Deployment Guide

Deploying the BIG-IP System for WAN-Optimized Acceleration of FTP traffic

Welcome to the F5® deployment guide for FTP. This document contains guidance on configuring WAN-optimized acceleration for FTP traffic between two BIG-IP® systems running the Application Acceleration Manager (AAM). BIG-IP version 11.0 introduced iApps™ Application templates, an extremely easy way to configure the BIG-IP system for accelerating FTP traffic over the WAN.

Products and applicable versions

Product	Versions
BIG-IP LTM, AAM	11.4, 11.4.1, 11.5, 11.5.1, 11.6 (BIG-IP AAM must be licensed and provisioned)
FTP	Not applicable
FTP iApp template	System iApp that ships with v11.4 and later
Deployment Guide version	1.2 (see *Document Revision History on page 15)*

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/iapp-ftp-dg.pdf.*

To provide feedback on this deployment guide or other F5 solution documents, contact us at *solutionsfeedback@f5.com*.

Contents

Why F5? 3
What is F5 iApp? 3
Prerequisites and configuration notes 3

Configuration scenarios 4

Using this guide 5

Preparing to use the iApp 6

Configuring the BIG-IP iApp for FTP 7
Advanced options 7
Template Options 7
Network 8
Virtual Servers 8
Optimization 9
iRules 10
Finished 10

Next steps 11
Modifying DNS settings to use the BIG-IP virtual server address 11

Appendix: Manual configuration table 12

Glossary 13

Document Revision History 15

Why F5?

The BIG-IP system provides a number of ways to accelerate and optimize FTP traffic over the WAN. The configuration described in this guide enables a secure, optimized tunnel for transporting FTP traffic between two BIG-IP systems are deployed in geographically distributed locations.

What is F5 iApp?

New to BIG-IP version 11, F5 iApp™ is a powerful new set of features in the BIG-IP system that provides a new way to architect application delivery in the data center, and it includes a holistic, application-centric view of how applications are managed and delivered inside, outside, and beyond the data center. The iApp template acts as the single-point interface for building, managing, and monitoring this implementation.

For more information on iApps, see the White Paper *F5 iApp: Moving Application Delivery Beyond the Network:* *http://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf*.

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- For this deployment guide, the BIG-IP LTM system ***must*** be running version 11.4 or later. If you are using a previous version of the BIG-IP, see the Deployment Guide index on F5.com. The configuration in this guide does not apply to previous versions.
- This deployment guide provides guidance for using the iApp for FTP found in version 11.4 and later. For users familiar with the BIG-IP system, there is a manual configuration table at the end of this guide. However, we strongly recommend using the iApp template.
- You must have the BIG-IP Application Acceleration Manager (AAM) licensed and provisioned on your BIG-IP system to use this iApp template. If you do not have BIG-IP AAM provisioned, the FTP iApp does not appear in the Template list.
- Before running the iApp template, you must have already configured the BIG-IP AAM for Symmetric Optimization. See the BIG-IP AAM documentation available on Ask F5 for specific instructions on configuring BIG-IP AAM for Symmetric Optimization: *http://support.f5.com/kb/en-us/products/big-ip-aam.html*. Using the Acceleration > Quick Start > Symmetric Properties on the BIG-IP systems on both sides of the WAN creates the required objects, as long as you enable Discovery.
- The *iSession* tunnel created between the BIG-IP systems is a shared BIG-IP system resource. And once configured, the settings in the iSession profile may overrule certain iApp encryption settings in order to avoid conflicts with the iSession tunnel encryption settings.
- Before beginning the iApp configuration, we recommend you refer to *Preparing to use the iApp on page 6*, for important information about using the iApp for FTP.

Important

This iApp template is intended to create an iSession tunnel between two BIG-IP systems. It does not create a pool of servers or other aspects of traditional load balancing, nor does it configure specific Symmetric Optimization objects such as local and remote endpoints. Only use this template if you have two BIG-IP systems in different locations and want the BIG-IP systems to secure and optimize FTP traffic between them.

