Deploying the BIG-IP System v9.x with Microsoft Office SharePoint 2007

Important: This guide has been archived. While the content in this guide is still valid for the products and versions listed in the document, it is no longer being updated and may refer to F5 or third party products or versions that have reached end-of-life or end-of-support.   For a list of current guides, see https://f5.com/solutions/deployment-guides.

Microsoft® Partner

Table of Contents

1

Deploying the BIG-IP LTM System with Microsoft Office SharePoint Server 2007

- Configuring the BIG-IP LTM system for Microsoft Office SharePoint 2007

- Configuring the BIG-IP LTM system for Microsoft Office SharePoint Server 2007 using SSL

Introducing the F5 and Microsoft Office SharePoint Server 2007 configuration

Welcome to the F5 and Microsoft® Office® SharePoint® 2007 Deployment Guide. This guide contains step-by-step procedures for configuring F5 devices for Office SharePoint 2007 resulting in a secure, fast and available deployment.

Microsoft Office SharePoint Server 2007 enables enterprises to develop an intelligent portal that seamlessly connects users, teams, and knowledge so that people can take advantage of relevant information across business processes to help them work more efficiently.

For more information on Microsoft Office SharePoint Server 2007, see **http://www.microsoft.com/sharepoint/default.mspx**

For more information on the F5 devices included in this guide, see **http://www.f5.com/products/**.

You can also visit the Microsoft page of F5's online developer community, DevCentral, for Microsoft forums, solutions, blogs and more: **http://devcentral.f5.com/Default.aspx?tabid=89.**

This Deployment Guide contains procedures for configuring the BIG-IP LTM system, the BIG-IP LTM system with SSL, the WebAccelerator module, and the FirePass controller. While we recommend using all of these products together with SharePoint 2007, it is not required. Simply use the sections for the products you have. This guide is broken up into the following sections:

◆ *Configuring the BIG-IP LTM system for Microsoft Office SharePoint 2007*, on page 1-6

◆ *Configuring the BIG-IP LTM system for Microsoft Office SharePoint Server 2007 using SSL*, on page 1-19

◆ *Configuring the F5 WebAccelerator module with Microsoft Office SharePoint 2007*, on page 2-1

◆ *Deploying the FirePass controller with Microsoft Office SharePoint 2007*, on page 3-1

Prerequisites and configuration notes

The following are general prerequisites for this deployment; each section contains specific prerequisites:

◆ All of the configuration procedures in this document are performed on F5 devices. For information on how to deploy or configure Microsoft Office SharePoint 2007, consult the appropriate Microsoft documentation.

◆ This document is written with the assumption that you are familiar with both the F5 devices and Microsoft Office SharePoint 2007. For more information on configuring these products, consult the appropriate documentation.

◆ *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 1-2.

◆ This Deployment Guide assumes that you have already installed the F5 devices in your network. It also assumes that you have performed basic configuration tasks such as creating Self IP addresses and VLANs. For more information on how to install F5 devices and configure the basic settings, refer to the appropriate F5 manual, available on **AskF5**.

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.

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.

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://sp2007.example.com**.

14. In the Start Addresses section, type the appropriate HTTPS URL. In our example, we type **https://sp2007.example.com**. All other settings are optional.

15. Click the **OK** button (see Figure 1.3, on page 1-4).

16. Repeat this entire procedure for each public URL to be deployed behind LTM.

Figure 1.1 *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.

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.

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

Configuring the BIG-IP LTM system for Microsoft Office SharePoint 2007

The first section in this Deployment Guide is for configuring the BIG-IP Local Traffic Manger (LTM) for the SharePoint 2007 devices.

Prerequisites and configuration notes

The following are prerequisites for this deployment:

◆ The BIG-IP LTM system should be running version 9.4 or later. The BIG-IP LTM version 9.2.3 and later include updates for HTTP profiles to more reliably support use with Microsoft Office SharePoint Server. Through the use of HTTP profiles, it is possible to use advanced features such as compression and HTTP iRule methods in conjunction with a SharePoint Server deployment.

◆ For certain *optional* optimization features, the appropriate module on the BIG-IP LTM system must be licensed (such as compression and RAM Cache).

◆ The Microsoft Office SharePoint Server must be the 2007 edition. For the Microsoft SharePoint Portal Server 2003 Deployment Guide, see **http://www.f5.com/solutions/deployment/sharepoint_bigip9_dg.html**

◆ All of the configuration procedures in this document are performed on the BIG-IP LTM system. For information on how to deploy or configure the Office SharePoint Server 2007, consult the appropriate Microsoft documentation. You should have at least basic familiarity with both products.

Configuration example

The BIG-IP system provides intelligent traffic management and high availability for Microsoft Office SharePoint Server 2007 deployments.
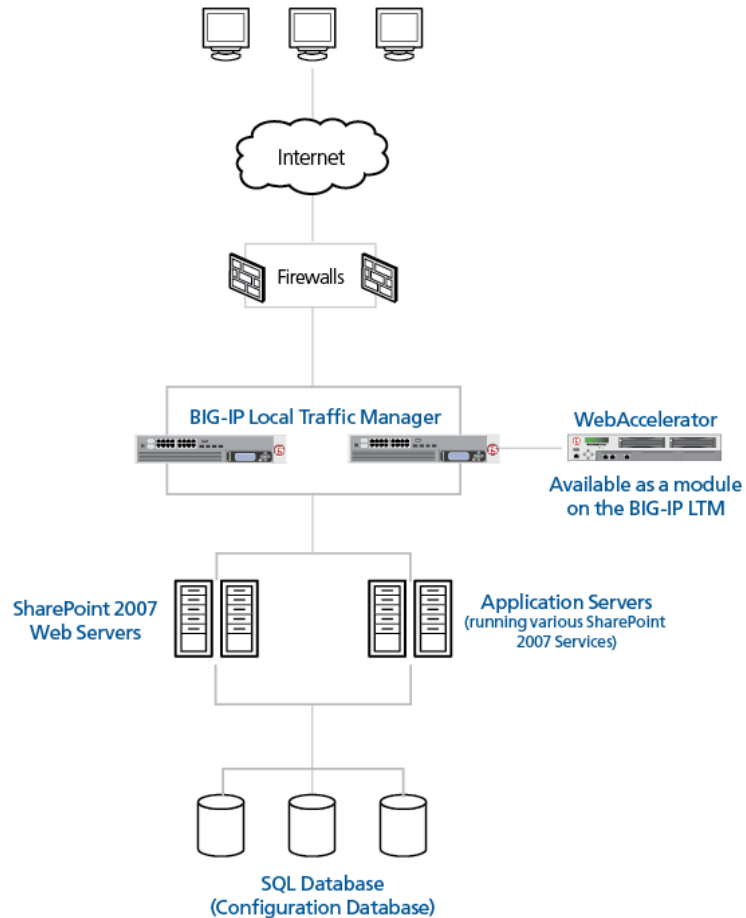
Figure 1.2 BIG-IP LTM SharePoint Server logical configuration

