绿盟数据库审计系统

产品白皮书

目录

插图索引

一. 产品简介

1.1 产品背景

数据库作为企业核心的信息资产，在黑客攻击日趋商业化的今天，获取以及篡改数据库内容往往能够给攻击者带来巨大的商业利益，而企业内部的管理人员对数据库的误操作以及蓄意的破坏也会给企业带来巨大的损失。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来确保关键数据库的安全性，对数据库进行安全审计；公安部国家电子政务等级保护、国家保密局 BMB17-2006 号文件中要求政府、涉密单位必须对与涉密敏感信息、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的采集，基于数据库协议解析与还原技术的数据库安全审计系统。本系统实现对数据库所有访问行为的监控和审计、对其中的危险操作进行多种方式的告警、对数据库访问行为进行多维度的统计并进行图形化展现。

本系统支持国内外主流数据库产品，包括 Oracle、SQL Server、DB2、Sybase、MySQL、Informix、PostgreSQL、HBase、MongoDB、达梦等国内外主流数据库产品。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最为可靠的追查依据和数据来源。

除了常规的风险行为审计功能之外，系统还内置数据库漏洞攻击行为和 SQL 注入攻击行为模型，通过产品专项的安全审计策略，可针对应用端的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格式报表以外，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，基于系统性能、风险统计、会话分析、语句分析等多个维度提供统计性报表进行分析，并支持定期推送功能。

二. 产品优势

2.1 业务系统无感审计（稳）

系统主要采用旁路镜像方式部署，将客户数据库的网络流量单向引出，能做到对客户业务网络零影响，对客户业务系统无感知，从而保证客户原有业务系统的稳定运行。

2.2 终端用户审计能力（准）

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，可直接定位到业务终端用户。

2.3 大数据架构和设计（快）

系统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，能实现全库检索，而且查询效率更高，对于客户常用的查询和检索场景，均能实现秒级响应。

2.4 数据类型全面审计（全）

系统支持数据库类型丰富全面。不仅支持市场主流关系型数据库，包括 Oracle、SQL Server、Sybase、DB2、MySQL、PostgreSQL、Informix 等，还支持国产数据库，包括达梦和人大金仓等，以及大数据（如 HBase 和 MongoDB 等）审计。

系统支持 SQL 语句、参数、函数全面审计。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。

系统支持网络协议完整。能完美支持 IPv4、IPv6 双栈网络协议数据流量的混合审计。

2.5 机器智能模型学习（智）

系统具备在目标网络中的数据库自动发现能力，并且支持自动对象参数配置，同时系统具备特定数据库的数据访问模型学习能力，可自动归纳学习数据库访问模型。

2.6 审计部署方式灵活（灵）

系统采用大数架构及分层模块化设计，具备极强的伸缩性，既支持硬件一体机方式，也可完美支持分布式部署，同时还支持纯虚拟化环境部署。

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，包括数据采集及协议解析、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：

- ✓ **数据采集及协议解析**：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**：按照系统下发配置的实时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**：负责的存储；
- ✓ **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。