Configuration scenarios

In this Deployment Guide, the BIG-IP system is configured to create a secure and optimized tunnel for FTP traffic. Using the options found in the iApp and the information in this deployment guide, you can configure the BIG-IP system for accelerating FTP traffic over the WAN.

Accelerating FTP traffic over the WAN

The iApp enables you to use the BIG-IP system's Application Acceleration Manager module to optimize and secure your web traffic over the WAN (wide area network). The iApp uses the default *iSession profile* to create a secure tunnel between BIG-IP systems to accelerate and optimize the traffic.

In this scenario, you must have a symmetric BIG-IP deployment (as shown in Figure 1), with a BIG-IP system between your clients and the WAN, and another between the WAN and your servers. For this template to function, you must run the iApp template on each of the BIG-IP systems.

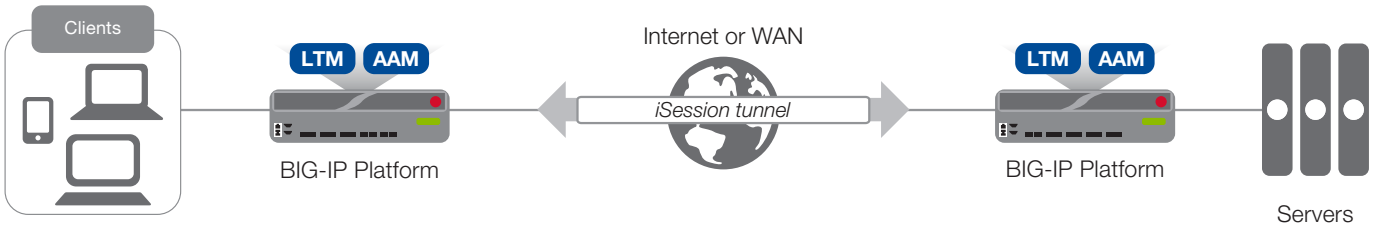

Figure 1: *Using an iSession tunnel to secure and optimize traffic between two BIG-IP systems*

Before running the iApp template, you must have already configured the BIG-IP AAM for Symmetric Optimization. See the BIG-IP AAM documentation available on Ask F5 for specific instructions on configuring BIG-IP AAM for Symmetric Optimization.

Using this guide

This guide is intended to help users deploy web-based applications using the BIG-IP system. This deployment guide contains guidance on two ways to configure the BIG-IP system: using the iApp template, and manually configuring the BIG-IP system.

Using this guide to configure the App template

We recommend using the iApp template to configure the BIG-IP system for your FTP implementation. The majority of this guide describes the iApp template and the different options the template provides for configuring the system for FTP.

The iApp template configuration portion of this guide walks you through the entire iApp, giving detailed information not found in the iApp or inline help. The questions in the iApp template itself are all in a table and at the same level. In this guide, we have grouped related questions and answers in a series of lists. Questions are part of an ordered list and are underlined and in italics or bold italics. Options or answers are part of a bulleted list, and in bold. Questions with dependencies on other questions are shown nested under the top level question, as shown in the following example:

1. ***Top-level question found in the iApp template***
   - *Select an object you already created from the list* (such as a profile or pool; not present on all questions. Shown in bold italic)
   - **Choice #1** (in a drop-down list)
   - **Choice #2** (in the list)
     a. *Second level question dependent on selecting choice #2*
        - **Sub choice #1**
        - **Sub choice #2**
          i). *Third level question dependent on sub choice #2*
              - **Sub-sub choice**
              - **Sub-sub #2**
                1). *Fourth level question (rare)*

Manually configuring the BIG-IP system

Users already familiar with the BIG-IP system can use the manual configuration tables to configure the BIG-IP system for the FTP implementation. These configuration tables only show the configuration objects and any non-default settings recommended by F5, and do not contain procedures on specifically how to configure those options in the Configuration utility. See *Appendix: Manual configuration table on page 12.*

Preparing to use the iApp

In order to use the iApp for FTP, it is helpful to have some information, such as server IP addresses and domain information before you begin. Use the following table for information you may need to complete the template. The table does not contain every question in the template, but rather includes the information that is helpful to have in advance. More information on specific template questions can be found on the individual pages.

