DEPLOYMENT GUIDE
Version 2.1

Deploying F5 with Microsoft SharePoint 2010

Microsoft® Partner

Table of Contents

1

Deploying the BIG-IP System with Microsoft SharePoint 2010

- Introducing the F5 Deployment Guide for Microsoft SharePoint 2010
- Configuring the BIG-IP system for SharePoint
- Running the Microsoft SharePoint application template

Introducing the F5 Deployment Guide for Microsoft SharePoint 2010

Welcome to the F5 and Microsoft® SharePoint® 2010 Deployment Guide. This guide contains step-by-step procedures for configuring multiple F5 products for SharePoint 2010, resulting in a secure, fast and available deployment.

SharePoint Server 2010 enables innovative business collaboration for organizations around the world. F5 has developed a flexible and intelligent application delivery network for SharePoint 2010 that drives your business ahead. To read more about the benefits of using F5 for SharePoint 2010, see the Application Ready Solution Guide: ***http://www.f5.com/pdf/application-ready-network-guides/microsoft-sharepoint-2010-arsg.pdf***.

You can also visit the Microsoft page of F5's online developer community, DevCentral, for Microsoft forums, solutions, blogs and more (requires free registration): ***http://devcentral.f5.com/Microsoft/*****.**

This guide is divided into the following chapters:

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:

- For detailed information on how to deploy or configure Microsoft SharePoint 2010, consult the appropriate Microsoft documentation.
- For this guide the BIG-IP LTM must be running version 10.0 or a later version in the 10.x series. If you are using a previous or later 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 *SSL Certificates on the BIG-IP system*, on page 1-21.
- ***Important:*** When using the BIG-IP LTM system for SSL offload, for each SharePoint Web Application that will be deployed behind LTM, you must configure your SharePoint Alternate Access Mappings and Zones allow users to access non-SSL sites through the SSL virtual server

and ensure correct rewriting of SharePoint site links. See *Configuring SharePoint Alternate Access Mappings to support SSL offload*, on page 1-4.

- While we strongly recommend using the application template, you can manually configure the BIG-IP system. See *Manually configuring the BIG-IP LTM system with SharePoint 2010*, on page 2-1.
- Version 10.0 though 10.2 of the BIG-IP System contain an Application Template that is labeled for use with SharePoint 2007. However, this template may be used without modification for SharePoint 2010. A future release of BIG-IP will update the version labeling.
- All links to external documentation at third-party sites are accurate as of the publication date of this guide. Although F5 cannot guarantee that those links will remain accurate and functional, we will make every effort to update this document if we become aware of changes. Additionally, since this guide was written before SharePoint 2010 reached General Availability status, in some cases online documentation was only available for older versions of SharePoint; F5 will provide updated links as those become available.

◆ **Tip**

If you are using Microsoft FAST Search Server 2010 for SharePoint 2010, see ***www.f5.com/pdf/deployment-guides/microsoft-fast-search-2010-dg.pdf***

Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP System (LTM and WebAccelerator)	10.0, 10.1, 10.2, 10.2.2
Microsoft SharePoint	SharePoint 2010

Revision history:

Version	Description
1.0	New deployment guide
1.1	Added optional procedure for enabling **X-Forwarded-For** on the BIG-IP LTM, and the section *Optional: Using X-Forwarded-For to log the client IP address in IIS 7.0 and 7.5*, on page 1-18 for instructions on configuring IIS to log the client IP address.
1.2	Removed the chapter *Using the F5 Management and Designer Packs with Microsoft SCOM and SharePoint* to reflect the withdrawal of the free version of the F5 Management Pack.
1.3	Added guidance on using a new SharePoint 2010 WebAccelerator Policy for SharePoint 2010 that can improve the performance of non-collaborative SharePoint sites, such as public-facing internet portals. See *Downloading and importing the WebAccelerator policy*, on page 3-4.

Version	Description
1.4	Added an additional configuration scenario for the BIG-IP Access Policy Manager (Web Access Management mode) in Chapter 4.
1.5	Added support for BIG-IP version 10.2.2.
1.6	Added link to the Microsoft FAST Search Server 2010 deployment guide.
1.7	In Chapter 4, added an iRule to the BIG-IP APM Web Access Management section that supports the ability for users to edit Microsoft Office documents from the within a SharePoint site.
1.8	Modified the optional section on using X-Forwarded-For to log the client IP address in IIS 7 and 7.5 to include installing the Custom Logging service role, and steps for editing the IIS Log Definition to include the X-Forwarded-For header (3-13-2012)
1.9	Added instructions for configuring SharePoint Alternate Access Mappings if offloading SSL on the BIG-IP system. (3-26-2012)
1.9.1	Added additional instructions to the Alternate Access Mappings section for ensuring the search results are properly displayed for HTTPS queries. (4-3-2012).
2.0	Added *Troubleshooting*, on page 1-15.
2.1	Removed the ARX chapter

Configuration example

The BIG-IP system provides intelligent traffic management and high availability for Microsoft SharePoint Server 2010 deployments.

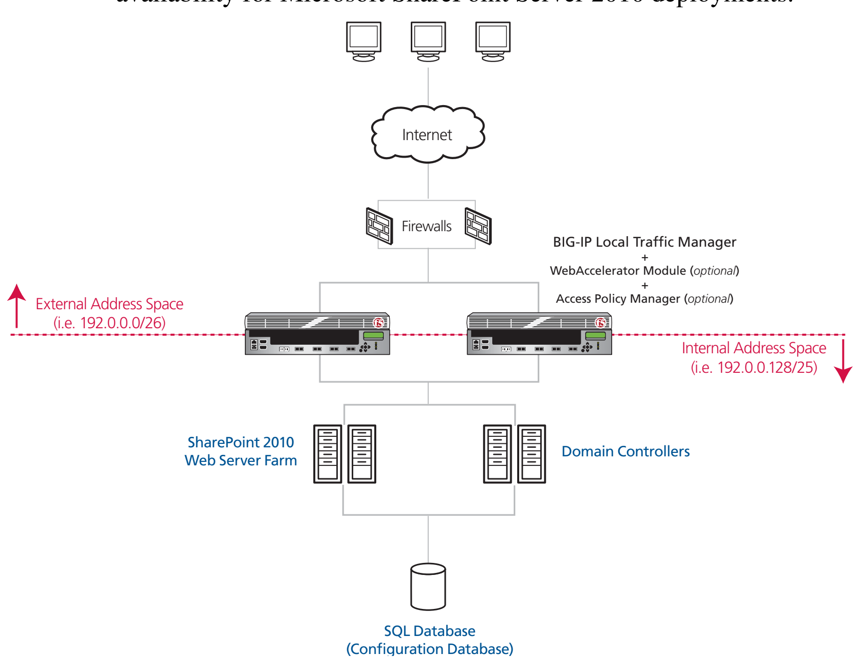

Figure 1.1 *Logical configuration example*

Configuring SharePoint Alternate Access Mappings to support SSL offload

If using the BIG-IP LTM system for SSL offload, for each SharePoint Web Application that will be deployed behind LTM, you must configure your SharePoint Alternate Access Mappings and Zones allow users to access non-SSL sites through the BIG-IP LTM SSL virtual server and ensure correct rewriting of SharePoint site links. For SSL offload, the Alternate Access Mapping entries must have URLs defined as https://<FQDN>, where FQDN is the name associated in DNS with the appropriate Virtual Server, and assigned to the SSL certificate within the Client SSL profile.

For each public URL to be deployed behind LTM, you must first modify the URL protocol of the internal URL associated with that URL and zone from http:// to https://: and then recreate the http:// URL. If you try to just add a new URL for HTTPS, it will not function properly.

For more information, see ***http://sharepoint.microsoft.com/blog/Pages/BlogPost.aspx?pID=804***.

To configure SharePoint Alternate Access Mappings

1. From SharePoint Central Administration navigation pane, click **Application Management**.
2. In the main pane, under Web Applications, click **Configure alternate access mappings**.
3. From the **Internal URL** list, click the Internal URL corresponding to the Public URL you want to be accessible through the BIG-IP LTM.
   The Edit Internal URLs page opens.
4. In the **URL protocol, host and port box**, change the protocol from **http://** to **https://**. You may want to make note of the URL for use in step 7.

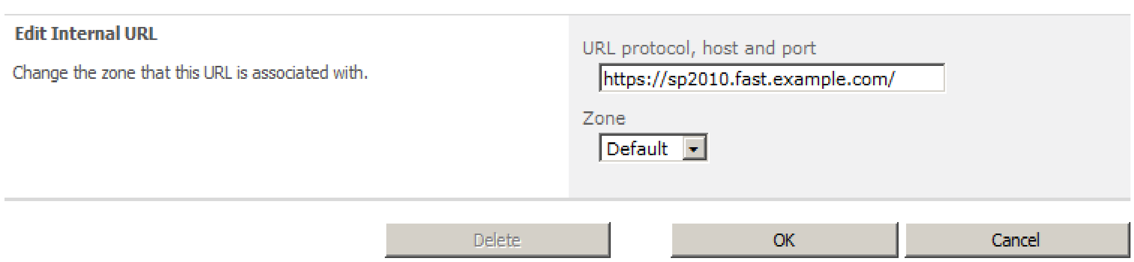

Figure 1.2 *Editing the Internal URL*

5. Click the **OK** button. You return to the Alternate Access Mappings page.
6. On the Menu bar, click **Add Internal URLs**.

7. In the **URL protocol, host and port box**, type the same internal URL used in step 4, but use the **http://** protocol. This allows access to the non-SSL site from behind the LTM.

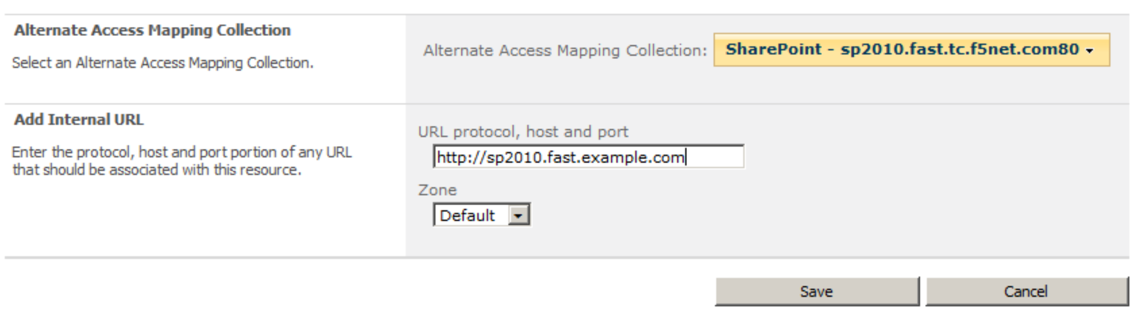

Figure 1.3 *Re-adding the HTTP Internal URL*

8. Click **Save**.
You must also add the new internal URL(s) to the list of Content Sources of Search Administration.
9. From the navigation pane, click **Application Management**, and then under **Service Applications**, click **Manage service applications**.
10. Click the name of your Search Service application. In our example, we are using Microsoft Fast Search Server, so the following examples are based on Fast Search Server.
11. In the navigation pane, click **Content Sources**.
12. On the Menu bar, click **New Content Source**.
13. In the **Name** box, type a name. We type **https://sp2010.fast.example.com**.
14. In the Start Addresses section, type the appropriate HTTPS URL. In our example, we type **https://sp2010.fast.example.com**. All other settings are optional.
15. Click the **OK** button (see Figure 1.4, on page 1-6).
16. Repeat this entire procedure for each public URL to be deployed behind LTM.