Configuration Tasks

To configure the BIG-IP and SharePoint 2007 devices for integration, you need to complete the following procedures:

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

If you are using the BIG-IP LTM system as an SSL proxy for your Office SharePoint 2007 deployment, be sure to see *Configuring the BIG-IP LTM system for Microsoft Office SharePoint Server 2007 using SSL*, on page 1-19 after you complete the procedures in this section.

◆ **Tip**

*We recommend you save your existing BIG-IP configuration before you begin the procedures in this Deployment Guide. To save your BIG-IP configuration, see **Appendix A: Backing up and restoring the BIG-IP system configuration**, on page 1-27.*

Connecting to the BIG-IP device

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

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

1. In a browser, type the following URL:
   https://<administrative IP address of the BIG-IP device>
   A Security Alert dialog box appears, click **Yes**.
   The authorization dialog box appears.

2. Type your user name and password, and click **OK**.
   The Welcome screen opens.

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

Creating the HTTP health monitor

The next 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 nodes (IP address and port combinations), and can be configured to use **send** and **recv** statements in an attempt to retrieve explicit content from nodes. We configure the health monitors first in version 9.0 and later, as health monitors are now associated at the pool level.

To configure a health monitor from the BIG-IP Configuration utility

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/1.0** 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, type **200 OK**. This is the default response to the Send String in our example.

Figure 1.3 *Creating the HTTP Monitor*

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

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.

   *Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings as applicable for your network.*

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

4. 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**.

5. 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 (node)**.

6. For this pool, we leave the Priority Group Activation **Disabled**.

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

8. In the **Address** box, add the first server to the pool. In our example, we type **10.10.100.151**

9. 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**.

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

11. Repeat steps 9-11 for each server you want to add to the pool. In our example, we repeat these steps once for the remaining server, **10.10.100.152**.

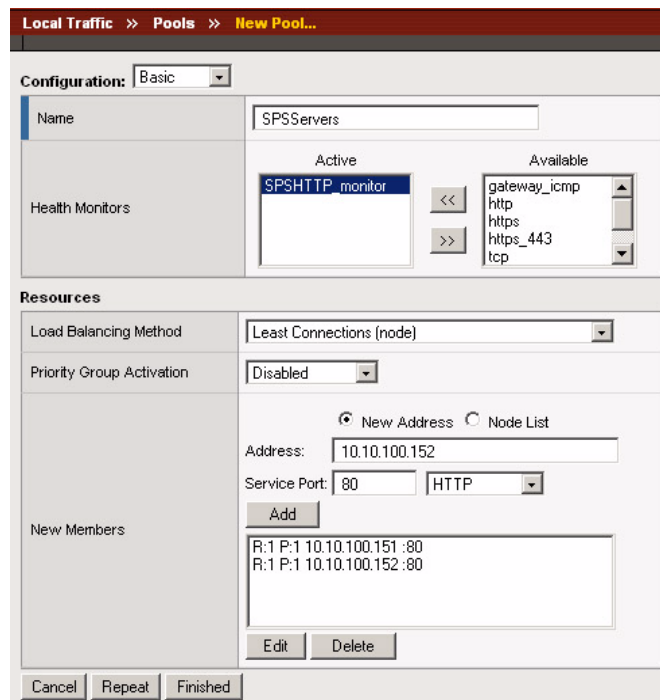12. Click the **Finished** button (see Figure 1.8).

Figure 1.4 *Adding the SharePoint server pool*

Creating profiles

BIG-IP version 9.0 and later use 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.

For this configuration, we create three new profiles: an HTTP profile, a TCP profile, and a cookie persistence profile.

◆ **Important**

*If you are using **NTLM** authentication, the default authentication method for SharePoint Server 2007, **do not** use a OneConnect profile on the BIG-IP system for this deployment. Note that a OneConnect profile is not part of this configuration in this guide.*

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 a new profile in BIG-IP LTM version 9.4, called **http-wan-optimized-compression-caching**, with a few additional modifications. This profile includes some default optimization settings that increase the performance of SharePoint 2007 over the WAN. 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.

◆ This profile is only available in BIG-IP LTM version 9.4 and later.

◆ *Important:* If you plan on using the WebAccelerator module for SharePoint 2007 (as shown later in this Deployment Guide) you should *not* use the **http-wan-optimized-compression-caching** HTTP profile, as the WebAccelerator module performs the compression duties in addition to its other optimizations.
If you are using BIG-IP LTM v9.4.2 or later with the WebAccelerator module, we recommend you configure an HTTP profile based off of the **http-acceleration** parent profile, and change the **Redirect Rewrite** option to **Matching** when appropriate (see first bullet). Any other settings in this case are optional.

◆ Note

The following procedure shows one way to optimize the Microsoft SharePoint 2007 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**. The HTTP Profiles screen opens.

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

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

4. From the **Parent Profile** list, 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. *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 1-24 for detailed information, including modifications to IIS to accurately log the client IP address.

7. In the Compression section, check the Custom box for **Compression**, and from the **Compression** list, select **Enabled**.

