



综合审计与责任分析系统关键技术与设计原理

周春楠

(亿阳安全技术有限公司 北京 100093)

摘 要:阐述了综合审计与责任分析系统的关键技术与设计原理,分析了网络行为审计、主机审计、数据库审计、堡垒主机审计、行为举证、责任分析相关技术,并介绍了系统特点、优势、网络部署拓扑结构,提高了信息系统业务和数据的安全性。

关键词:网络行为审计;主机审计;数据库审计;堡垒主机审计;责任分析

doi: 10.3969/j.issn.1000-0801.2013.11.026

Key Technology and Design Philosophy of the System of Global Audit and Duty Analysis

Zhou Chunnan

(BOCO Info-security Co., Ltd., Beijing 100093, China)

Abstract: The key technologies and design philosophy of the system of global audit and duty analysis system was stated in detail, and the related technologies such as network behavior audit, host audit, gateway audit, database audit, duty analysis, system characteristic, system advantage, system arrangement, were explained and the business and data safety of information system were improved.

Key words: network behavior audit, host audit, database audit, gateway audit, duty analysis

1 引言

随着行业、企业信息化建设的进一步深入,网络结构日趋完善,业务能力快速增强,业务数据越来越集中,随之而来的数据风险日益突出。如果政府、行业、事业单位、企业的关键业务数据被恶意篡改、破坏或重要机密数据外泄,都会造成不可估计的损失。

要保护这些数据,需要使用审计系统、身份和访问管理系统等应用安全产品,跟踪分析谁访问了数据库、操作了重要数据、复制了机密文件等。建设综合审计与责任分析系统,将获得全面的安全日志和事件场景回放,增强日志的管理、网络和信息系统的监控、安全事件的行为取证和责任分析,提高业务系统和重要数据的安全保障能力。

2 系统概述

综合审计与责任分析系统对网络设备、安全设备、主机、操作系统、应用系统、数据库操作等进行数据采集取证,为安全事件的追溯提供有效的证据,有效结合用户认证和访问授权模块,实现责任分析功能,构建可控的企业内部安全机制。该系统是集网络行为分析、日志分析、堡垒主机、数据关联分析、用户认证、用户行为取证、安全事件责任分析为一体的产品,系统以保护客户关键业务数据、财务数据、商业资料等机密信息为中心,满足了企业客户内部数据审计取证和监控的需求,通过网络数据流、主机日志、数据库、堡垒主机等多种途径采集取证、监控和记录企业工作人员操作这些重要数据的行为和后果,同时也记

录非授权人员企图操作这些重要数据的行为。根据这些行为的取证和分析,构建可控的企业内部数据安全,为完善企业内部相关安全制度提供强有力的保障。

综合审计与责任分析系统对局域网、广域网和互联网上的系统、应用和设备的日志进行实时采集、集中存储、实时分析、事后分析、异常报警,同时支持分布式、跨平台的统一智能化日志管理,可以对各类网络设备、安全设备、操作系统、Web 服务中间件、数据库和其他应用进行全面的日志管理,集合了网络行为审计、主机审计、数据库审计、堡垒主机审计等多种审计源,集中收集、分析信息系统中所有的日志,解决了“日志分布散、管理难”的问题。通过采用关联分析算法,解决了“日志查询难”的问题,使管理员把精力集中在最值得关心的日志上,时刻了解信息系统的运行状况,对事故进行快速响应。另外,由于采用了“实时收集,隔离备份”的机制,黑客无法完全删除入侵日志。遇到特殊安全事件和系统故障时,能确保日志完好和不被篡改,协助快速定位相关日志,并以此为依据进行事件回放、行为追溯、故障恢复和责任分析。

综合审计与责任分析系统是功能强大的智能化日志管理设备。一方面,可以随时了解整个信息系统的日志吞吐情况,在实时的日志分析中及时发现安全漏洞和非法访问行为,通过告警模块以声音、E-mail、手机短信息等方式及时通知管理员;另一方面,在事后分析和报表中提供多种运行分析报告,方便系统管理员从日志类型、特征、数量、内容中全面分析信息系统的运行状况,及时发现安全漏洞和非法访问行为,为系统今后的战略规划提供依据。

