Active Wall User Manual

用户手册

丽水市爱科网络有限公司

Active Network CO., Ltd

目 录

第一章 前言

1.1. 版本说明

本手册对应产品为：Active Wall V2.0

1.2. 读者对象

本书适合下列人员阅读:

- 网络工程师
- 网络管理人员
- 具备网络基础知识的用户

1.3. 本书约定

通用格式约定

格式	意义
宋体	正文采用宋体表示
黑体	除一级标题采用宋体加粗以外其余各级标题均采用黑体
楷体	警告提示等内容一律用楷体并且在内容四周增加方框与正文隔离

图形界面格式约定

格式	意义
<>	带尖括号“< >”表示按钮名，如“单击<确定>按钮”
[]	带方括号“[ ]”表示窗口名、菜单名、数据表、模块插件名和字段名等，如“弹出[新建用户]窗口”
/	多级菜单用“/”隔开，如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项

键盘操作约定

格式	意义
加尖括号的宋体字符	表示键名，如<Enter> 、<Tab>、 <Backspace>、 <a>等分别表示回车、制表、退格、小写字母 a
<键 1 + 键 2>	表示在键盘上同时按下几个键，如<Ctrl+Alt+A>表示同时按下 Ctrl、 Alt 、A 这三个键
<键 1，键 2>	表示先按第一键，释放，再按第二键。如<Alt ，F>表示先按<Alt>键，释放后再按<F>键

鼠标操作约定

格式	意义

单击	快速按下并释放鼠标的一个按钮
双击	连续两次快速按下并释放鼠标的一个按钮
拖动	按住鼠标的一个按钮不放移动鼠标

各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方,这些标志的意义如下:

 注意，警告提醒操作中应注意的事项。

 提示，对操作内容的描述进行必要的补充和说明。

第二章 产品介绍

2.1. 系统简介

《Active Wall》是一款专业的网络监控管理软件，支持网关、网桥、旁路、单机等多种监控模式，支持 VLAN 和跨网段监控，适合任何网络结构。无需客户端，只要在一台电脑上安装即可过滤控制局域网内部所有电脑的上网行为。它能有效监视、控制和记录内部电脑在互联网上的活动，实时记录局域网内计算机所有收发的邮件、浏览的网页以及 FTP 上传下载的文件，监视和管理网内用户的聊天行为，控制网内用户访问指定网络资源或网络协议。

系统使用最新的网络安全技术，能准确有效地对局域网内部计算机的所有上网行为进行审查和监控。主要功能有：

1. 网络身份验证：
   要求用户输入正确账号和密码后才可访问互联网，支持多种验证方式。
2. 时段过滤：
   根据时间段设置是否开放上网的功能，可给不同的组设定不同的上网时间段。
3. 端口过滤：
   通过开放或关闭一些端口，允许内部用户使用或禁止使用互联网上部分服务。有效拦截网络游戏、聊天、视频、音频等与工作无关的网络应用，使网络资源得到合理的利用。
4. 流量控制：
   控制网络内部每台电脑或全组的传输速度，设置网络内部每台电脑或全组每天允许的最大网络流量。合理安排公司的带宽资源，防止员工使用 P2P 工具占用过多的带宽。
5. 实时流量显示：
   可以实时显示和统计当前各协议的网络流量，反映网络拥塞情况和协议分布。
6. MAC 地址过滤：
   对内部电脑按网卡 MAC 地址过滤，并能将 MAC 地址绑定固定的 IP 地址。防止网内 IP 地址非法修改和盗用，合理利用有限的 IP 地址资源，实现统一管理。
7. IP 地址过滤：
   对外网的 IP 地址进行屏蔽和过滤，管理员通过设定的 IP 黑名单，可禁止内部电脑访问这些 IP 地址和网段。
8. DNS 过滤：

可以过滤内部电脑向互联网发出的域名查询请求，并能过滤色情、赌博、游戏等数十种域名分类库。

9. HTTP 过滤：
   对网内用户浏览的网页根据网址、网页内容、外发内容、外发文件等设定过滤条件。还可以保存用户浏览过的网页、外发文件，以便日后检查。
10. SMTP 过滤：
    全面监控网内所有用户发送出去的电子邮件，根据邮件标题、邮件内容、发信人地址、收信人地址、附件、邮件大小进行审查和阻断；同时可以将原始邮件保存下来，在企业商业机密数据发生外泄事件或其它类似事件发生时可以作为强有力的证据。
11. POP3 过滤：
    全面监控网内所有用户接收的电子邮件，根据邮件标题、邮件内容、发信人地址、收信人地址、附件、邮件大小进行审查和阻断；同时可以将原始邮件保存下来。
12. 即时聊天过滤：
    可有效监控用户使用 QQ、MSN、ICQ、网易泡泡、雅虎通、新浪 UC、阿里旺旺、迅雷、IRC、Jabber、BitTorrent、eDonkey 等即时通讯工具和 P2P 工具。
13. FTP 过滤：
    对网内用户用 FTP 上传和下载的文件进行审查过滤，并能保存原始文件，从而保证公司内部机密不被泄露。
14. HTTPS 过滤：
    有效监控内部电脑对外发起的 HTTPS 协议，可过滤允许访问的 IP、网段、SSL 协议类型、HTTPS 服务器数字证书，并能阻止 HTTPS 隧道代理。
15. 代理转发：
    可以与普通的代理服务器配合实现透明代理服务，而无需在客户端作任何代理设置。可实现如：网关杀毒、垃圾邮件处理等更高级的功能。
16. 日志文件输出：
    将网络监控的审计结果或告警信息保存到指定目录以便日后查询。
17. 告警邮件通知：
    可以设置关键字，当告警信息匹配该规则时以电子邮件的方式发送到指定邮箱，使管理员能够及时收到告警并对事件进行处理。
18. 告警消息通知：
    可以设置关键字，当告警信息匹配该规则时以信使消息的方式发送到指定电脑，使管理员能够及时收到告警并对事件进行处理。
19. 日志数据库输出：
    将网络监控的审计结果或告警信息保存到数据库中，以便日后查询和统计分析。

2.2. 系统特点

1. 更强的过滤引擎
   <<Active Wall>>使用自行开发的中间层驱动程序作为过滤引擎，比同类型产品所使用的 WinPCap 更底层。由于 WinPCap 是协议类型驱动，只能监听不能拦截。采用 WinPCap 驱动的监控软件，可以断开 TCP 会话，却无法拦截 UDP、ICMP、IGMP 等数据包。《Active Wall》过滤引擎经过长期的实践证明更稳定、更准确、效率更高。
2. 更多的监控模式

同类产品大多数都是使用旁路侦听模式监控网络，<<Active Wall>>除提供旁路模式之外，还提供了网关、网桥和单机模式，并且建议采用网管、网桥模式。使用旁路模式，由于网络结构的限制，只能对 TCP 数据包进行拦截。而<<Active Wall>>所提供的网关、网桥和单机模式可以拦截所有的数据包，保证过滤的准确有效。

3. 更高的系统性能

   <<Active Wall>>在设计时便以高性能为目标，在过滤模块中采用了最优化的算法，使得性能远远超过了同类型的产品。《Active Wall》最大可支持 10000 台电脑同时上网，域名分类目录库可达百万数量级，可轻松处理 100M 的流量而无明显速度下降。

4. 更灵活的监控配置

   <<Active Wall>>使用更多的配置选项来对网络内容进行审计，比如 HTTP 过滤可以针对网址、网页标题、网页内容、提交内容、上传文件、内容大小进行过滤；邮件过滤可以针对收信人地址、发信人地址、邮件标题、邮件正文、附件内容、邮件大小进行过滤。同时还支持通配符的输入匹配，并可调节匹配顺序，基本上涵盖了所有可能的组合条件，从而使监控配置更加灵活方便。

5. 更全面的保存纪录

   <<Active Wall>>不仅可记录用户浏览的网址、邮件标题，还可以根据监控设置保存网内用户所浏览过的网页、外发的内容、上传的文件、发送的邮件、接收的邮件等。内容保存功能可能让你在事件发生后有据可查。

6. 智能在线升级

   <<Active Wall>>提供类似杀毒软件的在线升级功能，让你能够轻轻松松地将软件升级到最新版本， 并且无需重启，新版本立即生效。

第三章 安装与卸载

3.1. 运行环境

硬件要求：

CPU：x86 兼容处理器，主频 266MHz 以上

内存：64M 以上

网卡：10~1000M 以太网卡

硬盘：10M 以上剩余空间

显卡：800*600 像素以上显示模式

软件要求：

32 位简体中文版 Windows 2000/XP/2003 操作系统

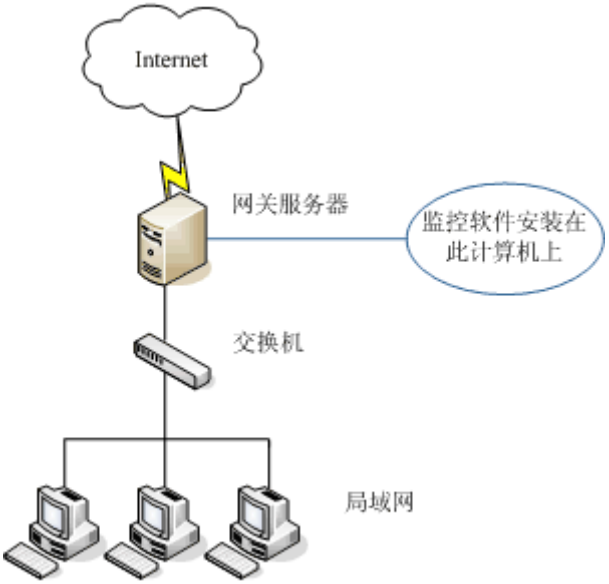
NDIS 兼容网卡驱动程序

需安装 TCP/IP 协议

3.2. 网络环境

网关模式：(推荐)

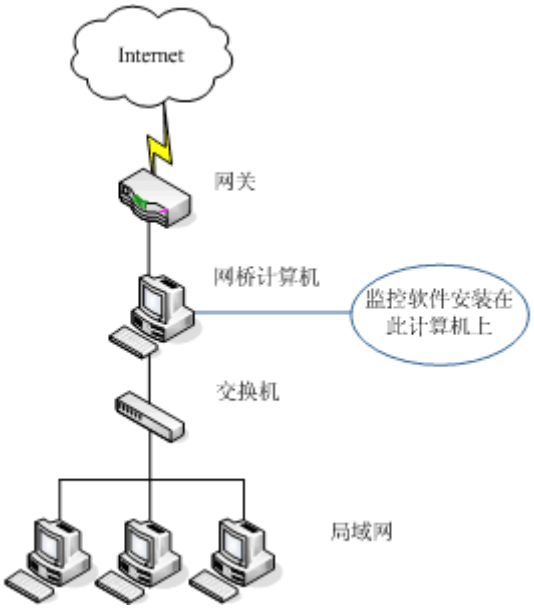
如果您的局域网使用安装有 Windows 操作系统的计算机作为网关服务器时，《Active Wall》只需安装在该服务器上，就可以监控所有通过该网关上网的计算机了。网关共享上网方式包括 NAT、路由、代理等多种方式，建议与 Windows 操作系统自带的路由和远程访问服务(RRAS)或 Internet 连接共享(ICS) 配合使用。



网关模式

网桥模式：

如果您的网关服务器不是 Windows 操作系统，您可以采用网桥模式。该模式需要一台安装有双网卡的计算机作为网桥(需 Windows XP 以上操作系统才支持网桥模式)，分别与网关、交换机相连接。《Active Wall》安装在该计算机上，就可以监控所有通过该网关上互联网的计算机了。网桥的配置请参阅[如何设置网桥]。

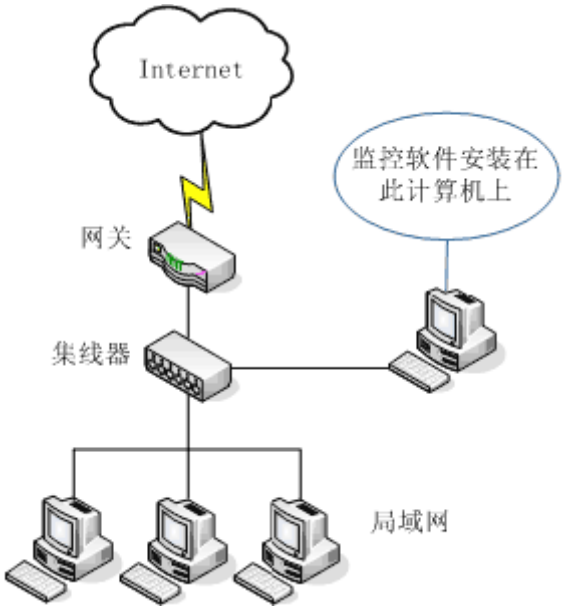


网桥模式

旁路模式：

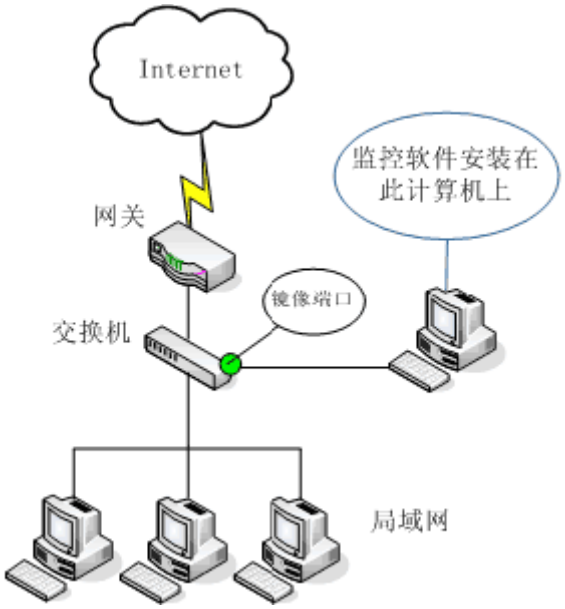
旁路模式支持以下四种网络拓扑:

1. 如果您的局域网中各计算机由共享式的 HUB 连成网络，那么《Active Wall》可以安装在局域网上的任意一台机器上。



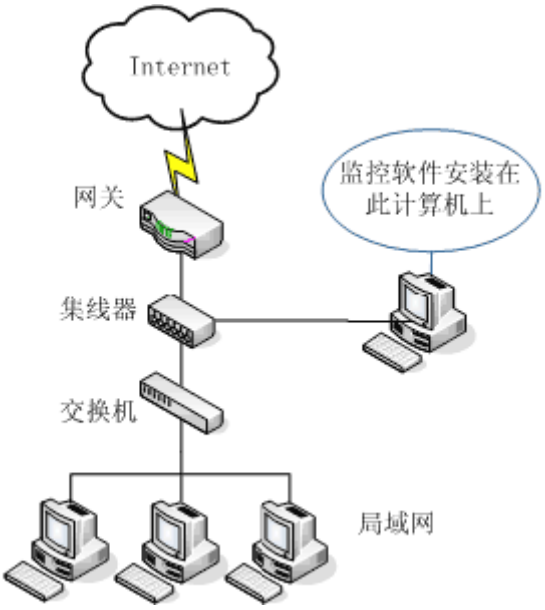
旁路模式一

2. 如果您的局域网使用可网管交换机连接，则需要在交换机上设置端口镜像，将所有的上网数据镜像到安装有《Active Wall》的计算机与交换机连接的端口上。



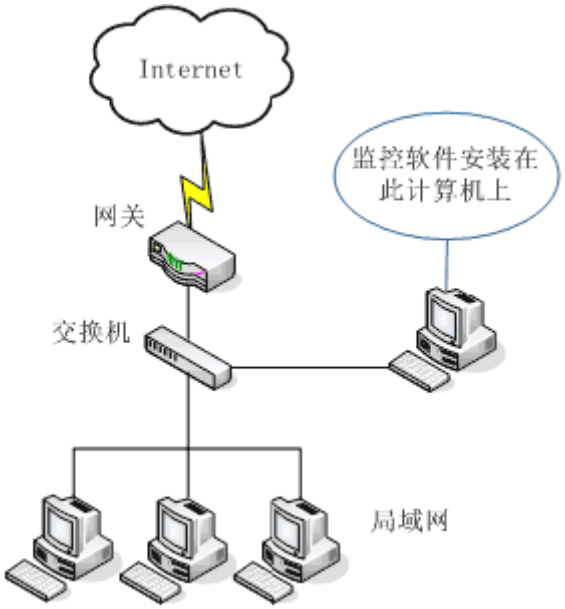
旁路模式二

3. 如果您的局域网使用普通交换机连接，不能设置镜像端口，您需要在网关和交换机之间增加一台 HUB，用该 HUB 将安装有《Active Wall》的计算机、交换机和网关连接起来。



