绿盟数据库审计系统

产品白皮书

© 2022 绿盟科技

■ **版权声明**

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属**绿盟科技**所有，受到有关产权及版权法保护。任何个人、机构未经**绿盟科技**的书面授权许可，不得以任何方式复制或引用本文的任何片断。

目录

一. 产品简介 2

二. 产品优势 3

三. 绿盟数据库审计系统 4

3.1 系统架构 4

3.1.1 功能分层 4

3.1.2 功能结构 5

3.2 产品功能 7

3.2.1 数据库操作行为记录 7

3.2.2 数据库操作行为审计 7

3.2.3 数据库操作行为检索 9

3.2.4 操作行为的统计分析 10

3.2.5 数据库安全审计报表 11

3.2.6 审计数据库自动发现 11

3.2.7 用户权限细粒度管理 11

3.2.8 三层应用的关联审计 12

3.2.9 双栈协议数据可审计 12

3.2.10 系统自身监控和管理 12

3.3 典型部署 13

3.3.1 镜像旁路部署 14

3.3.2 分布式部署 14

3.3.3 软探针部署 14

插图索引

图 3.1 系统功能分层 5
图 3.2 镜像旁路部署 14
图 3.3 分布式部署 15
图 3.4 软探针部署 15

一. 产品简介

1.1 产品背景

数据库系统中关键信息资产的高度集中化，使得数据库成为内部违规人员、外部不法分子攻击和获取敏感信息的主要目标。

数据库安全事件频繁发生，与数据库管理面临的安全挑战密切相关。面临的安全挑战概括为：

- 管理职责定位不清、流程待完善、运维操作待规范，以及第三方维护人员操作缺乏有效监控等。致使安全事件发生时，无法追责到人。
- 数据库内部操作不明晰，无法通过传统安全产品（如：防火墙、IDS、IPS 等）来检测发现恶意操作、资源滥用和敏感信息泄露等违规行为。
- 依赖数据库系统日志的审计方法，存在：影响数据库系统性能、数据库日志容易被篡改，难以体现审计信息的真实性等弊端。

因此，多项立法和规范要求相继建立，如针对上市公司的 SOX 法案，规定公司和组织必须采取一定措施，对数据库进行安全审计；信息安全技术网络安全等级保护基本要求以及国家保密局 BMB17-2006 号文件中要求涉密敏感信息、业务系统相关的网络行为进行安全审计。

近年来，随着数据篡改、泄密等事件的频繁爆发，行业用户已经普遍意识到数据库访问疏于监管所带来的巨大危害，数据库审计与防护产品受到空前关注。随着技术发展和用户需求的推动，数据库审计产品除了单纯的数据库审计功能之外，也逐渐增加了弱点发现、智能分析、关联审计等功能。

1.2 产品简介

绿盟数据库审计系统（NSFOCUS DAS）是一款通过对数据库网络流量采集，基于数据库协议解析与还原技术的安全审计类产品。本系统对数据库所有访问行为进行监控和审计；对其中的危险操作进行多种方式告警；对数据库访问行为进行多维度统计并进行图形化展现。

本系统支持国内、外主流数据库、非关系性数据库以及数据仓库。在不影响数据库原有性能，无需应用、网络环境改造的前提下，提供可靠数据库安全审计服务。

本系统提供语句、会话、IP、数据库用户、业务用户、响应时间、影响行数等多种维度的数据库操作记录和事后分析能力，可作为发生安全事件后的溯源依据和证据来源。

除常规风险行为审计之外,还内置了数据库漏洞攻击行为与 SQL 注入攻击行为审计模型，可针对恶意入侵行为进行审计和告警。

在审计报表方面，系统除了提供各种合规性报表以外，还提供报表自定义能力。用户可以根据自身需求选择报表内容和形式，创建自己所需报表；除了在线报表以外，系统还提供周期性报表，包括：日报、月报、周报、自定义周期报表等形式；以及，基于系统性能、风险统计、会话分析、语句分析等的多维度统计报表，并支持定期报表推送。

二. 产品优势

2.1 全面记录数据库访问行为

系统支持 SQL 语句、参数、函数的全面审计。记录内容全面，包括：人员、时间、位置、动作、对象、工具、结果等七要素的全面审计。SQL 审计类型全覆盖，包含：DQL、DML、DDL、DCL、函数和数据库存储过程。兼容数据库类型不仅支持市场主流关系型数据库，还支持非关系型以及国产化数据库。同时完美支持 IPv4、IPv6 双栈网络协议数据流量的审计以及混合审计。

