An Oracle White Paper
June 2011

Oracle Database Firewall 5.0 Sizing Best Practices

Introduction

Oracle Database Firewall provides the first line of defense for databases, helping prevent internal and external attacks from ever reaching the database. Highly accurate SQL grammar-based technology monitors and blocks unauthorized SQL traffic on the network, while flexible configuration options allow for efficient, cost-effective deployments across the enterprise. Oracle Database Firewall can be tailored to suit numerous environments with seamless support for an extensive range of hardware platforms, assuring that a deployed architecture can scale for future growth. This guide contains three sections. The first section provides a brief overview of the Oracle Database Firewall components. The second section provides a method for determining hardware requirements for individual Oracle Database Firewall deployments. The third section outlines the issues that will determine the placement and number of Oracle Database Firewalls and Oracle Management Servers throughout the enterprise.

Component Overview

Oracle Database Firewall deployments are comprised of two primary components: the Database Firewall and the Management Server. The Database Firewall is placed in-line or out-of-band on the network to inspect the network traffic. The Management Server is used for centralized configuration, administration, and reporting. SQL traffic logged by Database Firewalls is transferred to the central Management Server.

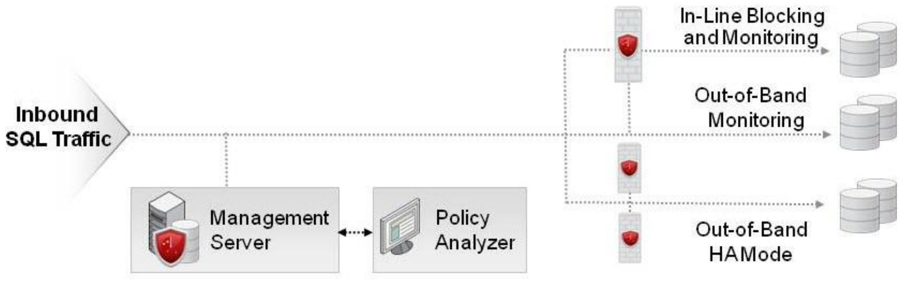

Figure 1: Oracle Database Firewall Components

Database Firewall Deployment Modes

The Database Firewall can be deployed in different configurations depending on your individual security requirements.

- In-line network blocking - SQL traffic is passed through the Database Firewall and inspected before it is forwarded to the database or blocked.
- Out-of-band passive network monitoring – A copy of the SQL traffic to and from the database is sent to the Database Firewall (usually by means of a span port) for analysis and alerting.
- Combined deployment: in-line and/or out-of-band deployments can be configured on the same Database Firewall and combined with local server-side, monitor-only agents for local connections.

The Database Firewall operates in two modes depending on your security and operational needs.

- Database Activity Monitoring (DAM): The system detects and logs unusual activity, and produces warnings, but does not block potential threats. It is also known as monitoring mode.
- Database Policy Enforcement (DPE): The system performs all the actions of database activity monitoring and blocks potential attacks. It is also known as blocking mode.

It is important to note that a single Database Firewall can provide heterogeneous, multi-database enforcement support for Oracle 8i, Oracle Database 10g and Oracle Database 11g databases simultaneously, as well as Microsoft SQL Server, Sybase ASE, Sybase SQL Anywhere, and IBM DB2 LUW databases.

Sizing Hardware Requirements

Database Firewall Sizing

The total number of transactions per second is the main factor used in planning for Database Firewall capacity.

CPU

As a result, available processing power is an important factor determining the capacity and performance of a Database Firewall. The number of cores required can be estimated by allocating one core for management overhead, and adding another core for every 5,000 SQL transactions per second monitored by Database Firewall. Table 1 lists the recommended number of CPU cores based on the total rate of SQL transactions per second for all databases protected by Database Firewall.

The “Oracle” column in the table represents the estimated transactions per second (TPS) that can be read by the Database Firewall. The “Other RDBMS” column in the table represents the number of TPS that can be read by the Database Firewall for the other supported databases. If you have a Database Firewall that is monitoring a combination of heterogeneous RDBMSs, then you can use an estimate of 5,000 TPS, otherwise the numbers in the columns can guide you on the number of COREs that are recommended.

