Deploying the BIG-IP ASM with Oracle Database Firewall

Welcome to the F5 Deployment Guide for the F5 BIG-IP® Application Security Manager™ (ASM) with Oracle® Database Firewall. This guide provides instructions on configuring the BIG-IP ASM for unparalleled security for Oracle Database Firewall deployments.

The BIG-IP ASM and Oracle Database Firewall solution links a web application firewall with a database firewall. The two products share common reporting for web-based attempts to gain access to sensitive data, subvert the database, or execute Denial of Service (DoS) attacks against an organization's databases. Unified reporting for both the web application firewall and database firewall provides more convenient and comprehensive security monitoring.

When threats to data are detected, they are monitored, alerted, or blocked, and the identity of the user is shared between BIG-IP ASM and Oracle Database Firewall. Malicious or compromised users can be isolated, forced to re-authenticate, or prevented from accessing the application, in real time. Subsequent attacks from the same user can be prevented, diverted, or rendered inert.

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 ASM, see
http://www.f5.com/products/big-ip/application-security-manager.html

Products and versions tested

Product	Version
BIG-IP ASM	10.2.1 HF3 and 10.2.2, 11.1, 11.2
Oracle Database Firewall	5.0 BUNDLED PATCH 2 (Patch 12317493), 5.1

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-dg.pdf*

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 10.2.1 HF3 or a later version of 10.x.

➤ You must have the BIG-IP ASM licensed and provisioned on your BIG-IP system.

➤ For information on modifying the Oracle Database Firewall configuration for BIG-IP ASM, see *http://download.oracle.com/docs/cd/E20465_01/doc/doc.50/e18695/f5_big_ip.htm#CEGEHHBA*

➤ 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.

➤ The configuration in this guide assumes you are using the BIG-IP Local Traffic Manager (LTM) and BIG-IP ASM on the same box. If you are using a stand-alone BIG-IP ASM device, you can follow the ASM configuration, but without the LTM, you will lose certain LTM traffic management functionality.

➤ For information on configuring the BIG-IP LTM for intelligent traffic management for Oracle Database Firewall deployments, including both Database Policy Enforcement (inline) mode and Database Activity Monitoring mode, see *http://www.f5.com/pdf/deployment-guides/oracle-database-firewall-ltm-dg.pdf*.

Configuration example

Web traffic is secured by BIG-IP ASM and database traffic is secured by Oracle Database Firewall. Security events are correlated and available in consolidated reports.
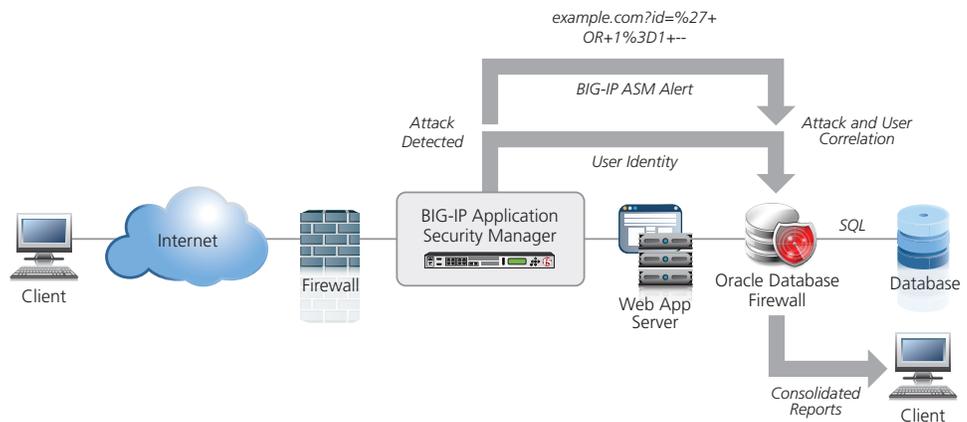

Figure 1: *Configuration example*

Configuring the BIG-IP ASM for Oracle Database Firewall

This section contains procedures for configuring the BIG-IP system for Oracle Database Firewall, as well as a example web application that resides in front of the Oracle Database Firewall and the Oracle database.

