Introducing the SSL Gateway

You can configure the SSL Gateway feature to proxy SSL traffic to your content servers. The web server on the BIG/ip Controller has a proxy feature that allows it to accept HTTPS connections (HTTP over SSL) and instead of serving the page itself, it can connect to another web server, retrieve the page, and then send the page to the original client.

A key component of the gateway feature is that the web server can retrieve the web page using an unencrypted HTTP request to the content server. The SSL Gateway converts HTTP requests that are encrypted with SSL, to unencrypted requests. Decrypting the request is necessary so that the header of the HTTP request can intelligently control how the request is handled.

When the web server connects to the content server, it uses the original client's IP address and port as its source address and port, so that it looks like the client (for logging purposes).

This chapter describes the following features of the BIG/ip Controller SSL Gateway:

- Hardware accelerator options
- Configuring an SSL Gateway
- Enabling and disabling an SSL Gateway
- Viewing the configuration of an SSL Gateway
- Optional SSL Gateway configuration

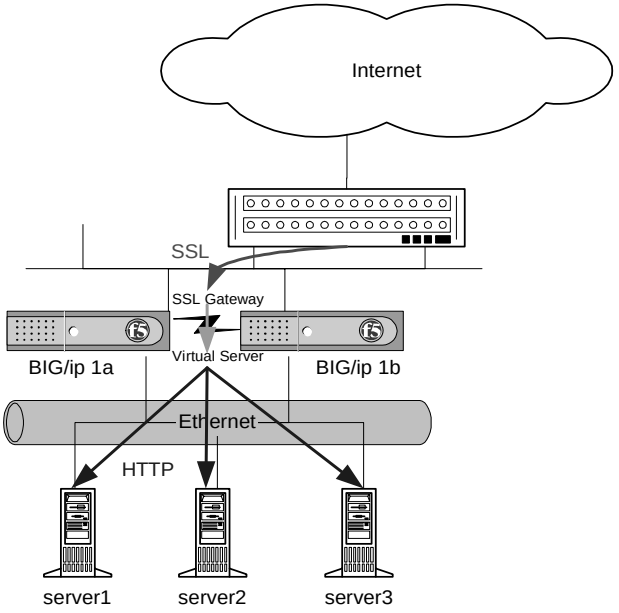

Figure 4.1 *An incoming SSL connection received by an SSL Gateway configured on a redundant BIG/ip Controller system*

Hardware acceleration options

Because the SSL Gateway feature is computationally intensive, we recommend that you use this feature on a BIG/ip Controller with an encryption accelerator installed. The BIG/ip Controller currently supports the Rainbow cryptoSWIFT encryption accelerator.

The BIG/ip Controller detects the cryptoSWIFT card at boot up and links the appropriate web server to the card.

◆ Note

Hardware acceleration greatly increases the number of concurrent SSL transactions the BIG/ip Controller can handle.

Configuring an SSL Gateway

There are several steps required to set up an SSL Gateway on the BIG/ip Controller. These steps include:

- Generating a key and obtaining a certificate
- Configuring the web server with the certificate and key
- Create an HTTP virtual server
- Create the SSL Gateway

An additional configuration option you can use with the SSL Gateway is a last hop pool for the SSL Gateway. If the SSL Gateway handles connections from external devices, you must create a last hop pool that contains the devices from which the BIG/ip Controller receives connections.

Generating a key and obtaining a certificate

In order to use the SSL Gateway feature you must obtain a valid x509 certificate from an authorized certification authority (CA) such as Verisign (http://www.verisign.com).

To obtain a valid certificate, you must have a private key. If you do not have a key, you can use the **genconf** and **genkey** utilities on the BIG/ip Controller to generate a key, a temporary certificate, and a request file you can submit to a certification authority (CA). If you have a key, you can use the **gencert** utility to generate a temporary certificate and request file. These utilities are described in the following list:

- **genconf**
  This utility creates a key configuration file that contains specific information about your organization. The genkey utility uses this information to generate a certificate.
- **genkey**
  After you run the **genconf** utility, run this utility to generate a temporary 30 day certificate for testing the SSL Gateway on the BIG/ip Controller. This utility also creates a request file that you can submit to a certification authority (CA) to obtain a certificate.

