ORACLE

SECURE DATA AT THE SOURCE
SAVE TIME AND MONEY

Security Inside Out | Oracle Database Security

ORACLE

Oracle Database Firewall Architecture Overview

Agenda

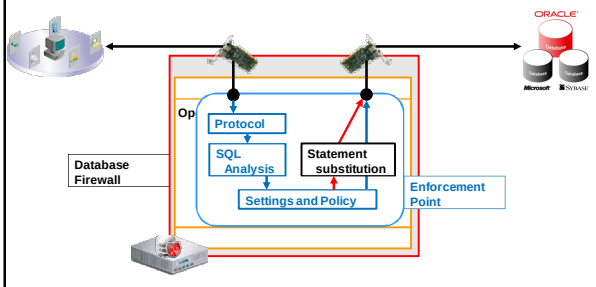
- Basic Terminologies and Components
- Deployment Architectures
- Product Deployment Example in Data Center
- Database Firewall Integration with F5 ASM

Basic Terminologies and Components

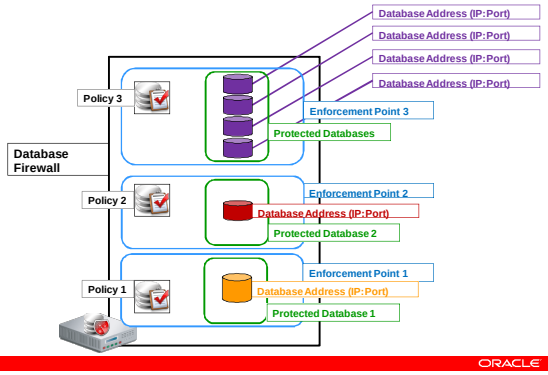
Enforcement Point and Protected Database

- Enforcement Point
  - An Oracle Database Firewall container that stores the settings that enforce the Database Firewall policies that you create
  - Applied to one physical segment on the network
  - Only one protected database per enforcement point
  - One DBFW can have multiple EP for different database platforms
- Protected Database
  - A list of IP:Port combinations of the same database type
    - Have many ports for the same physical database
    - MS Clustering can have multiple IPs for the same logical database
  - Most reports are based on the protected database name

Enforcement Point Architecture



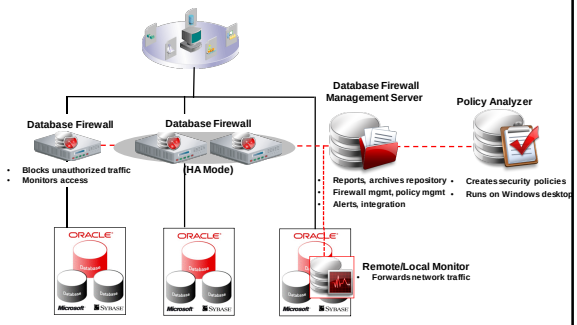
Enforcement Point Architecture



Heterogeneous Database Support

- Oracle 8i, 9i, 10g, 11g
- MS-SQL 2000, 2005, 2008
- Sybase 12.5.3 to 15
- SQL Anywhere v10
- DB2 for LUW

The Basic Components



Management Server

- Management Server is usually deployed as a separate appliance, and is connected to many DBFW's.
- It can also be run on the same physical hardware as a DBFW.
  - Must be installed when first configured. Cannot be retro-installed.
  - Affects performance of the DBFW.

Remote/Local Monitor

- Remote Monitor
  - Runs on the server operating system.
  - Sends database transactions to Oracle Database Firewall
- Local Monitor
  - Resides inside a database
    - Monitors local / non-network access.

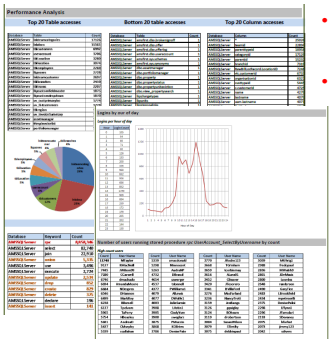
User Role Auditing

- Entitlement Reports
  - User names
  - User roles and privileges
  - Last changed, changed by whom and when
- Automated and transparent
  - User role reporting can be run ad-hoc or scheduled
  - Report on user roles and privileges
  - Deltas since the last report