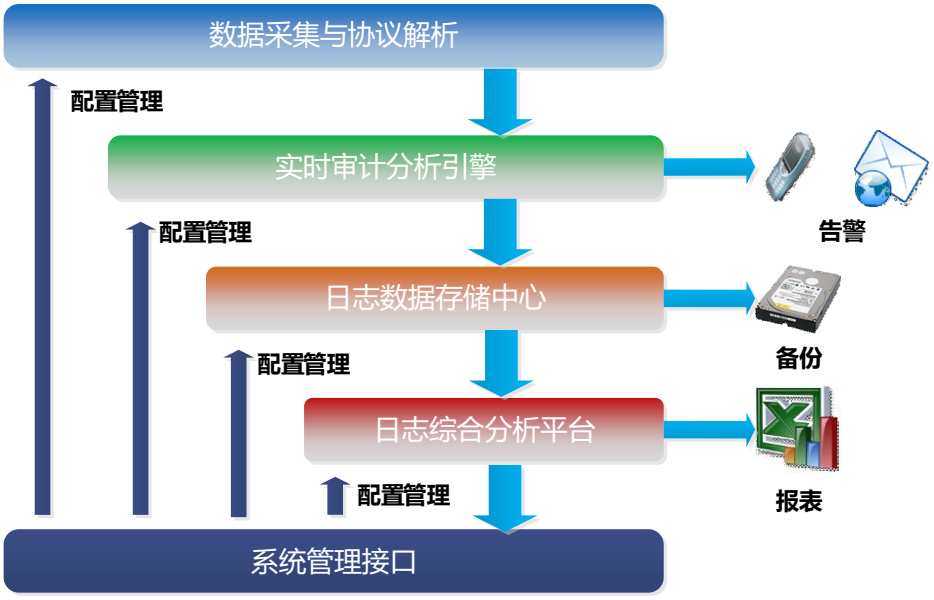

图 3.1 系统功能分层

3.1.2 功能结构

系统从功能结构上划分主要由以下几个模块组成：控制模块、审计模块、管理模块、存储模块、用户管理接口模块，各模块间关系如下图所示：

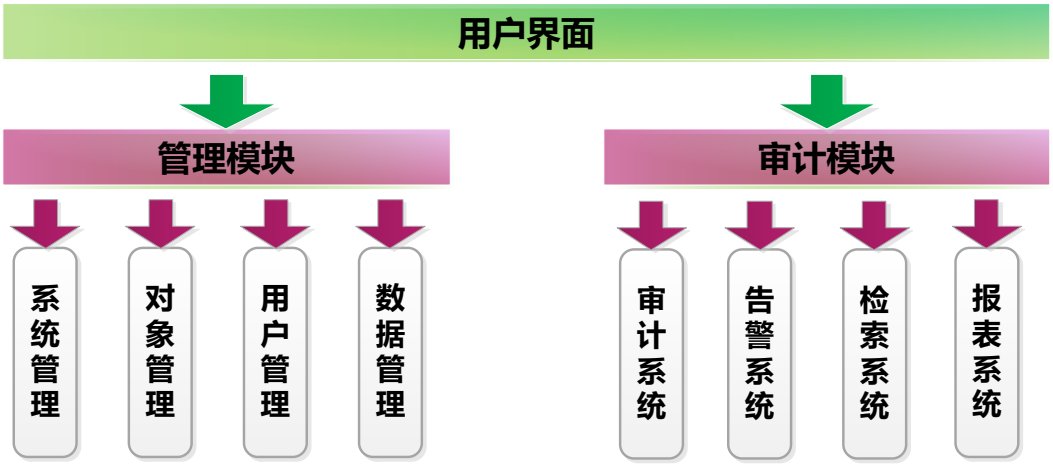

图 3.2 系统功能结构

管理模块

实现数据库审计对象管理、用户权限管理、系统运行参数配置管理，以及海量审计日志记录的存储管理，是系统业务功能实现的基础保障；

审计模块

实现数据库操作安全审计的业务功能，包括实时的数据库操作审计引擎、危险操作的告警系统、历史记录的离线检索、统计和分析系统以及在线、离线的报表系统等；

用户界面

用户界面是系统操作人员与数据库审计系统的人机接口，向用户提供界面友好的图形化结果展示，并提供系统配置管理和操作接口；另外，系统也预留第三方数据接口，实现用户数据的批量导入和审计系统的统计数据共享输出。

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，保存信息日志。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（如 create、drop、alter 等
- ✓ DML 数据操作类（如 select、insert、delete、update 等）
- ✓ DCL 数据控制类（如 grant 授权、revoke 取消授权等）
- ✓ TCL 事务操作类(如 Begin Transaction、Commit Transaction、Rollback Transaction 等）
- ✓ OTH 其它辅助类（视图、索引、过程等操作） 等数据库访问行为。

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，包含操作风险审计和会话事件审计。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，实现高效而精准的审计分析。

3.2.2.1 审计策略建立

审计策略支持审计黑白名单、模板语句、风险操作、SQL 注入和数据库漏洞等几个维度进行设置，其中：

✓ **审计黑白名单**

黑名单等同于禁止规则，针对特定的用户、访问终端、访问方式进行设置；

白名单等同于信任规则，针对指定的语句、操作设置放行忽略风险审计操作。

✓ **模板语句规则**

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成敏感语句或者信任语句规则，其中：

敏感语句：从安全性及执行性能等方面归纳出 SQL 常见的敏感语句；

信任语句：正常数据库访问语句设置为信任语句，可有效提升审计效率。

✓ **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；另外，用户也可以通过选择风险操作特征进行组合新建自己的风险操作规则。

✓ **SQL 注入检测**

系统预置数据库 SQL 注入判断规则，用户可启用、停用和调整优先级。另外，用户也可以通过选择 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 上公开了 2000 多个数据库安全漏洞，进行漏洞攻击行为研究，预置漏洞攻击检测判断规则库，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

系统可通过规则设置对各类数据库操作访问行为进行实时监测，对操作行为按照审计规则打上风险等级标签，其中风险等级标签分为：免审计、高风险、中风险、低风险四类。对网络中的异常数据库操作行为及时进行告警响应，实时显示告警信息并记录存储。告警信息可通过邮件或短信方式在通知管理员，以确保管理员在第一时间发现用户对数据库的违规操作。