- **gencert**
  If you already have a key, run this utility to generate a temporary certificate and request file for the SSL Gateway.

To generate a key configuration file using the genconf utility

If you do not have a key, you can generate a key and certificate with the **genconf** and **genkey** utilities. First, run the **genconf** utility from the root (/) with the following command:

```
/var/asr/gateway/bin/genconf
```

The utility prompts you for information about the organization for which you are requesting certification. This information includes:

- The fully qualified domain name (FQDN) of the server
- The two letter ISO code for your country
- The full name of your state or province
- The city or town name
- The name of your organization
- The division name or organizational unit

For example, Figure 4.2 contains entries for the server **my.server.net**:

```
Common Name (full qualified domain name): my.server.net
Country Name (ISO 2 letter code): US
State or Province Name (full name): WASHINGTON
Locality Name (city, town, etc.): SEATTLE
Organization Name (company): MY COMPANY
Organizational Unit Name (division): WEB UNIT
```

Figure 4.2 *Example entries for the* ***genconf*** *utility*

After you run the **genconf** utility, you can run the **genkey** utility to create a temporary certificate and a request file.

To generate a key using the genkey utility

After you run the **genconf** utility, you can generate a key with the **genkey** utility. Type the following command from the root (/) to run the **genkey** utility:

```
/var/asr/gateway/bin/genkey <server_name>
```

For the <**server_name**>, type the FQDN of the server to which the certificate applies. After the utility starts, it prompts you to verify the information created by the **genconf** utility. After you run this utility, a certification request form is created in the following directory:

```
/var/asr/gateway/requests/<fqdn>.req
```

The <**fqdn**> is the fully qualified domain name of the server. Please contact your certification authority (CA) and follow their instructions for submitting this request form.

In addition to creating a request form you can submit to a certification authority, this utility also generates a temporary certificate. The temporary certificate is located in:

```
/var/asr/gateway/certs/<fqdn>.cert
```

The <**fqdn**> is the fully qualified domain name of the server. Note that you must copy the key and certificate to the other controller in a redundant system. This temporary certificate is good for thirty days, after which time you are expected to have a valid certificate from your CA. If you do not have a certificate within 30 days, you can re-run this program.

WARNING

Be sure to keep your previous key if you are still undergoing certification. The certificate you receive is valid only with the key that originally generated the request.

To generate a certificate with an existing key with the gencert utility

To generate a temporary certificate and request file to submit to the certification authority with the **gencert** utility, you must first copy an existing key for a server into the following directory on the BIG/ip Controller:

/var/asr/gateway/private/

After you copy the key into this directory, type the following command at the command line:

/var/asr/gateway/bin/gencert <server_name>

For the <**server_name**>, type the FQDN of the server to which the certificate applies. After the utility starts, it prompts you for various information. After you run this utility, a certification request form is created in the following directory:

/var/asr/gateway/requests/<fqdn>.req

The <**fqdn**> is the fully qualified domain name of the server. Please contact your certification authority (CA) and follow their instructions for submitting this request form.

Additional information about keys and certificates

You must have a separate certificate for each domain name on each redundant pair of BIG/ip Controllers, regardless of how many non-SSL web servers are load balanced by the BIG/ip Controller.

If you are already running an SSL server you can use your existing keys to generate temporary certificates and request files. However, you must obtain new certificates if the ones you have are not for the following web server types:

- Apache
- OpenSSL
- Stronghold

WARNING

The BIG/ip Controller does not support Microsoft Internet Information Server (IIS) certificates.

Configuring the gateway with certificates

After you obtain a valid x509 certificate from a certification authority (CA) for the SSL proxy, you must copy it onto each BIG/ip Controller in the redundant configuration.

Copy the certificate into the following directory on each BIG/ip Controller in a redundant system:

/var/asr/gateway/certs/

◆ Note

*The certificate you receive from the certification authority (CA) should overwrite the temporary certificate generated by **genkey** or **gencert**.*

If you used the **genkey** or **gencert** utilities to generate the request file, a copy of the corresponding key should already be in the following directory on the BIG/ip Controller:

/var/asr/gateway/private/

◆ Note

The keys and certificates must be in place on both controllers in a redundant system before you configure the SSL proxy or the web server will not start. You must do this manually, the configuration synchronization utilities do not perform this function.