3 各审计系统比较及本系统优势

3.1 各审计系统比较

当前国际、国内信息安全领域中,审计系统大多为单独审计数据来源的产品,功能相对简单,没有行为举证、责任分析等功能,同时,审计系统、堡垒主机系统、身份认证和访问管理系统、责任分析系统等产品一般相互独立,没有实现这些产品和技术的融合。

现在国内外审计系统的主要技术和产品介绍如下。

(1) 抓取分组分析型网络审计产品

抓取分组分析型网络审计产品通过侦听并抓取信道中的 IP 数据分组,根据相关网络协议分析数据分组,从中发现网络中的违规行为和异常操作,记录存储,为各种 TCP 网络服务系统提供日志审计功能,对重要的网络服务

在 IP 层进行保护,可作为独立的产品单独部署。

根据产品的功能和部署位置,抓取分组分析型网络审计产品可分为上网行为管理与审计产品、基于网络行为的业务审计产品。前者部署在互联网出口处,多在交换机上旁路侦听,截获数据报文,进行采集、分析,审计内部用户访问互联网的内容和行踪,阻断在特定地点和时间不宜访问的互联网内容,预防或记录用户的违规和违法行为,防止内部信息泄漏,记录相关行为以供查询和举证。基于国情,国内这种基于抓取分组分析的上网行为管理与审计产品较多。

后者部署在核心业务安全域的交换机处,旁路侦听数据流,采集、解析数据分组,审计记录用户对主机、系统、应用、数据库的操作行为,保护网络中重要的业务系统,预防或记录用户的违规行为。

(2) 流量分析型网络审计产品

流量分析型网络审计产品通过收集网络设备的各种日志,借助异常流量分析技术分析网络中的流量,发现网络中的异常和违规行为。一般网管厂商根据网络设备日志管理,研发出流量分析型网络审计产品。

(3) 主机审计产品

主机审计产品对局域网、广域网上的网络设备、操作系统、应用系统、Web 服务器、中间件和其他应用等的日志进行采集、分析、集中存储、异常报警、事后查询。应用系统、操作系统等日志源对象,可以通过安装专用代理(agent)的方式采集日志。

(4) 数据库审计产品

数据库审计产品监控和记录所有对数据库的操作,保障信息系统核心数据得到规范存储、规范操作,对数据库异常操作或违规操作进行记录、追踪、报警,降低可能的安全风险,防范数据库信息泄露、非法修改等危险。一般支持对 Oracle、SQL Server、Sybase、IBM DB2 等多种关系型数据库的审计,能规避 SQL 注入、Oracle 目录遍历攻击、Oracle 拒绝服务攻击、SQL 缓冲区溢出攻击、SQL 函数漏洞攻击等破坏性风险。

审计分析:详细审计分析所有客户端对生产数据库访问的记录,包括客户端的 IP 地址、MAC 地址、计算机名、目的地址、客户端程序名、数据库名、表名、操作方式、操作内容、返回成功与否等。

数据采集过滤:可通过操作源 IP 地址、操作源 MAC 地址、计算机名、程序名、生产数据库名、生产数据库用户



名、操作内容、表名等设定过滤规则。

数据存储:可自定义审计数据保留天数,满足各相关法规对审计数据保留天数的要求;可自定义存储空间阈值,超过阈值则自动删除最老的历史数据,避免无磁盘空间可用,从而造成系统故障。

3.2 本系统的特点和优势

本系统融合了各种审计系统、身份和访问管理系统、责任举证和分析系统的功能,在国内产品中处于先进水平,其支撑系统已成功应用于中国移动通信集团公司的黑龙江、北京、湖北、贵州、山东、浙江、上海、陕西等 16 个省市分公司以及老挝电信、PICC、广安门医院等多个单位。本系统的技术特点和优势如下。

