

BIG-IP® e-Commerce Administrator Guide

version 4.0

Service and Support Information

Product Version

This manual applies to version 4.0 of the BIG-IP® e-Commerce Controller.

Obtaining Technical Support

Web	tech.f5.com
Phone	(206) 272-6888
Fax	(206) 272-6802
Email (support issues)	support@f5.com
Email (suggestions)	feedback@f5.com

Contacting F5 Networks

Web	www.f5.com
Toll-free phone	(888) 961-7242
Corporate phone	(206) 272-5555
Fax	(206) 272-5556
Email	sales@f5.com
Mailing Address	401 Elliott Avenue West Seattle, Washington 98119

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.

Copyright 1997-2001, F5 Networks, Inc. All rights reserved.

Trademarks

F5, BIG-IP, 3-DNS, SEE-IT, and GLOBAL-SITE are registered trademarks of F5 Networks, Inc. EDGE-FX, iControl, and FireGuard are trademarks of F5 Networks, Inc. Other product and company names are registered trademarks or trademarks of their respective holders.

Export Regulation Notice

The BIG-IP® Controller may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this BIG-IP® Controller 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.

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

This product includes software developed by Jochen Pohl for the NetBSD Project.

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

This product includes software developed by SigmaSoft, Th. Lockert.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed by Jason R. Thorpe for And Communications, <http://www.and.com>.

This product includes software developed for the NetBSD Project by Frank Van der Linden.

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed by Christos Zoulas.

This product includes software developed by Charles Hannum.

This product includes software developed by Charles Hannum, by the University of Vermont and State Agricultural College and Garrett A. Wollman, by William F. Jolitz, and by the University of California, Berkeley, Lawrence Berkeley Laboratory, and its contributors.

This product includes software developed by the University of Vermont and State Agricultural College and Garrett A. Wollman.

In the following statement, "This software" refers to the Mitsumi CD-ROM driver: This software was developed by Holger Veit and Brian Moore for use with "386BSD" and similar operating systems. "Similar operating systems" includes mainly non-profit oriented systems for research and education, including but not restricted to "NetBSD," "FreeBSD," "Mach" (by CMU).

In the following statement, "This software" refers to the parallel port driver: This software is a component of "386BSD" developed by William F. Jolitz, TeleMuse.

This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).

This product includes software developed by Darren Reed. (© 1993-1998 by Darren Reed).

This product includes software licensed from Richard H. Porter under the GNU Library General Public License (© 1998, Red Hat Software), www.gnu.org/copyleft/lgpl.html.

This product includes the standard version of Perl software licensed under the Perl Artistic License (© 1997, 1998 Tom Christiansen and Nathan Torkington). All rights reserved. You may find the most current standard version of Perl at <http://www.perl.com>.

Table of Contents



Introduction

Getting started	Intro-1
Choosing a configuration tool	Intro-1
Using the Administrator Kit	Intro-2
Stylistic conventions	Intro-3
Finding additional help and technical support resources	Intro-6
What's new in version 4.0	Intro-7
3-DNS on the BIG-IP Controller	Intro-7
OneConnect™ content switching with HTTP Keep-Alives	Intro-7
Bridging and Layer 2 forwarding	Intro-7
HTTP Redirect pool property	Intro-8
Load balance any IP protocol	Intro-8
Link aggregation and fail-over	Intro-8
On-the-fly content converter	Intro-8
SNAT automap feature	Intro-9
Health monitors	Intro-9
Performance monitors	Intro-9
Default controller configuration	Intro-9
Web-based Configuration utility enhancements	Intro-10
Learning more about the BIG-IP Controller product family	Intro-10

I

Configuring an SSL Accelerator

Introducing the SSL Accelerator	I-1
Configuring the SSL Accelerator	I-2
Generating a key and obtaining a certificate	I-3
Installing certificates from the certificate authority (CA)	I-9
Creating an SSL gateway	I-11
Additional configuration options	I-14

Glossary

Index

Introduction

- Getting started
- Using the Administrator Kit
- What's new in version 4.0
- Learning more about the BIG-IP Controller product family

Getting started

Before you start installing the controller, we recommend that you browse the ***BIG-IP Administrator Guide*** and find the load balancing solution that most closely addresses your needs. If the BIG-IP Controller 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, turn back to the Installation Guide for hardware installation instructions, and then return to the Administrator Guide to follow the steps for setting up your chosen solution.

Choosing a configuration tool

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

The First-Time Boot utility

All users will use the First-Time Boot utility, a wizard that walks you through the initial system set up. You can run the First-Time Boot utility from the command line, or from a web browser. The First-Time Boot utility prompts you to enter basic system information including a root password and the IP addresses that will be assigned to the network interfaces. The ***BIG-IP Installation Guide*** provides a list of the specific pieces of information that the First-Time Boot utility prompts you to enter.

