知道创宇

知道创宇日志管理综合分析系统

产品白皮书

北京知道创宇信息技术股份有限公司

目 录

1 前言.....3
2 产品应用需求.....5
2.1 日志审计管理需求.....5
2.2 安全审计法规遵循.....5
2.3 信息安全审计目标.....7
3 产品介绍.....9
3.1 产品概述.....9
3.2 体系结构.....10
4 功能介绍.....11
4.1 日志数据采集.....11
4.2 实时动态分析.....11
4.3 安全存储管理.....12
4.4 历史事件检索.....13
4.5 综合审计报告.....13
5 产品特性.....14
5.1 全面的日志采集能力.....14
5.2 可靠的安全保障能力.....14
5.3 专用的日志专家规则库.....15
5.4 灵活开放的查询条件.....15
5.5 高效的事件定位能力.....15
5.6 安全的旁路审计模式.....15
5.7 良好的扩展性设计.....16
5.8 丰富的合规性报表.....16
6 典型部署.....17
7 结论.....18

1 前言

随着政府、企事业各单位组织的信息化程度不断提高，对信息系统的依赖程度也随之增加，如何保障信息系统安全是所有单位都十分关注的一个问题。当前，大部分组织都已对信息安全系统进行了基本的安全防护，如实施防火墙、入侵检测系统、防病毒系统等。然而，信息系统维护过程中依然还面临着诸多的困难及风险，据研究指出，69%的攻击行为实际上都有日志留存，日志作为系统运行和网络访问时产生的重要事件记录，通过日志分析可检测系统运行是否异常以及及时发现网络中的可疑行为，但由于日志数量庞大、种类繁多、格式不统一、可读性差以及缺乏实时监控，导致日志难以管理和及时发现，缺乏日志实时分析使得信息化系统中存在着巨大的安全隐患，如：

- ✓ 系统运维风险：由于操作系统、硬件、应用程序等故障或配置错误导致系统异常运行，服务中断。这些异常行为往往会事先在系统及各类日志中有所反映，如果缺乏有效的日志审计手段，就无法及时发现这些安全隐患。
- ✓ 网络资源滥用：大部分企业对员工的上网行为都不进行直接控制，因此员工不适当或滥用公司网络资源的行为时有发生，如进行 BT 下载、观看在线电影、网上聊天以及访问非法网站的相关行为等等，这不仅是对公司管理制度的挑战，更使企业在国家相关法律法规的符合性上存在隐患，也容易造成企业资料泄密等后果。
- ✓ 应用及数据风险：企业中各类应用系统在对外服务的同时将面临各种用户访问行为造成的信息安全风险，包括用户非授权访问、管理员误操作、黑客恶意破坏等等，必须实行有效的安全审计手段。
- ✓ 安全事件定位风险：由于目前的应用系统往往都是相互关联的，一个故障现象，往往要对数台甚至数十台网络设备及主机的日志进行综合分析才能确定真正的故障原因，缺乏有效的统一安全事件审计平台可能导致无法及时进行故障定位甚至错误定位，此外，恶意破坏者获得系统权限后可以清理安全日志，从而导致无法正确定位安全日志。

此外，企业内部控制基本规范、SOX 法案、公安部 82 号令、等级保护等各类法律法规均对日志、行为审计有明确的要求，确保关键信息系统在可控、可审计状态下运行。

2 产品应用需求

2.1 日志审计管理需求

随着企业信息化建设的不断深入，各大类主机操作系统、网络设备、安全设备、以及业务应用系统都在不断的增长，各类设备与系统运行状态如何只能通过对其系统和网络中的产生的日志进行分析和检测得知，但系统产生的日志数量非常庞大，每天每个系统产生的日志量可能都数以百万计，且各类系统、设备及应用产生的日志都分散存储在自身的系统中，日志格式也均不统一，使日志检索、读取和管理非常的不便与繁琐，日志的产生也无法实时监控分析以及及时预警和发现，因此信息化系统中急需一个能够统一存储管理和实时监控分析的综合日志管理平台。

