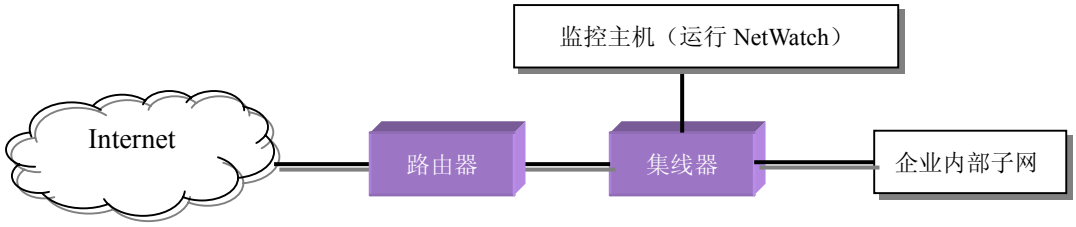
# NetWatch 网络监控和入侵检测系统

## 一、 简单介绍

NetWatch 是一个能对企业网络进行实时监控、对关键访问进行实时记录、并可以自动和手动切断网络连接、手动孤立和堵塞网络主机、防止 ARP 欺骗、具有简单的入侵检测功能、具有多种响应方式、支持和 NetMoon 防火墙的互动（自动和手动两种）的基于 Windows NT/Windows 2000 平台的网络监控系统。

## 二、 系统结构

NetWatch 是一个桌面版的网络监控和入侵检测系统。其中，监控主机是基于 Windows NT/Windows 2000 平台并运行 NetWatch 的一台普通 PC 机。NetWatch 可部署在企业出口的地方，也可部署在局域网内部。




NetWatch 部署在企业出口的地方

注意：由于 NetWatch 要对网络上的每一个数据包进行分析处理、故 NetWatch 运行在共享式局域网环境中。NetView 也可运行于交换式环境中，关于如何运行于交换环境中，请参见常见问题解答部分 。

## 三、 功能说明

其中 NetWatch 2.0 专业版提供如下的功能:

- 对企业网络连接信息进行实时监控(TCP 和 UDP)，并以列表和活动状态树的形式显示，用户可对每个连接进行更细的处理：切断连接、记录连接、跟踪连接、制定控制规则、制定和防火墙的互动规则、给客户端发送”信使”信息(WinPopup 信息)。
- 按客户端、服务端、服务和常用应用层协议对网络流量数据的进行统计显示。在按客户端和服务端进行流量显示的同时，可对指定的条目制定动态过滤规则、互动规则过滤、排除规则过滤。
- 对影响网络活动的每一个要素实施面向对象的管理。目前有网络对象、服务对象、时间对象、URL 对象、内容对象、消息对象。
- 灵活的过滤规则制定方式。目前有用户过滤规则、用户排除规则、一般过滤规则、URL 过滤规则、内容过滤规则、一般排除规则、入侵检测规则、IP 和 MAC 地址绑定规则等灵活多变的检测规则制定方式。
- 支持对 TCP 会话的实时跟踪功能，特别适合对 Telnet 、FTP 等交互式会话的实跟踪。
- 支持对端口扫描和 800 多种常见攻击方式的检测。
- 以可视化方式支持 Unix 下 ARPWatch 功能，跟踪网络内的 IP 地址变更，防止 ARP 欺骗。
- 可手工对主机进行堵塞和孤立功能。
- 可自动阻断 TCP 连接。
- 在规则过滤中， 可以以主机的 MAC 地址而不是 IP 地址进行过滤。

其中 NetWatch 2.0 企业版提供如下的功能:

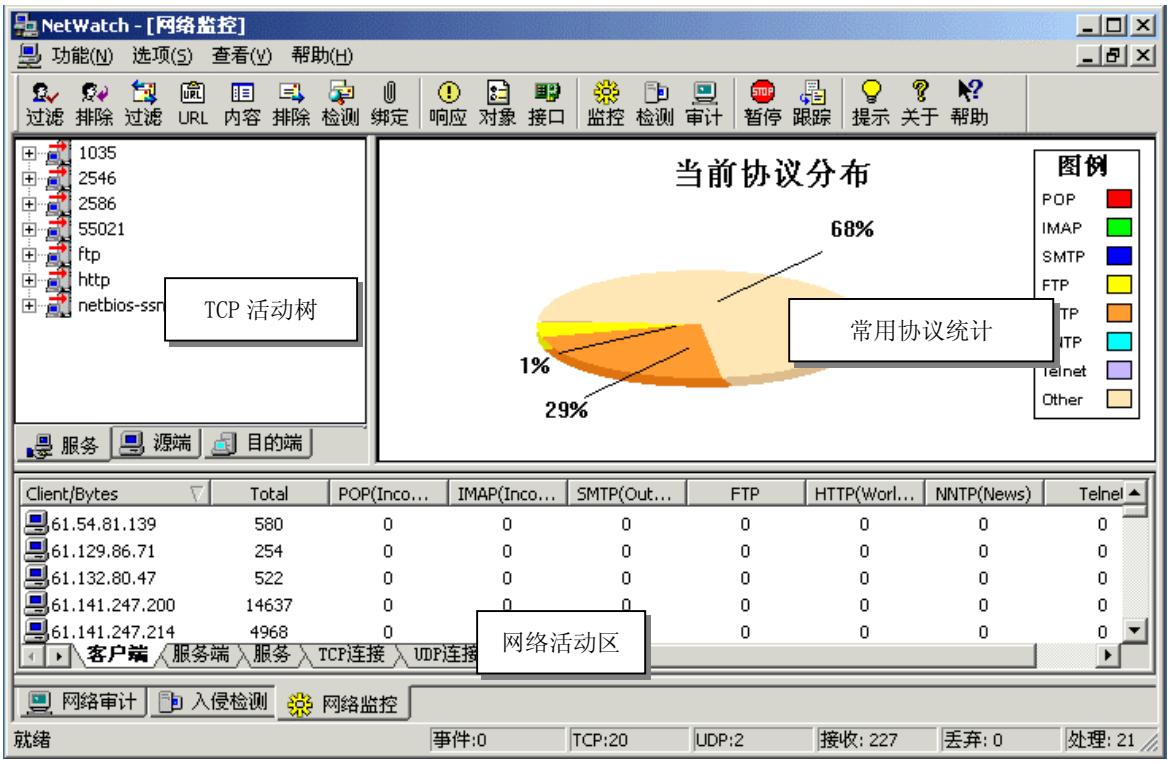
- NetWatch 2.0 专业版提供的所有功能。
- 在某一网络活动发生时，可以实施多种响应方式：发送邮件、自动阻断、发送 SNMP Trap、防火墙互动、发送 Syslog 信息。
- 特别支持和 NetMoon 放火墙的互动响应和第三方防火强的互动响应。

## 四、 运行环境和系统要求

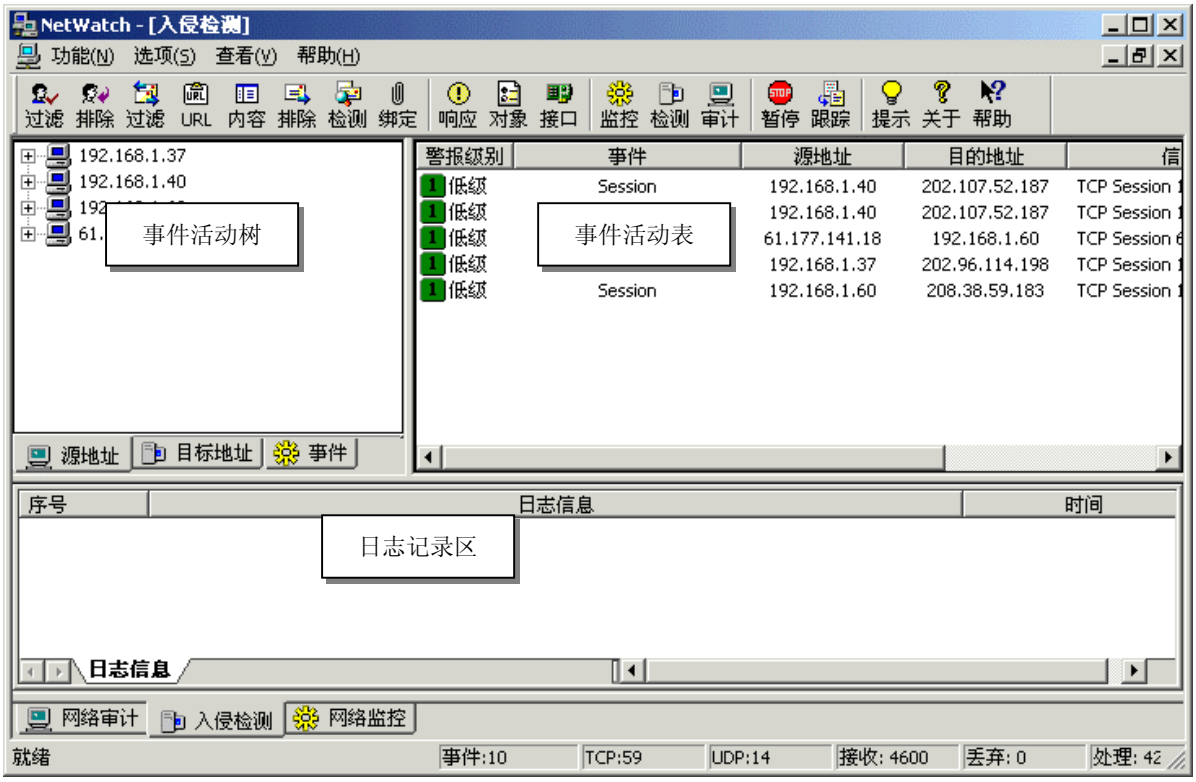
NetWatch 运行于 Windows NT 4.0(SP6) 和 Windows 2000 平台上。128M 内存（推荐 256M 内存）,PII 600 CPU,100M 硬盘空间。至少 800x600 的显示分辨率。

