

网络卫士安全审计系统

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..... | 2 |
| 3 | 产品功能..... | 4 |
| 4 | 运行环境与标准..... | 6 |
| 5 | 典型应用..... | 7 |
| 5.1 | 网络行为审计..... | 7 |
| 5.2 | 业务系统审计..... | 8 |

1 产品概述

网络卫士安全审计系统中的内容和行为审计子系统是由北京天融信公司自主研发的面向企业级用户、集内容审计与行为审计为一体的网络信息安全审计系统。内容和行为审计系统以旁路的方式部署在网络中，不影响网络的性能。内容和行为审计系统具有即时的网络数据采集能力、强大的审计分析功能以及智能的信息处理能力。通过使用该系统，可以实现如下目标：

- 对用户的网络行为监控、网络传输内容进行审计（如员工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、员工是否通过网络泄漏了公司的机密信息等等）。
- 实现对单位业务系统核心数据库的操作过程进行审计，有效保护业务数据的完整性。可以对违规行为进行审计记录与报警。
- 实现网络传输信息的保密存储。
- 实现网络行为后期取证。
- 对网络潜在威胁者予以威慑。该产品适用于对信息保密、控制非法信息传播比较关心的单位或需要实施网络行为

该产品适用于对信息保密、控制非法信息传播比较关心的单位或需要实施网络行为监控的单位和部门。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，以及大中型企业网络管理中心等。

2 产品特点

● 部署方式简便

- 旁路模式接入，不改变用户的网络拓扑结构，对用户的网络性能没有任何影响。
- 独立部署，方便灵活。
- 提供基于 Rich Client 技术的 WEB 管理界面。兼具 B/S 模式的便捷与 C/S 模式的高效、易用

● 高速的数据采集

分布式部署数据采集引擎，优化的数据采集技术，直接从内核中采集数据包。延迟小、效率高、实时性强。

● 智能包重组和流重组

具有强大的 IP 碎片重组（IP Fragments Reassembly）能力和 TCP 流重组（TCP Stream Reassembly）能力，任何基于协议碎片的逃避检测手段对本产品无效。

● 自适应深度协议分析

- 从链路层到应用层对协议进行深度分析。
- 自动识别基于 HTTP 协议的邮件、论坛等操作行为。
- 根据内容自动识别各个连接的应用协议类型。保障审计的准确性

● 数据海量存储和备份

系统内置海量数据存储空间，支持百兆、千兆网络环境下，高速、大流量数据的采集、存储。

灵活的远程备份功能，可以在不丢弃数据的同时保证系统持续稳定运行。

● 强大的数据挖掘功能

采用以相关度为核心，引入向量模型、查询串重构等技术的匹配算法，大大提高了全文检索的速度。对用户选定时间范围内的发件内容，根据预先设定的关键词库，自动快速的进行全文检索，匹配成功的内容将以醒目的字体颜色显示。

完善的自定义分析统计功能，可以实时统计任何一种网络行为属性，随时把握网络利用状况。

● 高度安全性和可靠性

- 系统管理平台提供基于 SSL 加密的 WEB 管理方式。
- 分权、分级、分角色的用户管理。
- 提供完善的系统日志审计功能
- 对于管理者 IP 白名单以外的地址自动隐藏系统 IP。

● 系统的良好可扩展性

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。

● 友好易用的界面设计

应用界面美观大方，操作方便。

3 产品功能

| 功能 | 描述 |
|-------------------|--|
| 支持数据库监控与审计 | <ul style="list-style-type: none"> ◇ 支持 Sybase, DB2, SQL Server, Oracle, mysql, informix 等多种主流数据库监控与审计, 实现用户数据库操作与结果跟踪 ◇ 支持数据库操作过程跟踪, 绑定变量识别 |
| 支持多种应用协议的监控、还原和审计 | <ul style="list-style-type: none"> ◇ Web 浏览 (HTTP): 能完全截获、记录、回放、归档被监测网络中所有用户浏览的 WEB 内容。 ◇ Web 发布 (HTTP): 能完全截获、记录、回放、归档被监测网络中所有用户通过 WEB 发表的内容。 ◇ 电子邮件 (POP3、SMTP、WEB MAIL): 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。 ◇ 文件下载 (FTP): 能记录、查询访问 FTP 服务器的用户名、口令, 回放用户在服务器上的操作过程、还原用户传输的数据。 ◇ 即时聊天 (MSN、QQ 等): 能完全记录用户登录时间、离开时间, 用户登录 IP 地址、目的 IP 地址, 聊天时使用的用户名; 还可以监视用户聊天频率、MSN 可还原用户聊天内容。 ◇ 远程登录 (TELNET): 能记录和查询访问服务器上 TELNET 的用户名和口令字; 能记录和回放用户在服务器上的操作过程。 ◇ P2P (BT, emule) 能记录进行 BT 操作的源、目的 IP, 访问时间与流量 ◇ 独立开发应用协议自动识别技术, 实现完整监控 |
| 强大的流量监控与统计功能 | <ul style="list-style-type: none"> ◇ 对重要 IP 进行流量监测, 并绘制出直观的流量曲线图、柱状图, 有效发现网上出现的异常流量。 ◇ 支持对历史流量统计分析。 ◇ 可以对各种应用的流量进行统计, 以曲线图直观显示, ◇ 可以统计各个主机流量详情, ◇ 可以分析网络各个时间每主机负载, 立即发现网络瓶颈 |
| 强大的报表与统计功能 | <ul style="list-style-type: none"> ◇ 支持多种条件的统计分析。 ◇ 完善的报表功能: 提供多种专业化报表和分析图表。 |
| 支持多种审计方式 | <ul style="list-style-type: none"> ◇ 实时监控: 对网络中各种应用进行实时监控分析。 ◇ 行为监控: 可以完全记录、回放用户的网络行为。 ◇ 内容查看审计: 支持网络数据内容的完全还原, 后期可以进行内容审计、取证。 ◇ 流量监控: 通过流量监控, 有效发现网上出现的异常流量。 |

