

网络卫士入侵检测系统

TopSentry

产品说明



北京市海淀区上地东路1号华控大厦100085

电话: +8610-82776666

传真: +8610-82776677

服务热线: +8610-8008105119

<http://www.topsec.com.cn>

版权声明

本手册的所有内容，其版权属于北京天融信公司（以下简称天融信）所有，未经天融信许可，任何人不得仿制、拷贝、转译或任意引用。本手册没有任何形式的担保、立场倾向或其他暗示。

若因本手册或其所提到的任何信息引起的直接或间接的资料流失、利益损失，天融信及其员工恕不承担任何责任。本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信恕不承担另行通知之义务。

版权所有 不得翻印© 1995-2009 天融信公司

商标声明

本手册中所谈及的产品名称仅做识别之用，而这些名称可能属于其他公司的注册商标或是版权，其他提到的商标，均属各该商标注册人所有，恕不逐一列明。

TopSEC®天融信

信息反馈

<http://www.topsec.com.cn>

目 录

1	产品概述.....	1
2	产品特点.....	1
3	产品功能.....	5
4	运行环境与标准.....	6
5	典型应用.....	8
5.1	基本的典型应用.....	8
5.2	多级管理部署方式.....	8

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 产品特点

增强的多重入侵检测技术

- 网络卫士 IDS 综合使用误用检测、异常检测、智能协议分析、会话状态分析、实时关联检测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。
- 采用基于协议分析的误用检测技术，实时跟踪各种系统、软件漏洞，并及时更新事件库，可以及时、准确地检测到各种已知攻击。
- 网络卫士 IDS 建立了完备的异常统计分析模型，用户还可以根据实际网络环境适当调整相关参数，更加准确地检测到行为异常攻击。并且，基于内置的强大协议解码器，网络卫士 IDS 能够检测到各种违背 RFC 协议规范的协议异常攻击。
- 内置了遵循 RFC 规范，并基于对协议在实践中的具体执行过程的充分理解而建立的协议解码器。通过详尽、细粒度的应用协议分析技术，提高了检测的准确性。
- 有些网络攻击行为仅靠检测单一的连接请求或响应是检测不到的，因为攻击行为包含在多个请求中。加入状态特性分析，即不仅仅检测单一的连接请求或响应，而是将一个会话的所有流量作为一个整体来考虑。网络卫士 IDS 能够维护完整的会话列表，并实时跟踪会话状态。通过重组网络数据包、监控并分析会话状态，在有效地防止 IDS 规避攻击的同时，不仅可以减少误报和漏报，而且可以大大提高检测性能。

- 天融信网络卫士安全管理系统（TSM）采用基于状态机的实时关联检测技术，对网络卫士 IDS 的报警事件和其他事件进行关联分析，有效地提高了 IDS 检测准确率。
- 内置 2800 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。
- 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。

高效的多层加速技术

- 采用专用的高速硬件平台，提供高速网络接口接入和全面优化的背板总线设计。
- 具有基于专用底层硬件驱动优化技术的底层抓包加速引擎。
- 通过特有的双网卡分流重组技术，可以利用双网卡分别处理上行和下行网络流量，相当于把网卡能力提升一倍，结合独有的流汇聚引擎，有效保证协议分析技术的应用。
- 采用增强直接用户空间访问（EDUA）技术，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，避免了数据的内存拷贝，不需要占用 CPU 资源，从而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。
- 多线程分散式重组引擎，大大提高了重组效率，解决了 IP 分片重组造成的性能瓶颈。
- 采用高效的流定位及状态型的协议分析技术。优化哈希（Hash）表查询，迅速定位每个报文所属 session；通过学习，模拟目标主机进行 TCP 流重组，有效的提高 TCP 流重组性能，并减少了误报；状态型的会话跟踪分析，优化了同一会话的检测速度；完整的协议分析，使得不需传统方式对每个数据包都进行检测，而是基于一个完整数据流进行分析。
- 无缝集成的优化智能模式匹配算法。协议解码器与模式匹配引擎采用无缝连接，在进行细粒度协议分析后进行高效的模式匹配，最大限度地提高性能。

强大的病毒蠕虫检测能力

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近千条的蠕虫检测规则。

SSL 加密访问检测技术

通过解码基于 SSL 加密的访问数据，分析、检测 SSL 加密访问中的攻击行为，从而可以保护内部提供 SSL 加密访问的重要服务器的安全性。

强大的报文回放能力

能够完整记录多种应用协议（HTTP、FTP、SMTP、POP3、TELNET 等）的内容，并按照相应的协议格式进行回放，清楚再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。

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。
 - 联动：防火墙、路由器联动等。
 - 阻断：引擎主动阻断。

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。

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。

多层次、分级管理

- 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。
- 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。
- 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。
- 升级管理：支持对事件特征库和系统的在线升级、文件包升级等升级方式，保证事件特征库和系统的及时更新。

