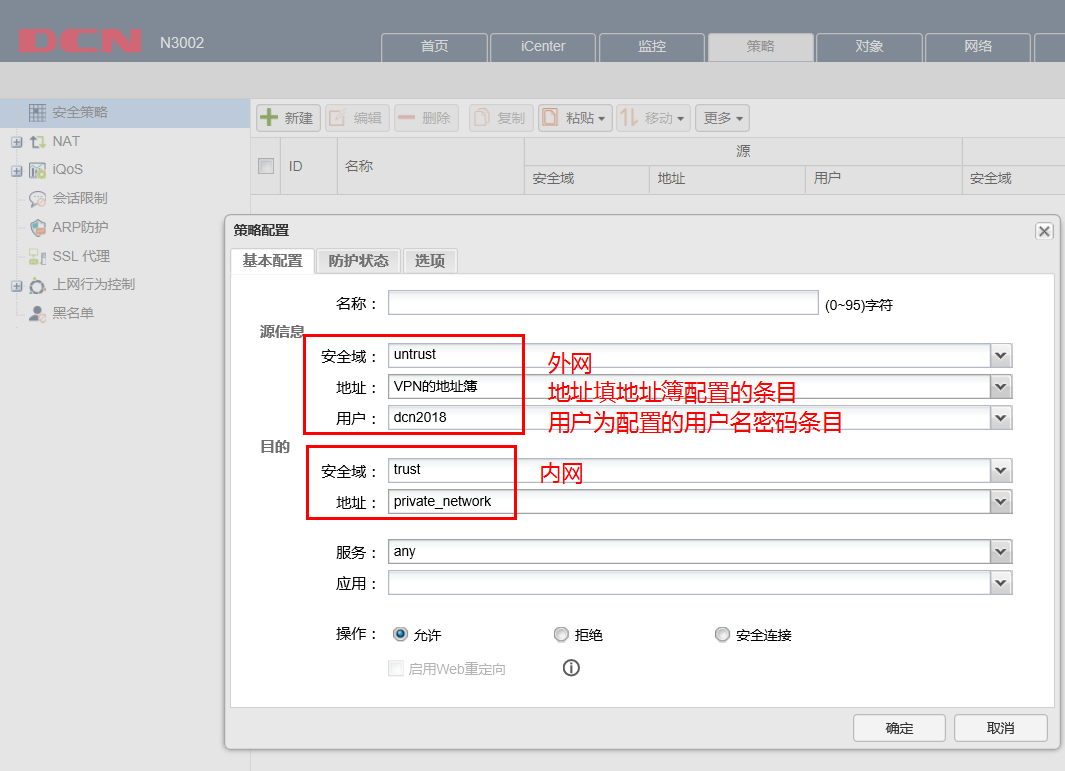
首先，需要有VPN的地址薄



接着，配置用户名密码为dcn2018



配置实现内外网的安全策略。



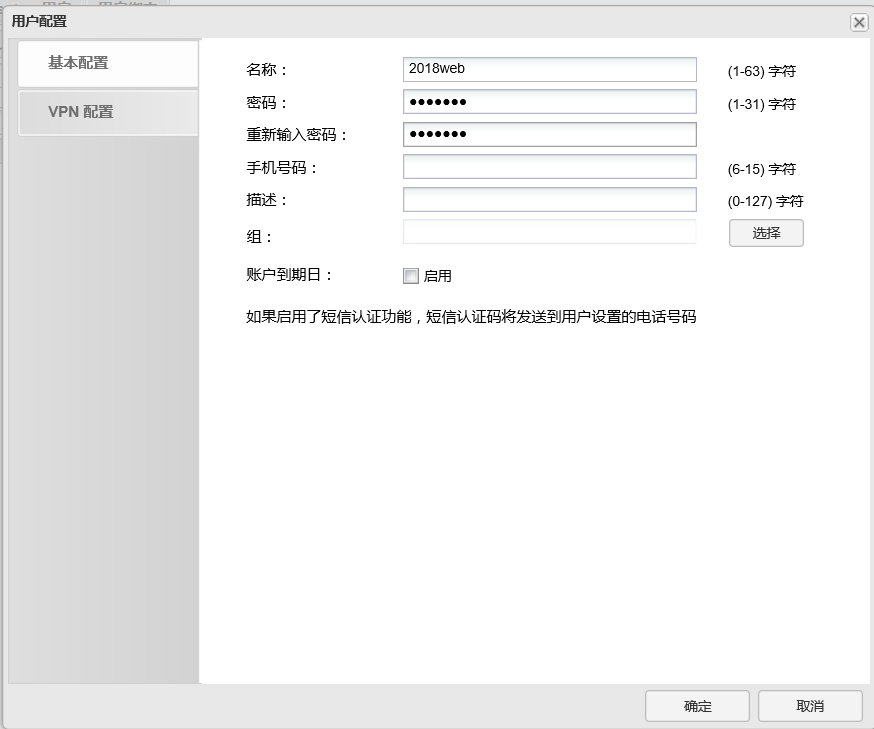
配置之后：



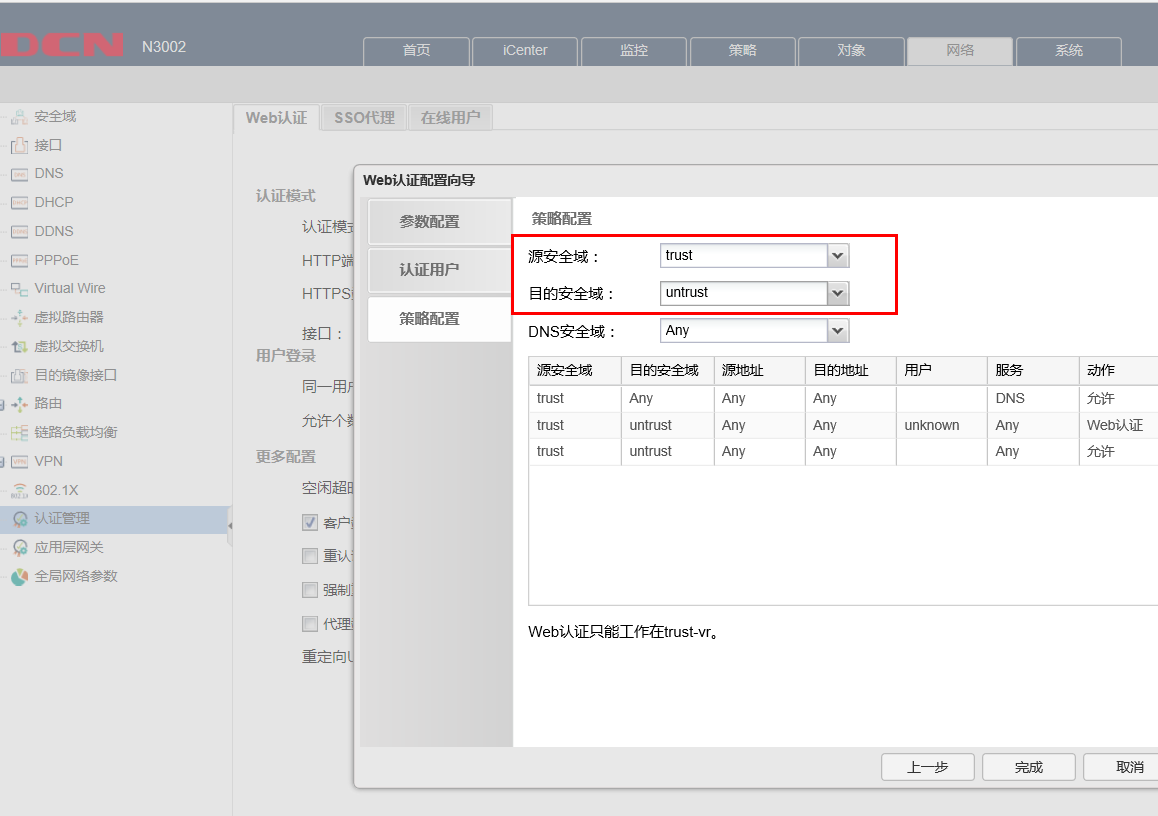
### 第4题：

**出于安全考虑，无线用户移动性较强，无线用户访问 