

An Oracle White Paper  
January 2011

# Oracle Database Firewall

---

Introduction .....	1
Oracle Database Firewall Overview .....	2
Oracle Database Firewall .....	2
White List for Positive Security Enforcement .....	3
Black List for Negative Security Enforcement .....	4
Exception List Security Enforcement .....	4
Host-Based Monitors.....	4
Oracle Database Firewall Management Server .....	5
Policy Management.....	5
Reporting.....	5
User Role Auditing .....	6
Stored Procedure Auditing .....	6
Integration with F5 BIG IP ASM .....	7
Integration with ArcSight .....	7
Conclusion .....	7

## Introduction

While there will continue to be much publicized cases of lost or stolen laptops containing personally identifiable information (PII), attempts to steal large amounts of information through attacks on servers is becoming increasingly common. In fact the recently published 2010 Data Breach Investigations Report published by the Verizon Risk Team showed that 98% of data breached came from servers<sup>1</sup>. Launching successful attacks on larger repositories can result in a more lucrative payday for the perpetrator and it goes without saying that application environments, data warehouses and database in general are becoming larger and more critical to business operations and thus pose a tempting target. While it is true that organized crime has become a major player in data breaches, insiders still account for a substantial number of data breaches. The 2010 Data Breach Investigations Report also noted that privilege misuse and hacking were the most common ways breaches occurred and frequently leveraged lost or stolen credentials and application SQL Injection vulnerabilities to gain unauthorized access. Securing data on servers requires multiple layers of protection spanning both technical and administrative functions. Without question simple preventive measures such as disabling unused accounts and prohibiting shared administrative accounts go a long way toward raising the security bar. In addition, solutions such as encryption and privileged user controls inside the database play an important part in securing applications. Those solutions, however, do not monitor the SQL sent to the database over the trusted connection path. Oracle Database Firewall enables perimeter security controls, providing a first line of defense around Oracle and non-Oracle databases.

---

<sup>1</sup> *2010 Data Breach Investigations Report* (Verizon Business)

## Oracle Database Firewall Overview

Oracle Database Firewall is an active, real-time database firewall solution that provides white list, black list and exception list policies, intelligent and accurate alerts, and monitoring with very low management and administrative costs. Oracle Database Firewall is independent of the database configuration and operation. This independent boundary of protective shielding helps reduce the risk of data loss and helps organizations manage an ever changing landscape of regulations.

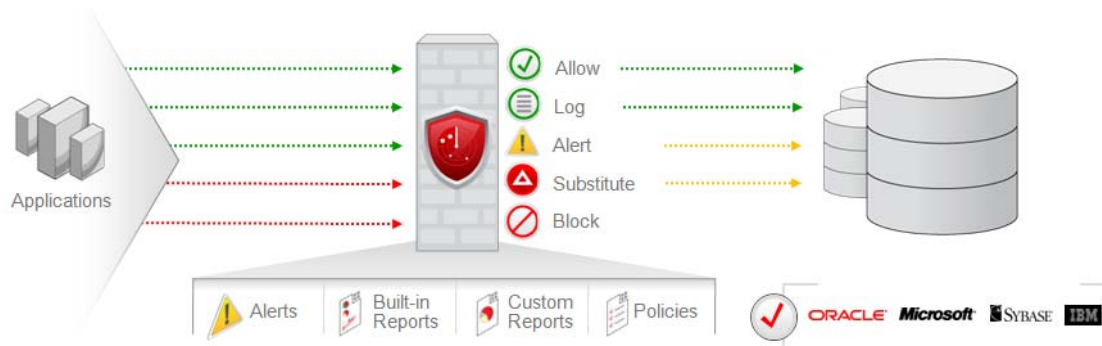


Figure 1 - Oracle Database Firewall

Unlike traditional SQL firewalls that relied on identifying out-of-policy SQL using strategies such as regular expressions, string matching, and schema comparison, Oracle Database Firewall delivers intelligent database firewall security, enabling policies to be set and adapted quickly and accurately. Organizations can choose to deploy Oracle Database Firewall in blocking mode as a database policy enforcement system to protect their database assets, or to just monitor database activity for supplemental auditing and compliance purposes.

Oracle Database Firewall monitors data access, enforces access policies, highlights anomalies and helps protect against network based attacks originating from outside or inside. Attacks based on SQL injection can be blocked by comparing SQL against the approved white list of application SQL. Oracle Database Firewall is unique and offers organizations a first line of defense, protecting databases from threats and helping meet regulatory compliance requirement.

## Oracle Database Firewall

Oracle Database Firewall is installed on the network either on a bridge or a span port and monitors every SQL transaction request. SQL statements are processed using powerful grammar-based analysis engine that decomposes and categorizes the SQL. In addition to purely looking at the SQL statement, policies can evaluate factors such as IP address, time, and program name.