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 Controller. Once you complete the installation instructions described in this guide, you can use the Configuration utility to

perform the 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 MIB or the SSH client. The Configuration utility requires Netscape Navigator version 4.7 or later, or Microsoft Internet Explorer version 5.0 or later.

The bigpipe and bigtop command line utilities

The **bigpipe**TM 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 Controller, you can use certain **bigpipe** commands, or you can use the **bigtop**TM utility, which provides real-time system monitoring. You can use the command line utilities directly on the BIG-IP Controller console, or you can execute commands via a remote shell, such as the SSH client (encrypted communications only), or a Telnet client (for countries restricted by cryptography export laws). For detailed information about the command line syntax, see the ***BIG-IP Reference Guide***, Chapter 2, *bigpipe Command Reference*, and the ***BIG-IP Administrator Guide***, Chapter 18, *Monitoring and Administration*.

Using the Administrator Kit

The BIG-IP[®] Administrator Kit provides all of the documentation you need to work with the BIG-IP Controller. The information is organized into the guides described below.

- ◆ **BIG-IP Installation Guide**

This guide walks you through the basic steps needed to get the hardware plugged in and the system connected to the network. Most users turn to this guide only the first time that they set up a controller. The ***BIG-IP Installation Guide*** also covers general network administration issues, such as setting up common network administration tools including Sendmail.

- ◆ **BIG-IP Administrator Guide**

This guide provides examples of common load balancing solutions, as well as additional administrative information. Before you begin installing the controller 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 basic descriptions of individual BIG-IP objects, such as pools, nodes, and virtual servers. It also provides syntax information for **bigpipe** commands, other command line utilities, configuration files, and system utilities.

- ◆ **F-Secure SSH User Guide**

This guide provides information about installing and working with the SSH client, a command line shell that supports remote encrypted communications. The SSH client and corresponding user guide is distributed only with BIG-IP Controllers that support encryption.

Stylistic conventions

To help you easily identify and understand important information, our documentation uses the stylistic conventions described below.

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 Controller 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**, Chapter 1, **bigpipe Command Reference***.

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
<code>\</code>	Indicates that the command continues on the following line, and that users should type the entire command without typing a line break.
<code>< ></code>	Identifies a user-defined parameter. For example, if the command has <your name> , type in your name, but do not include the brackets.

***Table Intro.1** Command line syntax conventions*

Item in text	Description
	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 Controller displays the syntax and usage associated with the command.

- ◆ **Third-party documentation for software add-ons**

The web server on the product contains online documentation for all third-party software, such as GateD.

- ◆ **Technical support via 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 obtain a customer ID and a password from the F5 Help Desk.

What's new in version 4.0

The BIG-IP Controller offers the following major new features in version 4.0, in addition to many smaller enhancements.

3-DNS on the BIG-IP Controller

With this release of the BIG-IP Controller, you can order the full wide-area load balancing functionality of the 3-DNS Controller combined with the local-area load balancing functionality of the BIG-IP Controller. An advantage you gain with this configuration is that the combined configuration requires less rack space.

OneConnect™ content switching with HTTP Keep-Alives

OneConnect content switching allows you to turn on the Keep-Alive functionality on your Web servers.

You can now configure BIG-IP Controller rules to support HTTP 1.1 Keep-Alive functionality. This feature allows you to benefit from the Keep-Alive features on your Web servers.

Another benefit of this feature is client aggregation. You can aggregate client connections by configuring a SNAT for inbound requests. This reduces the number of connections from the BIG-IP Controller to back-end servers and from clients to the BIG-IP Controller.

Bridging and Layer 2 forwarding

The bridging and Layer 2 forwarding functionality in this release provides the ability to bridge packets between VLANs and between VLANs on the same IP network. The layer 2 forwarding feature provides the ability to install a BIG-IP Controller without changing the IP network configuration. For an example of how to use layer 2 forwarding, see *VLAN group* in the ***BIG-IP Reference Guide***, Chapter 1, *Configuring the BIG-IP Controller*.

HTTP Redirect pool property

The HTTP redirect feature adds the ability to redirect clients to another site or server or to a 3-DNS Controller when the members of a pool they were destined for are not available. For more information, see *HTTP Redirect (specifying a fallback host)* in the ***BIG-IP Reference Guide***, Chapter 1, *Configuring the BIG-IP Controller*.

Load balance any IP protocol

The load balance any IP protocol feature provides the ability to load balance IP protocols other than TCP or UDP. This means that you can load balance VPN client connections across a number of VPNs, eliminating the possibility of a single point of failure.

Link aggregation and fail-over

The link aggregation feature provides the ability to combine multiple Ethernet links into a single trunk. This allows you to increase available bandwidth incrementally and improve link reliability. For more information, see *Trunks* in the ***BIG-IP Reference Guide***, Chapter 1, *Configuring the BIG-IP Controller*.