旁路模式三

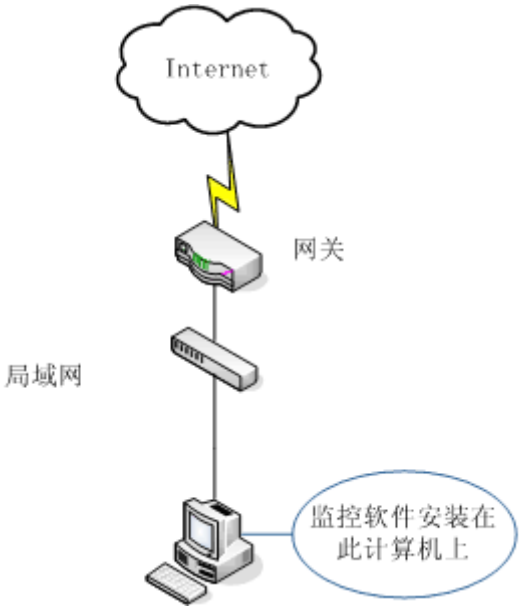
4. 如果您的局域网使用普通交换机连接，不能设置镜像端口且未增加 HUB 等共享式设备。您可以选择旁路模式并在[操作选项]中启用数据转发功能。



旁路模式四

注意：旁路模式具有一定的局限性，部分过滤模块将不能正常工作，详情请看已知问题。

单机模式：



单机模式

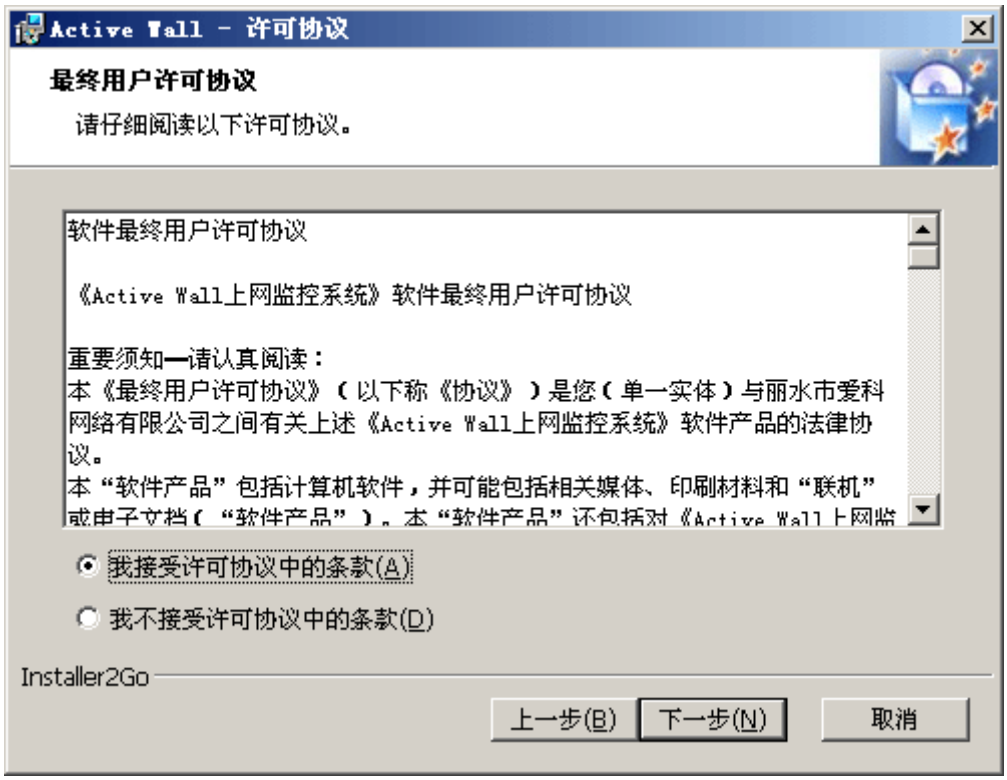
程序安装在局域网内部单机上，用于过滤本地单机访问互联网的内容。

注意：程序的监控模式必须要和当前的网络结构相匹配，否则将无法正常工作。

3.3. 安装程序

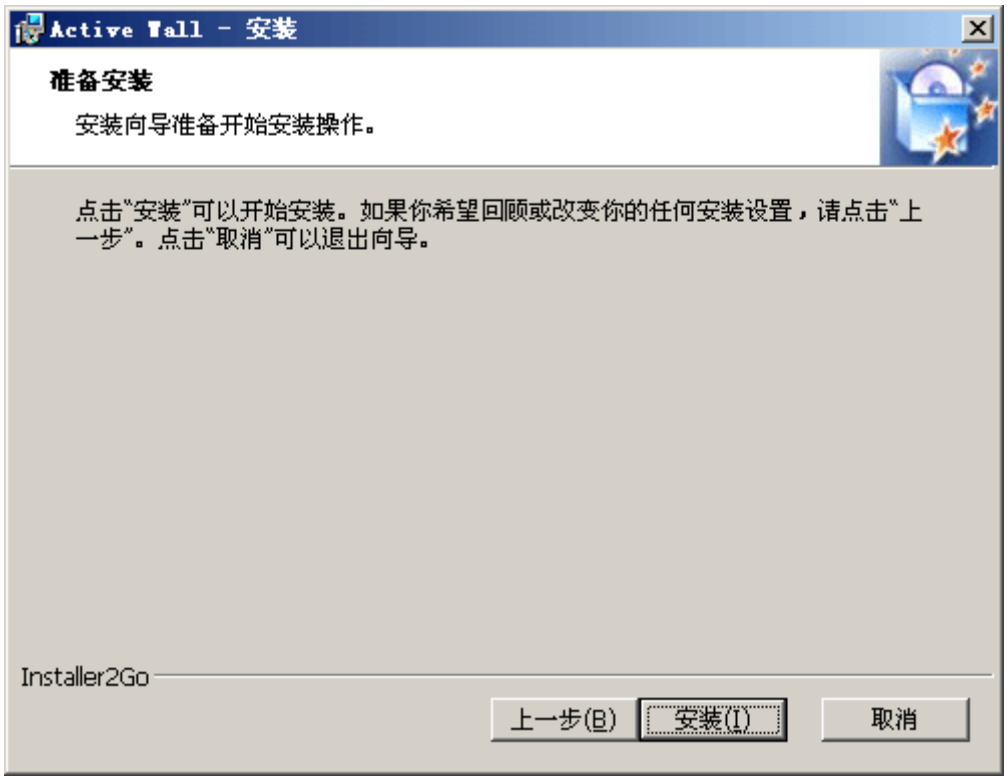
运行安装程序，首先出现安装向导欢迎界面，单击<下一步>按钮。

请仔细查看最终用户许可协议。如果同意该协议，请选择[我接受许可协议中的条款]，然后单击<下一步>按钮，继续安装程序。如果不同意该协议，请单击<取消>按钮，立即终止安装。

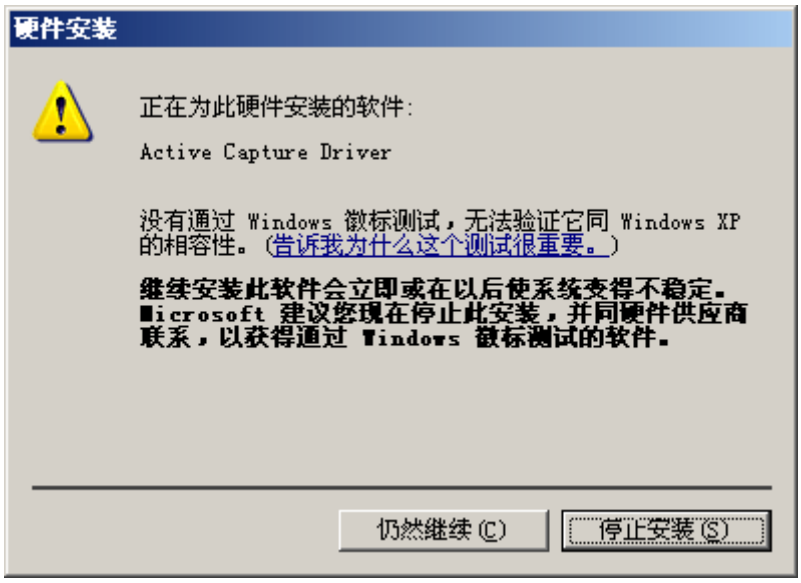


确定程序安装路径。系统默认安装目录为“C:\Program Files\AWall”，您也可以单击<浏览>按钮指定其它安装目录，确定后单击<下一步>按钮进入下一步。

单击<安装>按钮开始安装。



安装程序开始复制文件并安装驱动，WindowsXP 以上操作系统在安装过程中可能会弹出一个驱动的安全警告(如下图)，单击<仍然继续>按钮即可。

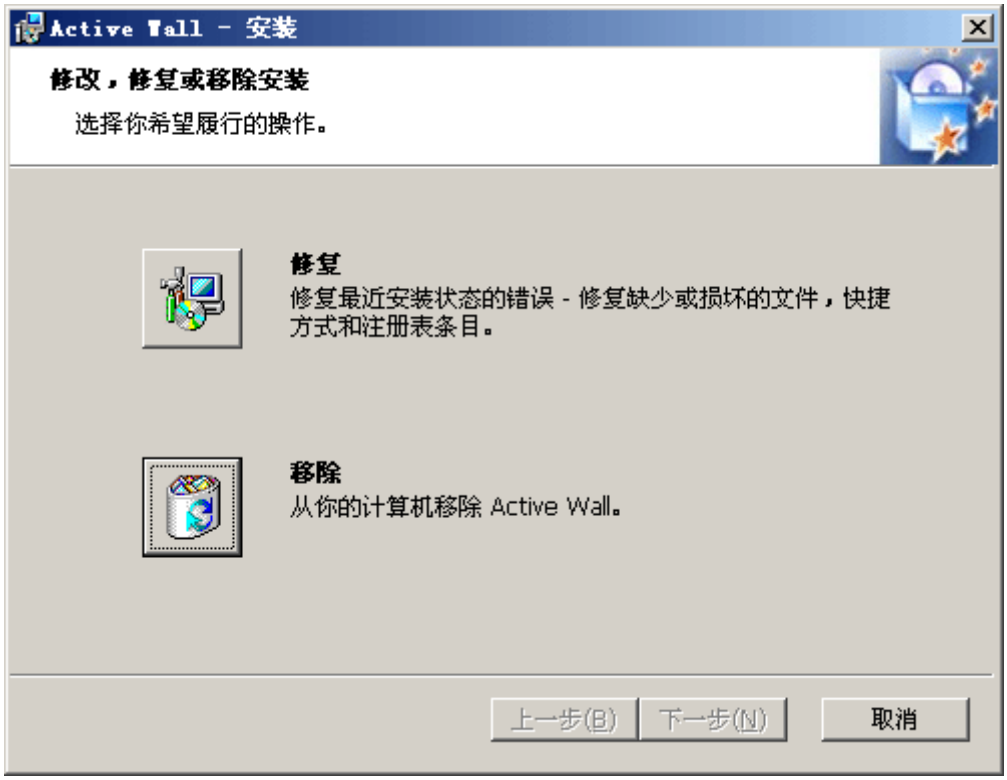


完成安装后，软件将自动开始运行。

注意：在安装过程中会暂时断开当前的网络连接，如果当前电脑有重要网络任务，请首先予以保存。

3.4. 程序卸载

重新运行安装程序，单击<移除>按钮即可卸载程序。



也可以通过[控制面板/添加删除程序]来卸载程序，方法是打开操作系统[控制面板]，双击[添加删除程序]，在程序列表中找到[Active Wall]，单击<删除>按钮，如图所示：

卸载完成后，请立即重新启动电脑。

注意：在卸载过程中会暂时断开当前的网络连接，如果当前电脑有重要网络任务，请首先予以保存。

第四章 系统使用说明

4.1. 启动软件

软件安装后，在操作系统[开始菜单]中，单击菜单[程序/Active Wall/启动服务]即可启动软件。软件启动后在系统任务栏会显示相应的图标，如下图所示：

也可以在操作系统命令提示符下输入命令“net start activewall”来启动软件。

提示：软件以 Windows 服务形式运行，显示名称为 “Active Wall”，默认随操作系统的启动而自动运行。

4.2. 用户登录

双击系统任务栏 Active Wall 软件图标，显示登录界面如下图所示：

输入管理员账号和密码，单击<登录>按钮登录系统。验证通过后才能进入管理界面。

提示：初次运行时管理员账号为 admin，默认密码为空。建议在登录后立即更改密码。

4.3. 启动/停止监控

软件运行后将自动进入监控状态。要暂停监控，单击菜单[系统操作/停止过滤]或单击工

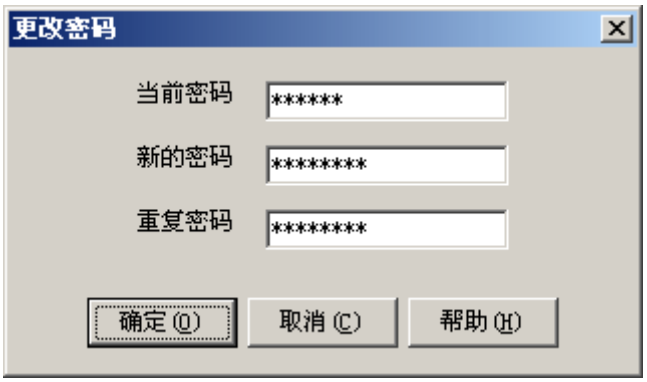
具栏上[停止过滤]的图标 即可。要启动监控，单击菜单[系统操作/启动过滤]或单击工具栏上[启动过滤]图标 即可。

4.4. 注销登录

登录系统后，单击菜单[系统操作/注销登录]即可注销登录。注销登录后程序缩小为系统托盘图标，软件仍然处于运行状态。

4.5. 更改密码

管理员可以通过以下方法更改登录密码，方法是单击菜单[系统操作/更改密码]，在弹出的[更改密码]对话框中重新设定密码。如下图所示：



4.6. 关闭软件

单击菜单[系统操作/退出系统]即可关闭软件。也可以在操作系统[开始菜单]中，单击菜单[程序/Active Wall/停止服务]或在操作系统命令提示符下输入命令“net stop activewall”来关闭软件。

4.7. 电脑管理

软件以电脑 IP 地址作为鉴别内部电脑的唯一依据。软件可以自动检测电脑的在线状态、统计数据收发状况，并显示在电脑列表中。如果开启了自动发现功能，对于新发现的 IP 地址，软件还将自动检测它的 MAC 地址和电脑名称，并添加到“默认组”电脑列表中。电脑的在线状态以直观的图标方式显示：

电脑当前在线且正在发送数据

电脑当前在线但没有发送数据

电脑当前不在线，在指定的时间内未检测到数据包

1、增加电脑

单击菜单[电脑管理/增加电脑]，或者在电脑列表中单击鼠标右键，单击菜单[增加电脑]，在弹出的对话框中输入电脑信息，单击<确定>按钮。如下图所示：

2、修改电脑

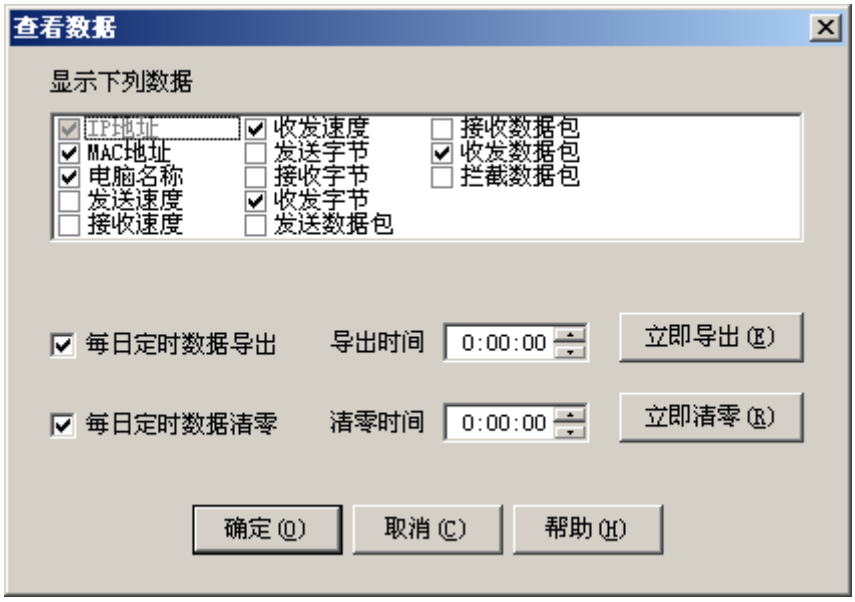
在电脑列表中选择要修改的电脑，单击菜单[电脑管理/电脑属性]，或者在电脑列表中单击鼠标右键，单击菜单[电脑属性]，在弹出的对话框中更改电脑信息，单击<确定>按钮。

3、删除电脑

在电脑列表中选择要删除的电脑，单击菜单[电脑管理/删除电脑]，或者在电脑列表中单击鼠标右键，单击菜单[删除电脑]。可以同时选择多台电脑一起删除。

4、查看数据

软件可对网络中的每台电脑进行详细的数据流量统计，并提供数据定时导出功能。在电脑列表中可显示以下数据项：IP 地址、MAC 地址、电脑名称、发送速度、接收速度、收发速度、发送字节、接收字节、收发字节、发送数据包、接收数据包、收发数据包、拦截数据包。配置界面如下图所示：



