BIG-IP® e-Commerce Solutions Guide

version 4.5

MAN-0060-01

Legal Notices

Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described herein. F5 reserves the right to change specifications at any time without notice.

Trademarks

F5, F5 Networks, the F5 logo, BIG-IP, 3-DNS, iControl, GLOBAL-SITE, SEE-IT, EDGE-FX, FireGuard, Internet Control Architecture, and IP Application Switch are registered trademarks or trademarks of F5 Networks, Inc. in the U.S. and certain other countries. All other product and company names are registered trademarks or trademarks of their respective holders. F5 trademarks may not be used in connection with any product or service except as permitted in writing by F5.

Patents

This product protected by U.S. Patent 6,374,300; Pending U.S. Patent 20020040400. Other patents pending.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

Export Warning

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

FCC Compliance

This equipment generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules, which are designed to provide reasonable protection against such radio frequency interference.

Operation of this equipment in a residential area may cause interference, in which case the user at his own expense will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This class A digital apparatus complies with Canadian I CES-003.

Standards Compliance

The product conforms to ANSI/UL Std 1950 and Certified to CAN/CSA Std. C22.2 No. 950.

Acknowledgments

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at the Lawrence Berkeley Laboratory.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

Table of Contents

Introduction

1
Configuring an SSL Accelerator

Glossary

Index

Introduction

Getting started

Before you start installing the BIG-IP® system, we recommend that you browse the ***BIG-IP Solutions Guide*** and find the load balancing solution that most closely addresses your needs. If the BIG-IP unit is running the 3-DNS® software module, you may also want to browse the ***3-DNS Administrator Guide*** to find a wide area load balancing solution. Briefly review the basic configuration tasks and the few pieces of information, such as IP addresses and host names, that you should gather in preparation for completing the tasks.

Once you find your solution and gather the necessary network information, refer to the ***Configuration Worksheet*** and ***Platform Guide*** for hardware installation instructions, and then return to the ***BIG-IP Solutions Guide*** to follow the steps for setting up your chosen solution.

Choosing a configuration tool

The BIG-IP system offers both web-based and command line configuration tools, so that users can work in the environment that they are most comfortable with.

The Setup utility

All users need to use the Setup utility (formerly known as First-Time Boot utility). This utility walks you through the initial system set up. You can run the Setup utility from the command line, or from a web browser. The Setup utility prompts you to enter basic system information including a **root** password and the IP addresses that will be assigned to the network interfaces. For more information, see the ***BIG-IP Reference Guide***.

The Configuration utility

The Configuration utility is a web-based application that you use to configure and monitor the load balancing setup on the BIG-IP system. Once you complete the instructions for the Setup utility described in this guide, you can use the Configuration utility to perform additional configuration steps necessary for your chosen load balancing solution. In the Configuration utility, you can also monitor current system performance, and download administrative tools such as the SNMP MIBs or the SSH client. The Configuration utility requires Netscape Navigator version 4.7, or Microsoft Internet Explorer version 5.0 or 5.5.

The bigpipe and bigtop command line utilities

The **bigpipe**™ utility is the command line counter-part to the Configuration utility. Using **bigpipe** commands, you can configure virtual servers, open ports to network traffic, and configure a wide variety of features. To monitor the BIG-IP system, you can use certain **bigpipe** commands, or you can use the **bigtop**™ utility, which provides real-time system monitoring. You can use the command line utilities directly on the BIG-IP system console, or you can run commands using a remote shell, such as the SSH client or a Telnet client. For detailed information about the **bigpipe** command line syntax, see the ***BIG-IP Reference Guide***.

Using the Administrator Kit

The BIG-IP Administrator Kit provides all of the documentation you need in order to work with the BIG-IP system. The information is organized into the guides described below. The following printed documentation is included with the BIG-IP unit.

- **Configuration Worksheet**
  This worksheet provides you with a place to plan the basic configuration for the BIG-IP system.

The following guides are available in PDF format from the CD-ROM provided with the BIG-IP system. These guides are also available from the first Web page you see when you log in to the administrative web server on the BIG-IP system.

- **Platform Guide**
  This guide includes information about the BIG-IP unit. It also contains important environmental warnings.
- **BIG-IP Solutions Guide**
  This guide provides examples of common load balancing solutions. Before you begin installing the hardware, we recommend that you browse this guide to find the load balancing solution that works best for you.
- **BIG-IP Reference Guide**
  This guide provides detailed configuration information for the BIG-IP system. It also provides syntax information for **bigpipe** commands, other command line utilities, configuration files, system utilities, and monitoring and administration information.
- **3-DNS Administrator and Reference Guides**
  If your BIG-IP system includes the optional 3-DNS module, your administrator kit also includes manuals for using the 3-DNS module. The ***3-DNS Administrator Guide*** provides wide area load balancing solutions and general administrative information. The ***3-DNS Reference Guide*** provides information about configuration file syntax and system utilities specific to the 3-DNS module.
- **BIG-IP Link Controller Solutions Guide**
  This guide provides examples of common link load balancing solutions using the Link Controller. Before you begin installing the hardware, we recommend that you browse this guide to find the load balancing solution that works best for you.

Stylistic conventions

To help you easily identify and understand important information, our documentation consistently uses these stylistic conventions.

Using the solution examples

All examples in this documentation use only non-routable IP addresses. When you set up the solutions we describe, you must use IP addresses suitable to your own network in place of our sample addresses.

Identifying new terms

To help you identify sections where a term is defined, the term itself is shown in bold italic text. For example, a ***virtual server*** is a specific combination of a virtual address and virtual port, associated with a content site that is managed by a BIG-IP system or other type of host server.

Identifying references to objects, names, and commands

We apply bold text to a variety of items to help you easily pick them out of a block of text. These items include web addresses, IP addresses, utility names, and portions of commands, such as variables and keywords. For example, with the **bigpipe pool <pool_name> show** command, you can specify a specific pool to show by specifying a pool name for the **<pool_name>** variable.

Identifying references to other documents

We use italic text to denote a reference to another document. In references where we provide the name of a book as well as a specific chapter or section in the book, we show the book name in bold, italic text, and the chapter/section name in italic text to help quickly differentiate the two. For example, you can find information about **bigpipe** commands in the ***BIG-IP Reference Guide***.

Identifying command syntax

We show complete commands in bold Courier text. Note that we do not include the corresponding screen prompt, unless the command is shown in a figure that depicts an entire command line screen. For example, the following command shows the configuration of the specified pool name:

```
bigpipe pool <pool_name> show
```

or

```
b pool <pool_name> show
```

Table Intro.1 explains additional special conventions used in command line syntax.

Item in text	Description
\	Indicates that the command continues on the following line, and that users should type the entire command without typing a line break.
< >	Identifies a user-defined parameter. For example, if the command has **<your name>**, type in your name, but do not include the brackets.
|	Separates parts of a command.
[ ]	Indicates that syntax inside the brackets is optional.
...	Indicates that you can type a series of items.

