

Deployment Guide

**Deploying Microsoft SharePoint Portal Server
2003 and the F5 BIG-IP System**



Introducing the BIG-IP and SharePoint Portal Server 2003 configuration

F5 and Microsoft have collaborated on a highly effective solution for intelligently directing traffic to Microsoft® SharePoint® Portal Server 2003 deployments with the BIG-IP system from F5. Microsoft SharePoint Portal Server 2003 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.

Organizations using the BIG-IP system benefit from mission-critical availability, intelligent traffic management, simple scalability, and enhanced security for Microsoft SharePoint Portal Server 2003 deployments.

For more information on the Microsoft SharePoint Portal Server 2003, see <http://www.microsoft.com/office/sharepoint/prodinfo/default.msp>

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

Prerequisites and configuration notes

The following are prerequisites for this deployment:

- ◆ The BIG-IP system must be running version 9.1 or later. We recommend version 9.2.3 or later. BIG-IP LTM version 9.2.3 includes updates for HTTP profiles to more reliably support use with Microsoft Sharepoint Portal Server. Through the use of HTTP profiles, it's possible to use advanced features such as compression and HTTP iRule methods in conjunction with a SharePoint Portal Server deployment.
- ◆ For certain *optional* optimization features, the appropriate module on the BIG-IP LTM system must be licensed (such as compression).

◆ Important

*If you are running the BIG-IP system 9.0 - 9.1, you must refer to **Solution 5140** on Ask F5 before continuing this Deployment Guide. For these versions, the BIG-IP system may require additional configuration steps that are outlined in the solution.*

- ◆ The SharePoint Portal Server must be the 2003 edition.
- ◆ All of the configuration procedures in this document are performed on the BIG-IP system. For information on how to deploy or configure the SharePoint Portal Server 2003, consult the appropriate Microsoft documentation.
- ◆ Briefly review the basic configuration tasks and the few pieces of information, such as IP addresses, that you should gather in preparation for completing this configuration.

◆ **Note**

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

Configuration example

The BIG-IP system provides intelligent traffic management and high availability for Microsoft SharePoint Portal Server 2003 deployments. This SharePoint configuration was built according to the Medium server farm deployment in Microsoft help documentation.

◆ **Tip**

Although only one BIG-IP device is necessary for this configuration, we strongly recommend a redundant BIG-IP device for the highest level of availability.

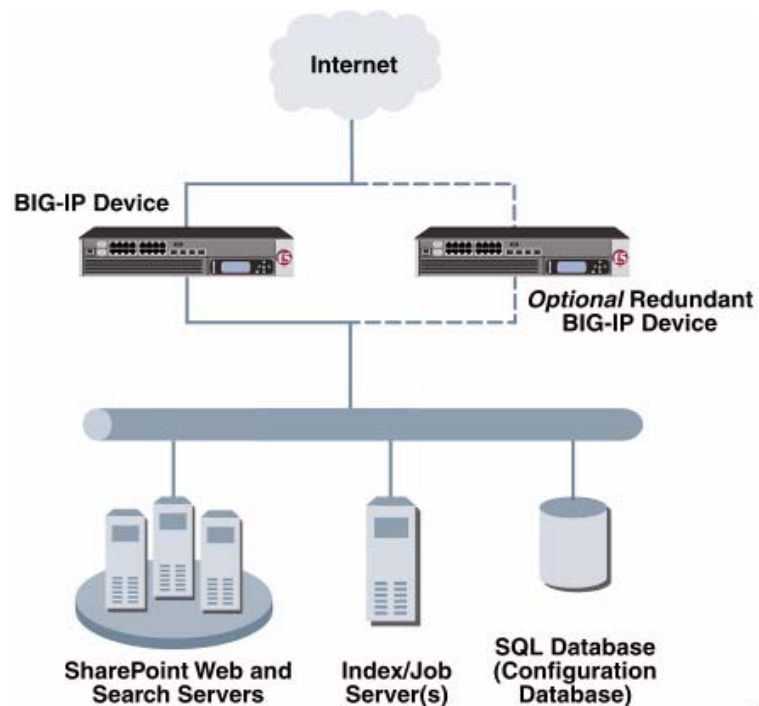


Figure 1 BIG-IP SharePoint Server logical configuration

Configuring the BIG-IP system for deployment with SharePoint devices

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

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

◆ 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 16.*

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

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 VLANs

A VLAN is a grouping of separate networks that allows those networks to behave as if they were a single local area network, whether or not there is a direct ethernet connection between them. For this configuration, you need to have both an external and internal facing VLAN on the BIG-IP system.