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

9. In the Content List section, add the following entries to the **Content Type** box one at a time, each followed by clicking **Include**:

   • application/pdf
   • application/vnd.ms-powerpoint
   • application/vnd.ms-excel
   • application/msword
   • application/vnd.ms-publisher

10. Check the Custom box for **Keep Accept Encoding**, and check the box to enable Keep Accept Encoding.

Figure 1.5 *Configuring the compression settings in the HTTP profile*

11. In the RAM Cache section, check the Custom box for **URI Caching**, and leave **URI List** selected.

12. 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.
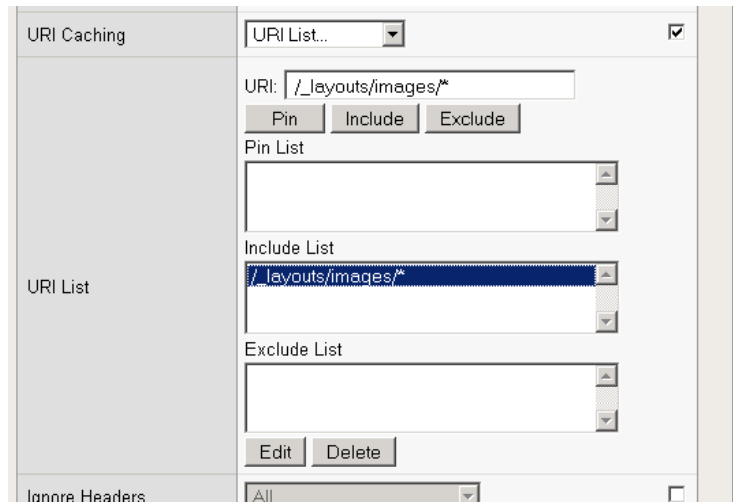
Figure 1.6 *Adding the image directory to the RAM cache URI include list.*

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

14. Click the **Finished** button.
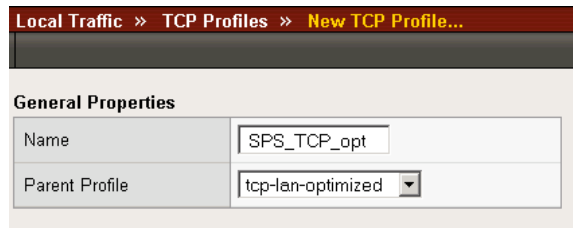
Creating a TCP profile

The next profile we create is the TCP profile. For SharePoint 2007, if your users are mostly connected to the BIG-IP LTM system via low loss local area networks (LANs), we recommend using another new profile available with BIG-IP LTM version 9.4 and later, called **tcp-lan-optimized**. This profile contains default settings designed to optimize the performance of your local TCP traffic in certain ways, without having to create a custom profile to do so.

To create a new TCP profile

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

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

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

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

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

6. From the **Parent Profile** list, select **tcp-lan-optimized**.

Figure 1.7 Configuring the tcp-lan-optimized profile

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

8. Click the **Finished** button.

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

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 based on the default 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 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_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 **192.168.104.147**.

6. In the **Service Port** box, type **80** or select **HTTP** from the list.

Figure 1.8 Adding the SharePoint 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 a TCP profile* section. In our example, we select **SPSTCP**.

10. Leave the **Protocol Profile (Server)** option at the default setting, or you can select **SPSTCP** from the list.

    *Important: If you are using NTLM authentication, the default authentication method for SharePoint Portal Server 2007, **do not** use a OneConnect profile on the BIG-IP system for this deployment. A OneConnect profile is not part of this configuration in this guide.*

11. From the HTTP Profile list, select the name of the profile you created in the *Creating an HTTP profile* section. In our example, we select **SPSHTTP** (see Figure 1.13).

Figure 1.9 Selecting the TCP and HTTP profiles for the virtual server

12. 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 **SPSServers**.

13. 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 1.10 Resources section of the add virtual server page

14. 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.

Synchronizing the BIG-IP configuration if using a redundant system

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

To synchronize the configuration using the Configuration utility

1. On the Main tab, expand **System**.

2. Click **High Availability**. The Redundancy screen opens.

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

4. Click the **Self --> Peer** button. The configuration synchronizes with its peer.

The BIG-IP LTM system is now configured to direct traffic to the Microsoft SharePoint Server 2007 deployment. If you are using the BIG-IP LTM system to offload SSL traffic from your SharePoint 2007 deployment, continue to the following section.

Configuring the BIG-IP LTM system for Microsoft Office SharePoint Server 2007 using SSL

This section describes how to configure the BIG-IP LTM system as an SSL proxy for a Microsoft Office SharePoint Server 2007 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. If you have not, start with *Configuring the BIG-IP LTM system for Microsoft Office SharePoint 2007*, on page 1-6.

◆ *Important:* When using the BIG-IP LTM system for SSL offload, for each Sharepoint Web Application that will be deployed behind LTM, configure your SharePoint Alternate Access Mappings and Zones according to the Microsoft documentation. 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. More information can be found here: **http://blogs.msdn.com/sharepoint/archive/2007/03/06/what-every-sharepoint-administrator-needs-to-know-about-alternate-access-mappings-part-1.aspx.**

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

• *Using SSL certificates and keys*
• *Create a Client SSL profile*
• *Creating the Redirect iRule*
• *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.

Creating the Redirect iRule

The Redirect iRule takes incoming HTTP requests (non-secure) and
redirects them to the correct HTTPS (secure) virtual server, without user
interaction

To create the Redirect iRule

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

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

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

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

```
when HTTP_REQUEST {
   HTTP::redirect https://[HTTP::host][HTTP::uri]
}
```
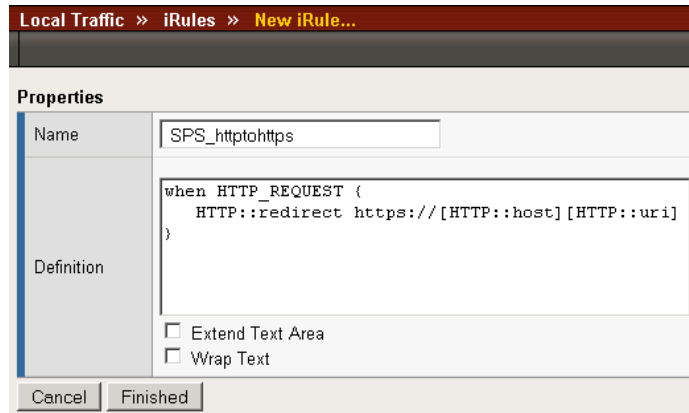
5. Click the **Finished** button.

