天融信 3.3 版本防火墙

常用功能配置手册

一、前言

我们制作本安装手册的目的是使工程技术人员在配置天融信网络卫士防火墙（在本安装手册中简称为“天融信防火墙”）时，可以通过此安装手册完成对天融信防火墙基本功能的实现和应用。

二、天融信3.3版本防火墙配置概述

天融信防火墙作为专业的网络安全设备，可以支持各种复杂网络环境中的网络安全应用需求。 在配置天融信防火墙之前我们通常需要先了解用户现有网络的规划情况和用户对防火墙配置及实现功能的诸多要求，建议参照以下思路和步骤对天融信防火墙进行配置和管理。

1、根据网络环境考虑防火墙部署模式（路由模式、透明模式、混合模式），根据确定好的防火墙的工作模式给防火墙分配合理的IP地址。

2、防火墙接口IP配置

3、区域和缺省访问权限配置

4、防火墙管理权限配置

5、路由表配置

6、定义对象（地址对象、服务对象、时间对象）

7、制定地址转换策略（包括四种地址转换策略：源地址转换、目的地址转换、双向转换、不做转换）

8、制定访问控制策略

9、其他特殊应用配置

10、配置保存

11、配置文件备份

☺ 提示：每次修改配置前，建议首先备份防火墙再修改配置，避免防火墙配置不当造成网络长时间中断。

三、天融信防火墙一些基本概念

接口：和防火墙的物理端口一一对应，如 Eth0、Eth1 等。

区域：可以把区域看作是一段具有相似安全属性的网络空间。在区域的划分上，防火墙的区域和接口并不是一一对应的，也就是说一个区域可以包括多个接口。在安装防火墙前，首先要对整个受控网络进行分析，并根据网络设备，如主机、服务器等所需要的安全保护等级来划分区域。

对象:防火墙大多数的功能配置都是基于对象的。如访问控制策略、地址转换策略、服务器负载均衡策略、认证管理等。可以说，定义各种类型的对象是管理员在对防火墙进行配置前首先要做的工作之一。对象概念的使用大大简化了管理员对防火墙的管理工作。当某个对象的属性发生变化时，管理员只需要修改对象本身的属性即可，而无需修改所有涉及到这个对象的策略或规则。防火墙中，用户可定义的对象类型包括：区域、地址、地址组、服务、服务组、以及时间等。

☺ 提示：对象名称不允许出现的特殊字符：空格、“’”、“″”、“\”、“/”、“;”、“″”、“$”、“&”、“<”、“>”、“#”、“+”。

☺ 提示：防火墙所有需要引用对象的配置，请先定义对象，才能引用。

四、防火墙管理

防火墙缺省管理接口为 eth0 口，管理地址为 192.168.1.254，缺省登录管理员帐号：用户名 superman，口令 talent。

防火墙出厂配置如下：

网络卫士防火墙在出厂时使用了以下默认配置：

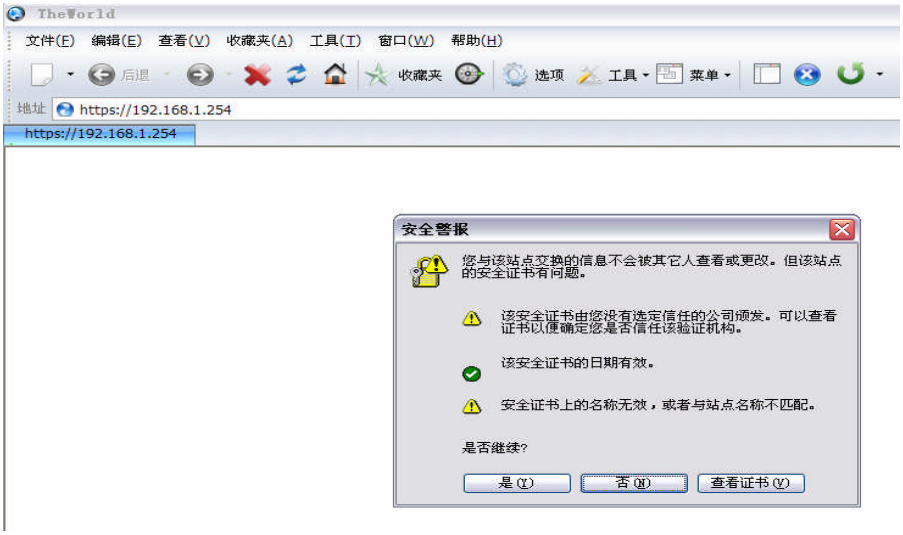
管理用户	管理员用户名	superman
	管理员密码	talent
系统参数	设备名称	TopsecOS
	同一管理员最多允许登录失败次数	5
	同一管理员最大并发管理数	5
	同一管理员最大并发管理地点	5
	最大登录用户数（管理员）	5
	最大连接数默认值	为该型号允许的最大连接数的三分之一
	空闲超时	3 分钟
物理接口	Eth0（或 LAN 口）	IP：192.168. 1.254
	其他接口	Shutdown
服务访问控制	WEBUI 管理（通过浏览器管理防火墙）	允许来自 Eth0（或 LAN 口）上的服务请求
	GUI 管理（通过 TOPSEC 管理中心）	允许来自 Eth0（或 LAN 口）上的服务请求
	SSH（通过 SSH 远程登录管理）	允许来自 Eth0（或 LAN 口）上的服务请求
	升级（对网络卫士防火墙进行升级）	允许来自 Eth0（或 LAN 口）上的服务请求
	PING（PING 到网络卫士防火墙的接口 IP 地址或 VLAN 虚接口的 IP 地址）	允许来自 Eth0（或 LAN 口）上的服务请求
	其他服务	禁止
地址对象	地址段名称	ANY
	地址段范围	0.0.0.0 - 255.255.255.255
日志	日志服务器 IP 地址	IP：192.168. 1.253
	日志服务器开放的日志服务端口	UDP 的 514 端口
高可用性（HA）		关闭

防火墙支持以下管理方式：

串口(console)管理方式：超级终端参数设置波特率 9600。输入 helpmode chinese 命令可以看到中文化菜单。

WEBUI 管理方式（https 协议）：在输入 URL 时要注意以“https://”作为协议类型，例如 https://192.168.1.254,推荐使用 IE 浏览器进行登录管理。

在浏览器输入：HTTPS://192.168.1.254，看到下列提示，选择“是”



TELNET 管理方式：模拟 console 管理方式

SSH 管理方式：模拟 console 管理方式

☺ 提示：要想通过 TELNET、SSH 方式管理防火墙，必须首先打开防火墙的服务端口，系统默认打开“HTTP”方式。在“系统管理”－“配置” －“开放服务”中选择“启动”即可，并且在开放服务里面相关接口区域添加 TELNET、SSH 方式等管理方式即可。

五、防火墙配置

（1）防火墙路由模式案例配置

在路由模式下，天融信防火墙类似于一台路由器转发数据包，将接收到的数据包的源 MAC 地址替换为相应接口的 MAC 地址，然后转发。该模式适用于每个区域都不在同一个网段的情况。和路由器一样，天融信防火墙的每个接口均要根据区域规划配置 IP 地址。

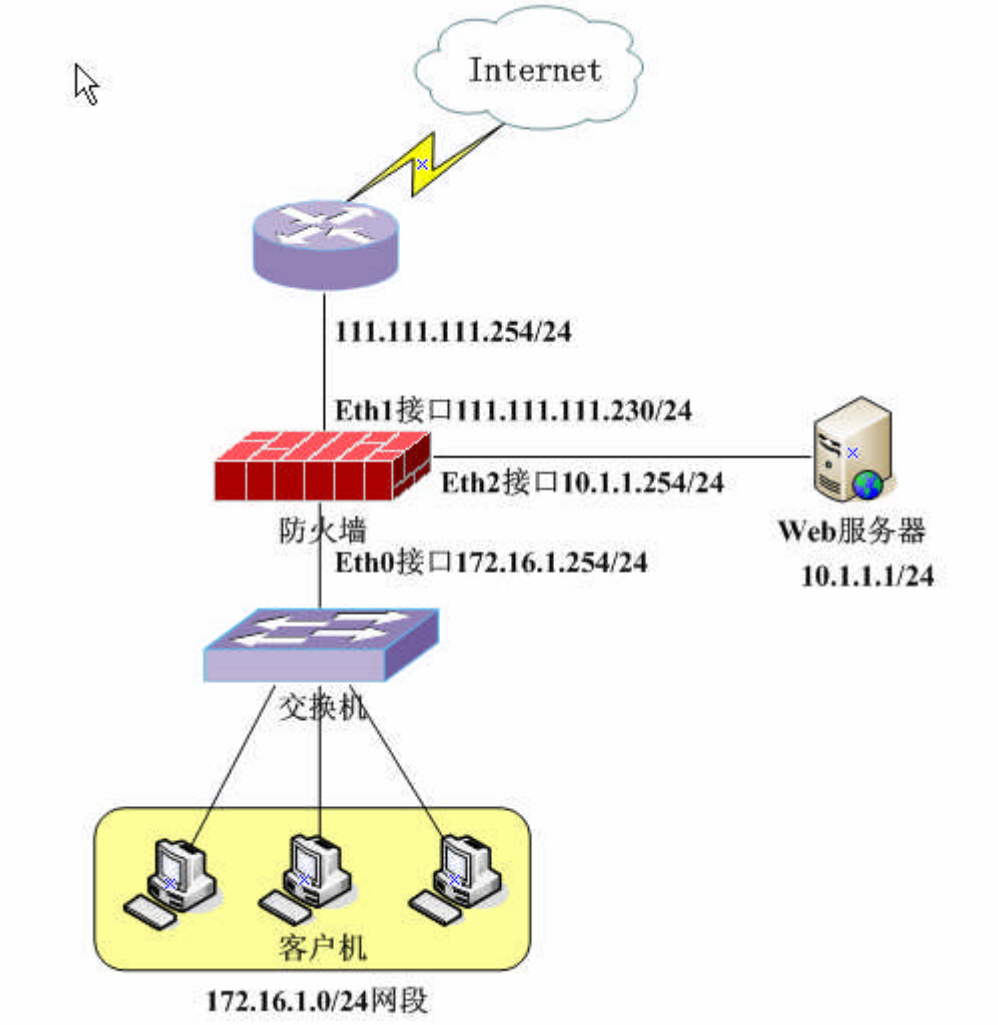
配置需求：

1、内网客户机可以访问互联网

2、外网仅可以访问 WEB 服务器 HTTP 应用，禁止其他访问

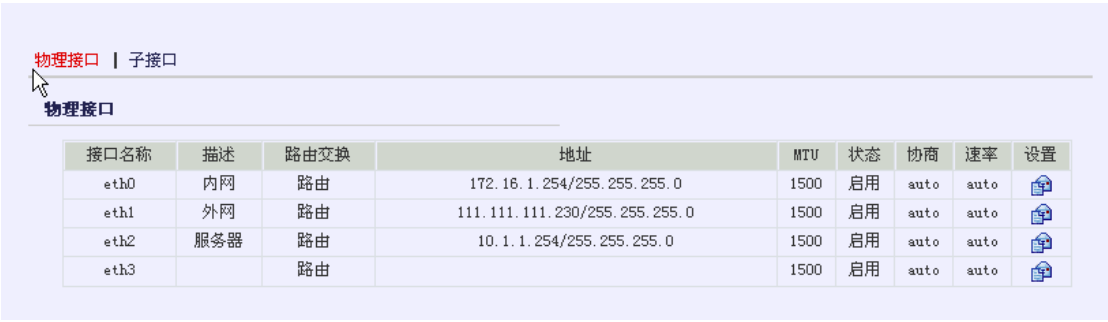
3、外网禁止访问内网

拓扑图如下：



1、防火墙接口 IP 地址配置

进入防火墙管理界面，点击”**网络管理“—“接口” — ”物理接口“**，依次点击每个接口的**“设置”**按钮可以添加每个接口的描述和接口IP地址。



物理接口 | 子接口

物理接口

接口名称	描述	路由交换	地址	MTU	状态	协商	速率	设置
eth0	内网	路由	172.16.1.254/255.255.255.0	1500	启用	auto	auto	
eth1	外网	路由	111.111.111.230/255.255.255.0	1500	启用	auto	auto	
eth2	服务器	路由	10.1.1.254/255.255.255.0	1500	启用	auto	auto	
eth3		路由		1500	启用	auto	auto	

2、区域和缺省访问权限配置

在**“资产管理”—“区域”**中定义防火墙区域（**接入相同安全等级的网络接口的组合为一个区域**），点击**“添加”**。权限选择为**“禁止访问”**，即访问该区域缺省权限为禁止访问。

依次创建若干区域（添加ETH0接口为“内网”区域； ETH1接口为“外网”区域；添加ETH2接口为“服务器”区域；）

☺ 提示：有几个安全等级就需要创建几个区域，即如果网络之间需要配置访问规则，那就需要配置不同的区域。

3、防火墙管理权限设置（定义希望从哪个区域管理防火墙）

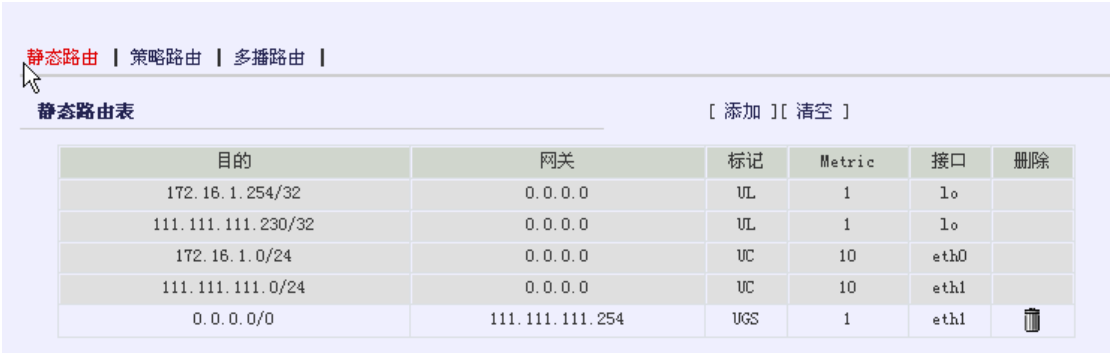
☺ 默认只能从ETH0接口对防火墙进行管理

“内网”区域添加对防火墙的管理权限(当然也可以对“外网”区域添加)，点击**“系统管理”—“配置”—“开放服务”**，点击添加，常用服务有WEBUI(即WEB管理)、ping、Telnet等（请根据管理需要添加相应管理服务）

