# 宝龙汉景网络卫士
# 用户手册

版本号：V 6.0



Address: 厦门市嘉禾路 305 号宝龙中心一期 3F

Tel: (0592)3979999 Fax: (0592)5091388

E-mail:linyz@powerlong.com

URL:http://www.SoftIBM.com

# 目 录

# 1 综述

宝龙汉景网络卫士是为了解决政府、企业内部 Internet 管理而诞生的。该系统在不影响网络运行效率和改变现有网络配置的条件下，可以对内部人员使用 Internet 网的情况进行有效的管理和控制。它可以做到：

1， 通过对网络连接状况和异常的监视，可以知道网络系统的状况，如果系统出现异常能够马上发现问题。

2， 员工上网情况的监控和分析，在开放网络资源的同时，最大限度的保证员工的工作效率。通过宝龙汉景网络卫士形成的多种统计报表和排行榜，可以帮助政府、企业管理者了解政府、企业员工的工作情况，提高管理效率。

3， 通过对于外发邮件和上载内容的监控、拦截、审核，防止政府、企业机密信息通过互联网泄漏出去。

4， 通过对网络行为的管理和限制，保证网络行为的有效性和信息的有效性。

宝龙汉景网络卫士是政府、企业管理的好帮手。它有效平衡了政府、企业上网所带来影响，在开放网络资源的同时，最大限度地保持了员工的工作效率。宝龙汉景网络卫士使用了最先进的网络底层监控技术和多进程共享内存技术，对原有网络没有任何不良影响。本产品包括一体化专业设备，可直接安放在总经理办公室，无需安装客户端软件、无需配置、无需手动启动、无需网管和技术人员加入，使用非常简单方便，公司老总一学就会。

宝龙汉景网络卫士是政府、企业管理的好管家。它对公司的上网行为进行了规范和调整，避免公司员工面对网络分散精力和注意力，保障了为工作而上网所盼望的网路通畅，直接提升政府、企业整体效率和生产力，节约了政府、企业的管理开销，并且保障了政府、企业的机密信息不通过互联网泄漏。

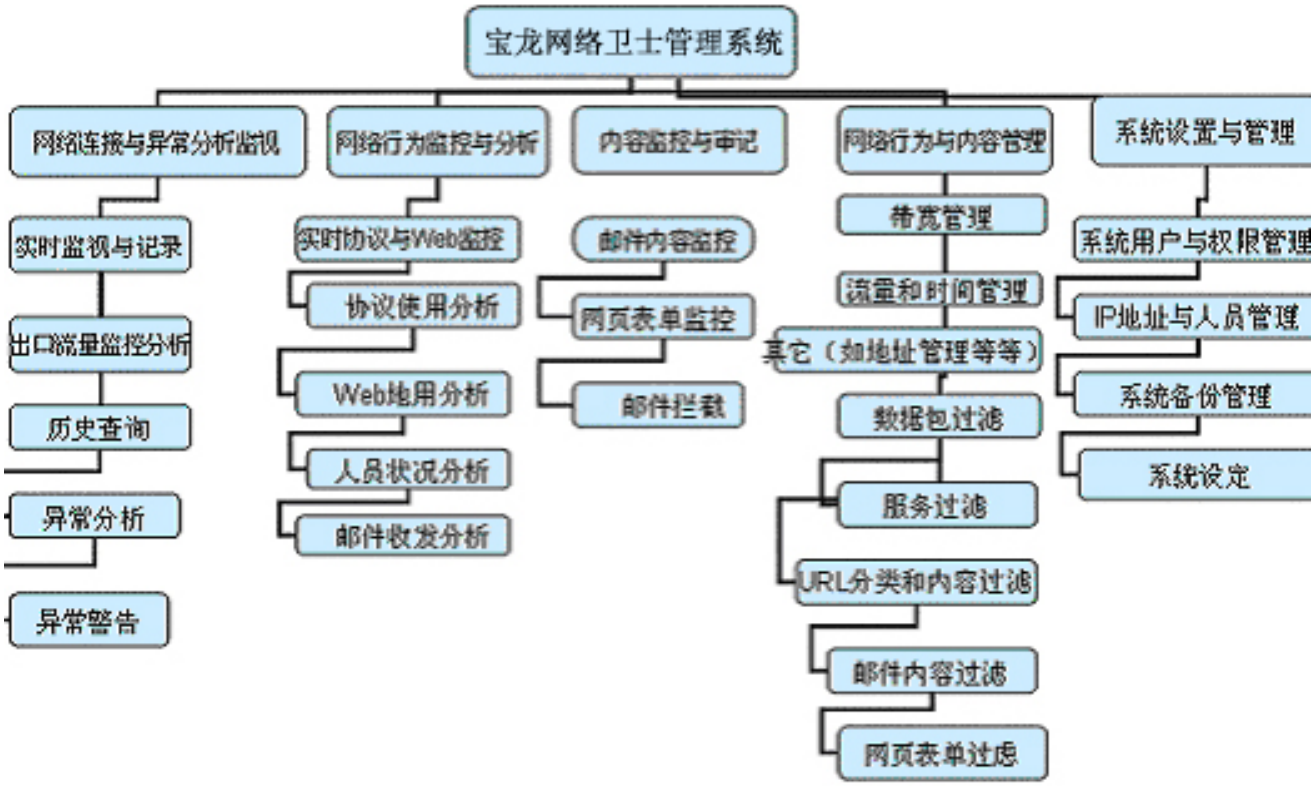
# 2 系统运行环境与结构

作为一个专用的网络行为管理产品，要求系统能够长期稳定地运行，为此，系统定制了专业设备作为宝龙汉景网络卫士的运行设备，该设备符合 Intel 服务器平台标准。在该设备上我们采用稳定的 OS 操作系统，并根据要求对系统内核和配置进行优化，使之运行更加安全、可靠。

宝龙汉景网络卫士为专业设备服务器，我们针对不同的客户类型设计了不同的网络接入方式，一般我们希望该服务器连接在 Internet 出口设备（如路由器或代理服务器）和交换机之间。由于宝龙汉景网络卫士具有代理、路由、NAT 等功能，所以也可以直接安装在 Internet 出口上，代替一般的出口网关。

# 3 功能与操作介绍

宝龙汉景网络卫士是政府、企业网络管理的好帮手。它对政府、企业的上网行为进行了规范和调整，避免公司员工面对网络分散精力和注意力，保障了为工作而上网所盼望的网路通畅，提高政府、企业整体效率，节约了政府、企业的管理开销。具体包括以下几大功能：



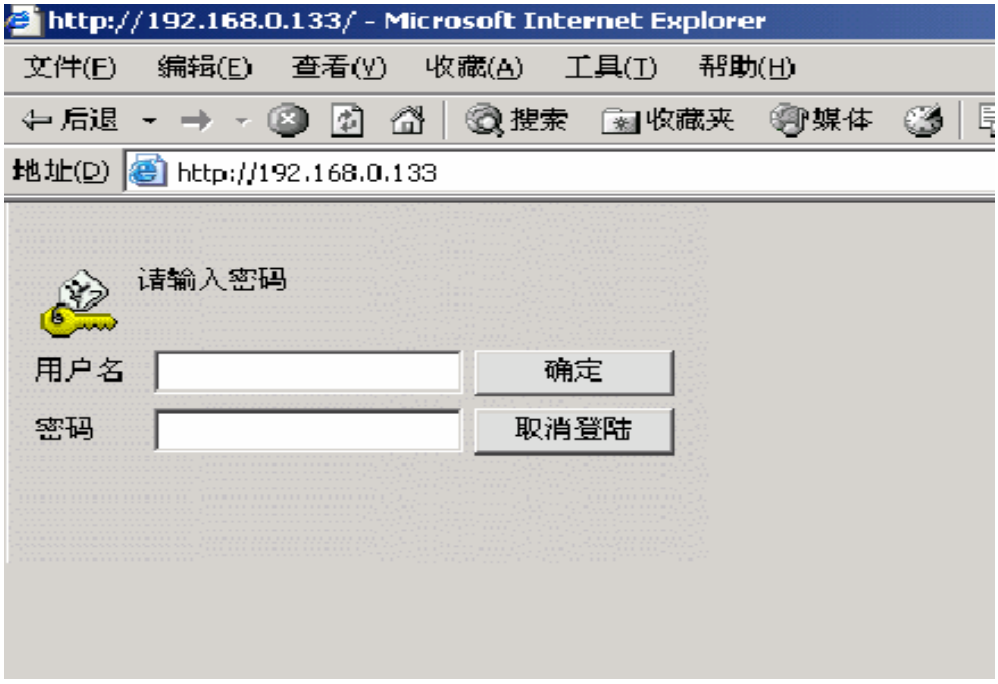

| 功能项 | | 功能描述 |
|---|---|---|
| 系统设置 | 网段设置 | 设置各个网段的管理方式以及用户与主机对应方式 |
| | 端口设置 | 设置各个端口的管理特征：免监控、监控或禁止访问 |
| | 用户管理 | 部门管理、用户设置 |
| | 邮件监控过滤 | 邮件监控的过滤规则，监控邮件会按照这些规则进行过滤分类 |
| | 网页表单过滤 | 邮件监控的过滤规则，监控邮件会按照这些规则进行过滤分类 |
| 网络 | 在线用户情况 | 系统中当前正在网络访问的主机列表和特征 |
| | 当前 IP 访问情况 | 当前正在进行的 IP 连接和信息，如流量、时间、端口等 |

| | | |
|---|---|---|
| 监视 | 当前 Web 访问情况 | 当前系统的 WEB 访问连接情况，包括主机、URL、时间、流量等 |
| | IP 访问历史记录查询 | 系统 IP 访问的历史记录及详细查询 |
| | 网站访问历史记录查询 | WEB 访问历史记录及详细查询 |
| | 邮件内容监控查看 | 系统的邮件内容监控及察看 |
| | 网页表单监控查看 | 系统网页表单监控及察看 |
| 分析报告 | 出口流量报告 | 网络出口一段时间内使用状况的图表 |
| | 协议使用报告 | 一段时间内网络各种协议访问情况，包括流量、连接时间、访问次数等 |
| | 网络流量报告 | 一段时间内网络流量情况图表 |
| | 用户使用报告 | 一段时间内各个用户网络使用情况 |
| | Web 使用报告 | 一段时间内 WEB 访问情况统计报表，包括流量、连接时间、次数 |
| | 目标连接报告 | 一段时间内 IP 访问情况报表 |
| 系统管理 | 系统用户管理 | 编辑系统管理用户与权限 |
| | 系统重起 | 重新启动系统 |
| | 系统关机 | 关闭系统 |

## 3.1 登陆系统

客户端使用微软 IE6.0 。 在管理客户端打开 IE 浏览器，输入：管理机 IP http://192.168.0.133 （该地址是作为例子，实际设置可能不同，请洽技术支持人员。）