Figure 1.11 Creating the iRule

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 1-16 to use the iRule you just created.

To modify the exisiting 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 iRule you created in the *Creating the Redirect iRule* section, and click the Add (**<<**) button. In our example, we select **SPS_httptohttps**.

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 **192.168.104.146**.

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 *Creating a TCP profile* section. In our example, we select **SPS_TCP_opt**.

10. 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**.

11. 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**.

12. From the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **SPSServers**.

13. 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**.

14. Click the **Finished** button.

This concludes the BIG-IP LTM configuration. If you are using a redundant BIG-IP LTM system, see *Synchronizing the BIG-IP configuration if using a redundant system*, on page 1-18.

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.

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

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

- BIG-IP configuration files

- BIG-IP license and passwords

- SSL certificates

- SSH keys

Saving and restoring the BIG-IP configuration

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

To save the BIG-IP configuration using the Configuration utility

1. In the navigation pane, click **System Admin**.
   The User Administration screen displays.

2. Click the Configuration Management tab.
   The Configuration Management screen displays.

3. In the **Save Current Configuration** section, type the path where you want your configuration file saved or choose a path from the list box. If no path is specified, the BIG-IP saves files to **/usr/local/ucs**. The BIG-IP appends the extension.ucs to file names without it.

4. Click the **Save** button to save the configuration file.

To restore a BIG-IP configuration

1. In the navigation pane, click **System Admin**.
   The User Administration screen displays.

2. Click the Configuration Management tab.
   The Configuration Management screen displays.

3. In the **Restore a Configuration** section, choose the configuration file you want to restore from the list box, or type the path where your configuration files were saved.

4. Click the **Restore** button.
   To check the status of the restoration, click the **View Log** button.
   You should wait a few moments for the log file to start generating
   before you click **View Log**. Repeated clicking of this button will
   update your screen with the most current log file information until
   the restoration is complete.

2

Configuring the F5 WebAccelerator module with Microsoft Office SharePoint 2007

- Configuring the WebAccelerator module

- Creating an HTTP Class profile

- Modifying the Virtual Server to use the Class profile

- Downloading and importing the WebAccelerator policy

- Creating an Application

Configuring the F5 WebAccelerator module with Microsoft Office SharePoint 2007

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 purchased and licensed the WebAccelerator module on the BIG-IP LTM system, version 9.4 or later.

◆ For BIG-IP version 9.4.0, you need to follow the simple procedure to download and import the policy for SharePoint 2007. Later versions will include this policy.

◆ This document is written with the assumption that you are familiar with the BIG-IP LTM system, WebAccelerator and Microsoft Office SharePoint Server 2007. Consult the appropriate documentation for detailed information.

◆ If you are using BIG-IP LTM 9.4.2 or later, you should have configured an HTTP profile using the **http-acceleration** parent. See *Creating an HTTP profile*, on page 1-12 for more details.

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 client with WAN latency logs onto the SharePoint site via the WebAccelerator. The user's request is accelerated on repeat visits by the WebAccelerator instructing the browser to use the dynamic or static object that is stored in its local cache. Additionally, dynamic and static objects are cached at the WebAccelerator so they can be served quickly 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.

Connecting to the BIG-IP device

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

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

1. In a browser, type the following URL:
   https://<administrative IP address of the BIG-IP device>
   A Security Alert dialog box appears, click **Yes**.
   The authorization dialog box appears.

2. Type your user name and password, and click **OK**.
   The Welcome screen opens.

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 **wa_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.f5.com** (see Figure 2.1).

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

c) Click the **Add** button.

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

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

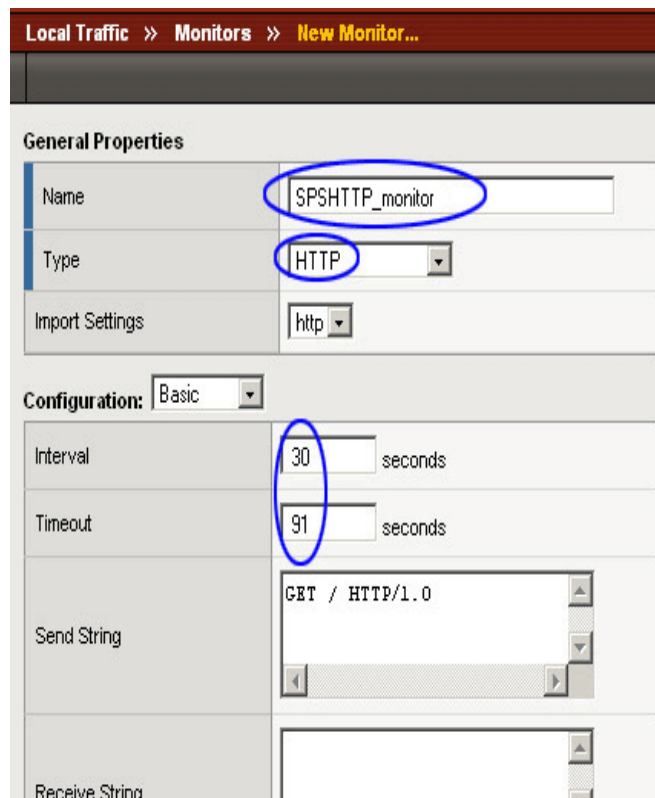8. Click the **Finished** button. The new HTTP class is added to the list.

Figure 2.1 Creating a new HTTP Class profile

Modifying the Virtual Server to use the Class profile

The next step is to modify the virtual server for your 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 **wa_class** (see Figure 2.2).