NUMBER OF CORES	PERFORMANCE: TRANSACTIONS PER SECOND (TPS)		
>= 2.8 GHZ	PLANNING FOR MIXED RDBMS ENVIRONMENT	ORACLE	OTHER RDBMS
2	5,600	4,200	8,400
4	16,800	12,600	25,200
6	28,000	21,000	42,000
8	39,200	29,400	58,800
10	50,400	37,800	75,600
12	61,600	46,200	92,400
14	72,800	54,600	109,200
16	84,000	63,000	126,000
32	173,600	130,200	260,400
48	263,200	197,400	394,800

Memory

Minimum:	2.0GB
Recommended:	1.0GB per Protected Database: moderate use 1.5GB per Protected Database: medium use 2.0GB per Protected Database: heavy use

The system will function with less memory, but a larger memory size will improve performance during periods of high throughput.

Disk

Minimum:	100 GB
Recommended:	300 GB

Disk space is used for temporary storage of log files containing the captured SQL traffic and associated data. Available disk space should be large enough to retain several days of log files in case communication between the Database Firewall and the Management Server is interrupted (e.g. link failure between data centers).

Management Server Sizing

The volume of transactions logged will be the primary influence on the specification of the Management Server.

CPU

Minimum: 1 core
Recommended minimum: 2 cores
Although the Management Server can operate on 1 core, it is recommended that 2 to 8 cores be available depending primarily on the amount of data being logged and the number and size of reports being generated. The number of databases being protected should be considered as a secondary factor.

Memory

Minimum: 2 GB
Recommended minimum: 4 GB
Memory should be increased up to 8 GB for systems with heavy loads.

Disk

When planning disk space requirements, follow the formula below, changing values as required for the target environment. Industry best-practices should be followed when choosing RAID configurations and disk type and speed.

Assumption:

- 1 statement = 1000 bytes of storage after binary logging, summarization, reporting and compression
- 10 statements = 10k
- 1,000 statements = 1Mk bytes
- 1,000,000 statements 1GB bytes
- Logging 1,000tps = 85m transactions per day logged
- 85 x 1GB = 85Gb / day
- 12 Days = 1 TB

Deployment Planning

High Availability Considerations

For high availability, it is recommended to deploy a secondary (standby) Management Server using the same hardware specification as the primary Management Server. This will enable it to stay synchronized with the primary during heavy loads, and ensure that it can properly perform the role as the primary unit.

Single Platform Deployments

In most cases, the Database Firewall and Management Server are deployed on separate, dedicated machines. However, it is possible to combine the two functions on one server. Determining the appropriate hardware specification required for a single platform deployment can be done most simply by combining the guidelines for a separate Database Firewall and Management Server.

For example, a deployment required to handle 15,000 transactions per second would require 4 CPU cores and 4GB of memory. The Management Server for this level of throughput could be the minimum, with one CPU core and 2GB of memory. The total required for the stand-alone unit would therefore be 5 CPU cores and 6GB of memory. Remember to ensure you have an adequate amount of disk space, with the speed of the disks and RAID configuration also impacting the performance.

As industry best practice, it is strongly recommended that a separate Management Server be deployed on separate dedicated hardware. This minimizes the potential for reporting, archiving and configuration functions of the management server to impact on the higher priority functions of blocking, alerting and logging performed by the Database Firewalls.

Many customers find it useful to undertake an initial sizing exercise to get an estimate for deployment planning. A stand-alone Management Server is ideal for monitoring database traffic at different points in the corporate network to collect and report the information required and to build initial policy baselines.

SQL Logging Policies

One of the primary factors determining the capacity of the Management Server will be the logging policy applied. In high through-put environments, a log-all policy is not recommended on several fronts. Firstly, the amount of data stored (one record for every query sent to the database) will soon create a repository much larger than the databases being protected. Secondly, a large amount of data often makes forensic and audit reporting more difficult by obscuring important transactions by the sheer volume of data.

