

# 目录

简明安装指南.....	4
<b>第一章 如何安装.....</b>	<b>5</b>
1、规格及特性.....	5
1.1 MAILGARD 外观.....	5
1.2 前面板(图 1-2).....	5
1.3 后面板 (图 1-3).....	5
2、环境要求.....	6
3、安装说明.....	6
3.1 如何做机械安装.....	6
3.2 配置与管理.....	6
3.3 设备连接方式.....	6
<b>第二章 邮件系统.....</b>	<b>8</b>
1 邮件系统简介.....	8
1.2 基本功能.....	8
2 如何管理邮件系统.....	8
2.1 域名管理.....	9
2.2 用户管理.....	10
2.2.1 如何新建用户邮件账号.....	11
2.2.2 如何设置用户访问权限.....	12
2.2.3 如何设置邮件监控.....	12
2.2.4 如何删除邮件账号.....	13
2.2.5 如何设置滞用用户.....	14
2.2.6 如何创建别名.....	14
2.2.7 如何删除别名.....	15
2.2.8 用户数据的导入与导出.....	16
2.3 设置群组管理.....	17
2.3.1 如何修改群组.....	17
2.3.2 如何删除部门或组.....	18
2.3.3 如何添加部门或组.....	18
2.3.4 如何设置“公共联系人”.....	19
2.3.5 如何修改公共联系人中邮件地址的信息.....	19
2.4 如何设置邮件功能.....	20
2.4.1 企业签名.....	20
2.4.2 设置短信提醒.....	20
2.4.3 设置邮件审核.....	21
2.4.4 设置邮件监控.....	22
2.4.5 如何对整个邮件域的账号进行监控.....	22
2.4.6 如何对某个账号进行监控.....	23
2.4.7 设置收发对象.....	23

2.4.8	如何设置反垃圾邮件 .....	23
2.4.9	如何设置黑名单 .....	24
2.4.10	如何设置白名单 .....	24
2.4.11	流量统计 .....	24
2.5	参数设置 .....	25
2.5.1	如何修改欢迎信 .....	25
2.5.2	修改系统 LOGO .....	25
2.5.3	如何修改管理员密码 .....	26
2.5.4	优化数据库 .....	26
2.6	如何查看日志 .....	27
3	如何使用邮件客户端系统 .....	27
3.1	邮件客户端系统所包含的功能摘要如下: .....	27
3.2	如何通过客户端登陆到邮件系统 .....	28
3.2.1	如何以 WEB 方式登录 .....	28
3.2.2	如何收邮件 .....	29
3.2.3	如何阅读邮件 .....	29
3.2.4	如何发邮件 .....	30
3.2.5	如何管理 webmail 邮箱 .....	31
3.2.6	通讯录 .....	33
3.2.7	如何管理设置自己的邮箱 .....	35
3.3	如何使用客户端软件收发 .....	40
3.3.1	如何使用 OUTLOOK .....	40
3.3.2	如何使用 Foxmail .....	46
<b>第三章</b>	<b>防火墙管理 .....</b>	<b>49</b>
1、	MAILGARD 佑友防火墙产品概述 .....	49
1.1	MAILGARD 佑友防火墙类型及特点 .....	49
2、	防火墙配置步骤 .....	49
2.1	如何登陆 MAILGARD 佑友防火墙管理配置界面 .....	49
2.2	系统管理 .....	51
2.2.1	功能模块 .....	51
2.2.3	如何修改系统时间 .....	52
2.2.4	如何修改管理员密码以及选择系统管理界面的语言版本 .....	52
2.2.5	如何对防火墙设置以及系统数据进行备份和恢复 .....	54
2.2.6	如何关机与重启动以及使用 MAILGARD 佑友的维护工具对网络进行简单的检查 .....	55
2.3	网络设置 .....	56
2.3.1	功能模块 .....	56
2.3.2	如何配置 MAILGARD 佑友防火墙 .....	56
2.3.3	如何设置静态路由以及主机路由 .....	58
2.3.4	如何设置 DHCP 服务 .....	59
2.3.5	如何设置 DNS 以及 DNS 中继 .....	60
2.3.6	如何配置动态域名 .....	60
2.4	上网控制 .....	62
2.4.1	功能模块 .....	62

2.4.2 如何添加上网用户以及设置上网权限.....	63
2.4.3 如何设置上网时间表.....	65
2.4.4 如何设置黑名单.....	66
2.4.5 如何设置白名单.....	67
2.4.6 如何把 IP 跟 MAC 地址进行绑定.....	68
2.5 防火墙.....	68
2.5.1 功能模块.....	68
2.5.2 如何自定义防火墙规则.....	68
2.5.3 如何设置 NAT 规则.....	70
2.5.4 如何设置端口映射.....	71
2.5.5 如何设置 DMZ 主机.....	72
2.5.6 设置 MAILGARD 佑友防火墙的安全选项.....	72
2.6 VPN 管理.....	73
2.6.1 功能模块.....	73
2.6.2 VPN 概述.....	73
2.6.3 设置 PPTP VPN.....	73
2.6.4 设置 IPSECVPN.....	75
2.6.5 设置 SSLVPN 服务.....	76
2.6.6 数字证书.....	77
2.7 流量控制.....	77
2.7.1 功能模块.....	77
2.7.2 如何查看连接状态.....	78
2.7.3 如何查看流量统计.....	78
2.7.4 如何对流量进行限制.....	80
2.8 入侵检测.....	82
2.8.1 功能模块.....	82
2.8.2 特征检测.....	82
2.8.3 攻击检测.....	83
2.8.4 连接控制.....	85
2.9 如何查看日志.....	85
2.9.1 功能模块.....	85
2.9.2 日志管理.....	85
2.9.3 防火墙日志.....	86
2.9.4 IPsec 日志.....	86
2.9.5 SSL 日志.....	86
2.9.6 PPP 日志.....	87
2.9.7 ARP 日志.....	87
2.9.8 用户日志.....	88

## 简明安装指南

1、设备接口如下图：



- \* 以太网接口：用普通网线（直通线）连接到交换机。
- \* ADSL 或宽带接口：用普通网线（直通线）连接到 modem 或者光纤转换器上。
- \* 扩展接口：通常适用于有多条外网线路接入。

2、默认登陆页面

先通过 <http://192.168.0.210> 打开控制面板（默认内网接口 IP 为 192.168.0.210）

3、各模块管理密码

模块名称	链接地址	账号	密码
邮件系统	<a href="http://mail.domain.com">http://mail.domain.com</a>	用户自定义	用户自定义
邮件管理	<a href="http://mail.domain.com/madmin">http://mail.domain.com/madmin</a>	admin@domain.com	hicomadmin
防火墙	<a href="http://192.168.0.210:888">http://192.168.0.210:888</a>	admin	admin
FTP	通过控制面板登录	admin	hadmin

## 第一章 如何安装

### 1、规格及特性

#### 1.1 MAILGARD 外观

MAILGARD 佑友™ 的外型尺寸为：426mmX394mmX45mm (1U 机架型)，如（图 1-1）。



（图 1-1）

#### 1.2 前面板(图 1-2)



（图 1-2）

#### 前面板指示灯说明

LED 指示灯	颜色	状态	描述
电源指示灯 (power)	绿色	亮	电源接通
	-	灭	电源未接通
硬盘指示灯 (HDD)	红色	闪烁	硬盘处于工作状态
Link/Act	黄色	亮	端口建立有效的连接，连接速度为 100Mbps
	绿色	闪烁	端口正在接受或发送数据

**注：具体以实物为准，不同型号的产品不同，上图仅供参考**

#### 1.3 后面板 (图 1-3)



（图 1-3）

## 2、环境要求

**MAILGARD佑友™** 设备可在如下的环境使用

输入电压：100V~240V

温度：-10~50℃

湿度：5~90%

为保证系统能长期稳定运行，应保证电源有良好的接地措施和防尘措施，保持使用环境的空气通畅和室温稳定。本产品符合关于环境保护方面的设计要求，产品的安放、使用和报废应遵照国家相关法律、法规要求进行。

### 电源：


**MAILGARD佑友™** 系列产品使用交流 100V~240V 电源，在接通电源之前，请确认您的电源有良好的接地措施。

## 3、安装说明

### 3.1 如何做机械安装

打开包装箱，箱中应有下面物品：

物品	数量
<b>MAILGARD佑友™</b> 主机	1 台
电源线（220V）	1 条
网络跳线（交叉线）	1 条
网络跳线（直连线）	1 条
机箱脚垫	4 个
用户手册	1 本
用户调查表	1 张
产品合格证	1 张

 检查和所有备件，如有任何损毁或缺失，请立即联系经销商。

### 3.2 配置与管理

在配置之前，需要配备一台能正常使用的电脑，电脑与 **MAILGARD佑友™** 连在同一个局域网内，通过网络对设备进行配置。

### 3.3 设备连接方式

3.3.1 在背板上连接电源线，打开电源开关，前面板的 Power 灯会点亮。

3.3.2 用标准的 RJ-45 以太网线将 LAN 口与内部局域网连接，对 **MAILGARD佑友™** 进行配置。

3.3.3 用标准的 RJ-45 以太网线将 WAN1 口与 Internet 接入设备相连接，如路由器，光纤收发器或 ADSL Modem 等。

3.3.4 多线路的 **MAILGARD 佑友™** 可以支持多条 Internet 线路，此时将扩展接口 1 与第二条 Internet 线路相连，扩展接口 2 与第三条 Internet 线路相连。

小贴士：

WAN 口直接连接 MODEM 应使用直连线，连接路由器应使用交叉线；LAN 口连接交换机应使用直连线，直接连接电脑网卡接口应使用交叉线。直连线与交叉线的区别在于网线两端的线序不同。如（图 1-4）



直连线线序图



交叉线线序图

（图 1-4）

## 第二章 邮件系统

### 1 邮件系统简介

MAILGARD 佑友具有强大的邮箱管理功能，能方便的对企业员工进行信箱的创建、分配、编辑、过滤、监控等功能，并且其操作简单，界面友好，支持 Outlook, Foxmail 等客户端程序。

#### 1.1 系统指标

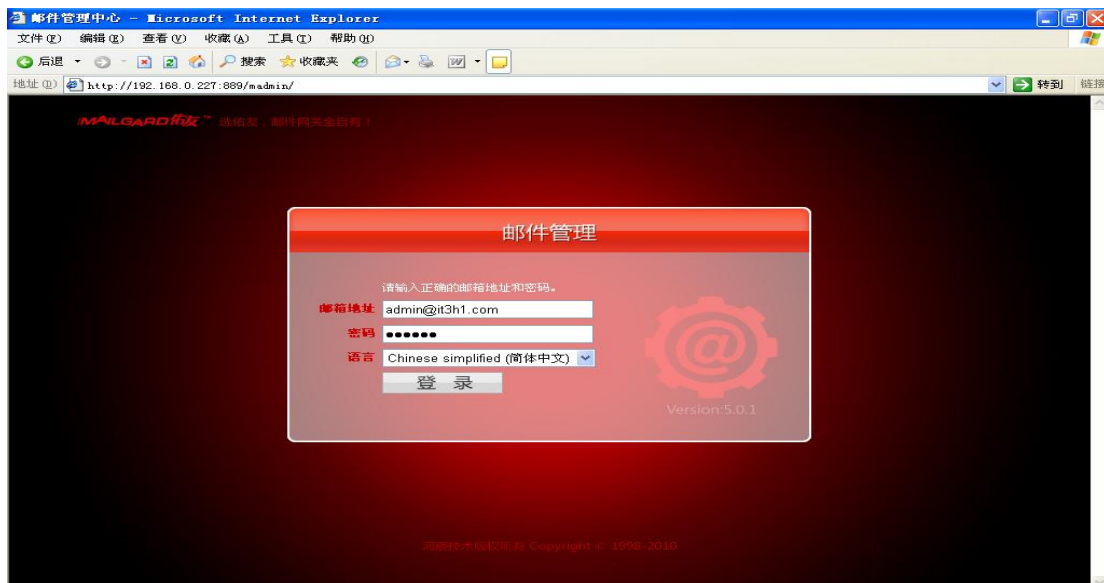
- ◇ 运行环境：Linux；
- ◇ 用户数：根据型号不同，支持数量不同；
- ◇ 支持邮件标准协议：SMTP/ESMTP、POP3、IMAP4、通过 SSL 加密传输方式的 Web 访问、支持所有标准邮件协议；
- ◇ 多语言支持：提供简体、繁体、英文的 Web 访问界面；

#### 1.2 基本功能

- ◇ 支持 SMTP/POP3/IMAP4/HTTP/HTTPS 协议；
- ◇ 支持 MIME、UUEncode/UUDecode 邮件编码/解码标准；
- ◇ 支持 GB2312、BIG5、HZ、UTF-8、UTF-7、ISO 等汉字编码标准；
- ◇ 邮件病毒扫描，内置杀毒引擎自动升级；
- ◇ 病毒、垃圾邮件告警信息提示；
- ◇ 基于 DNS MX 查找的邮件中转；
- ◇ 垃圾邮件过滤（垃圾邮件过滤为可选功能，标配不具有，以下同）；
- ◇ 邮件监控
- ◇ 邮件审核
- ◇ 邮件中继
- ◇ 全球邮
- ◇ 多域名管理与实现；

### 2 如何管理邮件系统

在 IE 浏览器地址栏中输入相应地址（一般是 http://mail.域名/madmin）便可进入邮件管理系统，进入 MAILGARD 佑友 邮件管理平台，将出现如下登录界面，如（图 3-1）。



（图 3-1）



在上图账号密码提示栏内输入正确的管理员用户账号和密码，选择合适的语言种类后，便可进入到邮件管理系统，如（图 3-2）。



（图 3-2）

管理员账号登录后就出现了（图 3-2）的邮件系统管理主界面，（也是单击左侧导航菜单“首页”会出现的界面），在这个界面上我们很直观的看到邮件域的一些信息，包括：用户列表，新建用户，群组列表，新建群组，系统信息，修改密码。

## 2.1 域名管理

MAILGARD 佑友支持多邮件域管理服务，并且可以进行多域名管理。具体的操作如下：

单击域名管理进入域名管理界面，可以看到域名管理包括域名列表，域管理员列表和新建域管理员。在域名列表中显示按字母和数字排列顺序的域名。和该邮件域下的用户数，用户别名，容量，创建日期，终止日期等信息如（图 3-3）。



（图 3-3）

## 2.1.1 如何新建域管理员

点击新建域管理员将在列表中看到所拥有的邮件用户，点击用户列表上的修改，如（图 3-4）。



（图 3-4）

点击修改将出现如（图 3-5）



（图 3-5）

你可以给该账号设置管理权让他属于邮件域的管理员，然后点击“修改并保存”。新建邮件域管理员账号完成。

## 2.2 用户管理

点击左侧导航栏菜单“用户列表将会出现以下，如（图 3-6）。



(图 3-6)

在这里可以看到该邮件域的域名，邮件用户名，用户数配额，已分配的邮件用户数，剩余的邮件用户数，和域空间的配额。同时你可以点击管理对邮件账号进行删除，和对邮件信息进行修改。

## 2.2.1 如何新建用户邮件账号

点击左侧导航栏菜单“新建用户”，如（图 3-7）。



(图 3-7)

输入用户名（若公司有多个域名请在用户名右栏中选择正确的域名），密码、用户的名字等相应的个人资料及邮箱空间和网盘的大小，设定相应限制条件，选择账号使用者所在的部门，最后单击“保存”按钮，即可创建相应的邮箱。以此类推，创建其它相应的邮箱账号。

## 2.2.2 如何设置用户访问权限

点击访问权限，如（图 3-8）。



（图 3-8）

在这里我们可以对该账号的访问权限进行严格的设置，共有五项限制策略，下面分别来进行说明。

第一项：该用户是否通过验证后向外部发邮件的权限，不勾选账号的使用者只能收发本公司邮件域的邮件，勾选为拥有向外部邮件域发送邮件的权限

第二项：设置该账号的使用者是否拥有收取邮件域邮件的权限，勾选“pop 收取邮件权限”，收取邮件的权限。点击“提交数据”即可。

第三项：imap 访问权限，该选项是指客户端是否在客户端做的改变都会同步回服务器(在网络连接正常的时候)，

第四项：限制该账号的使用者是否能使用 webmail 客户端界面，勾选“允许使用 webmail 界面”，然后点击“保存”即可。

第五项：是否进行短信提醒，当邮件用户开通短信提醒功能后，收到邮件会以手机短信的方式进行提醒。然后点击“保存”。

## 2.2.3 如何设置邮件监控

邮件监控的设置是指是否对该邮件用户发出的邮件和接受的邮件进行监控，当你需要监控的时候，你只要勾选 然后将监控邮件的邮件发送到下面指定的邮件地址，点击“保存”。就可以对选择的邮件进行监控。如（图 3-9）所示。



(图 3-9)

## 2.2.4 如何删除邮件账号

点击用户列表，用户列表将出现下（图 3-10）：



(图 3-10)

在这个界面上我们可以看到每个账号的详细信息包括：序号 用户名、邮件地址及其所在的邮件域、空间大小、网络盘大小、账号的状态以及这个账号所创建的时间。

在这里删除账号有两种方法：

- 1、直接单击所要删除账号后面对应的“删除”按钮。
- 2、勾选要删除的账号，单击页面左下角的“删除”按钮。

## 2.2.5 如何设置滞用用户

滞用用户就是贵公司员工长期没有使用的邮件账户。点击“滞用用户”如下（图 3-11）所示。



(图 3-11)

## 2.2.6 如何创建别名

在这个图中我们可以看到, 所建立的别名列表, 包括序号、别名、转发地址、所在域和最后修改时间等相关信息, 点击左侧导航栏菜单“用户别名”, 即可为你的邮件系统建立一个别名邮件地址, 发往该别名地址的邮件将会自动转发到你指定的邮件地址。如图 (3-12)



(图 3-12)

在 (图 3-12) 中, 在“创建别名”输入你要建立的别名邮件地址名称, “转到”处输入你要转发的邮件地址, 然后单击“新建别名”, 即完成创建, 如 (图 3-13)。



(图 3-13)

**小贴士：**

一般情况下，当 A 员工离职后管理员会删除其企业邮箱，但与 A 员工存在联系的客户可能仍将信件发往已删除的邮箱，这时，管理员可以新建别名，将 A 员工的邮件地址转到代替他的 B 员工的邮箱即可实现企业业务的无缝衔接。

**2.2.7 如何删除别名**

点击“用户别名”将出现如下（图 3-14）：



(图 3-14)

在这个图中我们可以看到，所建立的别名列表，包括序号、别名、转发地址、所在域和最后修改时间等相关信息，在这里可以进行修改和删除别名等相关操作。如果要删除别名信息，只需在勾选图中相应别名地址，进入如（图 3-15）所示画面，然后输入要更改信息，单击修改即可。



(图 3-15)

## 2.2.8 用户数据的导入与导出

点击右侧导航栏“导入导出”可以将你的邮件用户账号和设置导入和导出。注：必须正确选择文件的编码格式，否则将操作失败！MAILGOAD 服务器支持导入的文件不能超过 50M，所导出的文件用户名是小写。当你 所导出文件的邮件账号密码为空的时候，你可以给你的邮件账号设置密码（密码区分大小写，密码符合复杂性要求，必须 6-16 个字母，不支持空格），当你导出的邮件用户邮箱空间为空的时候，还可以设置邮件空间配额，如（图 3-16）。





当你想导出数据数据的时候。点击导入导出模块的“用户导出”可以将你邮件服务器上的邮箱账号和基本设置导出，提高工作效率，如（图 3-17）。



(图 3-17)

## 2.3 设置群组管理

在导航栏点击“**群组管理**”会出现部门/组的设置画面，在这里我们可以查看已经设置好的部门或组并能对其进行修改和删除操作。如（图 3-18）所示：



(图 3-18)

### 2.3.1 如何修改群组

可以添加新的部门和组，如（图 3-19）所示，点击组名所对应的“**修改**”。



(图 3-19)

按钮可以修改该组的组名、排序号、上一级群组及备注,然后点击“保存”即可。

### 2.3.2 如何删除部门或组

在(图 3-20)打勾选中部门或组名点击“删除”按钮,即可把该部门或组从系统中删除。



(图 3-20)

### 2.3.3 如何添加部门或组

在群组管理中点击“新建群组”按钮,会出现下图画面,如(图 3-21)所示:



(图 3-21)

在图中填写要创建的部门或组名，填写该组的排序号，选择该组的上一级群组，然后点击“保存”按钮即可成功添加。

### 2.3.4 如何设置“公共联系人”

在导航栏点击“公共联系人”会出现一张公共联系人列表的画面（这张表的内容会出现在这个邮件域里所有账号的公共通讯录里），如（图 3-22）；在这里可以执行“添加”、“删除”、“修改”等操作，另外还可以对该表执行导入，导出。



(图 3-22)

### 2.3.5 如何修改公共联系人中邮件地址的信息

在上（图 3-22）点击要修改的联系人所对应的“修改”按钮，会弹出该联系人的信息，如（图 3-23）所示，在这里我们可以对该联系人的信息进行修改，修改完成后点击图中的“修改”按钮即可修改成功。

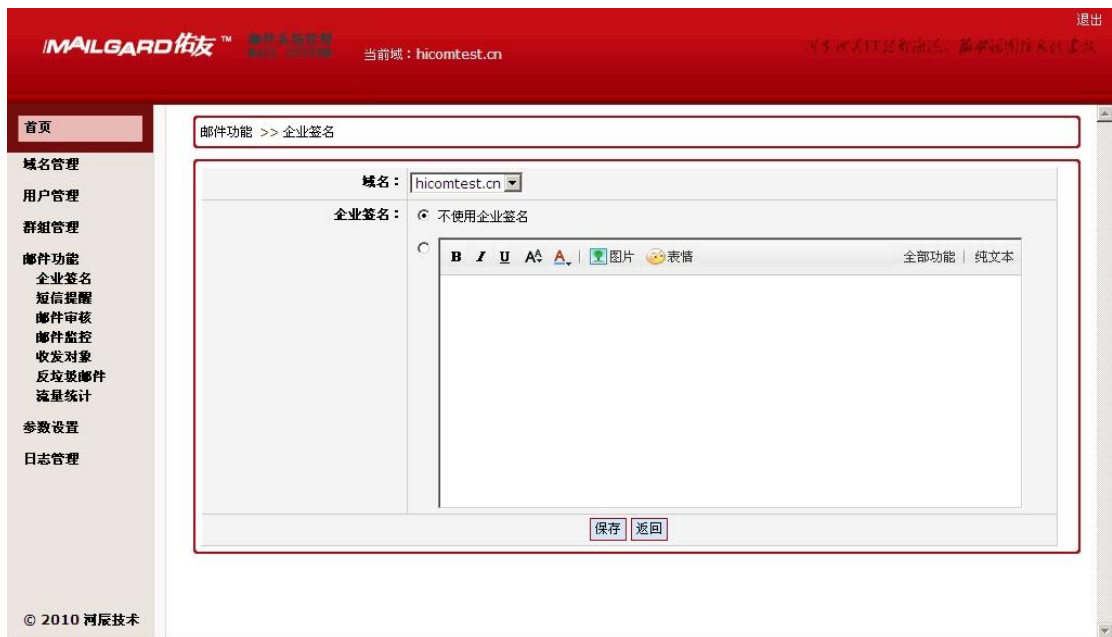


(图 3-23)

## 2.4 如何设置邮件功能

### 2.4.1 企业签名

在导航栏点击“企业签名”。会出现如下界面如（图 3-24），在这里可以设置企业签名，支持图片类型的签名。



(图 3-24)

### 2.4.2 设置短信提醒

点击“短信提醒”开启短信提醒功能，当收到邮件的时候系统便通过短信的方式提醒用户。如图 3-25 所示。



(图 3-25)

### 2.4.3 设置邮件审核

为了对某些用户发出的邮件进行有效地控制，系统提供了邮件审核功能。只有通过审核后的邮件，才能发送出去。邮件审核界面如下图（3-26）所示。可以勾选用户后点击“颁发审核资格”或“免去核资格”来决定用户是否拥有审核的权利。



(图 3-26)

如果需要为用户添加指定的审核员，则可以点击操作栏的设置审核人员按钮进行设置，设置界面如下图（3-27）所示。

邮件功能 >> 邮件审核 >> 选择审核员

真实姓名:	admin
邮件地址:	admin@hicomtest.cn
审核资格:	✓
通行证:	✓
审核员 (1):	admin@hicomtest.cn
审核有效期(分钟):	10
过有效期后:	立即发送

保存 关闭

(图 3-27)

## 2.4.4 设置邮件监控

在导航栏点击“邮件监控”。会出现如下界面如（图 3-28），这里我们可以设置对整个邮件域或单个邮件地址进行收邮件或是发邮件的监控。

MAILGARD 佑友™ 邮件系统管理 当前域: hicomtest.cn

域名管理 >> 域名列表

All 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

搜索

首页 上一页 下一页 尾页 每页 20 条记录

<input type="checkbox"/>	序号	被监控的域或帐号	监控帐号	监控方向	状态	管理
--------------------------	----	----------	------	------	----	----

没有数据

添加被监控的域 添加被监控的帐号 删除

首页 上一页 下一页 尾页 每页 20 条记录

© 2010 河辰技术

(图 3-28)