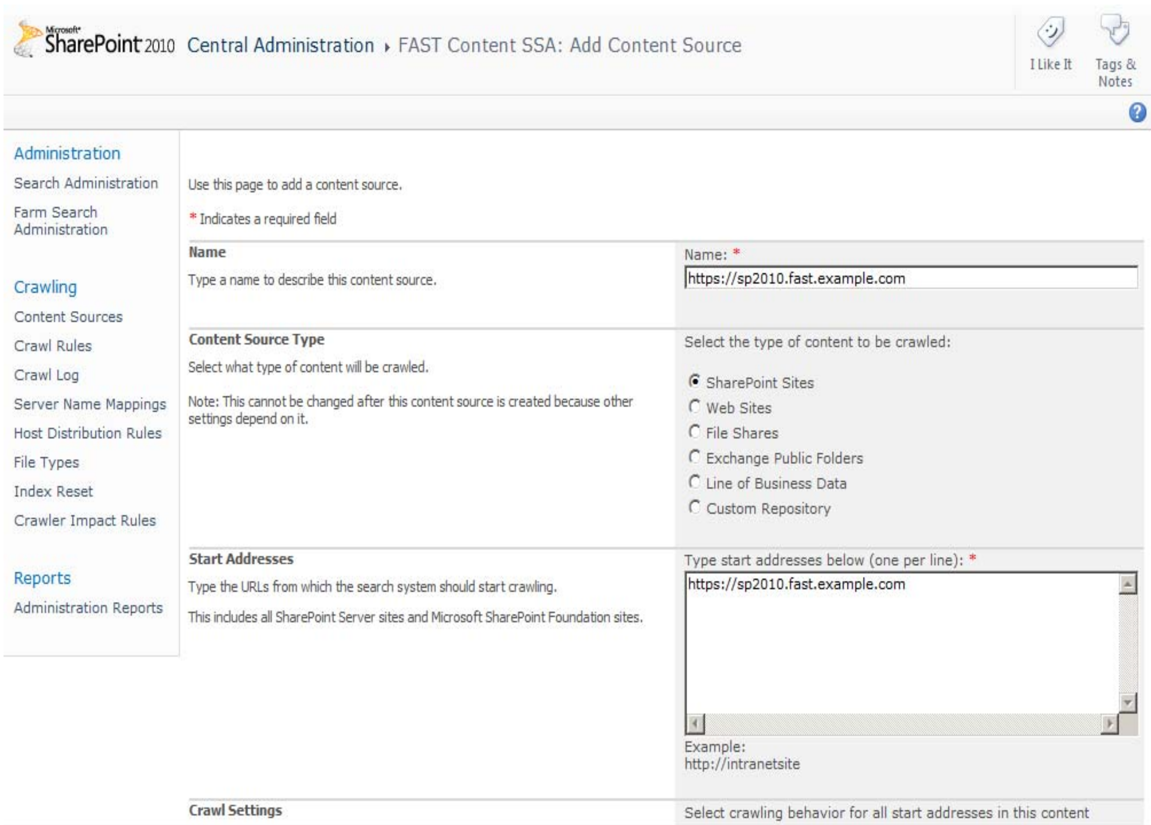

Figure 1.4 *Adding Content Source*

Displaying HTTPS SharePoint Search Results After Configuring Alternate Access Mappings for SSL Offloading

After configuring Alternate Access Mappings in SharePoint 2010 to support SSL offloading, you must perform the following procedure to ensure that search results are properly displayed for https:// queries. The examples below depict modifying the Content Search Service Application; however, you must also perform these steps on your Query Search Service Application.

To ensure HTTPS search results are displayed

1. From SharePoint Central Administration navigation pane, click **Application Management**.
2. Under Service Applications, click **Manage service applications**.
3. From the Service Application list, click your Content SSA. If you are using the default content SSA, this is “Regular Search”. If you are using FAST Search, this is the name you gave the content SSA (such as FAST Content SSA).
4. From the navigation pane, under Crawling, click **Index Reset**.

5. Click the **Reset Now** button to reset all crawled content.

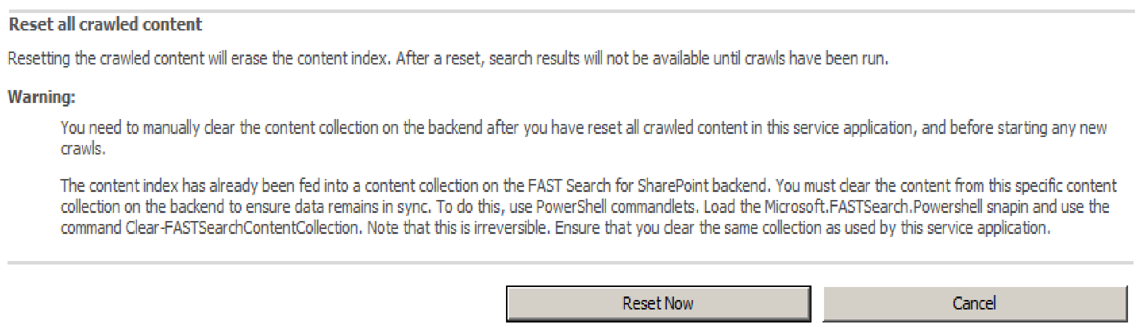

Figure 1.5 *Resetting the crawled content*

6. Return to your Content SSA (repeat steps 1-3).
7. From the navigation pane, under Crawling, click **Content Sources**.
8. Click the content source for which you just reset the search index.
9. From the Edit Content Source page, in the Start Full Crawl section, check the **Start full crawl of this content source** box and then click the **OK** button.

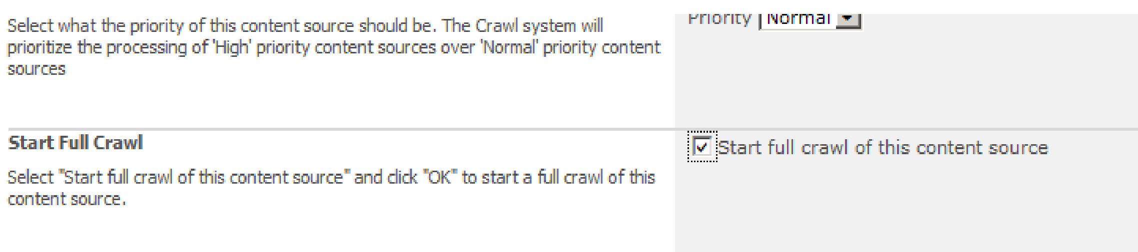

Figure 1.6 *Starting a full crawl of the content source*

When the crawl is complete, users should receive https:// addresses in their search query results.

Configuring the BIG-IP system for SharePoint

You can use the new Application Template feature on the BIG-IP system, to efficiently configure a set of objects corresponding to Microsoft SharePoint. 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.

If you prefer to manually configure the BIG-IP system, see *Manually configuring the BIG-IP LTM system with SharePoint 2010*, on page 2-1 and *Manually configuring the WebAccelerator module with SharePoint 2010*, on page 3-1.

◆ **Note**

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

◆ **Important**

All local traffic objects that an application template creates reside in administrative partition Common. Consequently, to use the application templates feature, including viewing the Templates list screen, you must have a user role assigned to your user account that allows you to view and manage objects in partition Common

Running the Microsoft SharePoint application template

To run the SharePoint application template, use the following procedure.

◆ **Important**

*As of the publication date of this document, current shipping versions 10.0 and greater of the BIG-IP software specify only **2007** as the supported version of SharePoint. As noted in the introduction to this guide, you may use that template without modification for SharePoint 2010.*

However, if you are using the WebAccelerator, we show you how to download the SharePoint 2010 policy from F5's DevCentral. DevCentral requires a free registration.

To run the Microsoft SharePoint 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 **Microsoft SharePoint**. The SharePoint application template opens.

4. In the Virtual Server Questions section, complete the following:

   a) You can type a unique prefix for your SharePoint objects that the template will create. In our example, we leave this setting at the default, **my_sharepoint**.

   b) Enter the IP address for this virtual server. The system creates a virtual server named **<prefix from step a>_virtual_server**. In our example, we type **192.0.2.10**.

   c) If the servers are configured to communicate responses to clients by 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 the **SNAT automap** feature to translate client source addresses to they appear to originate on the BIG-IP itself. See the Online Help for more information.
   In our example, we leave this at the default setting: **No**.

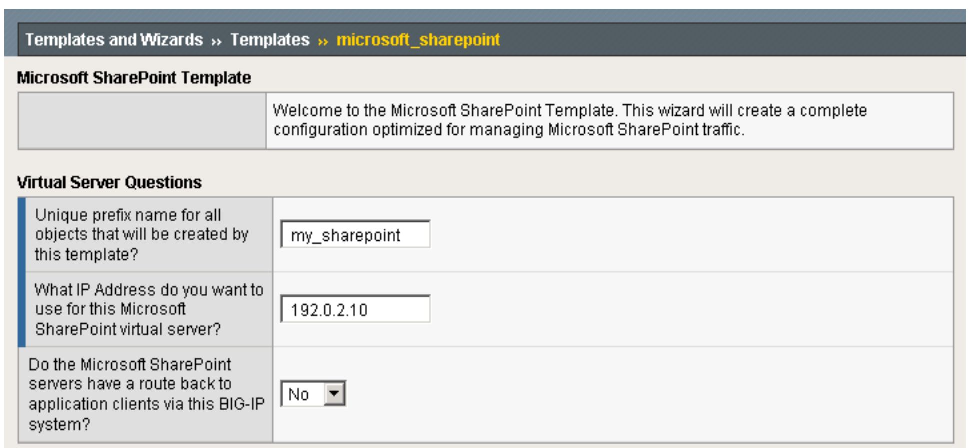

Figure 1.7 *Running the Microsoft SharePoint application template*

5. In the SSL Offload 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 SharePoint devices, select **Yes** from the list.
   The SSL options appear, including a note about configuring SharePoint Alternate Mappings and Zones (see the Configuration utility, or Figure 1.8 for the exact text). You can find more

information about Alternate Access Mappings in SharePoint 2010 at:
http://technet.microsoft.com/en-us/sharepoint/ff679917.aspx

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 *SSL Certificates on the BIG-IP system*, on page 1-21.

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 *SSL Certificates on the BIG-IP system*, on page 1-21.

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***.

