



Deploying TrafficShield with the BIG-IP system version 9.0 and later

- Introducing the TrafficShield and BIG-IP configuration
- Configuring the BIG-IP system for deployment with TrafficShield
- Configuring the TrafficShield device to reference the BIG-IP virtual server
- Appendix A: Backing up and restoring the BIG-IP system configuration

Introducing the TrafficShield and BIG-IP configuration

This Deployment Guide describes how to configure the BIG-IP system to load balance F5's TrafficShield application firewall device. Most of the configuration in this guide is performed on the BIG-IP system, it is not intended to be a configuration guide for the TrafficShield device.

Prerequisites and configuration notes

The following are prerequisites for this Deployment Guide:

- ◆ The BIG-IP system must be running version 9.0 or later. For versions 4.5.x or 4.6.x, see www.f5.com/solution-center/deployment-guides/ts-bigip45-dg.pdf
- ◆ The TrafficShield device must be running version 3.0 or later.
- ◆ Briefly review the basic configuration tasks and the few pieces of information, such as IP addresses, that you should gather in preparation for completing the BIG-IP system configuration.

Configuration example

In this configuration example, there is a BIG-IP system in a redundant configuration in front of the TrafficShield (also in a redundant configuration) and four web servers (see Figure 1.1). Traffic comes in to the BIG-IP system and is load balanced to a pool that contains both the TrafficShield device and the web servers. The BIG-IP system uses the priority setting on the pool members to direct traffic to the TrafficShield device, and only to the web servers in the unlikely event that the TrafficShield is unavailable (described in detail in the *Creating the TrafficShield and web server pool* section). The TrafficShield device processes the traffic, and sends it back to the BIG-IP system to be load balanced to the web server pool.

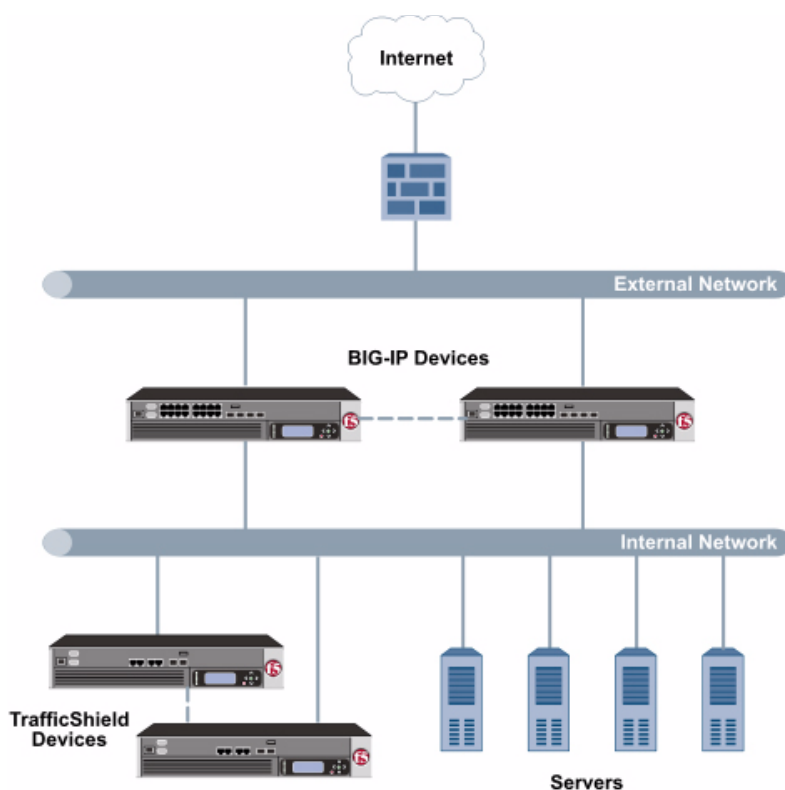


Figure 1.1 BIG-IP TrafficShield configuration example

Configuring the BIG-IP system for deployment with TrafficShield

To configure the BIG-IP for directing traffic to the TrafficShield devices, you need to complete the following procedures:

- *Connecting to the BIG-IP device*
- *Creating the pools*
- *Creating virtual servers*
- *Configuring a health monitor*
- *Synchronizing the BIG-IP configuration if using a redundant system*

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. Advanced users can also use the BIG-IP **bigpipe** command line interface,

but procedures are not included in this guide. Unless you are familiar with using the **bigpipe** command line interface, we recommend using the Configuration utility.

