



DEPLOYMENT GUIDE

DEPLOYING THE FIREPASS CONTROLLER WITH THE BIG-IP GTM SYSTEM

Deploying the FirePass controller with the BIG-IP Global Traffic Manager

Welcome to the BIG-IP Global Traffic Manager (GTM) and FirePass controller Deployment Guide. This guide gives you step by step configuration procedures on how to globally monitor and direct traffic to FirePass controllers at globally distributed sites or data centers.

For more information on the FirePass controller or BIG-IP GTM system, see <http://www.f5.com/products/>.

Prerequisites and configuration notes

The following are prerequisites for this deployment:

- ◆ The FirePass controller should be running version 6.0.1 or later.
- ◆ The BIG-IP GTM system must be running at least version 9.2.2. We strongly recommend using 9.4.3 or later.
- ◆ You should have familiarity with both the FirePass controller and BIG-IP GTM. We recommend you read this entire Deployment guide before you start the configuration. This is important because you need know what the names and addresses of configuration objects on the BIG-IP GTM will be while first configuring the FirePass controller (for example, you need to know the name of the Wide IP you will create on the BIG-IP GTM while configuring the FirePass controller).
- ◆ We assume both the FirePass controller and BIG-IP GTM have been installed, initially configured, and are on the network with the ability to reach each other.
- ◆ For this deployment, FirePass controller clustering must not be used for either load balancing or configuration synchronization. The FirePass controllers should be configured as standalone devices or in redundant pairs. We do not use clustering because the prelogon sequence is copied across all FirePass devices in the cluster, and redirects contained in the prelogon sequence will send all traffic to the cluster master, and consequently cluster nodes will be under utilized.

If your configuration requires clustering, we recommend you use a BIG-IP LTM device in conjunction with the FirePass and BIG-IP GTM devices. BIG-IP LTM will present the entire Firepass cluster as a single entity via a virtual server. The redirection required with the solution presented in this guide via prelogon inspection is compatible with a single virtual server.

- ◆ This configuration requires one additional address and host name per FirePass controller for use with the BIG-IP GTM.

- ◆ You must have an SSL server certificate that corresponds to the Wide IP host name that you will create on the GTM created and installed on each FirePass controller. For information on creating and installing certificates on the FirePass controller, see the *FirePass Controller Administrator Guide*, Chapter 4, **Using Server Certificates**.
- ◆ You need to provision a publicly accessible name for the Wide IP on the BIG-IP GTM.
- ◆ If you are running FirePass version 6.0.2, you must have HF-76259-3-1 installed for the prelogon sequence to run. For FirePass versions 6.0.1 and earlier, this hotfix is not required. For more information on Hot Fixes, see Ask F5.

Configuration scenario

In our example, the network is composed of two sites (Site A and Site B) each with its own FirePass controller. A BIG-IP GTM has been deployed at site B. Clients are able to connect to either FirePass and access network and application services.

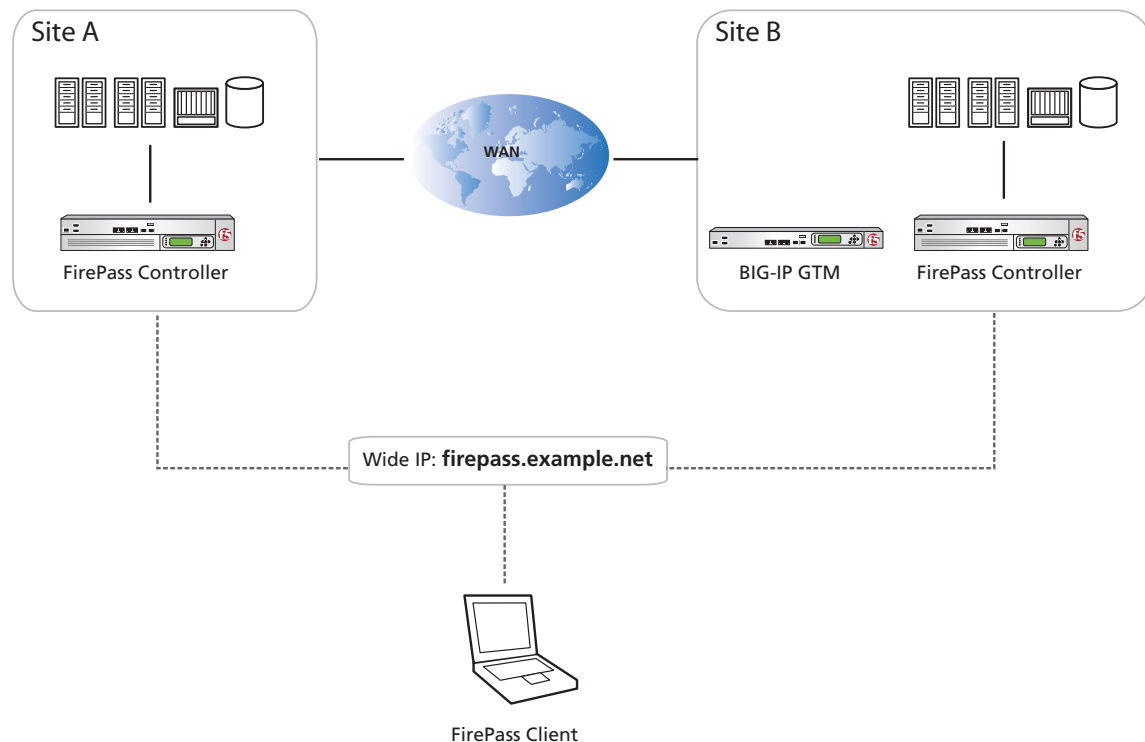


Figure 1 Simple configuration example

The Figure 2 on the following page shows the traffic flow.