## 2.4.5 如何对整个邮件域的账号进行监控

在邮件功能点击“添加被监控的域”按钮，会出现如下界面如（图 3-29）

MAILGARD 佑友™ 邮件系统管理 当前域: hicomtest.cn

域名管理 >> 域名列表

All 0 1 2 3 4 5 6 7 8 9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

搜索

首页 上一页 下一页 尾页 每页 20 条记录

添加被监控的域

被监控的域: hicomtest.cn

监控帐号: admin@hicomtest.cn (admin)

监控方向:  发出的邮件  接收的邮件

确定 取消

没有数据

添加被监控的域 添加被监控的帐号 删除

首页 上一页 下一页 尾页 每页 20 条记录

© 2010 河辰技术

(图 3-29)

在这里我们可以很直观的看到“被监控域”是“hicomtest.cn”，这代表要监控整个邮件域里的账号，在“监控账号”对应的下拉框中选择监控账号，选择勾选“发件监控”或“收件监控”，点击“保存”按钮

即设置成功。

#### 2.4.6 如何对某个账号进行监控

在(图 3-28)点击“添加被监控账号”按钮,会出现如下界面如(图 3-30)



(图 3-30)

点击要设置的被监控账号所对应的“添加监控”按钮,在这里我们可以很直观的看到“被监控账号”是“admin@hicomtest.cn”,在“监控账号”对应的下拉框中选择由哪个账号来监控 admin@hicomtest.cn 这个账号的收发邮件情况,然后选择勾选“发件监控”或“收件监控”,点击“保存”按钮即设置成功。

#### 2.4.7 设置收发对象

对于某些用户,想指定他只能发送或者接收去往或者来自某个范围地址的邮件,我们就可以使用收发对象功能。收发对象功能界面如下图(3-31)所示。



(图 3-31)

#### 2.4.8 如何设置反垃圾邮件

垃圾邮件的设置包含两项:第一项是黑名单设置,可以通过将某些邮件地址或某些邮件域添加到黑名

单的方式来使服务器拒绝接收其发送过来的邮件；当然垃圾邮件顾虑是一把双刃剑，垃圾邮件顾虑级别越高，那么正常的邮件被服务器误认为垃圾邮件给过滤掉的可能性也越大。那么这时我们可以通过另一项即白名单的设置即将某些邮件地址或某些邮件域添加到信任区，这样这些邮件地址或邮件域发送过来的邮件服务器不进行垃圾邮件过滤直接接收，这样就即能高效的过滤垃圾邮件又能防止对正常邮件的误判。

#### 2.4.9 如何设置黑名单

在导航栏点击“反垃圾邮件”默认会出现黑名单设置画面如下（图 3-32）所示。在图中的“邮箱地址或域名”对应的文本框里填写要拒绝接收的邮件地址或域名，填写备注后点击“添加到黑名单”即可成功设置。另外在这里我还可以看到之前设置的要过滤的邮件地址和域名并可以对其进行删除操作。



(图 3-32)

#### 2.4.10 如何设置白名单

在（图 3-32）中点击“白名单设置”，会出现白名单设置画面，如（图 3-33）所示，设置方法跟黑名单设置相类似。

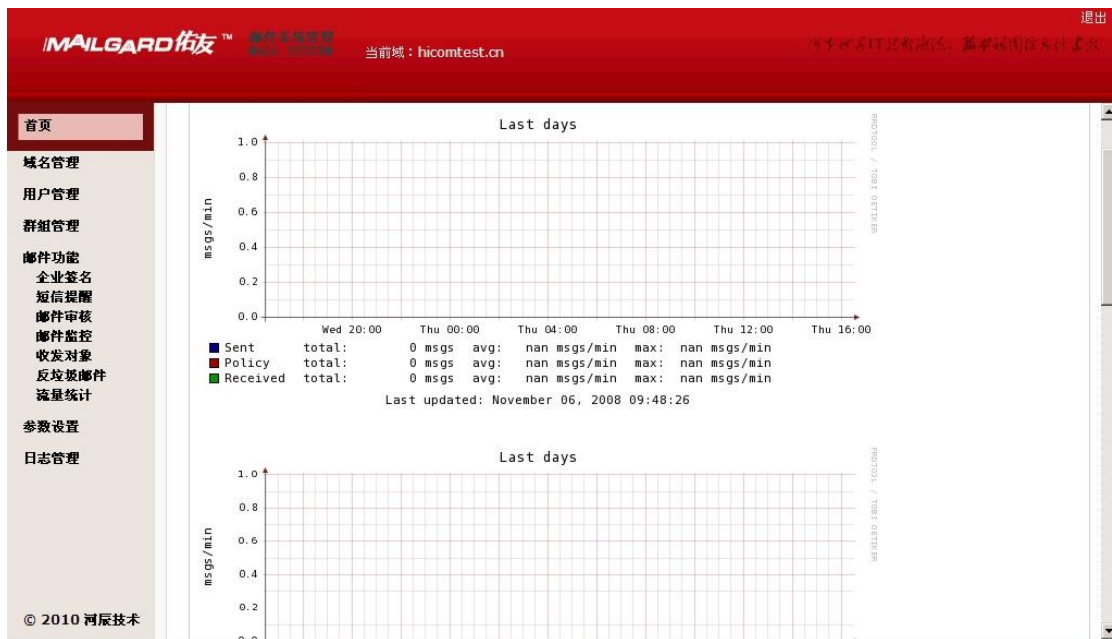


(图 3-33)

#### 2.4.11 流量统计

点击“流量统计”，可以查看到不同时间段内整个域的邮件发送及接收量的情况。如图（3-34）所示





(图 3-34)

## 2.5 参数设置

### 2.5.1 如何修改欢迎信

在导航栏点击“修改界面”会出现修改界面的画面，如图（图 3-35）所示。在图中填写要修改的主题和内容点击“保存”按钮即可成功修改。

参数设置 >> 欢迎信

主题: Welcome to use Mailgard. 欢迎使用佑友邮件系统。

内容: Thank you for using Mailgard. 感谢您使用佑友邮件系统。

保存

(图 3-35)

### 2.5.2 修改系统 LOGO

点击“修改 logo”，用户便可以把系统界面左上角的 LOGO 更改为本企业的 LOGO，默认 logo 是“MAILGARD 佑友”。修改页面如图（图 3-36）所示。



(图 3-36)

### 2.5.3 如何修改管理员密码

在导航栏点击“修改密码”会出先密码修改界面如（图 3-37）所示。在图中两个文本框中写入要修稿的密码点击“保存”按钮即可。



(图 3-37)

注：密码区分大小写，6-16 个字符。

### 2.5.4 优化数据库

在导航栏点击“优化数据库”将会出现数据库优化成功的画面，如（图 3-38）所示：



(图 3-38)

## 2.6 如何查看日志

察看日志功能可以为管理员提供操作的历史信息，以便于管理员察看历史的操作，建立了哪些邮箱，什么时间建立的，邮箱的名称是什么及一些相关的信息，点击左侧导航菜单“查看日志”就会弹出相关信息画面，如（图 3-39）。有了这些日志信息，给管理员的维护提供了方便，察看相关记录提供了历史依据。



(图 3-39)

## 3 如何使用邮件客户端系统

### 3.1 邮件客户端系统所包含的功能摘要如下：

- ◇ 提供多语言支持、SSL 加密传输方式的 Web 访问；
- ◇ OUTLOOK、FOXMAIL 等客户端软件收发邮件；
- ◇ 收取、发送、抄送内部、外部邮件；

- ◇ 显示邮件状态、附件、主题、发件人（包括姓名和邮箱地址）、日期、大小；显示邮件原文；
- ◇ 多附件邮件发送，收件地址可直接在发信页面或者地址簿页面，点选地址簿中的文件夹、群组发送或点击单个地址发送；
- ◇ 转发，并且可对原件的附件进行增加、删除操作；
- ◇ 回复信件、删除信件；
- ◇ 邮件通讯录管理：个人、地址信息一览、添加文件夹、组织地址、编辑、删除、复制、转移、发送信件等操作；
- ◇ 发邮件后，选择是否把已发送邮件存放在已发送邮件箱；
- ◇ 可撰写、预览、编辑、保存信件；
- ◇ 发信时可保存副本，可设置签名档；
- ◇ 显示邮箱状况列表；
- ◇ 按邮件接收日期查找邮件；
- ◇ 提供帮助信息；
- ◇ 支持在线修改密码；
- ◇ 设置用户使用 Web 方式访问的参数；
- ◇ 设置个人资料，其中的姓名设置与客户端设置别名一样，可在信件地址信息中标记出；
- ◇ 过滤器管理：新建、删除、更新过滤器。可多个过滤器联合作用，多种动作规则，动作包括：自动删除垃圾邮件；

## 3.2 如何通过客户端登陆到邮件系统

### 3.2.1 如何以 WEB 方式登录

在地址栏输入 <http://域名/> 或 <http://IP/webmail> 如河辰公司试用邮箱地址为：<http://mail.hechen.com>，将出现如下登录界面，如图（图 3-40）：



（图 3-40）

正确输入用户名和密码进入邮箱界面，如（图 3-41），界面左侧列表为栏目导航区，右侧为内容显示区。



### 栏目导航区

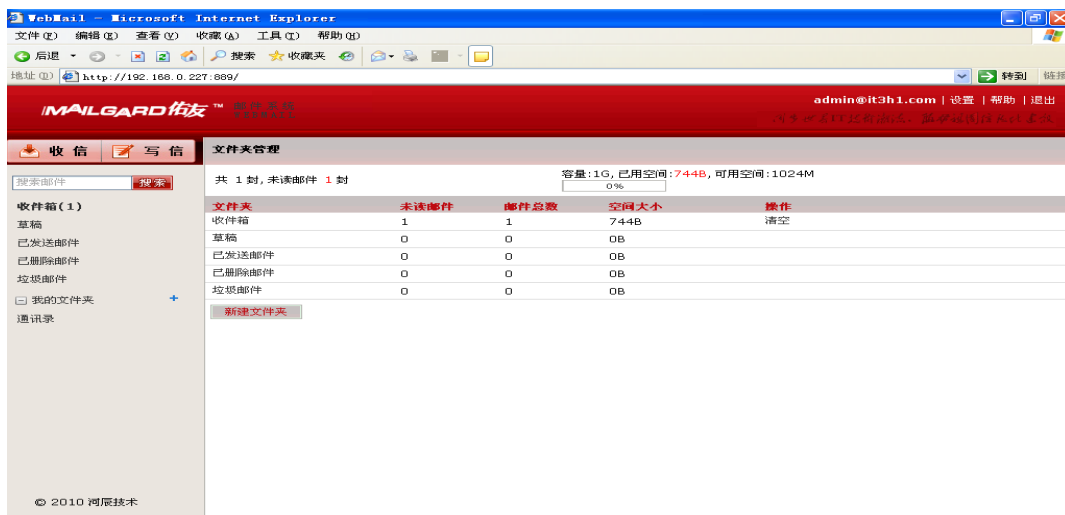
屏幕左侧所显示的列表即为栏目导航区。所列的是您的收件箱、草稿，已发邮件箱、已删除邮件和垃圾邮件，我的文件夹的栏目，可通过直接点击栏目的方式来选择显示。

### 内容编辑区

屏幕右侧为内容编辑区，显示您在栏目导航区选择的栏目内容。您可在此区域进行编写、删除、发送邮件等具体操作。

## 3.2.2 如何收邮件

进入 MAILGARD 佑友 邮件系统 web 页面后，在栏目导航区点击“收邮件”按钮或点击“收件箱”，屏幕右方就会出现您电子邮箱中所有收到的邮件及其相关信息的列表，显示的信息包括：状态、发件人、标题、日期和大小等，如图（图 3-42）

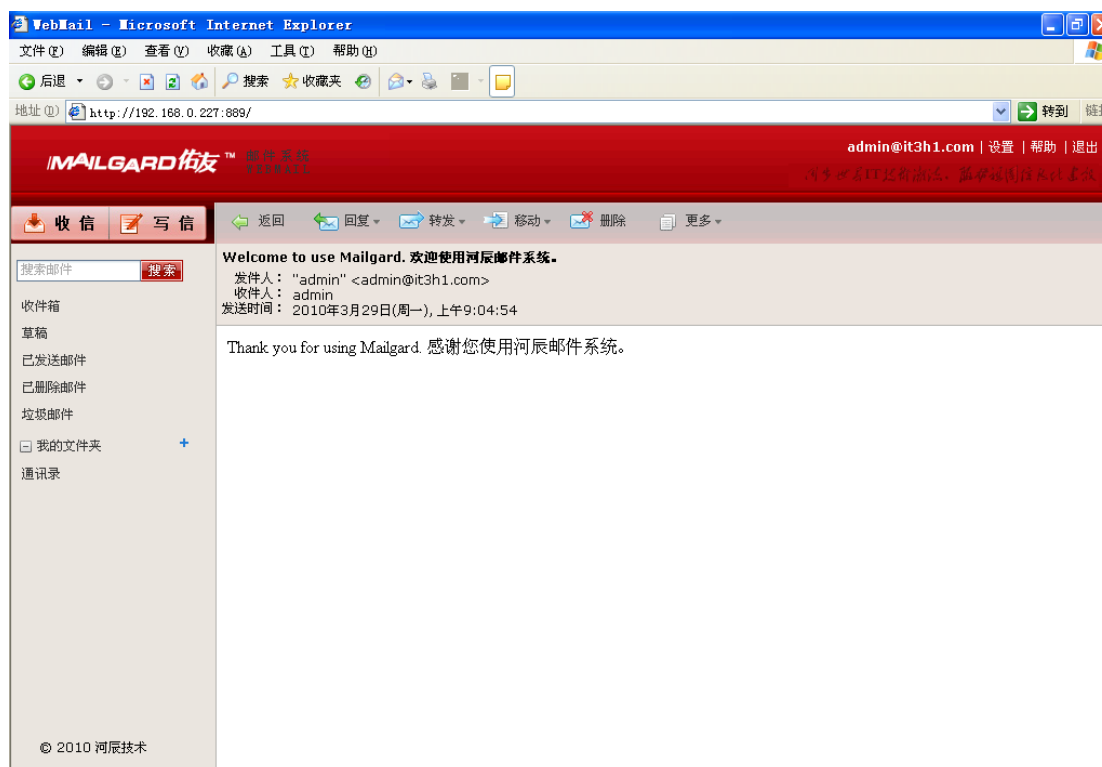


(图 3-42)

## 3.2.3 如何阅读邮件

点击列表中的发件人邮件地址或标题，即可查看该邮件的详细内容，包括：发件人、收件人、日

期、主题、正文和附件列表。同时，还提供针对当前邮件的操作，如（图 3-43）所示。



（图 3-43）

**返回：**返回到（图 3-37）的邮件列表。

**回复：**自动进入邮件发送页面，并自动填写收件人、主题及部分正文。

**回复所有人：**如果原邮件发送给多个用户，并且您希望给发件人和所有收件人回信，使用此功能。

**转发：**把当前邮件转发给其他人，自动进入邮件发送页面。

**移动：**将你收到的邮件移动到垃圾邮件箱或已删除邮箱。

**删除：**删除此邮件。

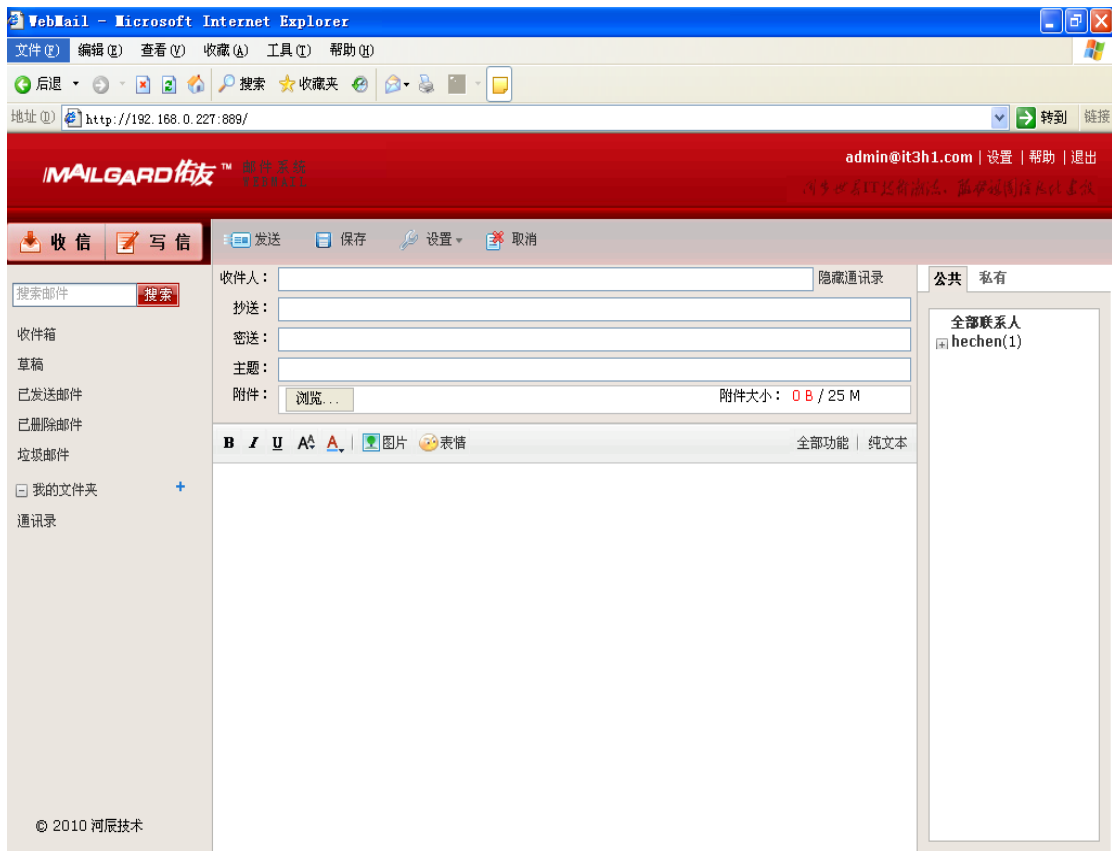
**转换：**是将因编码不同而导致的乱码的邮件正文转换成正常。

**更多：**在这个选项中你可以选择查看该邮件的邮件头，邮件。和该邮件使用哪种编码格式。

### 3.2.4 如何发邮件

点击（图 3-43）中栏目导航区的“写邮件”按钮，即可进入发送邮件页面，如（图 3-44）。发邮件时，您必须填写“收件人”的邮件地址。此外，还需填写邮件主题、邮件正文等，如果有附件可加入附件，您还可以决定是否抄送或密送给其他人。

点击“**设置**”则在收件人阅读信件时要求其回执给您以确认该邮件已经收到，不过此功能仅限于支持回执功能的邮件客户端；您还可以定义邮件发送的优先级，高优先级的邮件将被服务器优先发送。



(图 3-44)

### 如何填写收件人地址

您可以直接在“收件人”后面的文本框中输入电子邮箱地址，也可以点击右侧通讯录中的联系人自动添加。您可以填选多个收件人地址，用“,”分隔。“抄送”和“暗送”的填写方法同上。

### 如何添加附件

点击“浏览”按钮，在下拉窗口单击“浏览”，从打开的窗口中选择您需要发送的文件。选中文件后，点击打开，然后点击“增加”上传，即可将该文件加入“附件列表”中。如果附件列表中有您误选的附件，您可以选中它，点击“删除”按钮将其删除。考虑到网络的传输速度，我们把单个附件的大小限制在 25MB 以内。在做完了新邮件的编辑工作后，您可以选择：

**发送：**把新邮件发送给收件人，系统将告诉您发送是否完成。

**保存：**您可以把新邮件暂时存放在草稿箱中，以后再编辑、发送。

## 3.2.5 如何管理 webmail 邮箱

MAILGARD 佑友 邮件系统为您缺省设置的我的文件夹有收件箱、草稿箱、已发邮件箱，已删除邮件箱，垃圾箱和新建文件夹共六项栏目。点击在导航栏中的栏目，即可展开系统的所有缺省文件夹；如（图 3-45）。



(图 3-45)

邮箱管理页面包括系统邮箱部分，包括：收件箱、草稿箱、已发送邮件箱，已删除邮件箱，垃圾箱和新建文件夹等的列表（包括邮件总数、新邮件数和空间使用情况等）。

下面，我们分别介绍每个部分功能：

#### ✧ 收件箱

该邮件夹存放您收到的邮件，系统会显示有几封邮件没有阅读，并显示邮件的各种属性，如发件人地址、主题、日期和邮件的大小。同时您可以把某封邮件“删除”、“移动”到其它的文件夹。

#### ✧ 发件箱

用来备份您已发出的邮件。如果您在发信时勾选了“发件箱”一栏（系统默认勾选），会在您发邮件时保存一份副本到您的发件箱中。

#### ✧ 草稿箱

用来存放您未写完的信件（在写邮件时用户可以保存邮件，将其放到草稿箱），以后有需要时可以从草稿箱中调出来继续编辑和发送。

#### ✧ 垃圾箱

存放用户已删除的信件。当您删除一封邮件的时候，该邮件会自动转移到垃圾箱中，等待用户的进一步处理。如果是误删除，用户还可以在此恢复和直接查看其内容。如果用户想删除该邮件，可点击删除。同时您也可以把信件“移动”到其它的文件夹。

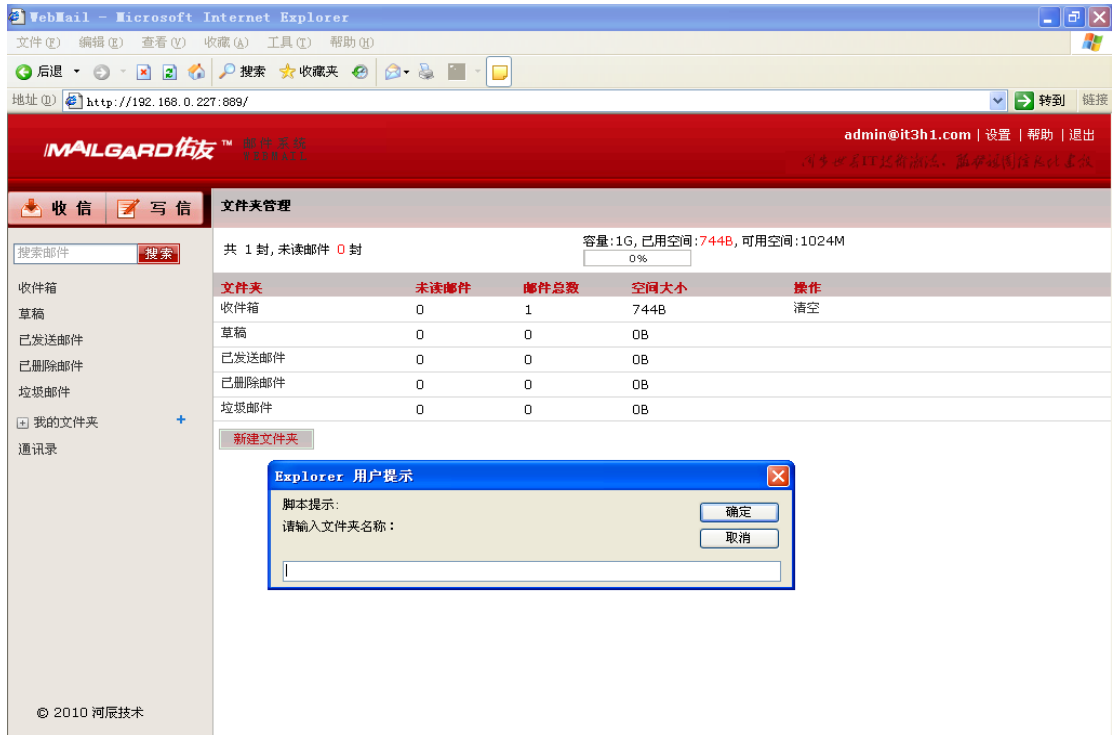
#### ✧ 我的文件夹

除系统默认邮箱外，您还可以建立符合自身需求的文件夹，还有助于大大提高您的工作效率。

#### 创建我的文件夹的方法有两种：

- (1) 在（图 3-45）中直接在“我的文件夹”后的文本框中写入要定义的文件名点击创建即可。
- (2) 点击导航栏后面的“+”号，系统会弹出对话框，如（图 3-46）：