◆ **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 1-20.*

Connecting to the BIG-IP device

The first step in this configuration is to connect to the BIG-IP system. You can connect to the BIG-IP system using the Configuration utility or the command line.

Connecting to the BIG-IP device using the Configuration utility

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.

Configuring the BIG-IP system for TrafficShield

To configure the BIG-IP system to load balance TrafficShield, you need to create pools, virtual servers, and a health monitor on the BIG-IP system.

Creating the pools

The first procedure in this configuration is to configure pools for the TrafficShield devices and the servers. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method.

For this configuration, you configure two pools on the BIG-IP system, one pool with the TrafficShield and servers, and one just for the servers.

Creating the TrafficShield and web server pool

The first pool we create includes both the TrafficShield and the servers. Using the priority setting on the BIG-IP pool, all traffic for this pool is sent to the TrafficShield device for processing because it has a higher priority setting. In the extremely unlikely event that the TrafficShield device is unavailable, traffic is automatically directed to the servers (with lower priority settings). This ensures that even if the TrafficShield is down, users can still access the web servers. For more information on directing traffic using priority, see the Online Help or the *Configuration Guide for Local Traffic Management*.

This pool uses the TrafficShield Service IP address. The Service IP is the address at which the TrafficShield security application unit receives requests directed to the Web application. In a network not protected by TrafficShield system, this would be the IP address of the web server.

To create the TrafficShield and server pool from the Configuration utility

1. On the Main tab, expand **Local Traffic**.
2. Click **Pools**.
The Pool screen opens.
3. 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.*

4. In the **Name** box, enter a name for your pool.
In our example, we use **trafficshield_pool**.
5. Leave the **Health Monitors** section empty for now, we configure a health monitor later in this guide.
6. From the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
7. From the **Priority Group Activation** list, select **Less than**.
The Priority Group configuration options display.

8. In the Available Members box, type **1**. If you are adding more than one TrafficShield device, set this number to equal the number of TrafficShield devices.
9. In the New Members section, make sure the **New Address** option button is selected.
10. In the **Address** box, we first add the TrafficShield device to the pool. Type the TrafficShield Web Application Service IP address. (see Figure 1.2).
In our example, we type **192.168.200.11**.



Figure 1.2 The finding the Web Application Service IP in the TrafficShield user interface.

11. In the **Service Port** box, type the service number you want to use for this device, or specify a service by choosing a service name from the list (for example **80** or **443**).
In our example, we type **80**.
12. In the **Priority** box, type a priority of **10**. A higher priority setting will receive traffic before lower settings.
13. Click the **Add** button to add the member to the list.
14. Repeat steps 9-12 for each of the web servers. In Step **11**, type a priority of **1** for each of the servers.

Important: *The priority setting (step 11) for the web servers must be lower than that of the TrafficShield device.*

In our example, we repeat these steps four times for each of the servers. In our example, we use **192.168.200.101 - .104** (see Figure 1.3).