2.2 安全审计法规遵循

★ **计算机信息系统保护等级划分准则（GB17859）**

计算机信息系统分等级保护制度是我国信息安全行业的国家标准，为提高我国信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设健康发展，提供了技术指导和监管依据。信息系统安全等级保护基本要求中，对安全审计的技术要求包含但不仅限于以下内容：

网络安全审计

本项要求包括：

1、应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；

2、审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

3、应能够根据记录数据进行分析，并生成审计报表；

4、应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等；

主机安全审计

本项要求包括：

a) 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；

b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；

c) 审计记录应包括日期和时间、类型、主体标识、客体标识、事件的结果等；

d) 应能够根据记录数据进行分析，并生成审计报表；

e) 应保护审计进程，避免受到未预期的中断；

f) 应保护审计记录，避免受到未预期的删除、修改或覆盖等；

应用安全审计

本项要求包括：

a) 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；

b) 应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；

c) 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；

d) 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能；

★ 商业银行信息技术风险管理指引（金融行业法规）

第二十五条：

（三） 制定最高权限系统账户的审批、验证和监控流程，并确保最高权限用户的操作日志被记录和监察。

（五） 在系统日志中记录不成功的登录、重要系统文件的访问、对用户账户的修改等有关重要事项，手动或自动监控系统出现的任何异常事件，定期汇报监控情况。

第二十六条：

（七） 以书面或电子格式保存审计痕迹。

（八） 要求用户管理员监控和审查未成功的登录和用户账户的修改。

第二十七条：商业银行应制定相关策略和流程，管理所有生产系统的活动日志，以支持有效的审核、安全取证分析和预防欺诈。日志可以在软件的不同层次、不同的计算机和网络设备上完成，日志划分为两大类：

（一） 交易日志。交易日志由应用软件和数据库管理系统产生，内容包括用户登录尝试、数据修改、错误信息等。交易日志应按照国家会计准则要求予以保存。

（二） 系统日志。系统日志由操作系统、数据库管理系统、防火墙、入侵检测系统和路由器等生成，内容包括管理登录尝试、系统事件、网络事件、错误信息等。系统日志保存期限按系统的风险等级确定，但不能少于一年。

商业银行应保证交易日志和系统日志中包含足够的内容，以便完成有效的内部控制、解决系统故障和满足审计需要；应采取适当措施保证所有日志同步计时，并确保其完整性。在例外情况发生后应及时复查系统日志。交易日志或系统日志的复查频率和保存周期应由信息科技部门和有关业务部门共同决定，并报信息科技管理委员会批准。

★ **萨班斯（SOX）法案**

针对安然、世通等公司的财务欺诈事件破产暴露出来的公司和证券监管问题，美国立法机构出台了萨班斯-奥克斯利法案（Sarbanes-Oxley Act），在公司治理、会计职业监管、证券市场监管等方面作出了许多新的规定。其核心内容包括 302、404 条款，其对企业内控管理提出了严格甚至苛刻的要求，特别是对财务信息系统内控管理的有效性要进行安全评估和审计，我国在北美上市公司均要接受 SOX 法案的审计和评估。日志管理综合分析系统，能够大大降低企业 SOX 法案合规性审计成本。

2.3 信息安全审计目标

从信息安全风险管理角度来看，针对各类系统的运行日志和用户网络、数据库访问行为的审计系统是信息安全保障体系中不可或缺的一部分，信息安全审计系统的目标包括：

（1）有效整合现有信息安全产品，形成统一的安全事件管理平台；

（2）通过全面的日志及行为分析弥补现有各类技术产品在威胁分析发现方面的不足；

（3）通过信息安全审计系统的部署满足相关法律法规要求；

（4）为安全事故的责任追查、故障定位提供有力的技术手段。

3 产品介绍

3.1.1 产品概述

知道创宇日志管理综合分析系统(以下简称日志管理综合分析系统)是知道创宇公司自主研发的拥有自主知识产权的专业信息安全审计产品，系统通过监测及采集信息系统中的系统安全事件、用户访问行为、系统运行日志、系统运行状态等各类信息，经过规范化、过滤、归并和告警分析等处理后，以统一格式的日志形式进行集中存储和管理，结合丰富的日志统计汇总及综合分析功能，实现对信息系统整体安全状况的全面审计。