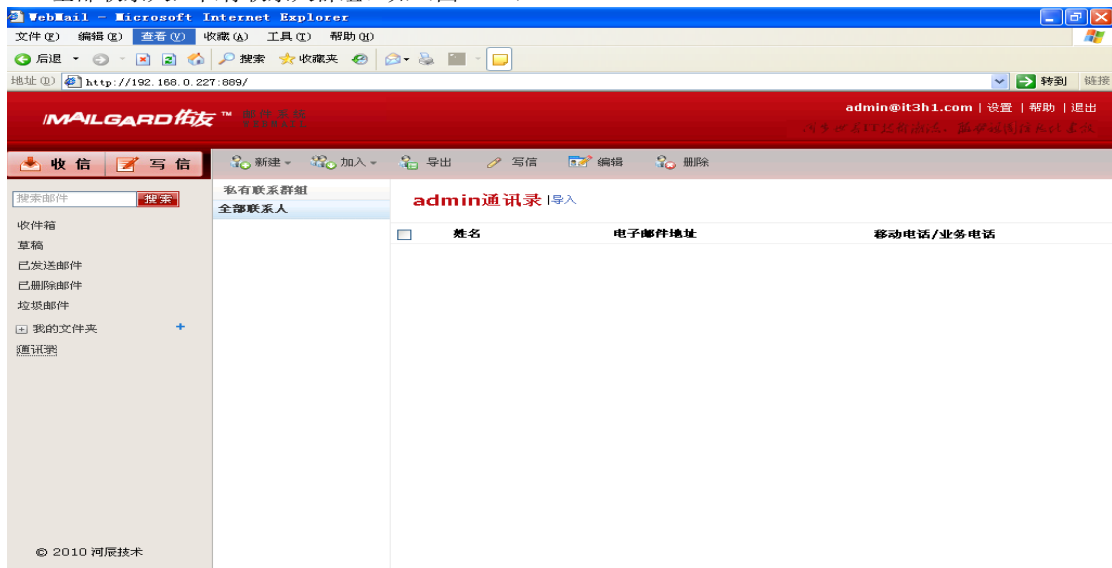


(图 3-46)

在文本框中输入要定义文件夹名字，点击“确定”即可。

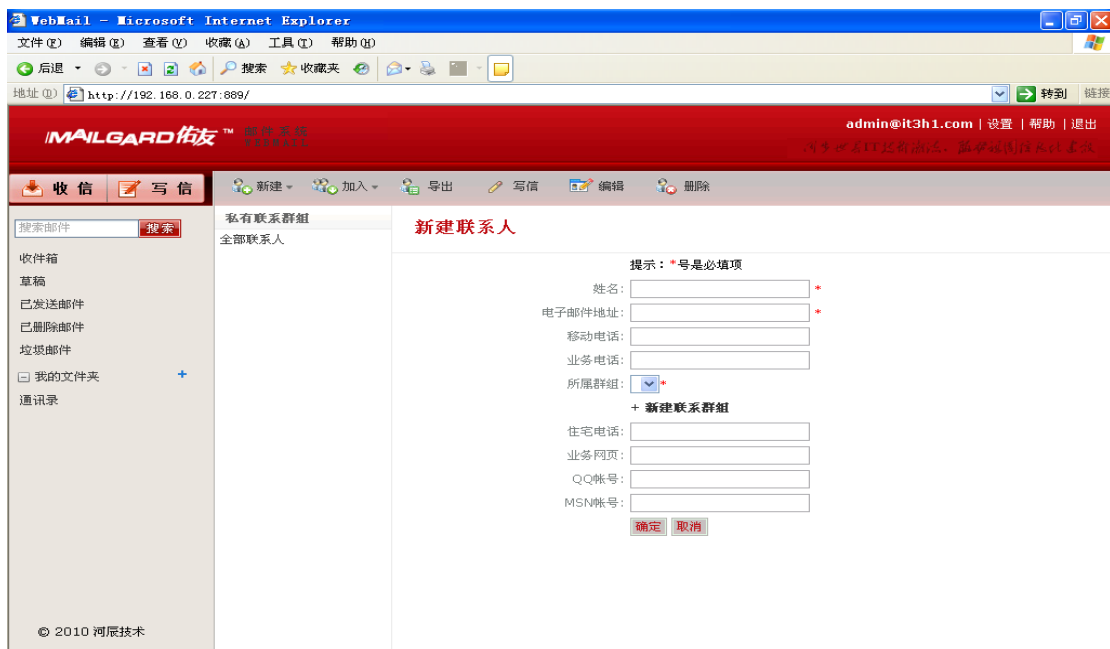
### 3.2.6 通讯录

“通讯录”包含了私有联系人和全部联系人群组的列表，展开“通讯录”，可以看到两个子选项：全部联系人，私有联系人群组。如（图 3-47）



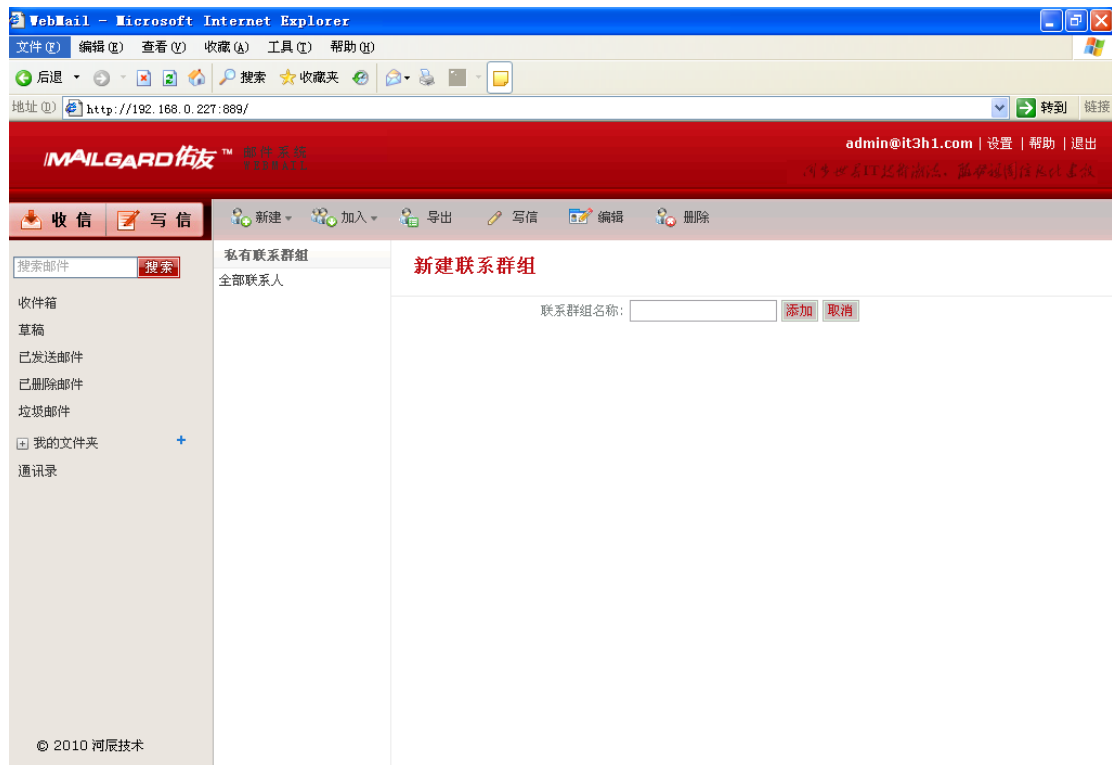
(图 3-47)

点击“新建”右方会出现联系人和联系人群组的信息，如下图（图 3-48）所示：



(图 3-48)

单击（图 3-48）右边“新建联系人”按钮，即可添加新的联系人，在各栏中填入相应信息，再点击保存完成添加过程（可以只填姓名和 E-mail）。修改过程与添加过程类似，您还可以删除联系人，导出联系人列表到 EXCEL 或从外部导入联系人列表。



(图 3-49)

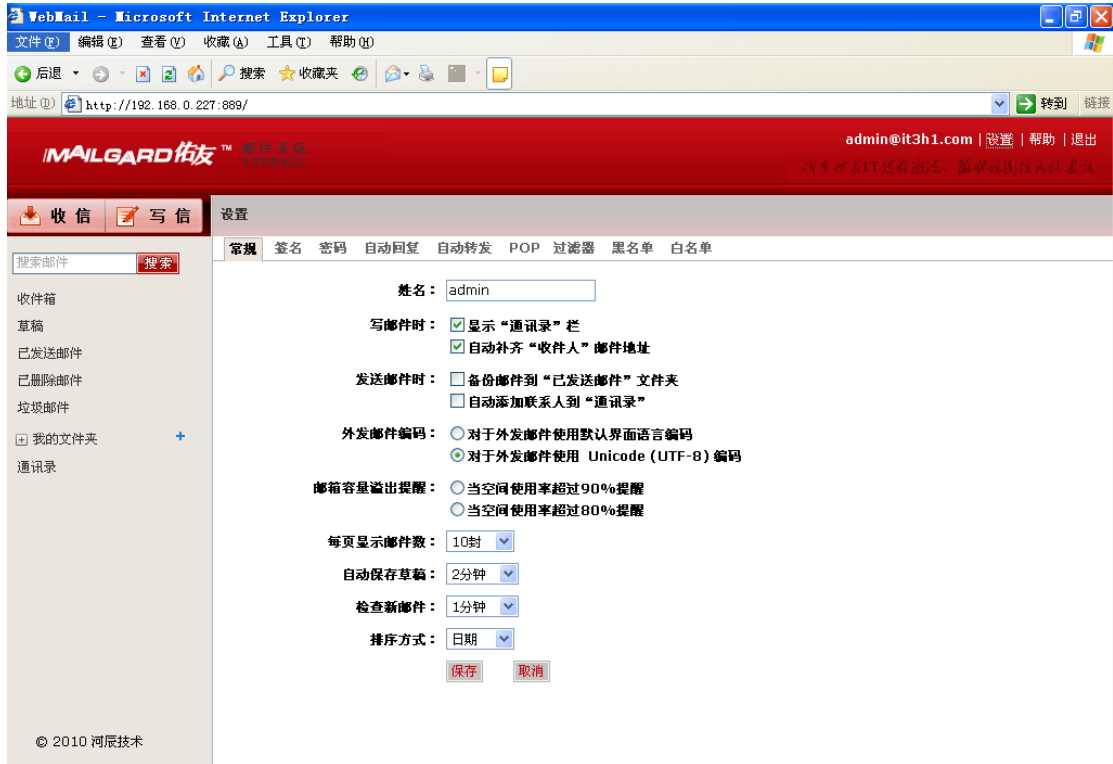
单击（图 3-48）右边“新建联系人群组”按钮在这里我们添加、删除及修改组的信息。点击添加按钮即会弹出添加联系人群组的对话框，如（图 3-49）所示。输入要创建的组名如：客户组、朋友组等、输入本组排序号、点击下拉框选择上一级群组，后点击保存即创建成功，创建完成后我们添加通讯录的时候就可以将联系人分组，这样查找起来及其方便。

### 3.2.7 如何管理设置自己的邮箱

您可以通过栏目导航区“**设置**”对自己的邮箱进行个性化和使用规则的设置。在系统设置下面共有九个子选项，如图（图 3-50），下面分别介绍各自选项的功能

#### 常规

在导航栏点击“**常规**”会出现默认参数设置画面，如（图 3-50）所示。您可以在这里设置您的姓名、系统缺省语言、缺省风格、每页显示邮件数量、显示或隐藏我的通讯录、填写收件人邮箱地址时是否自动补全、自动刷新信箱时间间隔、自动到保存草稿时间间隔和缺省邮件排序方式，修改后请点击“**保存**”按钮即可，若要还原初始设置，请点击“**恢复默认**”按钮。



(图 3-50)

**如何设置签名**若要创建或修改在邮件中的个人签名，在导航栏点击“**签名设置**”，右侧出现个性签名编辑窗口，如图（图 3-51），输入要显示的签名信息、个性图标（一般是公司的 LOGO 标）然后点击保存即可。



(图 3-51)

#### 如何修改密码

也许您需要经常更换自己的密码，以保证您邮箱的安全。这时可以在导航栏点击“密码修改”进入密码修改页面，如图（图 3-52）所示。先输入旧密码，再输入新密码，并对新密码进一步确认，即新密码确认。如果确认输入的新旧密码无误，点击“保存”按钮，即修改成功。



(图 3-52)

### 如何设置自动回复

自动回复功能使邮件服务器在收到邮件后马上为发件人发出一份由您定制的回复邮件。在导航栏点击“自动回复”会显示目前已存在的自动回复策略。点击右下角的“修改”和“删除”按钮来修改或删除相应策略，点击图中右上角“新建”来创建新的自动回复策略。如图（图 3-53），在新建窗口中，设置好合适的自动回复条件，填入自动回复的邮件内容，最后单击“添加”即可新建成功。

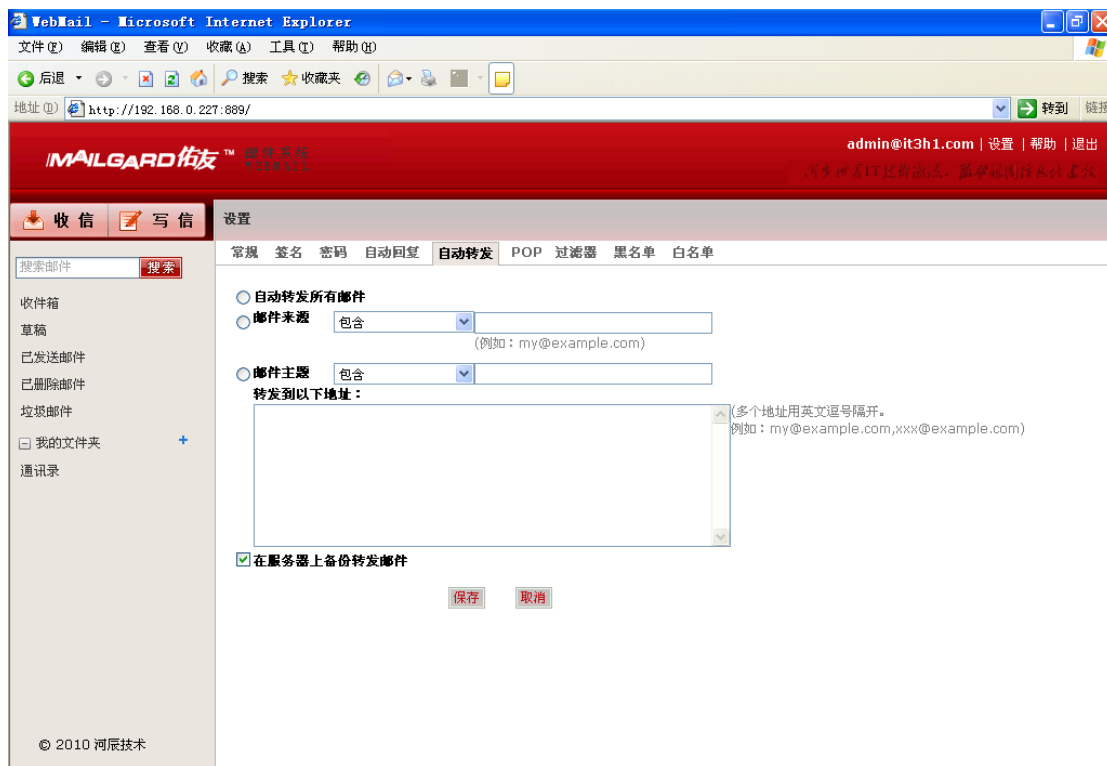


(图 3-53)

### 如何设置自动转发

自动转发功能使您可以设置将信箱中收到的邮件转发到另一个信箱中。点击“自动转发”会显示

目前已存在的自动转发策略，点击右下角的“修改”和“删除”按钮来修改或删除已经存在的转发策略。点击图中右上角“新建自动转发”按钮来创建新的自动转发策略，如（图 3-54）所示。在新建窗口中，设置好合适的自动转发条件，填入接受转发的邮箱地址，若自动转发后不用在本地邮箱保留此邮件，请取消“保留备份”的勾选，最后点击“保存”即可。



（图 3-54）

自动转发条件有 3 种：1. 自动转发所有邮件。2. 基于邮件来源转发邮件 3. 基于邮件主题转发。你可以根据具体情况设置转发策略。

**小提示：部分企业的销售、技术支持等部门对外有专用邮箱，比如 sales、techsupport，通过此功能可以将发往专用邮箱的邮件自动转发到相应部门的各个员工接收，这样客户不用记忆具体员工的邮箱地址，而即使有员工离职也仅需管理员更改内部转发地址即可。另外，如果您需要经常向某个部门的多名员工发送同一邮件，也可以利用自动转发功能，这样您每次只需往此邮箱发送一封邮件，此功能会把邮件自动转发给多名员工，免去了您发邮件时大量添加收件人地址的工作量。**

当您需要收取互联网信箱邮件时，点击栏目导航区“pop 收信设置”下的“收信”按钮即可，如（图 3-55）所示。另外在这里我们还可以对设置的 pop 收信账号进行修改或是删除。

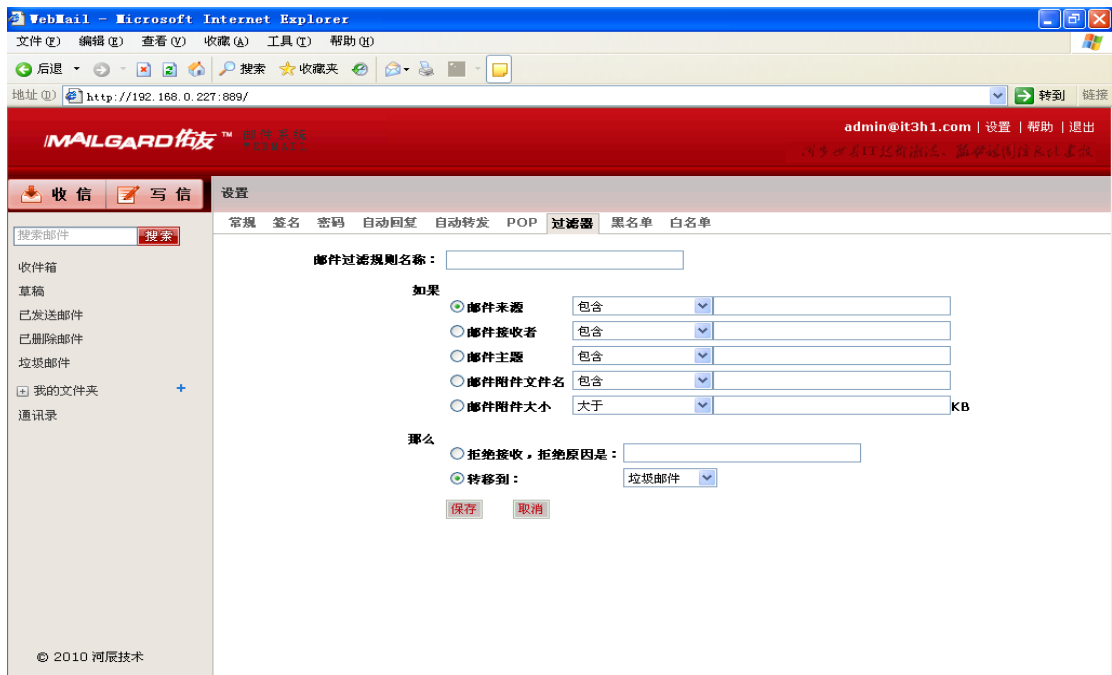


(图 3-55)

### 如何设置邮件过滤器

邮件过滤器可以让您制定合适的规则来设定拒绝收信的名单，或将信件转移到指定的文件夹中。黑名单功能用来设定拒绝接收的邮件，白名单功能用来设定可以直接接收的邮件域的邮件。

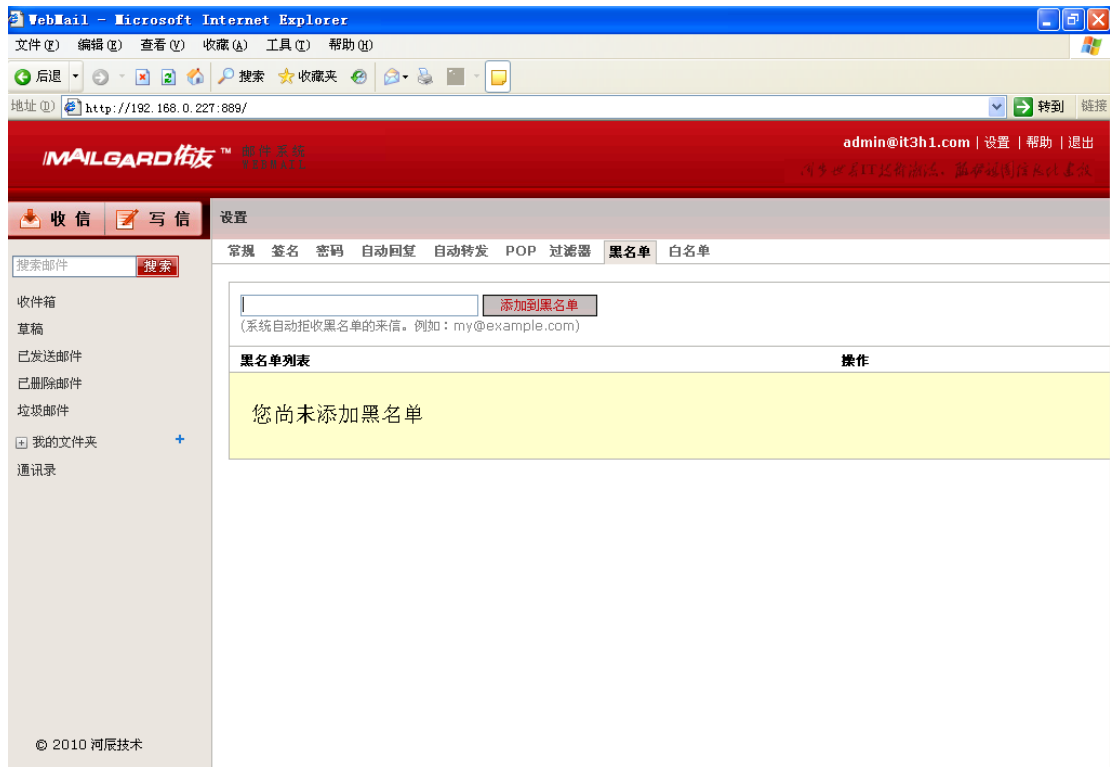
在导航栏点击“过滤器”会显示目前已存在的邮件过滤规则，点击图中右上角“新建”来创建新的邮件过滤规则，如（图 3-56）。在新建窗口中，填入过滤规则名称并设置好合适的过滤条件，选择是拒收还是转移，最后单击“添加”即可



(图 3-56)

在上(图 3-56)中点击“黑名单”会显示目前已存在的黑名单地址列表，如（图 3-57），在黑名单文本

框中输入要阻止的邮件地址或域名，点击添加即可阻止来自此邮件地址或邮件域发送过来的邮件



(图 3-57)

点击(图 3-51)中“白名单”会显示目前已存在的白名单地址列表，如(图 3-58)其界面与黑名单基本相同，在白名单文本框中输入可以接收的邮件地址或域名，点击添加即可保证此邮件地址或域名的邮件可接收而不过滤掉。



(图 3-58)

**小提示：任何具有垃圾邮件过滤功能的邮件服务器，不管其宣称功能如何强大，都不可能彻底杜绝垃**

圾邮件，有时候您需要定义自己的邮件过滤规则来弥补邮件服务器过滤能力的不足，从而达到进一步降低垃圾邮件数量的目的。另外，此功能并不只是针对垃圾邮件而设计。举个例子，您的公司与微软 Microsoft 公司保持紧密的商业联系，平时有大量的邮件互通，您可以定义过滤规则把来自微软公司 microsoft.com 的邮件自动转移到一个自定义文件夹，这将给您的阅读带来很大的方便。如果您的商业伙伴很多，您可以定义多条过滤规则将不同商业伙伴的邮件转移到各自特定的文件夹中。

### 3.3 如何使用客户端软件收发

#### 3.3.1 如何使用 OUTLOOK

前面介绍如何使用 MAILGARD 佑友提供的 Webmail 客户端来收发您的邮件，这样的功能很适合您在外办公时对邮件进行管理。同时，您也可以使用如 Outlook、Foxmail 这样的邮件客户端软件来使用 MAILGARD 佑友为您建立的邮件系统。下面，我们以 Outlook 2000 为例，来介绍一下客户端的配置方法。

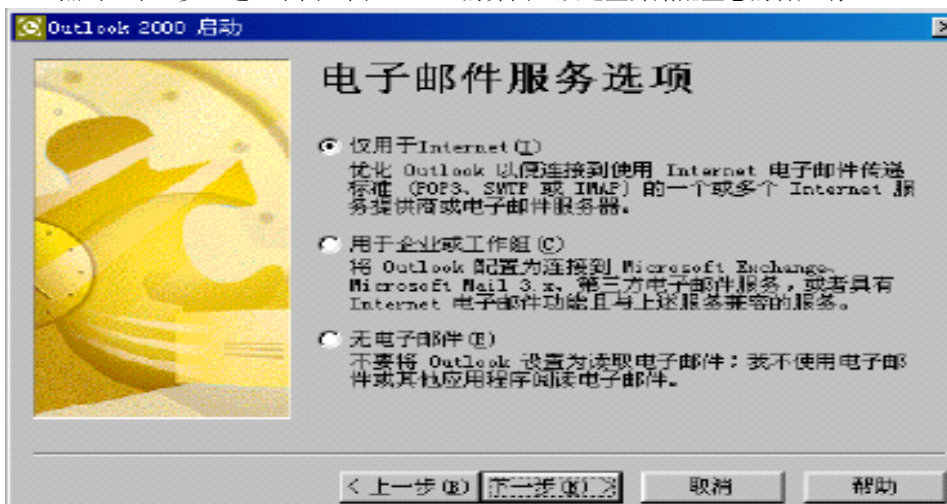
##### ◇ 首次使用 Outlook

如果您以前用过 Outlook 2003，则可跳过本节，如果您以前没有用过 Microsoft Outlook 2000，双击“Outlook 2000”图标后，则会出现如下图（图 3-59）所示的界面。



