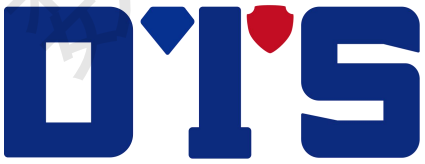
数达安全

数据库防火墙系统产品白皮书

V4R1

数达安全



重庆数达信息安全技术有限公司

2023 年 1 月

版权声明

重庆数达信息安全技术有限公司（简称“数达安全”）版权所有，并保留对本文档及本声明的最终解释权和修改权。

本文档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，除另有特别注明外，其著作权或其他相关权利均属数达安全所有。未经数达安全的书面授权许可，任何机构和个人不得以任何方式对本文档的任何部分进行复制、摘录、备份、修改、传播、翻译成其它语言、将其全部或部分用于商业用途。

免责条款

本文档仅用于为最终用户提供信息，其内容如有更新，恕不另行通知。

数达安全在编写本文档的时候已尽最大努力保证其内容准确可靠，但数达安全不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

数达安全

目录

数达安全

数达安全

1 产品背景

1.1 数据应用日益广泛

随着互联网技术和信息技术的迅速发展，以数据库为基础的信息系统在经济、金融、医疗等领域的信息基础设施建设中得到了广泛应用，越来越多的数据信息被不同组织和机构（例如统计部门、医院、保险公司等）搜集、存储以及发布，其中大量信息被用于行业合作和数据共享。

1.2 数据泄漏事件愈演愈烈

在新的网络环境中，由于信息的易获取性，这些包含在数据库系统中的关乎国家安全、商业或技术机密、个人隐私等涉密信息将面临更多的安全威胁。当前，日益增长的信息泄露问题已然成为影响社会和谐的一大障碍。

数据泄漏事件几乎覆盖所有行业，例如：

- **多行业：**2017 年 5 月，全球范围爆发针对 Windows 操作系统的勒索软件（WannaCry）感染事件，全球 100 多个国家数十万用户中招，国内企业、学校、医疗、电力等多个行业均遭受不同程度的影响；
- **政府部门：**2017 年 11 月，美国五角大楼服务器配置错误，意外暴露 18 亿公民信息；
- **互联网行业：**2017 年 3 月，京东内部员工涉嫌窃取 50 亿条用户数据；2016 年 9 月，雅虎证实，在 2013 年和 2014 年发生两起黑客攻击事件，致使 10 亿级用户账户信息泄露；
- **快递行业：**2016 年 8 月，顺丰内部员工因泄露用户数据依法受审；
- **电信行业：**2016 年 8 月，高考生徐某遭电信诈骗致死；
- **金融行业：**2012 年 4 月，visa 信用卡泄密事件致使 150 万个账户受影响；
- **医疗行业：**2008 年，深圳 4 万余名孕妇信息泄漏。

由上述案例可见，数据泄漏无处不在，且愈演愈烈。据 Verizon 公司的数据泄漏调查报告统计显示：有 90%以上的数据泄漏是由数据库被盗引起的。

1.3 数据安全威胁缺乏有效控制

现有的边界安全防护产品均采用协议识别、连接状态检查等技术路线作为防护手段，无法从根本上解决数据库层面面临的 SQL 注入、漏洞攻击等安全威胁。从根本上解决数据库数据安全问题需要专用的数据库安全设备。

1.4 国家政策法规的要求

《中华人民共和国网络安全法》第二十一条规定：国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

2 产品简介

数达安全数据库防火墙系统（DBFirewall System，简称 SD-DBFW），是一款基于数据库协议分析与访问行为控制的数据库安全防护产品，由重庆数达信息安全技术有限公司研发并具有完整的自主知识产权。

SD-DBFW 系统通过全面的数据库通讯协议解析，基于身份鉴别和行为分析的主动防御机制，能够主动实时监控、识别、告警、阻断针对数据库的安全威胁，实现数据库的行为特征分析、访问行为监控和危险操作阻断。

系统能够通过学习期对用户操作行为特征的提取、分类和整理，形成用户行为画像，即时建立每个用户的访问行为特征模型。通过该模型，不仅能够极大地减轻数据库安全防护策略的配置工作量，而且能够精准识别数据库账户被盗用带来的攻击威胁，实现主动防护。

系统具备异常行为、SQL 注入攻击和缓冲区溢出等的检测防护能力，并结合多因子身份鉴别机制，能够帮助用户抵御来自外部的各类攻击行为，同时有效控制内部用户的越权等非法操作，为用户业务稳定和数据安全保驾护航，并快速地满足合规要求。