Important →

Before beginning the BIG-IP ASM configuration, be sure to follow the instructions provided by Oracle for modifying the Oracle Database Firewall configuration for BIG-IP ASM at:
http://download.oracle.com/docs/cd/E20465_01/doc/doc.50/e18695/f5_big_ip.htm#CEGEHHBA

Configuring the BIG-IP LTM for your Web application

In this section, we configure the BIG-IP LTM system for your web application. In the following procedures, we use a generic web application running on Oracle WebLogic as an example. You can modify the BIG-IP configuration objects, such as the health monitor and the profiles, to suit your particular application.

If you already have an existing BIG-IP LTM deployment for your applications and want to add the BIG-IP ASM configuration described in this guide, you must make the following changes:

- **Create a new HTTP Class profile**
  To use the BIG-IP ASM with an existing configuration, you must create a HTTP Class profile with **Application Security** set to **Enabled**. See *Creating the HTTP Class profile on page 6* for instructions. After creating the HTTP Class profile, you must modify the existing virtual server to reference the profile.

- **Create a new iRule**
  You must create an iRule and add it to the virtual server. This iRule monitors the login page and generates a syslog message each time a user logs into the Web application. The message is routed to the Oracle Database Firewall, which logs the user name against SQL statements generated by the Web application server.
  To create the iRule, see *Creating the iRule on page 6*. After creating the iRule, you must modify the existing virtual server to reference the iRule.

If you do not have an existing BIG-IP configuration, use the following procedures.

Creating the HTTP health monitor
The first step is to set up a health monitor for the web application. This procedure is optional, but very strongly recommended. In our example, we create a HTTP health monitor. Choose the monitor that best serves the needs of your application.

To create a health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.

2. Click the **Create** button. The New Monitor screen opens.

3. In the **Name** box, type a name for the Monitor. In our example, we type **http-monitor**.

4. From the **Type** list, select **http**.

5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a (1:3) +1 ratio between the interval and the timeout (for example, the default setting has an interval of 5 and an timeout of 16). In our example, we use a Interval of **30** and a Timeout of **91**.

6. Configure any of the other settings as applicable for your application.

7.   Click the **Finished** button. The new monitor is added to the Monitor list.

Creating the Pool
The next step is to define a load balancing pool for the application servers. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. This pool uses the monitor you just created.

To create the pool

1.   On the Main tab, expand **Local Traffic**, and then click **Pools**. The Pool screen opens.

2.   Click the **Create** button. The New Pool screen opens.

3.   From the **Configuration** list, select **Advanced**.

4.   In the **Name** box, type a name for your pool. In our example, we use **weblogic-pool**.

5.   In the **Health Monitors** section, select the name of the monitor you created, and click the Add (**<<**) button. In our example, we select **http-monitor**.

6.   In the **Slow Ramp Time** box, type **300**. We recommend setting a Slow Ramp Time in conjunction with the Least Connections load balancing method, as to not overwhelm any newly added servers.

7.   From the **Load Balancing Method** list, select a load balancing method. We recommend **Least Connections (node)**.

8.   In the New Members section, make sure the **New Address** option button is selected.

9.   In the **Address** box, type the IP address of one of your application servers.

10. In the **Service Port** box, type the appropriate Port.

11. Click the **Add** button to add the member to the list.

12. Repeat steps 8-10 for each server

13. Click the **Finished** button.

Creating profiles
The BIG-IP system use configuration objects called profiles. A profile is an object that contains user-configurable settings for controlling the behavior of a particular type of network traffic.

In this section, we provide procedures on configuring some common profiles used in our example WebLogic application.

Creating the HTTP profile
The first new profile we create is an HTTP profile. The HTTP profile contains numerous configuration options for how the BIG-IP LTM system handles HTTP traffic.

To create a new HTTP profile

1.   On the Main tab, expand **Local Traffic**, and then click **Profiles**.

2.   Click the **Create** button.

3.   In the **Name** box, type a name for this profile. In our example, we type **weblogic-http**.

4.   From the **Parent Profile** list, select **http**.

5.   Modify any of the other settings as applicable for your network, In our example, we leave the settings at their default levels.

6.   Click the **Finished** button.

Creating the TCP profiles

The next profiles we create are the TCP profiles. In our example, we create both WAN and LAN optimized TCP profiles.

