Deploying the BIG-IP System v10.1 with SAP NetWeaver and Enterprise SOA: Enterprise Portal

Table of Contents

Deploying the BIG-IP WOM with SAP NetWeaver and Enterprise SOA

I

Deploying F5 with SAP NetWeaver and Enterprise SOA

Introducing the F5 SAP NetWeaver and Enterprise SOA configuration

Welcome to the F5 deployment guide for SAP® NetWeaver® and Enterprise SOA. This guide gives you step-by-step procedures on how to configure the BIG-IP system v10.1 with SAP Enterprise Portal deployments.

By taking advantage of this Application Ready infrastructure for SAP deployments organizations can achieve a secure, fast and available network infrastructure that reduces the total cost of operation and increases ROI.

SAP NetWeaver Portal unifies key information and applications to give users a single view that spans IT silos and organizational boundaries. It allows you to take full advantage of all your information resources – and maximize the return on your IT investments. And, its predefined business content accelerates implementation and reduces the cost of integrating your existing systems.

This guide contains the following chapters:

- *Configuring the SAP Enterprise Portal for load balancing with the BIG-IP LTM system*, on page 1-3

- *Configuring the F5 WebAccelerator module with SAP Enterprise Portal*, on page 2-1

- *Deploying the BIG-IP Edge Gateway with SAP NetWeaver and Enterprise SOA*, on page 3-1

- *Deploying the BIG-IP WOM with SAP NetWeaver and Enterprise SOA*, on page 4-1

The WebAccelerator, Edge Gateway, and WOM (WAN Optimization module) are all optional.

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

Prerequisites and configuration notes

All of the procedures in this Deployment Guide are performed on the BIG-IP system. The following are prerequisites for this solution:

- We recommend using the latest version of SAP NetWeaver and mySAP Business Suite applications. Our testing environment included both SAP ERP 6.0 based on NetWeaver 7.0 and SAP NetWeaver 2004 and mySAP ERP 2005. High availability was configured for Enterprise Portal and Composite Services on the front end along with Exchange Infrastructure (XI) now renamed to Process Integration (PI), Business Warehouse (BW), and SAP ERP Central Component (ECC).

- This document is written with the assumption that you are familiar with both F5 devices and SAP products. For more information on configuring these devices, consult the appropriate documentation.

◆ Make a list of the IP addresses and ports used by each SAP application component in your deployment, as these are used in the F5 configuration. Consult the SAP documentation and your SAP administrator for this information.

◆ For this deployment guide, the BIG-IP LTM system must be running version 10.1 or later. If you are using a previous version of the BIG-IP LTM system, see the *Deployment Guide* index.

◆ If you are using the BIG-IP system to offload SSL, we assume you have already obtained an SSL certificate and key, but it is not yet installed on the BIG-IP LTM system. For more information, see *Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment*, on page 1-35.

Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP System (LTM, WebAccelerator, Edge Gateway, WAN Optimization module)	10.1, 10.2.1
SAP ERP	6.0 (based on NetWeaver 7.0)
SAP NetWeaver	7.0 and NetWeaver 2004
mySAP ERP	2007

Revision history:

Document Version	Description
1.0	New deployment guide
1.1	Added advanced health monitor to LTM configuration. See *Using an advanced health monitor*, on page 1-14.
1.2	- Added Application Template configuration and moved manual LTM configuration to an Appendix A on page 1-23. - Added new health monitor and instructions for configuring the BIG-IP for dynamic load balancing based on CPU, memory and disk utilization.

Configuring the SAP Enterprise Portal for load balancing with the BIG-IP LTM system

This section contains a brief description of how to create a new *System* within SAP EP using the load balancing template that allows the BIG-IP LTM system to load balance the SAP devices.

◆ **Important**

This is just an overview of some of the SAP configuration details related to load balancing. For more detailed instructions on configuring your SAP solution, see the SAP documentation or contact SAP.

To create a new SAP System

1. Log on to the SAP Enterprise Portal (EP).

2. On the Menu bar, click **System Administration**, and then click **System Configuration**.

3. In the Detailed Navigation pane, click **System Landscape**.

4. Expand **Portal Content**, and then the name of your company/portal.

5. Right click **Systems**. From the Systems menu, select **New**, and then **System (from template)**. See Figure 1.1.
    You create a new System for each non EP SAP application type. The System Wizard opens.
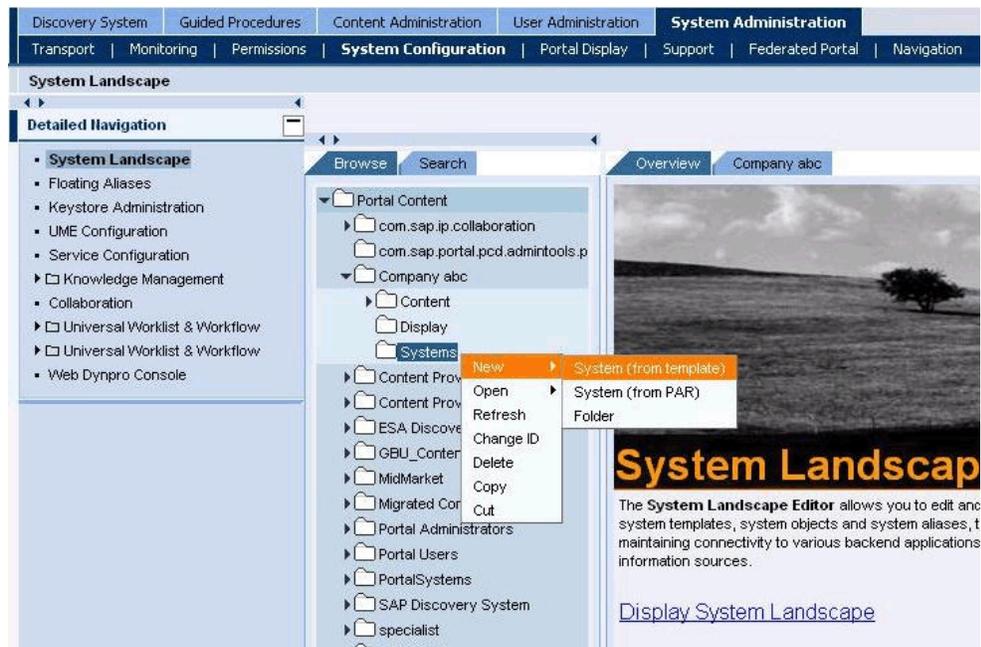
Figure 1.1 Creating a new System in the SAP Enterprise Portal

6. From the System Wizard, Template Selection, select **SAP system with load balancing** (you may need to scroll down to see this option depending on your installation). See Figure 1.2. Click the **Next** button.
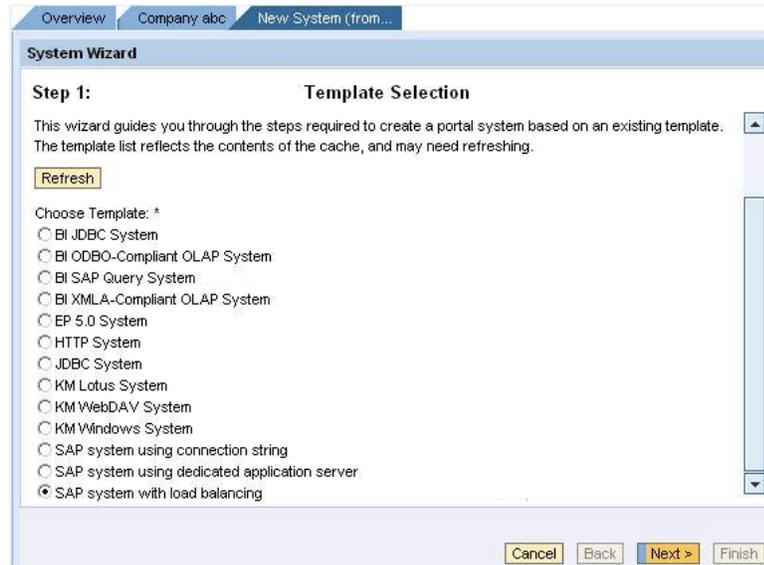
Figure 1.2 *Selecting the load balancing option from the System wizard*

7. In the General Properties step, enter the following information (see Figure 1.3):

   a) In the **System Name** box, type a name for this system, using the following syntax: **SAP <System Type> <System Name>**
   In our example, we type **SAP ECC**.

   b) In the **System ID** box, type a system ID, using the following syntax: **sap_<system id>**
   In our example, we type **sap_ecc**.

   c) In the **System ID** Prefix box, type a system ID using a prefix from the SAP deployment guidelines (**com.<companyname>.erp.ops.sys**). In our example, we type **com.companyabc.erp.ops.sys**.

   d) From the **Master Language** list, select a language. In our example, we select **English**.

   e) In the **Description** box, you can type an optional description of this system.

8. Click the **Next** button.
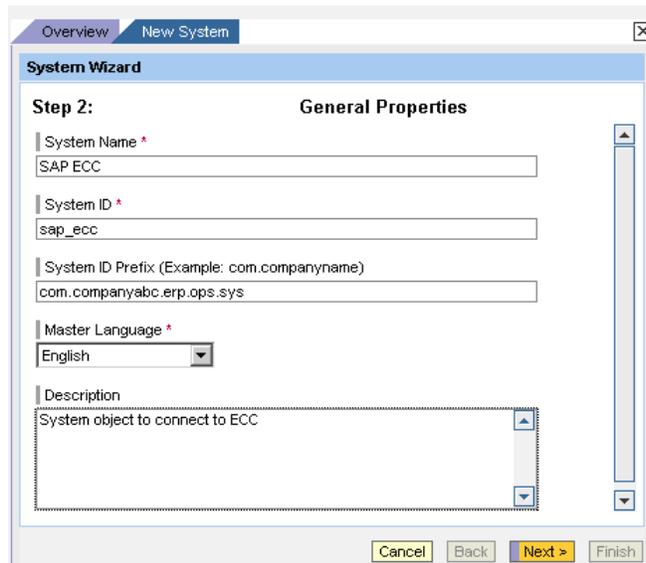
Figure 1.3 *Entering the General properties of the system*

9. Review the Summary screen. To accept your entries, click **Finish**.

10. In the **Choose your next step** menu, select **Open object for editing** and click **OK**.

11. Complete the Property Editor based on the table on the following page.

Property	Value	Example
Group	<Group ID>	ECC_PRD_01
ITS Host Name	<Load-balanced ITS server host name>:**80**<System #>	Gerp.ecc.site.com:8050 ***see warning below**
ITS Path	<Path to ITS home>	/sap/bc/gui/sap/its/
ITS Protocol	"http" or "https"	http
Logical System Name	<System ID>CLNT<System #>	RP1CLNT030
Message Server	<System message server>	usri-pdbx-c01.site.com
SAP Client (*)	<SAP Client>	030
SAP System ID	<System ID>	RP1
Server Port	36<System #>	3650
System Type	<Type of system>	SAP_R3
WAS Host Name	<Load-balanced WAS server host name>:5<System #>00	gerp-rp1-ecc.site.com:55000 ***see note on the following page**
WAS Path	<WAS path>	/webdynpro/dispatcher
WAS Protocol	"http" or "https"	http

Table 1 *SAP Property table*

◆ WARNING

** In the preceding examples, some of the entries include the port numbers. It is critical that **if you are using the BIG-IP LTM system to terminate SSL traffic, that you do NOT use port numbers as shown in the table**. If the application ports are hard coded, SSL termination will break the application.*

12. From the **Display selection** box, click **System Aliases**. The System Alias Editor opens.

13. In the **Alias** box, type at least one system alias for each object. Every object should have a system alias of the form **SAP_<System Type>_<Environment>** (for example SAP_SRM_QAS).