If you do not already have these VLANs configured on the BIG-IP system, or what to create new VLANs on the BIG-IP device for your SharePoint Portal Server deployment, use the following procedure to create a new VLAN.

To create a VLAN on the BIG-IP system

1. On the Main tab, expand **Network**, and then click **VLANs**.
The VLANs screen opens.
2. Click the **Create** button.
The new VLAN screen opens.
3. In the **Name** box, type a unique name for the VLAN. In our example we use **External**.
4. You can leave the **Tag** box empty, and the BIG-IP device automatically assigns a Tag by default. If your network requires a specific Tag, type the Tag in the box.
5. In the **Resources** section, from the Available list, select the interface that you want to associate with the External VLAN, and click the **Add (<<)** button to add the Interface to the **Untagged** list.
If your network requires tags, click the Add (>>) button to add the interface to the **Tagged** list.
In our example, we select **1.1** and add it to the **Untagged** list.
6. Click the **Finished** button.

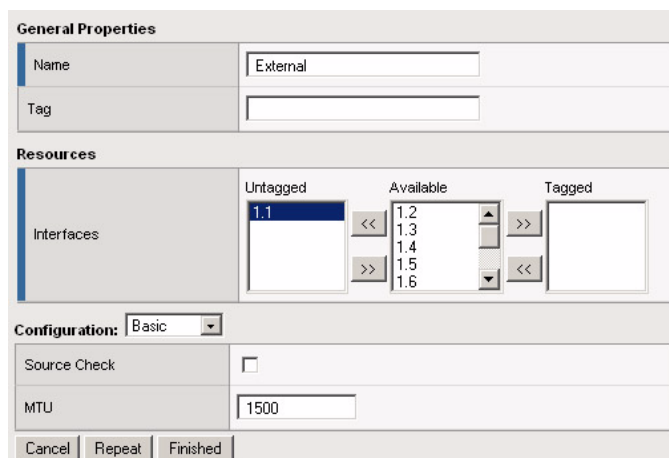


Figure 2 Adding a VLAN in the BIG-IP Configuration utility

Repeat this procedure for the internal facing VLAN, giving it a different name, and associating a different interface. In our example, we name the VLAN **Internal**, and associate it with the **1.2** interface as **Untagged**.

Creating the Self IP addresses

Self IP addresses are the IP addresses owned by the BIG-IP system that you use to access the internal and external VLANs. The next step in this configuration is to create two self IP addresses, one for each VLAN.

To create a self IP address

1. On the Main tab, expand **Network**, and then click **Self IPs**.
The Self IP screen opens.
2. Click the **Create** button.
The new Self IP screen opens.
3. In the **IP Address** box, type an IP address in the appropriate VLAN (the VLAN you choose in step 5).
In our example, we type **192.168.104.145**.
4. In the **Netmask** box, type the corresponding subnet mask.
In our example, we type **255.255.255.0**.
5. From the **VLAN** list, select the appropriate VLAN.
In our example, we select **external**.
6. Click the **Finished** button.
The new self IP address appears in the list.

Configuration	
IP Address	<input type="text" value="192.168.104.145"/>
Netmask	<input type="text" value="255.255.255.0"/>
VLAN	<input type="text" value="external"/>
Port Lockdown	<input type="text" value="Allow Default"/>
Floating IP	<input type="checkbox"/>
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>	

Figure 3 Adding a self IP address in the BIG-IP Configuration utility

- Repeat this procedure for the self IP on the internal facing VLAN,

◆ **Note**

If you are using a BIG-IP redundant configuration, you need to assign a floating IP. For more information about floating IPs and self IPs, refer to the BIG-IP documentation.

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 Extended Content Verification (ECV) 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 ECV health monitors are now associated at the pool level.