To create the TCP profiles

1. On the Main tab, expand Local Traffic, and then click Profiles.
2. On the Menu bar, from the **Protocol** menu, click **TCP**.
3. Click the **Create** button.
4. In the **Name** box, type a name for this profile. In our example, we type **weblogic-tcp-lan**.
5. From the **Parent Profile** list, select **tcp-lan-optimized**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Repeat** button.
8. Type a unique name for this profile. We use **weblogic-tcp-wan**.
9. From the **Parent Profile** list, select **tcp-wan-optimized**.
10. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
11. Click the **Finished** button.

Creating the persistence profile

The next profile we create is a Persistence profile. Create this profile if your application requires persistence. In this example, we create a Cookie persistence profile.

To create a new persistence profile

1. On the Main tab, expand Local Traffic, and then click Profiles.
2. On the Menu bar, click **Persistence**.
3. Click the **Create** button.
4. In the **Name** box, type a name for this profile. In our example, we type **weblogic-cookie**.
5. From the **Persistence Type** list, select **Cookie**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating a OneConnect profile

The next profile we create is a OneConnect profile. While this profile is optional, with OneConnect enabled, client requests can use existing, server-side connections, thus reducing the number of server-side connections that a server must open to service those requests. For more information on OneConnect, see the BIG-IP LTM documentation.

To create a new OneConnect profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, from the **Other** menu, click **OneConnect**.
3. Click the **Create** button.
4. In the Name box, type a name for this profile. In our example, we type **weblogic-oneconnect**.

5. From the **Parent Profile** list, ensure that **oneconnect** is selected.

6. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.

7. Click the **Finished** button.

Creating the HTTP Class profile

In this procedure, we create an HTTP Class profile. The HTTP class only enables the Application Security option in the class, and does not enforce any actual ASM policies.

To create the HTTP class

1. On the Main tab, expand **Application Security**, and then click **Classes**.

2. Click the **Create** button.

3. In the **Name** box, type a name. In our example, we type **oracle-db-firewall**.

4. From the **Application Security** list, make sure **Enabled** is selected.

5. Configure any of the other settings as applicable for your configuration.

6. Click **Finished**.

Creating the iRule

You can use an iRule to monitor the login page and generate a syslog message each time a user logs into the Web application. The syslog message contains the username of the Web application user, and the cookies associated with that user. The message is routed to the Oracle Database Firewall, which logs the username against SQL statements generated by the Web application server.

This iRule contains the required format of the syslog message, but must be customized to handle the specific login requirements of your Web application.

Because of potential errors with copying and pasting the iRule from this pdf file, it is a downloadable text file. We recommend downloading the text file, making any modifications for your specific login requirements, and then copy and pasting the iRule onto the BIG-IP system.

Use this link to download the iRule:
http://www.f5.com/solution-center/deployment-guides/files/oracle-logging-irule.txt

To create the iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**.

2. Click the **Create** button.

3. In the **Name** box, type a name for this profile. In our example, we type **oracle-logging-irule**.

4. In the **Definition** section, copy and paste the iRule from the text file
    http://www.f5.com/solution-center/deployment-guides/files/oracle-logging-irule.txt.
    Be sure you have made any modifications based on your login requirements.

5. Click the **Finished** button.

Creating the virtual server

Next, we configure a virtual server that references the objects you created in the preceding procedures.

To create the virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this virtual server. In our example, we type **weblogic-virtual**.
4. In the **Address** box, type the IP address for this virtual server.
5. In the **Service Port** box, type the appropriate port.
6. From the **Configuration** list, select **Advanced**.
7. From the **Protocol Profile (Client)** list, select the WAN optimized TCP profile you created. In our example, we select **weblogic-tcp-wan**.
8. From the **Protocol Profile (Server)** list, select the LAN optimized TCP profile you created. In our example, we select **weblogic-tcp-lan**.
9. From the **OneConnect Profile** list, select the OneConnect profile you created. In our example, we select **weblogic-oneconnect**.
10. From the **HTTP Profile** list, select the HTTP profile you created. In our example, we select **weblogic-http**.
11. *Optional*: From the **SNAT Pool** list, select **Automap**. SNATs can simplify the configuration. For more information on SNAT, see the BIG-IP LTM documentation.
12. In the Resources section, from the **iRules**, **Available** box, select the iRule you created, and then click the Add (**<<**) button to move it to the Enabled list.
13. From the **HTTP Class Profiles** list, select the HTTP Class profile you created, and then click the Add (**<<**) button to move it to the Enabled list.
14. From the **Default Pool** list, select the pool you created in Creating the pool, on page 7. In our example, we select **weblogic-pool**.
15. From the **Default Persistence Profile** list, select the persistence profile you created. In our example, we select **weblogic-cookie**.
16. Click the **Finished** button.