15. Click the **Finished** button.

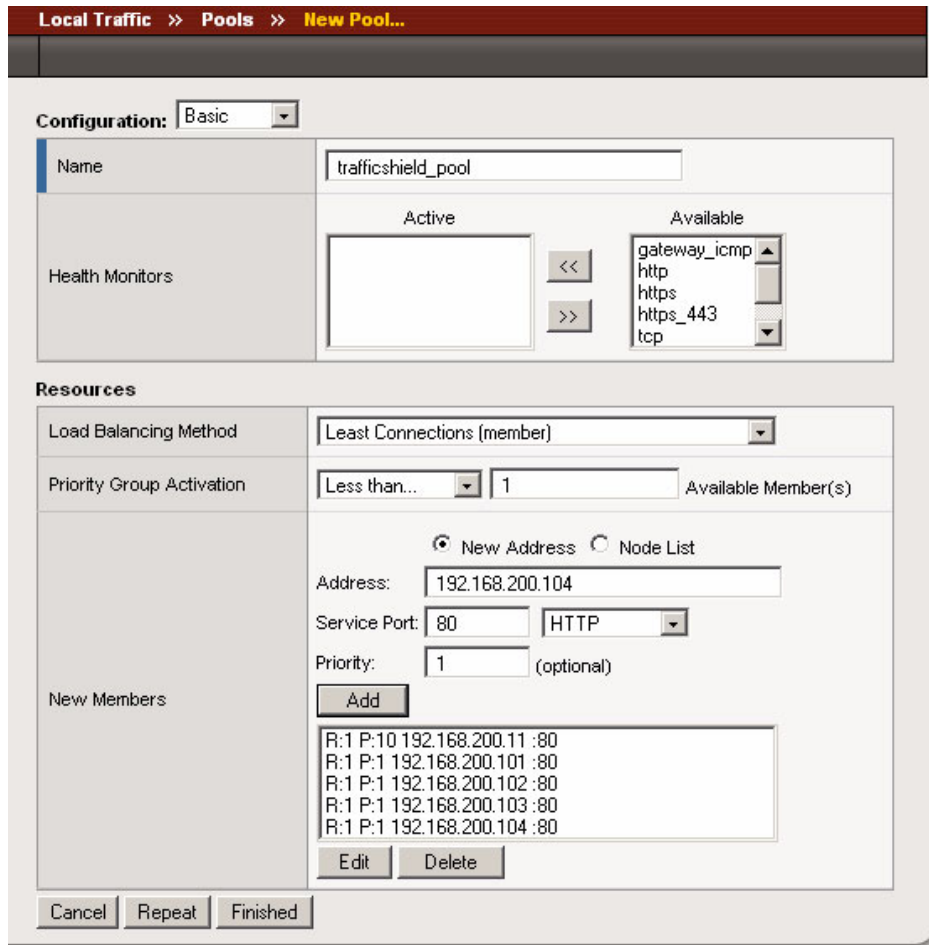


Figure 1.3 Adding a pool for the TrafficShield and servers

Creating the web server pool

The next step is to create a pool on the BIG-IP system that contains only the servers. After the TrafficShield device processes the traffic, it sends the traffic to this pool (through its associated virtual server).

To create the server pool from the Configuration utility

1. On the Main tab, expand **Local Traffic**.
2. Click **Pools**.
The Pool screen opens.
3. 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.*

4. In the **Name** box, enter a name for your pool.
In our example, we use **ts_server_pool**.
5. Leave the **Health Monitors** section empty for now, we configure a health monitor later in this guide.
6. From the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
In our example, we select **Least Connections (member)**.
7. In this pool, we leave the Priority Group Activation **Disabled**.
8. In the New Members section, make sure the **New Address** option button is selected.

*Tip: As this is the second pool you are creating, you can click the **Node List** option button, then select the web server IP Addresses from the list, so you do not have to type them again.*

9. In the **Address** box, add the first server to the pool. In our example, we type **192.168.200.101**.
10. 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 (for example **80** or **443**).
In our example, we type **80**.
11. Click the **Add** button to add the member to the list.
12. Repeat steps 9-11 for each of the web servers.
In our example, we repeat these steps three times for the remaining servers **192.168.200.102 - .104**.
13. Click the **Finished** button.

Creating virtual servers

The next step in this configuration is to define virtual servers that reference the pools you just created. BIG-IP version 9.0 and higher 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.

In this configuration, we use the default profile for HTTP. You can create a new profile based on the HTTP profile, with settings applicable to your environment, however, it is outside the scope of this Deployment Guide to show how to configure the HTTP profile. Before you start creating this virtual server, you can view the settings for the default HTTP profile to see

if it is applicable for your network (From the Local Traffic menu, click **Profiles**, then click **HTTP**). For more information on creating or modifying this profile, or applying profiles in general, see the BIG-IP documentation.

Creating the virtual server for the TrafficShield and server pool

The first virtual server we create is for the **trafficsshield_pool**, which contains both the TrafficShield device and the web servers.