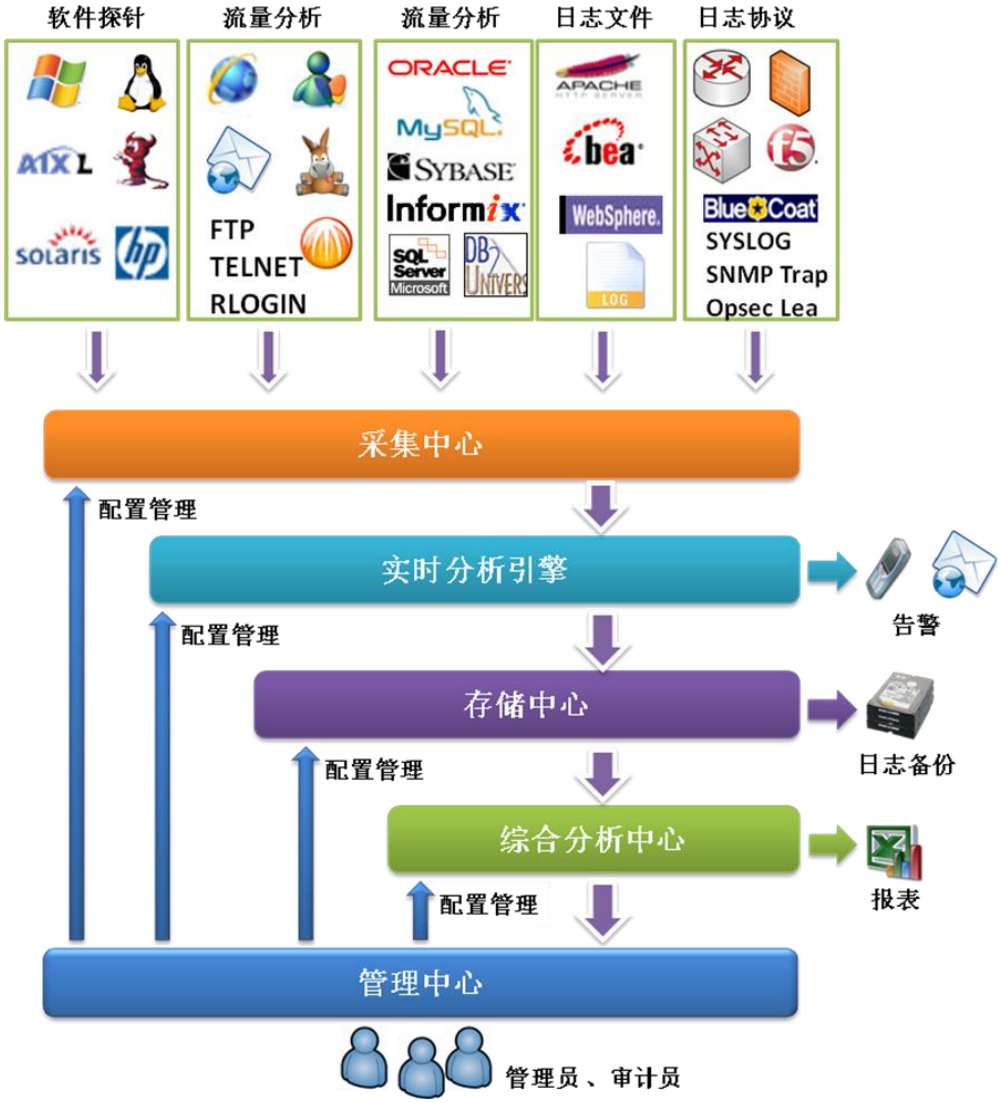
日志管理综合分析系统专注于对信息系统中各类主机、数据库、应用和设备的安全事件、用户行为、系统状态的实时采集、实时分析、异常报警、集中存储和事后分析，是支持分布式、跨平台的统一智能化日志管理及审计设备，可以对各类网络设备、安全设备、操作系统、WEB 服务、中间件、数据库和其它应用进行全面的安全审计。

