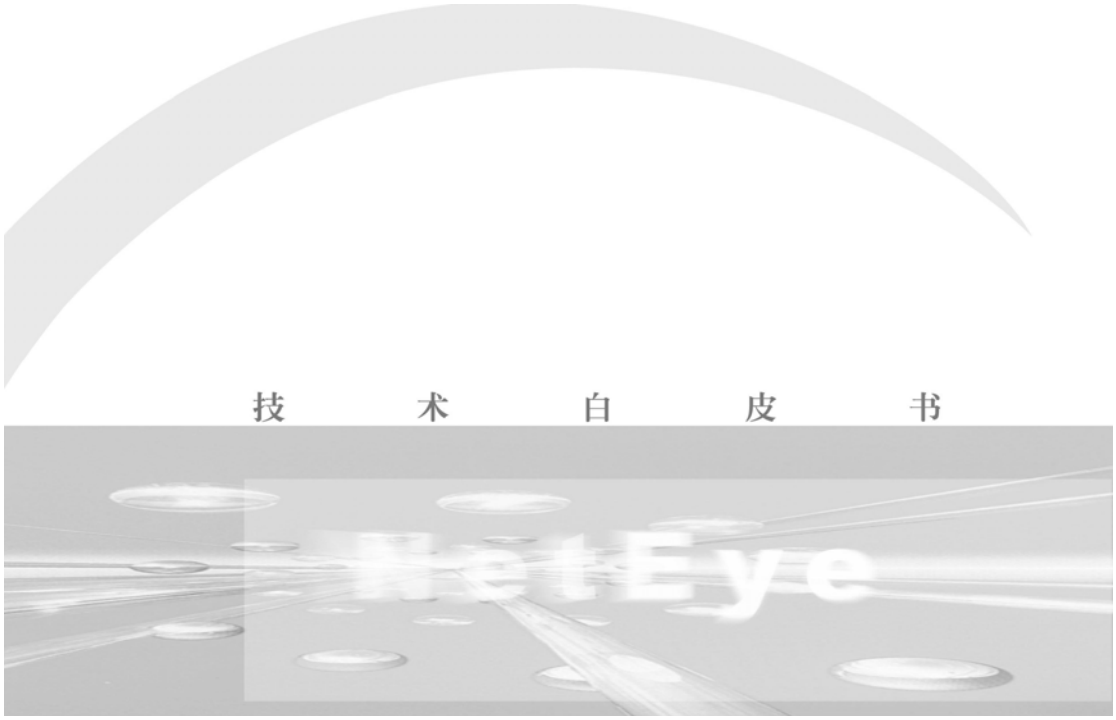
NEUSOFT 东软 软件创造客户价值

NetEye IDS 2.2
技术白皮书



沈阳东软软件股份有限公司

目录

一、概述 3
1、网络面临的主要威胁 3
2、入侵检测系统IDS，消除网络威胁 4
3、NetEye IDS 2.2, 给您提供全面的安全 5
二、系统结构 5
- 检测引擎 5
- NetEye IDS 管理主机 5

三、功能模块简介 6
1. 网络攻击与入侵检测功能 6
2. 多种通信协议内容恢复功能 8
3. 网络审计功能 11
4. 图表显示网络信息功能 12
5. 报表功能 14
6. 实时网络监控功能 15
7. 网络扫描器。 18
8. 数据备份恢复功能 19
9. 其它辅助管理，配置工具 20

四、技术特点 20
五、典型应用示例 23

一、概述

由于互联网络的发展，整个世界经济正在迅速地融为一体，而整个国家犹如一部巨大的网络机器。计算机网络已经成为国家的经济基础和命脉。计算机网络在经济和生活的各个领域正在迅速普及，一句话，整个社会对网络的依赖程度越来越大。众多的企业、各种组织、政府部门与机构都在组建和发展自己的网络，并连接到 Internet 上，以充分利用网络的信息和资源。网络已经成为社会和经济发展强大动力，其地位越来越重要。伴随着网络的发展，带来了很多的问题，其中安全问题尤为突出。了解网络面临的各种威胁，防范和消除这些威胁，实现真正的网络安全已经成了网络发展中最重要的事情。

1、网络面临的主要威胁

日益严重的网络信息安全问题，不仅使上网企业、机构及用户蒙受巨大的经济损失，而且使国家的安全与主权面临严重威胁。要避免网络信息安全问题，首先必须搞清楚触发这一问题的原因。总结起来，主要有以下几个方面原因：

（1）黑客的攻击:黑客对于大家来说，不再是一个高深莫测的人物，黑客技术逐渐被越来越多的人掌握和发展。目前，世界上有 20 多万个黑客网站，这些站点介绍一些攻击方法和攻击软件的使用以及系统存在的一些漏洞，因而系统、站点遭受攻击的可能性就变大了。尤其是现在还缺乏针对网络犯罪卓有成效的反击和跟踪手段，使得黑客攻击的隐蔽性好，“杀伤力”强，是网络安全的主要威胁。

（2）管理的欠缺:网络系统的严格管理是企业、机构及用户免受攻击的重要措施。事实上，很多企业、机构及用户的网站或系统都疏于这方面的管理。据 IT 界企业团体 ITAA 的调查显示，美国 90％的 IT 企业对黑客攻击准备不足。目前，美国 75％－85％的网站都抵挡不住黑客的攻击，约有 75％的企业网上信息失窃，其中 25％的企业损失在 25 万美元以上。

（3）网络的缺陷:因特网的共享性和开放性使网上信息安全存在先天不足。因为其赖以生存的 TCP/IP 协议族，缺乏相应的安全机制，而且因特网最初的设计考虑是该网不会因局部故障而影响信息的传输，基本没有考虑安全问题，因此它在安全可靠、服务质量、带宽和方便性等方面存在着不适应性。

（4）软件的漏洞或“后门”:随着软件系统规模的不断增大，系统中的安全漏洞或“后门”也不可避免的存在，比如我们常用的操作系统，无论是 Windows 还是 UNIX 几乎都存在或多或少的安全漏洞，众多的各类服务器、浏览器、一些桌面软件等等都被发现过存在安全隐患。可以说任何一个软件系统都可能会因为程序员的一个疏忽、设计中的一个缺陷等原因而存在漏洞，这也是网络安全的主要威胁之一。

(5)网络内部用户的误操作，资源滥用和恶意行为:再完善的防火墙也无法抵御来自网络内部的攻击，也无法对网络内部的资源滥用做出反应。

2、入侵检测系统 IDS，消除网络威胁

入侵检测技术 IDS 是一种主动发现网络隐患的安全技术。作为防火墙的合理补充，入侵检测技术能够帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、攻击识别和响应），提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息，并分析这些信息。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测。它可以防止或减轻上述的网络威胁：

(1)、识别黑客常用入侵与攻击手段

入侵检测技术通过分析各种攻击的特征，可以全面快速地识别探测攻击、拒绝服务攻击、缓冲区溢出攻击、电子邮件攻击、浏览器攻击等各种常用攻击手段，并做相应的防范。一般来说，黑客在进行入侵的第一步探测、收集网络及系统信息时，就会被 IDS 捕获。

(2)、监控网络异常通信

IDS 系统会对网络中不正常的通信连接做出反应，保证网络通信的合法性；任何不符合网络安全策略的网络数据都会被 IDS 侦测到并警告。

（3)、鉴别对系统漏洞及后门的利用

IDS 系统一般带有系统漏洞及后门的详细信息，通过对网络数据包连接的方式，对连接端口以及连接中特定的内容等特征进行分析，有效地发现网络通信中针对系统漏洞进行的非法行为。

（4)、完善网络安全管理。

IDS 通过对攻击或入侵的检测及反应，可以有效地发现和防止大部分的网络犯罪行为，给网络安全管理提供了一个集中、方便、有效的工具。使用 IDS 系统的数据监测、主动扫描、网络审计、统计分析功能，可以进一步监控网络故障，完善网络管理。

3、NetEye IDS 2.2，给您提供全面的安全

NetEye IDS 2.2 是东软股份最新开发的具有自主版权的网络入侵监测系统。利用独创的数据包截取技术对网络进行不间断的监控，扩大网络防御的纵深，同时采用先进的基于网络数据流实时智能分析技术判断来自网络内部和外部的入侵企图，进行报警、响应和防范。是防火墙之后的第二道安全闸门。同时具备强大的网络信息审计功能，可对网络的运行，使用情况进行全面的监控、记录、审计和重放，使用户对网络的运行状况一目了然。并且提供网络嗅探器和扫描器用于分析网络的问题，定位网络的故障。不但保障网络的安全，同时保障网络的健康运行。NetEye 入侵检测系统可对自身的数据库进行自动维护，不需要用户的干预。学习和使用及其简易，不对网络的正常运行造成任何干扰，是完整的网络审计，监测，分析和管理系统。NetEye IDS 可方便的进行大规模部署，便于进行集中管理。NetEye 入侵检测系统可与防火墙联动，自动配置防火墙策略，配合防火墙系统使用，可以全面保障网络的安全，组成完整的网络安全解决方案。

