Protecting Web Applications with Oracle Database Firewall and BIG-IP ASM

As access to the web continues to expand across the globe, securing applications from cross-site scripting (XSS) and SQL injection attacks becomes increasingly important. Independent technologies have been developed that provide state-of-the-art security at various tiers within the application architecture. However, the behind-the-scenes communication and correlated reporting across the security tiers has been missing.

The integration between F5® BIG-IP® Application Security Manager™ (ASM) and Oracle Database Firewall provides richer forensic information on SQL injection attacks through correlated reporting.

Providing Correlated Reporting

Securing applications accessible on the web is an evolving science that constantly attempts to address new threats and new technologies. Attacks such as sophisticated XSS and SQL injection are making application security increasingly difficult to maintain without equally sophisticated solutions in place.

Integrating security solutions greatly improves the ability of IT security staff to find and isolate attackers and attack vectors. Integration with F5 BIG-IP ASM enables Oracle Database Firewall to provide enhanced reporting that includes the application user name when a SQL injection pattern has been recognized and flagged by BIG-IP ASM.

In parallel, Oracle Database Firewall detects out-of-policy SQL and takes the appropriate policy action of blocking, alerting, or logging—but with more information for IT staff to deal with the threat.

Solution

When SQL injection threats are detected by BIG-IP ASM, a message is sent to the Oracle Database Firewall that includes the session information such as the identity of the web application user, the IP address, and the URL. Independently, Oracle Database Firewall monitors the inbound database SQL traffic, preventing the SQL injection or malicious SQL from reaching the database. The alerts that are generated from the detected SQL injection by Oracle Database Firewall combine the F5 session information with the Oracle alert information to create a single entry that can be sent to a centralized syslog service for additional monitoring. It can also be optionally consumed by your security information and event management (SIEM) software.

Oracle Database Firewall uses the session information sent from BIG-IP ASM—such as web user name, IP address, referrer URL, web form page URL, and BIG-IP ASM SQL injection description—in reports to provide enhanced correlated reporting.

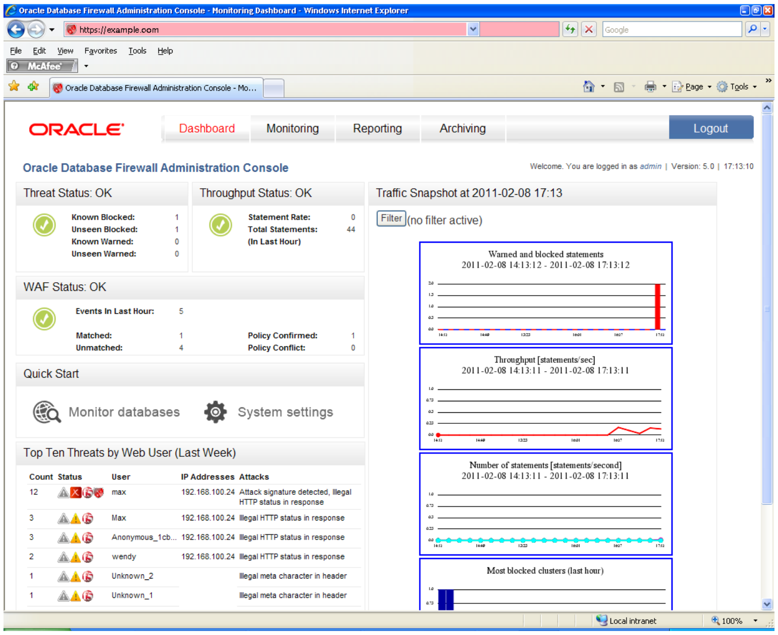
Key features

- SQL Injection Pattern Detection—Detects SQL injection attacks before they reach the server; BIG-IP ASM shares information with Oracle Database Firewall for reporting and response
- Cross-Site Scripting Detection—Identifies XSS attacks before they reach the software
- Consolidated Reporting—Provides security information in one location from both network and application infrastructures

Key benefits

- Increase Protection—Links a web application firewall and database firewall for unified security
- Enhance Efficiency—Detects attacks before they reach their targets
- Widen Footprint—Uses detection and protection features of both BIG-IP ASM and Oracle Database Firewall for maximum exposure
- Enable Coordinated Response—Gives IT security and database teams all of the information available about an attack when it happens

The following figure shows an integrated Oracle Database Firewall report with BIG-IP ASM session information.