Create an HTTP virtual server

After you configure the web server with the certificates and keys, the next step is to create a virtual server that references a pool that contains the HTTP servers for which the SSL Gateway will proxy connections. Note that before you create the HTTP virtual server, you must configure a pool that contains your HTTP servers. For more information about creating a pool, see *Defining pools*, on page 3-4.

Creating an HTTP virtual server in the F5 Configuration utility

1. Click Virtual Severs in the navigation pane.
   The Virtual Servers screen opens.
2. In the tool bar, click the **Add Virtual Server** button.
   The Add Virtual Server screen opens.

3. Add the attributes you want for the virtual server such as Address, Port, Unit ID (active-active only), and Interface.
4. In the Resources section, click **Pool**.
5. In the Pool list, select the pool of HTTP servers you want to use with the virtual server.
6. Click the **Apply** button.

Creating an HTTP virtual server from the command line

Note that before you create the HTTP virtual server, you must configure a pool that contains your HTTP servers. For more information about creating pool, see *Defining pools*, on page 3-4. After you have defined a pool that contains the HTTP servers, use the following syntax to create a virtual server that references the pool:

```
bigpipe vip <virt ip>:<port> use pool <pool_name>
```

For example, if you want to create a virtual server **20.1.1.1:80**, that references a pool of HTTP servers named **http_pool**, you could type the following command:

```
bigpipe vip 20.1.1.1:80 use pool http_pool
```

After you create the virtual server that references the pool of HTTP servers, you can create an SSL Gateway. The following section describes how to create an SSL Gateway.

Create an SSL Gateway

After you create the HTTP virtual server for which the SSL Gateway proxies connections, the next step is to create the SSL Proxy.

Creating an SSL Gateway in the F5 Configuration utility

1. Click Proxies in the navigation pane.
   This opens the Proxies screen.
2. In the toolbar, click the **Add Proxy** button.
   The Add Proxy screen opens.

3. In the **Proxy Address** box, type the IP address for the SSL Gateway.
4. In the **Proxy Netmask** box, type the netmask you want to use for this SSL Gateway. If you leave this setting blank, the BIG/ip Controller creates a default based on the network class of the IP address on the external (destination processing) interface. Type a user-defined netmask only if necessary.
5. In the **Proxy Broadcast** box, type the broadcast address you want to use for this SSL Gateway. The BIG/ip Controller automatically generates a broadcast address if you do not type one. Type a user-defined broadcast address only if necessary.
6. In the **Proxy Port** box, type the port number that the proxy server uses, or select a service from the list box. Note that if you select a service, the Configuration utility uses the default port number associated with that service.
7. In the **Unit ID** list, select the unit number you want to assign this SSL Gateway. Connections served by this SSL Gateway are managed by the controller assigned this unit ID. This only applies if this controller is running in active-active mode.
8. For **Interface**, select the destination processing interface on which you want to create the SSL Gateway. Select **default** to allow the F5 Configuration utility to select the interface based on the network address of the SSL Gateway. If you choose **None**, the BIG/ip Controller does not create an alias and generates no ARPs for the virtual IP address.
9. In the **Destination Address** box, type the IP address or host name of the node or virtual server to which the SSL Gateway maps. This should be the virtual server you created that references the pool of HTTP servers on your network that will respond to requests proxied by the SSL Gateway.
10. In the **Destination Port** box, type a port name or number, such as port 80 or http, or select the service name from the drop-down list.

11. In the **Destination Target** list, select the type of target to which the proxy sends connections. There are two options:
    - **External Node**
      Select External Node if the SSL Gateway proxies connections for an IP address of a server that resides on the network instead of a virtual server.
    - **Local Virtual Server**
      Select Local Virtual Server if the SSL Gateway proxies connections for a virtual server located on the BIG/ip Controller.
12. In the **SSL Certificate** box, type the name of the SSL certificate you installed on the BIG/ip Controller.
13. In the **SSL Key** box, type the name of the SSL key you installed on the BIG/ip Controller.
14. In the **Last Hop Pool** list, select the last hop pool that contains other network devices from which the BIG/ip Controller receives connections. This feature is optional. You only need to use this feature if the SSL Gateway is accepting connections from multiple network devices.
15. Click the **Apply** button.