全面高效，可靠易用的网络综合健康管理平台是 NetEye IDS 的设计理念。

二、系统结构

NetEye IDS 2.2 采用客户/服务器结构，由检测引擎和管理主机组成。

- **检测引擎**

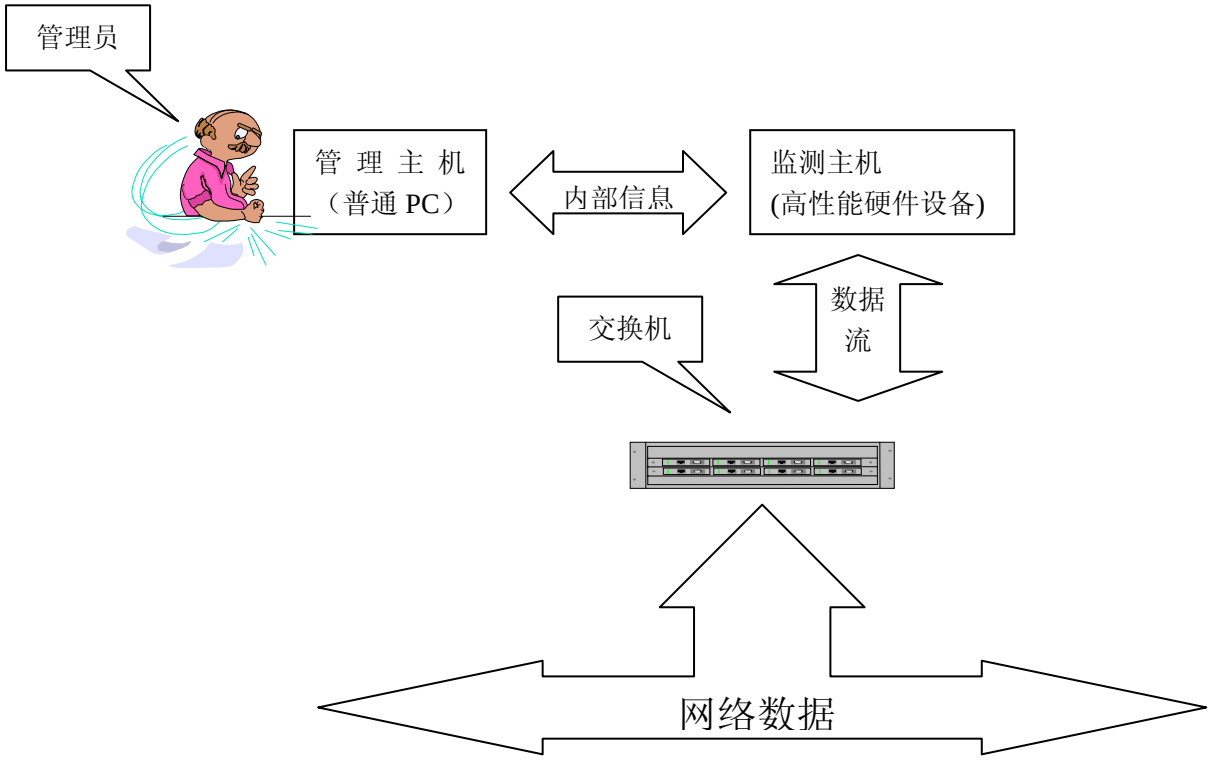
检测引擎是一个高性能的专用硬件，运行专用的安全操作系统，对网络中的所有数据包进行记录和分析。在重组网络数据流的基础上，综合利用模式匹配，异常识别，统计分析，协议分析，行为分析等多种方法判断是否有异常事件发生，并及时报警和响应。同时记录网络中发生的所有事件，以便事后重放和分析。

- **NetEye IDS 管理主机**

运行于 Windows 操作系统的中文图形化管理软件。 使用加密通道和检测引擎安全通信，可以查看分析一个或多个检测引擎，进行策略配置，系统管理。显示攻击事件的详细信息和解决对策。恢复和重放网络中发生的事件。提供工具分析网络运行状况。并可产生图文

并茂的报表输出。

整个系统结构示意图如下：



三、功能模块简介

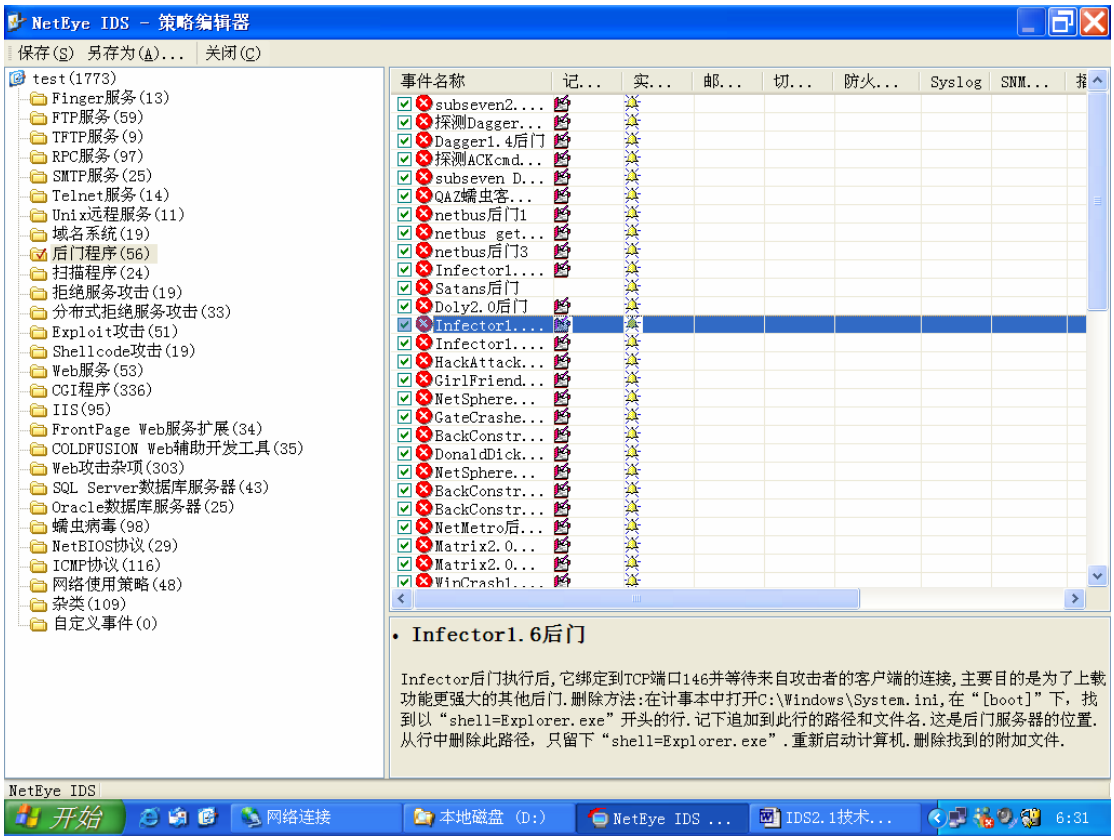
NetEye IDS 入侵监测系统 2.2 主要包括以下主要功能模块：

1. 网络攻击与入侵检测功能

利用数据流智能重组，轻松处理分片和乱序数据包。综合使用模式匹配，异常识别，统计分析，协议分析，行为分析等多种方法综合检测1700种以上的攻击与入侵行为。系统提供默认策略，用户也可以方便的定制策略。系统自带数据库存储攻击与入侵信息以便随时检索。系统还提供详细的攻击与入侵信息，包括发生时间、发起主机与受害主机地址、攻击类型、以及针对此类型攻击的详细解释与解决办法。并可采取实时报警，声音报警，记录到数据库，电子邮件报警，SysLog报警，SNMP Trap 报警 ，Windows 日志报警，Windows 消息报警，切断攻击连接，以及和防火墙联动，运行自定义程序等多种响应方式。管理员可根据检测到的攻击信息加强系统安全，并追究攻击者责任。举例如下：