4、路由表配置

添加静态路由，在**“网络管理”** — **“路由”**—**“静态路由”**，点击**添加**

☺ 添加缺省路由时，目的地址和目的掩码都为0.0.0.0，网关为下一条地址，其他选项为空。



☺ 如果防火墙和客户端之间有三层设备（比如三层交换机或者路由器），请注意添加相应静态路由。

5、**定义对象**（包括地址对象、服务对象、时间对象）

☺ 提示：防火墙所有需要引用对象(如地址转换策略、访问控制策略等)的配置，请先定义对象，才能引用。

<1>**定义地址对象**

添加单个主机对象

点击**"资源管理"－"地址"－"主机"**，点击右上角**"添加配置"**

添加地址范围

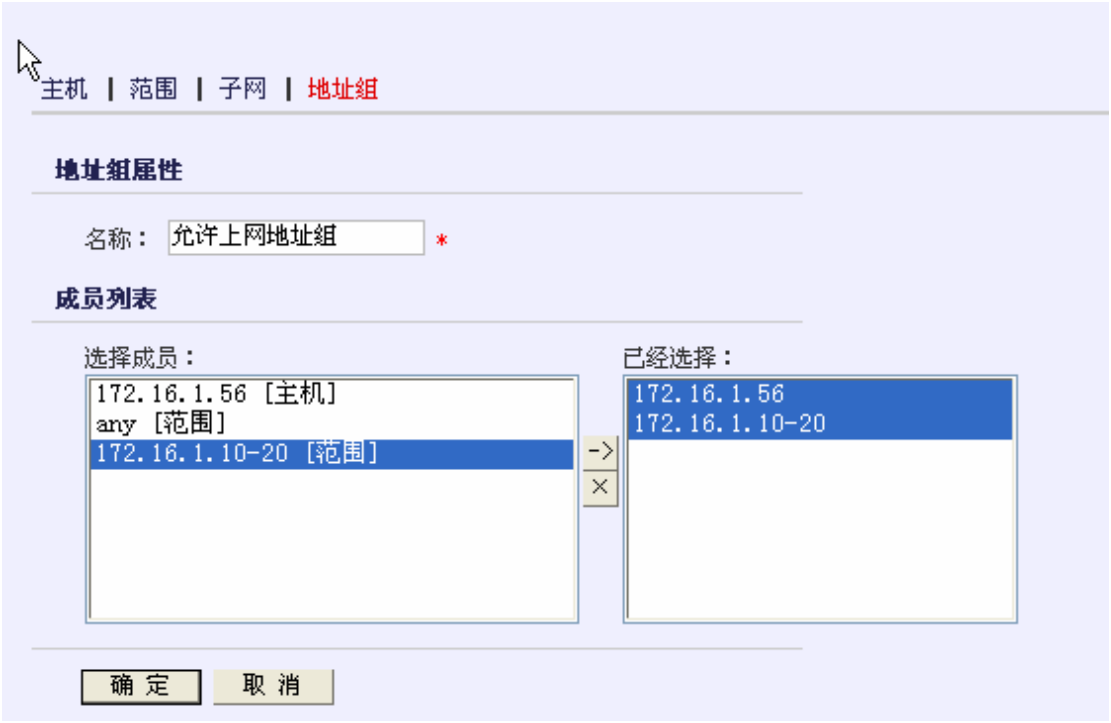
点击**"资源管理"－"地址"－"范围"**，点击右上角**"添加配置"**

添加子网

点击**"资源管理"－"地址"－"子网"**，点击右上角**"添加配置"**

添加地址组

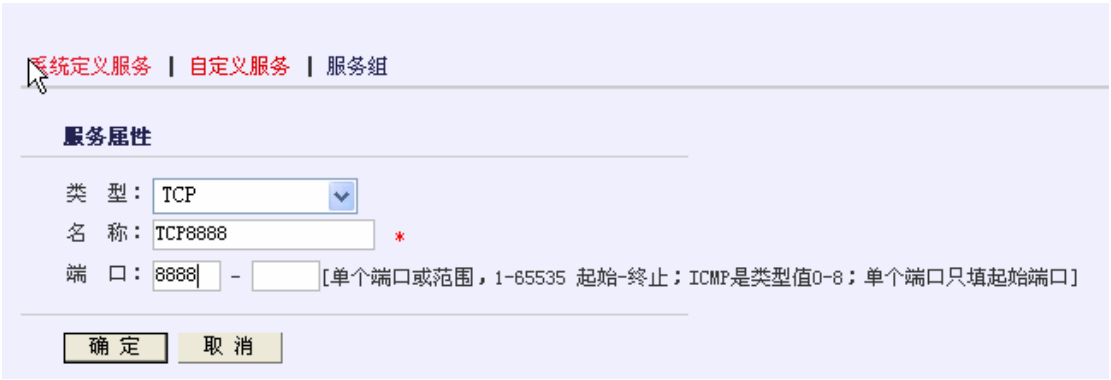
点击**"资源管理"－"地址"－"地址组"，**点击右上角**"添加配置"**

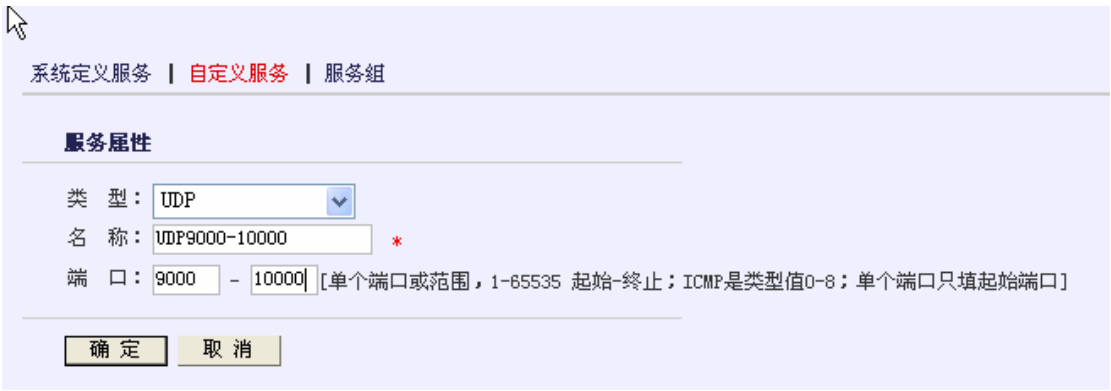


<2>定义服务对象

防火墙内置一些标准服务端口，，但有时用户的系统没有使用某些服务的标准端口，用户在端口引用时，需要我们通过自定义方式加以定义。

点击 **"资源管理"－"服务"－"自定义服务"**，点击**"添加"**，可以添加单个端口或范围 。注意单个端口只填起始端口





<3>定义时间对象

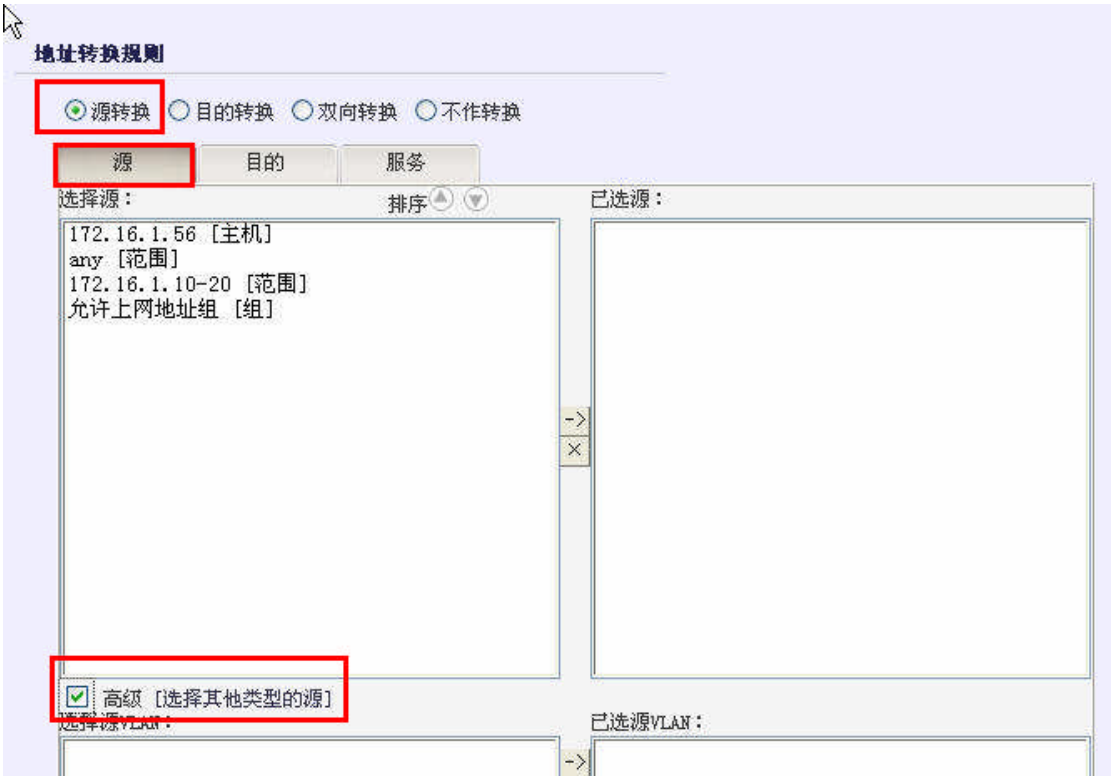
点击“资源管理”—“时间”，点击“添加”，可以设置单次和多次

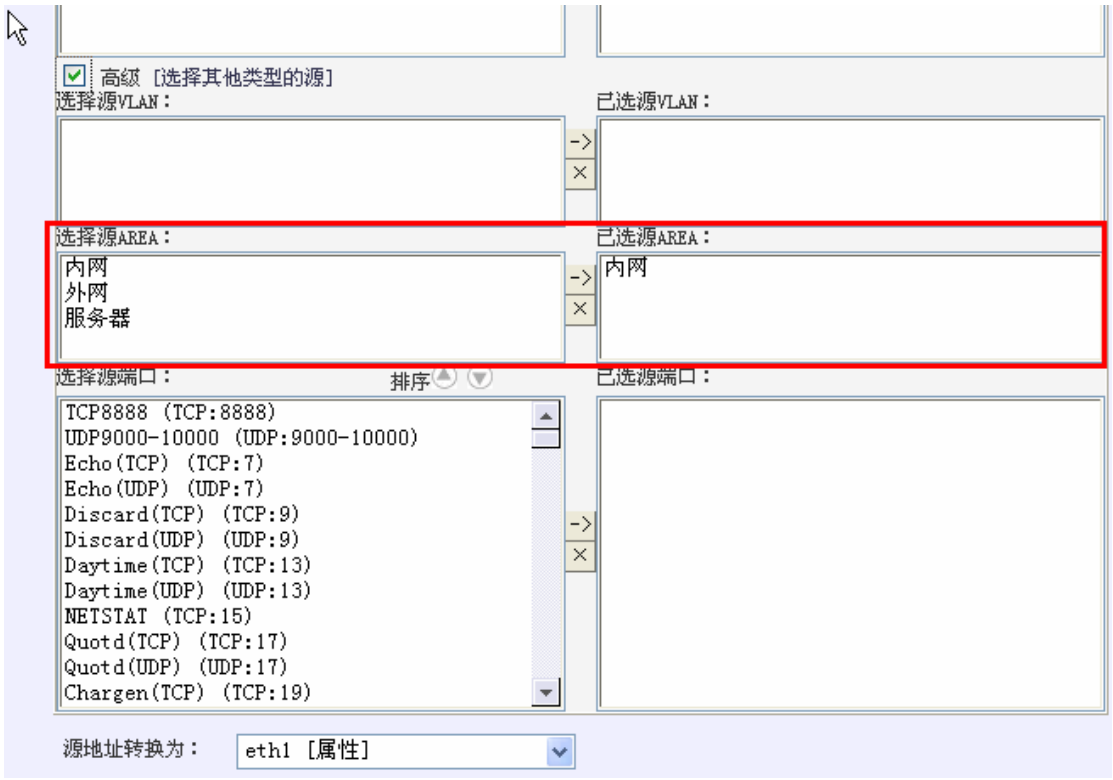
6、地址转换策略

<1>内网可以访问互联网，需要配置源转换

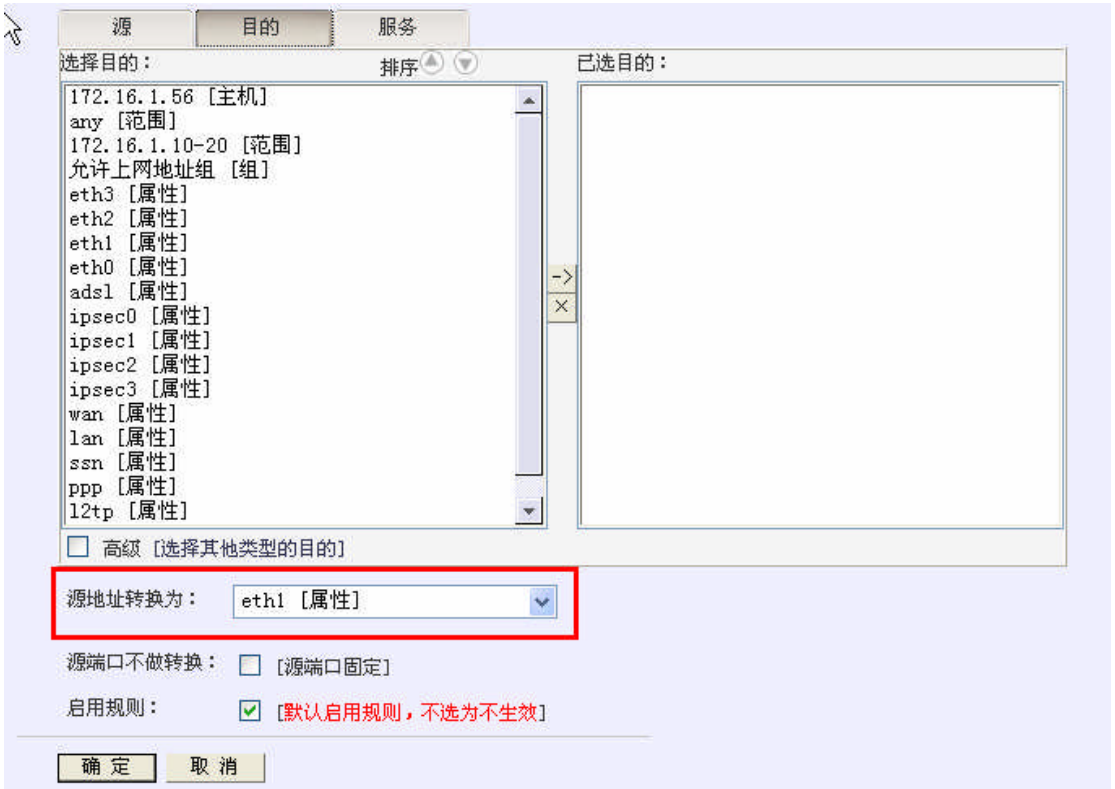
在“防火墙” — “地址转换”，点击 “添加”

选择“源转换”，点击“高级”，源选择源区域“内网”，目的选择目的区域“外网”，源转换为Eth1接口（即转换为Eth1接口IP地址）或者转换111.111.111.230主机地址。

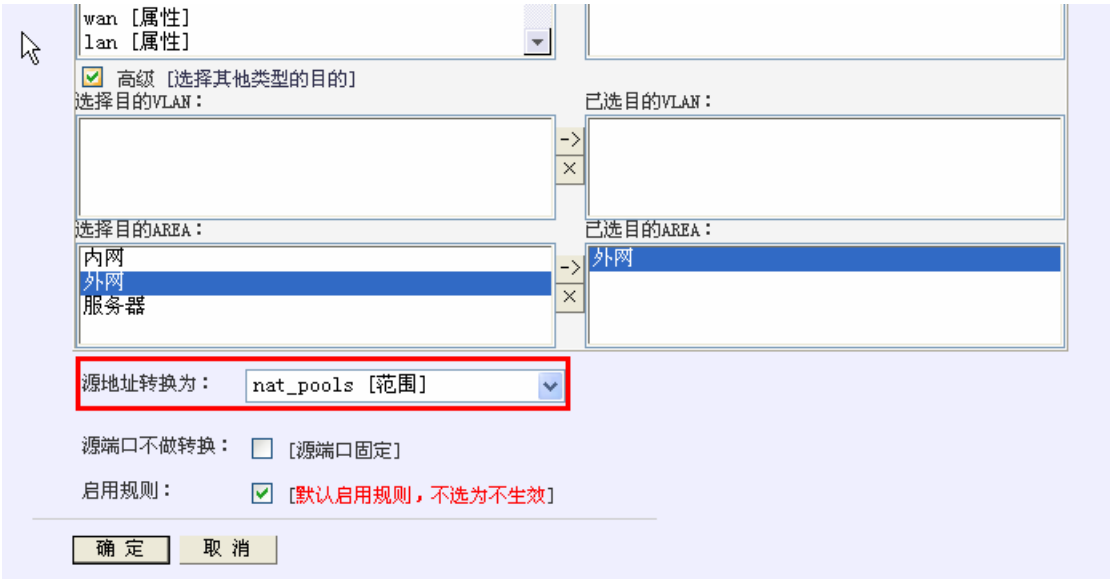



高级 [选择其他类型的源]
选择源VLAN：
已选源VLAN：
选择源AREA：
已选源AREA：
内网
外网
服务器
内网
选择源端口：
排序
已选源端口：
TCP8888 (TCP:8888)
UDP9000-10000 (UDP:9000-10000)
Echo(TCP) (TCP:7)
Echo(UDP) (UDP:7)
Discard(TCP) (TCP:9)
Discard(UDP) (UDP:9)
Daytime(TCP) (TCP:13)
Daytime(UDP) (UDP:13)
NETSTAT (TCP:15)
Quotd(TCP) (TCP:17)
Quotd(UDP) (UDP:17)
Chargen(TCP) (TCP:19)
源地址转换为：
eth1 [属性]


地址转换规则
源转换
目的转换
双向转换
不作转换
源
目的
服务
选择目的：
排序
已选目的：
172.16.1.56 [主机]
any [范围]
172.16.1.10-20 [范围]
允许上网地址组 [组]
eth3 [属性]
eth2 [属性]
eth1 [属性]
eth0 [属性]
adsl [属性]
ipsec0 [属性]
ipsec1 [属性]
ipsec2 [属性]
ipsec3 [属性]
wan [属性]
lan [属性]
ssn [属性]
ppp [属性]
l2tp [属性]
高级 [选择其他类型的目的]
选择目的VLAN：
已选目的VLAN：

