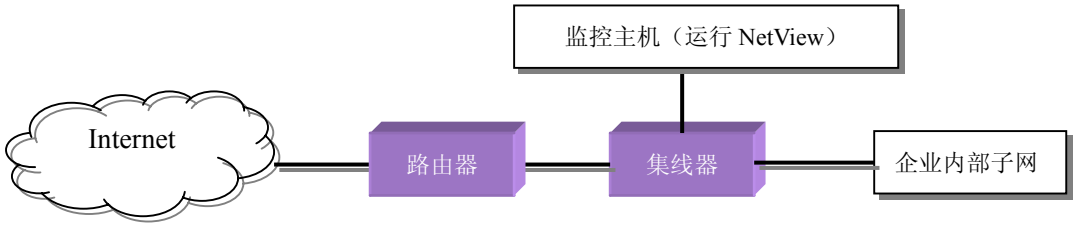
NetView 网络内容监控和审计系统

一、 简单介绍

NetView 是网络内容监控与审计系统,目前主要支持 HTTP、SMTP、POP3、NNTP、FTP、TELNET 协议。在以后的版本中将增加对其它应用层协议的还原和分析处理。NetView 是基于 Windows 平台的集网络数据包抓取技术、还原技术和分析技术、MIME 分析技术于一体的网络安全产品。主要运行于 Windows NT/Windows 2000 平台上。

二、 产品布署

NetView 是一个桌面版的应用协议监控与审计系统。其中，监控主机是基于 Windows NT/Windows 2000 平台并运行 NetView 的一台普通 PC 机。NetView 一般部署在企业网络出口的地方，也可部署在局域网内部。



NetView 部署在企业出口的地方

注意：由于 NetView 要对网络上的每一个数据包进行分析处理、故 NetView 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 。

强烈建议在运行 NetView 之前，先安装相关的杀毒软件包。以免在查看邮件内容时，使你的机器遭受病毒的侵害。

三、 功能说明

NetView V2.0 实现如下功能：

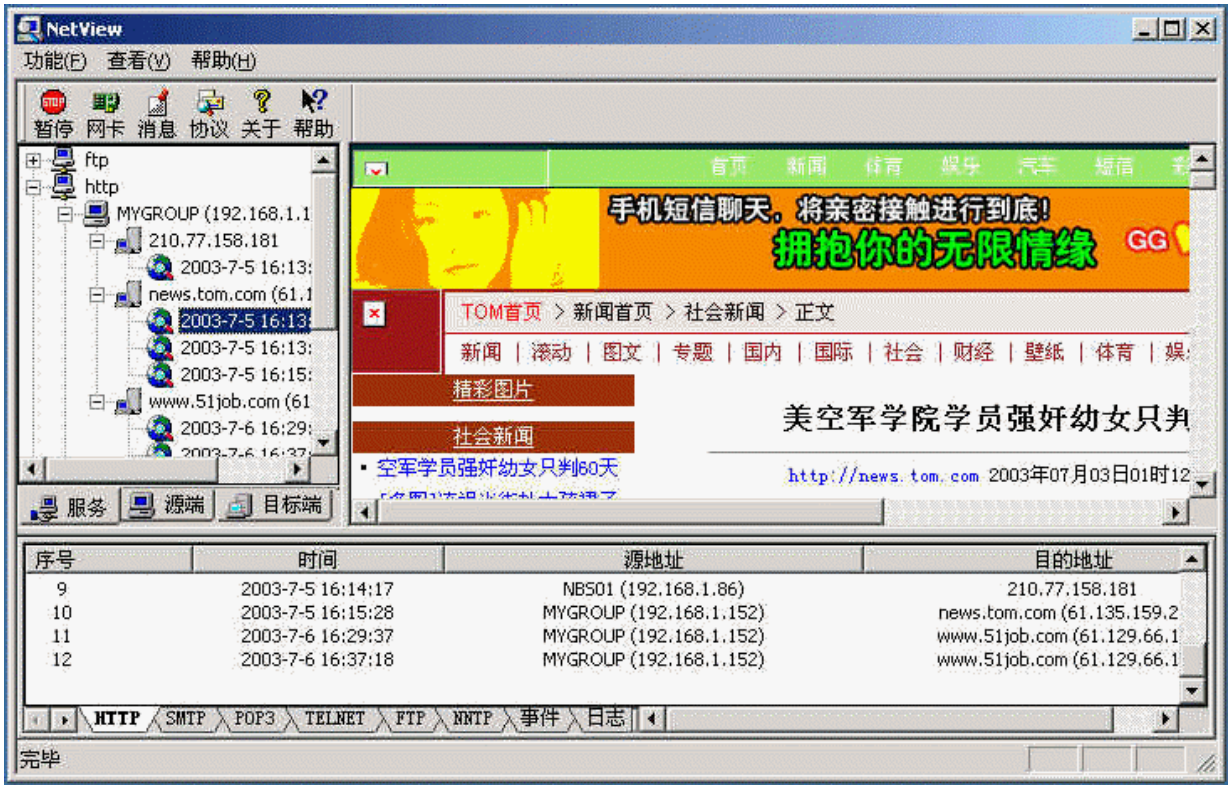
- 对常用的 HTTP、SMTP、POP3、NNTP、FTP、TELNET 协议进行数据包的内容还原和恢复，并以方便快捷的方式显示出来。
- 可随时给客户端发送”信使”信息(WinPopup 信息)。
- 强大的 SMTP、POP3 协议分析技术和还原技术。
- 强大的 MIME(**M**ultipurpose **I**nternet **M**ail **E**xtensions) 分析和显示技术。