To create the TrafficShield and web servers virtual server

1. On the Main tab, expand **Local Traffic**.
2. Click **Virtual Servers**.
The Virtual Server screen opens.
3. In the upper right portion of the screen, click the **Create** button.
The New Virtual Server screen opens.
4. In the **Name** box, type a name for this virtual server. In our example, we type **trafficsshield_virtual**.
5. In the **Destination** section, select the **Host** option button.
6. In the **Address** box, type the IP address of this virtual server. In our example, we use **192.168.210.100**.
7. In the **Service Port** box, type the service port, or select it from the list. In our example, we select HTTP.

General Properties	
Name	trafficsshield_virtual
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 192.168.210.100
Service Port	80 HTTP
State	Enabled

Figure 1.4 General Properties of the add virtual server page

8. In the Configuration section, leave the **Type** list at the default setting: **Load Balancing**.
*Note: For more (optional) virtual server configuration settings, from the Configuration list, select **Advanced**. Configure these settings as applicable for your network.*

- In the HTTP profile section, select **http** from the list.
Configure the rest of the Configuration section as applicable for your environment.

The screenshot shows the 'Configuration' section of a web interface. At the top, there is a 'Configuration:' dropdown menu set to 'Basic'. Below this, several configuration options are listed in a table-like format:

- Type:** Load Balancing (circled in blue)
- Protocol:** TCP
- OneConnect Profile:** None
- HTTP Profile:** http (circled in blue)
- FTP Profile:** None
- Client SSL Profile:** None
- Server SSL Profile:** None
- Authentication Profiles:** A section with 'Enabled' and 'Available' lists. The 'Available' list contains: ldap, radius, ssl_cc_ldap, ssl_ocsp, and tacacs.
- VLAN Traffic:** All VLANs

Figure 1.5 Configuration properties of the add virtual server page

- In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the TrafficShield and web server pool* section. In our example, we select **trafficshield_pool**.

The screenshot shows the 'Resources' section of a web interface. It contains the following configuration options:

- Default Pool:** trafficshield_pool (circled in blue)
- Default Persistence Profile:** None
- Fallback Persistence Profile:** None
- iRules:** A section with 'Enabled' and 'Available' lists. The 'Available' list contains: _sys_auth_ldap, _sys_auth_radius, _sys_auth_ssl_cc_ldap, _sys_auth_ssl_ocsp, and _sys_auth_tacacs.

At the bottom of the form, there are three buttons: 'Cancel', 'Repeat', and 'Finished'.

Figure 1.6 Resources section of the add virtual server page

- Click the **Finished** button.

Creating the virtual server for the web server pool

In this configuration, the TrafficShield device uses this virtual server as the destination for the traffic after it has been processed.

If your configuration requires persistence for the web servers, we recommend using the default Cookie persistence profile (Cookie persistence, Insert mode). However, if Cookie persistence is not acceptable in your network, you can create a form of simple persistence on the BIG-IP system using an expression. See the *Configuring expression-based persistence* section for this procedure.

◆ Note

Using persistence of any type is optional; only configure persistence if it is required in your environment.

To create the virtual server for the server pool

1. On the Main tab, expand **Local Traffic**.
2. Click **Virtual Servers**.
The Virtual Server screen opens.
3. In the upper right portion of the screen, click the **Create** button.
The New Virtual Server screen opens.
4. In the **Name** box, type a name for this virtual server. In our example, we type **ts_server_virtual**.
5. In the **Destination** section, select the **Host** option button.
6. In the **Address** box, type the IP address of this virtual server. In our example, we use **192.168.220.10**.
7. In the **Service Port** box, type the service port, or select it from the list. In our example, we select HTTP.
8. In the Configuration section, leave the **Type** list at the default setting: **Load Balancing**.

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

9. In the HTTP profile section, select **http** from the list.
Configure the rest of the Configuration section as applicable for your environment.
10. In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the web server pool* section. In our example, we select **ts_server_pool**.
11. **OPTIONAL:** If your deployment requires persistence, and you want to use the default **cookie** profile (cookie persistence, Insert mode), from the **Default Persistence Profile** list, select **cookie** (see Figure 1.7).