    Note that certain system aliases are required for the portal business packages to work; these aliases are listed in the following table:

System	Alias	For Bus Pack
ECC	SAP_R3_HumanResources	ESS / MSS
Web Dynpro runtime (ECC)	SAP_WebDynpro_XSS	ESS / MSS
SRM	SAP_EBP, SAP_R3_Procurement	SRM / Supplier Collaboration

Table 2 *System Aliases*

It is also important to note that system aliases cannot be transported - they must be assigned manually in each EP environment.

14. Click the **Save** button.

This completes the SAP configuration. For more information, consult the SAP documentation. Continue with the following section for configuring the BIG-IP system.

Configuring the BIG-IP LTM system for SAP Enterprise Portal

You can use the Application Template feature on the BIG-IP system, to efficiently configure a set of objects corresponding to SAP Portal. The template uses a set of wizard-like screens that query for information and then creates the required objects. At the end of the template configuration process, the system presents a list of the objects created and a description for how each object interacts with the application.

Be sure to see *Optional: Configuring the BIG-IP for dynamic load balancing based on CPU, memory and disk utilization*, on page 1-18 for additional configuration options.

◆ **Note**

Depending on which modules are licensed on your BIG-IP system, some of the options in the template may not appear.

Running the SAP Enterprise Portal application template

To run the SAP Enterprise Portal application template

1. Verify that your current administrative partition is set to **Common**. The Partition list is in the upper right corner.

2. On the Main tab, expand **Templates and Wizards**, and then click **Templates**. The Templates screen opens, displaying a list of templates.

3. In the Application column, click **SAP Enterprise Portal**. The SAP Enterprise Portal application template opens.

4. In the Template Questions section, you can type a unique prefix for your SAP Portal objects that the template will create. In our example, we leave this setting at the default, **my_sap_portal**.

5. From the **Do you want to import server pool members from the SAP Message Server** list, choose whether you want to automatically import the pool members from the SAP server.

   a) If you select **No**, continue with Step 6.

   b) If you select **Yes**, you see the following options:

   • In the IP address box, type the IP address of the SAP Message Server.

   • In the Port number box, type the port number of the SAP Message Server.

   • Click the **Import Pool Members** button.
   The BIG-IP system discovers the SAP Message server(s) and imports them into the template.

6. In the Enterprise Portal - Virtual Server Questions section, complete the following:

   a) Enter the IP address for this virtual server. The system creates a virtual server named **<prefix from step 4>_virtual_server**. In our example, we type **192.168.15.101**.

   b) If the Portal servers can communicate with the clients using a route through the BIG-IP system to deliver response data to the client, select **Yes** from the list. In this case, the BIG-IP does **not** translate the client's source address.

   If the BIG-IP system should translate the client's source address to an address configured on the BIG-IP system, leave the list at the default setting, **No**. Selecting **No** means the BIG-IP system will use SNAT automap. See the Online Help for more information.
   In our example, we leave this at the default setting: **No**.

Figure 1.4 *Running the SAP Portal application template*

7. In the SSL Offload Questions section, complete the following:

   a) If you are not using the BIG-IP system to offload SSL, leave this setting at the default, **No**. Continue with Step 6.

   If you are using the BIG-IP system to offload SSL from the SAP Portal devices, select **Yes** from the list. The SSL options appear.

   b) From the **Certificate** list, select the appropriate certificate you want to use for this deployment. If you plan to use a third party certificate, but have not yet installed it on the BIG-IP system, see *Using SSL certificates and keys*, on page 1-35.

c) From the **Key** list, select the appropriate key for the certificate. If you have not yet installed the key on the BIG-IP system, see *Using SSL certificates and keys*, on page 1-35.

For information on generating certificates, or using the BIG-IP LTM to generate a request for a new certificate and key from a certificate authority, see the **Managing SSL Traffic** chapter in the *Configuration Guide for Local Traffic Management*.

Figure 1.5 *Configuring the BIG-IP system for SSL Offload*

8. In the Enterprise Portal Server Load Balancing Questions section, complete the following:

a) From the Load Balancing Method list, select an appropriate load balancing method. In our example, we leave this setting at the default, **Least Connections (member)**.

b) Next, add each of the SAP Enterprise Portal Servers that are a part of this deployment.
Note: If you configured the template to import the pool members, you see a row in this section showing you which members were imported. You can modify these entries if necessary. If no modifications are needed, continue with Step c.

• In the **Address** box, type the IP address of the first Enterprise Portal server. In our example, we type **10.132.85.120**.

• In the **Service Port** box, leave the port at **51000**, unless you have modified the configuration on your SAP Enterprise Portal.

• Click the **Add** button. Repeat this step for each of the SAP Portal devices.

c) Next, type a number of seconds that the BIG-IP system issues the health check. In our example, we leave this at the default level, **30**.

d) If you have a specific HTTP request you would like to add to the health check, type it in the box after **GET /**. This is optional.

e) From the HTTP Version list, select **Version 1.1**. You should **not** use HTTP version 1.0 for SAP, as it will cause server issues.

A new row appears asking for the fully qualified DNS name (FQDN) that clients use to access the SAP Portal. In the box, type the FQDN for your SAP Portal deployment. Note that this FQDN should resolve to the virtual server on the BIG-IP system. In our example, we type **sapportal.siterequest.com**.

f) If you entered an HTTP request in step d, and want to enter a response string, type it here. This is optional.

Figure 1.6 *Configuring the Load Balancing options*

9. In the Protocol and Security Questions section, complete the following

a) If most clients will be connecting to the virtual server from a WAN, select **WAN** from the list. If most clients will be connecting from a LAN, select **LAN** from the list.
This option determines the profile settings that control the behavior of a particular type of network traffic, such as HTTP connections.

b) If you want to use the WebAccelerator module to accelerate the SAP Enterprise Portal traffic, select **Yes** from the list. If you do not want to use the WebAccelerator, select **No**. This option does not appear if you do not have the WebAccelerator module licensed. The WebAccelerator module can significantly improve performance for SAP deployments.

c) If you want to use the Application Security Manager to secure the SAP Portal traffic, select **Yes** from the list. If you do not want to use the Application Security Manager, select **No**. This option does not appear if you do not have the Application Security Manager (ASM) licensed. For more information, see the online help or the BIG-IP ASM documentation.

d) If you are using the Application Security Manager, from the Language Encoding list, select the appropriate language. In our example, we leave this at the default, **Unicode (utf-8)**.

e) If you are using the WebAccelerator module, in the **Host** box, type the fully qualified DNS name (FQDN) that your users will use to access the SAP Enterprise Portal deployment (the WebAccelerator application object's Requested Hosts field). Click the **Add** button. Type additional host names in the **Host** box, and then click **Add**. In our example, we type **sapportal.siterequest.com** and click the **Add** button.

Figure 1.7 Configuring the Optimization and Security settings

10. Click the **Finished** button. The BIG-IP system creates the relevant objects, and you see a summary of all the objects that were created.

Additional configuration options

After using the template to create the LTM configuration for SAP Portal, there are a some optional procedures you may wish to employ if applicable for your configuration. This section contains the following procedures:

- *Adding an NTLM profile if using NTLM authentication* on this page
- *Using an advanced health monitor*, on page 1-14
- *Optional: Configuring the BIG-IP for dynamic load balancing based on CPU, memory and disk utilization*, on page 1-18

Adding an NTLM profile if using NTLM authentication

If you are using NTLM authentication for your SAP deployment, you need to add a NTLM profile on the BIG-IP system in order for the system to work properly with the OneConnect profile. First you create the NTLM profile, and then associate it with the virtual server created by the template.

Creating the NTLM profile

Use the following procedure to create the NTLM profile.

To create the NTLM profile

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

2. On the Menu bar, from the **Other** menu, click **NTLM**. The NTLM Profile screen opens.

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

4. Complete any of the other settings as applicable for your configuration.

5. Click the **Finished** button.

Modifying the virtual server to use the NTLM profile

Use the following procedure to associate the profile you just created with the virtual server(s) created by the template. If the BIG-IP system is offloading SSL, you perform this procedure for both the HTTP and HTTPS virtual servers.

To modify the virtual server to use the NTLM profile

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

2. From the list, find the (first) virtual server that was created by the template. This virtual server uses the preface you specified in Step 4 on page 1-8. In our example we select **my_sap_portal_virtual_server**.

3. In the Configuration section, from the **NTLM Conn Pool** list, select the name of the NTLM profile you created in the preceding procedure. In our example, we select **sap-NTLM** (see Figure 1.8).

4. Click the **Update** button.

5. *Optional*: If you are offloading SSL from the Enterprise Portal deployment, repeat this procedure for the HTTPS virtual server that was created by the template. In our example, we repeat the procedure for the **my_sap_portal_https_virtual_server**.

Figure 1.8 *Adding the NTLM profile to the virtual server*

Using an advanced health monitor

The advanced health monitor uses an script to provide end to end monitoring. You can add this monitor to the pool created by the template.

◆ **Important**

This monitor requires a user account with access rights to the SAP portal. The user used to test should be configured to be a low privilege user. The lockout limits on this user should be increased, and especially during testing of the script, your SAP administrator should monitor the user to make sure the test user does not get locked out. The SAP administrator should unlock the account if this happens until the monitor is working properly

First, we download the script to a location accessible by the BIG-IP device. However, cutting and pasting is error-prone and therefore we provide instructions here on how to copy the file to the BIG-IP device using secure-copy (SCP).

To create the script, you must first copy the script into the BIG-IP device. The following procedures show you how to copy the file both on a Windows platform using WinSCP, and on Linux, UNIX or MacOS system using SCP.

To import the script on a Windows platform using WinSCP

1. Download the script from the following location to a computer that has access to the BIG-IP device:

http://www.f5.com/solutions/resources/deployment-guides/files/sap-portalmonitor.zip

2. Open a Windows compatible SCP client. We recommend WinSCP. It is available as a free download from http://winscp.net/.
   The login box opens.

3. In the **Host name** box, type the host name or IP address of your BIG-IP system.

4. In the **User name** and **Password** boxes, type the appropriate administrator log on information.

5. Click Login. The WinSCP client opens.

6. In the left pane, navigate to the location where you saved the script in step 1.

7. In the right pane, navigate to **/usr/bin/monitors/**.

8. In the left pane, select the script and drag it to the right pane.

9. You can now safely close WinSCP.

To import the script using Linux/Unix/MacOS systems

1. Download the script from the following location:

http://www.f5.com/solutions/resources/deployment-guides/files/sap-portalmonitor.zip

2. Open a terminal session.

3. Use your built in secure copy program from the command line to copy the file. Use the following syntax:

```
scp <source file> <username>@<hostname>:<Destination Directory and filename>
```

4. In our example, the command is:

```
scp sap-portal-monitor.pl root@bigip.f5.com:/usr/bin/monitors/sap-portal-monitor.pl
```

The next task is to change permissions on the file. These steps are performed in the BIG-IP Advanced Shell (see product documentation on how to configure users for Advanced shell access).

To change permissions on the monitor file

1. On the BIG-IP system, start a console session.

2. Type a user name and password, and then press Enter.

3. Change to the directory containing the creation script. In our example, we type: **cd /usr/bin/monitors**
   If you copied the script to a different destination, Use the appropriate directory.

4. Change the permissions on the script to allow for execute permission using the following command:

```
chmod 755 sap-portal-monitor.pl
```

5. Confirm that the permissions are correct by looking at the file using the following command:

```
ls -l sap-portal-monitor.pl
```

Confirm it looks like (the date will vary):

```
-rwxr-xr-x 1 root root 1454 Aug  8 21:17 sap-portal-monitor.pl
```

In the following procedure, we create the monitor on the BIG-IP LTM Configuration utility.

To configure the advanced health monitor

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

2. Click the **Create** button

3. In the **Name** box, type a name for this monitor. In our example, we type **sap-portal-monitor**.

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

5. In the Configuration section, in the **Interval** box, type an interval, keeping in mind the script logs in and logs out of your SAP Portal instance, so balance this with uptime requirements. We recommend once every 60 seconds to start, and adjusting later to suit your requirements. In our example, we type **60**.
   Note: When combined with the HTTP monitor (that can run more frequently than once every 60 seconds), uptime can be maintained with causing additional load on the SAP portal instances.