(1)实现了全面信息的采集,支持多种日志形式并存,综合实现了网络行为审计、主机日志审计、数据库审计、应用系统审计、堡垒主机审计。本系统由于融合了日志、网络分组、网络流量、数据库等多种审计源,相比其他单一的审计产品,综合审计与责任分析系统的覆盖范围更广,且具有更强的网络报文分析引擎,可以包容更多的网络协议。

如果仅是基于主机审计(HBA),只能通过采集日志获取人员行为,而由于主机日志来自各种复杂而庞大的设备,可能导致配置和管理成本过高,此时配合使用网络行为审计(NBA)就可以弥补。一般容易配置和管理的主机可以优先使用 HBA,其他设备和系统可以使用 NBA。

同理,如果仅是具有 NBA,就不能审计矢量图形协议(RDP 和 xWindow),此时就需要用主机审计弥补这个不足。所以说,主机审计和网络审计是相辅相成、相互补充的,也是本系统优势的体现。

(2)具有堡垒主机功能,实现对相关信息系统的保护。堡垒主机扮演着看门者的职责,所有对网络设备和服务器的请求都要从这扇“大门”经过。因此堡垒主机能够拦截非法访问和恶意攻击,阻断、过滤掉所有对目标设备的非法访问行为。

(3)实现综合审计、堡垒主机、身份管理、身份认证、访问授权等产品的融合,是集数据采集、协议解析、身份验证、集中取证、事件关联分析、访问权限控制各种技术于一体的新型产品,是应用安全产业的重要发展方向。本系统可实现实名制身份认证、综合审计、责任分析,能够将企业内部人员、厂商人员和其他业务相关人员的操作行为关联分析到具体人员。如使用身份令牌(token),当使用令牌的人员通过登录获取相应访问权限时,本系统就能够跟踪该

人员对生产数据的操作,能够为责任分析工作提供支持,追查事故等。

(4)采用专用硬件加速审计速度。

(5)底层采用通用接口,支持第三方安全软件,实现跨平台、跨区域的日志接入。

(6)采用标准的 XML 进行用户信息同企业各种资源的同步。

(7)广泛支持主流商业数据库,如 Oracle、Sybase、Informix、SQL Server、DB2、Taradata 主流版本,支持以上数据库的各种客户端和访问方式,包括 CLI、ODBC、JDBC 等;还支持常用非主流数据库,如 MySQL、PostgreSQL 等。

广泛支持 SQL 语句规范,还支持各个商业数据库自定义的 SQL 命令,支持的 SQL 命令分类如数据定义(DDL)、数据操作(DML)、数据控制(DCL)、数据检索和事务命令。

(8)具有丰富的审计自动报表,审计数据直接满足《萨班斯—奥克斯利法案》的相关规定和流程要求。

(9)支持各种应用系统,支持 B/S 结构和 C/S 结构并存。可以同时接入 C/S 系统、B/S 系统、各种网元、主机、网络设备和网络安全设备日志数据,进行综合审计、行为取证、监控管理。

4 综合审计与责任分析系统技术和设计

4.1 系统设计技术路线

针对安全产品的特点,本系统的技术路线是:

- 采用 J2EE 框架及技术;
- 采用面向对象的设计技术;
- 采用轻量目录服务协议技术,对其进行继承以及扩展;
- 采用跨系统的 Web Services 接口;
- 采用系统发展模式,贯彻全过程整体最优的技术路线;
- 基于分层、低耦合软件结构设计;
- 采用基于角色的访问控制(role-based policies access control, RBAC)模型。

4.2 系统结构

本产品基于多层、低耦合的系统设计,实现了数据标准化、数据聚合、数据关联、数据分析、实时报警、责任分析等功能,支持分布式、跨平台部署。系统自下而上分为 3 个层次,分别是采集层、数据层、应用层,如图 1 所示。