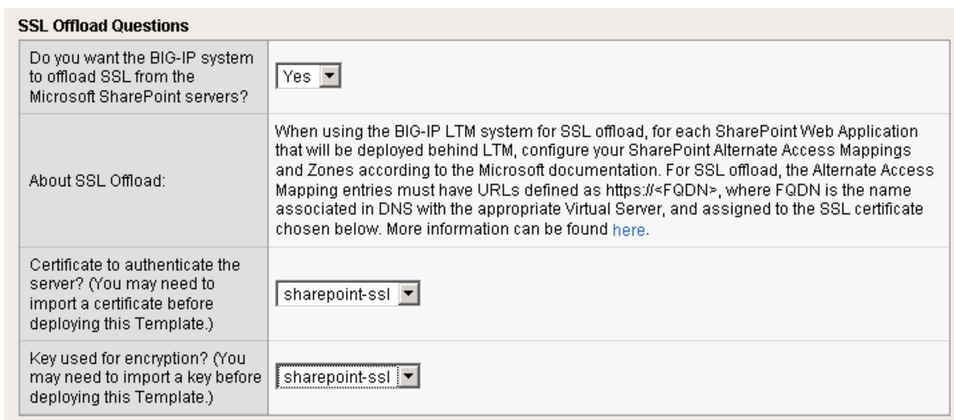

Figure 1.8 *Configuring the BIG-IP system for SSL Offload*

6. In the 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 SharePoint devices that are a part of this deployment.
In the **Address** box, type the IP address of the first SharePoint server. In our example, we type **192.0.2.129**.

In the **Service Port** box, type the appropriate port, or select it from the list. In our example, we select **HTTP** from the list.
Click the **Add** button. Repeat this step for each of the SharePoint 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. Note that HTTP 1.1 headers are added to the GET by default.

e) Select the HTTP version that the SharePoint servers expect clients to use. In our example, we select **Version 1.1**.

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

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

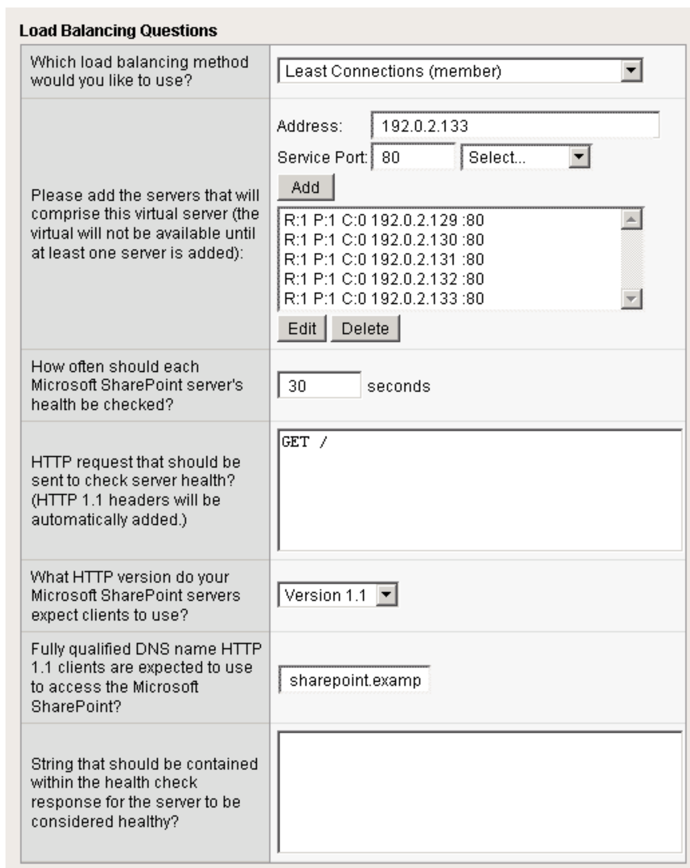

***Figure 1.9** Configuring the Load Balancing options*

7. 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 SharePoint 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 SharePoint deployments.

   Note: There is an optional SharePoint policy for WebAccelerator that can improve the performance of non-collaborative SharePoint sites, such as public-facing internet portals. This policy is not suitable for sites where users are changing or uploading content, or are making design changes to the site. See *Downloading and importing the WebAccelerator policy*, on page 3-4 for instructions on implementing this policy.

   c) If you want to use the Application Security Manager to secure the SharePoint 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 SharePoint deployment (the WebAccelerator application object's Requested Hosts field). Click the **Add** button. If you have additional host names, type each one in the **Host** box, followed by clicking the **Add** button.
   In our example, we type **sharepoint.example.com** and click the **Add** button (see Figure 1.10).

8. Click the **Finished** button.

After clicking Finished, the BIG-IP system creates the relevant objects. You see a summary screen that contains a list of all the objects that were created.

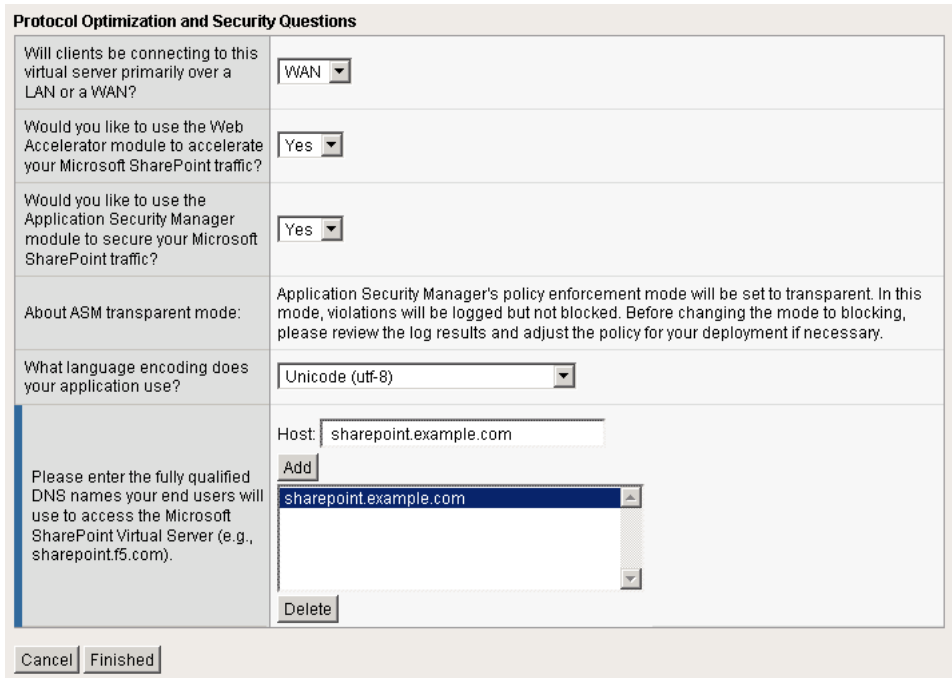

Figure 1.10 *Configuring the Protocol and Security options*

Optional: Creating the OneConnect profile

If you are ***NOT*** using NTLM authentication, we recommend you create one additional profile that was not created by template: 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. This can provide significant performance improvements for SharePoint implementations. For more information on OneConnect, see the BIG-IP LTM documentation.

In this section, we first create the OneConnect profile, then associate it with the virtual servers that were created by the Application template.

WARNING

If you are using NTLM authentication, the default authentication method for SharePoint Portal Server, do ***not*** *use a OneConnect profile on the BIG-IP system for this deployment.*

To create a new OneConnect 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 **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 **sharepoint-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.

The next task is to associate the OneConnect profile you just created with the virtual server(s) that were created by the Application Template. If you are not using the BIG-IP system to offload SSL, there is only one virtual server to modify; if you are offloading SSL, there are two.

To modify the existing SharePoint virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. From the Virtual Server list, find the HTTP virtual server that begins with the prefix you specified in step 4a. In our example, we left the prefix at the default, so we click **my_sharepoint-virtual_server**.
3. In the Configuration section, from the **OneConnect Profile** list, select the name of the profile you just created. In our example, we select **sharepoint-oneconnect**.
4. Click the **Update** button.

If you are using the BIG-IP system to offload SSL, repeat this procedure, but in step 2 select the HTTPS virtual server (it includes both the prefix you specified earlier, and is followed by **_https_**). In our example, we click **my_sharepoint_https_virtual_server**, and add our OneConnect profile.

Troubleshooting

Question:
Why does the SharePoint 2010 Document Library ribbon fail to load or get stuck on a status of **Loading…**?

Answer:
The F5 HTTP Compression profile may prevent the SharePoint Document Library ribbon from loading. Additionally, 401 Unauthorized responses may be seen for the ribbon object when analyzing HTTP traffic.

To solve this issue, create the following iRule and attach to the SharePoint virtual server to disable HTTP compression in responses to requests for this object.

To add the iRule

1. From the Main tab, expand **Local Traffic** and then click **iRules**.
2. Click the **Create** button.
3. In the **Name** box, give the iRule a name.
4. In the **Definition** section, copy and paste the following code:

```
when HTTP_REQUEST {
     if { [HTTP::uri] contains "commandui.ashx" } {
     COMPRESS::disable
     }
}
```

5. Click **Finished**.

You may need to clear the browser's cache after attaching the iRule.

After creating the iRule, you must attach it to the SharePoint virtual server.

To modify the existing SharePoint virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. From the Virtual Server list, find the HTTP virtual server that begins with the prefix you specified in step 4a. In our example, we left the prefix at the default, so we click **my_sharepoint-virtual_server**.
3. From the Menu bar, click **Resources**.
4. In the iRules section, click the **Manage** button.
5. From the **Available** list, click the name of the iRule you just created, and then click the Add (<<) button to move it to the Enabled list.
6. Click **Finished**.

Optional: Using the SharePoint 2010 WebAccelerator policy

If you are using the WebAccelerator, as of the initial publication date of this guide, BIG-IP software versions up to 10.2 list a Web Accelerator policy for SharePoint Services 2007, but not SharePoint 2010. Until this policy is a part of the user interface, we show you how to download the SharePoint 2010 policy from DevCentral. DevCentral requires a free registration.

Downloading and importing the WebAccelerator policy

You currently need to download and import the custom WebAccelerator policy (an XML file) for SharePoint 2010 from DevCentral. Later versions of the module will include this policy by default. Downloading and importing the policy is a simple two-part procedure.

◆ **Note**

You must be a member of DevCentral (requires a free registration) in order to download the policy.

To download and import the WebAccelerator policy

1. Open a web browser, and download the policy (an XML file) from the following page: ***http://devcentral.f5.com/wiki/default.aspx/WebAccelerator/Sharepoint2010WebAcceleratorPolicy.html***
2. Save the file in a place that is accessible from the WebAccelerator.
3. Return to the BIG-IP LTM system, and on the Main tab, expand **WebAccelerator**, and then click **Policies**. The Policy list opens.
4. In the upper-right section of the page, click **Import**.
5. Click the **Browse** button, and navigate to the location where you saved the XML file.
6. Click the **Import** button. The Policy is added to the list (see Figure 1.11).