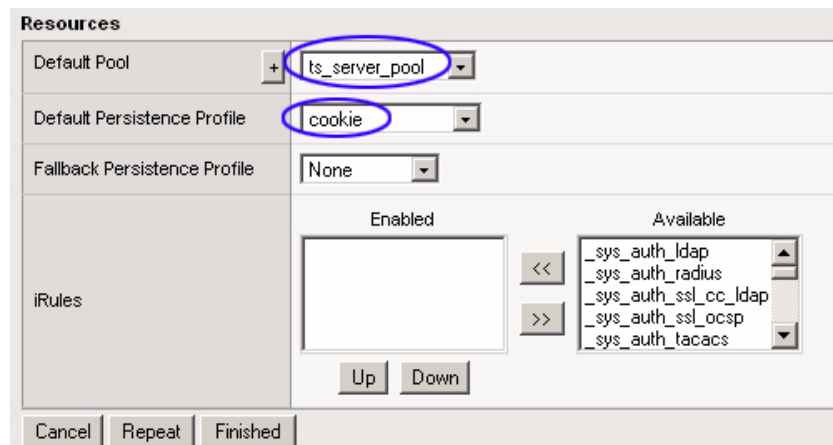


Figure 1.7 Applying the cookie profile to the virtual server (optional)

If Cookie persistence is not acceptable in your network, you can create a form of simple persistence using an expression. See the following section.

12. Click the **Finished** button.

Configuring expression-based persistence

If you cannot use Cookie persistence in your environment, you can use another form of persistence, based on an expression. The TrafficShield inserts the **X-Forwarded-For** header into the HTTP header, and sets the value of this header to the IP address of the client. By using this header for persistence, the BIG-IP system can create a form of simple persistence. The expression we use, `http_header("X-Forwarded-For")` creates a hash entry for each IP address, and persists based on that hash.

This configuration requires first creating an iRule that contains the expression, then creating a Persistence profile that calls the iRule, and finally associating the profile with the virtual server.

◆ Important

This is an optional configuration, persistence is not a requirement for this deployment. Only use this procedure if you require persistence and cannot use Cookie persistence.

To configure expression-based persistence on the virtual server

1. On the Main tab, expand **Local Traffic**.
2. Click **iRules**.
The iRules list opens.

3. In the upper right portion of the screen, click the **Create** button. The New iRule screen opens.
4. In the **Name** box, type a name for your iRule. In our example, we type **ts_persist_expression**.
5. In the Definition section, type the following:


```
when HTTP_REQUEST {
    persist uie [HTTP::header X-Forwarded-For]
}
```

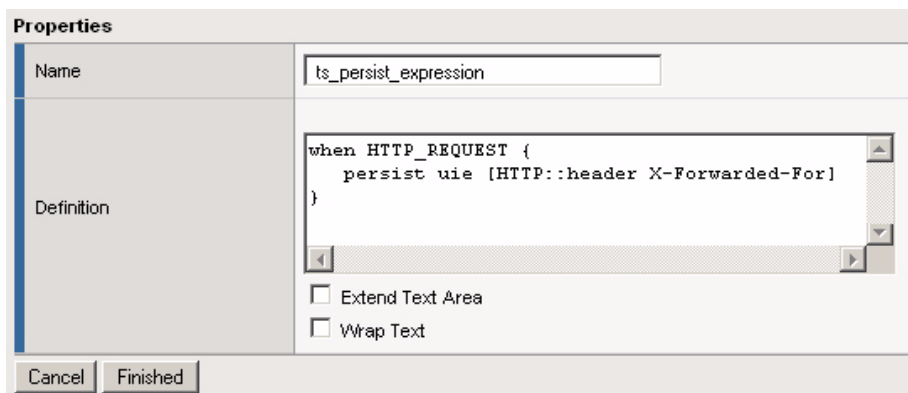


Figure 1.8 Adding the persistence expression to the iRule

6. Click the **Finished** button.

The next task is to create the Persistence Profile.
7. Under the **Local Traffic** menu, click **Profiles**. The HTTP Profiles screen opens.
8. On the Menu bar, click **Persistence**. The Persistence Profiles screen opens.
9. In the upper right portion of the screen, click the **Create** button. The New Persistence Profile screen opens.
10. In the **Name** box, type a name for this Persistence Profile. In our example, we type **ts_expression**.
11. From the Persistence Type list, choose **Universal**. The Configuration section appears.
12. From the Configuration section, in the **iRule** row, click a check in the **Custom** box. The iRule list box is now active.
13. From the **iRule** list box, select the name of the iRule you created in Step 4. In our example, we select **ts_persist_expression**.