2.2 审计数据处理迅速

NSFOCUS DAS 采用多通道处理，流量智能平衡技术，实时快速处理数据库访问流量。多线程、多链接并发入库，效率提升 2-3 倍。同时采用大数据计算和存储架构以及数据热交换技术，大大提高了实时数据处理效率，使得数据检索不仅范围更广，更能实现全库检索的秒级响应。

2.3 审计数据不丢失，不泄露

系统具备流量超限保护机制，当瞬时流量超过负载，自动开启自保护机制。确保自身稳定运行，防止历史审计数据受到大流量冲击引起的丢失。同时支持 SQL 返回结果集关键信息脱敏，遮蔽敏感数据，防止审计数据二次泄密。

2.4 应用用户准确关联

系统利用 WEB 插件关联技术，将应用层和数据库层的访问操作请求关联，可以追溯到应用层的最初访问数据及请求信息，直接定位到业务终端用户。

2.5 部署灵活

系统采用分层模块化设计，具备极强的伸缩性。支持：镜像旁路部署，AGNET 引流部署、虚拟化部署、分布式部署集中化管理、以及混合部署方式。有效应对复杂的网络环境，解决部署问题。

三. 绿盟数据库审计系统

3.1 系统架构

3.1.1 功能分层

系统按照不同的逻辑功能划分为以下四层功能实体，包括：数据采集引擎、实时审计分析引擎、数据存储中心和日志综合分析中心，其中：

- ✓ **数据采集引擎**：负责数据库流量的采集、数据库私有通信协议的解析、SQL 语法分析和其它预处理；

- ✓ **实时审计分析引擎**：按照系统下发的审计策略，处理数据库操作记录数据，输出风险等级及告警标志；

- ✓ **数据存储中心**：负责数据库审计日志与系统自身日志的存储与管理；

- ✓ **日志综合分析平台**：实现对数据库操作历史记录的离线处理，包括历史记录的检索，统计、综合分析及价值挖掘等。

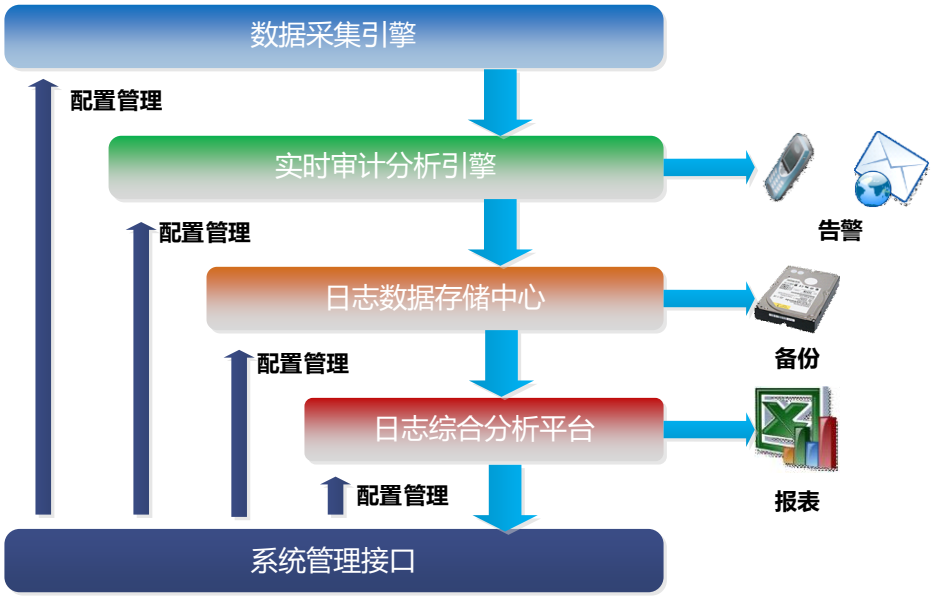
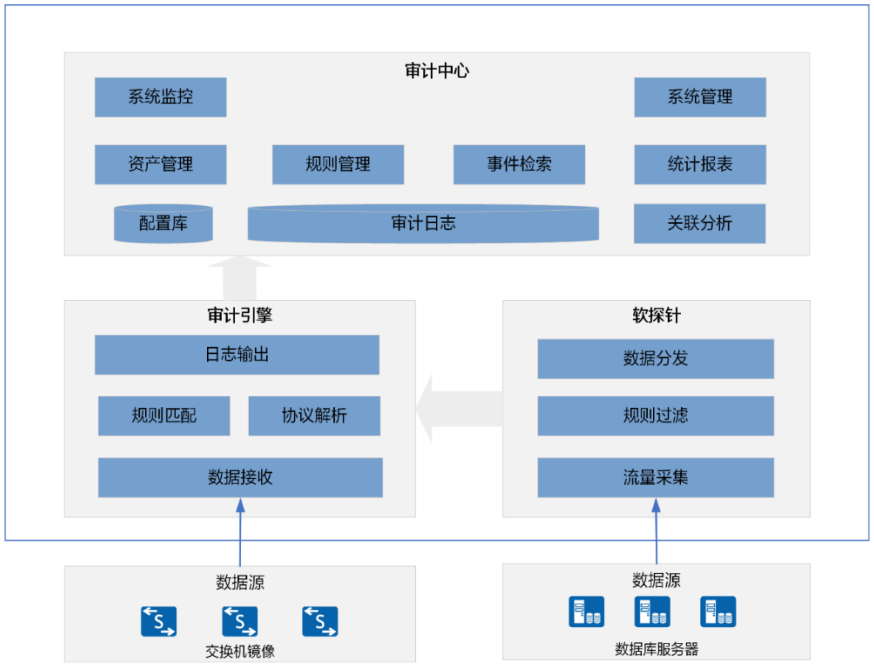