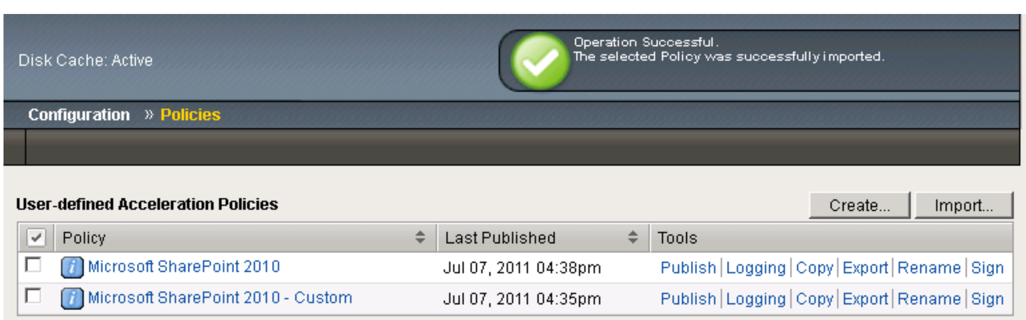

Figure 1.11 *SharePoint 2010 Policy*

7. On the Main tab, click **Applications**. The Applications list opens.
8. Click the name of the application that was created by the template. In our example, we used the default naming convention, so we click **my_sharepoint_web_acc_application**.
9. From the **Central Policy** list, select **Microsoft SharePoint 2010**.
10. Click the **Save** button.

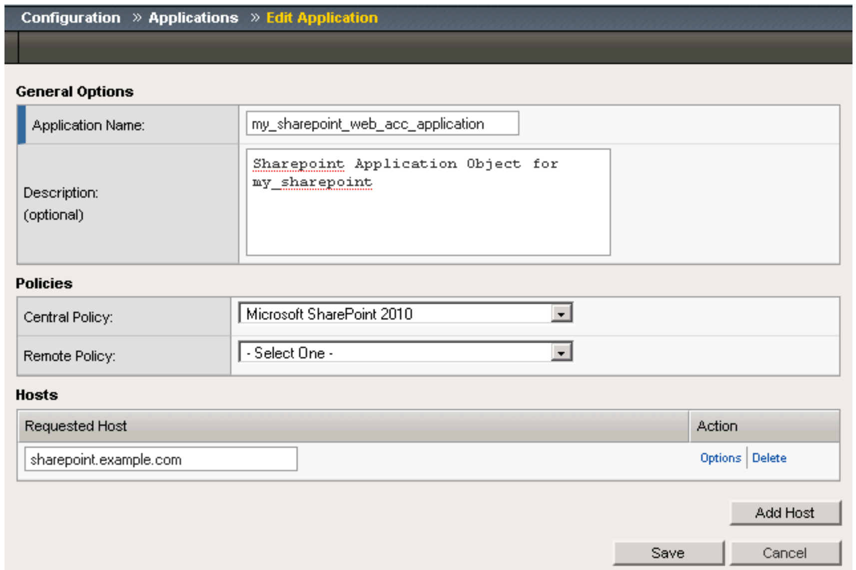

Figure 1.12 *WebAccelerator Edit Application page*

Optional: Using X-Forwarded-For to log the client IP address in IIS 7.0 and 7.5

When you configure BIG-IP LTM to use SNAT, the BIG-IP system replaces the source IP address of an incoming connection with its local self IP address (in the case of SNAT **Automap**), or an address you have configured in a SNAT pool. As a result, Microsoft IIS logs each connection with its assigned SNAT address, rather than the address of the client. By configuring an HTTP profile on the BIG-IP to insert an ***X-Forwarded-For*** header, the original client IP address is sent as well; however, in default IIS configuration, this information is not logged.

Beginning with IIS 7, Microsoft provides an optional Advanced Logging Feature for IIS that allows you to define custom log definitions that can capture additional information such as the client IP address included in the X-Forwarded-For header.

You must first enable X-Forwarded-For in the BIG-IP HTTP profile, and then add the log field to IIS.

Modifying the HTTP profile to enable X-Forwarded-For

The first task is to modify the HTTP profile created by the application template to enable the X-Forwarded-For header.

To modify the HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. From the HTTP profile list, select the profile created by the template. It is one of the following: **microsoft_sharepoint_http-wan-optimized-caching_shared_http** **microsoft_sharepoint_http-lan-optimized-caching_shared_http**.
3. In the Settings section, on the **Insert X-Forwarded-For** row, click the **Custom** box. From the list, select **Enabled**.
4. Click the **Update** button.

Deploying the Custom Logging role service

The next task is to deploy the Custom Logging role service. If you do not deploy this role service, you may receive a "Feature not supported" error when trying to edit the log definition in the next section.

To deploy the Custom Logging role service

1. From your Windows Server 2008 or Windows Server 2008 R2 device, open Server Manager.
2. In the Navigation pane, expand **Roles**.
3. Right-click **Web Server**, and then click **Add Role Services**.

4. Under *Health and Diagnostics*, check the box for **Custom Logging**, and then click the **Next** button.
5. On the Confirmation page, click **Install**.
6. After the service has successfully installed, click the **Close** button.

Adding the X-Forwarded-For log field to IIS

Before beginning the following procedure, you must have installed IIS Advanced Logging. For installation instructions, see http://www.iis.net/community/files/media/advancedlogging_readme.htm

◆ **Note**

If you are using IIS version 6, F5 has a downloadable ISAPI filter that performs a similar function to the Advanced Logging Feature discussed here. For information on that solution, see the DevCentral post at http://devcentral.f5.com/weblogs/Joe/archive/2009/08/19/x_forwarded_for_log_filter_for_windows_servers.aspx

To add the X-Forwarded-For log field to IIS

1. From your Windows Server 2008 or Windows Server 2008 R2 device, open the Internet Information Services (IIS) Manager.
2. From the Connections navigation pane, click the appropriate server, web site, or directory on which you are configuring Advanced Logging. The Home page appears in the main panel.
3. From the Home page, under IIS, double-click **Advanced Logging**.
4. From the Actions pane on the right, click **Edit Logging Fields**.
5. From the Edit Logging Fields dialog box, click the **Add Field** button, and then complete the following:
   a) In the **Field ID** box, type **X-Forwarded-For**.
   b) From the **Category** list, select **Default**.
   c) From the **Source Type** list, select **Request Header**.
   d) In the **Source Name** box, type **X-Forwarded-For**.
   e) Click the **OK** button in the Add Logging Field box, and then click the **OK** button in the Edit Logging Fields box.
6. Click a Log Definition to select it. By default, there is only one: %COMPUTERNAME%-Server. The log definition you select must have a status of Enabled.
7. From the Actions pane on the right, click **Edit Log Definition**.
8. Click the **Select Fields** button, and then check the box for the **X-Forwarded-For** logging field.
9. Click the **OK** button.
10. From the Actions pane, click **Apply**.

11. Click **Return To Advanced Logging**.
12. In the Actions pane, click **Enable Advanced Logging**.

Now, when you look at the logs, the client IP address is included.

SSL Certificates on the BIG-IP system

Before you can enable the BIG-IP LTM system to act as an SSL proxy, you must install a SSL certificate on the virtual server that you wish to use for SharePoint connections on the BIG-IP LTM 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 LTM system. 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***.

Importing keys and certificates

Once you have obtained a certificate, you can import this certificate into the BIG-IP LTM 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**. The list of existing certificates displays.
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.

2

Manually Configuring the BIG-IP LTM v10 with Microsoft SharePoint 2010

- Creating the HTTP health monitor
- Creating the pool
- Creating profiles
- Creating the HTTP virtual server
- Creating a default SNAT
- Configuring the BIG-IP LTM system for Microsoft SharePoint Server 2010 using SSL

Manually configuring the BIG-IP LTM system with SharePoint 2010

While we recommend using the application template, if you prefer to manually configure the BIG-IP LTM system rather than use the application template, perform the following procedures.

Creating the HTTP health monitor

The first step is to set up health monitors for the SharePoint devices. This procedure is optional, but very strongly recommended. For this configuration, we use an HTTP monitor, which checks pool members (IP address and port combinations), and can be configured to use **send** and **recv** statements in an attempt to retrieve explicit content from nodes.

To configure a 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 **SPSHTTP_monitor**.
4. From the **Type** list, select **http**.
5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout. In our example, we use a **Interval** of **30** and a **Timeout** of **91.**
6. In the **Send String** box, type a string. In our example, we type **GET / HTTP/1.1** to request the default page at the root level. You can modify this string to request a different resource or otherwise modify it as appropriate for your environment; however, in all cases, the Send String must be a valid HTTP request.
7. In the **Receive String** box, you can type an optional Receive string.
8. Click the **Finished** button. The monitor is added to the Monitor list.

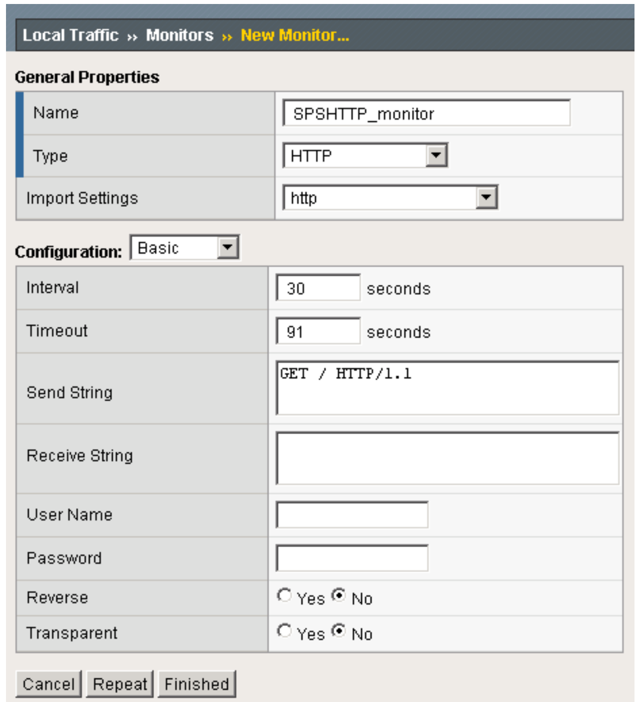

Figure 2.1 *Creating the HTTP Monitor*

Creating the pool

The next step in this configuration is to create a pool on the BIG-IP system. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. In this configuration, we create one pool for the SharePoint devices.

To create the SharePoint pool

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, enter a name for your pool. In our example, we use **SPS_Pool**.
5. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the HTTP health monitor* section, and click the Add (<<) button. In our example, we select **SPSHTTP_monitor**.

6. In the **Slow Ramp Time** box, type **300**. We set a higher Ramp Time because we are using the Least Connections load balancing method. This ensures that if a pool member becomes available after maintenance or a new member is added, the Least Connections load balancing algorithm does not send all new connections to that member (a newly available member will always have the least number of connections).

