Deployment Guide

Document Version 1.2

What's inside:

Configuring the BIG-IP LTM for FAST Search Server 2010 for SharePoint 2010

Welcome to the F5 deployment guide for Microsoft® FAST Search Server 2010 for SharePoint®. This document provides guidance on how to configure the BIG-IP LTM to optimize connections from SharePoint 2010 servers to a FAST Search Server 2010 farm.

FAST Search Server 2010 for SharePoint uses deep linguistics and text analytics technology to add tags and structure to unstructured information, automatically creating metadata directly from the content.

For more information on Microsoft FAST Search Server 2010, see *http://sharepoint.microsoft.com/en-us/product/capabilities/search/Pages/Fast-Search.aspx*

For more information on the BIG-IP LTM, see *http://www.f5.com/products/big-ip/local-traffic-manager.html*

For other deployment guides on configuring F5 devices with Microsoft SharePoint, see: *http://www.f5.com/solutions/resources/deployment-guides*

Products and versions tested

Product	Version
BIG-IP LTM	10.2.1, 10.2.2, 11
SharePoint FAST Search Server	2010

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- You must already have a working FAST Search for SharePoint 2010 deployment, and that you are using the default port numbers for each FAST service.
- If you are configuring the BIG-IP LTM as described in *Configuring a local virtual server for SharePoint 2010 on page 9* to ensure thumbnails are properly displayed in FAST search results, the virtual server you create must be on the same VLAN as the FAST Search servers; this section is written with the assumption that the SharePoint 2010 servers are also on this VLAN.

- Because SharePoint 2010 uses built-in load balancing to communicate with the FAST Search farm, you need to specify the IP address and service port of the BIG-IP LTM virtual server instead of individual server FQDNs when configuring the FAST Query SSA properties. This setting is found in SharePoint Central Administration>Application Management>Service Applications. Consult the Microsoft documentation for configuring FAST Search for more information.

- If you want to encrypt communication between SharePoint 2010 and the FAST Search Query service, follow the instructions from Microsoft for enabling SSL on the FAST Search servers and in the properties of the SharePoint 2010 Query SSA. Because FAST Search does not support SSL offloading, you will also need to apply a server SSL profile to the Query virtual server as described in this guide.

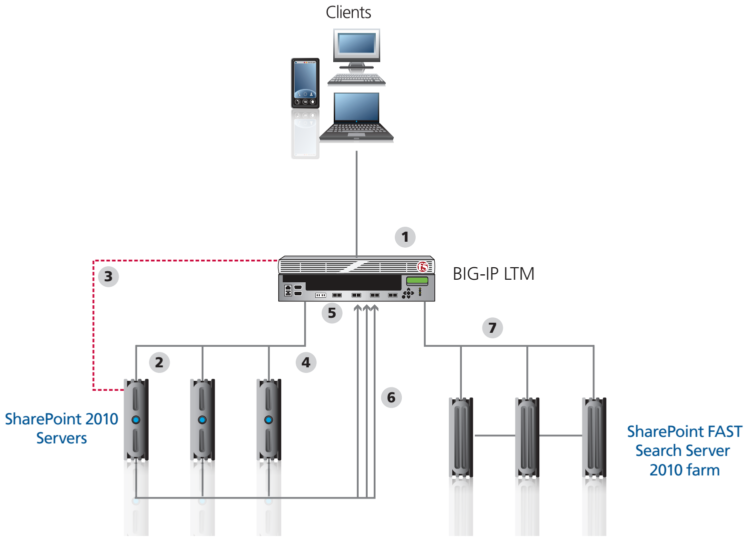
- You are NOT required to create all of the virtual servers described in this guide; you can choose to deploy any combination of them depending on how many FAST servers are running each role (for example, you may have only one server running FAST Admin service).

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 3*

Configuration example

The following diagram shows the traffic flow for the configuration described in this guide.



1. The user makes a request to the SharePoint server.
2. The external BIG-IP LTM virtual server receives the request and directs the user to an available SharePoint server.
3. If split DNS is not configured, and requests from the SharePoint 2010 front end servers to the SharePoint URL are routed through the external SharePoint virtual server on the BIG-IP LTM, users may experience missing thumbnails in FAST Search results when a request from the WFE server is load balanced to another server rather than to itself. To prevent this, we create a virtual server on the SharePoint server VLAN and the iRule in #5.