On-the-fly content converter

The on-the-fly content converter provides a simplified method of converting URLs in HTML files passing through the BIG-IP Controller to ARLs that point to the Akamai Freeflow Network™.

SNAT automap feature

The SNAT automap feature provides the ability to automatically map a SNAT to a BIG-IP Controller VLAN or self IP address. This simplifies the ability to load balance multiple internet ISPs. For more information, see *SNATs* in the **BIG-IP Reference Guide**, Chapter 1, *Configuring the BIG-IP Controller*.

Health monitors

This release contains predefined templates that you can use to define many different types of monitors (EAVs and ECVs) that check the health and availability of devices in the network. You can associate a monitor with a single node or many nodes. For more information, see the *Health monitors* in the **BIG-IP Reference Guide**, Chapter 1, *Configuring the BIG-IP Controller*.

Performance monitors

A performance monitor gathers statistics that are the basis for load balancing decisions made with the Dynamic Ratio load balancing method. You can implement Dynamic Ratio load balancing on RealNetworks RealServer platforms, Windows platforms equipped with Windows Management Instrumentation (WMI), and on platforms that support simple network management protocol (SNMP). For more information, see the *Configuring servers and the BIG-IP Controller for Dynamic Ratio load balancing* under *Pools* in the **BIG-IP Reference Guide**, Chapter 1, *Configuring the BIG-IP Controller*.

Default controller configuration

The BIG-IP Controller includes a default configuration that allows you to connect to a controller remotely and configure it by command line or from a web-based user interface. The default configuration provides a default IP address (RFC 1918) on the default internal VLAN or on the Admin VLAN if the controller has

three interfaces. You can connect to the default IP address and log on to the controller with the default user name and password. This provides the ability to run the First-Time Boot utility from a remote SSH client or from a web browser. For more information, see the ***BIG-IP Installation Guide***, Chapter 2, *Creating the Initial Software Configuration*.

Web-based Configuration utility enhancements

This release includes a number of improvements to the web-based Configuration utility. There are new wizards for tasks such as adding virtual servers, rules, monitors, and initial setup. A new tab-style navigation system simplifies navigation in the utility. In addition to the wizards for completing simple tasks, this release includes several configuration wizards that simplify creating a configuration for the BIG-IP Controller. These wizards include the Basic Site Configuration wizard, the Secure Site Configuration wizard, and the Active-active wizard.

Learning more about the BIG-IP Controller product family

The BIG-IP Controller 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 Controller to the BIG-IP HA Controller, which supports all BIG-IP Controller features.

- ◆ **The BIG-IP HA Controller with optional 3-DNS software module**

The BIG-IP HA Controller provides the full suite of local area load balancing functionality. The BIG-IP HA Controller also has an optional 3-DNS software module which supports wide-area load balancing.

◆ **The combined product BIG-IP Controller**

The combined product BIG-IP Controller provides the ability to choose from three different BIG-IP Controller feature sets. When you run the First-Time Boot utility, you specify the controller type:

• **The BIG-IP LB Controller**

The BIG-IP LB Controller provides basic load balancing features.

• **The BIG-IP FireGuard Controller**

The BIG-IP FireGuard Controller 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 an group of cache servers.

◆ **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.

I

Configuring an SSL Accelerator

- Introducing the SSL Accelerator
- Configuring the SSL Accelerator

Introducing the SSL Accelerator

The SSL Accelerator feature allows the BIG-IP Controller 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 Controller can retrieve the web page using an unencrypted HTTP request to the content server. With the SSL Accelerator feature, you can configure an SSL gateway on the BIG-IP Controller that decrypts HTTP requests that are encrypted with SSL. Decrypting the request off-loads SSL processing from the servers to the BIG-IP Controller. This also allows the BIG-IP Controller to use the header of the HTTP request to intelligently control how the request is handled.

When the SSL gateway on the BIG-IP Controller connects to the content server, it uses the original client's IP address and port as its source address and port, so that it appears to be the client (for logging purposes).

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

- Configuring an SSL Accelerator
- Enabling and disabling an SSL Accelerator
- Viewing the configuration of an SSL Accelerator
- Using an SSL Accelerator scalable configuration

◆ Note

All products except the BIG-IP LoadBalancer, BIG-IP FireGuard Controller, and the BIG-IP Cache Controller support this configuration. The features required for this configuration are optional on the BIG-IP Controller HA and Enterprise.

