



DEPLOYMENT GUIDE

CONFIGURING THE BIG-IP LTM SYSTEM WITH FIREPASS CONTROLLERS FOR LOAD BALANCING AND SSL OFFLOAD

Configuring the BIG-IP LTM system for use with FirePass controllers

Welcome to the *Configuring the BIG-IP LTM System with FirePass Controllers for Load Balancing and SSL Offload Deployment Guide*. This guide contains step-by-step procedures on configuring load balancing for FirePass controllers with the BIG-IP Local Traffic Manager, as well as using the BIG-IP LTM system to offload processor-intensive SSL transactions from the FirePass controllers.

Using the BIG-IP system for load balancing allows for much greater scalability than clustering alone, reduces the load on the FirePass clustering master unit, and provides more intelligent load balancing.

Using the BIG-IP LTM system to offload SSL traffic greatly reduces the CPU load on individual FirePass controllers, allowing for better responsiveness, throughput, and scalability.

Prerequisites and configuration notes

The following are prerequisites and configuration notes about this deployment:

- The BIG-IP LTM device should be running version 9.4 or later. This configuration is also applicable to v9.0 and later.
We recommend using the latest version of the BIG-IP LTM software.
- FirePass version 5.5 or later is installed on the FirePass controller(s). We recommend using version 6.0 or later. The SSL Offload functionality is introduced in FirePass version 5.5.
- FirePass platform specific notes:
 - If you are using the FirePass 1000 or 1200 platform, you can only use the SSL Offload portion of this guide.
 - Clustering is only available on the 4000, 4100 and 4300 platforms, although with the 1000 or 1200 platforms you have the additional option of load balancing a group of FirePass controllers.
 - If you are using the 4100 or 4300 platform, you should have administrative services configured on the management port.

- If you are using the 4000, 4300, 1200, or 1000 platforms, you should dedicate one port for administrative services. If this is not possible, create a VLAN interface for your management services to run on, and connect that VLAN to your management network. For information on how to configure VLANs and ports, see the FirePass documentation.
- **Important:** Desktop Access should be configured on an SSL web service on the FirePass controller. You cannot offload SSL for Desktop access.
- This document assumes that the FirePass controller(s) and the BIG-IP system are already installed in the network. For specific instructions on how to install the FirePass controllers, see the *FirePass Controller Getting Started Guide*. For the BIG-IP system, see the **Installation, Licensing, and Upgrades for BIG-IP Systems** guide.
- You must be familiar with both the FirePass and BIG-IP devices. Intermediate knowledge of the BIG-IP device, including the new iRule syntax (starting in version 9.0) is recommended.
- The default gateway of the FirePass controller must be a Self IP address of the BIG-IP LTM device on the VLAN that the FirePass controllers are attached to.
- Make sure the FirePass controller(s) are configured in the IP subnet that is behind the BIG-IP LTM system.

Deciding whether or not to cluster the FirePass devices

The FirePass controller supports clustering units together in order to provide a high degree of scalability and consistent user interface to a large number of remote access users. When using a BIG-IP LTM system in front of multiple FirePass controllers, you can also use the BIG-IP LTM device to load balance traffic to the FirePass controllers in both a clustered and non-clustered environment. When deciding to use clustering or load balancing, keep the following in mind:

◆ Load Balancing

If you are using an external authentication method, with external groups configured on the FirePass controller, and no user-defined favorites, we recommend configuring the BIG-IP LTM device to load balance and terminate SSL connections for the FirePass controllers. In this case, all the FirePass devices would have the same configuration, which can be easily replicated across each FirePass controller (see *Appendix A: Copying a FirePass configuration to multiple devices*, on page 22).

This Deployment Guide describes how to configure the BIG-IP LTM system for load balancing the FirePass devices as well as terminating SSL traffic at the BIG-IP LTM device.

◆ Clustering

If you have more than one FirePass controller, and your FirePass deployment includes the ability for end users to create their own Favorites, or you have local groups configured on the FirePass devices

we recommend you configure the FirePass controllers in a cluster. The BIG-IP device can still be used to load balance the cluster and offload SSL traffic.

◆ **Note**

There is a limit of ten FirePass devices to a cluster, if you are using more than ten FirePass devices, we recommend reconfiguring your environment to make use of external groups and pre-define all favorites for your users. With this revised configuration, there is not a limit of how many FirePass controllers can be deployed behind a BIG-IP system.