Internet 是需要采用实名认证，在防火墙上开启 web 认证，账号密码为 2018web。**

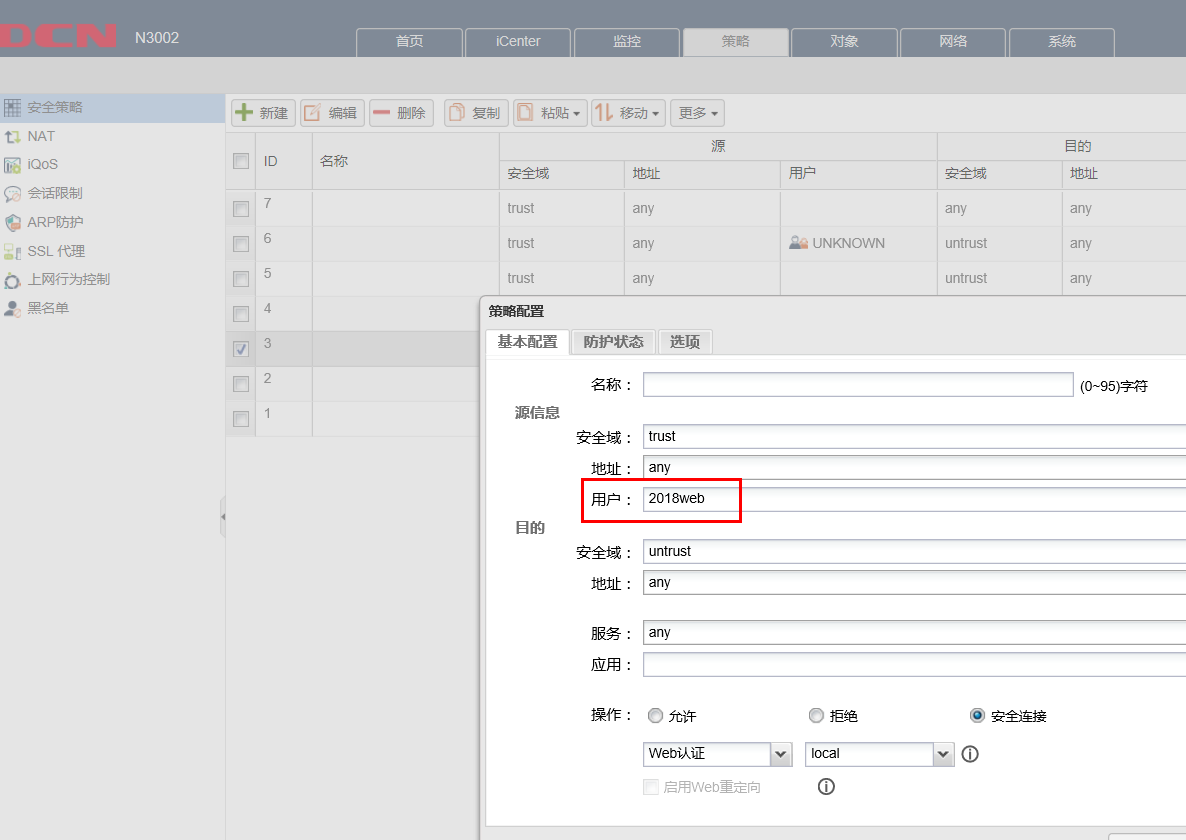
配置用户



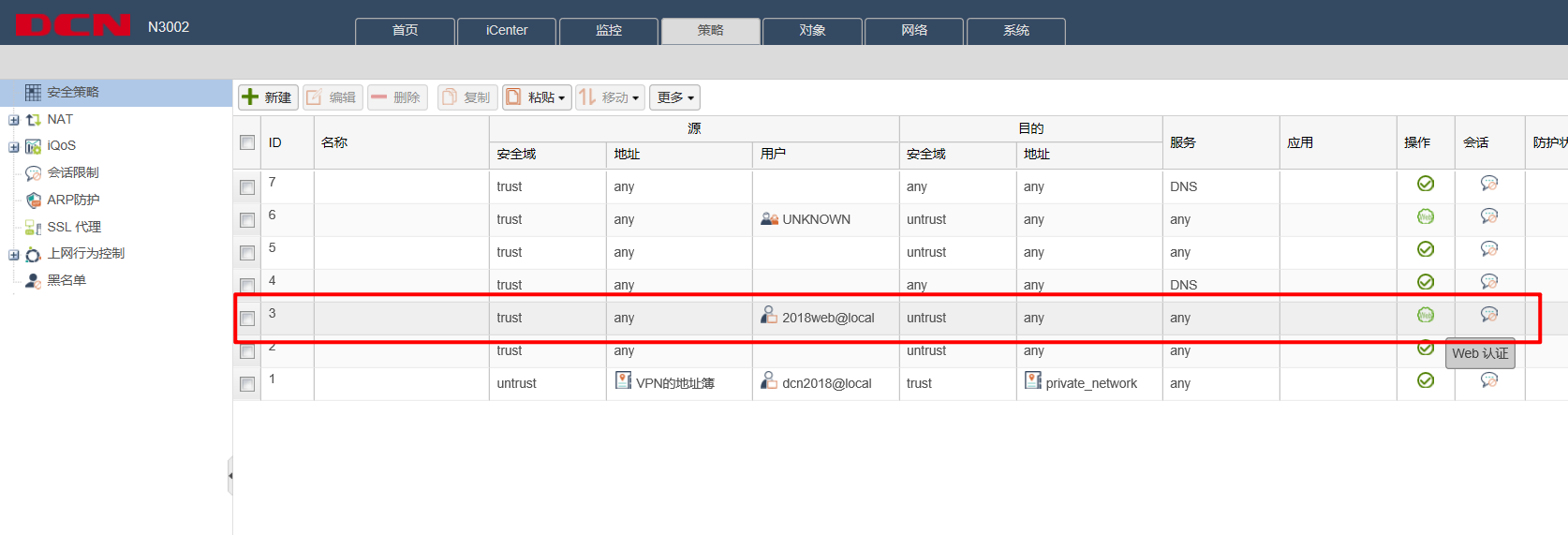
关联web认证



需要注意的是，配置了的认证管理，其实默认对unknown用户生效（范围太大了），我们需要到“安全策略”中，修改为特定用户，则“无线用户”