6. Click the **Finished** button. The HTTP Class Profile is now associated with the Virtual Server.
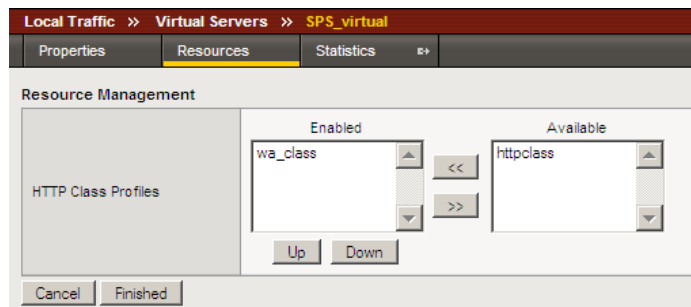
Figure 2.2 Adding the HTTP Class Profile to the Virtual Server

Downloading and importing the WebAccelerator policy

For the WebAccelerator module version 9.4.0, you need to download and import the custom policy for Microsoft Office SharePoint 2007. 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 copy and paste the following URL: **http://devcentral.f5.com/Policies/Sharepoint.xml**.

2. Save the **Sharepoint.xml** file in a place that is accessible from the WebAccelerator.

3. Return to the BIG-IP LTM system (see *Connecting to the BIG-IP device*, on page 1-8 for instructions). On the Main tab, expand **WebAccelerator**, and then click **Policies**. The Policy list opens.

4. At the bottom of the page, click **Import Policies**.

5. Click the **Browse** button, and navigate to the location where you saved the **Sharepoint.xml** file.

6. Click the **Import** button.
The Policy is added to the list. You choose the new policy in the next procedure.

Creating an Application

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

To create a new Application

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

2. Click the **New Application** button.

3. In the Application Name box, type a name for your application.
In our example, we type **SharePoint 2007**.

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

5. From the **Local Policies** list, select **Microsoft Sharepoint Services 2007**. This is a pre-defined policy created specifically for Microsoft Office SharePoint 2007 devices (see Figure 2.3).

6. 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.f5.com**
If you have additional host names, click the **Add Host** button and enter the host name(s).

7. Click the **Save** button.

Figure 2.3 *Configuring an Application on the WebAccelerator*

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.

3

Deploying the FirePass controller with Microsoft Office SharePoint 2007

- Configuring the FirePass controller

- Creating groups on the FirePass controller

- Limiting access for the Partner group

- Configuring Endpoint security

Deploying the FirePass controller with Microsoft Office SharePoint 2007

This section of the Deployment Guide shows you how to configure F5's FirePass controller for secure remote access to Microsoft® Office® SharePoint® Server 2007 deployments.

F5's FirePass® controller is the industry leading SSL VPN solution that enables organizations of any size to provide ubiquitous secure access for employees, partners and customers to applications such as Microsoft SharePoint Portal Server, while significantly lowering support costs associated with legacy client-based VPN solutions.

For more information on the Microsoft Office SharePoint Portal Server 2007, see **http://www.microsoft.com/sharepoint/default.mspx**

For more information on the FirePass controller, see **http://www.f5.com/products/FirePass/**.

Prerequisites and configuration notes

The following are prerequisites for this deployment:

◆ The FirePass controller should be running version 6.0 or later.

◆ This deployment was tested using Microsoft Office SharePoint Server 2007, load balanced by a BIG-IP LTM system as described in this Deployment Guide.

◆ All of the configuration procedures in this document are performed on the FirePass device. For information on how to configure the SharePoint Server, consult the appropriate Microsoft documentation.

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

◆ This Deployment Guide contains procedures for using Active Directory authentication only. There are many different authentication methods you can use with the FirePass controller; choose the one most applicable to your configuration.

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

Configuration scenario

For the scenario used in this Deployment Guide, the Microsoft Office SharePoint Server 2007 deployment, along with an Active Directory instance, resides behind a BIG-IP LTM system. There is a requirement to

allow employees remote access to all internal resources using the FirePass device. There is also a requirement for trusted partners to access the SharePoint deployment, although only to a limited subset of the portal, with no other access.

This Deployment Guide describes how to configure the FirePass controller to allow secure remote access to the SharePoint 2007 device(s), using Active Directory for authentication and how to configure the FirePass to give one group of users full access, and restrict users in the partner group to a certain directory. In our deployment, the FirePass device and the SharePoint deployment use a common Active Directory Domain Controller. This guide also contains procedures on configuring some endpoint security features, including antivirus checks.

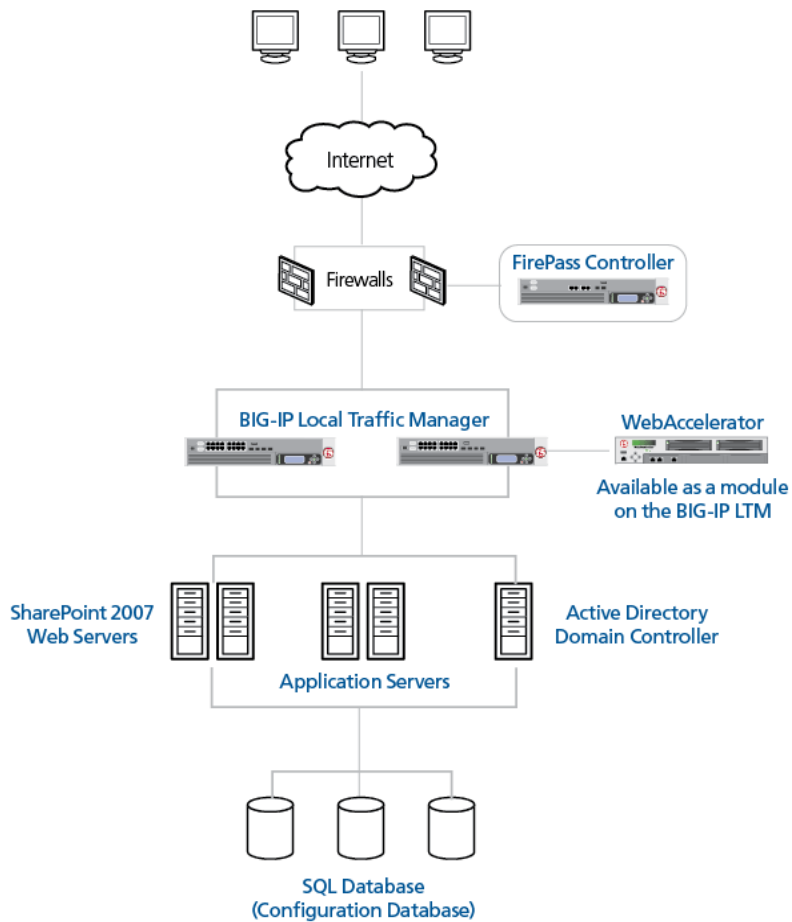Figure 3.1 shows a logical representation of this configuration.

