**数据库防火墙产品规划、设计文档**

**吕昭波**

**2014年06月03日**

目录

[一、 文档介绍 3](#_Toc389658849)

[二、 数据库防火墙（审计）产品功能介绍 3](#_Toc389658850)

[三、 需求和市场 3](#_Toc389658851)

[四、 产品部署及使用 3](#_Toc389658852)

[五、 功能模块规划 4](#_Toc389658853)

[1. 现有产品借鉴模块 4](#_Toc389658854)

[2. 用户认证（权限控制） 4](#_Toc389658855)

[3. 访问控制 6](#_Toc389658856)

[4. 审计日志 7](#_Toc389658857)

[5. 状态 7](#_Toc389658858)

[6. 其他 7](#_Toc389658859)

[六、 不足之处 7](#_Toc389658860)

[七、 市场产品分析 8](#_Toc389658861)

[1. 安华金和数据库防火墙系统/数据库审计系统 8](#_Toc389658862)

[2. 安恒信息明御®数据库审计与风险控制系统 8](#_Toc389658863)

[3. 北京安信通数据库审计系统 9](#_Toc389658864)

[4. 中安比特数据库防火墙系统/数据库综合审计系统 9](#_Toc389658865)

[5. 昂楷科技数据库审计 9](#_Toc389658866)

[八、 参考文档 9](#_Toc389658867)

[九、 结语 9](#_Toc389658868)

## 文档介绍

本文档为数据库防火墙（审计）产品设计文档，包括数据库防护和审计的需求、主要功能和作用、目前市场上的产品列举，对DBFW产品的详细功能规划分析，最后总结并给出DBFW研发期望和建议。