BIG-IP LTM Preparation table		
Basic/Advanced mode	In the iApp, you can use F5 recommended settings (Basic mode) which are a result of extensive testing and tuning. Advanced mode gives you the to configure the BIG-IP system on a much more granular level, configuring specific options, or even using your own pre-built profiles or iRules. Basic and Advanced "configuration mode" is independent from the Basic/Advanced list at the very top of the template which only toggles the Device and Traffic Group options (see page 7)	
Network	**Type of network between clients and BIG-IP**	**Type of network between servers and BIG-IP**
	LAN | WAN through another BIG-IP system	LAN | WAN through another BIG-IP system
Virtual Servers	*The Virtual server is the address clients use to access the servers.*	
	IP address for the virtual server: *Associated TCP service port (21 is the default for FTP):*	
Profiles	For each of the following profiles, the iApp will create a profile using the F5 recommended settings (or you can choose 'do not use' many of these profiles). While we recommend using the profiles created by the iApp, you have the option of creating your own custom profile outside the iApp and selecting it from the list. The iApp gives the option of selecting our the following profiles (some only in Advanced mode). Any profiles must be present on the system before you can select them in the iApp	
	FTP | TCP LAN | TCP WAN | iSession	
iRules	In Advanced mode, you have the option of attaching iRules you create to the virtual server created by the iApp. For more information on iRules, see https://devcentral.f5.com/irules Any iRules you want to attach must be present on the system at the time you are running the iApp.	

Configuring the BIG-IP iApp for FTP

Use the following guidance to help configure the BIG-IP system for FTP using the BIG-IP iApp template.

Getting Started with the iApp for FTP

To begin the FTP iApp Template, use the following procedure.

1. Log on to the BIG-IP system.
2. On the Main tab, expand **iApp**, and then click **Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name. In our example, we use **FTP-iapp_.**
5. From the **Template** list, select **f5.ftp**.
   The FTP template opens.

Advanced options

If you select **Advanced** from the **Template Selection** list at the top of the page, you see Device and Traffic Group options for the application. This feature, new to v11, is a part of the Device Management configuration. This functionality extends the existing High Availability infrastructure and allows for clustering, granular control of configuration synchronization and granular control of failover. To use the Device and Traffic Group features, you must have already configured Device and Traffic Groups before running the iApp. For more information on Device Management, see the product documentation.

1. ***Device Group***
   To select a specific Device Group, clear the **Device Group** check box and then select the appropriate Device Group from the list.
2. ***Traffic Group***
   To select a specific Traffic Group, clear the **Traffic Group** check box and then select the appropriate Traffic Group from the list.

Template Options

This section contains general questions about the way you configure the iApp template.

1. ***Do you want to see inline help?***
   Choose whether you want to see informational and help messages inline throughout the template, or if you would rather hide this inline help. If you are unsure, we recommend having the iApp display the inline help.
   Important and critical notes are always shown, no matter which selection you make.
   - **Yes, show inline help text**
     Select this option to see all available inline help text.
   - **No, do not show inline help text**
     If you are familiar with this iApp template, or with the BIG-IP system in general, select this option to hide the inline help text.

2. ***Which configuration mode do you want to use?***
   Select whether you want to use F5 recommended settings, or have more granular, advanced options presented.
   - **Basic - Use F5's recommended settings**
     In basic configuration mode, options like optimization profiles are set automatically. The F5 recommended settings come as a result of extensive testing with FTP traffic, so if you are unsure, choose Basic.
   - **Advanced - Configure advanced options**
     In advanced configuration mode, you have more control over individual settings and objects, such as server-side optimizations and iSession features. You can also choose to attach iRules you have previously created to the application service. The Advanced option provides more flexibility for experienced users.
     Advanced options in the template are marked with the Advanced icon: Advanced. If you are using Basic/F5 recommended settings, you can skip the questions with this icon.

Network

This section contains questions about your networking configuration.