If you are using a BIG-IP LTM system with a FirePass cluster, make sure that Load Balancing is disabled on the FirePass cluster master. Configuring clustering on the FirePass controllers is outside the scope of this document, and is documented in the Online Help and FirePass documentation.

◆ **Tip**

The FirePass controllers (except the FirePass 600) and BIG-IP devices can also be deployed in a redundant (fail-over) configuration, which provides an extra layer of availability. For information configuring a fail-over unit for either of these products, refer to the documentation.

Configuration example

In this configuration, a remote client logs onto the FirePass controller and requests a secure application on the internal corporate network. The request travels through the Internet and firewall to the virtual server assigned to the FirePass controller pool on the BIG-IP LTM system. The BIG-IP LTM system receives the request, negotiates the SSL transaction, and adds SSL connection information to the request header before sending it on to a FirePass controller. The FirePass controller performs the required authentication, and allows access to the requested application.

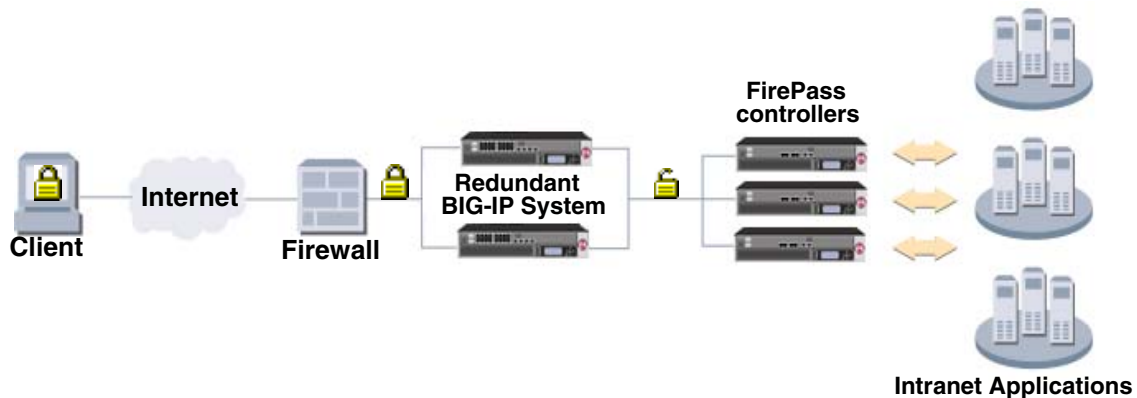


Figure 1 Example BIG-IP/FirePass deployment scenario

Configuring the FirePass controller

The first task is to configure the FirePass controller(s). If you are going to load balance the FirePass controllers, are using an external authentication method, with external groups configured on the FirePass controller, and no user-defined favorites, you can copy the configuration across the FirePass devices after performing the procedures below. See *Appendix A: Copying a FirePass configuration to multiple devices* for configuration information.

◆ **Note**

*If you were using an SSL certificate on the FirePass controller before configuring the SSL offload to the BIG-IP LTM device, make sure that the SSL Certificate for the FirePass controller is now in the Client SSL Profile on the BIG-IP device. See the **Creating a Client SSL profile**, on page 16 for information on the Client SSL profile.*

When you offload SSL processing, you configure the FirePass controller to allow "insecure" access so that you can establish an HTTP network connection between the controller and the BIG-IP device. The client access is not actually insecure, as the BIG-IP LTM device is terminating the SSL traffic.

There are four procedures to configure on the FirePass controller(s) for load balancing and SSL offload on the BIG-IP LTM system:

- *Modifying the clustering configuration*
- *Allowing insecure access*
- *Configuring the FirePass controller web services for SSL offload*
- *Finalizing the FirePass controller configuration*

For information on how to configure clustering on the FirePass controllers, see the Online Help or the FirePass documentation.

Modifying the clustering configuration

If you are using FirePass controllers in a clustered configuration, there are two additional configuration procedures you need to complete:

- *Disabling load balancing on a FirePass cluster*
- *Modifying the clustering synchronization time interval*

◆ **Note**

This section only applies to FirePass controllers in a clustered configuration. If you are not using clustering on the FirePass controllers, continue to the next section.

Disabling load balancing on a FirePass cluster

The first task is to disable load balancing on the FirePass controller. In this configuration, the load balancing duties are handled by the BIG-IP system.

To disable load balancing on the FirePass controller

1. From the lower navigation pane, click **Clustering**.
The Clustering Settings screen opens.
2. From the Load Balancing list, select **Off**.
Load balancing is now disabled on the FirePass controller.