(1)采集层

负责集中收集各类日志,自动记录每一次操作的必要信息,准确记录何人、何时、何地进行了何种操作。通过网络监听方式采集用户操作行为,包括登录、应用程序操作、数据库操作、FTP、发送 E-mail 等;安全设备、网络设备的日志通过 Syslog 发送给审计系统;通过 FTP、Server LOG 等方式采集核心网、传输网、数据网等网元产生的日志;通过 SNMP、Syslog、HTTP 等数据网络协议采集常见的数据设备日志;应用系统、操作系统等其他日志源对象,可以通过安装专用代理的方式采集日志,并发送给审计系统。

(2)数据层

通过分布式运行环境对外提供协议解析、设备解析配置、临时缓存文件区、数据过滤、数据标准化、数据筛选、数据聚合、数据关联、告警配置、日志数据库等服务。日志数据的存储主要分为关系型和对象型数据库两种类型,适用于不同的应用场合,存储海量数据的事件数据库是关系型的,而策略数据库是对象型的,便于策略的分发与同步。各模块的具体功能介绍见表 1。

表 1 各模块的具体功能

模块	功能
协议解析	能够接收来自各种设备的数据,根据设备解析配置文件,自动对消息体进行数据拆分;可以形成模块化或者产品,针对不同的设备,只需要配置其设备解析配置文件即可
设备解析配置	XML 或其他形式的文件,主要用来存放不同设备日志体的解析方法
临时缓存文件区	日志信息的临时存放文件,主要用来解决因网络出现故障导致数据丢失的问题
数据过滤	从采集端对数据进行第一级过滤,过滤的规则来自服务器端的配置
数据标准化	数据的格式化处理引擎,不同的生产厂商、不同的设备类型之间的日志格式都不一样,故在此进行标准化处理,便于分析统计
数据筛选	发现关键操作和重要事件,产生告警信息
数据聚合	对相同类型的数据进行汇聚化处理,减少最终日志信息的重复显示
数据关联	根据人员身份、操作时间、主要的网元 ID 等信息,对不同地方收集的日志关联成一个整体,可以根据人员、时间、业务等类别信息进行检索
告警配置	位于服务器端,是数据筛选引擎的接口程序
日志数据库	用于存放关联后的日志信息