更改电脑列表中显示的数据项：单击菜单[电脑管理/查看数据]，在弹出的对话框中选择相应的数据项，单击<确定>按钮。

数据导出：在对话框中单击<立即导出>按钮，填写导出的文件名，单击<保存>按钮。可将当前电脑列表中累计的数据统计信息导出到硬盘上以供分析。

数据清零：在对话框中单击<立即清零>按钮，可将当前电脑列表中累计的数据统计信息清零。

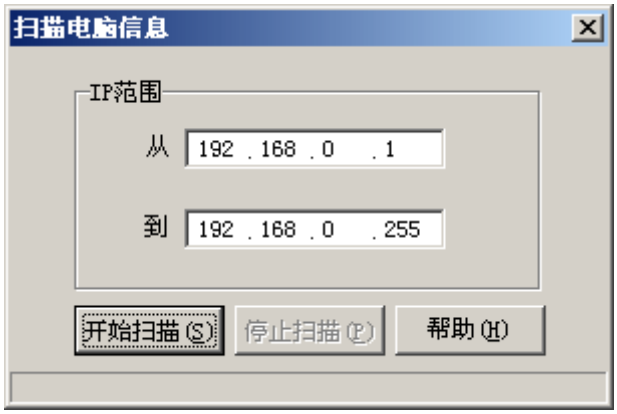
每日定时数据导出：在对话框中选择[每日定时数据导出]，填写导出时间，单击<确定>按钮。执行该操作后，每天到了指定时间，系统会自动导出数据统计信息。默认保存在安装路径的 Report 目录下，每日生成一个文件。

每日定时数据清零：在对话框中选择[每日定时数据清零]，填写清零时间，单击<确定>按钮。执行该操作后，每天到了指定时间，系统会自动将电脑列表中累计的数据统计信息清零。

提示：导出的数据为累计数据，与当前电脑列表中显示的数据相同。如果要统计每天的数据流量，建议同时设置定时数据导出和定时数据清零。另外程序重新启动后，数据将自动清零重新统计。

5、扫描网络

扫描电脑可以指定范围对同网段的电脑进行扫描，并将扫描到的电脑自动添加至“默认组”电脑列表中。单击菜单[电脑管理/扫描网络]，或者在电脑列表中单击鼠标右键，单击菜单[扫描网络]，在[扫描电脑信息]对话框中输入要扫描的起始 IP 和结束 IP，单击<开始扫描>按钮。如下图所示：



扫描网络功能可以自动扫描同一网段内的电脑 IP 地址，以及该 IP 对应的 MAC 地址和电脑名称。如果是新的 IP 将自动添加到“默认组”电脑列表中。

提示：扫描网络功能只能对同网段的 IP 进行扫描，为了确保没有地址遗漏，扫描的速度较慢。推荐采用自动发现功能，可达到更好的效果。

6、自动发现

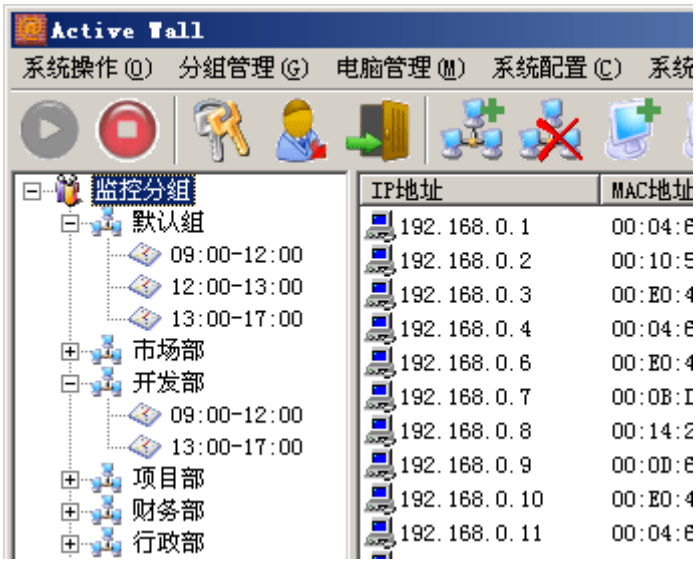
启用[自动发现]功能后，当系统检测到网络有新的电脑 IP 时，自动将该电脑添加到“默认组”电脑列表中。单击菜单[电脑管理/自动发现]，或者在电脑列表单击鼠标右键，单击菜单[自动发现]，选中后的菜单项前面将带勾，表示自动发现功能已经启用，未带勾表示没有启用。如下图所示，自动发现功能已经开启：

如果开启了自动发现功能，对于新发现的 IP 地址，软件将自动检测它的 MAC 地址和电脑名称，并添加到“默认组”电脑列表中。该功能等同于操作选项中“自动发现电脑并添加到默认组”选项。

提示：软件安装完成后第一次运行时，[自动发现]功能默认开启。

4.8. 分组管理

软件提供了电脑分组管理功能，每台电脑都属于唯一的一个组，管理员可以对不同的组设置不同的监控策略。在组列表中选中某一组后，电脑列表中将显示该组的所有电脑信息。如下图所示：



系统安装后自动创建“默认组”，管理员不能修改和删除该组。系统将自动发现和扫描到的电脑添加到“默认组”中。要更改电脑所属的组，可以选择要更改的电脑，然后用鼠标拖动到目标组中。

提示：默认组不仅包含该组下属的所有电脑，同时其他所有未显示在电脑列表中的未知电脑也受默认组策略的影响。

以下是对组的一些常用操作：

1、增加分组

单击菜单[分组管理/增加分组]，或者在组列表中单击鼠标右键，单击菜单[增加分组]，在弹出的对话框中输入组名称，单击<确定>按钮。

2、修改分组

在组列表中选择要修改的组，单击菜单[分组管理/分组属性]，或者在组列表中单击鼠标右键，单击菜单[分组属性]，在弹出的对话框中更改组名称，单击<确定>按钮。

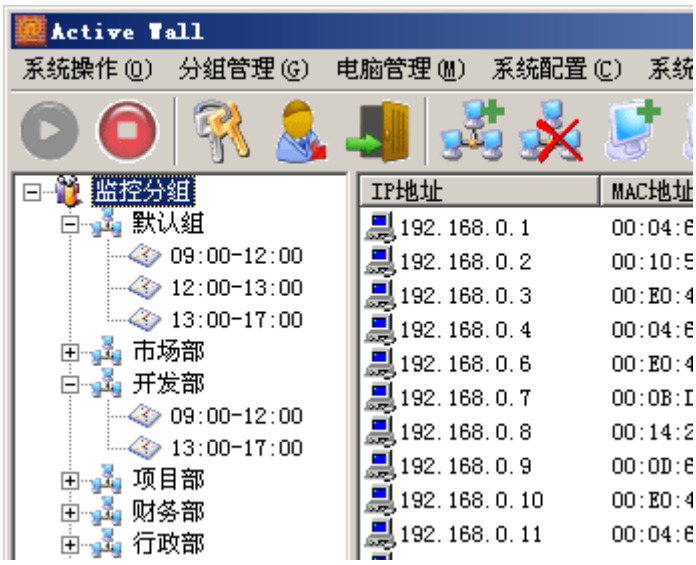
3、删除分组

在组列表中选择要删除的组，单击菜单[分组管理/删除分组]，或者在组列表中单击鼠标右键，单击菜单[删除分组]。

提示：删除组后该组的电脑将自动转移到默认组。默认组禁止删除。

4.9. 时段管理

软件提供了时段管理功能，每个分组下可以增加多个时段。管理员可以对不同的时段设置不同的监控策略。该分组下的电脑在该时间段内，自动应用该时段的策略。如下图所示：



1、增加时段

在组列表中选择要增加时段的组，单击菜单[分组管理/增加时段]，或者在组列表中单击鼠标右键，单击菜单[增加时段]，在弹出的对话框中输入时间段，单击<确定>按钮。

提示：新增加的时段将自动导入所在分组的策略。

2、修改时段

在组列表中选择要修改的时段，单击菜单[分组管理/时段属性]，或者在组列表中单击鼠标右键，单击菜单[时段属性]，在弹出的对话框中更改时间段，单击<确定>按钮。

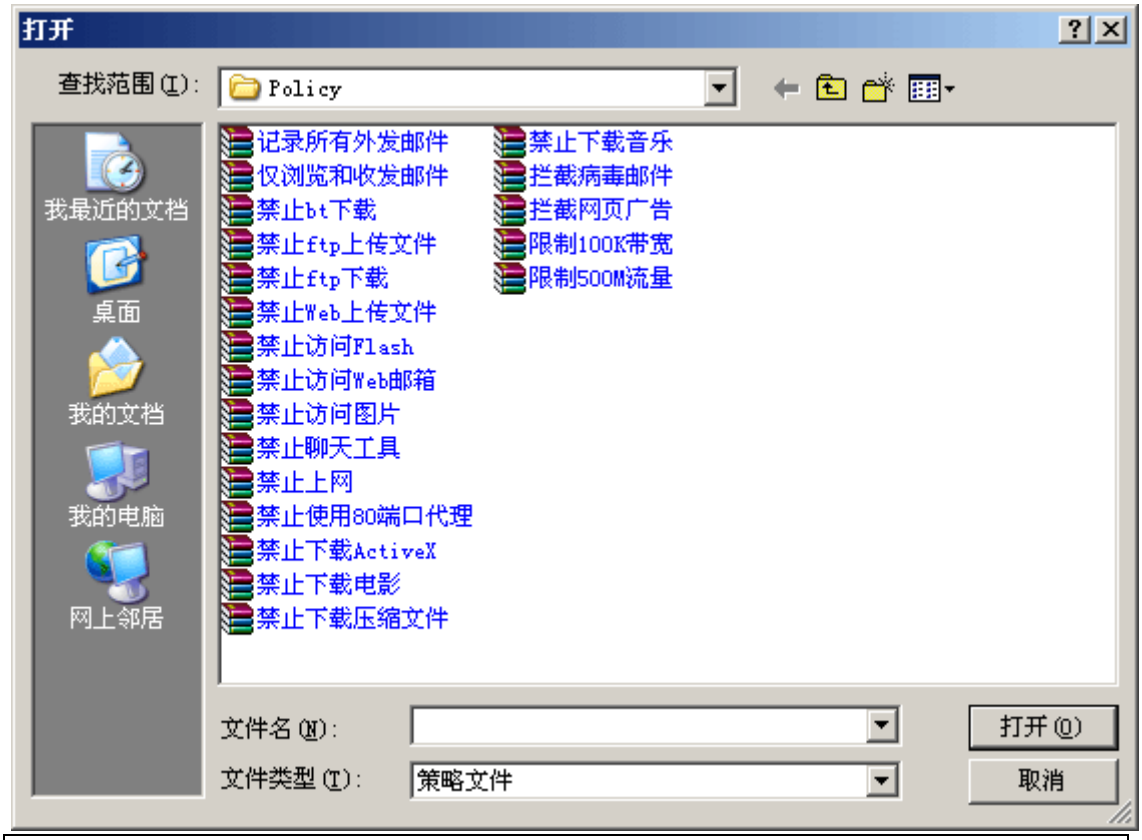
3、删除时段

在组列表中选择要删除的时段，单击菜单[分组管理/删除时段]，或者在组列表中单击鼠标右键，单击菜单[删除时段]。

4.10. 策略管理

1、导入策略

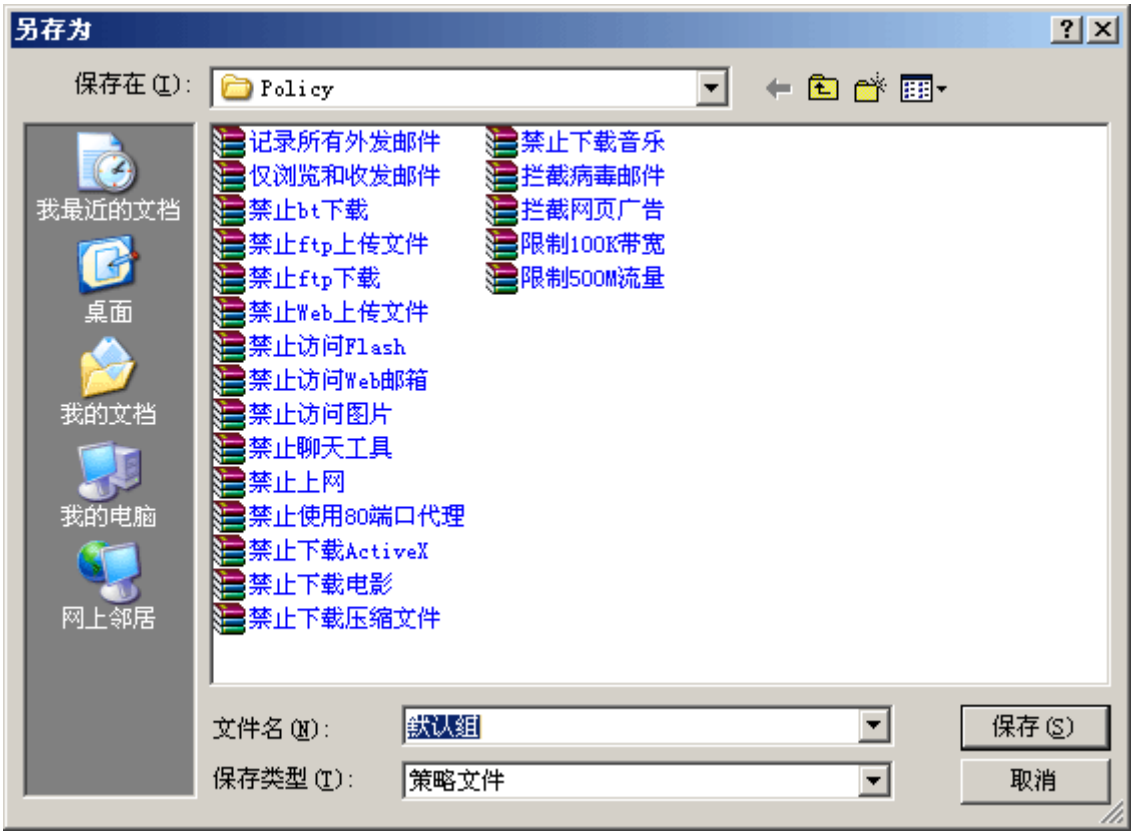
在组列表中选择要导入策略的组或时段，单击菜单[分组管理/导入策略]，或者在组列表中单击鼠标右键，单击菜单[导入策略]，选择所需导入的策略，单击<打开>按钮。



提示：导入的策略默认加在各模块的末尾。用户可能需要进入各模块配置界面，调整相应的顺序以使策略生效。更多的策略文件可以从 Active Wall 网站下载，详情请看联系方式。

2、导出策略

在组列表中选择要导出策略的组或时段，单击菜单[分组管理/导出策略]，或者在组列表中单击鼠标右键，单击菜单[导出策略]，填写导出策略文件名，单击<保存>按钮。



3、清除策略

在组列表中选择要清除策略的组或时段，单击菜单[分组管理/清除策略]，或者在组列表中单击鼠标右键，单击菜单[清除策略]。

注意：清除策略会清空该组所有策略设置，恢复到无任何策略的初始状态。

4、策略配置

在组列表中选择要配置策略的组或时段，单击菜单[分组管理/策略配置]，在子菜单中选择要配置的插件模块。或者在组列表中单击鼠标右键，单击菜单[策略配置]，在子菜单中选择要配置的插件模块。即可对该组或该时段配置与该插件相关的策略。

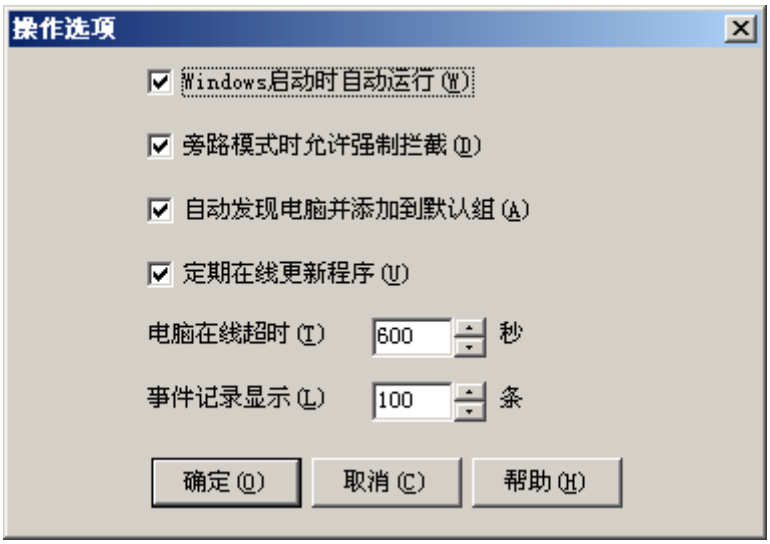
4.11. 选择网卡

系统提供网关、网桥、旁路和单机四种模式，请根据当前的网络拓扑结构选择正确的网络监控模式（详情请看网络环境 ）。单击菜单[系统配置/选择网卡]，在弹出的对话框中选择相应的监控模式，在[MAC 地址]列表中选择连接到局域网的内部网卡，并填写要监控的内部局域网地址范围。如果未指定局域网地址范围，则由程序自动识别判断。单击<确定>按钮保存配置。