Creating an SSL Gateway from the command line

Use the following command syntax to create an SSL Gateway. Use this syntax if you want to configure a proxy by specifying a bitmask instead of a netmask and broadcast address:

```
bigpipe proxy <ip>:<port> [/bitmask] [<ifname>] [<unit id>] target
   <server | vip> <ip>:<port> ssl enable key <key> cert <cert>
```

Use this syntax if you want to configure a proxy by specifying a netmask and broadcast address instead of a bitmask:

```
bigpipe proxy <ip>:<port> netmask <ip> [broadcast <ip>] [<ifname>]
   [<unit id>] target <server | vip> <ip>:<port> ssl enable key
   <key> cert <cert>
```

For example, you can create an SSL Gateway from the command line that looks like this:

```
bigpipe proxy 10.1.1.1:443 exp0 unit 1 { netmask 255.255.255.0
   broadcast 10.1.1.255 target vip 20.1.1.1:80 ssl enable key
   my_key cert my_certfile }
```

Note that when the configuration is written out in the **bigip.conf** file, the line **ssl enable** is automatically added. When the SSL Gateway is written in the **/etc/bigip.conf** file, it looks like this:

```
proxy 10.1.1.1:443 exp0 unit 1 {
    netmask 255.255.255.0
    broadcast 10.1.1.255
    target vip 20.1.1.1:80
    ssl enable
    key my_key
    cert my_certfile
}
```

Figure 4.3 *An example SSL Gateway configuration*

Enabling, disabling, or deleting an SSL Proxy

After you have created an SSL Gateway, you can enable, disable it, or delete it using the F5 Configuration utility or from the command line.

Enabling or disabling an SSL Gateway in the F5 Configuration utility

1. Click Proxies in the navigation pane.
   The Proxies screen opens.
2. In the Proxies list, select the SSL Gateway you want to enable or disable.
   The Proxy Properties screen opens.
3. In the Proxy Properties screen, clear the **Enable** box to disable the Proxy, or check the **Enable** box to enable the SSL Gateway.
4. Click the **Apply** button.

Deleting an SSL Gateway in the F5 Configuration utility

1. Click Proxies in the navigation pane.
   The Proxies screen opens.
2. In the Proxies list, select the SSL Gateway you want to delete.
   The Proxy Properties screen opens.
3. In the tool bar, click the **Delete** button.

Enabling, disabling, or deleting an SSL Gateway from the command line

You can enable, disable, or delete an SSL Gateway with the following syntax:

```
bigpipe proxy <ip>:<port> enable
bigpipe proxy <ip>:<port> disable
bigpipe proxy <ip>:<port> delete
```

For example, if you want to enable the SSL Gateway 209.100.19.22:443, type the following command:

```
bigpipe proxy 209.100.19.22:443 enable
```

For example, if you want to disable the SSL Gateway 209.100.19.22:443, type the following command:

```
bigpipe proxy 209.100.19.22:443 disable
```

For example, if you want to delete the SSL Gateway 209.100.19.22:443, type the following command:

```
bigpipe proxy 209.100.19.22:443 delete
```

Displaying configuration for an SSL Gateway from the command line

You can view the configuration information for an SSL Gateway in the from the command line with the show key word.

Displaying configuration information for an SSL Gateway from the command line

Use the following syntax to view the configuration for the specified SSL Gateway:

`bigpipe proxy <ip>:<port> show`

For example, if you want to view configuration information for the SSL Gateway 209.100.19.22:80, type the following command:

`bigpipe proxy 209.100.19.22:80 show`

```
SSL PROXY +---> 11.12.1.200:443 -- Originating Address -- Enabled   Unit 1
          |     Key File Name balvenie.scotch.net.key
          |     Cert File Name balvenie.scotch.net.cert
          |     LastHop Pool Name
          +===> 11.12.1.100:80 -- Destination Address -- Server


SSL PROXY +---> 11.12.1.120:443 -- Originating Address -- Enabled   Unit 1
          |     Key File Name balvenie.scotch.net.key
          |     Cert File Name balvenie.scotch.net.cert
          |     LastHop Pool Name
          +===> 11.12.1.111:80 -- Destination Address -- Vip
```