四、 运行环境和系统要求

NetView 运行于 Windows NT 4.0(SP6) 、Windows 2000 平台上。256M 内存（推荐 512M 内存）,PII 600 CPU,200-500M 硬盘空间。至少 800x600 的显示分辨率。

五、 监控界面

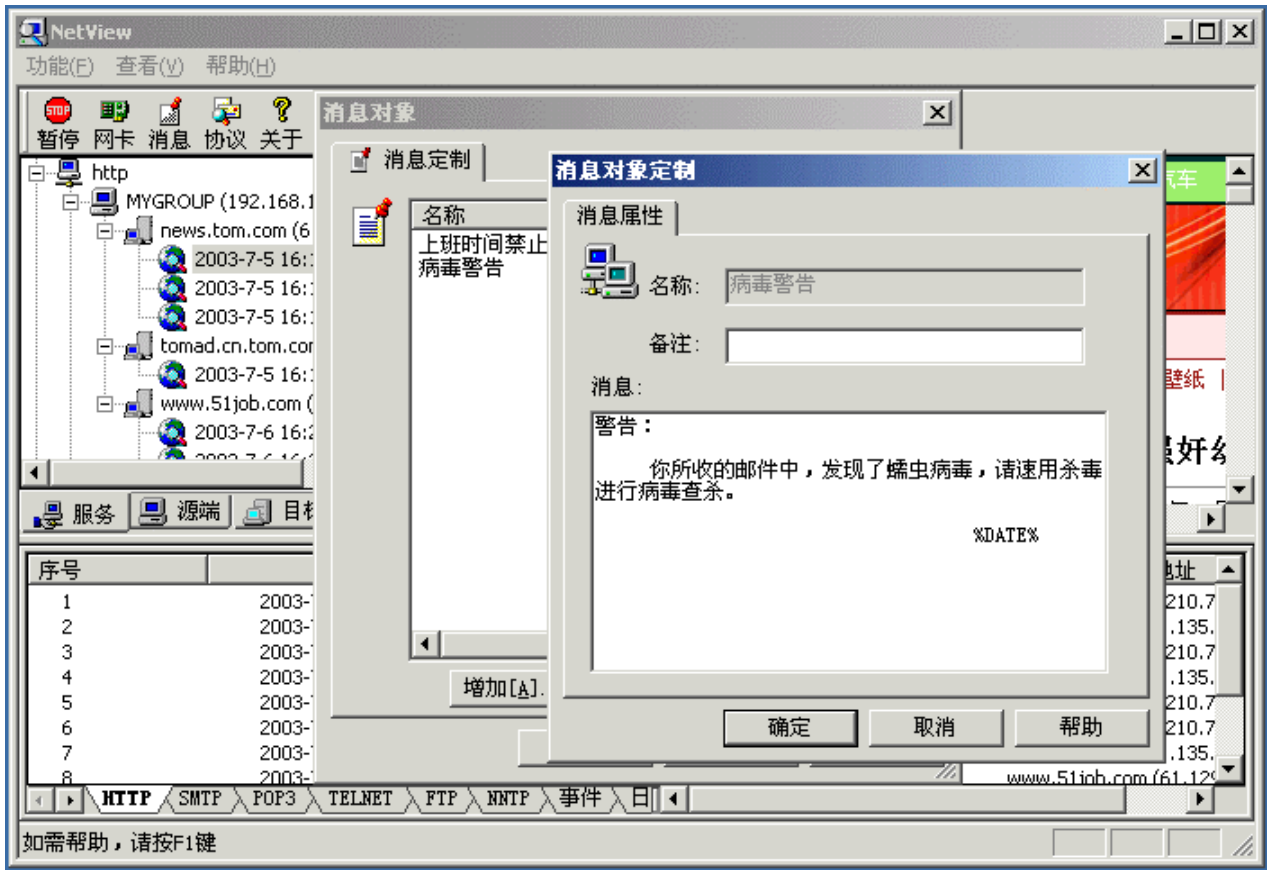
下面是 NetView 主监控界面。主监控界面由三个区域组成：活动树区、活动列表区、内容显示区。其中活动树区域主要用于对已经还原的网络数据进行分类，以利于用户的查找。活动列表区域主要是按照已还原数据的时间先后顺序进行排列，以利于用户查看最近的数据信息。内容显示区域主要用于对还原后的内容进行显示。目前可显示的有 HTTP 网页，SMTP 和 POP3 的邮件信息，NNTP、TELNET、FTP 的交互会话信息。下面显示的是从网站上截取的网页信息。