（图 3-59）

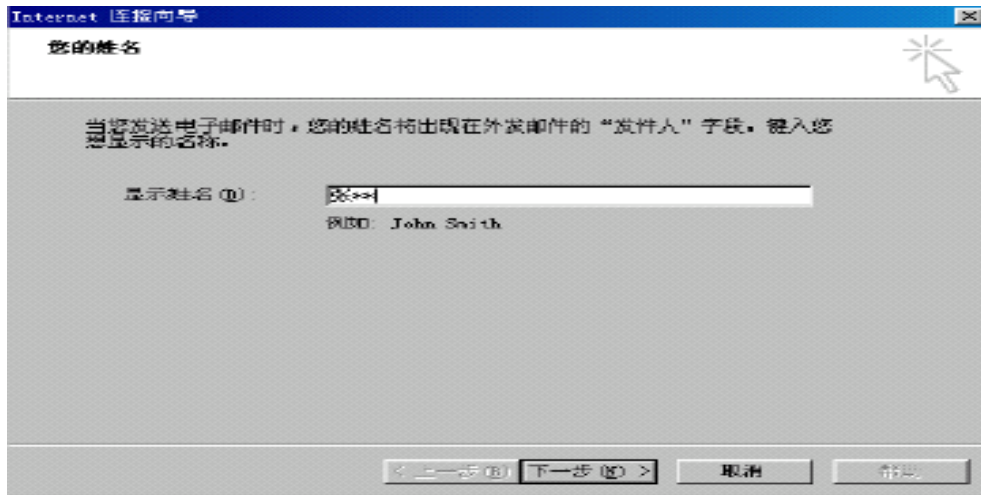
点击“下一步”进入下图（图 3-54）的界面，从这里开始配置您的客户端。



（图 3-60）

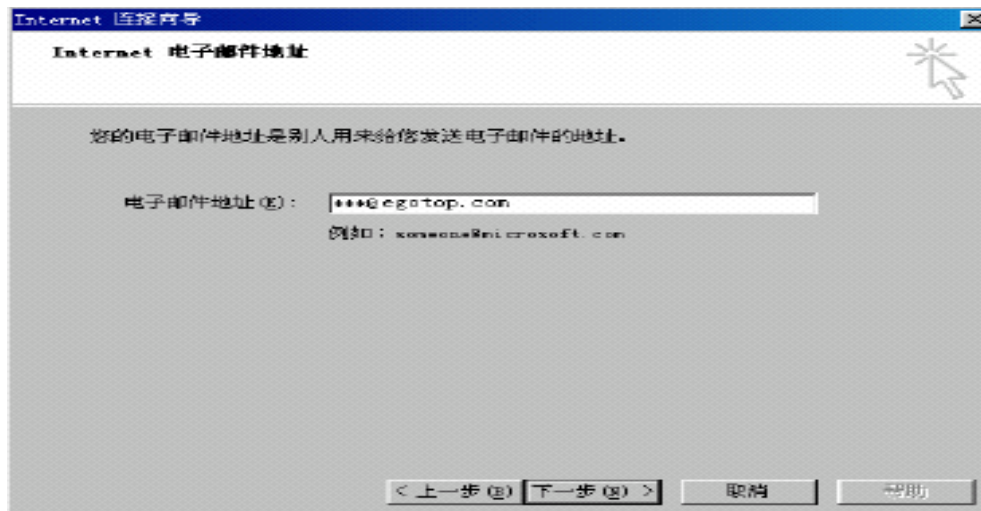
我们建议您选择第一项“仅用于 Internet (I)”，并点击“下一步”进入如（图 3-55）的界面。





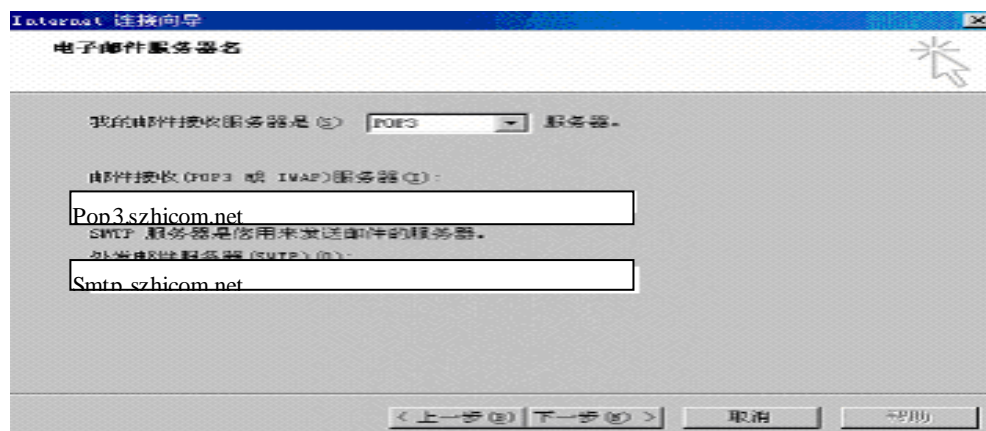
(图 3-60)

此处填写您的姓名，主要是为了让收件人知道信件是谁发给他的，填写后，点击“下一步”进入如图（图 3-61）界面。



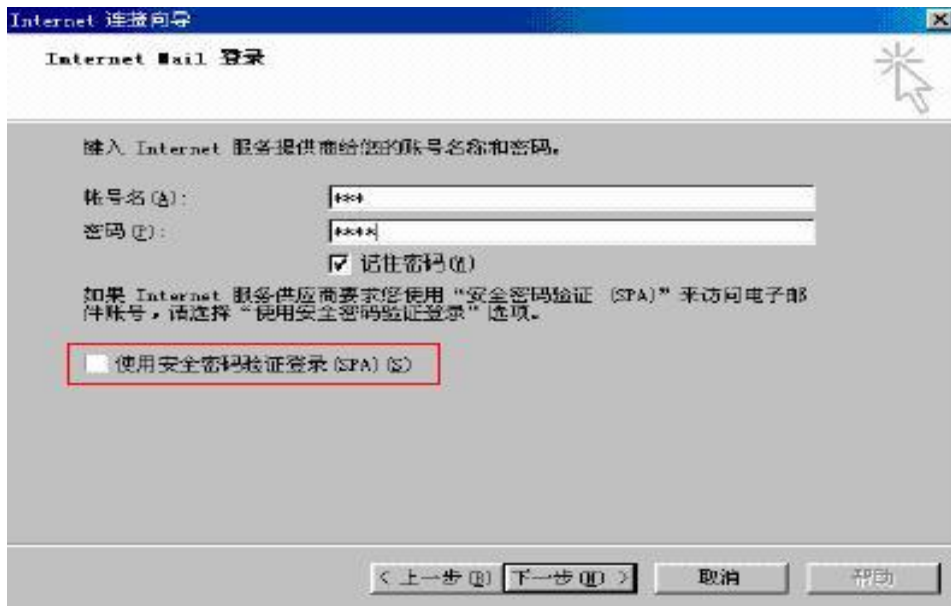
(图 3-61)

此处填写您的电子信箱地址，填写后，点击“下一步”进入如（图 3-62）界面。



(图 3-62)

填写后，点击“下一步”进入如（图 3-63）的界面。

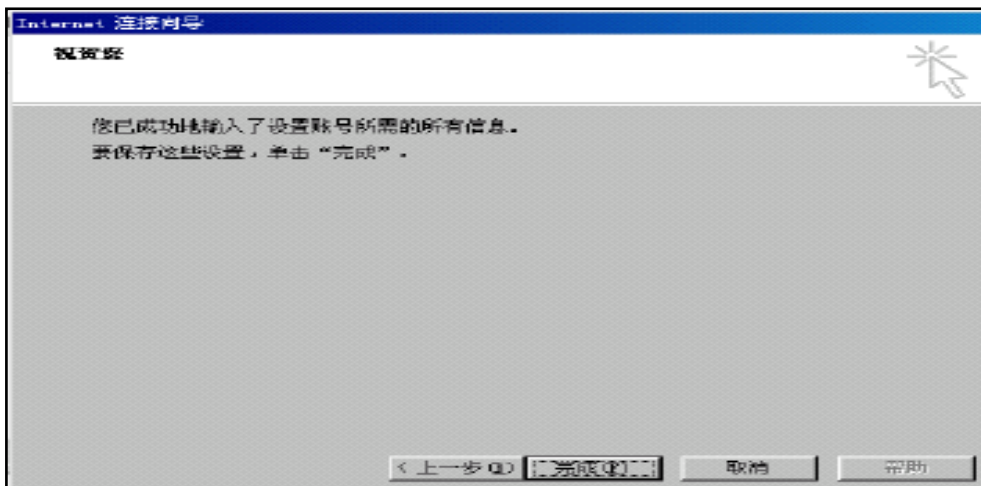


(图 3-63)

这里填写您的账号名和相应的密码，其中的账号名就是您的邮件地址，例如您的邮箱地址为 \*\*\*@szhicom.com，您填写的账号名就是“\*\*\*@szhicom.com”。另外，如果您想让 Outlook2000 每次启动时自动登录网络而不需要重新输入密码，那就选择“记住密码”选项，此外，MAILGARD 佑友不支持“使用安全密码验证登录”，即在红色方框中“使用安全密码验证登录”处可以不用打钩。

点击下一步进入 Internet 连接方式选择，此处的 Internet 连接方式，您可以根据您自己的实际情况选择，如果您使用拨号网络连接，请选择第一项；如果您的电脑已经连接到局域网，而该局域网已经同 Internet 连接，那么请选择第二项；一般选择第三项“手动建立 Internet 连接”。

点击“下一步”后进入如（图 3-64）的界面。



(图 3-64)

邮箱账号的基本信息已经输入，点击“完成”保存。

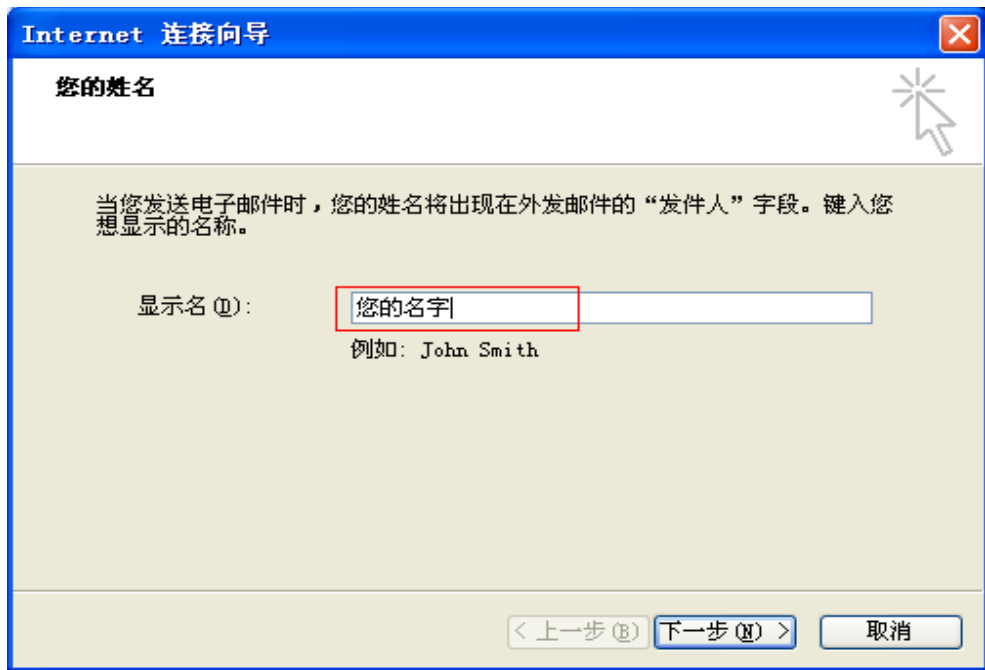
#### ◇ 如何设置 Outlook

设置邮件账号。点击 [工具] → [账号]，在 Internet 账户窗口，邮件选项下，点击 [添加]，选择“邮件”项。如下图（图 3-65）：



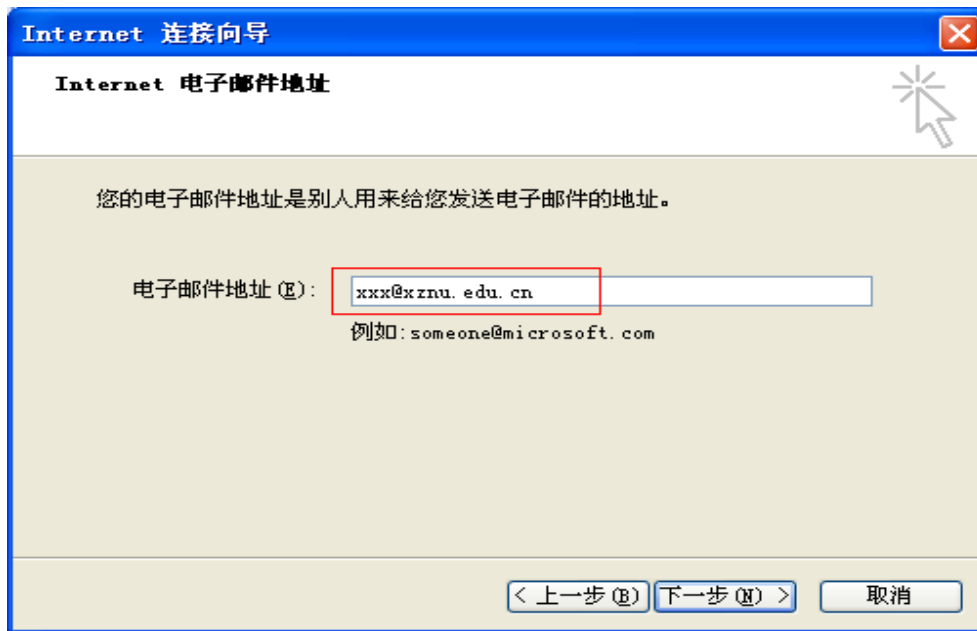
(图 3-65)

进入 Internet 连接向导，先是“您的姓名”项（填入您想在发件人处显示的名字），如（图 3-66）：



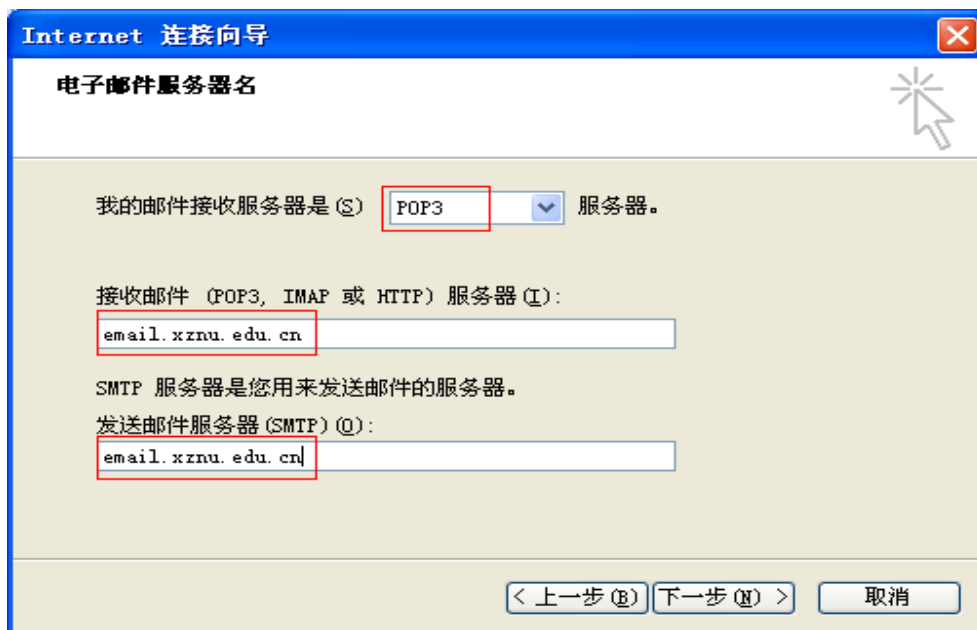
(图 3-66)

接着进入“Internet 电子邮件地址”项，一般情况下，我们选择“我想使用一个已有的电子邮件地址”，然后在电子邮件地址栏中填入已经申请过的有效电子邮件地址，如 [xxx@xznu.edu.cn](mailto:xxx@xznu.edu.cn)（图 3-67）。



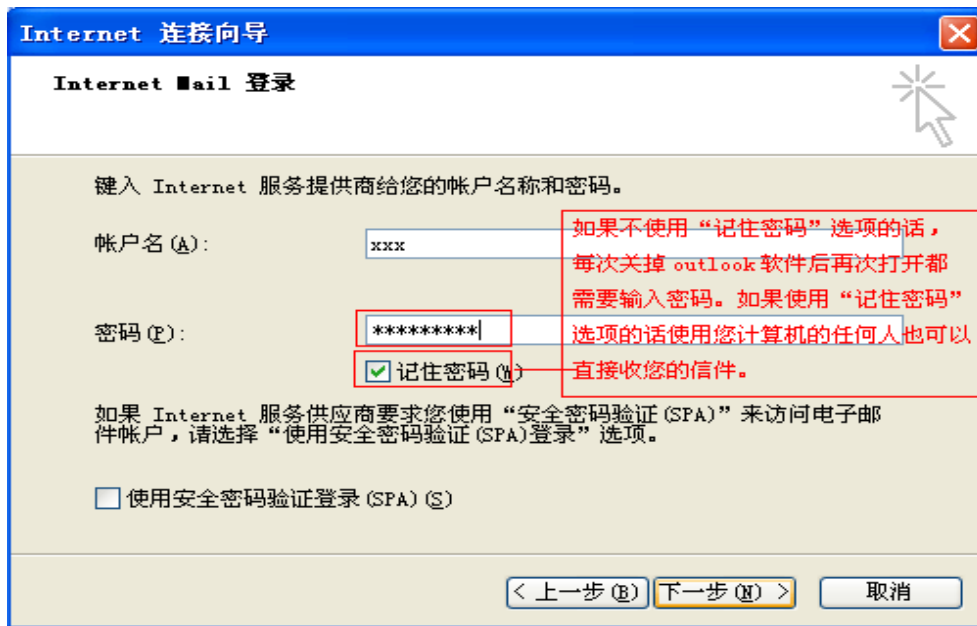
(图 3-67)

下一步比较重要，需要填入电子邮件服务器名，这依据您申请的邮箱而有所不同。现在我们所用的邮箱，大多采用 POP3 与 SMTP 服务器（图 3-68）。



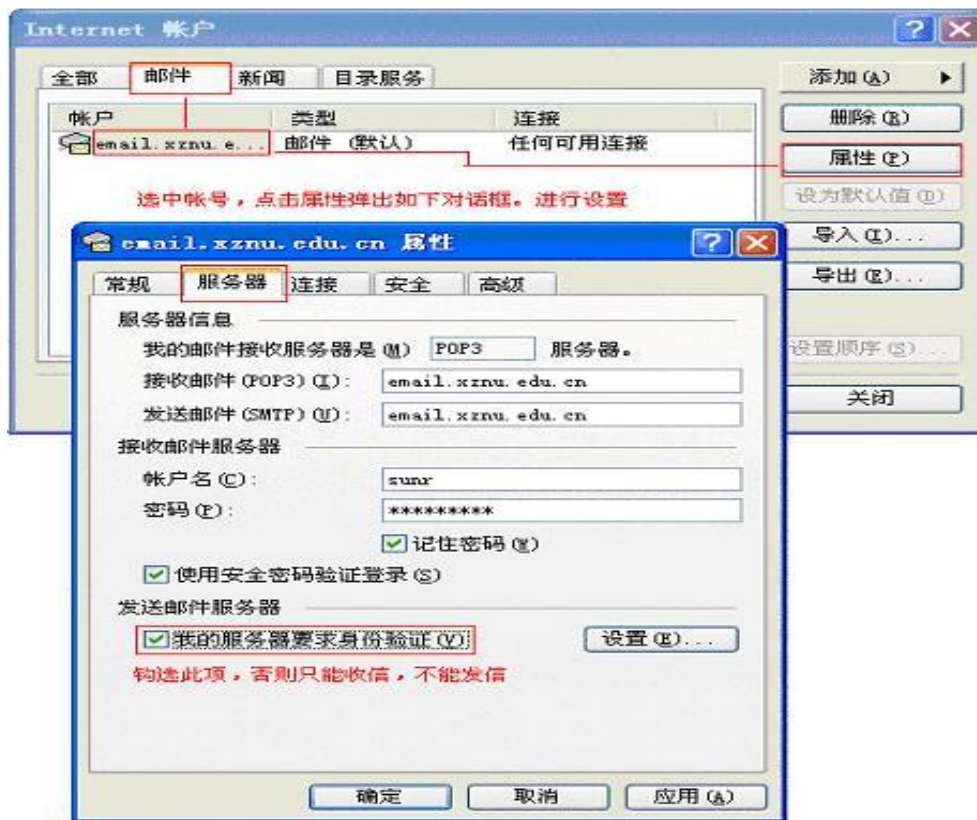
(图 3-68)

键入你的账户名和密码，就 OK 了（图 3-69）。



(图 3-69)

邮件系统通过 Outlook、Foxmail 等邮件软件发信件需要认证，所以还有一项设置。点击 [工具] → [账号]，在 Internet 账户窗口，邮件选项下，选中账户，点击属性弹出对话框，进行如下（图 3-70）的设置：



(图 3-70)

到此，邮件账户设置完成。现在可以开始接收、发送邮件了！

### 3.3.2 如何使用 Foxmail

前面介绍如何使用 MAILGARD 佑友提供的 Webmail 客户端及使用 Windows 自带的 Outlook 来收发您的邮件，下面我们再介绍一下怎样使用 Foxmail 来收发邮件。

在此我们默认您已经正确安装了 Foxmail，以下我们以 Foxmail 6.0 为例说明。

若是 Foxmail 还未设置账号，则运行 Foxmail 时就会出现“Foxmail 用户向导”；同样，若您已经在 Foxmail 中设置了账号，也可以从菜单“邮箱”->“新建邮件用户”中打开“Foxmail 用户向导”。如下图（图 3-71）所示：

The screenshot shows the '向导' (Wizard) window for creating a new user account. The title bar says '向导'. On the left is a vertical banner with the Foxmail 6 logo. The main content area is titled '建立新的用户帐户' (Create New User Account). Below the title, there is a red instruction: '红色项是您需要填写的。其它选填，如“密码”可在收发邮件时再输入。' (Red items are required. Other optional items, such as 'password', can be entered when sending and receiving mail.)

Fields and labels:

- [必填] 电子邮件地址 (A): [Text input field]
- 密码 (W): [Text input field]
- [必填] 帐户显示名称 (U): [Text input field]
- 邮件中采用的名称 (S): [Text input field]
- 邮箱路径 (M): [Text input field with '<默认>' (Default) selected]

Buttons at the bottom:

- < 上一步 (B) (Previous Step)
- 下一步 (N) > (Next Step)
- 取消 (C) (Cancel)
- 帮助 (H) (Help)

(图 3-71)

在（图 3-72）中点击“下一步”，进入如（图 3-67）所示设置界面，在这个界面中只需填入“邮件地址，密码”即可，所填的用户名用来标识您即将设置的那个账号。

The screenshot shows the '向导' (Wizard) window for specifying the mail server. The title bar says '向导'. On the left is a vertical banner with the Foxmail 6 logo. The main content area is titled '指定邮件服务器' (Specify Mail Server). Below the title, there is a red instruction: 'POP3 (PostOffice Protocol 3)服务器是用来接收邮件的服务器，您的邮件保存在其上。如public.guangzhou.gd.cn。' (POP3 (PostOffice Protocol 3) server is used to receive mail. Your mail is stored on it. For example, public.guangzhou.gd.cn.)