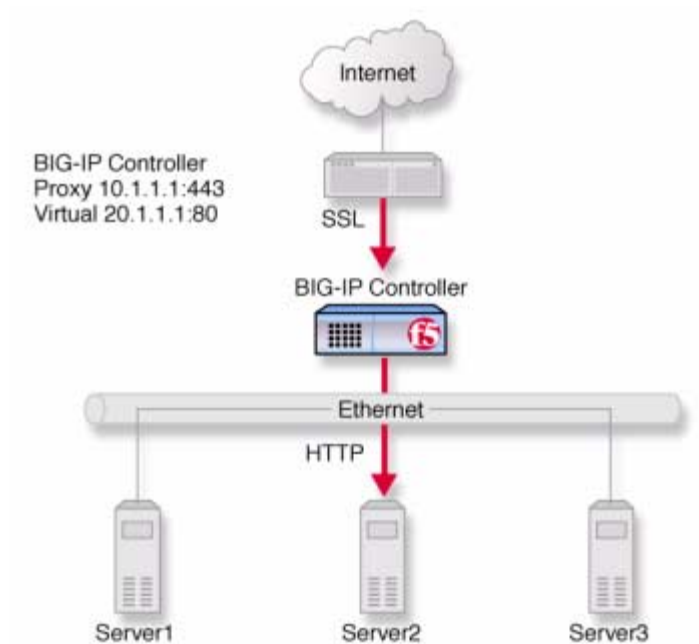


Figure 1.1 An incoming SSL connection received by an SSL Accelerator configured on a redundant BIG-IP Controller system

Configuring the SSL Accelerator

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

- Generating a key and obtaining a certificate
- Configuring the BIG-IP Controller with the certificate and key
- Creating an HTTP virtual server
- Creating the gateway 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). The following list contains some companies that are certificate authorities:

- Verisign (<http://www.verisign.com>)
- Digital Signature Trust Company (<http://secure.digistrust.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 with the Configuration utility or from the command line.

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 Controller or 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

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 Controller 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 Create SSL Certificate Request tab.
The New SSL Certificate Request screen opens.
3. In the Key Information section, select a key length and key file name.
 - **Key Length**
Select the key length you want to use for the key. You can choose either **512** or **1024** bytes.
 - **Keyfile Name**
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.
4. 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.
5. Click the **Generate Certificate Request** button.
After a short pause, the SSL Certificate Request screen opens.
 6. In the SSL Certificate Request screen, you can start the process of obtaining a certificate from a CA, and you can generate and install a temporary certificate.

- **Begin the process for obtaining a certificate from CA**
Click on 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 CA using the Configuration utility*, on page 1-9, for information about installing it on the BIG-IP Controller.
- **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 Controller. This certificate is valid for 10 years. This temporary certificate allows you to set up an SSL gateway 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 Controller 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 30 day certificate for testing the SSL Accelerator on the BIG-IP Controller. 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 from the root (/) with the following commands:

```
cd /  
/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
- 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 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 from the root (/) to run the **genkey** utility:

```
cd /usr/local/bin/genkey <server_name>
```

For the **<service_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/<fqdn>.req
```

The **<fqdn>** is the fully qualified domain name of the server. Please contact your 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 you must copy the key and certificate to the other controller in a redundant system.

This temporary certificate is good for ten years, but for an SSH 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 Controller:

```
/config/bigconfig/ssl.key/
```

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

```
cd /  
/user/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>.req
```

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 Controller in the redundant configuration. You can configure the accelerator with certificates using the Configuration utility or from the command line.

Installing certificates from the CA using the Configuration utility

1. In the navigation pane, click **Proxies**.
The Proxies screen opens.
2. Click the Install SSL Certificate tab.
The Install SSL Certificate screen opens.
3. In the **Certfile Name** box, type the fully qualified domain name of the server with the file extension **.crt**. If you generated a temporary certificate when you submitted a request to the CA, you can select the name of the certificate from the drop down list. This allows you to overwrite the temporary certificate with the certificate from the CA.

4. Paste the text of the certificate into the Install SSL Certificate window. Make sure you include the **BEGIN CERTIFICATE** line and the **END CERTIFICATE** line. For an example of a certificate, see Figure 1.3.
5. Click the **Write Certificate File** button to install the certificate.

```
-----BEGIN CERTIFICATE-----
MIIB1DCCAX4CAQAwDQYJKoZIhvcNAQEEBQAwdTELMAkGA1UEBhMCVVMxCzAJBgNV
BAGTAldBMRawDgYDVQQHEwdTZWF0dGx1MRQwEgYDVQQKEwtGNSBOZXR3b3JrczEc
MBoGA1UECxMTUHJvZHVjdCBEZXZlbG9wbWVudDETMDEGA1UEAxMKc2VydmVyLm51
dDAeFw0wMDA0MTkxNjMxNTlaFw0wMDA1MTkxNjMxNTlaMHUxCzAJBgNVBAYTA1VT
MQswCQYDVQQLIEwJXQTEQMA4GA1UEBxMHU2VhdHRsZTEUMBIGA1UEChMLRjUgTmV0
d29ya3MxHDAaBgNVBAsTE1Byb2RlY3QgRGV2ZWxvcG1lbnQxEzARBgNVBAMTCnNl
cnZlc5uZXQwXDANBgkqhkiG9w0BAQEFAANLADBIAGkEAsfCFXq3Jt+FevxUqBZ9T
Z7nHx9uaF5x9V5xMZygekjc+LrF/yazhm4PCxrws3gvJmgsTsh50YJrhJgfs2bE
gwIDAQABMA0GCSqGSIb3DQEBAUAA0EAdlq6+u/aMaM2qdo7EjWxl4TYQQGomYoq
eydlzb/3F0iJAYnDXnGnSt+CVvyRXtvmG7V8xJamzkyEpZd4iLacLQ==
-----END CERTIFICATE-----
```

