



Deploying the BIG-IP System with Oracle E-Business Suite 11i

- Introducing the BIG-IP and Oracle 11i configuration
- Configuring the BIG-IP system for deployment with Oracle 11i
- Configuring the BIG-IP system for Oracle 11i deployments with SSL traffic
- Appendix A: Backing up and restoring the BIG-IP system configuration

Introducing the BIG-IP and Oracle 11i configuration

Oracle and F5 have developed an effective way to direct traffic for Oracle E-Business Suite 11i deployments using the BIG-IP application traffic management device. When deployed with Oracle 11i, the BIG-IP product ensures fast delivery, always-on access, peak security and easy expansion for applications running on Oracle.

With Oracle E-Business Suite 11i and F5 Networks award-winning application traffic management products, enterprises achieve increased security, higher uptime and better performance from their Oracle-based applications, while increasing the return on investment of their e-business infrastructures.

For more information on the BIG-IP system, see <http://www.f5.com/products/big-ip/>.

For more information on the Oracle E-Business Suite 11i, see <http://www.oracle.com/applications/home.html>

Prerequisites and configuration notes

The following are prerequisites for this Deployment Guide:

- ◆ You must have an Oracle 11i deployment running version 11.5.9 or later, with the latest recommended patches.
- ◆ You have configured your Oracle 11i deployment according to the procedures outlined in Option 2.2, **HTTP Layer Hardware Load Balancing**, of the following Oracle MetaLink document:

http://metalink.oracle.com/metalink/plsql/ml2_documents.showFrameDocument?p_database_id=NOT&p_id=217368.1

You need a MetaLink user account to access this file. If you do not have an account, contact Oracle.

- ◆ The BIG-IP system must be running version 4.5 or later (the step-by-step configuration procedures in this Deployment Guide are for 4.5 or later, but do not include configuration steps for BIG-IP version 9.0 and later).
- ◆ Briefly review the basic configuration tasks and the few pieces of information, such as IP addresses, that you should gather in preparation for completing the BIG-IP system configuration.

◆ Note

All of the configuration procedures in this Deployment Guide are performed on the BIG-IP system. For specific information on how to configure Oracle 11i, consult the Oracle Documentation.

This document is written with the assumption that you are familiar with both the BIG-IP system and Oracle 11i. For more information on configuring these products, consult the appropriate documentation.

Configuration example

The BIG-IP system provides intelligent traffic management and high availability for Oracle 11i deployments. Through advanced health checking capabilities, the BIG-IP product recognizes when resources are unavailable or under-performing and directs traffic to another resource. The BIG-IP device tracks Oracle end-user sessions, which ensures the client maintains session state with the servers. The following diagram shows an example deployment with Oracle 11i and the BIG-IP system.