## 数据库防火墙（审计）产品功能介绍

（待完善）

## 需求和市场

略。

## 产品部署及使用

（待完善）

## 功能模块规划

### 现有产品借鉴模块

#### 1.1系统配置、网络（网络设置、路由、NAT）、对象

#### 1.2日志、告警

#### 1.3统计分析、报表

#### 1.4DOS防护、流量控制（待考虑）

#### 1.5系统状态

### 用户认证（权限控制）

作用：管理数据库中所有用户及权限。

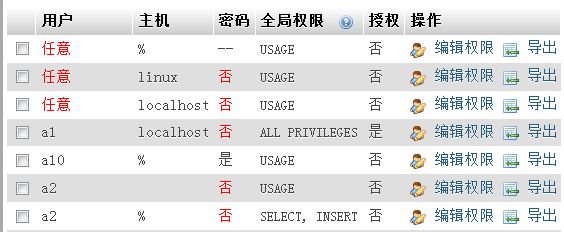
#### 2.1用户及权限

管理数据库系统中的用户及权限，进行自主访问控制。（可根据市场需要和性能进行强制访问控制。）

实现方式：通过SELECT等语句查询数据库系统中所有用户、权限，进行显示。

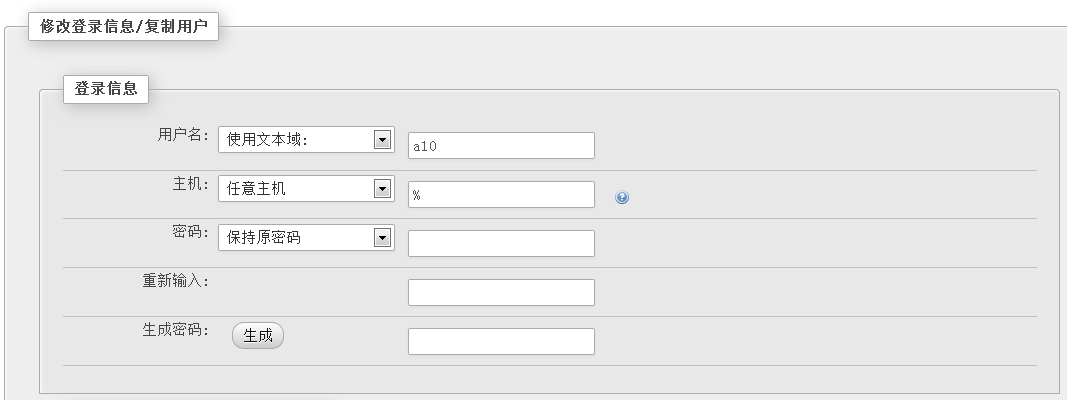
通过GRANT、REVOKE等语句对用户权限进行设置。

以下为MySQL用户权限管理界面截图。









#### 2.2基于角色的访问控制

针对用户可以拥有的权限设置不同的角色，如管理员、审计员、操作员、开发人员、测试人员等角色。创建用户时可以选择角色进行权限设置，同时也可以选择具体的权限，从而可以达到细粒度的访问控制。



#### 2.3二次认证

在向数据库提交SQL语句执行之前先在DBFW上对用户登录进行检查。基于配置中的允许登录的IP地址、MAC地址、时间段、应用程序、访问的数据库等字段进行检查，通过DBFW认证的登录才提交到数据库中进行认证，从而达到二次认证。

### 访问控制

#### IPTABLES访问控制

功能及实现参考SGFW等产品。

#### 基于SQL语句的访问控制

根据执行的SQL语句、用户、访问的数据库IP、时间段、动作进行访问控制。例如：审计员不能执行INSERT语句，开发人员不能在下班时间使用外网IP访问数据库等。

#### 白名单、黑名单

对源IP、目的IP、SQL语句、用户等设置白名单和黑名单。

### 审计日志

#### 4.1行为审计、内容审计、流量审计

对用户或应用程序对数据库的连接、数据操作、权限操作、数据库断开等行为进行审计。实现基本功能后重点考虑审计日志可视化。

#### 4.2实现方式

使用抓包工具对经过DBFW的数据进行记录，分析来源、目的等参数及数据包的内容，如数据库连接、SQL语句查询，记录响应结果，实现双向审计。记录的日志存入DBFW系统数据库。

工具选取：目前没有找到合适工具，需进一步查找。使用tcpdump可以分析出数据包中的SQL语句，感觉功能不足以满足DBFW审计的要求。Sniffit是Linux下一个抓包工具，只能抓取同一网段的数据包，目前只安装成功，未成功测试。

### 状态

实时的监控所有到数据库的连接信息、操作数、违规数、数据库用户连接信息、数据库服务器状态、统计数据等，管理员可以断开指定的连接。实现方式：通过数据库SQL语句（如STATUS等）、记录的日志进行统计显示。

DBFW的系统状态信息（参考SGFW等现有产品）。

### 其他

#### 6.1支持多种数据库、多场景

支持Orac1e、MS-SQL、IBM DB2、Sybase、Informix、MySQL等多种数据库，同时需考虑数据库集群、分布式数据库、云端数据库等场景。

## 不足之处

#### 7.1数据库漏洞、安全性扫描

#### 7.2针对数据库攻击进行防护

如SQL注入、缓冲区溢出等。

#### 7.3数据库数据备份、加密

#### 7.4数据恢复

防止误操作，可以根据日志恢复一些数据。

## 市场产品分析

### 安华金和数据库防火墙系统/数据库审计系统

**网址：**<http://www.schina.cn/a/fangan/shujufangxielou/17.html>

**安华金和数据库防火墙系统（简称Xsecure-DBFirewall）**，是一款基于数据库协议分析与控制技术的数据库安全防护系统。DBFirewall基于主动防御机制，实现数据库的访问行为控制、危险操作阻断、可疑行为审计。

DBFirewall通过SQL协议分析，根据预定义的禁止和许可策略让合法的SQL操作通过，阻断非法违规操作，形成数据库的外围防御圈,实现SQL危险操作的主动预防、实时审计。

