网络卫士入侵检测系统

技术白皮书

北京天融信公司

2004 年 6 月

注意

天融信网络卫士入侵检测系统

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**

目　　录

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、安全审计、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。

第1章 入侵检测系统概述

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、入侵检测、安全审计、数据加密、身份认证等等。其中入侵检测系统逐渐成为整个安全系统中非常重要的组成部分。

1.2 入侵检测系统概况

入侵检测系统(Intrusion Detection System)通过从计算机网络或计算机系统的关键点收集信息并进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。入侵检测系统可以说是防火墙系统的合理补充和延伸，如果说防火墙是第一道安全闸门，入侵检测系统则可以说是第二道安全闸门。入侵检测系统在不影响网络性能的前提下，实时、动态地保护来自内部和外部的各种攻击，同时有效地弥补了防火墙所能达到的防护极限。

根据进行入侵分析的数据来源的不同，可以将入侵检测系统分为基于网络的入侵检测系统（Network-Based Intrusion Detection System）和基于主机的入侵检测系统（Host-Based Intrusion Detection System）。

基于网络的入侵检测系统（NIDS）的数据来源为网络中传输的数据包及相关网络会话，通过这些数据和相关安全策略来进行入侵判断。

基于主机的入侵检测系统（HIDS）的数据来源主要为系统内部的审计数据，通过这些数据来分析、判断各种异常的用户行为及入侵事件。

1.3 入侵检测系统工作流程

通常入侵检测系统为了分析、判断特定行为或者事件是否为违反安全策略的异常行

为或者攻击行为，需要经过下列四个过程。

（1）数据采集阶段

网络入侵检测系统（NIDS）或者主机入侵检测系统(HIDS)都需要采集必要的数据用于入侵分析。

（2）数据过滤及缩略

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。

（3）检测/分析

根据定义的安全策略，进行检测/分析。

（4）报警及响应

一旦检测到违反安全策略的行为或者事件，进行报警及响应。

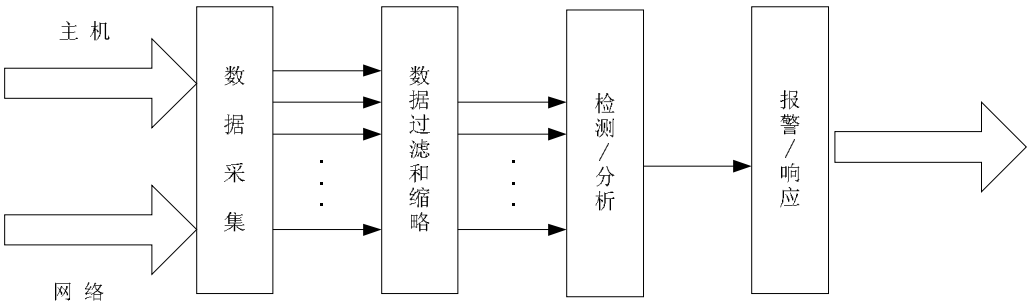

图 1-1 入侵检测流程图

1.3.1 网络入侵检测系统的必要性

目前通常通过防火墙进行网络安全防范。从理论上讲，防火墙可以说是第一层安全防范手段，通常安装在网络入口来阻止来自外部的攻击,其主要防范原理是对基于TCP/IP 的 IP 地址和端口进行过滤、限制。由于防火墙本身为穿透型（所有数据包需要经过防火墙才能到达目的地），因此为了提高其过滤、转发效率，通常不会对每个数据包或者数据流进行过多的、细致的分析和检查，但是恰恰有很多符合防火墙安全策略的数据包或者数据流中掺杂着恶意的攻击企图。虽然目前一些防火墙增强了对于应用层内容进行分析的功能，但是考虑到其因分析、处理应用层内容而导致的网络延迟增加，从实际应用角度来说，仍然存在一些局限性。

网络入侵检测系统由于以被动模式部署到现有网络中,因此可以在不影响网络结构及网络性能的情况下，执行各种复杂的应用层分析工作，从而可以成为防火墙有效的扩展。同时网络入侵检测系统通过与防火墙的联动，可以实现整体的安全防范体系。

