

网络卫士日志审计系统

TA-L 系列

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© 1995-2007 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
1.1	引言.....	1
1.2	系统组成.....	2
1.3	系统运行平台.....	3
1.4	系统工作流程.....	3
2	产品特点	5
2.1	功能特点.....	5
2.2	技术特点.....	8
3	产品功能	10
4	运行环境与标准	11
5	典型应用	12
6	声明	13

1 产品概述

1.1 引言

随着互联网规模的几何级数的增长，网络安全日益成为威胁网络正常运行的主要问题。当前解决网络安全问题的主要手段是在网络中增加防火墙、防病毒软件、IDS、VPN 等网络安全设备。这些网络中的各种安全设备（防火墙、IDS 系统、防病毒软件等）、操作系统（包括 Windows 和 Unix）、应用服务（email、www、ftp、DNS）等都可产生大量的日志数据。这些日志数据详实地记录了系统和网络的运行事件，是安全审计的重要数据。这些日志信息对于记录、检测、分析、识别各种安全事件和威胁有非常重要的作用，也是对当前网络安全情况进行评估的主要数据源。但由于目前网络设备越来越多，网络攻击的手段越来越多样，攻击方法越来越隐蔽，单纯的依靠某一种安全设备的事件来对网络安全情况进行评估和反应是远远不够的。

要对各类系统产生的安全日志实现全面、有效的综合分析，就必须为网络安全管理员建立一个能够集中收集、管理、分析各种安全日志的安全审计管理中心，使网络管理员不用像以前那样从庞杂的日志信息中手工搜寻网络入侵的行为，为管理员提供一个方便、高效、直观的审计平台，大大提高了安全管理员的工作效率和质量，更加有效地保障了网络的安全运行。

天融信公司根据现代安全技术发展的趋势和理念开发推出了日志审计系统，用于帮助企业实现网络事件和信息的有效管理及全面审计。日志审计系统针对大规模复杂网络而设计，通过多级部署实现对现有任意复杂网络的支持，广泛支持对现有网络设备及系统的日志的收集及审计，提供强大的可视化事件分析能力，基于 AI 及 IDS 技术多层次的实时审计有效发现潜在的入侵行为，并可根据用户策略进行多种模式的响应。

系统设计贯穿现代 PDR2（protection、detection、response、recovery）动态防御体系思想，与其它安全设备有效整合真正实现全网安全与动态防御。



图 1-1 PDR2 动态防御

日志审计系统为不同的网络设备提供了统一的事件管理分析平台,打破了企业中不同网络设备存在的信息鸿沟。系统提供了强大的监控能力,从网络到设备直至应用系统的监控。在对事件的监控信息的集中及关联分析的基础上,有效的实现了全网的安全预警、入侵行为的实时发现、入侵事件动态响应,通过与其它安全设备的联动来真正实现动态防御。

1.2 系统组成

日志审计系统主要由日志代理、安全审计中心、日志数据库、审计系统管理器四个部分组成。

1. 日志代理 (Agent)

收集各种操作系统、网络安全设备、应用程序的日志信息,过滤后发送给安全审计中心处理。日志代理是安全审计系统的触角。审计系统主要通过日志代理收集各类系统无法远程收集的信息。

2. 安全审计中心 (Audit Center)

接收日志代理和各种安全设备、系统转发的日志信息,集中保存在日志数据库,分析后通过审计系统管理器将分析前、后的结果呈现给用户。

3. 日志数据库 (DataBase)

保存各种日志信息、系统配置信息。

4. 审计系统管理器 (System Manager)

