网络卫士信息审计系统

技术白皮书

北京天融信公司

2004 年 6 月

注意

天融信网络信息审计系统

技术白皮书

本资料将定期更新，如欲获取最新相关信息，请访问天融信公司网站：www.topsec.com.cn
您的意见和建议请发送至：PLMC@topsec.com.cn

北京天融信公司
北京市海淀区知春路49号希格玛大厦4层，100080
4F Beijing Sigma Center No.49,Zhichun Road，Hai dian District, Beijing
电话(TEL)：010-82611122
传真（FAX ）：010-62304552

电子信箱：market@topsec.com.cn

公司简介

北京天融信公司是中国网络安全行业的领先企业，是目前国内最大的专业从事网络安全技术研究、产品开发和安全服务的高科技企业。同时天融信公司正向集团化、国际化迈进，努力成为中国网络安全领域内最优秀最具国际竞争力的企业。

天融信公司最早成立于 1995 年，目前公司总部设在北京，形成北京、武汉、成都三大研发中心，同时在上海、广州、西安、沈阳、成都、长沙、武汉等 29 个省市设有分支机构，拥有 500 多名信息安全专业研发、咨询与服务人员。

天融信公司于 1996 年推出了填补国内空白的中国第一套自主版权的防火墙产品，随后几年又推出了 VPN、IDS、安全监控、信息审计、安全管理、过滤网关等产品。组织并构建了 TOPSEC 联动协议安全标准，提出了一套集各类安全产品及集中管理、集中审计为一体的全面的、联动的、高效的、易于管理的 TOPSEC 安全解决方案。

2000 年至 2003 年，天融信公司连续四年市场份额均居国内安全厂商之首。特别指出的是，国际权威咨询机构 IDC 统计：天融信 2003 年下半年防火墙市场份额达到了 17.28%，名列所有国内外安全厂商第一位，打破了国内安全厂商长期处于弱势地位的局面，为国内网络安全企业树立了新的里程碑。到目前为止，天融信公司拥有覆盖全国，涉及政府、电信、金融、军队、能源、交通、教育、流通、邮政、制造等行业的万余家客户群体。

天融信 2003 年全年的防火墙市场份额达到了 15.17%，占所有安全产品市场份额的 7.77%，位居国内安全厂商之首，全年市场份额仅略次于国际厂商 Cisco。可以看出，天融信公司已经远远走在其他国内厂商的前面，而且在与国外领先厂商的竞争中，不仅在市场份额上首次超过他们，并在技术产品、解决方案及服务上逐步缩小与国外厂商的差距，进一步巩固并加强了其在行业的领先地位。

目　　录

第 1 章 信息审计系统概述

1.1 网络安全现状

当前政府、银行、企业等纷纷连接到互联网中，而且很多核心业务都基于网络来实现，网络逐渐成为这些用户完成相关业务的非常重要的、不可或缺的手段。同时，网络的不断普及也带来了其安全问题。据统计，基于网络的信息失窃在过去 5 年中以 200%以上的速度递增。深受其害的不仅有 Yahoo、Amazon、CNN 等商业网站或企业，还有大量的个人用户。网络安全已经成为国家与国防安全的重要组成部分，同时也是国家网络经济发展的关键。对入侵攻击的检测与防范、保障计算机系统、网络系统以及整个信息基础设施的安全已经成为刻不容缓的重要课题。

网络安全是一个系统的概念，有效的安全策略或者方案的制定，是网络信息安全的首要目标。目前网络安全的主要技术有访问控制、信息审计、安全审计、数据加密、身份认证等等。其中网络信息审计系统逐渐成为整个安全系统中非常重要的组成部分。

1.2 信息审计系统概况

信息审计系统是根据跟踪检测、协议还原技术开发的功能强大的信息审计系统，为网上信息的监测和审查提供完备的解决方案。它能以旁路、透明的方式实时高速的对进出内部网络的电子邮件和传输信息等进行数据截取和还原，并可根据用户需求对通信内容进行审计，提供高速的敏感关键词检索和标记功能，从而为防止内部网络敏感信息的泄漏以及非法信息的传播，它能完整的记录各种信息的起始地址和使用者，为调查取证提供第一手的资料。