DBFirewall面对来自于外部的入侵行为，提供SQL注入禁止和数据库虚拟补丁包功能；通过虚拟补丁包，数据库系统不用升级、打补丁，即可完成对主要数据库漏洞的防控。

**安华金和数据库监控与审计系统（简称xSecure-DBAudit）**能够实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据 库遭受到的风险行为进行告警，对攻击行为进行阻断。它通过对用户访问数据库行为的记录、分析和汇报，用来帮助用户事后生成合规报告、事故追根溯源，同时加强内外部数据库网络行为记录，提高数据资产安全。

### 安恒信息明御®数据库审计与风险控制系统

**网址：**http://www.dbappsecurity.com.cn/products/products02.html

**明御®数据库审计与风险控制系统（简称：DAS-DBAuditor）**是安恒信息在多年数据库安全理论研究与实践的基础上， 结合各类法令法规（如等级保护、分级保护、企业内控、SOX、PCI等）对数据库安全的要求，自主研发的业界首创细粒度审计、双向审计、全方位风险控制的 数据库安全审计产品。可帮助用户带来如下价值点：

全面记录数据库访问行为，识别越权操作等违规行为，并完成追踪溯源

跟踪敏感数据访问行为轨迹，建立访问行为模型，及时发现敏感数据泄漏

检测数据库配置弱点、发现SQL注入等漏洞、提供解决建议

为数据库安全管理与性能优化提供决策依据

提供符合法律法规的报告，满足等级保护、企业内控等审计要求。

### 北京安信通数据库审计系统

**网址：**http://www.bjaxt.com/chanpin.asp?id=111&title=%CA%FD%BE%DD%BF%E2%C9%F3%BC%C6%CF%B5%CD%B3

通过在网络中部署安全审计系统，可有效监控数据库访问行为，准确掌握数据库系统的安全状态，及时发现违反数据库安全策略的事件并实时告警、记录，便于进行安全事件定位分析，事后追查取证，从而保障数据库安全。

系统采用旁路方式接入用户网络中，通过监测及采集数据库系统中的安全事件、用户登录行为、用户操作行为、及所有对数据库的使用情况等各类信息，经 过规范化、过滤、还原、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，结合丰富的日志汇总、分析、统计、排名等关联分析功能，实现对 数据库系统安全状况的全面审计。

### 中安比特数据库防火墙系统/数据库综合审计系统

**网址：**<http://www.csbit.cn/chanpin/2014-02-13/1123.html>

**数据库防火墙**所采用的主动防御技术能够主动实时监控、识别、告警、阻挡绕过企业网络边界（FireWall、IDS/IPS等）防护的外部数据攻击、来自于内部的高权限用户（DBA、开发人员、第三方外包服务提供商）的数据窃取、破坏、损坏的等，从数据库SQL语句精细化控制的技术层面，提供一种主动安全防御措施，并且，结合独立于数据库的安全访问控制规则，帮助用户应对来自内部和外部的数据安全威胁。

**中安比特数据库审计系统**是一款基于数据库协议进行分析并实时记录的系统。该系统通过多重机制获取数据库和用户或应用程序 之间的通信内容，根据安全策略分析通信内容的风险，实现完全独立于数据库的审计功能。并提供可视化的审计日志检索和回放功能，记录的同时，对非法及越权行 为及时告警。

### 昂楷科技数据库审计

**网址：**http://www.ankki.com/web/pros.asp?id=511

**数据库审计**是指对审计日志和事务日志进行审查从而跟踪各种对数据库操作的行为，一般审计主要记录对数据库的操作、对数据库的改变执行该项目操作的人以及其他的属性。这些数据库一般被记录到独立的平台中并且具备较高的准确性和完整性，针对数据库活动或状态进行取证检查时，审计可以准确的反馈数据库的各种变化对我们分析数据库的各类正常异常违规操作提供证据。

## 参考文档

GB/T 20273—2006 信息安全技术 数据库管理系统安全技术要求

## 结语