Figure 1.3 An example of a certificate

After the certificate is installed, you can continue with the next step in creating an SSL gateway for the server.

Installing certificates from the CA from the command line

Copy the certificate into the following directory on each BIG-IP Controller 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 Controller:

```
/config/bigconfig/ssl.eky/
```

◆ WARNING

The keys and certificates must be in place on both controllers in a redundant system before you configure the SSL Accelerator. You must do this manually; the configuration synchronization utilities do not perform this function.

Creating an SSL gateway

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

To create an SSL gateway 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 gateway from the command line

Use the following command syntax to create an SSL gateway:

```
b proxy <ip>:<port> [vlans add <vlan_list>] [<unit id>] target <server | virtual> <ip>:<port> ssl enable key <key> cert <cert>
```

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

```
b proxy 10.1.1.1:443 unit 1 target virtual 20.1.1.1:80 ssl enable key my.server.net.key cert my.server.net.crt }
```

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 **/config/bigip.conf** file, it looks like the text in Figure 1.4.

```
proxy 10.1.1.1:https unit 1 {  
    netmask 255.255.255.0  
    broadcast 10.1.1.255  
    target virtual 20.1.1.1:80  
    ssl enable  
    key my.server.net.key  
    cert my.server.net.crt  
}
```

Figure 1.4 An example SSL gateway configuration

Enabling, disabling, or deleting an SSL gateway

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

To enable or disable an SSL gateway using the Configuration utility

1. In the navigation pane, click **Proxies**.
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.

To delete an SSL gateway using the Configuration utility

1. In the navigation pane, click **Proxies**.
The Proxies screen opens.
2. Click the **Delete** button for the SSL gateway you want to delete.

To enable, disable, or delete an SSL gateway from the command line

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

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

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

```
b proxy 209.100.19.22:443 enable
```

If you want to disable the SSL gateway **209.100.19.22:443**, type the following command:

```
b proxy 209.100.19.22:443 disable
```

If you want to delete the SSL gateway **209.100.19.22:443**, type the following command:

```
b proxy 209.100.19.22:443 delete
```

Displaying the configuration for an SSL gateway from the command line

You can view the configuration information for an SSL gateway from the command line by using the **show** keyword.

To display configuration information for an SSL accelerator gateway from the command line

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

```
b 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:

```
b proxy 209.100.19.22:443 show
```

You can see sample output of this command in Figure 1.5.