4. The Host entry on the SharePoint server points to the internal virtual server on the BIG-IP LTM. The SharePoint SSA is configured to use the BIG-IP LTM virtual servers for FAST search.
5. A BIG-IP virtual server on the same local VLAN as the SharePoint 2010 servers includes an iRule that ensures each request is directed to the same server that made it, so thumbnails are properly displayed.
6. The search request travels from the SharePoint servers to the FAST virtual servers on the LTM.
7. The BIG-IP LTM directs the request to the appropriate FAST server.

Configuring SharePoint Alternate Access Mappings to support SSL offload

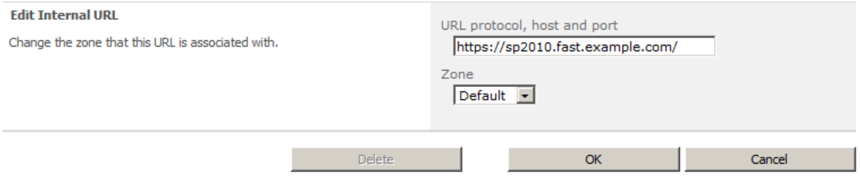
When using the BIG-IP LTM system for SSL offload, for each SharePoint Web Application that will be deployed behind LTM, you must configure your SharePoint Alternate Access Mappings and Zones allow users to access non-SSL sites through the BIG-IP LTM SSL virtual server and ensure correct rewriting of 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

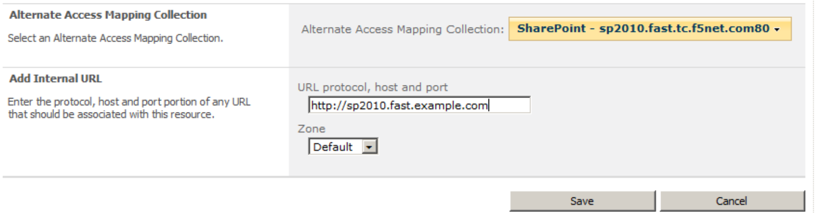
1. From SharePoint Central Administration navigation pane, click **Application Management**.
2. In the main pane, under Web Applications, click **Configure alternate access mappings**.
3. From the **Internal URL** list, click the Internal URL corresponding to the Public URL you want to be accessible 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.


Edit Internal URL
Change the zone that this URL is associated with.

URL protocol, host and port
https://sp2010.fast.example.com/

Zone
Default

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.


Alternate Access Mapping Collection
Select an Alternate Access Mapping Collection.

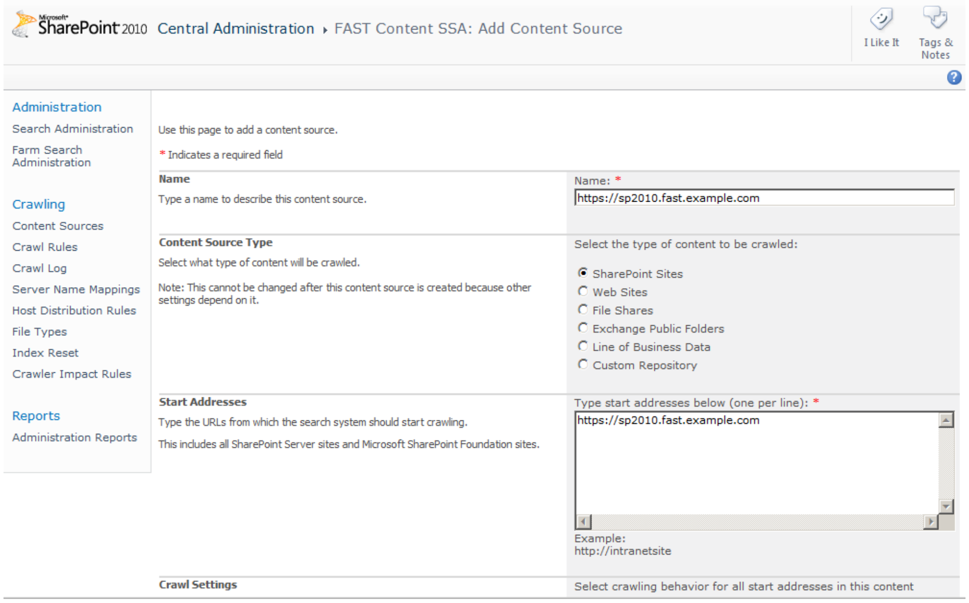
Alternate Access Mapping Collection: SharePoint - sp2010.fast.tc.f5net.com80

Add Internal URL
Enter the protocol, host and port portion of any URL that should be associated with this resource.