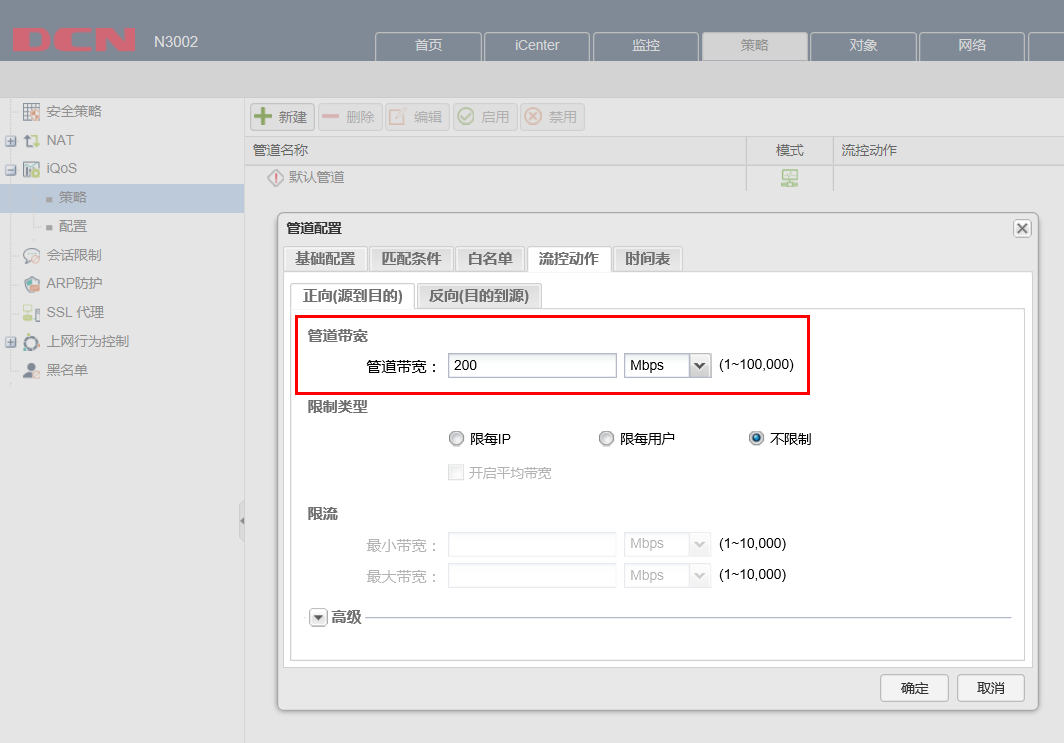
最后查看安全策略：



### 第5题

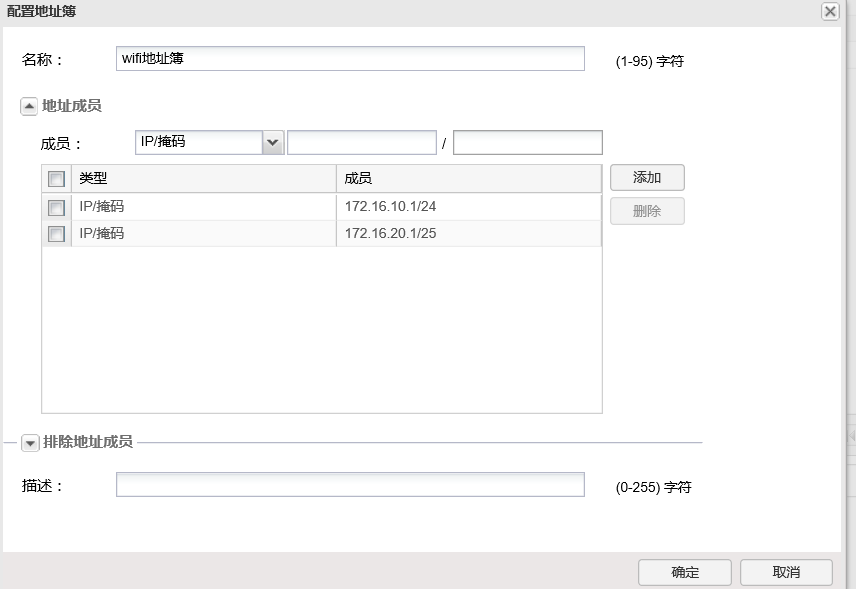
**为了合理利用网络出口带宽，需要对内网用户访问Internet进行流量控制，园区总出口带宽为200M**