## 五、 监控界面

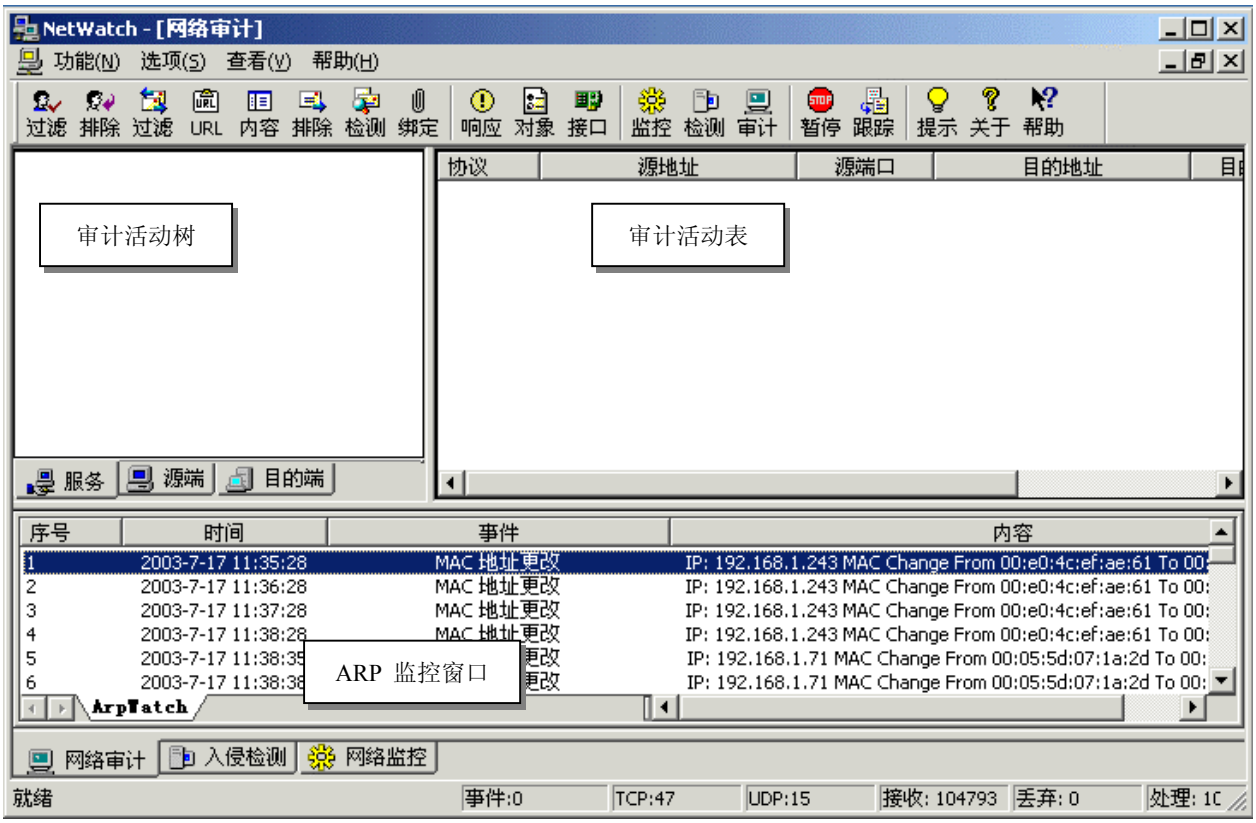
下面是 NetWatch 主监控检测界面。NetWatch 由三大部分组成：网络监控、入侵检测、网络审计组成。 其中网络监控包括三个部分：TCP 活动树、常用协议统计、网络状态区。