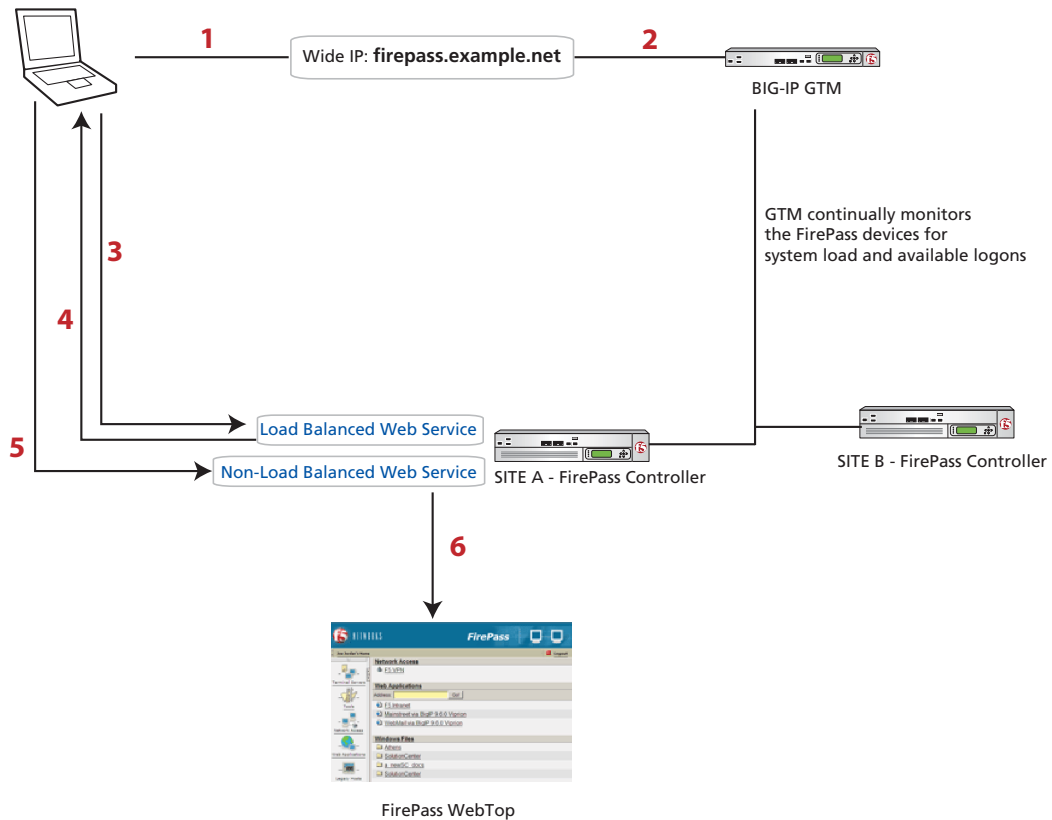


Figure 2 Deployment scenario traffic flow

1. The user enters the wide IP name in a web browser.
2. Based on information from the health monitor on the BIG-IP GTM, the GTM selects a FirePass controller for the user to access.
3. The user's browser connects to a load balanced service on the selected FirePass controller, and a pre-logon sequence runs.
4. The pre-logon sequence directs the users browser to a local logon service.
5. The user's browser connects to the local logon service and the user logs in.
6. The user is granted access to resources gated by the FirePass controller.

Configuring the FirePass controller

In this deployment, we first configure the FirePass controllers. In order to complete this configuration, you must know the address and host name that you will use when configuring the BIG-IP GTM wide IP. In the context of FirePass controllers, a BIG-IP GTM *wide IP* is a collection of one or more domain names that maps to one or more groups of web services configured on FirePass controllers. The Global Traffic Manager load balances name resolution requests across the services that are defined in the wide IP that is associated with the requested domain name.

Configuring the FirePass to allow GTM monitoring

The first procedure in this configuration is to configure the FirePass controllers to allow the BIG-IP GTM system to monitor them.

To configure the FirePass to allow GTM monitoring

1. From the navigation pane, click **Device Management**, expand **Monitoring**, and then click **Load Status Access Security**.
2. Make sure that **Do not use password for Load Status query** is *not* checked. If there is a check in the box, click to uncheck it.
3. In the **New Password** box, type a new password. Retype the password in the **Confirm New Password** box. This password is separate from any other FirePass authentication, and is only used for basic authentication (HTTP) for accessing the Load Status page.
4. Click the **Update** button.
5. *Optional:* You can limit Load Status page access to a specific set of IP addresses. Type IP addresses/masks separated by commas in the **Load Status Access Security** box, and then click the **Apply** button. In our example, we leave this at the default setting.

Important: If you do configure Load Status Access Security, make sure you type the IP address/mask of all big3d agents that could possibly monitor the Firepass devices.