1.3 信息审计系统工作流程

通常信息审计系统为了分析、判断特定行为或者事件是否为违反安全策略的异常行为，需要经过下列四个过程。

（1）数据采集

网络信息审计系统都需要采集必要的数据用于审计分析。

（2）数据过滤/协议还原

根据预定义的设置，进行必要的数据过滤及缩略，从而提高检测、分析的效率。同时对数据进行协议还原，提取用户关心的内容数据。

（3）数据存储

将内容数据按一定的策略进行本地或远程存储。

（4）数据分析/审计/报警

根据定义的安全策略，进行审计/分析。一旦检测到违反安全策略的行为或者事件，进行报警。

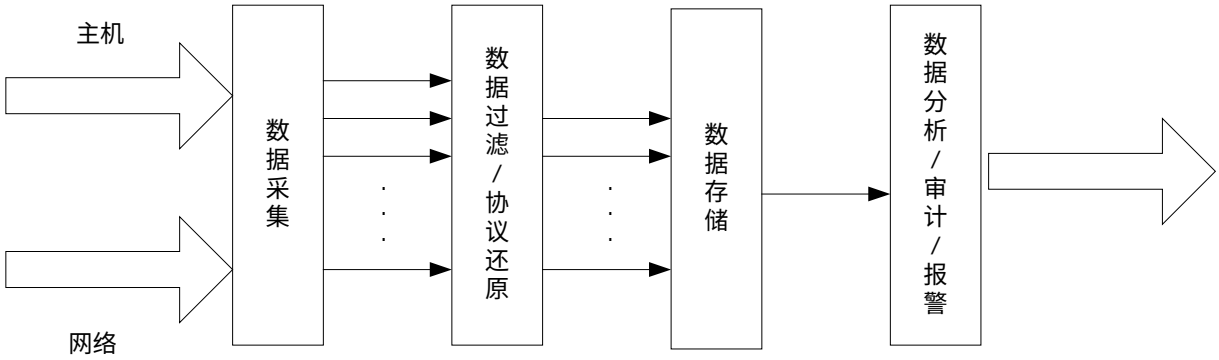


图 1-1 信息审计流程图

1.4 网络信息审计系统的必要性

随着网络应用的发展，越来越多的单位拥有自己的网络并且连入了 Internet，网络的普及为人们的工作、生活带来极大便利的同时，也带来了新的问题，网络为泄露企业的商业机密、技术资料、传播非法和黄色信息也提供了便利，甚至有人在使用网络过程中无意或故意地泄露国家机密，利用网络从事非法活动，严重危害社会安全。一套技术先进的信息审计系统将很好的监测网上信息的交流，能够做到发现问题及时解决。

最常用的安全技术和产品为防火墙和入侵检测，但是对于网络犯罪取证和网络行为监控而言，防火墙和入侵检测将无能为力，取证和监控则需要内容信息审计技术。内容信息审计是一个安全的网络必须支持的功能特性，审计是记录用户使用计算机网络系统所访问的所有资源和访问的过程，它是提高安全性的重要工具。它不仅能够识别谁访问了系统，还能够成功的还原系统的相关协议。同时对于确定是否有网络攻击的情况，确定问题和攻击源很重要。

有许多对网络传输内容非常敏感的政府部门、安全部门、教育部门、金融部门都非常需要信息审计系统。

第 2 章 产品简介

2.1 产品概述

网络卫士信息审计系统是由北京天融信公司自主研发的基于网络的信息审计系统。北京天融信公司基于多年来积累的安全产品研发和实施经验，集中强大的研发队伍推出具有完善功能和出色性能的信息审计产品。