1.3.2 主要的网络入侵检测技术

目前网络入侵检测系统主要采用误用检测和异常行为检测方法来实现入侵检测的目的。

- 误用检测技术
  - 基于规则误用检测
  - 基于状态迁移误用检测
  - 基于模型误用检测

- 异常行为检测技术
  - 统计异常检测
  - 特征选择异常检测
  - 模式预测异常检测
  - 神经网络异常检测

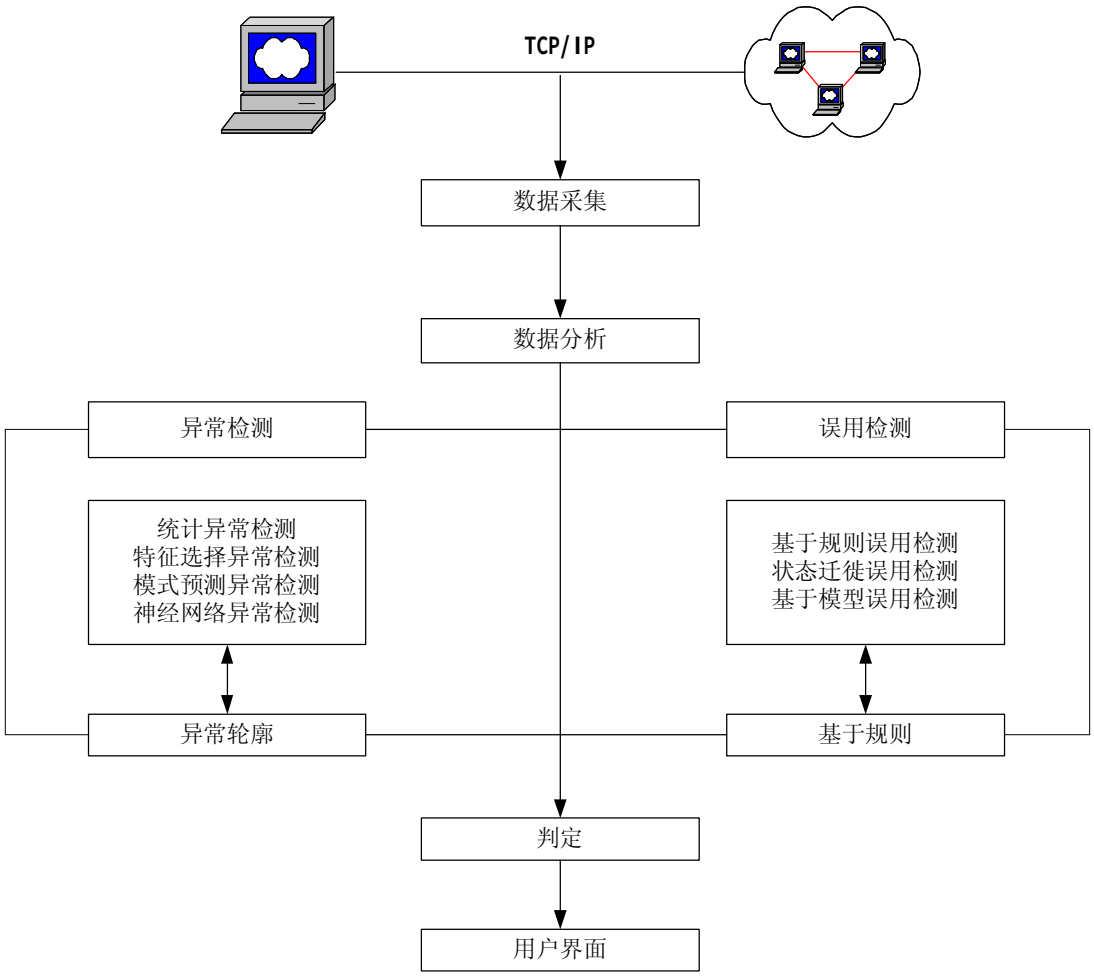

图 1-2 入侵检测技术参考模型

第2章 产品简介

2.1 产品概述

网络卫士入侵检测系统是由北京天融信公司自主研发的基于网络的入侵检测系统。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入侵检测产品。

网络卫士入侵检测系统部署于网络中的关键点，实时监控各种数据报文及网络行为，提供及时的报警及响应机制。其动态的安全响应体系与防火墙、路由器等静态的安全体系形成强大的协防体系，大大增强了用户的整体安全防护强度。

2.2 产品组成

网络卫士入侵检测系统主要包括两部分组件：检测引擎和控制台。检测引擎采用专用硬件设备以旁路方式接入检测网络,控制台提供显示和管理配置功能。

2.2.1 引擎

检测引擎包括以下组件：

- 检测组件

通过检测组件实时分析、检测各种网络事件。

- 响应组件

用于与控制台通讯并实时传输各种事件。

- 日志组件

用于管理实时事件之外的各种日志。

- 监控组件

是引擎的 Watch-dog 组件,实时监控各种组件是否正常工作。如果组件工作不正常，将会“唤醒”相关组件，以保证系统的正常运行。

2.2.2 控制台

控制台主要为管理入侵检测引擎提供图形化管理界面。通过控制台可以管理、配置检测引擎的各种参数及安全策略。同时用户可以通过控制台查看由引擎发送的各种入

侵检测事件，并生成各种报表。控制台包括以下组件：

Ø 控制台主程序

通过控制台主程序可以实现详尽的系统设置、实时监控报警事件。控制台主程序为用户提供了方便友好的图形化接口，用户可以非常简单地进行各种设置。

Ø 报警器

报警器作为控制台的一个组件，可以单独安装，实时接收各种入侵事件，而无需与控制台主程序在同一台主机中运行。从而解决了管理员无法实时与运行控制台主程序的主机进行交互时的问题。