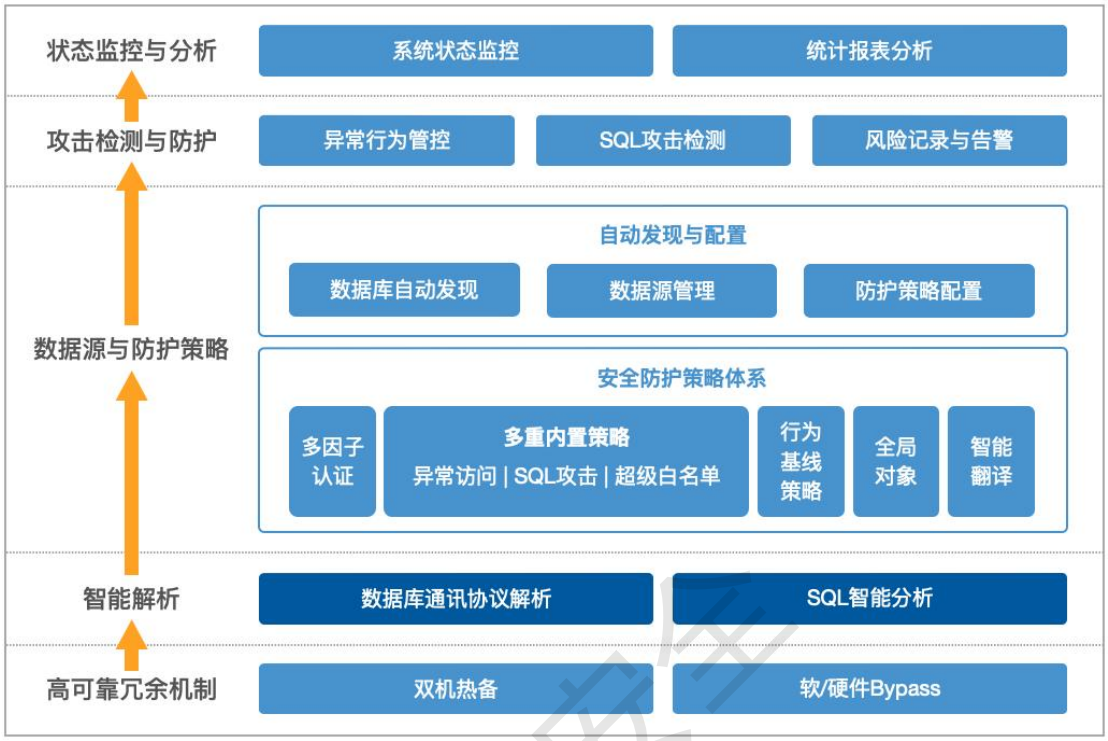
SD-DBFW 系统采用串联的方式部署在数据库服务器和应用服务器之间，能够屏蔽直接访问数据库的通道，防止数据库节点被各类攻击者、扫描工具发现，从而诱发的各类攻击行为，保证核心业务安全、平稳地运行。系统支持“直路透明”、“旁路代理”等多种部署方式，结合双机热备、负载分担等部署模式，以及软/硬件 Bypass 功能，能够保证业务运行不中断，提高系统的高可靠性。

SD-DBFW 系统具有平台化、智能化、高可靠、高性能的特点，能够广泛应用于金融、电信、互联网、医疗等行业领域，以及政府部门、军工、涉密单位等。

数达安全

3 产品架构

SD-DBFW 系统结构分为五大部分，如下图：



数据库防火墙系统架构图

- **高可靠冗余机制：**通过双机热备和软/硬件 Bypass 的多重处理机制，实现高可靠冗余特性，保障业务连续运行；
- **智能解析：**对抓取的数据流量包进行数据库通讯协议解析和 SQL 智能分析；
- **数据源与防护策略：**自动用户网络中的数据库节点，并对其进行数据源管理；根据不同的数据库厂家，预定义了不同的规则体系，帮助用户提升策略配置的有效性；
- **攻击检测与防护：**实时监控数据库访问行为，根据预定义策略进行精准化策略匹配，能够及时发现异常行为、SQL 攻击等风险事件，并对其进行风险记录与阻断告警；
- **状态监控与分析：**对系统的运行状态、数据库业务的各项指标进行可视化监控，以及对风险事件进行细粒度的统计分析。

4 功能特性

4.1 高可靠冗余机制

系统提供透明部署模式下的多重高可靠冗余方案：

- 系统采用双机部署时，系统能够实时同步各类安全策略配置，当主机出现异常时触发主备切换，保持业务流量不中断；
- 系统采用单机部署时，当系统出现异常，通过软/硬件 Bypass 功能，能够及时导通业务通道，防止系统出现单点故障导致的业务中断。