URL protocol, host and port
http://sp2010.fast.example.com

Zone
Default

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



Use this page to add a content source.

* Indicates a required field

Name
Type a name to describe this content source.

Name: *
https://sp2010.fast.example.com

Content Source Type
Select what type of content will be crawled.

Note: This cannot be changed after this content source is created because other settings depend on it.

Select the type of content to be crawled:
● SharePoint Sites
○ Web Sites
○ File Shares
○ Exchange Public Folders
○ Line of Business Data
○ Custom Repository

Start Addresses
Type the URLs from which the search system should start crawling.

This includes all SharePoint Server sites and Microsoft SharePoint Foundation sites.

Type start addresses below (one per line): *
https://sp2010.fast.example.com

Example:
http://intranetsite

Crawl Settings
Select crawling behavior for all start addresses in this content

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

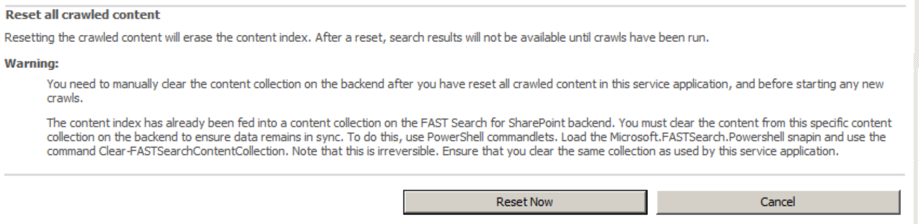
After configuring Alternate Access Mappings in SharePoint 2010 to support SSL offloading, you must perform additional steps to ensure that search results are properly displayed for https:// queries. The examples below depict modifying the Content Search Service Application; however, you must also perform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



Reset all crawled content

Resetting the crawled content will erase the content index. After a reset, search results will not be available until crawls have been run.

Warning:

You need to manually clear the content collection on the backend after you have reset all crawled content in this service application, and before starting any new crawls.

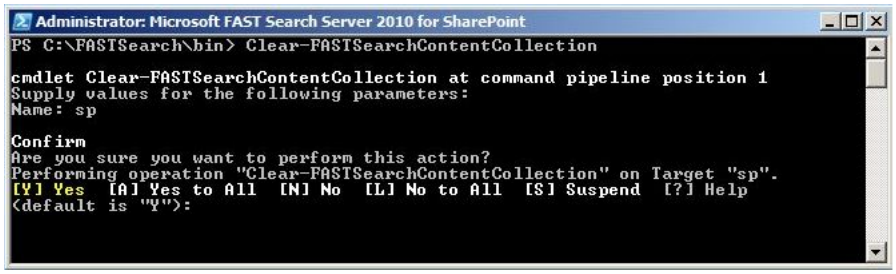
The content index has already been fed into a content collection on the FAST Search for SharePoint backend. You must clear the content from this specific content collection on the backend to ensure data remains in sync. To do this, use PowerShell commandlets. Load the Microsoft.FASTSearch.Powershell snapin and use the command Clear-FASTSearchContentCollection. Note that this is irreversible. Ensure that you clear the same collection as used by this service application.

The next three steps are performed on the FAST servers.

6. Log into one of the FAST servers and open the FAST Search Server SharePoint PowerShell console.
7. From a prompt, run the following command against the content collection for which you are resetting the index:

```
Clear-FASTSearchContentCollection
```