浏览器中将会出现：




第一次登陆系统，使用默认用户名： a d m i n 和默认密码： 1 1 1

输入完毕，按确定键进行身份认证。如果通过身份认证会出现：


点击“是（Y）”进入系统。

## 3.2 系统设置

系统使用前要进行必要的设置，

1 网段设置：设置需要监控的各个网段的管理方式以及用户与主机对应方式；

2 端口设置：设置各个端口的管理特征：免监控、监控或禁止访问；

3 用户管理:部门管理、用户设置；

4 邮件监控过滤:邮件监控的过滤规则，监控邮件会按照这些规则进行过滤分类；

5 网页表单过滤:邮件监控的过滤规则，监控邮件会按照这些规则进行过滤分类；

## 3.2.1系统网段设置

对整个网络进行设置，并选择适合单位的验证方式。用户可以任意选择一种方式来进行网络设置。

可选择基于 IP 地址、基于 MAC 地址、基于身份认证以及免监控和禁止访问。

基于 IP 地址帮定适用于静态 IP 方式，每人对应一个 IP 地址；基于 MAC 地址帮定适用于动态 IP，例如 DHCH 方式,每人对应一个 MAC 硬件地址;基于本地验证方式时用户要上网必须首先到 http:// 监控机 IP:8080 进行身份验证；免监控时这段地址不需要监控；禁止访问这段 IP 地址禁止访问。

对用户网络行为监控之前，首先应对系统进行设置，以便系统可以按照监管人员的要求对局域网中用户进行监控。

### ＩＰ绑定：

用户如采用的是固定的 IP 地址，可以选择基于“IP 绑定”的方式来进行管理，只要输入公司的起始 IP 和终止 IP，然后按“添加”键。


### MAC 绑定：

用户如采用的是动态的 IP，则可以选择基于 MAC 绑定方式来进行管理，只要在界面中输入需要监管的 IP 地址段的 IP 范围，然后按“添加”键。这时候无论你的 IP 地址怎样改变都不会影响他的监控。

### 本地验证：

如果公司需要采用上网之前需要验证的方式，则可以选择本地验证，只要在界面中输入需要监管的 IP 地址段的 IP 范围，然后按添加键。这时候相应的用户，如需上网都必须在宝龙汉景网络卫士管理系统网络行为监控系统软件 V2.0 的界面中进行用户登录验证，即用户要上网必须首先到 http:// 监控机 IP:8080 进行身份验证

### 免于监控：

输入起始 IP 和终止ＩＰ，选择“免于监控“，则这段ＩＰ地址的用户将不受到监控。

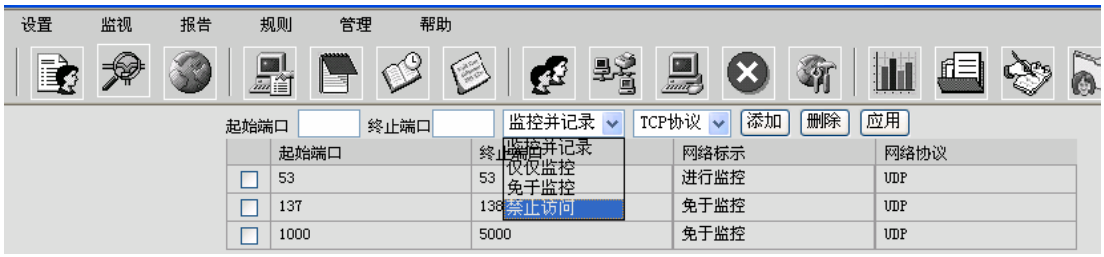
### 禁止访问：

输入起始 IP 和终止ＩＰ，选择“禁止访问“，则这段ＩＰ地址的用户不能访问外网。

**＊注意：要使网段设置立马生效，按“应用网段设置”**

## 3.2.2系统端口设置

单击**设置---》端口设置**，对各个端口的状态进行设置。每个端口有四种状态：监控并记录，仅仅监控、免于监控、禁止访问。系统默认监控并记录所有端口信息。

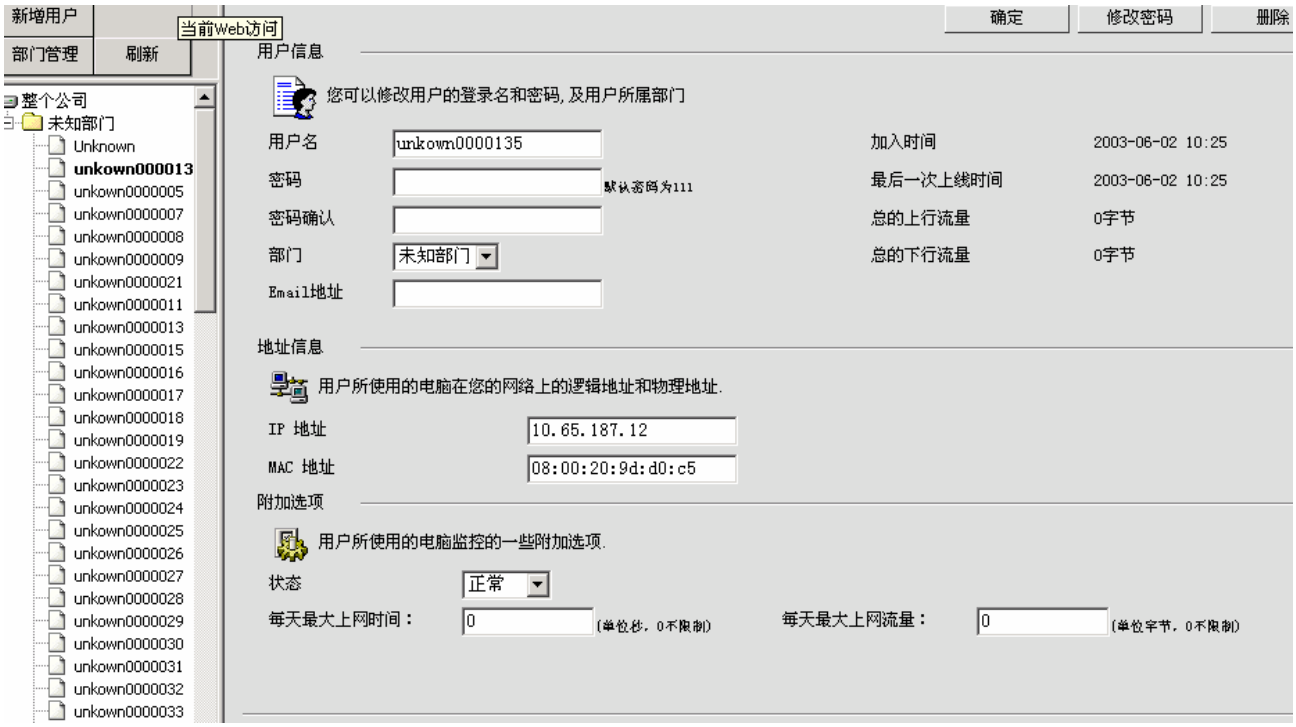



图：系统端口设置。

＊ **注意：要使端口设置立马生效，按“应用”**

## 3.2.3 系统用户管理

单击 设置---》用户管理进入系统用户管理




图：系统用户设置。

使用该功能可以对接入局域网的所有用户分部门管理。对于部门或用户的添加、修改和删除。用户密码、从属部门、Ｅｍａｉｌ地址、用户状态和上网时间制定都在这里进行操作。

**注意：**

1、 如果在“网段设置”里被定义为本地验证的用户，需要在此设定登录密码；

2、 在状态栏选择客户在系统内的状态，如选择“免监控”，则该用户将不被系统所监控；

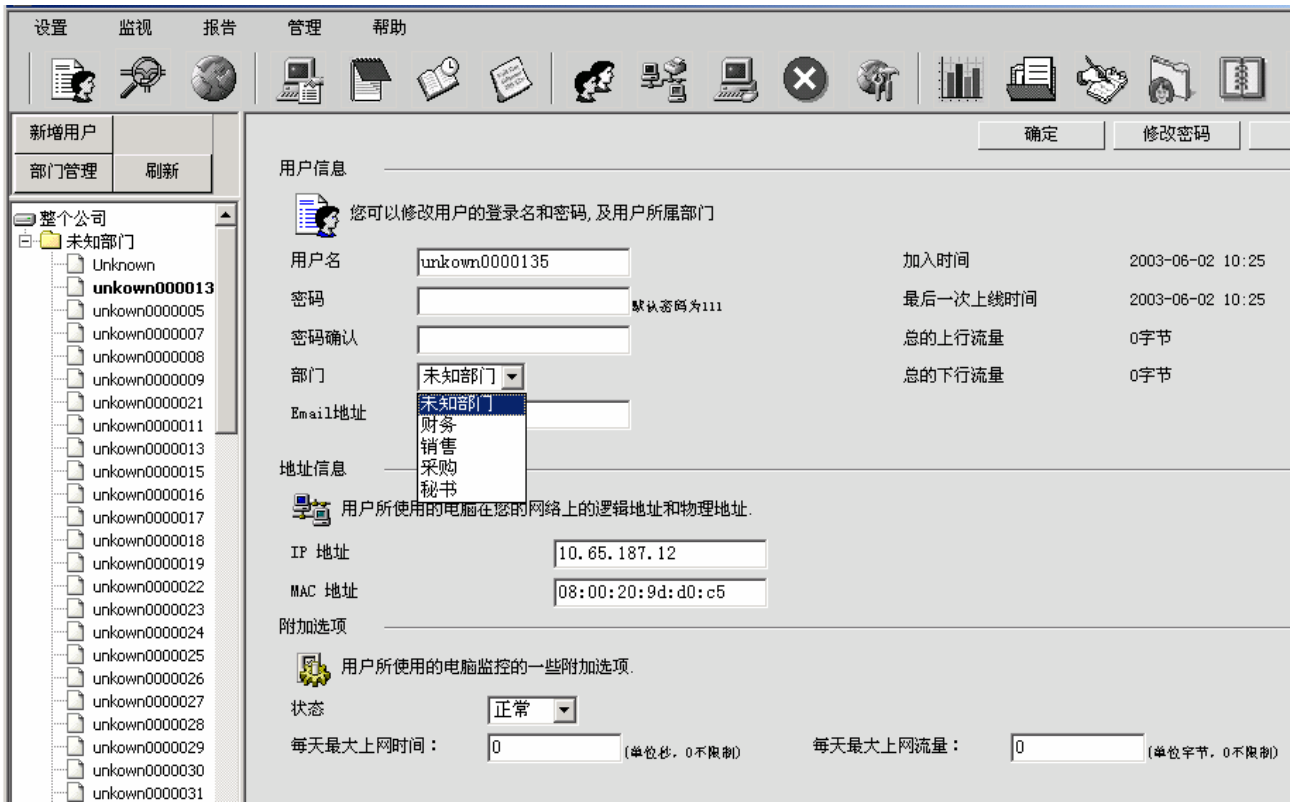
３、MAC 地址为该用户计算机中的全球唯一标示的网卡地址。系统会自动识别，也可以自行修改；

４、如果需要进行时间限制，在每天最大上网流量和最大上网时间添上相应的数据。在设定的时间段内，用户能够正常上网，当用户的上网时间总数超过了设定时间的总数时，用户将不能在上网；

**用户部门编辑**


图：用户系统部门编辑。

在用户组名称的输入框里填写部门名称，如秘书，之后点击“添加”。此部门名称将自动添加到下方的用户组名称列表中。在点击任意用户名，在部门选项里秘书也会自动出现在列表中，如下图：