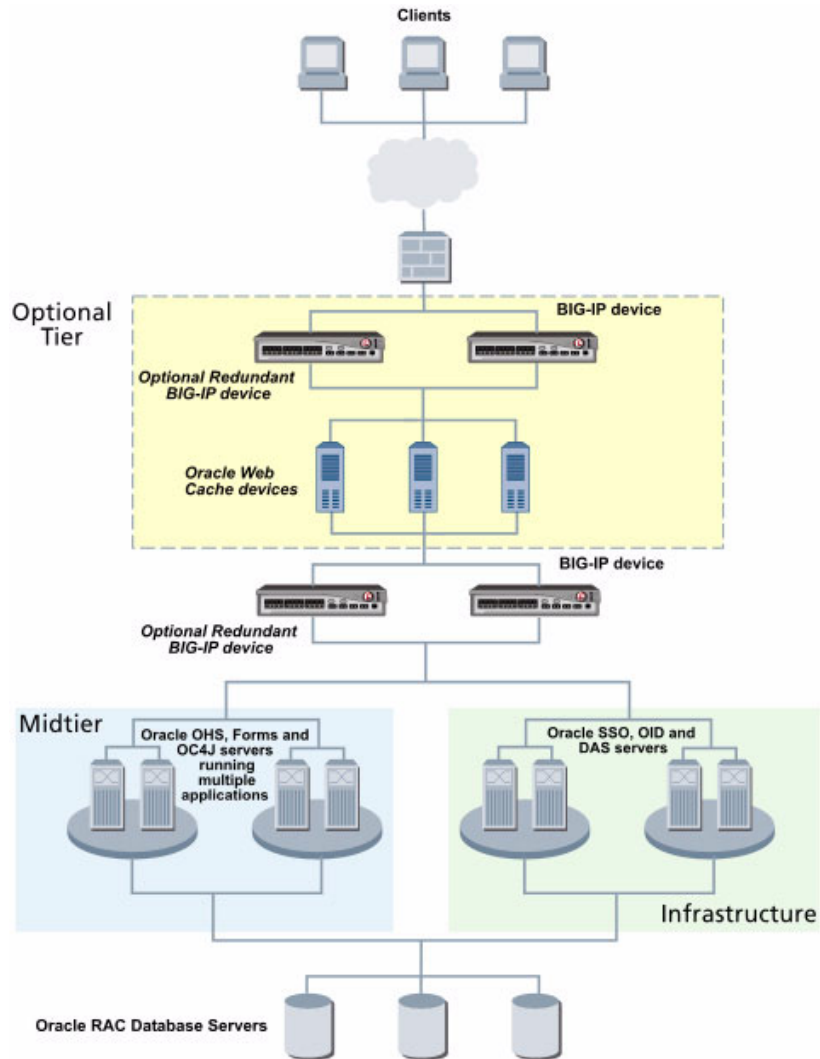


Figure 1.1 BIG-IP Oracle 11i configuration example

Configuring the BIG-IP system for deployment with Oracle 11i

To configure the BIG-IP for directing traffic to the Oracle devices, you need to complete the following procedures:

- *Connecting to the BIG-IP device*
- *Creating the pool*
- *Creating the HTTP virtual server*
- *Configuring a health monitor*
- *Synchronizing the BIG-IP configuration if using a redundant system*

◆ Important

*If your Oracle 11i deployment uses SSL, follow the procedures in **Configuring the BIG-IP system for Oracle 11i deployments with SSL traffic**, on page 1-11.*

The BIG-IP system offers both web-based and command line configuration tools, so that users can work in the environment that they are most comfortable with. This Deployment Guide contains procedures to configure the BIG-IP system using the BIG-IP web-based Configuration utility only. If you are familiar with using the **bigpipe** command line interface you can use the command line to configure the BIG-IP device, however, we recommend using the Configuration utility.

◆ Tip

*We recommend you save your existing BIG-IP configuration before you begin the procedures in this Deployment Guide. To save your BIG-IP configuration, see **Appendix A: Backing up and restoring the BIG-IP system configuration**, on page 1-15.*

Connecting to the BIG-IP device

The first step in this configuration is to connect to the BIG-IP system. Use the following procedure to access the BIG-IP web-based Configuration utility using a web browser.

To connect to the BIG-IP system using the Configuration utility

1. In a browser, type the following URL:
https://<administrative IP address of the BIG-IP device>
A Security Alert dialog box appears, click **Yes**.
The authorization dialog box appears.
2. Type your user name and password, and click **OK**.
The Configuration Status screen opens.

Once you are logged onto the BIG-IP system, the initial screen, called the Configuration Status page, displays. From the Configuration status page, you can access the Configuration utility, documentation such as manuals and release notes, and software downloads.

3. From the Configuration Status screen, click **Configure your BIG-IP (R) using the Configuration utility**.
The Configuration utility opens to the Network Map screen.

Creating the pool

The first procedure in this configuration is to configure a pool for the Oracle devices. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. In this Deployment Guide, we configure one pool for our Oracle devices. For this pool, we use cookie persistence, Insert mode, the recommended persistence method for Oracle E-Business Suite.