6. In the **Timeout** box, type a timeout. In our example **181**.

7. In the **External Program** box, type the path to the script. In our example, we type **/usr/bin/monitors/sap-portal-monitor.pl**.
   If you changed the name of the script file, you must change this command.

8. In the Variables section, we assign three variables: the hostname of the SAP portal, and the username and password of the user that is used to simulate the login. Complete the following:

   a) In the **Name** field type **username**, and in the **Value** box, type the user name of the user that simulates the loginlick **Add**. In our example we type **g.washington** in the Value box.

   b) In the **Name** field type **password**, and in the **Value** box, type the associated password. Click **Add**. In our example we type **Pass1word** in the Value box.

   c) In the **Name** field, type **hostname**, and in the **Value** box, type your fully qualified host name; this should be the same URL that users use to visit the site in their web browser. Click **Add**. In our example we type **sap-portal.example.com** in the Value box.

9. Click **Finished**.

Figure 1.9 *External monitor configuration*

Modifying the pool to use the monitor

The next task for the health monitor is to associate it with the pool that was created by the template.

To modify the pool to use the advanced monitor

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

2. From the list, find the pool that was created by the template. This pool uses the preface you specified in Step 4 on page 1-8. In our example we select **my_sap_portal__pool**.

3. In the Configuration section, from the **Health Monitors** list, select the name of the monitor you created in the preceding procedure and then click the Add (<<) button to add it to the Active list.

4. From the **Active** list, select the name of the monitor created by the template and click the Remove (>>) button to remove it.

5. Click the **Update** button.

Optional: Configuring the BIG-IP for dynamic load balancing based on CPU, memory and disk utilization

In some cases, batch jobs and asynchronous connections create situations were the load on a particular SAP Instance (server) is high without a corresponding number of connections. In these scenarios, it is useful to configure dynamic load balancing instead of connection based or round robin load algorithms. By using dynamic load balancing with SNMP, servers with higher load can be sent fewer connections or be ineligible to receive traffic altogether.

The use of dynamic load balancing with the SNMP monitor is recommend in conjunction with either basic or advanced monitors for SAP traffic. Specifically, the application monitors detect the up/down status of your SAP Instances while the SNMP monitor helps to control the amount of traffic each server receives.

Creating Dynamic load balancing with SAP is a multiple step process involving both the SAP servers and the BIG-IP LTM.

Modifying the SAP configuration

On your SAP Servers, activate SNMP monitoring using a standard agent. If your SAP services are running on Windows Servers, the built-in SNMP agent may be a good starting point. On Linux, multiple free and commercial SNMP agents are available.

In either case, agents typically fall into two designs, both adhering to certain standards on Object IDs (OIDs) for CPU, memory, disk and other hardware information.

Install and configure your SNMP agent to accept incoming connections from the self-IP address of your BIG-IP device.

For specific instructions on configuring the SAP devices, see the SAP documentation.

Configuring the BIG-IP LTM

For this configuration, there are three tasks: configuring the health monitor, adding the monitor to the SAP nodes, and modifying the load balancing pool.

Creating the SNMP monitor

The first task is to create the new health monitor.

To create the 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 **SAP-CPU**.

4. From the **Type** list, select **SNMP DCA**.

5. In the Community box, type the community string of the agent you have configured. In our example, leave the default, **public**.

6. From the Version list, select the appropriate version. In our example, we select **v2c**.

7. From the **Agent Type** list, select an agent type. In general, if the server running your SAP instance is Linux, select **UCD**. If it's Windows, select **Win2000**. In our example, we select **WIN2000**.

   In the next steps, we establish thresholds that determine the weight that dynamic load balancing uses to direct traffic to an individual pool member.

8. In the **CPU Threshold** box, type a percentage. We type **80**.

9. In the **Memory Threshold** box, type a percentage. We type **80**.

10. In the **Disk Threshold** box, type a percentage. We type **98**.

    In this example, the weight of the server varies between 1 and 100, with 1 meaning that the host is ineligible to receive traffic, to 100 meaning that is fully capable of receiving traffic. Values in between work as a ratio between pool members to distribute traffic.

11. Configure any of the other settings as applicable. In our example, we leave the defaults.

12. Click **Finished** (see Figure 1.10, on page 1-20).

Figure 1.10 SNMP DCA monitor configuration

Adding the monitor to the nodes

The next task is to add the health monitor you just created to the SAP nodes on the BIG-IP system that were created by the template. These BIG-IP LTM *nodes* are the IP addresses you added in step 8b of the template procedure.

To add the monitor to the nodes

1. On the Main tab, expand **Local Traffic**, and then click **Nodes**. The Node list page opens.

2. From the list, click an IP address that corresponds to an SAP server.

3. In the Configuration section, from the Health Monitors list, select Node Specific. The Select Monitors box appears.

4. From the **Select Monitors Available** list, select the name of the monitor you just created and click the Add (<<) button to add it to the **Active** list. In our example, we select **SAP-CPU**.

5. Click the **Update** button.

6. Repeat steps 2-5 for each of the SAP nodes in this configuration.

Modifying the pool

The final task in this section is to modify the load balancing pool created by the tempate to use the **Dynamic** load balancing method.

To modify the pool

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

2. From the **Pool** list, click the name of the pool that was created by the template. This pool is prefaced with the prefix you specified in step 4 of the template procedure. The default prefix is **my_sap_portal**. In our example, we click **my_sap_portal_pool**.

3. On the menu bar, click **Members**.

4. From the Load Balancing Method list, select **Dynamic Ratio (Member)**.

5. Click **Update**.
   You have now created Dynamic Load balancing based on the criteria in your SNMP monitor.

Enabling logging

In order to view statistics about the load balancing algorithms' ability to weight traffic properly, enable logging as shown in the following procedure.

You can also test the monitor by creating one SNMP DCA monitor with thresholds set very low and applying this monitor to one pool member. By watching the number of connections. You should see that the machines with lower thresholds receive no or fewer connections.

Be sure to disable logging after you are satisfied that the SNMP monitors are working properly.

To enable logging

1. Log in to the BIG-IP system command line.

2. Enable monitor logging monitor by typing the following command:

   `bigpipe db Snmp.SNMPDCA.Log true`

   The **/var/tmp/snmpdca.log** file contains entries similar to the following example:

```
========== /usr/bin/monitors/SNMPDCA_monitor ==========
Node Address: 10.0.18.1
SNMP version: v1, community = public, port: 161
Monitor: snmp_dca
Agent Type: UCD
User OIDs:
Mem OIDs:
.1.3.6.1.4.1.2021.4.5.0 - 523904.000000
.1.3.6.1.4.1.2021.4.6.
- 386296.000000
Cpu OIDs:
.1.3.6.1.4.1.2021.11.50.0 - 537468.000000
.1.3.6.1.4.1.2021.11.52.0 - 364422.000000
.1.3.6.1.4.1.2021.11.51.0 - 1.000000
.1.3.6.1.4.1.2021.11.53.0 - 975292152.000000
Disk OIDs:
.1.3.6.1.4.1.2021.9.1.9.1 - 54.000000
i = 0, util = 26.265881, threshold=70.000000, coeff=1.000000
i = 1, util = 0.092388, threshold=80.000000, coeff=1.500000
i = 2, util = 54.000000, threshold=90.000000, coeff=2.000000
Main:Weight =42 (weight1 = 0.000000, weight2 = 42.021229)
```

◆ Note

For BIG-IP platforms that contain a hard drive, the snmpdca.log file will be recorded in two places. The snmpdca.log file is recorded in the /var/tmp/snmpdca.log file and the /shared/tmp/snmpdca.log file.

To disable monitor logging

When you are satisfied that the SNMP monitors are working properly, disable monitoring using the following procedure.

1. Log in to the BIG-IP system command line.

2. Enable monitor logging monitor by typing the following command:

   `bigpipe db Snmp.SNMPDCA.Log false`

This completes the Dynamic load balancing section.

Appendix A: Manually configuring the BIG-IP LTM system for deployment with SAP

In this section, we show you how to manually configure the BIG-IP LTM system. Note that we strongly recommend using the Application Template for configuring SAP Portal.

A SAP deployment can be incredibly large and complex, deployed in infinite variations, with number of different SAP applications and components. In this deployment guide, we focus on providing high availability and acceleration for the SAP Enterprise Portal. For instructions for SAP application components such as ERP Central Component (ECC) or Process Integration (PI) please see the appropriate deployment guide on f5.com.

Prerequisites and configuration notes

The following are prerequisites for this chapter:

◆ The BIG-IP LTM system must be running version 10.0 or later, we strongly recommend running version 10.1 or later.

◆ If you are using the BIG-IP LTM system for load balancing the SAP services, you **do not** need to use the *SAP Web Dispatcher* for load balancing traffic. This allows you to devote the resources that would have been dedicated to Web Dispatcher to servicing other aspects of the application.

◆ We assume that the BIG-IP LTM device is already installed in the network, and objects like Self IPs and VLANs have already been created. For more information on configuring these objects, see the BIG-IP LTM manuals.

◆ If you are using the BIG-IP LTM system to offload SSL traffic from the SAP devices, you must already have obtained an SSL Certificate (but not necessarily installed it on the BIG-IP LTM system). For more information about offloading SSL traffic, see *Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment*, on page 1-35.

Connecting to the BIG-IP LTM device

Use the following procedure to access the BIG-IP LTM web-based Configuration utility using a web browser.

To connect to the BIG-IP LTM system

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 Welcome screen opens.

Once you are logged onto the BIG-IP system, the Welcome screen of the new Configuration utility opens. From the Configuration utility, you can configure and monitor the BIG-IP system, as well as access online help, download SNMP MIBs and Plug-ins, and search for specific objects.

Creating the health monitor

In this section, we configure a health monitor for SAP Portal. We provide two example monitors, a simple HTTP monitor, and an advanced monitor that provides end-to-end monitoring using a external script.

There is one more optional monitor monitor that allows the BIG-IP to use dynamic load balancing based on CPU, memory and disk utilization.

Creating the monitor for Dynamic load balancing

In some cases, batch jobs and asynchronous connections create situations were the load on a particular SAP Instance (server) is high without a corresponding number of connections. In these scenarios it is useful to configure dynamic load balancing instead of connection based or round robin load algorithms. By using dynamic load balancing with SNMP, servers with higher load can be sent fewer connections or be ineligible to receive traffic altogether.

To create the SNMP monitor, you must follow two procedures found in the preceding chapter:

◆ *Modifying the SAP configuration*, on page 1-18

◆ *Creating the SNMP monitor*, on page 1-18

After modifying the SAP configuration and creating the monitor, there is one additional step after creating the pool in the following procedure to add the health monitor to the nodes.

Creating the advanced monitor using the script

If you want to create an advanced monitor, use the procedure *Using an advanced health monitor*, on page 1-14.

Note that you do not have to use the procedure Modifying the Pool, as we have not yet configured the pool in this section.

If you create the advanced monitor, you do not have to create the HTTP monitor described in the next procedure.

Creating the HTTP health monitor

If you did not create the advanced monitor, we recommend you create an HTTP health monitor. Although the monitor in the following example is quite simple, you can configure optional settings such as Send and Receive Strings to make the monitor much more specific. You can also use one of the other types of monitors available on the BIG-IP LTM system.

To configure the HTTP health monitor

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

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 **sap_http**.

4. From the **Type** list, select **HTTP**. The HTTP Monitor configuration options appear.

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. In our example, we use an **Interval** of **30** and a **Timeout** of **91.**

6. In the **Send String** and **Receive Rule** boxes, you can add a Send String and Receive Rule specific to the device being checked (see Figure 1.11).

Figure 1.11 Creating the HTTP Monitor

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

Remember that if you configure a Send String and Receive String specific to one of the application components, you should create a new monitor for the other components.

Creating the pool

The next step is to create a pool on the BIG-IP LTM system for the SAP Enterprise Portal nodes.