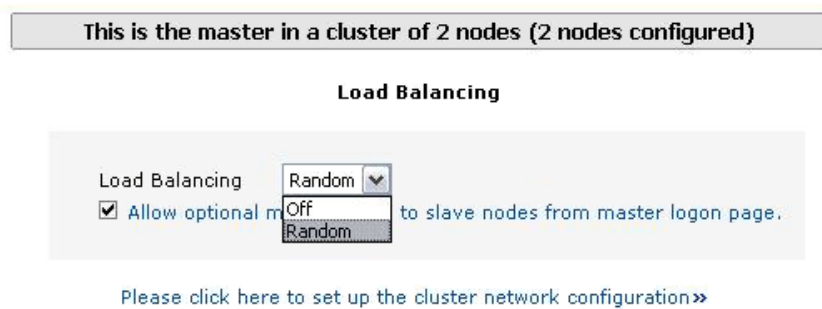


Figure 2 Turning off load balancing on the FirePass controller cluster

Modifying the clustering synchronization time interval

If you have a large number of FirePass controllers with clustering enabled, you can greatly reduce the clustering traffic by modifying the **Cluster Synchronization Time Interval**. This is especially useful if using external user groups and external authentication, but you want to periodically synchronize global and group settings from the cluster master node to any slave nodes (instead of manually copying a configuration from one FirePass controller to the others).

To modify the clustering synchronization time interval on the FirePass controller

1. From the lower navigation pane, click **Device Management**. From the Device Management options in the upper section, expand **Configuration**, and then click **Clustering and Failover**.
The Clustering and Failover configuration screen opens.
2. Scroll down to the **Cluster Synchronization Time Interval** section.
3. In the **Synchronization Interval** box, type the number of seconds you want to configure between synchronization. We recommend a value of **300** (five minutes), which greatly reduces the amount of clustering traffic.
4. Click the **Apply Clustering/Failover Settings** button.

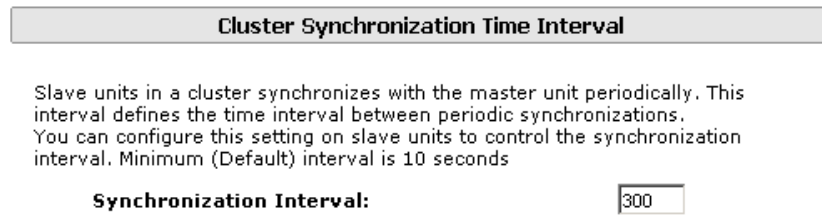


Figure 3 Configuring the synchronization time interval

Allowing insecure access

Because the BIG-IP LTM system is offloading the SSL traffic, the FirePass controller must be configured to allow insecure access in order to support HTTP interactions with the BIG-IP LTM device. **Remember that this is not actually allowing insecure access**, as the SSL traffic is terminated at the BIG-IP system.

◆ WARNING

Make sure that all connections to the FirePass devices are going through the BIG-IP LTM system. If you allow insecure access as described in the following procedure and there are connections that are not going through the BIG-IP LTM device, you are truly allowing insecure access to the FirePass controller, which should not be allowed.

To allow insecure access

1. Log into the FirePass device as an administrator.
2. From the lower navigation pane, click **Device Management**. From the Device Management options in the upper section, expand **Security**, and click **User Access Security**.
3. In the User Access Security section at the top of the page, click the **Allow insecure access** option button.

-
- Restart the service by clicking the **Requires services restart** link next to User Access Security at the top of the page.



Figure 4 Allowing insecure access so the BIG-IP LTM can offload the SSL traffic

When you see the Restart Screen, the service has been restarted. You do not need to click any of the links to restart the service again.

Configuring the FirePass controller web services for SSL offload

Use the following procedure to configure each web service for SSL offload using the BIG-IP system. The following procedure shows you how to modify an existing web service for SSL offload.

If you are creating a new web service on the FirePass controller, make sure you follow steps 4, 5 and 6 in the following procedure when configuring the web service.

To modify an existing web service on the FirePass controller

- From the lower navigation pane, click **Device Management**. From the Device Management options in the upper section, expand **Configuration**, and then click **Network Configuration**. The IP Config tab of the Network Configuration screen opens.
- Click the **Web Services** tab. The Web Server Configuration screen opens.
- Find the Host/Port combination you want to modify from the Web Server Configuration table, and click **Configure**.
- Click to clear the **Use SSL** box, if it is checked.
- Clear the contents of the **HTTPS URL to Redirect to** box, if applicable.
- Click the **Do not redirect to HTTPS** box.
- Click the **Offload SSL processing to a BIG-IP Local Traffic Manager** box to enable SSL offload to the BIG-IP device.