To create the pool from the Configuration utility

1. In the navigation pane, click **Pools**.
The Pools screen opens.
2. Click the **Add** button.
The Add Pool screen opens.
3. In the **Pool Name** box, enter a name for your pool.
In our example, we use **oracle_http**.
4. In the **Load Balancing Method** box, enter your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
In our example, we select **Predictive (member)**, where connections are sent to a node based on a combination of the number of current connections and the response time of the node over time.
5. In the **Resources** section, you add the web servers to the pool.
 - a) In the **Member Address** box, type the IP address of the Oracle server. In our example, we type **150.150.150.7**.
 - b) In the **Service** box, type the service number you want to use for this device, or specify a service by choosing a service name from the list (for example **8000**).
In our example, we type **8000**, the default Oracle 11i server port.
 - c) The **Member Ratio** and **Member Priority** boxes are optional.
 - d) Click the Add button (>>) to add the member to the **Current Members** list.
 - e) Repeat steps a-d for each server you want to add to the pool. In our example, we repeat these steps twice for the other servers (**150.150.150.8 and .9**). See Figure 1.2.

6. The other fields in the Add Pool screen are optional. Configure these fields as applicable for your network. (For additional information about configuring a pool, click the **Help** button.)
7. Click the **Done** button.

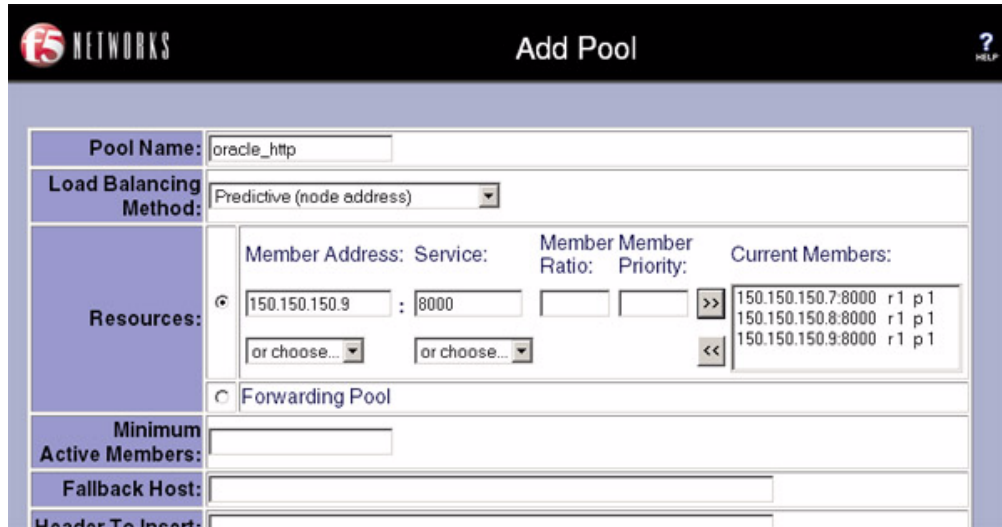


Figure 1.2 Adding the members to the *oracle_http* pool in the BIG-IP Configuration utility

8. In the Pool screen, from the Pool Name list, click the name of the pool you just created.
In our example, we click **oracle_http**.
9. Click the Persistence tab.
The Persistence screen for the pool opens.
10. In the Persistence Type section, click the option button for **Active HTTP Cookie**.
11. From the Method list, select **Insert**.
12. In the **Expiration** box, type an expiration for the cookie. In our example we type 30 in the **Minutes** box.
***Important:** The cookie expiration should be at least equal to the application session timeout for the Oracle 11i servers. The default application session timeout is 30 minutes. You could also leave the Expiration blank, and the cookie will expire when the browser is closed.*
13. Click the **Apply** button.

The screenshot shows the configuration interface for a pool named 'oracle_http'. The 'Persistence Type' section is expanded, and 'Active HTTP Cookie' is selected. The 'Method' dropdown is set to 'Insert', and the 'Expiration' is set to 30 minutes. Other options like 'None', 'SSL', 'SIP', 'Simple', 'Destination Address Affinity', 'Expression', and 'Passive HTTP Cookie' are also visible.

Figure 1.3 Configuring active cookie persistence, Insert mode

Creating the HTTP virtual server

The next step in this configuration is to define a virtual server that references the pool you just created.