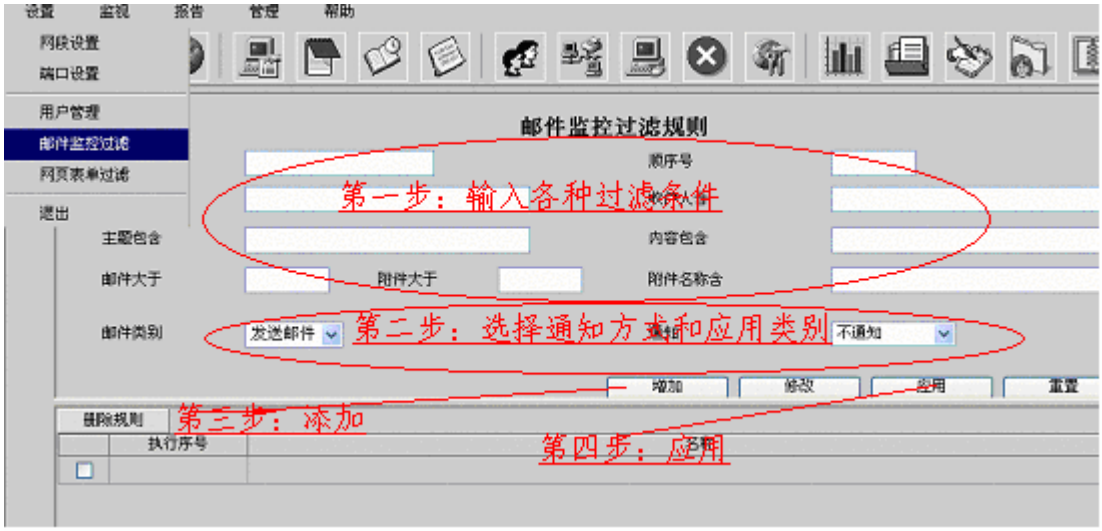



## 3.2.4 邮件过滤

对于保密性比较强的单位，可以选用邮件监控模块，该功能可以实现对局域网中收发的所有邮件进行监控的目的。同时还可以根据条件设定敏感邮件，系统将自动把敏感邮件存放到指定的区域，以便查看。系统将自动将监控结果按使用者进行分类。

单击设置—》邮件监控设置进行设置

在此可以设定按： 发件人地址、 收件人地址、邮件主题、邮件内容、邮件大小、附件名称、附件大小等条件进行设定，符合条件的邮件可以选择控制方式。




发件人含、收件人含、主题包含、内容包含和附件名称含的输入框里输入的是客户关心的关键字，例如下图：


* 规则名：分类过滤规则的名称一般包含规则的属性关键字，便于客户管理规则。
* 顺序号：即下面的执行序号。分类过滤规则的顺序号是优先级的概念，当一个邮件满足多个规则是，邮件将优先的隶属于高优先级的规则里。优先级从高到底 1 －＞N．
* 邮件大于和附件大于应填写数字，单位是字节；
* 邮件类别：定义此规则应用于发邮件还是接收邮件；
* 通知：当选择“通知“时，后面会出现一个输入框，请输入被通知人的Ｅｍａｉｌ地址，当有符合次规则的邮件被监听到时，系统会发给被通知人报警信息。
* 点击规则列表中的规则，其内容将显示在上面的各个输入框里，可以进行修改，然后点击“修改”，此规则讲更新。
* 所有输入框的关键字，是*并*的关系，即满足所有的条件才属于此规则；
* 如果希望更新或新规则立即生效，请点击“应用”键。

## 3.2.5表单过滤设置

单击设置—》网页表单监控设置进行设置，表单过滤设置操作类似邮件过滤操作。在此可以设定按：主机

名含、网址包含，附件名称含、附件大小等条件进行设定，符合条件的表单可以选择过滤方式。

* 规则名：分类过滤规则的名称一般包含规则的属性关键字，便于客户管理规则。
* 顺序号：即下面的执行序号。分类过滤规则的顺序号是优先级的概念，当一个邮件满足多个规则是，邮件将优先的隶属于高优先级的规则里。优先级从高到底１－＞Ｎ.
* 用户名含、主机名含、网址包含、内容包含和附件名称得输入框请输入关键字；
* 所有输入框的关键字，是*并*的关系，即满足所有的条件才属于此规则；
* 内容大于和附件大于，请输入数字，单位是字节
* 通知：当选择“通知“时，后面会出现一个输入框，请输入被通知人的Ｅｍａｉｌ地址，当有符合次规则的邮件被监听到时，系统会发给被通知人报警信息。
* 点击规则列表中的规则，其内容将显示在上面的各个输入框里，可以进行修改，然后点击“修改”，此规则讲更新。
* 如果希望修改规则优先级，只需修改数序号即可；


上图示表单上载监控过滤规则图

# 3.3 网络监视

通过这部分功能，管理人员可以查看局域网内任一台电脑正在上网的信息，包括其访问的 IP 地址、协议、流量和访问时间。

首先，在“当前 IP 访问”中，系统会不断更新并显示最新访问 Internet 的记录，包括用户名、部门、其电脑的 IP 地址、目前正在访问的 IP 地址、访问时间及其服务类型和进出流量以及出口流量进行监控。

其次，可以通过“当前在线用户”查看当前各用户正在进行的访问，包括用户名、其电脑的 IP 地址、目前正在访问的 IP 地址、访问时间及其服务类型和进出流量。

有时，管理者并不关心网站的进出流量，而只想看公司内部的电脑是否上了与工作无关的网站，这时，管理者还可以进行更为简单直观的监视，点击“监视”中的“当前 WEB 访问”

在这里，系统提供给管理者每位用户所浏览的详细地址，并提供链接，点击网址链接，就可以看到每个用户分别在上什么网站，浏览什么内容，从而很直观的判断该用户是在看新闻或者查阅资料等。

## 3.3.1 当前在线用户状况

管理人员点击“监视”中的“在线用户”，查看当前系统网络主机连接情况。包括其访问的 IP 地址、协议、流量和访问时间。

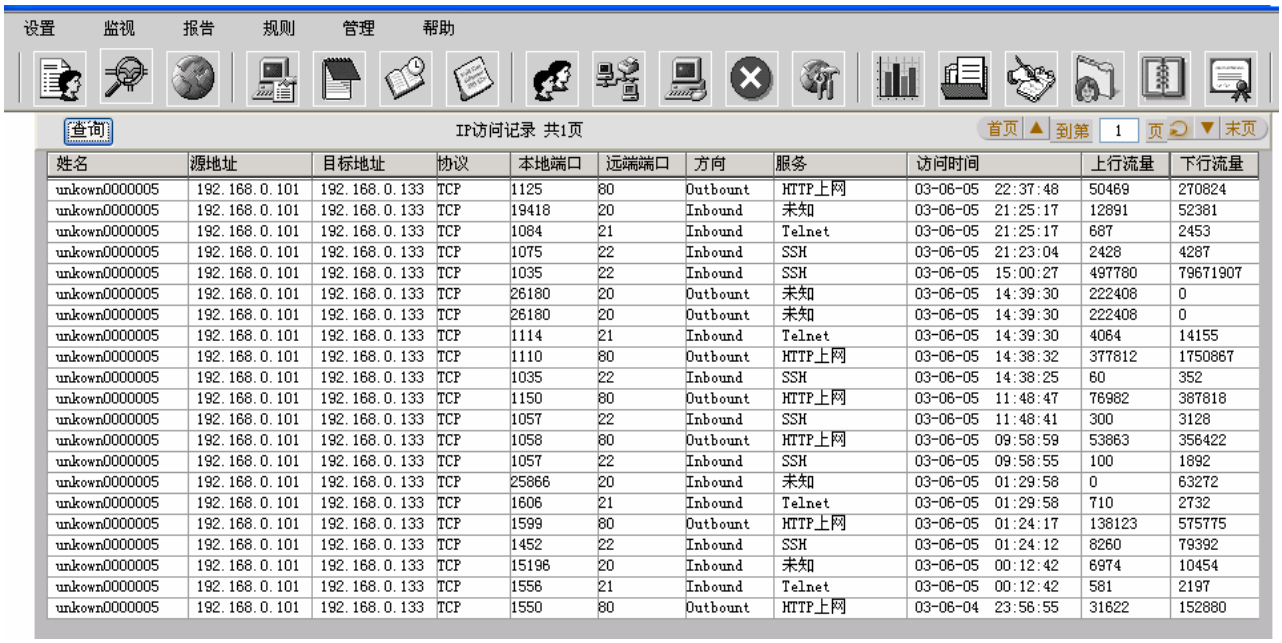

## 3.3.2 当前网络连接状况

管理人员点击“监视”中的“当前 IP 访问”，可以查看当前各用户正在进行的访问，从这里主要可以查看用户访问的 IP 地址、服务类型、进出流量及访问时间等，如图 1。