8. Type **Y** to confirm. You can exit the command prompt.



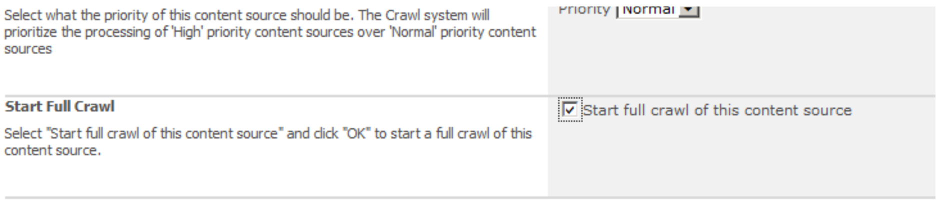
Administrator: Microsoft FAST Search Server 2010 for SharePoint

```
PS C:\FASTSearch\bin> Clear-FASTSearchContentCollection

cmdlet Clear-FASTSearchContentCollection at command pipeline position 1
Supply values for the following parameters:
Name: sp

Confirm
Are you sure you want to perform this action?
Performing operation "Clear-FASTSearchContentCollection" on Target "sp".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

9. Return to your Content SSA (repeat steps 1-3).
10. From the navigation pane, under Crawling, click **Content Sources**.
11. Click the content source for which you just reset the search index.
12. 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.



Select what the priority of this content source should be. The Crawl system will prioritize the processing of 'High' priority content sources over 'Normal' priority content sources

Priority Normal

Start Full Crawl

Select "Start full crawl of this content source" and click "OK" to start a full crawl of this content source.

☑ Start full crawl of this content source

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

Configuring the BIG-IP LTM for FAST Search Server 2010

Use the following tables to configure the BIG-IP LTM system. The tables contain a list of BIG-IP LTM configuration objects, along with any non-default settings. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

As mentioned in the prerequisites, you are not required to create all virtual servers listed in the table, depending on your configuration.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitors (*Main tab-->Local Traffic -->Monitors*)	***HTTP monitor for the Query service***	
	Name	Type a unique name
	Type	**HTTP** (or HTTPS using SSL for the Query service)
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	HTTP monitor for the Admin service	
	Name	Type a unique name
	Type	**HTTP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	HTTP monitor for the Resource Store	
	Name	Type a unique name
	Type	**HTTP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	TCP monitor for the Content service	
	Name	Type a unique name
	Type	**HTTP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
Pools (*Main tab-->Local Traffic -->Pools*)	***Query service pool***	
	Name	Type a unique name
	Health Monitor	Select the HTTP(S) monitor you created for Query
	Slow Ramp Time[1]	**300**
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**
	Address	Type the IP Address of the FAST Search server running the Query service role
	Service Port	**13287** (**13286** if using SSL) Click **Add** to repeat Address and Service Port for all nodes)
	Admin service pool	
	Name	Type a unique name
	Health Monitor	Select the HTTP monitor you created for the Admin service
	Slow Ramp Time[1]	**300**
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**
	Address	Type the IP Address of the FAST Search server running the Admin service role
	Service Port	**13257** Click **Add** to repeat Address and Service Port for all nodes)

This table continues on the following page

[1] You must select Advanced from the Configuration list for these options to appear.

BIG-IP LTM Object	Non-default settings/Notes		
Pools (*Main tab-->Local Traffic -->Pools*)	***Resource Store pool***		
	Name	Type a unique name	
	Health Monitor	Select the HTTP monitor you created for Resource Store	
	Slow Ramp Time[1]	**300**	
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**	
	Address	Type the IP Address of the FAST Search server running the Resource Store	
	Service Port	**13255** Click **Add** to repeat Address and Service Port for all nodes)	
	Content service pool		
	Name	Type a unique name	
	Health Monitor	Select the HTTP(S) monitor you created for Content	
	Slow Ramp Time[1]	**300**	
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**	
	Address	Type the IP Address of the FAST Search server running the Content service role.	
	Service Port	**13391** Click **Add** to repeat Address and Service Port for all nodes)	
Profiles (*Main tab-->Local Traffic -->Profiles*)	***OneConnect*** (*Profiles-->Other*)	Name	Type a unique name
		Parent Profile	**oneconnect**
	TCP LAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
	Client SSL[2] (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate and key	Select your Certificate and Key
	Server SSL[2] (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**serverssl**
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	***Query service virtual server***		
	Name	Type a unique name.	
	Destination Address	Type the IP address for this virtual server	
	Service Port	**13287** (**13286** if using SSL)	
	Protocol Profile (Client)[1]	Select the TCP LAN profile you created above	
	SSL Profile (Client)[2]	If using SSL, select the Client SSL profile you created above	
	SSL Profile (Server)[2]	If using SSL, select the Server SSL profile you created above	
	SNAT Pool	**Automap**	