注意：选择的监控模式必须要和当前的网络结构相匹配，选择的网卡必须要是连接局域网的内部网卡，否则程序将无法正常工作。

4.12. 操作选项

软件的基本运行参数可以在操作选项中更改。单击菜单[系统配置/操作选项]可以打开操作选项配置界面，如下图所示：



各参数选项说明如下：

1. Windows 启动时自动运行：

勾选该项，则软件随着 Windows 操作系统启动而自动运行(用户无需登录)。未勾选，则 Windows 操作系统启动后，用户需要手动启动软件。

2. 旁路模式时启用数据转发：

该选项仅当软件以旁路模式运行时有效。旁路模式由于网络结构的限制，有一定的局限性。勾选该项，则允许软件对局域网内其他电脑的上网数据进行中转。未勾选，则不允许软件启用数据转发。数据转发采用 ARP 欺骗方式，对网络性能有一定影响，因此只适合小型网络。

3. 自动发现电脑并添加到默认组

该选项等同于自动发现菜单选项。勾选该项，当系统检测到网络有新的电脑 IP 时，自动将该电脑添加到“默认组”电脑列表中。未勾选，则新的电脑不会自动添加到默认组，但仍然受默认组策略的影响。

4. 定期在线更新程序：

勾选该项，则允许软件定期连接到更新服务器上检测最新的软件版本信息。当检测到有新的版本，系统会自动从网上进行下载。未勾选，则软件不会自动更新，用户需要手动单击[在线更新]菜单以获取软件最新版本。

5. 电脑在线超时：

调整该参数，将影响电脑列表中显示的电脑在线状态。当系统在指定的时间内未检测到从该电脑发出的数据包，则认为该电脑已经不在线。

6. 事件记录显示：

调整该参数，将影响事件记录列表中显示的记录条数。事件记录列表用于滚动显示最新的事件，当事件记录超过该数目时，最先的纪录将被从列表中移除。

4.13. 插件管理

软件的功能模块以插件的方式提供，管理员可动态装载或卸载功能插件。单击菜单[系统配置/插件管理]，界面如下图所示：

在插件模块名称前打勾表示加载该模块，去掉勾表示不加载该模块。上下移动按钮用于调整插件的装载顺序，模块的先后顺序确定了数据包过滤匹配的先后顺序。

为了加快过滤的速度提升系统的性能，建议只加载需要的模块，停止暂时未用到的模块。各模块的先后过滤顺序对系统也有一定影响，系统安装时已经设定了最优的顺序。

选中模块后单击<配置>按钮，或在模块名称上双击鼠标左键即可弹出该模块的配置对话框。配置完成后，在插件管理对话框上单击<确定>按钮，各模块配置即刻生效。

第五章 插件操作说明

策略说明：

策略决定了软件对监控到的数据包在符合配置条件时所采取的动作，共有如下 5 种处理动作：

1. 通过：表示允许数据包通过，不产生事件记录
2. 拦截：表示阻止数据包通过，不产生事件记录
3. 通过并记录：表示允许数据包通过，同时产生事件记录
4. 通过并保存：表示允许数据包通过，同时产生事件记录，并保存当前会话的相关内容（例如 HTTP 过滤保存网页内容，SMTP 过滤保存发送的邮件内容，POP3 过滤保存接收的邮件内容等。）
5. 拦截并记录：表示阻止数据包通过，同时产生事件记录

通配符说明：

Active Wall 支持的通配符有两个：“*”号和“?”号。“*”表示零至多个字符，“?”表示一个字符。例如：

1. comput* 可匹配 computer(*代表 er)、computation(*代表 ation)、computing(*代表 ing)
2. wom?n 可匹配 woman(?代表 a)、women(?代表 e)
3. “*”号和“?”号可混合使用，*.sin?.* 可匹配 news.sina.com.cn(*代表 news，?代表 a， *代表 com.cn)、www.sino.com(*代表 www，?代表 o，*代表 com)

事件记录说明：

所谓事件记录是各监控模块检测到数据包符合配置条件时所产生的信息，这些信息会滚动显示在程序主界面上。如果日志文件输出或日志数据库输出模块已加载，则这些事件记录会保存到文件或数据库中供日后查询。

5.1. 网络身份验证

启用网络身份验证后，要求用户输入正确的账号密码才可访问互联网。Active Wall 网络身份验证模块支持多种验证方式：

1. 基于 IIS 的基本身份验证、Windows 集成身份验证、摘要身份验证。
2. 基于 Apache、Netscape 等其他 WEB 服务器的各种身份验证。
3. 基于 ASP、PHP、CGI、Java、.NET 的网页表单验证。
4. 基于 C/S 结构的自定义身份验证。

操作说明：

1. 在[监控分组]里选择要设置网络身份验证的电脑组。
2. 输入验证服务器的 IP 和端口。
3. 勾选[启用网络身份验证]，表示对该组启用身份验证；否则表示不对该组启用身份验证。
4. 单击<确定>按钮保存当前设置，单击<取消>按钮取消当前设置。

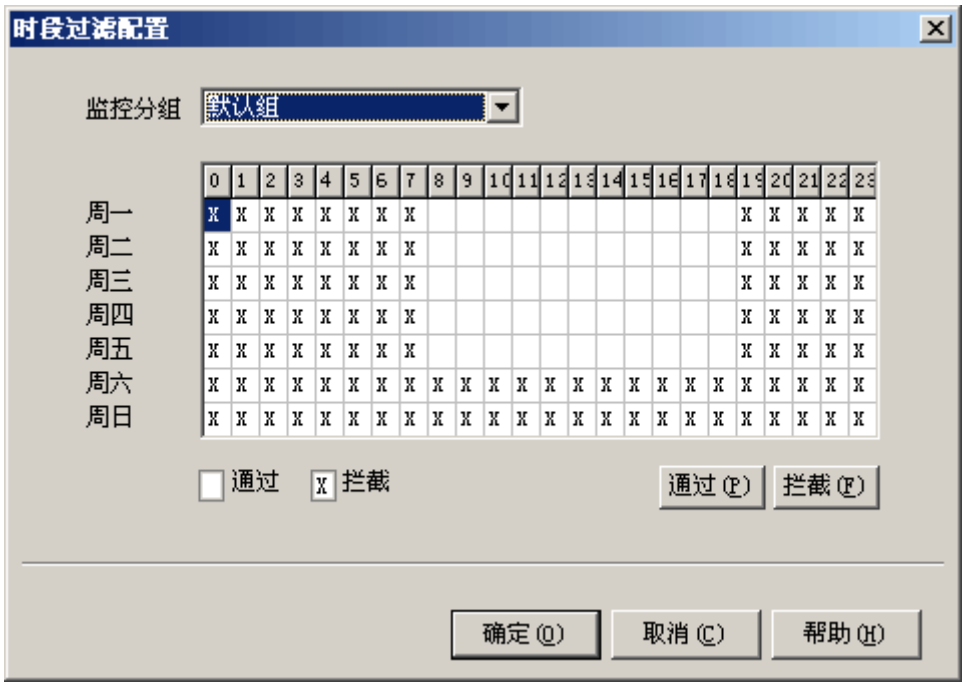
补充说明：

1. [服务器 IP]：验证服务器的 IP 地址。服务器 IP 不能采用 127.0.0.1，而必须填写对内网其它电脑可以识别的有效 IP 地址。
2. [端口]：验证服务器的端口。如果是 WEB 身份验证，通常为 80。
3. 服务器 IP 和端口为所有组共享的全局参数。这意味着：如果您如果修改了某一组的服务器 IP 和端口，其它各组也同样受影响。
4. 局域网内部用户访问验证服务器，必须要通过 Active Wall 所在的网关，否则网络身份验证模块将无法正常工作。
5. 验证服务器配置：由于 Active Wall 支持的身份验证方式众多，不能一一罗列，详情请看技术论坛。

提示：如使用 WEB 身份验证请尽量不要采用静态网页，防止 IE 使用缓存而导致 Active Wall 无法检测到验证数据包。

5.2. 时段过滤

时段过滤模块可以按周设置一天内允许上网的时间段，最小单位为小时。配置对话框如下所示：



操作说明：

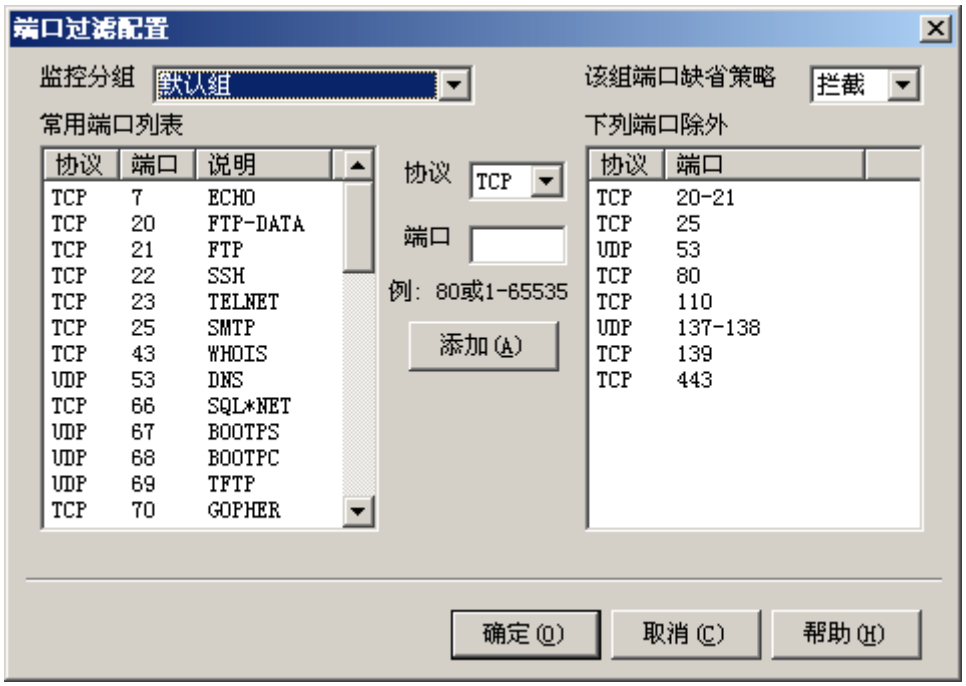
1. 在[监控分组]里选择要设置时段过滤的电脑组。
2. 用鼠标单击选中视图上的方格（可以按住鼠标左键拖动选中多个方格），每个方格代表一星期中某天的某个小时。要禁止该组在该时间上网，单击<拦截>按钮即可，视图上将用“X”表示禁止上网的时间。单击<通过>按钮表示该时间允许上网，视图上将用空白表示允许上网的时间。
3. 单击<确定>按钮保存当前设置，单击<取消>按钮取消当前设置。

补充说明：

1. 时段视图：时段视图为一个 24*7 的方格视图。横坐标以小时为单位，范围从 0~23；纵坐标以天为单位，范围从周一~周日（ISO 8601 标准）。视图中的每个方格表示一个小时的时间。例如：（横坐标：0，纵坐标：周一）表示周一的 0 点至 1 点；（横坐标：17，纵坐标：周五）表示周五的 17 点至 18 点。
2. 时段过滤模块仅限制用户是否能够上网，其最小单位为小时。如果要根据时间做更细致的监控策略请采用分组中的时段管理功能。

5.3. 端口过滤

端口过滤模块通过开放或关闭一些端口，允许内部用户使用或禁止使用互联网上部分服务。配置对话框如下所示：



操作说明：

1. 在[监控分组]里选择要设置端口过滤的电脑组。
2. 在[该组端口缺省策略]中选择该组的缺省策略。
3. 双击[常用端口列表]中的常用端口可以把该端口添加到右边的[下列端口除外]列表中。
4. 如果要添加的端口不在[常用端口列表]中，可以先在[协议]下拉列表中选择协议，然后在[端口]输入框中输入端口或端口范围，单击<添加>按钮添加到[下列端口除外]列表。
5. 在右边[下列端口除外]列表中选择要删除的端口或端口范围，单击鼠标右键，单击[删除]菜单，可删除当前选择的端口或端口范围。
6. 单击<确定>按钮保存当前设置，单击<取消>按钮取消当前设置。

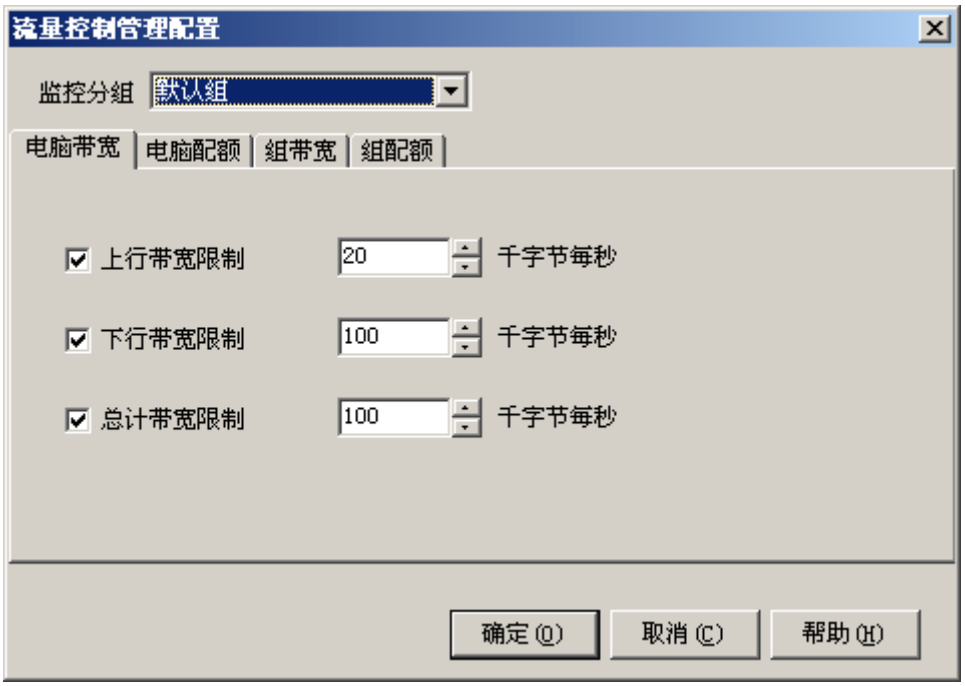
补充说明：

1. [该组端口缺省策略]与[下列端口除外]列表有互斥关系。如果缺省策略为[拦截]，则[下列端口除外]列表中出现的端口为[通过]。如果缺省策略为[通过]，则[下列端口除外]列表中出现的端口为[拦截]。
2. 添加端口时，如果端口与[下列端口除外]列表中已有的端口号连续，且协议相同，将自动合并为一条端口范围。

注意：UDP 53 端口为 DNS 域名解析服务端口，屏蔽该端口可能导致其他网络应用无法正常运行。

5.4. 流量控制

流量控制模块用于控制网络内部每台电脑或全组的传输速度，及设置网络内部每台电脑或全组每天允许的最大网络流量。配置对话框如下所示：



操作说明：

1. 在[监控分组]里选择要设置流量控制的电脑组。
2. [电脑带宽]限制：限制当前组每台电脑的网络传输速度，选中要限制的项目，输入数值。可分别对上行、下行、总计带宽进行限制。
3. [电脑配额]限制：限制当前组每台电脑每天的总流量，选中要限制的项目，输入数值。可分别对上行、下行、总计配额进行限制。
4. [组带宽]限制：限制当前组全部电脑累加的网络传输速度，选中要限制的项目，输入数值。可分别对上行、下行、总计带宽进行限制。
5. [组配额]限制：限制当前组全部电脑累加的每天的总流量，选中要限制的项目，输入数值。可分别对上行、下行、总计配额进行限制。
6. 单击<确定>按钮保存当前设置，单击<取消>按钮取消当前设置。

补充说明：

1. 带宽：指网络传输速度，以千字节每秒为单位。
2. 配额：指每天传输的流量，以兆字节每天为单位。
3. 上行：指局域网发送给互联网的字节。
4. 下行：指局域网从互联网接收的字节。
5. 总计：指上行、下行累加的字节。
6. 此处统计的字节不仅包含 TCP、UDP 的内容长度，而且包括以太网头部、IP 头、TCP 头的数据包总长度。

5.5. 实时流量显示

实施流量显示模块用于设置主界面中[流量显示]的显示方式，管理员可以设置显示何种流量统计图。配置对话框如下所示：

操作说明：

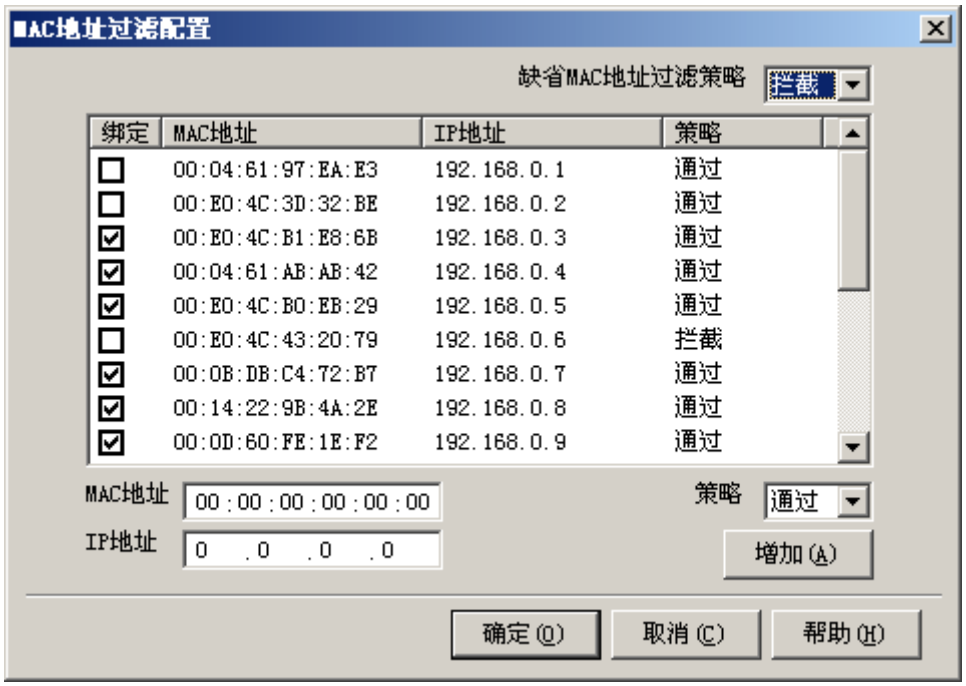
1. 在[显示以下协议]中打勾选中的选项表示显示该项的流量统计图。
2. 在统计模式中选择按数据包个数统计还是按字节流量统计。
3. 在[显示峰值]中可以设置当前显示的最高峰值。
4. 单击<确定>按钮保存当前设置，单击<取消>按钮取消当前设置。