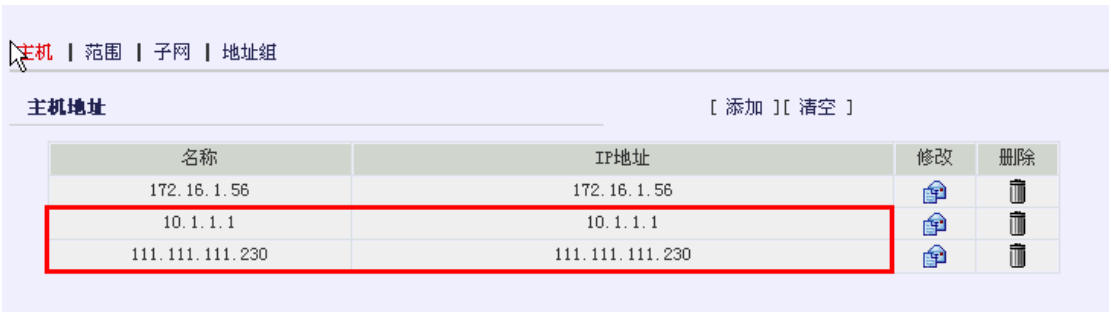


☺ 如果需要源地址转换为一段地址，则首先需要创建一段地址范围，且该地址范围不能设置排除IP地址。



<2>Web服务器发布，需要配置目的转换

首先需要添加Web服务器地址对象（10.1.1.1，服务器真实地址）、外网访问的地址对象（111.111.111.230，合法地址），具体配置见**定义对象**章节。



☺ 目的转换有两种方式：地址转换、端口转换。

地址转换：从一个 IP 地址到另一个 IP 地址的映射。安全网关设备将到达

映射地址（合法IP）的所有信息流中的目标IP 地址转换成主机 IP 地址（即服务器真实地址）。**地址转换建议在映射地址资源充裕时、服务器使用端口较多且端口不连续、服务器端口不是固定端口时使用。**

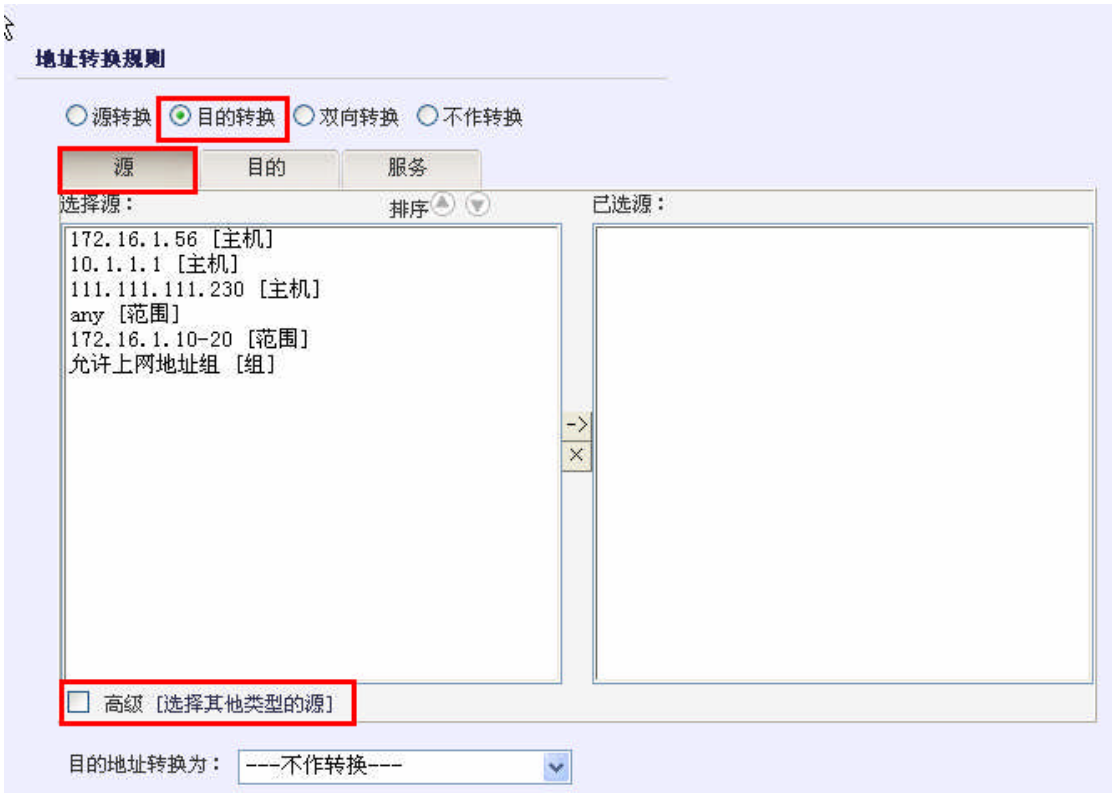
端口转换：从一个 IP 地址到基于目标端口号的多个IP 地址的映射，即单个 IP 地址可以托管从若干服务（使用不同的目标端口号标识）到同样多主机的映射。**端口转换建议在映射地址资源短缺且服务器端口为固定端口时使用。**

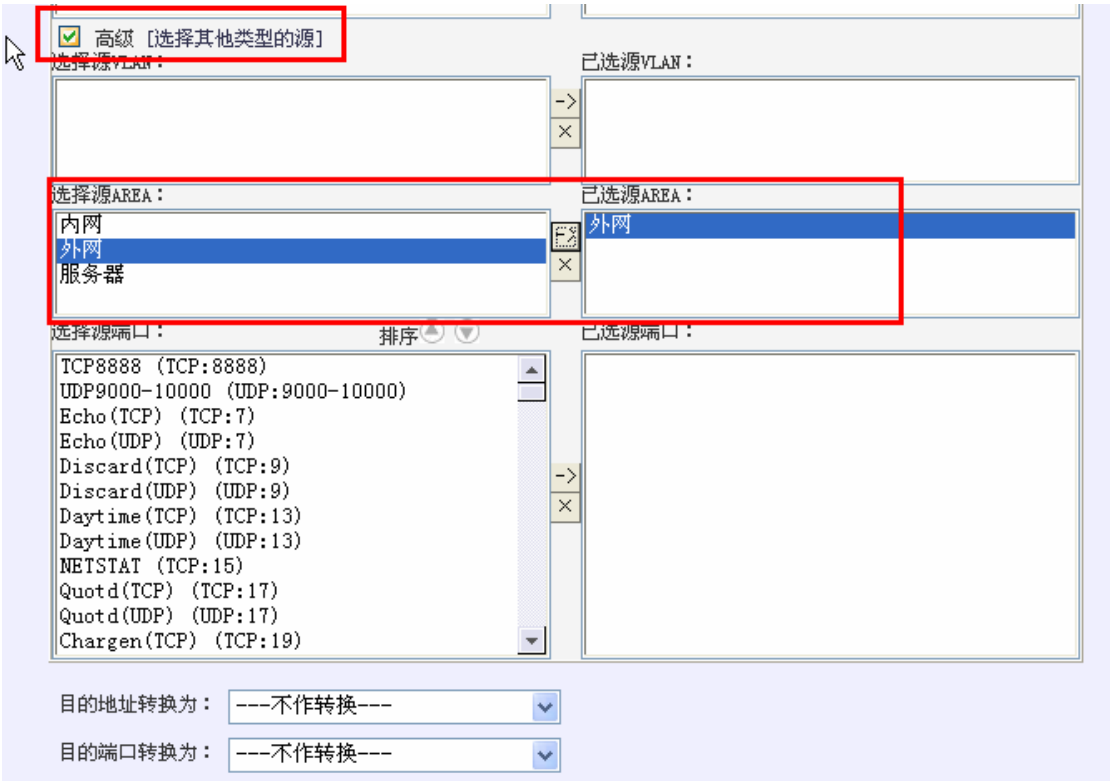
配置Web服务器映射有两种方式：

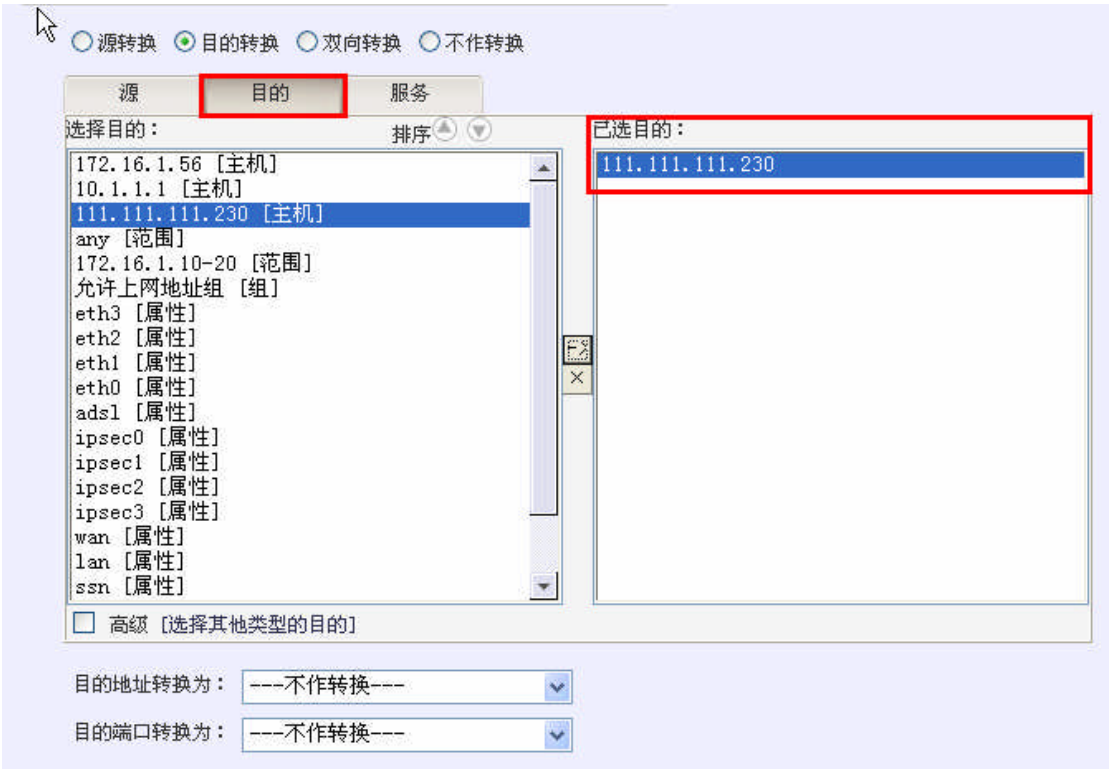
（Ⅰ）端口转换

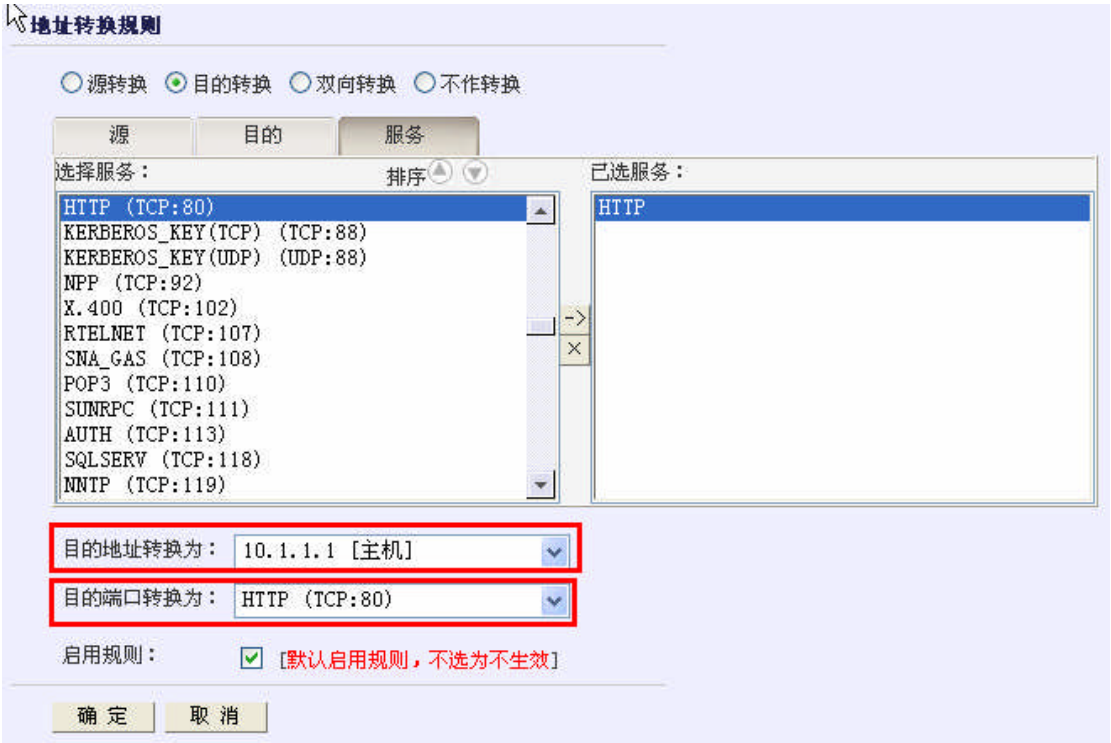
在**“防火墙” — “地址转换”**，点击 **“添加”**

选择**“目的转换”**，点击**“高级”**，源选择源区域**“外网”**，目的选择**“外网访问的地址对象（111.111.111.230）”**，服务选择**“HTTP”**服务，目的地址转换为选择**“Web服务器地址对象（10.1.1.1），即服务器真实地址”**，目的端口转换为**“HTTP”**服务。




高级 [选择其他类型的源]
选择源VLAN：
已选源VLAN：
选择源AREA：
内网
外网
服务器
已选源AREA：
外网
选择源端口：
排序
已选源端口：
TCP8888 (TCP:8888)
UDP9000-10000 (UDP:9000-10000)
Echo(TCP) (TCP:7)
Echo(UDP) (UDP:7)
Discard(TCP) (TCP:9)
Discard(UDP) (UDP:9)
Daytime(TCP) (TCP:13)
Daytime(UDP) (UDP:13)
NETSTAT (TCP:15)
Quotd(TCP) (TCP:17)
Quotd(UDP) (UDP:17)
Chargen(TCP) (TCP:19)
目的地址转换为：
---不作转换---
目的端口转换为：
---不作转换---