To create a new pool for the Enterprise portal servers

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

2. In the upper right portion of the screen, 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 the pool. We use **sap_portal**.

5. In the **Health Monitors** section, select the name of the monitor(s) you created in the *Creating the health monitor* section, and click the Add (**<<**) button. In our example, we select **sap-portal-monitor** and **SAP-CPU**.

6. *Optional*: **In the Slow Ramp Time** box, type **300**.
   Because we are using the Least Connections load balancing method, we set the Slow Ramp Time in order to ensure that if a pool member becomes available after maintenance or a new member is added, the BIG-IP does not send all new connections to that member (a newly available member always has the least number of connections). Set a Slow Ramp time if your SAP servers are designed for high traffic environments.

7. From the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network). In our example, we select **Least Connections (member)**.

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

9. In the **Address** box, add the first server to the pool. In our example, we type **10.132.81.1**.

10. In the **Service Port** box, type the appropriate port. In our example, we type **51000**. Your SAP Portal services might be running on a different TCP port, such as port **80**. Type the proper port number here, and the BIG-IP LTM system properly performs the translation.

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

12. Repeat steps 9-11 for each SAP Enterprise Portal server. In our example, we repeat these steps for **10.132.81.2** and **10.132.81.3**.

13. Click the **Finished** button.
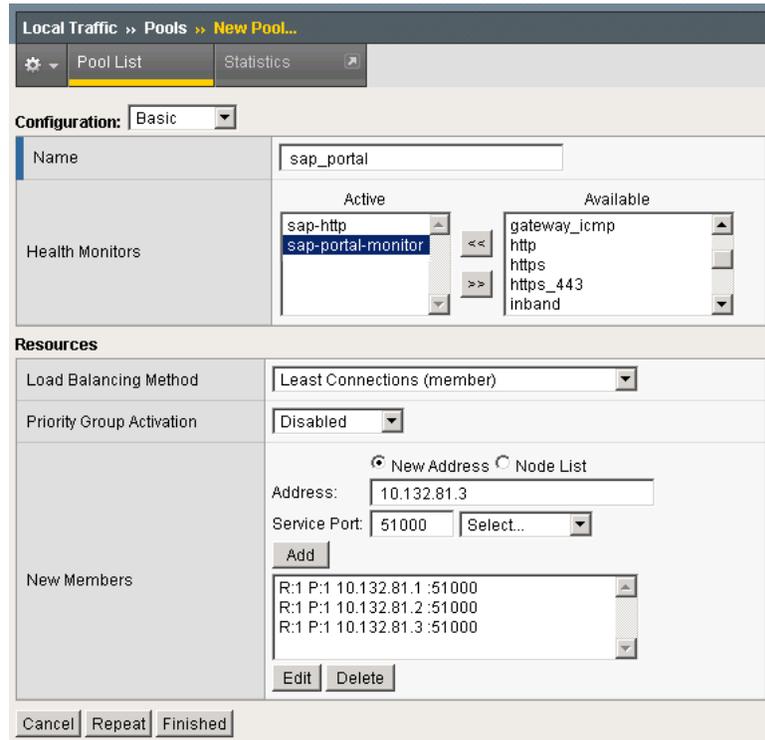
Figure 1.12 Creating the pool for the Enterprise Portal devices

Adding the SNMP monitor to the nodes

If you created the SNMP monitor, and selected the Dynamic load balancing method, you must now associate the health monitor with the SAP nodes on the BIG-IP system.

To add the monitor to the nodes

1. On the Main tab, expand **Local Traffic**, and then click **Nodes**. The Node list page opens.

2. From the list, click an IP address that corresponds to an SAP server.

3. In the Configuration section, from the **Health Monitors** list, select **Node Specific**. The Select Monitors box appears.

4. From the **Select Monitors Available** list, select the name of the monitor you created in *Creating the SNMP monitor*, on page 1-18 and then click the Add (**<<**) button to add it to the **Active** list. In our example, we select **SAP-CPU**.

5. Click the **Update** button.

6. Repeat steps 2-5 for each of the SAP nodes in this configuration.

Creating profiles

The BIG-IP system uses profiles to make configuration easier. A *profile* is an object that contains user-configurable settings, with default values, for controlling the behavior of a particular type of network traffic, such as HTTP connections. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

Although it is possible to use the default profiles, we strongly recommend you create new profiles based on the default parent profiles, even if you do not change any of the settings initially. Creating new profiles allows you to easily modify the profile settings specific to this deployment, and ensures you do not accidentally overwrite the default profile.

For this configuration, we create the following profiles: an HTTP profile, a TCP profile, a OneConnect profile and two persistence profiles. If you are using the BIG-IP LTM system to terminate SSL traffic, there are additional profiles you need to create. See *Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment*, on page 1-35.

Creating an 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. In the following example, we base our HTTP profile off of the **http-acceleration** parent profile, as we are using the WebAccelerator. If you are not using the WebAccelerator, we recommend using the **http-wan-optimized-compression-caching** parent.

In our example, we also configure the HTTP profile to encrypt the SAP cookie as well as the BIG-IP LTM cookie. This helps prevent cookie tampering attacks by denying malicious users from modifying the otherwise cleartext cookie to gain unauthorized access. Although encrypting cookie is optional, we recommend it.

If you are using the BIG-IP LTM system to offload SSL traffic from the SAP deployment, you need to configure an alternate HTTP profile, among other settings. After completing the Enterprise Portal configuration, be sure to see *Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment*, on page 1-35.

To create a new HTTP profile

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

2. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.

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

4. From the **Parent Profile** list, select **http-acceleration** if you are using the WebAccelerator. If you are not using the WebAccelerator, select **http-wan-optimized-compression-caching**.

5. *Optional:* Click a check in the Custom box in the **Encrypt Cookies** row. Type the name of the cookies you want to encrypt, with a space between each cookie. In our example, we type the name of the SAP cookie (**MYSAPSSO2** by default), and the BIG-IP cookie (**BIGipServer<**Name_of_Pool**>** by default, so in our example, **BIGipServersap_portal**).
You can either modify the Cookie Passphrase or leave it at the default. In our example, we leave it at the default.

6. Check the Custom box for **Content Compression**, and leave **Content List** selected.

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

8. Click the **Finished** button.

Creating the TCP profiles

The next profiles we create are the TCP profiles. If most of the Enterprise Portal users are accessing the portal via a Local Area Network, we recommend using the base TCP profile as the parent. If the majority of the Enterprise Portal users are accessing the system from remote or home offices, we recommend using **tcp-wan-optimized** (for client side TCP connections) and **tcp-lan-optimized** (for server-side TCP connections). In our example, we leave these profiles at their default levels; you can configure any of the options as applicable for your network.

Creating the WAN optimized TCP profile

First we configure the WAN optimized profile. Remember, if most users are accessing the portal via the LAN, use the base TCP profile instead of this WAN optimized profile.

To create a new TCP WAN optimized profile

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

2. On the Menu bar, from the **Protocol** menu, click **tcp**.

3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.

4. In the **Name** box, type a name for this profile. In our example, we type **sap_tcp-wan**.

5. From the **Parent Profile** list, select **tcp-wan-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 **Finished** button.

Creating the LAN optimized TCP profile

Now we configure the LAN optimized profile. If you have already created a simple TCP profile, based off the default TCP profile (and not the WAN optimized profile above), you do not need to create another TCP profile, continue with the next procedure.

To create a new TCP profile

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

2. On the Menu bar, from the **Protocol** menu, click **tcp**.

3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.

4. In the **Name** box, type a name for this profile. In our example, we type **sap_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 **Finished** button.

Creating a OneConnect profile

The next profile we create is a OneConnect profile. With OneConnect enabled, client requests can utilize existing, server-side connections, thus reducing the number of server-side connections that a server must open to service those requests. Testing has demonstrated that this can provide significant performance improvements for SAP implementations. For more information on OneConnect, see the BIG-IP LTM documentation.

In our example, we leave all the options at their default settings. You can configure these options as appropriate for your network.

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**. The Persistence Profiles screen opens.

3. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.

4. In the **Name** box, type a name for this profile. In our example, we type **sap_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 an NTLM profile if using NTLM authentication

If you are using NTLM authentication, you need to add a NTLM profile on the BIG-IP system in order for the system to work properly with the OneConnect profile. This is only necessary if you are using NTLM.

To create the NTLM profile

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

2. On the Menu bar, from the **Other** menu, click **NTLM**.

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

4. Complete any of the other settings as applicable for your configuration.

5. Click the **Finished** button.

Creating persistence profiles

The final profiles we create are Persistence profiles. In this case, we create two persistence profiles; a default and a fallback persistence profile. Because we are using HTTP cookie insert persistence as our default mode, we need the fallback mode in case the user's device does not accept cookies.

Creating the Cookie Persistence profile

The first persistence profile we create is the Cookie Persistence profile. In this profile there are some optional settings you can configure, such as the method of cookie persistence and the expiration. In out experience, SAP expects persistence to be maintained for 8 hours. As a result, we set the time out value in this profile to 8 hours and 1 minute.

To create a new cookie persistence profile

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

2. On the Menu bar, click **Persistence**. The Persistence Profiles screen opens.

3. In the upper right portion of the screen, click the **Create** button. The New Persistence Profile screen opens.

4. In the **Name** box, type a name for this profile. In our example, we type **sap_cookie**.

5. From the **Persistence Type** list, select **Cookie**.
   The configuration options for cookie persistence appear.
   Make sure the Parent Profile is set to **Cookie**.

6. In the **Expiration** row, click a check in the Custom box. Clear the Session Cookie box, and the Expiration values appear. In the **Hours** box, type **8**, and in the **Minutes** box, type **1**.

7. Modify any of the other settings as applicable for your network.

8. Click the **Finished** button.

Creating the Fallback Persistence profile

Now we configure the fallback persistence profile. In our example, we use Source Address Affinity for the fallback persistence type.

To create a new fallback persistence profile

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

2. On the Menu bar, click **Persistence**.
   The Persistence Profiles screen opens.

3. In the upper right portion of the screen, click the **Create** button.
   The New Persistence Profile screen opens.

4. In the **Name** box, type a name for this profile. In our example, we type **sap_source**.

5. From the **Persistence Type** list, select **Source Address Affinity**.
   The configuration options for Source Address Affinity persistence appear.

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 the virtual server

Next, we configure a virtual server that uses the profiles and pool you created in the preceding procedures.

To create the virtual server

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

2. In the upper right portion of the screen, click the **Create** button.
   The New Virtual Server screen opens.

3. In the **Name** box, type a name for this virtual server. In our example, we type **sap_portal_vs**.

4. In the **Destination** section, click the **Host** button.

5. In the **Address** box, type the IP address of this virtual server. In our example, we use **10.133.21.15**.

6. In the **Service Port** box, type **80**.

Figure 1.13 *Creating the new virtual server*

7. From the Configuration list, select **Advanced**.
   The Advanced configuration options appear.

8. Leave the **Type** and **Protocol** lists at their default settings: **Standard** and **TCP**.

9. From the **Protocol Profile (Client)** list, select the name of the profile you created in the *Creating the WAN optimized TCP profile* section. In our example, we select **sap_tcp-wan**.

10. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **sap_tcp-lan**.

11. From the **OneConnect Profile** list, select **sap_oneconnect**.

12. *Optional*: If you are using NTLM authentication, from the **NTLM Conn Pool** list, select the profile you created in *Creating an NTLM profile if using NTLM authentication*. In our example, we are not using NTLM authentication, so we leave this at the default setting.

13. From the HTTP Profile list, select the name of the profile you created in the *Creating an HTTP profile* section. In our example, we select **sap_http-opt** (see Figure 1.14).

Figure 1.14 *Selecting the profiles for the virtual server*

14. In the Resources section, from the **Default Pool** list, select the pool you created in *Creating the pool*. In our example, we select **sap_portal**.

15. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating persistence profiles* section. In our example, we select **sap_cookie**.

16. From the **Fallback Persistence Profile** list, select the profile you created for the fallback persistence method in the *Creating persistence profiles* section. In our example, we select **sap_source**.