日志管理综合分析系统可以帮助企业管理员随时了解整个 IT 系统的运行情况，通过实时的日志分析及时发现系统异常和非法访问行为；另一方面，通过事后分析和丰富的报表系统，管理员方便高效地对信息系统进行有针对性的安全审计。遇到特殊安全事件和系统故障，日志管理综合分析系统可以确保日志完整性和可用性，协助管理员进行故障快速定位，并提供客观依据进行追查和恢复。

因此，**日志管理综合分析系统**可以帮助用户有效降低 IT 系统的故障而带来的损失，降低 IT 系统的运维成本和管理的复杂度，显著提高系统整体的安全性、可靠性和运行效率，保证 IT 系统 7X24 的正常、持续、稳定运行，降低信息系统的整体安全风险。

3.2 体系结构

本产品基于嵌入式 64 位 Linux 系统，由日志采集模块、事件检索模块、审计报表模块、综合管理模块组成。日志管理综合分析系统采用 B/S 架构，管理员通过 HTTPS 方式对主机进行管理。日志管理综合分析系统的系统架构如图所示。



日志管理综合分析系统系统结构

4 功能介绍

知道创宇日志管理综合分析系统提供智能化的日志生命周期管理模型，集日志数据采集、实时动态分析、安全存储管理、历史事件检索、综合审计报告功能于一体，帮助用户快速、有效地完成信息系统安全审计工作。

4.1 日志数据采集

知道创宇日志管理综合分析系统通过多种对审计对象无干扰的日志采集方式，实现信息系统中几乎所有不同类型的日志数据的采集。

日志采集方式：

标准协议：采集 SYSLOG、SNMP_TRAP、OPSEC_LEA 协议类日志信息；

网络抓包：通过旁路侦听解析数据包，形成网络访问行为日志记录；

日志文件：通过专用脚本上传信息系统中存在的各类日志文本；

审计对象类型：

操作系统：Windows、LINUX、AIX、HP-UX、SCO UNIX、SOLARIS…

网络设备：交换机、路由器、负载均衡、代理设备…

安全设备：防火墙、IDS/IPS、UTM、防病毒墙、VPN…

应用系统：WEB Server、FTP Server、MAIL Server、WebLogic、Tomcat…

数据库操作：Oracle、DB2、MSSQL、SyBase、MySQL、Informix…

网络访问行为：网页浏览、BBS、文件传输、邮件收发、IM 聊天、BT…

日志管理综合分析系统将形式各异的各类日志数据采集并进行归一化处理后，形成日志管理综合分析系统专用日志格式，通过字段翻译转义，降低对审计员的技术要求，更方便于日志阅读及后续程序处理。

