



12

Configuring HTTPS Load Balancing with Data Compression

- Introducing HTTPS load balancing with compression
- Creating an SSL key and certificate
- Creating a custom Client SSL profile
- Creating a custom HTTP profile for compression
- Creating a pool
- Creating a virtual server

Introducing HTTPS load balancing with compression

When you want to enable data compression of HTTPS traffic, and load balance the traffic, you can configure the BIG-IP® system to perform the SSL handshake that target web servers normally perform. A common way to configure the BIG-IP system is to enable it to decrypt client requests before sending them on to a server, and encrypt server responses before sending them back to the client.

In general, the way to configure the BIG-IP system to perform SSL handshaking (and thus process HTTPS traffic), is to first request and install an SSL key and certificate onto the BIG-IP system. Using the key/certificate pair, the BIG-IP system can act as a server to decrypt the client request before sending it on to the server, and it can encrypt the server response before sending it back to the client.

After installing the key/certificate pair, you can create a custom Client SSL profile. A *Client SSL profile* is a type of traffic profile that determines the way that the BIG-IP system processes client requests that are sent by way of a fully SSL-encapsulated protocol (in this case, HTTPS requests).

Next, you create a custom HTTP profile and enable data compression on the BIG-IP system. Then, you must create a pool of servers for load balancing the HTTPS requests.

Finally, you must create a virtual server to process the HTTPS traffic, according to the settings you configured in the custom Client SSL profile.

For more detailed, background information on SSL certificates, SSL profiles, load balancing pools, and virtual servers, see the *Configuration Guide for BIG-IP® Local Traffic Management*.

Creating an SSL key and certificate

Before you can load balance HTTPS traffic and enable compression, you must create an SSL key and certificate to install onto the BIG-IP system. With an SSL key and certificate, and the custom Client SSL profile that you create next, the BIG-IP system can perform the SSL handshaking normally performed by a target web server.

For purposes of testing that you can pass HTTPS traffic successfully, you can use a self-signed certificate, rather than one signed by a trusted certificate authority.

To create a self-signed key/certificate pair

1. On the Main tab of the navigation pane, expand **Local Traffic**, and click **SSL Certificates**.
This displays a list of existing SSL certificates.
2. On the upper-right corner of the screen, click **Create**.
This opens the New SSL Certificate screen.
*Note: If the **Create** button is unavailable, this indicates that your user role does not grant you permission to create SSL certificates.*
3. In the **Name** box, type a name for the certificate, such as **my_cert**.
4. From the **Issuer** list, select **Self**.
5. In the **Common Name** box, type either the IP address for the virtual server you will create later on in this chapter, or a DNS name that resolves to the virtual server's IP address.
6. In the **Division** box, type your company name.
7. In the **Organization** box, type your department name.
8. In the **Locality** box, type your city name.
9. In the **State or Province** box, type your state or province name.
10. From the **Country** list, select the name of your country.
11. In the **E-mail Address** box, type your email address.
12. In the **Challenge Password** box, type a password.
13. In the **Confirm Password** box, re-type the password you typed in the **Challenge Password** box.
14. In the Key Properties area of the screen, from the **Size** list, select **1024**.
15. Click **Finished**.

Creating a custom Client SSL profile

The next task in configuring HTTPS load balancing with compression is to create a custom Client SSL profile. A **Client SSL profile** is a group of settings that enable the BIG-IP system to perform decryption and encryption for client-side SSL traffic. Some of the data you specify in the Client SSL profile are the names of the key and certificate you created in the previous section.

After you create the custom Client SSL profile, you create a load balancing pool, and then create a virtual server, assigning the custom profile to that virtual server.

To create a custom Client SSL profile

1. On the Main tab of the navigation pane, expand **Local Traffic**, and click **Profiles**.
The HTTP Profiles screen opens.
2. From the SSL menu, choose Client SSL.
This displays a list of any existing Client SSL profiles, including the default profile **clientsssl**.
3. In the upper-right corner of the screen, click **Create**.
The New Client SSL Profile screen opens.
*Note: If the **Create** button is unavailable, this indicates that your user role does not grant you permission to create a profile.*
4. In the **Name** box, type a name for the custom profile, such as **clientsssl_profile**.
5. Ensure that the **Parent Profile** setting is set to **clientsssl**.
6. For the **Certificate** setting, check the Custom box on the far right side of the screen.
7. From the **Certificate** list, select the name of the certificate you created in the previous section.
Using our example, this name would be **my_cert.crt**.
8. For the **Key** setting, check the Custom box on the far right side of the screen.
9. From the **Key** list, select the name of the key you created in the previous task.
Using our example, this name would be **my_cert.key**.
10. Click **Finished**.