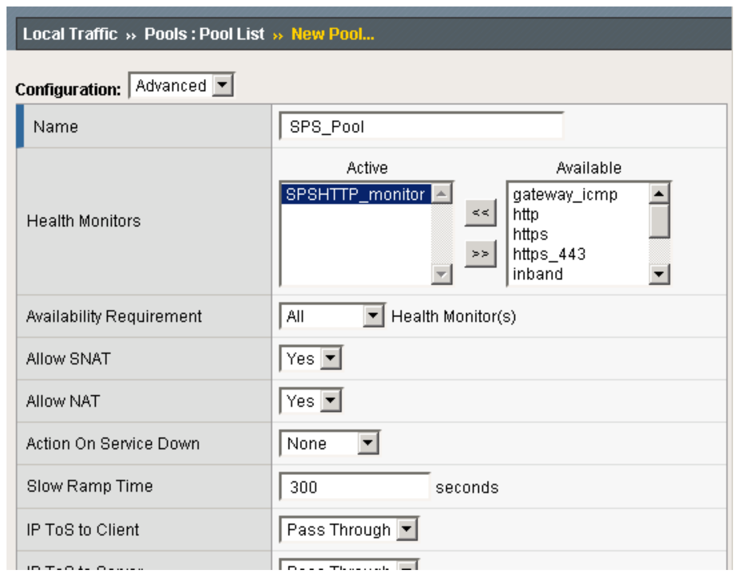

Figure 2.2 *Pool Configuration options (truncated)*

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. For this pool, we leave the Priority Group Activation **Disabled**.
9. In the New Members section, make sure the **New Address** option button is selected.
10. In the **Address** box, add the first server to the pool. In our example, we type **192.0.2.129**.
11. In the **Service Port** box, type the service number you want to use for this device, or specify a service by choosing a service name from the list.
    In our example, we type **80**.
12. Click the **Add** button to add the member to the list.
13. Repeat steps 9-11 for each server you want to add to the pool.
14. Click the **Finished** button (see Figure 2.3).

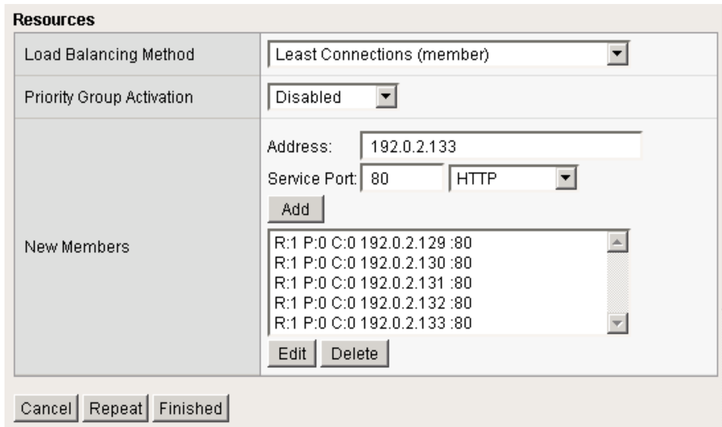

Figure 2.3 *Adding the SharePoint server pool*

Creating profiles

The next task to create the BIG-IP profiles. 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. 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.

Creating an HTTP profile

The first new profile we create is an HTTP profile. 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. There are a couple modifications to make no matter which profile you are using.
There are a couple of caveats for using this profile:

- If you are ***not*** terminating SSL (HTTPS) connections on the BIG-IP LTM, you must leave the **Redirect Rewrite** option at **None** (the default setting). **Redirect Rewrite** is meant to capture HTTP 3XX redirects and rewrite them to use HTTPS. See Step 5 in the following procedure.
- You must have Compression and RAM Cache licensed on your BIG-IP LTM system. Contact your Sales Representative for more information.

◆ **Note**

The following procedure shows one way to optimize the Microsoft SharePoint 2010 configuration that has been tested in real-world scenarios by F5, and shown to give the greatest improvement. These procedures and the specific values given in some steps should be used as guidelines, modify them as applicable to your configuration.

To create a new HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. 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 **SPS_HTTP_opt**.
4. From the **Parent Profile** list:
   - If you are using the WebAccelerator, select **http-acceleration**.
   - If you are not using the WebAccelerator, select **http-wan-optimized-compression-caching**.
5. If you intend to terminate SSL (HTTPS) connections on the BIG-IP LTM, in the Settings section, check the Custom box for **Redirect Rewrite**, and from the **Redirect Rewrite** list, select **Matching**. Otherwise, leave this at the default setting (**None**).
6. In the Compression section, check the Custom box for **Compression**, and from the **Compression** list, select **Enabled**.
7. In the RAM Cache section, check the Custom box for **URI Caching**, and leave **URI List** selected.
8. From the URI List section, in the **URI** box, type **/_layouts/images/*** and click the **Include** button. This ensures that all of the layout images are cached on the BIG-IP LTM system.

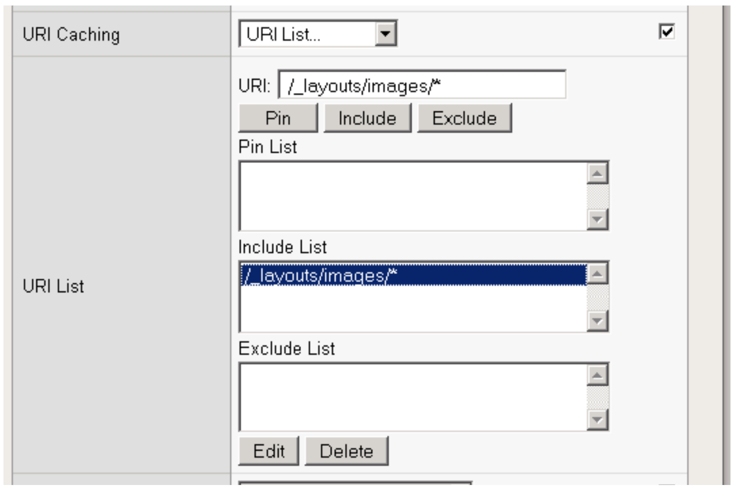

Figure 2.4 *URI Caching*

9. *Optional:* If you want to enable the X-Forwarded-For header for accurate logging, check the Custom box for **Insert X-Forwarded-For**, and from the list, select **Enabled**. See *Optional: Using X-Forwarded-For to log the client IP address in IIS 7.0 and 7.5*, on page 1-18 for detailed information, including modifications to IIS to accurately log the client IP address.
10. Modify any of the other settings as applicable for your network.
11. Click the **Finished** button.

Creating the TCP profiles

The next profiles we create are the TCP profiles. If most of the Microsoft SharePoint users are accessing the devices via a Local Area Network, we recommend using the **tcp-lan-optimized** (for server-side TCP connections) parent profile. If the majority of the users are accessing the system from remote or home offices, we recommend using an additional TCP profile, called **tcp-wan-optimized** (for client 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 LAN optimized TCP profile

First we configure the LAN optimized profile. If you do not want to use this optimized profile, you can choose the default TCP parent profile.

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 **SPS-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 the WAN optimized TCP profile

Now we configure the WAN optimized profile. Remember, if most of the users are accessing the system over the LAN or other low latency links, you do not need to create this 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 **SPS-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 a cookie persistence profile

The final profile we create is a Cookie Persistence profile. We recommend using the default cookie method for this profile (HTTP cookie insert), but you can change other settings, such as specifying a cookie expiration.

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 **SPSCookie**.
5. From the **Persistence Type** list, select **Cookie**.
   The configuration options for cookie persistence appear.
6. Modify any of the settings as applicable for your network.
7. Click the **Finished** button.

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

Creating the OneConnect profile

If you are ***NOT*** using NTLM authentication, we recommend you create one additional profile: 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. This can provide significant performance improvements for SharePoint implementations that do not use NTLM. For more information on OneConnect, see the BIG-IP LTM documentation.

WARNING

*If you are using NTLM authentication, the default authentication method for SharePoint Portal Server, do **not** use a OneConnect profile on the BIG-IP system for this deployment.*

To create a new OneConnect 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 **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 **SPS_oneconnect**.
5. From the **Parent Profile** list, ensure that **oneconnect** is selected.
6. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating the HTTP virtual server

Next, we configure a HTTP virtual server that references 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 **SPS_http_virtual**.
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 **192.0.2.10**.
6. In the **Service Port** box, type **80** or select **HTTP** from the list.

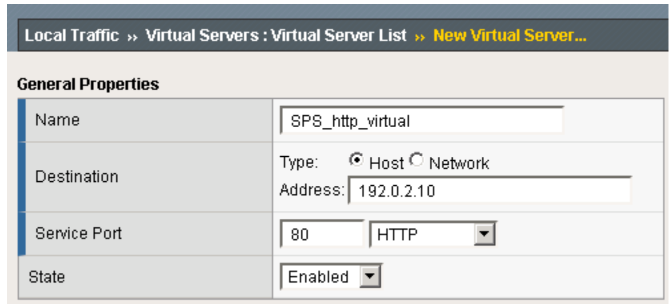

Figure 2.5 General Properties of the virtual server

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 the name of the profile you created in the *Creating the WAN optimized TCP profile* section. If you did not create a WAN optimized profile, select the LAN optimized profile as in the following Step. In our example, we select **SPS-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 **SPS-tcp-lan**.
11. From the **OneConnect Profile** list, if you created the optional OneConnect profile, select the profile you created in *Creating the OneConnect profile*, on page 2-7.
12. From the **HTTP Profile** list, select the profile you created in the *Creating an HTTP profile* section. In our example, we select **SPS_HTTP_opt**.

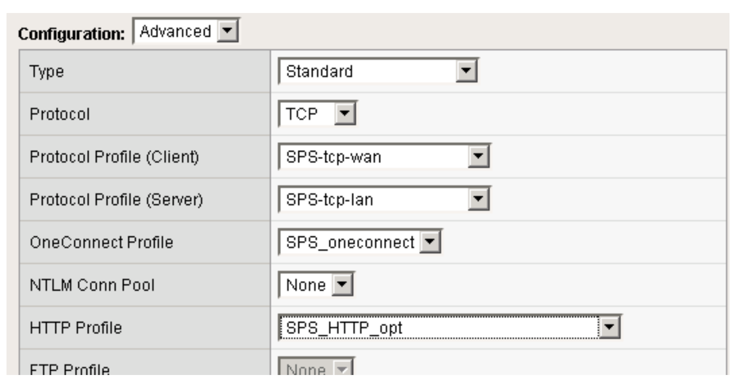

Figure 2.6 Configuration options of the virtual server (truncated)

13. In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **SPS_pool**.
14. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating a cookie persistence profile* section. In our example, we select **SPSCookie**.

Figure 2.7 *Resources section virtual server (truncated)*

15. Click the **Finished** button.

Creating a default SNAT

A secure network address translation (SNAT) ensures the proper routing of connections from the Index server to the Search server. In this configuration, we configure a default SNAT.

◆ Note

If you do not want source address translation on client connections from the external VLAN, you can disable the default SNAT for the external VLAN.