图 3.1 系统功能分层

3.1.2 功能结构

绿盟数据库审计系统采用多平面软件架构设计，包含：日志采集、数据解析、业务管理等，如下图示：



- **数据源**

数据库审计系统的数据源为数据库网络流量，可从两个途径获取：一是通过交换机旁路镜像功能将数据库流量从镜像口输出，进入数据库审计系统；另一个是在数据库服务器上安装软探针，采集数据库网络流量，再将流量发送给数据库审计引擎。

- **软探针**

软探针部署于数据库服务器，用于采集数据库流量，按照一定规则进行数据过滤后，通过网络将数据库流量数据发送给数据库审计引擎。

- **审计引擎**

接收来自于交换机镜像或者软探针采集来的流量数据，进行网络协议、数据库协议解析后，还原数据库操作语句。再根据审计规则进行实时比对审计，生成具有风险标识的审计记录。

- **审计中心**

审计中心包含：资产管理、规则管理、关联分析、系统监控、系统管理、事件检索、统计报表等功能模块。审计中心接收审计引擎的审计日志，存储于数据库集群中，用于后续检索统计。同时，关联分析模块抽取审计日志数据，进行离线数据挖掘和加工，形成智能分析结果，满足客户数据分析需求。

3.2 产品功能

3.2.1 数据库操作行为记录

系统支持多种国内外主流数据库以及大数据类型，采用旁路镜像或者软探针方式采集数据，经过通信协议解析和 SQL 语法分析，获取数据库会话和操作行为相关信息，形成记录并保存。系统详细记录每次操作的发生时间、数据库类型、源 MAC 地址、目的 MAC 地址、源端口、目标端口、数据库名、用户名、客户端 IP、服务器端 IP、操作指令、操作返回状态值。系统支持记录的行为包括：

- ✓ DDL 数据定义类
- ✓ DML 数据操作类
- ✓ DCL 数据控制类
- ✓ TCL 事务操作类
- ✓ OTH 其它辅助类

3.2.2 数据库操作行为审计

本系统对数据库操作行为进行全面的审计，包含：操作风险审计与会话事件审计。在此基础上实现多维的访问分析、语句分析和会话分析进行问题追踪。通过对数据库审计策略的制定，建立数据库操作的风险特征与审计行为的映射规则。审计引擎根据制定的审计规则对捕获的 SQL 语句进行专业的 SQL 语法分析，并根据 SQL 行为特征和关键特征，实现高效精准的审计分析。