提供给用户一个方便、直观的管理接口。通过管理器用户可以查看日志、报表等各种信息结果。

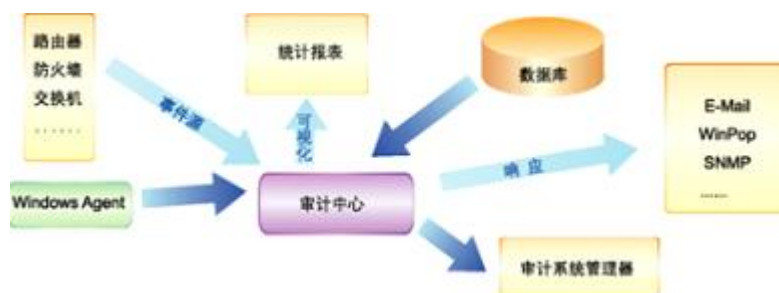


图 1-2 天融信日志审计系统组成

1.3 系统运行平台

代理程序运行平台：WINDOWS 2K/XP/2003。

安全审计中心平台：WINDOWS 2K/XP/2003。

日志数据库系统：MS SQL SERVER 2000 版本。

审计系统管理器运行平台：WINDOWS 2000/XP/2003 操作系统平台上。

1.4 系统工作流程

日志审计系统的系统工作流程可分为四个主要过程：

1. 网络事件的收集：

通过本地（主要通过代理）或远程信息收集等方式收集来自网络中不同设备、系统及应用的日志及实时监视信息（系统提供对不同设备、系统、应用及服务的监视），同时将收集到的信息根据统一的信息格式进行标准化处理。

2. 事件的处理：

对接收到的已格式化的事件信息进行处理，首先按审计策略进行事件的过滤，然后对大量的同类事件进行归并处理，避免产生事件风暴。事件的归并能简化后续的分析及方便用户的查看。处理后的事件分别发送至智能实时检测引擎及数据库系统。同时，根据制定的响应策略对不同事件进行不同方式的响应。

3. 事件的可视化分析

通过对系统数据库中历史数据的分析，从不同角度（按网络设备、系统、事件类型等），按系统预设的不同模板生成分析结果，并根据用户的要求通过丰富的图表来显示分析的结果。分析涵盖了对事件的归类统计及事件的变化发展趋势。

