Deployment Guide

Document version: 1.0

What's inside:

Deploying the BIG-IP LTM with Oracle Database Firewall

Welcome to the F5 Deployment Guide for the F5 BIG-IP® Local Traffic Manager™ (LTM) with Oracle® Database Firewall. This guide provides instructions on configuring the BIG-IP LTM for intelligent traffic management for Oracle Database Firewall deployments.

Why F5

The BIG-IP LTM provides high availability, load balancing, simple scalability and high operational resiliency for Oracle Database Firewall deployments. In an Oracle Database Firewall environment, the BIG-IP LTM provides intelligent traffic management and high availability by monitoring and managing connections to the Database Firewall Proxy services running in Inline Database Policy Enforcement (DPE) Mode, also called Proxy Mode. The Database Firewalls can now be run in Active-Active mode, enabling higher levels of availability, performance, and scalability.

In addition, the LTM's Oracle JDBC Client libraries allow thorough monitoring of both the Database Firewall Policy engine, and the Database server behind the firewall. The LTM also keeps persistence records for connections to always be directed to the same firewall for a specified period of time, to ensure traffic flows to and from each Database Firewall is symmetric. In addition, if the Database Firewall is running in out of band in Database Activity Monitoring (DAM) Mode, the BIG-IP LTM's Interface Mirroring capabilities can send network traffic to the Database Firewall for analysis and reporting.

For more information on Oracle Database Firewall, see
http://www.oracle.com/technetwork/database/database-firewall/overview/index.html

For more information on the F5 BIG-IP LTM, see
http://www.f5.com/products/big-ip/big-ip-local-traffic-manager/overview/

Products and versions tested

Product	Version
BIG-IP LTM	11.1 and 11.2
Oracle Database Firewall	5.1 and later

Important: *Make sure you are using the most recent version of this deployment guide, available at* *http://www.f5.com/pdf/deployment-guides/oracle-database-firewall-ltm-dg.pdf*

ORACLE DATABASE READY

To provide feedback on this deployment guide or other F5 solution documents, contact us at *solutionsfeedback@f5.com*.

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- You must be running BIG-IP version
- The BIG-IP system must be initially configured with the proper VLANs and Self IP addresses. For more information on VLANs and Self IPs, see the online help or the BIG-IP documentation.
- For information on the F5 and Oracle integration between the BIG-IP Application Security Manager (ASM) web application firewall and the Oracle Database Firewall, see *http://www.f5.com/pdf/deployment-guides/oracle-database-firewall-dg.pdf*

Configuration example

There are two modes of deployment described in this guide, Database Policy Enforcement (inline) mode, and Database Activity Monitoring mode. The following graphics show a logical configuration diagram for each mode.

Database Policy Enforcement (inline) mode

In this mode, as described in the introduction, the BIG-IP LTM provides traffic management and high availability by monitoring and managing connections to the Database Firewall Proxy services. This allows you to run the Oracle Database Firewalls in Active-Active mode, enabling higher levels of availability, performance, and scalability.

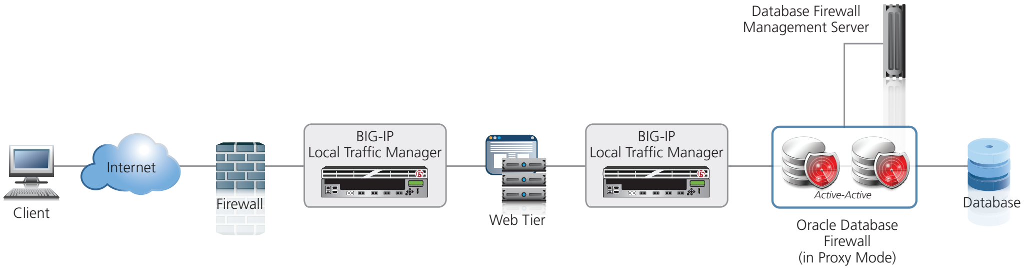

Figure 1: *Database Policy Enforcement mode logical configuration example*

Database Activity Monitoring mode

For Database Activity monitoring mode, you can use the Port Mirroring capabilities of the BIG-IP LTM to send network traffic to the Database Firewall for analysis and reporting.