入侵检测包括事件活动树、事件活动列表、日志记录区。

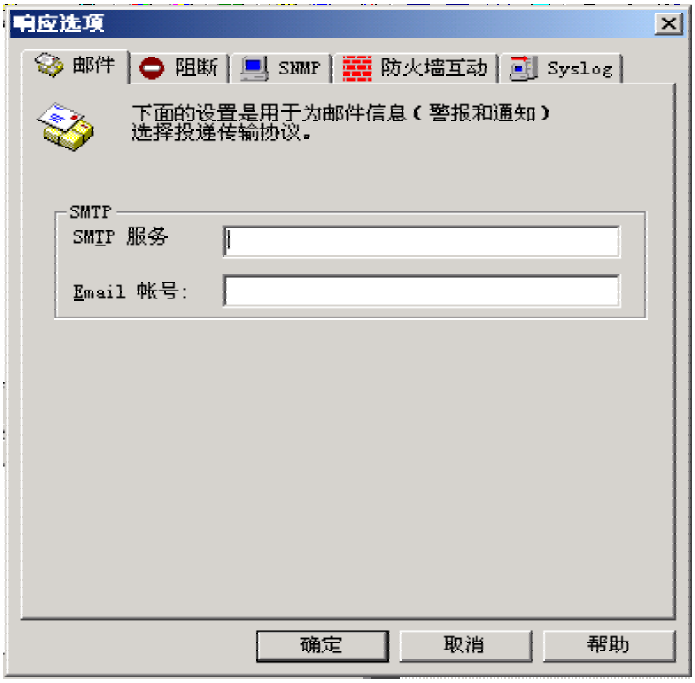



网络审计包括审计活动树、审计活动表和 ARP 监控窗口。




## 六、 响应配置界面

下图是响应方式配置窗口：

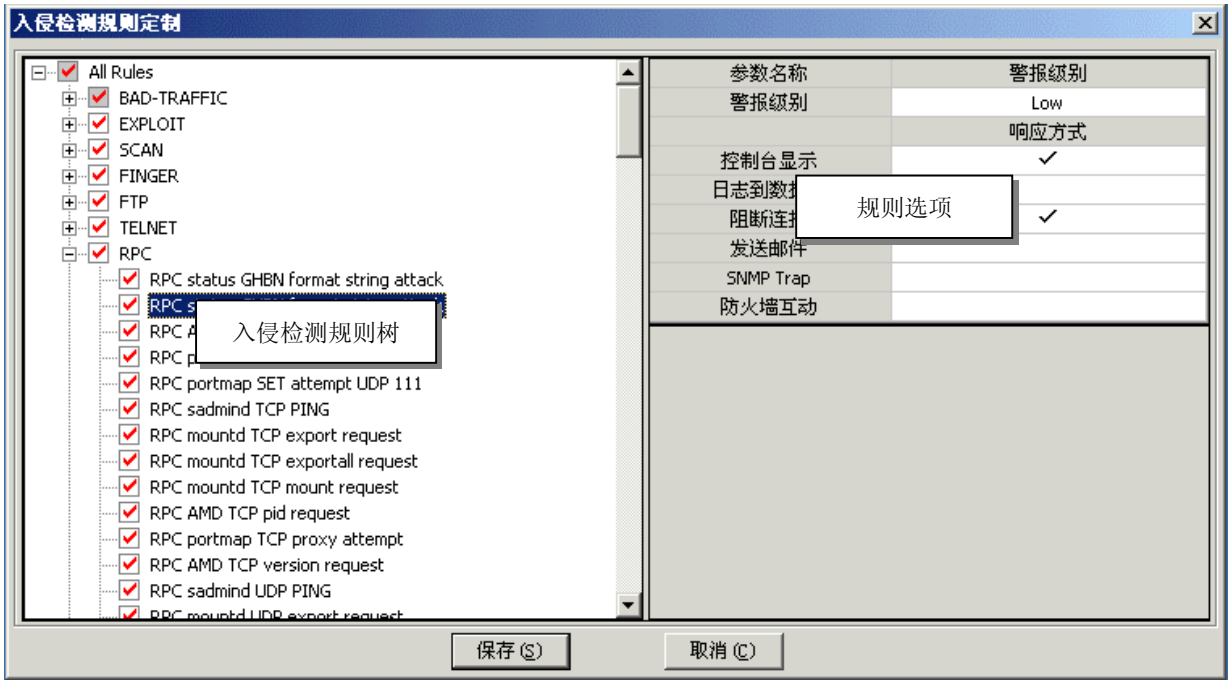



目前 NetWatch V2.0 专业版只支持日志、邮件和 Syslog 响应方式的支持。

## 七、 规则配置界面

下面是规则过滤窗口。注意：由于 NetWatch 不是网关级的产品，所以的它的阻断功能可能对 TCP 协议比较有效。对于其它协议的阻断，建议采用和 NetWatch 互动的防火墙产品进行。