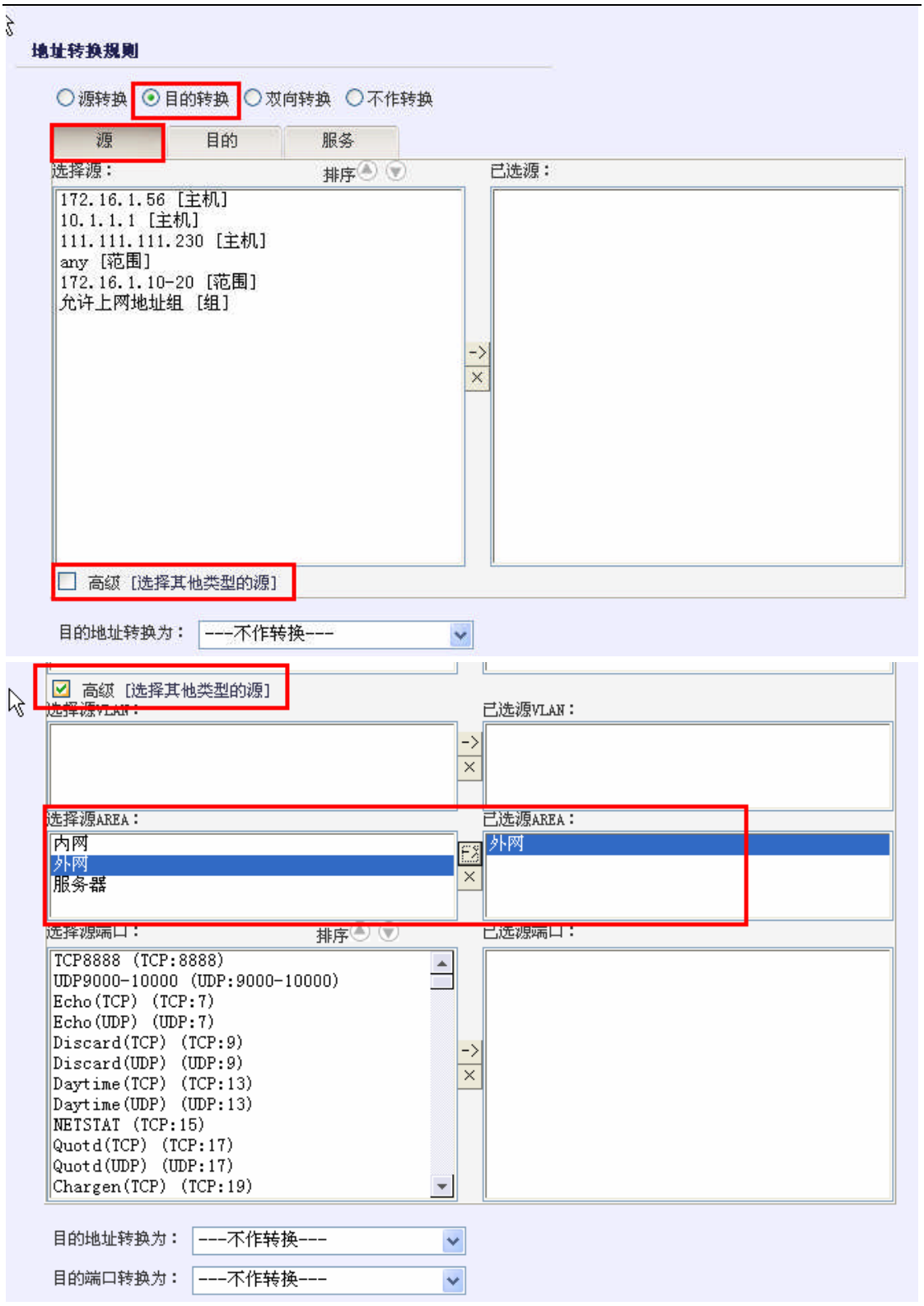

源转换
目的转换
双向转换
不作转换
源
目的
服务
选择目的：
排序
已选目的：
111.111.111.230
172.16.1.56 [主机]
10.1.1.1 [主机]
111.111.111.230 [主机]
any [范围]
172.16.1.10-20 [范围]
允许上网地址组 [组]
eth3 [属性]
eth2 [属性]
eth1 [属性]
eth0 [属性]
adsl [属性]
ipsec0 [属性]
ipsec1 [属性]
ipsec2 [属性]
ipsec3 [属性]
wan [属性]
lan [属性]
ssn [属性]
高级 [选择其他类型的目的]
目的地址转换为：
---不作转换---
目的端口转换为：
---不作转换---

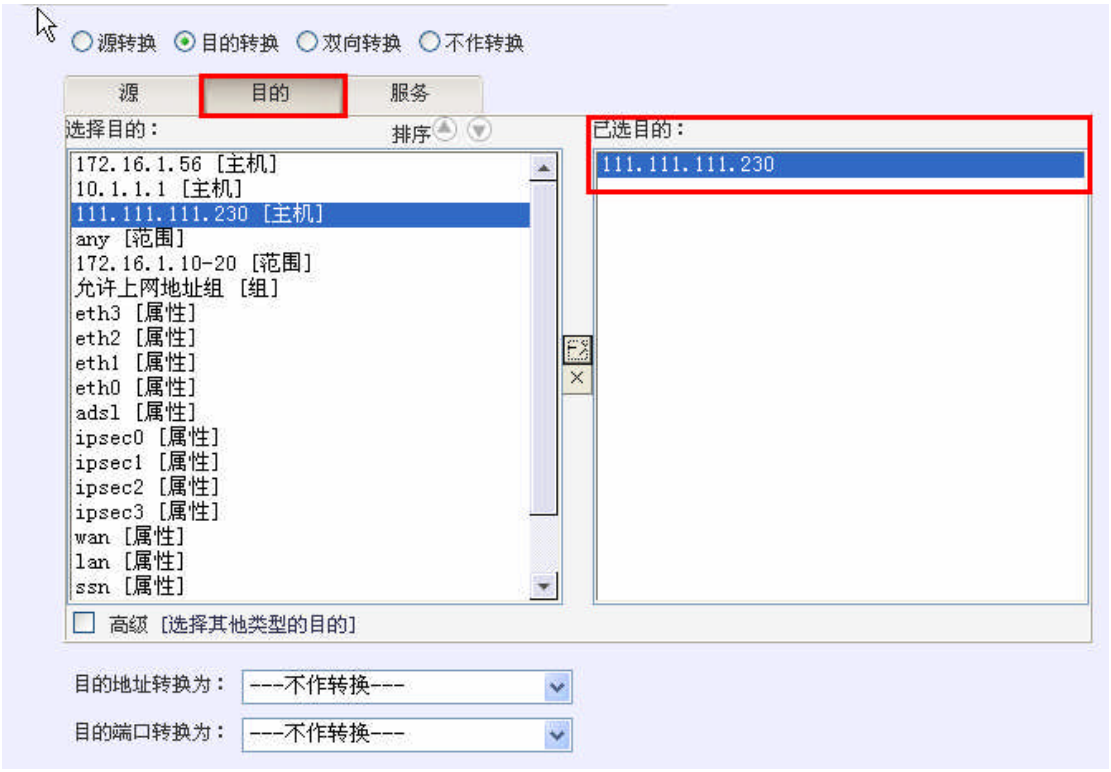


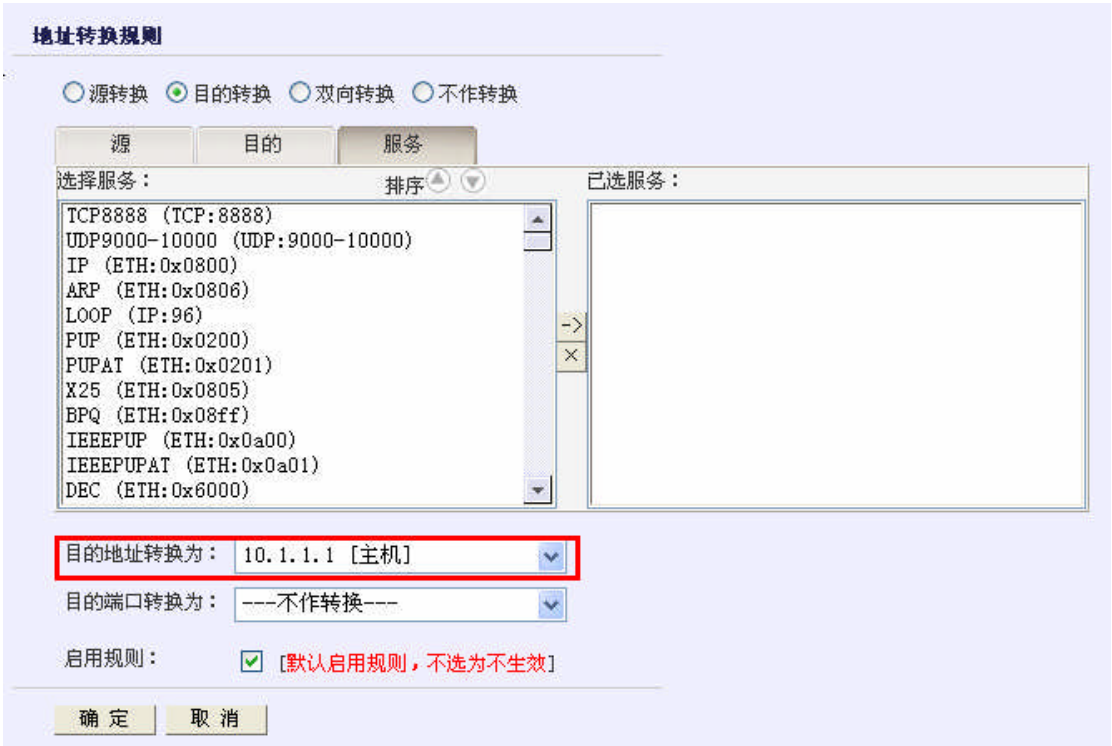
（Ⅱ）地址映射

在**“防火墙” — “地址转换”**，点击 **“添加”**

选择**“目的转换”**，点击**“高级”**，源选择源区域**“外网”**，目的选择**“外网访问的地址对象（111.111.111.230）”**，目的地址转换为选择**“Web服务器地址对象（10.1.1.1），即服务器真实地址”**。


地址转换规则
源转换
目的转换
双向转换
不作转换
源
目的
服务
选择源：
排序
已选源：
172.16.1.56 [主机]
10.1.1.1 [主机]
111.111.111.230 [主机]
any [范围]
172.16.1.10-20 [范围]
允许上网地址组 [组]
高级 [选择其他类型的源]
目的地址转换为：
---不作转换---
高级 [选择其他类型的源]
选择源VLAN：
已选源VLAN：
选择源AREA：
已选源AREA：
内网
外网
服务器
外网
选择源端口：
排序
已选源端口：
TCP8888 (TCP:8888)
UDP9000-10000 (UDP:9000-10000)
Echo(TCP) (TCP:7)
Echo(UDP) (UDP:7)
Discard(TCP) (TCP:9)
Discard(UDP) (UDP:9)
Daytime(TCP) (TCP:13)
Daytime(UDP) (UDP:13)
NETSTAT (TCP:15)
Quotd(TCP) (TCP:17)
Quotd(UDP) (UDP:17)
Chargen(TCP) (TCP:19)
目的地址转换为：
---不作转换---
目的端口转换为：
---不作转换---





第一条为内网访问外网做源转换；

第二条为外网访问WEB服务器的映射地址，防火墙把包转发给服务器的真实IP。

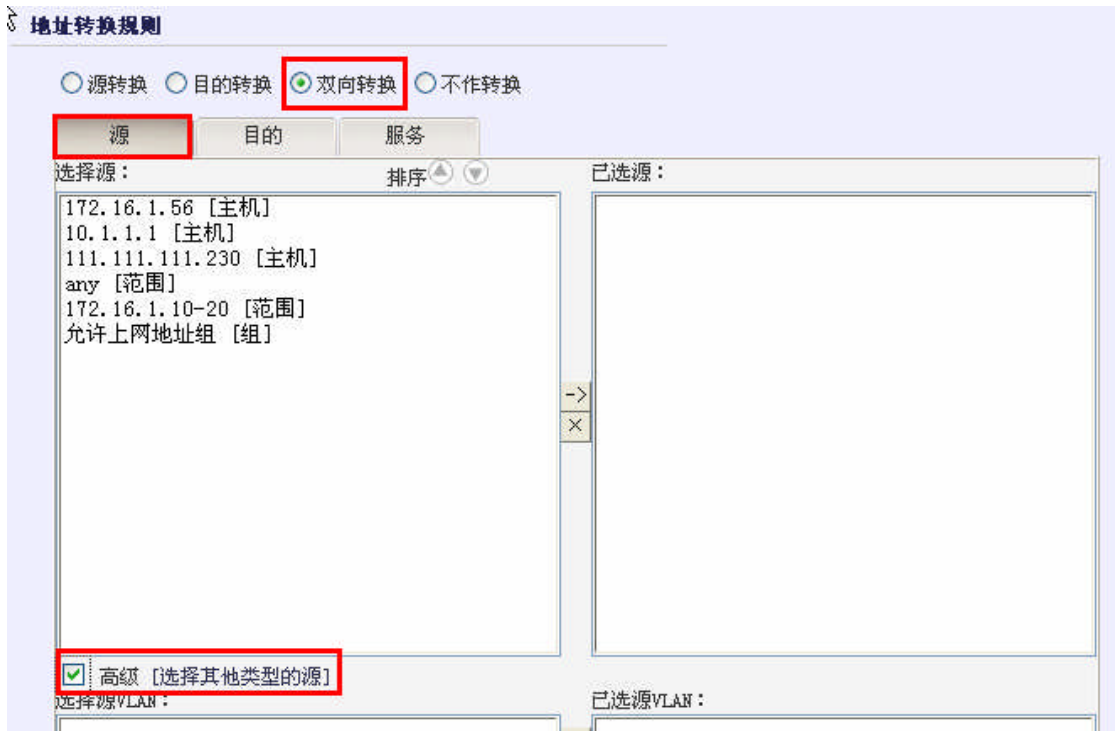
☺ **地址转换需要注意的问题：**

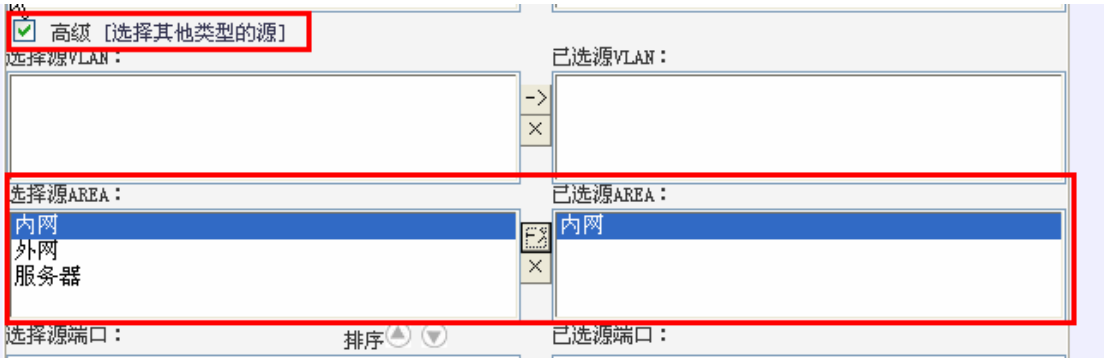
1、天融信防火墙先匹配目的转换规则，再对其他的地址转换规则按照从上往下的顺序进行匹配，在目的转换规则中也是按照排列顺序进行匹配。在匹配过程中，一旦存在一条匹配的地址转换规则，防火墙将停止检索，并按所定义的规则处理数据包，所以规则的类型和先后顺序决定了数据包的处理方式，目的NAT规则要优先于其他NAT 规则。

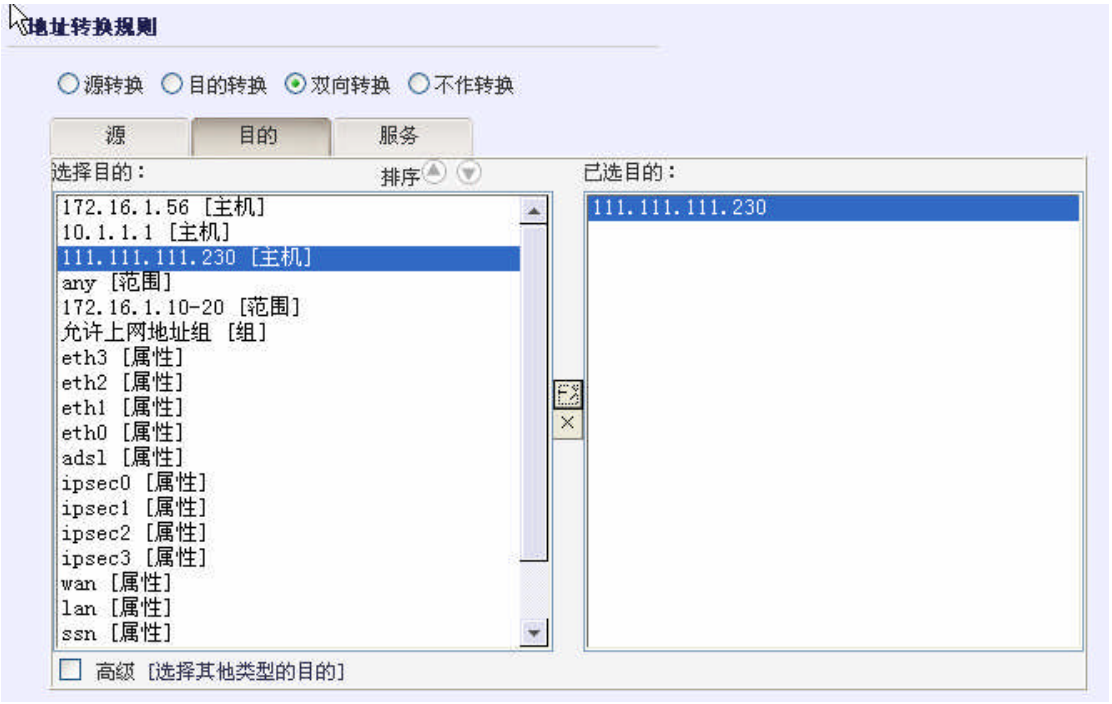
2、**如果内网用户需要通过服务器映射地址访问web服务器时，还需针对内网添加地址转换。**如案例如果内网需要访问111.111.111.230（合法地址）来访问web服务器需要单独添加地址转换。下面以端口转换为例，地址转换请参照外网访问web服务器。