14. If you want to set a Timeout for the persistence, click a check in the Custom box for **Timeout**. The Timeout options are now active. Leave the Timeout list box set to **Specify**, and in the **Timeout** box, enter a timeout for the persistence, in seconds. In our example, we use **600** seconds, the same timeout value as the TrafficShield default security timeout.

General Properties

Name	ts_expression
Persistence Type	Universal
Parent Profile	universal

Configuration Custom

Mirror Persistence	<input type="checkbox"/>	<input type="checkbox"/>
Match Across Services	<input type="checkbox"/>	<input type="checkbox"/>
Match Across Virtual Servers	<input type="checkbox"/>	<input type="checkbox"/>
Match Across Pools	<input type="checkbox"/>	<input type="checkbox"/>
iRule	ts_persist_expression	<input checked="" type="checkbox"/>
Timeout	Specify... 600 seconds	<input checked="" type="checkbox"/>

Cancel Repeat Finished

Figure 1.9 Configuring the Persistence Profile to use the iRule

15. Click the **Finished** button.

The next task is to associate this profile with the virtual server.

16. Under the **Local Traffic** menu, select **Virtual Servers**.
17. From the Virtual Servers list, click the name of the virtual server you created in the *Creating the virtual server for the web server pool* section. In our example, we click **ts_server_virtual**. The Virtual Server Properties screen opens.
18. On the menu bar, click **Resources**. The Virtual Server Resources screen opens.
19. From the **Default Persistence Profile** list, select the name of the profile you created in Step 10. In our example, we select **ts_expression** (see Figure 1.10).
20. Click the **Update** button. The virtual server is now configured to use the persistence profile you created, which references the expression-based iRule.



Figure 1.10 Selecting the persistence profile for the virtual server

Configuring a health monitor

For this configuration, we recommend creating a Monitor profile based on the HTTP monitor. This monitor uses **send** statements in an attempt to retrieve explicit content from nodes.

If the TrafficShield device is protecting multiple Web Applications, you need a separate monitor profile for each application instance, as the Send String will be different for each application being monitored.

To configure the ECV health monitor

1. On the Main tab, expand **Local Traffic**.
2. Click **Monitors**.
The Monitor List screen opens.
3. In the upper right portion of the screen, click the **Create** button.
The New Monitor screen opens.
4. In the **Name** box, type a name for this monitor. In our example, we type **ts_monitor_http**.
5. From the **Type** list, select **HTTP**.
The Configuration options for HTTP monitor appear.

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

6. In the **Interval** and **Timeout** boxes, 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**). We recommend a slightly higher ratio. In our example, we enter **30** in the **Interval** box and **91** in the **Timeout** box.
7. In the Send String and Receive Rule sections, you can add a Send String and Receive Rule specific to the device being checked. If you do use the Send and Receive options, be sure that your use well-formed HTTP requests.

For example, you can use the following syntax as a Send String:

```
GET /<page name> HTTP/1.0  
Host:<your host>
```

So in our example, our Monitor Screen looks like Figure 1.11.

General Properties	
Name	ts_monitor_http
Type	HTTP
Import Settings	http
Configuration: Basic	
Interval	30 seconds
Timeout	91 seconds
Send String	GET /index.html HTTP/1.0 Host: www.mycompany.com
Receive String	
User Name	
Password	
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>	

Figure 1.11 Creating the expression-based monitor

8. Click the **Finished** button.
9. From the **Local Traffic** menu, click **Pools**.
The Pool List screen opens.

10. Click the name of the pool you created in the *Creating the web server pool* section. In our example, we click **ts_server_pool**. The Pool Properties screen opens.
11. In the Health Monitors section, from the **Available** list, select the name of the health monitor you just created. In our example, we select **ts_monitor_http**, and click the Add (<<) button. The monitor now appears as **Active** (see Figure 1.12).