Figure 1.15 *Resources section of the add virtual server page*

17. Click the **Finished** button. The BIG-IP LTM configuration for SAP Enterprise Portal is now complete.

Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment

The BIG-IP LTM device can be configured as an SSL proxy, offloading the SSL duties from the servers. F5's testing, performed in conjunction with SAP, demonstrated significant increases in efficiency for the Enterprise Portal and component application servers when SSL processing was offloaded to the F5 BIG-IP LTM. If you want to use this functionality, you must complete the following procedures.

◆ **Important**

This section is optional, and only necessary if you are using the BIG-IP LTM system for offloading SSL.

Using SSL certificates and keys

Before you can enable the BIG-IP system to act as an SSL proxy, you must install a SSL certificate on the virtual server that you wish to use for SAP connections on the BIG-IP device. For this Deployment Guide, we assume that you already have obtained an SSL certificate, but it is not yet installed on the BIG-IP system. For information on generating certificates, or using the BIG-IP system to generate a request for a new certificate and key from a certificate authority, see the Managing SSL Traffic chapter in the *Configuration Guide for Local Traffic Management*.

Importing keys and certificates

Once you have obtained a certificate, you can import this certificate into the BIG-IP system using the Configuration utility. By importing a certificate or archive into the Configuration utility, you ease the task of managing that certificate or archive. You can use the Import SSL Certificates and Keys screen only when the certificate you are importing is in Privacy Enhanced Mail (PEM) format.

To import a key or certificate

1. On the Main tab, expand Local Traffic.

2. Click **SSL Certificates**.
   This displays the list of existing certificates.

3. In the upper right corner of the screen, click **Import**.

4. From the **Import** list, select the type of import (**Key** or **Certificate**).

5. Select the import method (text or file).

6. Type the name of the key or certificate.

7. Click **Import**.

8. If you imported the certificate in the preceding steps, repeat the entire procedure for the key.

Creating additional profiles

When using the BIG-IP LTM system to offload SSL traffic, you need to create two additional profiles. The first is a new Client SSL profile, and the second is a slightly modified HTTP profile that instructs the SAP server to respond with the appropriate content, and directs the BIG-IP LTM system to rewrite the URI in all HTTP redirect responses.

The following profiles can be created whether you are configuring the BIG-IP LTM for the Enterprise Portal or application component servers.

Creating a Client SSL profile

The first profile is the SSL profile. This profile contains the SSL certificate and Key information for offloading the SSL traffic.

To create a new Client SSL profile

1. On the Main tab, expand **Local Traffic**.

2. Click **Profiles**.
   The HTTP Profiles screen opens.

3. On the Menu bar, from the **SSL** menu, select **Client**.
   The Client SSL Profiles screen opens.

4. In the upper right portion of the screen, click the **Create** button.
   The New Client SSL Profile screen opens.

5. In the **Name** box, type a name for this profile. In our example, we type **sap_clientssl**.

6. In the Configuration section, click a check in the **Certificate** and **Key** Custom boxes.

7. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.

8. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.

9. Click the **Finished** button.

For more information on creating or modifying profiles, or SSL Certificates, see the BIG-IP documentation.

Creating the new HTTP profile

The next profile is a new HTTP profile that contains the necessary client header, along with the rewrite/redirect setting. You must have an HTTP profile with the settings in the following procedure for each SAP virtual server that will be offloading SSL.

If you have already created an HTTP profile as described earlier in this guide, you can modify that profile with the modifications found in the following procedure.

To create a new HTTP profile for SSL

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

2. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.

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

4. From the **Parent Profile** list, ensure that **HTTP** is selected.

5. In the **Request Header Insert** row, click a check in the Custom box. In the box, type: **clientprotocol: https**.

6. In the **Redirect Rewrite** row, click a check in the Custom box. From the list, select **Matching**.

7. *Optional for virtual servers requiring Cookie Persistence:* In the **Encrypt Cookies** row, click a check in the Custom box. Type the name of the cookies you want to encrypt, with a space between each cookie. In our example, we type the name of the SAP cookie (**MYSAPSSO2** by default), and the BIG-IP cookie (**BIGipServer**<*Name_of_Pool*> by default, so in our example, **BIGipServersap_portal**).

   You can either modify the Cookie Passphrase or leave it at the default. In our example, we leave it at the default level.

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

9. Click the **Finished** button (see Figure 1.16).

Figure 1.16 Creating the HTTP profile for SSL deployments

For more information on creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation.

Creating the Redirect iRule

The next step is to create an iRule that redirects all traffic to same hostname (stripping port if it exists), same URI over HTTPS. This iRule catches the traffic that incorrectly comes in on HTTP and redirects it to HTTPS. This ensures that SSL traffic remains on the virtual server that supports the traffic. The iRule will be applied to an HTTP Virtual Server where required.

To create the redirect iRule

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

2. In the upper right portion of the screen, click the **Create** button. The New iRule screen opens.

3. In the **Name** box, enter a name for your iRule. In our example, we use **sap_httptohttps**.

4. In the Definition section, copy and paste the following iRule:

```
when HTTP_REQUEST {
  HTTP::redirect https://[getfield [HTTP::host] ":" 1][HTTP::uri]
}
```

5. Click the **Finished** button.

The iRule is now complete. You use this iRule when you modify the existing SAP Enterprise Portal virtual server on port 80 in *Modifying the SAP Enterprise Portal virtual server*, on page 1-40.

Creating an HTTPS virtual server

The next step is to create a virtual server for the SSL offload that will use the Client SSL profile you just created. The example virtual server is for SAP Enterprise Portal. As a result, TCP WAN and LAN optimized profiles are used along with a Cookie Persistence profile. These settings would not necessarily apply if this were a virtual server dedicated to managing traffic between SAP application components.

To create a new HTTPS virtual server

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

2. In the upper right portion of the screen, click the **Create** button.
   The New Virtual Server screen opens.

3. In the **Name** box, type a name for this virtual server. In our example, we type **sap_portal_ssl**.

4. In the **Destination** section, select the **Host** option button.

5. In the **Address** box, type the IP address of this virtual server. In our example, we use **10.133.21.15**.

6. In the **Service Port** box, type **443**, or select **HTTPS** from the list.

7. From the Configuration list, select **Advanced**.
   The Advanced configuration options appear.

8. Leave the **Type** list at the default setting: **Standard**.

9. From the **Protocol Profile (Client)** list, select a tcp profile. If you are configuring this virtual server for Enterprise Portal, select the tcp profile you created in *Creating the WAN optimized TCP profile*.

10. From the **Protocol Profile (Server)** select the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **sap_tcp-lan** from the list.

11. From the **OneConnect Profile** list, select **sap_oneconnect**.

12. From the **HTTP Profile** list, select the name of the profile you created in the *Creating the new HTTP profile* section. In our example, we select **sap_ssl**.

13. From **SSL Profile (Client)** list, select the name of the profile you created in the *Creating a Client SSL profile* section. In our example we select **sap_clientssl**.

14. In the Resources section, from the **Default Pool** list, select the pool you created for your SAP Portal nodes in the *Creating the pool* section. In our example, we select **sap_portal**.

15. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating persistence profiles* section. In our example, we select **sap_cookie**.

16. From the **Fallback Persistence Profile** list, select the profile you created for the fallback persistence method in the *Creating persistence profiles* section. In our example, we select **sap_source**.

17. Click the **Finished** button.

Modifying the SAP Enterprise Portal virtual server

In this procedure, we modify the portal virtual server on port 80 that you created in the *Creating the pool*, on page 1-26, to use the iRule instead of the pool. This iRule is in place to ensure that any accidental requests to port 80 are redirected to the SSL virtual server.

To modify the Enterprise Portal virtual server to use the iRule

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

2. From the list, click the virtual server you created in *Creating the virtual server*, on page 1-32. In our example, we click **sap_portal_vs**. The Virtual Server properties page opens.

3. On the Menu bar, click **Resources**.

4. In the iRules section, click the **Manage** button.
   The iRules Resource Management screen opens.

5. From the **Available** list, select the iRule you created in the *Creating the Redirect iRule* section, and click the Add (<<) button.
   In our example, we select **sap_httptohttps**.

6. Click the **Finished** button.
   You return to the Resources page.

7. From the **Default Pool** list, select **None**.

8. Click the **Update** button.

This concludes the steps necessary to use the BIG-IP LTM system to offload SSL traffic.

2

Configuring the F5 WebAccelerator module with SAP Enterprise Portal

• Configuring the WebAccelerator module

• Configuring the WebAccelerator in a symmetric deployment

Configuring the F5 WebAccelerator module with SAP Enterprise Portal

In this section, we configure the WebAccelerator module for the SAP Enterprise Portal (EP) devices to increase performance for end users. The F5 WebAccelerator is an advanced web application delivery solution that provides a series of intelligent technologies designed to overcome problems with browsers, web application platforms and WAN latency issues which impact user performance.

For more information on the F5 WebAccelerator, see *http://www.f5.com/products/big-ip/product-modules/webaccelerator.html.*

The WebAccelerator can be deployed either symmetrically or asymmetrically. By deploying BIG-IP WebAccelerator in a symmetric configuration, Web application performance can increase 40x over unaccelerated applications. WebAccelerator is the only product on the market that can be deployed in both asymmetric and symmetric configurations simultaneously, giving organizations the freedom to choose the most appropriate configuration for their environment. See *Configuring the WebAccelerator in a symmetric deployment*, on page 2-7 for information about optionally configuring the WebAccelerator in a symmetric deployment.

Prerequisites and configuration notes

The following are prerequisites for this section:

◆ We assume that you have already configured the BIG-IP LTM system for directing traffic to the SAP deployment as described in this Deployment Guide.

◆ You must have purchased and licensed the WebAccelerator module on the BIG-IP LTM system.

◆ For this configuration, you must have created an HTTP profile on the BIG-IP LTM system that has RAM Cache enabled. In our example (*Creating an HTTP profile*, on page 1-28) we use a parent profile that includes RAM Cache. If you did not create an HTTP profile with RAM Cache enabled, you must create a new HTTP profile, based on a parent profile that uses RAM Cache (we recommend HTTP Acceleration) and associate it with the virtual server.

◆ This document is written with the assumption that you are familiar with the BIG-IP LTM system, WebAccelerator and SAP Enterprise Portal. Consult the appropriate documentation for detailed information.

◆ For the optional symmetric deployment, all of the above prerequisites apply, and the two BIG-IP devices must have the ability to communicate over TCP port **4353**.

Configuration example

Using the configuration in this section, the BIG-IP LTM system with WebAccelerator module is optimally configured to accelerate traffic to SAP Enterprise Portal servers. The BIG-IP LTM with WebAccelerator module both increases end user performance as well as offloads the servers from serving repetitive and duplicate content.

In this configuration, a remote client with WAN latency logs onto the SAP portal via the WebAccelerator. The user's request is accelerated on repeat visits by the WebAccelerator instructing the browser to use the dynamic or static object that is stored in its local cache. Additionally, dynamic and static objects are cached at the WebAccelerator so that they can be served quickly without requiring the server to re-serve the same objects.

Optionally, if additional sites will be optimized using the BIG-IP Edge Gateway or other installations of WebAccelerator, a symmetric deployment may provide advantages to the remote office. Follow the instructions at the end of this chapter for symmetric deployment guidelines.

Configuring the WebAccelerator module

Configuring the WebAccelerator module requires creating an HTTP class profile and creating an Application. The WebAccelerator device has a large number of other features and options for fine tuning performance gains, see the *WebAccelerator Administrator Guide* for more information.

Creating an HTTP Class profile

The first procedure is to create an HTTP class profile. When incoming HTTP traffic matches the criteria you specify in the WebAccelerator class, the system diverts the traffic through this class. In the following example, we create a new HTTP class profile, based on the default profile.