1. ***What type of network connects clients to the BIG-IP system?***
   Choose the type of network that connects your clients to the BIG-IP system. If you choose LAN, the BIG-IP system uses this information to determine the default TCP optimization profile. If you choose WAN through another BIG-IP system, the system uses a secure an optimized tunnel (called an iSession tunnel) for traffic between BIG-IP systems on opposite sides of the WAN.

   If you are configuring the client-side BIG-IP system, you should select Local area network here. If you are configuring the server-side BIG-IP system, you should select WAN through another BIG-IP system.

   - **Local area network (LAN)**
     Select this option if you are configuring the client-side BIG-IP system. The system creates a TCP profile optimized for LAN clients. In this case, the iApp creates a TCP profile using the *tcp-lan-optimized* parent with no additional modifications.
   - **WAN through another BIG-IP system**
     Select this option if client traffic is coming to this BIG-IP system from a remote BIG-IP system across a WAN. As mentioned in the introduction to this question, the iApp creates an iSession tunnel between this BIG-IP system and the BIG-IP system you will configure (or already have configured) on the other side of the WAN.

2. ***What type of network connects servers to the BIG-IP system?***
   Choose the type of network that connects your servers to the BIG-IP system. Similar to the question about clients connecting to the BIG-IP system, if you choose LAN, the BIG-IP system uses this information to determine the default TCP optimization profile. If you choose WAN through another BIG-IP system, the system uses a secure an optimized tunnel (called an iSession tunnel) for traffic between BIG-IP systems on opposite sides of the WAN.

   If you are configuring the client-side BIG-IP system, you should select WAN through another BIG-IP system here. If you are configuring the server-side BIG-IP system, you should select Local area network.

   - **Local area network (LAN)**
     Select this option if the servers connect to the BIG-IP system on a LAN. This field is used to determine the appropriate TCP profile. In this case, the iApp creates a TCP profile using the *tcp-lan-optimized* parent with no additional modifications.
   - **WAN through another BIG-IP system**
     Select this option if servers are across a WAN behind another BIG-IP system. As mentioned in the introduction to this question, the iApp creates an iSession tunnel between this BIG-IP system and the BIG-IP system you will configure (or already have configured) on the other side of the WAN.

3. ***Which VLANs transport client traffic?*** Advanced
   Select which of your BIG-IP VLANs are transporting client traffic. By default, all of the VLANs on the box are Selected. If you want the BIG-IP system to only accept client traffic from specific VLANs, select the appropriate VLAN(s) from the **Selected** list, and then click the Remove (**>>**) button.

Virtual Servers

This section gathers information for the BIG-IP *virtual server* used to facilitate the iSession tunnel.

1. ***On what IP address will the BIG-IP listen for the application?***
   Type the IP address on which the BIG-IP system should expect FTP traffic. This IP address becomes the BIG-IP virtual server address, which contains the iSession profile for the iSession tunnel, as well as other profiles you select in the Optimization section. If necessary for your configuration, this can be a network address (and you must specify an IP mask in the following question).

2. ***If using a network virtual address, what is the IP mask?***
   If you specified a network address for the virtual server (allowing the virtual server to handle multiple IP addresses), you must enter the full network mask that represents the address range. If you specified a single address for the virtual server, you may leave this field blank.

3. ***What TCP port will the application use?***
   Specify the TCP port for FTP. The default port for FTP is 21.

Optimization

In this section, you answer questions about how you want the BIG-IP system to optimize the delivery of your FTP traffic. This entire section only appears if you selected Advanced mode.

1. ***Create a new FTP profile or use an existing one?*** Advanced
   The FTP profile contains FTP-specific optimization settings. Choose whether you want to the iApp to create the recommended FTP profile or if you have created a FTP for this deployment.

   Unless you have requirements for configuring specific settings, we recommend allowing the iApp to create a new FTP profile. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Services : FTP** if you want to create a custom FTP profile. To select any new profiles you create, you need to restart or reconfigure this template.

   - **Create the recommended FTP profile**
     Leave this default option to have the system create a new FTP profile.
   - *Select an existing FTP profile*
     If you have already created a FTP profile for this implementation, you can select it from the list.