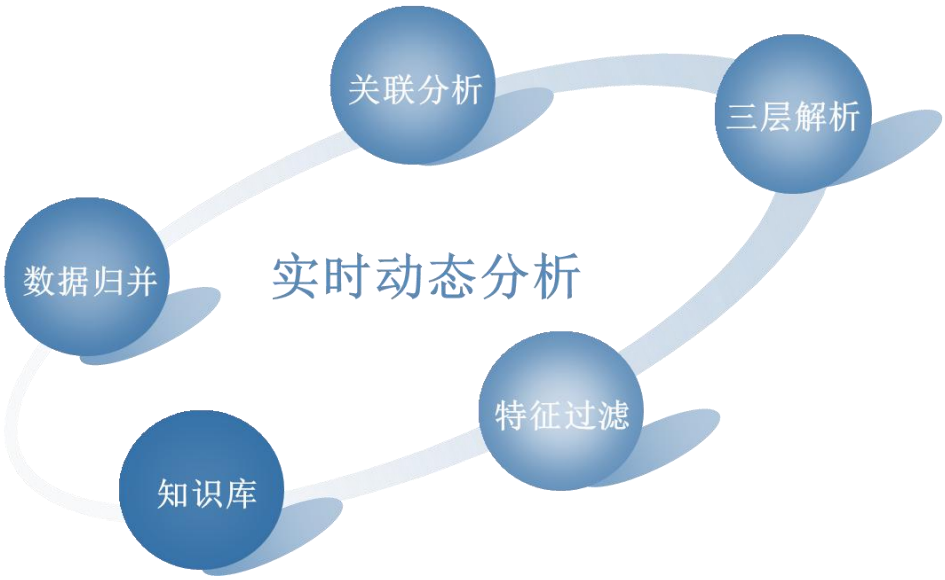
4.2 实时动态分析

知道创宇日志管理综合分析系统通过基于日志内容深度分析的日志专家规则库，对采集到的日志数据进行实时动态分析，将网络非法访问、数据违规操作、

系统进程异常、设备故障等高危安全事件，从海量日志数据中提取出来，并通过桌面屏幕、邮件、短信、SYSLOG、SNMP 等方式通知管理员及时处理。

知道创宇日志管理综合分析系统同时开放了灵活的规则定义条件，用户可以根据自己的需要，通过日志管理综合分析系统个性化的定制贴合自己实际应用环境的审计规则库，更细致地关注信息系统的安全事件，及时发现安全隐患。

知道创宇日志管理综合分析系统支持多层业务系统的访问数据源解析，通过同时抓取前端 Web 层（http/https）访问数据流及后端数据库操作，基于时间戳、会话标识等要素进行关联匹配，以确定符合数据库操作请求的 WEB 访问，通过三层审计更精确地定位事件发生前后所有层面的访问及操作请求。



4.3 安全存储管理

知道创宇日志管理综合分析系统采用专用的硬件平台和精简优化的操作系统，确保审计系统底层的安全。日志管理综合分析系统配置了系统防火墙、自带存储空间采用 Raid5 存储架构和专用日志存储系统确保日志数据存储的安全。系统进行了日志的防篡改、防删除设计，任何人都无法对原始日志数据进行改动。日志管理综合分析系统支持日志数据异地手备份和自动归档功能，并且归档文件通过加密方式存储，以保证日志数据的完整性、安全性和可用性。

4.4 历史事件检索

知道创宇日志管理综合分析系统支持基于内容关键字、源（目标）IP 地址、用户、时间、操作关键字等多重条件组合，对历史事件进行快速检索和精确定位。日志管理综合分析系统支持查询模板定制功能，方便用户多次对关注的事件使用模板检索。日志管理综合分析系统支持查询结果按协议分类呈现及导出功能，方便用户查看。

4.5 综合审计报告

知道创宇日志管理综合分析系统提供丰富的合规性报表模块（如 SOX 法案、等级保护），满足用户的日常审计需求。系统支持手动/自动报表功能，不但支持用户多条件组合生成报表，系统还支持自动生成：日、周、月、季度、年度综合报表，支持自定义常态报表模块定制，报表可以 MS EXCEL、HTML 等多格式导出，全方位、多角度对数据库系统、数据库服务器、相关网络设备安全性进行审计。

5 产品特性

5.1 全面的日志采集能力

完整全面的采集日志信息是日志审计的基础，日志管理综合分析系统基于对多种平台、常用协议及多类应用系统的深入分析，运用多种灵活的、安全的、可靠的采集手段，构建全网日志管理审计平台，包括主流的操作系统日志（Windows系统、HP-UX、AIX、Solaris、BSD、Linux）、上网行为记录（HTTP、FTP、TELNET、MSN、QQ、BT、SMTP/POP 等）、六大类各版本的主流数据库操作行为（DB2、Oracle、Mysql、MSSQL SERVER、Sybase、Informix）、网络设备及安全设备日志（支持 SYSLOG、SNMP_trap、Opsec_lea 协议）、应用系统日志（IIS、APACHE、SERV-U、Weblogic、Symantec 等所有文本型日志文件），真正实现全面的、统一的日志管理审计系统平台。