Oracle Database Firewall Administration Console - Monitoring Dashboard - Windows Internet Explorer
https://example.com
Google
File Edit View Favorites Tools Help
McAfee
Oracle Database Firewall Administration Console - Mo...
Page
Tools
ORACLE
Dashboard
Monitoring
Reporting
Archiving
Logout
Filter
Monitor databases
System settings
Local intranet
100%

Oracle Database Firewall Administration Console

Welcome. You are logged in as *admin* | Version: 5.0 | 17:13:10

Threat Status: OK

Known Blocked:	1
Unseen Blocked:	1
Known Warned:	0
Unseen Warned:	0

Throughput Status: OK

Statement Rate:	0
Total Statements: (In Last Hour)	44

WAF Status: OK

Events In Last Hour:	5		
Matched:	1	Policy Confirmed:	1
Unmatched:	4	Policy Conflict:	0

Quick Start

Top Ten Threats by Web User (Last Week)

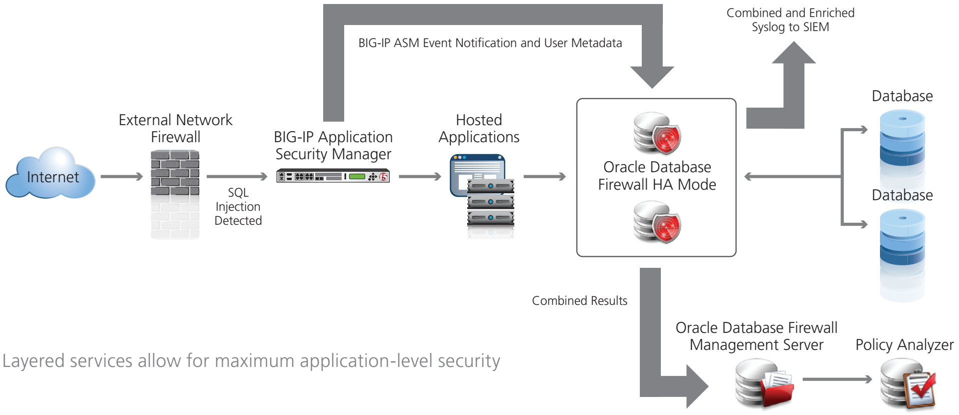
Count	Status	User	IP Addresses	Attacks
12		max	192.168.100.24	Attack signature detected, Illegal HTTP status in response
3		Max	192.168.100.24	Illegal HTTP status in response
3		Anonymous_1cb...	192.168.100.24	Illegal HTTP status in response
2		wendy	192.168.100.24	Illegal HTTP status in response
1		Unknown_2		Illegal meta character in header
1		Unknown_1		Illegal meta character in header

Traffic Snapshot at 2011-02-08 17:13

(no filter active)

Oracle Database Firewall Administration Console

With this integration, security and out-of-policy events from BIG-IP ASM and Oracle Database Firewall due to SQL injection attacks are consolidated into one logging, reporting, and optionally syslog output.


BIG-IP ASM Event Notification and User Metadata
Combined and Enriched Syslog to SIEM
Internet
External Network Firewall
SQL Injection Detected
BIG-IP Application Security Manager
Hosted Applications
Oracle Database Firewall HA Mode
Database
Database
Combined Results
Oracle Database Firewall Management Server
Policy Analyzer

Layered services allow for maximum application-level security

BIG-IP ASM communicates metadata information to Oracle Database Firewall for enhanced reporting and response management.

Learn more

For more information about BIG-IP Security solutions, use the search function on f5.com to find these resources.

Product overview

BIG-IP Application Security Manager Overview

Datasheet

BIG-IP Application Security Manager Datasheet

White paper

BIG-IP Application Security Manager XML Firewall Features

Analyst report

BIG-IP Application Security Manager XML Firewall Features

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com