管理者可以从其中提供的“服务”类型来判断该用户正在做的操作，因此，如果有人正在使用 ICQ 等工具聊天，可以马上知道。


图 4.1：当前网络连接状况。

## 3.3.3 IP 访问历史记录与查询

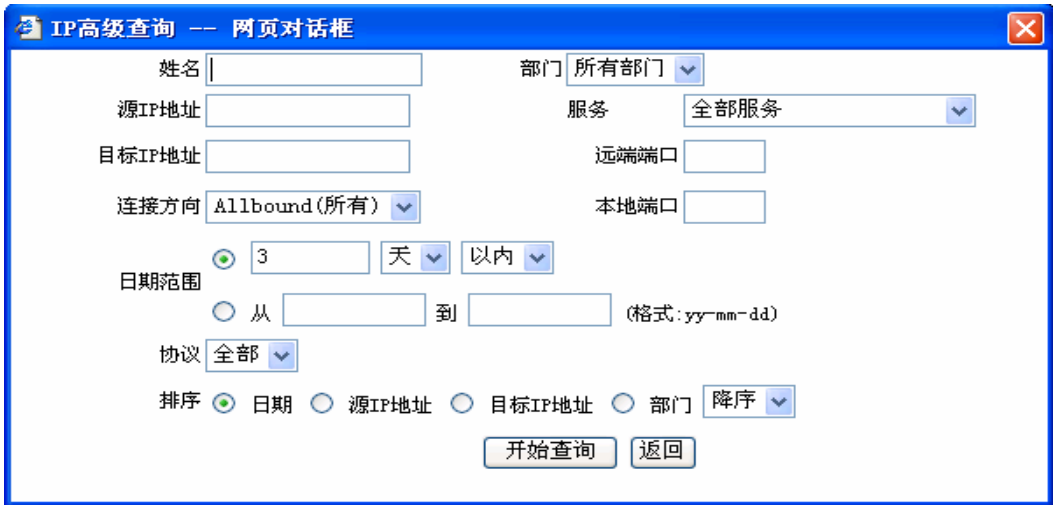



| 姓名 | 源地址 | 目标地址 | 协议 | 本地端口 | 远端端口 | 方向 | 服务 | 访问时间 | 上行流量 | 下行流量 |
|---|---|---|---|---|---|---|---|---|---|---|
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 1125 | 80 | Outbount | HTTP上网 | 03-06-05 22:37:48 | 50469 | 270824 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 19418 | 20 | Inbound | 未知 | 03-06-05 21:25:17 | 12891 | 52381 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 1084 | 21 | Inbound | Telnet | 03-06-05 21:25:17 | 687 | 2453 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 1075 | 22 | Inbound | SSH | 03-06-05 21:23:04 | 2428 | 4287 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 1035 | 22 | Inbound | SSH | 03-06-05 15:00:27 | 497780 | 79671907 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 26180 | 20 | Outbount | 未知 | 03-06-05 14:39:30 | 222408 | 0 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 26180 | 20 | Outbount | 未知 | 03-06-05 14:39:30 | 222408 | 0 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 1114 | 21 | Inbound | Telnet | 03-06-05 14:39:30 | 4064 | 14155 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 1110 | 80 | Outbount | HTTP上网 | 03-06-05 14:38:32 | 377812 | 1750867 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 1035 | 22 | Inbound | SSH | 03-06-05 14:38:25 | 60 | 352 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 1150 | 80 | Outbount | HTTP上网 | 03-06-05 11:48:47 | 76982 | 387818 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 1057 | 22 | Inbound | SSH | 03-06-05 11:48:41 | 300 | 3128 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 1058 | 80 | Outbount | HTTP上网 | 03-06-05 09:58:59 | 53863 | 356422 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 1057 | 22 | Inbound | SSH | 03-06-05 09:58:55 | 100 | 1892 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 25866 | 20 | Inbound | 未知 | 03-06-05 01:29:58 | 0 | 63272 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 1606 | 21 | Inbound | Telnet | 03-06-05 01:29:58 | 710 | 2732 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 1599 | 80 | Outbount | HTTP上网 | 03-06-05 01:24:17 | 138123 | 575775 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 1452 | 22 | Inbound | SSH | 03-06-05 01:24:12 | 8260 | 79392 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 15196 | 20 | Inbound | 未知 | 03-06-05 00:12:42 | 6974 | 10454 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 1556 | 21 | Inbound | Telnet | 03-06-05 00:12:42 | 581 | 2197 |
| unkown0000005 | 192.168.0.101 | 192.168.0.133 | TCP | 1550 | 80 | Outbount | HTTP上网 | 03-06-04 23:56:55 | 31622 | 152880 |

图：系统详细的 IP 访问。

管理员在点击查询按扭后，可以在查询框内输入自己想要查询的内容的名称进行强大的组合查询，查询的内容包括姓名、部门、源目标 IP 地址、日期（以内、以前或指定日期）、协议等。并可对各类的查询结果进行排序。

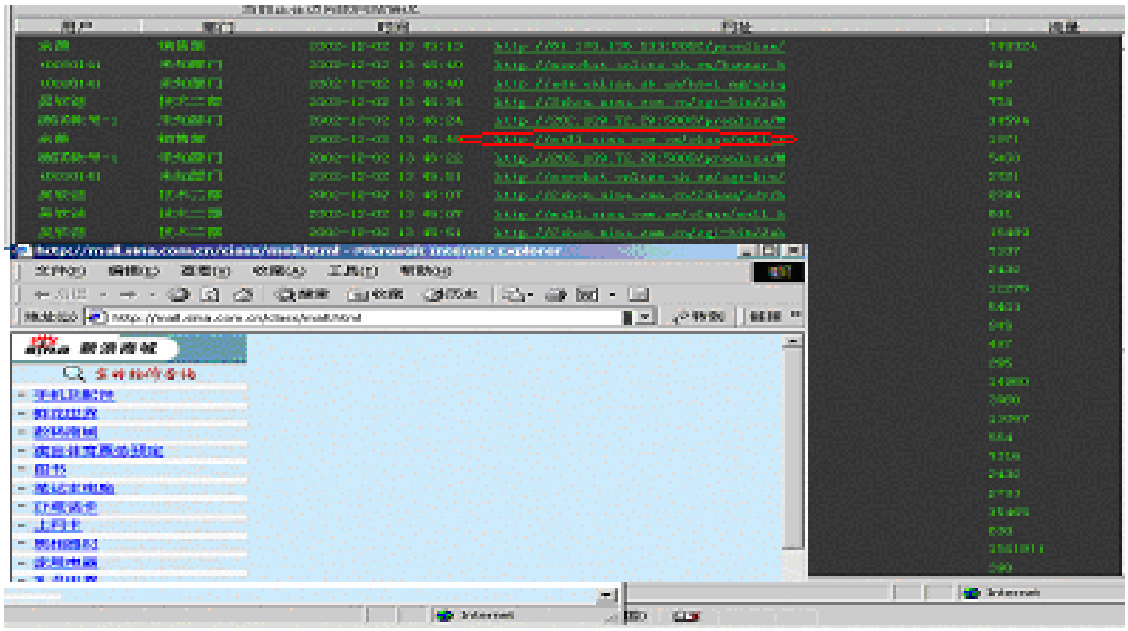
通过对 IP 访问的分析，可以了解网络系统的状况和发现异常。通过对网络出口流量的流量的分析，了解网络的负载和使用情况。管理员可以通过各种图形查看目前整个公司的一个网络流量趋势图。非常的直观，其包括上行、下行、总计。管理员可以通过当前的的出口流量的走势，分析出公司在什么时间段内会出现网络拥挤、堵塞，从而能够进一步的对网络进行调整。管理员随时可以在该处对以前各个时间段的所有的网络流量的趋势图进行查阅、分析。




图：网络访问记录高级自定义查询。

## 3.3.4上网实时监控与历史记录

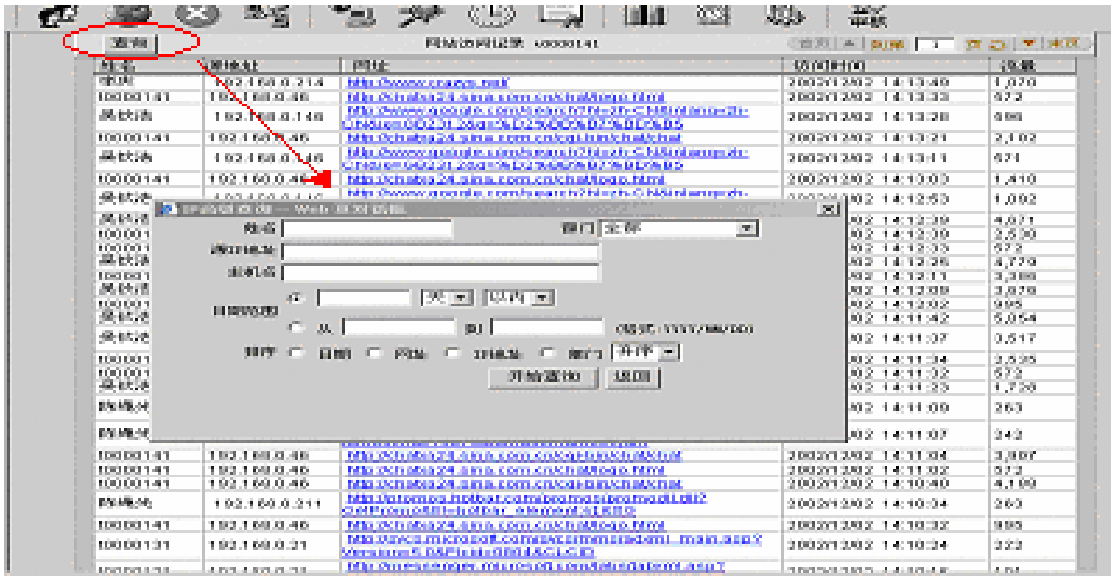
单击监视---》当前 WEB 访问可以看到系统中正在进行的 WEB 访问情况，包括流量、时间、访问的 URL 等信息。如果监控系统可以访问外网，当点击某个ＵＲＬ时，会弹出次网址得页面，如下图：



图：当前上网记录。

## 3.3.5上网历史记录和查询

管理者除了可以查询不同用户的访问情况，还可以查询每个用户在某一时间所浏览过的地址，并且该地址提供了链接，点击该链接就可以直接看到该地址所提供的网页内容。点击“监视”中的“网站访问查询”按钮，就可以进入查询窗口.



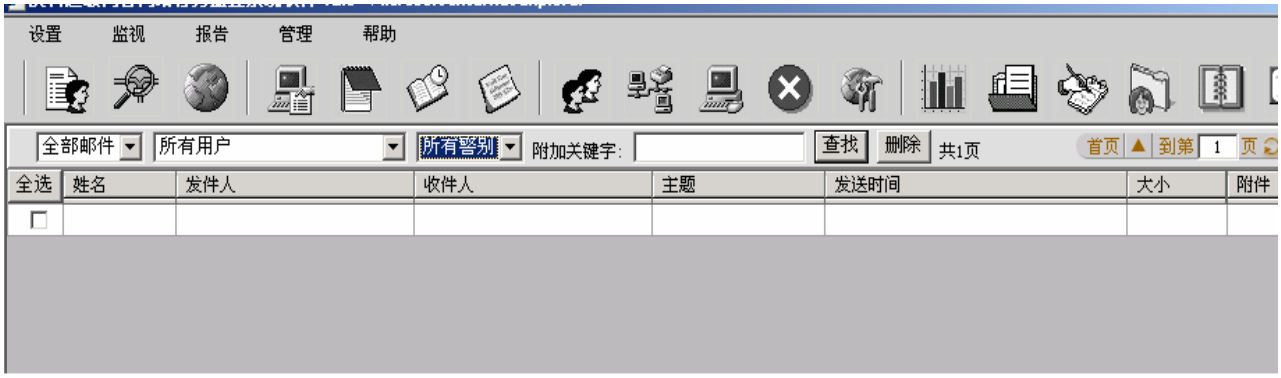
图：用户上网记录与超级查询

可以在查询框内输入自己想要查询的内容的名称进行强大的组合查询，查询的内容包括姓名、部门、源目标 IP 地址、主机名、日期（以内、以前或指定日期）、时间段（天、周、月）、协议等。并可对各类的查

询结果进行排序。输入完毕，请按开始查询进行查询操作。

## 3.3.6邮件内容监控

管理员可以通过选择“监视”中的“邮件内容查看”来对公司所有人员的接收的邮件的内容进行查看，包括发送的时间。管理员查看邮件时 3 个选项，默认为：全部邮件、所有用户和所有警别。也可以通过输入关键字进行邮件的查找，附加关键字和前 3 项是“并”的关系。第一项包含：全部邮件、发送邮件、接收邮件。第二项包含：所有用户和用户列表。第三项包含：所有警别和警别列表，警别列表与设置里的邮件控制过滤的规则对应。