限制园区总出口带宽



**对除无线用户以外的用户限制带宽，每天上午9:00到下午 6:00 每个 IP 最大下载速率为 2Mbps，上传速率为 1Mbps；**

首先，配置无线用户的地址簿



配置白名单（wifi用户访问外网）

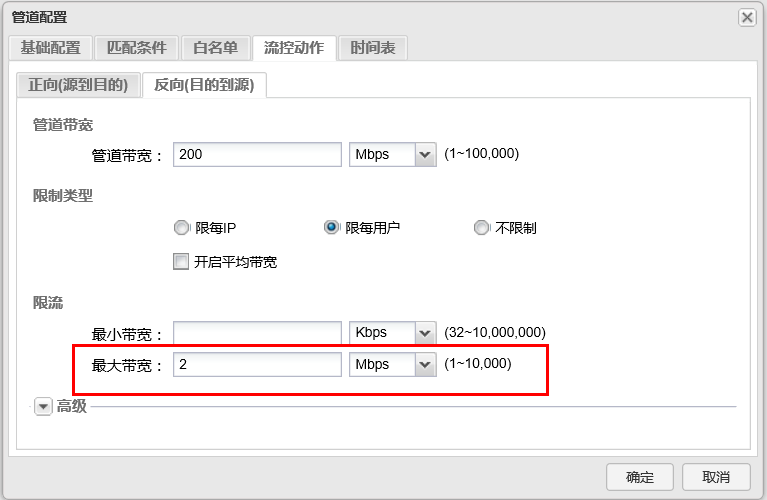


普通用户限时：



普通限流配置：





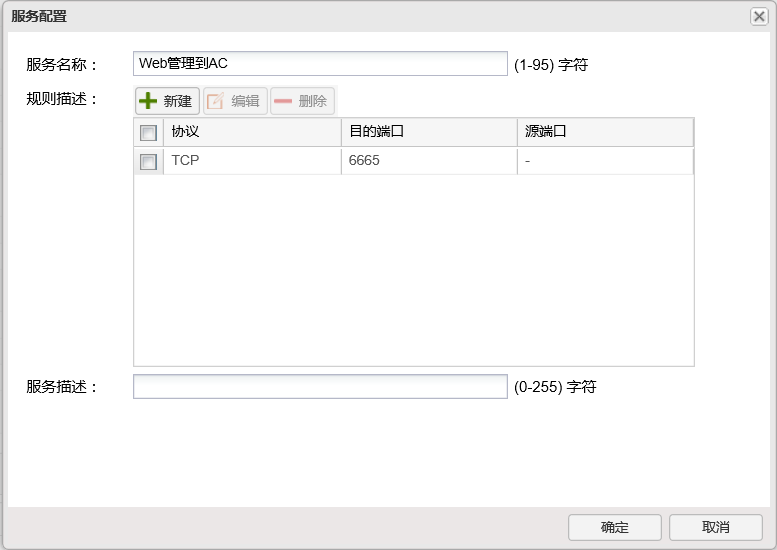
配置之后：



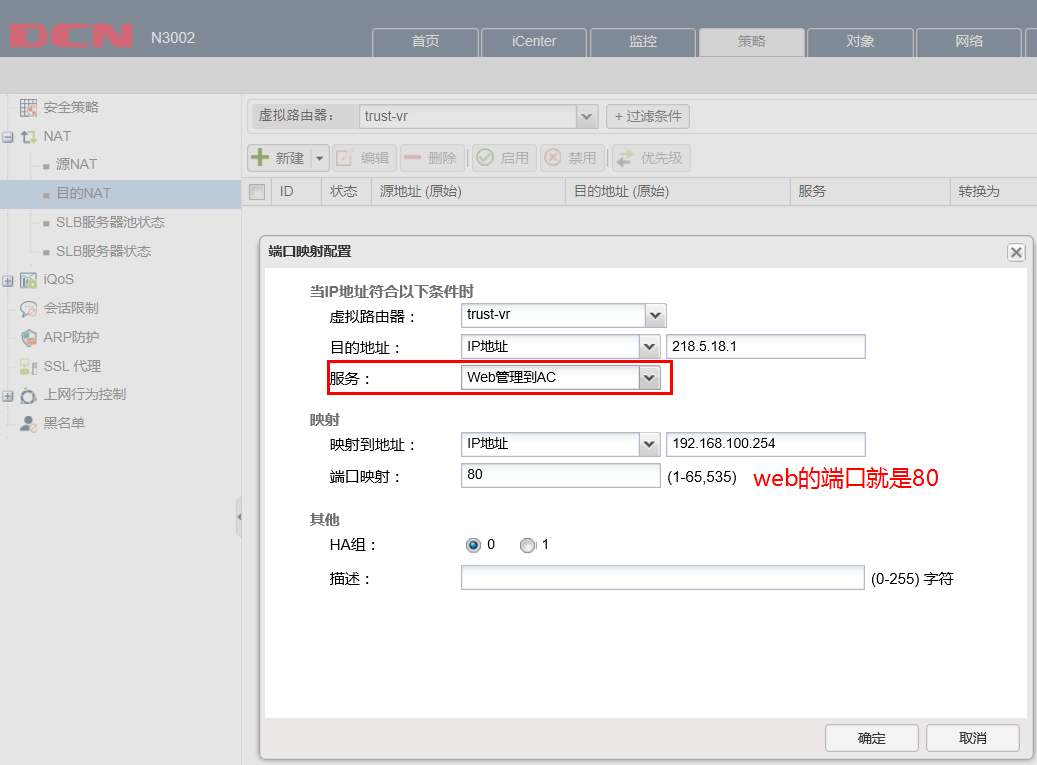