This completes the BIG-IP LTM configuration. Continue with configuring the BIG-IP ASM on the following page.

Configuring the BIG-IP ASM

In this section, we configure the Web Application and Policy on the BIG-IP ASM.

Creating the Logging Profile
The first task in the ASM configuration is to create the Logging Profile. The logging profile contains information on where requests to the web application are logged (the Oracle Database Firewall), and which part of requests are logged.

To create the logging profile

1. On the Main tab, expand **Application Security**, and then click **Options**.
2. On the Menu bar, click **Logging Profiles**.
3. Click the **Create** button.
4. In the **Profile Name** box, type a name. In our example, we type **oracle-logging**.
5. Click the **Remote Storage** box.
6. In the **Server IP** box, type the IP address of the Oracle Database Firewall. This should be the same as the Destination IP you defined when configuring the Enforcement Point in your Oracle Database Firewall configuration.

    For information on setting up an Enforcement Point on your Oracle Database Firewall for the BIG-IP ASM, see: *http://download.oracle.com/docs/html/E18695_05/f5_big_ip.htm#CEGFIFEA*
7. In the **Server Port** box, type **5514**. This should be the same as the Destination Port you defined when configuring the Enforcement Point in your Oracle Database Firewall configuration.
8. In the **Storage Format** section, from the **Available Items** box, select each of the following items one at a time, and then click the Add (<<) button after each.

    Important ➝ *It is critical that these items are in the order below.*

    a. violations

    b. unit_hostname

    c. management_ip_address

    d. policy_name

    e. policy_apply_date

    f. x_forwarded_for_header_value

    g. support_id

    h. request_status

    i. response_code

    j. method

    k. protocol

    l. uri

    m. query_string

    n. ip_client

    o. *For BIG-IP ASM v10*: web_application_name
       For BIG-IP ASM v11: http_class_name

    p. request

9. Click the **Create** button.

Configuring the Web Application and Security Policy
The next task is to configure the Web Application with a Security policy. When you created the
HTTP Class profile, the BIG-IP ASM automatically creates a Web Application with the same name.

To configure the Web Application and Security Policy

1. On the Main tab, expand **Application Security**, and then click **Web Applications**.

2. From the **Web Application** List, locate the Web Application for this application. The Web
    Application has the same name as your HTTP Class Profile. In our example, it is
    oracle-db-firewall.

    In the **Active Security Policy** column, click the **Configure Security Policy** link.

3. In the **Deployment Scenarios** section, click **Manual Deployment**, and then click the
    Next button.

4. From the **Application Language** list, select an application language.

5. From the **Application-Ready Security Policy** list, select **Rapid Deployment security
    policy (http)**.

6. Click **Next**.

7. In the **Systems** section, from the **Available Systems** list, select **Oracle** and then click the
    Add (**<<**) button to move it to Assigned Systems. If your web/application server is present in
    the Available Systems list, also select it and then click the Add button. In our example, we
    also select **BEA Systems WebLogic Server**.

8. Make sure the **Enable Signature Signing** box is checked.

9. Click **Next**.

10. Click **Finished**. The Properties page of the Policy opens.

11. On the Menu bar, click **Blocking**, and then click **Settings**.

12. In the Configuration section, we recommend you leave the **Enforcement mode** set to
    Transparent until you have had a chance to review the configuration and make any
    necessary changes before switching to Blocking.

13. We recommend you enable the following required events to send through the syslog. For
    each of the following events, click a check in the **Learn** and **Alarm** boxes.