8. Click the **Update** button.

Interfaces VLAN IP Config Routing DNS Hosts **Web Services** Desktop Misc Finalize

Note: after updating the individual sections, you **must** go to the **Finalize Section** and finalize the new configuration.

Web Service Configuration for firepass.company.xyz:443

Define a hostname to be used by the browser and associate it with the corresponding IP address and port for this service. Leave hostname empty to use the IP address.

Hostname:

IP Address:

Port:

Please check this box if this is a secure service running HTTPS protocol.

Use SSL :

Normally a remote user should **never** be allowed access over HTTP. An HTTP service is generally defined only to support redirects to HTTPS.

HTTPS URL to redirect to:

Do not redirect to HTTPS:

Please specify the Agents bound to this service. Please [read help](#) for more information.

User Login

Admin Login :

Desktop:

WebAccess Bypass:

Offload SSL processing to a BIG-IP Local Traffic Manager

Figure 5 Modifying the web service for SSL offload

◆ **Note**

The host names for the web services should match the DNS entry for the virtual server on the BIG-IP LTM system. The same goes for the fully qualified domain name (FQDN) on the FirePass controllers.

The next step is to finalize the FirePass configuration.

Finalizing the FirePass controller configuration

The final step for the FirePass controller configuration is to finalize the configuration changes you have made.

◆ Important

*You **must** finalize the configuration using the following procedure. If you do not finalize the configuration, the changes will not be applied.*

To finalize the configuration changes

1. On the menu bar, click the **Finalize** tab. Note that the Finalize tab does not display unless you have made configuration changes. The configuration page displays, showing the changes to the configuration that you have made. Review the changes.
2. Click the **Finalize changes** button.
3. You will see a Non-SSL server defined warning (see Figure 6). Ignore this warning, as the BIG-IP device will be handling the SSL transactions.
4. Click **Apply Changes**.
5. Click **Apply Changes and Restart**.

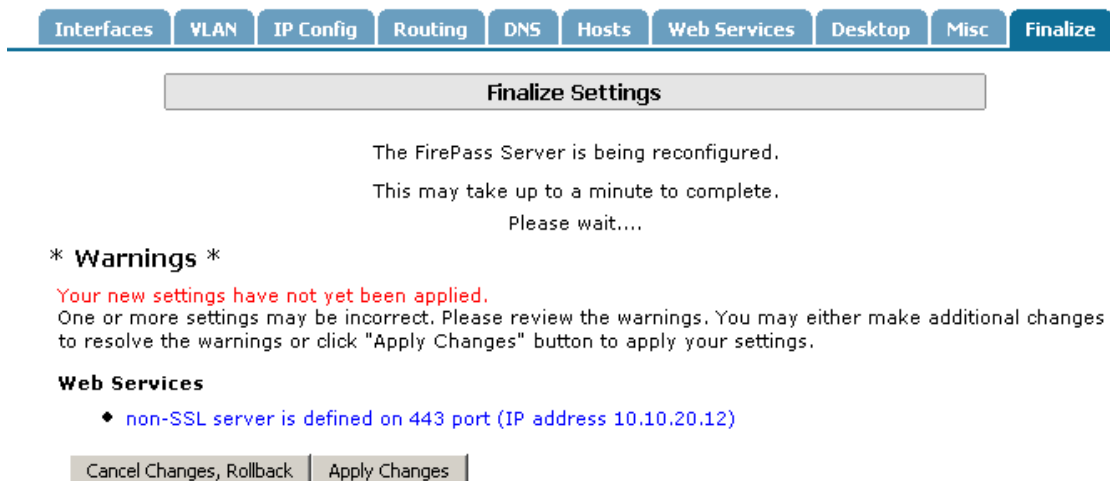


Figure 6 Non-SSL server warning.

After the controller has restarted, the FirePass configuration is complete.

If you are using the BIG-IP LTM system to load balance the FirePass controllers as described at the beginning of this document, and all the FirePass devices will have the same configuration, see *Appendix A: Copying a FirePass configuration to multiple devices*, on page 22 to save the configuration, and then copy the configuration to the other FirePass devices.

Configuring the BIG-IP LTM system

With the configuration of the FirePass controllers now complete, we now configure the BIG-IP LTM system.