3.2.3 数据库操作行为检索

用户在检索数据库历史操作日志记录时，系统可以通过多条件相结合的方式进行日志查询，根据日志的类型、发生时间、不同字段内容等进行精细匹配，如：日志源 IP、日志发生时间、数据库操作信息字段内容等，从而实现日志的快速准确定位。

3.2.3.1 风险检索

风险检索通过列表清单的方式逐条展现每条风险语句详情。通过具体的 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、展现风险语句的详细信息。查询条件包括：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、会话等。

3.2.3.2 语句检索

针对数据库操作记录进行在线查询，查询条件可自定义任意字段的组合查询。SQL 语句分析项包括：SQL 语句、捕获时间、数据库用户、客户端 IP、执行结果、影响行数等信息。

数据库操作记录可下钻到数据库操作详情，并且可关联出相关会话信息。

3.2.3.3 会话检索

系统支持会话记录的检索，条件包括数据库用户、客户端 IP、MAC 地址、工具和应用以及 OS 用户等，针对查询出的记录，可下钻到关联的 SQL 语句，进一步可查看语句详情。

3.2.3.4 告警检索

系统不仅支持实时告警，同时对告警事件进行记录存档，支持检索历史告警信息，并可进一步下钻查看具体的告警信息。

3.2.4 操作行为的统计分析

3.2.4.1 多维度统计与分析

本系统对系统整体及单一数据库实例提供多维度和多时间粒度的审计记录统计功能，分别从风险、语句、会话和访问来源多个层面进行统计与分析，帮助用户高效地掌握数据库运行的安全态势并快速锁定风险目标。

✓ **访问源分析**

系统可以针对审计范围内的数据库各个实例，从访问源头入手进行风险分析，对数据库风险操作快速定位到终端与用户。

✓ **风险类型分析**

系统通过对被保护的数据库进行各种风险类型统计结果的查询及分析，主要包含以下几种：敏感语句、SQL 注入、漏洞攻击、风险操作，可获取数据库运行的当前风险态势。风险的结果与策略管理中的规则是息息相关的，根据策略管理中配置的规则会产生相应的风险。

✓ **语句类型分析**

系统记录了审计范围内的所有数据库语句记录，系统可以清晰的对数据库访问的各类 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**

系统对数据库的所有会话行为进行分类统计、分析和追踪，包括会话统计、会话检索、失败登录、活跃会话、应用会话等。通过会话分析，可以快速的进行风险定位，提高数据库风险分析的效能。

3.2.4.2 可视化展现与钻取

系统通过定制的模块化展板，利用仪表盘、柱状图、折线图、饼图、直方图、热力图等多种形式向用户直观剖析和展示数据库运行安全状态，提供系统整体和单一数据库实例两个层面的可视化展示，其中：

系统整体层面是对数据库审计系统监控范围内的所有数据库运行态势进行整体展示，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；

单一数据库实例层面展示的指标内容与系统整体基本一致，区别只在于指标统计的范围为单一数据库实例，只体现当前数据库实例的相关统计信息。

系统支持数据库统计指标下钻分析，从统计指标均可下钻到具体的数据库操作记录，进一步可查看数据库操作行为的具体信息。对于分析数据库风险操作提供了有力的技术支撑。

3.2.5 数据库安全审计报表

系统通过动态报表的方式对数据库操作行为审计结果进行统计分析。系统内置丰富的报表模板，其中大部分报表均符合 SOX 法案、等级保护等法规标准对信息系统的审计需求。另外用户也可以根据自身的实际需求选择报表内容，自定义生成审计报表。

系统支持在线报表和周期性报表两种方式，在线报表由用户手工操作，选定报表周期后生成报表，并可手工导出，格式支持 PDF 和 HTTP 两种；

周期性报表系统内置日报、周报、月报三种时间粒度，支持周期性自动通过 E_MAIL 方式定时推送到指定用户邮箱。

从报表内容上，系统内置报表可划分为综合报表和专项报表以及自定义报表，其中综合报表基于系统级和单库级别对审计信息做全量综合分析，内容最为全面，主要包括：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；而专项报表是根据风险、性能、客户端、失败信息等多个维度分别建立独立分析报表，用于满足等级保护等法规标准。

3.2.6 审计数据库自动发现

系统通过对数据库网络流量的采集和数据解析，利用各数据库类型私有通信协议各自特征，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、通信端口等信息。