| 功能 | 描述 |
|----------------|--|
| | <ul style="list-style-type: none"> ◇ 报表统计：通过统计分析，发现网络中潜在的危险。 ◇ 对应事件到人：可以确定各个 IP 所在地。 |
| 支持多种报警响应方式 | <ul style="list-style-type: none"> ◇ 邮件报警 ◇ Syslog ◇ SNMPTrap ◇ 短信报警(需要单独购买短信模块) |
| 灵活全面的审计策略 | <ul style="list-style-type: none"> ◇ 采集策略 ◇ 关键词策略 ◇ 流量监控策略 ◇ 报警响应策略 ◇ 统计分析策略 ◇ 关联分析策略，实现不同种类事件间的关联分析 |
| 强大的资源监控和日志功能 | <ul style="list-style-type: none"> ◇ 支持系统资源的实时监控。 ◇ 提供完整的操作日志、系统日志记录,可以进行方便的查看、导入导出。 |
| 支持多种编码、压缩格式 | <ul style="list-style-type: none"> ◇ 支持多种编码方式：Base64、Quoted-Printable、UTF-7、UTF-8、EBCDIC。 ◇ 支持多种压缩格式：Zip、Rar、Arj、Gz 等，可支持多达十四层的压缩。 |
| 高速、完整、海量信息处理能力 | <ul style="list-style-type: none"> ◇ 零拷贝高速抓包。 ◇ 分布式数据采集、数据处理。 ◇ 强大的包重组和流重组能力，可以监控各种基于协议碎片的逃避检测行为。 |
| 增强的自身安全性 | <ul style="list-style-type: none"> ◇ 基于 SSL 协议的加密数据传输。 ◇ 支持基于 CA 的身份认证。 ◇ 审计引擎不对外开放端口。 ◇ 分权、分级、分角色的用户管理。 ◇ 系统日志审计功能。 ◇ 特有 IP 隐藏功能，最大化保障系统安全性 |
| 旁路方式接入网络 | <ul style="list-style-type: none"> ◇ 使用交换机镜像口、共享式 HUB 接入网络，不影响网络部署方式、不影响网络性能。 ◇ 即插即用，安装非常简单。 |
| 强大便捷的部署、管理方式 | <ul style="list-style-type: none"> ◇ 提供功能强大的串口管理功能。 ◇ 友好易用的界面，易于上手使用。 |

| 功能 | 描述 |
|----|-------------------------|
| | ◇ 提供详细的帮助，极大地减轻了管理员的负担。 |

4 运行环境与标准

电源：

电压：AC 110/220V

频率：50/60HZ

电流：3.0A (最大)

功率：260W (最大)

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

GB/T18019-1999

GB/T18020-1999

参考的安全规范及标准(相对参考):

UL 1950

EN 41003

AS/NZS 3260

AS/NZS 3548 Class A

CSA Class A

FCC Class A

EN 60555-2

VCCI (ClassII) 抗干扰性:

IEC 1000 4 2 (ESO)

IEC 1000 4 3 (辐射敏感性)

IEC 1000 4 4 (电快速瞬变)