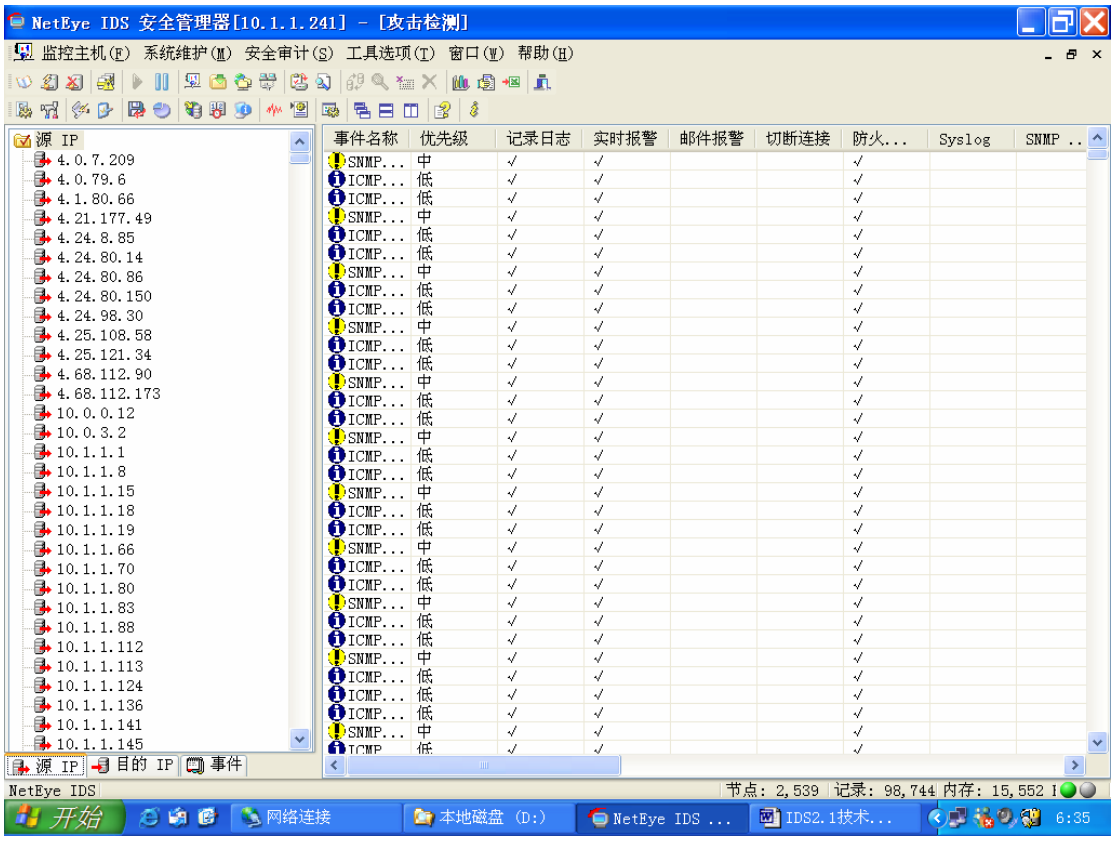
- 策略编辑：

用户可根据自身网络状况定义相应策略。有效的提高了入侵检测的针对性和有效性。同时，用户也可自定义攻击检测规则，扩充检测范围。



- 攻击事件查询：

查询历史攻击事件，分析攻击者的行为。

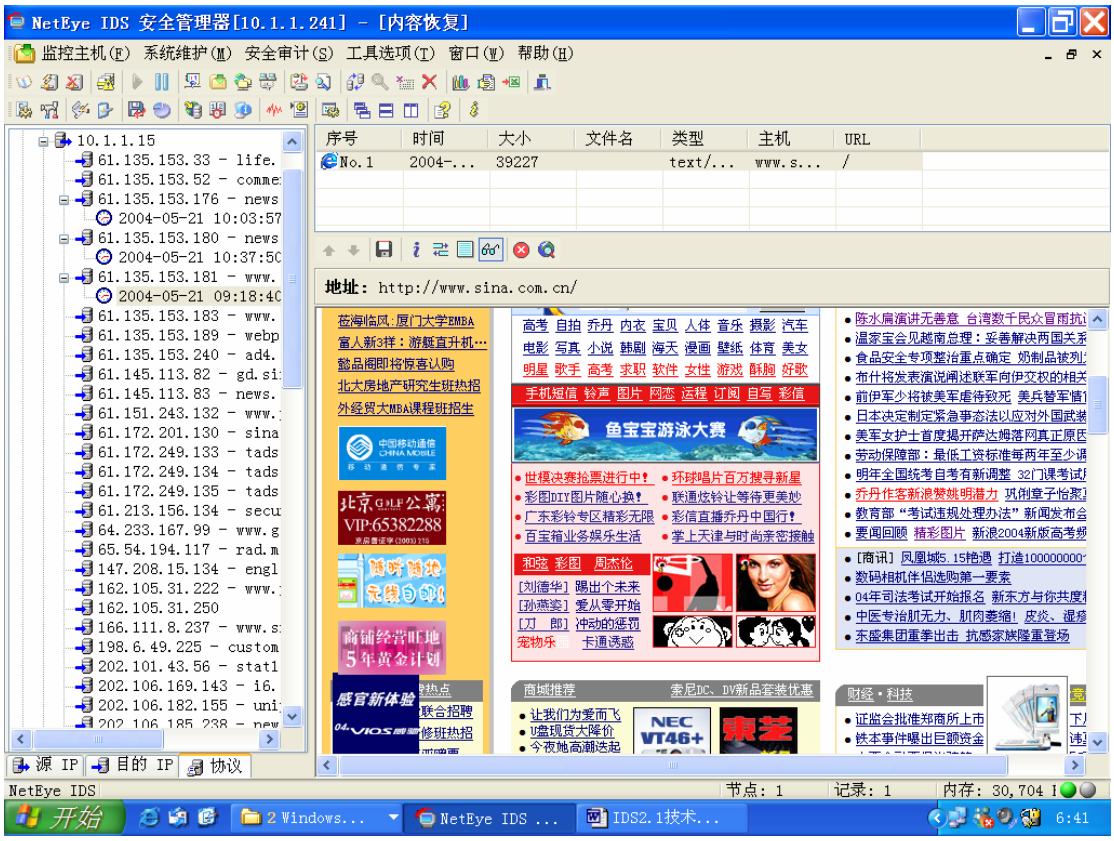


2. 多种通信协议内容恢复功能

NetEye IDS 2.2 入侵监测系统针对多种常用的应用协议（HTTP、FTP、SMTP、POP3、TELNET， NNTP, IMAP, DNS, Rlogin, Rsh, MSN, Yahoo MSG）数据连接的内容恢复的功能，能够完全记录通信的过程与内容，并将其回放。并可自定义协议，便于扩充。此功能对于了解攻击者的攻击过程，监控内部网络中的用户是否滥用网络资源,发现未知的攻击具有很大的作用。举例如下：