补充说明：

1. 总流量：表示经过服务器的所有协议的流量。
2. TCP：显示以传输控制协议(Transmission Control Protocol)方式经过服务器的流量。
3. UDP：显示以用户数据报协议(User Datagram Protocol)方式经过服务器的流量。
4. ICMP：显示以互联网控制信息协议(Internet Control Message Protocol)方式经过服务器的流量。
5. IGMP：显示以互联网群组管理协议(Internet Group Management Protocol)方式经过服务器的流量。
6. 统计模式可按数据包个数统计也可按字节长度统计。按数据包个数统计时，显示在主界面上的为流经服务器的数据包个数(P=Packet)；按字节流量统计时，显示在主界面上的为流经服务器的千字节长度(K=KByte)。
7. 按字节流量统计时，统计的字节不仅包含 TCP、UDP 的内容长度，而且包括以太网头部、IP 头、TCP 头的数据包总长度。

5.6. MAC 地址过滤

MAC 地址过滤模块可以设定内部电脑按网卡 MAC 地址过滤，并能将 MAC 地址绑定固定的 IP 地址。配置对话框如下所示。



操作说明：

1. [缺省 MAC 地址过滤策略]中选择默认策略为通过或拦截。
2. 在列表框选择要做更改的项目，单击鼠标右键，在弹出菜单中可以单击[地址绑定]绑定当前所选地址；单击[取消绑定]取消所选地址的绑定，单击[删除地址]删除当前所选地址;单击[导入地址]可以导入在主程序界面中所有电脑的 MAC 与 IP 地址。
3. 要编辑某项，可在列表中双击该项，编辑完成后单击<增加>按钮保存。
4. 要添加新地址，先输入[MAC 地址]和[IP 地址]，在[策略]中选择策略，然后单击<增加>按钮。
5. 单击<确定>按钮保存当前设置，单击<取消>按钮取消当前设置。

补充说明：

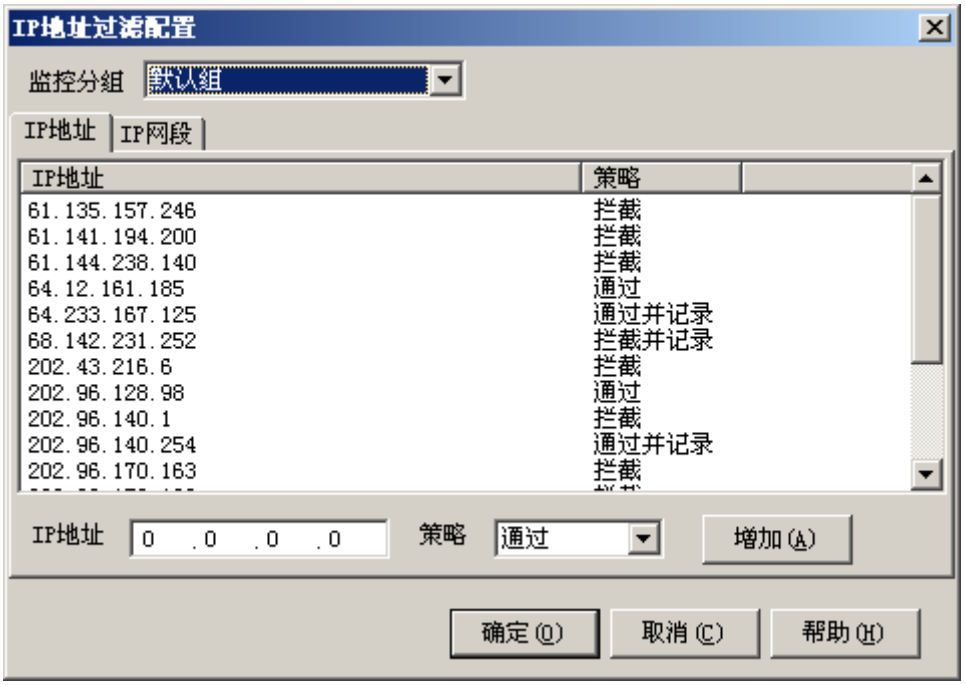
1. [缺省 MAC 地址过滤策略]：表示没有出现在 MAC 地址列表框中的所有其他 MAC 地址的处理策略。
2. 在 MAC 地址列表框中，如果某一 MAC 地址的策略为通过，则允许该 MAC 地址通过；并检查[地址绑定]策略。
3. 在 MAC 地址列表框中，如果某一 MAC 地址的策略为拦截，则禁止该 MAC 地址通过。
4. [地址绑定]：勾选的项目表示该 MAC 地址与 IP 地址是绑定的。地址绑定后，该 MAC 地址只能使用指定的 IP 地址，如果更改为其他的 IP 地址则不允许通过。
5. MAC 地址过滤模块只能应用于单一网段的网络环境中。

提示：MAC 地址是网卡的物理地址。由于软件以 IP 鉴别局域网用户，为防止用户随意更改 IP 地址，建议启用 MAC-IP 绑定功能。

注意：如果您的网络采用了 DHCP 服务器自动分配 IP 地址，请在 DHCP 服务器中为每个 MAC 地址指定固定的 IP 地址，再启用 MAC-IP 绑定。

5.7. IP 地址过滤

IP 地址过滤模块可以过滤内部电脑对互联网上的 IP、网段地址的访问。配置对话框如下所示：



操作说明：

1. 在[监控分组]里选择要设置 IP 地址过滤的电脑组。
2. 在列表框中双击左键，即可编辑选中的项目，单击<增加>按钮保存。
3. 添加 IP 过滤：选择[IP 地址]，输入 IP 地址，选择策略，单击<增加>按钮。
4. 添加网段过滤：选择[IP 网段]，输入网络号及掩码长度，选择策略，单击<增加>按钮。
5. 在列表框选择要更改的项目，单击鼠标右键，单击菜单[删除]可删除当前选择的项目。
6. 单击<确定>按钮保存当前设置，单击<取消>按钮取消当前设置。

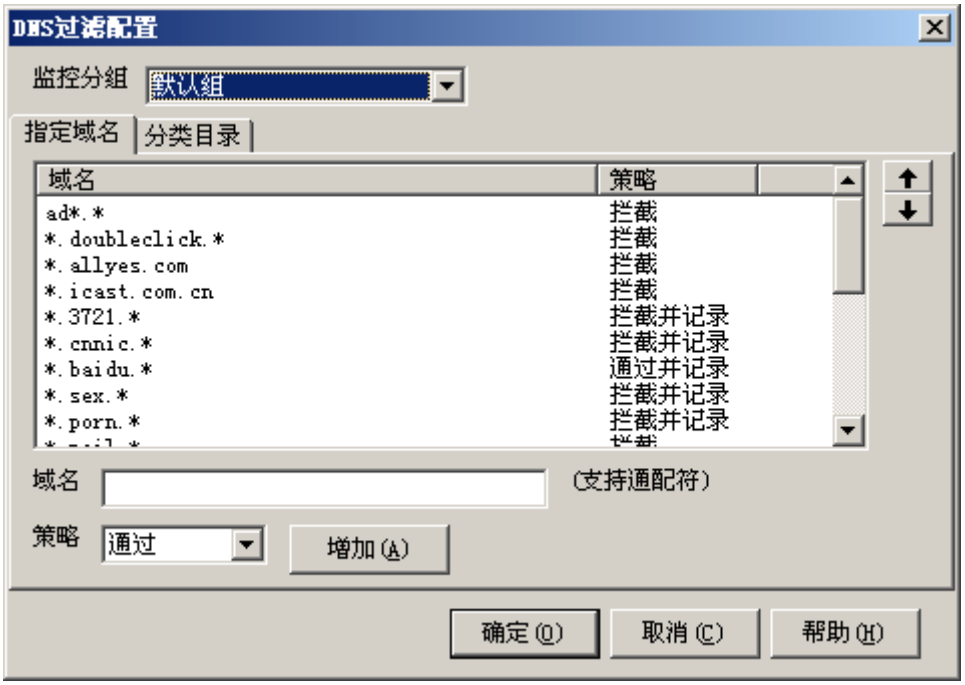
补充说明：

1. [IP 网段]：采用 CIDR 网络前缀表示法(RFC 1878)。如网络号 210.31.233.0，子网掩码 255.255.255.0 可表示成 210.31.233.0/24；网络号 166.133.0.0，子网掩码 255.255.0.0 可表示成 166.133.0.0/16；网络号 192.168.0.0，子网掩码 255.255.255.240 可表示成 192.168.0.0/28 等。
2. 过滤顺序按 IP、网段范围从小到大进行过滤。例如 IP 为"61.141.238.1"策略为"通过"，而 IP 网段"61.141.238.0/24"策略为"拦截"，则表示 61.141.238.0/24 的网段中只有 61.141.238.1 能通过，其它 IP 都被拦截。

提示：本模块过滤的 IP、网段是指互联网上的地址，而非局域网内部 IP。要过滤内部 IP 请在主程序中为该 IP 所属的组设定过滤策略即可。

5.8. DNS 过滤

DNS 过滤模块可以过滤内部电脑向互联网发出的域名查询请求（DNS 协议）。配置对话框如下所示：



操作说明：

1. 在[监控分组]里选择要设置 DNS 过滤的电脑组。
2. 在输入框中输入内容，在[策略]中选择相应的策略，单击<增加>按钮增加或保存输入框中的内容。
3. 在指定域名列表框中选择要更改的项目，单击<向上>或<向下>箭头按钮可移动该项目的先后顺序。
4. 在指定域名列表框中选择要更改的项目，单击鼠标右键，单击[删除]菜单可删除当前选择的项目。
5. [指定域名]：在[域名]输入框中输入域名，在[策略]中选择处理策略，然后单击<增加>按钮即可。当用户访问的域名与列表中的条目相匹配时执行对应策略，域名过滤支持通配符。
6. [域名分类]：在[分类目录]列表框中选择相应分类条目，在[策略]中选择处理策略，然后单击<更新>按钮。或选择相应分类，单击右键选择处理策略。当用户访问的域名与列表中的域名分类库地址相匹配时执行对应策略。
7. 单击<确定>按钮保存当前设置，单击<取消>按钮取消当前设置。

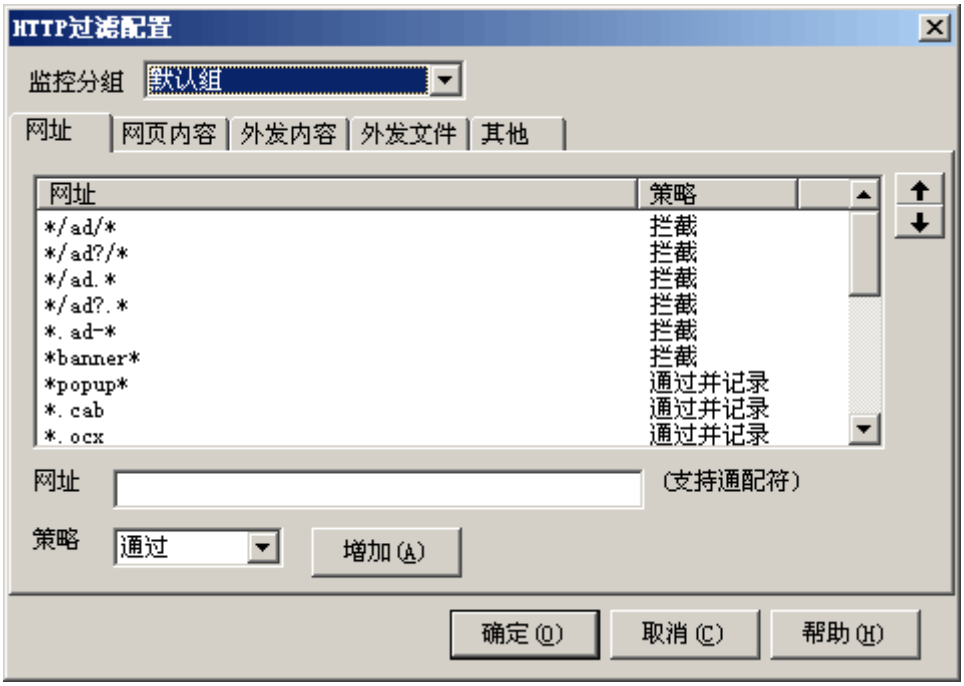
补充说明：

1. [指定域名]过滤按从上到下的顺序过滤，域名过滤支持通配符。例如首条（域名“www.google.com”、策略“通过”），第二条（域名“*.google.*”、策略“拦截”），表示只有“www.google.com”能通过，而其它包含“.google.”的域名都被拦截。
2. 域名过滤顺序为先匹配[指定域名]，再匹配[域名分类]。如果域名与[指定域名]中某一项目匹配则立即应用该项目策略，而不再查询[域名分类]。

提示：电脑在解析域名时，首先在本地的 DNS 缓存中查找，如果找不到才向外发送域名查询数据包，否则直接将缓存中的 DNS 解析项返回。因此对 DNS 域名进行过滤时有一定的滞后性，新加入的策略可能不会立即影响到被监控电脑，须等这些电脑上的 DNS 缓存过期后才能生效。

5.9. HTTP 过滤

HTTP 过滤模块用于对超文本传送协议（HTTP）进行过滤，该模块可以根据网址、网页内容、外发内容、外发文件等设定过滤条件。配置对话框如下所示：



操作说明：

1. 在[监控分组]里选择要设置 HTTP 过滤的电脑组。
2. 在输入框中输入内容，在[策略]中选择相应的策略，单击<增加>按钮增加或保存输入框中的内容。
3. 在列表框中选择要更改的项目，单击<向上>或<向下>箭头按钮可移动该项目的过滤先后顺序。
4. 在列表框中选择要更改的项目，单击[删除]菜单可删除当前选择的项目。
5. [网址]：在[网址]输入框中输入内容，该地址不包含“http://”前缀。在[策略]中选择相应的策略，单击<增加>按钮增加或保存输入框中的内容。当用户访问的网页地址与列表中的条目相匹配时执行对应策略，网址过滤支持通配符。
6. [网页内容]：在[关键字]输入框中输入内容，在[策略]中选择相应的策略，单击<增加>按钮增加或保存输入框中的内容。当用户访问的网页内容包含有列表中的条目时执行对应策略。
7. [外发内容]：在[关键字]输入框中输入内容，在[策略]中选择相应的策略，单击<增加>按钮增加或保存输入框中的内容。当用户通过浏览器外发的内容包含有列表中的条

目时执行对应策略。

8. [外发文件]：在[文件名]输入框中输入内容，在[策略]中选择相应的策略，单击<增加>按钮增加或保存输入框中的内容。当用户通过浏览器外发的文件名与列表中的条目相匹配时执行对应策略，外发文件过滤支持通配符。
9. [禁止 HTTP 隧道代理]：选中时禁止用户使用代理服务器或非 HTTP 协议的客户端软件通过 HTTP 端口访问互联网。
10. [禁止以 IP 访问主机]：选中时禁止用户以 IP 形式（如：http://64.233.189.22）直接访问服务器，而必须以域名形式访问（如：http://www.google.com）。
11. [限制外发内容大小]：选中该选项，在同一行输入要限制的内容大小数值(千字节)。启用限制后，如果用户通过浏览器向外发送的内容超过设定的大小，该行为将被拦截。
12. [限制下载内容大小]：选中该选项，在同一行输入要限制的内容大小数值(千字节)。启用限制后，如果用户通过浏览器访问的网页或下载的文件超过设定的大小，该行为将被拦截。
13. [限制文件保存大小]：当应用“通过并保存”策略时，模块须对相关文件进行缓存。如果超过指定的大小则放弃缓存，防止文件占用过多的内存。该选项默认启用，默认大小为 5 兆。
14. 单击<确定>按钮保存当前设置，单击<取消>按钮取消当前设置。