IEC 1000 4 5 （电源）

IEC 1000 3 2 （谐波）

5 典型应用

5.1 网络行为审计

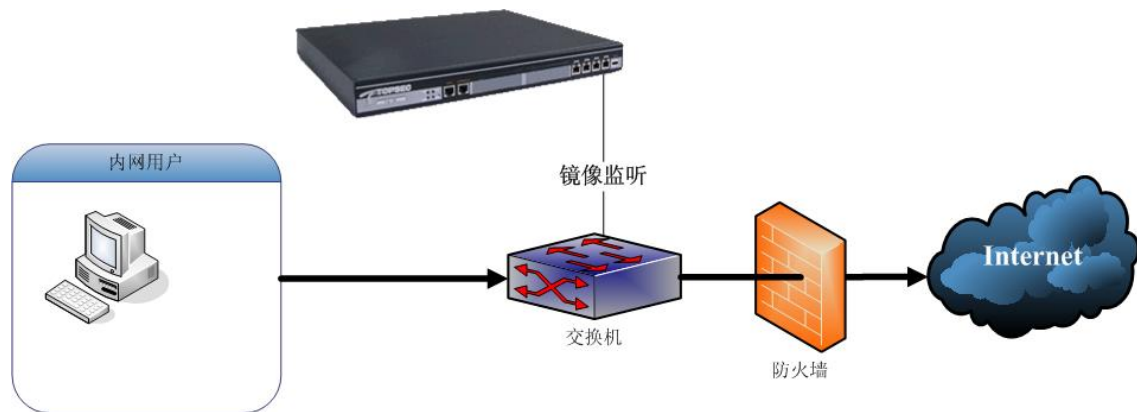


图 5-1 系统部署图

通过在核心交换机上部署 TA-W 系统可以对内网用户的所有上网行为进行记录与监控。同时通过强大的审计分析功能可以准确定位网络行为历史事件的详情，并进行回放，可以在事件发生后第一时间定位到责任人。

通过内置多样化的报表，可以给出当前网络的利用情况，统计分析出多种组和条件的 Top 排名。

利用 TA-W 系统的流量分析功能，可以了解当前网络的带宽占用情况，可以实现应用/IP/时间/接口四个维度的流量统计分析与报表生成。

5.2 业务系统审计

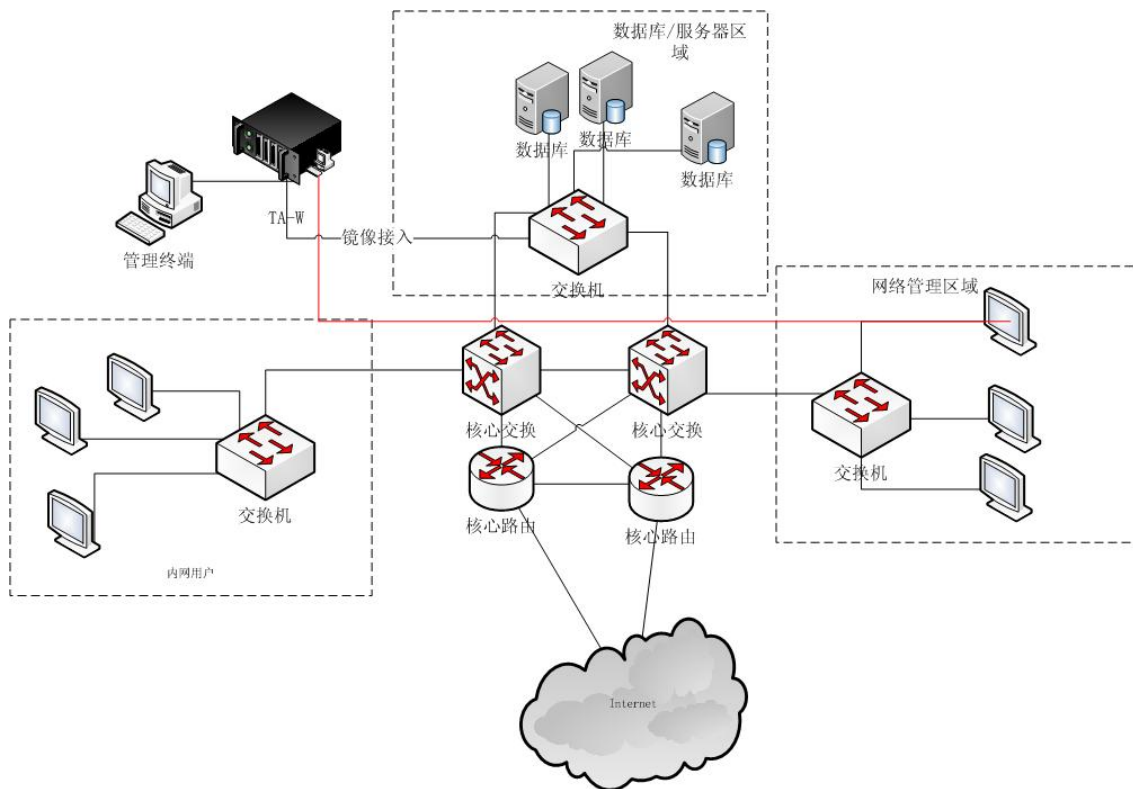


图 5-2 系统部署图

TA-W 通过数据库服务器所在的主交换机镜像口取得网络中所有对于数据库访问的数据包，并对数据包进行重组与协议解析还原。通过对解析结果的再分析实现对数据库访问的监控与审计。

TA-W 系统内置自身审计与 IP 隐藏等安全防护功能，可以有效防止非法用户访问 TA-W 系统或恶意删除、篡改监控日志。

通过用户定义的规则，TA-W 系统可以对访问事件进行危险级别划分，对于不同危险级别的事件可以提供多种报警响应方式，及时通知用户。

TA-W 在内容审计的同时还为用户提供了网络流量分析、并发连接数据分析功能，可以让用户深入了解数据库系统的应用与负载情况。

通过统计分析功能，用户可以统计访问事件中任意一个字段的发生频率，如源 IP 访问频率，目的 IP 访问频率，数据库访问频率，不同操作类别的访问频率。通过这一功能，用户可以了解业务系统的应用情况与系统瓶颈。

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。