To create a default SNAT

1. On the Main tab, expand **Local Traffic**, and then click **SNATs**. The SNATs screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New SNAT screen opens.
3. In the **Name** box, type a name for this SNAT. In our example, we type **DefaultSNAT**.
4. In the **Translation** list, select **Automap**.
5. ***Optional:*** If you to disable (or enable) the default SNAT for specific VLANs, from the VLAN Traffic list, select either **Enabled on** or **Disabled on** from the list. From the Available list, select the appropriate VLAN and click the Add (**<<**) button to move it to the Selected list.
6. Click the **Finished** button.

Configuring the BIG-IP LTM system for Microsoft SharePoint Server 2010 using SSL

This section describes how to configure the BIG-IP LTM system as an SSL proxy for a Microsoft SharePoint Server 2010 deployment. If you are not using the BIG-IP LTM system to offload SSL traffic, you do not need to perform these procedures.

◆ **Note**

This section is written with the assumption that you have already configured your BIG-IP LTM system for a SharePoint deployment as described in this Deployment Guide.

Prerequisites and configuration notes

The following are additional prerequisites for this section:

- You need an SSL certificate for your site that is compatible with the BIG-IP LTM system. For more information, consult the BIG-IP documentation.
- You have already configured the BIG-IP LTM system as described in this Deployment Guide.
- ***Important:*** See *Configuring SharePoint Alternate Access Mappings to support SSL offload*, on page 1-4 for critical information about configuring SharePoint for the BIG-IP LTM and SSL offload.

This section contains following procedures for configuring the BIG-IP LTM system:

- *Using SSL certificates and keys*
- *Create a Client SSL profile*
- *Modifying the HTTP virtual server*
- *Creating the HTTPS virtual server*

Using SSL certificates and keys

Before you can enable the BIG-IP LTM system to act as an SSL proxy, you must install a SSL certificate on the virtual server that you wish to use for SharePoint 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 LTM 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 LTM 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 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**.

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

Create a Client SSL profile

The next step in this configuration is to create an SSL profile. This profile contains the SSL certificate and Key information for offloading the SSL traffic.

To create a new Client SSL profile based on the default 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 **SPS_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.

Modifying the HTTP virtual server

The next task is to modify the HTTP virtual server you created in *Creating the HTTP virtual server*, on page 8 to use the iRule you just created.

To modify the existing SharePoint virtual server

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 SharePoint virtual server you created in the *Creating the HTTP virtual server* section. In our example, we click **SPS_virtual**.
3. On the menu bar, click **Resources**.
   The Resources page for the virtual server opens.
4. From the **Default Pool** list, select **None**. This virtual server no longer requires the load balancing pool, as traffic is redirected to the HTTPS virtual server we create in the following procedure.
5. Click the **Update** button.
6. In the iRules section, click the **Manage** button.
   The Resource Management screen opens.
7. From the **Available** list, select the built-in iRule **_sys_https_redirect**, and click the Add (**<<**) button.
8. Click the **Finished** button.

Creating the HTTPS virtual server

The final task in this section is to create a HTTPS virtual server.

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 **SPS_httpsvirtual**.

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 **192.0.2.10**.
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 the name of the profile you created in the *Creating the WAN optimized TCP profile* section. If you did not create a WAN optimized profile, select the LAN optimized profile as in the following Step. In our example, we select **SPS-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 **SPS-tcp-lan**.
11. From the **HTTP Profile** list, select the name of the profile you created *Creating an HTTP profile* section. In our example, we select **SPS_HTTP_opt**.
12. From the **SSL Profile (Client)** list, select the name of the SSL profile you created in the *Create a Client SSL profile* section. In our example, we select **SPS_clientssl**.
13. From the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **SPSServers**.
14. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating a cookie persistence profile*. In our example, we select **SPSCookie**.
15. Click the **Finished** button.

This concludes the BIG-IP LTM configuration. See *Troubleshooting*, on page 1-15 for useful information.

3

Deploying the WebAccelerator v10 with Microsoft SharePoint 2010

- Creating an HTTP Class profile
- Modifying the Virtual Server to use the Class profile
- Creating an Application

Manually configuring the WebAccelerator module with SharePoint 2010

In this section, we configure the WebAccelerator module for SharePoint devices to increase performance for end users of SharePoint. 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/WebAccelerator/***.

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 SharePoint devices as described in this Deployment Guide.
- You must have licensed and provisioned the WebAccelerator module on the BIG-IP LTM system.
- This document is written with the assumption that you are familiar with the BIG-IP LTM system, WebAccelerator and Microsoft SharePoint Server 2010. Consult the appropriate documentation for detailed information.
- You should have configured an HTTP profile using the **http-acceleration** parent. See *Creating an HTTP profile*, on page 2-4 for more details.
- BIG-IP software versions up to 10.2.2 list a Web Accelerator policy for SharePoint Services 2007, but not SharePoint 2010. Until this policy is a part of the user interface, we show you how to download the SharePoint 2010 policy from DevCentral. DevCentral requires a free registration.
- There are also instructions for using an optional WebAccelerator policy that offers better performance for non-collaborative SharePoint sites. This policy requires a change to the Intelligent Browser Referencing (IBR) delimiter value in WebAccelerator. Note that changing this delimiter value will affect all applications that use WebAccelerator Intelligent Browser Referencing.
- In this guide, we assume you are configuring the WebAccelerator in an Asymmetric configuration. If plan on using a Symmetric configuration, but have not yet initially configured the central and remote WebAccelerator systems, refer to Chapter 3, *Initial Configuration and Maintenance Tasks*, in the **Configuration Guide for the BIG-IP WebAccelerator System**.

Configuration example

Using the configuration in this section, the BIG-IP LTM system with WebAccelerator module is optimally configured to accelerate traffic to Microsoft SharePoint 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 user connects to a SharePoint site through a BIG-IP LTM that is running the WebAccelerator module. On the first visit, documents that are not compressed by SharePoint are compressed by WebAccelerator for faster download. The WebAccelerator also marks objects for long-term caching by the browser.

On subsequent visits, the user experience is accelerated because the browser uses the dynamic or static objects that are stored in its local cache rather than retrieving them again over the WAN. Additionally, dynamic and static objects are cached at the WebAccelerator so they can be served quickly to all clients, whether on first or repeat visits, without requiring the server to re-serve the same objects.

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. In the upper right portion of the screen, click the **Create** button. The New HTTP Class Profile screen opens.
3. In the **Name** box, type a name for this Class. In our example, we type **sharepoint-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, 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 SharePoint site. In our example, we type **sharepoint.example.com** (see Figure 3.1).

   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 SharePoint deployment.

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

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

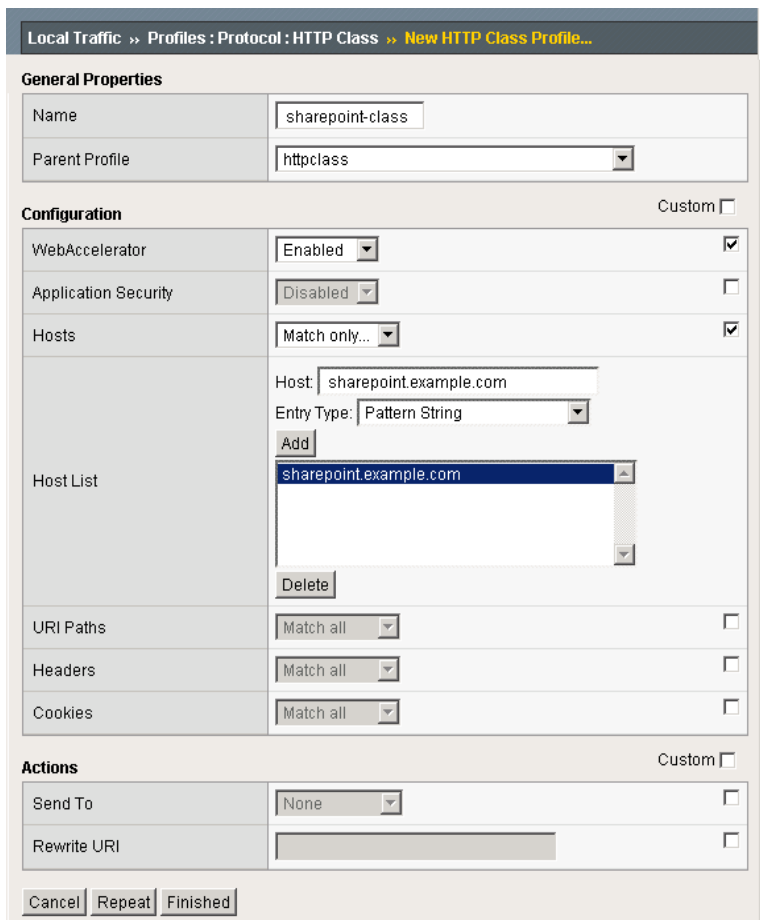

Figure 3.1 *Creating a new HTTP Class profile*

Modifying the Virtual Server to use the Class profile

The next step is to modify the virtual server for your SharePoint 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 your SharePoint deployment. In our example, we click **SPS_virtual**.
   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 **sharepoint_class** (see Figure 3.2).
6. Click the **Finished** button. The HTTP Class Profile is now associated with the Virtual Server.

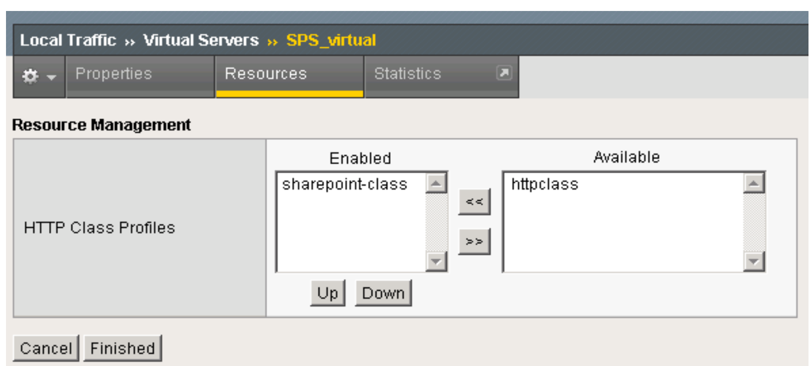

Figure 3.2 *Adding the HTTP Class Profile to the Virtual Server*

Downloading and importing the WebAccelerator policy

You currently need to download and import the custom WebAccelerator policy (an XML file) for SharePoint 2010 from DevCentral. Later versions of the module will include this policy by default. Downloading and importing the policy is a simple two-part procedure.

There are two policies you can choose from, depending on your configuration. The standard SharePoint 2010 policy, and a new policy that can improve the performance of non-collaborative SharePoint sites, such as public-facing internet portals. This policy is not suitable for sites where users are changing or uploading content, or are making design changes to the site. If you choose to use the new policy for non-collaborative sites, there is one additional procedure you must follow after downloading and importing the policy.

◆ **Note**

You must be a member of DevCentral (requires a free registration) in order to download the policy.