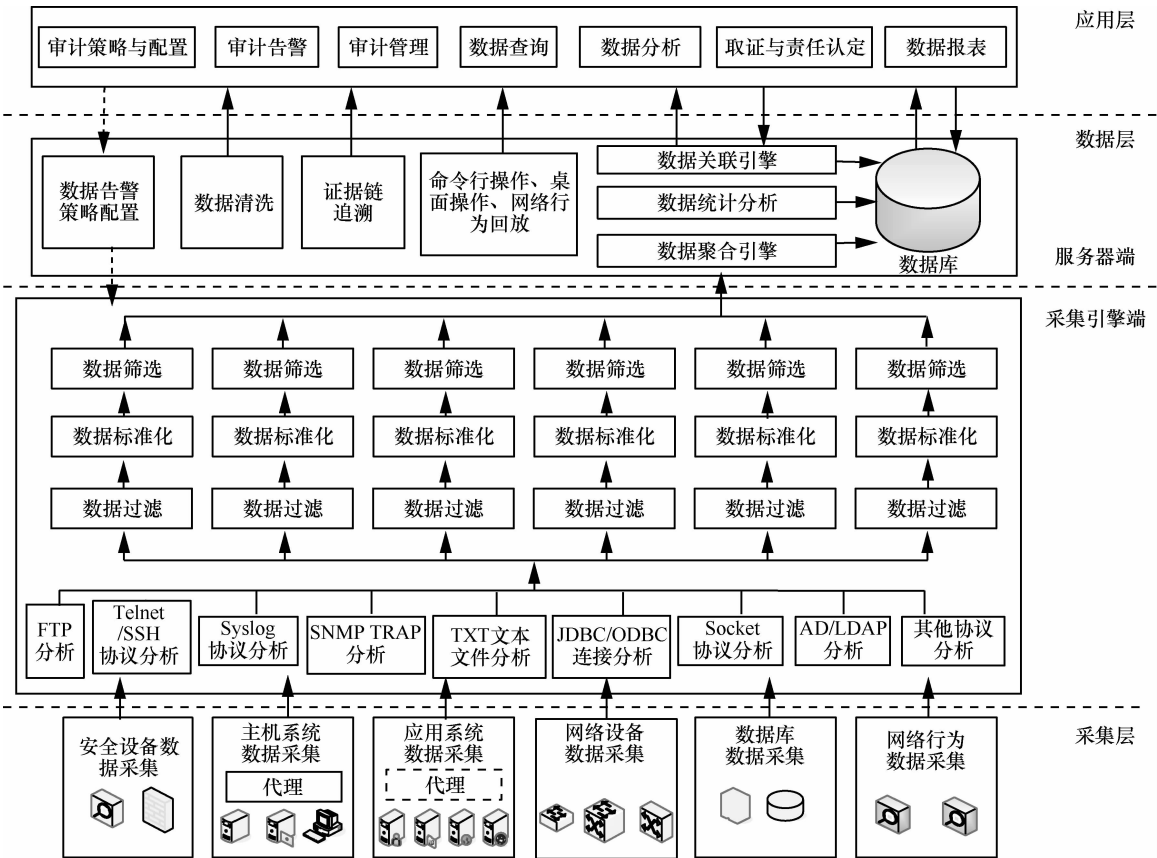


图 1 系统总体结构



(3)应用层

应用层直接面向管理员和系统用户,在这个层次,管理人员制定安全策略,查询关心的日志信息,监控安全态势,完成应急响应、取证和责任分析、报表输出。

4.3 系统功能

综合审计与责任分析系统根据用户的实际工作需要,提供了强大的功能,将繁琐的日志管理和分析工作变得简单。该产品的主要功能如图2所示,具体介绍如下。

- 网络审计:对网络数据进行协议还原和分析,支持 HTTP、POP3、SMTP、FTP、Telnet、Rlogin、RSH 等网络通信协议。
- 主机审计:对各种网络设备、安全设备、主机系统、应用系统的日志进行采集并进行标准化处理。
- 数据库审计:对主流数据库的操作进行取证。支持数据库打开审计选项方式审计和网络监听方式取证,以更好地贴近用户的需求。
- 堡垒主机:提供标准的 Telnet、SSH 和 FTP 文件传输代理服务;兼容各类 UNIX 平台和网络设备,支持各种标准的 Telnet、SSH、FTP 客户端,兼容大多数终端类型,如 Xterm、VT100、VT200、Ansi、Dec、Linux 等。
- 集中取证:通过对各种日志的采集进行日志的整理和保存,包括事件的定义、事件处理知识库等功能。
- 责任分析:综合事件关联模型、关联引擎、事件重放、责任举证。
- 分布式消息中间件:提供良好的分布式部署环境,支持异步消息通信机制、P2P 协议、SSL 加密技术及数据流压缩技术,以适应各种网络环境的需要。
- 网络拓扑图:显示审计系统服务器、采集引擎的在线情况。
- 系统状态图:审计系统服务器的性能实时监测,包括 CPU 使用情况、内存使用情况、网络负载情况、硬盘使用情况。
- 规则告警:对满足规则管理中所定义规则的日志进行呈现。
- 用户认证:用户认证系统,支持多种认证方式;也可以通过第三方 CA 或 4A 系统进行用户身份的识别、系统准入。
- 用户管理:进行基于角色的用户管理,通过身份的确认和规则的下发,对用户的权限进行严谨的控制。用户属性包括名称、角色、口令、联系方式(固定

电话、移动电话、E-mail)、用户描述信息;用户角色属性包括名称、权限、角色描述信息。

- 资源管理:对网络中被管理的全部设备进行分组分类,通过自身类型、使用日志对象类型、主要用途、重要性进行划分。
- 探测器管理:为收集满足条件的日志信息而对探测器进行包括名称、探测器 IP 地址、目的 IP 地址、目的端口、是否在线、发送方式(不发送、实时发送、周期发送)、发送周期、删除等的配置管理。
- 告警信息:配置短信、邮件等告警方式,以便在产生告警信息时及时通知管理员。