Ø 跟踪器

当发生各种攻击事件时，管理员可以方便的调用跟踪器对攻击源地址或者目的地址进行各种跟踪确认操作，来确定其身份。

Ø 报表生成器

通过控制台中基于 Crystal Report 的报表生成器，可以生成用户需要的各种报表。

2.3 产品功能结构

网络卫士入侵检测系统内部功能结构如下图所示：

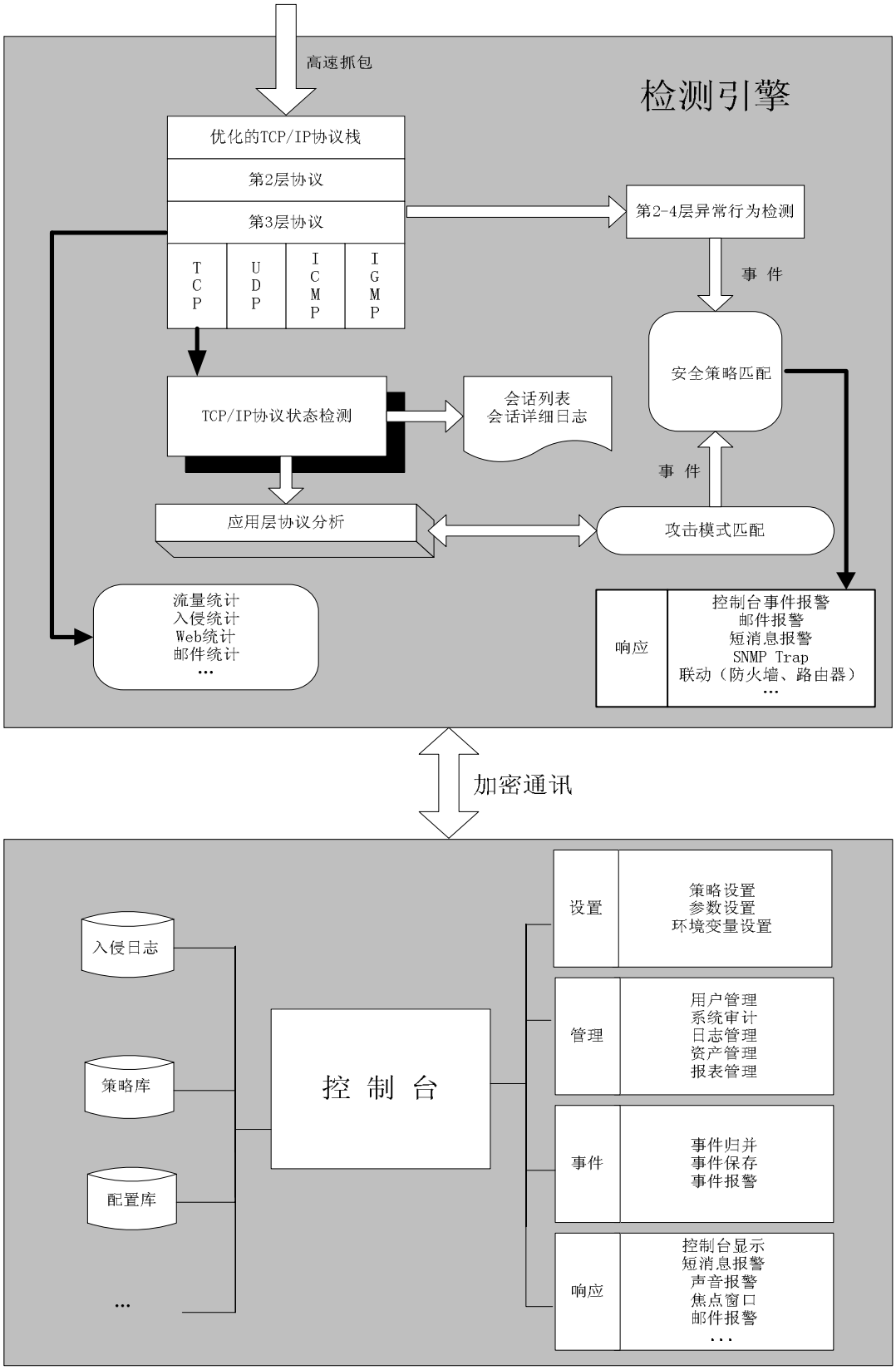

图 **2-1** 网络卫士入侵检测系统功能结构图

2.4 产品型号

网络卫士入侵检测系统产品分为三个型号，各型号产品参数如下表所示：

型号	NGIDS	NGIDS-E	NGIDS-UF
类别	百兆标准 IDS	百兆高端 IDS	千兆 IDS
规格 （长*宽*高）	1U 机架式 430×290×44.5mm	1U 机架式 430×450×44.5 mm	2U 机架式 430×470×89 mm
重量	6.5kg	10.8kg	14.3kg
网络接口	3 个 10/100Base-TX	3 个 10/100Base-TX	1 个 10/100Base-TX 1 个 10/100/1000Base-TX 1 个千兆光纤（多模） 可扩展 1 个千兆光纤（多模）
串口	1 个 RS－232C	1 个 RS－232C	1 个 RS－232C
环境要求	工作温度： -5°C 至 45°C 储存温度： -10°C 至+55°C 工作湿度： 5%至 90%相对湿度	工作温度： -5°C 至 45°C 储存温度： -10°C 至+55°C 工作湿度： 5%至 90%相对湿度	工作温度： -5°C 至 45°C 储存温度： -10°C 至+55°C 工作湿度： 5%至 90%相对湿度
电源 (交流输入电压)	220VAC±30%	220VAC±30%	220VAC±30%

第3章 产品功能

3.1 网络入侵检测功能

l 检测基于TCP/IP协议的各种网络活动和攻击行为

网络卫士入侵检测系统具有 2500 条以上的入侵检测规则,并不断地进行更新。网络卫士入侵检测系统使用细粒度检测技术，支持协议分析技术，误用检测技术，协议异常检测，可有效防止各种攻击和欺骗。同时能够通过策略编辑器中的用户自定义功能定制针对网络中各种 TCP/IP 协议的网络事件监控。

检测规则组	典型实例
拒绝服务	各种SNA类型和应用层的强力攻击行为,包括消耗目的端各种资源如网络带宽、系统性能等攻击。主要攻击类型有TCP Flood，UDP Flood，Ping Abuse等。