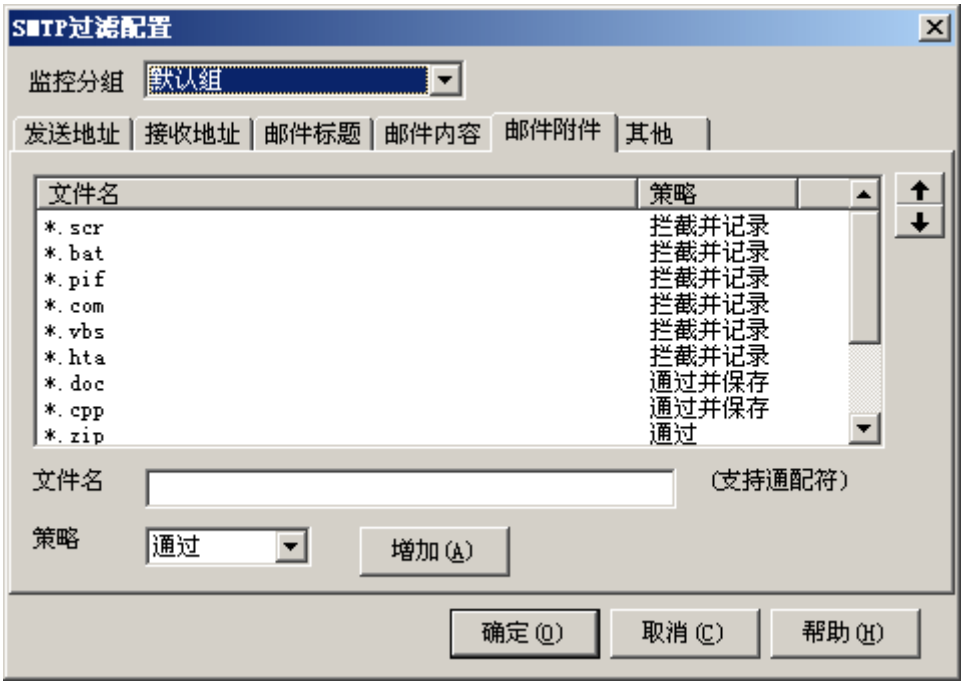
补充说明：

1. [网址]过滤按从上到下的顺序过滤，网址过滤支持通配符。例如首条（网址“admin.*”、策略“通过”），第二条（网址“ad*”、策略“拦截”），表示以“admin.”开始的网址能通过，而其它以“ad”开始的网址都被拦截。
2. [网页内容]过滤按从上到下的顺序过滤。例如首条（关键词“医学”、策略“通过”），第二条（关键词“性爱”、策略“拦截”），表示网页内容中包含“医学”的网页能通过，而其它网页内容中包含“性爱”的网页都被拦截。
3. [外发内容]过滤按从上到下的顺序过滤。例如首条（关键词“合同”、策略“拦截”），第二条（关键词“@”、策略“通过并保存”），表示外发内容中包含“合同”被拦截，而其它外发内容中包含“@”都允许通过并保存外发内容副本到硬盘。
4. [外发文件]过滤按从上到下的顺序过滤，外发文件过滤支持通配符。例如首条（文件名“*.doc”、策略“拦截”），第二条（文件名“*”、策略“通过并记录”），表示外发文件后缀名为“.doc”的被拦截，而其它外发文件都允许通过并记录相关事件。
5. 外发内容过滤仅对“HTTP-POST”协议有效，对“HTTP-GET”协议外发的内容请用网址过滤。
6. 对网页内容和外发内容过滤时，软件能自动识别 ANSI 和 UTF8 文本格式。
7. 在一次 HTTP 请求响应过程中包含了多次过滤，只要有一次过滤策略结果为“拦截”或“拦截并记录”，则本次连接将立即被结束。


提示：由于 HTTP 是互联网上最常用的协议，许多软件为了突破防火墙都采用 HTTP 隧道技术与外部联系。要禁止这些软件使用 HTTP 的 80 端口，只需启用[禁止 HTTP 隧道代理]即可。

5.10. SMTP 过滤

SMTP 过滤模块可对通过 SMTP 协议发送的邮件进行过滤，该模块可以根据外发邮件的发送地址、接收地址、邮件标题、邮件内容、邮件附件和邮件大小等设定过滤条件。配置对话框如下所示：



操作说明：

1. 在[监控分组]里选择要设置 SMTP 过滤的电脑组。
2. 单击<增加>按钮增加或保存输入框中的内容。
3. 在列表框中选择要更改的项目，单击<向上>或<向下>箭头按钮可移动该项目的过滤先后顺序。
4. 在列表框中选择要更改的项目，单击鼠标右键，单击[删除]菜单可删除当前选择的项目。
5. [发送地址]：在[发送地址]输入框中输入内容，在[策略]中选择处理策略，然后单击<增加>按钮即可。当外发邮件的发送地址与列表中的条目相匹配时执行对应策略，发送地址过滤支持通配符。
6. [接收地址]：在[接收地址]输入框中输入内容，在[策略]中选择处理策略，然后单击<增加>按钮即可。当外发邮件的接收地址与列表中的条目相匹配时执行对应策略，接收地址过滤支持通配符。
7. [邮件标题]：在[邮件标题]输入框中输入内容，在[策略]中选择处理策略，然后单击<增加>按钮即可。当外发邮件的邮件标题与列表中的条目相匹配时执行对应策略，邮件标题过滤支持通配符。
8. [邮件内容]：在[关键字]输入框中输入内容，在[策略]中选择处理策略，然后单击<增加>按钮即可。当外发邮件的邮件内容包含有列表中的条目时执行对应策略。
9. [邮件附件]：在[文件名]输入框中输入内容，在[策略]中选择处理策略，然后单击<增加>按钮即可。当外发邮件的邮件附件与列表中的条目相匹配时执行对应策略，邮件附件过滤支持通配符。

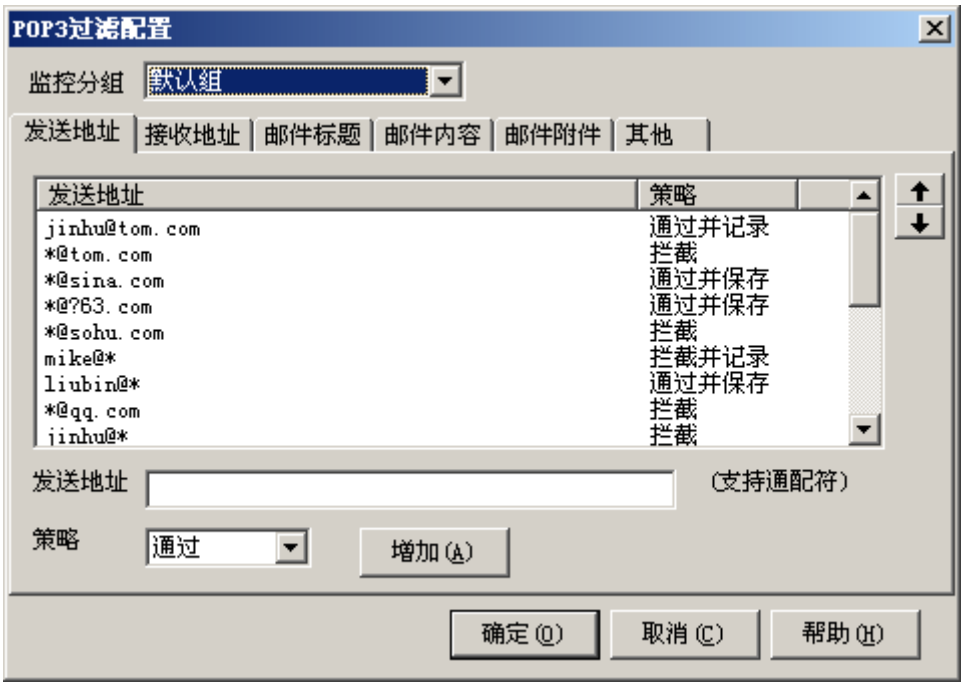
10. [限制外发邮件大小]：选中该选项，在同一行输入要限制的内容大小数值(千字节)。启用限制后，如果用户外发的邮件大小超过设定的大小，该行为将被拦截。
11. [限制文件保存大小]：当应用“通过并保存”策略时，模块须对相关文件进行缓存。如果超过指定的大小则放弃缓存，防止文件占用过多的内存。该选项默认启用，默认大小为 5 兆。
12. 单击<确定>按钮保存当前设置，单击<取消>按钮取消当前设置。

补充说明：

1. SMTP 过滤模块仅对通过 SMTP 协议发送的邮件有效，要过滤 WEB 发送的邮件请用 HTTP 过滤模块。
2. [发送地址]过滤按从上到下的顺序过滤，发送地址过滤支持通配符。
3. [接收地址]过滤按从上到下的顺序过滤，接收地址过滤支持通配符。
4. [邮件标题]过滤按从上到下的顺序过滤，邮件标题过滤支持通配符。
5. [邮件内容]过滤按从上到下的顺序过滤。
6. [邮件附件]过滤按从上到下的顺序过滤，邮件附件过滤支持通配符。
7. 在一次 SMTP 邮件发送过程中包含了多次过滤，只要有一次过滤策略结果为“拦截”或“拦截并记录”，则本次连接将立即被结束。

5.11. POP3 过滤

POP3 过滤模块可对通过 POP3 协议接收的邮件进行过滤，该模块可以根据接收邮件的发送地址、接收地址、邮件标题、邮件内容、邮件附件和邮件大小等设定过滤条件。配置对话框如下所示：



操作说明：

1. 在[监控分组]里选择要设置 POP3 过滤的电脑组。
2. 单击<增加>按钮增加或保存输入框中的内容。
3. 在列表框中选择要更改的项目，单击<向上>或<向下>箭头按钮可移动该项目的过滤

先后顺序。

4. 在列表框中选择要更改的项目，单击鼠标右键，单击[删除]菜单可删除当前选择的项目。
5. [发送地址]：在[发送地址]输入框中输入内容，在[策略]中选择处理策略，然后单击<增加>按钮即可。当接收邮件的发送地址与列表中的条目相匹配时执行对应策略，发送地址过滤支持通配符。
6. [接收地址]：在[接收地址]输入框中输入内容，在[策略]中选择处理策略，然后单击<增加>按钮即可。当接收邮件的接收地址与列表中的条目相匹配时执行对应策略，接收地址过滤支持通配符。
7. [邮件标题]：在[邮件标题]输入框中输入内容，在[策略]中选择处理策略，然后单击<增加>按钮即可。当接收邮件的邮件标题与列表中的条目相匹配时执行对应策略，邮件标题过滤支持通配符。
8. [邮件内容]：在[关键字]输入框中输入内容，在[策略]中选择处理策略，然后单击<增加>按钮即可。当接收邮件的邮件内容包含有列表中的条目时执行对应策略。
9. [邮件附件]：在[文件名]输入框中输入内容，在[策略]中选择处理策略，然后单击<增加>按钮即可。当接收邮件的邮件附件与列表中的条目相匹配时执行对应策略，邮件附件过滤支持通配符。
10. [限制接收邮件大小]：选中该选项，在同一行输入要限制的内容大小数值(千字节)。启用限制后，如果用户接收的邮件大小超过设定的大小，该行为将被拦截。
11. [限制文件保存大小]：当应用“通过并保存”策略时，模块须对相关文件进行缓存。如果超过指定的大小则放弃缓存，防止文件占用过多的内存。该选项默认启用，默认大小为 5 兆。
12. 单击<确定>按钮保存当前设置，单击<取消>按钮取消当前设置。

补充说明：

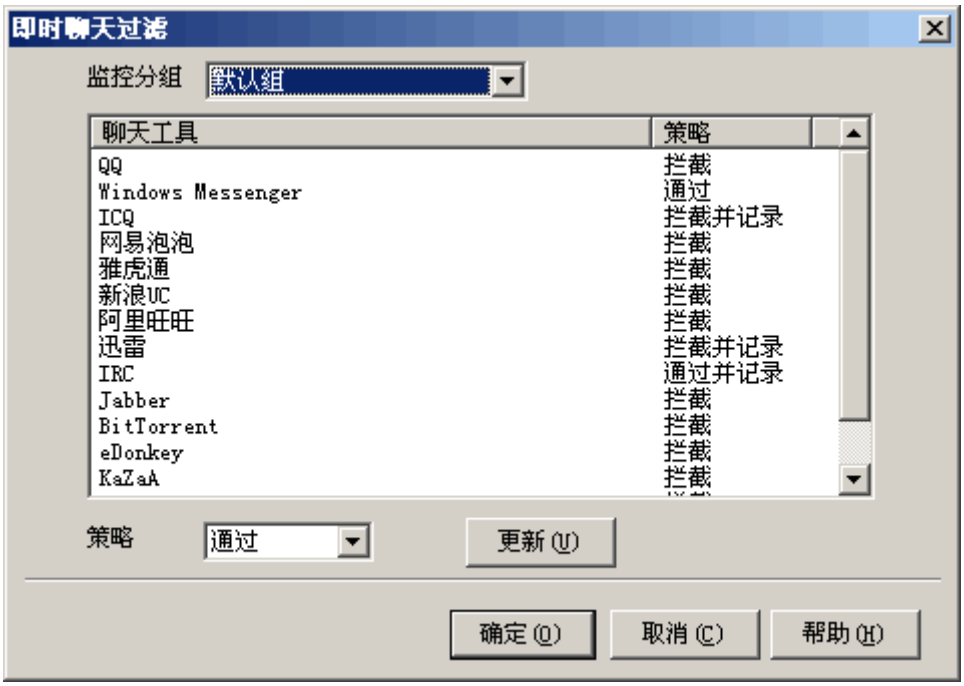
1. POP3 过滤模块仅对通过 POP3 协议接收的邮件有效，要过滤 WEB 接收的邮件请用 HTTP 过滤模块。
2. [发送地址]过滤按从上到下的顺序过滤，发送地址过滤支持通配符。
3. [接收地址]过滤按从上到下的顺序过滤，接收地址过滤支持通配符。
4. [邮件标题]过滤按从上到下的顺序过滤，邮件标题过滤支持通配符。
5. [邮件内容]过滤按从上到下的顺序过滤。
6. [邮件附件]过滤按从上到下的顺序过滤，邮件附件过滤支持通配符。
7. 在一次 POP3 邮件接收过程中包含了多次过滤，只要有一次过滤策略结果为“拦截”或“拦截并记录”，则本次连接将立即被结束。

 注意：POP3 过滤模块不会主动删除被拦截的邮件。而邮件客户端软件通常按队列顺序接收邮件，这可能导致该账户后续的邮件无法接收，除非用户手动删除 POP3 服务器上被拦截的邮件。

5.12. 即时聊天过滤

即时聊天过滤模块用于过滤 QQ、MSN、ICQ、网易泡泡、雅虎通、新浪 UC、阿里旺旺、迅雷、IRC、Jabber、BitTorrent、eDonkey 等即时通讯工具和 P2P 工具。配置对话框如

下所示：



操作说明：

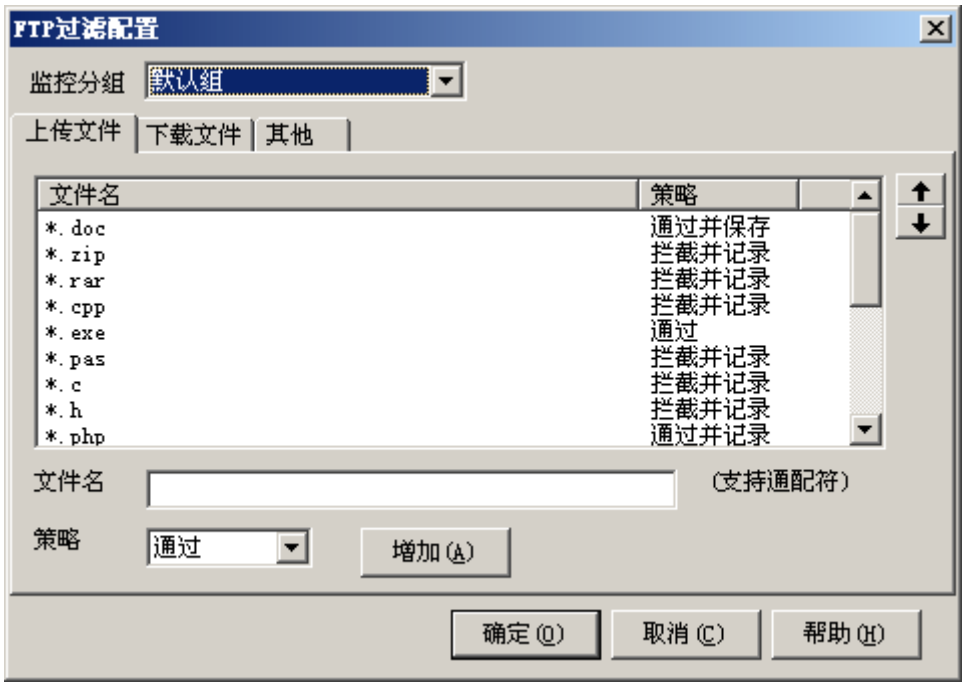
1. 在[监控分组]里选择要设置即时聊天过滤的电脑组。
2. 在[聊天工具]列表框中选择相应聊天工具条目，在[策略]中选择处理策略，然后单击<更新>按钮。或选择相应聊天工具，单击右键选择处理策略。当用户使用聊天工具与列表聊天工具条目相匹配时执行对应策略。
3. 单击<确定>按钮保存当前设置，单击<取消>按钮取消当前设置。