The screenshot shows two configuration sections. The first section, titled "Load Status Page Name and Password", contains a checkbox labeled "Do not use password for Load Status query" which is unchecked. Below it are three input fields: "Logon Name" with the value "gtmuser", "New Password" with "*****", and "Confirm New Password" with "*****". An "Update" button is located to the right of the confirm password field. The second section, titled "Load Status Access Security", contains the text "Limit Load Status page access to the following set of IP address/mask (comma separated list; leave empty to deny all):". Below this is an input field containing the value "all" and an "Apply" button to its right.

Figure 3 Configuring the FirePass to allow BIG-IP GTM monitoring

◆ **Note**

The IP address mask will initially have a default value of **all**. Once an IP address / mask is placed in the ACL field, **all** cannot be re-entered. You can use an address and mask pair of 0.0.0.0/1 as an equivalent configuration to **all**.

◆ **Note**

If your policy is that the admin console can only be accessed from the management network, be sure to set the IP access restrictions for IP access security (for more information, refer to the Limit IP Access section of the Admin Access Security page in the FirePass online help).

Setting the Network Configuration options

In this section, we configure the IP addresses of the FirePass controller so that the BIG-IP GTM monitor and direct traffic to FirePass controllers. We recommend three FirePass IP addresses for this configuration, one for management, one for use in the BIG-IP GTM wide IP, and one for statically resolved host names (one that is not in the Wide IP and does not change based on the load balancing method/decision).

You may already have IP addresses configured, but we recommend adding at least one additional external IP address.

In order to maintain proper session state, FirePass client connections must remain at the same FirePass controller that the user logged into. To achieve this, the FirePass will redirect the user from the load balanced host name to a non-load balanced hostname once the load balancing decision has been made. The user session is then established using the non-load balanced name.

To set the Network Configuration options

1. From the navigation pane, click **Device Management**, expand **Configuration**, and then click **Network Configuration**.
2. From the Add New IP section, in the **IP Address /Netmask** boxes, type the appropriate IP address and Netmask.
3. In the **Broadcast** box, you can optionally type a broadcast IP.
4. From the **Interface** list, select the appropriate interface for this IP address.
5. Click the **Add New** button.
6. Repeat these steps for the BIG-IP GTM Wide IP, and the address for the statically resolved host name.

Interfaces VLAN IP Config Routing DNS Hosts Web Services Misc

IP Configuration

Fields marked by * are required
Fields marked by color are optional

*IP Address/Netmask	*Interface	Broadcast	
10.1.103.214 / 22	eth0	10.1.103.255	Delete
10.133.50.197 / 26	VLAN: siteBOutside	10.133.50.255	Delete
10.133.50.198 / 26	VLAN: siteBOutside	10.133.50.255	Delete
10.133.50.200 / 26	VLAN: siteBOutside	10.133.50.255	Delete

Update

Add New IP

*IP Address/Netmask: 10.133.50.196 / 26
 Broadcast IP: 10.133.50.255
 *Interface: VLAN: siteBOutside
 Add New

Figure 4 Configuring the FirePass IP address for use with BIG-IP GTM

Configuring the Host options

In this section, we configure the Fully Qualified Domain Name (FQDN) of the FirePass controller. In this configuration, the FQDN must match the name of the Wide IP you will configure on the BIG-IP GTM device.

To configure the Host options

1. From the navigation pane, click **Device Management**, expand **Configuration**, and then click **Network Configuration**.
2. Click the Hosts tab.
3. In the **FQDN** of the controller box, type the domain name that you will use for the Wide IP on the BIG-IP GTM.
4. Click the **Update** button.

The screenshot shows a configuration interface with a navigation bar at the top containing tabs: Interfaces, VLAN, IP Config, Routing, DNS, Hosts, Web Services, and Misc. The 'Hosts' tab is selected. Below the navigation bar, there is a section titled 'FQDN of the controller' with a text input field containing 'firepass.example.net' and an 'Update' button. Below this is a section titled 'Static Hostnames' with a sub-section 'Add new static hostname' containing two input fields labeled 'Hostname:' and 'IP:', and an 'Add New' button.

Figure 5 Configuring the GTM Wide IP as the FQDN of the FirePass

Modifying the Web Service options

In this section, we modify the Web Service options on the FirePass controller. The first procedure is only necessary if you use an externally available service for redirecting clients to an HTTPS web service. If you do not, skip to the next procedure.

To modify the HTTP port 80 Web Service options

1. From the navigation pane, click **Device Management**, expand **Configuration**, and then click **Network Configuration**.
2. Click the Web Services tab.

3. From the **Web Server Configuration** table, click the **Configure** link if you use an externally available service for redirecting clients to an HTTPS web service. Otherwise continue to the following procedure.
4. Make sure that the Host Name is set to the BIG-IP GTM Wide IP name.
5. In the **HTTPS URL to redirect to** box, type address of the BIG-IP GTM Wide IP, preceded by **https://**.
6. Make sure that the **Do not redirect to HTTPS** box is *unchecked*. Clear the box if it is checked.
7. In the bottom section where you specify the agents bound to this service, ensure that all the options are *unchecked*.
8. Click the **Update** button.

[Interfaces](#)
[VLAN](#)
[IP Config](#)
[Routing](#)
[DNS](#)
[Hosts](#)
[Web Services](#)
[Misc](#)

Web Service Configuration for firepass.example.net:80

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 Logon

Admin Logon :

WebAccess Bypass:

Offload SSL processing to a BIG-IP Local Traffic Manager

[Back to Services Configuration >>](#)

Figure 6 Configuring the port 80 Web Service

Now we modify the HTTPS port 443 Web Service.