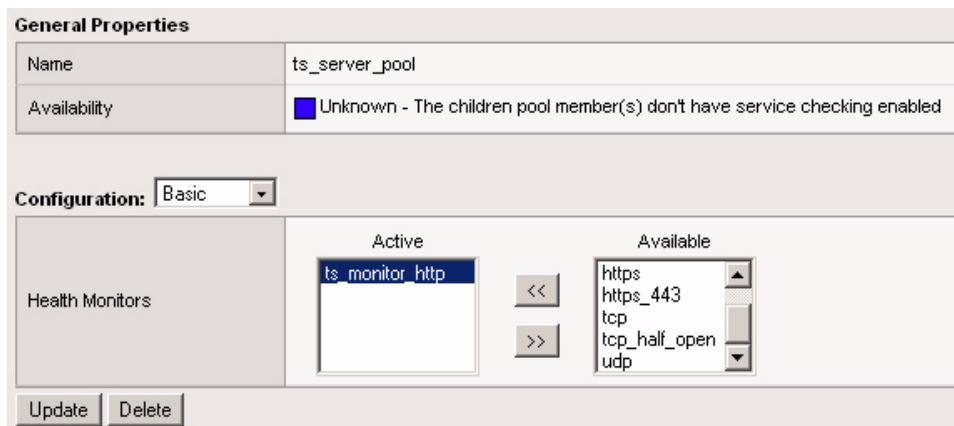


Figure 1.12 Activating the health monitor for the pool

12. Click the **Update** button.

◆ Important

If TrafficShield is protecting more than one Web Application, repeat this procedure for each Web Application, using a unique name and Send String.

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.

Configuring the TrafficShield device to reference the BIG-IP virtual server

In order for traffic to be load balanced by the BIG-IP system to the web servers, the TrafficShield device must be configured with the virtual IP address of the web servers (the virtual server you created in the *Creating the virtual server for the web server pool* section) as the TrafficShield Web Application Web Server IP address.

◆ Note

*This Deployment Guide is not intended to provide instructions on how to configure the TrafficShield device. For detailed information on how to configure TrafficShield, see the **TrafficShield Installation and Configuration Guide**, or refer to the Online Help.*

You can specify the TrafficShield Web Server IP address when you create a new Web Application within TrafficShield, or by modifying an existing Web Application.

To specify the Web Server IP address on a new Web Application from the TrafficShield device

1. From the TrafficShield user interface, click **Administration**, and then click **Web Applications**.
2. Click the **Add** button.
The Web Application Wizard opens.
3. Type a Fully Qualified Domain Name, and click the **Next** button.
4. Type a Service IP and Netmask, and click the **Next** button.
The HTTP Settings screen opens.
5. In the **Web Server IP** box, type the IP address of the virtual server you created in the *Creating the virtual server for the web server pool* section.

In our example, we type **192.168.220.10** (see Figure 1.13).
Click the **Next** button.