Table Intro.1 *Command line syntax conventions*

Finding additional help and technical support resources

You can find additional technical information about this product in the following locations:

- **Release notes**
  Release notes for the current version of this product are available from the product web server home page, and are also available on the technical support site. The release notes contain the latest information for the current version, including a list of new features and enhancements, a list of fixes, and, in some cases, a list of known issues.
- **Online help**
  You can find help online in three different locations:
  - The web server on the product has PDF versions of the guides included in the Administrator Kit.
  - The web-based Configuration utility has online help for each screen. Simply click the **Help** button.
  - Individual **bigpipe** commands have online help, including command syntax and examples, in standard UNIX man page format. Simply type the command followed by the word **help**, and the BIG-IP system displays the syntax and usage associated with the command.
- **Third-party documentation for software add-ons**
  The BIG-IP distribution CD contains online documentation for all third-party software.

- **Technical support through the World Wide Web**
  The F5 Networks Technical Support web site, **http://tech.f5.com**, provides the latest technical notes, answers to frequently asked questions, updates for administrator guides (in PDF format), and the Ask F5 natural language question and answer engine.

◆ **Note**

All references to hardware platforms in this guide refer specifically to systems supplied by F5 Networks, Inc. If your hardware was supplied by another vendor and you have hardware-related questions, please refer to the documentation from that vendor.

What’s new in version 4.5

The BIG-IP system offers the following major new features in version 4.5, in addition to many smaller enhancements.

Enhanced support for managing SSL connections

This release includes several new features designed to further simplify the administration of SSL connections. These features include extensive web-based screens for centralized key management, and support for certificate revocation lists (CRLs).

Another new SSL feature is the ability for an SSL proxy to interoperate with an LDAP database to authorize users based on client certificates. This LDAP database can reside either locally on the BIG-IP system, or remotely on another server on your network.

Lastly, you can now limit the number of connections coming into an SSL proxy, for security or load balancing reasons.

For more information on managing SSL connections, see the ***BIG-IP Reference Guide***, Chapter 7, *SSL Accelerator Proxies*.

Easy system account creation

With this release, the BIG-IP system now offers a centralized Setup screen to set the passwords for the three system accounts: **root**, **admin**, and **support**. For the **support** account, you can also specify whether to allow command line access, Web access, or both.

For more information on managing user accounts, see the ***BIG-IP Reference Guide***, Chapter 15, *Administering the BIG-IP System*.

Security enhancements

You can now use the Setup utility to configure a remote LDAP or RADIUS authentication server. With this feature, you no longer need to directly edit configuration files to set up your LDAP or RADIUS authentication server. For more information about configuring remote authentication, see the ***BIG-IP Reference Guide***, Chapter 2, *Using the Setup Utility*.

Also, this release of the BIG-IP system expands the number of user roles that you can assign to user accounts for the purpose of user authorization. In addition to the standard Full Read/Write, Partial Read/Write, and Read-Only access levels, you can now choose from three additional access levels. These access levels define which of the three interfaces an administrator can use to access the BIG-IP system (the Configuration utility, the command line interface, or the iControl interface). These user authorization roles are stored in the local LDAP database on the BIG-IP system and are designed to operate in concert with centralized LDAP and RADIUS authentication. For more information on managing user accounts, see the ***BIG-IP Reference Guide***, Chapter 15, *Administering the BIG-IP System*.

Other useful security features in this release are intrusion detection and protection from denial-of-service attacks. This release includes two new features to assist in detecting network intruders--VLAN mirroring and clone pools. By enabling a clone pool, any traffic directed to a pool is automatically sent to a node within a replicated pool. The release also includes two new global variables to define high water and low water marks, for the adaptive reaping of connections. For more information VLAN mirroring and clone pools, see the ***BIG-IP Reference Guide***, Chapter 3, *Post-Setup Tasks*, *VLANs*, and Chapter 4, *Pools*.

Universal Inspection Engine

The Universal Inspection Engine (UIE) allows you to apply business decisions to applications and web servics, and provides granular control for switching, persistence, and application level security. The BIG-IP system version 4.5 has the ability to read all HTTP or TCP content.

- **Universal content switching**
  Through a number of new rule elements, such as a set of functions and the variables **http_content** and **tcp_content**, you can now write expressions within rules that search not only HTTP headers, but also HTTP and TCP data content to make load balancing decisions. As part of the new iRules syntax, these new variables and functions significantly enhance your ability to select the pools that most suit your traffic management needs.

- **Universal persistence**
  Universal persistence allows you to persist on any string within a packet, or persist directly on a specific pool member. You can enable universal persistence by including rules-syntax expressions within a pool definition. In this way, a pool can perfom load-balancing operations such as sending traffic to a specific node within the pool, or load-balancing traffic based on any string or node that you define. Furthermore, the rules syntax has been expanded to allow rules to intelligently persist requests to cache servers based on more granular information in a request.

Universal persistence is particularly useful for persisting HTTP or TCP content that is unique to your application. Examples of universal persistence are for i-mode phone users, and for working with BEA Weblogic servers by creating persistence maps on BEA Weblogic identifiers. For more information about the Universal Inspection Engine and iRules, see the ***BIG-IP Reference Guide***, Chapter 5, *iRules*.

Other rule enhancements

In addition to the new rule functions and variables designed for universal content switching, the rules syntax has been further expanded to include two new rule statements, **log** and **accumulate**.

Furthermore, you can now store your class lists externally instead of within the **bigip.conf** file. Storing your class lists externally improves performance and allows for incremental updates to those lists. To support this feature, you can store external class lists using either the Configuration utility or the iControl interface. For more information about these new functions, see the ***BIG-IP Reference Guide***, Chapter 5, *iRules*.

Enhanced support for global variables

A number of new global variables are included in this release, such as variables that define high water and low water marks for the adaptive reaping of connections to prevent denial-of-service attacks. Also, the Configuration utility now shows all global variables and presents them in categories, according to function. For more information about these global variables, see the ***BIG-IP Reference Guide***, Appendix A, *bigpipe Command Syntax*.

RealServer plug-in for UNIX systems

With this release comes support for RealSystem® Server systems running on the UNIX operating system. This feature provides the ability to dynamically load balance and monitor UNIX systems that are running the RealSystem® Server application. Once you have compiled and installed the plug-in, you can set up your pool for dynamic load balancing, and create a health monitor to monitor the traffic load on the RealSystem® Server system. For more information about the RealSystem Server plug-in, see the ***BIG-IP Reference Guide***, Chapter 11, *Monitors*.

New health monitor features

This release includes a new EAV health monitor, **udp**, which allows you to check the status of UDP connections. Also, the **reverse** attribute, which marks a node as **down** based on a received string, is now available for the **https** and **https_443** monitors. For more information about these monitors, see the ***BIG-IP Reference Guide***, Chapter 11, *Monitors*.

Other load balancing enhancements

This release includes several new load balancing features, including enhanced administration of load-balanced connections. For example, through the Configuration utility, **bigpipe** command, or **bigapi**, you can now dump connections verbosely, or configure a timeout for idle HTTP connections. Also, by writing rule-type expressions within pool definitions, you can cause a pool to send a connection directly to one of its pool members. For more information these features, see the ***BIG-IP Reference Guide***, Chapter 5, *iRules* and Chapter 4, *Pools*.