下图是协议入侵检测规则定制窗口：

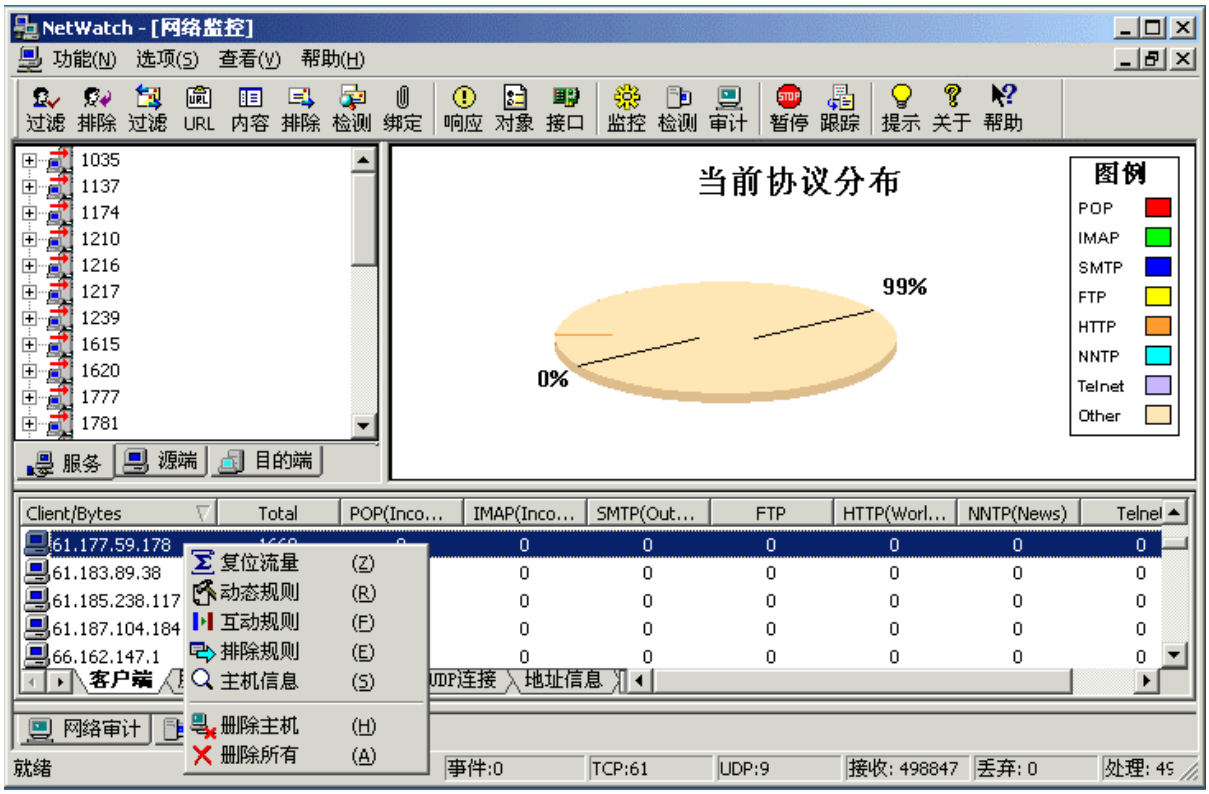



## 八、 网络活动监控

NetWatch 对网络活动的监控主要体现在对网络流量的统计、对网络活动的控制。下图是活动控制界面。

### 8.1、流量统计部分

在客户端或服务端流量统计部分右键单击某一条目，则出现如下菜单：



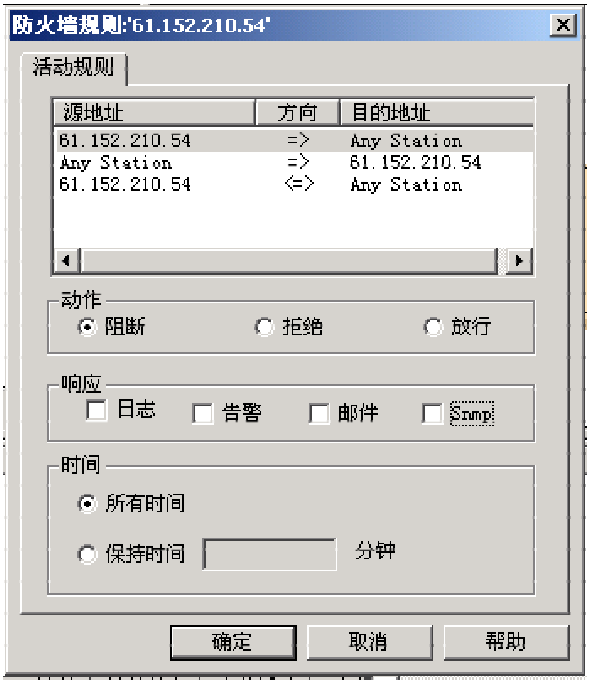

其中“复位所有流量”使所有流量信息置为 0；“删除主机信息“即删除当前条目信息；“删除所有信息”即删除所有条目。

### 8．1．1、动态规则对话框

选择”动态规则”则出现如下对话框：

### 8．1．2、互动规则对话框

选择”互动规则”则出现如下对话框：

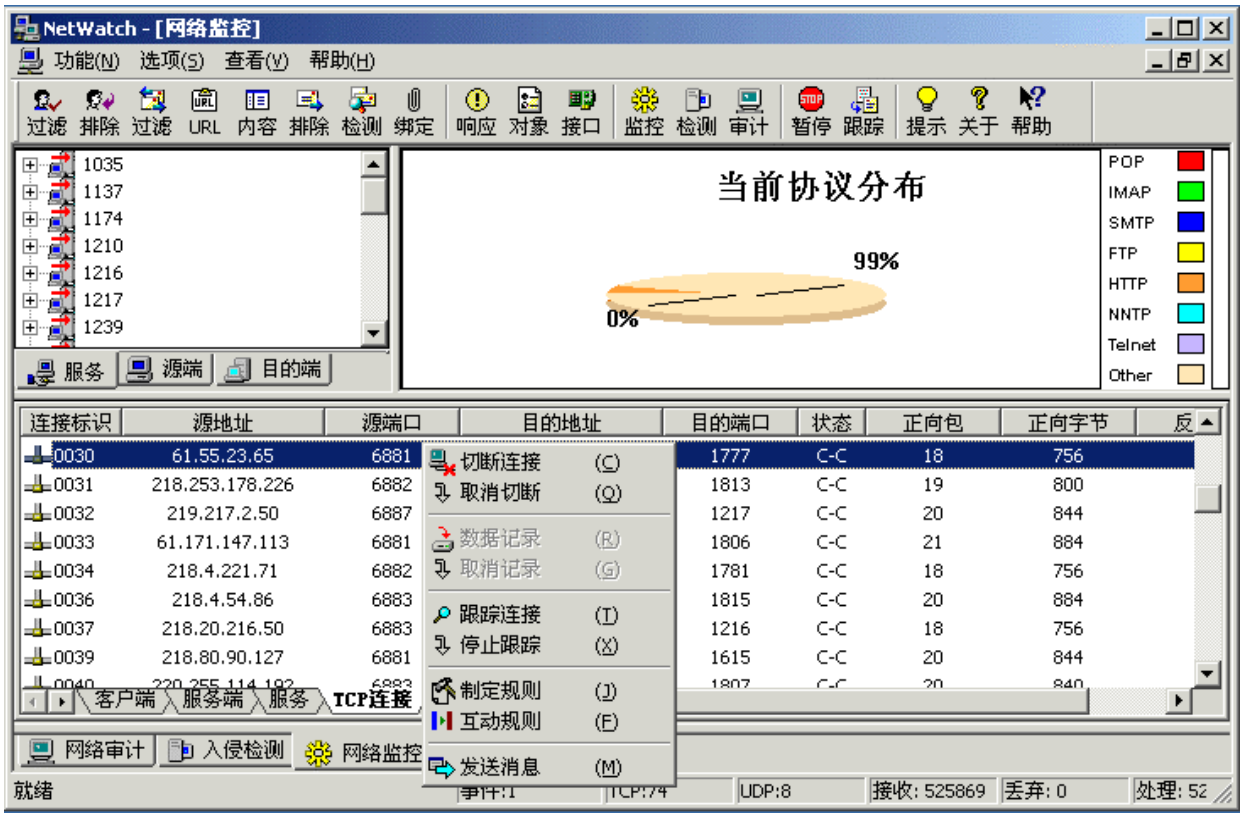