双击邮件列表中的邮件，就可以看到邮件的具体内容，如要删除任意邮件，只要在复选框内选中该邮件，然后按删除键就可以完成。

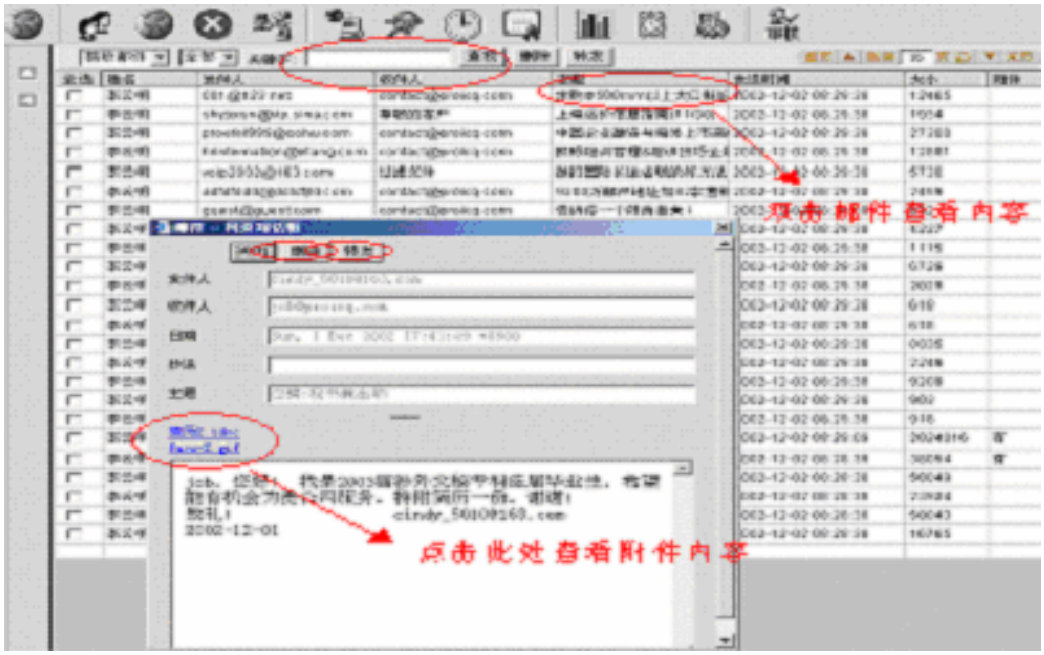


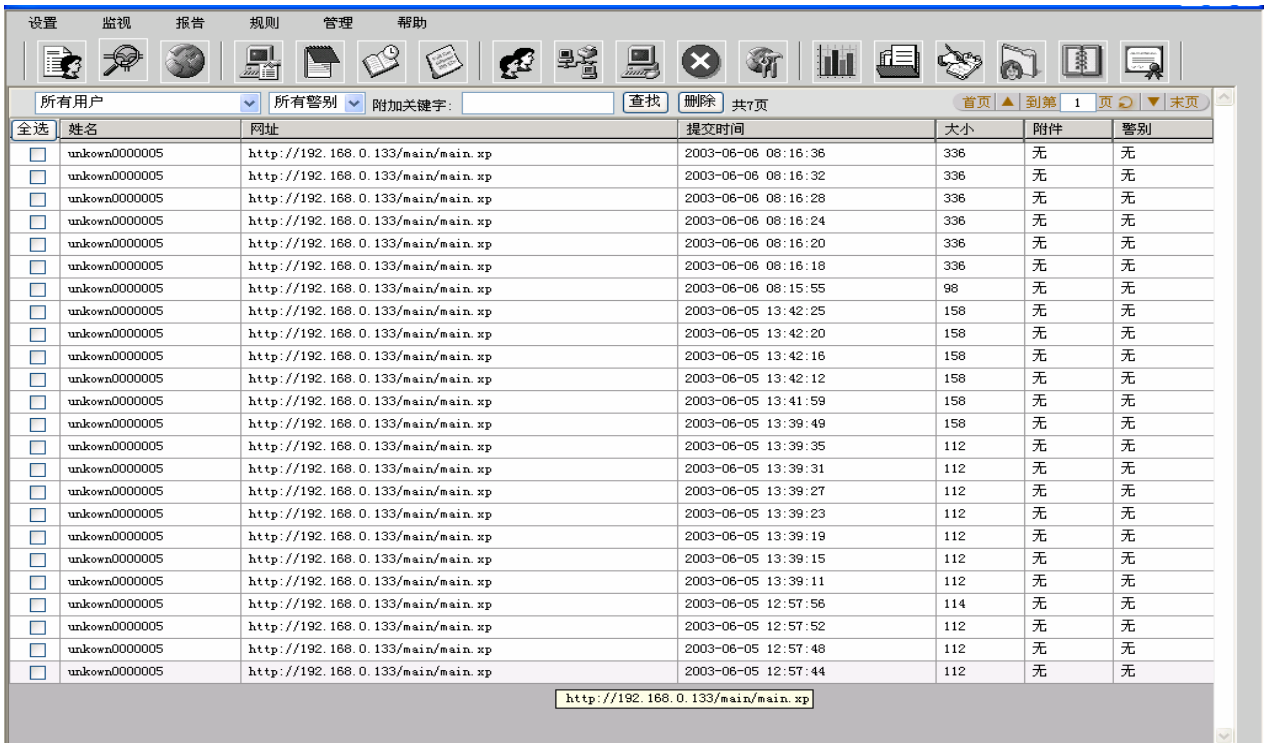

图 邮件内容监控

## 3.3.7网页表单查看:

管理员可以通过选择“监视”中的“网页表单查看”来对公司所有人员的通过 WEB MAIL 所收发的邮件、上载下传的内容、BBS 内的内容等进行查看。

双击网页表单列表内的单条信息，就可以看到表单提交的具体内容。如要删除任何记录，只要在复选框内选中该条记录，然后按删除键就可以完成。

管理员也可以通过两个选项和一个关键字来进行表单内容查找。两个选项是：“所有用户”和“所有警别”。其中“所有用户”包含：所有用户和用户列表；所有警别包含：所有警别和警别列表，警别列表与设置里的网页表单过滤规则对应。两个选项和一个关键字的查询关系是“并”。




图：网页表单。

## 3.4 上网情况统计、分析与报表

可以按用户统计在指定时间内上网的情况，包括流量、连接时间等。可以按服务方式进行分类统计。如：可以统计某个人在指定的时间内邮件系统的使用情况，网站的浏览时间，ICQ 的使用时间等。

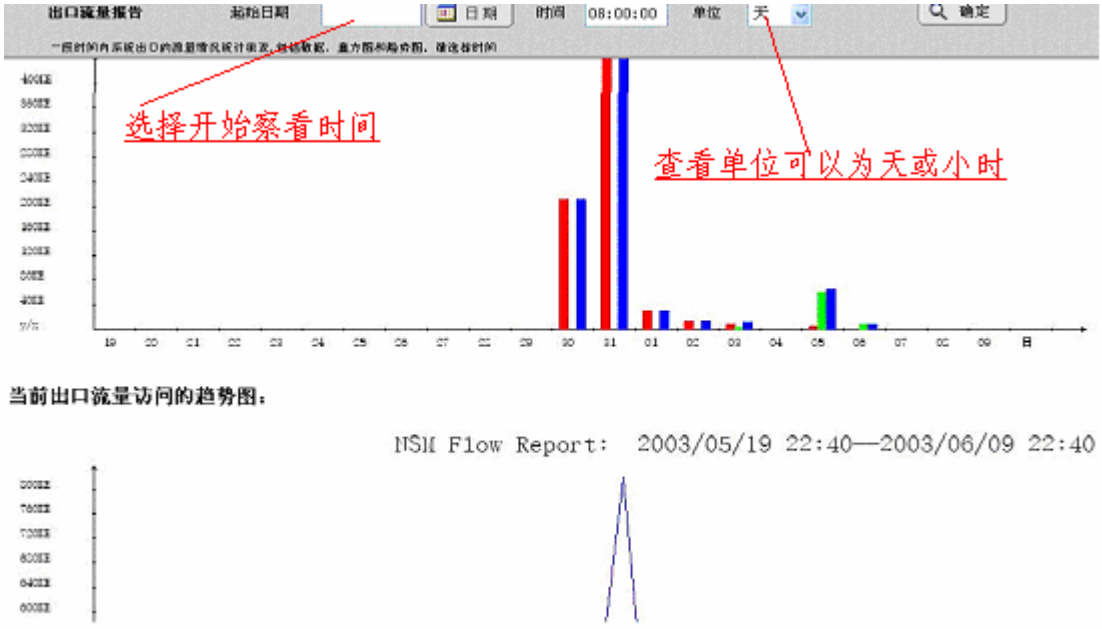
- ✧ 统计排列员工上网时间。
- ✧ 统计排列员工上网流量。
- ✧ 统计排列员工最常去的网站 IP 地址。
- ✧ 上网情况的分析，访问最频繁的网站分析，上网最多的人员分析及上网排行榜等。

### 3.4.1 网络出口状况

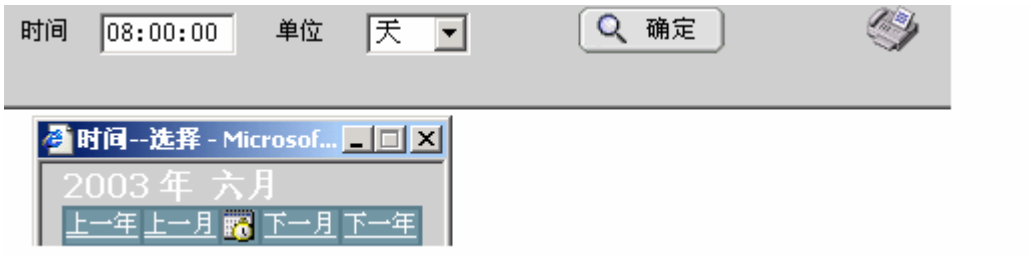
单击 报告----》出口流量报告　可以查看当前和一段时间内网络的出口流量情况。可以按小时、天等为时间间隔进行统计。

首先点击“日期”按键，系统会弹出时间选择对话框，在里面可以进行上一年、上一月、下一月和下一年的操作，在日期表里点选日期。选择的日期将自动填充到起始日期输入框里，然后点击确定，开始查询。