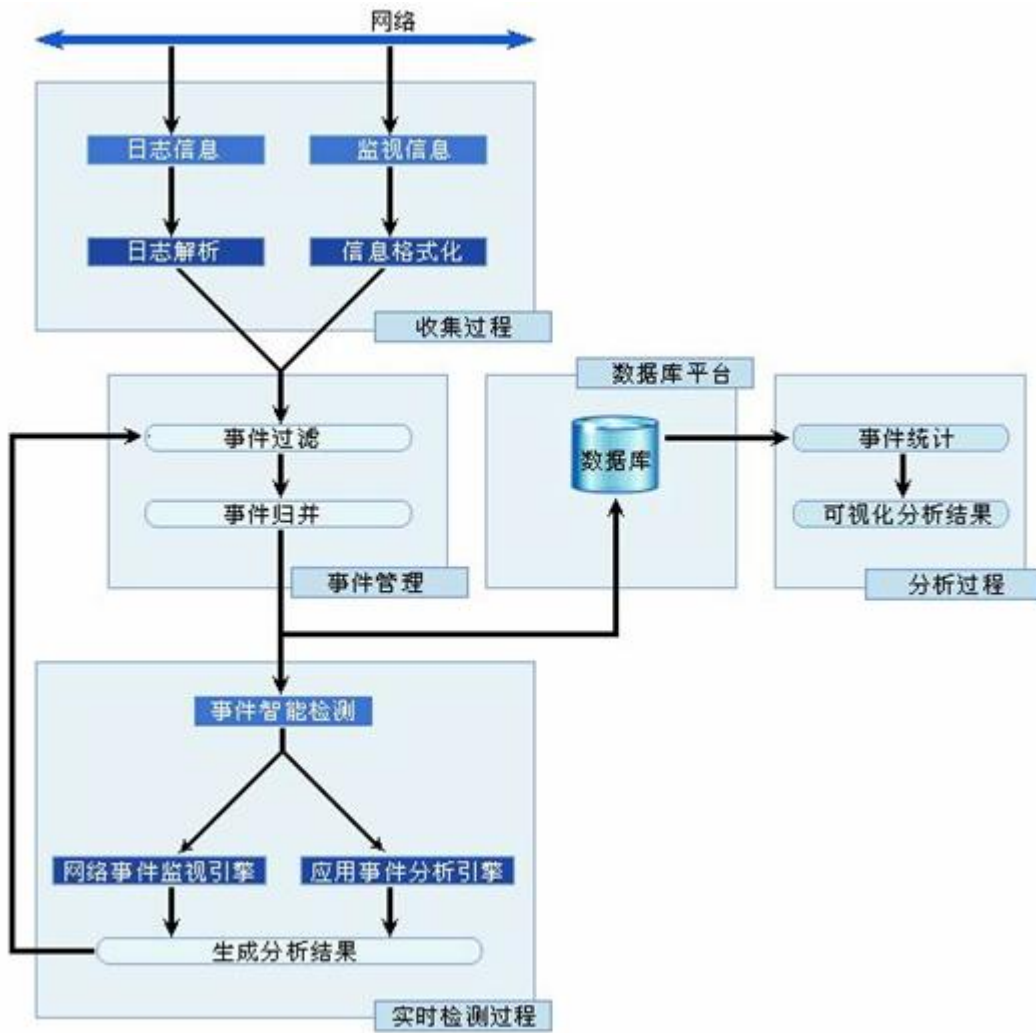


图 1-3 系统工作流程

2 产品特点

天融信日志审计系统设计中融入了先进的安全理念和思想，实现上采用了软件及安全技术的最新成果。因此无论是在功能上还是在技术上都有许多独特之处。

2.1 功能特点

- **多级部署支持复杂网络**

各种应用的庞大及复杂化导致网络结构日益复杂，为网络事件的管理提出了挑战。面对复杂网络，应用日志审计系统，管理员可以根据网络拓扑的实际情况，划分不同的审计区域部署多级审计服务器，即便是在包含 NAT 的网络多层结构中，也可以轻松实现有效的事件管理和审计。

- **跨平台的最全面的日志信息采集及管理**

系统全面支持安全设备（如防火墙，IDS、AV 等）、网络设备（如 router、switch）、应用系统（如 Web、Mail、ftp、Database）、操作系统（如 Windows、Linux、Unix）等多种产品及系统的日志数据的采集和分析。支持对不同日志格式的分类、筛选、最大效率保存；日志自动导出、导入、删除、备份、恢复、转发等日志管理功能。提供了多样、灵活的日志信息查询，同时支持按用户设定的条件进行不同日志的相关查询，有效地把不同设备及平台的事件关联起来，帮助管理员实现更加全面、深入的分析事件。

系统提供迄今为止最为全面的日志信息采集功能。提供对各厂商的网络设备及服务的日志支持，支持厂商及设备如下。

防火墙：支持天融信所有系列的防火墙。

支持思科所有系列的防火墙。

同时系统备有标准格式支持所有可以产生 Syslog 日志的防火墙。

IDS：

支持收集 Snort 所有系列的 IDS 日志。

支持收集北方计算中心 IDS 日志

过滤网关：

支持收集天融信所有系列的过滤网关。

路由器：

思科所有系列的路由器。

同时系统备有标准格式支持所有可以产生 Syslog 日志的路由器。

交换机：

思科所有系列的交换机。

华为所有系列交换机。

北电所有系列交换机。

同时系统备有标准格式支持所有可以产生 Syslog 日志的交换机。

标准 Syslog 日志收集：

支持收集各种操作系统、网络设备产生的 Syslog 日志。如：Linux、Unix、
可以产生 Syslog 日志的交换机、防火墙等。

Windows Eventlog 日志：

支持各种 Windows 平台的 EventLog 日志收集。如：Win2000/XP/2003 等等。

ORACLE 数据库日志：

支持读取 Oracle 本身的日志信息，对 Oracle 数据库日志进行审计。

HTTP 服务：

支持收集 Apache 服务和 IIS 服务的 HTTP 日志。

EMAIL 服务：

支持收集 Exchange 服务的日志。

FTP 服务：

支持收集 IIS 服务的 FTP 日志。

DATABASE 服务：

支持收集 SqlServer 数据库、DB2 数据库的操作日志。

其他产品的日志直接记录到日志审计系统日志库，在用户界面上提供通用库通用表查询功能，可以直接查到该产品的日志信息。对于已经入日志审计系统日志库的业务系统日志，系统还提供业务系统专用的数据库表和日志查询显示界面。

● 全面丰富的分析报表

系统在对收集的事件进行详尽的分析及统计的基础上支持丰富的报表, 实现分析结果的可视化。为了帮助管理员对网络事件进行深度的挖掘分析, 系统提供多达 300 多种的报表模板, 支持管理员从不同方面进行网络事件的可视化分析, 不仅支持对网络事件的按条件统计, 更提供了对如防火墙流量等变化趋势的形象表现。对于分析结果系统提供了表格及多种图形表现形式 (柱状图、曲线图), 使管理员一目了然。