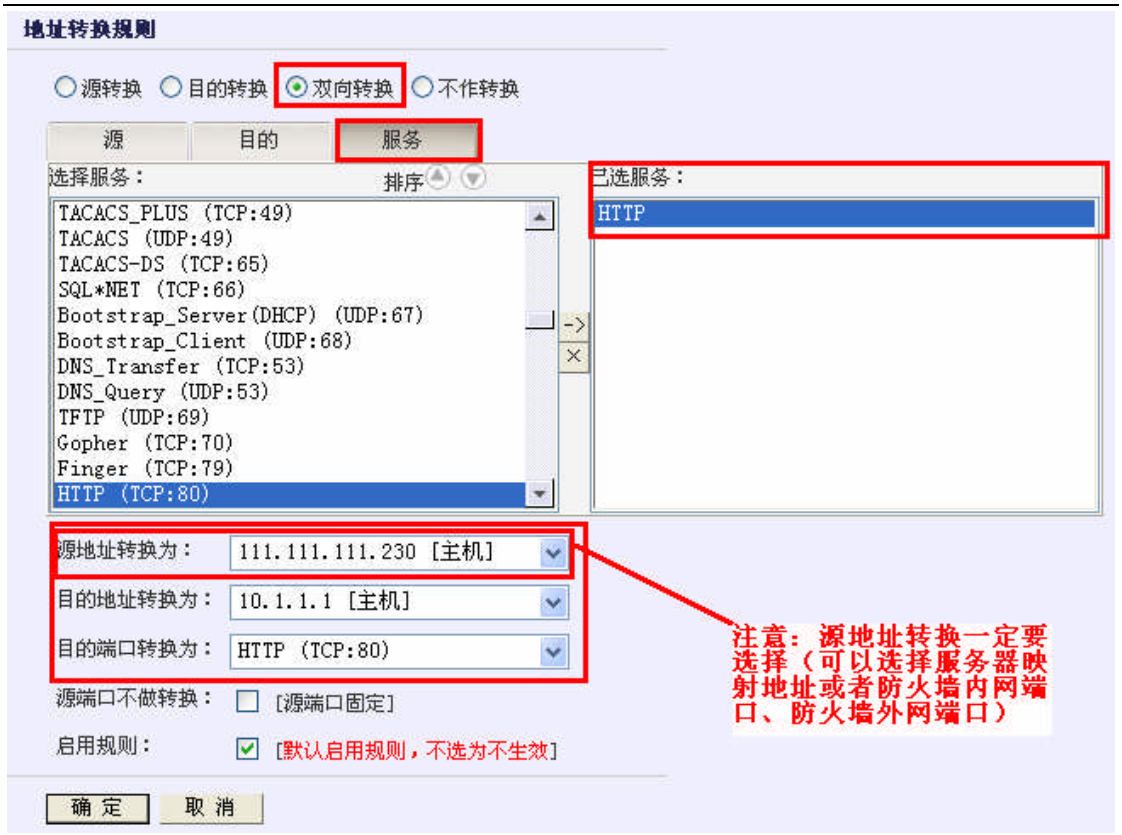
在**“防火墙” — “地址转换”**，点击 **“添加”**

选择**“双向转换”**，点击**“高级”**，源选择源区域**“内网”**，目的选择**“外网访问的地址对象（111.111.111.230）”**，服务选择**“HTTP”**服务，目的端口转换为**“HTTP”**服务。源地址转为选择**“外网访问的地址对象（111.111.111.230）”**，目的地址转换为选择**“Web服务器地址对象（10.1.1.1），即服务器真实地址”**，目的转换为选择**“HTTP服务“**。


地址转换规则
源转换
目的转换
双向转换
不作转换
源
目的
服务
选择源：
排序
已选源：
172.16.1.56 [主机]
10.1.1.1 [主机]
111.111.111.230 [主机]
any [范围]
172.16.1.10-20 [范围]
允许上网地址组 [组]
高级 [选择其他类型的源]
选择源VLAN：
已选源VLAN：


高级 [选择其他类型的源]
选择源VLAN：
已选源VLAN：
选择源AREA：
已选源AREA：
内网
外网
服务器
选择源端口：
排序
已选源端口：


地址转换规则
源转换
目的转换
双向转换
不作转换
源
目的
服务
选择目的：
排序
已选目的：
172.16.1.56 [主机]
10.1.1.1 [主机]
111.111.111.230 [主机]
any [范围]
172.16.1.10-20 [范围]
允许上网地址组 [组]
eth3 [属性]
eth2 [属性]
eth1 [属性]
eth0 [属性]
adsl [属性]
ipsec0 [属性]
ipsec1 [属性]
ipsec2 [属性]
ipsec3 [属性]
wan [属性]
lan [属性]
ssn [属性]
111.111.111.230
高级 [选择其他类型的目的]



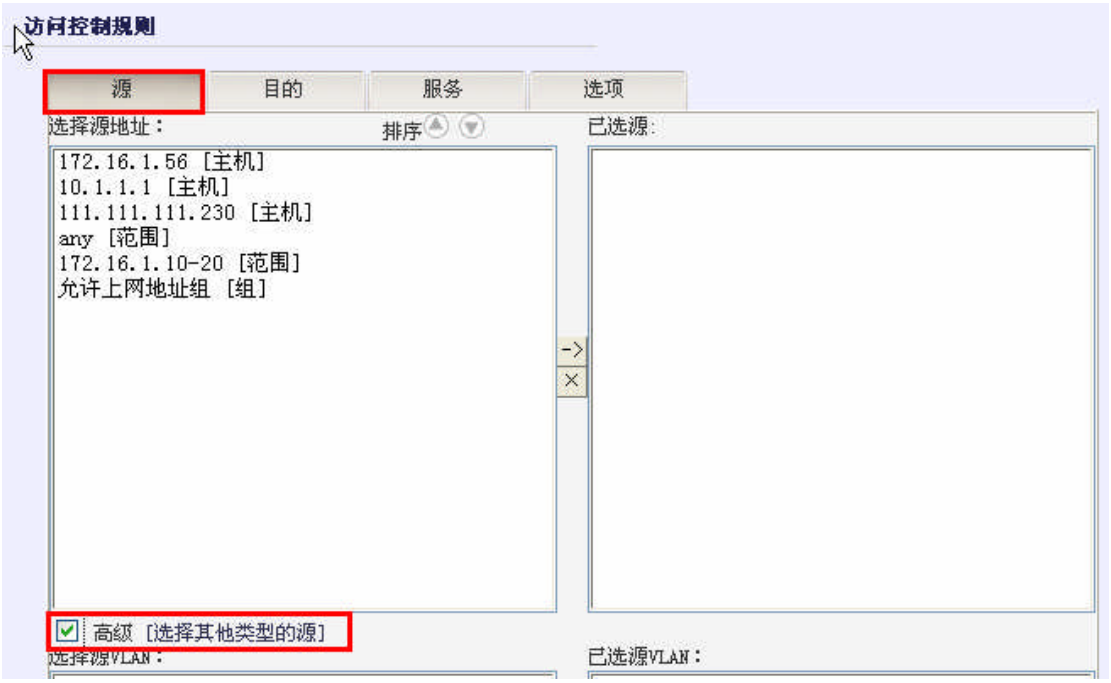
7、制定访问控制策略

在**“防火墙”** — **“访问控制”**，点击 **“添加”**

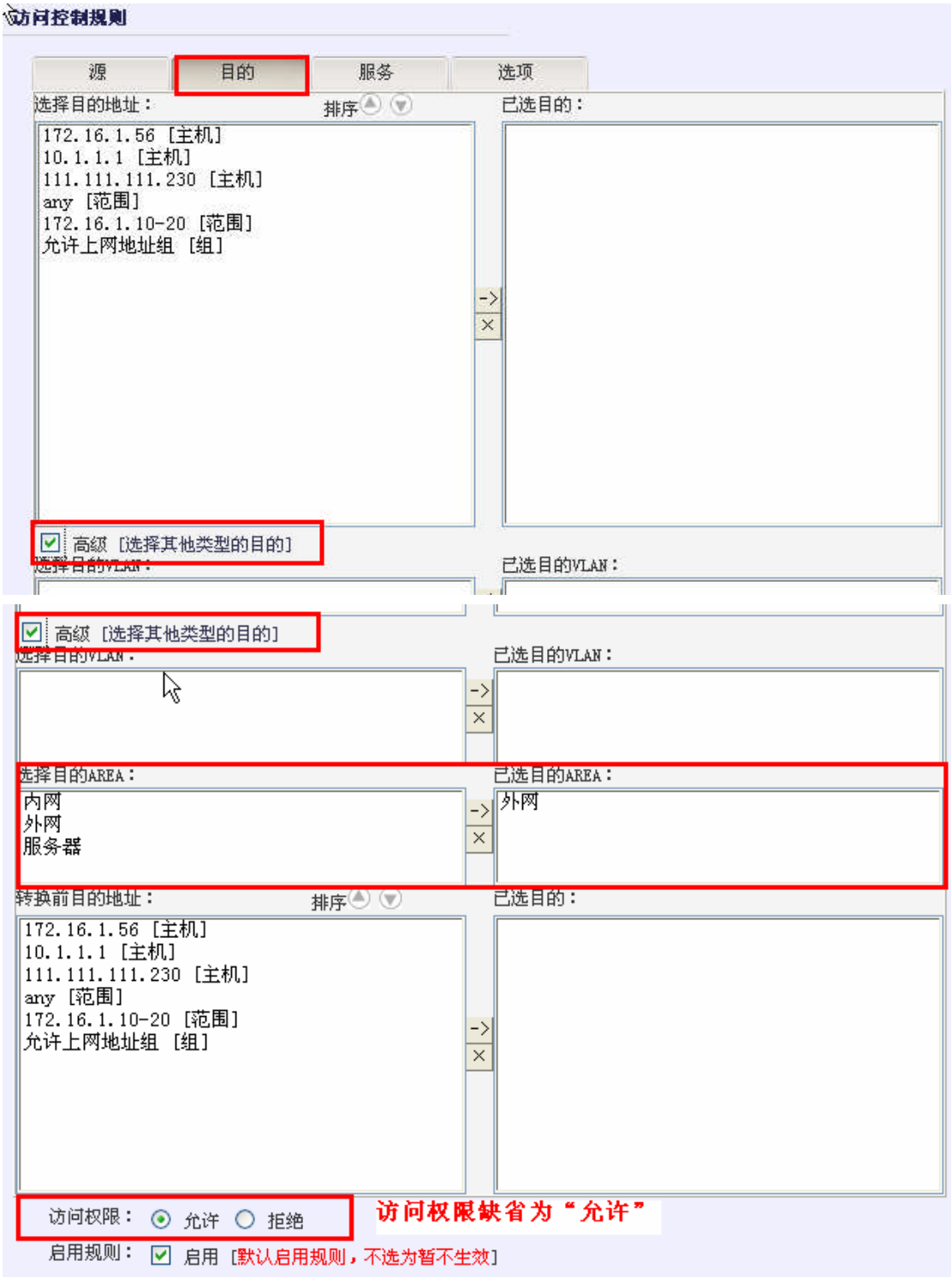
<1>第一条规则定义内网可以访问外网

在**“防火墙”** — **“访问控制”**，点击 **“添加”**

选择**“源”**，点击**“高级”**，源选择源区域**“内网”**，目的选择目的区域**“外网”** ，点击**“高级”**，动作“允许”（默认选项）。


访问控制规则
源
目的
服务
选项
选择源地址：
排序
已选源:
172.16.1.56 [主机]
10.1.1.1 [主机]
111.111.111.230 [主机]
any [范围]
172.16.1.10-20 [范围]
允许上网地址组 [组]
高级 [选择其他类型的源]
选择源VLAN：
已选源VLAN：


高级 [选择其他类型的源]
选择源VLAN：
已选源VLAN：
选择源AREA：
已选源AREA：
内网
外网
服务器
内网
选择源端口：
排序
已选源端口：
TCP8888 (TCP:8888)
UDP9000-10000 (UDP:9000-10000)
Echo(TCP) (TCP:7)
Echo(UDP) (UDP:7)
Discard(TCP) (TCP:9)
Discard(UDP) (UDP:9)
Daytime(TCP) (TCP:13)
Daytime(UDP) (UDP:13)
NETSTAT (TCP:15)
Quotd(TCP) (TCP:17)
Quotd(UDP) (UDP:17)
Chargen(TCP) (TCP:19)
访问权限： 允许 拒绝
启用规则： 启用 [默认启用规则，不选为暂不生效]

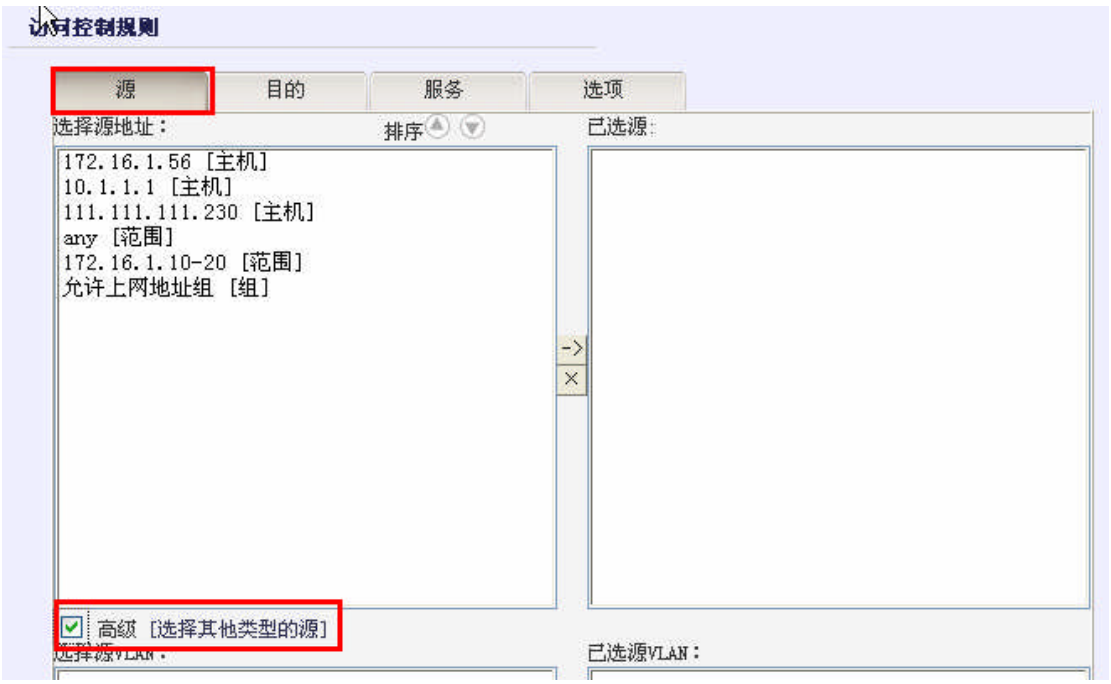


<2>第二条规则定义外网可以访问服务器的对外发布的应用端口，只能访问服务器http应用。

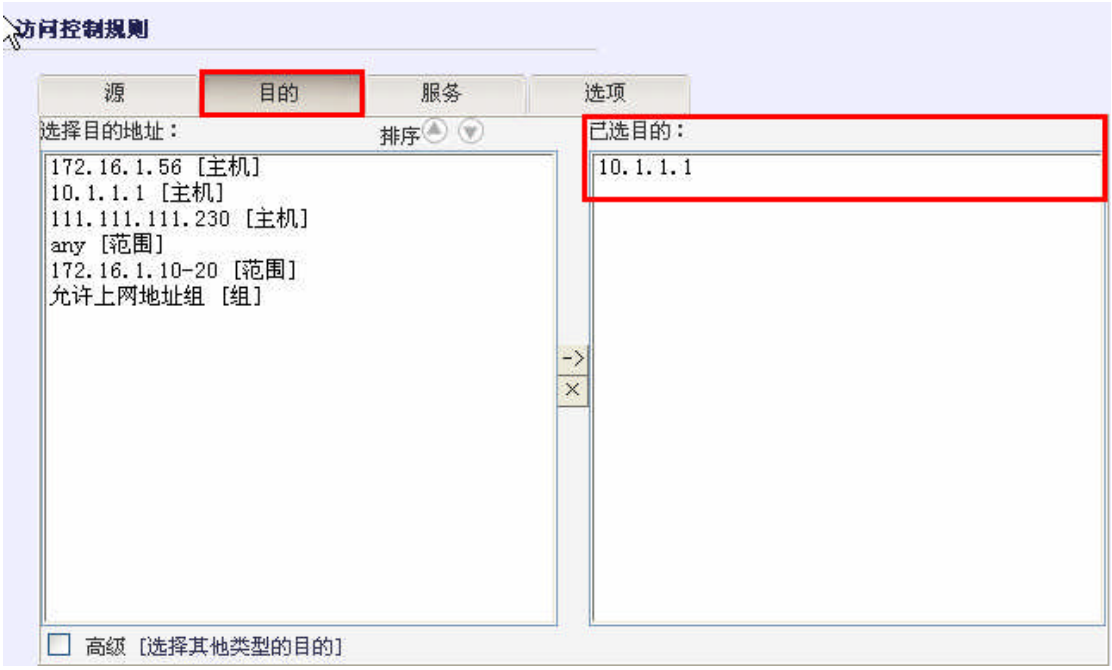
在**“防火墙” — “访问控制”**，点击 **“添加”**

选择**“源”**，点击**“高级”**，源选择源区域**“内网、外网”**， 目的选择“Web**服务器地址对象（10.1.1.1），即服务器真实地址**”， 服务选择”HTTP服务”，