To create a new HTTP class profile

1. On the Main tab, expand **WebAccelerator**, and then click **Classes**. The HTTP Class Profiles screen opens.

2. Click the **Create** button.

3. In the **Name** box, type a name for this Class. In our example, we type **SAP_class**.

4. From the Parent Profile list, make sure **httpclass** is selected.

5. In the Configuration section, from the **WebAccelerator** row, make sure **Enabled** is selected.

6. In the Hosts row, click the Custom box, and then from the list select **Match Only**. The Host List options appear.

   a) In the **Host** box, type the host name that your end users use to access the SAP Enterprise Portal. In our example, we type **myportal.companyxyz.com** (see Figure 2.1).

   b) Leave the Entry Type at **Pattern String**.

   c) Click the **Add** button.

   d) Repeat these sub-steps for any other host names users might use to access the SAP deployment.

7. The rest of the settings are optional, configure them as applicable.

8. Click the **Finished** button. The new HTTP class is added to the list.

Figure 2.1 Creating a new HTTP Class profile

Modifying the Virtual Server to use the Class profile

The next step is to modify the virtual server for your SAP deployment on the BIG-IP LTM system to use the HTTP Class profile you just created.

To modify the Virtual Server to use the Class profile

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

2. From the **Virtual Server** list, click the name of the virtual server you created for the SAP Enterprise Portal. In our example, we click **sap_portal_vs**.
   The General Properties screen for the Virtual Server opens.

3. On the Menu bar, click **Resources**.
   The Resources screen for the Virtual Server opens.

4. In the HTTP Class Profiles section, click the **Manage** button.

5. From the **Available** list, select the name of the HTTP Class Profile you created in the preceding procedure, and click the Add (**<<**) button to move it to the Enabled box. In our example, we select **SAP_class** (see Figure 2.2).

6. Click the **Finished** button. The HTTP Class Profile is now associated with the Virtual Server.
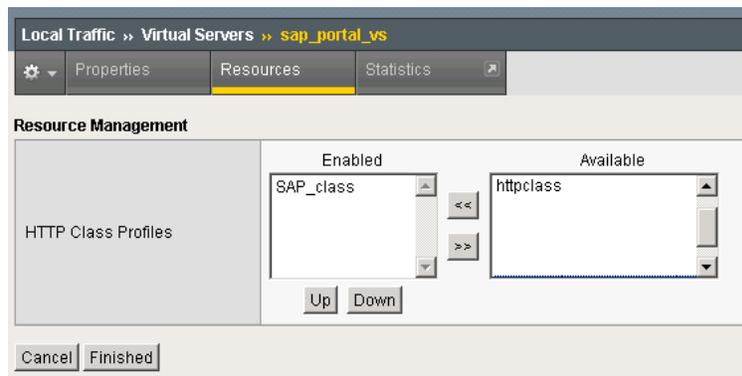

Figure 2.2 Adding the HTTP Class Profile to the Virtual Server

◆ **Important**

*You must have created an HTTP profile on the BIG-IP LTM system that has RAM Cache enabled. In our example (**Creating an HTTP profile**, on page 1-28) we use a parent profile that includes RAM Cache. If you did not create an HTTP profile with RAM Cache enabled, you must create a new HTTP profile, based on a parent profile that uses RAM Cache (such as HTTP Acceleration), and modify the virtual server to use this new profile.*

*To create the HTTP profile, use **Creating an HTTP profile**, on page 1-28, selecting the HTTP Acceleration parent profile. You must leave RAM Cache enabled; all other settings are optional. To modify the virtual server, follow Steps 1 and 2 from the preceding procedure to access the virtual server, and then from the HTTP Profile list, select the name of the new profile you just created and click Update.*

Creating an Application

The next procedure is to create a WebAccelerator Application. The Application provides key information to the WebAccelerator so that it can handle requests to your application appropriately.

To create a new Application

1. On the Main tab, expand **WebAccelerator**, and then click **Applications**. The Application screen of the WebAccelerator UI opens in a new window.

2. Click the **Create** button.

3. In the Application Name box, type a name for your application. In our example, we type **SAP EP**.

4. In the **Description** box, you can optionally type a description.

5. From the **Central Policies** list, select **SAP Portal**. This is a pre-defined policy created specifically for SAP Enterprise Portal devices (see Figure 2.3).

6. If you are deploying WebAccelerator in a symmetrical deployment, from the **Remote Policy** list, select **SAP Portal**.
   If you not deploying a remote unit, leave this option at the default.

7. In the **Requested Host** box, type the host name that your end users use to access the SAP deployment. This should be the same host name you used in Step 6a in the preceding procedure. In our example, we type **myportal.companyxyz.com**
   If you have additional host names, click the **Add Host** button and enter the host name(s).

8. Click the **Save** button.

Figure 2.3 *Configuring an Application on the WebAccelerator (not a symmetrical deployment)*

The rest of the configuration options on the WebAccelerator are optional, configure these as applicable for your network. With this base configuration, your end users will notice an marked improvement in performance after their first visit.

Configuring the WebAccelerator in a symmetric deployment

If you are using the WebAccelerator device in a symmetric configuration, you must also perform the following procedure on the remote WebAccelerator device. We also recommend that you consult BIG-IP documentation available on *Ask F5*.

Configuring the Remote WebAccelerator

In this section, we configure the remote WebAccelerator device. That is the one in the remote data center, furthest from the servers.

The remote device will log into the Central device and copy the configuration. This is done using the command line.

◆ **Note**

This procedures requires a Self IP address on the BIG-IP system. This Self IP can be a self-IP that is created specifically for the connection between the two BIG-IP systems, or one that is configured for other purposes. See the BIG-IP documentation about how to create Self IP addresses. Make sure that the Self IP addresses for symmetric WebAccelerator can communicate each way over TCP port 4353.

To configure the remote WebAccelerator using the command line

1. Log into the Remote Device via the command line. Refer to the product documentation on how to enable terminal access.

2. Change directory to **/usr/local/wa/scripts**:

   `cd /usr/local/wa/scripts`

3. Execute the wam_add.pl script:

   `./wam_add.pl`

   This script walks you through the instructions on how to synchronize from your Central Device to your Remote Device. The steps are as follows:

   a) Read the Warning and indicate that you are absolutely sure you want to continue. Type **Y**, then press Enter.

   b) Type the Self IP address of the Central WebAccelerator (see note above). In our case, we type:

   `10.133.58.235`

   c) Type the password for the Central WebAccelerator:

   `<your root password>`

d) An SSH key trust is established with the Central WebAccelerator. In this step, you are asked if you want to connect to the self-IP you entered in step 2. Type Yes, and then press Enter.

The script then synchronizes configuration settings and remote any errors. You may be prompted for the password one more time.
You then see the following message:

The WebAccelerator configuration has been successfully retrieved from central WebAccelerator [10.133.58.235]. This WebAccelerator should now remain synchronized with the central.

This indicates Symmetric WebAccelerator has been configured successfully. Any changes to application policies are synchronized between the Central and the Remote Device.

To verify the process was successful, you can return to the WebAccelerator web interface, and click **Symmetric Deployment** in the navigation pane. You should see a green circle icon next to each data center.

This concludes the WebAccelerator configuration.

3

Deploying the BIG-IP Edge Gateway with SAP NetWeaver and Enterprise SOA

Deploying the BIG-IP Edge Gateway with SAP NetWeaver and Enterprise SOA

This section of the Deployment Guide shows you how to configure F5's Edge Gateway for secure remote access to SAP deployments.

F5 BIG-IP® Edge Gateway™ is an access solution that brings together SSL VPN remote access, security, application acceleration, and availability services for remote users. BIG-IP Edge Gateway drives identity into the network to provide context-aware, policy-controlled, secure remote access to applications at LAN speed.

Prerequisites and configuration notes

The following are prerequisites for this deployment:

◆ The BIG-IP Edge Gateway should be running version 10.1 or later.

◆ This deployment was tested using SAP ERP 6.0 based on NetWeaver 7.0, load balanced by a BIG-IP LTM system as described in this Deployment Guide. For information on how to configure SAP devices, consult the appropriate SAP documentation.

◆ Our configuration scenario uses previously defined Active Directory groups to provide authentication and simple user maintenance. For information on how to configure Active Directory groups, consult the proper documentation.

◆ This deployment Guide is written to the scenario outlined in the following section. It is meant as a template; modify the configuration as necessary for your deployment.

Configuration scenario

For the scenario used in this deployment guide, the SAP deployment, along with an LDAP instance (for AAA services), reside behind a BIG-IP Edge Gateway in the Seattle location. In this scenario we illustrate a requirement to allow global employees remote access to all internal resources and to provide Wide Area Network acceleration services for branch offices.

This deployment guide first describes how to setup Edge Gateway to provide remote access in the branch office, located in London in our example. The same procedure is then be repeated for an Edge Gateway located in Seattle. Object caching of HTTP and HTTPS portal elements is achieved through the use of symmetric WebAccelerator (WAM). WAN optimization is achieved through the WOM module. The complete package of WAM, WOM and Remote Access comprise the product which is Edge Gateway.

Configuring the BIG-IP Edge Gateway

In this section, we configure the BIG-IP Edge gateway device in the branch office, located in London in our example. To configure the BIG-IP Edge you must complete the following procedures:

- *Configuring remote access*, following
- *Creating a Webtop*, on page 3-5
- *Creating an AAA Server*, on page 3-6
- *Creating an Access Profile*, on page 3-7
- *Editing the Access Profile with the Visual Policy Editor*, on page 3-7
- *Creating the Network Access BIG-IP configuration objects*, on page 3-10
- *Creating the profiles*, on page 3-10
- *Creating the virtual servers*, on page 3-12

Configuring remote access

To configure Remote Access, a Device Wizard is included in the product that assists in the setup of Network Access. In this guide, we describe the steps to complete the configuration manually.

To configure remote access

1. On the Main tab, expand **Access Policy**, and then click **Network Access**.

2. Click the **Create** button.

3. In the **Name** box, type a name for this Network Access Profile. In our example, we type **London_Remote_Access**. You can optionally type a description.

4. In the General Settings section, next to **Lease Pool**, click the Add (**+**) button. The Lease Pool is the pool of IP Addresses that clients receive when they connect to the VPN.

   a) In the **Name** box, type a name for the Lease pool. In our example, we type **London_Lease_Pool**.

   b) Click the **IP Address Range** button.

   c) In the **Start IP Address** and **End IP Address** boxes, type the appropriate IP addresses. In our example, we allow addresses from **10.0.1.1** to **10.0.1.255**.

   d) Click the **Add** button.

e) Click the **Finished** button. You return to the Network Access list.

Figure 3.1 *Configuring the Lease Pool*

5. If necessary, from the **Lease Pool** list, select the lease pool you just created. In our example, we select **London_Lease_Pool**.

6. From the **Compression** list, select **GZIP Compression**. This allows both the web browser client and the thick client to take advantage of compression between the client and the remote access server.

   Note: If DTLS is configured (UDP based communication between client and Remote Access Server) GZIP compression is automatically disabled. DTLS and GZIP for SSL VPN access is not currently supported.

Figure 3.2 *Configuring Network Access*

7. From the **Client Settings** list, select **Advanced**.

8. In the Traffic Options section, you can choose to Force all traffic through the tunnel, or use split tunneling. With Split Tunneling enabled, the administrator needs to indicate which subnets should be routed through the VPN tunnel. If Split tunneling is not allowed, all traffic will go through the tunnel.

a) If you want all traffic to go through the tunnel, click **Force all traffic through tunnel**, and continue with Step 8.

b) If you want to use split tunneling, click **Use split tunneling** for traffic. The split tunneling options appear.

- In the LAN Address Space section, type the IP address and Mask of the LAN Address space that should go through the tunnel. In our example we indicate that **192.168.0.0/16** is all LAN space.

- In the DNS Address Space section, type the DNS name(s) that are used in the target LAN.

- In the Exclude Address Space section, type the IP address and Mask of any address space that should be excluded. For example, if a portion of **192.168.0.0/16** should be excluded, it can be entered here. In our example, we indicate that **192.168.10.0/24** is excluded.