Stored Procedure Auditing

- Stored procedure contents
  - Its not enough to know a procedure was run, it is important to know what SQL was executed when the procedure is called.
- Stored procedure reports
  - Name
  - Content
  - Threat rating (injection risk, system tables etc).
  - Stored procedure type (DML, DDL, DCL, SELECT etc)
  - Last changed, changed by whom and when
- Automated and transparent
  - Stored procedure reporting can be run adhoc or scheduled

Reporting

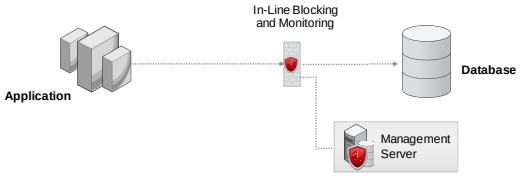


- **Database Firewall log data consolidated into reporting database**
- **Over 130 built in reports that can be modified/customized**
  - **Entitlement report for database attestation**
  - **Activity and privileged user reports**
  - **Supports demonstrating PCI, SOX, HIPAA, etc.**

Deployment Architectures

Deployment Architecture 1:

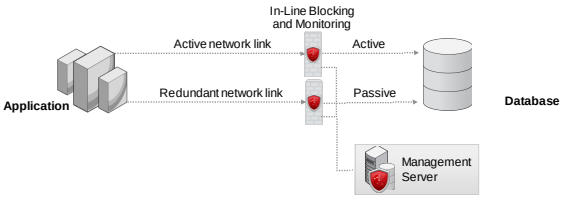
In-line Blocking



- In-line with active blocking policy
- Central control by Firewall Management Server allows for easy expansion

Deployment Architecture 2:

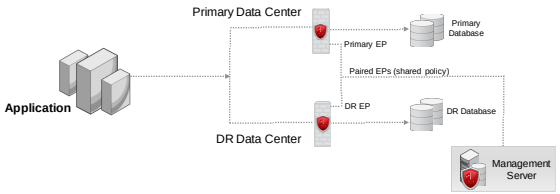
In-line Blocking with Redundant Network



- In-line with active blocking policy
- Two database firewalls on separate network links provides security in the event of network failover to redundant network link
- Centrally controlled by one Firewall Management Server

Deployment Architecture 3:

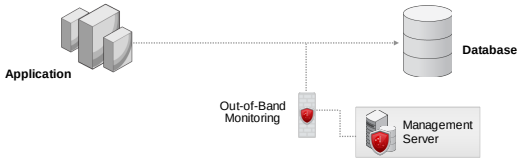
Protecting Redundant Databases with Deploying Paired Enforcement Points



Pairing Enforcement Points:

- Allows any change to the policy to be automatically applied to both databases
- Prevents duplicate records appearing for User Role and Stored Procedure auditing

Deployment Architecture 4:
Out-of-Band Monitoring

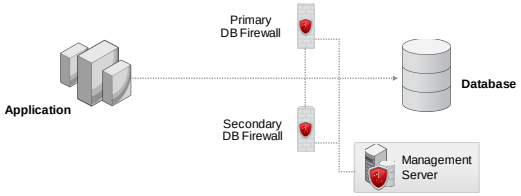


- Out-of-Band monitoring with real time alerting
- Centrally controlled by Firewall Management Server allows for easy expansion

ORACLE

 19

Deployment Architecture 5:
Out-of-Band Monitoring with HA

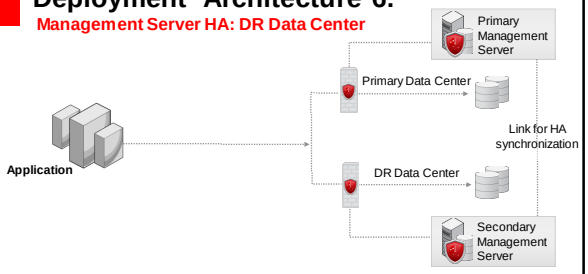


- Out-of-Band monitoring with real time alerting
- HA pair of DB Firewalls with Primary (active) unit and Secondary (standby)
- Both DB Firewalls process all traffic. Management Server removes duplicate events
- HA available at no extra cost