```
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.crt
+====> 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.crt
+====> 11.12.1.111:80 -- Destination Address -- virtual
```

Figure 1.5 Output from the *bigpipe proxy show* command

Additional configuration options

Whenever you configure a BIG-IP Controller, you have a number of options.

- ◆ You have the option in all configurations to configure a redundant BIG-IP Controller for fail-over. Refer to *Redundant System* in the **BIG-IP Reference Guide, Configuration Objects and Properties**.
- ◆ All configurations have health monitoring options. Refer to *Health Monitors* in the **BIG-IP Reference Guide, Configuration Objects and Properties**.
- ◆ When you create a pool, there is an option to set up persistence and a choice of load balancing methods. Refer to *Pools* in the **BIG-IP Reference Guide, Configuration Objects and Properties**.

Glossary

Any IP Traffic

Any IP Traffic is a feature of the BIG-IP Controller that allows it to load balance protocols other than TCP and UDP.

ARL (Akamai Resource Locator)

A URL that is modified to point to content on the Akamai Freeflow Network™. In content conversion (Akamaization), the URL is converted to an ARL, which retrieves the resource from a geographically nearby server on the Akamai Freeflow Network for faster content delivery.

BIG-IP active unit

In a redundant system, the BIG-IP active unit is the controller that currently load balances connections. If the active unit in the redundant system fails, the standby unit assumes control and begins to load balance connections.

BIG-IP web server

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

bigpipe

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

BIG/stat

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

BIG/top

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

big3d

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

BIND (Berkeley Internet Name Domain)

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

cacheable content determination

Cacheable content determination is a process that determines the type of content you cache on the basis of any combination of elements in the HTTP header.

cacheable content expression

The cacheable content expression determines, based on evaluating variables in the HTTP header of the request, whether a BIG-IP Cache Controller directs a given request to a cache server or to an origin server. Any content that does not meet the criteria in the cacheable content expression is deemed non-cacheable.

cache_pool

The `cache_pool` specifies a pool of cache servers to which requests are directed in a manner that optimizes cache performance. The BIG-IP Cache Controller directs all requests bound for your origin server to this pool, unless you have configured the hot content load balancing feature and the request is for hot (frequently requested) content. See also *hot* and *origin server*.

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.

content affinity

Content affinity ensures that a given subset of content remains associated with a given cache server to the maximum extent possible, even when cache servers become unavailable, or are added or removed. This feature also maximizes efficient use of cache memory.

content converter gateway

A content converter gateway is a gateway for converting URLs to ARLs. See also *ARL*.

content demand status

The content demand status is a measure of the frequency with which content in a given hot content subset is requested over a given *hit_period*. Content demand status is either hot, in which case the number of requests for content in the hot content subset during the most recent *hit_period* has exceeded the *hot_threshold*, or cool, in which case the number of requests during the most recent hit period is less than the *cool_threshold*. See also *cool*, *cool_threshold*, *hit_period*, *hot*, *hot content subset*, and *hot_threshold*.

content_hash_size

Specifies the number of units, or hot content subsets, into which the content is divided when determining whether content is hot or cool. The requests for all content in a given subset are summed, and a state (hot or cool) is assigned to each subset. The *content_hash_size* should be within the same order of magnitude as the actual number of requests possible. For example, if the entire site is composed of 500,000 pieces of content, a *content_hash_size* of 100,000 is typical.

If you specify a value for *hot_pool*, but do not specify a value for this variable, the cache statement uses a default hash size of 10 subsets. See also *cool*, *hot*, and *hot content subset*.

content stripes

In products that support caching, content stripes are cacheable content subsets distributed among your cache servers.

cookie persistence

Cookie persistence is a mode of persistence you can configure on the BIG-IP Controller where the controller stores persistent connection information in a cookie.

cool

Cool describes content demand status when you are using hot content load balancing. See also *content demand status*, *hot*, and *hot content load balancing*.

cool threshold

The cool threshold specifies the maximum number of requests for given content that will cause that content to change from hot to cool at the end of the hit period.

If you specify a variable for `hot_pool`, but do not specify a value for this variable, the cache statement uses a default `cool_threshold` of 10 requests. See also *cool*, *hit_period*, and *hot*.

default VLANs

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

default wildcard virtual server

A default wildcard virtual server has an IP address and port number of `0.0.0.0:0` or `*:*` or `"any":"any"`. This virtual server accepts all traffic which does not match any other virtual server defined in the configuration.

dynamic load balancing

Dynamic load balancing modes use current performance information from each node to determine which node should receive each new connection. The different dynamic load balancing modes incorporate different performance factors such as current server performance and current connection load.

Dynamic Ratio load balancing mode

Dynamic Ratio mode is like Ratio mode (see Ratio mode), except that ratio weights are based on continuous monitoring of the servers and are therefore continually changing. Dynamic Ratio load balancing may currently be implemented on RealNetworks RealServer platforms, on Windows platforms equipped with Windows Management Instrumentation (WMI), or on a server equipped with either the UC Davis SNMP agent or Windows 2000 Server SNMP agent.

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.

EAV (Extended Application Verification)

EAV is a health check that verifies an application on a node by running that application remotely. EAV health check is only one of the three types of health checks available on a BIG-IP Controller. See also *health check*, *health monitor* and *external monitor*.

ECV (Extended Content Verification)

ECV is a health check that allows you to determine if a node is up or down based on whether the node returns specific content. ECV health check is only one of the three types of health checks available on a BIG-IP Controller. See also *health check*.

external monitor

A user-supplied health monitor. See also, *health check*, *health monitor*.

external VLAN

The external VLAN is a default VLAN on the BIG-IP Controller. 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.