Figure 3.3 Split tunneling options

9. The remaining options are also administrative, configure the settings as applicable to your configuration. In our testing and architecture we generally recommend the following settings:

   a) In the Client Side Security section, we select **Prohibit routing table changes during Network Access Connection**.

   b) In the Reconnect To Domain section, we select **Synchronize with Active Directory policies on connection establishment**.

   c) In the DTLS section, check the box to enable DTLS. We recommend using DTLS protocol for optimum performance.

   Note: DTLS uses UDP port 4433 by default. Arrange to open this port on firewalls as needed.
   For DTLS, a UDP Virtual Server is required (described in Creating the virtual servers, on page 12).

10. Click **Finished**.

Creating a Connectivity Profile

The next task is to create a connectivity profile.

To create a connectivity profile

1. On the Main tab, expand **Access Policy**, and then click **Connectivity Profile**.

2. Click the **Create** button.

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

4. Configure the rest of the options as applicable to your configuration. In our example, we leave all settings at the default.

5. Click **Finished**.

Creating a Webtop

In the BIG-IP Edge, a Network Webtop is a *pointer* that initiates the download of the Edge client for browsers. Note that to distribute the non-browser version of the BIG-IP Edge client for Windows, you must do so using other methods, the Webtop does not distribute this client.

To create a Webtop

1. On the Main tab, expand **Access Policy**, and then click **Webtops**.

2. Click the **Create** button.

3. In the **Name** box, type a name for this webtop. In our example, we type **London_Webtop**.

4. From the **Type** list, select **Network Access**.

5. If you want the browser window to be minimized to the system tray for Windows hosts, check the **Enabled** box.

6. Click **Finished**.

Figure 3.4 *Webtop configuration*

Creating an AAA Server

The Edge Gateway does not have a built-in authentication store therefore an authentication source must be specified. In this procedure, we create an AAA server.

To create an AAA server

1. On the Main tab, expand **Access Policy**, and then click **AAA servers**.

2. Click the **Create** button.

3. In the **Name** box, type a name for this profile. In our example, we type **Seattle_LDAP_server** because we traverse the wide-area-network back to Seattle to perform authentication.

4. From the **Type** list, select the appropriate authentication method. For this example, we select **LDAP**.

5. In the Configuration section, type the appropriate information relevant to your authentication method. In our LDAP example, we provide the Host name for the LDAP server, the Admin DN, the Admin Password and we leave the timeout at default.

6. Click **Finished**.

Creating an Access Profile

The Access Profile ties together all of the other pieces in order to create a Network Connection VPN Tunnel. The Access Profile is also where the Visual Policy Editor (VPE) is located, which allows for complex workflows to be designed.

To create an Access Profile

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.

2. Click the **Create** button.

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

4. In the *Settings* section, configure the options as applicable for your configuration. In our example, we leave all of the settings at their defaults. Note that depending on licensing, the number of concurrent users may be limited. The other timeouts are administrative choices.

5. In the *Configuration* section, configure the settings as applicable to your environment. In our example, we accept all of the defaults. We are not using Single-Sign-On configurations or specific Logout URIs. However, we do leave **Secure Cookie** checked.

6. In the *Language Settings* section, if you are configuring the Edge Gateway in a language other than English, configure as applicable for your language. In our example, we accept English as the default language.

7. Click **Finished**.

Editing the Access Profile with the Visual Policy Editor

The next task is to open the London Access Policy and edit the Access Policy using the Visual Policy Editor (VPE). The VPE is a powerful visual scripting language that offers virtually unlimited options in configuring an Access Policy. For detailed information on the VPE please see the product documentation.

In the following procedure, we configure a policy using the Visual Policy Editor. However, Device Wizards provide an easy way to create more interesting policies, including ones that check for Virus Software and other prerequisites before allowing a user to logon. In this guide, it is our goal to get you oriented with the concepts of the Visual Policy Editor. In this example, we create a Login Page, an LDAP auth, and assign the resources allowed.

To edit the Access Profile

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.

2. Locate the Access Profile you just created, and in the Access Policy column, click **Edit**.
The Visual Policy Editor opens in a new window.

3. Click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.

4. Click the **Logon Page** option button, and then click the **Add Item** button at the bottom of the box.

5. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.

6. Click the **Save** button.

7. Click the **+** symbol between **Logon Page** and **Deny**.

8. In the Authentication section, click the **LDAP Auth** option button, and then click the **Add Item** button.
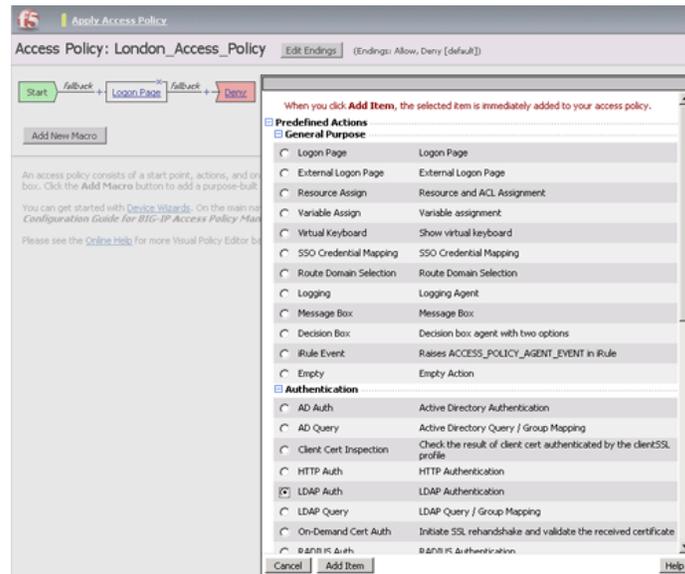
Figure 3.5 LDAP Auth configuration in the VPE

9. From the Server list, select the AAA Source you created in *Creating an AAA Server*, on page 6.

10. Add **SearchDN** and **SearchFilter** items as applicable for your configuration.

11. Click the **Save** button. You now see two paths, **Successful** and **Fall Back**.

12. Click the **Deny** box from the path leading from Successful. The Select Ending box opens.

13. Click the **Allow** button, and then click **Save**. In our example, we leave the fallback as Deny.

14. Click the **+** symbol between **LDAP Auth** and **Allow**.

15. In the General Purpose section, click the **Resource Assign** option button, and then click **Add Item**.

16. Click the **Add new entry** button.

17. Click **Set Network Access Source**, and then click the option button for the Network Access Source you created in *Configuring remote access*, on page 3-2. In our example, we click **London_Remote_Access**. This associates the Lease Pool and other settings. Click the **Update** button. You return to the Resource Assign page.

18. Click **Set Webtop**, and then click the option button for the Webtop you created in *Creating a Webtop*, on page 5. In our example, we click **London_Webtop**. Click the **Update** button.
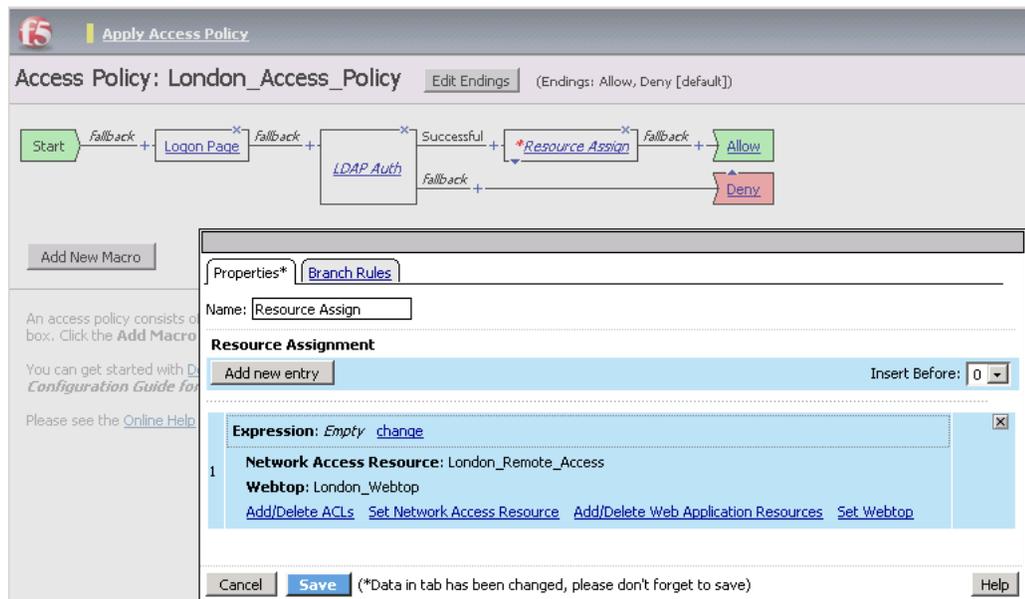
Figure 3.6 Resource Assigning configuration

19. Click the **Save** button. The Resource Assignment window closes and you return to the Visual Policy Editor main page.

    At this point you have the basics for a functional access policy.

20. Click the yellow **Apply Access Policy** link in the upper left part of the window. You always have to apply an access policy before it takes effect.

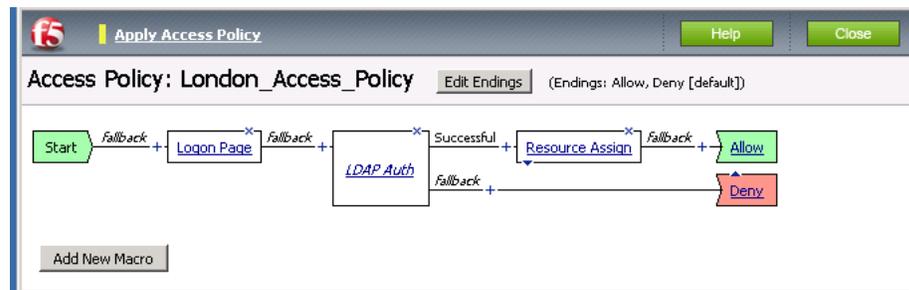21. Click the **Close** button on the upper right to close the VPE.

Figure 3.7 Completed Access Policy

Creating the Network Access BIG-IP configuration objects

The next task is to create the external Virtual Server that allows users to initiate their connection to the SSL VPN from either the web browser or the BIG-IP Edge Client for Windows. In our example, we have chosen to allow DTLS as a connection method and we will create two virtual servers, one for TCP 443 and one for UDP 4433.

The first task is to create profiles that are used by the virtual servers.

Creating the profiles

The next step is to create the profiles. Although you may use the default profiles, we strongly recommend you create new profiles based on the default parent profiles. By creating new profiles, you may easily modify the profile settings specific to your deployment without altering default global behaviors.

Creating TCP profiles

The next task is to create the TCP profiles. We recommend creating **tcp-lan-optimized** and **tcp-wan-optimized** profiles.

Creating the LAN optimized TCP profile

The first TCP profile we create is the LAN optimized profile.

To create a new LAN optimized TCP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens by default.

2. On the Menu bar, from the **Protocol** menu, select **TCP**.

3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.

4. In the **Name** box, type a name for this profile. In our example, we type **edge_tcp_lan**.

5. Modify any of the settings as applicable for your network. See the online help for more information on the configuration options. In our example, we leave the settings at their default levels.

6. Click the **Finished** button.

Creating the WAN optimized TCP profile

The next task is to create the WAN optimized profile.

To create a new WAN optimized TCP profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, from the **Protocol** menu, select **TCP**.

2. Click the **Create** button. The New TCP Profile screen opens.

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

4. Modify any of the settings as applicable for your network. See the online help for more information on the configuration options. In our example, we leave the settings at their default levels.

5. Click the **Finished** button.

Creating the HTTP profile

The next profile to create is the HTTP profile. This profile is required for the VPN to function. This should be a simple HTTP profile with no optimization (compression or caching).

To create the HTTP profile

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

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

3. Modify any of the settings as applicable for your network, but ***do not*** enable compression or RAM Cache. See the online help for more information on the configuration options. In our example, we leave the settings at their default levels.