Use the following procedures to configure the BIG-IP LTM to load balance and offload SSL from the FirePass controllers:

- *Connecting to the BIG-IP LTM system*
- *Using SSL certificates and keys*
- *Creating a health monitor*
- *Creating a pool*
- *Creating profiles*
- *Creating the Redirect iRule*
- *Creating the virtual server*
- *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 B: Backing up and restoring the BIG-IP system configuration**, on page 24.*

The BIG-IP LTM 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 LTM system using the BIG-IP web-based Configuration utility only.

◆ Note

If the BIG-IP LTM device you are using in front of the FirePass controller(s) is not a dedicated device (you are using it in front of additional devices, you can create VLANs on the BIG-IP LTM device to separate FirePass controller traffic from your other application traffic. Configuring VLANs on the BIG-IP LTM and FirePass devices is outside the scope of this document. See the appropriate product's documentation for information on how to configure VLANs.

Connecting to the BIG-IP LTM system

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 authentication 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 configure and access information on monitoring the BIG-IP system.

Using SSL certificates and keys

Before you can enable the BIG-IP LTM system to offload connections from your FirePass devices, you must install a SSL certificate on the virtual server that you wish to use for FirePass connections on the BIG-IP LTM device. For this Deployment Guide, we assume that you already have obtained an SSL certificate, but it is not yet installed on the BIG-IP LTM system. For information on generating certificates, or using the BIG-IP 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 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** list, select the type of import (**Key** or **Certificate**).
5. Select the import method (text or file).
6. Type the name of the key or certificate.
7. Click **Import**.

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

Creating a pool

The next step is to create a pool for the FirePass nodes on the BIG-IP device.

To create a pool

1. On the Main tab, expand **Local Traffic**, and then click **Pools**. The Pool screen opens.
2. Click the **Create** button. The New Pool screen opens.
3. In the **Name** box, type a name. In our example, we type **FP_pool**.
4. In the Health Monitor section, from the Available list, select **tcp**, and click the Add (<<) button to move it to the Active box. In the following procedure, we create an ICMP monitor for the nodes.
5. From the **Load Balancing** list, select a load balancing method appropriate for your configuration. For information on the different load balancing methods, see the Online Help or the BIG-IP manual.
6. In the New Members section, in the Address box, enter the address of one of the Web Services on the FirePass device.
7. In the Service Port box, type **443**, or select **HTTPS** from the list. The port must be 443, so you cannot do port translation on the BIG-IP.
8. Click the **Add** button.
9. Repeat steps 5-7 for each FirePass node.
10. Click the **Finished** button.

The screenshot shows the 'New Pool' configuration screen in the BIG-IP management console. The configuration is set to 'Basic'. The pool name is 'FP_pool'. Under 'Health Monitors', 'tcp' is moved from the 'Available' list to the 'Active' list. The 'Resources' section is configured with 'Round Robin' as the load balancing method and 'Disabled' for priority group activation. In the 'New Members' section, the 'New Address' radio button is selected. The address is '10.10.10.3', the service port is '443', and the protocol is 'HTTPS'. The 'Add' button has been clicked, resulting in three members being listed: 'R:1 P:1 10.10.10.1 :443', 'R:1 P:1 10.10.10.2 :443', and 'R:1 P:1 10.10.10.3 :443'. The 'Finished' button is highlighted.

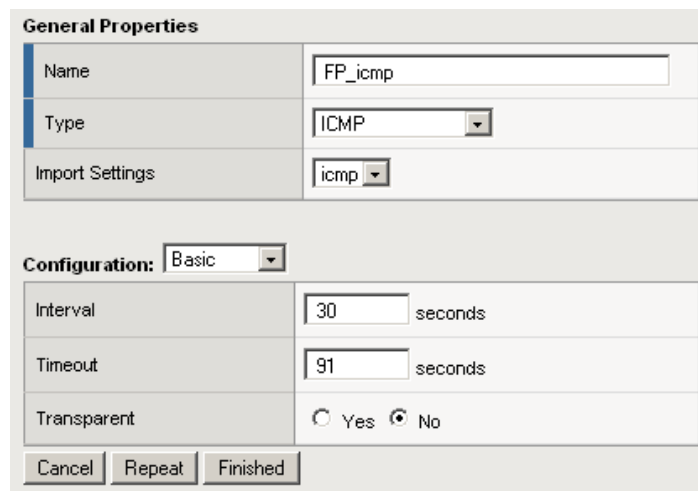
Figure 7 Creating the pool for the FirePass controllers

Creating a health monitor

The next step is to set up a health monitor for the FirePass nodes. For this configuration, we configure a simple ICMP monitor. You can create a more sophisticated health monitor if needed for your deployment. When configuring the virtual server, we also configure a fallback persistence method. For information on the different health monitors and how to configure them, see the Online Help or BIG-IP system documentation.