To configure the HTTPS port 443 Web Service options

1. From the navigation pane, click **Device Management**, expand **Configuration**, and then click **Network Configuration**.
2. Click the Web Services tab.
3. From the **Web Server Configuration** table, click the **Configure** link for the existing externally available host on port 443.
4. Make sure that the Host name is set to the BIG-IP GTM Wide IP name.
5. Check the **Use SSL** box.
6. From the **Certificate** list, select the certificate for the BIG-IP GTM Wide IP host name. If you do not have certificate, see the *FirePass Controller Administrator Guide*, Chapter 4, **Using Server Certificates**.
7. Make sure the **User Logon** and **Admin** boxes are checked.
8. Uncheck the **WebAccess Bypass** and **Offloading SSL to a BIG-IP Local Traffic Manager** boxes.
9. Click the **Update** button.

Creating the new Web Services

In this section, we create new web services for the static (non-load balanced) host names. Again, the first procedure is only necessary if you use an externally available service for redirecting clients to an HTTPS web service. If you do not, skip to the next procedure.

To create new port 80 web service

1. From the navigation pane, click **Device Management**, expand **Configuration**, and then click **Network Configuration**.
2. Click the Web Services tab.
3. In the **Add new service** section, from the **IP** list, select the IP you created for the static name in the *Setting the Network Configuration options* section from the list.
4. In the Port box, type **80**.
5. In the **Name** box, type the static Host name.
6. Leave the **SSL** box unchecked.
7. Click the **Add New** button.
The Web Service Configuration options page opens.
8. In the **HTTPS URL to redirect to** box, type address of the BIG-IP GTM Wide IP, preceded by **https://**.

9. Leave all other settings at their default (unchecked) levels, and click the **Update** button.

Now we create a new HTTPS port 443 Web Service

To create new port 443 web service

1. From the navigation pane, click **Device Management**, expand **Configuration**, and then click **Network Configuration**.
1. Click the Web Services tab.
2. In the **Add new service** section, from the **IP** list, select the IP you created for the static name in the *Setting the Network Configuration options* section from the list.
3. In the Port box, type **443**.
4. In the **Name** box, type the static Host name.
5. Check the **SSL** box.
6. Click the **Add New** button.
The Web Service Configuration options page opens.
7. From the Certificate list, select the certificate for the non-load balanced name.
8. Check the User Logon box, and leave all other boxes unchecked.
9. Click the **Update** button.
10. Click the **Back to Services Configuration** link.

Finalizing the configuration

The final step in this section is to finalize the configuration changes you just made.

To finalize the configuration

1. Click the **Finalize Section** link (or the Finalize tab)
2. Review the settings.
3. Click the **Finalize Changes** button. You are prompted to reboot the FirePass controller.

Configuring the PreLogon Sequence

The next procedure is to configure a new pre-logon sequence, or prepend new prelogon actions to an existing pre-logon sequence. This is necessary to ensure that all user sessions have been passed to a FirePass controller by the BIG-IP GTM so that the system is appropriately load balanced. The port 80 web service takes care of this when the user enters

http://firepass.example.net in a web browser or standalone FirePass client. A check in the prelogon sequence performs redirection when the user enters **https://firepass.example.net** in a web browser or standalone FirePass client, and directs the user to the non-load balanced service on the local FirePass controller; for example **https://firepass-a.example.net**.

To configure a PreLogon Sequence

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Pre-Logon Sequence**.
2. In the New Sequence section at the bottom of the page, type a name for the sequence in the **Create New Sequence** box. In our example, we type **GTM-Sequence**.
3. From the **Based on** list, select **template: Empty**.
4. Click the **Create** button.
The new sequence appears in the Select Sequence to Use table.
5. In the row of the sequence you just created, click the **Edit** button.

***Warning** - Do not click the option button in front of the sequence name yet. If you click the option button, the **Edit** link will be replaced with the **View** link, and you are not able to edit the sequence.*

The Pre-Logon Sequence Editor opens.

6. In the SubSequences section, click the **Open subsequences management** link.
The Subsequences options appear on the right.
7. In the Add subsequence box, type a name for this subsequence. In our example, we type **gtm-logon-check**.
8. Move the cursor between **Subsequence:gtm-logon-check** and the **Logon Denied** box. A small add [+] link appears on the arrow. Click that **Add** link.
The Change Sequence panel appears on the right.
9. In the Change Sequence panel, from the **Using** list, select **New Action**, and then click the **Apply Changes** button.
The New Action box appears in the subsequence.

10. On the right, from the **Edit Action** section, type a name for the action in the Name box where it currently says New Action. In our example, we type **CheckLBStatus**. In the **Description** box, you can optionally type a description. Click the **Update Details** button.