上图：时间选择框图

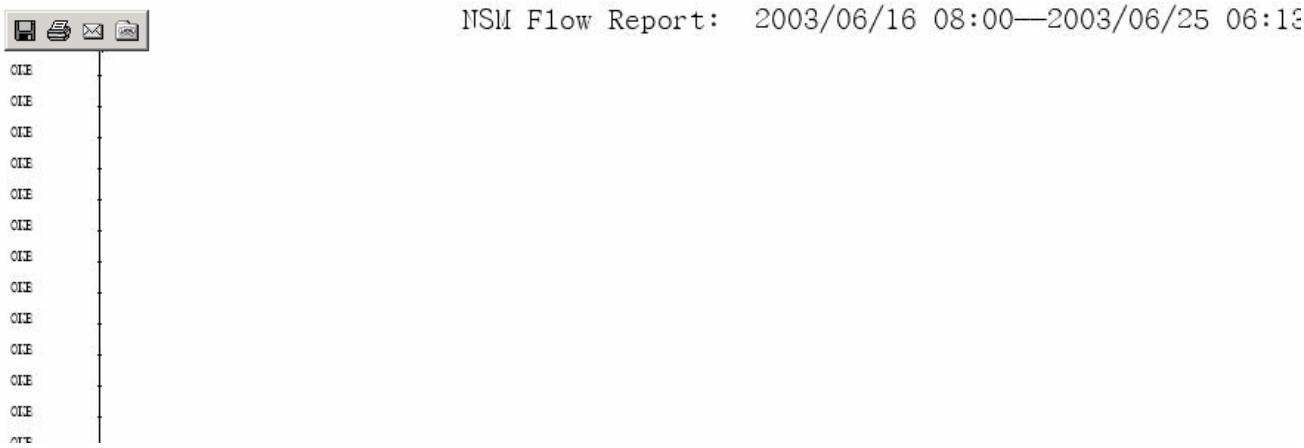



上图：系统出口流量分析




“确定”键右边的的图标，是打印功能。它将打印查询结果。

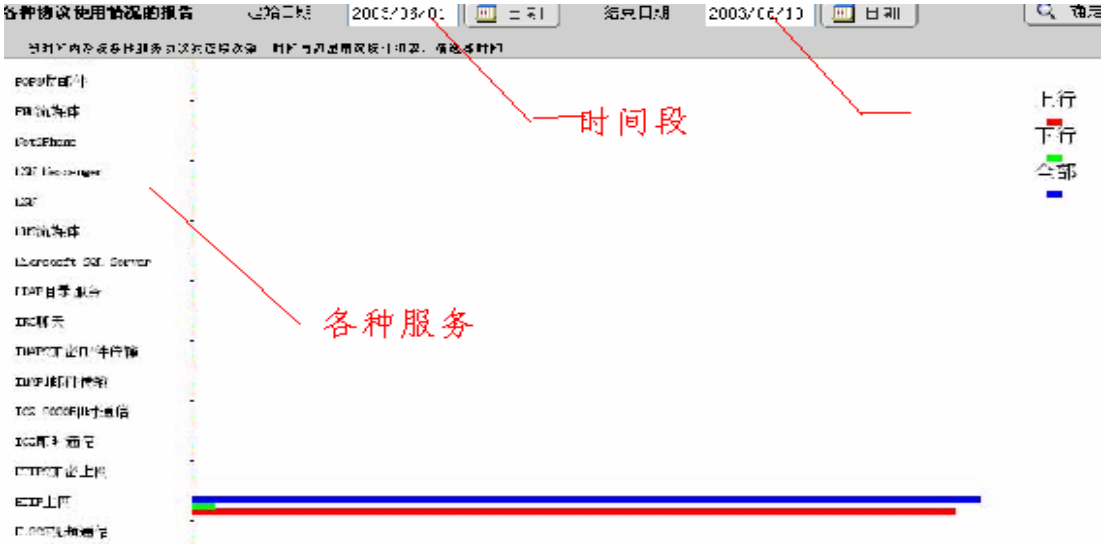

**当前出口流量访问的直方图：**




当鼠标在各种流量图上晃动时，图的左上角将出现一排四个按键，如上图所示。它们的功能分别是：保存此图、打印此图、在电子邮件中发送次图形和打开“图形收藏”文件夹。

## 3.4.2协议使用情况报告

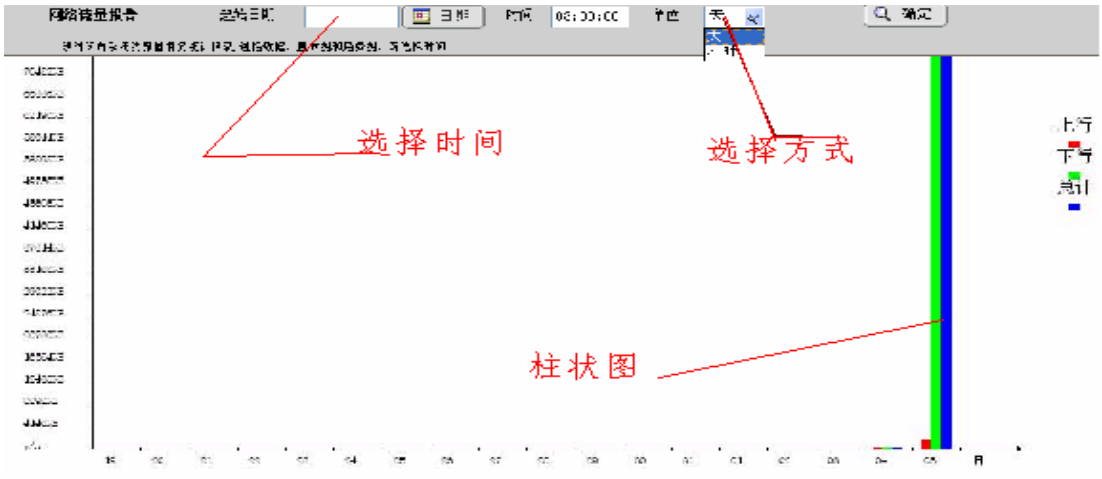
单击 报告----》协议使用情况报告　查看一段时间内各种协议的流量、连接时间、次数等信息的统计报表。




图：协议使用情况报告。

## 3.4.3流量情况统计报表

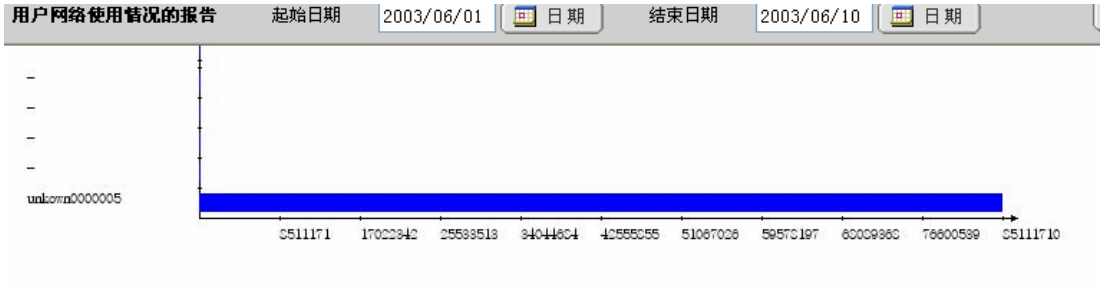
单击 报告----》流量情况统计报表　查看一段时间内系统的流量情况统计报表,包括数据，直方图和趋势图。用户可以选择时间以及时间方式




图：流量情况统计报表.

## 3.4.4人员访问统计报表

单击 报告----》人员访问统计报表　查看一段时间内系统的员工流量情况统计报表,包括数据，直方图和趋势图。用户可以选择时间以及时间方式。




| 姓名 | 流量[字节] | 连接时间（秒） |
|---|---|---|
| unkown0000005 | 85111710 | 21050 |

## 3.4.5网站访问情况的报告

单击 报告----》网站访问情况的报告　查看网站访问情况的排行榜，包括前 3 0 名访问最多次数、流量和连接时间的站点。

前 30 名访问次数最多站点, [NSM Web Usage Report: 2003/06/01--2003/06/09]

| 域名 | 访问次数 | 流量[字节] | 连接时间[秒] |
|---|---|---|---|
| www1.dqt.com.cn | 82 | 50975 | 264 |
| 10.60.237.138 | 80 | 76361 | 2182 |
| 10.61.184.121 | 70 | 62717 | 1670 |
| chat.daqing.net | 63 | 157949 | 3443 |
| 10.64.192.15 | 63 | 60932 | 568 |
| 202.96.140.78:30228 | 60 | 66723 | 1214 |

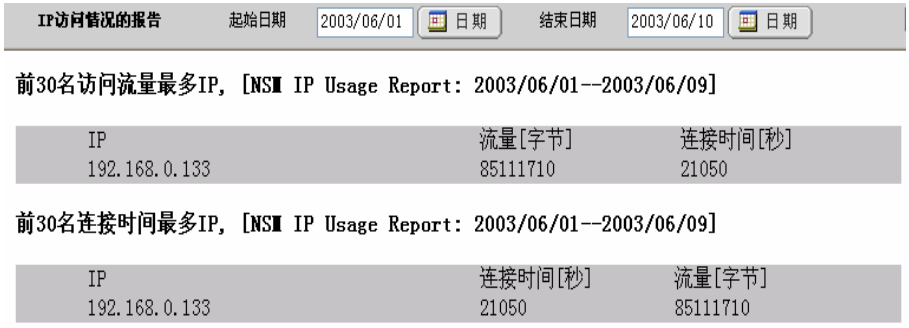
| | | | | |
|---|---|---|---|---|
| | www.nease.net | 45 | 12635 | 293 |
| | 10.64.6.96 | 35 | 113904 | 5569 |
| | 202.97.246.223:9999 | 32 | 12135 | 32 |
| | 10.65.157.18 | 28 | 22584 | 84 |
| | sina.allyes.com | 26 | 68026 | 142 |
| | life.sohu.com | 22 | 17425 | 33 |
| | media.gs.dq.cnpc.com.cn | 20 | 9512 | 20 |
| | 210.12.97.99 | 19 | 5175 | 19 |

前 30 名访问流量最多站点, [NSM Web Usage Report: 2003/06/01--2003/06/09]

前 30 名连接时间最多站点, [NSM Web Usage Report: 2003/06/01--2003/06/09]

## 3.4.6 目标访问情况的报告

单击 报告----》目标连接情况的报告 选择时间，查看一段时间内系统的 IP 连接时间、流量情况统计报表。




图：一段时间内系统的 IP 连接、流量情况统计报表。

# 3.5 网络行为的管理、限制和内容审核

## 3.5.1 带宽管理

带宽管理的可以实现网络带宽的合理分配。本功能可以实现对每个用户上网带宽的限制。

## 3.5.2 上网时间控制

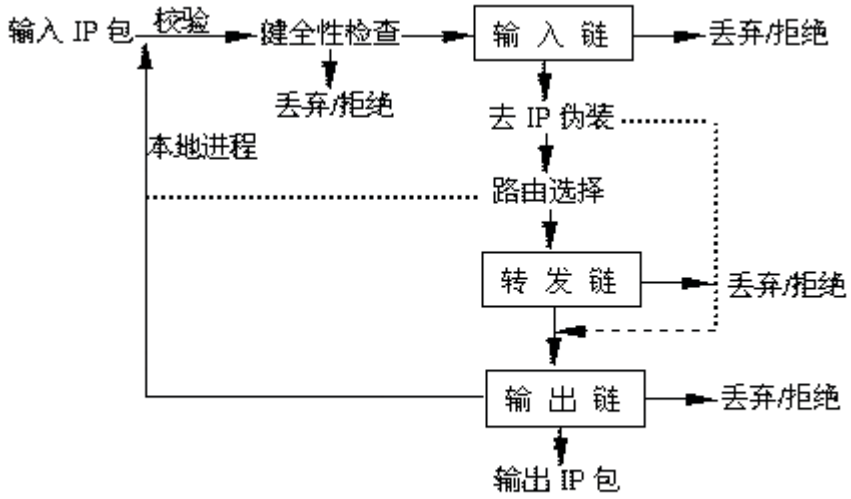
管理者可以分配给公司全部或其中某一用户一定的上网时间（按时间总数来计算），在设定的时间段内，用户能够正常上网，当用户的上网时间总数超过了设定时间的总数时，用户将不能在上网。