3 产品功能

功能	描述
安全功能	采用高稳定、高安全、高效率、高扩展、模块化、多平台支持的 TOS 操作系统。
	采用创新技术：综合应用会话分析、智能协议分析、异常状态检测等先进的检测技术。
	入侵检测：系统内置 2800 余种入侵检测规则，可以细粒度检测各种入侵攻击企图。
	网络入侵阻断：系统可以阻断对特定服务器的访问或来自特定用户的服务。
	灵活的响应方式：系统对所检测到的入侵企图和违背设定安全策略的活动提供了多种响应方式。
	提供强大的病毒（蠕虫）检测功能及强大的可疑事件（SNA）检测能力。
	与第三方安全产品联动功能：系统可通过 TOPSEC 或 OPSEC 等协议与第三方防火墙互动，可以与 Cisco 路由器互动，组成强大的联合防御体系。
	支持与天融信安全审计系统（TA）、天融信安全管理系统（TSM）联动。
	内置强大的、灵活的协议解码器，用户可根据需求灵活定义协议和各种入侵检测规则。
	分级管理功能：支持大型分布式网络环境下的分级部署管理功能，即可支持多级控制台管理。
支持天融信可信网络架构（TNA）。	
监控功能	实时会话监控：提供实时监控当前 TCP 会话并根据需要进行切断、保存会话内容的功能。
	实时系统监控：系统以图形方式实时监控 IDS 引擎的 CPU、内存等资源信息及实时网络流量信息。
	协议还原与内容监控：监控并还原邮件内容（POP3, SMTP, IMAP, WEB MAIL）；监控并记录 WWW、FTP、TELNET 等 TCP 会话的访问信息。
报表与统计	流量统计：提供基于各种协议的流量统计功能和基于访问端、服务端的流量统计功能。
	提供网络流量统计报表、丰富的入侵事件报表、针对当前系统设置的详细分析报表和用户自定义报表。
增强安全性	增强的安全性：系统提供了采集入侵相关信息、发出入侵警报以及限制网络访问等功能，以保护服务器免受外部和内部的攻击；
	增强的自身安全性：采用 stealth 技术，有效地防止暴露入侵检测系统的存在，控制台引擎间的通讯采用 SSL 加密认证，从而有效地保护了入侵检测系统自身的安全性。
管理功能	简单、实用的图形化用户界面。
	全中文的串口管理功能。
	强大的在线帮助功能：提供强大的入侵规则及产品使用在线帮助，极大地减轻了管理员的负担。
	便捷的升级功能：系统通过自身集成的在线升级模块方便地对入侵检测库和产品模块进行升级。
	分布式探测与集中式管理相结合。

4 运行环境与标准

电源:

➤ 百兆设备:

电压: AC 110/220V

频率: 50/60HZ

电流: 5.0A (110v) /3.0A (220v) (最大)

功率: 250W (最大25摄氏度)

➤ 千兆设备:

电压: AC 100~240V (±10%)

频率: 50/60HZ (±3HZ)

电流: 8.0~5.0A (最大)

功率: 350W (最大25摄氏度)

环境:

运行温度: 0 - 45 摄氏度

非运行温度: -20 - 65 摄氏度

相对湿度: 10 - 90%@40 摄氏度, 非冷凝

国家标准:

GB/T18336-2001

GA/T403.1-2002

BMB13-2004

GB/T9813-2000

GB/T4857.5-1992

参考的安全规范及标准(相对参考):

UL 60950

EN 61000

IEC 950

NEMKO EN 60950

AS/NZS CISPR 22: 2002 Class B

CSA 22.2 NO.234 LEVEL 3

FCC Part 15 Subpart J, Class ‘B’ 115Vac

EC

EN 55022: 1998+A1: 2000, ClassB

EN 61000-3-2: 2000

EN 61000-3-3: 1995+A1: 2001

CISPR 22: 1997+A1: 2000 Class B

抗干扰性:

IEC 61000-4-2: 2001 (ESD)

IEC 61000-4-3: 2002 (辐射敏感性)

IEC 61000-4-4: 1995 (电快速瞬变)

IEC 61000-4-5: 2001 (电源)

IEC 61000-4-6: 2001 (谐波)