4.1.1 双机热备

系统能够支持基于主备备份和负载分担运行模式下的双机部署方式，以应对数据库多链路冗余组网下的部署。

- 两台设备通过心跳网口发送 KeepAlive 保活报文进行主备间探测与切换，并采用会话同步、策略同步机制，保证双机之间的一致性，保障系统的连续防护能力；
- 当数据库采用集群、多链路冗余部署时，系统可以通过多组负载分担的部署方式，为每一条业务链路提供单独的保护能力。

4.1.2 软/硬件 Bypass

系统实时监控网卡的运行状态，具备硬件断电 Bypass 和软件异常 Bypass 导通能力，具体包括：

- 在进程挂死、CPU 使用率超限和网卡瞬时流量超限等特定条件下的自动 Bypass 能力，能够有效防止单点失效，保障业务流量不中断；
- 手动启动 Bypass 能力，在应急情况下导通网络通道，避免异常阻断。

4.2 智能解析

数据库通讯协议解析，是数据库安全关键技术要求中的核心部分，其准确度和全面度直接关系到防火墙产品的效果，因此，也常常是恶意攻击者的主要攻击对象。

SD-DBFW 系统具备多种类型的数据库通讯协议解析能力，能够实现包括参数化的 SQL 语句、嵌套 SQL 语句和各种长 SQL 语句的精准解析，并通过将解析出的 SQL 语句与 SQL 注入特征库、漏洞库等进行语句模式识别，准确过滤出高危操作或攻击行为，为系统防护提供风险拦截和实时报警的技术保障。

4.3 数据源与防护策略

4.3.1 数据源管理与配置

系统提供对默认的安全防护策略采用可信访问机制，可以帮助业务系统的快速接入，减少因为安全策略配置而导致的业务系统停机风险。通过快捷的风险访问策略设置，对数据库访问行为进行实时监控与精准化策略匹配。

系统提供策略同步功能，一次配置即可将策略下发给相同类型的所有数据库使用，避免重复操作，减少面对数据库集群时的安全策略配置工作量。

4.3.2 安全防护策略体系

系统结合多年数据安全经验和大量客户需求，基于 TCP/IP 协议栈模型，并根据数据库的访问行为特征及不同数据库类型的特点，为用户提供了多层次、精细化的数据库安全防护策略体系，使数据库的安全防护级别达到最高等级。

4.3.2.1 多因子认证

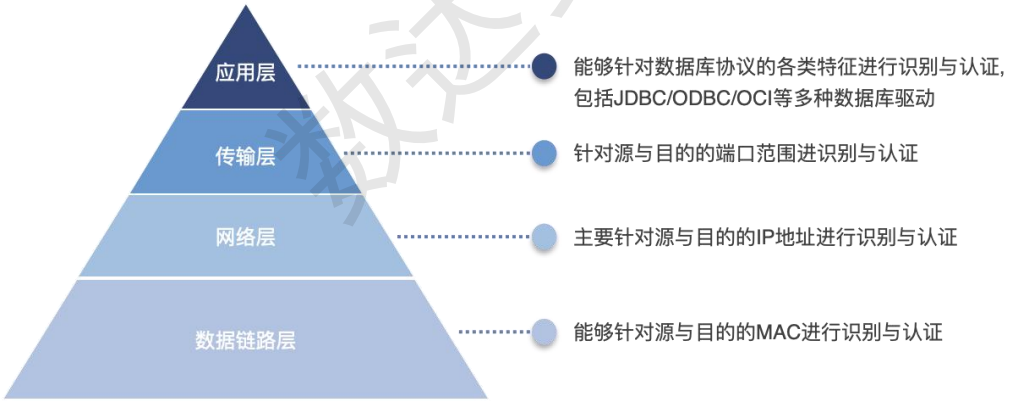
系统采用多因子的组合认证方式对访问者进行身份鉴别，能够弥补单一的“用户名+密码”认证方式安全性的不足，同时满足合规要求。

应用程序对数据库进行访问时，必须经过数据库防火墙和数据库自身的多重认证，包括但不限于：时间（访问时间）、来源（数据库用户、访问者主机 IP、主机名、主机系统用户、客户端应用程序）、行为（访问对象、操作类型、其他行为特征）。

系统支持通过多因子组合方式，预定义包括白名单、风险监控和黑名单三种类型的防护策略：

- **白名单：**被判定为无风险的访问行为的集合；
- **风险监控：**被判定为存在一定风险的访问行为的集合；
- **黑名单：**被判定为高风险的访问行为的集合。

基于多因子认证方式，可实现 TCP/IP 网络协议层面的协议栈防护机制：



TCP/IP 网络协议栈防护机制示意图

4.3.2.2 多重内置策略

- **异常访问**

系统内置 130 余种异常操作行为特征，包括脱库、撞库、删表等高危操作，以及批量数据篡改、大规模数据泄露等风险行为类型。

启用异常访问策略，系统能够针对不同的数据库访问来源，提供对数据的访问权限、操作权限等的有效管控。结合对 NO WHERE 语句的风险判断，避免大规模数据泄露和篡改。