Figure 3.1 *FirePass SharePoint 2007 logical configuration*

Configuring the FirePass controller

To configure the FirePass controller for allowing secure remote access to the SharePoint deployment, you need to complete the following procedures:

- *Connecting to the FirePass controller*
- *Creating groups on the FirePass controller*
- *Limiting access for the Partner group*
- *Configuring auto-logon*
- *Configuring Endpoint security*

Connecting to the FirePass controller

To perform the procedures in this Deployment Guide you must have administrative access to the FirePass controller.

To access the Administrative console, in a browser, type the URL of the FirePass controller followed by **/admin/**, and log in with the administrator's user name and password.

Once you are logged on as an administrator, the Device Management screen of the Configuration utility opens. From here, you can configure and monitor the FirePass controller.

Creating groups on the FirePass controller

In this configuration, we configure two types of groups on the FirePass controller, Resource and Master groups. *Master groups* contain user information, including details about authentication methods. *Resource groups* contain information about applications (resources) that are available to FirePass controller users.

Creating the Resource groups

Resource groups allow you to preconfigure specific applications and access by group, and assign the group to a master group or an individual user. For this configuration, we create two resource groups, one for employees and one for partners, in order to create different Favorite links to the SharePoint deployment.

To configure a resource group

1. From the navigation pane, click **Users**, expand **Groups**, and then click **Resource Groups**.

2. Click the **Create new group** button.
   The Group Management - Create New Group screen opens.

3. In the **New group name** box, type a name for your group and click the **Create** button. In our example we type **Employees_SP**. The new group appears on the Resource Groups table.

4. From the Resource Groups table, find the row with the name of the group you just created. In this row, from the Portal access column, click **Edit** (see Figure 3.2). The Web Applications section of the Resource Group page opens.

Figure 3.2 *The Resource groups table*

5. Under Web Application Favorites, click **Add New Favorite**. The Favorite options display.

6. Type a name for the Favorite. In our example, we type **SharePoint - Employee Access**. This Favorite link only displays for members of the Employee group.

7. In the **URL** box, type the URL used to access the SharePoint deployment. If you are using a BIG-IP LTM system in front of the SharePoint deployment, this URL should point to the SharePoint virtual server address. In our example, we type **http://sharepoint07.f5.com/default.aspx**.

8. Click the **Add to allow list** link to the right of the URL box. This adds the URL to the list of URLs the users are allowed to access.

9. Configure the rest of the settings as applicable to your deployment.

10. Click the **Add New** button. The new Favorite is added to the list. (see Figure3.3).

Figure 3.3 *Adding a Web Application Favorite to the Employee group*

11. Repeat this procedure for the **Partner** resource group, typing appropriate names for the group and the Favorite. In step 7, type the path to the appropriate section of the SharePoint deployment that Partners are entitled to access.
For example, the employee Favorite might point to **http://sharepoint.f5.com/default.aspx**, while the partner Favorite would point to
http://sharepoint.f5.com/sites/partners/default.aspx

Creating the Master groups

FirePass controller master groups are composed of users, authentication methods, and security and policy information. The next task is to create Master groups that will use the resource groups we just created.

To create a new Master Group

1. From the navigation pane, click **Users**, and expand **Groups**.
The Master Groups list screen opens.

2. Click the **Create new group** button.
The Group Management Create New Group screen opens.

3. In the **New group name** box, type the name of your group. In our example we type **SharePointAD**.

4. In the **Users in group** box, select **External.**

5. From the Authentication method list, select **Active Directory**.

6. In the **Copy settings from** list, make sure **Do not copy** is selected (see Figure 3.4).

7. Click the **Create** button.
   The General tab of the new Master Group displays.

Figure 3.4 *Creating a new Master Group*

8. Click the Resource Groups tab.
   The Resource Groups screen opens.

9. From the **Available** box, select the name of the Resource group you created in the *Creating the Resource groups* section. In our example, we select **Employees_SP**.

10. Click the **Add** button to move the group to the **Selected** box, and click the **Update** button. The Resource group is now associated with the Master group.

Configuring the Master group for Active Directory authentication

The next procedure is configuring the Master group to use Active Directory authentication.

◆ **Important**

The FirePass controller has a number of different authentication methods to choose from; use the method applicable to your configuration. However, this guide only contains instructions on configuration Active Directory authentication. See the online help or FirePass documentation for more information on configuring other authentication methods.

To configure the FirePass Master group to use Active Directory authentication

1. From the navigation pane, click **Users**, expand **Groups**, and then click **Master Groups**.

2. Click the name of the Master group you created in the *Creating the Master groups* section. In our example, we select **SharepointAD**.

3. Click the Authentication tab.
   The Active Directory Authentication tab opens.

4. In the **Configure Active Directory Settings** section, configure the appropriate settings for your Active Directory deployment. Type the fully qualified domain name in the **Domain** name box, and IP addresses or DNS names for the Kerberos (Domain Controller) and WINS servers in their respective boxes.

5. Click the **Save Settings** button.

Figure 3.5 Active Directory Authentication settings

6. You can optionally click **Test Saved Settings** to test the Active Directory authentication.

7. Click the **Select Domain Group** link.
   The Active Directory Authentication screen opens.
   *Important: Be sure you have entered the **Domain admin name and password** and saved the settings before clicking Select Domain Group.*

8. From the list, select the Active Directory Domain group the user must belong to in order to authenticate, and click the **Select Group** button (see Figure 3.6).

9. Click the **Save Settings** button again. You can also click the **Test Saved Settings** button to test the configuration.