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 **FP_icmp**.
4. From the **Type** list, select **ICMP**. The ICMP Monitor configuration options appear.
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 (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**.



General Properties	
Name	FP_icmp
Type	ICMP
Import Settings	icmp

Configuration: Basic

Interval	30 seconds
Timeout	91 seconds
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No

Cancel Repeat Finished

Figure 8 Creating the ICMP Monitor

6. Click the **Finished** button. The new monitor is added to the Monitor list. Now we associate this monitor with each FirePass node.
7. On the Main tab, expand **Local Traffic**, and then click **Nodes**. The Node screen opens.

8. From the Node list, click the first of the FirePass nodes.
The Node properties screen opens.
9. In the Configuration section, from the Health Monitors list, select **Node Specific**.
The Select Monitors section displays.
10. From the Available list, select the name of the monitor you created in step 3. In our example, we select **FP_icmp**.
11. Click the **Update** button.
12. Repeat steps 7-11 for each FirePass node.

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.

Creating an HTTP profile

We first create a new HTTP profile, based of the default HTTP profile.

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 **FP_http**.
5. From the **Parent Profile** list, ensure that **http** is selected.
6. In the Settings section, locate the **Header Erase** row, and click the Custom box on the far right.
In the **Header Erase** box, type the following:

```
BIGIP_HTTPS BIGIP_SSL_PROTOCOL BIGIP_SSL_CIPHER BIGIP_SSL_CIPHER_USEKEYSIZE
```

7. Click the Custom box in the **OneConnect Transformations** row. In the Enable box, click to clear the box, which disables OneConnect Transformations (see Figure 9).
8. Leave the rest of the options at their default settings and then click the **Finished** button.

General Properties	
Name	FP_http
Parent Profile	http
Settings Custom	
Basic Auth Realm	<input type="checkbox"/>
Fallback Host	<input type="checkbox"/>
Header Insert	<input type="checkbox"/>
Header Erase	BIGIP_HTTPS BIGIP_SSL_PROTOCOL BIGIP_SSL_ <input checked="" type="checkbox"/>
Response Chunking	Preserve <input type="checkbox"/>
OneConnect Transformations	<input type="checkbox"/> Enabled <input checked="" type="checkbox"/>
Redirect Rewrite	None <input type="checkbox"/>
Maximum Header Size	32768 bytes <input type="checkbox"/>
Pipelining	Enabled <input type="checkbox"/>
Insert XForwarded For	Disabled <input type="checkbox"/>

Figure 9 Creating the HTTP profile

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

Creating a persistence profile

The next profile we create is a persistence profile. Using persistence is required when you are using the BIG-IP LTM device to load balance more than one FirePass controller, however the method of persistence depends on your site requirements. In this example, we show how to create a cookie persistence profile.

To create a new cookie persistence 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, click **Persistence**.
The Persistence Profiles screen opens.

4. In the upper right portion of the screen, click the **Create** button. The New Persistence Profile screen opens.
5. In the **Name** box, type a name for this profile. In our example, we type **FP_cookie**.
6. From the **Persistence Type** list, select **Cookie**. The configuration options for cookie persistence appear.
7. Modify any of the settings as applicable for your network. In our example, we leave the options at the default levels.
8. Click the **Finished** button.

General Properties	
Name	FP_cookie
Persistence Type	Cookie
Parent Profile	cookie

Configuration		Custom
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"/>
Cookie Method	HTTP Cookie Insert	<input type="checkbox"/>
Cookie Name		<input type="checkbox"/>
Expiration	<input checked="" type="checkbox"/> Session Cookie	<input type="checkbox"/>

Cancel Repeat Finished

Figure 10 Creating the Persistence Profile

Creating a Client SSL profile

The next profile we create is a Client 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 **FP_ssl**.
 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 next step in this configuration is to create an iRule on the BIG-IP LTM device that inserts information about the SSL connection into the request header, which is required for proper FirePass functionality.

◆ Important

This iRule is specific to BIG-IP LTM version 9.4 and later. If you are using an earlier version of the BIG-IP LTM system, see http://www.f5.com/solutions/deployment/ssl_offload_dg.html.