Support for Link Controller

This release of the BIG-IP system includes an add-on Link Controller module for all BIG-IP HA systems. This module includes such features as support for single routers with multiple IP addresses and uplinks, full duplex billing support, and support for multiple outbound router pools. Also included is a significantly enhanced Web user interface, designed to ease basic link-controller configuration steps and provide more detailed statistics information.

Learning more about the BIG-IP product family

The BIG-IP platform offers many different software systems. These systems can be stand-alone, or can run in redundant pairs, with the exception of the BIG-IP e-Commerce Controller, which is only available as a stand-alone system. You can easily upgrade from any special-purpose BIG-IP system to the BIG-IP HA software, which supports all BIG-IP features.

- **The BIG-IP system**
  The complete version of the BIG-IP software provides the full suite of local area load balancing functionality. The BIG-IP unit also has an optional 3-DNS software module which supports wide-area load balancing.

- **The BIG-IP Link Controller**
  The BIG-IP Link Controller uses metrics and thresholds to manage inbound and outbound traffic through multiple gateways (routers) and Internet Service Providers (ISPs).

- **The BIG-IP e-Commerce Controller**
  The BIG-IP e-Commerce Controller uses SSL acceleration technology to increase the speed and reliability of the secure connections that drive e-commerce sites.

- **The BIG-IP special purpose products**
  The special purpose BIG-IP system provides the ability to choose from three different BIG-IP feature sets. When you run the Setup utility, you specify one of three types:

  - **The BIG-IP Load Balancer**
    The BIG-IP Load Balancer provides basic load balancing features.

  - **The BIG-IP FireGuard**
    The BIG-IP FireGuard provides load balancing features that maximize the efficiency and performance of a group of firewalls.

  - **The BIG-IP Cache Controller**
    The BIG-IP Cache Controller uses content-aware traffic direction to maximize the efficiency and performance of a group of cache servers.

Additional resources

You can find additional technical information about this product in the following resources:

- **CD**
  You can download additional documentation such as the ***BIG-IP Reference Guide*** and the ***BIG-IP Solutions Guide***.

- **Release notes**
  Release notes for the current version of this product are available from the product web server home page, and are also available on the technical support site. The release notes contain the latest information for the current version, including a list of new features and enhancements, a list of fixes, and, in some cases, a list of known issues.

- **Online help**
  You can find help online in three different locations:

  - The web server on the product has PDF versions of the guides included on the Software and Documentation CD.
  - The web-based Configuration utility has online help for each screen. Simply click the **Help** button.
  - Individual **bigpipe** commands have online help, including command syntax and examples, in standard UNIX man page format. Simply type the command followed by the word **help**, and the BIG-IP software displays the syntax and usage associated with the command.

- **Third-party documentation for software add-ons**
  The Product and Documentation CD contains online documentation for all third-party software, such as the Advanced Routing Modules.

- **Technical support through the World Wide Web**
  The F5 Networks Technical Support web site, **http://tech.f5.com**, provides the latest technical notes, answers to frequently asked questions, updates for administrator guides (in PDF format), and the Ask F5 natural language question and answer engine. To access this site, you need to register at **http://tech.f5.com**.

1

Configuring an SSL Accelerator

- Introducing the SSL Accelerator
- Configuring the SSL Accelerator
- Introducing the SSL Accelerator scalable configuration
- Using SSL-to-server
- Additional configuration options

Introducing the SSL Accelerator

The SSL Accelerator feature allows the BIG-IP system to accept HTTPS connections (HTTP over SSL), connect to a web server, retrieve the page, and then send the page to the client.

A key component of the SSL Accelerator feature is that the BIG-IP system can retrieve the web page using an unencrypted HTTP request to the content server. With the SSL Accelerator feature, you can configure an SSL proxy on the BIG-IP system that decrypts HTTP requests that are encrypted with SSL. Decrypting the request offloads SSL processing from the servers to the BIG-IP system and also allows the BIG-IP system to use the header of the HTTP request to intelligently control how the request is handled. (Requests to the servers can optionally be re-encrypted to maintain security on the server side of the BIG-IP system as well, using a feature called SSL-to-server.)

When the SSL proxy on the BIG-IP system connects to the content server, and address translation is not enabled, the proxy uses the original client's IP address and port as its source address and port. In doing so, the proxy appears to be the client, for logging purposes.

This chapter describes the following features of the BIG-IP SSL Accelerator:

- Configuring an SSL Accelerator
- Using an SSL Accelerator scalable configuration
- Using SSL-to-server

◆ **Note**

If you have FIPS-140 security modules installed in the BIG-IP system, you must initialize the security world before you configure the SSL Accelerator for encrypted traffic. For more information, see the ***Platform Guide: 520/540****, available on the Software and Documentation CD.*

◆ **Note**

All products except the BIG-IP LoadBalancer, BIG-IP FireGuard Controller, and the BIG-IP Cache Controller support this configuration.

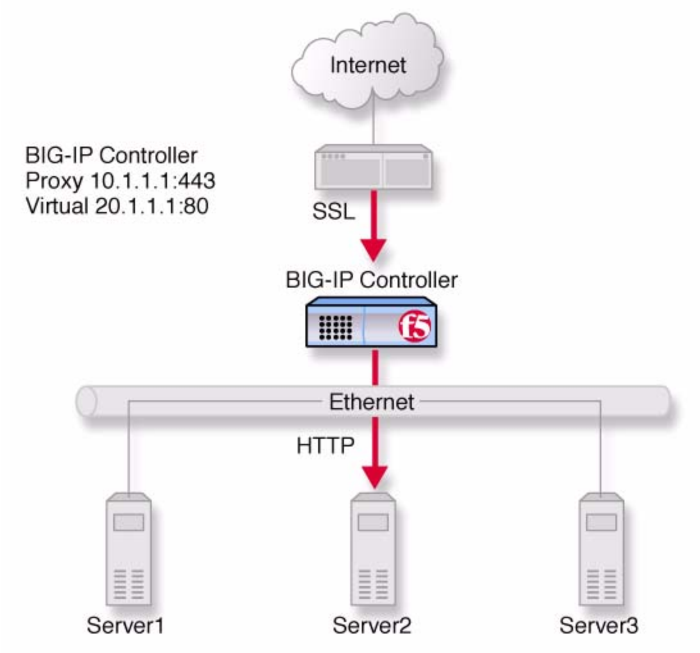

Figure 1.1 *An incoming SSL connection received by an SSL Accelerator configured on the BIG-IP system*

Configuring the SSL Accelerator

There are several tasks required to set up the SSL Accelerator on the BIG-IP system. These tasks include:

- Generating a key and obtaining a certificate
- Configuring the BIG-IP system with the certificate and key
- Creating the proxy for the SSL Accelerator

Generating a key and obtaining a certificate

In order to use the SSL Accelerator feature, you must obtain a valid x509 certificate from an authorized certificate authority (CA).