2.2 产品功能结构

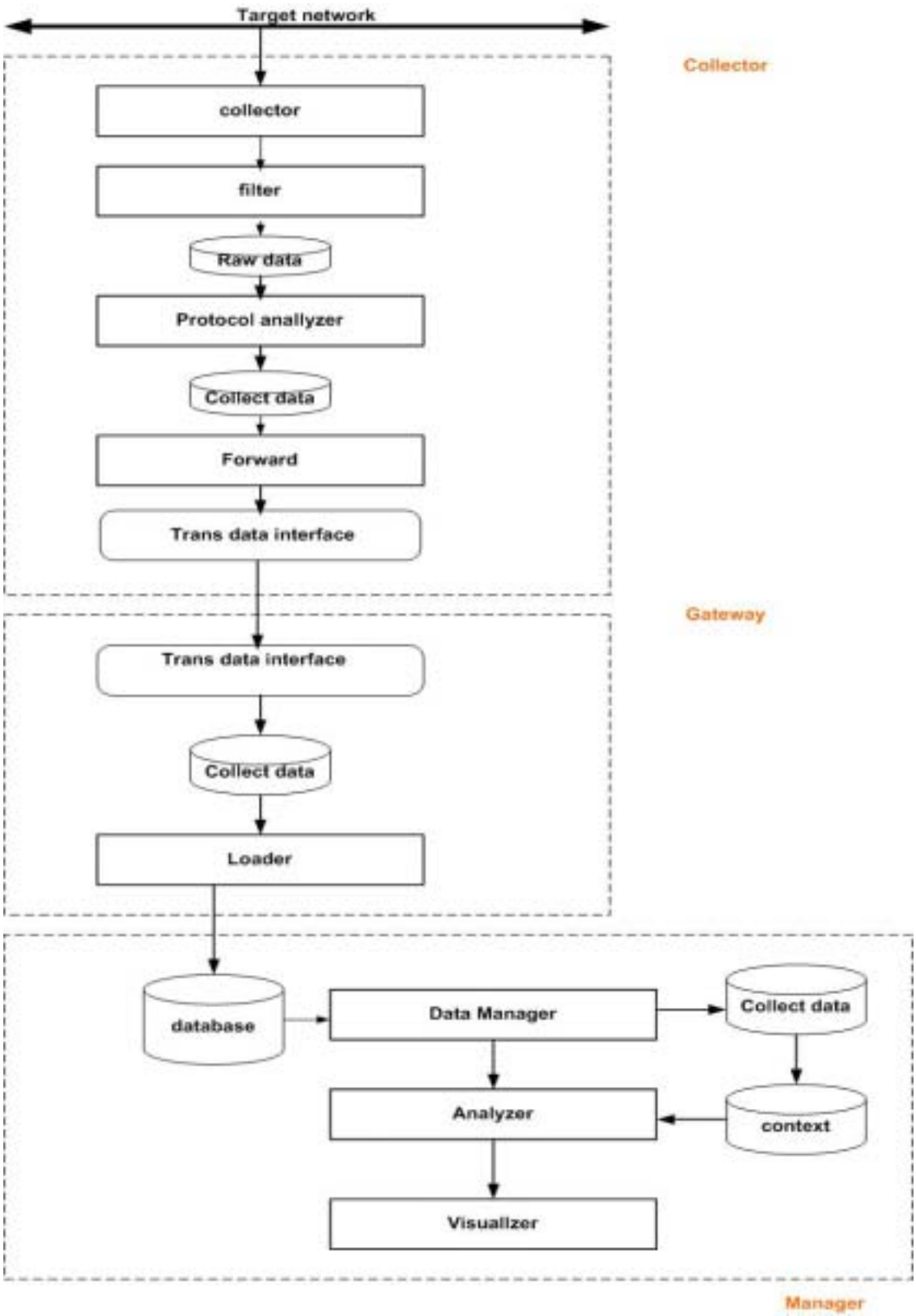


图 2-1 网络卫士信息审计系统功能结构图

2.3 产品组成

网络卫士信息审计系统主要包括三部分组件：采集器，网关，综合管理器。其中采集器为我公司开发的软硬件一体的设备,网关和综合管理器的硬件为普通的PC机或PC服务器，上面分别运行由我公司开发的网关程序和综合管理器程序。

采集器对流经HUB/SW的信息进行采集、还原，并把还原信息发送给网关，支持常用的多种网络协议，包括www,FTP,SMTP，POP3，ICQ等；网关对采集器传送过来的数据进行重组、转换，并将转换后的发件内容信息存放在本地或远程磁盘中；数据摘要信息存入数据库；综合管理器，提供给用户一个管理平台，用于对采集到的发件信息进行审计，加工和处理并向管理人员提供图形化的管理界面。

2.2.1 采集器

采集器主要包括如下子模块：

- 数据采集模块（**collector**）
  主要功能是采集网路监听数据，并将数据临时保存，如保存在内存中

- 数据过滤模块（**filter**）
  主要功能是对采集的数据根据设定的规则（主要是 IP 地址）进行初步过滤，将用户不关心的数据舍弃。该功能包括对过滤 IP 地址的维护，如增加，删除

- 协议分析还原模块（**protocol analyzer**）
  对采集的数据进行协议分析,去掉协议数据部分,将真正的数据提取出来。如 smtp，pop3，imap4，将邮件体和附件提取出来。支持协议包括：smtp，pop3,imap4,ftp,http,netbios,msn等。

- 数据传输模块（**farword**）可选，当需要远程存储时使用该模块
  主要是将采集后的数据按规定格式存储和传输。可存储于本地，也可存储于远程的其他介质上。

2.2.2 网关

网关主要包括如下子模块：

- 数据存储模块（**loader**）
  主要是将协议分析后的数据按规定文件格式存储和传输。可存储于本地，也可存储于远程的其他介质,存储位置能和综合管理器子系统共享，便于数据内容的分析和过滤。具体可采用 NFS，也可采用 TCP/IP socket 传输。同时将存储文件信息记录如发生时间，目的 IP，源 IP，文件名称，文件大小，存储位置等信息记入数据库，便于管理员查询和管理。