- **SQL 攻击**

系统采用主动防御机制，内置基于 CVE 的 SQL 注入&缓存区溢出特征库和数据库漏洞

库，提供对 SQL 攻击进行特征分析和风险鉴别能力，以及漏洞特征检测和防御技术。内置特征点在 500 个以上，基本能够抵御所有常见的风险事件。

启用 SQL 攻击策略，当发生 SQL 注入或漏洞攻击行为，系统能够实时捕获到对应的 SQL 语句及相关会话信息，基于精准的 SQL 语法分析，系统可以准确定位 SQL 语句中的操作谓词和常量表达式，保障注入、攻击行为防护的准确性。

- **超级白名单**

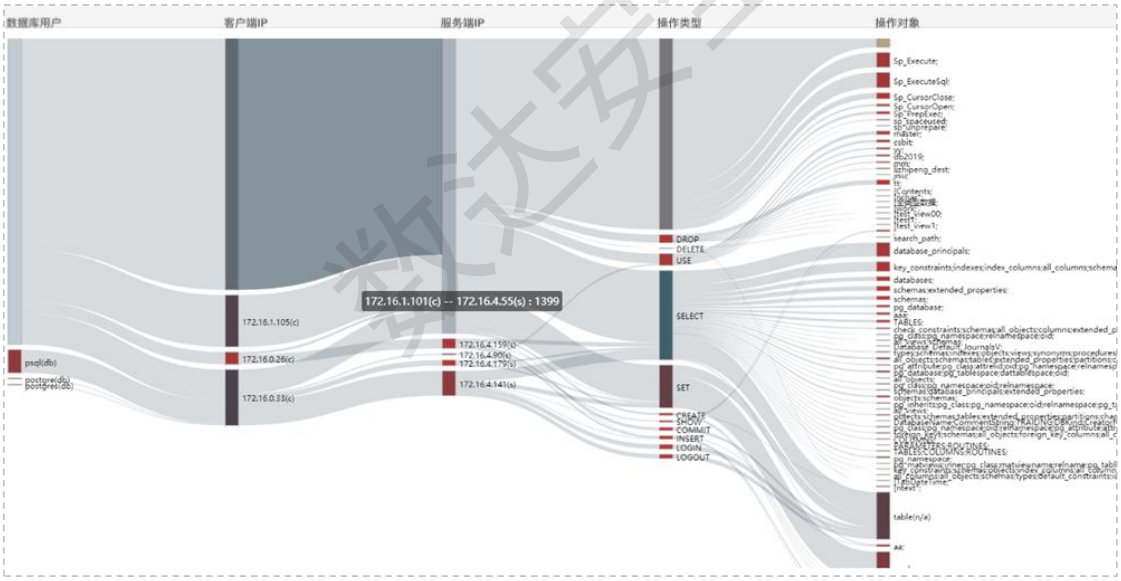
系统将一系列无风险的高频 SQL 操作进行汇总，并内置形成超级白名单。例如，使用数据库连接工具（例如 SQL Developer）登录数据库时会对数据库发送设置环境信息的 SQL 语句，这些操作通常是没有风险的，不需要进行监控。

启用超级白名单，将会屏蔽此类信息，显著减少日志中的干扰项，提高日志的利用效率，并能一定程度上缓解存储压力。

4.3.2.3 行为基线策略

防火墙产品的防护策略一般能够解决常见的攻击或异常访问事件，但对于被盗用的合法用户执行的不合规操作，难以被普通的防护策略识别。

系统能够通过自定义学习期，对包括业务操作、特权操作和工具操作的数据库访问操作，按照访问来源、访问途径、访问对象、操作行为、操作次数等几个方面对其进行自动学习，完成语句、会话的建模分析，形成用户行为的基线策略，构建数据库安全防护基础模型。



用户行为基线模型

启动行为基线策略后，系统将提取用户的访问行为特征数据，通过检查访问行为与基线的偏差来识别风险，对偏离基线的操作行为进行风险告警，并根据预定义的处理方式，对偏离基线行为进行风险阻断。不仅能够对非法场景下的合法行为实现精准识别，提高系统的安全防护能力，而且能够避免规则的复杂配置，减少人工压力。

4.3.2.4 全局对象

系统为策略提供了全局对象特征库，支持客户端 IP、工具名称、OS 用户、数据库用户、表名、列名、SQL 关键字、时间范围等多种全局对象的特征配置与管理。通过自学习的方式提取各类数据库行为的特征，用户可以根据实际需要直接选取，方便策略的直接引用，大大