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

- On the Main tab, expand **Local Traffic**, and then click **Monitors**. The Monitors screen opens.
- Click the **Create** button. The New Monitor screen opens.
- In the **Name** box, type a name for the Monitor. In our example, we type **SPSHTTP_monitor**.
- From the **Type** list, select **http**. The HTTP Monitor configuration options appear.
- 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 (for example, the default setting has an interval of **5** and an timeout of **16**). In our example, we use a **Interval** of **30** and a **Timeout** of **91**.

-
- In the Send String and Receive Rule sections, you can add a Send String and Receive Rule specific to the device being checked.

Important Note:

When using the **GET** send string, you must end the string by including the **HTTP** protocol at the end of the statement. Use the following syntax:

GET <fully qualified path name> HTTP/1.0

For example:

GET /www/support/customer_info_form.html HTTP/1.0

The screenshot shows the 'New Monitor...' configuration window. The 'General Properties' section includes fields for Name (SPSHTTP_monitor), Type (HTTP), and Import Settings (http). The 'Configuration' section is set to 'Basic' and includes fields for Interval (30 seconds) and Timeout (91 seconds). The 'Send String' field contains 'GET / HTTP/1.0'. The 'Receive String' field is empty. Blue circles highlight the Name, Type, Interval, and Timeout fields.

Figure 4 Creating the HTTP Monitor

- Click the **Finished** button.
The new 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

- On the Main tab, expand **Local Traffic**, and then click **Pools**.
The Pool screen opens.
- 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 Figure5).

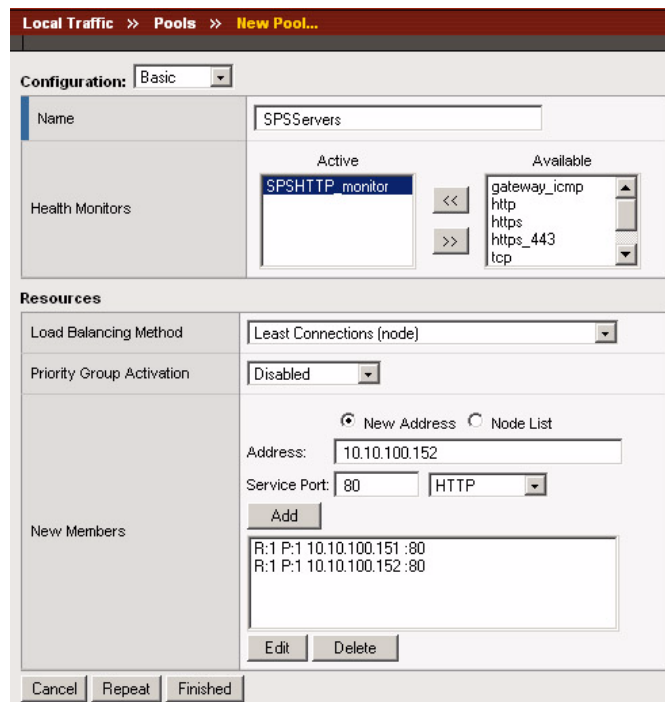


Figure 5 Adding the SharePoint server pool

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.

There are additional configuration steps if you want to optimize the BIG-IP system for SharePoint deployments. These optional portions of the configuration will be clearly marked with *Optional Optimization:*

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 Portal Server 2003, **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 our example, we leave all the options at their default settings. You can configure these options as appropriate for your network.

The first new profile we create is an HTTP profile. In our example, we leave all the options at their default settings, unless you are configuring the optimized deployment. The HTTP profile is where the optional Intelligent Compression options are located (which must be licensed on your BIG-IP system). If you have not licensed the module, you will not see the options described in the procedures.

◆ **Note**

The following procedure shows one way to optimize the Microsoft SharePoint configuration that has been tested in real-world scenarios by F5 using the Gomez Performance Network, 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 based on the default HTTP profile

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**.
The HTTP Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button.
The New HTTP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **SPSHTTP**.
5. From the **Parent Profile** list, ensure that **HTTP** is selected.

***Optional Optimization:** The following 8 steps are optional and show one way to optimally configure Compression on the BIG-IP system. If your configuration does not contain compression, skip to Step 14.*

6. In the Settings table, from the **Response Chunking** section, click a check in the Custom box. From the list, select **Unchunk**. This allows for more efficient caching and compression.