To download and import the WebAccelerator policy

1. Open a web browser, and download the appropriate policy (an XML file) from DevCentral:
    - Standard SharePoint 2010 policy: ***http://devcentral.f5.com/wiki/default.aspx/WebAccelerator/Sharepoint2010WebAcceleratorPolicy.html***
    - SharePoint 2010 policy for non-collaborative sites: ***http://devcentral.f5.com/wiki/default.aspx/WebAccelerator/SharePoint2010WebAcceleratorPolicyForNonCollaborativeSites.html***
2. Save the file in a place that is accessible from the WebAccelerator.
3. Return to the BIG-IP LTM system, and on the Main tab, expand **WebAccelerator**, and then click **Policies**. The Policy list opens.
4. In the upper-right section of the page, click **Import**.
5. Click the **Browse** button, and navigate to the location where you saved the XML file.
6. Click the **Import** button. The Policy is added to the list (see Figure 3.3). You choose the new policy in the next procedure.

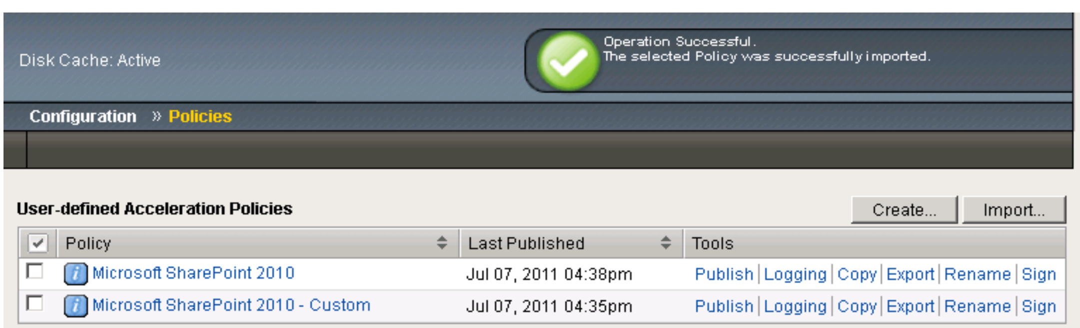

Figure 3.3 *Both of the SharePoint 2010 Policies*

Modifying the Intelligent Browser Referencing Delimiter if using the non-collaborative policy

If you are using the SharePoint 2010 policy for non-collaborative sites as described previously, you must modify the Intelligent Browser Referencing (IBR) delimiter.

◆ **Note**

If you are using the standard SharePoint 2010 policy, you do not need to modify the IBR delimiter. Continue with the next section.

◆ **WARNING**

Modifying this delimiter value changes the setting for all applications that use Intelligent Browser Referencing. Keep that in mind if you are using WebAccelerator with IBR for other applications.

To modify the IBR delimiter, follow the instructions found on DevCentral:
http://devcentral.f5.com/wiki/default.aspx/WebAccelerator/ModifyingTheIBRDelimiterForSharePointPolicy.html

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.

As mentioned in the prerequisites, we assume you are configuring the WebAccelerator in an Asymmetric configuration. If you are using a Symmetric configuration, see the **Configuration Guide for the BIG-IP WebAccelerator System** for specific configuration tasks related to the remote WebAccelerator system.

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 **New Application** button.
3. In the Application Name box, type a name for your application.
   In our example, we type **SharePoint2010-WebAccelerator**.
4. In the **Description** box, you can optionally type a description for this application.
5. From the **Central Policy** list, select the appropriate policy:
   - For the Standard SharePoint 2010 WebAccelerator Policy, select **Microsoft SharePoint 2010**.

- For the SharePoint 2010 WebAccelerator Policy for non-collaborative sites, select **Microsoft SharePoint 2010-Custom**.

6. *Optional*: If you are using the WebAccelerator in a Symmetric configuration, from the **Remote policy** list, select the same policy you selected in step 5. See the WebAccelerator documentation for more information about configuring the WebAccelerator in a Symmetric configuration.

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

8. Click the **Save** button.

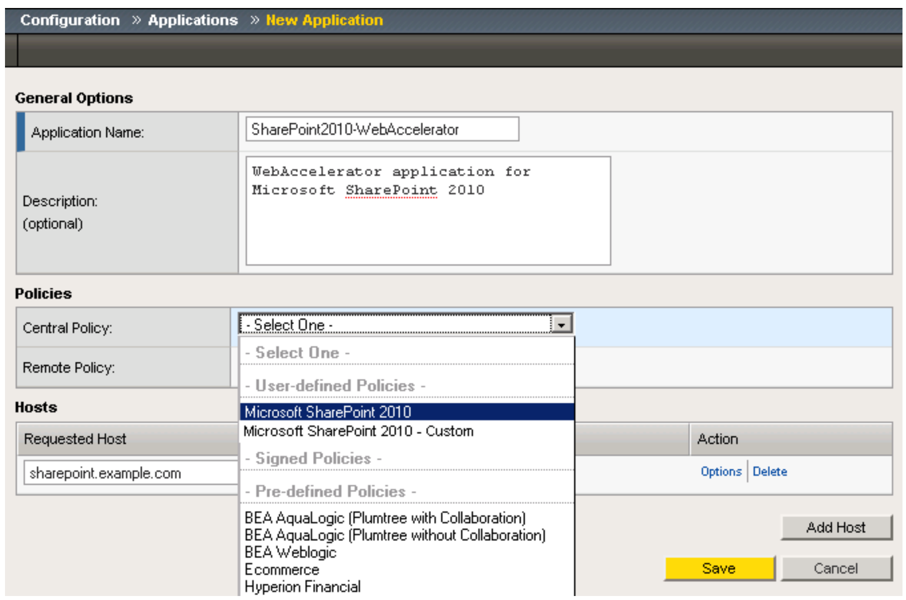

Figure 3.4 Selecting the Central policy

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.

4

Deploying Access Policy Manager with Microsoft Active Directory for SharePoint 2010 Access

- Configuring the BIG-IP APM for SharePoint access
- Configuring the BIG-IP APM in Portal mode
- Configuring the BIG-IP APM in Web Access Management mode

Configuring the BIG-IP APM for SharePoint access

In this chapter, we provide guidance on configuring the BIG-IP Access Policy Manager (APM) for SharePoint 2010 for pre-authentication of users in Active Directory before allowing connectivity to a Microsoft SharePoint server pool.

This chapter is broken up into two sections with different configuration options. Choose the method applicable for your configuration:

- **APM Portal mode**
  In this scenario, the BIG-IP APM uses a Web Application, which configures a remote access connection to your SharePoint deployment through a single external virtual server. Portal mode provides secure interaction with SharePoint, using link rewriting technology. This allows you to provide secure extranet access to internal web applications like SharePoint without creating a full VPN connection. This method is more secure, but can be more resource intensive.
- **Web Access Management**
  Using Web Access Management, the BIG-IP APM module performs an authentication check before sending traffic to the BIG-IP LTM virtual server for SharePoint. This method only proxies authentication, and does not send all traffic through the BIG-IP APM module.

Prerequisites and configuration notes

- BIG-IP must have DNS and NTP configured.
- Active Directory and BIG-IP should ideally share a common time source, but in any case must have times that are closely synchronized.
  See the BIG-IP product documentation on how to configure DNS and NTP.
- The DNS server(s) that are configured in BIG-IP must be able to resolve all forward and reverse zones associated with the Active Directory domain used by SharePoint. Additionally, the BIG-IP must be able to resolve the Host Name used in the Web Application configuration section (see below).
- End users must be able to resolve the name associated with the IP address for the virtual server that you create in the final step of this process. That name is distinct from the FQDN that you have configured your SharePoint application to use and which the BIG-IP makes use in the Web Application configuration.
- The login form created below only works if users supply their user name without accompanying domain information, for example, just **username** rather than **domain\username** or **username@fully.qualified.domain.name**.
- If users are able to edit Microsoft Office files from within the SharePoint site, there is an additional iRule you must include on page 4-11.

Configuring the BIG-IP APM in Portal mode

Use this section if you want to use BIG-IP APM in Portal mode for SharePoint. As mentioned in the introduction, the BIG-IP APM uses a Web Application, which configures a remote access connection to your SharePoint deployment through a single external virtual server. Portal mode provides secure interaction with SharePoint, using link rewriting technology. This allows you to provide secure extranet access to internal web applications like SharePoint without creating a full VPN connection. This method is more secure, but can be more resource intensive.

Creating the Rewrite Profile

The first task is to create the rewrite profile.

To create the Rewrite profile

1. On the Main tab, expand **Access Policy**, and then click **Rewrite Profiles**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **SharePoint-Rewrite**.
4. Leave the **Client Caching Type** list at the default (**CSS and JavaScript**).
5. Click the **Finished** button.

Creating the SSO Configuration

Next, we create a Single Sign-On Configuration that defines the credentials that will be cached.

To create the SSO configuration

1. On the Main tab, expand **Access Policy**, and then click **SSO Configurations**.
2. Click the **Create** button.
3. In the Name box, type a name for this profile. In our example, we type **SharePoint-Access-SSO**.
4. From the **SSO Method** list, select the appropriate SSO method. In our example, we select **NTLMv1**.

   Note: Unless you altered the default configuration of the Windows Server 2008 servers that run your SharePoint server pool to only accept NTLMv2 authentication, you should select NTLMv1.

5. In the **Username Source** box, type the user name source. In our example, we leave the default setting **session.sso.token.last.username**, which will be correct for most configurations.
6. In the **Password Source** box, type the user name source. In our example, we leave the default setting **session.sso.token.last.password**, which will also be correct for most configurations.
7. In the **NTLM domain** box, type the NetBIOS version of your domain name. In our example, we type **mydomain**. Do ***not*** use the fully qualified domain name (e.g. 'mydomain.example.com').
8. Click **Finished**.

Creating the web application

The next task is to create the Web Application.

To create the Web Application

1. On the Main tab, expand **Access Policy**, and then click **Web Applications**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this web application. In our example, we type **SharePoint-application**. You can optionally type a description.
4. Modify any of the settings as applicable for your configuration. In our example, we leave the settings at their default levels.
5. Click the **Create** button. The web application is saved, and the Resource Items section appears at the bottom of the page.
6. In the **Resource Items** section, click the **Add** button.
7. In the Destination section, click the appropriate option button, and type the applicable value in the box. In our example, we are providing access to a particular host, although the destination could also be a BIG-IP LTM virtual server that load balances a pool of SharePoint servers. We click the **Host Name** button, and in the **Host Name** box, type **sharepoint.mydomain.siterequest.com**. (Note: the BIG-IP must be able to resolve this host name to the correct IP address, whether that be an individual server or a BIG-IP virtual).
8. In the **Port** box, type the appropriate port. In our example, SharePoint is an HTTP application and we are doing all TLS/SSL processing on the BIG-IP, so we type **80**, the standard HTTP port.
9. From the **Scheme** list, select the appropriate scheme. In our example, we select **http**.