系统记录数据库自动发现相关信息，经用户手工确认并完善后，即可将自动发现的数据库加入到被审计数据库集合中启动对该数据库的审计。

数据库自动发现功能大大减少了审计产品部署时用户的配置工作量，增强了系统的易用性，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

系统采用基于角色的权限控制机制，即系统只对角色分配权限，用户只能通过拥有一个或者多个角色来获取权限，而不能直接对用户分配权限，完全满足三权分立的合规性要求。

每个用户在创建的时候可以被赋予相应的角色权限。基于用户的实际业务需求可划分不同产品功能权限。实现不同用户针对指定的数据库进行专项的审计管理。

本系统采用三权分立模式默认内置三个角色，分别是：

- ✓ **系统管理员**：具备系统配置和管理权限；
- ✓ **安全管理员**：具备数据库审计操作的权限；
- ✓ **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

关联应用层的访问和数据库层的访问操作请求，可以追溯到应用层的最初访问数据及请求信息；突破传统非精确关联的时间关联匹配层的最初访问数据及请求信息；突破传统非精确关联的时间关联匹配模式，实现精确关联匹配。

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、Jboss 和 WebLogic 等。

3.2.9 双栈协议数据可审计

系统兼容 IPv4 和 IPv6 的网络环境，可运行于混合网络环境中，根据客户实际的网络环境进行适配；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。

3.2.10 系统自身监控和管理

3.2.10.1 系统监控告警功能

系统除了实现对被审计数据库的监控和审计，对自身系统的运行状态也进行状态监控，监控内容包括主要：系统硬件资源、数据库流量、软件模块状态等，其中：

- ✓ **系统硬件资源监控**：主要是监控系统的 CPU、内存、硬盘使用情况，对操作阈值的情况进行告警提醒。
- ✓ **数据库流量监控**：主要是监控数据库采集端的入口实时流量和变化趋势，对实时流量超出阈值进行告警，对流量变化提前做出预警。

- ✓ **软件模块状态：**是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**

  系统提供手工和 NTP 两种时间同步方式，通过对全系统自身的时间同步，保证了审计数据时间戳的精确性，避免了审计事件时间误差给事后审计分析工作带来的影响，提升了工作效率。

- ✓ **审计日志管理**

  审计系统需要经常对审计日志库进行维护，以保证系统的稳定运行。系统可以对日志库进行定时或者手工的备份或删除，以保证在存储一定期限的审计日志前提下，用户能查询到最新的日志。

  如果用户忘记设置日志的自动维护，当系统存储日志超过某一限定值，可能会威胁系统的正常运行，为了防止这一状况发生，数据库审计系统会自动删除最老日期的审计日志。

- ✓ **系统升级管理**

  系统提供系统软件和数据库漏洞库升级功能，当厂家对软件或数据库漏洞库进行了升级或者更新，用户可以自行升级到最新版本。

3.3 典型部署

系统采用分层模块化架构设计，数据采集、协议解码、审计引擎和审计中心各模块在业务功能逻辑上相互独立，采用松耦合接口方式进行数据交互，使得系统部署方式灵活，能适应各种用户网络场景。

系统典型的部署模式包括独立设备部署、分布式部署模式和软探针部署模式，具体描述如下：

3.3.1 独立设备部署模式

独立设备部署模式是最为常见的部署模式，适用于绝大多数用户应用场景，数据库审计设备直接通过用户交换机镜像方式旁路采集用户各业务数据库的网络流量进行审计，部署网络拓扑如下图所示：