10. Repeat this procedure to create a Master group for the Partners. In our example, we name the group **SharepointADPartners**. Be sure to select the appropriate Active Directory Domain group in step 13.
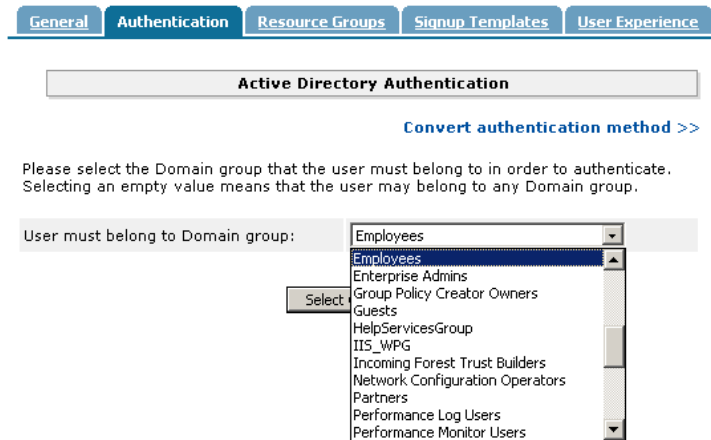

Figure 3.6 Selecting the Active Directory Domain Group

Limiting access for the Partner group

The FirePass controller allows you to limit access for specific groups on a very granular level. In this scenario, we limit access for the Partner group to only the Favorite we configured earlier, as well as restricting the areas of SharePoint they can access by URL.

To limit access for the Partner group

1. From the navigation pane, click **Portal Access**.

2. Under Web Applications, click **Master Group Settings**.

3. From the **Master Group** list at the top of the page, select the Master Group you created in the *Creating the Master groups* section. In our example, we select **SharePointADPartners**.
   The configuration settings for the Master group open.

4. In the **Access limitation** section, make sure there is a check in the **Show administrator-defined favorites only** box.

5. In the **Access Control Lists** section, configure URL pattern matches to allow and deny based on your deployment. In our example, we type the following (separated by commas) in the **Allow** box to restrict the Partner group to these areas of our SharePoint deployment:

   */_vti*bin/*,*/sites/partners/*,*/_layouts/*,*/MySite/*

   We leave the **Deny** box blank, which allows access to all URLs that pass the allow test (see Figure 3.7). The FirePass checks the deny list, then looks for matches in the allow list, then takes the default

action.

For more information on configuring the Access Control section, see the online help.

6. Click the **Update** button. The new settings take effect after any users currently logged onto the FirePass controller log out.

Figure 3.7 Restricting access to the SharePoint deployment

Configuring auto-logon

The FirePass device allows auto-logon (single sign-on) to sites supporting basic or NTLM authentication with user's FirePass credentials. In our scenario, we configure this option to allow single sign-on (SSO).

To configure SSO/NTLM for auto-login

1. From the navigation pane, click **Portal Access**.

2. Under Web Applications, click **Master Group Settings**.

3. From the **Master Group** list at the top of the page, select the Master Group you created in the *Creating the Master groups* section for employees. In our example, we select **SharepointAD**.
   The configuration settings for the Master group open.

4. In the **NTLM and Basic Auth Proxy** section, click a check in the **Auto-login to Basic and NTLM auth protected sites using FirePass user credentials** box.
   The NTLM and Basic Auth domain boxes display.

5. In the **NTLM Auth Domain (optional)** box, you can type the default Domain to be used in conjunction with the auto-login support.

6. In the **Basic Auth Domain (optional)** box, you can type the default Domain to be used in conjunction with the auto-login support. When specified, this value is prepended to the user name in the during Basic authentication (for example MYDOMAIN\username).

7. Click the **Update** button.

Figure 3.8 Configuring NTLM Master Group Settings

8. Repeat this procedure for the other Master group. In our example, we select **SharepointADPartners** from the **Master Group** list.

Configuring Endpoint security

One of the strong security features of the FirePass controller is the ability to set endpoint security on a extremely granular level.

In the following procedures, we configure a pre-logon check for anti-virus software on Windows machines. The FirePass controller uses this information to deny SharePoint access for members of the Partner Resource group if they do not have the appropriate software. In this configuration example, the FirePass device also denies access to *any* client that is determined to have a virus.

For more information on endpoint security, see the online help.

Creating a pre-logon sequence

The pre-logon sequence allows administrators to create one or more sequences of inspections for items such as installed antivirus programs or OS patch levels.

To configure a pre-logon sequence

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Pre-Logon Sequence**.

2. In the New Sequence section at the bottom of the page, type a name for the sequence in the **Create New Sequence** box. In our example, we type **SharePointBasic**.

3. From the **Based on** list, select **template: Collect information with no pre-logon actions**.

4. Click the **Create** button.
   The new sequence appears in the Select Sequence to Use table.

5. In the row of the sequence you just created, click the **Edit** button.
   *Warning - Do not click the radio button next to the sequence yet. If you click the radio button, the **Edit** link will be replaced with the **View** link, and you are not able to edit the sequence.*

   The Pre-Logon Sequence Editor opens.

6. Move the curser between **Sequence Start** and the box. A small add **[+]** link appears on the arrow (see the circle marked **1** in Figure 3.9). Click **Add**.
   The Change Sequence panel appears on the right.

7. Click the **Check for Antiviruses** option button, and click the **Apply Changes** button.
   The Edit Action panel opens.

   Note: The Check for Antiviruses is an optional feature on the FirePass controller. If your device does not have this license, you will not see this option.

8. Under **Inspectors**, click **Windows Antivirus Checker**.
   The Endpoint Inspector Details page opens in a new window.

9. Configure these options as applicable for your deployment. For more information, click **Help**.

10. Click the **Update** button.

11. In the Sequence pane, find **AV installed**, and click the associated Logon Denied Page link (see the circle marked **2** in Figure 3.9).
    The End Page Properties pane appears on the right.

12. From the Type box, select **Logon Allowed Page**. This allows a user to logon if they have an antivirus checker installed. You can optionally type a message for failed logons.

13. Repeat steps 11 and 12 for the **Fallback** option.

14. *Optional:* You can click the Logon Allowed Page or Logon Denied Page links for the other options to produce a custom message when a user is denied access. You can also change the actions taken as a result of the virus checker's findings. For example, you might still want to allow a user to login if there is virus checking software installed, but not currently running.