5.2 可靠的安全保障能力

- ✓ 系统底层采用嵌入式 64 位 Linux 系统，系统内核已进行全面精简、优化，从而在内核级别保障系统本身及日志的安全性；
- ✓ 采用自主研发的专有文件型数据库，避免了主流数据库本身带来的安全问题；
- ✓ 系统内置安全防火墙系统，可以设定严格的访问源，从而避免了绝大部分的无关流量，进一步保障系统本身的安全性；
- ✓ 系统对内部的管理帐号具有严格的细粒度的权限控制，能够有效防止内部管理员的越权访问，避免日志数据被越权访问、恶意删除。
- ✓ 系统内部存储为 SATA 硬盘 Raid5 阵列，即能保障日志信息在设备内的安全存储需求，又能保障高效的检索速度；

5.3 专用的日志专家规则库

日志管理综合分析系统自带基于日志内容分析的专家规则库，实时针对日志源数据进行等级划分，智能分析日志信息中所反映出的诸如设备故障、配置错误、系统警告、应用程序出错、传播违规违法信息、数据库敏感操作等信息，并能及时通过邮件或短信方式通知管理员。

5.4 灵活开放的查询条件

日志管理综合分析系统在接收日志信息时，根据不同的日志种类进行不同的格式化处理，在保留所有日志原始信息的同时将日志根据字段进行分割处理。用户在检索日志时，可以根据日志的类型，字段内容进行精细匹配，如：日志源 IP、日志生成时间、任意字段内容等；从而实现日志的快速准确定位；

日志管理综合分析系统支持不限次数的多重条件查询规则设定，支持的操作符有：>、<、=、不等于、包含、开闭区间等等常用逻辑运算符；支持跨日志查询，管理员能够通过设定规则条件，对日志进行精确定位匹配。

5.5 高效的事件定位能力

日志管理综合分析系统采用了知道创宇公司自主开发的基于海量日志索引的日志检索引擎，避免了在采用关系数据库在处理海量日志数据时的低效率问题，采用了“基于预测的动态索引技术”、“数据正交分组技术”及“适应磁盘的索引存储”“即时结果反馈技术”等核心技术手段，实现了对日志的高速检索能力。对日志管理综合分析系统缓存中的日志（最近入库的日志），日志管理综合分析系统对四重以内组合条件查询，能够在 5 秒内即返回完整的检索结果。

5.6 安全的旁路审计模式

- ✓ **日志管理综合分析系统**对数据库操作访问、上网行为等审计内容支持采用全旁路方式进行审计，不在网络中串联设备；不在主机上安装客户端软件；不改变客户原有的登陆方式。

- ✓ **日志管理综合分析系统**进行维护、升级时不会影响到正常业务的运行，也不会影响到网络性能。

5.7 良好的扩展性设计

- ✓ **日志管理综合分析系统支持在业务规模及审计管理范围扩大情况下的平滑升级，主要的系统可扩展及伸缩性能力主要表现在以下几个方面。**
  - 网络探测器的负载均衡

当单台网络探测器不能支持大流量的网络访问监听及分析时，可针对不同的访问源区域，进一步增加网络探测器来分担现有探测器压力。

- 日志采集及实时分析系统的负载均衡

当系统的审计范围扩大或安全事件发生频率的提高，造成系统需要实时接收和分析的日志量超出了系统可支持的日志吞吐量时，系统支持将日志采集及实时分析系统模块分离出来，进行多台负载均衡的部署，能够支撑更高并发日志量条件下的审计分析。