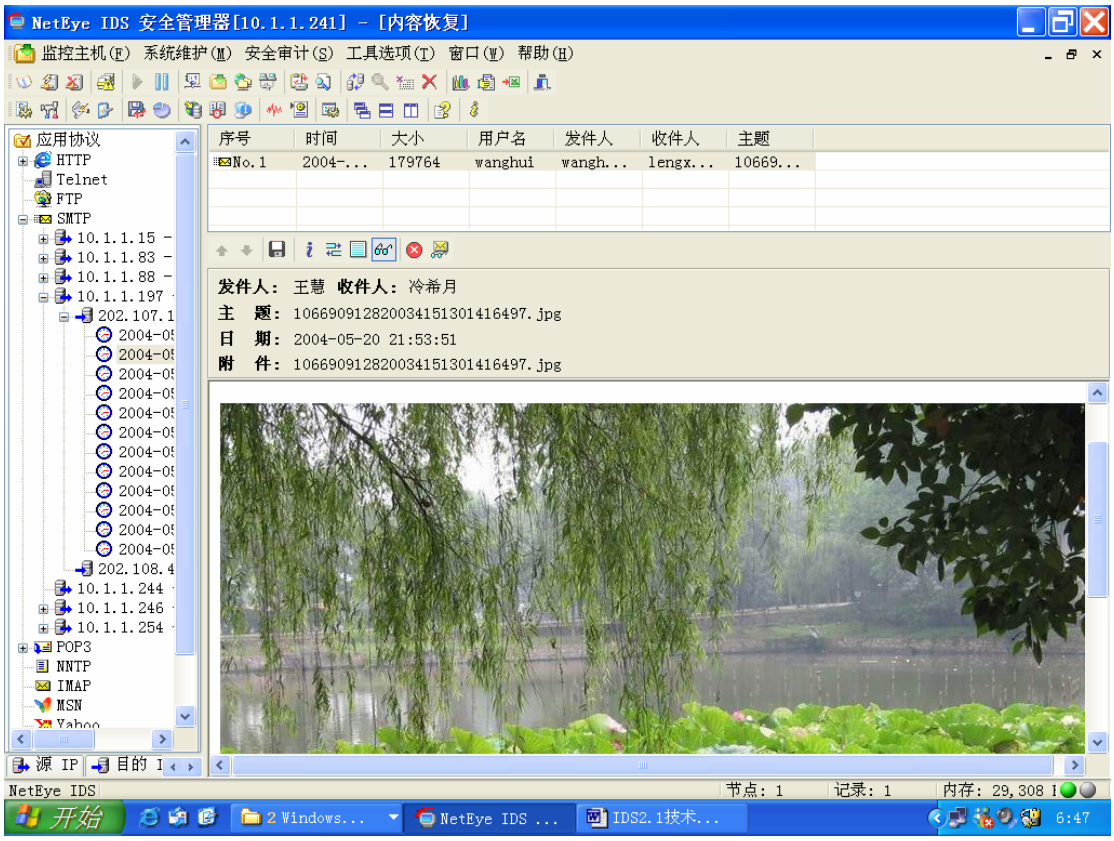
- HTTP通信内容恢复：

可恢复HTTP通信的所有内容，包括文本和图形。包括原始的会话信息。便于分析基于HTTP协议的攻击行为。



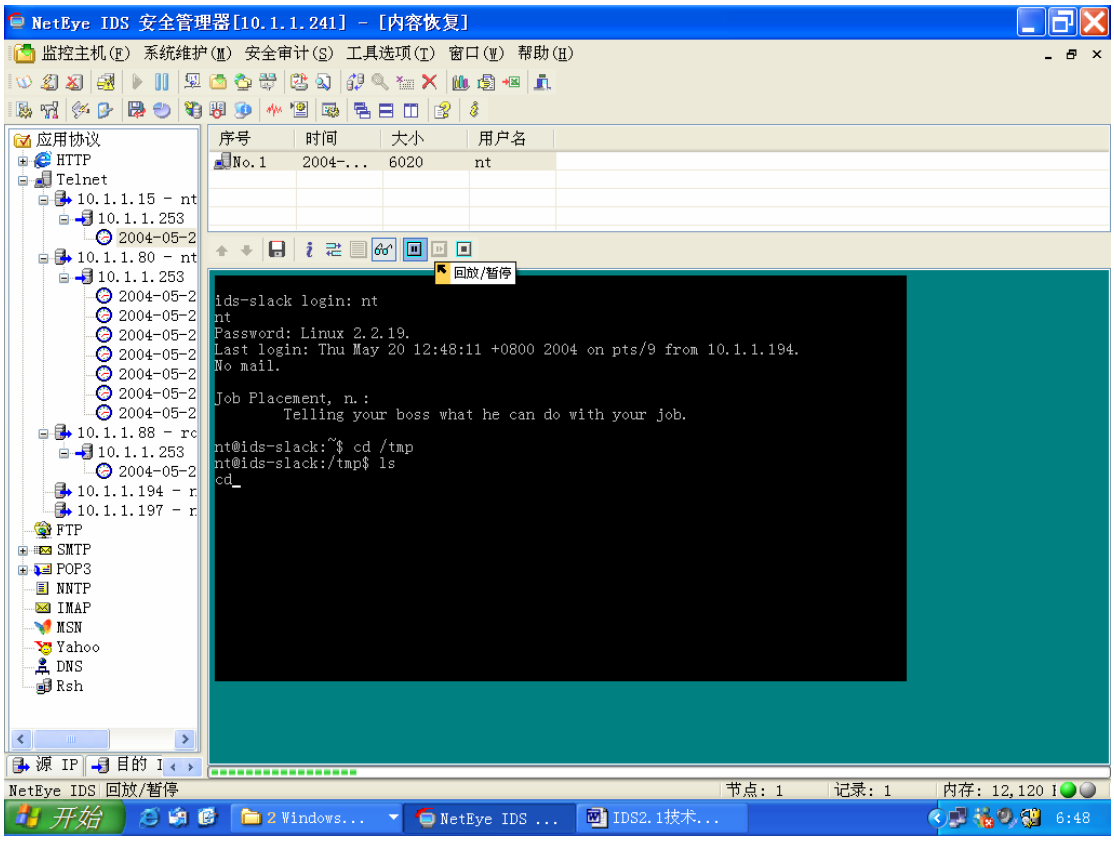
- POP3或SMTP协议内容恢复。

可完整的恢复电子邮件的标题，正文，附件，会话信息。并可根据管理员权限决定是否显示邮件内容，做到安全和用户隐私的兼顾。



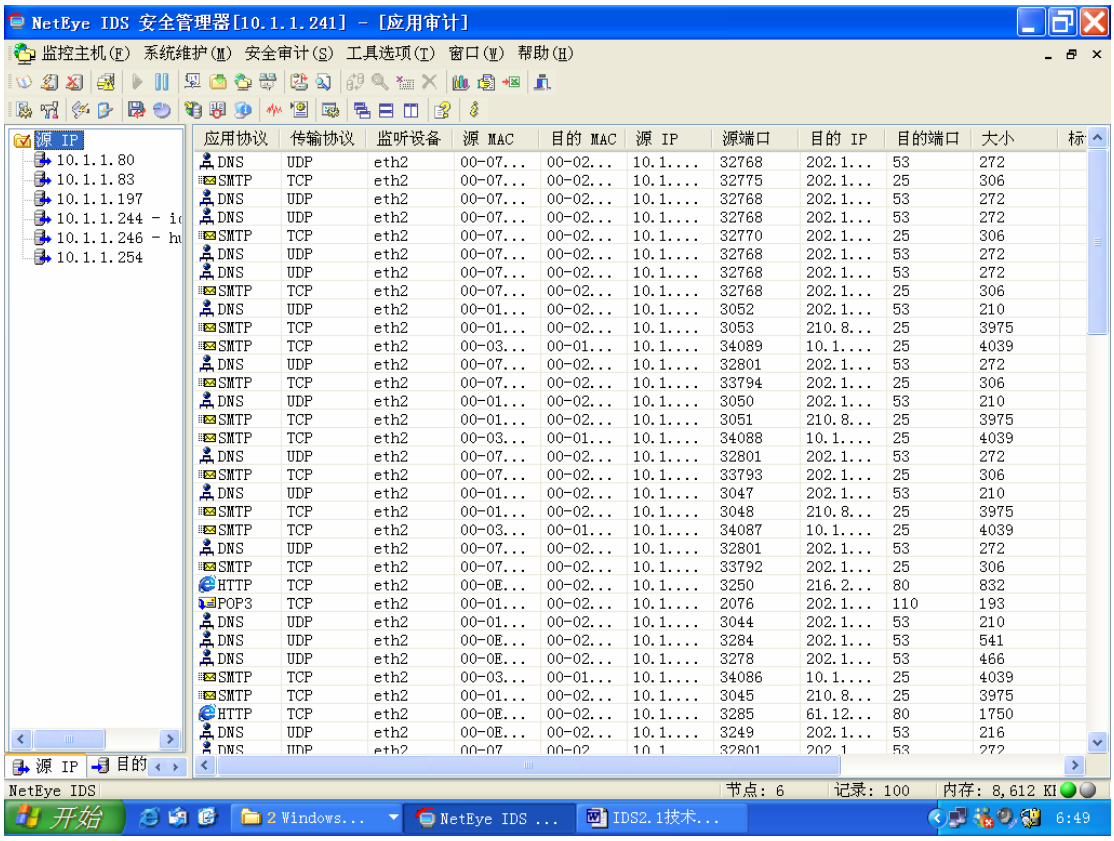
- TELENT 协议内容回放

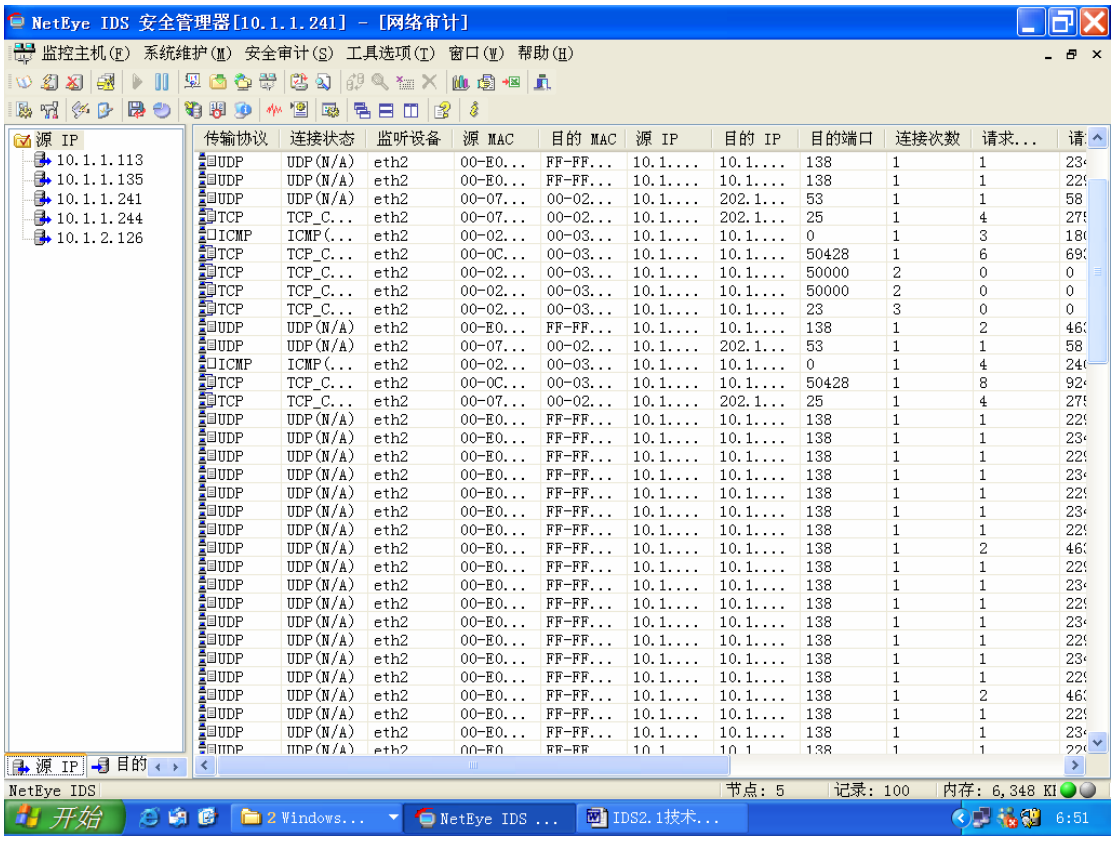
对TELENT等协议的会话进行完整重放，便于管理员了解攻击者或恶意用户做过的操作。