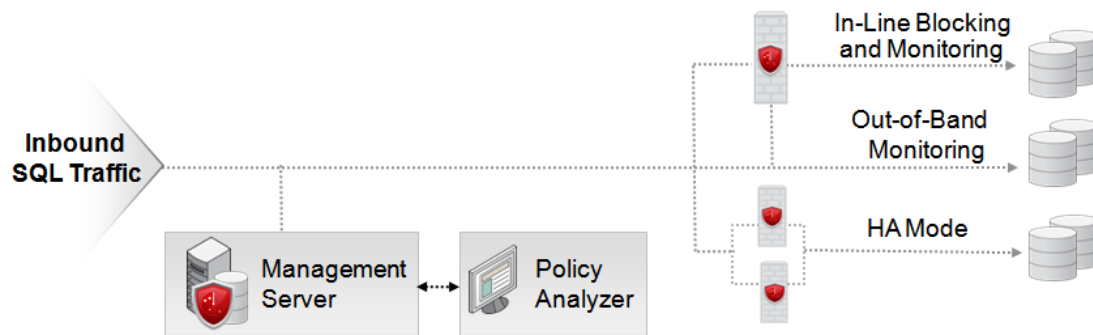


Figure 2 - Oracle Database Firewall Deployment Topology

A single Oracle Database Firewall can monitor and protect many databases at once. Oracle Database Firewall can be deployed in multiple scenarios:

- **In-line network blocking mode and out-of-band passive network monitoring.** In-line means that the SQL traffic is passed through the Oracle Database Firewall and inspected before it is forwarded to the database or blocked. Out-of-band means that the SQL traffic is copied to Oracle Database Firewall while at the same time the SQL is sent directly to the database usually by mean of a span port. These can be used simultaneously for different databases.
- **Heterogeneous, multi-database, enforcement.** For example, one device can support Oracle 8i, Oracle Database 10g and Oracle Database 11g databases simultaneously, as well as SQL Server and Sybase databases.
- **Combined deployments.** In-line and/or out-of-band Oracle Database Firewall deployment can be combined with a local server-side, monitor-only agent for local connections.

Oracle Database Firewall can be deployed a high availability configuration. It is recommended that two firewalls be deployed so that SQL monitoring is not interrupted.

### White List for Positive Security Enforcement

Oracle Database Firewall enforces zero-defect database security policies using a white list security model. The white list policy is a set of approved SQL statements that can be sent to the database. Oracle Database Firewall compares SQL traffic with the approved white list and then based upon the policy, it chooses to block, substitute or alert on the SQL statement.

The Oracle Database Firewall baseline can be configured to block all out-of-policy events. This can be implemented as

- Block the SQL statement
- Modify the request using SQL statement substitution
- Alert on all out of policy SQL statements, in addition to blocking or in lieu of

In many cases, the best solution is to apply statement substitution. Statement substitution provides a means of making Oracle Database Firewall transparent to detection by hackers and is more transparent to the existing application.

In simple terms statement substitution is the process of taking an out-of-policy statement and changing it for a new statement that will not return any data.

**TABLE 1. EXAMPLES OF ORACLE DATABASE FIREWALL SQL STATEMENT SUBSTITUTION**

ORIGINAL STATEMENT (FRAUDULENT)	SUBSTITUTED STATEMENT	DATABASE RESPONSE (RESULT)
SELECT * FROM tbl_users;	SELECT * FROM tbl_users WHERE 'a' = 'b';	No record found.
DROP TABLE tbl_accounts;	SELECT * FROM aaabbbccc;	Error. Table not known.
UPDATE tbl_accounts SET accounts = '123' WHER user = 'Fred';	SELECT DUAL SET 'Fred';	Error. Incorrect Syntax.

## Black List for Negative Security Enforcement

In addition to the white list, positive security enforcement model, Oracle Database Firewall also supports a black list model that enables policies to specify blocking of specific SQL statements. As with white list policies, black list policies can be configured to allow specific statements based on factors such as IP address, time of day and program.

## Exception List Security Enforcement

Exception lists policies supplement white list and black list policies by allowing specific policies to be created for specific activities. For example, exception list policies could be used to enable a remote administrator to diagnose a particular application performance issue.

## Host-Based Monitors

Oracle Database Firewall also provides very lightweight host-based monitors or agents that monitor databases. The host monitor sends the information to the Oracle Database Firewall for monitoring, logging and alerting purposes. The characteristics and operation of the Oracle Database Firewall monitors are listed in the Table 1.

**TABLE 2. CHARACTERISTICS AND OPERATION OF ORACLE DATABASE FIREWALL MONITORS**

MONITOR TYPE	OPERATION METHODS
Remote Monitor	Software monitor (agent) installed on the host operating system. Agent monitors specified network traffic bound for one or many database schemas or catalogs. Captures SQL transactions and sends back traffic to the Oracle Database Firewall for real-time alerting, post-event compliance, and monitoring reports. A Remote Monitor is used when the Oracle Database Firewall cannot be deployed in front of the database host to capture incoming SQL.