动作“允许”（默认选项）。


访问控制规则
源
目的
服务
选项
选择源地址：
排序
已选源：
172.16.1.56 [主机]
10.1.1.1 [主机]
111.111.111.230 [主机]
any [范围]
172.16.1.10-20 [范围]
允许上网地址组 [组]
高级 [选择其他类型的源]
选择源VLAN：
已选源VLAN：


高级 [选择其他类型的源]
选择源VLAN：
已选源VLAN：
选择源AREA：
已选源AREA：
内网
外网
服务器
外网
选择源端口：
排序
已选源端口：


访问控制规则
源
目的
服务
选项
选择目的地址：
排序
已选目的：
172.16.1.56 [主机]
10.1.1.1 [主机]
111.111.111.230 [主机]
any [范围]
172.16.1.10-20 [范围]
允许上网地址组 [组]
10.1.1.1
高级 [选择其他类型的目的]

第一条规则定义内网可以访问外网。源选择**“外网”**；目的可以选择目的区域—**“外网”**，动作“允许”（默认选项）。

第二条规则定义外网可以访问服务器的对外发布的应用端口，只能访问服务器http应用。源选择**“内网、外网”**，目的选择服务器真实的IP地址10.1.1.1，服务选择“HTTP”服务。

☺ 访问规则需要注意的问题：

访问控制规则描述了天融信防火墙允许或禁止匹配访问控制规则的报文通过。防火墙接收到报文后，将顺序匹配访问控制规则表中所设定规则。一旦寻找到匹配的规则，则按照该策略所规定的操作（允许或丢弃）处理该报文，不再进行区域缺省属性的检查。如果不存在可匹配的访问策略，天融信防火墙将根据目的接口所在区域的缺省属性（允许访问或禁止访问），处理该报文。区域属性设置请参见 “3、区域和缺省访问权限配置”。

1、规则作用有顺序

2、访问控制列表遵循第一匹配规则

3、规则的一致性和逻辑性

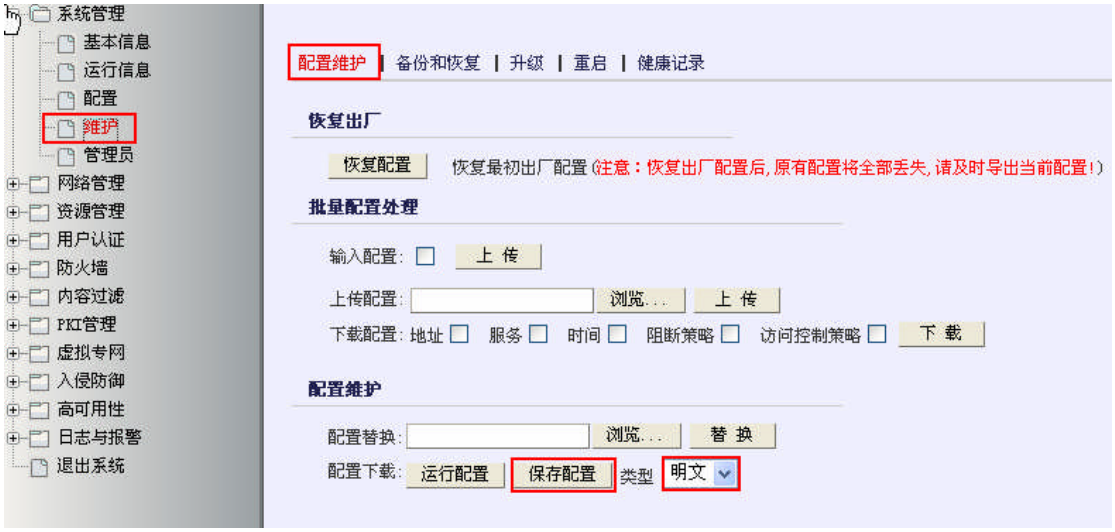
10、配置保存

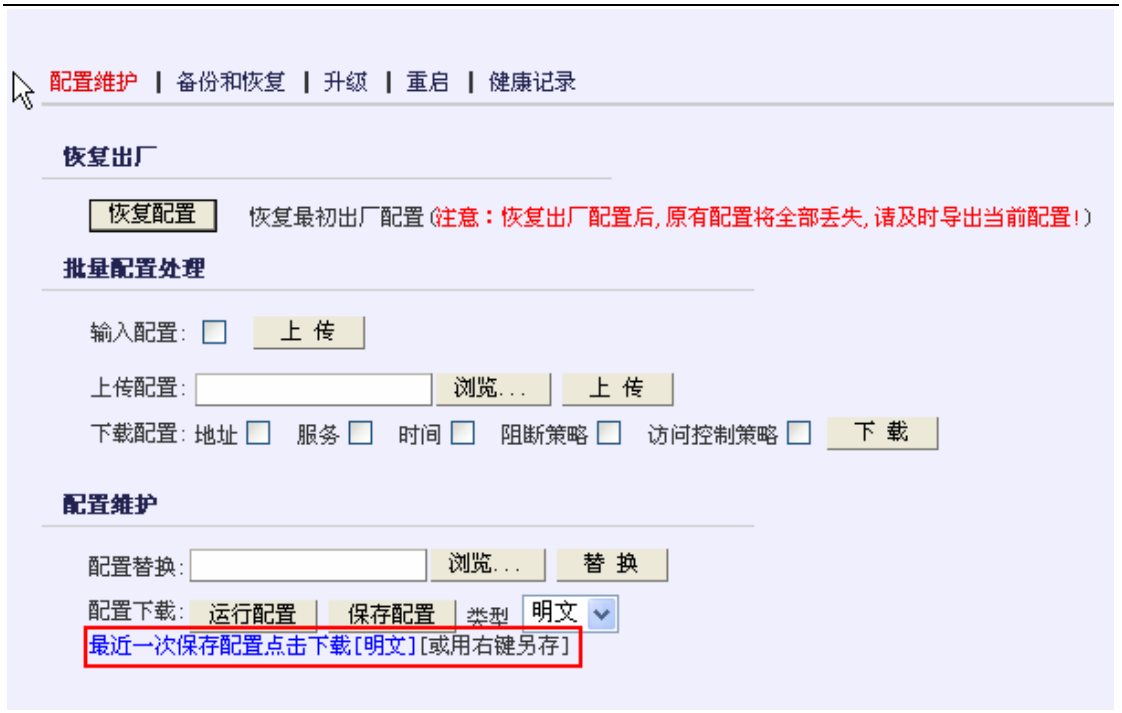
点击管理界面右上角**“保存配置”**

☺ 配置完成后，配置立即生效，但是一定要保存配置，否则设备断电或重新启动后未保存配置将丢失。保存的配置将作为下次设备启动配置。

11、配置文件备份

配置完成并确认运行正常以后，请备份配置文件。选择**“系统管理”—“维护”—“配置维护”**，选择**“保存配置”**





☺ 提示：每次修改配置前，建议首先备份防火墙再修改配置，避免防火墙配置不当造成网络长时间中断。

（2）防火墙透明模式案例配置

在透明模式下，天融信防火墙的所有接口均作为交换接口工作。也就是说，对于同一VLAN 的数据包在转发时不作任何改动，包括IP 和MAC 地址，直接把包转发出去。同时，天融信防火墙可以在设置了IP 的VLAN 之间进行路由转发。

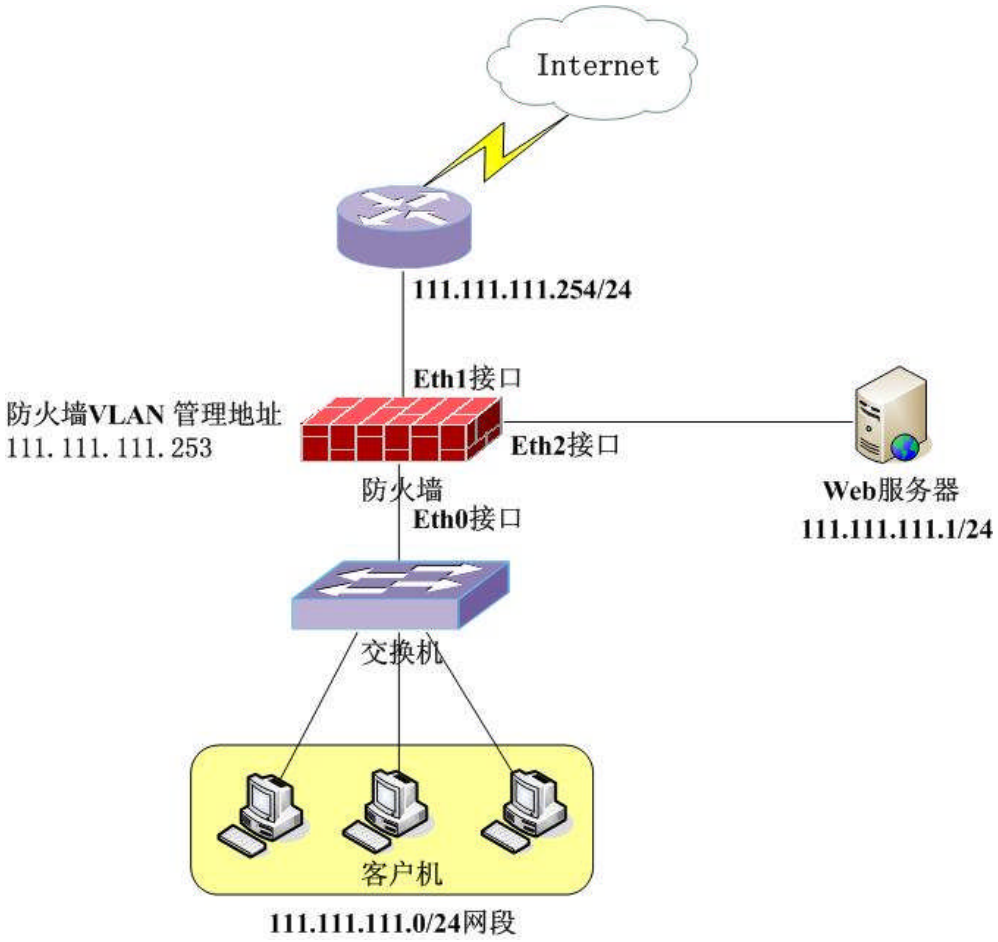
配置需求：

1、内网客户机可以访问互联网

2、外网仅可以访问 WEB 服务器 HTTP 应用，禁止其他访问

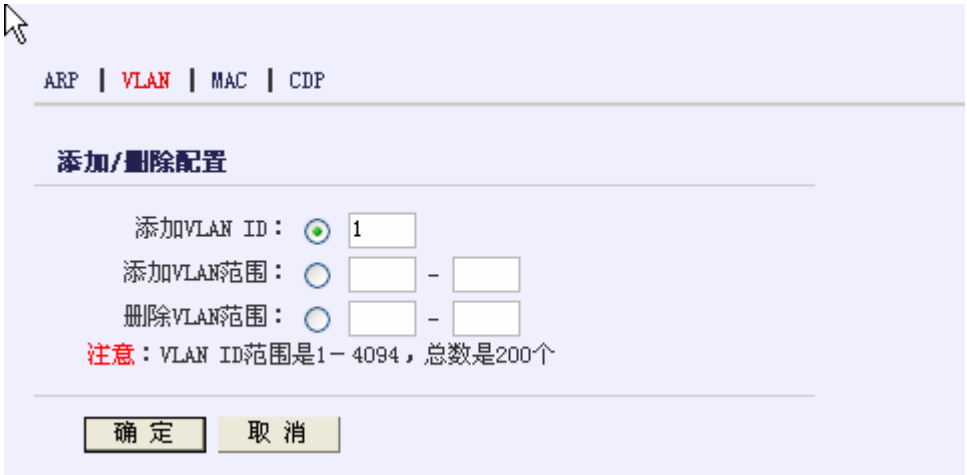
3、外网禁止访问内网

拓扑图如下：



1、防火墙接口IP配置

<1>定义一个VLAN(本案例创建VLAN 1)，点击“网络管理”—“二层网络”—“VLAN”—“添加/删除VLAN范围”。



<2>设置VLAN 1接口IP地址及子网掩码。

<3>分别把ETH0、ETH1、ETH2接口加入到VLAN 1中，点击”网络管理“—“接口” — ”物理接口“，依次点击接口的“设置”按钮可以把接口加入到VLAN 1中。

2、区域和缺省访问权限配置

在**“资产管理”—“区域”**中定义防火墙区域（**接入相同安全等级的网络接口的组合为一个区域**），点击**“添加”**。权限选择为**“禁止访问”**，即访问该区域缺省权限为禁止访问。

依次创建若干区域（添加ETH0接口为“内网”区域； ETH1接口为“外网”区域；添加ETH2接口为“服务器”区域；）

☺ 提示：有几个安全等级就需要创建几个区域，即如果网络之间需要配置访问规则，那就需要配置不同的区域。

3、防火墙管理权限设置（定义希望从哪个区域管理防火墙）

☺ 默认只能从ETH0接口对防火墙进行管理

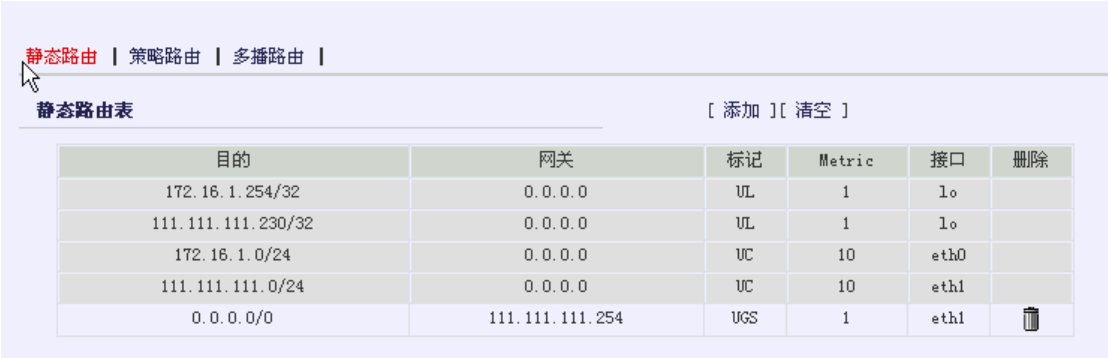
“内网”区域添加对防火墙的管理权限(当然也可以对“外网”区域添加)，点击**“系统管理”—“配置”—“开放服务”**，点击添加，常用服务有WEBUI(即WEB管理)、ping、Telnet等（请根据管理需要添加相应管理服务）

4、路由表配置

☺ 如果防火墙和客户端之间有三层设备（比如三层交换机或者路由器），非VLAN接口地址网段需要管理防火墙时，请注意添加相应静态路由。该路由只参与防火墙管理，与数据通信无关。如果不需要跨网段管理防火墙，无需设置路由表。