2.2.3 综合管理器

综合管理器主要包括如下子模块：

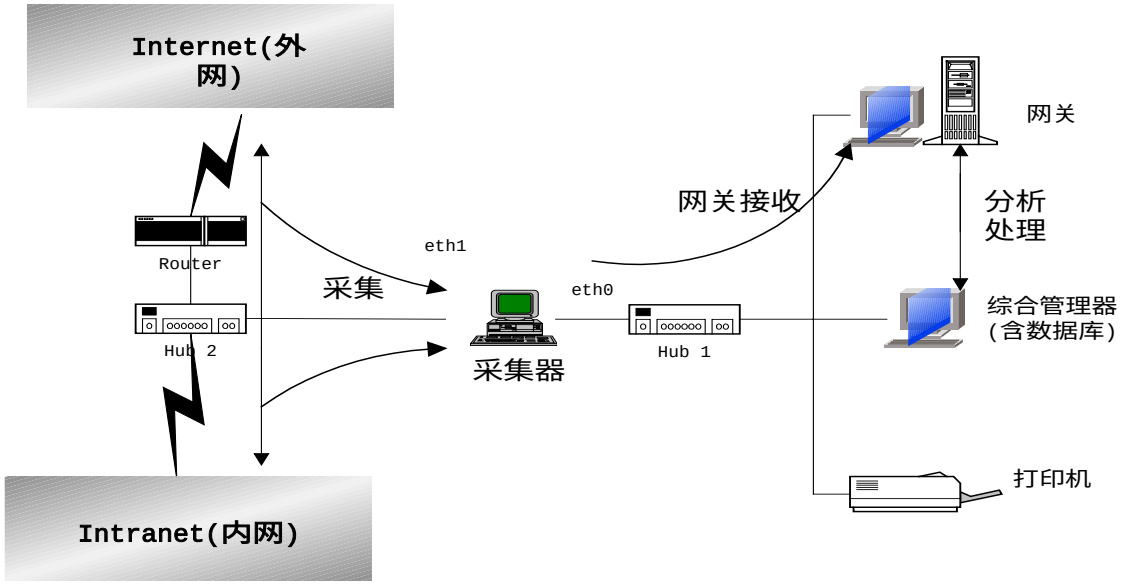
- 管理模块（**data manager**）
  主要完成对采集数据和用户的管理，包括对采集数据查询，备份，删除；对报警事件查询，删除；对 infowatch 系统管理员的增加，删除，查询，设置和修改权限，口令等操作。

- 数据内容分析过滤模块（**analyzer**）
  根据管理员设定的关键字，关键词，对采集的数据内容进行检索，若命中，记入数据库并报警。

- 数据显示模块（**visuallzer**）
  接受用户对界面操作请求，并将请求发送给管理模块，管理模块将处理结果返回，根据返回的数据生成表格，直方图等，可以给以直观的显示，告知用户操作结果，报警信息，统计和查询结果。

2.4 运行模式介绍

主要按着数据流动的顺序对该系统进行介绍。整个系统具体的数据流动图如下：



采集器的 eth1 连在被采集网络出口的 HUB 上，由于 HUB 的广播式的通讯方法和采集器的 eth1 采用的混杂模式，采集器能够接受到所有经过该 HUB 的数据包，采集器根据本身的采集规则（包括需要采集的协议和需要采集的地址范围）来决定哪些包是需要采集的和哪些是不需要的。而对于采集器连到交换机的情况下就需要定义被采集口和采集口，在支持这种定义采集口（有时也叫分析口）的交换机上将采集器连到采集口即可；对于不支持定义采集口的交换机，直接相连将不能实现采集功能，需要进行特殊处理，如增加支持采集口定义的

交换机或在速度要求不高的环境下增加 100M 的 HUB。

网关上的网关程序启动以后，根据提供的采集器的 eth0 接口（eth0 运行在普通模式下）地址与采集器建立通讯连接，网关将采集器采集下来的数据包接收下来，网关程序将对数据包重新组装和编号后以一种特有的格式保存在本地硬盘。

综合管理器与网关之间的通讯使用网络共享目录的方法，网关将自己存放数据的磁盘共享出来，综合管理器将网关共享的数据盘映射成为本地的网络驱动器，这样综合管理器软件就可以使用网关上的数据了，综合管理器对网关上的发件数据分析完以后再将生成的索引信息再写回网关。

在综合管理器上的数据库中存放着关键词等其他辅助信息，经过审计信息综合管理器软件将中标或涉密的发件信息也存储在数据库中，以备查询使用，数据库中还存放着生成的报表和其他需要记录的信息。

第 3 章 产品功能

系统总体分为三个部分：采集器，网关，综合管理器。采集器对流经 HUB/SW 的信息进行采集、还原，并把还原信息发送给网关，支持常用的多种网络协议，包括 www,FTP,SMTP，POP3，ICQ 等；网关对采集器传送过来的数据进行重组、转换，并将转换后的发件信息存放在本地硬盘中；数据库，存放采集数据摘要信息，用户设定的关键字和涉密发件的信息，并提供报表；综合管理器，提供给用户一个管理平台，用于对采集到的发件信息进行审计。主要功能包括：