3.2.2.1 审计策略建立

审计策略支持：黑白名单、模板语句、风险操作、SQL 注入检测和数据库漏洞检测等几个维度的策略设置。

- ✓ **黑白名单**

  针对特定账号、访问工具、访问方式等进行黑白名单设置，实现针对数据库行为的审计告警或信任放行；

- ✓ **模板语句**

  系统对数据库操作语句进行分类归纳形成语句模板，用户可以将语句模板设置为：敏感语句或信任语句，有效提升审计效率；

- ✓ **风险操作**

  系统预置风险操作判断规则，用户可启用、停用、编辑和调整优先级；也可以通过选择风险操作特征进行组合新建风险操作规则。

- ✓ **SQL 注入检测**

  系统预置数据库 SQL 注入审计规则，用户可启用、停用和调整优先级。也可以通过选择 SQL 注入特征进行组合新建自己的 SQL 注入规则。

- ✓ **漏洞攻击检测**

  系统基于 CVE 数据库安全漏洞，进行漏洞攻击行为研究，预置漏洞攻击检测规则库，用户可启用、停用和调整风险优先级。

3.2.2.2 审计动作定义

系统支持风险行为等级标记，等级共分为：高风险、中风险、低风险以及可信任四类。可对异常行为及时告警响应，明确风险级别。告警可通过邮件、短信、syslog、SNMP、企微、钉钉等方式通知管理员，确保第一时间发现违规行为。

3.2.3 数据库操作行为检索

检索历史操作日志时，系统可通过多种条件相结合方式进行日志查询。根据日志的类型、发生时间、字段内容等进行精细匹配（如：源 IP、发生时间、数据库操作信息字段等），快速准确定位风险事件。

3.2.3.1 风险检索

通过列表清单方式，逐条展现风险语句详情。按照：SQL 语句、操作时间、风险类别、风险名称、风险等级、数据库用户、客户端 IP 等维度展现风险语句的详细信息。风险检索提供包括：风险类别、风险级别、数据库用户、客户端 IP、工具与应用、OS 用户、会话以及高级查询等检索条件，满足风险精准定位的要求。

3.2.3.2 语句检索

针对数据库操作记录进行在线查询检索，检索维度包括：SQL 语句、捕获时间、数据库用户、客户端 IP、执行结果、影响行数等。同时，语句检索结果支持信息下钻以及关联会话。

3.2.3.3 会话检索

系统支持会话记录检索，查询条件包括：数据库用户、客户端 IP、MAC 地址、应用工具、以及 OS 用户等。同时，查询结果可进行 SQL 关联语句下钻，进一步查看会话详情。

3.2.3.4 告警检索

系统支持实时告警，可对告警事件进行归档。还支持检索历史告警信息，以及告警信息下钻。

3.2.4 操作行为的统计分析

3.2.4.1 多维度统计与分析

系统对全局或单一审计对象，均提供多维度的审计记录功能。分别从：风险、语句、会话和访问来源等多个层面进行统计与分析，帮助用户准确掌握数据库安全态势，快速锁定风险目标。

✓ **风险类型分析**

系统可向受保护数据库提供各种风险类型统计和详细信息查询，提供：敏感语句、SQL 注入、漏洞攻击、风险操作等维度的风险统计展现。

✓ **语句类型分析**

系统可对数据库访问 SQL 语句进行分类统计和分析。分析方式包括：SQL 统计、语句检索、模板检索、失败 SQL 分析、TOP SQL 语句分析等。

✓ **会话分析**

系统可对数据库所有会话行为进行分类统计、分析和追踪，主要包括：会话统计、会话检索、失败登录、活跃会话、应用会话等。

✓ **访问源分析**

系统可对全局或单一审计对象，针对风险行为进行操作人员的快速定位和风险溯源。

3.2.4.2 可视化展现与钻取

系统通过仪表盘、柱状图、折线图、饼图、直方图等多种图表形式，直观剖析和展示数据库运行状态。提供整体可视化展示，展示内容包括：审计总时长、审计语句总量、风险语句总量、风险语句类型分布、审计语句数量趋势、风险语句数量变化趋势、SQL 语句类型分布、审计语句事件实时告警状态等；

且支持数据库统计下钻与分析，进一步查看详细的数据库操作行为。对分析数据库风险操作提供了有力支撑。

3.2.5 数据库安全审计报表

系统内置丰富的报表模板，报表符合 SOX 法案、等级保护等相关对数据库安全审计的内容要求。另外也可以根据实际需求要求，自定义报表内容。

审计报表支持：在线报表、周期性报表两种。或手动或自动生产报表内容，并提供邮件报表推送和在线页面下载。报表格式，支持：PDF、PDF、HTML 三种类型；周期性报表有：日、周、月报三种时间粒度可选。

审计报表内容，包括：系统概况、数据库总体访问情况、数据库性能状态、数据库会话分布、数据库语句类型分布、数据库操作风险分布状况等；

3.2.6 审计数据库自动发现

系统通过对数据库流量采集和数据解析，利用各数据库类型的协议特征，实现对不同类型数据库的自动识别。同时，还可从协议内容种获取到更为精确的数据库参数，比如：数据库版本号、协议版本号、通信端口等。数据库自动发现信息，经用户手工确认并完善后，即可将被发现的数据库加入到审计对象中。