4.4 多种审计日志管理和查询

系统能采集、管理、查询多种审计日志,包括主机审计日志、网络审计日志、堡垒主机日志、数据库审计日志、系统日志和关键操作。管理员可以查询到各种日志信息。

- 主机审计日志:主机、网络设备、安全设备等通过 Syslog、SNMP 方式传送给审计系统的日志。根据起止时间、设备类型、场所、重要程度、自定义参数进行查询。
- 网络审计日志:网络行为日志。根据用户名称、IP 地址、操作命令、起止时间进行查询。
- 堡垒主机日志:堡垒主机命令行操作审计日志。
- 数据库日志:数据库访问操作日志,根据用户名称、IP 地址、操作命令、起止时间进行查询。
- 系统日志:对审计系统本身操作的日志。根据操作人员的用户名称、起止时间、日志重要程度(高、中、低3个等级)进行查询,也可以根据日志的描述信息进行模糊查询。

4.5 堡垒主机

堡垒主机是一种被加固的可以防御进攻的计算机,具备坚强的安全防护能力,用来实现用户访问控制、用户命令过滤(阻断)、生成命令日志、回放用户会话过程。

当用户登录网络设备和主机时,需要先登录访问堡垒主机,由堡垒主机进行认证登录,用户需通过堡垒主机登录网络设备,所有访问流量均经过堡垒主机,因此堡垒主机可以实现对访问内容的详细审计。在部署堡垒主机时,需配合网络的安全设置,使得对网络设备的访问只能经由堡垒主机跳转,从而确保审计的不可绕过性。