补充说明：

1. 即时聊天过滤模块通过过滤一些常用即时通讯工具的端口、域名、IP 列表实现过滤功能。
2. 大多数即时聊天软件都支持代理或 HTTP 隧道的方式登录，要彻底拦截聊天工具，建议与端口过滤模块配合使用，同时在 HTTP 过滤模块中启用[禁止 HTTP 隧道代理]。
3. 即时聊天软件仍在不断的发展中，要保证过滤功能有效，建议定时执行在线升级功能。

5.13. FTP 过滤

FTP 过滤模块用于对文件传输协议（FTP）传输的文件进行过滤，该模块可根据上传、下载的文件名以及文件大小设定过滤条件。配置对话框如下所示：



操作说明：

1. 在[监控分组]里选择要设置 FTP 过滤的电脑组。
2. 单击<增加>按钮增加或保存输入框中的内容。
3. 在列表框中选择要更改的项目，单击<向上>或<向下>箭头按钮可移动该项目的过滤先后顺序。
4. 在列表框中选择要更改的项目，单击鼠标右键，单击[删除]菜单可删除当前选择的项目。
5. [上传文件]：在[文件名]输入框中输入内容，在[策略]中选择处理策略，然后单击<增加>按钮即可。当上传的文件名与列表中的条目相匹配时执行对应策略，上传文件过滤支持通配符。
6. [下载文件]：在[文件名]输入框中输入内容，在[策略]中选择处理策略，然后单击<增加>按钮即可。当下载的文件名与列表中的条目相匹配时执行对应策略，下载文件过滤支持通配符。
7. [限制上传文件大小]：选中该选项，在同一行输入要限制的内容大小数值(千字节)。启用限制后，如果用户上传的文件大小超过设定的大小，该行为将被拦截。
8. [限制下载文件大小]：选中该选项，在同一行输入要限制的内容大小数值(千字节)。启用限制后，如果用户下载的文件大小超过设定的大小，该行为将被拦截。
9. [限制文件保存大小]：当应用“通过并保存”策略时，模块须对相关文件进行缓存。如果超过指定的大小则放弃缓存，防止文件占用过多的内存。该选项默认启用，默认大小为 5 兆。
10. 单击<确定>按钮保存当前设置，单击<取消>按钮取消当前设置。

补充说明：

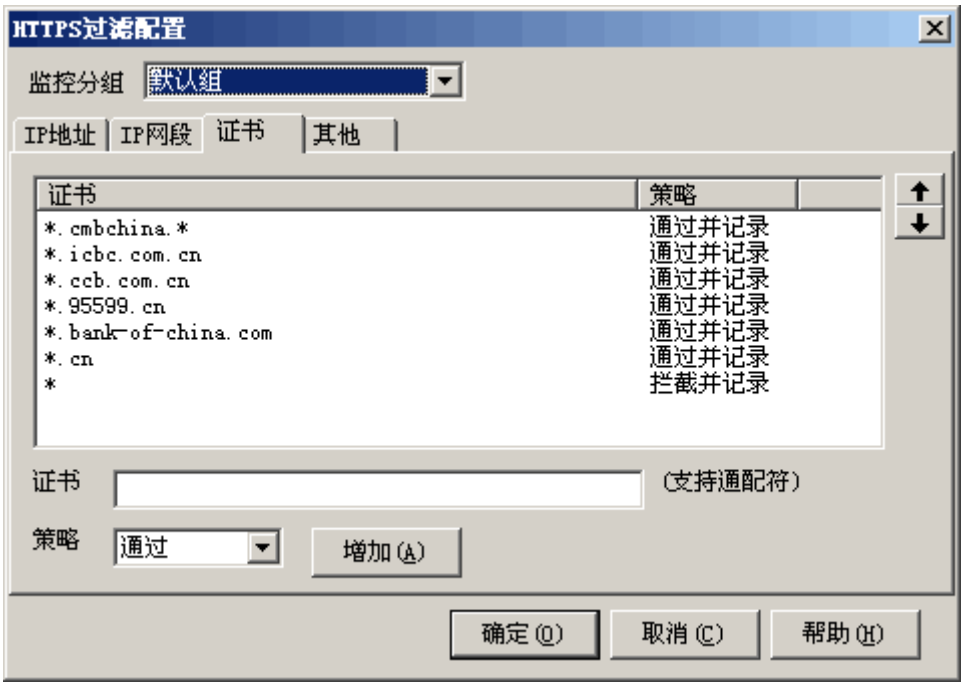
1. [上传文件]过滤按从上到下的顺序过滤，上传文件过滤支持通配符。例如首条（文件名“*.doc”、策略“拦截”），第二条（文件名“*”、策略“通过并记录”），表示上传文件后缀名为“.doc”的被拦截，而其它上传文件都允许通过并记录相关事件。
2. [下载文件]过滤按从上到下的顺序过滤，下载文件过滤支持通配符。例如首条（文

件名“*.exe”、策略“拦截”），第二条（文件名“*”、策略“通过并记录”），表示下载文件后缀名为“.exe”的被拦截，而其它下载文件都允许通过并记录相关事件。

3. FTP 支持断点续传，当断点续传的文件应用“通过并保存”策略时，用户可能需要手工合并保存到硬盘上的各文件块。该功能不影响被监控客户端的操作。
4. FTP 过滤模块同时支持 PORT 和 PASV 模式。

5.14. HTTPS 过滤

HTTPS 过滤模块用于对加密超文本传送协议（HTTPS）进行过滤，该模块可以根据 IP 地址、IP 网段、数字证书、加密协议版本等设定过滤条件。配置对话框如下所示：



操作说明：

1. 在[监控分组]里选择要设置 HTTPS 过滤的电脑组。
2. 在输入框中输入内容，在[策略]中选择相应的策略，单击<增加>按钮增加或保存输入框中的内容。
3. 在列表框中选择要更改的项目，单击<向上>或<向下>箭头按钮可移动该项目的过滤先后顺序。
4. 在列表框中选择要更改的项目，单击[删除]菜单可删除当前选择的项目。
5. [IP 地址]过滤：选择[IP 地址]，输入 IP 地址，选择策略，单击<增加>按钮。当用户访问的 HTTPS 服务器 IP 地址与列表中的条目相匹配时执行对应策略。
6. [IP 网段]过滤：选择[IP 网段]，输入网络号及掩码长度，选择策略，单击<增加>按钮。当用户访问的 HTTPS 服务器 IP 网段与列表中的条目相匹配时执行对应策略。
7. [证书]过滤：过滤允许访问的HTTPS服务器数字证书。在[证书]输入框中输入内容，在[策略]中选择相应的策略，单击<增加>按钮增加或保存输入框中的内容。当用户访问的HTTPS服务器数字证书与列表中的条目相匹配时执行对应策略，证书过滤支持通配符。
8. [禁止 HTTPS 隧道代理]：选中时禁止用户使用非标准 SSL 加密协议的客户端软件通

过 HTTPS 端口访问互联网。

9. [禁止访问无证书服务端]：选中时禁止用户访问采用 SSL 加密但无数字证书的非标准 HTTPS 服务器。
10. [禁止使用 SSL 2.0]：选中时禁止用户使用 SSL 2.0 加密协议访问 HTTPS 服务器。
11. [禁止使用 SSL 3.0]：选中时禁止用户使用 SSL 3.0 加密协议访问 HTTPS 服务器。
12. [禁止使用 TLS 1.0]：选中时禁止用户使用 TLS 1.0 加密协议访问 HTTPS 服务器。

补充说明：

1. [IP 网段]：采用 CIDR 网络前缀表示法(RFC 1878)。如网络号 210.31.233.0，子网掩码 255.255.255.0 可表示成 210.31.233.0/24；网络号 166.133.0.0，子网掩码 255.255.0.0 可表示成 166.133.0.0/16；网络号 192.168.0.0，子网掩码 255.255.255.240 可表示成 192.168.0.0/28 等。
2. 过滤顺序按 IP、网段范围从小到大进行过滤。例如 IP 为"61.141.238.1"策略为"通过"，而 IP 网段"61.141.238.0/24"策略为"拦截"，则表示 61.141.238.0/24 的网段中只有 61.141.238.1 能通过，其它 IP 都被拦截。
3. [证书]过滤按从上到下的顺序过滤，证书过滤支持通配符。例如首条（证书“*.icbc.com.cn”、策略“通过”），第二条（证书“*.cn”、策略“拦截”），表示服务端数字证书中以“.icbc.com.cn”结尾的允许通过，而其它以“.cn”结尾的数字证书都被拦截。


提示：由于 HTTPS 是互联网上常用的协议，许多软件为了突破防火墙都采用 HTTPS 隧道技术与外部联系。要禁止这些软件使用 HTTPS 的 443 端口，只需启用[禁止 HTTPS 隧道代理]和[禁止访问无证书服务端]即可。

5.15. 代理转发

代理转发模块支持 DNS、HTTP、SMTP、POP3、FTP、IMAP、NNTP 协议。使用该模块可以与普通的代理服务器配合实现透明代理服务，而无需在客户端作任何代理设置。代理转发模块自动将普通应用协议转换成应用代理协议并转发给指定的代理服务器，以实现如：网关杀毒、垃圾邮件处理等更高级的功能。设置对话框如下所示：

操作说明：

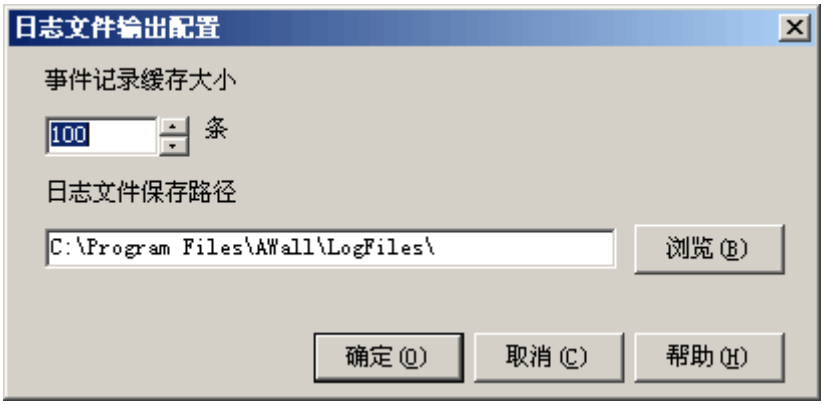
1. 在[监控分组]里选择要设置代理转发的电脑组。
2. 在[IP 地址]、[端口]中填写要转发的代理服务器 IP 地址和端口。
3. 在[转发模式]中选择要启用的转发模式。DNS 协议只有端口转发模式，无需选择。
4. 在[分隔符]中选择“账号-服务器”分隔符。DNS 协议和 HTTP 协议无需选择。
5. 如要将该组某种协议转发给代理服务器，则需要在此协议选项卡中勾选[转发到]选项。
6. 单击<确定>按钮保存当前设置，单击<取消>按钮取消当前设置。

补充说明：

1. [IP 地址]不能采用 127.0.0.1，而必须填写对内网其它电脑可以识别的有效 IP 地址。
2. 每种协议的[IP 地址]、[端口]、[转发模式]、[分隔符]都是为所有组共享的全局参数。这意味着：如果您如果修改了某一组的[IP 地址]、[端口]、[转发模式]、[分隔符]，其它各组也同样受影响。
3. 局域网内部用户访问代理服务器，必须要通过 Active Wall 所在的网关，否则代理转发模块将无法正常工作。
4. 转发模式必须根据代理服务器的配置来设定。对普通代理服务器通常采用应用代理模式。端口转发模式应用在特殊配置下，例如 http 端口转发可应用于 SQUID 透明代理模式。
5. 分隔符必须根据代理服务器的配置来设定。以 POP3 协议为例：原账号为 user、pop3 服务器为 pop.server.com。如果代理服务器要求客户端更改账号为 user#pop.server.com，则分隔符为#。
6. 启用代理转发模块后，客户端无需再设置代理。该模块能自动将客户端的数据转发给代理服务器实现代理上网。

5.16. 日志文件输出

日志文件输出模块将各过滤模块根据策略生成的事件记录以文件形式输出到硬盘。配置对话框如下所示：



操作说明：

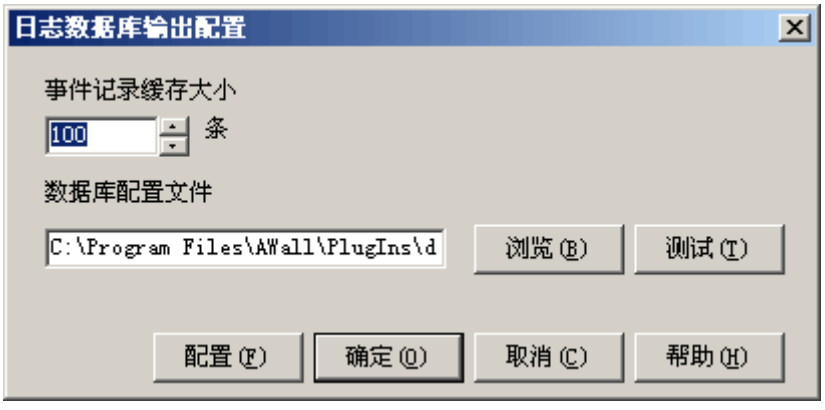
1. 在[事件记录缓存大小]中填写缓存记录条数。
2. 单击<浏览>按钮选择日志文件保存路径。
3. 单击<确定>按钮保存当前设置，单击<取消>按钮取消当前设置。

补充说明：

1. [事件记录缓存大小]：该数值表示缓存在内存中的事件记录的最大条数，默认为 100 条。数值太大会占用较多的内存，数值太小会有较多的硬盘 IO 操作而影响性能。
2. [日志文件保存路径]：表示日志文件保存的绝对路径，日志文件输出模块将每天生成一个日志文件存放在该目录下。

5.17. 日志数据库输出

日志数据库输出模块将各过滤模块根据策略生成的事件记录输出到指定的数据库。配置对话框如下所示：



操作说明：

1. 在[事件记录缓存大小]中填写缓存记录条数。
2. 单击<浏览>按钮选择数据库连接配置文件(*.udl)。
3. 单击<测试>按钮可以测试配置文件所指定的数据库链接是否可用。

4. 单击<配置>按钮可以更改 UDL 文件中保存的数据库连接信息。
5. 单击<确定>按钮保存当前设置，单击<取消>按钮取消当前设置。

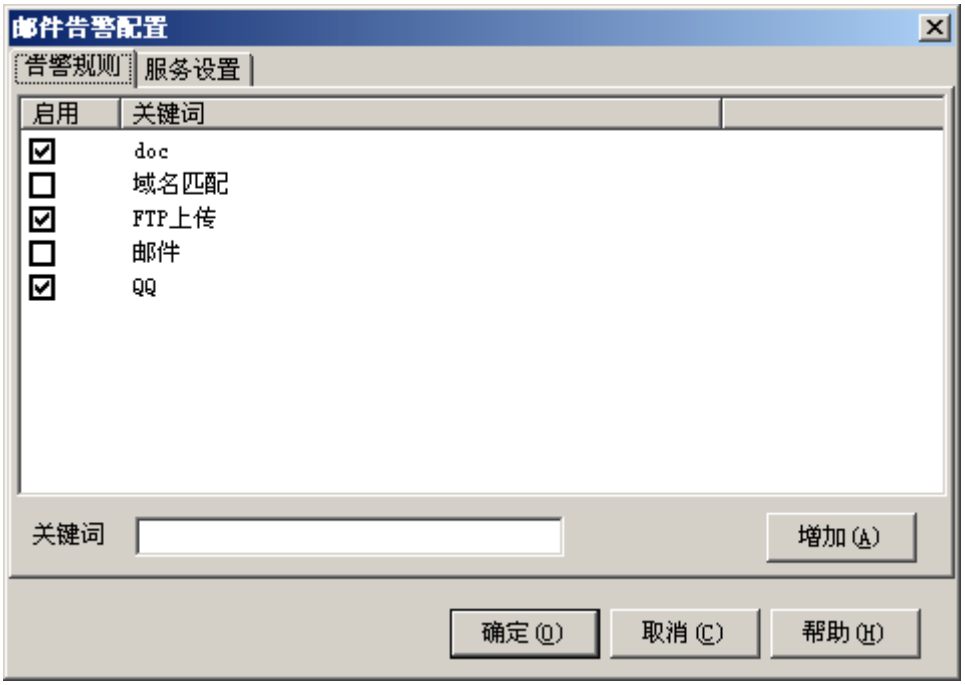
补充说明：

1. [事件记录缓存大小]：该数值表示缓存在内存中的事件记录的最大条数，默认为 100 条。数值太大会占用较多的内存，数值太小会有较多的硬盘 IO 操作而影响性能。
2. [数据库配置文件]：保存数据库连接信息的 udl 文件。UDL 是通用数据连接文件，通过该文件可以保存数据库连接字符串。
3. 安装程序自带 Access 类型的数据库。用户可以直接输出到 Access 的数据库中，也可另外创建数据库，再更改数据库连接输出到自己的数据库中。
4. 创建数据库时请参照以下语句，建立表结构：

```
CREATE TABLE [EventLog] (
[ID] [int] IDENTITY (1, 1) PRIMARY KEY ,
[EventTime] [datetime] NOT NULL ,
[LanIP] [nvarchar] (15) NOT NULL ,
[WanIP] [nvarchar] (15) NOT NULL ,
[PlugIn] [nvarchar] (20) NOT NULL ,
[Act] [int] NOT NULL ,
[Msg] [nvarchar] (255) NOT NULL ,
[Res] [ntext] NULL
)
```