10. Configure the Paths and Headers section as applicable. We leave these sections blank.
11. From the **Resource Item Properties** list, select **Advanced**.
12. From the **Compression** list, select **GZIP Compression**. While this is optional, enabling this allows the BIG-IP APM browser component to further compress content when necessary, providing bandwidth and download time savings.
13. From the **SSO configuration** list, select the SSO object you configured in Creating the SSO configuration, above. In our example, we select **SharePoint-Access-SSO**.
14. In the **Home Tab** row, you can optionally chose to enable the Home Tab. The Home Tab is a browser component that is inserted dynamically through the Access Virtual and allows users to browser pages within the context of BIG-IP APM. The Home Tab also allows users to log out. By clearing the Home Tab box, this feature is hidden.
15. Configure the rest of the settings as applicable to your configuration.
16. Click **Finished**.

Creating a Webtop

The next task is to create a Webtop that specifies the end user destination.

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 **SharePoint-Webtop**.
4. From the **Type** list, select **Web Applications**.
5. In the **Web Application start URI** box, type the start URI. This is the URI of the destination application that the user hits once they are authenticated and entitled to the resource. In our case, we enter the URI that our SharePoint Server has been configured to use, **http://sharepoint.siterequest.com**.
6. Click **Finished**.

Creating an Authentication Source (AAA Server)

The next task is to create an Authentication Source that specifies an Active Directory 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 **SharePoint-AAA-AD**.
4. From the **Type** list, select the appropriate authentication method. For this example, we select **Active Directory**.
5. In the Domain Controller row, type the IP address or DNS name of the Active Directory server you'll be using. The BIG-IP must have network connectivity to this server.
6. In the **Domain Name** box, type the fully qualified domain name (FQDN) of your domain. (Note: unlike the SSO configuration, you must use the FQDN rather than the short NetBIOS domain name). In our example, we type **mydomain.siterequest.com**.
7. You do not need to supply an Admin Name or Admin Password.
8. Click **Finished**.

Creating an Access Profile

The next task is to create an Access Profile and a Visual Policy which provides a logon page, authentication against the Active Directory AAA source, SSO Credential mapping and a resource assignment. If you would optionally like to include a pre-login anti-virus check, follow the example shown in the Tivoli section of this document.

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 **SharePoint_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, from the **SSO Configurations** list, select the name of the SSO Configuration you created in *Creating the SSO Configuration*, on page 4-2. In our example, we type **SharePoint-Access-SSO**.

6. In our example and for most SharePoint applications, leave all other settings at their default values. Consult the BIG-IP documentation if you need details on configuring Language Settings.
7. Click **Finished**.

Editing the Access Profile with the Visual Policy Editor

The next task is to 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.

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. Select 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 on the between **Logon Page** and **Deny**.
8. Select the **AD Auth** option in the Authentication section, then click **Add Item**.
9. In the **Server field of the resulting AD Auth Active Directory** properties box, select the AAA source you created in *Creating an Authentication Source (AAA Server)*, on page 4-4. In our example, we select **SharePoint-AAA-AD**.
10. Click the **Save** button. You now see two paths, ***Successful*** and ***Fall Back***.
11. At the end of the **Successful** path, click **Deny** in the ending box.
12. Select the **Allow** option, and click **Save**. The ending for Successful should now be **Allow**, and the ending for Fallback should be **Deny**.
13. Click the **+** symbol on the Successful path between **AD Auth** and **Allow**.

14. Select the **SSO Credential Mapping** item from the General Purpose section, then click **Add Item**. In our configuration example, we leave the settings for **SSO Token Username** and **SSO Token Password** at their default settings. Click **Save**.
15. Click the **+** symbol between **SSO Credential Mapping** and **Allow**.
16. Select the **Resource Assign** item from the General Purpose section, then click **Add Item**.
17. Click **Add New Entry**, then **Add/Delete Web Application Resources**.
18. Select the web application you created above. In our example, we select **SharePoint-application**. The counter on the Web Application Resource tab changes from 0 to 1.
19. Click the Webtop tab. Select the Webtop you created above. In our example, we select **SharePoint-Webtop**. The counter on the Webtop tab changes from 0 to 1.
20. Click **Update**, and then click **Save**.
21. 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.
22. Click the **Close** button on the upper right to close the VPE.

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 **SharePoint-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, and then click **SSL Certificates**. This displays the list of existing certificates
2. In the upper right corner of the screen, click **Import**.
3. From the **Import Type** list, select the type of import (**Certificate** or **Key**).
4. In the **Certificate** (or **Key**) **Name** box, type a unique name for the certificate or key.
5. In the **Certificate** (or **Key**) **Source** box, choose to either upload the file or paste the text.
6. Click **Import**.
7. 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 **SharePoint_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 server

The final task is to create the virtual server.

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. 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 **SharePoint-vs**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address for this Access Virtual on APM.
   Note: This is different than the application VIP. This is the front-end service that users connect to.
   In our example, we type **10.133.56.124**.
6. In the **Service Port** box, type **443**, or select **HTTPS** from the list.
7. 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 **SharePoint-http**.
8. 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 **SharePoint-https**.
9. 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 4-5. In our example, we select **SharePoint_Access_Policy**.
10. From the **Rewrite Profile** list, select the profile you created in *Creating the Rewrite Profile*, on page 2. In our example, we select **SharePoint-Rewrite**.
11. Leave all other settings at the default levels (**Do not** configure any of the options in the WAN Optimization section).
12. Click the **Finished** button.

This completes this section of the BIG-IP APM configuration.

Configuring the BIG-IP APM in Web Access Management mode

Use this section if you want to use the BIG-IP APM to proxy authentication only, without sending all SharePoint traffic through the BIG-IP APM Web Application.

Important

For this section, you must have configured your BIG-IP LTM to offload SSL from the SharePoint 2010 deployment. You could have configured SSL offload using the application template, or manually, as described in ***Configuring the BIG-IP LTM system for Microsoft SharePoint Server 2010 using SSL****, on page 2-11.*

Because this section uses some of the same configuration objects as the previous section, we refer back to those procedures where they are the same, rather than repeat the procedures here.

Creating the SSO configuration

To create the SSO configuration, use the procedure *Creating the SSO Configuration*, on page 4-2. There are no required changes for this section.

Creating an Authentication Source

The next task is to create an Authentication Source on the BIG-IP APM. To create the Authentication Source, use the procedure *Creating an Authentication Source (AAA Server)*, on page 4-4. There are no required changes for this section.

Creating an Access Profile

The next task is to create an Access Profile on the BIG-IP APM. To create the Access Profile, use the procedure *Creating an Access Profile*, on page 4-5. There are no required changes for this section.

Editing the Access Policy with the Visual Policy Editor

After creating the objects above, use the following procedure to edit the Access Policy on the BIG-IP APM using the Visual Policy Editor (VPE).

To configure the Access Policy

1. On the Main tab, expand **Access Policy**, and click **Access Profiles**.
2. Locate the Access Profile you just created, and then, in the Access Policy column, click **Edit**. The VPE 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 the **Add Item** button at the bottom.
5. Configure the Logon Page properties as applicable, and click **Save**. In our example, we leave the defaults.
6. Click the **+** symbol between **Logon Page** and **Deny**.
7. In the Authentication section, click the **AD Auth** option button, and click **Add Item**.
8. In the **Active Directory** properties box, from the **Server** list, select the AAA server you created in this section. The rest of the settings are optional. Click **Save**.
9. On the Successful path between **AD Auth** and **Deny**, click the **+** symbol.
10. Click the **SSO Credential Mapping** option button, and then click **Add Item**.
11. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults. Click the **Save** button.
12. On the fallback path between **SSO Credential Mapping** and Deny, click the **Deny** box. Click the **Allow** option button, and click **Save**.
13. Click the yellow **Apply Access Policy** link in the upper left part of the window. You must apply an access policy before it takes effect.

Creating the iRule to support editing Microsoft Office documents

If you are using the APM in Web Access Management mode and your SharePoint users have the ability to edit Microsoft Office documents within a SharePoint site, you must configure the following iRule to allow this functionality through the APM.

To create the iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**.
2. 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 **sharepoint-APM**.

4. In the **Definition** section, copy and paste the following iRule, omitting the line numbers (line 23 must be entered as a single line):

```
1    when HTTP_REQUEST {
2        if { [HTTP::cookie exists "MRHSession"] } {
3            # Remember the session ID to be used on the response
4            set MRHSHint [HTTP::cookie value "MRHSession"]
5            # Strip off the SharePoint hint cookie so backed does not see it
6            if { [HTTP::cookie exists "MRHSHint"] } {
7                HTTP::cookie remove "MRHSHint"
8            }
9        } elseif { [HTTP::cookie exists "MRHSHint"] } {
10           HTTP::cookie insert name "MRHSession" value [HTTP::cookie value "MRHSHint"]
11           # Refresh the SharePoint hint cookie
12           set MRHSHint [HTTP::cookie value "MRHSHint"]
13           # Strip off the SharePoint hint cookie so backed does not see it
14           HTTP::cookie remove "MRHSHint"
15       }
16   }
17   when ACCESS_ACL_ALLOWED {
18       set timeout [ACCESS::session data get "session.inactivity_timeout"]
19       set secure [PROFILE::access "secure_cookie"]
20       set clientip [ACCESS::session data get "session.user.clientip"]
21       # Check source address
22       if { not ( $clientip equals [IP::remote_addr] ) } {
23           ACCESS::respond 401 content "<html><body>Error: Failure in Source Address Check</body></html>" Connection Close
24       }
25   }
26   when HTTP_RESPONSE {
27       if { not [info exists timeout] } {
28           set timeout 60
29       }
30       if { not [info exists secure] } {
31           set secure 1
32       }
33       if { [info exists MRHSHint] } {
34           # Insert a SharePoint hint cookie
35           HTTP::cookie insert name "MRHSHint" value $MRHSHint
36           # Keep the life of SharePoint hint cookie same as session cookie
37           # Also make it persistent.
38           HTTP::cookie expires "MRHSHint" $timeout relative
39           if { $secure equals "1" } {
40               HTTP::cookie secure "MRHSHint" enable
41           }
42           HTTP::cookie path "MRHSHint" "/"
43           unset MRHSHint
44       }
45   }
```

5. Click the **Finished** button.

Modifying the virtual server

The next task is to modify the BIG-IP LTM virtual server you created (either using the template or manually) to use the Access Policy. If you created the iRule as described in the previous section, you add the iRule to the virtual server as well.

To modify the LTM virtual server to use the Access Policy

1. On the Main tab, expand **Local Traffic** and then click **Virtual Servers**.
2. From the **Virtual Server** list, click the name of the SharePoint virtual server on port 443. If you used the application template, the default virtual server name is **my_sharepoint_https_virtual_server.** If you created the configuration manually, this is the virtual server you created in *Creating the HTTPS virtual server*, on page 2-13.
3. From the **Access Profile** list, select the name of the Access profile you just created.
4. Click the **Update** button.
5. *If you created the iRule to allow editing of Microsoft Office documents from a SharePoint site through the APM only*: On the Menu bar, click **Resources**.
6. In the **iRules** section, click the **Manage** button.
7. From the **Available** list, select the iRule you created in *Creating the iRule to support editing Microsoft Office documents*, on page 4-11, and then click the Add (**<<**) button to move it to the **Enabled** box.
8. Click **Finished**.

This completes the configuration.