预探测攻击（扫描）	各种SNA类型和应用层的预探测攻击行为。主要攻击类型有TCP SYN Scan,TCP ACK Scan,Ping Sweep,TCP FIN Scan等。
后门	BackOrifice2000,Netbus pro2,subseven等
代码攻击	基于应用层的各种可疑活动，未经授权访问，缓存溢出、蠕虫检测、口令猜测、非法目录或文件访问、篡改、遍历等攻击事件

l 协议解码

对常用网络应用层协议解码分析，记录网络中的异常行为。

检测规则组	典型实例
网络活动监控（用户自定义）	基于TCP/IP的各种协议分析事件,如：HTTP、SMTP、FTP、TELNET等应用层协议连接、关闭，Pop3命令连接请求、应答，各种应用层协议的关键字解码等

l 智能IP碎片重组

对所监视网络中的IP碎片报文重组后进行分析，防止IP碎片欺骗。

l 事件风暴处理功能

可将一定时间范围内的同种攻击类型事件合并成同一条在控制台进行显示并记录

攻击次数，从而达到防止控制台被报警事件洪水淹没屏幕的目的。

- 协议过滤和误报处理功能

能够将不需要入侵检测系统记录的某类 TCP/IP 协议的数据流做过滤处理。同时，对出现的误报事件，可以针对事件规则名和事件发生的源或目的地址进行排除，避免同类事件再次出现在控制台，干扰管理员，也减少了入侵检测系统不必要的负担。

3.2 增强功能

- 敏感会话监控

监控网络中常用的敏感信息。如监视网络中用户访问网站的 URL 地址,收发邮件的主题中包含敏感字符串等。

- 文件传输监控

对FTP和MSN协议中上传和下载的文件名做详细记录。

- 实时网络会话监控

基于会话监控，实时记录网络中 TCP/IP 协议的网络连接情况，并可以对原始报文内容进行记录。

- 文件完整性检查

可以在入侵检测系统控制台的策略编辑器中设定需要监控的文件名称和路径,一旦控制台中某指定文件被复制、删除或篡改，控制台就会自动报警。

- 网络事件回放

能够把常用的应用协议（HTTP、FTP、SMTP、POP3、TELNET）内容恢复，并按照相应的协议格式完整展现,清楚展现入侵者的攻击过程，重现内部网络资源滥用时泄漏的保密信息内容。

3.3 配置和策略管理功能

- 事件规则的定制

用户可根据需要自定义入侵规则。对系统内置的入侵规则，用户可以根据需要修改报警级别，响应方式等内容。

- 多种响应方式

对入侵规则可以提供记录常规日志（同时将事件传送并显示到控制台的实时窗口中）、记录详细日志（获取原始报文）、防火墙联动(支持的防火墙联动协议包括TOPSEC协议、OPSEC协议和IAP协议)、路由器联动、发送电子邮件、报警器报警、报警灯报警、