Fields and labels:

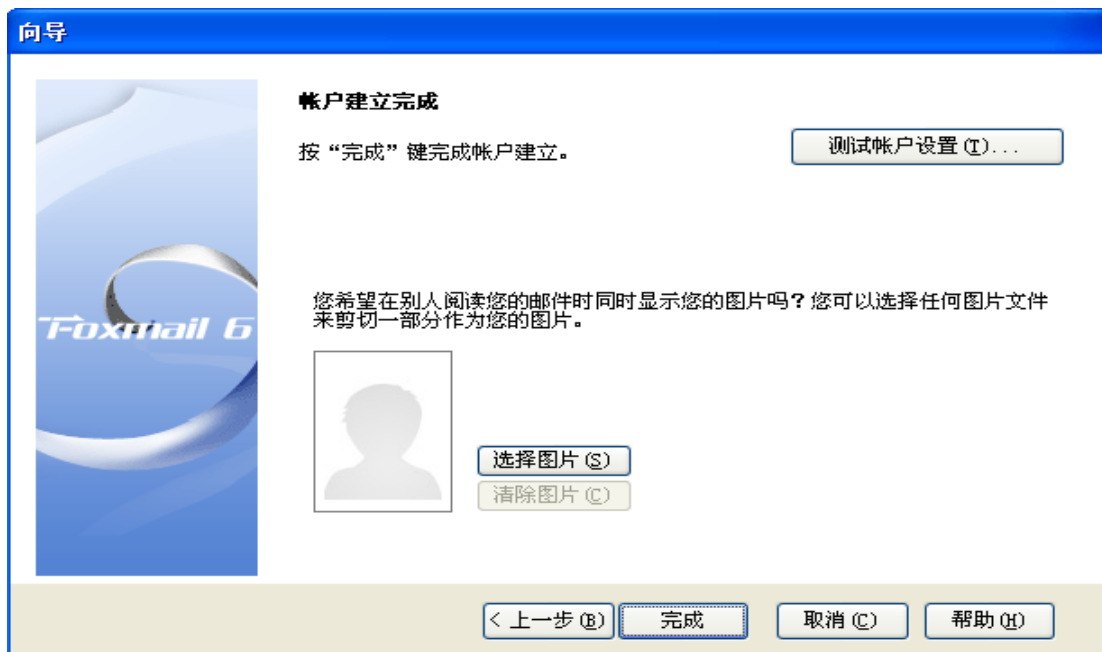
- 接收服务器类型 (T): [Dropdown menu showing 'POP3']
- 接收邮件服务器 (I): [Text input field containing 'pop.hechen.com']
- 邮件帐户 (A): [Text input field]
- SMTP (Simple Mail Transfer Protocol)服务器用来中转发送您发出的邮件。SMTP服务器与POP3服务器可以不同。 (SMTP server is used to relay mail sent by you. SMTP server and POP3 server can be different.)
- 发送邮件服务器 (O): [Text input field containing 'smtp.hechen.com']

Buttons at the bottom:

- < 上一步 (B) (Previous Step)
- 下一步 (N) > (Next Step)
- 取消 (C) (Cancel)
- 帮助 (H) (Help)

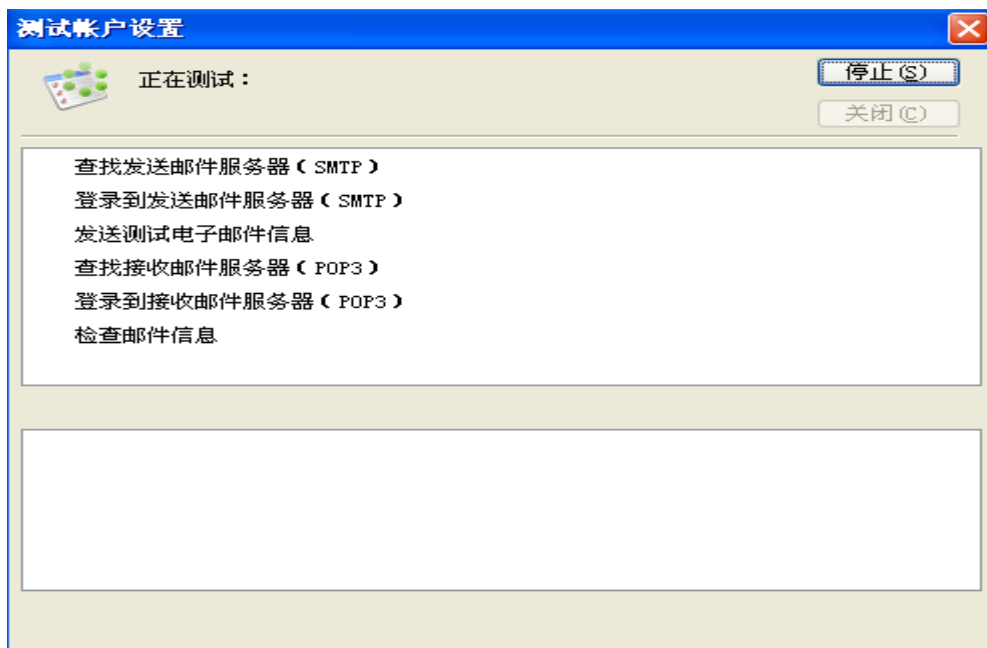
(图 3-72)

填入好用户名(U)后,在(图3-72)中点击“下一步”,进入如(图3-73)所示的测试帐户设置界面。测试你所设置的邮件用户帐户是否正确。因为这一步的填写将直接关系到,您是否能接收及发送邮件。



(图 3-73)

点击“测试帐户设置”,进入如(图3-74)所示的邮件服务器设置,这一步中 Foxmail 系统都已经设置好,当你的测试的帐户没有错误时。该邮件帐户已经可以使用。



(图 3-74)

点击下一步,进入最后一步设置,保持默认即可,直接点击“完成”,便完成了我们在 Foxmail

中账号的设置（图 3-75）。



（图 3-75）

完成这些设置后，会自动进入 Foxmail 程序主界面，在主界面左侧您可以看见刚才所设置的邮件账号。至此，您便可以使用该账号进行邮件的收发了。

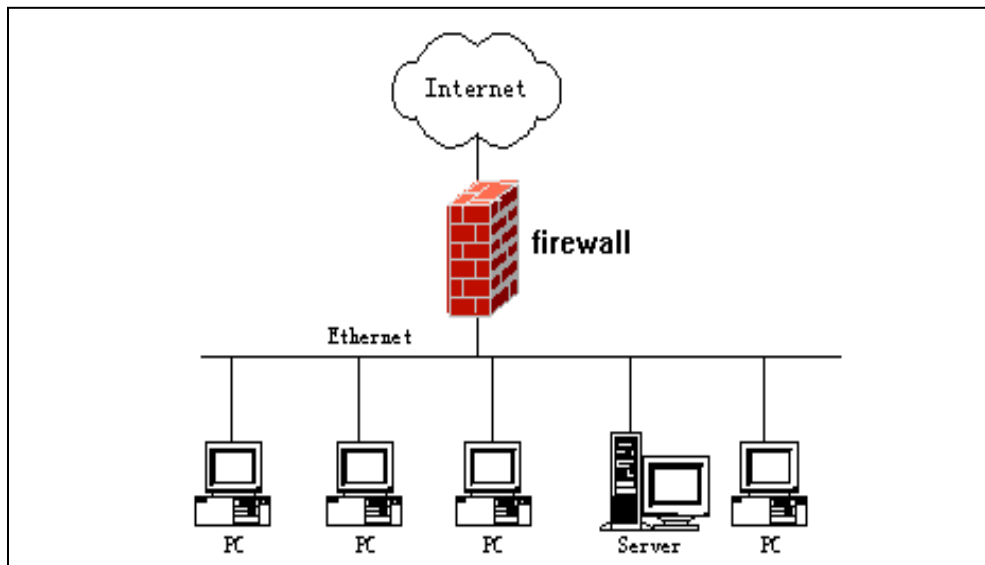


## 第三章 防火墙管理

### 1、MAILGARD 佑友防火墙产品概述

#### 1.1 MAILGARD 佑友防火墙类型及特点

- ◇ MAILGARD 佑友防火墙类型为**网络级**防火墙，它不同于一般计算机上所安装的各种单机版防火墙。
- ◇ MAILGARD 佑友内置防火墙支持标准和扩展的 ACL 包过滤、状态检测防火墙和防 DoS（Denial of Service，拒绝服务）功能。不仅保护内部网络免遭外来攻击，还可以使用策略表有效控制内部主机对外部资源的访问，对一些特殊的网络应用程序进行精确的控制，形成内外网络之间的安全保护屏障。
- ◇ MAILGARD 佑友内置防火墙支持标准的 NAT、DMZ 等应用，还支持 IP/MAC 地址绑定以进一步提高安全性。
- ◇ MAILGARD 佑友内置防火墙的 NAT 特性支持 H. 323 协议，可以识别 H. 225. 0（RAS、Q. 931）、H. 245 消息，完成对这些报文载荷的地址转换，从而使 MAILGARD 佑友内置防火墙设备可以完全透明地支持多媒体应用。
- ◇ 防火墙对流经它的网络通信进行扫描，这样能够过滤掉一些攻击，以免其在目标计算机上被执行。防火墙还可以关闭不使用的端口，而且它还能禁止特定端口的流出通信，封锁特洛伊木马。



（网络防火墙使内部网络和因特网隔离）图 1-1

### 2、防火墙配置步骤

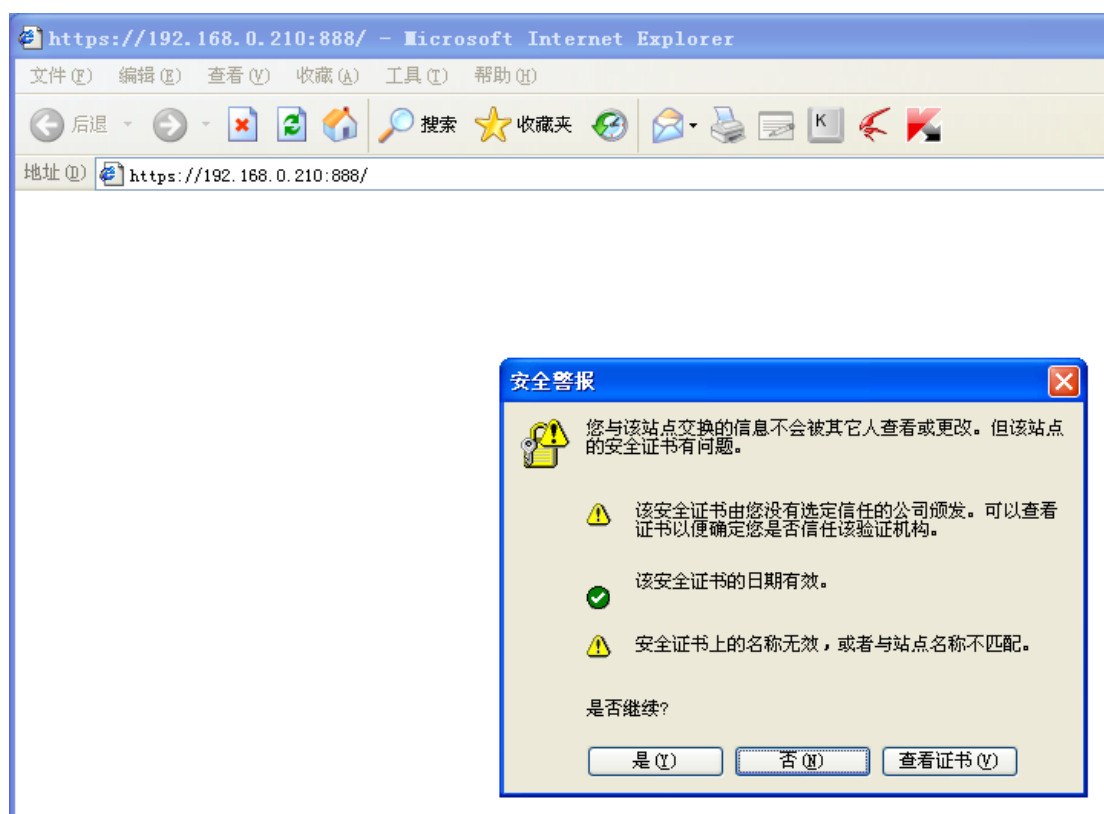
#### 2.1 如何登陆 MAILGARD 佑友防火墙管理配置界面

2.1.1 按照前面的安装方法，连接好以后，通过 web 界面来管理配置 MAILGARD 佑友防火墙设备。

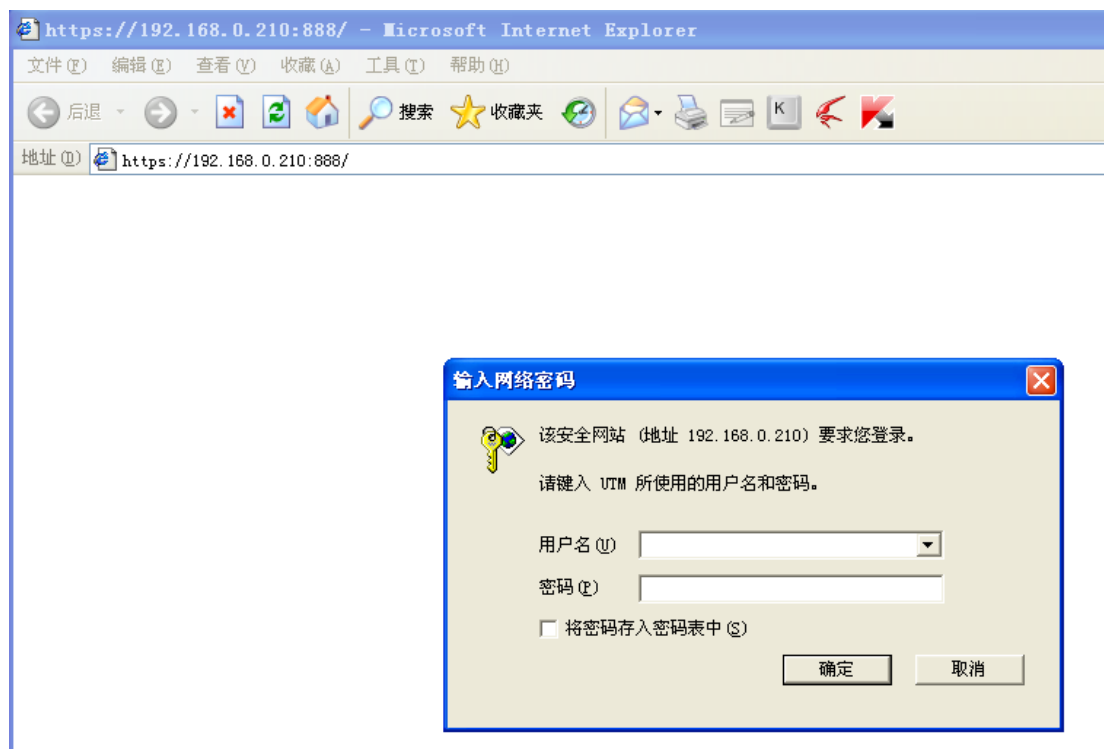
方法如下：

首先在本机器上配置一个跟 MAILGARD 佑友防火墙同一网段的 IP 地址（MAILGARD 佑友防火墙默认局域网接口的 IP 地址是 192.168.0.210），然后在 IE 浏览器中输入 MAILGARD 佑友防火墙的默认登

陆 IP 及端口，比如 <https://192.168.0.210:888>，如(图 2-1，图 2-2)



(图 2-1)



(图 2-2)

登陆框输入[用户名]和[密码]点击[登陆]即可登陆。

小贴士:

默认出厂的用户名跟密码是 admin, 强烈建议配置好以后修改密码。

2.1.2 登陆管理界面后, 将看到如下信息, 如 (图 2-3)。



(图 2-3)

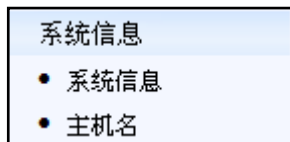
## 2.2 系统管理

### 2.2.1 功能模块



### 2.2.2 如何查看系统信息

系统管理-系统信息



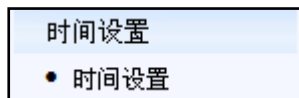
系统信息可以显示系统的主要信息, 比如硬件版本, 软件版本以及 CPU 内存信息等。如 (图 2-4)



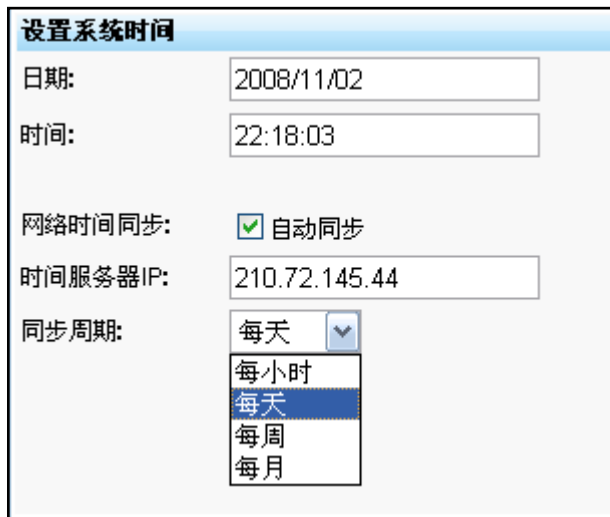
图(2-4)

### 2.2.3 如何修改系统时间

#### 系统信息-时间设置



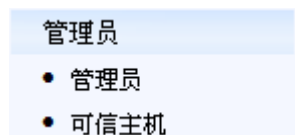
系统时间选项可以手动设置系统的时间，同时也可以设置系统与标准的时间服务器进行同步，可以选择同步的频率，每小时；每天；每星期和每月进行同步一次时间。系统默认的时间服务器地址是中国国家授时中心的时间服务器：210.72.145.44。如(图 2-5)



(图 2-5)

### 2.2.4 如何修改管理员密码以及选择系统管理界面的语言版本

#### 系统管理-管理员



- ◇ 设置管理界面的语言版本及简体中文与繁体中文版。
- ◇ 修改管理员密码，密码长度是 6-13 位字母或者数字。如（图 2-6，图 2-7）

管理员			
登录账号	权限	语言	
admin	可读可写	简体中文	

(图 2-6)

### 编辑管理员

编辑管理员:

权限:  可读可写  只读

语言:  ▼

更改密码

密码:

确认密码:

(图 2-7)

- ◇ 设置新的管理员，并设置对应权限。（图 2-8，图 2-9）

### 编辑管理员

编辑管理员:

权限:  可读可写  只读

语言:  ▼

更改密码

密码:

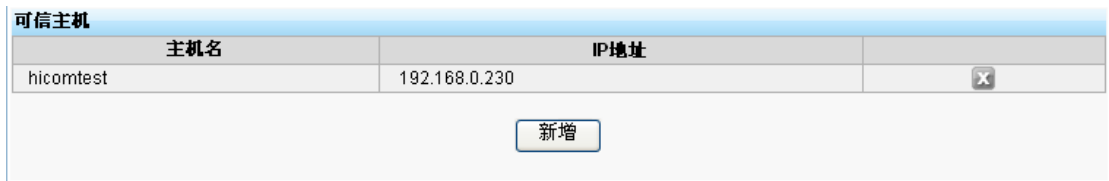
确认密码:

(图 2-8)



(图 2-9)

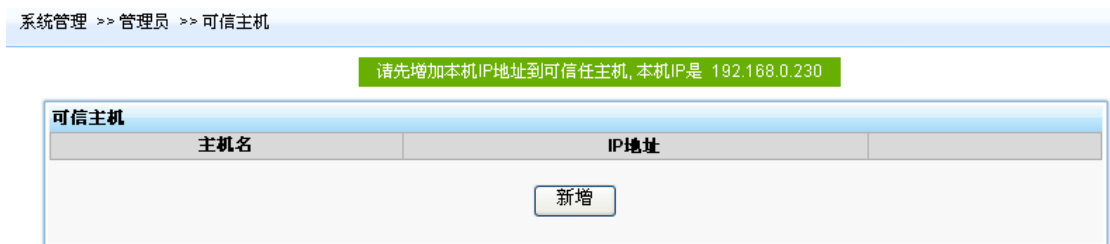
◇ 设置可信主机，非可信主机访问受限。(图 2-10, 图 2-11, 图 2-12)



(图 2-10)



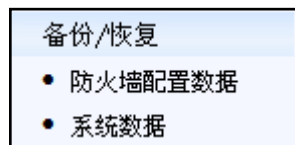
(图 2-11)



(图 2-12)

## 2.2.5 如何对防火墙设置以及系统数据进行备份和恢复

### 系统信息-备份/恢复



防火墙配置数据备份是针对当前设置的防火墙的规则策略进行备份，假如您对这个防火墙的操作不是非常的熟练，建议在修改和新建规则之前进行防火墙配置数据备份，备份的数据以 MAILGARD 佑友 系统数据格式保存在系统，也可以下载到本地电脑进行保存。点击恢复的时候即可恢复备份数据。如（图 2-13）



(图 2-13)

系统数据备份是对整个的系统数据进行备份，包括网站数据，邮箱数据以及数据库。备份的数据将以 MAILGARD 佑友 系统数据格式保存在系统，也可以下载到本地电脑保存。如（图 2-14）



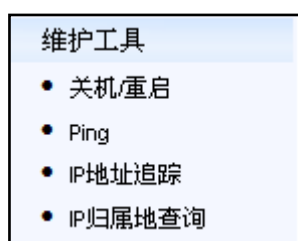
（图 2-14）

小贴士：

系统数据备份由于是对网站数据，邮箱数据以及数据库进行备份，假如数据量大的时候备份的时间会稍微长些，请耐心等待，有新的备份时候可以清除上一次备份，以免大量的数据备份在系统对使用造成影响。

## 2.2.6 如何关机与重启动以及使用 MAILGARD 佑友的维护工具对网络进行简单的检查

系统信息-维护工具，维护工具包括关机/重启；ping 命令；IP 地址追踪；IP 归属地查询。



- ◇ 关机与重启功能是在有需要情况下对服务器进行关机与重启操作，关机在执行关机操作后 3~4 分钟关闭电源即可。一般情况下 MAILGARD 佑友 服务器可以 24 小时运行，无需关机。
- ◇ Ping 命令是在 MAILGARD 佑友 服务器上执行用来检查从 MAILGARD 佑友 到目的地址最基本的网络连通性。源地址指 MAILGARD 佑友 某接口的 IP 地址。
- ◇ IP 地址追踪功能是用来查询从服务器到某个目的 IP 地址中间所经过的路由环节以及 IP 地址信息。如（图 2-15）。



（图 2-15）

◇ IP 归属地查询是用于查询某个公网 IP 地址的具体信息。如（图 2-16）

The screenshot shows a web interface titled "IP 归属地查询" (IP Location Query). It features a search box with the IP address "202.96.134.134" and a "查询" (Query) button. Below the search box, there is a section titled "详细信息" (Detailed Information) containing the following data:

IP 归属地	: 广东省深圳市 电信
inetnum	: 202.96.128.0 - 202.96.191.255
netname	: CHINANET-GD
descr	: CHINANET Guangdong province network
descr	: Data Communication Division
descr	: China Telecom
country	: CN
admin-c	: CH93-AP
tech-c	: IC83-AP
mnt-by	: APNIC-HM
mnt-lower	: MAINT-CHINANET-GD
changed	: hm-changed@apnic.net 20040906
status	: ALLOCATED PORTABLE
changed	: hm-changed@apnic.net 20041210
source	: APNIC
person	: Chinanet Hostmaster
nic-hdl	: CH93-AP
e-mail	: anti-spam@ns.chinanet.cn.net
address	: No.31 ,jingrong street,beijing
address	: 100032
phone	: +86-10-58501724
fax-no	: +86-10-58501724

（图 2-16）

## 2.3 网络设置

### 2.3.1 功能模块



### 2.3.2 如何配置 MAILGARD 佑友防火墙

LAN 接口和 WAN 接口 IP 地址以及外网接入方式等。

#### 网络设置-网络接口





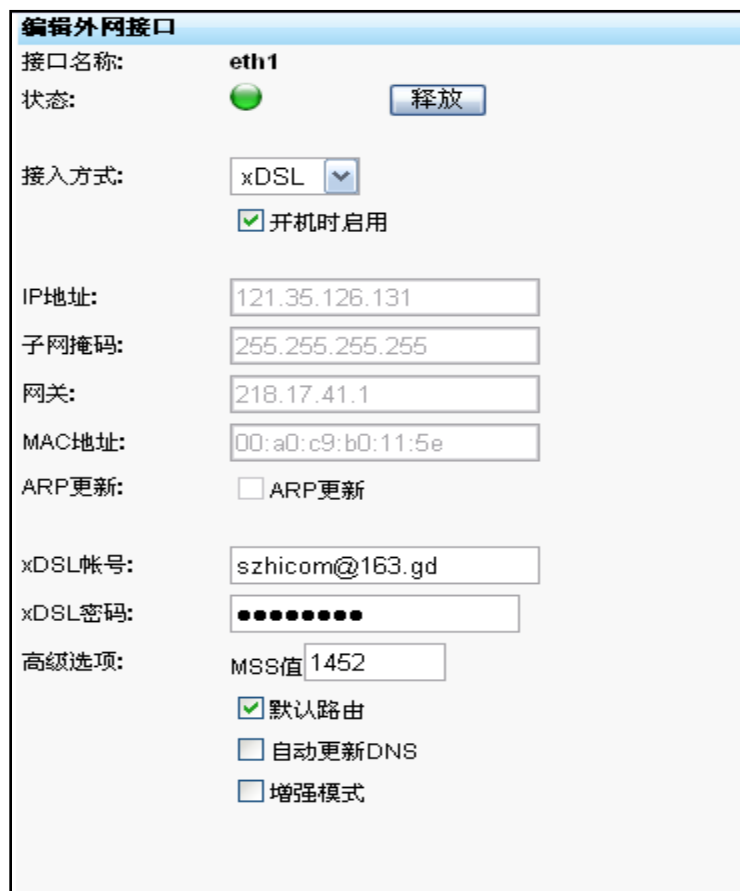
**内网接口：**配置内网接口(LAN)IP 地址，以及重启内网接口，当状态显示为绿色时候，表示接口正常连接。显示灰色的时候，表示接口连接不正常或者未连接。如（图 2-17）。



内网接口	
接口名称:	eth0
状态:	<span style="color: green;">●</span> <span>重启</span>
IP地址:	192.168.0.254
子网掩码:	255.255.255.0
MAC地址:	00:a0:c9:b0:11:5d
ARP更新:	<input checked="" type="checkbox"/> ARP更新