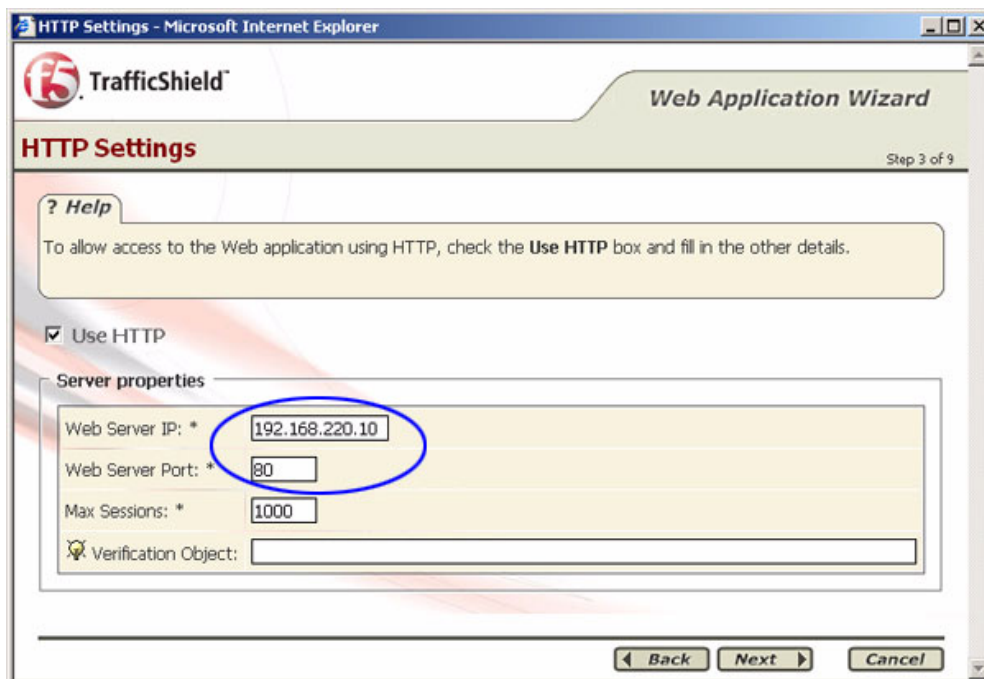


Figure 1.13 Adding the virtual server address to the TrafficShield Web Application

6. Configure the rest of the new Web Application as applicable to your deployment. For additional information on adding a new Web Application in TrafficShield, see the Online Help or the *Installation and Configuration Guide*.

To specify the Web Server IP address on an existing Web Application from the TrafficShield device

1. From the TrafficShield user interface, click **Administration**, and then click **Web Applications**.
The current list of Web Applications opens.
2. Click the option button for the Web Application that contains the relevant web servers, and click the **Edit** button.

3. In the HTTP Settings section, in the **Web Server IP** box, type the IP address of the virtual server you created in the *Creating the virtual server for the web server pool* section. In our example, we type **192.168.220.10** (see Figure 1.14).

The screenshot shows the TrafficShield Administration interface. At the top, there are navigation tabs for Monitoring, Policy Manag., and Administration. The current page is 'Administration' and the path is 'Configuration >> Web Applications'. The current user is 'admin' and the version is '3.0.11'. There are 'Update TrafficShield' and 'Cancel Changes' buttons. The interface is divided into 'Configuration' and 'Maintenance' sections. Under 'Configuration', there are sub-sections for 'Web Applications', 'System', 'Users', 'Alerts', 'Character Sets', and 'Defaults'. Under 'Maintenance', there are sub-sections for 'System', 'Upgrades', 'Backup', 'Permanent IPs', 'Licensing', and 'Downloads'. The 'Web Applications' section is active, showing 'Service Properties' and 'HTTP Settings'. In the 'Service Properties' section, the 'Fully Qualified Domain Name' is 'www.mycompany.com', 'Service IP' is '192.168.100.10', and 'Service IP Netmask' is '255.255.255.0'. In the 'HTTP Settings' section, the 'Use HTTP' checkbox is checked, 'Web Server IP' is '192.168.220.10' (circled in red), 'Web Server Port' is '80', and 'Max Sessions' is '1000'. There is also a 'Verification Object' field.

Figure 1.14 Editing the Web Server IP to be the address of the BIG-IP virtual server

4. Click the **Update TrafficShield** button.
The TrafficShield now uses the BIG-IP virtual server as the web server IP address.

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

We recommend saving your BIG-IP configuration before you begin this configuration. The System-->Archive 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).

To save the BIG-IP configuration

1. On the Main tab, expand **System**, and then click **Archive**.
The Archives List screen opens.
2. Click the **Create** button.
The New Archive screen opens.
3. In the **File Name** box, type a name for this configuration file.
In our example, we type **pre_trafficshield_config**.
4. Click the **Finished** button to save the configuration file.

To restore a BIG-IP configuration

1. On the Main tab, expand **System**, and then click **Archive**.
The Archives List screen opens.
2. From the Archives List, click the **Upload** button.
The Upload Configuration Archives screen opens.
3. In the **File Name** box, type the full path name to the location where the configuration file (*.ucs) that you want to install is located.
Alternately, you can click the Browse button to navigate to the configuration file.

*Note: Check the **Overwrite existing archive file** option if you want the system to upload and install the file that you typed in the File Name box, even if that file already exists on the system. If you do not check this option, the system sends an error message if a file of the same name already exists on the system.*

4. Click the **Upload** button to install the selected configuration file onto the system.