声音报警、焦点窗口、手机短信报警、TCP阻断、SNMP Trap、用户自定义程序执行等多种响应方式,方便用户设置。

- 策略模板定制

为用户提供缺省策略、最大化策略、WWW策略、FTP策略、Email策略等多种定制策略模板，用户可以根据自己的网络情况选择模板，省去了配置的麻烦。

- 日志审计和报表

强大的日志审计功能。用户可根据需要从任意角度定制审计查询条件。

3.4 系统安全功能

- 远程安全管理

采用SSL加密信道和身份认证方法对传输信息进行处理，从而保证数据安全性和完整性。

- 管理日志审计

提供对用户操作的审计功能。用户登录控制台后的操作信息在控制台中实时显示，对修改用户信息等敏感操作则记录到数据库中。

- 控制台身份认证和权限分级管理

通过网络卫士入侵检测系统控制台的身份认证,能够有效保证控制台的安全和集中的管理。权限分级管理是指控制台采用多级管理员、分权限的管理方式对入侵检测系统进行管理。网络卫士入侵检测系统提供了三种不同的等级权限，包括超级管理员、普通管理员和只读管理员，超级管理员拥有对控制台和引擎的全部操作权限，而其他级别管理员只拥有部分权限，从而确保了控制台自身的管理集中化和安全性。

3.5 扩展功能

- 网络流量统计功能

能够对网络引擎监控的网段进行流量统计，采用图形化和数字结合的方式显示。可以分不同的引擎、不同的源、目的地址查看TCP连接数目，网络字节流量，网络数据包数，会话连接数等多种统计信息。

- 引擎状态监控

可以通过控制台以图形方式实时显示网络引擎的抓包情况（字节数、数据包数、连接数、丢包率）以及引擎端资源消耗情况。

- 日志管理功能

提供数据库管理功能，可以对日志信息备份、删除、压缩和恢复。提供备份文件信

息记录和显示功能，防止备份文件的丢失。

- 事件规则库升级

支持在线自动升级、在线手动升级以及文件包升级三种升级方式。在控制台端可以对检测引擎进行远程升级。

3.6 分级管理功能

对大型分布式网络环境提供分级部署管理功能，能够支持多级控制台管理的复杂部署结构和两级简单部署结构。通过分级管理，可以实现策略下发和报警事件上传等功能。

第4章 产品技术特点

4.1 产品特点

4.1.1 增强的入侵检测技术

- 综合使用误用检测、异常检测、智能协议分析、会话状态分析等多种入侵检测技术，大大提高了准确度，减少了漏报、误报现象。
- 通过优化的、专用的、高效的模式匹配算法，大大提高了检测效率。
- 通过详尽、细粒度的应用协议分析技术，大大提高了应用层攻击检测能力。
- 基于优化的 TCP/IP 协议栈及可疑网络活动（SNA）处理器，增强了 DoS、扫描等攻击事件检测能力。
- 内置 2500 种以上入侵规则，提供对 DoS、扫描、代码攻击、病毒、后门等各种攻击的检测能力。
- 通过解码基于 SSL 加密的通讯数据，分析、检测基于 SSL 加密通讯的攻击行为，从而可以保护内部重要的提供 SSL 加密的服务器的安全性。

4.1.2 强大的蠕虫检测能力

实时跟踪当前最新的蠕虫事件，针对当前已经发现的蠕虫攻击及时提供相关事件规则。对于存在系统漏洞但尚未发现相关蠕虫事件的情况，通过分析漏洞来提供相关的入侵事件规则，最大限度地解决蠕虫发现滞后的问题。

网络卫士入侵检测系统内置 400 条以上的蠕虫检测规则。

4.1.3 丰富的响应方式

- 控制台响应
  - 报警：包括控制台报警、报警器报警、报警灯报警、焦点窗口报警、声音报警、邮件报警、手机短信报警等。
  - 日志保存：将日志保存在本地数据库或者远程数据库中。
- 引擎响应
  - 报警：向控制台发送报警信息、邮件报警、手机短信报警、报警器报警、SNMP 报警、自定义程序报警等。

- Ø 联动：防火墙、路由器联动等。
- Ø 阻断：引擎主动阻断。

4.1.4 方便、灵活的策略编辑器

内置多种策略模板，用户可根据实际网络环境灵活选择、应用。策略编辑器简单、易用，便于管理员制定各种安全策略。内置强大的协议解码器，用户可以灵活地自定义各种入侵规则，具有极强的扩展性。

4.1.5 灵活的部署方式

支持控制台、引擎分离的分布式部署方式。不仅支持基于 HUB 的共享环境、基于交换机镜像功能的交换环境，而且还支持基于专用的流量分流设备 TAP 的部署方案。

4.1.6 多层次、分级管理

- l 引擎管理：产品构架为基于 C/S 模式的控制台与检测引擎分离的结构。从控制台可以对引擎进行详尽的配置，同时向引擎分发升级更新文件，并可以控制引擎停止、重启等。
- l 数据库管理：支持多种数据库，包括本地 ACCESS 数据库、外挂 SQL SERVER 数据库。可以对数据库日志进行有效的备份、删除、压缩和恢复操作。
- l 策略管理：内置了多种策略模板，在策略模板基础上，用户可以添加新的策略集，并可以对具体策略项进行编辑处理。同时，支持策略集的导出和导入，便于控制台的迁移。
- l 升级管理：支持对事件特征库和系统的在线自动升级、在线手动升级以及文件包升级三种升级方式，保证事件特征库和系统的及时更新。