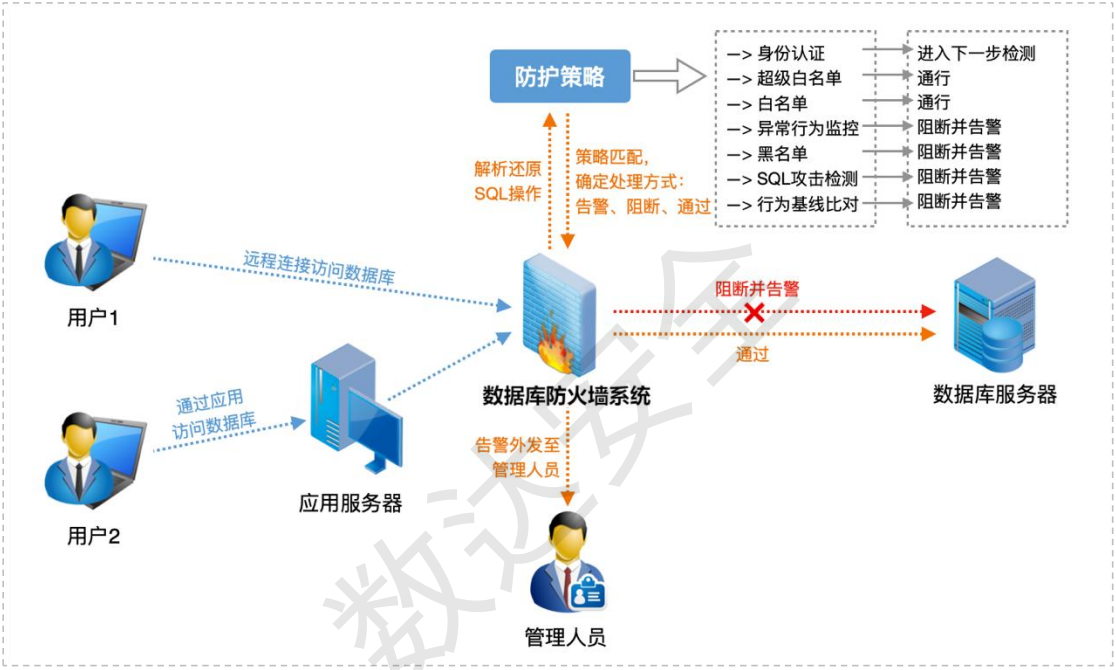
降低策略配置的数据准备工作。

4.3.2.5 智能翻译

系统提供基于 SQL 类型、表和字段的智能翻译功能，能够根据定义的翻译字典内容，自动将日志中的 SQL 语句翻译地更加贴近业务，便于用户对于风险日志的理解，了解风险事件内容。

4.4 攻击检测与防护

系统对访问数据库的网络数据包进行实时的监控分析和策略匹配，能够识别数据库的异常访问和攻击行为，及时进行会话级阻断，从而有效保护核心数据的安全。



数据库防火墙系统工作原理图

4.4.1 异常行为管控

系统能够实时监控数据库的连接信息、风险状态等，并对数据库的各类用户行为进行严格的监控和管理，及时阻断未经授权的数据库操作，防止内部攻击或者越权操作行为的发生。

系统通过内置各类数据库的异常访问行为特征库，能够有效的阻止数据库被脱库、撞库、批量篡改数据、批量删除数据等严重安全事件的发生。

4.4.2 SQL 攻击检测

系统内置基于 CVE 的 SQL 注入&缓存区溢出特征库和数据库漏洞特征库，用户可通过启用引擎的 SQL 攻击策略，对 SQL 注入或漏洞攻击行为进行特征分析和风险鉴别，能够实时监控并及时阻断利用数据库漏洞对数据库进行攻击或数据泄露的行为。

系统自动记录攻击事件信息，包括：攻击发生的时间、攻击行为的来源（IP、主机等）、攻击者身份（数据库用户、操作系统用户）、攻击对象和具体的攻击行为等信息。

4.4.3 风险记录与告警

系统能够对命中策略的数据库风险访问行为日志进行汇聚、查询和告警处理，满足客户对突发事件的即时知情需求。

具体包括:

- 对风险告警进行分级、分类等聚合统计，方便用户对告警信息的查看、管理和风险趋势的预判;
- 支持对告警日志的查询统计和误报处理，从而提高告警日志的准确性和可读性;
- 提供 Syslog、Email、FTP、SNMP、短信等多种告警日志外发方式，使用户在非登录状态下能够及时收到告警信息。

4.5 .自动学习

系统将自动学习每一个用户的访问语句,进行模式提取和分类,自动生成行为特征模型,并可以对学习结果进行处理。同时能将用户访问行为与特征模型进行比对，增加了防御攻击的精确性。