3．应用审计和网络审计功能

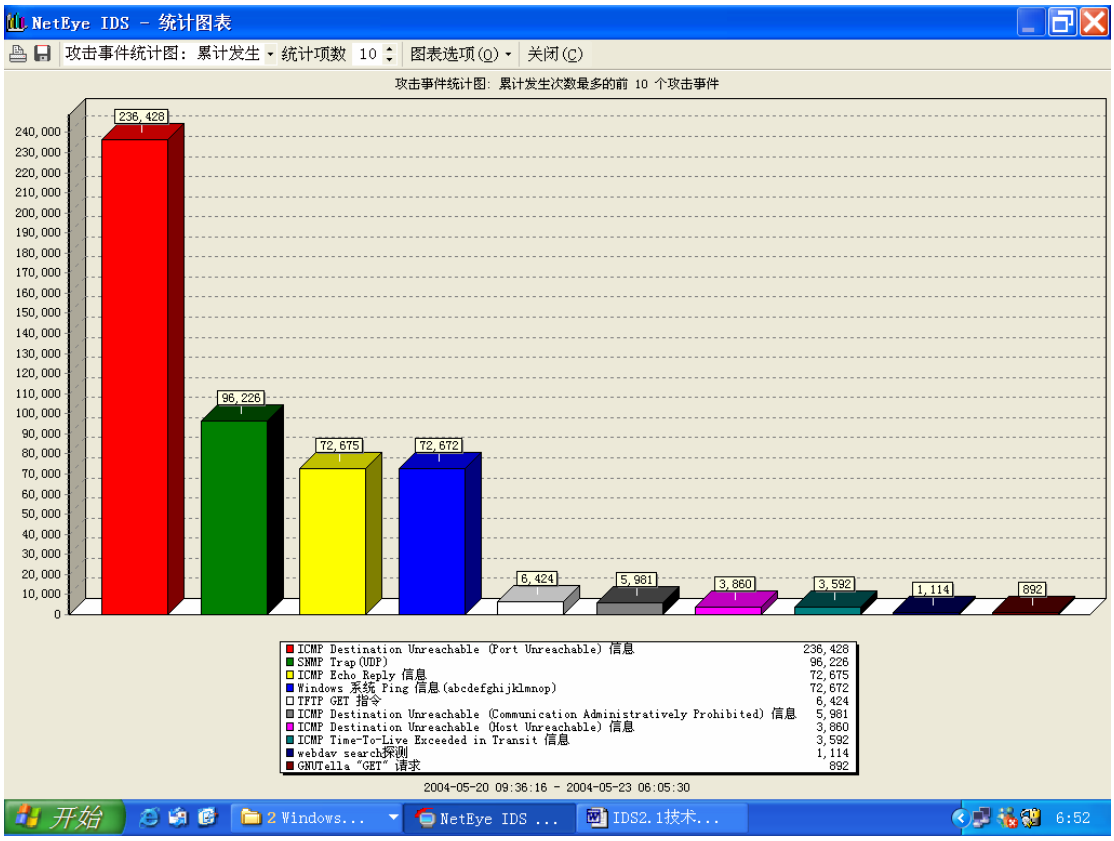
全面审计网络中发生的所有应用和连接，是完整的网络审计日志

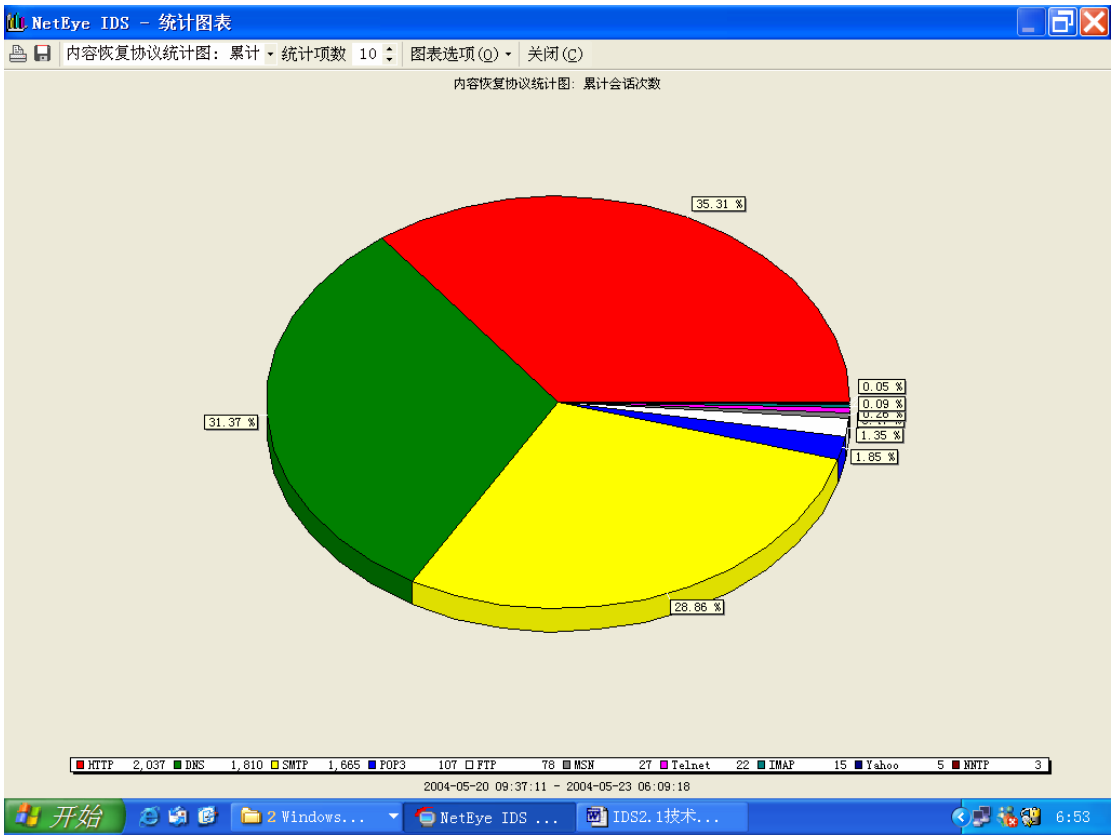




4．图表显示网络信息功能

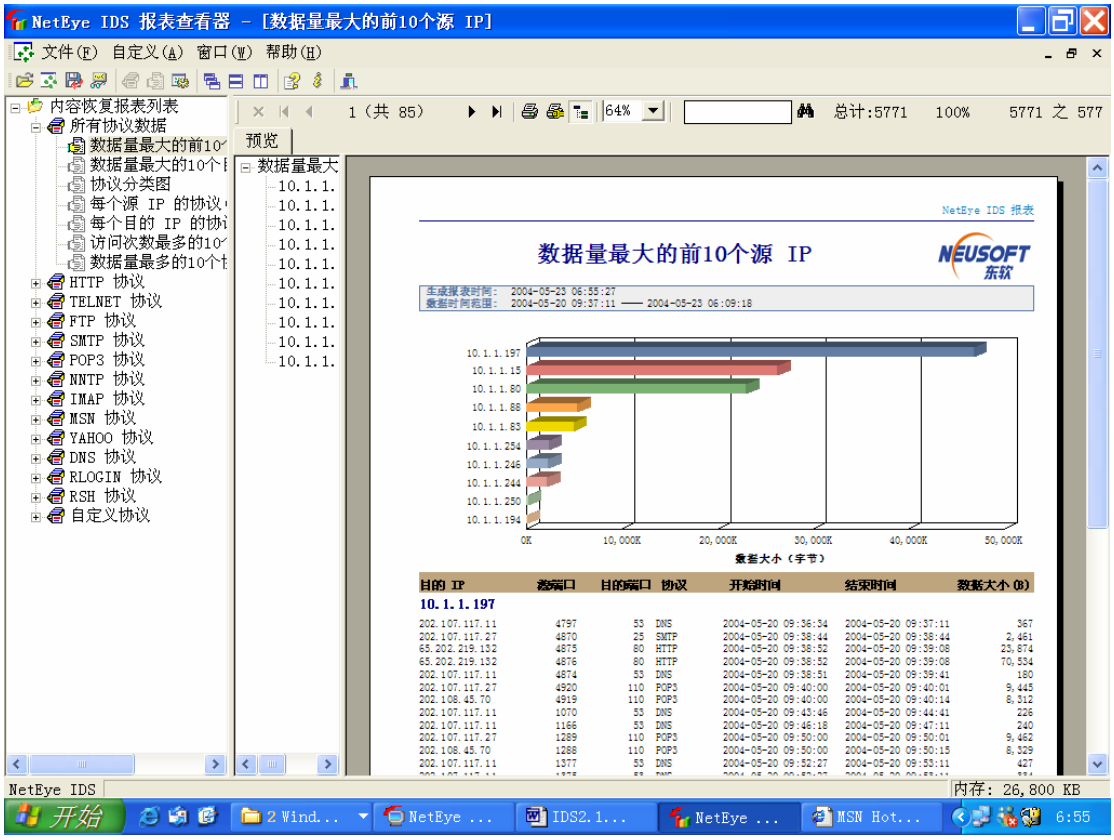
用多种图表全面显示网络的安全和使用状况，便于管理员直观的了解网络状况。

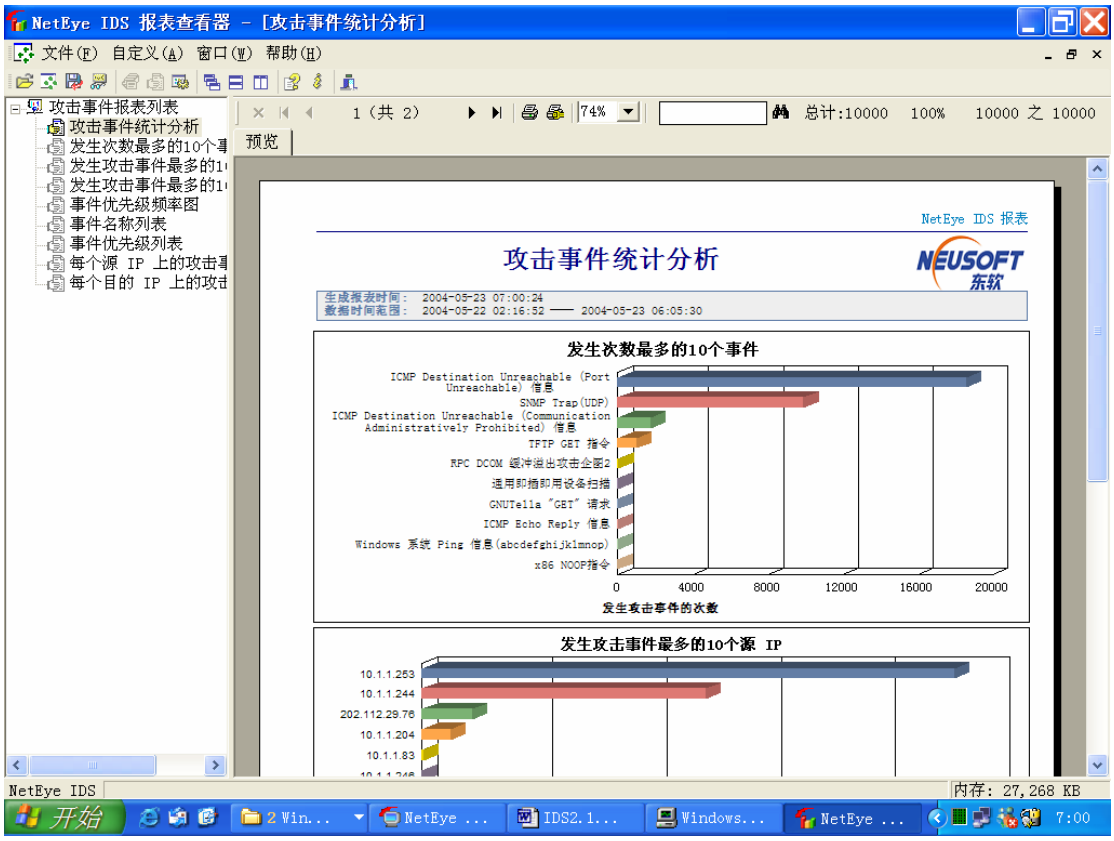

NetEye IDS - 统计图表
攻击事件统计图：累计发生
统计项数 10
图表选项(O)
关闭(C)
攻击事件统计图：累计发生次数最多的前 10 个攻击事件
240,000
230,000
220,000
210,000
200,000
190,000
180,000
170,000
160,000
150,000
140,000
130,000
120,000
110,000
100,000
90,000
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
236,428
96,226
72,675
72,672
6,424
5,981
3,860
3,592
1,114
892
ICMP Destination Unreachable (Port Unreachable) 信息 236,428
SNMP Trap(UDP) 96,226
ICMP Echo Reply 信息 72,675
Windows 系统 Ping 信息(abcdefghijklmnop) 72,672
TFTP GET 指令 6,424
ICMP Destination Unreachable (Communication Administratively Prohibited) 信息 5,981
ICMP Destination Unreachable (Host Unreachable) 信息 3,860
ICMP Time-To-Live Exceeded in Transit 信息 3,592
webdav search探测 1,114
GNUTella "GET" 请求 892
2004-05-20 09:36:16 - 2004-05-23 06:05:30
开始
2 Windows...
NetEye IDS ...
IDS2.1技术...
6:52


NetEye IDS - 统计图表
内容恢复协议统计图：累计
统计项数 10
图表选项(O)
关闭(C)
内容恢复协议统计图：累计会话次数
35.31 %
31.37 %
28.86 %
1.85 %
1.35 %
0.05 %
0.09 %
HTTP 2,037 DNS 1,810 SMTP 1,665 POP3 107 FTP 78 MSN 27 Telnet 22 IMAP 15 Yahoo 5 NNTP 3
2004-05-20 09:37:11 - 2004-05-23 06:09:18
开始
2 Windows...
NetEye IDS ...
IDS2.1技术...
6:53