## 3.5.3 上网流量控制

管理者可以分配给公司全部或其中某一用户一定的上网流量（按流量总数来计算），在设定的流量段内，用户能够正常上网，当用户的上网流量总数超过了设定流量的总数时，用户将不能在上网。

## 3.5.4 IP 包过滤

建立一个基于 IP 包过滤的防火墙系统。支持包过滤的核心中有三个规则列表，这些列表称为防火墙链。三个链分别称为输入链、输出链和转发链。当一个包从 Internet 进入配置了防火墙的主机时，内核使用输入链决定该包的取舍。如果该包没有被丢弃，则内核继而调用转发链决定是否将包发送到某个出口，最后包要被发出前，内核通过输出链来做决定。




一个链是一系列规则的列表。每个规则规定，如果包的包头与规则相匹配，那么对包进行相应的处理。如果该规则与包不匹配，则引入链中的下一条规则。如果没有要引入的规则，内核根据内置策略决定如何做。在一个有安全意识的系统中，该规则通常告诉内核将包拒绝或丢弃。

通过适当配置 IP 过滤规则，即三条链的过滤策略，该防火墙可以控制输入的包来自信任的 IP 网段，也可配置为只对外开放指定的 TCP/UDP 端口号。这些策略可分别指定到防火墙主机的某固定接口设备如以太网卡、PPP 连接等。除这三条链外，我们还可以配置用户自定义的规则链。在三条链的执行中可随时跳转到自定义链执行，完成后再回到主链，这使过滤规则可以相当灵活。

系统采取单步操作，方便易用。

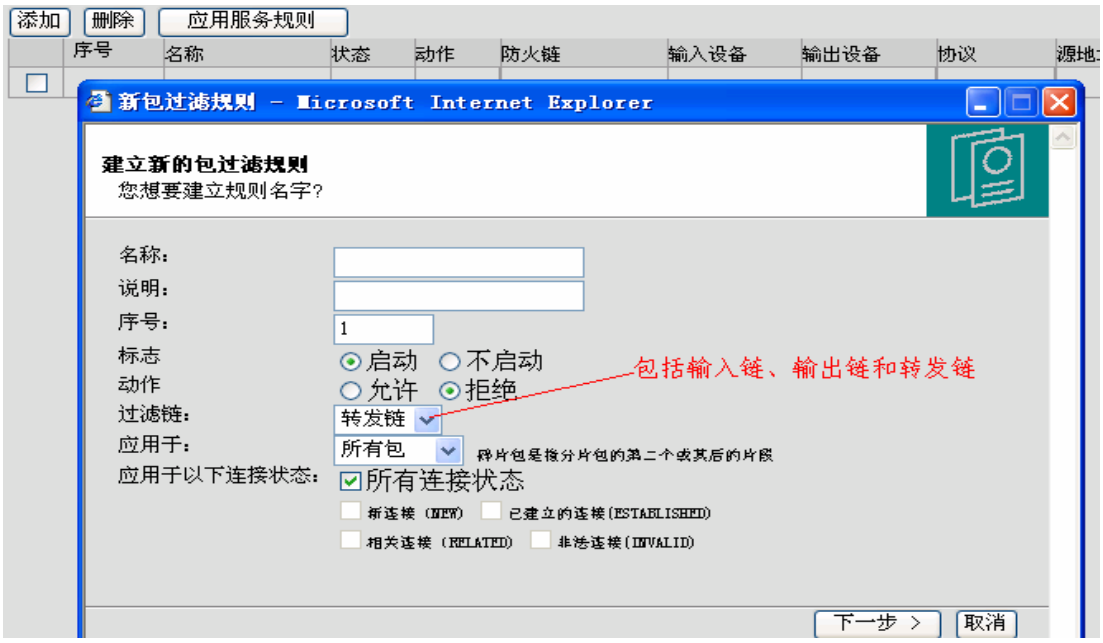



图 4-12

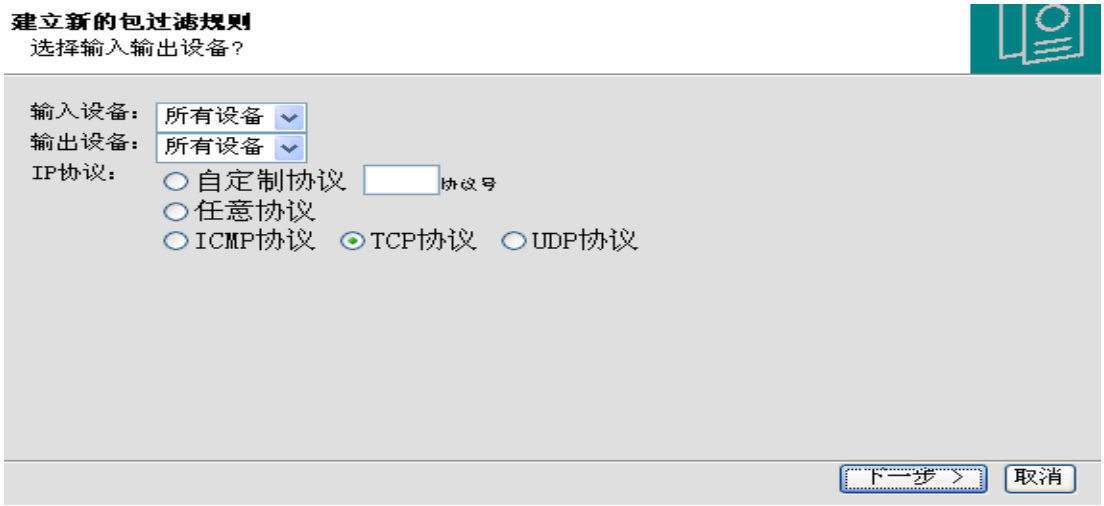
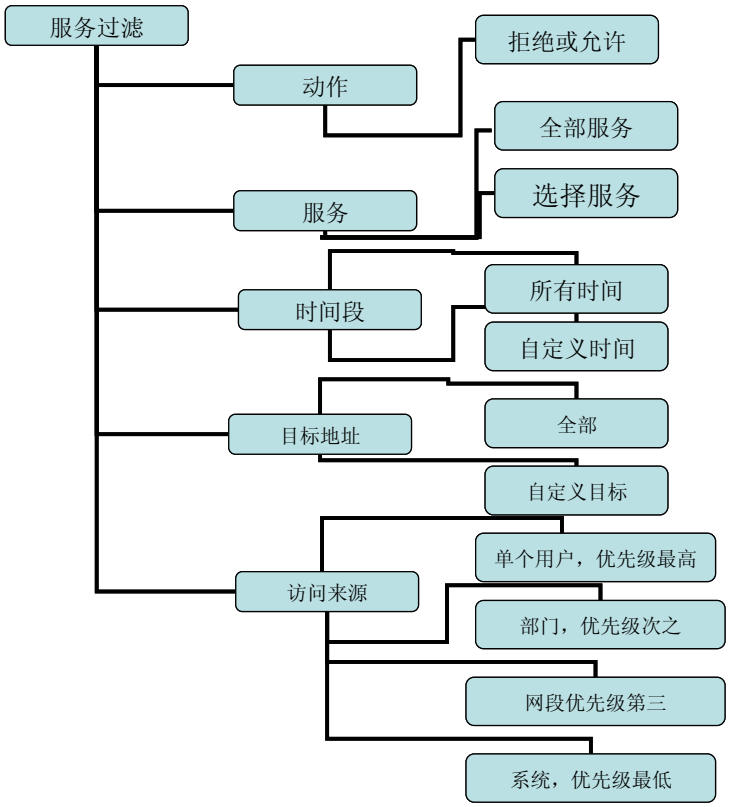



图 4-13

## 3.5.5服务过滤

系统对特定服务进行限制和管理。整个系统服务过滤的体系如下：



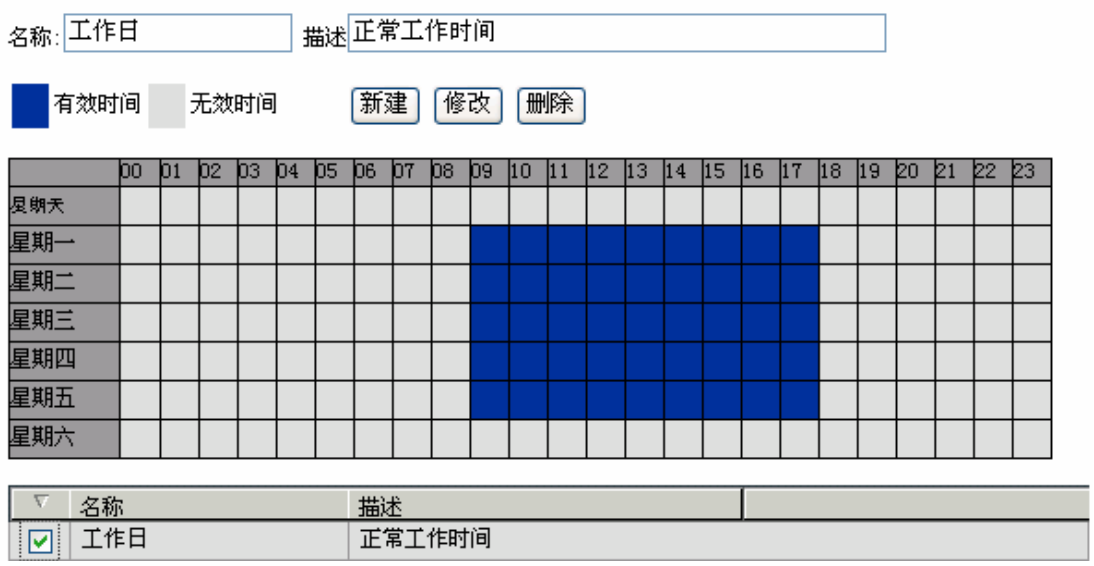




图 4.14：定义系统的时间段。


图 4.15：定义新的服务规则。


图 4.16：定义新的服务规则：选择服务。

## 3.5.6Web 与 URL 过滤

系统对 WEB 服务进行内容透过滤。既可以对 50 种用户自定义的 URL 类别进行过滤，也可以对单个 URL 进行过滤。


图 4.17：定义新的 URL 规则：选择 URL 类别。

管理员可以自定义 50 个 URL 类别。


图 4.17：定义 URL 类别。

## 3.5.7 发送邮件过滤

对于保密性比较强的单位，可以选用邮件监控及拦截审计模块，该功能可以实现对局域网中收发的所有邮件进行监控的目的。同时还可以根据条件设定敏感邮件，系统将自动把敏感邮件存放到指定的区域，以便查看。系统将自动将监控结果按使用者进行分类。

另外政府、企业正大量采用邮件来进行信息交流，它已经成为一个不可或缺的工具，但我们更应清醒地看到，

在同时，邮件信息的管理的漏洞日益突出，政府、企业的信息是无价的，一些关键性信息的泄露，可以给政府、企业带来无法弥补的损失。为了洞察先机，做到事前防范，保障政府、企业有一个安全的信息交流环境，在国内率先开发了邮件拦截审计功能