添加静态路由，在**“网络管理”** — **“路由”**—**“静态路由”**，点击**添加**

☺ 添加缺省路由时，目的地址和目的掩码都为0.0.0.0，网关为下一条地址，其他选项为空。



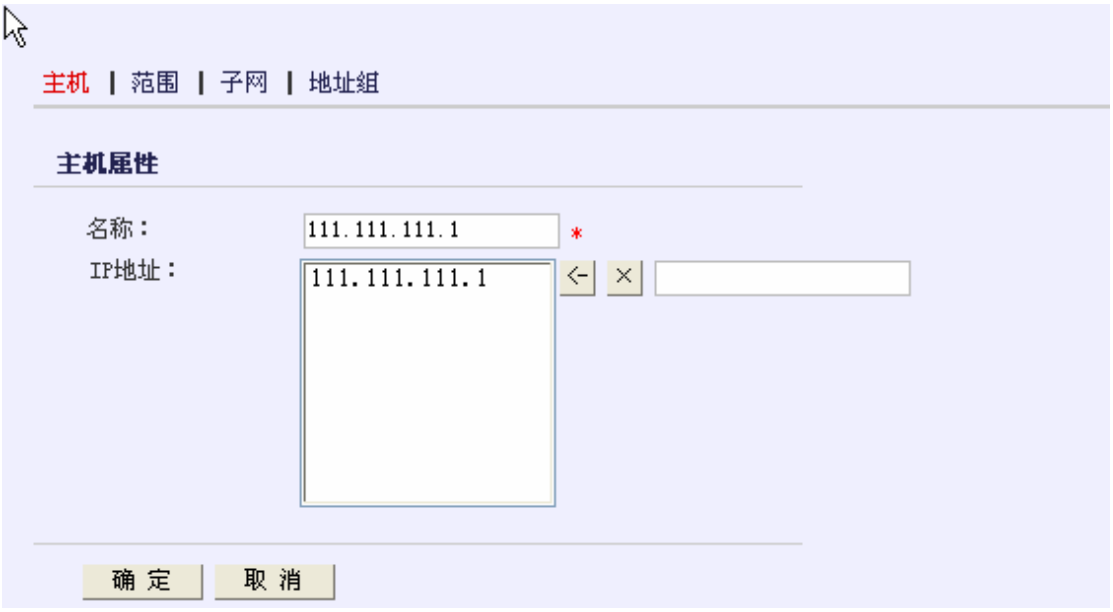
5、定义对象（包括地址对象、服务对象、时间对象）

☺ 提示：防火墙所有需要引用对象(如地址转换策略、访问控制策略等)的配置，请先定义对象，才能引用。

<1>定义地址对象

添加单个主机对象

点击**”资源管理“—“地址”—“主机”，**点击右上角**“添加配置”**



添加地址范围

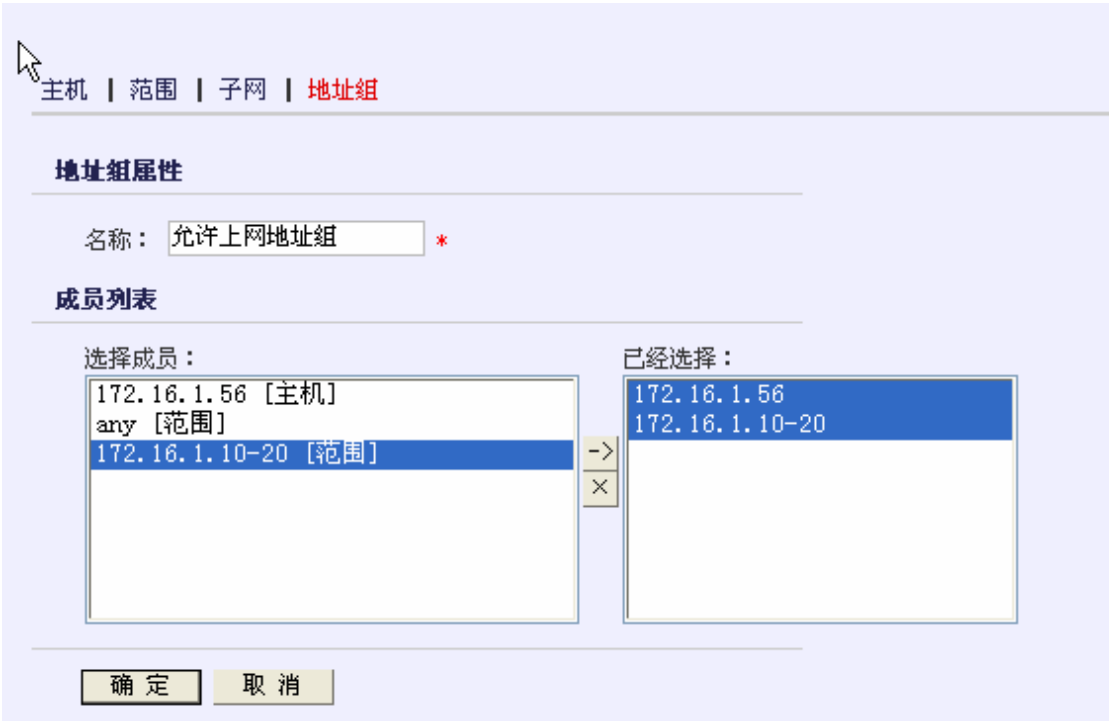
点击**”资源管理“－“地址”－“范围”，**点击右上角**“添加配置”**

添加子网

点击**”资源管理“－“地址”－“子网”，**点击右上角**“添加配置”**

添加地址组

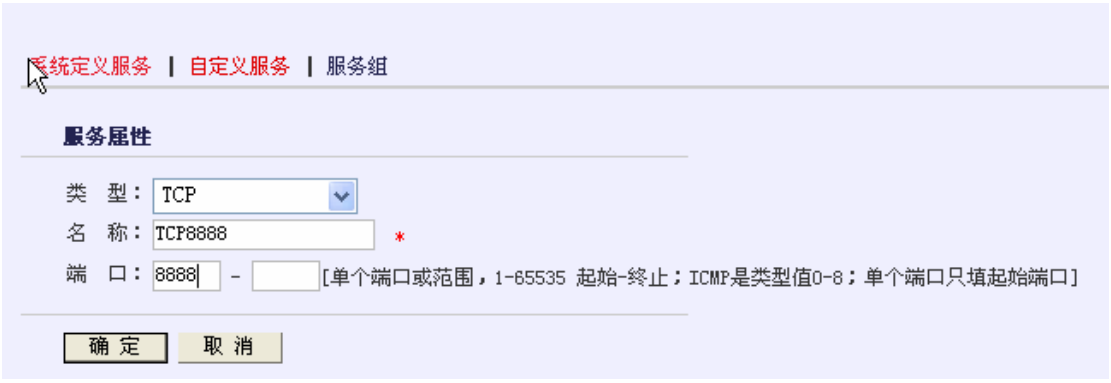
点击**"资源管理"－"地址"－"地址组"，**点击右上角**"添加配置"**

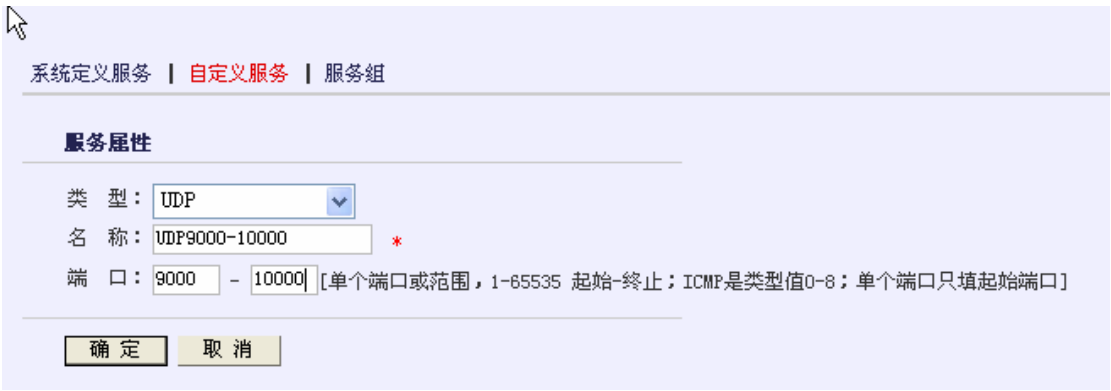


<2>定义服务对象

防火墙内置一些标准服务端口，，但有时用户的系统没有使用某些服务的标准端口，用户在端口引用时，需要我们通过自定义方式加以定义。

点击 **"资源管理"－"服务"－"自定义服务"**，点击**"添加"**，可以添加单个端口或范围 。注意单个端口只填起始端口





<3>定义时间对象

点击“资源管理”—“时间”，点击“添加”，可以设置单次和多次

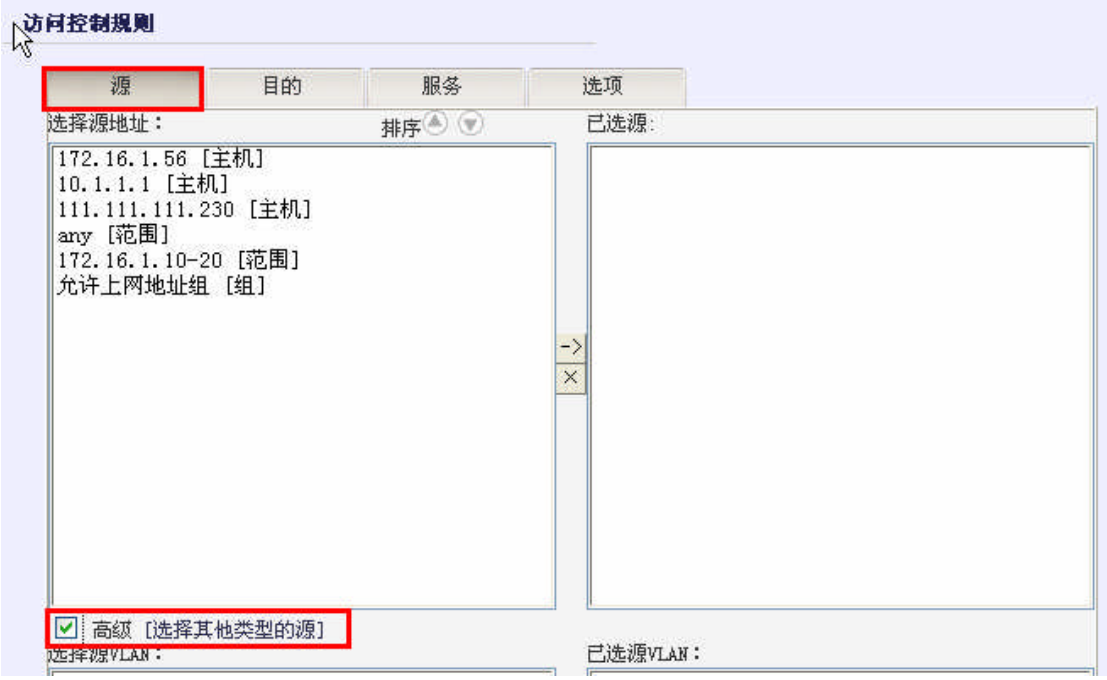
7、制定访问控制策略

在**“防火墙” — “访问控制”**，点击 **“添加”**

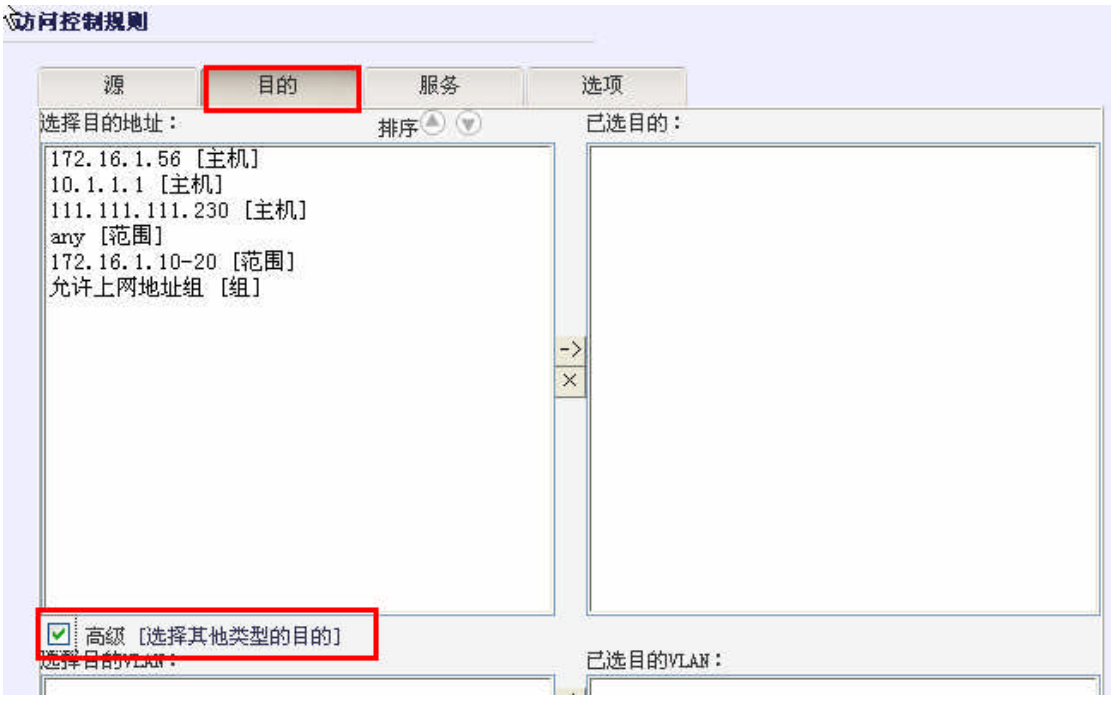
<1>第一条规则定义内网可以访问外网

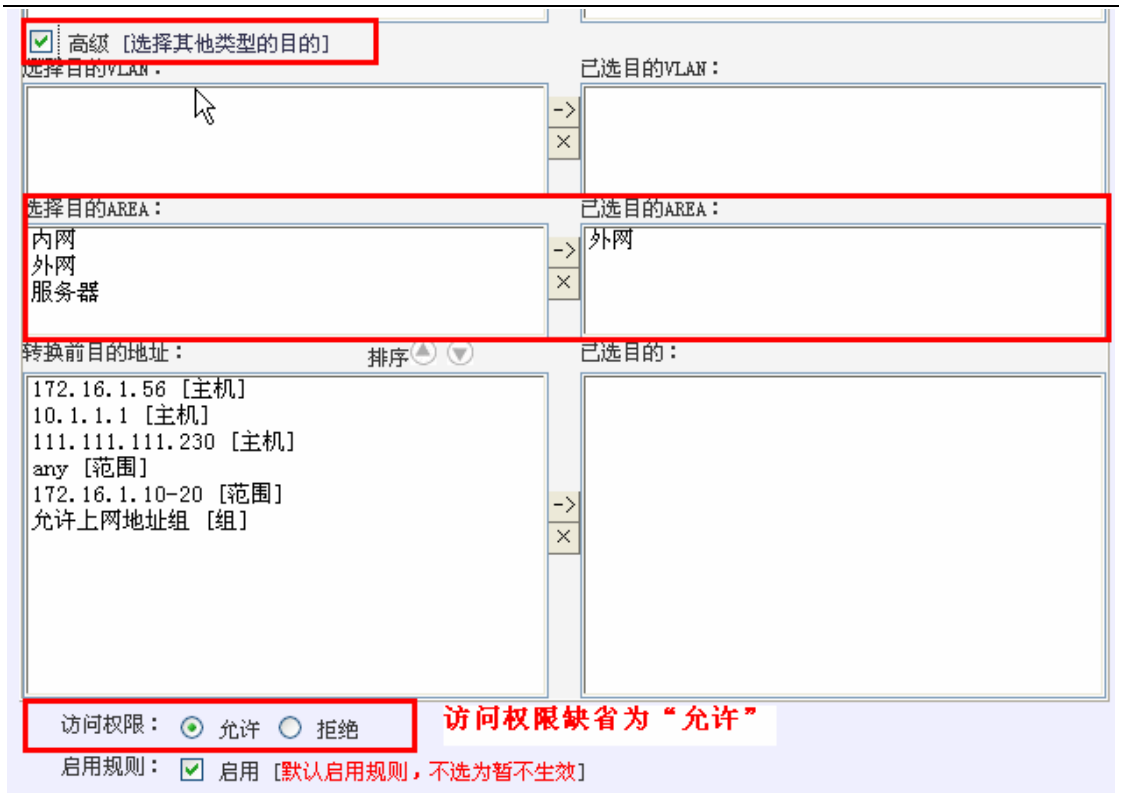
在**“防火墙” — “访问控制”**，点击 **“添加”**

选择**“源”**，点击**“高级”**，源选择源区域**“内网”**，目的选择目的区域**“外网”** ，点击**“高级”**，动作“允许”（默认选项）。




高级 [选择其他类型的源]
选择源VLAN：
已选源VLAN：
选择源AREA：
已选源AREA：
内网
外网
服务器
内网
选择源端口：
排序
已选源端口：
TCP8888 (TCP:8888)
UDP9000-10000 (UDP:9000-10000)
Echo(TCP) (TCP:7)
Echo(UDP) (UDP:7)
Discard(TCP) (TCP:9)
Discard(UDP) (UDP:9)
Daytime(TCP) (TCP:13)
Daytime(UDP) (UDP:13)
NETSTAT (TCP:15)
Quotd(TCP) (TCP:17)
Quotd(UDP) (UDP:17)
Chargen(TCP) (TCP:19)
访问权限： 允许 拒绝
启用规则： 启用 [默认启用规则，不选为暂不生效]