3.1 网络信息内容监测和取证功能

包括：数据传输（FTP 协议），
网页浏览（HTTP 协议），
电子邮件收发（SMTP ，POP3，IMAP 协议），
远程登陆（TELNET 协议）
网上邻居（NETBIOS 协议）
网络聊天（IRC 协议）
即时通讯（ICQ，MSN，QQ 协议等）
完成的监控功能可根据用户的需要，包括内容的完全，记录，解码，还原，归档。本功能是网络信息监控和取证系统的主要功能，通过对网络信息内容的完全监控，企业信息系统管理员或安全审计员可对网络信息泄密事件进行有效的监控和取证 ;也可以完全掌握员工上网情况，比如是否在工作时间上网冲浪，网上聊天，是否访问内容不健康的网站等等。信息审计的对象包括对敏感信息的审计、对资源滥用的审计、对特定行为的审计等。

1） **FTP 监控**

- 能记录、查询访问服务上 FTP 用户名、口令字；
- 能记录和回放用户在服务器上的操作过程；
- 对指定端口，指定 IP 或 IP 地址段进行监控
- 根据设定的关键词或关键字组合对传输的内容查询、分析、统计，检查可以是自动的
- 对符合条件的相关内容形成证据文件，提供强有力的监控证据文件。设定的条件包括指定时间、指定 IP 地址或 IP 段、协议、用户名、文件名
- 根据用户指定条件，生成报表

2） **HTTP 监控**

- 能完全截获，记录，回放，归档被监测网络网段中所有用户浏览 WEB 页的内容，包括：各种文件，如 HTML 文件、图像文件、文本文件等。
- 强大的网页内容过滤功能
  * 可对用户访问的某个特定网站进行监控
  * 可对指定端口，指定 IP 地址或 IP 段进行监控
  * 可根据设定的关键词或关键字组合对网页内容查询、分析、统计，检查可以是自动的；
- 强大的网页数据管理功能
  * 根据用户选择的条件，如按时间，IP 地址，URL 等，对网页数据查询，排序，删除等

操作

* 根据用户指定条件，如某时间段，对数据导出，导入，方便系统管理员或安全审计员对上网者进行细致监控。

- 根据用户指定条件，生成报表

3） 电子邮件监控

- 能完全截获，记录，回放，归档被监测网络中所有用户收发的电子邮件，其内容包括：
  * 收件人和发件人各自的邮件地址
  * 收件人和发件人各自的 IP 地址
  * 电子邮件的主题
  * 电子邮件的内容
  * 电子邮件附件的完全还原，并可将附件导出
  * 能对压缩的附件进行最多十四层的解压

- 强大的电子邮件过滤功能
  * 对指定收件人，发件人进行监控
  * 对指定端口，IP 地址或 IP 段进行监控
  * 根据设定关键词，截取涉密或敏感邮件，进行邮件内容过滤

- 强大的邮件数据管理功能
  * 根据用户选择的组合条件，如按时间， IP 地址，邮箱地址等，对邮件数据查询，排序，删除等操作
  * 根据用户指定条件，如某时间段，对邮件数据导出，导入，方便系统管理员或安全审计员对泄密的邮件进行细致监控。
- 根据用户指定条件，生成报表

4） 远程登陆监控

- 能记录、查询访问服务上 TELNET 用户名、口令字；
- 能记录和回放用户在服务器上的操作过程；
- 对指定端口，指定 IP 或 IP 地址段进行监控
- 根据设定的关键词或关键字组合对传输的内容查询、分析、统计，检查可以是自动的
- 对符合条件的相关内容形成证据文件，提供强有力的监控证据文件。设定的条件包括指定时间、指定 IP 地址或 IP 段、协议、用户名
- 根据用户指定条件，生成报表

5） 网上邻居监控

- NETBIOS 和 SMB 协议解码，分析和还原
- 记录和报告用户访问过的“ 网上邻居 ”上的其他主机 IP 和名称
- 记录、报告用户访问过的“ 网上邻居 ”中的各种资源，包括文件、目录、打印机等
- 对指定端口，指定 IP 或 IP 地址段进行监控
- 根据用户指定条件，生成报表

6） **网络聊天和即时通讯监控**

内部员工在工作时间上网聊天是违反规章制度的行为，同时也是泄密的重要渠道，本系统支持对多种即时网络聊天协议内容的截获、记录、回放、归档

- 支持 MSN、AOL、ICQ、IRC 等多种即时通协议
- 能完全还原用户聊天的全部内容
- 能对指定端口、指定 IP 地址或地址段进行审计
- 根据用户指定条件，生成报表

7） **数据库审计**

- 能够实时监控并记录网络用户对数据库服务器的读、写、查询、添加、修改以及删除等操作。
- 根据用户指定条件，生成报表

3.2 各种发件内容的还原审查

将采集到的各种发件（HTTP，SMTP，FTP，TELNET，NETBIOS，QQ）进行还原，包括浏览的页面还原，压缩文件的解压还原，管理可以直接审查发信的明文，为最终确定发信内容提供确证手段。对于通过页面发送邮件也可以自动分析，并还原成邮件的格式展现给使用者。对于邮件的附件文件可以直接打开，比如使用 WORD 可以直接打开附件的内容。