4. Click the **Finished** button.

Creating a Client SSL profile

The next step is to create an SSL profile. This profile contains SSL certificate and Key information for offloading SSL traffic. The first task is to import the certificate and key (for this Deployment Guide, we assume that

you already have obtained the required SSL certificates, but they are not yet installed on the BIG-IP LTM system. If you do not have a certificate and key, see the BIG-IP documentation).

To import a key or certificate

1. On the Main tab, expand Local Traffic.

2. Click **SSL Certificates**. This displays the list of existing certificates

3. In the upper right corner of the screen, click **Import**.

4. From the **Import Type** list, select the type of import (**Certificate** or **Key**).

5. In the **Certificate** (or **Key**) **Name** box, type a unique name for the certificate or key.

6. In the **Certificate** (or **Key**) **Source** box, choose to either upload the file or paste the text.

7. Click **Import**.

8. If you imported the certificate, repeat this procedure for the key.

The next task is to create the SSL profile that uses the certificate and key you just imported.

To create a new Client SSL profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, from the **SSL** menu, select **Client**.

2. Click the **Create** button.

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

4. In the Configuration section, click a check in the **Certificate** and **Key** Custom boxes.

5. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.

6. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.

7. Click the **Finished** button.

Creating the virtual servers

The next task is to create the virtual servers for TCP 443 and UDP 4433.

To create the virtual server

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

2. In the upper right portion of the screen, click the **Create** button. The New Virtual Server screen opens.

3. In the **Name** box, type a name for this virtual server. In our example, we type **edge-tcp-443**.

4. In the **Destination** section, select the **Host** option button.

5. In the **Address** box, type the IP address of this virtual server. In our example, we use **10.133.20.200**.

6. In the **Service Port** box, type **443**, or select **HTTPS** from the list.

7. In the Configuration section, select **Advanced** from the list. The Advanced configuration options appear.

8. From the **Protocol Profile (Client)** list, select the name of the profile you created in the *Creating the WAN optimized TCP profile* section. In our example, we select **edge_tcp_wan**. This is optional.

9. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **edge_tcp_lan**.

10. From the **HTTP Profile** list, select the name of the profile you created in the *Creating the HTTP profile* section. In our example, we select **edge-http**.

11. From the **SSL Profile (Client)** list, select the SSL profile you created in the *Creating a Client SSL profile* section. In our example, we select **edge_https**.

12. In the Access Policy section, from the **Access Profile** list, select the name of the policy you created in *Creating an Access Profile*, on page 7. In our example, we select **London_Access_Policy**.

13. From the **Connectivity Profile** list, select the profile you created in *Creating a Connectivity Profile*, on page 5. In our example, we select **London_Connectivity_Profile**.

14. Leave the **Rewrite Profile** list set to **None**.

15. **Do not** configure any of the options in the WAN Optimization section.

16. Click the **Finished** button (this virtual server does not have any Resources).

17. Repeat this entire procedure for the UDP virtual server with the following exceptions.
    In Step 3, give this virtual server a unique name.
    In Step 5, use the appropriate IP address.
    In Step 6, in the **Service Port** box, type **4433**.
    After Step 7, from the **Protocol** list, select **UDP**.
    All other settings are the same.

Configuring the BIG-IP Edge for the second data center

Return to *Configuring the BIG-IP Edge Gateway*, on page 3-2 and repeat all procedures in this guide to configure the BIG-IP Edge for the second data center (Seattle in our example). Use unique names for the configuration objects.

As an option, you can use the BIG-IP Global Traffic Manager (GTM) to direct users to the closest Edge Gateway. The BIG-IP GTM configuration is outside the scope of this document.

4

Deploying the BIG-IP WOM with SAP NetWeaver and Enterprise SOA

Deploying the BIG-IP WOM with SAP NetWeaver and Enterprise SOA

In this chapter, we configure the BIG-IP WAN Optimization Module (WOM). BIG-IP WOM overcomes network and application issues on the WAN to ensure that all your users get the application availability and performance they need to stay productive. These services are integrated directly on your F5 BIG-IP device and include superior compression, encryption, and traffic control capabilities that dramatically reduce your bandwidth usage and enable you to improve quality of service for the critical applications that drive your business.

Prerequisites

The following are prerequisites for the WOM deployment:

◆ You must have two WOM instances, one in each data center.

◆ TCP Port 443 must be open between the two boxes.

Configuring the BIG-IP WAN Optimization module

In this section, we configure the BIG-IP WAN Optimization Module. Much of the configuration needs to be completed on both the local and remote BIG-IP systems.

Performing the initial configuration tasks

In this section, we configure the BIG-IP system with required VLAN and Self IP address information. Complete these procedures only if you do not already configured these objects on the BIG-IP LTM.

Creating a VLAN

The task is to create a VLAN on the BIG-IP LTM system.

◆ **Note**

You may already have a VLAN on the BIG-IP system for the networks that will be optimized, including the SAP servers. If you do, continue with **Creating a self IP**, *on page 4-2.*

To create a VLAN

1. On the Main tab, expand **Network**, and then click **VLANs**.
   The VLANs screen opens.

2. Click the **Create** button.
   The new VLAN screen opens.

3. In the **Name** box, type a unique name for the VLAN. In our example we use **sap-vlan**.

4. In the **Tag** box, you can optionally type a tag. In our example, we leave this blank, and the BIG-IP LTM automatically assigns a tag.

5. In the Resources section, from the **Available** list, select the interface that will have access to tagged traffic, and add it to the **Untagged** box by clicking the Add (<<) button.
   In our example, we select **1.14**.

6. Click the **Finished** button.

Creating a self IP

Self IP addresses are the IP addresses owned by the BIG-IP LTM system that you use to access the VLANs. The next step in this configuration is to create a self IP address that is used in the local end point BIG-IP configuration.

To create a self IP address

1. On the Main tab, expand **Network**, and then click **Self IPs**.
   The Self IP screen opens.

2. Click the **Create** button.
   The new Self IP screen opens.

3. In the **IP Address** box, type a static IP address that resides on the VLAN you created in the preceding procedure.

4. In the **Netmask** box, type the corresponding subnet mask.

5. From the **VLAN** list, select the VLAN you created in *Creating a VLAN*. In our example, we select **sap-vlan**.

6. From the **Port Lockdown** list, select **Allow None**.

7. Click the **Finished** button. The new self IP address appears in the list.

8. Repeat this entire procedure on the remote endpoint BIG-IP system.
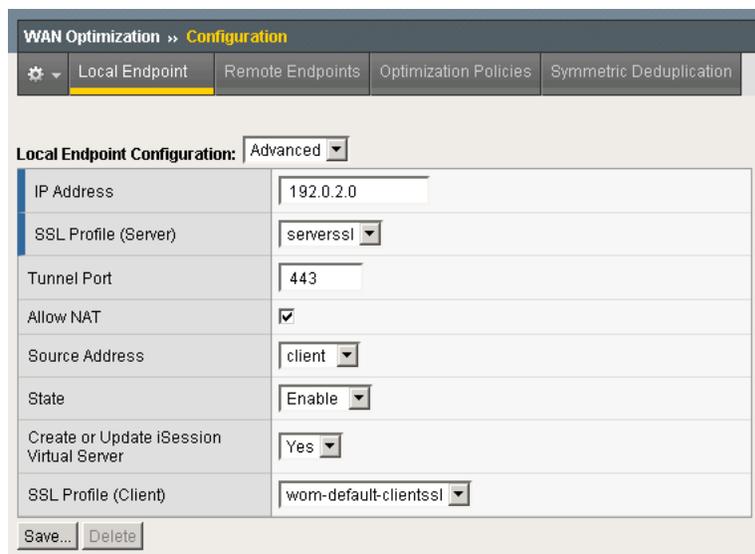
Configuring the WAN optimization module

In this section, we configure the WAN optimization module (WOM). The WAN optimization module allows you to encrypt and accelerate data between BIG-IP devices, accelerate applications across the WAN, and much more.

One of the options in configuring the WAN optimization module is the choice to use Dynamic Discovery. The benefit of dynamic discovery is that it reduces configuration complexity. However, when dynamic discovery is used, the BIG-IP currently disables iSession routing in order to prevent inadvertent routing loops. In our environment, dynamic discovery is allowed, but care was taken to ensure iSession routing was enabled.

To configure the WOM module

1. On the Main tab of the local BIG-IP system, expand **WAN Optimization**, and then click **Configuration**. The Local Endpoint Configuration screen opens.

2. In the **IP Address** box, type the BIG-IP self IP address you provisioned for iSession endpoint in the data center.

3. Make sure the **Create iSession Virtual Server** list is set to **Yes**.

4. Click the **Save** button.

Figure 4.1 Local Endpoint configuration

5. In the **Advertised Routes Configuration** section, click the **Create** button. The Advertised Route is the local subnet that the local endpoint advertises to all configured remote endpoints to which it is connected.

6. In the **Alias** box, type an alias for this route. This is optional. In our example, we type **vlan_1057**.

7. In the **Subnet Address** box, type the appropriate subnet address. In our example, we type **10.133.57.0**.

8. In the **Netmask** box, type the associated netmask. In our example, we type **255.255.255.0**.

9. Make sure the **Enabled** box is checked.

10. Click the **Finished** button.

Figure 4.2 Advertised Routes configuration

11. In the **Dynamic Discovery** section, we leave the default settings.

12. *Important:* Repeat this entire procedure on the remote endpoint BIG-IP system, using the appropriate BIG-IP self IP address in step 2, and the appropriate Advertised Route information.

After performing this procedure on both BIG-IP systems, continue with the following procedure, in which you connect your two BIG-IP systems together via an iSession tunnel by identifying each remote endpoint. If dynamic discovery was left on (as in step 11), you only perform the following procedure on one of the BIG-IP systems. If you did not, you must repeat this procedure on the remote BIG-IP system.

To configure the remote endpoints

1. On the Main tab of the local BIG-IP system, expand **WAN Optimization**, and then click **Configuration**.

2. On the Menu bar, click **Remote Endpoints**.

3. Click the **Create** button.

4. From the **Remote Endpoint** list, select **Advanced**.

5. In the **IP Address** box, type the IP address you provisioned for remote iSession endpoint.

6. *Important:* From the **Routing** list, select **Enabled**.

7. Click **Finished**.

8. If you disabled dynamic discovery in the previous procedure, you must repeat this procedure on the remote BIG-IP system.

Ensuring that iSession routing is enabled

As mentioned previously, if Dynamic Discovery is enabled, the BIG-IP system automatically sets remote endpoint routing to disabled. In this configuration, we want to ensure that remote endpoint routing is enabled (as in step 6 of the preceding procedure).

We recommend you check that routing is enabled after anytime the BIG-IP system reboots or hotfix/upgrade installations, as routing may revert to disabled to avoid any routing loops.

To ensure that iSession routing is enabled

1. On the Main tab of the local BIG-IP system, expand **WAN Optimization**, and then click **Configuration**.

2. On the Menu bar, click **Remote Endpoints**.

3. From the Remote Endpoints table, click the IP address of the appropriate endpoint.

4. From the **Routing** list, make sure that **Enabled** is selected. If it is not, select **Enabled** from the list.

5. Click the **Update** button.

6. Repeat this procedure on the remote BIG-IP system.

Creating the WAN Optimization policy

The next task is to create the WAN optimization policy. For this configuration, we create a new optimization policy for SAP.

To create a new WAN Optimization policy

1. On the Main tab, expand **WAN Optimization**, and then click **Configuration**.

2. On the Menu bar, click **Optimization Policies**.

3. Click the **Create** button.

4. From the **Common Application Optimization Policies** table, check the **http_optimize_client** box.

5. In the Select VLANs section, from the **LAN VLANs** and **WAN VLANs Available** lists, select the appropriate VLAN for your WOM networks, and then click the Add (<<) button.

6. Click the **Apply** button.

You have now enabled optimization on port 80, which optimizes all traffic in your SAP configuration.