4.2 技术特点

4.2.1 增强直接用户空间访问（EDUA）技术

通常情况下网卡驱动程序在内核空间的 DMA 缓冲空间保存所接收到的数据报文，而入侵检测引擎工作在上层的用户空间，因此无法直接访问内核空间中的数据，需要通过系统调用将网卡中的数据包拷贝到用户层缓冲空间之后再去读取。在这些过程中会频繁发生

CPU 中断而影响整个 IDS 系统的性能。

网络卫士入侵检测系统通过重写网卡驱动程序，使得网卡驱动程序与上层系统共享一块内存区域，网卡从网络上捕获到的数据报文直接传递给入侵检测系统，这个过程避免了数据的内存拷贝，不需要占用 CPU 资源，最大程度的将有限的 CPU 资源让给协议分析和模式匹配等进程去利用，提高了整体性能。同时通过将用户空间中的大量内存空间映射到内核层的 DMA 缓冲空间，从而使原来有限的 DMA 缓冲空间得到有效扩展，解决了高峰期因缓冲空间有限而发生丢包的现象。

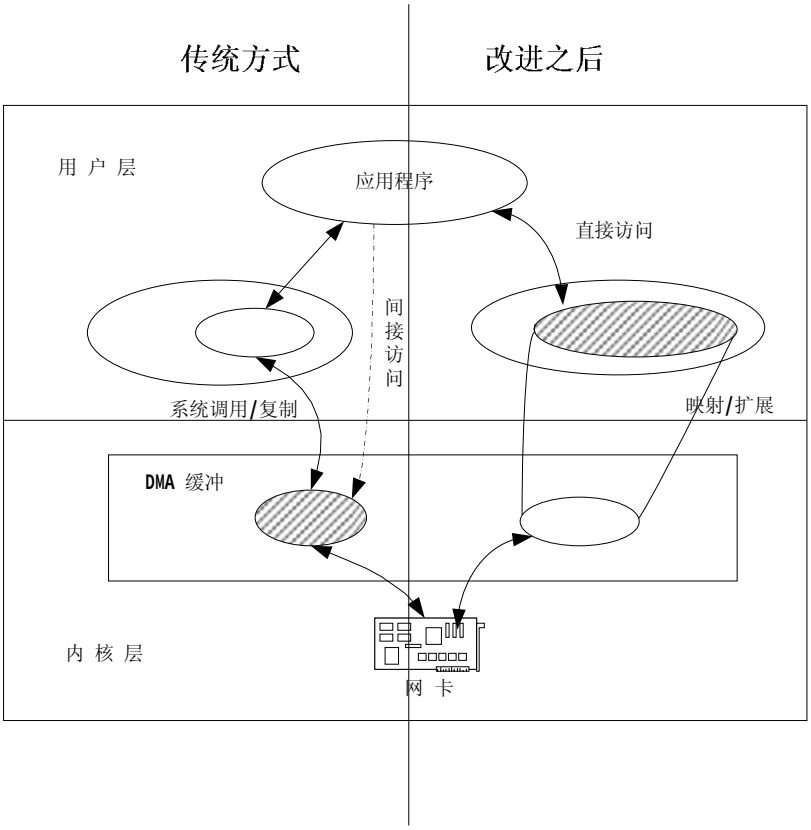

图 4-1 增强直接用户空间访问技术示意图

4.2.2 优化的 IP 分片重组技术

对于入侵检测系统来说，IP 分片重组是进行检测工作最为基本且至关重要的内容。由于网络环境中的 MTU 限制，一些 IP 报文在传输时需要进行分片传输,在对这些报文进行进一步分析之前需要进行分片重组,因此 IP 分片重组的效率也是直接影响到系统开销及整体性能的一个非常重要的因素。为了最大限度地提高 IP 分片重组效率，网络卫士入侵检测系统采用了多线程分散式 IP 分片重组机制，从而有效解决了因 IP 分片重组造成的性能瓶颈。

4.2.3 高效的 TCP 流汇聚及匹配机制

基于状态分析的入侵检测系统，在实际环境中需要维护和管理大量的 TCP 会话流，因此是否能够针对每一个数据报文高效、准确地判断和匹配相关 TCP 流成为影响整个处理性能的重要环节。网络卫士入侵检测系统通过优化的 TCP 流定位算法快速、准确地确定相关会话，从而减少系统资源消耗并提高处理效率。