3.3 实现自动关键词发件内容审计检查

用户选择需要进行检查的发件的时间范围，由计算机自动进行全文检索，根据用户设定的关键词库，系统快速进行匹配，对于匹配成功的情况，系统将通过醒目颜色在发件列表中标示出具体那个发件中标，打开发件将通过醒目的颜色标示符合条件的关键词的位置。

3.4 网络数据的综合分析和统计功能，生成用户需要的各种图表

- 根据管理员指定组合条件，如时间，协议，IP 地址或 IP 地址网段，流量等，生成用户需要的各种图表（报表，直方图，饼图等），包括：
  - ✶ 针对协议，可以统计监测网络中各协议数据，可以得到用户关心的协议的流量，各协议发生数量，点击某一记录，可得到关于该记录的具体内容，如协议，IP,发生时间，发件明文内容等。
  - ✶ 针对 IP 地址，可以对某台主机的操作进行某段时间的全程监控，如一天，一个星期，关于该主机上网情况，收发邮件统计，网络聊天内容，上传和下载数据，访问其他主机情况。总之，在该主机的对于网络操作可以跟踪和还原。
  - ✶ 报警统计，可以检索某时间段（如一天，一周，一月等）内发生的报警信息，点击

某一记录，可以得到关于该报警记录的所有可能信息，如 IP,发生时间，明文内容，若是邮件，发件人地址，收件人地址等信息，便于管理和监察人员跟踪，了解和取证。

3.5 网络监测数据的存储和维护功能

- 管理员可设定各协议数据存储和备份路径
- 管理员可将数据导出
- 管理员可将数据导入

管理员可设定数据自动定时更新周期，若不指定操作，自动覆盖。

3.6 分权，分级，分角色的用户管理功能

- 分权，分级，分角色的用户管理和授权系统
  - ✶ 安全审计管理系统是一个多用户系统,允许若干不同级别和身份的用户操作和使用系统。
  - ✶ 对管理员设定不同角色，并赋予其不同的操作权限，通过对这些操作权限的排列组合，可定义用户需要的不同级别的多个用户。如超级管理员可对任何数据读取和删除，一般管理员可根据赋予的权限，对部分或全部数据读取和删除，但其对敏感数据（如报警数据只有读取而没有删除和导入，导出操作权限），以保护取证数据的完整性真实性。

3.7 简单方便的系统配置功能

管理员可通过简单，美观，友好的配置界面，对系统进行配置，如配置采集器，网关和综合管理器。

管理员也可方便的配置需过滤的内容，如关键词，IP 或 IP 地址段，监控协议等。

3.8 网络通讯连接状态和流量监测功能

本功能是以连线图的形式实时，直观的显示出网络中哪些主机正在通讯，连线的粗细表示主机间相对流量的大小，本功能有助于网络管理员即时了解网络连接和通信数据流量状况，还可以根据用户要求，统计某一时间段（如一天，一周，一个月等）的网络总体流量和某一时间段的流量曲线图，可以得到何时处于流量高峰，便于管理员监控和调节。

第 4 章 产品技术特点

4.1 各种压缩格式附件的自动解压与显示

该系统是唯一实现了自动显示附件压缩文档的审计产品，对于邮件中的附件，系统对于压缩文件能自动解压，自动显示最终的文件给用户，并支持多达 14 层的压缩分解。

4.2 网络数据获取能力优越，丢包率低

基于自主知识产权的天融信独创的核检测技术，构造了一个安全、高效、可靠的安全审计系统，性能优越

4.3 不改变网络系统的拓扑结构及效率

旁路模式，不改变用户的网络拓扑结构，对用户的通信性能没有任何影响。

4.4 强大的包重组和流重组能力

具有强大的 IP 碎片重组（IP Fragments Reassembly）能力，和 TCP 流重组（TCP Fragments Reassembly）能力，任何基于协议碎片的逃避检测手段对本产品无效，目前类似产品中只有本产品完全支持各种碎片的重组。

4.5 支持多种网络协议

支持数据链路层中 IEEE 802.3 MAC、PPP、FDDI、Token Ring、L2TP 等协议的分析和解码、网络层中 IP、IPX、ICMP、IGMP、ARP、SLIP 等协议的分析和解码，传输层中 TCP、UDP 等协议的分析和解码，应用层中 HTTP、SMTP、POP3、IMAP、Telnet、FTP、SMB、NetBIOS、SMB、MSN Messenger、ICQ、AOL 等协议的分析和解码。

4.6 支持代理通讯协议

支持 MS Proxy、SOCK 4 和 SOCK 5 三种代理通讯协议的分析和解码，这在同类产品中是

绝无仅有的。

4.7 良好的可扩展性

分布式部署，集中式管理，使系统具有良好的可扩展性，系统根据用户规模，可通过增加和减少机器，方便的扩容。面向对象的设计，减少对象间的耦合性，提高模块的独立性，在出现问题时，尽量减小问题涉及的范围。