**Local Monitor** Additional tables are installed into the monitored databases to capture SQL traffic that originates from sources that have direct access to the database, such as console users or batch jobs that run on the database server. The Oracle Database Firewall collects the data by querying the database at regular intervals, and then uses the data in the same manner as statements originating from database clients. Depending on the design of the policy, the statements may be logged and/or produce alerts.

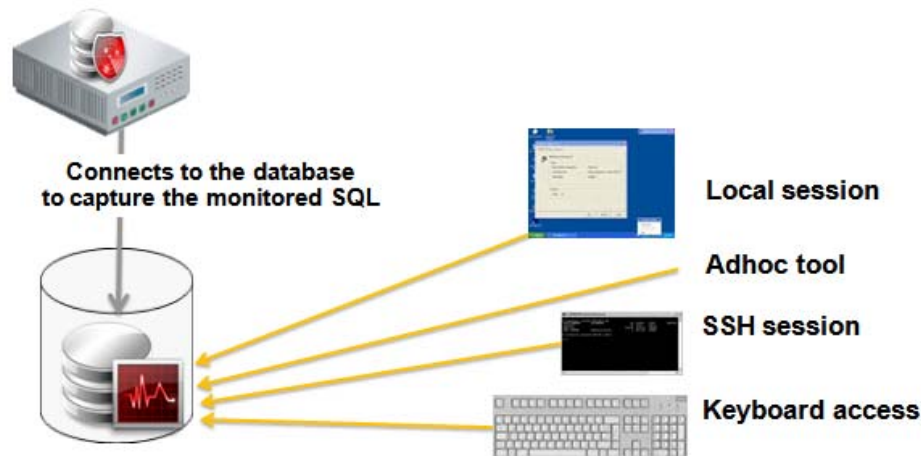


Figure 3 - Oracle Database Firewall Local Monitor

## Oracle Database Firewall Management Server

The Oracle Database Firewall Management Server centrally manages Oracle Database Firewall policies, consolidates data from the Oracle Database Firewalls, stores database activity data, and provides dozens of out-of-the-box reports.

### Policy Management

Oracle Database Firewall delivers simple and easy to use policy management tools that build upon the powerful strengths of the SQL grammar-based analysis approach. Oracle Database Firewall can define a white list of approved SQL language for a given database and define a positive security model. Oracle Database Firewall policy management groups queries together that have the same effect on the database. Oracle Database Firewall allows factors such as IP addresses, client programs, and time of day to be associated with SQL. When the Oracle Database Firewall policy management uses factors on the network, fine-grained and powerful policies can be built to determine when, where, and how changes in a production environment occur.

### Reporting

Oracle Database Firewall ships with dozens of predefined reports that can be used for Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA) and other privacy and compliance regulations. Oracle Database Firewall records all available details about events and makes all of the



- Type of stored procedure, date created, last modified, details of any modification
- Action of stored procedure (DML, DCL, DDL, DML etc.)
- Threat rating based on key SQL grammar such as SYSTEM, UPDATE, etc.

With SPA, any changes to the stored procedures are detected and the actual change is highlighted in precise detail and automated reports can be scheduled for distribution to interested parties.

### Integration with F5 BIG IP ASM

Oracle Database Firewall integrates with F5 BIG-IP Application Security Manager using a plug-in connector. The combination of Oracle Database Firewall and F5 BIG-IP Application Security Manager enables security and monitoring for both applications and databases within an enterprise.

If you are also using the BIG-IP ASM interface, and an attack originates from the internet, Database Firewall provides the actual IP address and application user of the attacking Web client. This feature enables you to pinpoint the source of the internet-based attack. You can configure the integration by using the Database Firewall Administration Console.

### Integration with ArcSight

The ArcSight Security Information Event Management (SIEM) system is a centralized system for logging, analyzing, and managing log messages from different sources. ArcSight SIEM enables Oracle Database Firewall to provide full details of security alerts or other selected event types, including the message text, priority and IP address of any attacker.

## Conclusion

Securing data on servers requires multiple layers of protection spanning both technical and administrative functions. Oracle Database Firewall delivers intelligent database firewall security, enabling policies to be set based on SQL grammar-based analysis approach. Oracle Database Firewall validates application SQL against white list, black list and exception list policies, and to prevent SQL injection from reaching the database to begin with. Oracle Database Firewall provides dozens of out-of-the-box reports that assist with a wide range of privacy and compliance regulations, including SOX, HIPAA and PCI. Flexible deployment options include inline blocking and out-of-band passive monitoring of network SQL traffic. Oracle Database Firewall enables perimeter security controls, which strengthen database security by providing a first line of defense against threats originating from both outside and inside the organization.



Oracle Database Firewall  
January 2011

Oracle Corporation  
World Headquarters  
500 Oracle Parkway  
Redwood Shores, CA 94065  
U.S.A.

Worldwide Inquiries:  
Phone: +1.650.506.7000  
Fax: +1.650.506.7200  
oracle.com



Oracle is committed to developing practices and products that help protect the environment

Copyright © 2011, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd. 0410

**SOFTWARE. HARDWARE. COMPLETE.**