4.2.4 细粒度的协议分析及智能模式匹配算法

网络卫士入侵检测系统采用了基于协议分析的优化模式匹配算法，通过内置的强大应用协议解码器，对网络会话及数据报文进行快速分流并及时调用无缝集成的模式匹配引擎进行快速搜索匹配。由于在进行细粒度的协议分析基础之上调用相关模式匹配引擎，因此大大缩小了匹配搜索范围并提高了匹配效率。同时在进行模式匹配时，一次匹配可以同时针对若干个相关规则进行，从而大大提高了其效率。

第5章 典型应用

5.1 小规模网络环境

这种部署适合于小型单一网段。通常集中监控网络出入口的关键路径，监控所有进出的数据流量。

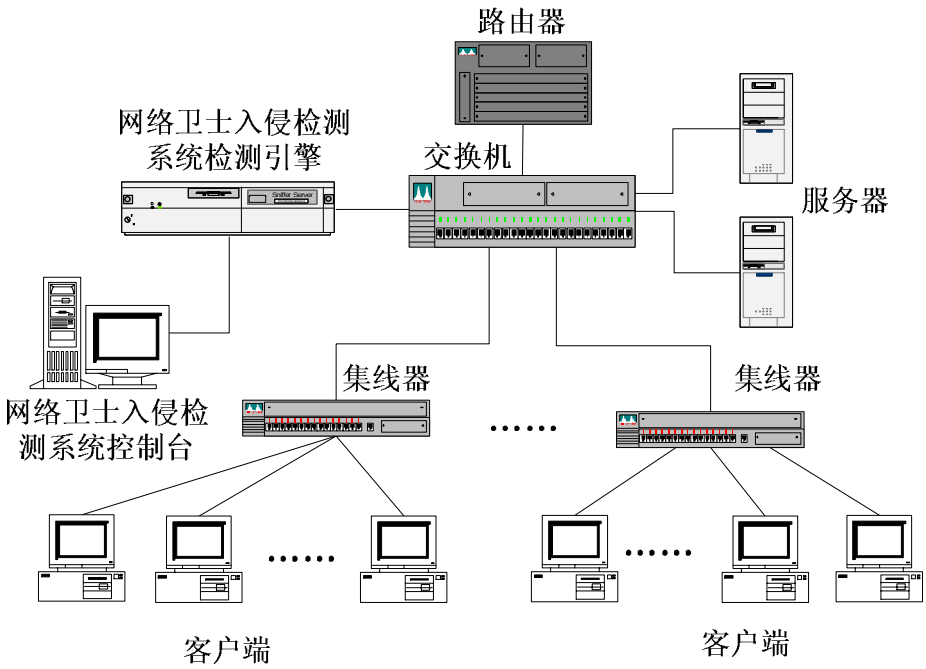