### 第6题：

**DCFW 上配置 NAT 功能，使 PC3 能够通过 Web 方式正常管理到 AC，端口号使用 6665;）合理配置安全策略;**

首先，由于题目说“通过Web方式”，所以需要配置服务薄（对象-->服务薄）



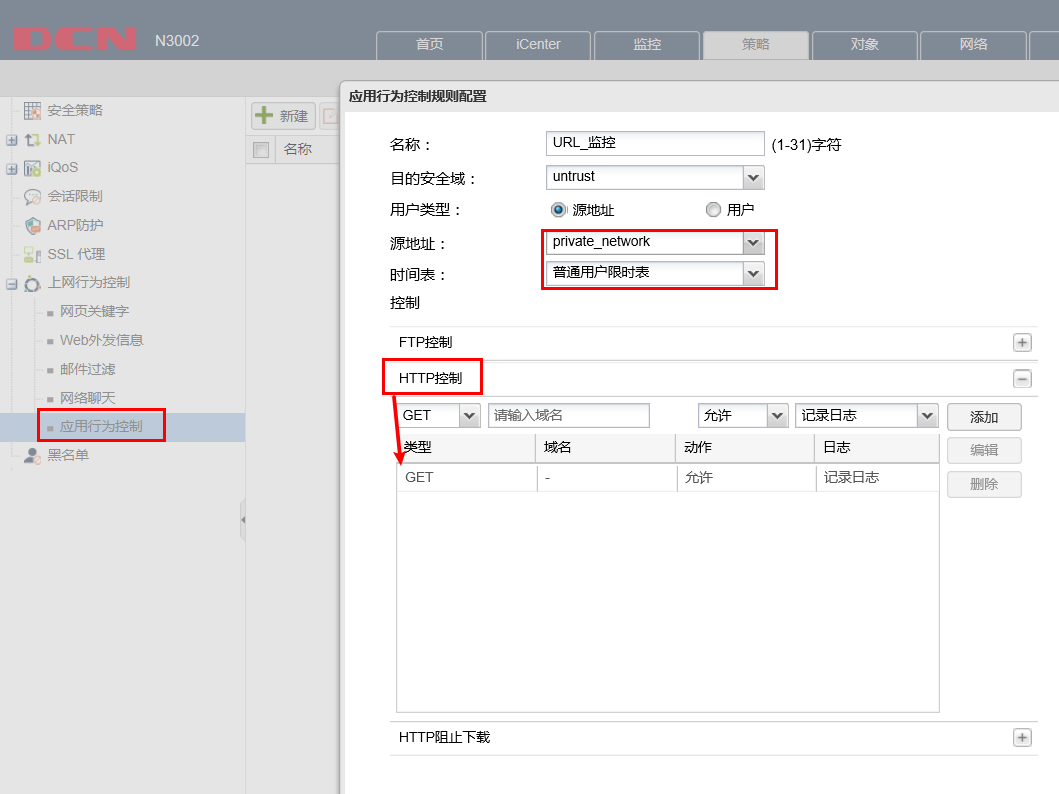
接着，配置目的NAT，目的接口则是FW上面的接口了





### 第7题：

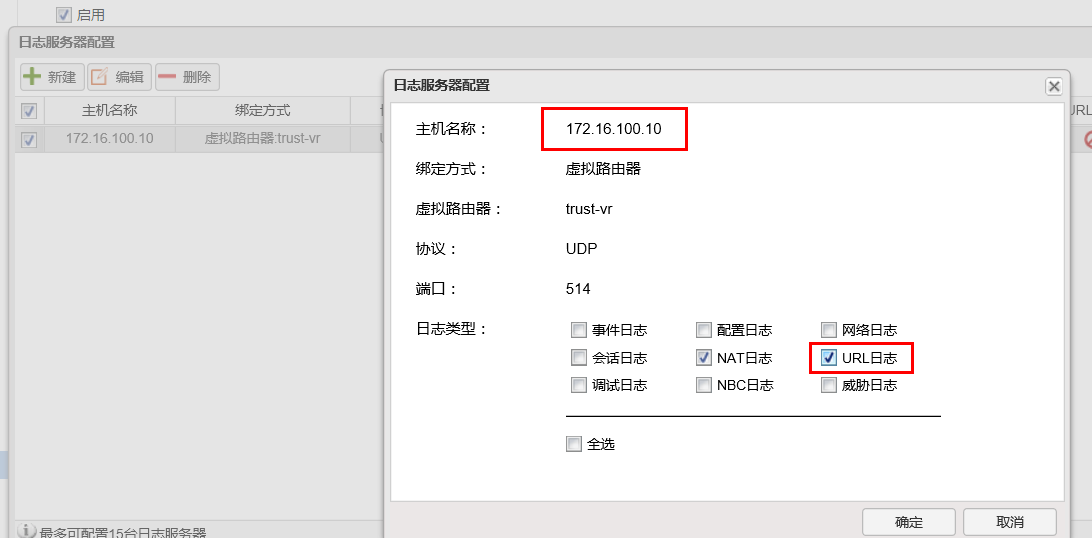
**在 DCFW 做相关配置要求防火墙能够记录每天 9:00-18:00 内网用户访问外网的 URL**