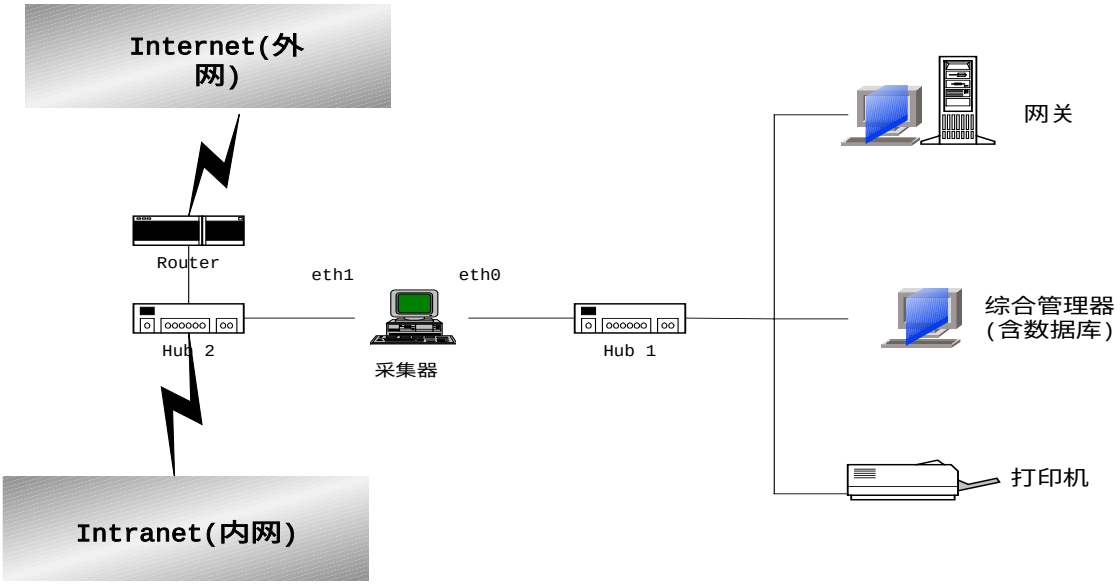
4.8 界面设计友好易用

应用界面美观大方，操作方便。

第 5 章 典型应用

5.1 典型部署

该系统典型的运行环境如下图：



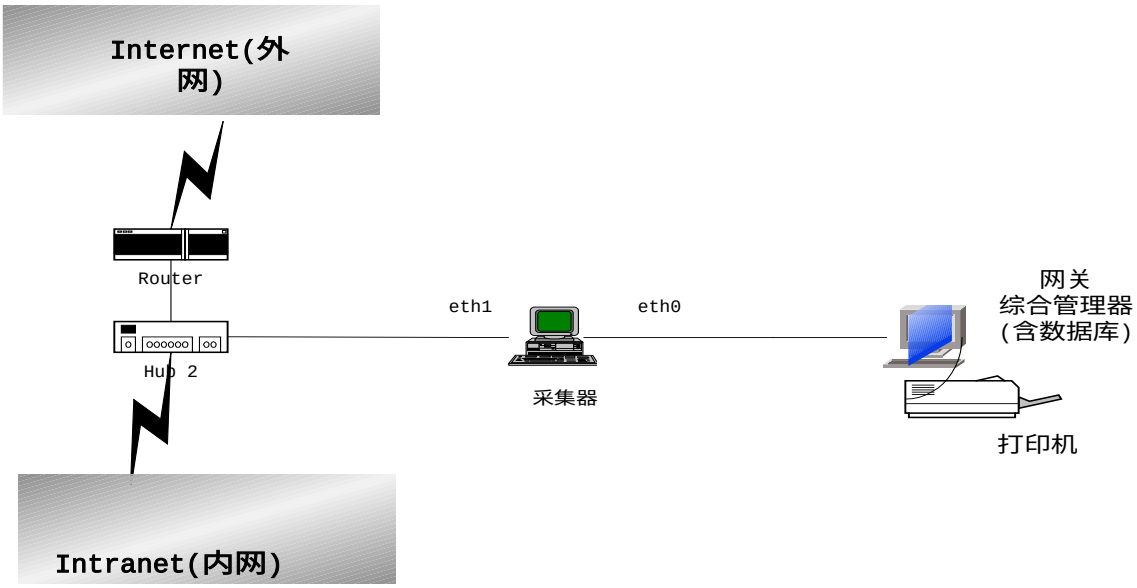
采集器的 eth0 口为与网关通讯的接口，采集的数据通过 eth0 口传输到网关，eth1 为采集口，负责采集数据，在支持二点采集的采集器上还会有 eth2 口，该口也为采集口，eth0 口运行在普通模式下，eth1 和 eth2 口运行在混杂模式下。采集器可以通过 console 口或 telnet 登录进行配置管理。