数据库自动发现功能大大降低了产品部署成本，增强了系统易用性，做到了真正意义上的免实施操作。

3.2.7 用户权限细粒度管理

系统采用具备权限控制机制，用户只能使用已分配管理员权限的账号，进行指定页面登录与隔离操作。完全满足三权分立的合规性要求。

本系统默认内置三个管理员角色，分别是：

- ✓ **系统管理员**:具备数据库审计操作的权限；
- ✓ **配置管理员**：具备系统配置和管理权限；
- ✓ **审计管理员**：具备对系统操作进行审计的权限。

3.2.8 三层应用的关联审计

本系统利用 Web 插件技术，关联业务客户端 IP、业务用户与数据库操作记录，回填相关信息，可以准确定位到应用用户和应用 IP。从实际监控价值出发，可以将应用 IP 和用户纳入审计策略，制定风险规则。满足了数据库审计监控的全面性需求。

系统支持的应用类型包含了现有主流的应用架构，如：Tomcat、WebSphere 和 WebLogic 等。

3.2.9 双栈协议数据可审计

系统具备同时支持 IPv4、IPv6 协议的数据库网络流量的接入、解析和审计，并在系统界面上统一展现。兼容 IPv4 和 IPv6 以及混合网络环境中，可根据客户实际的网络环境进行自由配置；

3.2.10 系统自身监控和管理

3.2.10.1 系统监控告警功能

系统除实现对数据库的监控与审计，对自身系统的运行状态也进行实时监控。监控内容包括主要：系统硬件资源、数据库流量、软件模块健康状态等。其中：

- ✓ **系统硬件资源监控**：监控系统 CPU、内存、硬盘使用情况，对磁盘使用情况进行告警提醒。

- ✓ **数据库流量监控：**监控数据库采集端，实时流量与变化趋势。对流量变化提前做出预警，对流量超限进行告警。

- ✓ **软件模块健康状态：**监控系统各主要软件模块的运行状态，对异常进行告警和自动恢复。

3.2.10.2 系统维护配置管理

- ✓ **时间同步管理**

  提供手工同步、NTP 同步、浏览器同步三种时间同步方式。通过对全系统自身的时间同步，保证审计数据时间戳的精确性。避免了对审计溯源带来的影响，提升了审计准确性和效率。

- ✓ **审计日志管理**

  系统支持对审计日志进行维护，以保证系统稳定运行。可对系统日志进行定时、手工备份或删除，保证系统日志完整性和有效性，防止因系统日志量过大引起的系统瘫痪。

- ✓ **系统升级管理**

  系统提供系统软件以及漏洞规则库升级功能。供给用户独立的升级包程序，由用户可自行升级。

3.3 典型部署

系统采用分层模块化架构设计（主要模块包括：数据采集、协议解码、审计引擎和审计中心），在业务功能逻辑上相互独立。因采用松耦合接口方式进行数据交互，所以系统部署可更加灵活，可适应各种网络环境。