5．报表功能

NetEye IDS 2.2 入侵监测系统提供灵活，方便， 图文并茂的报表功能。便于管理员检索和保存信息。举例如下：

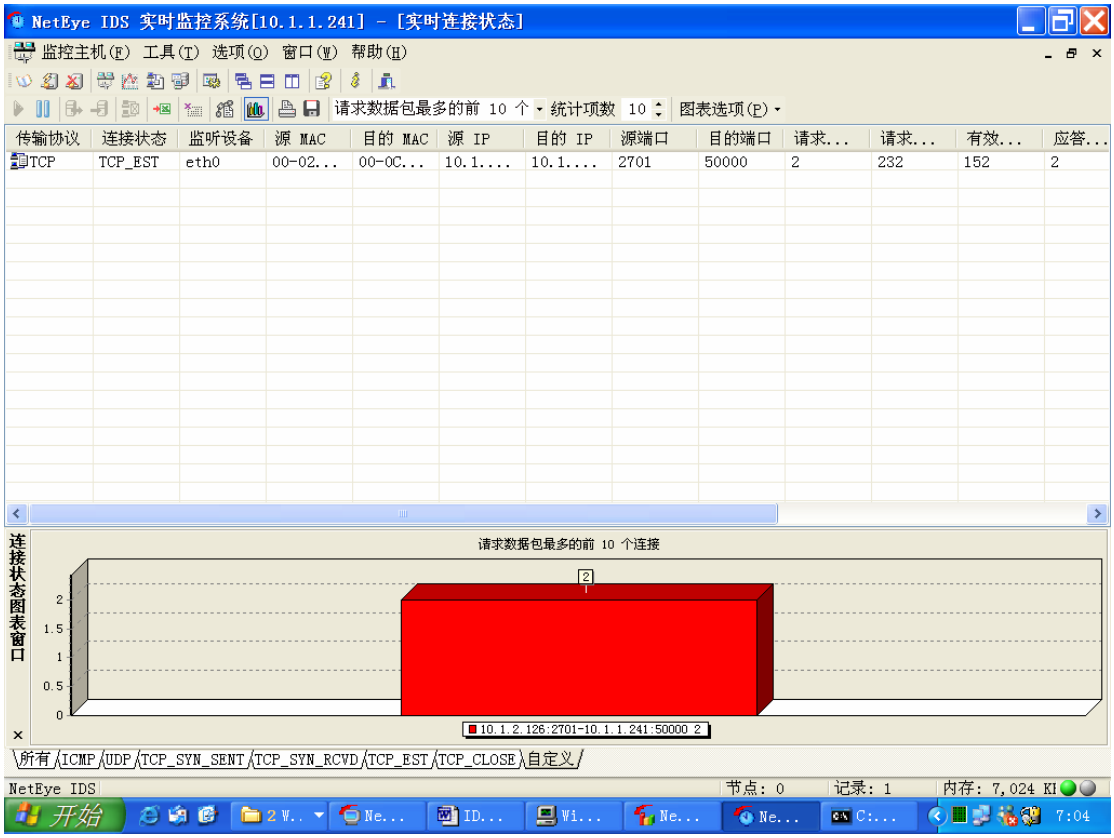




6. 实时网络监控功能

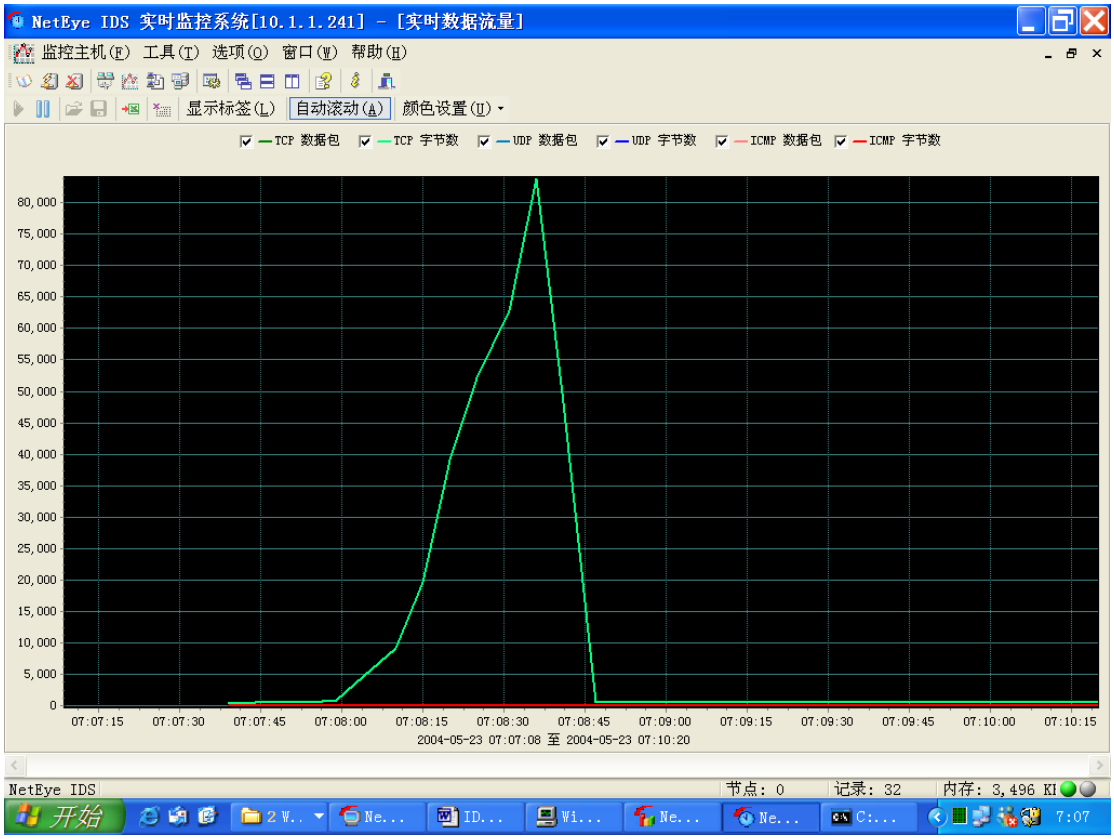
- 实时连接监控

实时监控网络当前连接，显示网络用户信息，可随时断开可疑连接，最大限度的保证网络安全。



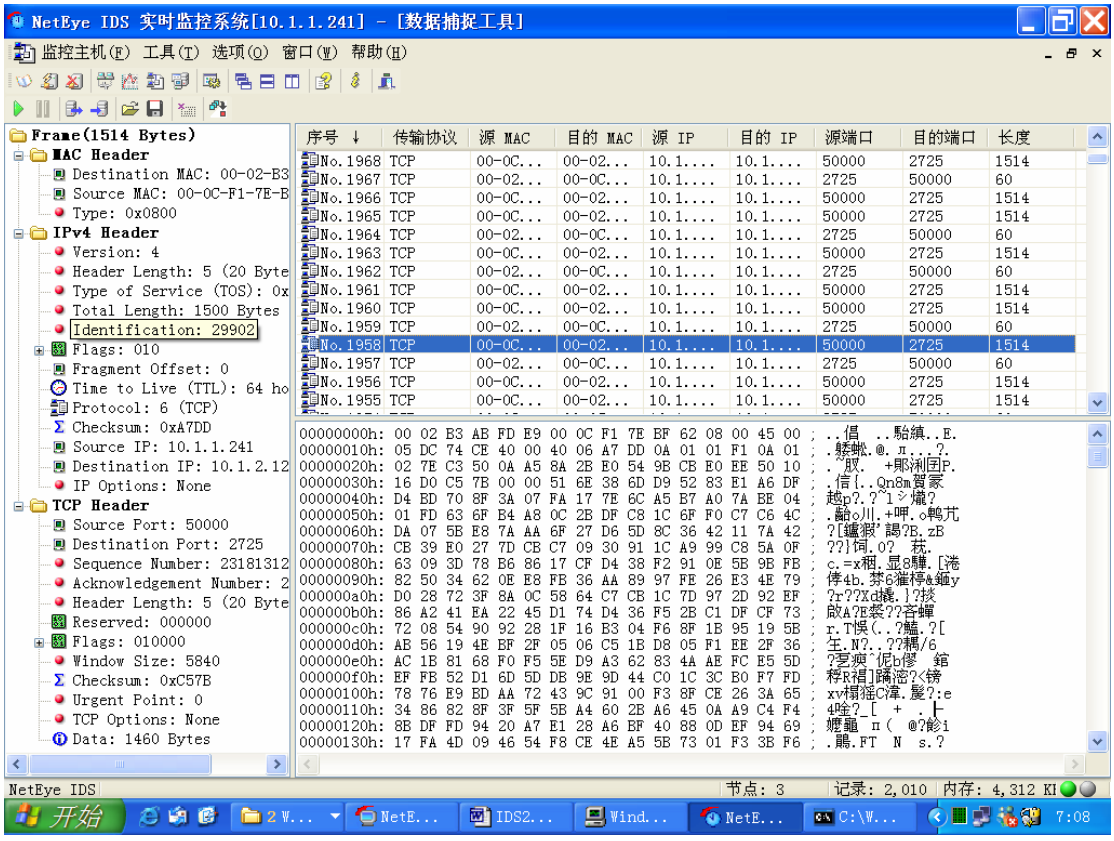
- **实时网络流量监控**

  实时监控网络当前流量状况，便于用户发现网络异常，定位网络故障。



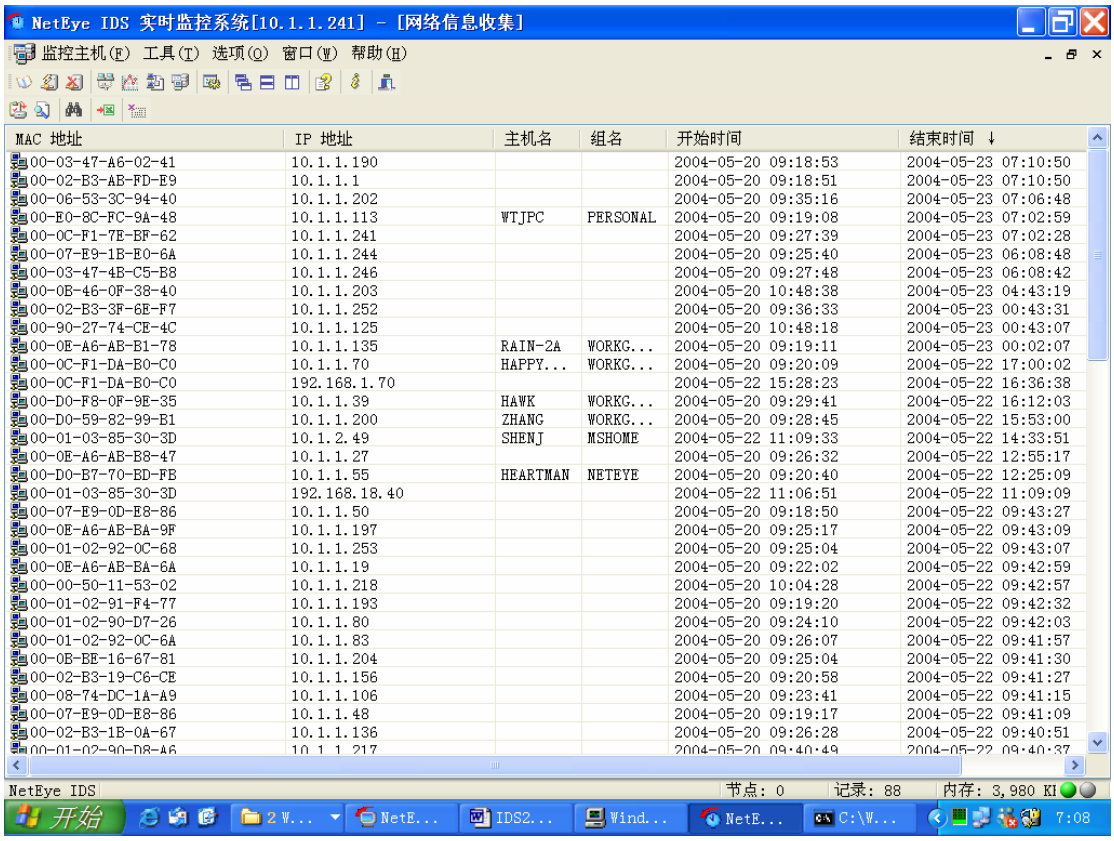
- 网络嗅探器

对网络中的数据包进行分析，解码。查找网络问题。



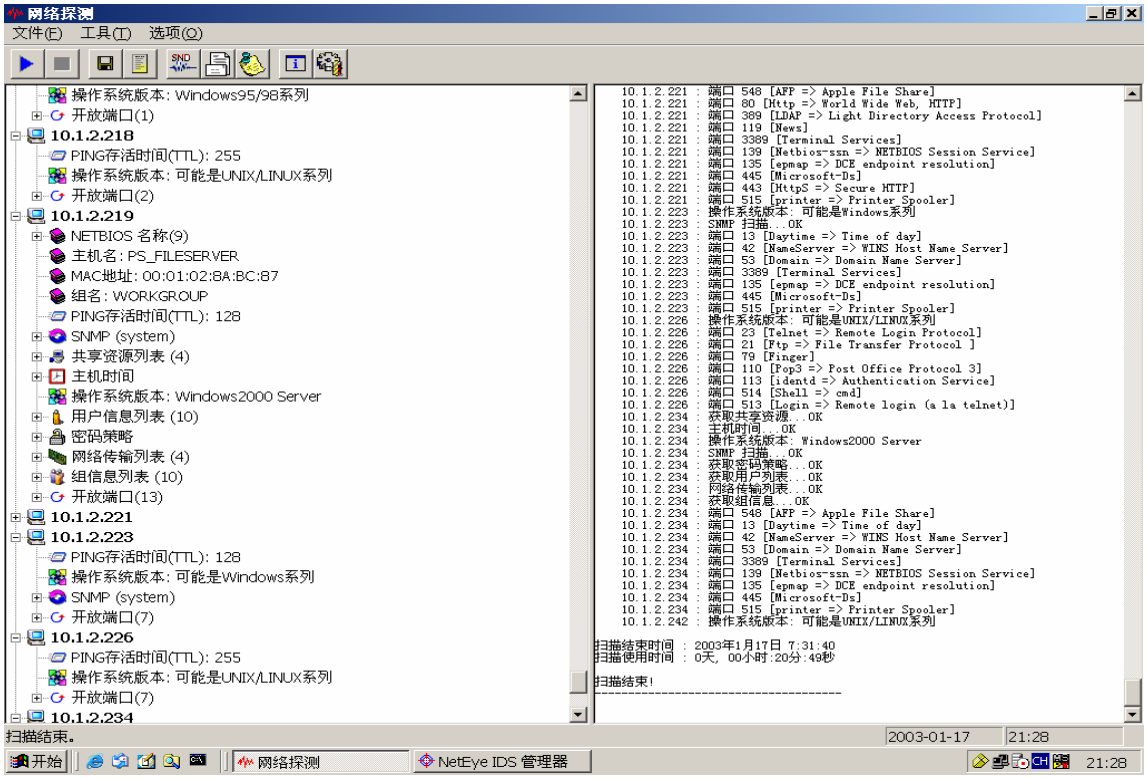
- 网络用户信息收集

全面收集网络用户信息，包括 IP 地址，MAC 地址，用户名，组名，便于确定攻击者身份，并可方便的解决 IP 地址冲突等网络故障。



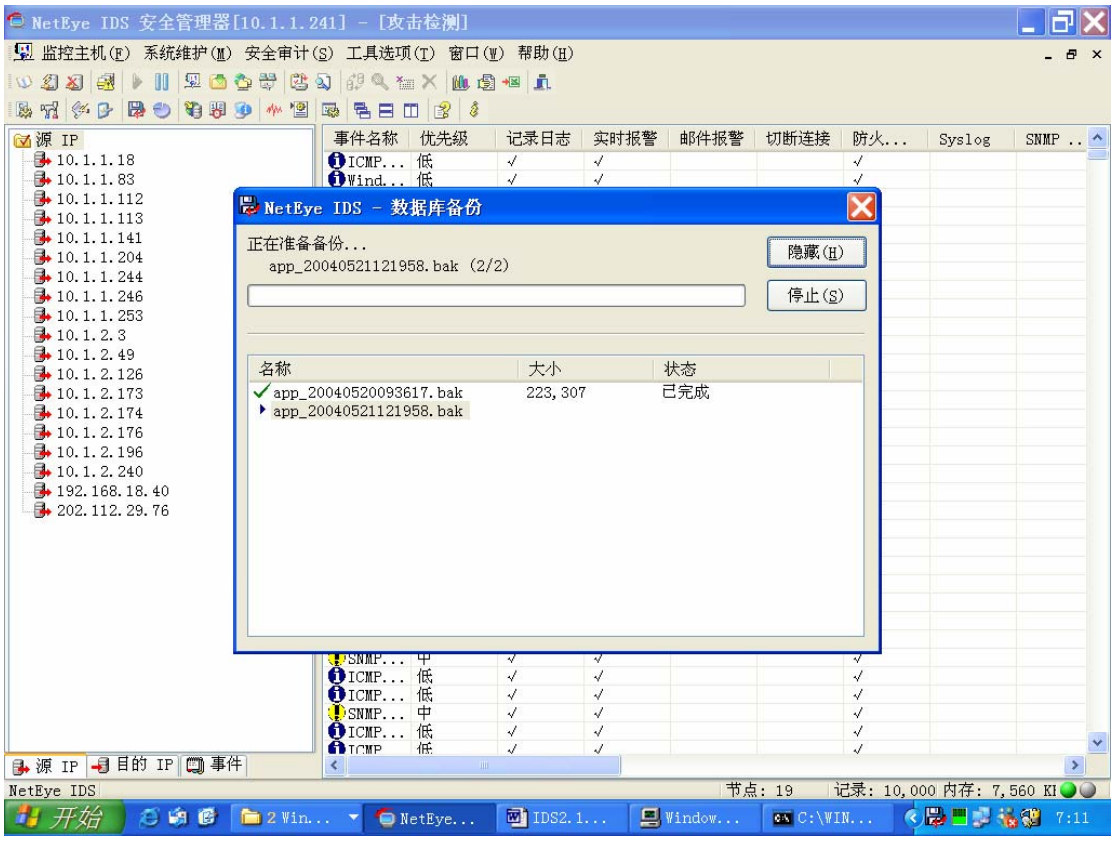
7. 网络扫描器。

主动扫描网络，发现网络问题。

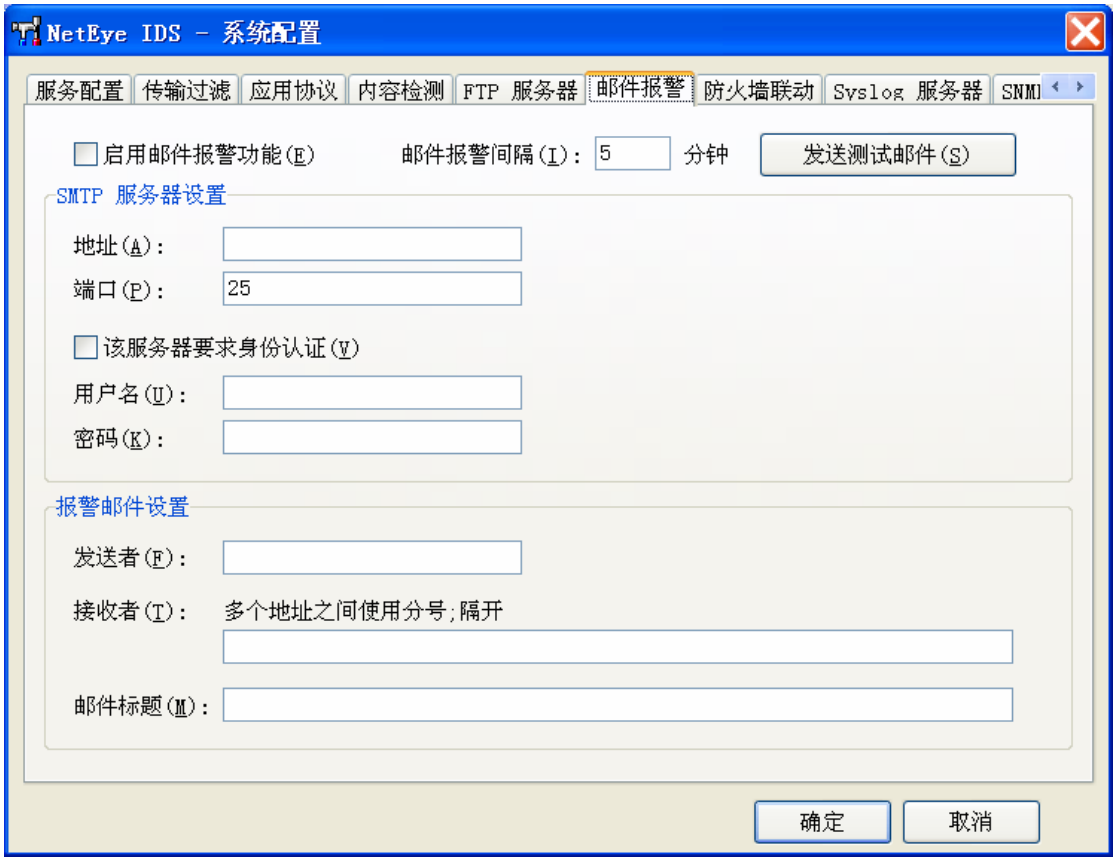