配置结果：



**保存在日志服务器；**

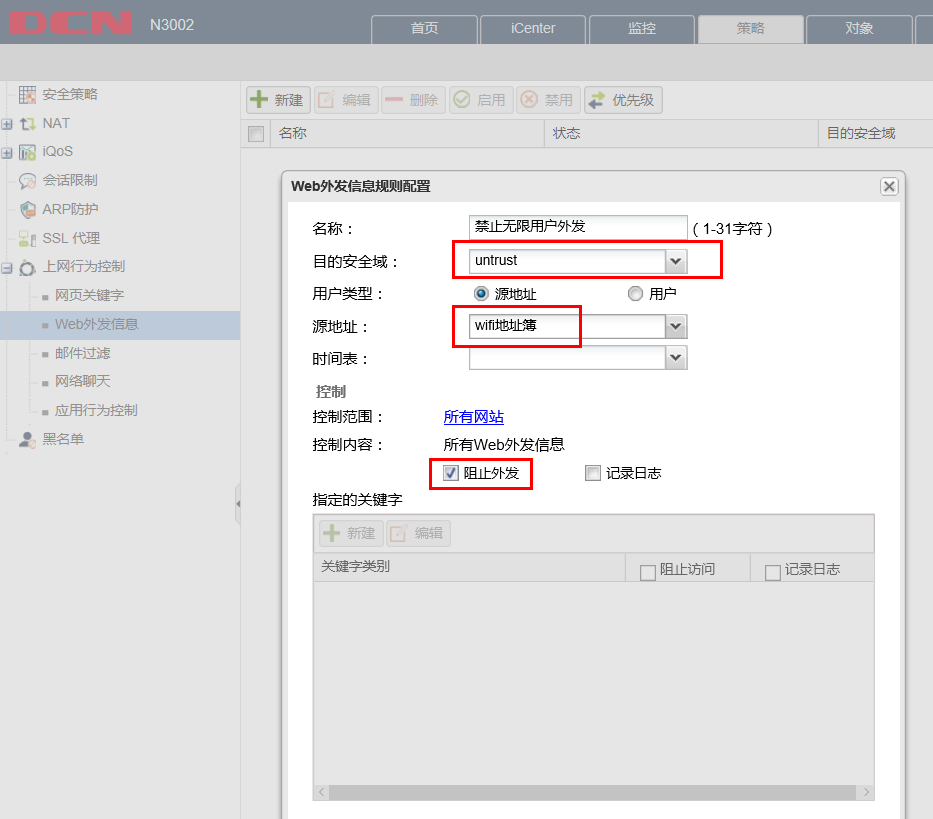


配置结果：



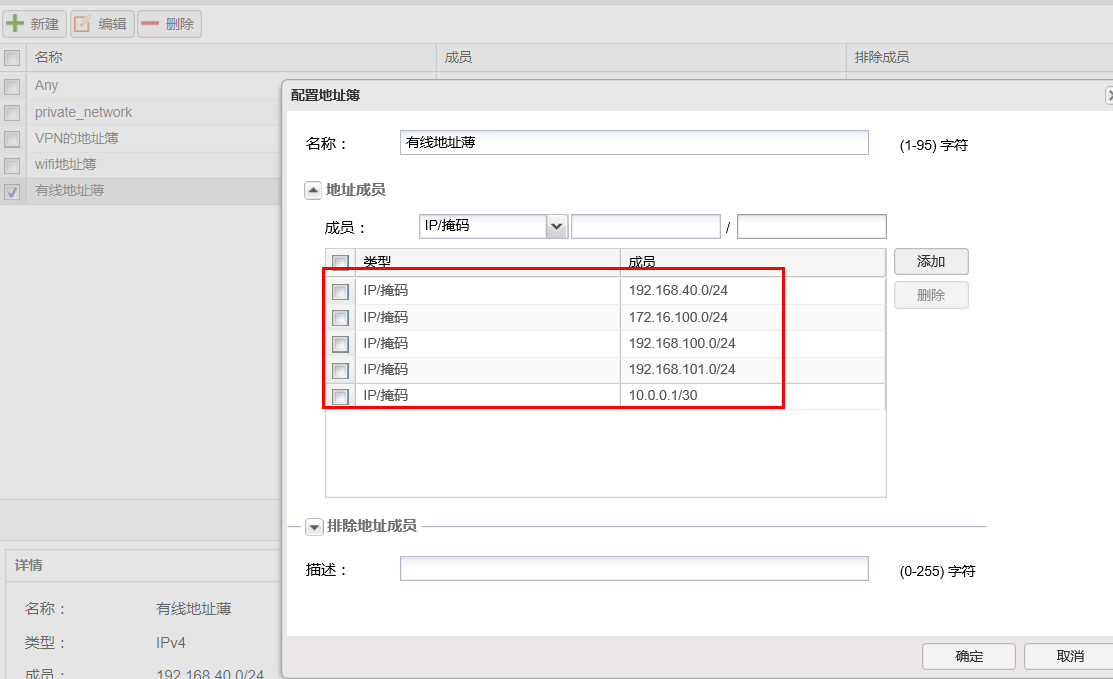
### 第8题

**配置防火墙 Web 外发信息控制策略，禁止内网无线用户到所有网站的 Web外发信息控制；**

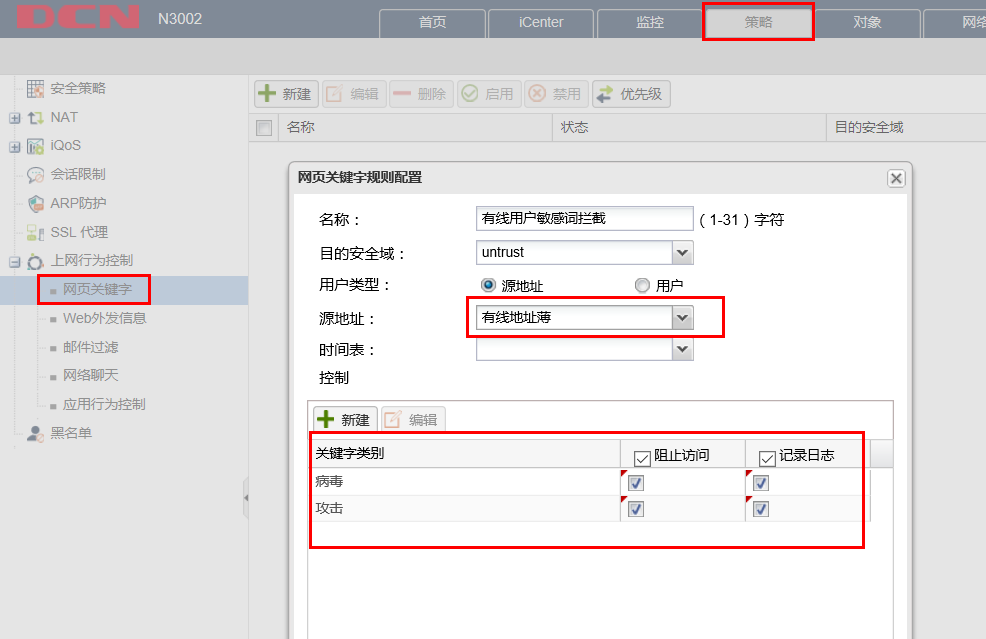


**内网有线用户到外网网站 Web 外发信息控制，禁止外发关键字“攻击”“病毒”，信任值为 1，并记录相关日志。