堡垒主机还具备图形终端审计功能,能够对多平台的多种终端操作进行审计,如 Windows 平台远程桌面(RDP)形式的图形终端操作。

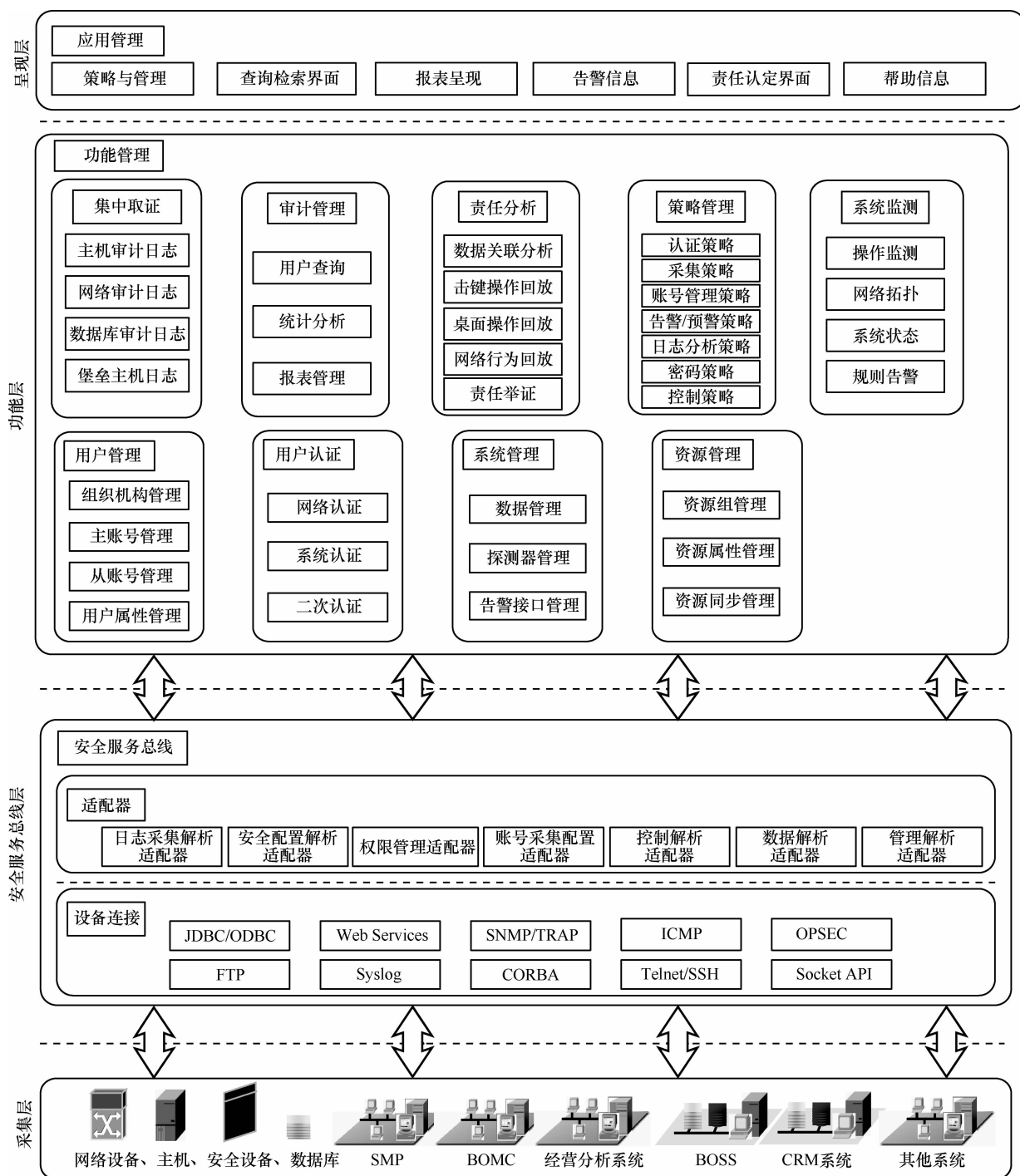


图 2 综合审计与责任分析系统功能架构

4.6 安全事件责任

当使用身份令牌或数字证书等的人员通过登录获取相应访问权限时,系统就能够跟踪该人员对生产数据的操作,能够为责任分析工作提供支持,通过审计记录、关联分析和事件分析等功能,认定安全事件的责任人。

通过关联分析用户身份管理中的主账号、IP 地址等,

实现用户实名审计跟踪。企业或事业单位用户通过堡垒主机的主账号制认证后,身份管理模块向网络审计服务器发送包含该用户主账号等信息的消息,网络审计服务器将消息中的主账号(可关联个人身份证等实名制信息)和审计服务器的原日志包中的用户名、IP 地址等信息进行关联,这样即使用户使用 root、administrator 等非实名制的账号登入