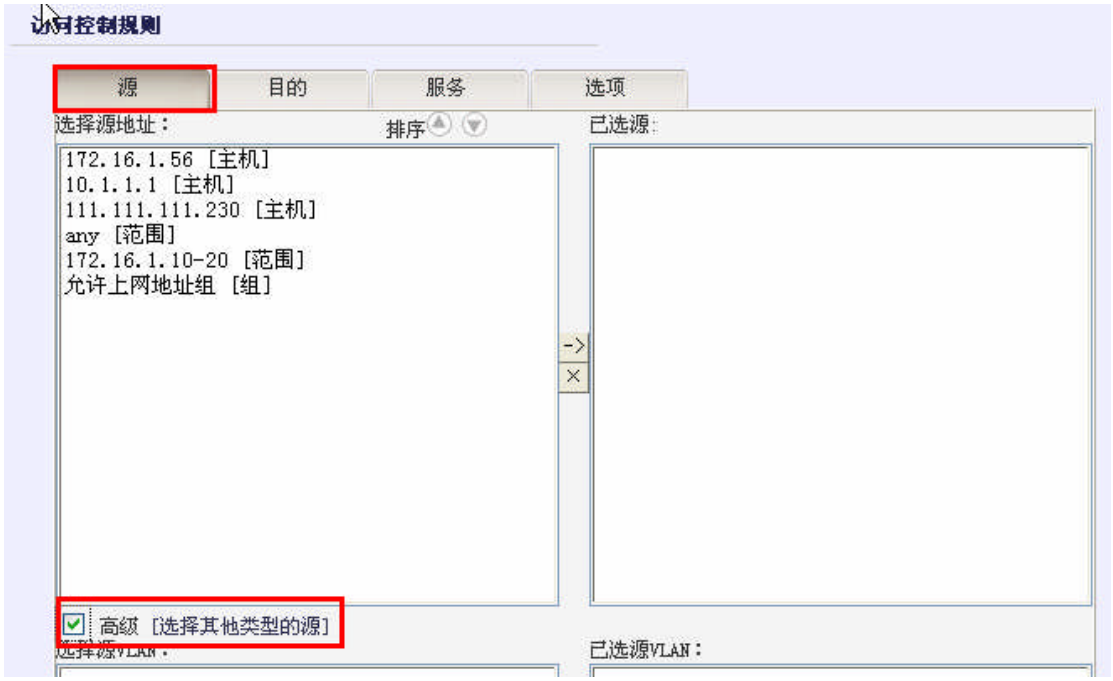

访问控制规则
源
目的
服务
选项
选择目的地址：
排序
已选目的：
172.16.1.56 [主机]
10.1.1.1 [主机]
111.111.111.230 [主机]
any [范围]
172.16.1.10-20 [范围]
允许上网地址组 [组]
高级 [选择其他类型的目的]
已选目的VLAN：

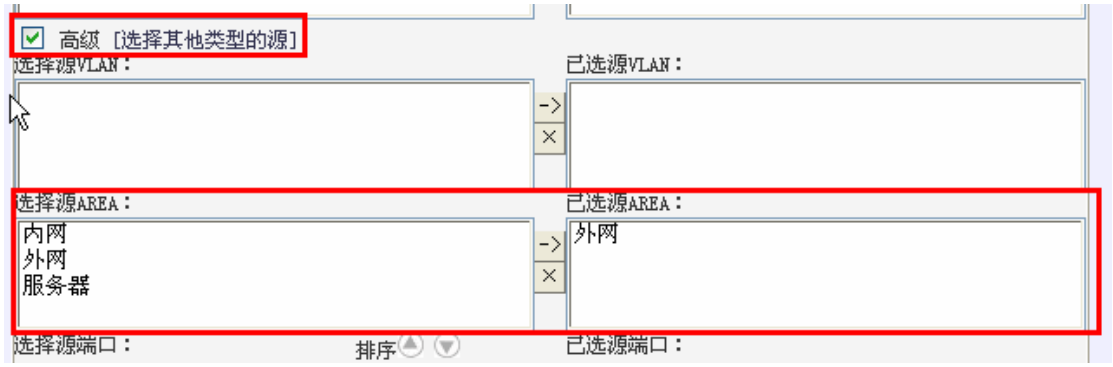


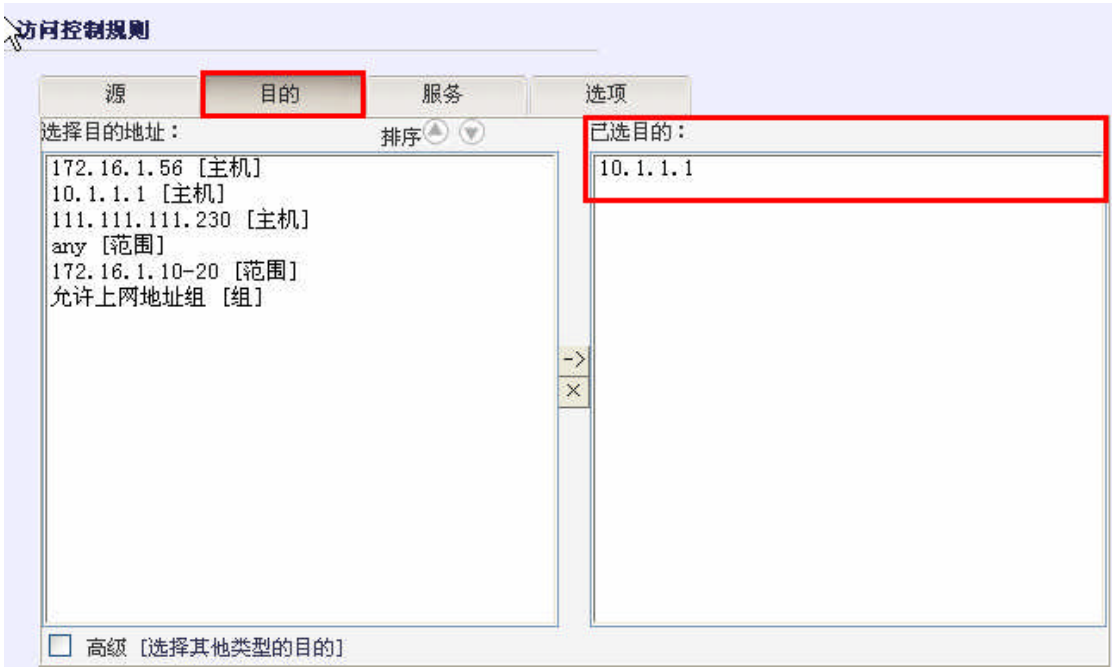
<2>第二条规则定义外网可以访问服务器的对外发布的应用端口，只能访问服务器http应用。

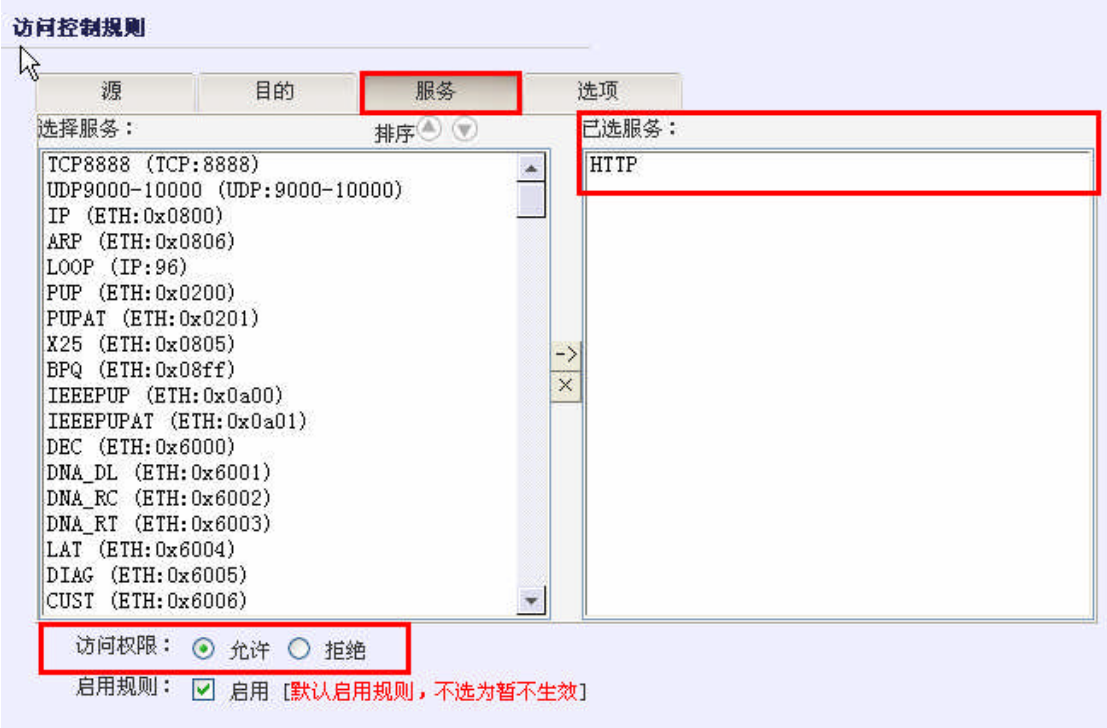
在**“防火墙” — “访问控制”**，点击 **“添加”**

选择**“源”**，点击**“高级”**，源选择源区域**“内网、外网”**， 目的选择“**Web服务器地址对象（111.111.111.1），即服务器真实地址**”， 服务选择”**HTTP服务**”，动作**“允许”**（默认选项）。


访问控制规则
源
目的
服务
选项
选择源地址：
排序
已选源：
172.16.1.56 [主机]
10.1.1.1 [主机]
111.111.111.230 [主机]
any [范围]
172.16.1.10-20 [范围]
允许上网地址组 [组]
高级 [选择其他类型的源]
选择源VLAN：
已选源VLAN：


高级 [选择其他类型的源]
选择源VLAN：
已选源VLAN：
选择源AREA：
已选源AREA：
内网
外网
服务器
外网
选择源端口：
排序
已选源端口：


访问控制规则
源
目的
服务
选项
选择目的地址：
排序
已选目的：
172.16.1.56 [主机]
10.1.1.1 [主机]
111.111.111.230 [主机]
any [范围]
172.16.1.10-20 [范围]
允许上网地址组 [组]
10.1.1.1
高级 [选择其他类型的目的]



第一条规则定义内网可以访问外网。源选择**“外网”**；目的可以选择目的区域—**“外网”**，动作“允许”（默认选项）。

第二条规则定义外网可以访问服务器的对外发布的应用端口，只能访问服务器http应用。源选择**“内网、外网”**，目的选择服务器真实的IP地址111.111.111.1，服务选择“HTTP”服务。

☺ **访问规则需要注意的问题：**

访问控制规则描述了天融信防火墙允许或禁止匹配访问控制规则的报文通过。防火墙接收到报文后，将顺序匹配访问控制规则表中所设定规则。一旦寻找到匹配的规则，则按照该策略所规定的操作（允许或丢弃）处理该报文，不再进行区域缺省属性的检查。如果不存在可匹配的访问策略，天融信防火墙将根据目的接口所在区域的缺省属性（允许访问或禁止访问），处理该报文。区域属性设置请参见 “3、区域和缺省访问权限配置”。

1、规则作用有顺序

2、访问控制列表遵循第一匹配规则

3、规则的一致性和逻辑性

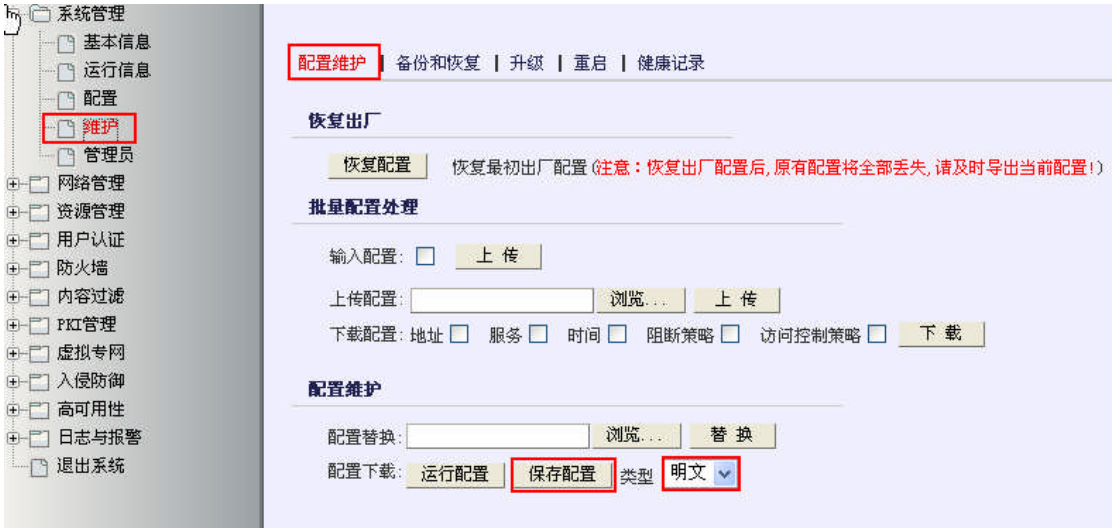
10、配置保存

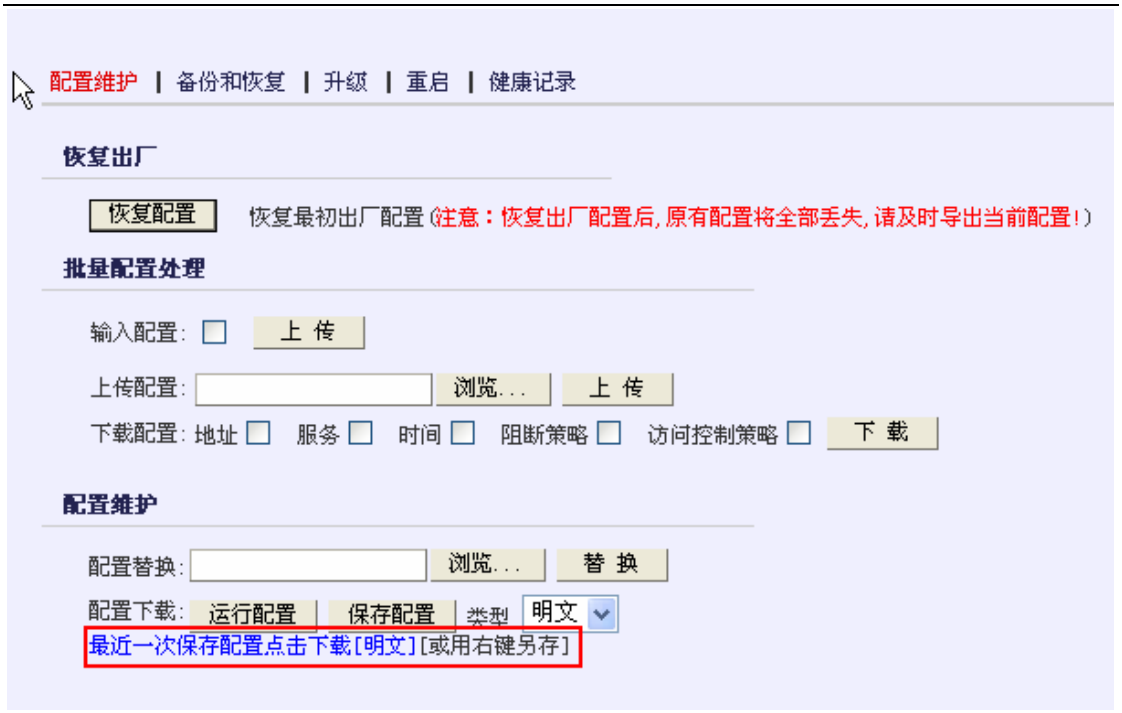
点击管理界面右上角**“保存配置”**

☺ 配置完成后，配置立即生效，但是一定要保存配置，否则设备断电或重新启动后未保存配置将丢失。保存的配置将作为下次设备启动配置。

11、配置文件备份

配置完成并确认运行正常以后，请备份配置文件。选择**“系统管理”—“维护”—“配置维护”**，选择**“保存配置”**





☺ 提示：每次修改配置前，建议首先备份防火墙再修改配置，避免防火墙配置不当造成网络长时间中断。