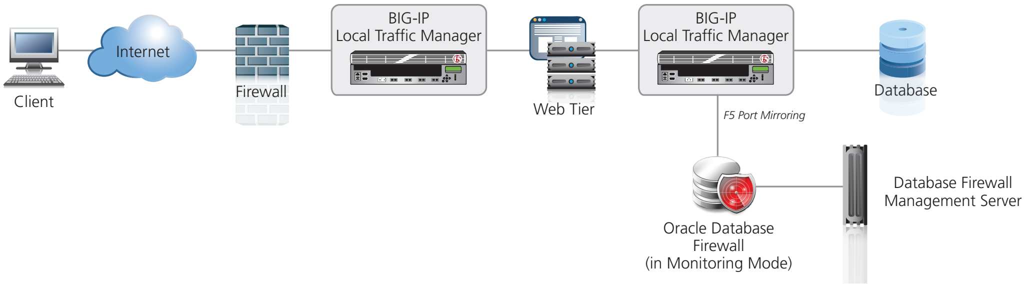

Figure 2: *Database Activity Monitoring mode logical configuration example*

Configuring the BIG-IP LTM for Oracle Database Firewall in Database Policy Enforcement (inline) Mode

Use the following table to configure the BIG-IP LTM for the Oracle Database Firewall in Database Policy Enforcement (inline) mode.

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitor *(Main tab-->Local Traffic -->Monitors)*	***Name***	Type a unique name	
	Type	**Oracle**	
	Interval	**60**	
	Timeout	**181**	
	Send String	**"Select status from V$SYSTEM"**	
	Receive String	**OPEN**	
	User Name	Type the user name of an Oracle DB user. We recommend creating an account specifically for this monitor.	
	Password	Type the associated password.	
	Connection String	**(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=%node_ip%)(PORT=%node_port%))(CONNECT_DATA=(SERVICE_NAME=dbXX))(SERVER=dedicated))** Replace red text with your Service Name.	
Pool *(Main tab-->Local Traffic -->Pools)*	***Name***	Type a unique name	
	Health Monitor	Select the monitor you created above	
	Slow Ramp Time[1]	**300**	
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**	
	Address	Type the IP Address of a DBFW Proxy node	
	Service Port	Type the appropriate port. This is the *Proxy Port* that you defined as the *Enforcement Point* on the DBFW. In our example, we type **15212** Click **Add** to repeat Address and Service Port for all nodes	
	Important: If you have configured a Default Monitor for nodes on your BIG-IP system, and this default monitor is an ICMP monitor, you must remove the Default Monitor from the Database Firewall nodes you just added to the pool, or change the default monitor type. The Database Firewall's iptables service blocks all ICMP traffic. By default, the BIG-IP system does not assign a Default monitor to the nodes. Check **Local Traffic > Nodes >Default Monitor** to see if your system is using a default monitor. To remove the default monitor from a node, from the Nodes screen, click a node, and then select None. You can also change the Default monitor type.		
Profiles *(Main tab-->Local Traffic -->Profiles)*	***TCP*** *(Profiles-->Protocol)*	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
		Idle Timeout	**3600**[2]
	Persistence *(Profiles-->Persistence)*	Name	Type a unique name
		Persistence Type	**Source Address Affinity**
		Timeout	**3600**[2]

[1] You must select Advanced for this option to appear.

[2] SQL connections through the BIG-IP system and the Database Firewall may remain inactive for long periods of time. The idle timeout values in the TCP profile and the persistence profile may need to be increased to match your database environment.

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	***Name***	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**1521**
	Protocol Profile (Client)[1]	Select the TCP profile you created above
	SNAT Pool	**None** **Important**: This should be set to **None**. If SNAT is enabled, the DFBW cannot use any Client IP Address based Policies.
	Default Pool[2]	Select the pool you created above
	Persistence Profile[2]	Select the Persistence profile you created

This completes the BIG-IP LTM configuration for Database Policy Enforcement mode.

Configuring the BIG-IP LTM for Oracle Database Firewall in Database Activity Monitoring Mode

In this section, we show you how to configure the BIG-IP LTM If you are running the Oracle Database Firewall in Database Activity Monitoring (DAM) Mode. The BIG-IP LTM configuration takes advantage of the Interface Mirroring feature; you simply configure this Mirror port with source and destination interfaces.

To configure Interface mirroring

1. On the Main tab, expand **Network**, and then click **Interfaces**.
2. On the Menu bar, click Interface Mirroring.
3. From the **Interface Mirroring State** list, select **Enabled**.
4. From the **Destination Interface** list, select the BIG-IP interface that the Oracle Database Firewall network interface is connected.
5. From the **Mirrored Interfaces Available** list, select the BIG-IP interface where the client-to-database traffic exists, and then click the Add (<<) button to move it to the selected list.
6. Click **Update**.

The BIG-IP LTM is now configured to mirror database traffic to the Oracle Database Firewall. This completes the LTM configuration of Database Activity Monitoring mode.

Document Revision History

Version	Description	Date
1.0	New document	09-19-2012

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