4.6 状态监控与分析

4.6.1 系统状态监控

系统将防护时间、风险统计、会话统计、网络流量统计、资源使用率、Bypass 状态等自身的防护状态进行了集中可视化展示,能够使用户对系统当前运行状态和防护情况一目了然。

4.6.2 统计报表分析

系统监控防护状态，生成风险实时报表，能够直观了解到各类风险事件的发生情况，是将防护日志进行数据化分析的具体表现形式。

系统提供了丰富的报表模板，包括审计报表、安全趋势等，并支持自定义报表的统计属性。通过选用报表模板发布执行报表任务，能够实现对风险日志及阻断行为进行各种粒度的报表输出、统计趋势展示等。

4.7 敏感发现

系统通过内置敏感数据识别规则，能够识别用户数据库中的敏感数据，提供敏感数据的分布报告，用户了解敏感数据的分布情况后针对敏感数据制定访问控制策略。

4.8 报表分析

报表是将记录的日志进行数据化分析的具体表现形式，数据库防火墙提供《场景的操作异常分析》《来源的风险行为分析》《操作的风险统计分析》《结果的风险防护分析》等，可以真实的反应数据库的业务运行状况，数据安全风险情况等等。

- 报表预览根据系统内置的报表模板将对应的日志进行统计展示，提供分析数据的能力，同时提供清晰的信息便于阅读和图形的可视化展示。
- 支持邮件定期发送报表，有利于观察、分析数据的动态。

数达安全

5 典型部署

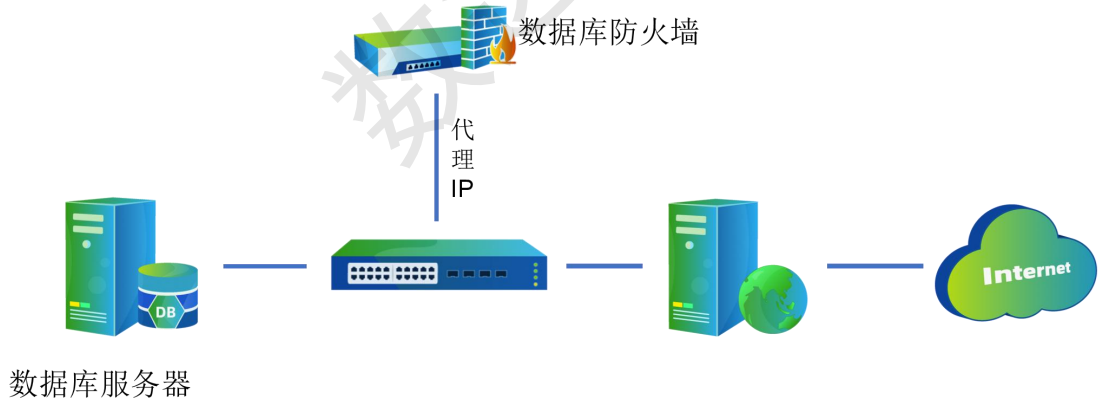
5.1 直路透明模式

将 SD-DBFW 设备物理串联数据库计算节点之前，所有用户访问的网络流量都串联流经设备。通过硬件零拷贝技术，应用端看到的数据库地址不变，且在数据链路层，数据帧的源和目的 MAC 均不会被改变。

直路透明模式部署图

5.2 旁路代理模式（虚拟环境解决方案）

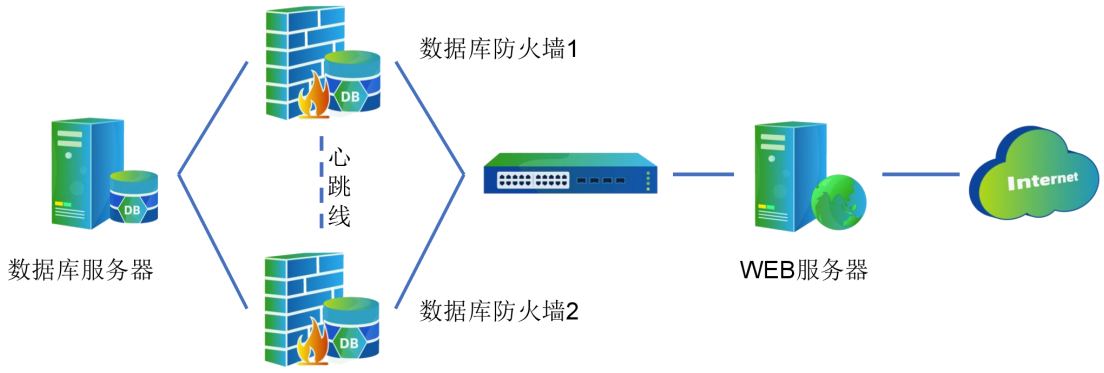
将 SD-DBFW 设备旁路接入数据库所在网络，各类应用采用逻辑串联方式，连接设备地址，所有访问数据库的流量都经过防火墙设备的过滤和转发。通过代理接入模式，网络拓扑结构不变。