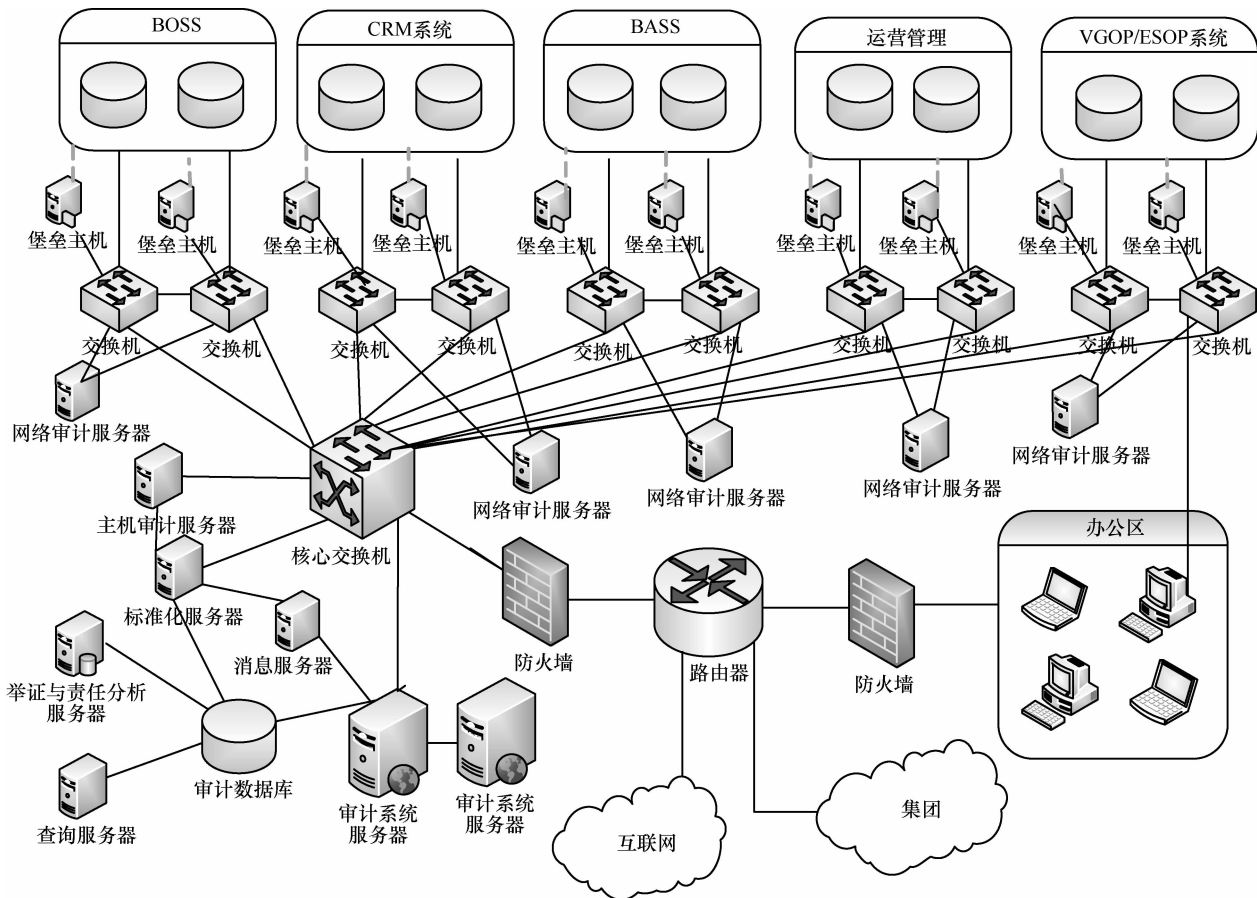


图3 综合审计与责任分析系统部署

应用系统,网络审计服务器也能关联分析出访问操作用户的实名,实现用户实名审计跟踪。

对越权访问、违反企业安全策略等行为进行采集取证,实现电子证据(数据电文)的存储和查询功能;实现了控制台按键操作信息的过程回放功能;在发布软件的支持下实现RDP操作的过程回放功能;实现了网络行为(Telnet,SSH等)的过程回放功能。最终通过与用户认证、授权系统模块的结合,实现从操作到自然人映射的责任分析功能。

5 系统网络部署

本系统的企业级网络部署如图3所示。

6 结束语

总之,综合审计与责任分析系统具有全面的安全日志采集、关联分析、查询举证、安全告警、事件场景回放、责任分析等功能。支持统一的身份管理、授权管理和访问控制策略下发,将安全事件的行为取证与用户关联起来,具有良好的证据收集和和责任分析功能,保护了关键业务数据、

财务数据、商业资料等机密信息,满足了企事业单位内部数据审计、员工操作审计和信息系统监控的需求,极大地提高了信息资产风险的防范能力,提高了信息系统业务和数据的安全性。

参考文献

- 1 ISO 10181-7:1996. 信息安全框架 信息技术开放系统互连开放系统安全框架第7部分:安全跟踪和告警框架, 1996
- 2 QB-Y-049-2013. 中国移动通信企业标准: 中国移动业务支撑网安全管理平台技术规范 V2.0.0. 中国移动集团公司, 2013

[作者简介]



周春楠,男,亿阳安全技术有限公司董事长,主要研究方向为电信网络管理和网络安全。

(收稿日期:2013-10-25)