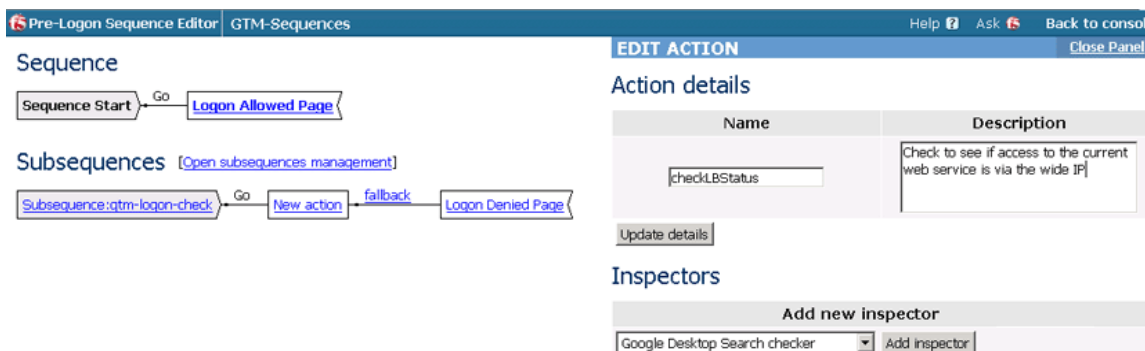


Figure 7 Adding a new action to the subsequence

11. Move the cursor between the new action name you just created (**CheckLBStatus** in our example) and the **fallback** link. A small add [+] link appears on the arrow. Click that **Add** link. The **Insert Rule** box opens on the right.

12. In the Insert Rule section, type a name for the rule in the **Name** box. In our example, we type **AccessViaWideip**. In the rule box, use the following rule syntax:

```
session.network.server.host == "<wide IP name>"
```

In our example, we type:

```
session.network.server.host == "firepass.example.net"
```

Click the **Insert Rule** button.

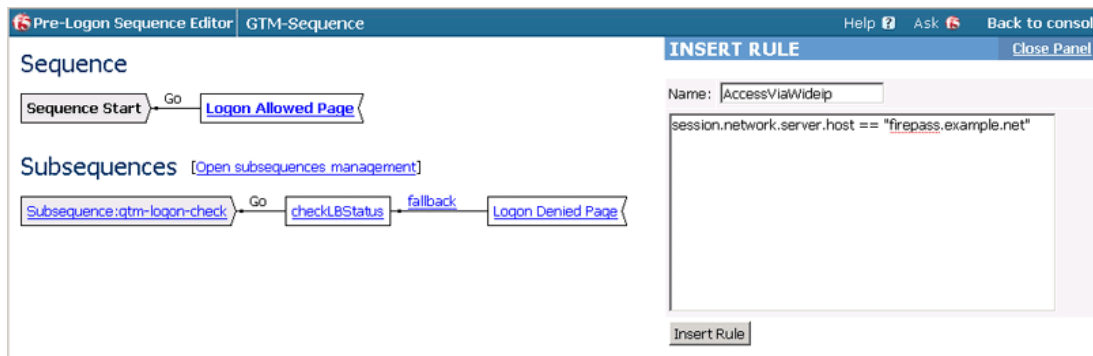


Figure 8 Inserting the Rule for the PreLogon Sequence

It is important to remember if you are running FirePass version 6.0.2, you must have HF-76259-3-1 installed for this prelogon sequence to run. For FirePass versions 6.0.1 and earlier, this hotfix is not required. For more information on Hot Fixes, see Ask F5.

13. Click the **Logon Denied Page** link box. The End Page Properties options open on the right. You have two options:

If you have an existing PreLogon sequence for anti-virus or other pre-logon checks, this sequence should be inserted here. You must modify this existing sequence to have the successful sequence path direct users to the URL for the non-load balanced URI on the FirePass controller.

If you do not have any other PreLogon sequences, from the **Type** list, select **External Logon Page (Client data posted)**. In the **External URL** box, type the URL for the non-load balanced URI on the FirePass controller, and then click the **Update** button.

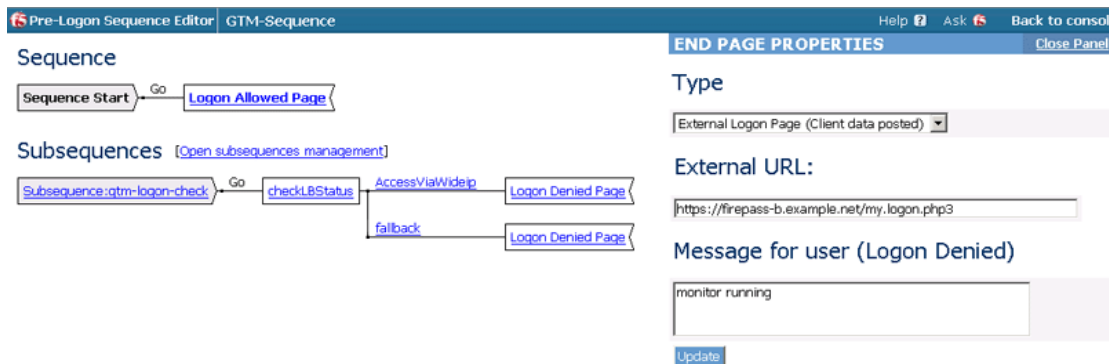


Figure 9 Modifying the End Page properties to direct to the non-load balanced URI on the FirePass

14. In the Subsequences section, from the **Fallback** branch, click the **Logon Denied Page** link box after the fallback link. The End Page Properties options open on the right.

15. From the **Type** list, select **Redirect (No client data posted)**. In the **External URL** box, type the BIG-IP GTM wide IP host name, and then click the **Update** button. In our example, we type **https://firepass.example.net**.