图 **5-1** 小规模网络环境应用图

5.2 多子网分布式环境

这种方式适合于存在多个子网的中型网络环境。管理员为每个重要的网段部署一个检测引擎，并分别将检测到的事件发送到集中管理控制台。

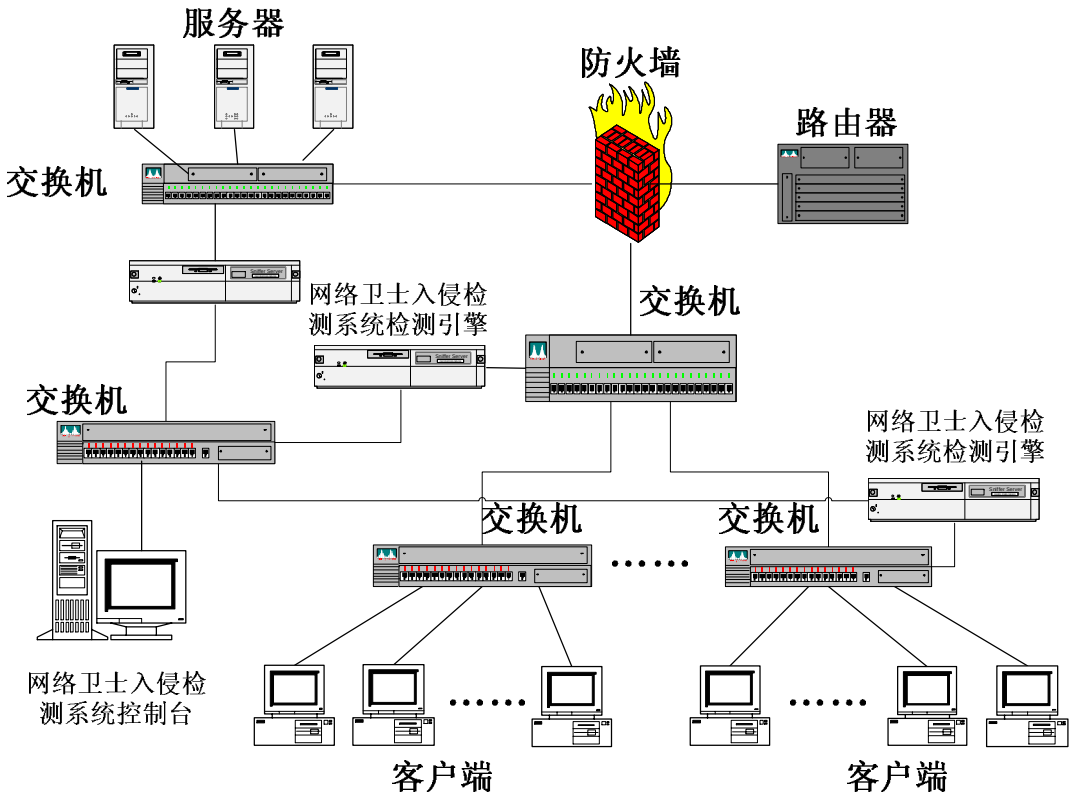

图 5-2 多子网分布式环境应用图

5.3 分级管理环境

这种部署适合于拥有各级分支机构的大型网络环境。通过将控制台进行分级部署，可以统一部署全局安全策略，并由下级管理员根据本地的安全策略进行相应调整或完善。

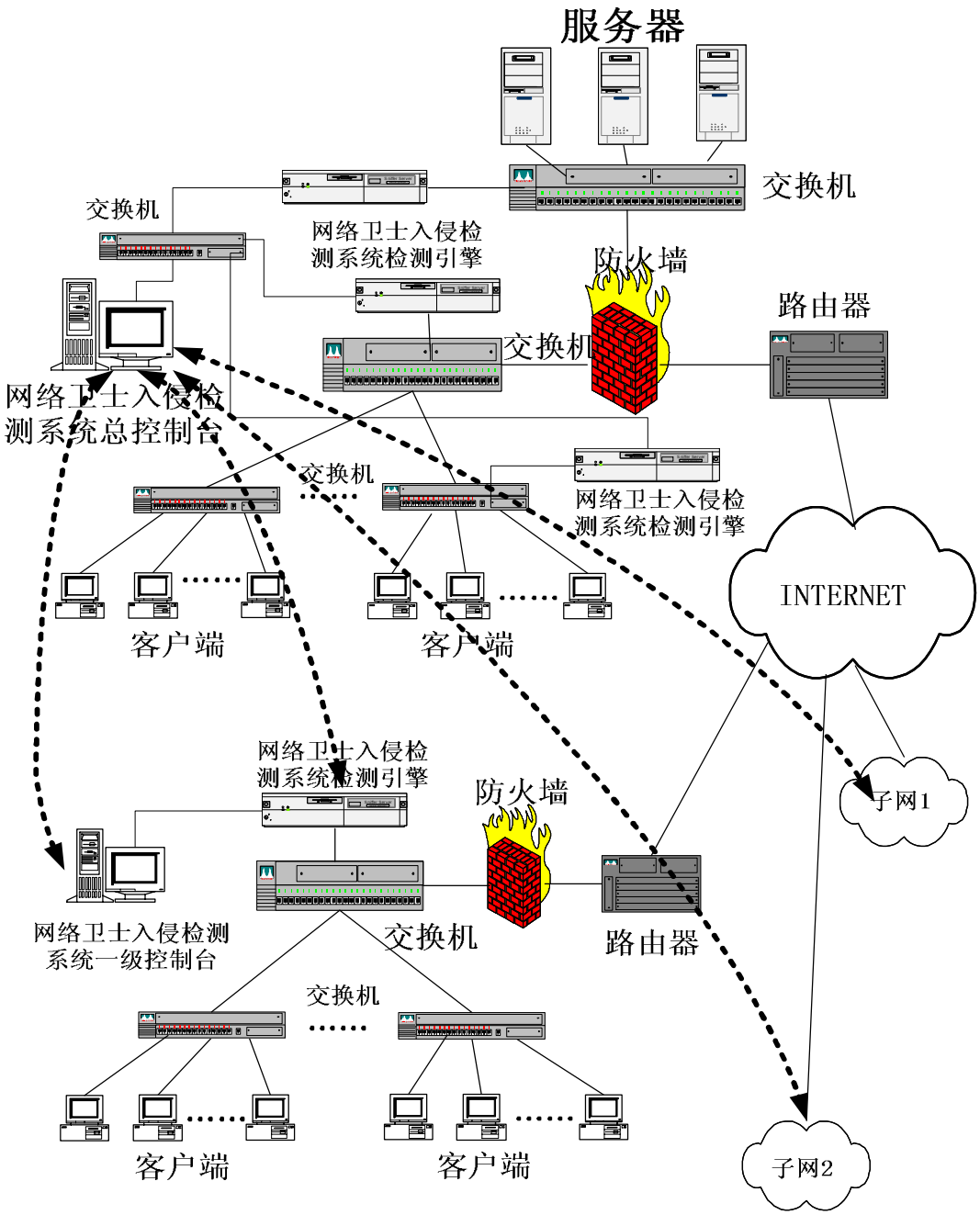

图 **5-3** 分级管理环境应用图