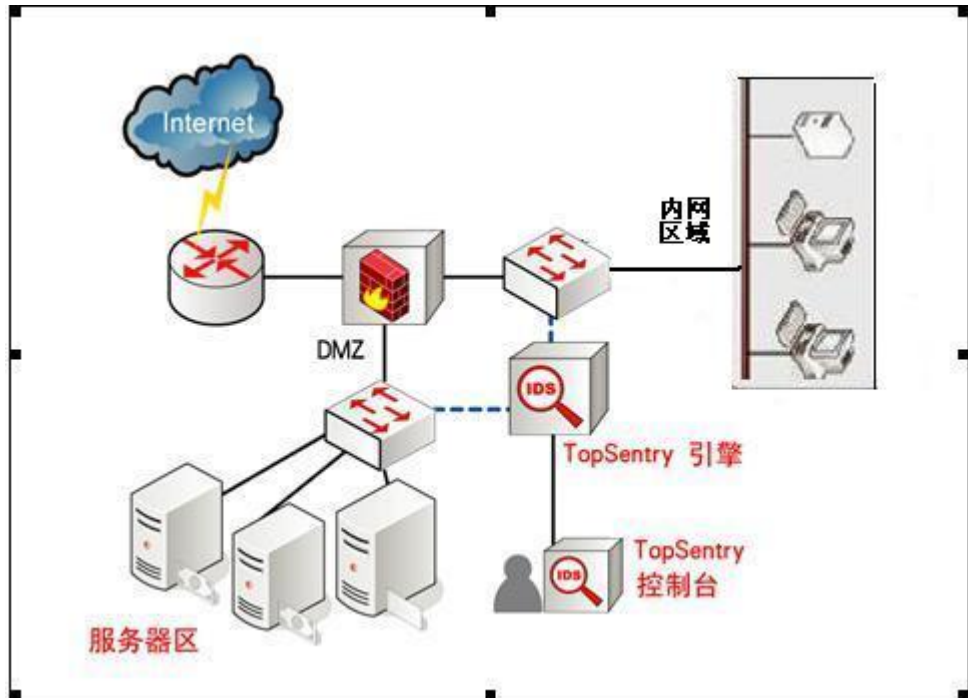
IEC 61000-4-8: 2001

IEC 61000-4-11: 2001

5 典型应用

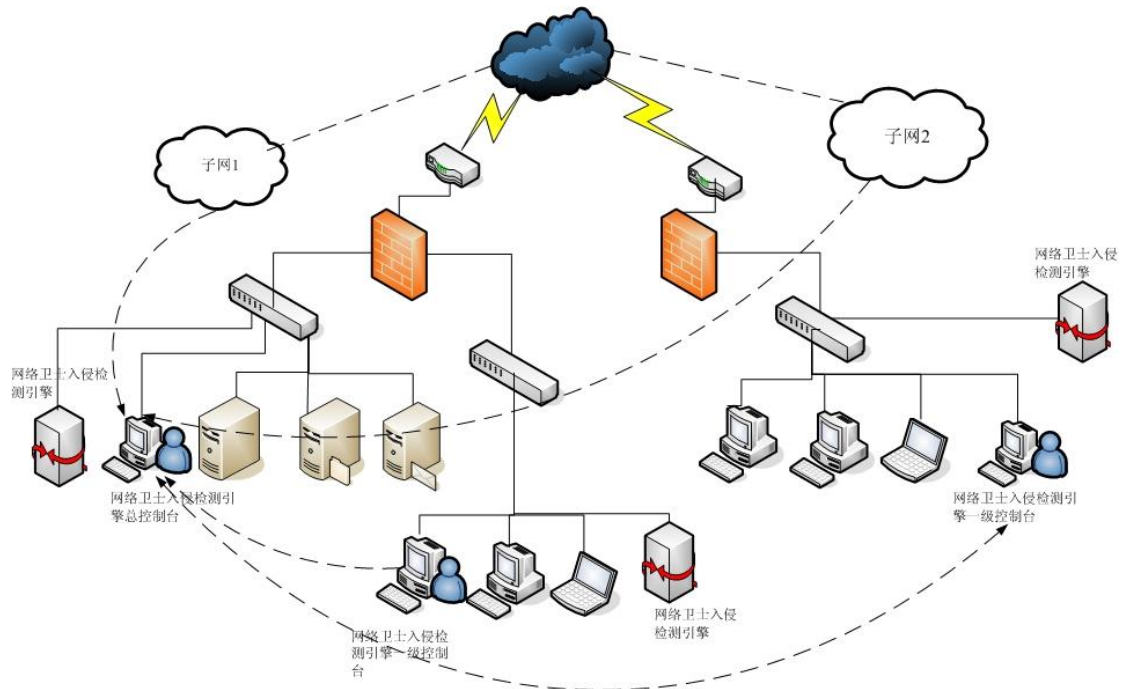
5.1 基本的典型应用

对于一般中小型企业的网络部署，TopSentry 的监听口可通过端口镜像来同时监控内网和 DMZ 区的入侵，起到入侵检测的作用。部署如下图：



5.2 多级管理部署方式

为了满足用户复杂网络环境中部署多台网络卫士入侵检测设备，来实现对用户整个环境的完全保护，天融信的网络入侵检测设备可以实现多级部署的方式，分布在用户不同网络中的入侵检测引擎可以和总控制台统一实现入侵保护。示意的部署如下图：



声明：

1. 本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信恕不另行通知。
2. 本手册中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此可能产生的差异为正常现象，相关问题请咨询天融信客户服务中心 400-610-5119 或者 800-810-5119。
3. 本手册中没有任何关于其他同类产品的对比或比较，天融信也不对其他同类产品表达意见，如引起相关纠纷应属于自行推测或误会，天融信对此没有任何立场。
4. 本手册中提到的信息为正常公开的信息，若因本手册或其所提到的任何信息引起了他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。