Creating a custom HTTP profile for compression

To enable HTTP data compression on the BIG-IP system, you must create a custom HTTP profile. An *HTTP profile* defines the way that you want the BIG-IP system to manage HTTP traffic.

After you create the custom HTTP profile, you create a load balancing pool. Then you create a virtual server, assigning the custom HTTP profile to that virtual server.

To create a custom HTTP profile for compression

1. On the Main tab of the navigation pane, expand **Local Traffic**, and click **Profiles**.
This displays a list of any existing HTTP profiles, including the default profile **http**.
2. In the upper-right corner of the screen, click **Create**.
The New HTTP Profile screen opens.
*Note: If the **Create** button is unavailable, this indicates that your user role does not grant you permission to create a profile.*
3. In the **Name** box, type a name for the custom profile, such as **http_compress**.
4. Ensure that the **Parent Profile** setting is set to **http**.
5. In the Settings area of the screen, retain all default values.
6. For the **Compression** setting, on the far right side of the screen, check the Select box and select **Enabled** from the list.
7. If you want to base compression on URIs specified in the HTTP request headers:
 - a) Locate the **URI Compression** setting, check the Select box on the far right of the screen, and select **URI List** from the list.
This displays the **URI List** settings.
 - b) Specify any regular expressions that you want to include or exclude from compression.
Examples of regular expressions are ***\pdf**, ***\gif**, or ***\html**.
8. If you want to base compression on the type of response content:
 - a) Locate the **Content Compression** setting, check the Select box on the far right of the screen, and select **Content List** from the list.
This displays the **Content List** settings.

- b) Specify values for content you want to include or exclude from compression.
Examples of content types that you can specify are **application/pdf** and **image/****.
9. For all other settings in the Compression area of the screen, retain the default values, or configure them to suite your needs.
10. Click **Finished**.

Creating a pool

The next task in the process is to create a load balancing pool to load balance HTTPS connections. After you create the pool, you assign it to a virtual server that you create.

To create a pool for load balancing HTTPS traffic

1. On the Main tab of the navigation pane, expand **Local Traffic**, and click **Pools**.
The Pools screen opens.
2. In the upper-right corner of the screen, click **Create**.
The New Pool screen opens.
*Note: If the **Create** button is unavailable, this indicates that your user role does not grant you permission to create a pool.*
3. In the **Name** box, type a name for the pool, such as **https_pool**.
4. For the **Health Monitors** setting, from the **Available** box select **https** or **https_443**, and click the Move button (<<) to move the monitor name to the **Active** box.
5. In the Resource area, for the **New Members** setting, add the pool members:
 - a) Click the **New Address** option.
 - b) In the **Address** box, type the IP address of a server in the pool.
 - c) In the **Service Port** box, type **80**, or select **HTTP**.
 - d) Click **Add**.
 - e) Repeat steps b, c, and d for each server in the pool.
6. Click **Finished**.

Creating a virtual server

The final task in configuring HTTPS load balancing is to define a virtual server that references the custom Client SSL profile and the load balancing pool that you created in previous tasks.

To create a virtual server for HTTP compression

1. On the Main tab of the navigation pane, expand **Local Traffic**, and click **Virtual Servers**.
The Virtual Servers screen opens.
2. In the upper-right corner of the screen, click **Create**.
The New Virtual Server screen opens.
*Note: If the **Create** button is unavailable, this indicates that your user role does not grant you permission to create a virtual server.*
3. In the **Name** box, type a name for the virtual server, such as **vs_clientssl**.
4. In the **Destination** box, verify that the type of virtual server is **Host**, and in the **Address** box, type an IP address for the virtual server.
5. In the **Service Port** box, type **443**, or select **HTTPS** from the list.
6. In the Configuration area of the screen, retain the value of the **Protocol** setting, **TCP**.
7. From the **HTTP Profile** list, select the name of the HTTP profile that you created.
Using our example, this value would be **http_compress**.
8. From the **Client SSL Profile** list, select the custom Client SSL profile that you created in a previous section. In our example, this value would be **clientssl_profile**
This assigns the custom Client SSL profile to the virtual server.
9. In the Resources area of the screen, locate the **Default Pool** setting and select the pool name that you created in a previous section.
Using our example, this would be **https_pool**.
10. From the **Default Persistence Profile** list, select **source_addr**.
This implements the default profile for source address affinity persistence.
11. Click **Finished**.

You can now test the configuration by attempting to pass HTTPS traffic through the virtual server. Check to see that the BIG-IP system includes and excludes the responses that you specified in the custom HTTP profile, and that the system compresses the data as specified.