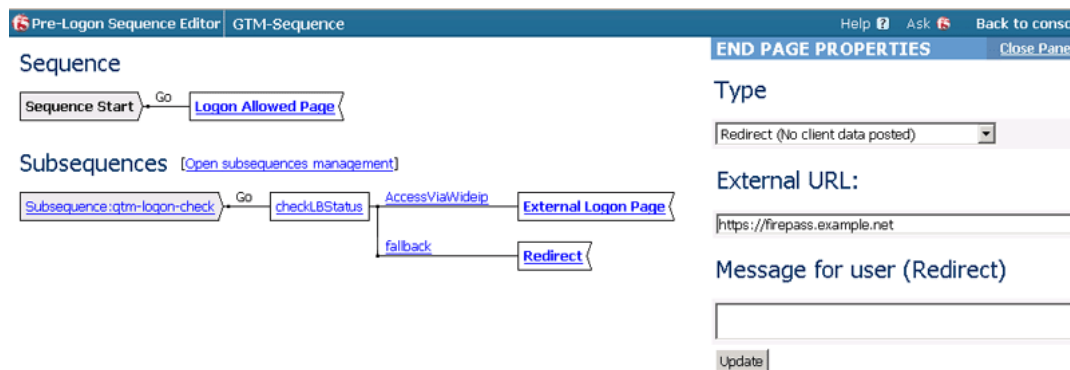


Figure 10 Configuring the Fallback option to be the host name of the BIG-IP GTM wide IP

16. In the Sequence section, move the cursor between **Sequence Start** and the **Logon Allowed Page** box. A small add [+] link appears on the arrow. Click that **Add** link. The Change Sequence panel appears on the right.
17. From the **Change Sequence** list, select **Replace action (deletes branches after)**.
18. In the Subsequences section, click the button for the name of the subsequence you just created, and click the **Apply Changes** button. In our example, we click **Subsequence: gtm-logon-check**. When you are finished, your sequence should look like the following example:

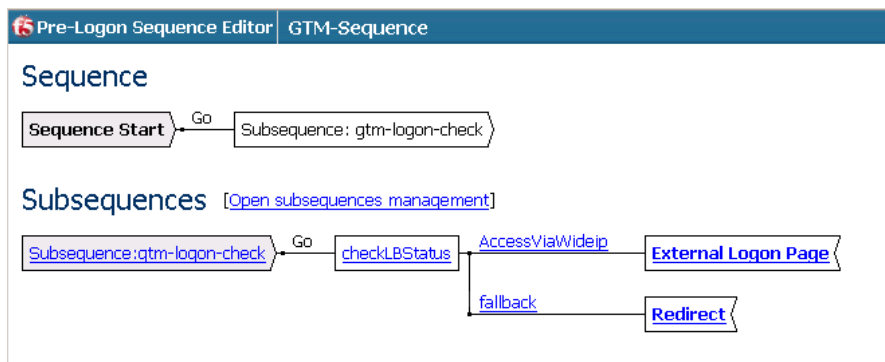


Figure 11 The completed PreLogon Sequence

19. Click the **Back to Console** link in the upper right. The PreLogon Sequence page opens.

-
20. In the Select Sequence to Use section, click the button for the Sequence you just created, and then click the **Apply** button. In our example, we click the button for **GTM-Sequence**.

Configuring the BIG-IP GTM system

In this section, we configure the BIG-IP GTM system to monitor and load balance the FirePass controllers.

Connecting to the BIG-IP GTM system

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

To connect to the BIG-IP GTM 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 GTM system, as well as access online help, download SNMP MIBs and Plug-ins, and search for specific objects.

Configuring the external health monitor

The first step in the BIG-IP GTM configuration is to create a health monitor for the FirePass devices. For this configuration, we use a EAV health monitor, which uses an external script to check the status of the FirePass devices. You can either **download the script** from F5, or see *Appendix A: EAV script code*, on page 25 to create the script yourself.

The EAV monitors the FirePass controllers and provides the ability to alter traffic flows based on the FirePass. The BIG-IP GTM is able to make informed load balancing decisions based upon exceeding a configurable threshold for one minute UNIX load average or concurrent session usage.

An upcoming release of the BIG-IP GTM will include built-in support for monitoring FirePass devices, which will eliminate the need for this external script.

◆ Important

*If you are using the BIG-IP GTM in a redundant configuration, you need to copy this script on to both GTM systems. The script is not copied over using the **configsync** command. You also need to copy the EAV anywhere there is a big3d agent that could monitor the FirePass devices.*

To create health monitor

1. Download the script (found at www.f5.com/solution-center/deployment-guides/files/gtm-firepass-eav.pl) or create your own perl script based on the script in *Appendix A: EAV script code*, on page 25.
2. Save the script file on the BIG-IP GTM system in the `/usr/bin/monitors` directory. For example, run the following command from a command line,

```
scp gtm-firepass-eav.pl root@bigip.example.net:/usr/bin/monitors
```

3. From the command line, run the following command:

```
chmod +x /usr/bin/monitors/gtm-firepass-eav.pl.
```

This enables BIG-IP LTM to execute the script.
4. On the Main tab, expand **Global Traffic**, and then click **Monitors**. The Monitors screen opens.
5. Click the **Create** button. The New Monitor screen opens.
6. In the **Name** box, type a name for the Monitor. In our example, we type **firepass-eav**.
7. From the **Type** list, select **External**. The External monitor options display.
8. In the **Interval** box, type a time in seconds. In our example, we type **15**. This setting determines how frequently the monitor runs.
9. In the **Timeout** box, type a time in seconds. We recommend this is at least three times the interval, plus one second. In our example, we type **61**. This setting determines how long the target has in which to respond to the monitor request.
10. In the **Probe Timeout** box, type a number of seconds.
11. In the **External Program** box, type the name of the script you uploaded to the BIG-IP GTM system. In our example, we type **firepass-eav.pl**.
12. In the **Arguments** box, you specify values required by the script for load average and concurrency percentage, in that order, separated by a space. These values depend on your configuration. We recommend a max concurrency of 90 to 95%, however you may need to adjust this down according to usage pattern. In our example, we type **12 80** (see Figure 12).
13. Click the **Finished** button.