ORACLE

 20

Deployment Architecture 6:
Management Server HA: DR Data Center

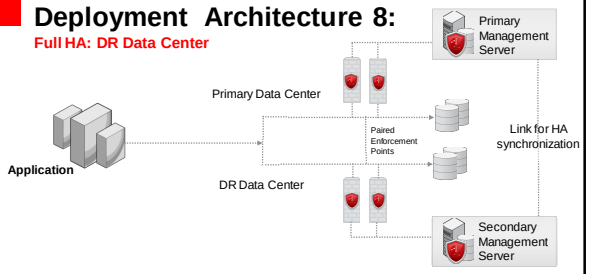


- In-line blocking in both Primary and Disaster Recovery Data Centers
- HA Management Servers: one point of control for multiple data centers
- Data Centers can operate independently should communication between sites be lost

ORACLE

 21

Deployment Architecture 8:
Full HA: DR Data Center

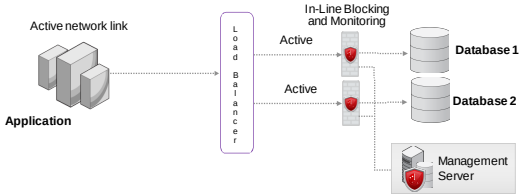


- Redundant Database Firewalls in both Primary and Disaster Recovery Data Centers
- HA Management Servers: one point of control for multiple data centers
- Data Centers can operate independently should communication between sites be lost
- Enforcement Points paired across redundant pairs of Database Firewalls

ORACLE

 22

Deployment Architecture 9:
Load Balancing



- In-line with active blocking policy
- Two database firewalls on separate network links provide seamless security
- Centrally controlled by one Firewall Management Server
- Requires session-based load balancing

ORACLE

 23

Product Deployment Example in Data Center

ORACLE

 24

Product Deployment Example
Basic Data Center Environment

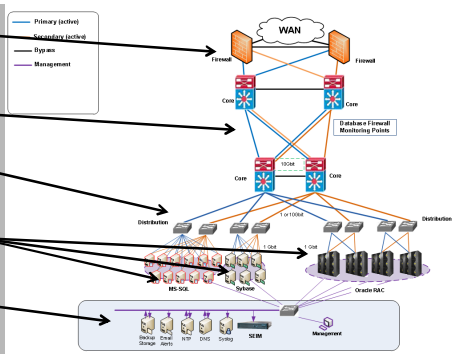
External Network Firewall

Core Network Switches

Distribution network switches

Database and Application Farms

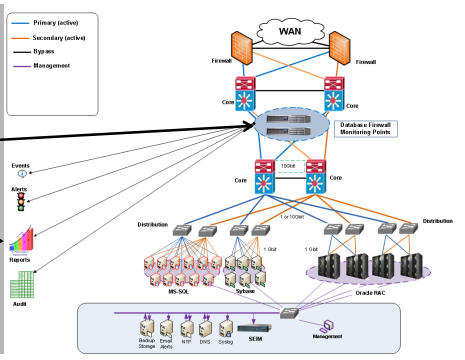
Management Infrastructure



Product Deployment Example
DBFW in-line

Database Firewall deployed in-line to protect all databases from traffic entering and leaving the data center

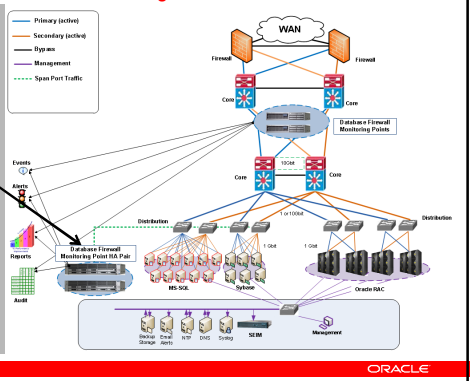
Database firewall alerts, events, audit logs and reports



Product Deployment Example
DBFW Out-of-Band Monitoring

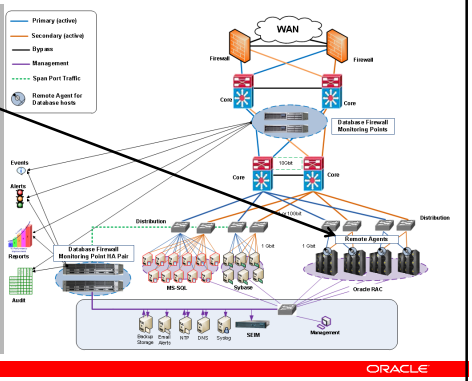
Database Firewall deployed out-of-band to provide real-time monitoring and alerting and audit reports