- 缓存日志存储及检索的负载均衡

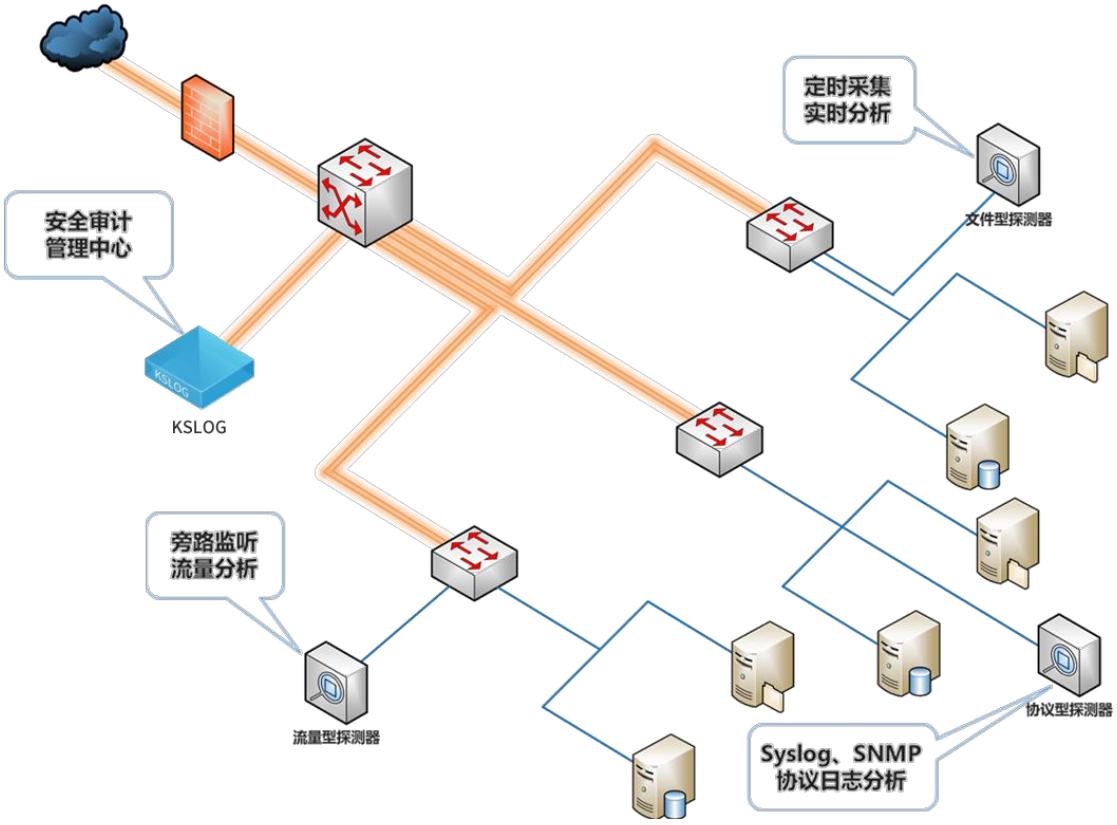
当用户缓存日志的日志保留天数及数量需要大幅度提高，造成审计人员进行日志检索及报表生成过程中的速度降低时，系统支持对多台缓存日志存储及检索模块的负载均衡。

5.8 丰富的合规性报表

日志管理综合分析系统审计报表均根据各行业审计需求、国家法律法规相关要求进行专门设计，如：

- ✓ 满足 82 号令审计需求，对特定上网行为进行日志记录并通过报表系统对异常行为进行集中审计；
- ✓ 根据 SOX 法案审计需求，对数据库操作、主机操作进行审计，并研发了大量满足 SOX 法案审计需求的报表。如用户登录/登出报表、特定操作统计报表、关键操作明细报表等等。

6 典型部署



日志管理综合分析系统部署示意图

7 结论

通过知道创宇日志管理综合分析系统的部署，可以协助用户有效掌握信息系统安全状态，预防敏感信息泄露，实现对信息系统安全事件的整体关联分析、评估、调查及安全事件的准确跟踪定位，为信息系统整体安全策略的制定提供权威可靠的依据。