F-Secure SSH

F-Secure SSH is an encryption utility that allows secure shell connections to a remote system.

fail-over

Fail-over is the process whereby a standby unit in a redundant system takes over when a software failure or a hardware failure is detected on the active unit.

fail-over cable

The fail-over cable directly connects the two controller units together in a redundant system.

Fastest mode

A dynamic load balancing mode that bases connection distribution on which server currently exhibits the fastest response time to node pings.

FDDI (Fiber Distributed Data Interface)

FDDI is a multi-mode protocol used for transmitting data on optical-fiber cables at speeds up to 100 Mbps.

First-Time Boot utility

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

floating self IP address

An additional self IP address for a VLAN that serves as a shared address by both units of a BIG-IP Controller redundant system.

forward proxy caching

Forward proxy caching is a configuration in which a BIG-IP Cache Controller redundant system uses content-aware traffic direction to enhance the efficiency of an array of cache servers storing Internet content for internal users.

health check

A health check is a BIG-IP Controller feature that determines whether a node is **up** or **down**. Health checks are implemented through health monitors. See also *health monitor*, *ECV*, *EAV*, and *external monitor*.

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**. Different monitors exist for checking different services. See also *health check*, *EAV*, *ECV*, and *external monitor*.

hit period

The hit period specifies the period, in seconds, over which to count requests for particular content before determining whether to change the state (hot or cool) of the content.

If you specify a value for *hot_pool*, but do not specify a value for this variable, the cache statement uses a default hit_period of 10 seconds. See also *cool*, *hot*, and *hot_pool*.

host

A host is a network server that manages one or more virtual servers that the 3-DNS Controller uses for load balancing.

hot

Hot is a term used to define frequently requested content based on the number of requests in a given time period for a given hot content subset. See also *hot content subset*.

hot pool

A hot pool is a designated group of cache servers to which requests are load balanced when the requested content is hot. If a request is for hot content, the BIG-IP Cache Controller redundant system directs the request to this pool.

hot content load balancing

Identifies hot or frequently requested content on the basis of number of requests in a given time period for a given hot content subset. A hot content subset is different from, and typically smaller than, the content subsets used for content striping. Requests for hot content are redirected to a cache server in the hot pool, a designated group of cache servers. This feature maximizes the use of cache server processing power without significantly affecting the memory efficiency gained by cacheable content determination. See also *hot*, *hot content subset*, and *hot pool*.

hot content subset

A hot content subset is different from, and typically smaller than, the content subsets used for cacheable content determination. This is created once content has been determined to be hot and is taken or created from the content subset. See also *cacheable content determination*.

hot threshold

The hot threshold specifies the minimum number of requests for content in a given hot content subset that will cause that content to change from cool to hot at the end of the period.

If you specify a value for `hot_pool`, but do not specify a value for this variable, the cache statement uses a default `hot_threshold` of 100 requests. See also *cool*, *hot*, *hot content subset*, and *hot pool*.

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)

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

intelligent cache population

Intelligent cache population allows caches to retrieve content from other caches in addition to the origin web server. Use this feature when working with non-transparent cache servers that can receive requests destined for the cache servers themselves. Intelligent cache population minimizes the load on the origin web server and speeds cache population. See also *non-transparent cache server* and *transparent cache server*.

interface

The physical port on a BIG-IP Controller. See also *link*.

IPSEC

IPSEC (Internet Security Protocol) is a communications protocol that provides security for the network layer of the Internet without imposing requirements on applications running above it.

iQuery

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

internal VLAN

The internal VLAN is a default VLAN on the BIG-IP Controller. 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.

last hop

A last hop is the final hop a connection took to get to the BIG-IP Controller. You can allow the BIG-IP Controller to determine the last hop automatically to send packets back to the device from which they originated. You can also specify the last hop manually by making it a member of a last hop pool.

Least Connections mode

A dynamic load balancing mode that bases connection distribution on which server currently manages the fewest open connections.

link

A link is a physical interface on the BIG-IP Controller 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.

load balancing mode

A particular method of determining how to distribute connections across an array.

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.

member

Member is a reference to a node when it is included in a particular pool. Pools typically include multiple member nodes.

minimum active members

The number of members that must be active in a priority group in order for the BIG-IP Controller to send its requests to that group. If the number of active members falls below this number, requests are sent to the next highest priority group (the priority group with the next lowest priority number).

mirroring

A feature on the BIG-IP Controller that preserves connection and persistence information in a BIG-IP Controller redundant system.

miss request

When a cache does not have requested content and cannot respond to the request, it is called a miss request.

monitor

The BIG-IP Controller 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 destination IP address or IP address:port

The monitor destination IP address or address: port for a user defined monitor is used mainly for setting up a node alias for the monitor to check. All nodes associated with that monitor will be marked down if the alias node (destination IP address:port) is marked down. See also *node alias*.

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 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 Controller 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 daemon, 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 Controller 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 Controller.

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 Controller uses to verify the status of multiple nodes. When the BIG-IP Controller uses a node alias to check node status, it pings the node alias. If the BIG-IP Controller 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