◆ Important

*If you downloaded the script, you must open the file in an editor and set the **my \$pass** parameter to equal the name of your password. This password should be the same across all FirePass devices in this configuration.*

Global Traffic > Monitors > New Monitor...

General Properties

Name: firepass-eav

Type: External

Import Settings: external

Configuration: Basic

Interval: 15 seconds

Timeout: 61 seconds

Probe Timeout: 5 seconds

External Program: firepass-eav.pl

Arguments: 12 80

Variables

Name = Value

Add

Edit Delete

Cancel Repeat Finished

Figure 12 Creating the external health monitor

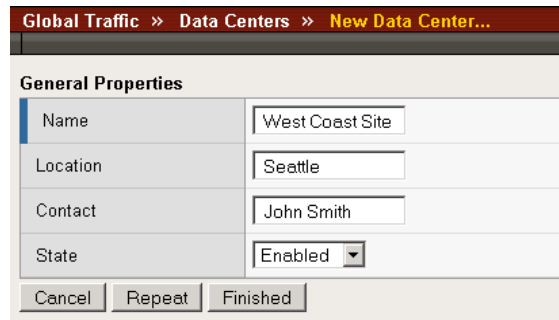
Configuring the Data Center objects

The next step is to create BIG-IP GTM Data Center objects for each data center with a FirePass controller that is part of this configuration. If you already have the data center objects configured, you can skip this procedure.

To create the Data Center objects

1. On the Main tab, expand **Global Traffic**, and then click **Data Centers**.
The Data Center screen opens.
2. Click the **Create** button.
The New Data Center screen opens.
3. In the **Name** box, type a name for the data center. In our example, we type **West Coast Site**.
4. In the **Location** box, type the physical location of the data center. In our example, we type **Seattle**. This field is optional.

-
5. In the **Contact** box, type the name of the administrator for this data center. In our example, we type **John Smith**. This field is optional.
 6. Click the **Finished** button.
 7. Repeat this procedure for any other data centers.



The screenshot shows a dialog box titled "Global Traffic » Data Centers » New Data Center...". It has a "General Properties" section with the following fields:

Name	West Coast Site
Location	Seattle
Contact	John Smith
State	Enabled

At the bottom of the dialog are three buttons: "Cancel", "Repeat", and "Finished".

Figure 13 Creating a new Data Center

Creating the Data Center Server objects

The next step is to create Data Center Server objects for each of the FirePass controllers in this deployment.

To create the Data Center Server objects

1. On the Main tab, expand **Global Traffic**, and then click **Servers**. The Servers screen opens.
2. Click the **Create** button. The New Server screen opens.
3. In the **Name** box, type a name for this server. In our example, we type **Seattle-FirePass-1**.
4. From the **Product** list, select **Generic Host**.
5. In the **Address** box, type the IP address of the Wide IP that you provisioned for the FirePass controller.
6. The Translation section is optional.
7. From the **Data Center** list, select the appropriate Data Center.

The screenshot shows the 'New Server...' configuration window. The 'General Properties' section includes:

- Name:** Seattle-Firepass-1
- Product:** Generic Host
- Address:** 10.50.133.197
- Translation:** (optional)
- Data Center:** West Coast Site
- Status:** Enabled

An 'Address List' section is also present, featuring an 'Add' button and a list of addresses with 'Remove', 'Edit', 'Up', and 'Down' buttons.

Figure 14 Configuring the Server objects for the FirePass device

8. In the **Health Monitors** section, from the Available list, select **https**. We recommend you create a new HTTPS monitor using the https parent monitor, but select the canned monitor for simplicity.
9. From the Resources section, in the **Name** box, type a descriptive name so you know which web service on the Firepass this corresponds to.
10. In the **Address** box, type the IP address of the FirePass controller.
11. In the **Service Port** box, type **443** or select HTTPS from the list.
12. The Translation and Translation Port settings are optional, configure if applicable for your configuration.
13. Click the **Add** button.

The screenshot shows the 'Resources' configuration window. The 'Virtual Server List' section includes:

- Name:** Seattle-FirePass-1
- Address:** 10.133.50.197
- Service Port:** 443
- Service:** HTTPS
- Translation:**
- Translation Port:** Select...
- Add** button
- Virtual Server List:** Seattle-FirePass-1: 10.133.50.197:443
- Remove**, **Edit**, **Up**, **Down** buttons
- Cancel**, **Repeat**, **Create** buttons

Figure 15 Configuring the Resources section of the BIG-IP GTM server

-
14. Click the **Finished** button.
 15. Repeat this entire procedure for each FirePass controller in your deployment.

Creating the Wide IP pools

In this section, we create the Wide IP pools. In our configuration, we create three pools, one that contains the FirePass devices in our West Coast site, one for the FirePass devices in the East Coast site, and one that contains all of the FirePass controllers.