8．数据备份恢复功能

采用多种策略，手动备份或自动备份事件数据库，完成全面的信息审计。



9．其它辅助管理，配置工具。



四、技术特点

NetEye IDS 2.2采用了多种先进技术，在实用的基础上做到了稳定、高效，易用、易维护。

- 高效独特的数据截取技术

直接从内核接收网络数据，减少中间环节，缩短了系统调用时间，从而提高截取网络数据包的速度和效率，系统运行效率高，可以监测高速网络，丢包率极低。经各种测试证明，NetEye IDS 性能极为优秀。

- 完整的数据流恢复技术

完整的数据重组，恢复技术。把网络连接作为数据流分析，而不是一个个孤立的数据包。完全处理数据分片和乱序的问题。

- 网络通信完全监测。

记录网络上的一切数据包。尽量做到实时分析，当遇到网络流量高峰的时候，可以

根据记录下来的数据流进行事后分析。入侵活动可以具有很大的时间跨度和空间跨度，有预谋的入侵活动往往有较周密的策划、试探和技术性准备，一个入侵活动的各个步骤有可能在一段相对长的时间跨度和相当大的空间跨度之上分别完成，给预警带来困难。事后分析可以全面完整的处理此类攻击事件。

- 中文图形化管理

提供基于 WINDOWS 系统的中文图形化管理工具，使一切信息查看、管理和配置都变得极其方便，简单易学。全部攻击与入侵事件的描述都使用中文，清楚明了。整体的设计使其非常适合中国人使用。