-
7. In the Compression table, from the Compression row, click a check in the Custom box, then select **Enabled** from the list.
 8. In the Content list section, we leave the settings at the default level, configure as applicable for your deployment.
 9. In the Compression Buffer Size section, click a check in the Custom box. In the **Compression Buffer Size** box, type **131072**.
 10. In the gzip Compression Level section, click a check in the Custom box. From the list, select a level of compression suitable to your configuration. For the most compression, select **9 - Most Compression (Slowest)**.
 11. In the gzip Memory Level section, click a check in the Custom box. From the list, select **16** kilobytes.
 12. In the gzip Window size section, click a check in the Custom box. From the list, select **64** kilobytes.
 13. In the HTTP/1.0 Requests section, click a check in the Custom box. Click a check in the box to enable HTTP/1.0 requests.
 14. Modify any of the other settings as applicable for your network.
 15. Click the **Finished** button.

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

Creating a TCP profile

The next profile we create is the TCP profile. The BIG-IP system's TCP Express feature set provides a number of enhancements and optimizations to TCP handling that enhance end user experience, so there are also *Optional Optimization* steps in this procedure.

To create a new TCP profile based on the default 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 **SPSTCP**.

Optional Optimization: The following 4 steps are optional and show one way to optimally configure Compression on the BIG-IP system. If your configuration does not contain compression, skip to Step 10.

6. In the Configuration table, locate **Proxy Buffer Low**, and click a check in the Custom box on the far right. In the Proxy Buffer Low box, type **131072**.
7. In the **Proxy Buffer High** section, click a check in the Custom box, and in the Proxy Buffer High box, type **131072**.
8. In the **Send Buffer** section, click a check in the Custom box, and in the Send Buffer box, type **65535**.
9. In the **Receive Window** section, click a check in the Custom box, and in the Receive Window box, type **65535**.
10. Modify any of the settings as applicable for your network.
11. 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 virtual server

Next, we configure a 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.

General Properties	
Name	SPS_virtual
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network
	Address: 192.168.104.147
Service Port	80 HTTP
State	Enabled

Figure 6 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 2003, **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.

- 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 7).

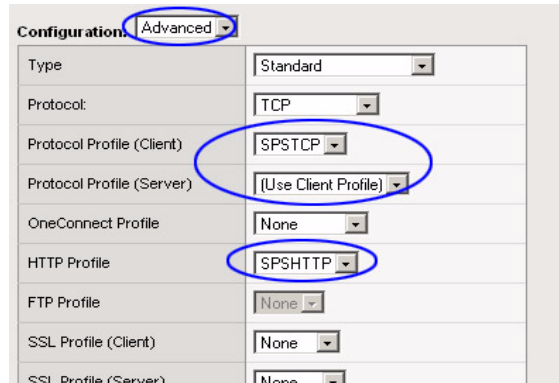


Figure 7 Selecting the TCP and HTTP profiles for the virtual server

- 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**.
- 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**.

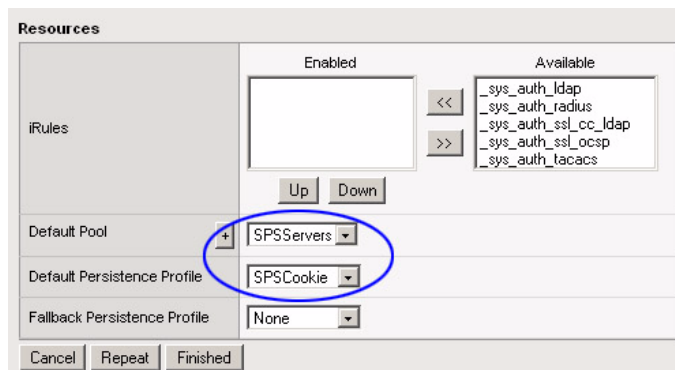


Figure 8 Resources section of the add virtual server page

- 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 system is now configured to direct traffic to the Microsoft SharePoint Portal Server 2003 deployment.

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. In our example, we type **pre_SPS_backup.ucs**.
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.

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.