### 8．1．3、排除规则对话框

选择”排除规则”则出现如下对话框：


### 8.2、网络连接部分

在 TCP 连接或 UDP 连接部分右键单击某一条目，则出现如下菜单：




其中:“切断连接”为切断当前连接;“取消切断”为如果当前连接还没有断开，则可以取消切断连接;“数据记录”为对当前连接的数据进行实时记录，供以后进行还原回放;”取消记录”为如果 NetWatch 对当前连接正在进行记录，则取消记录并删除此记录项;”跟踪连接”为显示跟踪窗口并实时显示此连接的数据包; ”停止跟踪”为如果当前连接正被跟踪则停止跟踪。其它菜单项在下面详细描述:

### 8．2．1 制定规则

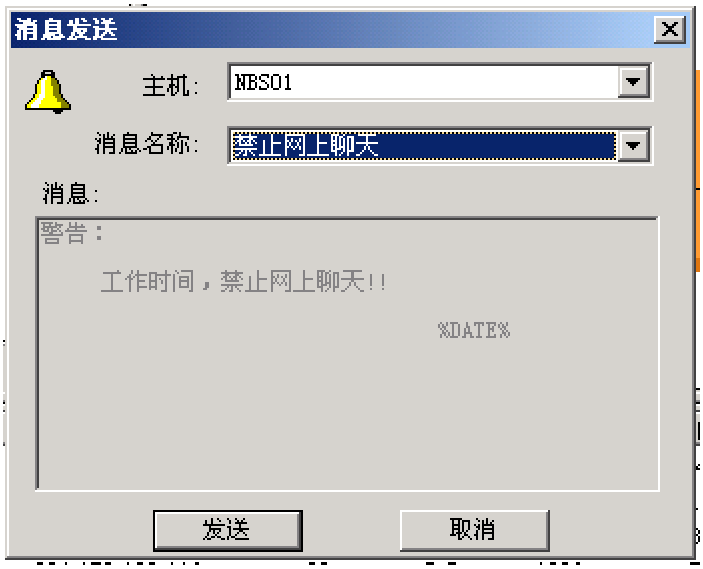
选择”制定规则”则出现如下对话框:


### 8．2．2 互动规则

选择” 互动规则”则出现如下对话框：

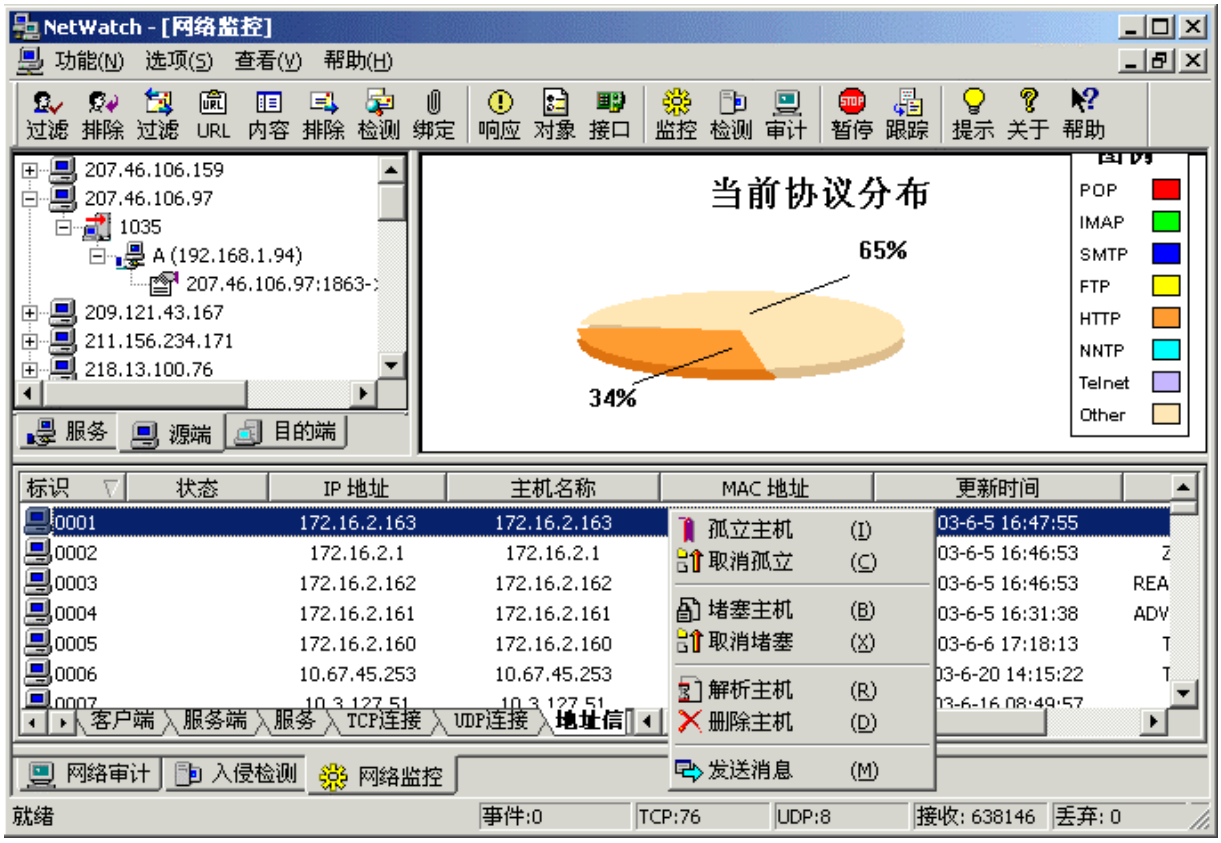

### 8．2．3 发送消息

选择” 发送消息”则出现如下对话框：




### 8.3、主机操作部分

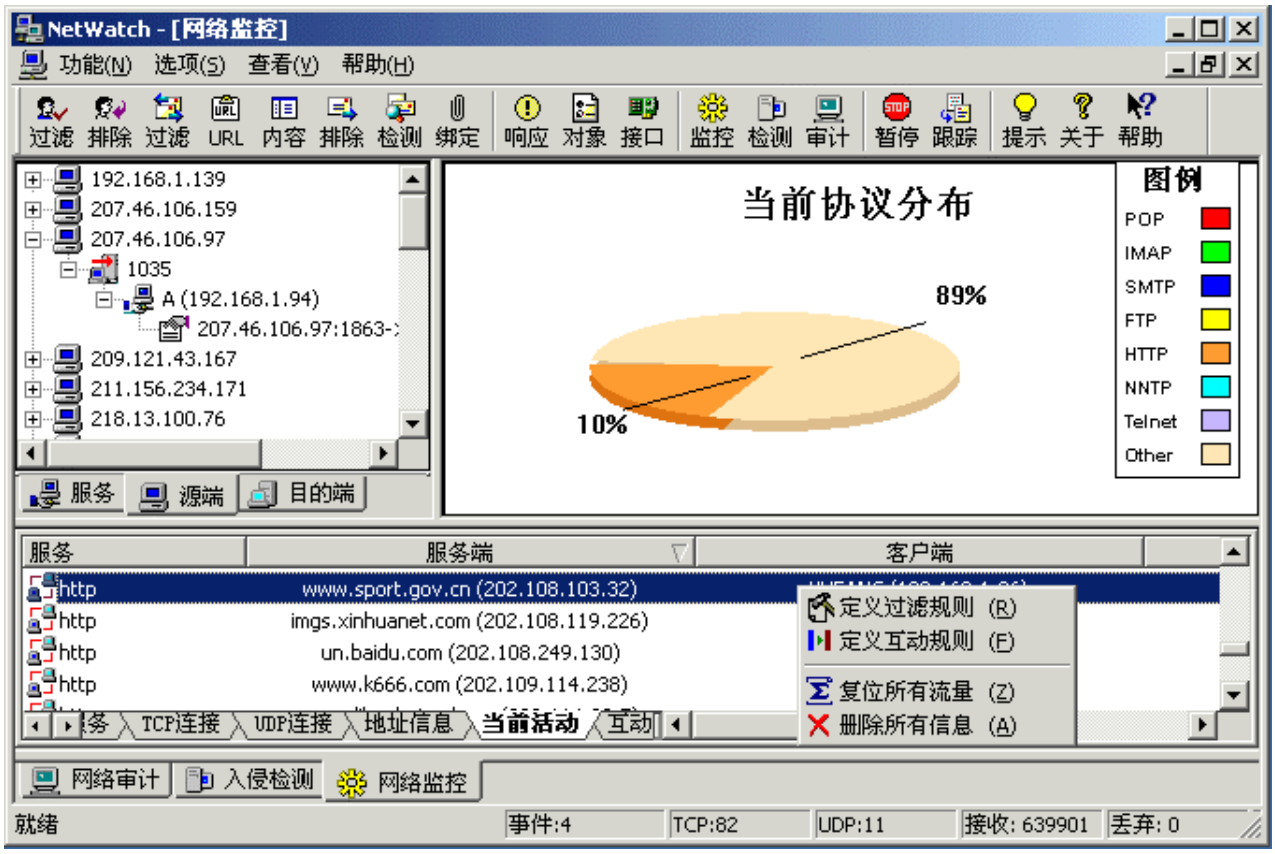
在地址信息部分右键单击某一条目，则出现如下菜单：




其中:“孤立主机”为使某一主机处于孤立状态，不能与任何主机进行通讯;“取消孤立”为如果当前主机处于孤立状态，则可以取消此主机的孤立状态;“堵塞主机”为对当前主机的 TCP 和 UDP 连接进行拦截;“取消堵塞”为如果当前主机处于堵塞状态则取消堵塞状态; ”解析主机”为重新解析此主机的名称; ”删除主机”为删除这一主机项。

### 8.4、当前活动部分

在当前活动部分右键单击某一条目，则出现如下菜单:




其中:“复位所有流量”为使所有活动的流量复位;“删除所有信息”为删除所有的当前活动。其它菜单项在下面解释:

### 8．4．1 定义过滤规则

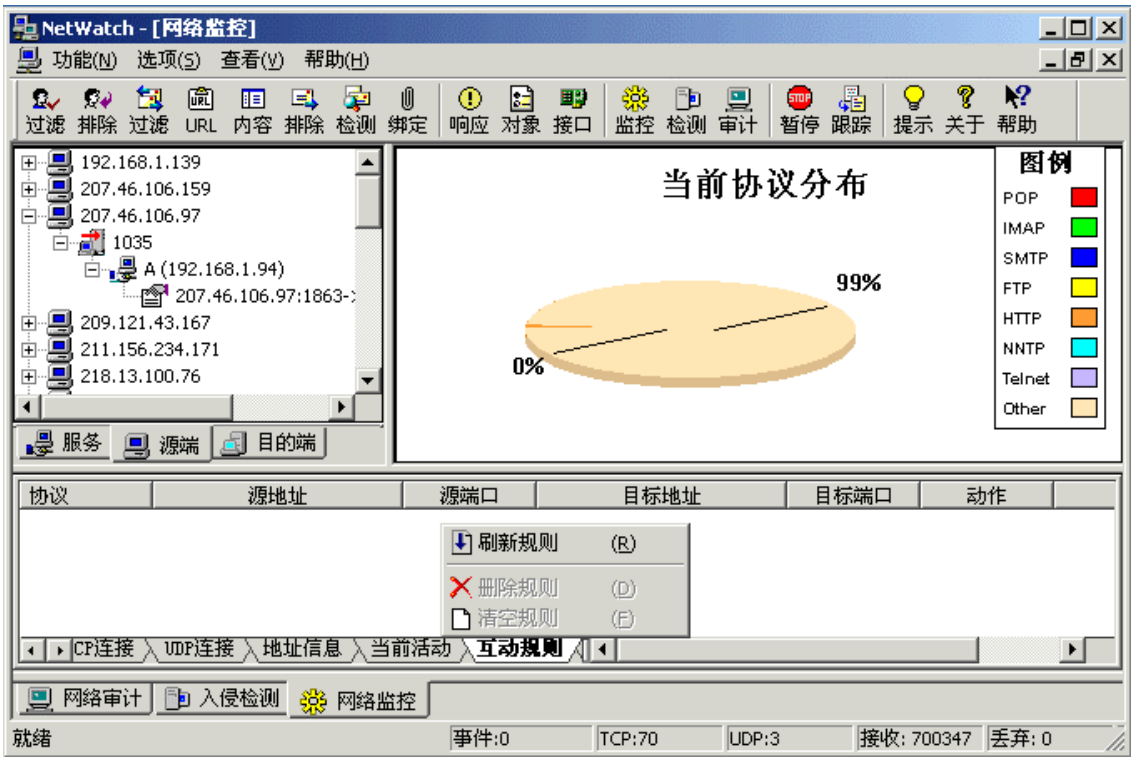
选择”定义过滤规则”则出现如下对话框:

### 8．4．2 定义互动规则

选择” 定义互动规则”则出现如下对话框：


### 8.5、互动规则部分

在互动规则部分右键单击某一条目，则出现如下菜单：



## 九、 特别注意

由于 NetWatch 的功能比较丰富，上面仅仅是一些操作界面，具体的功能描述需要很多的精力和时间。这将在以后的版本更新中进行增加。

NetWatch 适合企业的网络管理人员、系统管理人员和安全管理人员使用，用于发现问题，排除故障及发现安全漏洞。使用此软件请遵守国家的相关法律和法规的规定。禁止使用此软件进行网络破坏活动。凡使用此软件对网络进行破坏并造成后果的，本公司概不负责。