To create the HTTP virtual server using the Configuration utility

1. In the navigation pane, click **Virtual Servers**.
The Virtual Servers screen opens.
2. Click the **Add** button.
The Add Virtual Server screen opens.
3. Enter the IP address and service for the virtual server, then click the **NEXT** button.
In our example, we use **192.168.200.10** with service of **80**. The Configure Basic Properties screen displays.
Click the **Next** button again.

- Click the **Pool** option button, and from the list, select the pool you created in the *Creating the pool* section.
In our example, we select **oracle_http** (see Figure 1.4).

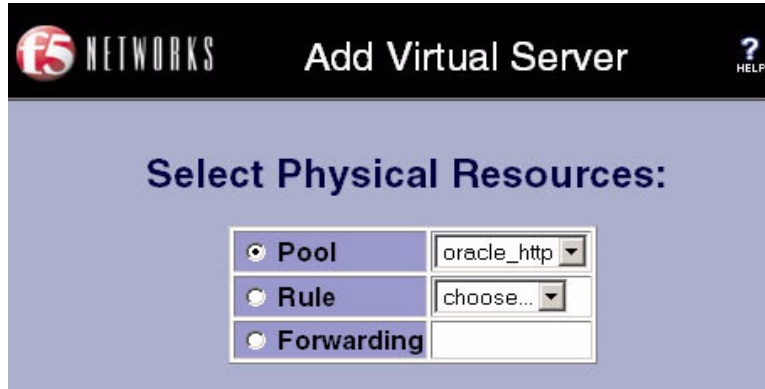


Figure 1.4 Selecting the `oracle_http` pool while creating the virtual server

- Click the **Done** button. For additional information about configuring a virtual server, click the **Help** button.

To view the virtual server, click the virtual server in the list. In our example, the virtual server properties are shown in Figure 1.5.

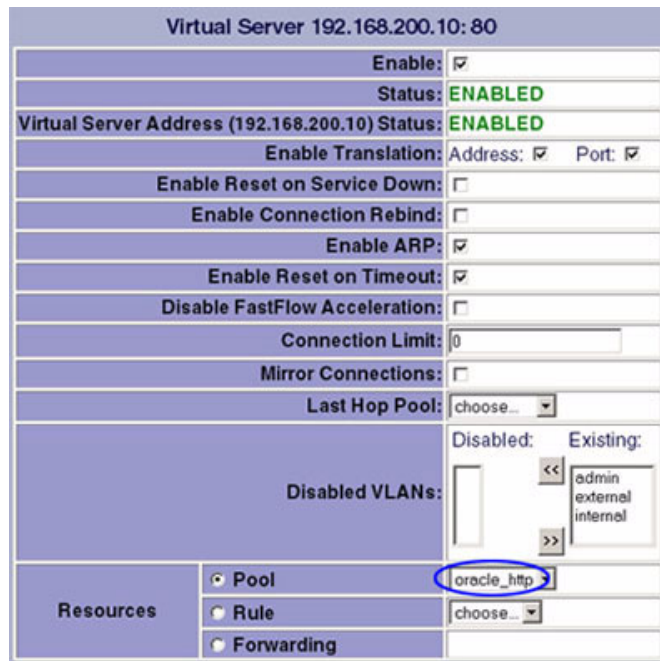


Figure 1.5 The HTTP virtual server in the BIG-IP Configuration utility.

Configuring a health monitor

We recommend you configure at least an ICMP health monitor for all the Oracle devices in this configuration. If you want to configure more advanced monitors for specific devices, we recommend using the template for the HTTP Extended Content Verification (ECV) monitor. The HTTP ECV monitors nodes (IP address and port combinations), and can be configured to use **send** and **recv** statements in an attempt to retrieve explicit content from nodes. The following procedures show you how to configure both the ICMP and ECV monitors.

To configure an ICMP health monitor using the BIG-IP Configuration utility.