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 Controller uses the node ping and health check features to determine node status.

non-cacheable content

Content that is not identified in the cacheable content condition part of a cache rule statement.

non-transparent cache server

Cache servers that can receive requests that are destined for the cache servers themselves.

origin server

The web server on which all original copies of your content reside.

origin pool

Specifies a pool of servers that contain original copies of all content. Requests are load balanced to this pool when any of the following is true: the requested content is not cacheable, no cache server is available, or the BIG-IP Cache Controller redundant system is redirecting a request from a cache server that did not have the requested content.

Observed mode

A dynamic load balancing mode that bases connection distribution on a combination of two factors: the server that currently hosts the fewest connections and has the fastest response time.

performance monitor

A performance monitor gathers statistics and checks the state of a target device.

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.

pool

A pool is composed of a group of network devices (called members). The BIG-IP Controller load balances requests to the nodes within a pool based on the load balancing method and persistence method you choose when you create the pool or edit its properties.

port

A port is can be 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.

port-specific wildcard virtual server

A port-specific wildcard virtual server is a wildcard virtual server that uses a port number other than **0**.

Predictive mode

A dynamic load balancing mode that bases connection distribution on a combination of two factors: the server that currently hosts the fewest connections, and also has the fastest response time. Predictive mode also ranks server performance over time, and passes connections to servers which exhibit an improvement in performance rather than a decline.

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*.

ratio

A ratio is a parameter that assigns a weight to a virtual server for load balancing purposes.

Ratio mode

The Ratio load balancing mode distributes connections across an array of virtual servers in proportion to the ratio weights assigned to each individual virtual server.

receive expression

A receive expression is the text string that the BIG-IP Controller looks for in the web page returned by a web server during an extended content verification (ECV) health check.

redundant system

Redundant system refers to a pair of controllers that are configured for fail-over. In a redundant system, there are two controller units, one running as the active unit and one running as the standby unit. If the active unit fails, the standby unit takes over and manages connection requests.

RFC 1918 addresses

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

remote administrative IP address

An IP address from which a controller allows shell connections, such as Telnet or SSH.

remote server acceleration

A configuration in which a BIG-IP Cache Controller redundant system uses content-aware traffic direction to enhance the efficiency of an array of cache servers that cache content for a remote web server.

Round Robin mode

A static load balancing mode that bases connection distribution on a set server order. Round Robin mode sends a connection request to the next available server in the order.

self IP address

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

send string

A send string is the request that the BIG-IP Controller sends to the web server during an extended content verification (ECV) health check.

service

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

SNAT (Secure Network Address Translation)

A SNAT is a feature you can configure on the BIG-IP Controller. 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 Controller 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 problems associated with the latter.

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.

sod (switch over daemon)

The sod is a daemon that controls the fail-over process in a redundant system.

source processing

Source processing means that the interface rewrites the source of an incoming packet.

SSL gateway

A gateway for decrypting HTTP requests to an HTTP server and encrypting the reply.

standby unit

A controller in a redundant system that is always prepared to become the active unit if the active unit fails.

stateful site content

Content that maintains dynamic information for clients on an individual basis and is commonly found on e-commerce sites. For example, a site that allows a user to fill a shopping cart, leave the site, and then return and purchase the items in the shopping cart at a later time has stateful site content which retains the information for that client's particular shopping cart.

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.

static site content

A type of site content that is stored in HTML pages, and changes only when an administrator edits the HTML document itself.

sticky mask

A sticky mask is a special IP mask that you can configure on the BIG-IP Controller. 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 cache server

A transparent cache server can intercept requests destined for a web server, but cannot receive requests.

transparent node

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

trunk

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

user-defined monitor

A user-defined monitor is a custom monitor configured by a user, based on a system-supplied monitor template. For some monitor types, you must create a user-defined monitor in order to use them. For all monitor types, you must create a user-defined monitor to change system supplied monitor default values.

virtual address

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

virtual port

A virtual port is the port number or service name associated with one or more virtual servers managed by the BIG-IP Controller. 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 Controller 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*.

watchdog timer card

A watchdog timer card is a hardware device that monitors the BIG-IP Controller for hardware failure.

wildcard virtual server

A virtual server that uses an IP address of **0.0.0.0**, ***** or **"any"**. A wildcard virtual server accepts connection requests for destinations outside of the local network. Wildcard virtual servers are included only in Transparent Node Mode configurations.

Index

A

Administrator Kit, description Intro-2

B

BIG-IP Controller product family Intro-10

bigpipe utility Intro-2

bigtop utility Intro-2

browser, supported versions Intro-2

C

Configuration utility, web-based Intro-1

F

First-Time Boot utility

defined Intro-1

F-Secure SSH client

remote administration Intro-2

I

IP addresses

defining Intro-1

L

load balancing

configuring Intro-1

monitoring Intro-1

M

MIB. See SNMP MIB

monitoring, command-line utilities Intro-2

R

root password

defining Intro-1

S

SNMP MIB Intro-2

SSH client. See F-Secure SSH client

SSL Accelerator

configuring 1-2

configuring with certificates and keys 1-9

creating an SSL Gateway 1-11

deleting 1-12

disabling 1-12

enabling 1-12

hardware acceleration 1-2

obtaining certificates and keys 1-3

view configuration information 1-13

T

technical support Intro-6

U

utilities Intro-2