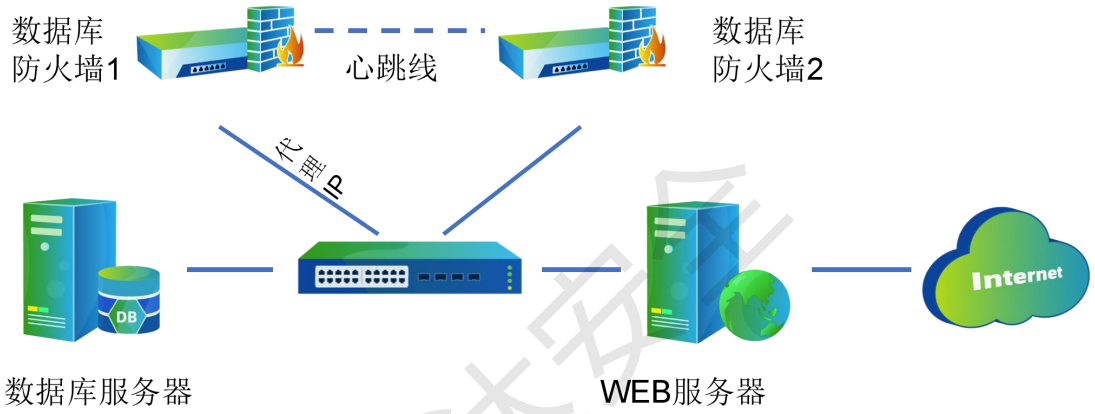
旁路代理模式部署图

5.3 双机热备模式

将两台 SD-DBFW 设备串联接入用户网络，设备之间基于 HA 心跳线进行探测监控与切换。当单台设备出现异常，可以快速地将业务流量切换到对端设备。系统基于会话同步和策略同步机制，保障两台设备之间的信息同步。



直路透明模式下双机热备部署图

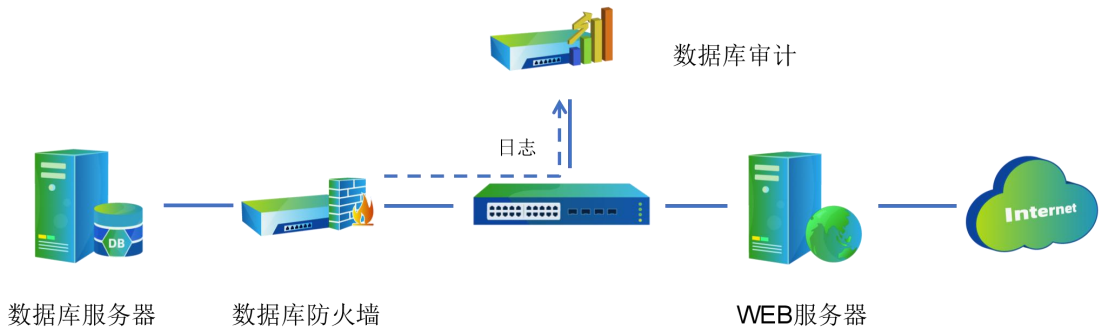


旁路代理模式下双机热备部署图

5.4 混合部署模式

将数据库防火墙接入数据库所在网络，客户端逻辑连接防火墙设备地址，所有对数据库的访问流量都流经该设备进行过滤和转发。同时将日志发给审计系统，与审计系统配合使用，对数据库进行审计与防护。

。



6 产品优势

6.1 全面的策略体系

系统区别于传统的网络防火墙，具有网络和应用行为的多个层次的全面防护体系。不仅能够在 TCP/IP 协议栈的 2-4 层上对源和目的的 IP、端口号、MAC 等进行访问控制，更能够实时监控数据库操作行为，对 SQL 注入攻击和异常访问等进行风险鉴别和非法阻断。

6.2 细粒度的访问控制

系统采用多因子的认证方式，对数据库访问者的身份进行多重鉴别。基于 5W1H 模型，能够实现对数据库访问行为的访问时间、访问来源、使用工具、目标对象以及具体操作进行多层次的识别和认证，访问控制粒度更全面、更精细。