系统典型的部署模式包括：镜像旁路部署、分布式部署和软探针部署，具体描述如下：

3.3.1 镜像旁路部署

镜像旁路部署是最为常见的部署模式，适用于绝大多数用户应用场景。通过用户交换机镜像方式，达到数据采集和审计记录的部署要求。

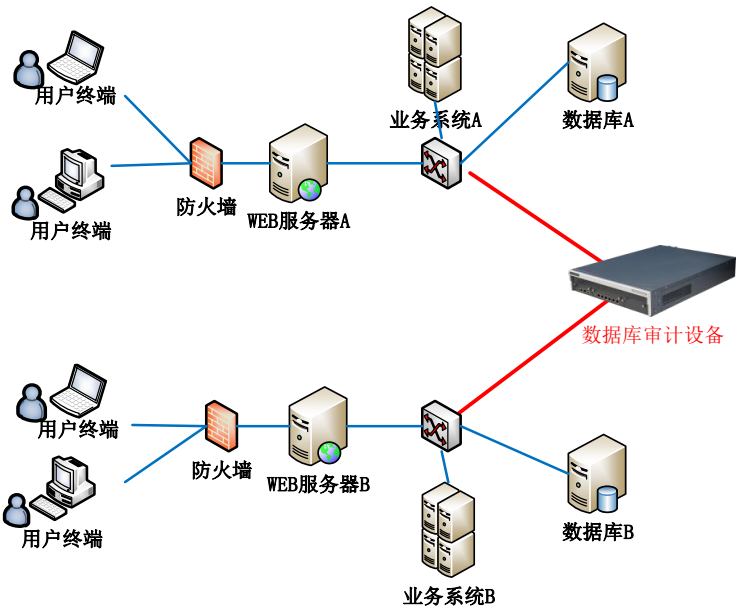


图 3.2 镜像旁路部署

3.3.2 软探针部署

软探针部署模式是系统提供独立的支持数据采集的 AGENT 软件，部署于数据库或业务系统所在操作系统中，监听并回传数据流量，达到主动引流和审计的要求。此种部署方式，适用于虚拟化、云以及无法通过交换机镜像流量的网络环境。

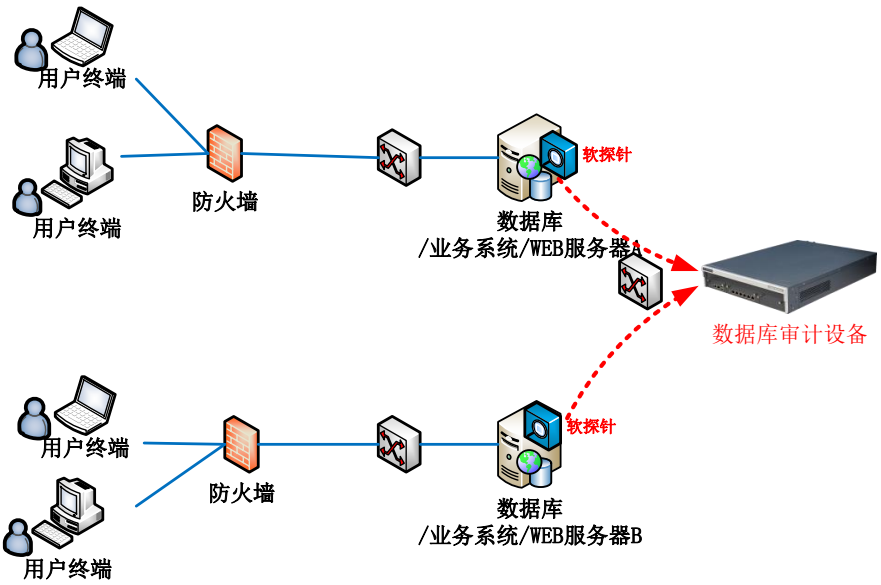


图 3.3 软探针部署

3.3.3 分布式部署

分布式部署将审计引擎与审计中心进行分离。审计中心负责日志分析与存储，审计引擎作为独立探针负责数据的采集、解析。一个审计中心可管理多个审计探针，适用于大型集团式分级业务的部署要求，

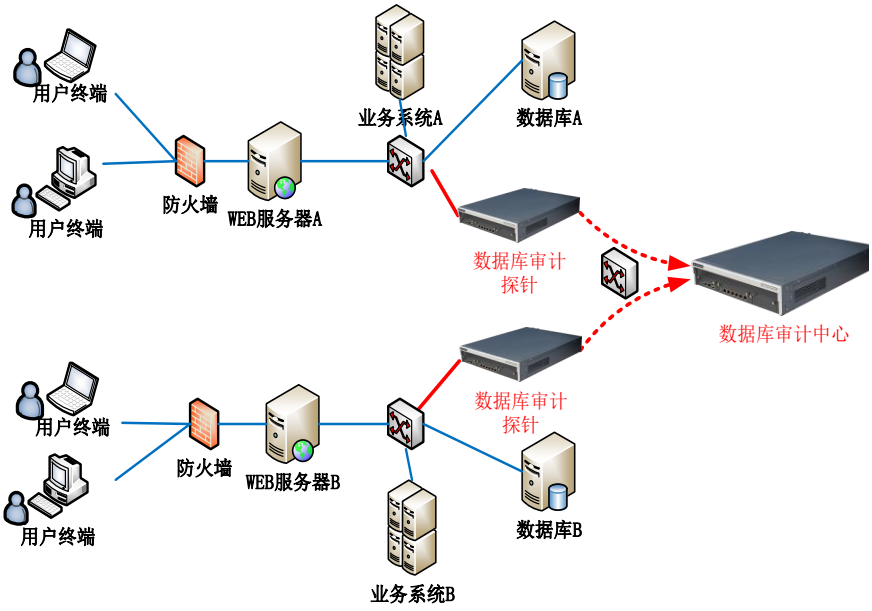


图 3.4 分布式部署