(图 2-17)

**外网接口：**配置外网的接入方式，支持 ADSL，固定 IP 和 DHCP 等多种接入方式，ADSL 拨号上网的时，断线能自动拨号，同时 MAILGARD 佑友防火墙也提供了手动拨号的功能。如（图 2-18）



编辑外网接口	
接口名称:	eth1
状态:	<span style="color: green;">●</span> <span>释放</span>
接入方式:	xDSL <span>▼</span>
	<input checked="" type="checkbox"/> 开机时启用
IP地址:	121.35.126.131
子网掩码:	255.255.255.255
网关:	218.17.41.1
MAC地址:	00:a0:c9:b0:11:5e
ARP更新:	<input type="checkbox"/> ARP更新
xDSL帐号:	szhicom@163.gd
xDSL密码:	●●●●●●●●
高级选项:	MSS值 1452
	<input checked="" type="checkbox"/> 默认路由
	<input type="checkbox"/> 自动更新DNS
	<input type="checkbox"/> 增强模式

(图 2-18)

**扩展接口：**扩展接口可以作为内网接口使用，也可以作为外网接口使用。作为内网接口时候，可以

完全从物理上完全隔离不同的局域网。作为外网接口的时候，主要是用来多条外网线路捆绑，实现负载均衡。如（图 2-19）

扩展接口							
接口名称	开机时启用	接入方式	IP地址	子网掩码	网关	状态	
eth2	✓	固定IP	194.0.0.1	255.255.255.0		●	⊕ ⊞
eth3	✓	固定IP	195.0.0.1	255.255.255.0		●	⊕ ⊞

（图 2-19）

**虚拟接口：**虚拟接口相当于在一个网络接口上面配置多个 IP 地址。作用有两个方面，内网虚拟接口和外网虚拟接口。

**内网虚拟接口**可以利用 **MAILGARD 佑友**来把内网划分成多个网段，比如内网接口我们默认配置的 IP 地址是 192.168.0.210，子网掩码是 255.255.255.0，这时候内网的电脑都是 192.168.0.x，以 192.168.0.210 为默认网关上网，当上网电脑台数增加，已经超过 254 台电脑出现一个网段的 IP 地址不够用的时候，我们可以通过新增内网虚拟接口方式另外划分一个网段，如新增内网虚拟接口，IP 地址是 192.168.1.210，子网掩码是 255.255.255.0，内网就可以把新增加的电脑设置成 192.168.1.x，子网掩码为 255.255.255.0，以 192.168.1.210 为默认网关。

**外网虚拟接口**主要是用来把某一公网 IP 地址通过 DMZ 或者端口映射方式映射给内网的某台应用服务器，实现对外发布内网的服务器。前提条件是有多多个固定 IP 地址外网接如方式，比如 ISP 服务商提供一组 IP 地址为 121.15.170.170-173，子网掩码是 255.255.255.248，网关为 121.15.170.169。我们可以在 **MAILGARD 佑友**防火墙上上面设置外网接口 IP 地址是 121.15.170.170，增加外网虚拟接口，IP 地址是 121.15.170.171。

**小贴士：**

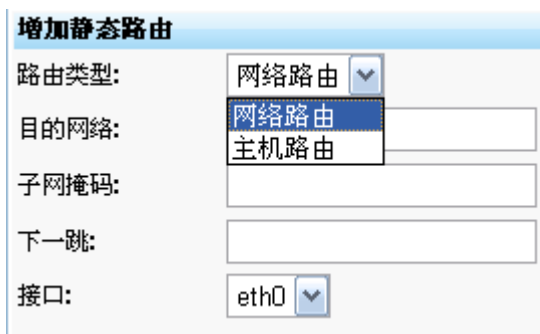
在配置虚拟接口或者扩展接口的时候，不能为同一网段的 IP，比如内网接口的 IP 地址是 192.168.0.210 那么我们在配置虚拟接口或者扩展接口的时候就不能设置成 192.168.0.x。

**2.3.3 如何设置静态路由以及主机路由**

网络设置-路由管理



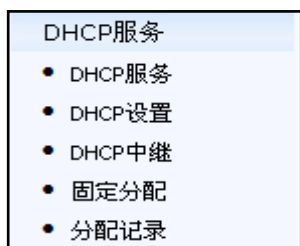
- ◇ 路由表：系统默认自动产生的路由表信息
- ◇ 静态路由：根据不同的网络环境自行可设置静态路由和主机路由。如（图 2-20）



（图 2-20）

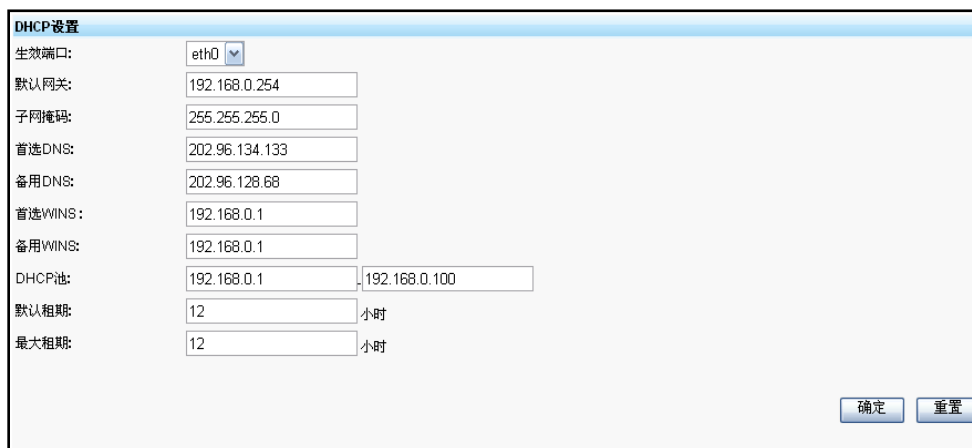
## 2.3.4 如何设置 DHCP 服务

网络设置-DHCP 服务



**DHCP 服务：** 设置 DHCP 服务启动与停止以及开机自启动。

**DHCP 设置：** 配置 DHCP 服务的默认网关以及 DHCP 池等。如（图 2-21）



DHCP设置配置窗口，包含以下配置项：

生效端口:	eth0
默认网关:	192.168.0.254
子网掩码:	255.255.255.0
首选DNS:	202.96.134.133
备用DNS:	202.96.128.68
首选WINS:	192.168.0.1
备用WINS:	192.168.0.1
DHCP池:	192.168.0.1 - 192.168.0.100
默认租期:	12 小时
最大租期:	12 小时

底部按钮：确定、重置

（图 2-21）

**DHCP 中继：** 主要是通过 DHCP 中继功能来使用网络上的其它 DHCP 服务器。启用 DHCP 中继功能时候，MAILGARD 佑友防火墙的本身的 DHCP 功能要处于停止状态。如（图 2-22）



DHCP中继配置窗口，包含以下配置项：

启用服务

服务状态:   重启服务

中继网络接口: eth1

DHCP服务器IP: 192.168.0.253

(注:如有多个网络接口或IP地址,用空格分开)

底部按钮：确定、重置

（图 2-22）

**固定分配：** 固定分配功能是让 MAC 地址为 xx:xx:xx:xx:xx:xx 某台电脑 DHCP 自动获取 IP 地址时候，固定获取某一 IP 地址。在设置固定分配时设置完需要重启 DHCP 服务才能生效。如(图 2-23)



主机标识	主机MAC地址	固定分配的IP地址	
aaa	00:1E:C9:00:E7:36	2.2.2.2	<input type="text"/> <input type="text"/>

底部按钮：新增

（图 2-23）

分配记录：显示 DHCP 已经分配的 IP 地址记录的详细信息。如（图 2-24）

主机名	MAC地址	分配的IP地址	获取时间
	00:10:b5:ef:88:cd	192.168.0.96	5 2008/10/24 23:48:39
	00:10:b5:ef:86:54	192.168.0.97	6 2008/10/25 06:29:25
hhpserver	00:1e:c9:00:e7:36	192.168.0.99	5 2008/10/31 00:20:20
	00:0c:29:96:c5:53	192.168.0.94	5 2008/10/31 03:38:11
	00:0c:29:de:66:55	192.168.0.98	5 2008/10/31 03:38:51
PC-200807151105	00:0d:60:89:76:20	192.168.0.100	0 2008/11/02 23:40:42
sl-03server	00:21:70:fe:34:9f	192.168.0.95	0 2008/11/02 23:56:14
hicom-14133264d	00:0c:29:4a:e2:59	192.168.0.93	1 2008/11/03 00:07:13

全部删除

(图 2-24)

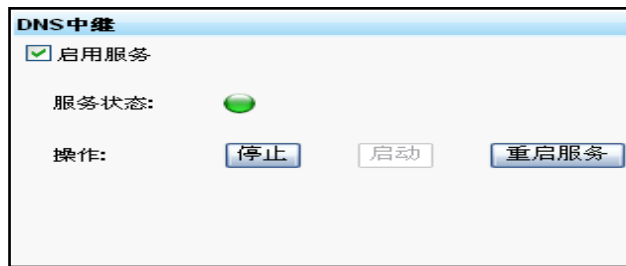
### 2.3.5 如何设置 DNS 以及 DNS 中继

网络设置-DNS 设置



**DNS Client:** 设置 DNS 服务器地址。

**DNS 中继:** DNS 中继的作用主要是用来中继内网电脑的 DNS 请求，启用 DNS 中继服务，内网的电脑的 DNS 可以直接设置为 MAILGARD 佑友防火墙 IP 地址。比如 MAILGARD 佑友服务器的 IP 地址是 192.168.0.210，启用 DNS 中继服务，电脑的的 DNS 地址就可设置为 192.168.0.210。

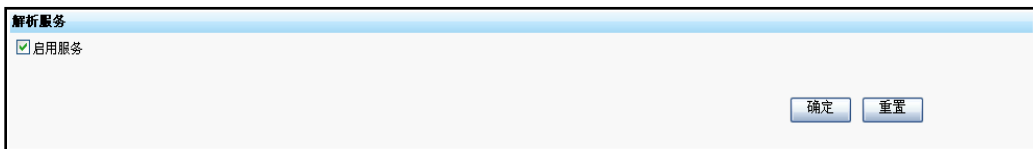


### 2.3.6 如何配置动态域名

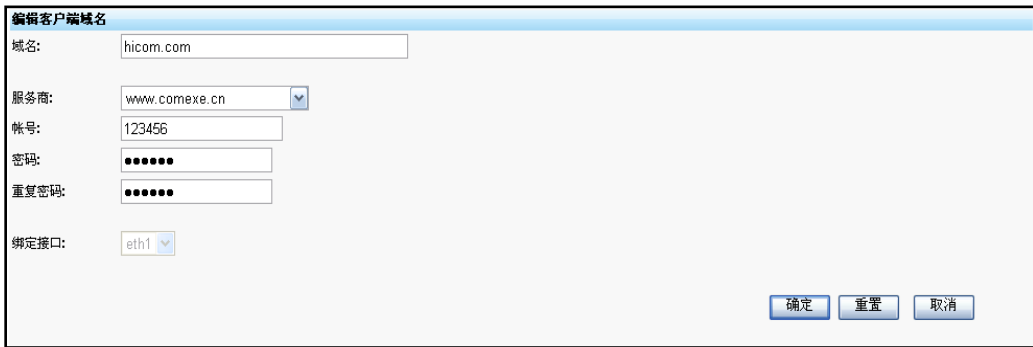
网络设置-DDNS 设置



**解析服务:** 设置启用 DDNS 服务，勾选表示启用该服务。

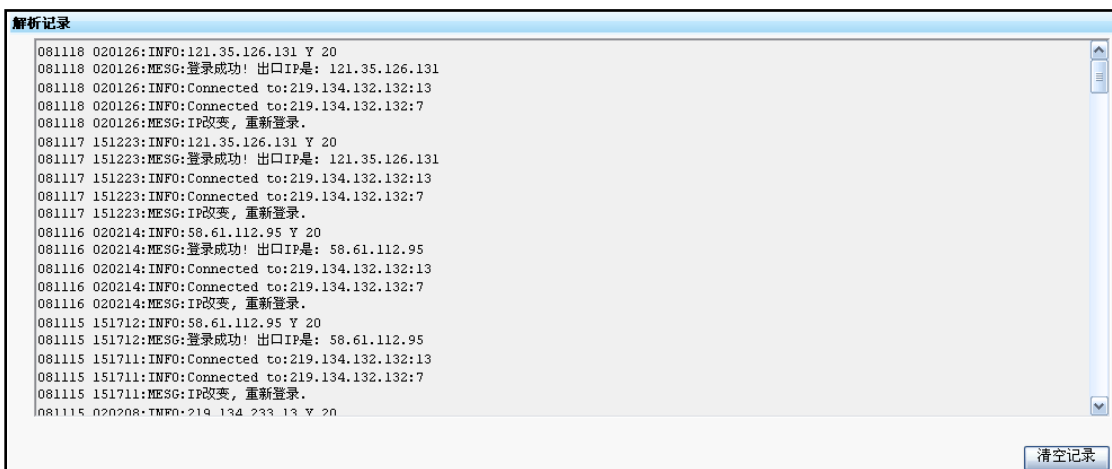


**动态域名:** 配置动态域名客户端，支持国内外多个动态域名解析服务商，比如科迈 (comexe.cn) 希网 (www.3322.org) 等。配置动态域名时候，前提条件必须是该域名 DNS 解析服务器地址已经指向该动态域名解析服务商的 DNS 服务器地址，并做好相应的解析服务。如(图 2-25)



(图 2-25)

**解析记录：** 显示动态域名解析记录，如（图 2-26）。



(图 2-26)

## 域名相关知识

动态域名服务 DDNS (Dynamic Domain Name Server) 是动态域名服务的缩写，DDNS 是将用户的动态 IP 地址映射到一个固定的域名解析服务上，用户每次连接网络的时候客户端程序就会通过信息传递把该主机的动态 IP 地址传送给位于服务商主机上的服务器程序，服务项目器程序负责提供 DNS 服务并实现动态域名解析。

### 什么是 A 记录

A (Address) 记录，是用来指定主机名（或域名）对应的 IP 地址记录。用户可以将该域名下的网站服务器指向到自己的 web server 上。

### 什么是 mx 记录

MX (Mail Exchanger) 记录，是邮件交换记录，它指向一个邮件服务器，用于电子邮件系统发邮件时根据 收信人的地址后缀来定位邮件服务器。例如，当 Internet 上的某用户要发一封信给 user@mydomain.com 时，该用户的邮件系统通过 DNS 查找 mydomain.com 这个域名的 MX 记录，如果 MX 记录存在，用户计算机就将邮件发送到 MX 记录所指定的邮件服务器上。

### 什么是 ns 记录

NS (Name Server) 记录，是域名服务器记录，用来指定该域名由哪个 DNS 服务器来进行解析。

### 检查 MX 记录是否存在的方法

进行 DNS 查询的一个非常有用的工具是 nslookup，可以使用它来查询 DNS 中的各种数据。可以在 Windows 的命令行下直接运行 nslookup 进入一个交互模式，在这里能查询各种类型的 DNS 数据。DNS 的名字解析数据可以有各种不同的类型，有设置这个 zone 的参数的 SOA 类型数据，有设置名字对应的 IP 地址的 A 类型数据，有设置邮件交换的 MX 类型数据。这些不同类型的数据均可以通过 nslookup 的交互模式来查询，在查询过程中可以使用 set type 命令设置相应的查询类型。如：

```
C:\>nslookup
Default Server: [202.106.184.166]
Address: 202.106.184.166
> set type=mx
> sina.com.cn
Default Server: [202.106.184.166]
Address: 202.106.184.166
Non-authoritative answer:
sina.com.cn MX preference = 10, mail exchanger = sinamx.sina.com.cn
sina.com.cn nameserver = ns1.sina.com.cn
sina.com.cn nameserver = ns3.sina.com.cn
sinamx.sina.com.cn internet address = 202.106.187.179
sinamx.sina.com.cn internet address = 202.106.182.230
ns1.sina.com.cn internet address = 202.106.184.166
ns3.sina.com.cn internet address = 202.108.44.55
```

如果所要查的某域名的 MX 记录不存在，则出现与以下类似的提示：

```
C:\>nslookup
> set type=mx
> amafdsfxit.com.cn
Default Server: [202.106.184.166]
Address: 202.106.184.166
*** 202.106.184.166 can't find amaxit.com.cn: Non-existent domain
```

## 2.4 上网控制

### 2.4.1 功能模块



## 2.4.2 如何添加上网用户以及设置上网权限

上网控制-上网用户



**上网用户：**MAILGARD 佑友防火墙作为网关设备使用时，内网的电脑通过 MAILGARD 佑友上网时，必须要在防火墙添加上网用户以及设置相应的权限。上网用户可以是单个 IP 地址，也可以是连续的 IP 地址，同样也支持网段的格式。如（图 2-27）

（图 2-27）

**权限组：**MAILGARD 佑友防火墙默认有两个权限组，全权限和零权限。全权限根据字面意义理解，就是对上网行为不做任何的控制。相反零权限的意思那就是没有任何权限，也就是不能上网。但是在实际的使用环境中我们会遇到一种情况是：有一部分电脑用户上网给全权限太高，给零权限不行，那么就需要自己定义权限。根据上图我们看到在新增加上网用户选择权限时候有新建组选项，那就是新增加权限组的意思。新建权限组有两种方式，一种就是添加上网用户时候直接新建权限组，另一种就是直接在权限组中新增。如（图 2-28，图 2-29）

### 增加/编辑上网用户

用户名称:

IP地址:
   
 单个 
  
 连续  - 
  
 网段  /

部门:

权限:
   
 X 零权限
   
 ✓ 全权限
   
 关联 
  
 新建组

(图 2-28)

### 编辑权限组

权限组:

时间表:
   
 全时段  关联

上网:
   
 禁止  允许  黑名单   白名单

发邮件:
   
 禁止  允许  黑名单   白名单

收邮件:
   
 禁止  允许  黑名单   白名单

文件传输:
   
 FTP  BT  Kugoo  eMule  100Bao  迅雷

禁止下载:
   
 .exe  .mp3  .swf  .gif  .jpeg  .pdf  .rar  .tar  .zip  .flv

聊天工具:
   
 QQ  MSN  POPO  Yahoo  ICQ  POCO

在线游戏:
   
 中国游戏在线  联众世界  边锋网络游戏

在线视频:
   
 PPLive/PPStream/UUSee/QQLive

其它:

注:以逗号分开的单个端口或连续端口,如 21,22,90:100,8080

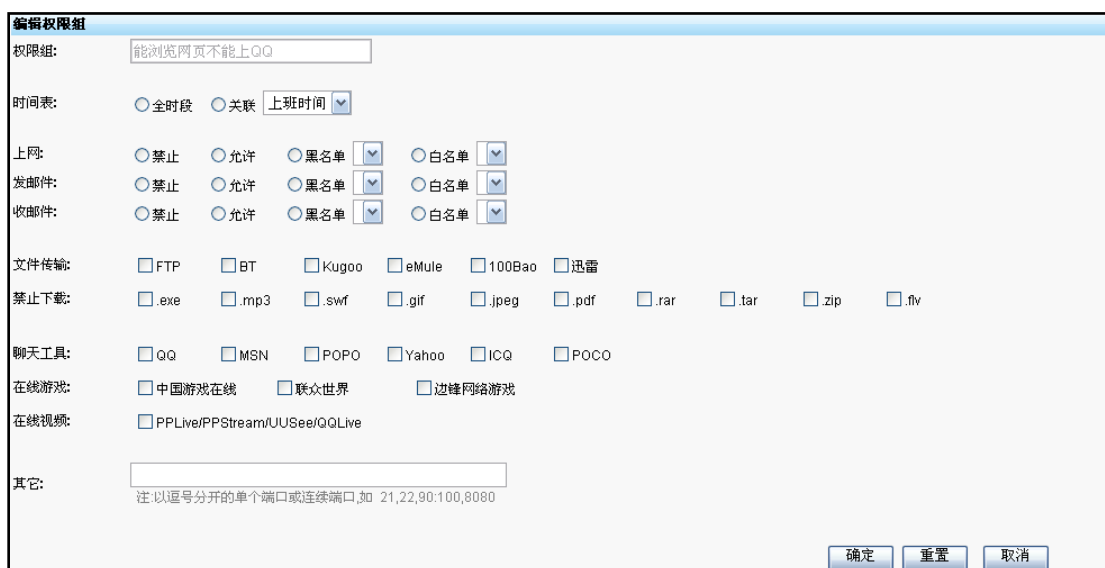
(图 2-29)

新建权限组上网权限设置说明。如 (图 2-30, 图 2-31)

权限组	时间表	上网	发邮件	收邮件	文件传输	禁止下载	聊天工具	在线游戏	在线视频	其它	
能浏览网页不能上QQ					...	...	...	...	...		
<input type="button" value="新增"/> <span style="float: right;"><input type="button" value="编辑"/></span>											



(图 2-30)



(图 2-31)

- ◇ 时间表：设置好时间表后，选择关联相应的时间表，可以基于不同时间段对上网行为进行控制。
- ◇ 上网：上网的意思就是浏览网页，可以选择禁止或者允许以及黑白名单的方式指定允许访问某个网站或者不允许访问某个网站。
- ◇ 发邮件：用来限制 smtp 方式（outlook 或者 foxmail 等）发送邮件，可以选择禁止或者允许以及黑白名单的方式来指定允许和禁止使用某个 smtp 服务器地址发送邮件。
- ◇ 收邮件：用来限制 pop 方式（outlook 或者 foxmail 等）接收邮件，可以选择禁止或者允许以及黑白名单的方式来指定允许和禁止使用某个 pop 服务器地址接收邮件。
- ◇ 文件传输：勾选为允许使用，不勾选为禁止使用，默认为禁止。
- ◇ 禁止下载：勾选为禁止，不勾选为允许，默认为允许。
- ◇ 聊天工具：勾选为允许使用，不勾选为禁止使用，默认为禁止。
- ◇ 在线游戏：勾选为允许使用，不勾选为禁止使用，默认为禁止。
- ◇ 在线视频：勾选为允许使用，不勾选为禁止使用，默认为禁止。
- ◇ 其它：作用于自定义开放内网用户访问外网某个服务器的某个特殊端口。

### 2.4.3 如何设置上网时间表

上网控制-时间表



**时间表：**按星期，小时，分钟设置。时间按 24 小时计时制。填写时间时候起始时间少于结束时间，比如早上 8:01 到晚上 12:00 我们不能填写 08:01-0:00，而是 08:01-24:00。如(图 2-32)

**新增时间表**

标识名称:

星期: 一 二 三 四 五 六 日

起止时间:  全天24小时  
 指定  -

(图 2-32)

#### 2.4.4 如何设置黑名单

上网控制-黑名单

**黑名单**

- 上网黑名单
- 发邮件黑名单
- 收邮件黑名单

**上网黑名单:** 上网黑名单添加方式以表名和名单的形式添加，表名跟名单形式主要意思是可以添加多个黑名单表名，不同的黑名单表名可以加入多个黑名单名单。实现不同部门不同权限组使用不同的浏览网页黑名单。如（图 2-33，图 2-34）

**上网黑名单**

表名	名单
新增表名: <input type="text" value="人事部浏览网页黑名单"/>	<input type="button" value="新增"/>
新增名单: <input type="text"/>	<input type="button" value="新增"/>

(图 2-33)

**上网黑名单**

表名	名单
人事部浏览网页黑名单	
新增表名: <input type="text"/>	<input type="button" value="新增"/>
新增名单: <input type="text" value="人事部浏览网页黑名单"/>	<input type="text" value="www.abc.com"/> <input type="button" value="新增"/>

(图 2-34)

发邮件黑名单：设置同上。如（图 2-35，图 2-36）

表名	名单
----	----

新增表名: 人事部发邮件黑名单

新增名单:

(图 2-35)

表名	名单
人事部发邮件黑名单	

新增表名:

新增名单: 人事部发邮件黑名单  smtp.163.com

(图 2-36)

收邮件黑名单：设置同上。如（图 2-37，图 2-38）

表名	名单
----	----

新增表名: 人事部收邮件黑名单

新增名单:

(图 2-37)

表名	名单
人事部收邮件黑名单	

新增表名:

新增名单: 人事部收邮件黑名单  pop.163.com

(图 2-38)

## 2.4.5 如何设置白名单

上网控制-白名单

白名单
• 上网白名单
• 发邮件白名单
• 收邮件白名单

上网、发邮件和收邮件的白名单设置方法可参考黑名单设置。

## 2.4.6 如何把 IP 跟 MAC 地址进行绑定 防止内网电脑用户盗用上网权限。

上网控制-IP/MAC



**IP-MAC:** 自动扫描内网电脑的电脑 MAC 地址，进行绑定。达到两个不同权限不同 IP 地址不能互相盗用上网权限情况。

**其他未绑定 IP 地址:** 设置没有绑定 MAC 地址的内网电脑允许或者禁止使用，当选择禁止使用使用，内网没有绑定 MAC 地址电脑将不能与 MAILGARD 佑友防火墙通信。

## 2.5 防火墙

### 2.5.1 功能模块



### 2.5.2 如何自定义防火墙规则 防火墙-规则定义



**规则定义:** 定义源地址，端口和目的地址，端口以及字符过滤，连接频率，并发会话连接数等来自定义防火墙规则，自定义规则也可以定义源 MAC 地址来进行设置，可对速度进行限制，能同时关联时间表和应用层过滤。如（图 2-39，图 2-40）

**增加规则定义**

入接口: == 不绑定接口

源地址: ==

单个IP  
 连续IP  
 网段  
 MAC地址  
 任意地址

出接口: == 不绑定接口

目的地址: ==

单个IP  
 连续IP  
 网段  
 任意地址

应用层过滤:  关联 QQ过滤

协议: == 全部

源端口: ==

(图 2-39)