1. In the navigation pane, click **Monitors**.
The Network Monitors screen opens.
2. From the Network Monitors screen, click the Basic Associations tab.
The Basic Association screen opens.
3. In the **Node Address** section, from the list, select **ICMP**.
4. In the **Node** column, locate the Oracle node addresses, and click a check in the **Add** box for each node address.

In our example, we check the Add box for all of the Oracle nodes.

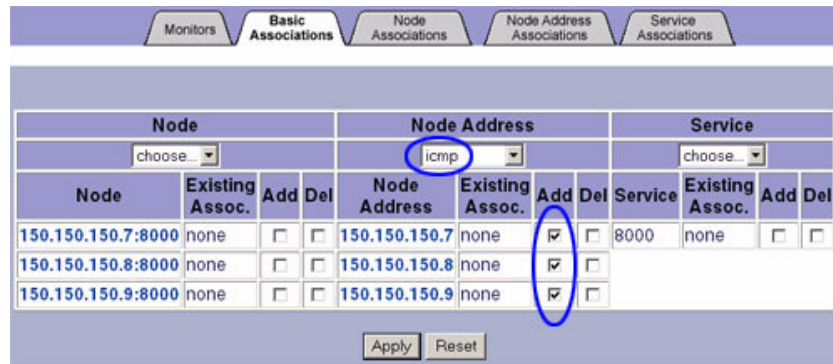


Figure 1.6 Associating the ICMP monitor with the nodes

5. Click **Apply**.
You now see the **ICMP** in the Existing Associations column of the **Node Address** section for each of the Oracle devices. (see Figure 1.7).

For additional information associating a monitor, click the **Help** button.

Node Address			
choose... ▾			
Node Address	Existing Assoc.	Add	Del
150.150.150.7	icmp	<input type="checkbox"/>	<input type="checkbox"/>
150.150.150.8	icmp	<input type="checkbox"/>	<input type="checkbox"/>
150.150.150.9	icmp	<input type="checkbox"/>	<input type="checkbox"/>

Figure 1.7 Nodes associated with the ICMP monitor

You can now configure the optional HTTP ECV monitor. In this example, we configure an HTTP ECV monitor for the Oracle devices.

To configure the ECV monitor

1. In the navigation pane, click **Monitors**.
The Network Monitors screen opens.
2. Click the **Add** button.
The Add Monitor dialog box opens.
3. In the Add Monitor screen, type the name of your monitor (it must be different from the monitor template name), in our example, we type **oracle_apps_monitor**.
In the **Inherits From** box, select the **http** monitor template from the list. Click the **Next** button.

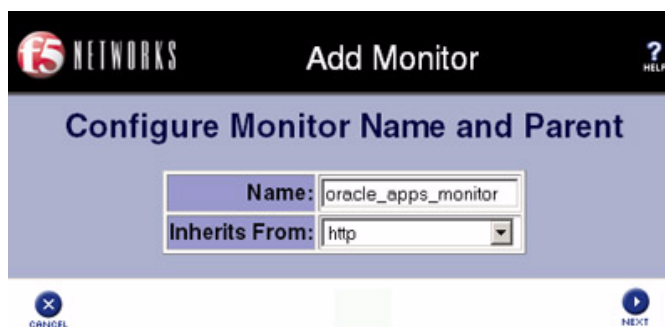


Figure 1.8 Creating the monitor in the BIG-IP Configuration utility

4. In the Configure Basic Properties section, type an **Interval** and **Timeout** value. 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**). We recommend a slightly higher ratio. In our example, we enter **30** for the Interval and **91** for the Timeout.
Click the **Next** button.
The Configure ECV HTTP Monitor screen opens.

5. In the Configure ECV HTTP Monitor screen, you can add a Send String and Receive Rule specific to that application. Complete the relevant information, and click the **Done** button.
The Add Monitor dialog box closes, and you return to the Network Monitors screen.
6. From the Network Monitors screen, click the Basic Associations tab.
The Basic Association screen opens.
7. In the **Node** section, from the list, select the name of the monitor you created in Step 3. In our example, we select **oracle_apps_monitor**.
8. In the **Node** column, locate the Oracle nodes relevant to this monitor, and click a check in the **Add** box for each node.