5.18. 告警邮件通知

告警邮件通知模块以电子邮件的方式有选择的将紧急信息发送到指定的邮箱。配置对话框如下所示：



操作说明：

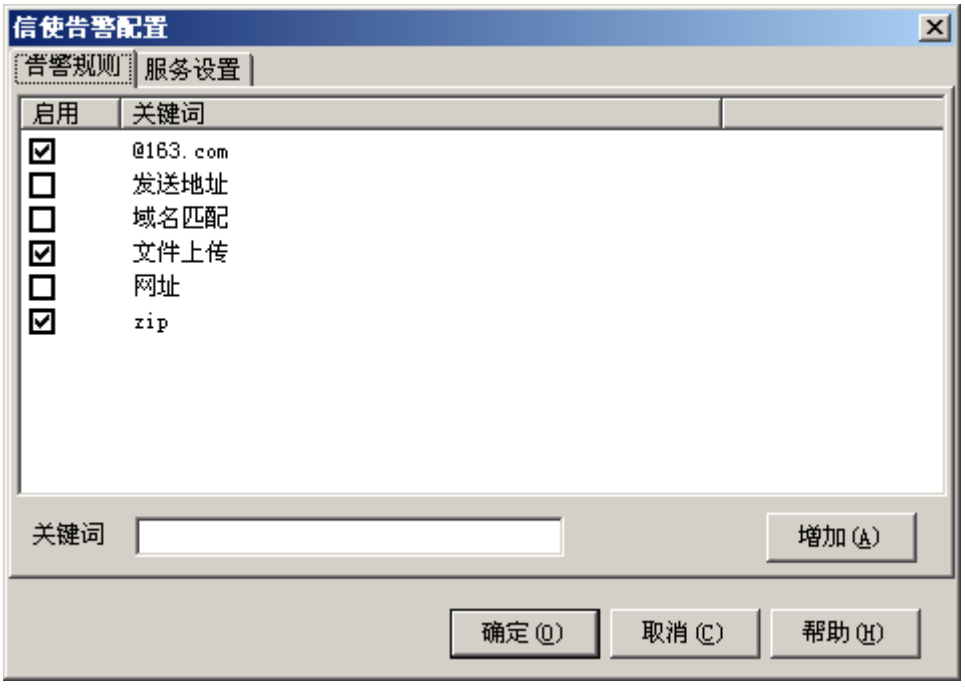
1. 单击<增加>按钮增加或保存输入框中的内容。
2. 在列表框中选择要更改的项目，单击鼠标右键，单击[删除]菜单可删除当前选择的项目。
3. [告警规则]：在[关键词]输入框中输入内容，然后单击<增加>按钮即可。当事件记录内容包含列表中启用的关键词内容时将发送告警邮件到指定邮箱。
4. 在[服务设置]中填写发送邮件时必需的收发邮箱、SMTP 服务器等配置信息。
5. 单击<测试>测试当前的服务设置是否正确，如果正确可以在接收邮箱中收到测试邮件。
6. 单击<确定>按钮保存当前设置，单击<取消>按钮取消当前设置。

补充说明：

1. [接收邮箱]：接收告警邮件的邮箱地址。
2. [发送邮箱]：发送邮件的邮箱地址。
3. [SMTP 服务器]：发送邮件的 SMTP 服务器地址。
4. [SMTP 服务器需要身份认证]：有些 SMTP 服务器需要验证用户身份才允许发送邮件，如果 SMTP 邮件服务器需要身份验证，请勾选该项目，并填写[账号]、[密码]。
5. [账号]：SMTP 验证账号。如果 SMTP 邮件服务器需要身份验证，请填写[账号]。
6. [密码]：SMTP 验证账号。如果 SMTP 邮件服务器需要身份验证，请填写[密码]。

5.19. 告警消息通知

告警邮件通知模块以 Windows 信使消息的方式有选择的将紧急信息发送到指定的电脑桌面。配置对话框如下所示：



操作说明：

1. 单击<增加>按钮增加或保存输入框中的内容。
2. 在列表框中选择要更改的项目，单击鼠标右键，单击[删除]菜单可删除当前选择的项目。

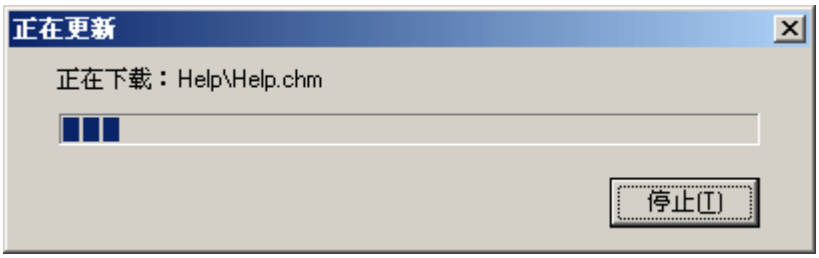
3. [告警规则]：在[关键词]输入框中输入内容，然后单击<增加>按钮即可。当事件记录内容包含列表中启用的关键词内容时将发送告警消息到指定电脑。
4. 在[目标机器]中填写接收信使消息的电脑，通常为管理员电脑。
5. 单击<测试>可以测试信使消息是否能够发送到目标机器。
6. 单击<确定>按钮保存当前设置，单击<取消>按钮取消当前设置。

提示：Windows 信使服务默认是关闭的。要使用信使告警功能，发送电脑和接收电脑都必须开启 Windows 信使服务。

第六章 升级注册

6.1. 在线升级

单击菜单[系统帮助/在线更新]，系统将连接到更新服务器上检测最新的软件版本信息。当检测到有新的版本，系统会自动从网上进行下载：



更新过程中，系统将重新启动程序并应用新的版本。

6.2. 软件注册

单击菜单[系统帮助/软件注册]，将弹出的软件注册对话框。未注册用户可以看到软件自动生成的序列号；已注册用户将可以看到注册的用户名、序列号、授权数以及注册码。

如果您想通过购买正式版软件成为注册用户，请与当地的授权代理商或直接与我们的销售人员取得联系。

通过成为注册用户，您可以

1. 鼓励作者并发展和增进软件的功能，制作新的软件版本；
2. 获得全功能的软件版本的权利；
3. 通过电子邮件、电话、传真等方式获得免费的技术支持和帮助；
4. 可在商业或是其它环境下使用软件；
5. 获得用户身份校验信息和其它的高级功能。

第七章 疑难解答

7.1. 常见问题

7.1.1. 软件安装失败是什么原因？

1. 请检查当前安装的电脑是否满足软件安装要求，详见[运行环境]。
2. 请以管理员身份登录系统再安装本软件。
3. 在软件安装过程中，出现硬件安装警告时请单击<仍然继续>按钮。
4. 检查操作系统的驱动程序签名选项是否为阻止，请将它设为忽略或警告。
5. 软件在卸载后，需要重新启动后才能再次安装。

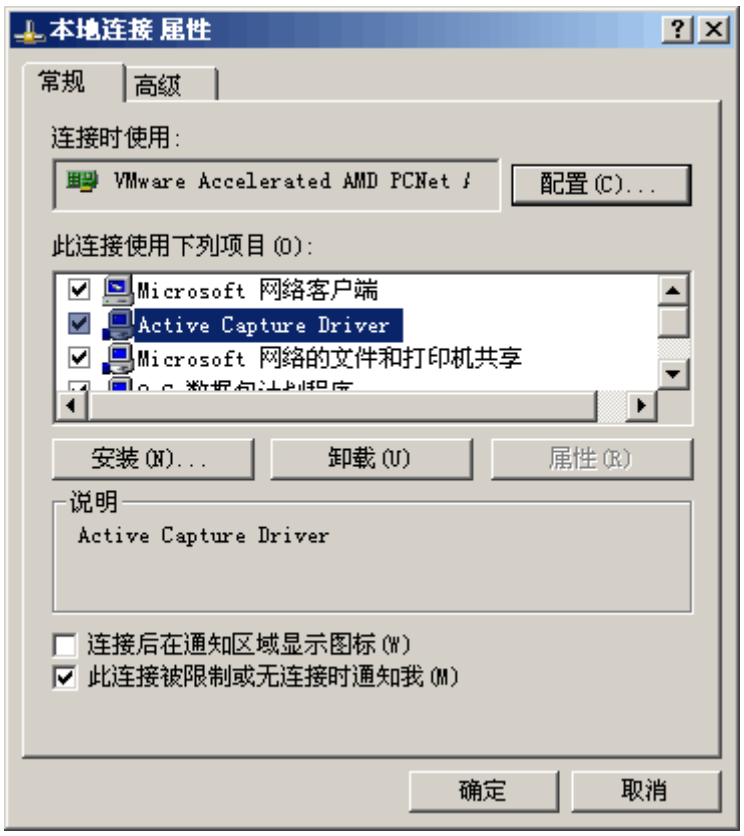
7.1.2. 如何选择网卡和监控模式？

1. 请根据当前网络的结构，选择正确的监控模式，详见[网络环境]。
2. 如果当前网络与上述网络结构都不符合，请改造当前网络以满足要求。
3. 请选择连接局域网内部的网卡，详见[选择网卡]。


提示：推荐采用网关模式。网关模式更加稳定，对网络性能影响较小。且在网关模式下所有模块都能正常工作。

7.1.3. 网卡名称列表是空的怎么办？

1. 请检查驱动安装是否正常，查看连接局域网内部的网卡属性中是否有如图所示的[Active Capture Driver]项目。



2. 如未勾选[Active Capture Driver]，请打勾选择该项目。
3. 如未发现[Active Capture Driver]，请卸载软件，并重新启动后再次安装。在软件安装过程中，出现硬件安装警告时请单击<仍然继续>按钮。
4. 如果已经勾选[Active Capture Driver]，请取消该项目，点击确定后再重新选择该项目。出现硬件安装警告时请单击<仍然继续>按钮。

7.1.4. 默认组出现许多外网 IP 是什么原因？

1. 请检查当前的网络结构与选择的监控模式是否匹配，详见[如何选择网卡和监控模式]。
2. 请检查是否正确的选择了连接局域网内部的网卡，详见[选择网卡]。
3. 请设置正确的局域网地址范围，详见[选择网卡]。

7.1.5. 软件是否能够应用于多个网段？

1. 软件以 IP 为识别电脑的依据，能够应用于多个网段。
2. 不同网段的电脑通信一般要经过路由，数据包中的源 MAC 地址会被替换为路由的 MAC 地址。因此软件在多网段的环境中运行时，请不要绑定 MAC 和 IP 地址。

7.1.6. 为什么使用 Windows 的远程终端登录看不到程序？

1. 软件是以 Windows 服务形式运行，因此只对第一个本地登录的账号可见。
2. 要让远程终端登录的用户能够操作软件，请在登录时用以下命令开启登录客户端：“mstsc/console”。
3. 我们推荐采用VNC进行远程管理，关于VNC请查看官方网站：http://www.realvnc.com

7.1.7. 如何设置网桥？

1. 在 Windows 操作系统中打开"网上邻居"属性，同时选择两块网卡对应的连接如："本地连接"、"本地连接 2"。单击鼠标右键，选择<桥接>菜单，操作系统自动帮您实现网络桥。

2. 桥接完成以以后，两块网卡的 IP 地址自动消失，如果想要让网桥电脑能与网络中的其他电脑通讯，你需要选择"网络桥"，单击鼠标右键，选择<属性>菜单，设置网桥的 IP 地址。

3. 配置网桥时，您需要首先在操作系统中设置好网桥，然后再安装《Active Wall》，否则驱动无法找到正确的网卡。如果您未设置好网桥就已经安装了《Active Wall》，请首先卸载，设置好网桥后再次安装。
4. 安装后在《Active Wall》的[系统配置/选择网卡]菜单中将出现 3 块网卡列表，其中有两块网卡 IP 地址为 0.0.0.0 是真实网卡，而另外一块有 IP 地址的则是网桥虚拟网卡地址。用户需要选择连接内网的真实网卡（IP 地址为 0.0.0.0）。

7.2. 已知问题

7.2.1. 网页压缩输出时内容过滤无效

HTTP 过滤模块中，网页内容过滤能够自动识别 ANSI 和 UTF8 格式，并进行关键词匹配。但是当某些 WEB 服务器对输出的网页内容启用 gzip 压缩后，HTTP 过滤模块由于无法识别而自动忽略网页内容过滤。

7.2.2. 旁路模式的局限性

如果软件选择使用旁路模式工作，由于网络结构的限制，无法拦截 UDP、ICMP 数据包，部分过滤模块将不能正常工作。如果用户选择了“旁路模式时启用数据转发”选项，则程序会采取 ARP 欺骗的方式，对所有的上网数据进行中转。数据转发对网络性能有一定影响，只适合小型网络。

7.2.3. 域名过滤有滞后性

局域网内的电脑在解析域名时，首先在本地的 DNS 缓存中查找，如果找不到才向外发送域名查询数据包，否则直接将缓存中的 DNS 解析项返回。因此对 DNS 域名进行过滤时有一定的滞后性，新加入的策略可能不会立即影响到被监控电脑，须等这些电脑上的 DNS 缓存过期后才能生效。

第八章 联系我们

8.1. 技术支持

我们将为注册用户提供免费的技术支持，我们推荐您在这之前首先阅读帮助文件，同时也可以访问我们的技术论坛，获取最新的使用帮助、经验技巧及策略文件。如果以上方法仍不能解决您的问题，请与我们的技术人员联系以获取技术支持，我们的技术人员会为您解答问题。

在请求技术支持时最好注意以下几个问题:

1. 请首先在线升级软件到最新版本；
2. 请详细描述问题发生的具体过程；
3. 请告知当前网络的拓扑结构和选择的监控模式；
4. 请告知使用的操作系统及软件版本等；
5. 尽可能把你们的情况详细地告诉我们。

8.2. 意见建议

您的意见和建议有利于我们把软件做的更好，如果您有什么建议和意见，请立即写信给我们。

我们非常高兴可以得到注册或非注册用户的反馈信息，包括发现 BUG、使用意见、对功能的看法及建议。具有普遍意义的功能建议将直接加入软件的更新版本。在这里先感谢给我们写信或至电的朋友，不论是表扬或批评，我们都非常感谢你们的支持与帮助。我们也希望这次新版本的推出不辜负大家的厚爱，在此谨向所有关心、支持我们以及给予建议的朋友表示真诚地感谢。

8.3. 联系方式

公司名称： 丽水市爱科网络有限公司
电　　话： 0578-2519007
传　　真： 0578-2536303
邮政编码： 323000
通信地址： 丽水市灯塔街 242 号 204
网　　址： http://www.activenet.cn/
电子信箱： support@activenet.cn
技术论坛： http://forum.activenet.cn/

第九章 协议标准

9.1. 协议标准

本软件参照并遵从以下互联网协议标准：

IEEE 802.3 - 10BASE-T
IEEE 802.3u - 100BASE-TX
IEEE 802.3z - 1000BaseSX,1000BaseLX
RFC 768 - User Datagram Protocol
RFC 791 - Internet Protocol
RFC 792 - Internet Control Message Protocol
RFC 793 - Transmission Control Protocol
RFC 821 - Simple Mail Transfer Protocol
RFC 822 - STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES
RFC 826 - Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware
RFC 959 - File Transfer Protocol
RFC 977 - Network News Transfer Protocol

RFC 1034 - Domain names - concepts and facilities
RFC 1035 - Domain names - implementation and specification
RFC 1112 - Host extensions for IP multicasting
RFC 1323 - TCP Extensions for High Performance
RFC 1519 - Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy
RFC 1521 - MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies
RFC 1522 - MIME (Multipurpose Internet Mail Extensions) Part Two: Message Header Extensions for Non-ASCII Text
RFC 1631 - The IP Network Address Translator (NAT)
RFC 1700 - Assigned Numbers
RFC 1725 - Post Office Protocol - Version 3
RFC 1738 - Uniform Resource Locators (URL)
RFC 1866 - Hypertext Markup Language - 2.0
RFC 1867 - Form-based File Upload in HTML
RFC 1869 - SMTP Service Extensions
RFC 1918 - Address Allocation for Private Internets
RFC 1939 - Post Office Protocol (POP) - Version 3
RFC 1945 - Hypertext Transfer Protocol -- HTTP/1.0
RFC 1951 - DEFLATE Compressed Data Format Specification version 1.3
RFC 1952 - GZIP file format specification version 4.3
RFC 2044 - UTF-8, a transformation format of Unicode and ISO 10646
RFC 2045 - Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
RFC 2046 - Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types
RFC 2047 - MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text
RFC 2048 - Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures
RFC 2049 - Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples
RFC 2060 - Internet Message Access Protocol (IMAP) - Version 4 Rev 1
RFC 2068 - Hypertext Transfer Protocol -- HTTP/1.1
RFC 2070 - Internationalization of the Hypertext Markup Language
RFC 2131 - Dynamic Host Configuration Protocol
RFC 2236 - Internet Group Management Protocol, Version 2
RFC 2246 - The TLS Protocol Version 1.0
RFC 2279 - UTF-8, a transformation format of ISO 10646
RFC 2396 - Uniform Resource Identifiers (URI): Generic Syntax
RFC 2616 - Hypertext Transfer Protocol -- HTTP/1.1
RFC 2617 - HTTP Authentication: Basic and Digest Access Authentication
RFC 2818 - HTTP Over TLS