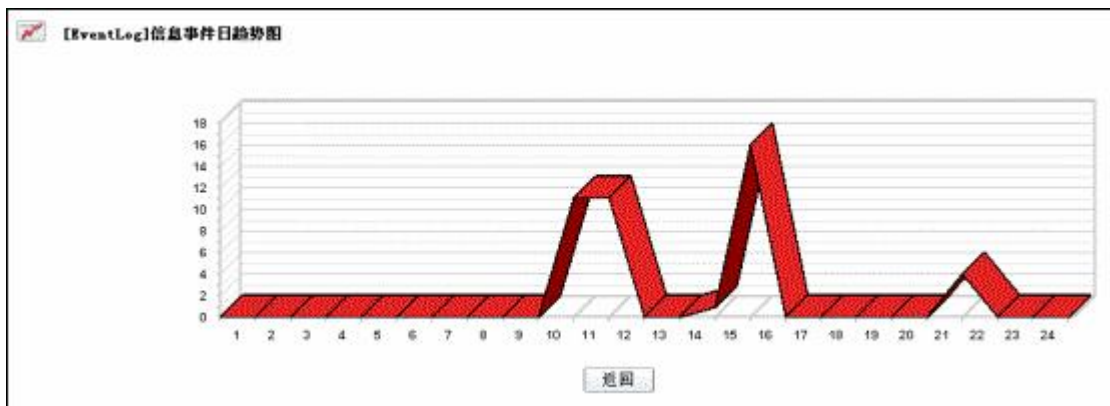


图 2-1 分析报表界面图

● 直观便捷的系统管理

系统提供强大便捷的管理界面, 用户可以在网络中的任意节点对系统及网络事件进行方便、有效的管理, 大大减轻了管理员的工作强度, 提高了工作效率。

通过管理界面可以便捷地实现对日志数据、审计策略、系统及不同组件进行集中、可视化的管理。同时提供了基于角色的权限访问控制。

● 全面强大的监视功能

日志审计系统不仅支持对网络设备及主机的全面监视(在线情况及设备基本性能信息等), 也支持对系统应用的监视。系统同时还提供了对多种网络服务(SMTP、POP3、WEB、FTP、DHCP 等)的监视, 强大全面的监视功能使得对于大型复杂网络中设备的监管变得易如反掌。

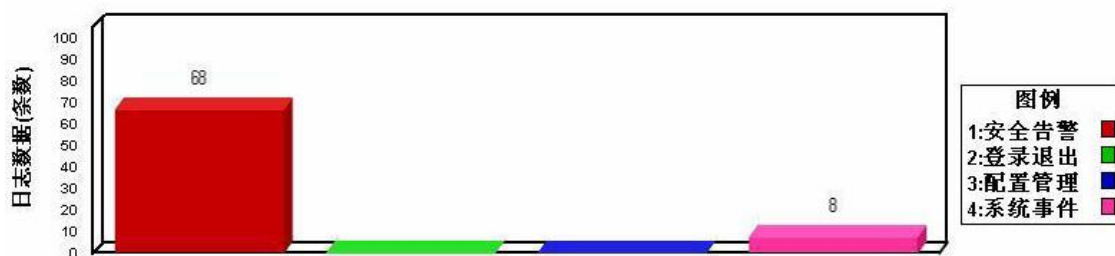


图 2-2 监视界面图

- 多样的响应方式

根据定义的事件的危险级别采用 EMAIL、铃声、SNMP 等多种响应方式。

2.2 技术特点

- 先进的多级架构设计

日志审计系统采用业界领先的多级架构设计，系统具有良好的网络适应性和伸缩性；同时支持多套系统级联部署，上级系统能方便地管理下级系统，因此，系统可以非常方便、快捷地部署在大型复杂的网络环境中。同时，多级审计结构也有效地解决了含有 NAT 的复杂网络中事件的收集和审计问题。

- 高柔韧性及可靠性的类微内核系统模式

微内核（Micro-Kernel）是经典的高可靠性 OS 设计模式，日志审计系统为了实现系统可靠性与性能的平衡采用了一种类似微内核的系统模式。可以通过在系统内核上简单地添加或移去功能插件来满足不同用户的要求并实现对系统的扩展。建立在内核之上的分立功能插件实现了错误的隔离，从而提高了系统安全性。这一系统模式贯穿了系统的各个部分（审计服务器、Agent 等）。

● 基于 **SSL** 技术安全通讯

SSL(Secure SocketLayer)是 netscape 公司设计的主要用于 web 的安全传输协议。这种协议在 WEB 上获得了广泛的应用。日志审计系统间通过 SSL (Secure Socket L) Layer) 实现保密通讯, 增强了数据的安全性也提高了系统的整体安全性。有效的防止了数据被恶意监听、修改及非法接入系统。用户可以根据自身的网络环境选择采用加密通讯或普通通讯, 同时系统支持两种方式间的自动切换。