◆ **Note**

*If you have FIPS-140 hardware installed in the BIG-IP system, see the **Platform Guide: 520/540**, **Configuring the Security World on BIG-IP** on the product and documentation CD for instructions on how to generate a key and obtain a certificate.*

The following list contains some companies that are certificate authorities:

- Verisign (**http://www.verisign.com**)
- Digital Signature Trust Company (**http://secure.digsigtrust.com**)
- GlobalSign (**http://www.globalsign.com**)
- GTE Cybertrust (**http://www.cybertrust.gte.com**)
- Entrust (**http://www.entrust.net**)

You can generate a key, a temporary certificate, and a certificate request form using either the Key Management System (KMS) within the Configuration utility, or the **bigpipe proxy** command.

Note that we recommend using the Configuration utility for this process. The certification process is generally handled through a web page. Parts of the process require you to cut and paste information from a browser window in the Configuration utility to another browser window on the web site of the CA.

Additional information about keys and certificates

You must have a separate certificate for each domain name on each BIG-IP system or pair of BIG-IP units in a redundant system, regardless of how many non-SSL web servers are load balanced by the BIG-IP system.

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

Generating a key and obtaining a certificate using the Configuration utility

To obtain a valid certificate, you must have a private key. If you do not have a key, you can use the Configuration utility on the BIG-IP system to generate a key and a temporary certificate. You can also use the Configuration utility to create a request file you can submit to a certificate authority (CA). You must complete three tasks in the Configuration utility to create a key and generate a certificate request.

- Generate a certificate request
- Submit the certificate request to a CA and generate a temporary certificate
- Install the SSL certificate from the CA

Each of these tasks is described in detail in the following paragraphs.

To create a new certificate request using the Configuration utility

1. In the navigation pane, click **Proxies**.
   The Proxies screen opens.

2. Click the Cert Admin tab.

3. Click the **Generate New Key Pair/Certificate Request** button.

4. In the **Key Information** section, select a key length, and specifya key file name.

   - **Key Length**
     Select the key length you want to use for the key. You can choose **512**, **1024, 2048** or **4096** bits.

   - **Key Identifier**
     Type in the name of the key file. This should be the fully qualified domain name of the server for which you want to request a certificate. You must add the **.key** file extension to the name.

5. In the **Certificate Information** section, type the information specific to your company. This information includes:

   - **Country**
     Type the two letter ISO code for your country, or select it from the list. For example, the two-letter code for the United States is **US**.

- **State or Province**
  Type the full name of your state or province, or select it from the list. You must enter a state or province.
- **Locality**
  Type the city or town name.
- **Organization**
  Type the name of your organization.
- **Organizational Unit**
  Type the division name or organizational unit.
- **Domain Name**
  Type the name of the domain upon which the server is installed.
- **Email Address**
  Type the email address of a person who can be contacted about this certificate.
- **Challenge Password**
  Type the password you want to use as the challenge password for this certificate. The CA uses the challenge password to verify any changes you make to the certificate at a later date.
- **Retype Password**
  Retype the password you entered for the challenge password.

6. Click the **Generate Key Pair/Certificate Request** button.
   After a short pause, the Generate Certificate Request screen opens.
7. Use the Generate Certificate Request screen to start the process of obtaining a certificate from a CA, and then to generate and install a temporary certificate.
   - **Begin the process for obtaining a certificate from CA**
     Click the URL of a CA to begin the process of obtaining a certificate for the server. After you select a CA, follow the directions on their web site to submit the certificate request. After your certificate request is approved, and you receive a certificate back from the CA, see *Installing certificates from the certificate authority (CA)*, on page 1-8, for information about installing it on the BIG-IP system.
   - **Generate and install a temporary certificate**
     Click the **Generate Self-Signed Certificate** button to create a self-signed certificate for the server. We recommend that you use the temporary certificate for testing only. You should take your site live only after you receive a properly-signed certificate from a certificate authority. When you click this button, a temporary certificate is created and installed on the BIG-IP system. This certificate is valid for 10 years. This temporary certificate allows you to set up an SSL proxy for the SSL Accelerator while you wait for a CA to return a permanent certificate.

Generating a key and obtaining a certificate from the command line

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 system to generate a key and a temporary certificate. The **genkey** and **gencert** utilities automatically generate a request file that you can submit to a certificate 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 10-year certificate for testing the SSL Accelerator on the BIG-IP system. This utility also creates a request file that you can submit to a certificate 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 Accelerator.

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 with the following commands:

```
/usr/local/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. Note that this FQDN must be RFC1034/1035-compliant, and cannot be more than 63 characters long (this is an x509 limitation).
- 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

As an example, Figure 1.2 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 1.2 *Example entries for the **genconf** utility*

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 to run the **genkey** utility:

```
/usr/local/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 certificate request form is created in the following directory:

/config/bigconfig/ssl.csr/<fqdn>.csr

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

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

/config/bigconfig/ssl.crt/<fqdn>.crt

The **<fqdn>** is the fully qualified domain name of the server.

Note that the keys and certificates are copied to the other BIG-IP system in a redundant system when you synchronize the configurations. For more information about synchronizing configurations, see the ***BIG-IP Reference Guide***, Chapter 13, *Configuring a Redundant System*.

This temporary certificate is good for ten years, but for an SSL proxy you should have a valid certificate from your CA.

◆ **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 using the gencert utility

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

/config/bigconfig/ssl.key/

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

```
/usr/local/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 certificate request form is created in the following directory:

/config/bigconfig/ssl.crt/<fqdn>.csr

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

Installing certificates from the certificate authority (CA)

After you obtain a valid x509 certificate from a certificate authority (CA) for the SSL Accelerator, you must copy it onto each BIG-IP system in the redundant configuration. You can configure the accelerator with certificates using the Configuration utility or from the command line.

To install certificates from the CA using the Configuration utility

1. In the navigation pane, click **Proxies**.
   The Proxies screen opens.
2. Click the Cert Admin tab.
3. In the Key List column, locate the key pair for which you want to install a certificate.
4. In the Certificate ID column, click the name of the certificate you want to install.
   This displays the properties of that certificate.
5. Click the **Install Certificate** button
6. Provide the requested information for either Option 1 or Option 2.
7. Click the **Install Certificate** button.

Figure 1.3 shows an example of a certificate..