To create the Redirect iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**. The iRules screen opens.
2. In the upper right portion of the screen, click the **Create** button. The iRule screen opens.
3. In the Name box, type a name for this iRule. In our example, we type **FP_ssloffload**.
4. In the Definition section, type (or copy and paste) the following iRule:

```

when RULE_INIT {
  set ssl_handshake 0
}
when CLIENTSSL_HANDSHAKE {
  set ssl_handshake 1
}
when CLIENTSSL_CLIENTCERT {
  set ssl_handshake 1
}
when HTTP_REQUEST {
  set http_disable 0
  if { $ssl_handshake == 1 } {
    HTTP::header replace "BIGIP" "on"
    HTTP::header replace "BIGIP_SSL_CIPHER" "[SSL::cipher name]"
    HTTP::header replace "BIGIP_SSL_CIPHER_USEKEYSIZE" "[SSL::cipher bits]"
    HTTP::header replace "BIGIP_SSL_PROTOCOL" "[SSL::cipher version]"
    set ssl_handshake 0
  }
  if { [HTTP::uri] starts_with "/myvpn" } {
    set http_disable 1
  }
  if { [HTTP::uri] starts_with "/tunnel" } {
    set http_disable 1
  }
}
when HTTP_REQUEST_SEND {
  if { $http_disable != 0 } {
    HTTP::disable
  }
}

```

Figure 1.11 iRule for SSL offload

5. Click the **Finished** button.

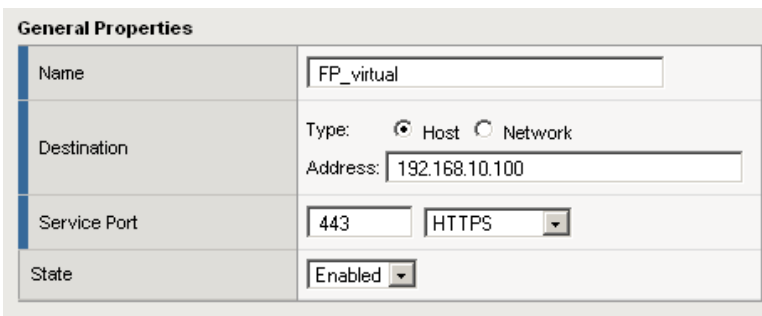
This new iRule appears in the list.

Creating the virtual server

The next step in this configuration is to create a virtual server on the BIG-IP LTM device. The virtual server uses the profile and the pool you created.

To define the virtual server using the Configuration utility

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**.
The Virtual Server 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 **FP_virtual**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address of this virtual server. This should be on the external VLAN of the BIG-IP device.
6. In the **Service Port** box, type **443** or select **HTTPS** from the list.



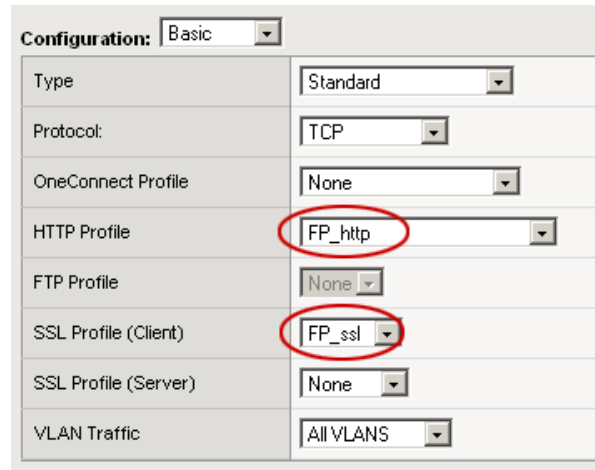
The screenshot shows the 'General Properties' configuration form for a virtual server. The form is divided into four sections: Name, Destination, Service Port, and State. The Name field contains 'FP_virtual'. The Destination section has 'Host' selected as the Type and '192.168.10.100' in the Address field. The Service Port section has '443' in the port field and 'HTTPS' selected in the dropdown menu. The State section has 'Enabled' selected in the dropdown menu.

General Properties	
Name	FP_virtual
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 192.168.10.100
Service Port	443 HTTPS
State	Enabled

Figure 1.1 Adding the FirePass virtual server

7. Leave the **Type** list at the default setting: **Standard**.
8. 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 **FP_http**.