六、其它功能介绍

6．1、信使消息定制

点中消息定义按钮，则出现如下界面：



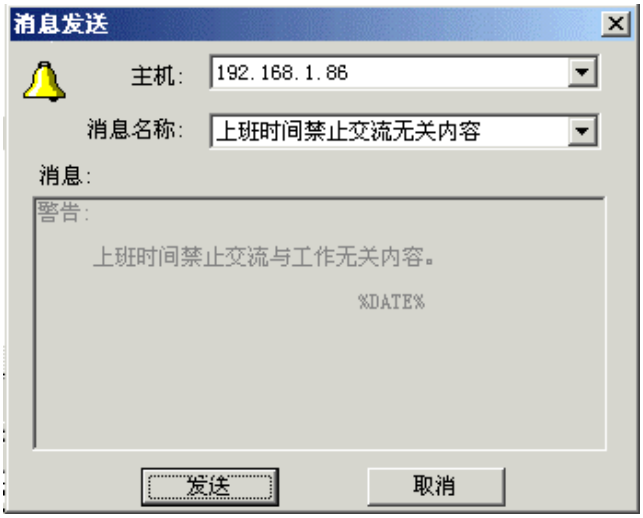
按《增加》按钮，新建消息对象；选中相应的消息，按《删除》按钮，则删除消息对象；选中相应的消息，按《属性》按钮则修

改消息。在消息对象定制完成后，下面就可以给某个 Windows 主机发送消息了。

6．2、发送信使消息

在活动树或活动列表，右健选中某一个数据连接，将出现如下菜单。

选择发送警告消息，则出现如下对话框：



选择相应的消息名称，点击发送按钮，则消息发出。

注意：此功能只能用于向基于 Windows 平台的用户发送信使消息。

6．3、查看会话内容

在上面的菜单中，选择《查看会话内容》，则将把此会话的内容经过解码、分析后在显示区域显示出来。

6．4、查看原始内容

在上面的菜单中，选择《查看原始内容》，则将把此会话的内容不经解码就在显示区域显示出来。

6．5、删除会话内容

在上面的菜单中，选择《删除会话内容》，则将把此会话的数据库表项连同相关的文件删除。支持对多个表项的同时删除。

6．6、选择网络接口

选择工具栏上的《选择接口》，将配置你机器上监控的网络接口。在你的机器有多个网络接口，并和两个及两个以上的网络相连时，请进行此项设置。此项设置将用于对哪个网络进行监控。

6．7、协议还原设置

用于对哪些应用层协议进行还原和分析。选择感兴趣的协议。

6．8、暂停和恢复协议还原

工具栏上的第一个按钮是一个双向开关。选择它，将可以暂停协议的还原或恢复协议的还原。