目的端口: ==

字符过滤: == 十进制

连接频率: == / 秒 突发连接数 模式 任意

速度限制: == 不限 < K byte

并发会话数: 匹配掩码位

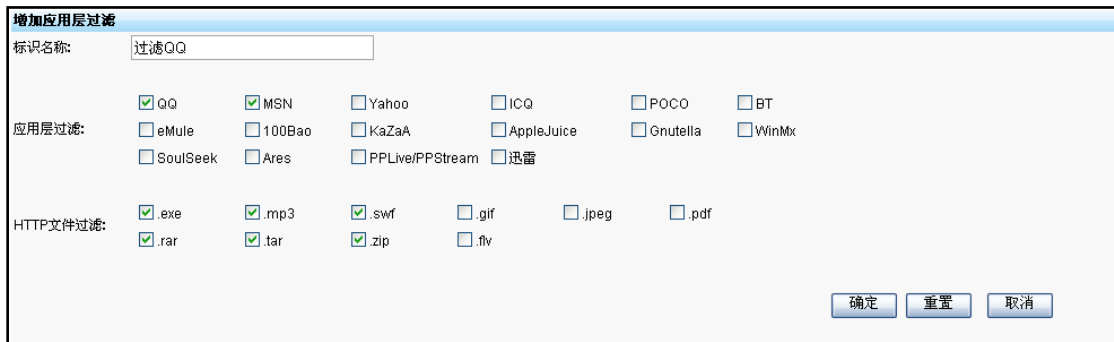
SYN:  匹配TCP会话中的SYN报文

时间表:  全时段  关联

动作:  禁止  允许

(图 2-40)

**应用层过滤：** 设置应用层过滤，设置好以后在自定义规则中关联该应用层过滤。如（图 2-41）



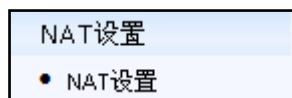
（图 2-41）

**小贴士：**

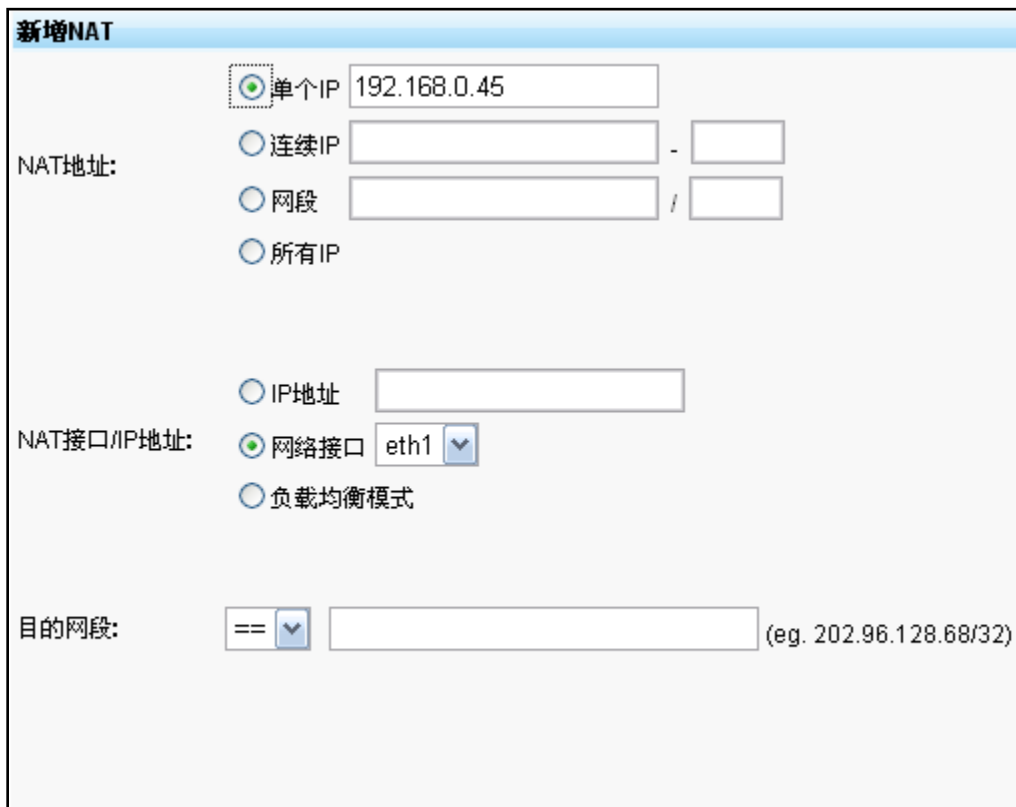
一般对上网行为的管理在上网用户及用户权限设置即可，防火墙自定义规则主要面向对网络有一定基础，对整个上网的数据流向非常清楚，来自行定义防火墙规则。错误的设置会导致会出现不能上网等情况。

### 2.5.3 如何设置 NAT 规则

#### 防火墙-NAT 设置



**NAT 设置：** 针对源 IP 地址设置 NAT 规则，可指定某个接口或者某个 IP 地址进行 NAT，支持多线路接入时负载均衡 NAT 模式。如（图 2-42）



（图 2-42）

## 2.5.4 如何设置端口映射

### 防火墙-端口映射



**端口映射：**把外网的某个 TCP 或者 UDP 端口映射到内网某台电脑的某个 TCP 或者 UDP 端口，主要用来发布内网服务器。若外网接入是固定 IP 地址，可以直接映射外网 IP 到内网服务器某个端口。如外网接如是固定 IP 地址 219.133.133.133, 我们想让外面访问 219.133.133.133 的 TCP9000 端口映射到内网的 192.168.0.211 的 TCP80 端口，把 192.168.0.211 的网站对外发布。设置如（图 2-43）

**新增端口映射**

外网IP地址/接口:  外网IP 219.133.133.133  
 外网接口 eth1

外网端口: 9000

内网IP地址: 192.168.0.211

内网端口: 80

协议:  TCP  UDP

映射模式:  双向映射

(图 2-43)

小贴士:

端口映射选择映射外网 IP 地址时候，前提条件必须是外网接入是固定 IP 地址，外网接入是动态 IP 由于 IP 地址不固定所以不能选择映射外网 IP 地址，只能选择外网接口。如（图 2-44）

**新增端口映射**

外网IP地址/接口:  外网IP  外网接口 eth1

外网端口: 9000

内网IP地址: 192.168.0.211

内网端口: 80

协议:  TCP  UDP

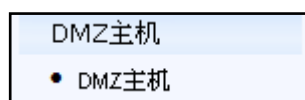
映射模式:  双向映射

(图 2-44)

- ◇ 双向映射的理解：从上图我们可以看出，访问 MAILGARD 佑友防火墙的外网接口的 9000 端口时候，MAILGARD 佑友的端口映射功能会把 9000 端口转到内网服务器的的 80 端口。这时候我们会想到这是一个单向的访问（外面其他地方访问 MAILGARD 佑友的 9000 端口），那么双向访问的意思就是从内网访问外网的 9000 的端口，如果我们勾选此选项，那就意味内网的电脑用户访问 9000 端口的时候通过 MAILGARD 佑友防火墙的双向映射功能就等于是访问 192.168.0.211 的 80 端口。
- ◇ 端口映射设置的注意事项：前面已经对端口映射的功能进行了说明，在设置的时候我们大家当然要注意如下几个问题：
- ◇ 被映射的某台服务器的某个端口一定要处于开发并允许访问状态，且有 MAILGARD 佑友处于同一局域网，能正常通信。
- ◇ 被映射的某台服务器必须是最终要以 MAILGARD 佑友防火墙为网关。

### 2.5.5 如何设置 DMZ 主机

防火墙-DMZ 主机



- ◇ DMZ 主机也是用来发布内网的服务器，与端口映射功能主要区别在于端口映射只是映射某些端口，而 DMZ 主机是映射所有端口，相当于把局域网的某台服务器直接接在外网。
- ◇ DMZ 主机设置的时候可以选择外网 IP 地址和外网接口，外网 IP 的意思把某个外网 IP 地址直接映射给局域网的某台服务器，让外网直接访问此 IP 地址就可访问局域网的该服务器。前提必须是在外网接入是固定 IP。选择外网接口的时候就是当访问 MAILGARD 佑友防火墙的外网接口时候直接全部转到内网的某台服务器。
- ◇ 在使用 DMZ 主机时候注意，当 MAILGARD 佑友服务器上除了防火墙功能模块还有邮件跟网站模块时候，假如我们使用的是 ADSL 线路接入，设置了 DMZ。如(图 2-45)



(图 2-45)

从上图我们可以看出，整个意思是当访问服务器外网接口时候。都转到内网的服务器 192.168.0.211，这时候 MAILGARD 佑友服务器上的网站跟邮箱都不可用。

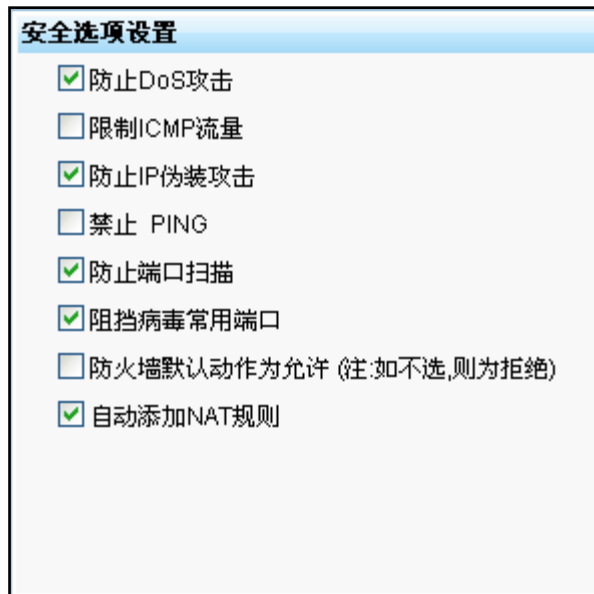
### 2.5.6 设置 MAILGARD 佑友防火墙的安全选项

防火墙-安全选项



安全选项用来设置防火墙阻止互联网的一些常见攻击手段。如（图 2-46）





(图 2-46)

**小贴士:**

安全选项一般保持默认设置即可, 设置不当将会降低防火墙安全性。在安全选项里面有一项叫自动添加 NAT 规则, 勾选为当添加上网用户的时候能自动添加 NAT 规则, 不勾选则不添加 NAT 规则。

## 2.6 VPN 管理

### 2.6.1 功能模块



### 2.6.2 VPN 概述

- ◇ VPN 的英文全称是“Virtual Private Network”，翻译过来就是“虚拟专用网络”。顾名思义，虚拟专用网络我们可以把它理解成是虚拟出来的企业内部专线。它可以通过特殊的加密的通讯协议在连接在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条专有的通讯线路，就好比是架设了一条专线一样，但是它并不需要真正的去铺设光缆之类的物理线路。这就好比去电信局申请专线，但是不用给铺设线路的费用。一句话，VPN 的核心就是在利用公共网络建立虚拟私有网。
- ◇ VPN 网关支持 ADSL 线路，支持 PPTP SSL IPSEC 协议。可实现点对网，网对网多种互通形式。

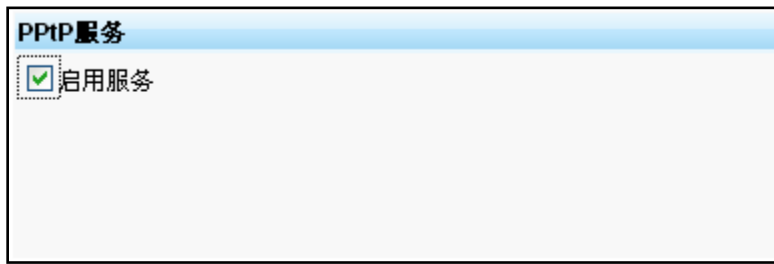
### 2.6.3 设置 PPTP VPN

VPN 管理-PPTP



- ◇ MAILGARD 佑友防火墙 pptpVPN 用来实现点对网 VPN,“PPTP 服务”选项勾选为启用 PPTPVPN 服务,

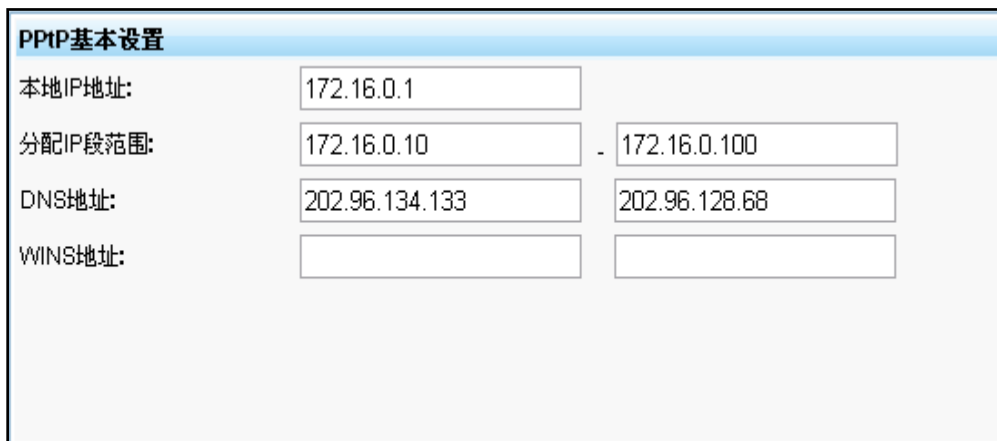
并开机自动运行该服务。不勾选则不启动该服务。



PPTP服务

启用服务

参数设置：如（图 2-47）



PPTP基本设置

本地IP地址: 172.16.0.1

分配IP段范围: 172.16.0.10 - 172.16.0.100

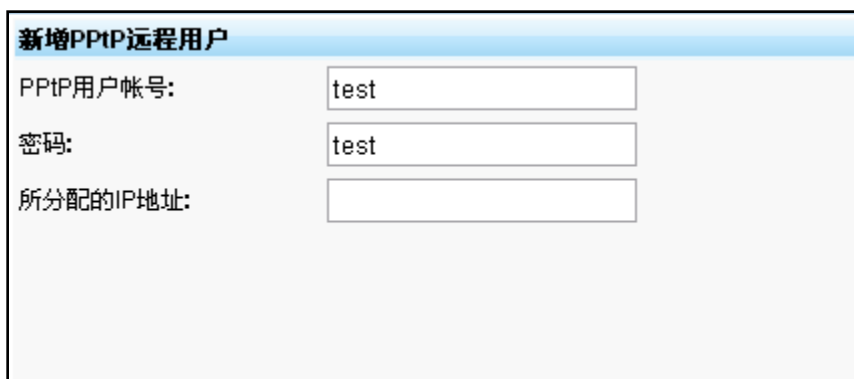
DNS地址: 202.96.134.133 202.96.128.68

WINS地址:

（图 2-47）

PPTPVPN 参数设置，本地 IP 地址以及分配 IP 段范围设置的时候，我们注意不要使用跟局域网同网段的 IP 地址，比如我们局域网是 192.168.0.0/255.255.255.0 那么我们 PPTPVPN 设置时候就不要设置成 192.168.0.0/255.255.255.0 了，我们可以另外设置一个网段，比如 172.16.0.0/255.255.255.0 网段。首先定义 PPTPVPN 本地 IP 地址为 172.16.0.1, 分配范围用来定义分配给 PPTPVPN 用户 IP 地址范围。

“远程用户”用来设置 PPTPVPN 远程用户和密码已经所指定分配的 IP 地址。如（图 2-48）



新增PPTP远程用户

PPTP用户帐号: test

密码: test

所分配的IP地址:

（图 2-48）

## 2.6.4 设置 IPSECVPN

### VPN 管理-IpSec

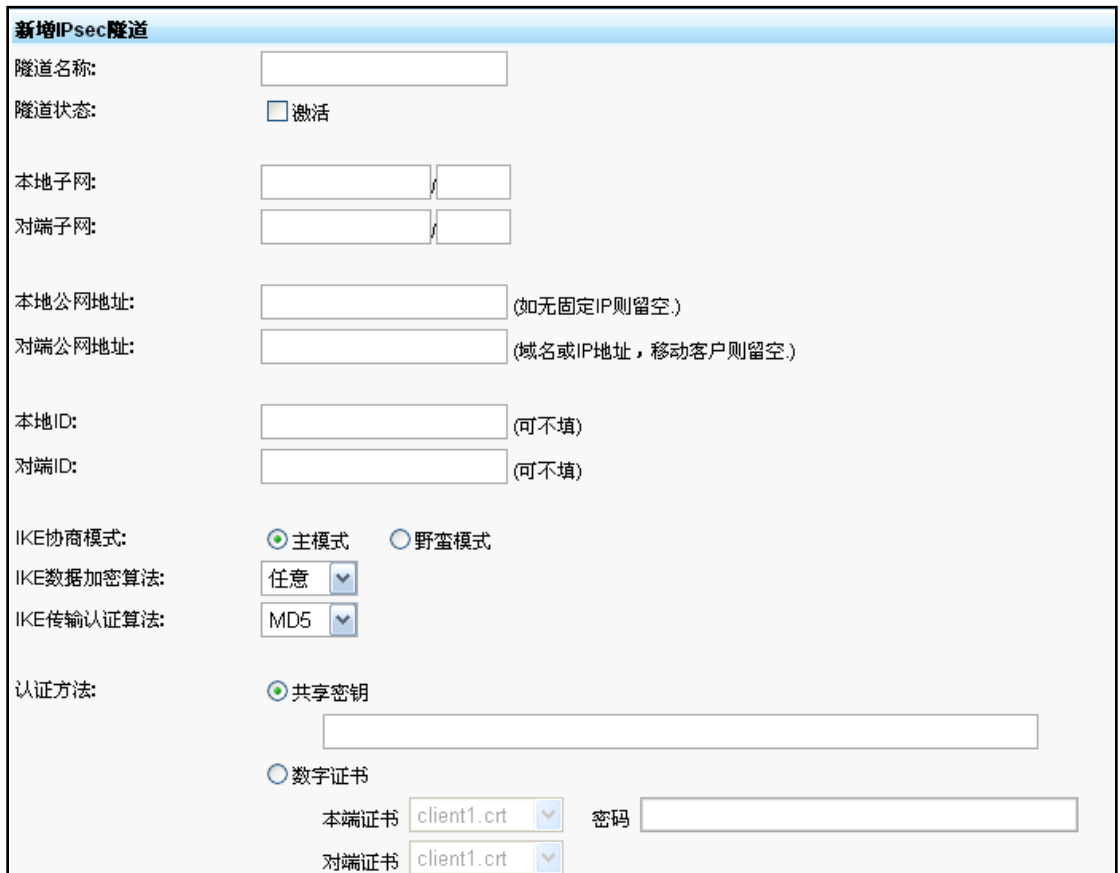
基于 IPsec 协议 VPN 为网对网 VPN，适合两地办公局域网互联成一个大的虚拟局域网，此功能需要两台标准 IPSEC 协议的 VPN 设备才能启用。



- ✧ “IpSec 服务” 设置启动 IpSec 服务，勾选为启用并开机运行，不勾选为则不启用。



- ✧ “IpSec 隧道” 点击新增即可对基于 IPsec 协议的 VPN 进行详细配置。填入隧道名称，激活隧道，本地公网地址（若无固定 IP 请留空），对端公网地址，本地子网，对端子网，再选择 IKE 协商模式，数据加密算法，传输认证算法，认证方法，IPsec 服务模式，链路模式等。确定后回到原界面，在对端 VPN 设备也配置好相应的参数后，勾选“启用服务”再确定即可成功启用 IPsec 协议的 VPN 功能。如（图 2-49）

A screenshot of the "新增IPsec隧道" (New IPsec Tunnel) configuration form. It contains the following fields and options:

- 隧道名称: [Text input]
- 隧道状态:  激活
- 本地子网: [Text input] / [Text input]
- 对端子网: [Text input] / [Text input]
- 本地公网地址: [Text input] (如无固定IP则留空)
- 对端公网地址: [Text input] (域名或IP地址，移动客户则留空)
- 本地ID: [Text input] (可不填)
- 对端ID: [Text input] (可不填)
- IKE协商模式:  主模式  野蛮模式
- IKE数据加密算法: [Dropdown menu] 任意
- IKE传输认证算法: [Dropdown menu] MD5
- 认证方法:  共享密钥 [Text input]  
 数字证书  
    本端证书: [Dropdown menu] client1.crt 密码: [Text input]  
    对端证书: [Dropdown menu] client1.crt

(图 2-49)

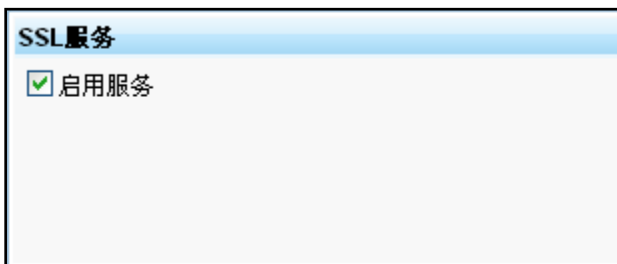
## 2.6.5 设置 SSLVPN 服务

### VPN 管理-SSL

基于 SSL 协议 VPN 为网对网 VPN。此功能适合两地办公局域网互联成一个大的虚拟域网，需要两台 VPN 设备互连。



- ◇ “SSL 服务” 设置启动 IPSec 服务，勾选为启用并开机运行，不勾选为则不启用。



- ◇ “客户端模式” 作为 SSLVPN 的客户端，请在客户端模式配置新增服务端的公网 IP 或域名用于与 VPN 服务端互联，然后再填写服务端设备所在的局域网 IP 与掩码，数字证书，数据加密算法及是否进行数据压缩。如（图 2-50）



The image shows a form titled "新增SSL服务端地址" with the following fields and options:

- 服务器端公网IP地址**: Input field for IP address, port dropdown set to 1194, and a "新增" button.
- 其它路由网段**: Input field for subnet/mask, and a "新增" button.
- 随机选择服务器**:  随机选择服务器
- 服务器内网IP地址/掩码**: Input field for internal IP/mask.
- 数字证书**: Dropdown menu set to client1.crt
- 数据加密算法**: Dropdown menu set to BF-CBC
- 压缩**:  启用压缩

(图 2-50)

- ◇ “服务端模式” 作为 SSLVPN 的服务端，请在服务端模式新增客户端的内网 IP 地址和掩码，数字证书，数据加密，以及加密算法保持与客户端一致。如（图 2-51）

**服务端模式参数设置**

客户端内网IP地址	子网掩码	数字证书
新增SSL客户端:	<input type="text"/>	数字证书 client1.crt <input type="button" value="新增"/>
VPN虚拟网段:	<input type="text"/>	
VPN端口:	1194	
数据加密算法:	BF-CBC	
压缩:	<input type="checkbox"/> 启用压缩	

(图 2-51)

“连接的客户端状态”显示 VPN 客户端连接状态。

## 2.6.6 数字证书

### VPN 管理-数字证书



“数字证书”如 (图 2-52)

证书名称	上传日期	
client1.crt	2007/01/22 11:36	
client1.key	2007/01/22 11:36	
client10.crt	2008/02/27 16:35	
client10.key	2008/02/27 16:35	
client2.crt	2007/01/22 11:36	
client2.key	2007/01/22 11:36	
client3.crt	2007/01/22 11:36	
client3.key	2007/01/22 11:36	
client4.crt	2007/01/22 11:36	
client4.key	2007/01/22 11:36	
client5.crt	2007/01/22 11:36	
client5.key	2007/01/22 11:36	
client6.crt	2008/02/27 16:35	
client6.key	2008/02/27 16:35	
client7.crt	2008/02/27 16:35	
client7.key	2008/02/27 16:35	
client8.crt	2008/02/27 16:35	

(图 2-52)