The Oracle Database Firewall has been designed as a security product from the beginning, with the ability to identify database queries of significance from a security and/or audit perspective in real time in a sub-millisecond timeframe. The accuracy and speed with which the Database Firewall operates allows the end-user to deploy a selective logging policy, knowing that activity identified as legitimate can be discarded with confidence as a valid part of an accurate white list. Likewise, the end user can also be confident that only interactions relevant to security and audit requirements will be logged and/or alerted. It is important to remember that the vast majority of entries in an Oracle Database Firewall white list will consist of expected transactions. Audit and security events are identified through a combination of session factors, significant white list entries, polices based on statement-types and sensitive tables, and general out-of-policy events (anomalies).

Deployment Reference Architectures

Given the flexibility of Oracle Database Firewall, deployment planning should start with understanding the existing network infrastructure in the context of security and compliance requirements.

Objectives to be considered are:

- Monitoring versus policy enforcement
- Security versus SQL Logging
- System resilience and high-availability

Allocation of Database Firewalls to Protected Databases

The number and choice of databases protected by a given Database Firewall depends on the distribution of databases across the network infrastructure. The choice will also be affected by any preference for a particular size of hardware on which to deploy the Database Firewall. For example, depending on current hardware and maintenance costs, it may be more cost-effective to deploy two or three mid-range servers versus one high performance machine.

Network Infrastructure

- Distribution Layer - The Distribution Layer of the network is comprised of the group of switches directly attached to database servers. At this level, multiple small-to-mid-sized Database Firewalls are deployed for in-line or span-port monitoring of traffic near the database. If preferred, a smaller number of larger Database Firewalls with multiple network interfaces can be used instead.
- Core Layer - The Core Layer (or network backbone) includes high-end switches and high-speed cables. A small number of larger Database Firewalls can monitor uplink traffic at the core (up to 10GB per network segment) in-line or via span-ports to capture SQL traffic from other segments of the corporate network or from external sources. Note that when deployed in Database Policy Enforcement (DPE) mode, the databases protected by a given network segment must be in the same subnet as the IP address assigned to the corresponding bridge on the Database Firewall. This restriction does not apply to Database Activity Monitoring (DAM) mode, whether deployed in-line or via a span port.
- Multiple Data Centers - For centralized management, one Management Server can control Oracle Database Firewalls deployed across multiple data centers.
- Distributed Management – Database Firewalls can be managed by a local Management Server to suit local network topologies. Corporate security and auditing policies may encourage a separation of management between data centers or between departments. Deploying a separate Management Server may also be desirable where interconnectivity between data centers is limited by bandwidth restrictions or data protection policies.

Requirements for Resiliency, High-Availability and Testing

- High Availability Systems – Database Firewalls are compatible with a number of resilient network technologies, monitoring both primary and secondary network links. For blocking mode, HA deployments must preserve session integrity across any given Database Firewall bridge, and must utilize standard TCP/IP. When failing over, the HA configuration must also initiate new sessions across the alternate link. In addition, there is a special mode for span-port deployments that allows a resilient pair of Database Firewalls to monitor the same traffic without creating duplicate events. Management Servers can also be deployed as resilient pairs, with one Management Server operating as the primary unit, and synchronizing configuration settings and reporting data with the secondary unit.
- Load Balanced Environments – Database Firewalls can be deployed as multiple individual units immediately in front of the database servers to match the performance and high-availability

architecture of the protected systems. Load balancers must retain session integrity through any given Database Firewall bridge and must utilize standard TCP/IP.

- Failover/Backup Data Centers – Redundant Database Firewalls can be deployed in backup data centers, running in active mode with the latest policy settings to ensure protection for the backup systems the instant a failover occurs.
- Testing and Development - Most customers find it beneficial to deploy one or more Database Firewalls in their testing and development environments. In addition to the valuable summary of SQL traffic it provides, it can be used to develop and update white list policies before new systems or functionality is released.

Conclusion

Increasingly sophisticated threats combined with the push toward data consolidation and cloud computing are just a few of the reasons why Oracle Database Firewall is critical to safeguarding data. Data breach investigations have shown that security controls must be multi-layered to protect against threats that range from account misuse to SQL injection attacks. In addition, the ever changing regulatory landscape and renewed focus on privacy demonstrates the need for solutions to be transparent and cost effective to deploy.

ORACLE®

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

Oracle Database Firewall 5.0 Sizing Best Practices
June 2011
Author: Stuart Sharp

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

Hardware and Software, Engineered to Work Together