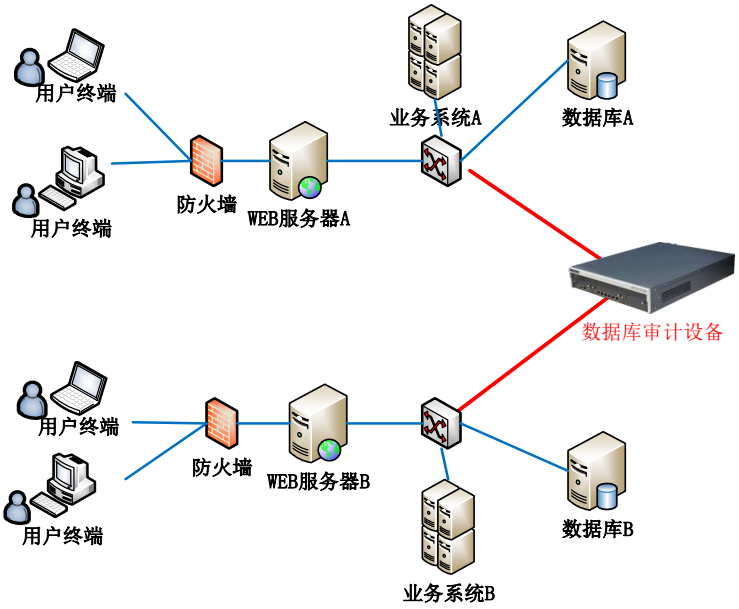

图 3.3 独立设备部署模式

3.3.2 分布式部署模式

分布式部署将审计系统的探针审计引擎及审计中心功能分离，审计中心统一负责数据库审计日志数据的存储和分析，审计探针引擎负责数据库操作数据的采集、解析和审计，一个审计中心可管理多个审计探针和审计引擎，该部署模式适用于大型集团式分级业务网络用户场景，部署网络拓扑如下图所示：

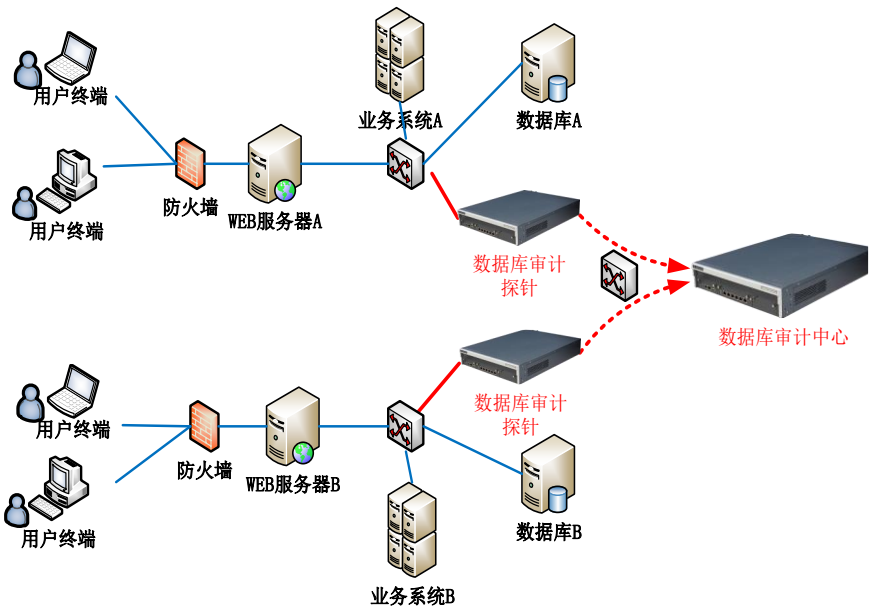

图 3.4 分布式部署模式

3.3.3 软探针部署模式

软探针部署模式是将物理探针引擎功能分拆，将数据采集功能变更为软件模块部署于客户数据库服务器上，其余的数据解析和审计功能则后移到审计设备。此种部署模式适用于 WEB 服务器与数据库合设以及虚拟化场景，部署网络拓扑如下图所示：

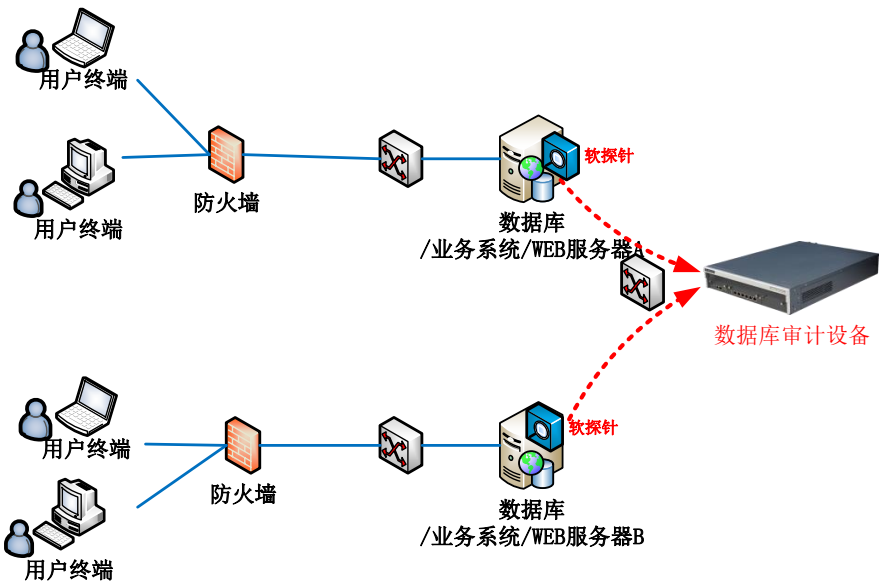

图 3.5 软探针部署模式