**

①创建有线地址薄，将内网的IP段添加进地址薄



②配置关键词及行为：阻止访问以及记录日志



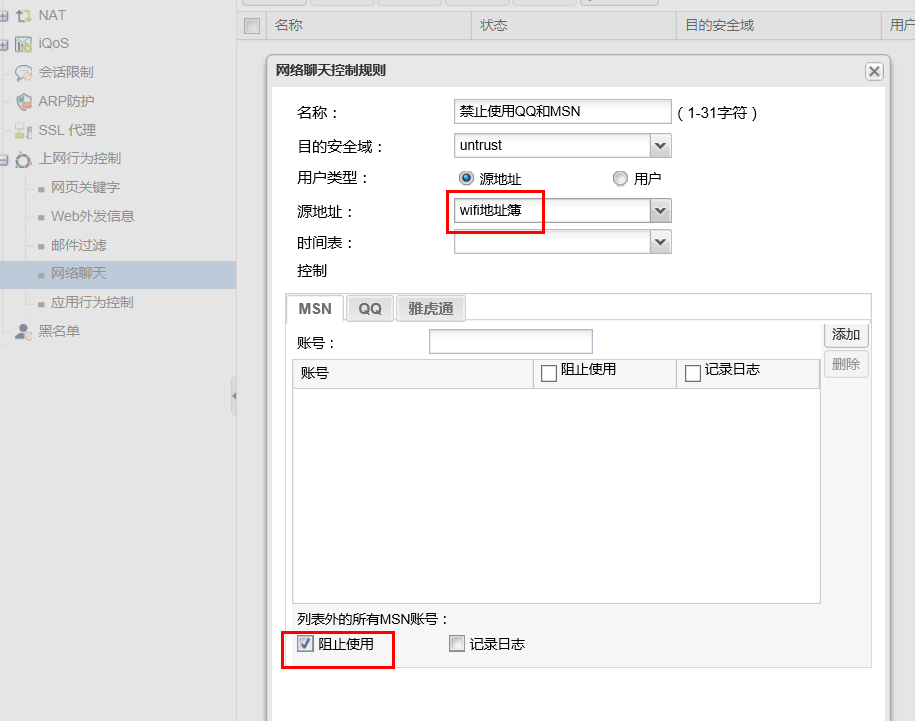
同时，信任值设置为1



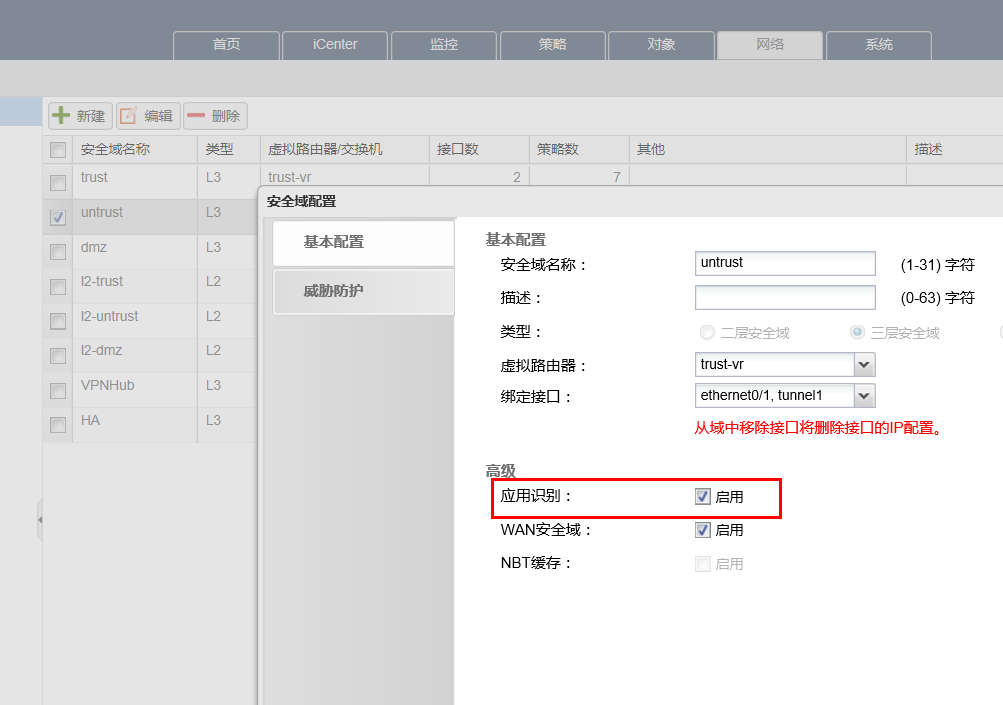


### 第9题

**DCFW 做相关配置要求内网用户不能登录 QQ 和 MSN**

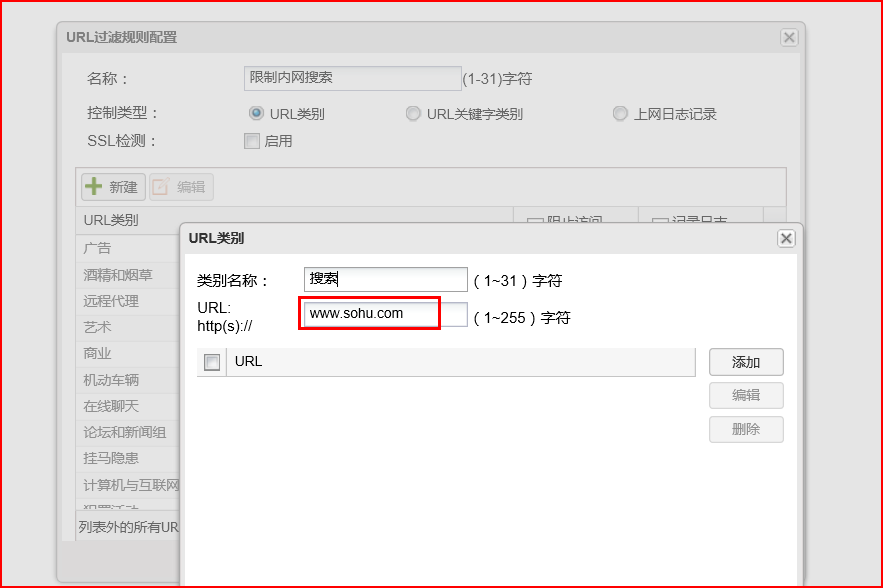