This provides auditing for all traffic within the data center



Product Deployment Example
DBFW Host-based Monitors

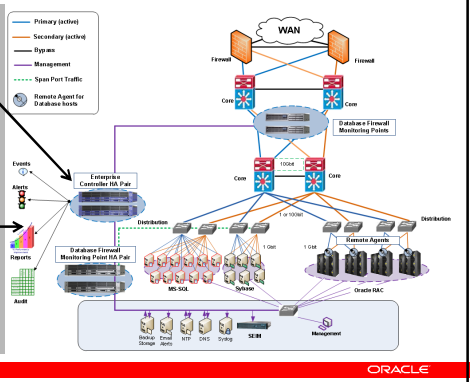
Remote and Local Monitors:
Host-based agents used to deliver transaction events and information back to Database Firewall appliances



Product Deployment Example
Management Server

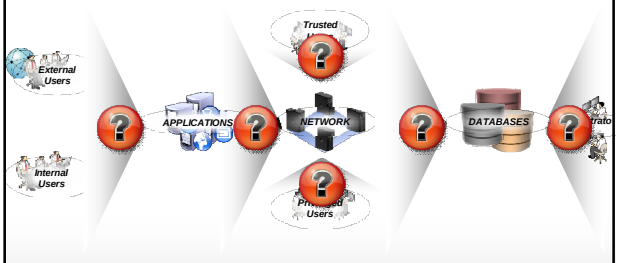
An Enterprise Controller from centralised management of all Appliances, Monitoring Points and Remote Monitors

All reports and Audit data is centralised onto one platform for easy management and administration



Database Firewall Integration with F5 ASM

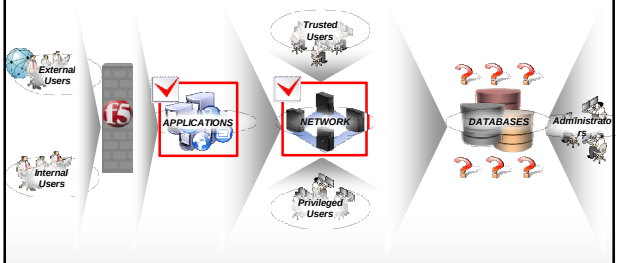
Security Landscape at a Glance



Trillions of packets travel **through the network** every day

Billions of SQL requests travel to the database every day

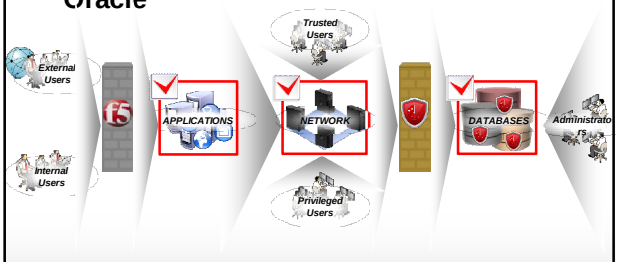
Web Application Security Lanscape



Applications and Networks are fully secured with F5

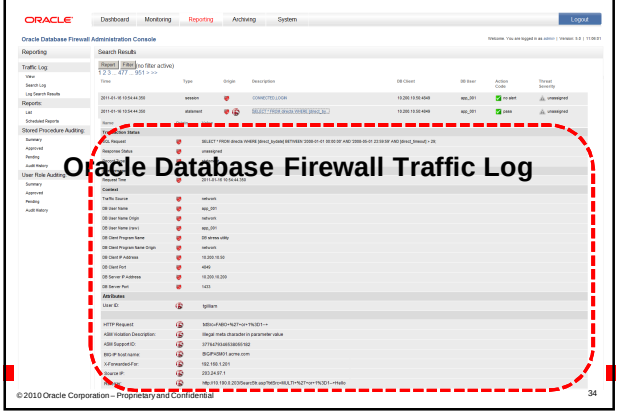
How can we further secure the Databases?

End-to-End Security with F5 and Oracle



Two Best of Breed Technologies to Deliver

Integrated Application Data Security Solution



For More Information

or

oracle.com/database/security