网关上运行网关程序，该程序主要负责与采集器通讯，将采集器采集的数据包接受下来，并将包按顺序组装起来，并且以特定的格式存储在本地。

综合管理器运行综合管理软件，该软件使用的后台数据库为安装在本地的数据库。综合管理器主要对网关上存储的采集数据进行加工和处理并向管理人员提供图形化的管理界面。

5.2 精简型部署

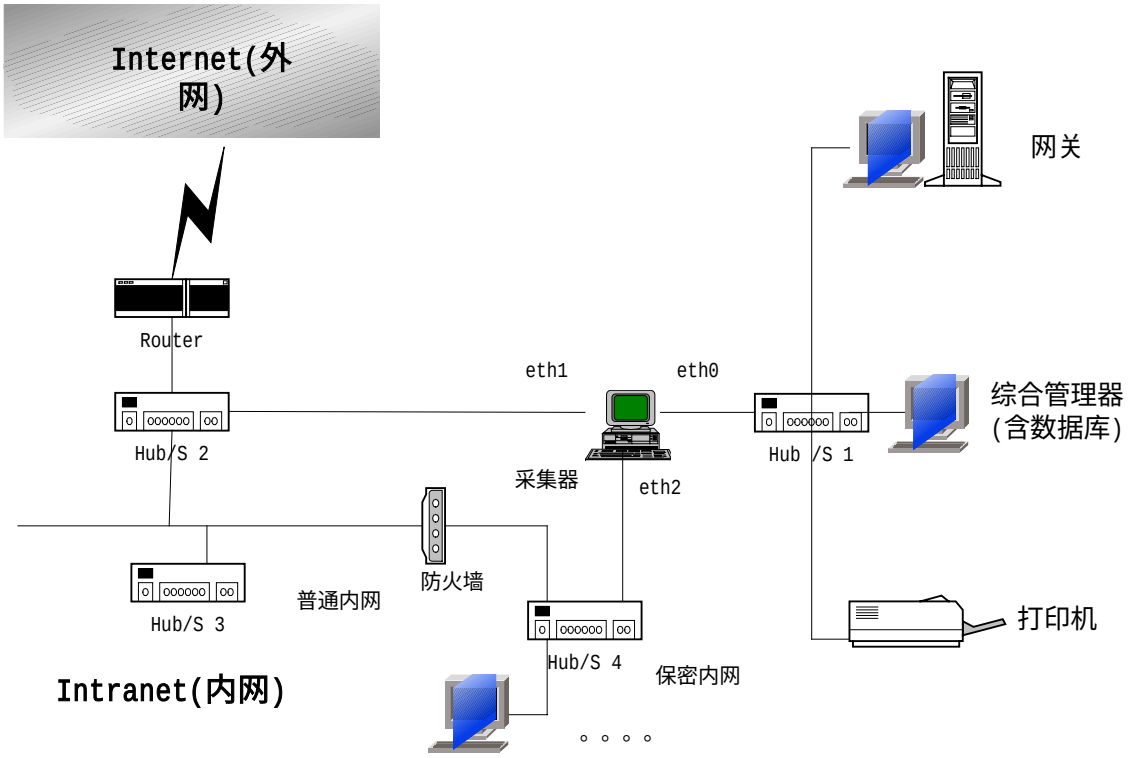
对于一些网络吞吐量比较小的环境下可以考虑将网关软件和综合管理器运行在同一台计算机上，结构图如下：



在这种情况下，可以使用一台高档的 PC 或 PC 服务器作主机并直接接一台打印机，该机器上需要安装网关程序、数据库和综合管理器软件，然后使用交叉线直接与采集器的 eth0 口相连。在使用综合管理器软件时不需要映射远程网关，只需要指定当地存放数据的位置即可。

5.3 多点采集

对于一些内部有安全子网等有其他需要多点采集需要的情况，可以使用有两个采集口的采集器进行多点采集，典型的应用如下图：



在该种应用环境下，将采集器的第二个采集口 eth2 连到需要采集的保密内网的主干交换机上，而只需要一套网关和综合管理器就可以达到安全审计的要求。

第 6 章 应用领域

该系统能对网上交换的信息进行采集和智能的处理，十分适合那些对信息保密和非法信息传播等问题比较关心的单位和部门，如政府、军队机关的网络管理部门；公安、保密、司法等国家授权的网络安全监察部门；金融、电信、电力、保险、海关、商检、学校、军工等各行业网络管理中心；大中型企业网络管理中心等。该系统能有效防范机密外泄，以及防范利用网络的方便进行非法的活动。以便正确合理地利用网络资源，尽可能的减少网络负面效应造成的损失。同时对网络犯罪的侦破和取证也可以提供有力的支持。