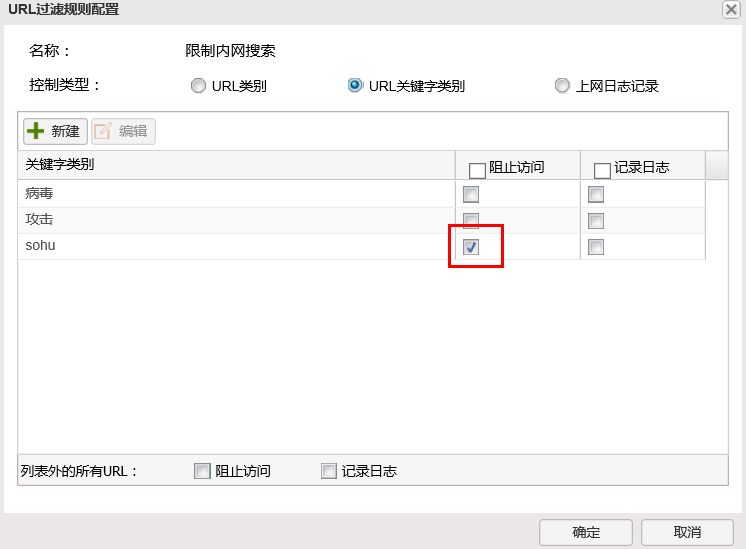
并且，需要在untrust安全域中，配置应用识别，防火墙才能知道什么是“QQ”和"MSN"



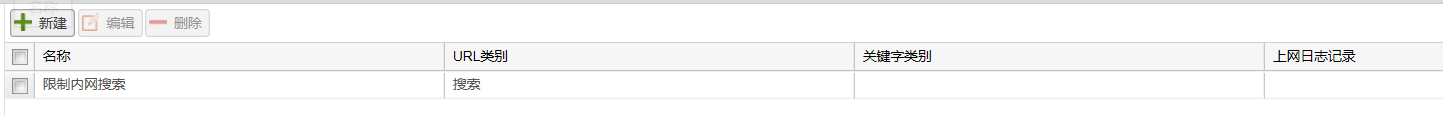
### 第10题

**DCFW 上配置限制内网用户访问 www.sohu.com 限制内网用户访问 URL 中带有 sohu 关键字的所有网站;**





配置结果：



### 疑点



第十题这里，为什么URL类别和关键字类别只能出现一个

而且，无法绑定用户，不知道是否生效。