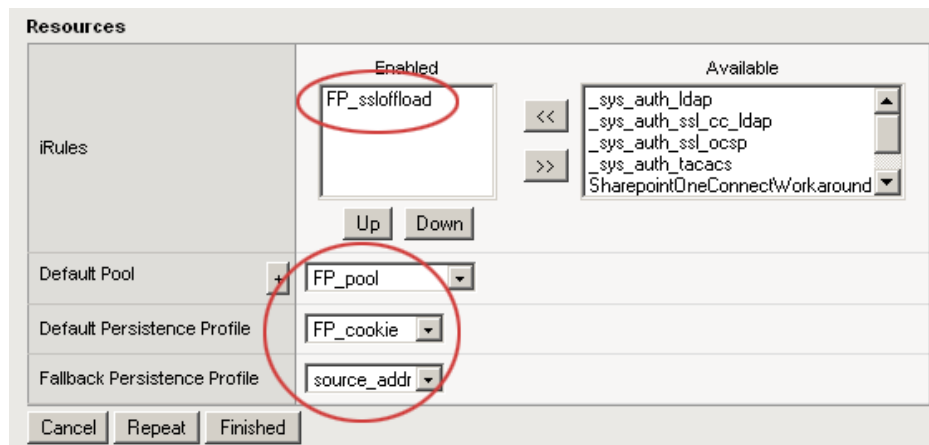
- From the **SSL Profile (Client)** list, select the name of the profile you created in the *Creating a Client SSL profile* section. In our example, we type **FP_ssl**.



Configuration: Basic	
Type	Standard
Protocol	TCP
OneConnect Profile	None
HTTP Profile	FP_http
FTP Profile	None
SSL Profile (Client)	FP_ssl
SSL Profile (Server)	None
VLAN Traffic	All VLANs

Figure 1.2 Selecting the HTTP and SSL profiles for the virtual server

- In the Resources section, select the iRule you created in the *Creating the Redirect iRule* section. In our example, we select **FPssl_offload**.
- In the Default Pool section, select the name of the pool you created in the *Creating a pool* section. In our example we select **FP_pool**.
- From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating a persistence profile* section. In our example, we select **FP_cookie**
- From the **Fallback Persistence Profile** list, select **source_addr**. This allows the BIG-IP system to use the source address as a fallback persistence method.



Resources	
iRules	Enabled FP_ssl_offload
	Available _sys_auth_ldap _sys_auth_ssl_cc_ldap _sys_auth_ssl_ocsp _sys_auth_tacacs SharepointOneConnectWorkaround
Default Pool	FP_pool
Default Persistence Profile	FP_cookie
Fallback Persistence Profile	source_addr
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>	

Figure 1.3 Resources section of the add virtual server page

-
14. 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.

Appendix A: Copying a FirePass configuration to multiple devices

When you want to use the same configuration across multiple FirePass devices (ideal for load balancing using the BIG-IP system), you can use the backup/restore functionality on the FirePass device to copy a single configuration to multiple devices.

Important

*When copying/distributing FirePass configurations, only global settings, user accounts, groups, webifyer settings, and favorites configuration are included in the configuration file. For these procedures, you **should not** restore the network configuration (or certificates if not using the BIG-IP device for offloading SSL). The network configuration must be configured on each device, and each FirePass controller must be appropriately licensed.*

Backing up the FirePass controller

The first step is to create a backup of your current configuration, which creates a configuration file you can copy to the other controllers. This creates backups that include the FirePass global settings, user accounts, groups, webifyer settings, and favorites.

To back up the FirePass controller

1. From the lower left navigation pane, click **Device Management**.
2. From the upper navigation pane, expand **Maintenance** and then click **Backup/Restore**.
3. Click **Create backup of your current configuration**.
The File Download dialog box opens. Click the Save button, and when the Save As dialog box opens, save the file to an easy-to-remember location on the network.

After you have backed up your configuration, you can use that file to upload to other FirePass devices. Remember that you must configure the network settings on each FirePass controller.

To upload the configuration to another FirePass device

1. Log on to the other FirePass controller as an administrator.
2. If the network settings have not been configured, configure them as applicable for your deployment.
3. From the lower left navigation pane, click **Device Management**.
4. From the upper navigation pane, expand **Maintenance** and then click **Backup/Restore**.

-
5. Under *Restore FirePass controller configuration from a previous backup*, click the **Browse** button to search for the backup file you created in the preceding procedure.

A FirePass backup file name appears similar to the following:
backup-bip044371s-URM-5.5-20050914174102.zip.

6. Click **Restore your saved configuration**.
7. Choose to restore **Networking Configuration, Users and Groups Settings**, or both from the review-settings page.
8. Click **Restore** to start the restore process.

Repeat this procedure for each FirePass device.

Appendix B: 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 up 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_firepass_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.
 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.