	Default Pool	Select the Query service pool you created above	
	Admin service virtual server		
	Name	Type a unique name.	
	Destination Address	Type the IP address for this virtual server	
	Service Port	**13257**	
	Protocol Profile (Client)[1]	Select the TCP LAN profile you created above	
	SNAT Pool	**Automap**	
	Default Pool	Select the Admin service pool you created above	

This table continues on the following page

[1] You must select Advanced from the Configuration list for these options to appear.

[2] Client SSL and Server SSL profiles are only required if you are using SSL for your Query service.

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	***Resource Store virtual server***	
	Name	Type a unique name.
	Destination Address	Type the IP address for this virtual server
	Service Port	**13255**
	Protocol Profile (Client)[1]	Select the TCP LAN profile you created above
	SNAT Pool	**Automap**
	Default Pool	Select the Resource Store pool you created above
	Content service virtual server	
	Name	Type a unique name.
	Destination Address	Type the IP address for this virtual server
	Service Port	**13391**
	Protocol Profile (Client)[1]	Select the TCP LAN profile you created above
	SNAT Pool	**Automap**
	Default Pool	Select the Content service pool you created above

[1] You must select Advanced from the Configuration list for these options to appear.

This completes the configuration. If applicable, continue with *Configuring a local virtual server for SharePoint 2010 on page 9.*

Configuring a local virtual server for SharePoint 2010

If you are not using split DNS, and requests from the SharePoint 2010 front end servers to the SharePoint URL are routed through the external SharePoint virtual server on the BIG-IP LTM you may see problems with missing thumbnails in FAST Search results when a request from the WFE server is load balanced to another server rather than to itself.

In this case, you need to configure a virtual server on the same local VLAN as the SharePoint 2010 servers that includes an iRule. The iRule ensures each request is directed to the same server that made it.

You must also add a host entry to the WFE servers directing all requests for the SharePoint URL to the IP address of the internal SharePoint virtual server. See the Microsoft documentation for instructions.

Use the following table to create the objects on the BIG-IP LTM. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitors (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name	
	Type	**HTTP**	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
Pools (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name	
	Health Monitor	Select the HTTP monitor you created above	
	Load Balancing Method	**Round Robin**	
	Address	Type the IP Address of your SharePoint server	
	Service Port	**80** Click **Add** to repeat Address and Service Port for all nodes	
Profiles (*Main tab-->Local Traffic -->Profiles*)	***Persistence*** (*Profiles-->Persistence*	Name	Type a unique name
		Persistence Type	**Source Address Affinity**
	TCP LAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
iRules (*Main tab-->Local Traffic -->iRules*)	***Name***	Type a unique name	
	Definition	See ***Creating the iRule definition on page 10*** for the iRule definition	
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	***Name***	Type a unique name.	
	Destination Address	Type the IP address for this virtual server	
	Service Port	**80**	
	Protocol Profile (Client)[1]	Select the TCP LAN profile you created above	
	SNAT Pool	**Automap**	
	iRule	Enable the iRule you created above	
	Default Pool	Select the pool you created above	
	Default Persistence Profile	Select the persistence profile you created above	

[1] You must select Advanced from the Configuration list for these options to appear.

Creating the iRule definition

Use the following code for the Definition section of the iRule, omitting the line numbers.

Critical →

Be sure to change the red text below to the name of the pool you created in the table.

```
when CLIENT_ACCEPTED {
    set pm_selected 0
    foreach { pm } [members -list internal-SharePoint-pool-name] {
    if { $pm equals “[IP::remote_addr] 80” } {
        set pm_selected 1
        pool internal-SharePoint-pool-name member [IP::remote_addr]
    }
}
if { $pm_selected equals 0 } {
    pool internal-SharePoint-pool-name
    }
}
```

This completes the configuration.

Document Revision History

Version	Description	Date
1.0	New document	N/A
1.1	Added instructions for configuring SharePoint Alternate Access Mappings if offloading SSL on the BIG-IP system.	3-26-2012
1.2	Added additional instructions to the Alternate Access Mappings section for ensuring the search results are properly displayed for HTTPS queries.	4-2-2012

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc. **Corporate Headquarters**	**F5 Networks** **Asia-Pacific**	**F5 Networks Ltd.** **Europe/Middle-East/Africa**	**F5 Networks** **Japan K.K.**
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	f5j-info@f5.com