6.3 高可靠的冗余特性

保障数据库正常业务的有效运行，是防火墙产品的首要任务。SD-DBFW 系统具备多重链路冗余机制，实现高可靠的部署特性。

- **双机热备**

系统支持双机主备部署，可高效融入用户已有网络拓扑。两台设备通过 HA 心跳线进行主备间探测，网络异常时能够实现秒级切换，保证业务流量正常运转。

- **软/硬件 Bypass**

系统实时监控网卡运行状态，能够在进程挂死、CPU 使用率超限和网卡瞬时流量超限等特定条件下的自动 Bypass，防止单点失效，保障业务流量不中断；而且能够在应急情况下手动触发 Bypass，导通网络避免异常阻断。

6.4 强大的协议兼容性

系统支持 OCI/JDBC/OLEDB/ODBC 等常见协议，能够支持 Oracle、MySQL、MSSQL、Sybase、DB2、达梦 6/7、人大金仓、神州通用、InforMix、PostgreSQL、Gbase、Hive、MongoDB、Redis、TeraData、Cache、Kafka、ElasticSearch、HANA、MariaDB、Hbase 等多种数据库类型，几乎涵盖了所有关系型数据库和主流的大数据平台，兼容性强。

6.5 安全易用的处理机制

- 使用高性能硬件平台、内核优化技术，满足高负载环境下的性能要求；
- 智能学习，对数据库访问语句自动进行模式提取与分类，并生成特征模型，避免规则的复杂配置；
- 纯透明的部署方式，应用程序的使用环境以及授权用户的数据库操作管理过程均不会被改变。

7 产品价值

7.1 应对外部攻击威胁

外部黑客利用软件缺陷或潜在漏洞，能够通过 SQL 注入或漏洞攻击入侵目标系统，致使数据库泄漏、账号盗取、系统瘫痪等。

系统通过内置基于 CVE 的 SQL 注入&缓冲区溢出特征库，能够快速有效地识别 SQL 注入攻击、缓存区溢出等风险，并及时进行拦截阻断，有效应对数据库被攻击的威胁。

7.2 应对内部访问风险

DBA、研发人员等内部权限用户，能够直接访问数据库，有意无意的高危操作或越权访问，易对数据库造成破坏。

系统通过内置和自定义的访问控制规则，并结合黑白名单屏蔽处理机制，能够有效防范内部人员泄密、违规备份、权限滥用等访问风险。

7.3 审计追踪非法行为

系统能够通过对风险行为进行 Syslog、SNMP、邮件、短信等方式的告警，并记录风险访问行为日志，便于事后追踪分析，解决数据库风险难以追踪溯源的问题。

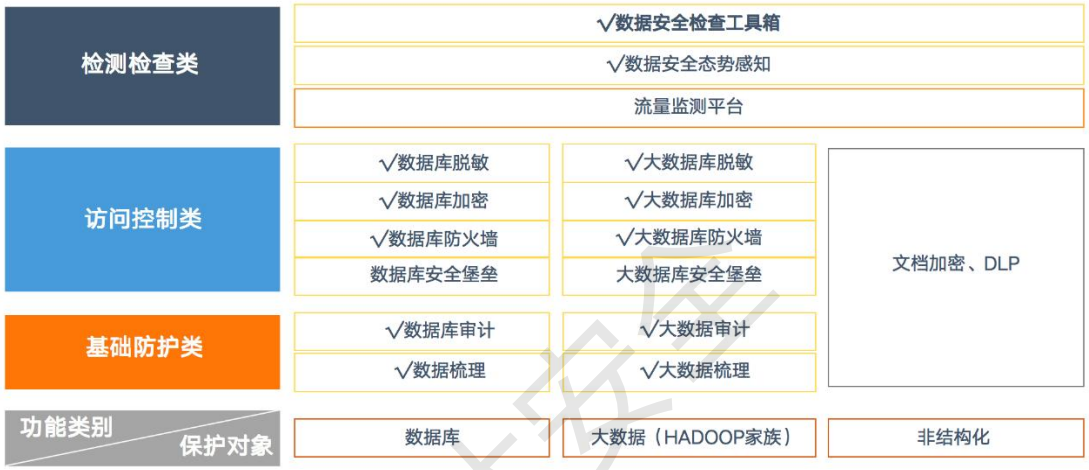
数达安全

8 公司简介

重庆数达信息安全技术有限公司是数据安全领域的引领者，核心团队专注数据安全 20 余年。公司的主要目标是对数据库、大数据、文件等数据对象的存管用（存储、管理、使用）全生命周期全场景实现全面的安全防护。

公司成熟产品根据防护能力分为基础防护类、访问控制类以及检查监测和溯源类。公司还将持续推出具有高度 AI 特性的数据安全新产品。得益于深厚的技术积累，公司系列产品的功能和性能在业内首屈一指。近年来承担了多个国家级、几十个省部级单位、几千客户的数据安全保障体系的建设任务。

产品矩阵如下图所示。



重庆数达信息安全技术有限公司在全国二十多个省设置了办事处，服务全国客户。