Figure 4.4 *Output from the* ***bigpipe proxy show*** *command*

Optional SSL Gateway configuration

Depending on your network configuration, the SSL Gateway may require additional configuration. For example, in cases where the BIG/ip Controller receives connections from several devices, such as routers or firewalls, you must configure a last hop pool for the SSL Gateway. The last hop pool must contain the IP addresses of the routers or firewalls from which the BIG/ip Controller receives connections.

Create a last hop pool that includes additional network devices

If the virtual server you configured for the SSL Gateway accepts connections from firewalls or routers in addition to SSL connections, you must configure a last hop pool for the SSL Gateway. This last hop pool must contain any other devices, such as firewalls or routers, through which connections are received by the BIG/ip Controller.

Creating a last hop pool with additional network devices in the F5 Configuration utility

1. Click Pools in the navigation pane.
   This opens the Pools screen.
2. In the toolbar, click the **Add Pool** button.
   The Add Pool screen opens.
3. In the **Pool Name** box, type in the name you want to use for the pool.
4. Click on the load balancing method list and select the load balancing method you want to use for this pool.
5. Use the resources options to add the devices from which the BIG/ip Controller receives connections. To add devices to the pool, type the IP address in the **Node Address** box, type the port number in the **Port** box, and then type in the ratio or priority for this node. Finally, to add the node to the list, click the add **(>>)** button.
   - **Node Address**
     Type in the IP addresses of routers or other devices from which the BIG/ip Controller receives connections.
   - **Port**
     Type in the port number of the port you want to use for this node in the pool.
   - **Ratio**
     Type in a number to assign a ratio to this node within the pool. For example, if you are using the ratio load

balancing method and you type a **1** in this box, the node will have a lower priority in the load-balancing pool than a node marked **2**.

- **Priority**
  Type in a number to assign a priority to this node within the pool. For example, if you are using a priority load-balancing method and you type a **1** in this box, the node will have a lower priority in the load-balancing pool than a node marked **2**.
- **Current Members**
  This is a list of the member nodes that are part of the load balancing pool.

6. Click the **Apply** button.

Creating a last hop pool with additional network devices from the command line

Use the following syntax to configure a last hop pool for the SSL Gateway that contains the additional network devices:

```
bigpipe pool <pool_name> {lb_mode <lb_mode_specification> member
   <member_definition>... <member_definition>}
```

For example, you might use the following command to create a last hop pool that contains the loopback device and two routers:

```
bigpipe pool ssllasthop_pool {lb_mode ratio_member member
   11.12.1.100:80 ratio 1 priority 1 member 11.12.1.101:80 ratio 1
   priority 1 11.12.1.102:80 ratio 1 priority 1}
```

After you create the last hop pool, you must modify the SSL Gateway so that it references the last hop pool. The next section describes how to do this with the F5 Configuration utility or from the command line.

Modify the SSL Gateway so that it references the last hop pool

After you create the last hop pool that contains other devices, such as firewalls or routers, you can reference it from the SSL Gateway either from the F5 Configuration utility, or from the command line.

Adding a last hop pool to an SSL Gateway in the F5 Configuration utility

1. Click Proxies in the navigation pane.
   The Proxies screen opens.
2. In the Proxies list, select the SSL Gateway to which you want to assign the last hop pool.
   The Proxy Properties screen opens.
3. In the Last Hop Pool list, select the last hop pool that contains additional network devices.
4. Click the **Apply** button.

Adding a last hop pool to an SSL Gateway from the command line

Use the following syntax to reference a last hop pool from an SSL Gateway:

```
bigpipe proxy <ip>:<port> lasthop pool <pool_name>
```

For example, if you want to assign the last hop pool named **ssllasthop_pool** to the SSL proxy **11.12.1.200:443**, type the following command:

```
bigpipe proxy 11.12.1.200:443 lasthop pool
   ssllasthop_pool
```