在此可以设定按： 发件人地址（可多条）、 收件人地址（可多条）、邮件主题、邮件内容、邮件大小、附件名称、附件大小等条件进行设定，符合条件的邮件可以选择控制方式。控制方式有：正常发送、拒绝发送、转发邮件、等待确认。同时，可以设定是否保留邮件备份、是否通知发件人、收件人、其他管理人员。该规则可以设定多条规则。

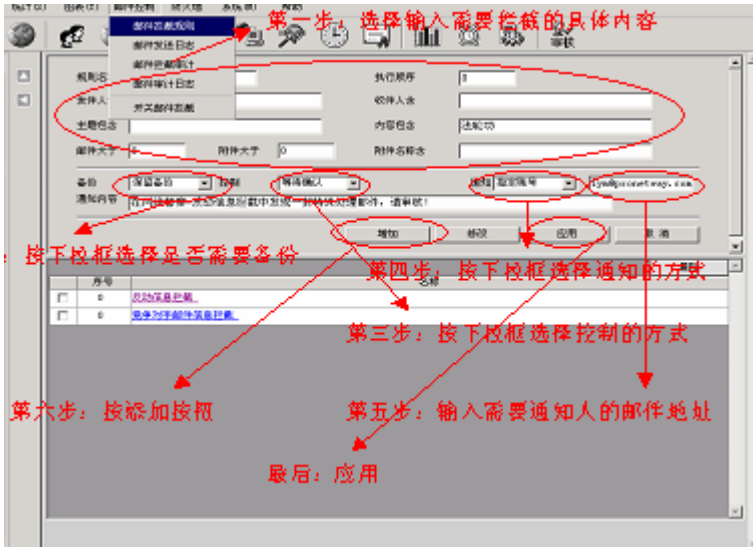



图 4.18：邮件发送过滤设定。


图 4.19：邮件发送审核。

# 3.6 系统管理与设置

## 3.6.1 系统网段设置

对整个网络进行设置，并选择适合公司的验证方式。用户可以任意选择一种方式来进行网络设置。可选择基于 IP 地址、基于 MAC 地址、基于身份认证等

在对用户监视之前，首先应对系统进行一些设置，以便系统可以按照监管人员的要求对局域网中用户进行监视。

用户如采用的是固定的 IP 地址，可以选择基于 IP 地址的方式来进行管理，只要输入公司的起始 IP 和终止 IP，然后按应用键。

用户如采用的是动态的 IP，则可以选择基于 MAC 地址的方式来进行管理，只要在界面中输入需要监管的 IP 地址段的 IP 范围，然后按应用键。这时候无论你的 IP 地址怎样改变都不会影响他的监控。

如果公司需要采用上网之前需要验证的方式，则可以选择本地验证，只要在界面中输入需要监管的 IP 地址段的 IP 范围，然后按应用键。这时候相应的用户，如需上网都必须在宝龙汉景网络卫士管理系统的界面中进行用户登录验证。

如公司需要与 NT 服务的域管理进行统一认证，则可以选择第三方认证，只要在界面中输入需要监管的 IP 地址段的 IP 范围，与验证服务器的地址，然后按应用键。

在免于监控中输入相应的需要免监控的 IP 地址段，则这段的用户将不受到监控

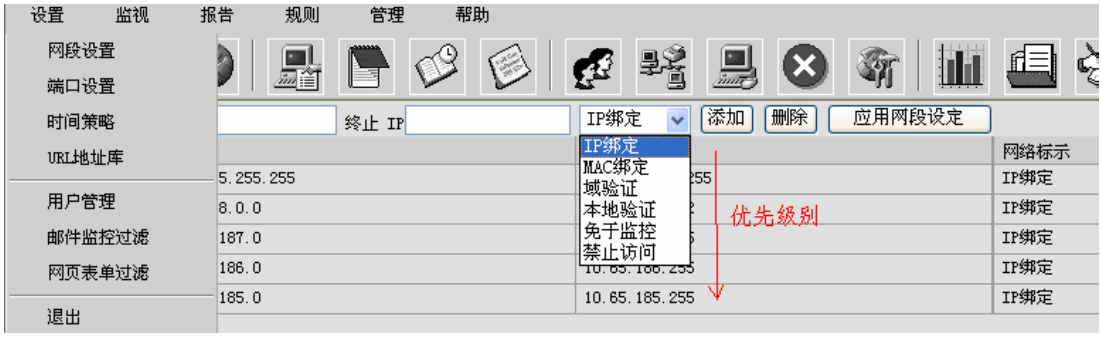



图 4.19：系统网段设置。

## 3.6.2 系统端口设置

对各个端口的状态进行设置。


图 4.20：系统端口设置。

## 3.6.3 多级管理权限

对于管理用户，可以根据权限设定相应的用户可以管理网络的权限，权限的设定可以细分到每一个功能。

图 4.21：系统权限设置。

## 3.6.4 系统用户管理

使用该功能可以对接入局域网的所有用户分部门管理。对于部门或用户的添加、修改和删除,带宽的分配、密码的设定都在这里进行操作。

如果是选用身份验证登录的方式的用户，需要在此设定登录密码
输入该用户的邮件地址，以便在邮件监控的时候能够确认
可在带宽限制处输入给予该客户的最大的带宽。
在状态栏选择客户在系统内的状态，如选择“免监控”，则该用户将不被系统所监控
“加入时间”可以空白，系统会自动将系统时间添加入该用户信息。
MAC 地址为该用户计算机中的全球唯一标示的网卡地址。系统会自动识别

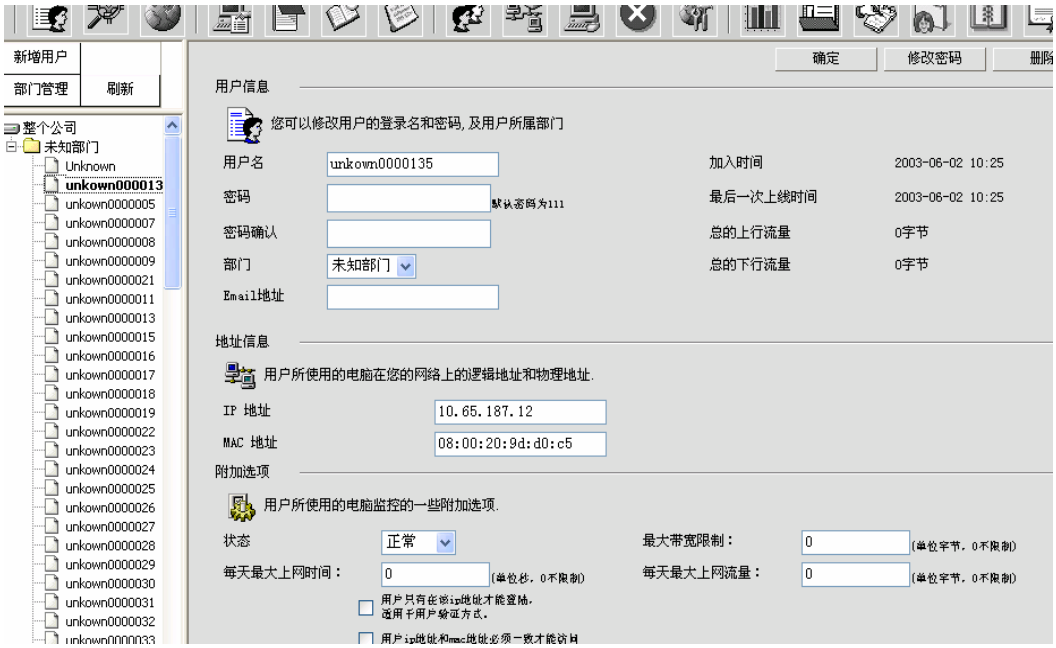



图 4.22：系统用户设置。

# 4 系统技术特点

宝龙汉景网络卫士管理系统是完全基于公司自身的技术开发的，公司拥有从底层到用户界面的全部技术。

系统采用的各种技术为公司在长期的开发和研究中积累的。系统采用最新版本的加固内核。Ip 包监控使用链路层数据包截获和还原技术。访问控制和流量控制基于 Netfilter 的架构。系统的协议分析和过滤技术均为公司在开发各种 Internet 服务应用时开发的技术。系统的内存管理是经过长时间考验的稳定的技术。

基于 Web 的管理界面采用采用公司自主版权的中间件服务器宝龙 网络卫士安全中间件平台开发。整个系统具有以下特点：

**1. 不影响原有的网络配置**

**2. 运行效率高**

**3. 可以长时间运行**

**4.基于三层结构的 Web 管理**
**5.不需要特殊的系统维护**

# 5 宝龙汉景网络卫士管理系统的优势

**1. 为什么要选用宝龙 网络卫士硬件产品：可靠稳定、适应高速网络与出口**
宝龙 网络卫士硬件的优点：硬件独获 Intel 服务器平台认证，可靠高效，内建安全软件，使用专属强化的 OS，管理方便，更换容易，软硬件搭配较固定。
而且要支持百兆以上网络，硬件产品几乎是必选的方案。

**2. 为什么要选用宝龙 网络卫士国内产品：内核专有，管理灵活适用，对国情了解**
首先，这是一套审计管理系统，必须和政府、企业的管理方法和用户使用习惯相适应。
我们针对国内推出的不良网址库，主要就是针对中文网址，并且支持网络升级。
我们的按部门管理、角色管理、免检控管理、跨网段管理这些都是很有特色和扩展性的。

**3. 为什么要上网络审计产品：功能专业，与代理软件、防火墙功能上区别很大**
互联网审计系统在国外已经是区别于其他安全产品的独立分类。
据 IDC 的报告,互联网访问控制系统，作为一个工具手段已经发展成又一个应用主体：
• 截至至 2003 年,超过 2.72 亿的全球职员在使用互联网。
• IDC 评估全球互联网访问控制软件的市场从 1998 年的 3500 万美金，增长到 1999 年的 6300 万美金，预计到 2004 年市场将增长到 5.62 亿美金。
• 从 1999 年到 2004 年，IDC 预计互联网访问控制软件在下列地区每年的增长量为：美国 40%，欧洲 54%，亚洲/太平洋 69%，其他地区 47%。
在未来，IDC 相信互联网访问控制系统将通过自动化、知识驱动型的互联网使用优化增强政府、企业员工的效率，成为政府、企业安全管理的重要组成部分。
所以，政府、企业除了防火墙等其它安全产品外，对于专业的网络审计，必须要购买相应的专业化产品，才能真正达到全面有力管理的目的。

**4. 宝龙 网络卫士的其他优势**
在国内外著名政府、企业大型网络上的实施经验和性能保证，我们在数千台电脑、ATM525M 网络中可以稳定运行。(中石油大庆管理局、铜陵有色金属等超大型政府、企业)，我们在实测结果中，达到了在 500 万记录中查询速度不超过 3 0 秒，体现了系统的效率和优化。

丰富的行业实施经验，我们在烟草、电力、政府、大型制造业、教育、公安都有众多的成功案例。

个性化的整合服务（定制界面 与原有系统整合)，我们基于对邮件内核技术的了解、对防火墙技术的掌握、对 Windows 端开发的技术，可以依据大客户的本身需求，对系统响应调整，适应政府、企业的个性化要求。