```
-----BEGIN CERTIFICATE-----
MIIB1DCCAX4CAQAwDQYJKoZIhvcNAQEEBQAwdTELMAkGA1UEBhMCVVMxCzAJBgNV
BAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMRQwEgYDVQQKEwtGNSBOZXR3b3JrczEc
MBoGA1UECxMTUHJvZHVjdCBEZXZlbG9wbWVudDETMBEGA1UEAxMKc2VydmVyLm5l
dDAeFw0wMDA0MTkxNjMxNTlaFw0wMDA1MTkxNjMxNTlaMHUxCzAJBgNVBAYTAlVT
MQswCQYDVQQIEwJXQTEQMA4GA1UEBxMHU2VhdHRsZTEUMBIGA1UEChMLRjUgTmV0
d29ya3MxHDAaBgNVBAsTE1Byb2R1Y3QgRGV2ZWxvcG1lbnQxEzARBgNVBAMTCnNl
cnZlci5uZXQwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAsfCFXq3Jt+FevxUqBZ9T
Z7nHx9uaF5x9V5xMZYgekjc+LrF/yazhmq4PCxrws3gvJmgpTsh50YJrhJgfs2bE
gwIDAQABMA0GCSqGSIb3DQEBBAUAA0EAd1q6+u/aMaM2qdo7EjWx14TYQQGomYoq
eydlzb/3FOiJAynDXnGnSt+CVvyRXtvmG7V8xJamzkyEpZd4iLacLQ==
-----END CERTIFICATE-----
```

Figure 1.3 *An example of a certificate*

To install certificates from the CA from the command line

Copy the certificate into the following directory on each BIG-IP system in a redundant system:

/config/bigconfig/ssl.crt/

◆ **Note**

*The certificate you receive from the certificate 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 system:

/config/bigconfig/ssl.key/

◆ **WARNING**

*In a redundant system, the keys and certificates must be in place on both BIG-IP units before you configure the SSL Accelerator. To do this you must synchronize the configurations in the redundant system. For details, see the **BIG-IP Reference Guide**,* Chapter 13, ***Configuring a Redundant System***.

Creating an SSL proxy

After you create the HTTP virtual server for which the SSL Accelerator handles connections, the next step is to create a client-side SSL proxy. This section also contains information about managing an SSL proxy.

To create an SSL proxy using the Configuration utility

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

3. In the Add Proxy screen, configure the attributes you want to use with the proxy. For additional information about configuring a proxy, click the **Help** button.

To create an SSL proxy from the command line

Use the following command syntax to create an SSL proxy:

```
b proxy <ip>:<service> \
target <server | virtual> <ip>:<service> \
clientssl enable \
clientssl key <clientssl_key> \
clientssl cert <clientssl_cert>
```

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

```
b proxy 10.1.1.1:443 \
target virtual 20.1.1.10:80 \
clientssl enable \
clientssl key my.server.net.key \
clientssl cert my.server.net.crt
```

Introducing the SSL Accelerator scalable configuration

This section explains how to set up a scalable one-armed SSL Accelerator configuration. This configuration is useful for any enterprise that handles a large amount of encrypted traffic.

With this configuration, you can easily add BIG-IP e-Commerce Controllers to keep up with expanding SSL content, or a growing array of SSL content servers without adding more BIG-IP units.

Figure 1.4 shows a scalable configuration. The configuration includes a BIG-IP system; the BIG-IP e-Commerce Controllers **Accelerator1**, **Accelerator2**, **Accelerator3**, and **Accelerator4**; and the server array **Server1, Server2, Server3,** and **Server4**.

The following sections refer to Figure 1.4 as an example of how you can set up such a configuration.

◆ **Note**

The IP addresses shown in these configurations are examples only. When implementing your configuration, choose IP addresses that are consistent with your network or networks.

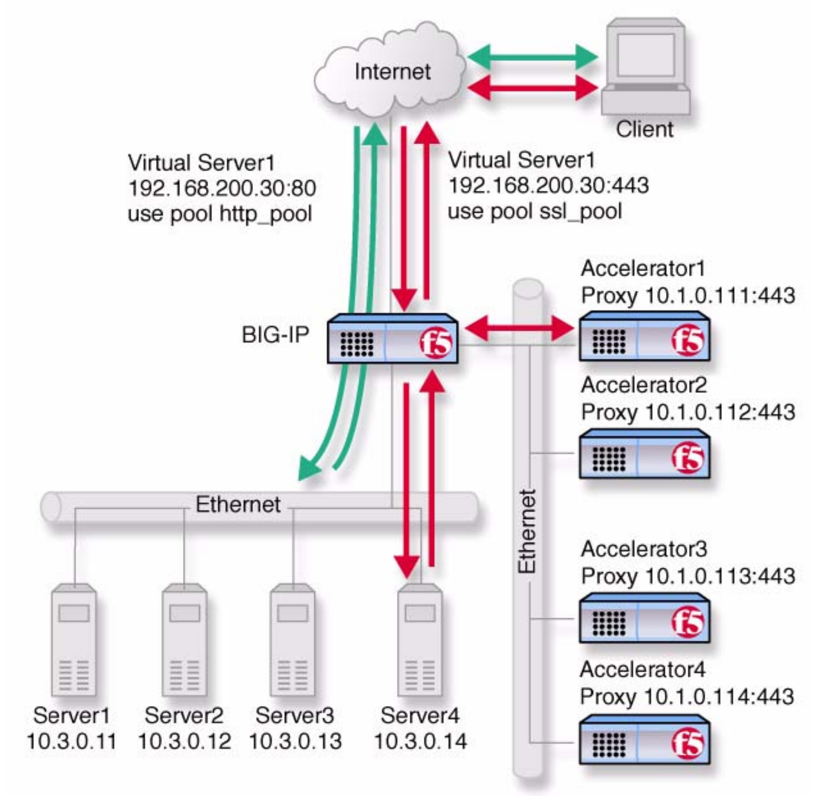

***Figure 1.4** An SSL Accelerator scalable configuration*

Creating the scalable e-Commerce Controller configuration

To implement the scalable configuration, you must configure the BIG-IP system that load balances the servers and e-Commerce Controllers, each e-Commerce Controller, and each node that handles connections from the e-Commerce Controller.

First, complete the following tasks on the BIG-IP system that you want to use to load balance connections to the e-Commerce Controllers:

- **Create two load balancing pools**
  One pool load balances HTTP connections using the IP addresses of the web servers, the other pool load balances SSL connections to the e-Commerce Controllers.

- **Create virtual servers**
  Create virtual servers that reference the load balancing pools. Create one virtual server for the pool load balancing the SSL connections to the accelerators, and another virtual server for the pool that load balances the HTTP connections to the servers. Disable external VLAN for the HTTP virtual server to prevent clients from making a direct connection, bypassing the e-Commerce Controllers.

- **Enable service 80 and service 443**
  Enable service **80** and service **443** on the BIG-IP system.
- **Set the idle connection timer**
  Set the idle connection timer for service **443**.

Next, complete the following tasks for the e-Commerce Controllers:

- **Set up SSL proxies**
  Set up an SSL proxy for each accelerator
- **Enable service 443**
  Enable service **443** for encrypted traffic.

Configuring the BIG-IP system that load balances the e-Commerce Controllers

To configure the BIG-IP system that load balances the e-Commerce Controllers, complete the following tasks on the BIG-IP system. This section describes how to complete each task.

- Create two load balancing pools. One pool load balances HTTP connections using the IP addresses of the web servers, the other pool load balances SSL connections from the e-Commerce Controller proxies.
- Create virtual servers that reference the load balancing pools.
- Enable port **80** and port **443** on the BIG-IP system.

Creating load balancing pools

You need to create two pools, a pool to load balance connections using the IP addresses of the content server nodes and a pool to load balance the SSL proxys.

To create the pools using the Configuration utility

1. In the navigation pane, click **Pools**.
   The Pools screen opens.
2. Click the **Add** button.
   The Add Pool screen opens.
3. For each pool, enter the pool name and member addresses in the Add Pool screen. (For additional information about configuring a pool, click the **Help** button.)

   Configuration notes

   *For this example, create an HTTP pool named **http_virtual**. This pool contains the following members:*
   Server1 (10.3.0.11)

Server2 (10.3.0.12)
Server3 (10.3.0.13)
Server4 (10.3.0.14)

*For this example, you could create an e-Commerce Controller pool named **ssl_proxys**. This pool contains the following members:*
accelerator1 (10.1.0.111)
accelerator2 (10.1.0.112)
accelerator3 (10.1.0.113)
accelerator4 (10.1.0.114)

To define a pool from the command line

To define a pool from the command line, use the following syntax:

```
b pool <pool_name> { member <member_definition> ...  member <member_definition>}
```

For example, if you want to create the pool **http_virtual** and the pool **ssl_proxys**, you would type the following commands:

```
b pool http_virtual { \
member 10.3.0.11:80 \
member 10.3.0.12:80 \
member 10.3.0.13:80 \
member 10.3.0.14:80 }
```

```
b pool ssl_proxys { \
member 10.1.0.111:443 \
member 10.1.0.112:443 \
member 10.1.0.113:443 \
member 10.1.0.114:443 }
```

Creating the virtual servers

Create a virtual server that references the pool that is load balancing the SSL connections, and another virtual server that references the pool that load balances the HTTP connections through the e-Commerce Controller proxies.

To define a standard virtual server that references a pool using the Configuration utility

1. In the navigation pane, click **Virtual Servers**.
2. Click the **Add** button.
   The Add Virtual Server screen opens.
3. For each virtual server, enter the virtual server address and pool name. (For additional information about configuring a virtual server, click the **Help** button.)

Configuration notes

*To create the configuration described in Figure 1.4, create a virtual server **192.168.200.30** on port **443** that references the pool of e-Commerce Controllers.*

*To create the configuration described in Figure 1.4, create a virtual server **192.168.200.30** on port **80** that references the pool of content servers.*

To define the virtual servers from the command line

To define a standard virtual server from the command line, use the following syntax:

```
b virtual <virt_IP>:<service> use pool <pool_name>
```

Note that you can use host names in place of IP addresses, and that you can use standard service names in place of port numbers.

To create the virtual servers for the configuration in Figure 1.4, you type the following commands:

```
b virtual 192.168.200.30:443 use pool ssl_proxys
b virtual 192.168.200.30:80 use pool http_virtual \
vlans external disable
```

Enabling ports 80 and 443 on the BIG-IP system

For security reasons, the BIG-IP ports do not accept traffic until you enable them. In this configuration, the BIG-IP system accepts traffic on port **443** for SSL, and on port **80** for HTTP. For this configuration to work, you must enable port **80** and port **443**.

Use the following command to enable these ports:

```
b service 80 443 tcp enable
```

Setting the idle connection timer for port 443

In this configuration, you should set the idle connection timer to clean up closed connections on port **443**. You need to set an appropriate idle connection time-out value, in seconds, so that valid connections are not disconnected, and closed connections are cleaned up in a reasonable time.

To set the idle connection timeout using the Configuration utility

1. In the navigation pane, click **Virtual Servers**.
2. In the Virtual Servers list, click the virtual server you configured for SSL connections.
   The Virtual Server Properties screen opens.
3. Click the Virtual Service Properties tab.
   The Virtual Service Properties screen opens.

4. In the **Idle connection timeout TCP (seconds)** box, type a timeout value for TCP connections. You can use the default setting of **1005**, unless you are creating a client-side SSL proxy, in which case you should specify a value of **10**.
5. Click **Apply**.

To set the idle connection time-out from the command line

To set the idle connection time-out, type the following command:

```
b service <service> timeout tcp <timeout>
```

The **<timeout>** value is the number of seconds a connection is allowed to remain idle before it is terminated. You can use the default setting of **1005**, unless you are creating a client-side SSL proxy, in which case you should specify a value of **10**.

The **<service>** value is the port on the wildcard virtual server for which you are configuring out-of-path routing.

Configuring the e-Commerce Controllers

The next step in the process is to configure the e-Commerce Controllers. Complete the following tasks on each e-Commerce Controller:

- Set up an SSL proxy for each e-Commerce Controller
- Enable port 443
- Set the idle connection timer for port 443

Setting up an SSL proxy for each e-Commerce Controller

The first task you must complete on the e-Commerce Controller is to set up a client-side proxy for each e-Commerce Controller with the HTTP virtual server as target server.

To create an SSL proxy using the Configuration utility

1. In the navigation pane, click **Proxies**.
   The Proxies screen opens.
2. Click the **Add** button.
   The Add Proxy screen opens.
3. In the **Proxy Type** section, click the **SSL** check box.
4. In the Add Proxy screen, configure the attributes you want to use with the proxy. For additional information about configuring a Proxy, click the **Help** button or see the ***BIG-IP Reference Guide***.

Configuration note

*For this example, create the following proxies on **Accelerator1**, **Accelerator2**, **Accelerator3**, and **Accelerator4**, respectively: **10.1.0.111:443**, **10.1.0.112:443**, **10.1.0.113:443**, and **10.1.0.114:443**.*

To create an SSL proxy from the command line

Use the following command syntax to create an SSL proxy:

```
b proxy <ip>:<service> target server <ip>:<service> clientssl enable clientssl key
    <clientssl_key> clientssl cert <clientssl_cert>
```

For example, to create the SSL proxys **accelerator1**, **accelerator2**, **accelerator3** and **accelerator4**, you use the following commands on these four e-Commerce Controllers, respectively. Note that the target for each proxy is the HTTP virtual server **192.168.200.30:80**.

For **accelerator1**, type the following command:

```
b proxy 10.1.0.111:443 \
target server 192.168.200.30:80 \
clientssl enable \
clientssl key my.server.net.key \
clientssl cert my.server.net.crt
```

In this example, to complete the configuration for **accelerator2**, type the following command:

```
b proxy 10.1.0.112:443 \
target server 192.168.200.30:80 \
clientssl enable \
clientssl key my.server.net.key \
clientssl cert my.server.net.crt
```

In this example, to complete the configuration for **accelerator3**, type the following command:

```
b proxy 10.1.0.113:443 \
target server 192.168.200.30:80 \
clientssl enable \
clientssl key my.server.net.key \
clientssl cert my.server.net.crt
```

In this example, to complete the configuration for **accelerator4**, type the following command:

```
b proxy 10.1.0.114:443 \
target server 192.168.200.30:80 \
clientssl enable \
clientssl key my.server.net.key \
clientssl cert my.server.net.crt
```

Enabling port 443

For security reasons, the ports on the e-Commerce Controllers do not accept traffic until you enable them. In this configuration, the e-Commerce Controller accepts traffic on port **443** for SSL. For this configuration to work, you must enable port **443**. Use the following command to enable this port:

```
b service 443 tcp enable
```

Using SSL-to-server

As described so far, SSL acceleration offloads SSL from the server to the BIG-IP system. In some situations, security requirements demand that traffic on the internal VLAN (that is, behind the virtual server) be encrypted as well, or more exactly, re-encrypted. This server-side re-encryption requires that the servers handle the final SSL processing, but SSL acceleration is still obtained because the process is faster than allowing SSL client connections directly to the servers. (This is because session keys are re-used and because more efficient ciphers are used for the server-side SSL connections.) Figure 1.5 shows the e-Commerce Controller configuration of Figure 1.1 with SSL-to-server added. Note that the only diagrammatic difference is that both client-side and server-side traffic are now labeled **SSL**, and the virtual server is now configured for service **443**.

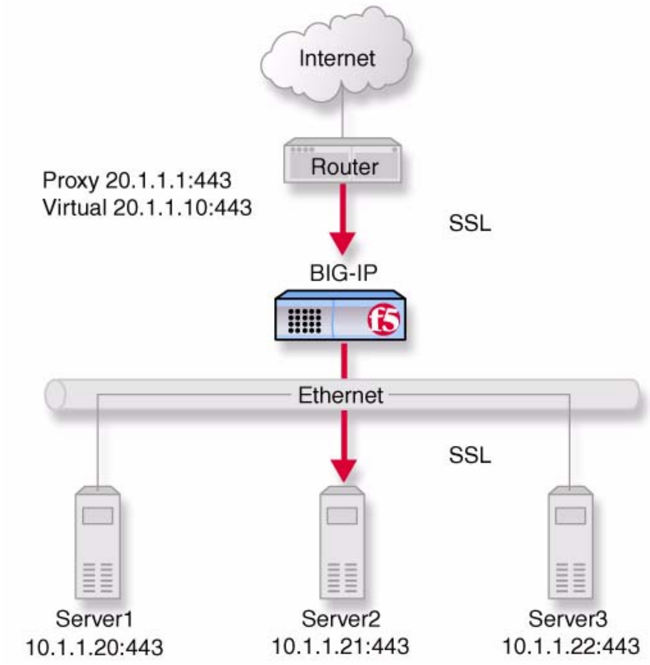

Figure 1.5 *An incoming SSL connection with SSL-to-server*

Configuring an e-Commerce Controller with SSL-to-server

Since SSL-to-server is typically used together with standard, client-side SSL acceleration, configuring SSL-to-server involves the same tasks used in the preceding solutions (*Configuring the SSL Accelerator*, on page 1-3 and *Introducing the SSL Accelerator scalable configuration*, on page 1-11), with the following exceptions:

- The servers must be equipped and enabled for SSL processing.

- In most cases, you will want to configure the server pool and virtual server as HTTPS rather than HTTP and change the proxy targets accordingly.
- For the proxy or proxies, you must enable server-side SSL.

Optionally, you may configure a second certificate on the proxy to authenticate it to the servers as a trusted client.

◆ **Note**

Enabling the SSL-to-Server feature without enabling a client-side SSL proxy is not recommended.

Configuring a server pool and virtual server for HTTPS

To configure the server pool and virtual server for HTTPS for the non-scalable configuration, simply perform the steps in *Creating an SSL proxy*, on page 1-9, only rename the pool **https_pool** and substitute service **443** for service **80** for both the nodes and for the virtual server. (Also, give the virtual server a different IP address.) If you use the command line, you accomplish these tasks as follows:

```
b pool https_pool { \
member 10.1.1.20:443 \
member 10.1.1.21:443 \
member 10.1.1.22:443 }
b virtual 20.1.1.1:443 use pool https_pool
```

To configure the server pool members and virtual server for HTTPS for the scalable configuration, perform the steps in *Creating load balancing pools*, on page 1-13, only rename the pool **https_virtual** and substitute service **443** for service **80** for all nodes and for the virtual server. If you use the command line, you accomplish these tasks as follows:

```
b pool https_virtual { \
member 10.3.0.11:443 \
member 10.3.0.12:443 \
member 10.3.0.13:443 \
member 10.3.0.14:443 }

b pool ssl_proxys { \
member 10.1.0.111:443 \
member 10.1.0.112:443 \
member 10.1.0.113:443 \
member 10.1.0.114:443 }

b virtual 192.168.200.30:443 use pool ssl_proxys
b virtual 192.168.200.40:443 use pool https_virtual
```

Configuring the proxy for server-side SSL

To configure the proxy for server-side SSL for the non-scalable configuration, perform the steps in *Creating an SSL proxy*, on page 1-9, specifying the **serverssl enable** attribute in addition to the **clientssl enable** attribute. Also, when specifying the target virtual server, we recommend that you configure the target virtual server as HTTPS instead of HTTP. If you use the command line, you accomplish these tasks as follows:

```
b proxy 20.1.1.1:443 \
target virtual 20.1.1.10:443 \
clientssl enable  \
clientssl key my.server.net.key \
clientssl cert my.server.net.crt \
serverssl enable
```

Optionally, you may specify a key file and a certificate file for the proxy as a client. This is done as follows:

```
b proxy 20.1.1.1:443 \
target virtual 20.1.1.10:443 \
clientssl enable \
clientssl key my.server.net.key \
clientssl cert my.server.net.crt \
serverssl enable \
serverssl key my.client.net.key \
serverssl cert my.client.net.key
```

Additional configuration options

Whenever a BIG-IP system is configured, you have a number of options:

- When you create an SSL proxy, you have a number of options that you can configure. Refer to Chapter 7, *SSL Accelerator Proxies*, in the ***BIG-IP Reference Guide***.
- You have the option in all configurations to configure a BIG-IP redundant system for fail-over. Refer to Chapter 13, *Configuring a Redundant System,* in the ***BIG-IP Reference Guide***.
- All configurations have health monitoring options. Refer to Chapter 11, *Monitors,* in the ***BIG-IP Reference Guide***.
- When you create a pool, there is an option to set up persistence and a choice of load balancing methods. Refer to Chapter 4, *Pools,* in the ***BIG-IP Reference Guide***.

Glossary

BIG-IP web server

The BIG-IP web server runs on a BIG-IP system and hosts the Configuration utility.

bigpipe

The **bigpipe** utility provides command line access to the BIG-IP system.

BIG/stat

BIG/stat is a statistical monitoring utility that ships on the BIG-IP system. This utility provides a snap-shot of statistical information.

BIG/top

BIG/top is a statistical monitoring utility that ships on the BIG-IP system. This utility provides real-time statistical information.

big3d

The **big3d** agent is a monitoring utility that collects metrics information about paths between a BIG-IP system and a specific local DNS server. The **big3d** agent runs on BIG-IP units and it forwards metrics information to 3-DNS systems.

BIND (Berkeley Internet Name Domain)

BIND is the most common implementation of DNS, which provides a system for matching domain names to IP addresses.

chain

A chain is a series of filtering criteria used to restrict access to an IP address. The order of the criteria in the chain determines how the filter is applied, from the general criteria first, to the more detailed criteria at the end of the chain.

default VLANs

The BIG-IP system is configured with two default VLANs, one for each interface. One default VLAN is named **internal** and one is named **external**. See also *VLAN*.

dynamic site content

Dynamic site content is site content that is automatically generated each time a user accesses the site. Examples are current stock quotes or weather satellite images.

external VLAN

The external VLAN is a default VLAN on the BIG-IP system. In a basic configuration, this VLAN has the administration ports locked down. . In a normal configuration, this is typically a VLAN on which external clients request connections to internal servers.

floating self IP address

A floating self IP address is an additional self IP address for a VLAN that serves as a shared address by both units of a BIG-IP redundant system.

health check

A health check is a BIG-IP system feature that determines whether a node is **up** or **down**. Health checks are implemented through health monitors. See also *health monito*r.

health monitor

A health monitor checks a node to see if it is **up** and functioning for a given service. If the node fails the check, it is marked **down**.

HTTP redirect

An HTTP redirect sends an HTTP 302 Object Found message to clients. You can configure a pool with an HTTP redirect to send clients to another node or virtual server if the members of the pool are marked **down**.

ICMP (Internet Control Message Protocol)

ICMP is an Internet communications protocol used to determine information about routes to destination addresses, such as virtual servers managed by BIG-IP and 3-DNS systems.

interface

The physical port on a BIG-IP system is called an interface. See also *link*.

internal VLAN

The internal VLAN is a default VLAN on the BIG-IP system. In a basic configuration, this VLAN has the administration ports open. In a normal configuration, this is a network interface that handles connections from internal servers.

iQuery

A UDP based protocol used to exchange information between BIG-IP units and 3-DNS systems. The iQuery protocol is officially registered for port 4353.

last hop

A last hop is the final hop a connection took to get to the BIG-IP system. You can allow the BIG-IP system to determine the last hop automatically to send packets back to the device from which they originated.

link

A link is a physical interface on the BIG-IP system connected to another physical interface in a network.

link aggregation

The link aggregation feature allows you to combine a number of links together to act as one interface.

loopback adapter

A loopback adapter is a software interface that is not associated with an actual network card. The nPath routing configuration requires you to configure loopback adapters on servers.

MAC (Media Access Control)

MAC is a protocol that defines the way workstations gain access to transmission media, and is most widely used in reference to LANs. For IEEE LANs, the MAC layer is the lower sublayer of the data link layer protocol.

MAC address

A MAC address is used to represent hardware devices on an Ethernet network.

monitor

The BIG-IP system uses monitors to determine whether nodes are **up** or **down**. There are several different types of monitors and they use various methods to determine the status of a server or service.

monitor instance

You create a monitor instance when a health monitor is associated with a node, node address, or port. It is the monitor instance that actually performs the health check, not the monitor.

monitor template

A monitor template is a system-supplied health monitor that is used primarily as a template to create user-defined monitors, but in some cases can be used as is. The BIG-IP system includes a number of monitor templates, each specific to a service type, for example, HTTP and FTP. The template has a template type that corresponds to the service type and is usually the name of the template.

named

Named is the name server utility, which manages domain name server software.

NAT (Network Address Translation)

A NAT is an alias IP address that identifies a specific node managed by the BIG-IP system to the external network.

node

A node is a specific combination of an IP address and port (service) number associated with a server in the array that is managed by the BIG-IP system.

node address

A node address is the IP address associated with one or more nodes. This IP address can be the real IP address of a network server, or it can be an alias IP address on a network server.

node alias

A node alias is a node address that the BIG-IP system uses to verify the status of multiple nodes. When the BIG-IP system uses a node alias to check node status, it pings the node alias. If the BIG-IP system receives a response to the ping, it marks all nodes associated with the node alias as **up**. If the controller does not receive a response to the ping, the it marks all nodes associated with the node alias as **down**.

node port

A node port is the port number or service name that is hosted by a specific node.

node status

Node status indicates whether a node is **up** and available to receive connections, or **down** and unavailable. The BIG-IP system uses the node ping and health check features to determine node status.

persistence

A series of related connections received from the same client, having the same session ID. When persistence is turned on, a controller sends all connections having the same session ID to the same node instead of load balancing the connections.

port

A port is represented by a number that is associated with a specific service supported by a host. Refer to the Services and Port Index for a list of port numbers and corresponding services.

rate class

You create a rate filter from the Configuration utility or command line utility. When you assign a rate class to a rate filter, a rate class determines the volume of traffic allowed through a rate filter. See also *rate filter*.

rate filter

Rate filters consist of a basic filter with a rate class. Rate filters are a type of extended IP filter. They use the same IP filter method, but they apply a rate class, which determines the volume of network traffic allowed through the filter. See also *rate class*.

remote administrative IP address

The remote administrative IP address is an IP address from which a controller allows shell connections, such as Telnet or SSH.

RFC 1918 addresses

An RFC 1918 address is an IP address that is within the range of non-routable addresses described in the IETF RFC 1918.

self IP address

Self IP addresses are the IP addresses owned by the BIG-IP system that you use to access the internal and external VLANs.

service

Service refers to services such as TCP, UDP, HTTP, and FTP.

Setup utility

The Setup utility walks you through the initial system configuration process. You can run the Setup utility from either the command line or the Configuration utility start page.

SNAT (Secure Network Address Translation)

A SNAT is a feature you can configure on the BIG-IP system. A SNAT defines a routable alias IP address that one or more nodes can use as a source IP address when making connections to hosts on the external network.

SNAT automap

This feature allows the BIG-IP system to perform a SNAT automatically on any connection that is coming from the controller’s internal VLAN. It is easier to use than traditional SNATs and solves certain problem associated to traditional SNATs.

SNMP (Simple Network Management Protocol)

SNMP is the Internet standard protocol, defined in STD 15, RFC 1157, developed to manage nodes on an IP network.

SSL gateway

An SSL gateway is a gateway for decrypting HTTPS requests to an HTTP server and encrypting the reply.

state mirroring

State mirroring is a feature on the BIG-IP system that preserves connection and persistence information in a BIG-IP redundant system.

static load balancing modes

Static load balancing modes base connection distribution on a pre-defined list of criteria; it does not take current server performance or current connection load into account.

sticky mask

A sticky mask is a special IP mask that you can configure on the BIG-IP system. This mask optimizes sticky persistence entries by grouping more of them together.

tagged VLAN

You can define any interface as a member of a tagged VLAN. You can create a list of VLAN tags or names for each tagged interface.

transparent node

A transparent node appears as a router to other network devices, including the BIG-IP system.

trunk

A trunk is a combination of two or more interfaces and cables configured as one link. See also *link aggregation.*

virtual address

A virtual address is an IP address associated with one or more virtual servers managed by the BIG-IP system.

virtual port

A virtual port is the port number or service name associated with one or more virtual servers managed by the BIG-IP system. A virtual port number should be the same TCP or UDP port number to which client programs expect to connect.

virtual server

Virtual servers are a specific combination of virtual address and virtual port, associated with a content site that is managed by a BIG-IP system or other type of host server.

VLAN

VLAN stands for virtual local area network. A VLAN is a logical grouping of network devices. You can use a VLAN to logically group devices that are on different network segments.

VLAN name

A VLAN name is the symbolic name used to identify a VLAN. For example, you might configure a VLAN named marketing, or a VLAN named development. See also *VLAN*.

Index