    RFC Violations section

    a. **Evasion technique detected**

    Access Violations section

    a. **Request length exceeds defined buffer size**

    b. **Illegal HTTP status in response**

    Input Violations section

    a. **Illegal dynamic parameter value**

    b. **Illegal meta character in header**

    c. **Illegal meta character in parameter value**

    d. **Illegal parameter data type**

     e. **Illegal parameter numeric value**

     f. **Illegal parameter value length**

     g. **Illegal query string or POST data**

     h. **Illegal static parameter value**

     i. **Parameter value does not comply with regular expression**

Negative Security Violations section

     a. **Attack signature detected**

14. Click the **Save** button.

Configuring the Security policy to use the Logging policy

The next task is to configure the Security policy to use the logging profile you created.

To configure the policy to use the logging profile

1. On the Main tab, expand **Application Security**, and then click **Web Applications**.

2. From the **Web Application** List, click the Web Application you created. The Web Application has the same name as your HTTP Class Profile. In our example, it is **oracle-db-firewall**.

3. From the **Logging Profile** list, select the name of the Logging profile you created in *Creating the Logging Profile on page 8*.

4. Click the **Update** button.

Applying the Security policy

Use the following procedure to apply the Security policy.

To apply the policy

1. On the Main tab, expand **Application Security**, and then click **Web Applications**.

2. From the **Web Application** List, click the Web Application you created.

3. Click the **Apply Policy** button.

Configuring syslog-ng.conf

To enable the iRule syslog messages to be transmitted to the Oracle Database Firewall, it is necessary to log in to the BIG-IP command line and execute the following BIG-IP ASM command, which modifies **/etc/syslog-ng /syslog-ng.conf** (do not modify the file directly, because changes will not persist after you restart the system):

To configure syslog-ng.conf

1. On the BIG-IP system, start a console session. Log on as **root**.

2. You can either use bigpipe or TMSH to enable iRule syslog messages to be transmitted to the Oracle Database Firewall. Use the appropriate command syntax (all on one line), replacing the red text as noted below:

a. __bigpipe__:

```
bigpipe syslog include '"destination d_dbfw { tcp(\"dbfw_ip_
address\" port(dbfw_port));};log { source(local); filter(f_local3);
destination(d_dbfw);};"'
```

Where __*dbfw_ip_address*__ and __*dbfw_port*__ are the IP address and port number of the Oracle Database Firewall. This should be the same IP address and port of the server you specified in Steps 6 and 7 of *Creating the Logging Profile on page 8.*
In our example, the command is:

```
bigpipe syslog include '"destination d_dbfw { tcp(\"192.168.0.181\"
port(5514));};log { source(local); filter(f_local3); destination(d_dbfw);};"'
```

The two instances of the syslog destination name (d_dbfw) need to be changed only in the unlikely event that the destination name is already in use. The port number is normally 5514.

b. __TMSH__

```
modify sys syslog remote-servers add {<dbfw_server_name> {host <dbfw_
IP_address> remote-port <dbfw_port>}}
```

Where __*dbfw_server_name*__ is the name of your server, and __*dbfw_IP_address*__ and __*dbfw_port*__ are the IP address and port number of the Oracle Database Firewall. This should be the same IP address and port of the server you specified in Steps 6 and 7 of *Creating the Logging Profile on page 8.*

In our example, the command is:

```
modify sys syslog remote-servers add { d_dbfw {host 192.168.0.181 remote-port
5514}}
```

You must also save the change to the system configuration using the following command:

```
save sys config
```

For more information on syslog TMSH commands, please see Support Solution # SOL13083 on support.f5.com.:
http://support.f5.com/kb/en-us/solutions/public/13000/000/sol13083.html?sr=18091813

This completes the configuration.

Document Revision History

Version	Description	Date
1.0	New deployment guide	08-05-2011
1.1	Added a TMSH command option to *Configuring syslog-ng.conf on page 10.*	12-15-2011
1.2	- Added support for BIG-IP ASM version 11.1 and 11.2. - Added a link in the prerequisites section to the BIG-IP LTM deployment guide for Oracle Database firewall.	09-19-2012
1.3	Added a new Storage Format value to Step 8-o of the Logging Profile configuration for BIG-IP ASM version 11.0.	09-21-2012