● 采用 **XML** 技术实现信息交换

日志审计系统的数据文件及其部分系统的配置采用 XML 文件形式存储, XML 不仅提供了清晰的结构化的信息表现能力, 同时作为一种流行的标准的信息交换形式, 使得系统的数据及信息可以在不同平台及系统间自由交换, 为与其它系统、平台进行有效整合提供了保障。

3 产品功能

功能类别	子功能	说明
日志	日志收集	<ul style="list-style-type: none"> ◇ 日志审计系统收集任何系统或设备的日志前都需要设置日志收集源和日志代理，即定义收集哪些系统（或设备）的哪些日志 ◇ 日志代理包括域控制代理、windows 日志代理 ◇ 日志审计系统通过加密锁控制日志收集源的数量
	日志查询	<ul style="list-style-type: none"> ◇ 支持按照日志类型查询日志 ◇ 支持按照日志格式查询日志 ◇ 支持按照审计域查询日志 ◇ 提供业务系统日志查询界面 ◇ 界面上提供通用库通用表查询功能，方便用户查询其他产品的日志信息。
	日志监视	<ul style="list-style-type: none"> ◇ 根据过滤条件，实时监视各类日志
报表	报表统计任务	<ul style="list-style-type: none"> ◇ 统计报表的生成是基于日志源的，管理员通过输入相应的参数来有计划地订制一批报表任务，报表任务可根据用户预先设定的条件立即执行或按一定周期执行
	报表模版	<ul style="list-style-type: none"> ◇ 日志审计系统内置了丰富的报表模板供用户使用，报表模板定义了报表中显示的日志内容
	报表浏览	<ul style="list-style-type: none"> ◇ 支持浏览、查找、删除和导出报表
系统监控 报警	安全审计系统监视	<ul style="list-style-type: none"> ◇ 监视安全审计系统的性能信息，包括 CPU 信息、内存信息和磁盘使用信息
	日志代理信息监视	<ul style="list-style-type: none"> ◇ 监视代理的性能信息，包括被监控代理的 CPU 信息、内存信息和磁盘使用信息
	安全审计信息监视	<ul style="list-style-type: none"> ◇ 监视安全审计系统服务器自身的日志信息
	报警方式管理	<ul style="list-style-type: none"> ◇ 日志审计系统支持事件的安全响应，包括 5 种响应方式，分别是：Email 报警、WINPOP 报警、SNMP 报警、铃声报警和 GUI 报警
	报警策略管理	<ul style="list-style-type: none"> ◇ 定义事件的报警方式，即定义什么样的事件采取什么样的报警方式 ◇ 用户可以定义自动告警功能，而且用户可以自定义告警内容及管理员应采取的措施，保证报警信息能够足以提醒安全保密管理人员有安全事件发生。
	数据库报警管理	<ul style="list-style-type: none"> ◇ 用户设置审计日志的存储空间阈值、指定当审计存储空间将满时采取的告警方式。则系统将按照设置，自动提醒系统管理员采取措施。
	用户管理	<ul style="list-style-type: none"> ◇ 支持基于用户组的权限分配和管理，权限包括查询日志、系统配置、报表和安全分析、实时监视四种，管理员可自行组合使用 ◇ 支持用户组/用户的添加、删除和修改等操作
	IP 组管理	<ul style="list-style-type: none"> ◇ 支持根据 IP 地址范围定义 IP 组 ◇ 支持 IP 组的添加、删除和修改操作
	数据库管理	<ul style="list-style-type: none"> ◇ 支持数据库备份 ◇ 支持历史数据库管理
	多级域管理	<ul style="list-style-type: none"> ◇ 日志审计系统支持多级域部署 ◇ 支持上级域下发策略给下级域 ◇ 支持下级域上传日志给上级域 ◇ 支持上级域查询下级域的日志信息

4 运行环境与标准

➤ 日志数据库

操作系统:

中英文 windows 2000/2003 服务器版

数据库系统:

MS SQL Server 2000

【注意】: 在 Windows 2003 下需要升级至 Microsoft SQL Server 2000 Service Pack 3;

不支持 MS SQL Server 7.0;

最低配置:

CPU : P4 1.7G

内存: 512M

硬盘: 40G

推荐配置:

CPU: P4 2.4G

内存: 1G

硬盘: 80G

➤ 网络卫士安全审计系统 TopAudit

操作系统:

中英文 windows 2000/2003 服务器版

最低配置:

CPU : P4 1.7

内存: 512M

硬盘: 40G

推荐配置:

CPU: P4 2.4G

内存: 1G

硬盘: 80G

➤ 审计系统管理器

操作系统:

中英文 windows 2000/XP/2003

推荐配置:

CPU: P4 2.4G

内存: 512M

硬盘: 80G

➤ 日志代理

操作系统:

中英文 windows 2000/XP/2003

配置要求:

根据可能产生日志的情况适当挑选硬件即可。

5 典型应用

日志审计系统适合应用于结构较为复杂的企业内部网络,与天融信的网络卫士系列防火墙及其它各种支持 TOPSEC 安全协议的网络设备配合使用,可以最大限度地保障用户网络的安全性。一种典型的配置如下图所示:

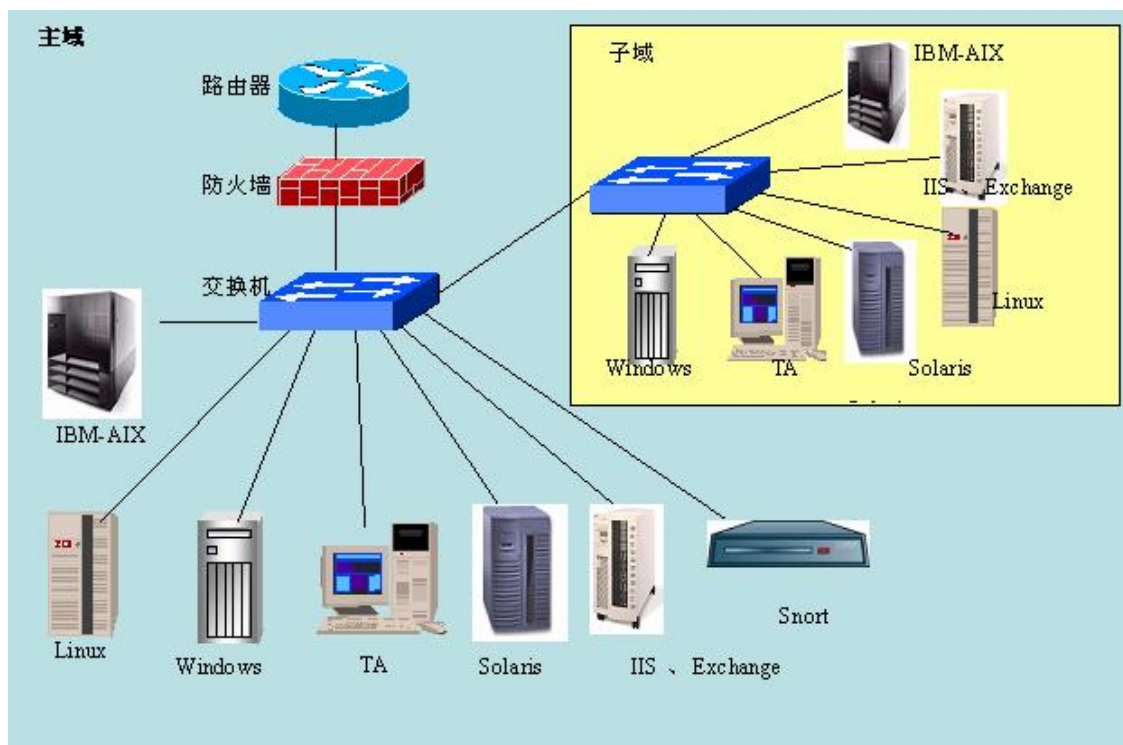


图 5-1 天融信日志审计系统典型应用案例

上图中企业内部网分成两部分,分别由两个日志审计系统收集各自域中的的所有设备的日志。主域的日志审计系统可以收集处理位于企业内部网中主域中的主机的系统日志、服务器的应用系统日志、入侵检测系统、路由器、交换机等网络设备的日志信息;子域的

日志审计系统能收集处理位于子域中的主机系统日志、服务的应用系统日志等各种设备的日志信息，同时还可以把日志上传到主域的日志审计系统中，主域的日志审计系统收到子域上传的日志也可以查询处理子域中的主机日志、服务器的应用系统日志，也可以把策略下发到子域中。主域和子域的实时监控网络状态及各种安全事件，有效管理全网的安全事件，实现全网的动态安全。主域的实时监控还可以监控子域所监控的网络状态和各种安全事件。

6 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，产品功能和性能请以产品说明书为准。
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。