To create the Wide IP pool

1. On the Main tab, expand **Global Traffic**, and then click **Pools** under Wide IP.
The Pools screen opens.
2. Click the **Create** button.
The New Pool screen opens.
3. In the **Name** box, type a name for this pool. In our example, we type **WC-FirePass-pool**.
4. In the **Health Monitors** section, from the **Available** list, select the name of the External monitor you created in *Configuring the external health monitor*, and click the Add (<<) button. In our example, we type **firepass-eav**.
5. In the **Load Balancing** method section, from the Preferred list, select a load balancing method appropriate for your configuration.
6. From the **Virtual Server** list, select the one of the Servers you just created for a FirePass controller, and click the **Add** button.
7. Repeat step 6 for all of the servers (FirePass devices) in this data center. All of the Servers you select for this pool must be in the same data center.
8. Click the **Finished** button (see Figure 16).

Figure 16 Creating the GTM pool

9. Repeat this procedure to create a pools for the FirePass devices in other data centers. Each pool should contain all of the FirePass devices in that particular data center.
In our example, we create one additional pool named **EC-FirePass-pool** for the FirePass devices in our East Coast data center.
10. Repeat this procedure creating a pool for all of the FirePass devices in this configuration.
In our example, we name the pool **AllFirePasses**.

Creating the Wide IP

The final procedure in this configuration is to create a Wide IP on the GTM system.

To create the Wide IP

1. On the Main tab, expand **Global Traffic**, and then click **Wide IPs**. The Pools screen opens.
2. Click the **Create** button. The New Wide IP screen opens.
3. In the **Name** box, type a name for this Wide IP. This should be the name that you have used for the Wide IP on the FirePass devices. In our example, we type **firepass.example.net**.
4. In the **Pools** section, from the **Load Balancing** list, select a load balancing method. For more information on BIG-IP GTM load balancing methods, see the online help or the FirePass documentation.
5. In the **Pool List** section, from the **Pool** list, select the name of one of the pools you created in *Creating the Wide IP pools*, on page 21, and click the Add button. In our example, we select **WC-FirePass-pool**.
6. Repeat step 5 for any additional FirePass pools you created. Do not add the pool you created for all FirePass devices in this step.
7. From the Last Resort Pool list, select the name of the pool you created for all FirePass devices. In our example, we type **AllFirePasses**.
8. Click the **Finished** button (see Figure 17).

Global Traffic >> Wide IPs >> New Wide IP...

General Properties: Basic

Name: firepass.example.net

State: Enabled

iRules

iRule: [Empty]

Add

iRule List

Remove Up Down

Pools

Load Balancing Method: Round Robin

Persistence: Disabled

Pool: WC-Firepass-pool

Ratio: 1

Add

Pool List

WC-Firepass-poolRatio(1)
EC-Firepass-poolRatio(1)

Remove Edit Up Down

Last Resort Pool: AllFirePasses

Cancel Repeat Finished

Figure 17 Creating the Wide IP

This completes the configuration.

Appendix A: EAV script code

The following is the code for the EAV script. You must change the \$pass entry to be the name of your password.

```
#!/usr/bin/perl
use strict;
use MIME::Base64;

open(DEBUG, ">>/root/debug.log");

my $host = $ARGV[0];
my $port = $ARGV[1];

# 1 Minute load average Threshold and session usage percentage threshold
# must both be specified, or neither must be specified
my $MinLoadAverageThreshold = $ARGV[2];

# specifying an amount less than 100 will accomodate caching DNS
# servers or other devices that might resolve the WideIP and not
# send the request to GTM for resolution
my $sessionUsagePercentageThreshold = $ARGV[3];

# change the $pass parameter to suit -- must use the same password on
# each FirePass
my $user = 'gtmuser';
my $pass = 'password';
my $request;
my $sessionUsagePercentage;
my $MinLoadAverage;
my $largestDatabaseTableSize;
my @response;

$host =~ s/::ffff://g;

print DEBUG "HOST: $host, PORT: $port, USER: $user, PASS: $pass, PERCENTAGE:
$sessionUsagePercentageThreshold, LOAD: $MinLoadAverageThreshold\n";

my $openssl = "openssl s_client -ign_eof -connect ${host}:${port}";

$request = "GET /load_status.php HTTP/1.1\r\n"
    . "Host: ${host}:${port}\r\n"
    . "Content-Length: " . length($request) . "\r\n"
    . "Authorization: Basic " . MIME::Base64::encode("$user:$pass", '') . "\r\n"
    . "Connection: close\r\n"
    . "\r\n"
    . "${request}\r\n";

chop (@response = qx(echo "${request}" | ${openssl} 2>/dev/null));

for (@response) {
    if ( $_ =~ /(Usage|Percentage|Average|table): \d/ ) {
        my ($name, $val) = split /:/, $_;
        chop($sessionUsagePercentage = $val) if (/Percentage/);
        $MinLoadAverage = $val if (/Load Average/);
        $largestDatabaseTableSize = $val if (/Database table/);
    }
}

# when a device is marked UP it means that session utilization is below the
# threshold, and the 1 Minute load average is below the threshold
if ( ($sessionUsagePercentage < $sessionUsagePercentageThreshold) && ($MinLoadAverage <
$MinLoadAverageThreshold) ) {
    print "UP\n";
}

exit(0);
```