In our example, we check the **Add** box for **150.150.150.7:8000**, **150.150.150.8:8000**, and **150.150.150.9:8000**.
9. Click **Apply**.
You now see the **oracle_apps_monitor** in the Existing Associations column of the **Node** section for each of the Oracle devices.

For additional information associating a monitor, click the **Help** button.

Synchronizing the BIG-IP configuration if using a redundant system

If you are using a redundant BIG-IP configuration, the final step is to synchronize the configuration to the peer BIG-IP device.

To synchronize the configuration using the Configuration utility

1. In the navigation pane, click **System**.
The Network Map screen opens.
2. Click the Redundant Properties tab.
The Redundant Properties screen opens.
3. Click the **Synchronize Configuration** button.

To synchronize the configuration from the command line

Synchronize the configuration from the command line using the **bigpipe config sync** command:

```
bigpipe config sync all
```

The **bigpipe config sync all** command synchronizes the following configuration files:

- The common **bigdb** keys
- All files in **/config** (except **bigip_base.conf**)

Use the **bigpipe config sync** command without the all option to synchronize only the boot configuration file **/config/bigip.conf**.

Configuring the BIG-IP system for Oracle 11i deployments with SSL traffic

If your Oracle E-Business Suite 11i deployment requires SSL, the configuration on the BIG-IP system is slightly different. For Oracle 11i deployments using SSL, you need to configure an SSL proxy and a loopback virtual server on the BIG-IP system, in addition to creating the pool and health monitor.

◆ Note

If you are not using SSL in your deployment, you do not need to perform this part of the deployment.

◆ Important

*To prepare your Oracle 11i deployment for load balancing SSL, you must follow the procedures outlined in Option 2.2, **HTTP Layer Hardware Load Balancing**, of the following Oracle MetaLink document:*

http://metalink.oracle.com/metalink/plsql/ml2_documents.showFrameDocument?p_database_id=NOT&p_id=217368.1

Specifically, option 2.2.3 contains steps relevant to the SSL accelerator.

To configure the BIG-IP for directing SSL traffic to the Oracle devices, you need to complete the following procedures from the first section of this document:

- *Connecting to the BIG-IP device*, on page 1-3
- *Creating the pool*, on page 1-4
- *Configuring a health monitor*, on page 1-8
- *Synchronizing the BIG-IP configuration if using a redundant system*, on page 1-10

And then the following additional procedures:

- *Creating the loopback virtual server for the SSL proxy*, on page 1-12
- *Creating the SSL proxy*, on page 1-12

Creating the loopback virtual server for the SSL proxy

The SSL proxy uses a loopback virtual server for the SSL proxy. To create this loopback virtual server, use the following steps.

◆ Note

Before you configure the virtual server, you must have already configured the pool (see [Creating the pool](#), on page 1-4).

To create the loopback virtual server

1. In the navigation pane, click **Virtual Servers**.
The Virtual Servers screen opens.
2. Click the **Add** button.
The Add Virtual Server screen opens.
3. Enter the IP address and service for the loopback virtual server, then click the **NEXT** button.
In our example, we use **127.0.0.51** with service of **8000**. The Configure Basic Properties screen displays.
Click the **Next** button again.
4. Click the **Pool** option button, and from the list, select the pool you created in the *Creating the pool* section.
In our example, we select **oracle_http**.
5. Click the **Done** button. For additional information about configuring a virtual server, click the **Help** button.

To view the virtual server, click the virtual server in the list.

For more information on configuring the proxy addresses, refer to the ***BIG-IP Reference Guide***.

Creating the SSL proxy

The next step is to create an SSL proxy. An SSL proxy is a gateway for decrypting HTTP requests to an HTTP server and encrypting the reply. The SSL proxy on the BIG-IP system offloads the task of SSL encryption/decryption from the server, which frees processing cycles for those servers, and provides a central location for certificate management.