    In our example, we click **Logon Denied Page** next to **Virus Detected**, and type a message informing the user there is a virus on their computer.

15. When you are finished, click **Back to Console** in the upper right corner of the screen (see the circle marked 3 in the following figure).
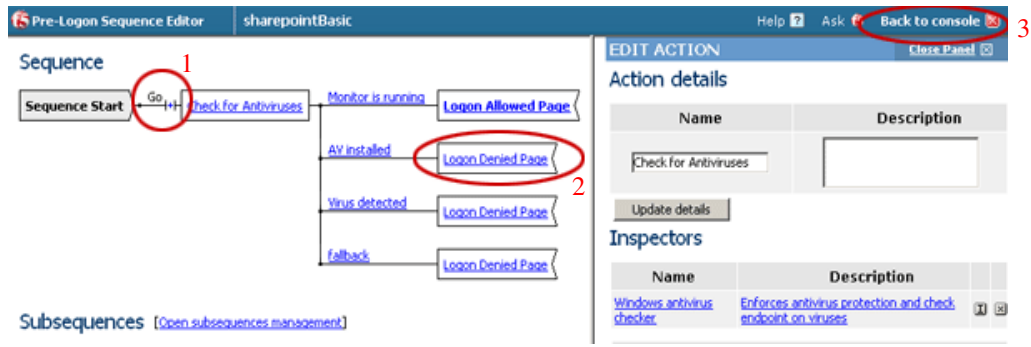   You return to the Pre-Logon Sequence main page.

Figure 3.9 The Pre-Logon Sequence Editor

16. From the **Select Sequence to Use** section, click the option button next to the sequence you just created. In our example, we click **sharepointBasic**.

17. Click the **Apply** button.

Protected Configurations

Protected Configurations allow administrators to specify the criteria the endpoint systems must meet to enable access to the various resources. In this procedure, we create a protected configuration for the partner group in order make additional security requirements for that group.

To configure Protected Configurations

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Protected Configurations**.

2. Click **New Protection Configuration**.

3. In the Protected configuration ID box, type a name for this configuration. In our example, we type **Partner_config**. You can optionally type a description.

4. Leave the Mode list at the default setting, **Check endpoint protection, grant access if check passed** (see Figure 3.10).

Figure 3.10 The General tab of the Protected Endpoint Configuration screen

5. Click the Protected Criteria tab.

6. On the menu bar, click **Information Leaks**.

7. From the Required safety measures or checks list, select **Cache Cleaner** and click the **Add** button. This will remove content from the cache when a user logs off.

Figure 3.11 The Protection Criteria tab of the Protected Endpoint Configuration screen

Important: *The Cache Cleaner feature is currently Windows only. It does not work with Apple Macintosh or Linux systems.*

8. On the menu bar, click **Virus Attack**

9. From the list, select **Antivirus** and click the **Add** button.

10. Click the **I** icon next to Antivirus to configure the antivirus properties (see Figure 3.12). The Select trusted anti-viruses screen opens. Configure these properties as applicable for your configuration, and click the **Save** button.

    You return to the Protection Criteria tab of the Protected Endpoint Configuration page.
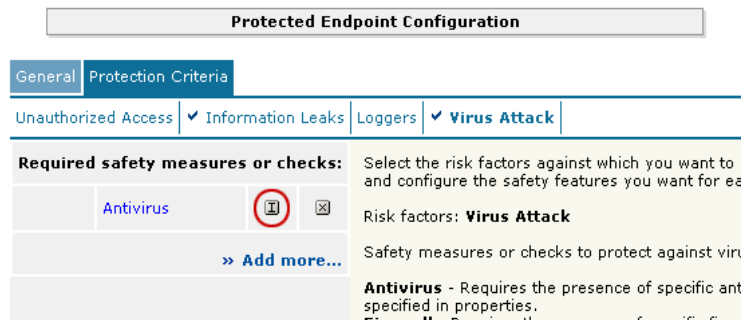
11. Click the **Save** button.

Figure 3.12 The Edit button for Antivirus properties

Protecting the Resources

The next step is to associate the protected configuration you just created with a resource.

To protect the resources

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Protect Resources**.

2. From the Resource Table, expand **Web Applications**.

3. Find the **Partners** resource group (in our example, **Partners_SP**), and click the **Select** link next to the Favorite you configured.

4. From the **Configuration to protect selected resources** list, select the name of the configuration you created in the preceding procedure. In our example, we select **Partner_config**.

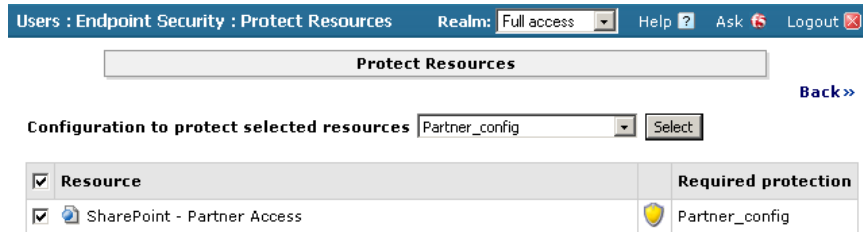5. Click the box next to the Favorite name, and click the **Select** button. A shield image appears in the row.

Figure 3.13 Adding the Protected Configuration to the Resource

Configuring post-logon actions

The final step is to configure a post-logon action in which the FirePass device injects an Active X control or plug-in to clean the client browser's web cache.

To configure the post-logon action

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Post-Logon Actions**.

2. Click a check in the **Inject ActiveX/Plugin to clean-up client browser web cache** box. A list of options displays.

3. Configure these options as applicable for your deployment. In our example, we leave these options at their default settings.

Conclusion

The FirePass controller is now configured to allow secure remote access to the Microsoft Office SharePoint Server 2007 deployment. Remember that the procedures in this Deployment Guide are specific to the scenario described in *Configuration scenario*, on page 3-1. Use this guide as a template, and modify the configuration as applicable to your deployment.