- 使用模式匹配，异常识别，统计分析，协议分析，行为分析等多种方法识别入侵

系统拥有入侵事件及入侵模式数据库，可以检测 1700 多种网络入侵和攻击行为。采用多种方法全面分析攻击而不是依赖单一的检测手段。系统漏洞、系统后门、CGI 漏洞、系统扫描、缓冲区溢出攻击、蠕虫病毒等各种危害系统的入侵和攻击都可轻易识别。入侵模式数据库可非常容易的进行升级以检测最新攻击。

- 操作简单，自动维护，不需用户干预

系统智能程度相当高，可用性极好。操作简单，易于掌握，自身维护自身数据库，自动处理各种异常情况，无须用户干预，维护代价小。系统预装默认监控规则，无须用户编写和加载。可以说是最容易使用的 IDS。

- 接入简便，不需改变现有网络拓朴结构

系统的接入非常方便，只需根据网络的物理结构将它连接到交换机的广播口或共享式 HUB 上即可立即开始工作，支持 802.1q 和 PPPOE 等协议解码。支持多监听端口和网桥接入等监听方式。而不需要改变网络的物理结构及网络逻辑划分和配置，原有网络拓朴结构依然完好无损，网络通信毫无影响。

- 支持多用户分权管理和分布式部署，便于监控大型网络

管理权限细分，可进行多级用户分权管理。可安装于大型网络的各个物理子网中，分布式监控网络的各个部分，可进行多级分布式管理，达到分布安装，全网监控，集中管理。

- 实时监控网络当前运行状况，为用户人为监控和分析提供有力工具

提供实时连接报告，当前网络中用户行为一目了然，可以实时地从中直接发现网络中用户滥用网络资源的情况，如访问未授权的服务器等。另外，网络扫描等异常行为也可从中看出。

- 多样的攻击响应方式

可提供实时报警，声音报警，记录到数据库，电子邮件报警，SysLog 报警，SNMP Trap 报警 ，Windows 日志报警，Windows 消息报警，切断攻击连接，以及和防火墙联动，运行自定义程序等多种响应方式，便于管理员快速准确的对攻击做出反应。

- 全面的内容恢复，支持多种常用协议

除了可以对已知的入侵行为进行监测外，系统还可以对网络应用层的协议进行恢复，目前实现的主要协议有：HTTP、FTP、SMTP、POP3、TELNET，NNTP, IMAP, DNS, Rlogin, Rsh, MSN, Yahoo MSG。还可自定义协议，便于扩充。管理员可以很直观地看到任何人的信件内容（包括附件）、TELNET 或者 FTP 用户所作的操作、都去过哪些网站和看过哪些内容（包括文字和图片的再现）。通过此功能不但可以简单的发现攻击事件，而且可以重现整个攻击过程；不但可以发现外部黑客的攻击，而且可以发现内部用户的恶意行为；不但可以发现已知攻击，而且可以发现未知攻击。

- 灵活的查询，报表功能

可对网络中的攻击事件，访问记录进行灵活的查询，并可根据查询结果输出图文并茂，美观的报表。

- 自身的高度安全性和隐蔽性

系统本身采用专用硬件，运行安全的操作系统，检测引擎和管理主机之间通讯采用 128 位加密。检测引擎为黑洞式结构，监测口无 IP,攻击者无法发现，保证了自身的安全性和隐蔽性。

- 集成的网络管理和诊断平台

系统集成多种网络分析，诊断工具，便于发现网络故障，定位网络问题。

- 强大的信息审计功能

全面审计网络信息，并可方便的进行备份和恢复。

- 全面的网络健康管理平台

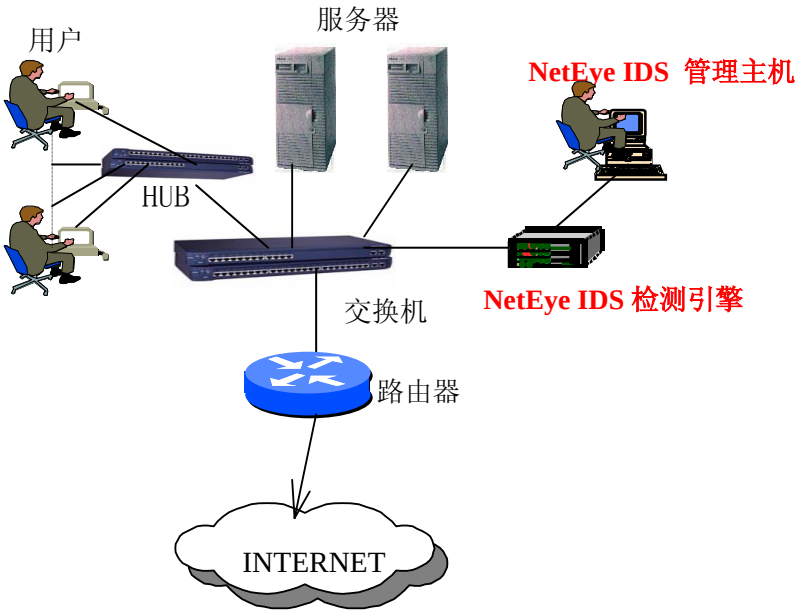
依靠单一的技术无法处理日益复杂的网络安全和故障问题。NetEye IDS 综合采用多种技术全面处理网络风险。通过被动监听和主动发现方式的结合，攻击识别和内容恢复的结合，实时监控和事后审计的结合。检测攻击和检测网络故障的结合。NetEye IDS 构成了全面的网络健康管理平台。

五、典型应用示例

- **简单区域网应用示例**

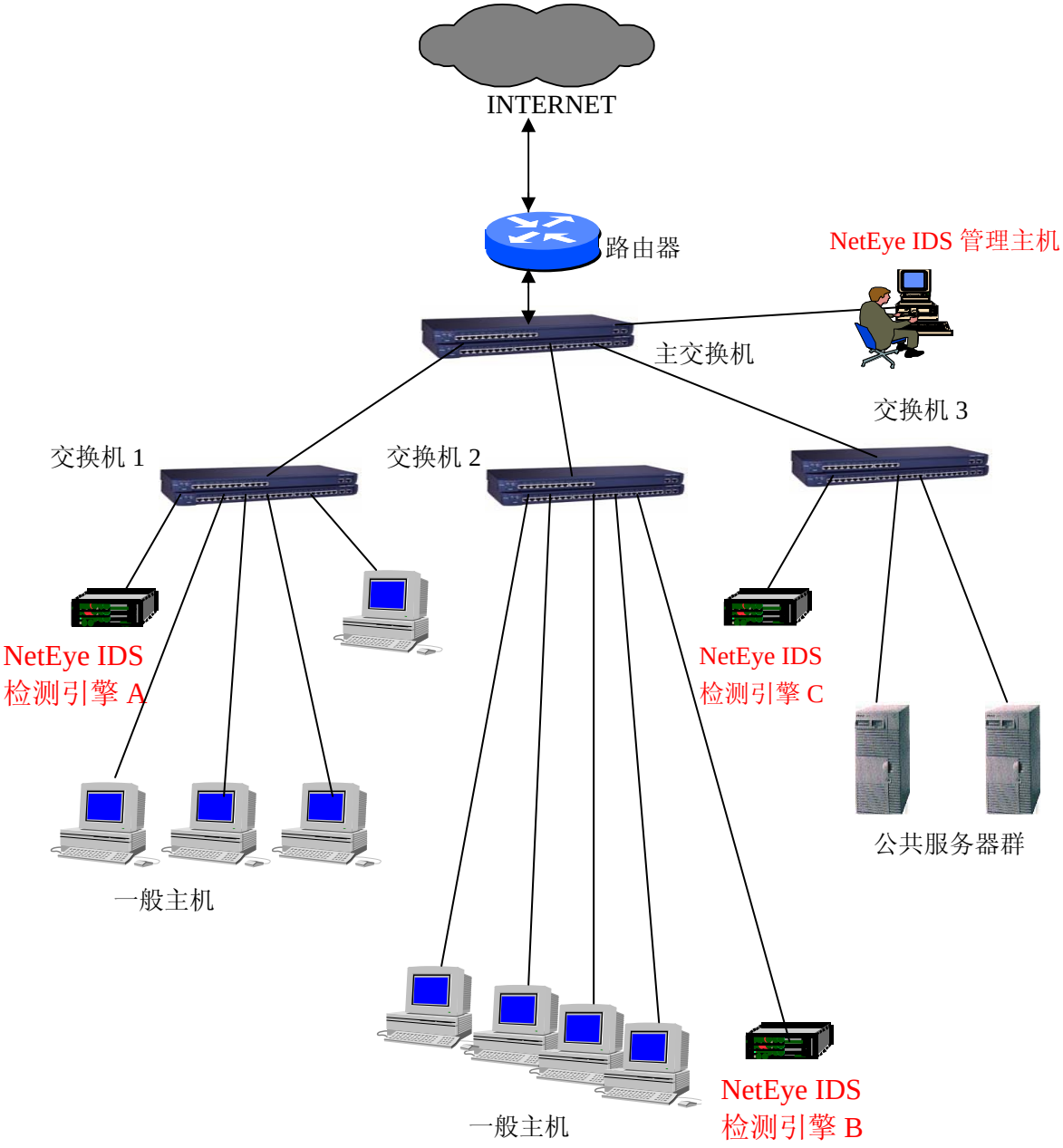
此种区域网连接较为简单，内部网络中各机构的主机使用共享式 HUB 连接到交换机上，或主机直接连接到交换机上，交换机不设 VLAN，交换机再通过路由器接入 INTERNET。这种情况下，将 NetEye IDS 监测主机接到交换机的广播口（监听口）即可监听到内部网络间的所有通信及内部网络到 INTERNET 的所有通信。

网络结构示意图如下：



- **分布式监测应用示例**

网络结构相对复杂，内部网络中各机构间使用交换式 HUB 或从交换机连接到主交换机上，通过主交换机连接路由器接入 INTERNET，此时，在主交换机的广播口（监听口）上无法监听到从交换机上的机器间的通信，为了全面监控网络，捕捉内部网间的恶意攻击与入侵行为，就需要将 NetEye IDS 监测主机接到从交换机上。这种情况下的网络结构示意图如下：


INTERNET
路由器
NetEye IDS 管理主机
主交换机
交换机 3
交换机 1
交换机 2
NetEye IDS
检测引擎 A
NetEye IDS
检测引擎 C
公共服务器群
一般主机
一般主机
NetEye IDS
检测引擎 B

沈 阳 东 软 软 件 股 份 有 限 公 司
地址：沈阳浑南高新技术产业开发区·东大软件园
传真：024-23784036　邮编：110179
网址：www.neusoft.com