◆ Important

Before creating the SSL proxy on the BIG-IP system, you should have a certificate issued by a recognized certificate authority. The applet used by Oracle 11i does not work with the BIG-IP device's self-signed certificates.

To create an SSL proxy from the Configuration utility

1. From the navigation pane, click **Proxies**.
The Proxies screen opens.

2. Click the **Add** button.
The Add Proxy screen appears.
3. In the Proxy Type section, click a check in the SSL box.
4. In the **Proxy Address** box, type the originating (source) IP address. This must be a valid IP address or host name. For a web site, use the registered address to which your clients connect. In our example, we use **192.168.20.51**.
5. In the Proxy Service box, type **https**, or choose **https** from the list.
6. In the **Destination Address** box, type the address of the loopback virtual server you created in the *Creating the loopback virtual server for the SSL proxy* section. In our example, we type **127.0.0.51**.
7. In the **Destination Service** box, type the same port you used for the pool in the *Creating the pool* section on page 1-4. In our example, we type **8000**.
8. In the **SSL Certificate** box, type the name of the SSL certificate for the server, or select it from the list.
9. In the **SSL Key** box, type the SSL key for the server, or select it from the list of installed keys. It is very important that you choose the key that you used to create the certificate you selected in the SSL Certificate box.

Figure 1.9 Adding the SSL proxy

10. Click the **Next** button.
11. From the **Rewrite Redirects** list, select **All**. When you select **All**, the proxy always rewrites URIs as if they matched the originally requested URIs.
12. The other fields in the Add Proxy window are optional. Configure these fields as applicable for your network. (For additional information about configuring a Proxy, click the **Help** button.)
13. Click the **Done** button to add the Proxy.

◆ **Note**

*If you have not already done so, you must follow the procedures outlined in Option 2.2, **HTTP Layer Hardware Load Balancing**, of the following Oracle MetaLink document:*

http://metalink.oracle.com/metalink/plsql/ml2_documents.showFrameDocument?p_database_id=NOT&p_id=217368.1

Specifically, option 2.2.3 contains steps relevant to the SSL accelerator.

◆ **Important**

*Be sure to perform the procedures **Configuring a health monitor**, on page 1-8, and **Synchronizing the BIG-IP configuration if using a redundant system**, on page 1-10 before finishing the configuration.*

Appendix A: Backing up and restoring the BIG-IP system configuration

We recommend saving your BIG-IP configuration before you begin this configuration. When you save the BIG-IP configuration, it collects the following critical data and compresses it into a single User Configuration Set (UCS) file:

- BIG-IP configuration files
- BIG-IP license and passwords
- SSL certificates
- SSH keys

Saving up and restoring the BIG-IP configuration using the Configuration utility

The Configuration Management screen allows you to save and restore all configuration files that you may edit to configure a BIG-IP system. These configuration files are called a User Configuration Set (UCS). The Configuration Management screen contains sections for saving and restoring a configuration. The list boxes in these sections display only files in the `/usr/local/ucs` directory. If you want to save or restore files from another directory, you must type the full path in the box.

To save the BIG-IP configuration using the Configuration utility

1. In the navigation pane, click **System Admin**.
The User Administration screen displays.
2. Click the Configuration Management tab.
The Configuration Management screen displays.
3. In the **Save Current Configuration** section, type the path where you want your configuration file saved or choose a path from the list box. If no path is specified, the BIG-IP saves files to `/usr/local/ucs`. The BIG-IP appends the extension `.ucs` to file names without it. In our example, we type **pre_oracle_backup.ucs**.
4. Click the **Save** button to save the configuration file.

To restore a BIG-IP configuration using the Configuration utility

1. In the navigation pane, click **System Admin**.
The User Administration screen displays.
2. Click the Configuration Management tab.
The Configuration Management screen displays.

3. In the **Restore a Configuration** section, choose the configuration file you want to restore from the list box, or type the path where your configuration files were saved.
4. Click the **Restore** button.
To check the status of the restoration, click the **View Log** button. You should wait a few moments for the log file to start generating before you click **View Log**. Repeated clicking of this button will update your screen with the most current log file information until the restoration is complete.