## 2.7 流量控制

### 2.7.1 功能模块



## 2.7.2 如何查看连接状态

### 流量控制-连接状态



**连接状态：**查看 MAILGARD 佑友防火墙的连接状态，通过连接状态可以看出局域网上网用户与外网的连接状态，对解决内部局域网故障有辅助作用，连接状态记录是实时刷新，不可保留记录。如(图 2-53)

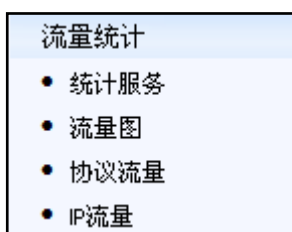
源IP:源端口	目的IP:目的端口	协议	状态	时间
127.0.0.1:18249	127.0.0.1:58053	tcp	ESTABLISHED	0:29:59
127.0.0.1:27199	127.0.0.1:28274	tcp	TIME_WAIT	0:00:23
127.0.0.1:11103	127.0.0.1:11200	tcp	TIME_WAIT	0:00:54
127.0.0.1:53183	127.0.0.1:10785	tcp	TIME_WAIT	0:01:24
127.0.0.1:35050	127.0.0.1:18070	tcp	TIME_WAIT	0:01:55
127.0.0.1:49465	127.0.0.1:49018	tcp	TIME_WAIT	0:01:59
192.168.0.46:1269	192.168.0.213:8088	tcp	TIME_WAIT	0:00:54
192.168.0.46:1344	192.168.0.213:8088	tcp	CLOSE	0:00:05
192.168.0.46:1303	192.168.0.213:8088	tcp	TIME_WAIT	0:01:24
192.168.0.46:1346	192.168.0.213:8088	tcp	CLOSE	0:00:05
192.168.0.46:1336	192.168.0.213:8088	tcp	CLOSE	0:00:05
192.168.0.46:1348	192.168.0.213:8088	tcp	CLOSE	0:00:05
192.168.0.46:1338	192.168.0.213:8088	tcp	CLOSE	0:00:05
192.168.0.46:1339	192.168.0.213:8088	tcp	CLOSE	0:00:05
192.168.0.46:1360	192.168.0.213:8088	tcp	CLOSE	0:00:09
192.168.0.46:1353	192.168.0.213:8088	tcp	CLOSE	0:00:05
192.168.0.46:1349	192.168.0.213:8088	tcp	CLOSE	0:00:05

源IP  源端口  目的IP  目的端口

(图 2-53)

## 2.7.3 如何查看流量统计

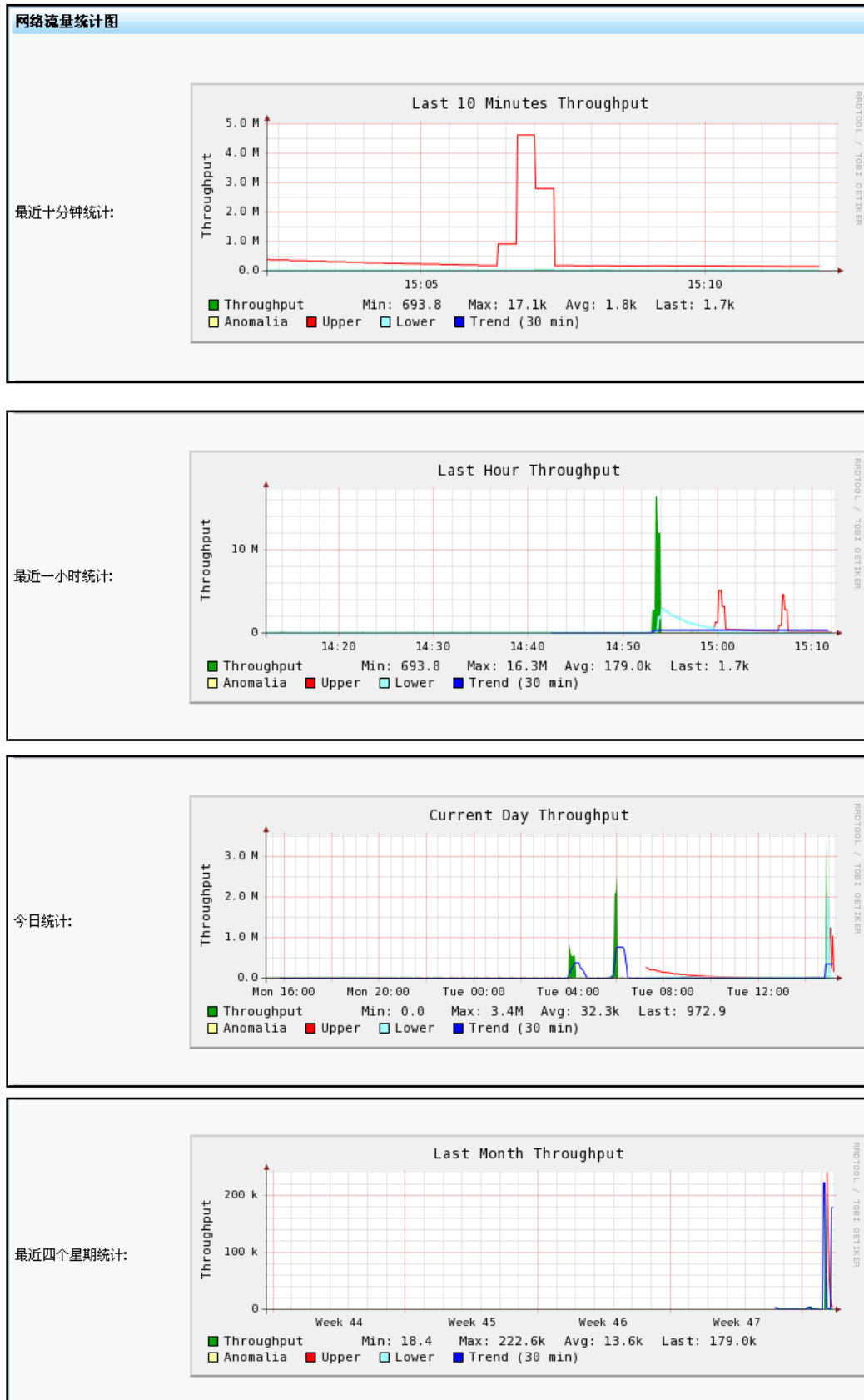
### 流量控制-流量统计



**统计服务：**勾选为启用流量统计服务，并开机自动启动流量统计服务，当状态显示为绿色的时候，表示流量统计服务处于运行的状态。



**流量图：**最近十分钟，一个小时，今日和最近四个星期的流量。如(图 2-54)



(图 2-54)

**协议流量:** 按照每台机器的 IP, 记录了各种协议的流量和总计流量。如 (图 2-55)

协议流量																		
标识	总计	TCP	UDP	ICMP	ICMPv6	DLC	IPX	Decnet	ARP	AppleTalk	NetBios	OSI	IPv6	STP	IPsec	OSPF	IGMP	Others
192.168.0.12	980.2M	65.8M	913.8M	598.8K	0	0	0	0	54.1K	0	0	0	0	0	0	0	120	0
192.168.0.60	99.1M	98.5M	593.0K	140	0	0	0	0	53.9K	0	0	0	0	0	0	0	0	0
192.168.0.230	69.8M	66.5M	2.8M	12.7K	0	0	0	0	452.3K	0	0	0	0	0	0	0	600	0

(图 2-55)

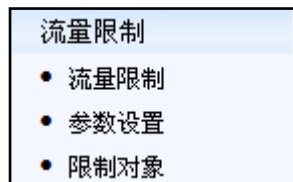
**IP 流量：**按照每台机器的 IP，记录了各种应用层数据流量和总计流量。如（图 2-56）

IP流量																		
标识	总计	FTP	HTTP	DNS	Telnet	NBios	Mail	DHCP	SNMP	NNTP	NFS/AFS	VoIP	SSH	Dc++	eDonkey	BT	Msg	Others
192.168.0.12	980.5M	20.7K	53.5M	150.2K	0	101.1K	702	0	0	0	556	1.9K	4.1M	0	156.0K	71	1.7K	
192.168.0.60	101.1M	0	76.8M	183.5K	0	16.8K	177.3K	0	0	0	514	0	0	0	0	16.8K	0	
192.168.0.230	69.4M	744	55.1M	133.1K	0	123.1K	127.4K	0	0	0	0	1.4K	8.6M	0	0	0	0	
192.168.0.242	38.1M	0	32.3M	96.2K	0	10.4K	0	0	0	0	10.9K	172	0	0	0	1.0K	0	
192.168.0.254	25.4M	167.7K	5.6K	0	0	0	3.4K	0	0	0	21.9K	4.6K	84.5K	0	0	8.0K	17.2K	
192.168.0.15	20.9M	0	4.9K	0	0	8.8K	3.4K	0	0	0	20.7K	3.4K	0	0	0	8.0K	17.2K	
192.168.0.46	19.1M	0	8.3M	6.2K	0	8.1K	376.3K	0	0	0	1.2K	1.2K	407.5K	0	0	0	0	

(图 2-56)

## 2.7.4 如何对流量进行限制

流量控制-流量限制



- ✧ **流量限制：**设置流量限制启动，停止或者重启，勾选启用服务表示设备启动即运行流量限制服务，不勾选则不运行。



- ✧ **参数设置：**在设置流量限制之前，必须先要准确的设置好线路带宽参数，如图，设置内网接口参数，因为内网接口连接的是局域网，带宽参数不做设置，为最大带宽；外网接口参数设置正确的外网接入的上行和下载的带宽参数，此设置请务必正确设置。设置错误将会影响流量限制功能的精确度。如（图 2-57）





(图 2-57)

- ◇ **限制对象:** 针对源端口, 源 IP 地址, 源网段; 目的端口, 目的 IP 地址, 目的网段以及方向和接口设置正常时的流量及空闲时流量。在设置流量限制对象的时候我们要注意单位换算, bit 与 Byte, 正常我们用下载工具下载所说的是 Byte。如 (图 2-58)



(图 2-58)

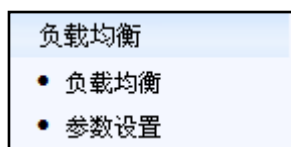
小贴士:

单位换算

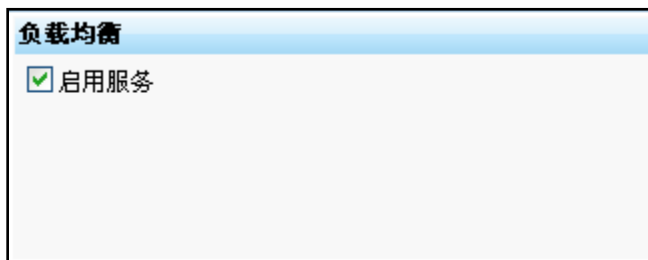
- 1 G = 1024 M
- 1 M(兆) = 1024 K (千字节)
- 1 K = 1024 Byte (字节)
- 1 B = 8 bits (位)

### 2.7.5 如何设置负载均衡

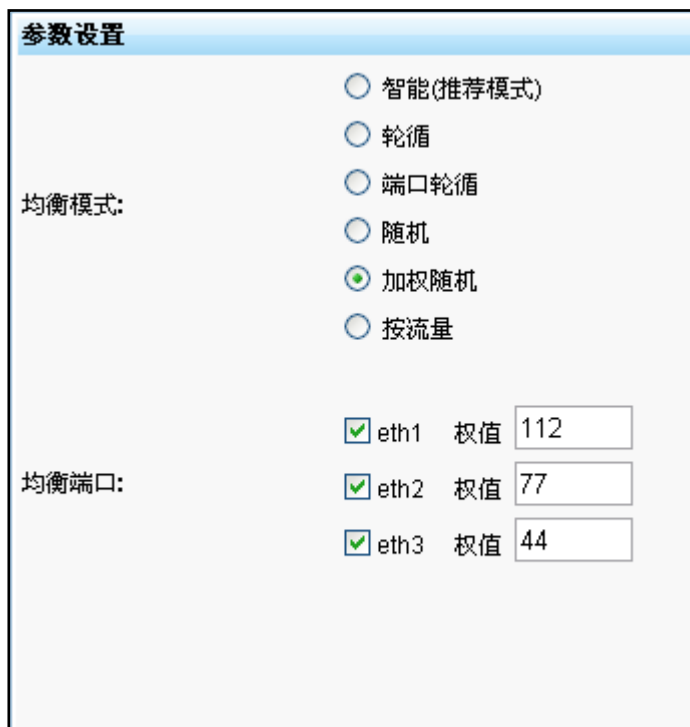
#### 流量控制-负载均衡



- ◇ **负载均衡:** 设置启用负载均衡, 勾选时表示启动时自动运行改服务, 不勾选时则为不启动。



✧ **参数设置:** 设置负载均衡端口和模式, 模式设置的时候一般默认为智能模式, 均衡端口选择均衡的外网接入端口。如 (图 2-59)



(图 2-59)

## 2.8 入侵检测

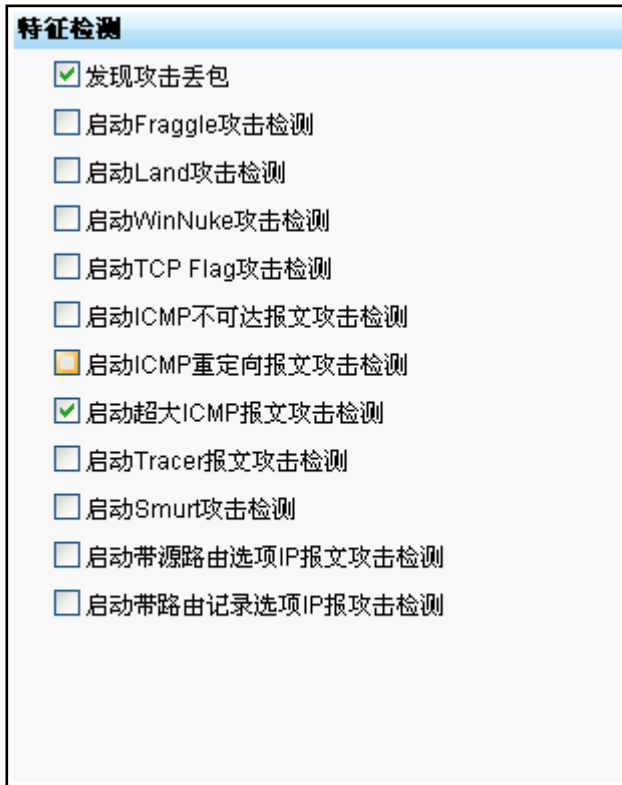
### 2.8.1 功能模块



### 2.8.2 特征检测



**特征检测:** 基于 Fraggle 攻击, TCP Flag 攻击等入侵特征检测, 勾选为启用, 不勾选则为不启用。如 (图 2-60)

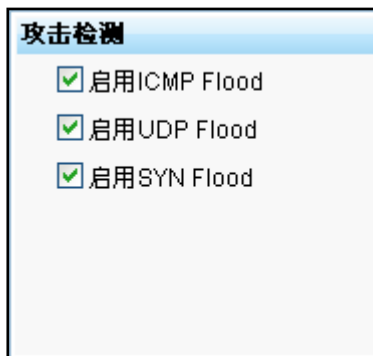


(图 2-60)

### 2.8.3 攻击检测



**攻击检测：** 设置是否启用 ICMP Flood 和 UDP Flood 以及 SYN Flood 攻击检测。勾选为启用，不勾选则为不启用。



**ICMP Flood：** 设置 ICMP Flood 攻击源 IP，攻击目的以及限制阈值。如（图 2-61）

**ICMP Flood**

攻击源IP:

攻击目的:  防火墙  
 内网

限制阈值:

(图 2-61)

**UDP Flood:** 设置 UDP Flood 攻击源 IP, 攻击目的以及限制阈值。如 (图 2-62)

**UDP Flood**

攻击源IP:

攻击目的:  防火墙  
 内网

限制阈值:

(图 2-62)

**SYN Flood:** 设置 SYN Flood 攻击源 IP, 攻击目的以及限制阈值。如 (图 2-63)

**SYN Flood**

攻击源IP:

攻击目的:  防火墙  
 内网

限制阈值:


(图 2-63)

## 2.8.4 连接控制



**连接控制：**基于源 IP 地址，源端口和目的 IP 地址，目的端口以及连接阈值对连接进行控制。

如（图 2-64）



The '编辑连接控制' (Edit Connection Control) form contains the following fields:

- 源地址: [Text input field]
- 源端口: [Text input field]
- 目的IP地址: [Text input field]
- 目的端口: [Text input field]
- 限制阈值: [Text input field]

（图 2-64）

## 2.9 如何查看日志

### 2.9.1 功能模块



### 2.9.2 日志管理

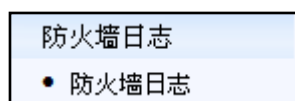


**日志管理：** 关闭或打开日志记录功能, 勾选为打开该项日志记录，不勾选则为关闭。设置完毕点击

确定即可生效。



### 2.9.3 防火墙日志



**防火墙日志：**记录 MAILGARD 佑友防火墙日志，可查看、删除、下载。如（图 2-65）

防火墙日志 (16个, 963.00byte)			
日志文件	创建日期	大小	
firewall.log	2008/11/22 04:40	1.00byte	[view] [refresh] [delete]
firewall.log.1	2008/11/01 19:45	636.00byte	[view] [refresh] [delete]
firewall.log.2	2008/10/24 16:35	1.00byte	[view] [refresh] [delete]
firewall.log.3	2008/10/23 01:10	1.00byte	[view] [refresh] [delete]
firewall.log.4	2008/10/17 08:39	95.00byte	[view] [refresh] [delete]
firewall.log.5	2008/10/14 14:09	1.00byte	[view] [refresh] [delete]
firewall.log.6	2008/09/25 11:38	160.00byte	[view] [refresh] [delete]
firewall.log.7	2008/09/11 15:40	1.00byte	[view] [refresh] [delete]
firewall.log.8	2008/08/20 09:49	1.00byte	[view] [refresh] [delete]
firewall.log.9	2008/08/20 00:02	60.00byte	[view] [refresh] [delete]
firewall.log.10	2008/08/12 07:56	1.00byte	[view] [refresh] [delete]
firewall.log.11	2008/08/05 16:15	1.00byte	[view] [refresh] [delete]
firewall.log.15	2008/07/07 07:52	1.00byte	[view] [refresh] [delete]
firewall.log.12	2002/09/07 22:34	1.00byte	[view] [refresh] [delete]
firewall.log.13	2002/09/01 17:01	1.00byte	[view] [refresh] [delete]
firewall.log.14	2002/08/19 22:17	1.00byte	[view] [refresh] [delete]

（图 2-65）

**小贴士：**

防火墙的日志记录功能请注意及时清理，不要保留过多，以免影响正常使用。

### 2.9.4 IPsec 日志

记录 IPsecVPN 日志。

### 2.9.5 SSL 日志

SSL 日志：SSLVPN 日志信息。如（图 2-66）

SSL日志 (1个, 66.00byte)			
日志文件	创建日期	大小	
sslvpn-status.log	2008/07/30 14:17	66.00byte	[view] [refresh] [delete]

（图 2-66）

## 2.9.6 PPP 日志

**PPP 日志：** PPP 拨号日志，此日志功能记录的主要是 ADSL 拨号和 PPTVPN 拨号记录。如（图 2-67）

PPP日志 (5个, 67.32K)			
日志文件	创建日期	大小	
pptpd.log	2008/11/24 11:23	35.10K	 
pptpd.log.1	2008/11/02 13:59	12.49K	 
pptpd.log.2	2008/10/26 16:30	3.90K	 
pptpd.log.3	2008/10/19 22:40	9.04K	 
pptpd.log.4	2008/10/12 09:32	6.79K	 

[全部删除](#)

(图 2-67)

## 2.9.7 ARP 日志

ARP 日志用来记录 MAILGARD 佑友防火墙接收的局域网 ARP 广播信息。如（图 2-68）

ARP日志 (5个, 2.15M)			
日志文件	创建日期	大小	
arpalert.log.1	2008/11/06 17:36	1.92M	 
arpalert.log	2008/10/26 04:02	0.00byte	 
arpalert.log.2	2008/10/22 16:47	77.84K	 
arpalert.log.3	2008/10/15 13:48	3.84K	 
arpalert.log.4	2008/10/14 12:56	160.18K	 

[全部删除](#)

ARP日志 arpalert.log	
Dec 1 08:56:36	arpalert: seq=876, mac=00:1e:c9:00:e7:36, ip=192.168.0.254, type=flood, dev=eth0, vendor="(null)"
Dec 1 08:56:41	arpalert: seq=880, mac=00:1e:c9:00:e7:36, ip=192.168.0.254, reference=00:a0:c9:b0:11:5d, type=mac_error, dev=eth0, vendor="(null)"
Dec 1 08:56:41	arpalert: seq=931, mac=00:1e:c9:00:e7:36, ip=192.168.0.254, type=flood, dev=eth0, vendor="(null)"
Dec 1 08:56:46	arpalert: seq=944, mac=00:1e:c9:00:e7:36, ip=192.168.0.254, reference=00:a0:c9:b0:11:5d, type=mac_error, dev=eth0, vendor="(null)"
Dec 1 08:56:46	arpalert: seq=986, mac=00:1e:c9:00:e7:36, ip=192.168.0.254, type=flood, dev=eth0, vendor="(null)"
Dec 1 08:56:51	arpalert: seq=1038, mac=00:1e:c9:00:e7:36, ip=192.168.0.254, reference=00:a0:c9:b0:11:5d, type=mac_error, dev=eth0, vendor="(null)"
Dec 1 08:56:51	arpalert: seq=1041, mac=00:1e:c9:00:e7:36, ip=192.168.0.254, type=flood, dev=eth0, vendor="(null)"
Dec 1 08:56:56	arpalert: seq=1084, mac=00:1e:c9:00:e7:36, ip=192.168.0.254, reference=00:a0:c9:b0:11:5d, type=mac_error, dev=eth0, vendor="(null)"
Dec 1 08:56:56	arpalert: seq=1096, mac=00:1e:c9:00:e7:36, ip=192.168.0.254, type=flood, dev=eth0, vendor="(null)"
Dec 1 08:57:01	arpalert: seq=1151, mac=00:1e:c9:00:e7:36, ip=192.168.0.254, type=flood, dev=eth0, vendor="(null)"
Dec 1 08:57:06	arpalert: seq=1152, mac=00:1e:c9:00:e7:36, ip=192.168.0.254, reference=00:a0:c9:b0:11:5d, type=mac_error, dev=eth0, vendor="(null)"
Dec 1 08:57:06	arpalert: seq=1206, mac=00:1e:c9:00:e7:36, ip=192.168.0.254, type=flood, dev=eth0, vendor="(null)"
Dec 1 08:57:11	arpalert: seq=1208, mac=00:1e:c9:00:e7:36, ip=192.168.0.254, reference=00:a0:c9:b0:11:5d, type=mac_error, dev=eth0, vendor="(null)"
Dec 1 08:57:11	arpalert: seq=1261, mac=00:1e:c9:00:e7:36, ip=192.168.0.254, type=flood, dev=eth0, vendor="(null)"

(图 2-68)

**小贴士：**

ARP 日志记录的是 MAILGARD 佑友防火墙接收到的 ARP 广播信息。可以根据日志记录帮助解决 ARP 欺骗病毒。

## 2.9.8 用户日志

可以明晰的查到各个管理员的登录操作日志。(图 2-69)

The image shows a user log interface. At the top, there is a table titled "用户日志 (1个, 2.11K)". The table has three columns: "日志文件", "创建日期", and "大小". Below the table, there is a detailed view of the "infomin.log" file, showing a list of log entries with timestamps and user actions.

日志文件	创建日期	大小
infomin.log	2010/04/30 11:45	2.11K

```
用户日志 infomin.log
2010/04/30 09:03:55 : INFO : 管理员admin : 管理员 : 已增加 "admin1"
2010/04/30 09:18:21 : INFO : 管理员admin : 登录 : 登录IP地址 192.168.0.15
2010/04/30 09:19:47 : INFO : 管理员admin : 登录 : 登录IP地址 192.168.0.46
2010/04/30 09:21:52 : INFO : 管理员admin : 登录 : 登录IP地址 192.168.0.230
2010/04/30 09:22:11 : INFO : 管理员admin : 登录 : 登录IP地址 192.168.0.230
2010/04/30 09:25:03 : INFO : 管理员admin : 登录 : 登录IP地址 192.168.0.230
2010/04/30 09:25:36 : INFO : 管理员admin : 登录 : 登录IP地址 192.168.0.230
2010/04/30 09:26:01 : INFO : 管理员admin : 登录 : 登录IP地址 192.168.0.230
2010/04/30 09:26:57 : INFO : 管理员admin : 登录 : 登录IP地址 192.168.0.230
2010/04/30 09:27:09 : INFO : 管理员admin : 登录 : 登录IP地址 192.168.0.230
2010/04/30 09:32:20 : INFO : 管理员admin : 登录 : 登录IP地址 192.168.0.230
2010/04/30 09:43:41 : INFO : 管理员admin : 登录 : 登录IP地址 192.168.0.230
2010/04/30 10:30:29 : INFO : 管理员admin : 登录 : 登录IP地址 192.168.0.230
2010/04/30 10:30:36 : INFO : 管理员admin : 管理员 : 已删除 "admin1"
2010/04/30 10:52:53 : INFO : 管理员admin : 管理员 : 已增加 "hicomtest"
2010/04/30 10:53:30 : INFO : 管理员hicomtest : 登录 : 登录IP地址 192.168.0.230
2010/04/30 10:54:34 : INFO : 管理员admin : 登录 : 登录IP地址 192.168.0.230
2010/04/30 10:55:01 : INFO : 管理员admin : 可信主机 : 请先增加本机IP地址到可信主机, 本机IP是
192.168.0.230
2010/04/30 10:56:03 : INFO : 管理员admin : 可信主机 : 已增加 "hicomtest 192.168.0.230"
2010/04/30 11:45:11 : INFO : 管理员admin : 登录 : 登录IP地址 192.168.0.230
```

(图 2-69)