2. ***How do you want to optimize client-side connections?*** Advanced
   The client-side TCP profile optimizes the communication between the BIG-IP system and the client by controlling the behavior of the traffic which results in higher transfer rates, improved connection reliability and increased bandwidth efficiency.

   Unless you have requirements for configuring specific TCP optimization settings, we recommend allowing the iApp to create a new profile. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Protocol : TCP** to create a TCP profile. To select any new profiles you create, you need to restart or reconfigure this template.

   - **Create the recommended client-side TCP optimization profile**
     Select this option to have the system create the recommended TCP profile. The type of profile is determined by your selection to the "What type of network connects clients to the BIG-IP system" question.
   - *Select the TCP profile you created from the list*
     If you created a custom TCP profile for this implementation, select it from the list.

3. ***How do you want to optimize server-side connections?*** Advanced
   The server-side TCP profile optimizes the communication between the BIG-IP system and the server by controlling the behavior of the traffic which results in higher transfer rates, improved connection reliability and increased bandwidth efficiency.

   Unless you have requirements for configuring specific TCP optimization settings, we recommend allowing the iApp to create a new profile. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Protocol : TCP** to create a TCP profile. To select any new profiles you create, you need to restart or reconfigure this template.

   - **Create the recommended server-side TCP optimization profile**
     Select this option to have the system create the recommended TCP profile. The parent profile is determined by your selection to the "What type of network connects servers to the BIG-IP system" question.
   - *Select the TCP profile you created from the list*
     If you created a custom TCP profile for this implementation, select it from the list.

4. ***Create a new iSession tunnel profile or use an existing one?*** Advanced
   The iSession profile contains the settings for the secure and optimized tunnel between this BIG-IP system and the remote BIG-IP system. Choose whether you want to the iApp to create the recommended iSession profile or if you have created a iSession profile for this deployment.

Unless you have requirements for configuring specific settings, we recommend selecting the default iSession profile (**isession**) or allowing the iApp to create a new iSession profile. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Services : iSession** if you want to create a custom iSession profile. To select any new profiles you create, you need to restart or reconfigure this template.

- *Select an existing iSession profile*
  If you have already created a iSession profile for this implementation, you can select it from the list.
- **Create the recommended iSession profile**
  Leave this default option to have the system create a new iSession profile.

  a. *Which iSession features do you want to use?*
  This question does not appear in version 11.5 and later if you selected "WAN through another BIG-IP system" connecting clients to the BIG-IP system and "Local area network (LAN)" connecting servers to the BIG-IP system.

  The three major options of the iSession profile are WAN encryption, Adaptive Compression, and Deduplication. For each of the following, select **Yes** or **No**.

  - **WAN encryption**
    WAN encryption specifies whether the traffic on the outbound connection is encrypted. If you select Yes, the system uses the SSL profiles specified on the local and remote endpoints of the iSession connection. The local and remote endpoint configuration are not a part of this iApp. See the BIG-IP AAM documentation.
  - **Adaptive Compression**
    Adaptive compression selects and adjusts the optimal compression algorithm for the current traffic, based on link speed.
  - **Deduplication**
    Deduplication specifies whether the system optimizes traffic using symmetric data deduplication (locating byte patterns that were previously sent over the WAN, and replacing them with references).

iRules

In this section, you can add custom iRules to the FTP deployment. This entire section is available only if you selected Advanced mode.

iRules are a scripting language that allows an administrator to instruct the system to intercept, inspect, transform, direct and track inbound or outbound application traffic. An iRule contains the set of instructions the system uses to process data flowing through it, either in the header or payload of a packet.

1. ***Do you want to add any custom iRules to the configuration?*** Advanced
   Select if have preexisting iRules you want to add to your FTP implementation.

   Warning

   While iRules can provide additional functionality not present in the iApp, iRules are an advanced feature and should be used only if you understand how each iRule will affect your deployment, including application behavior and BIG-IP system performance.

   If you do not want to add any iRules to the configuration, continue with the following section.

   If you have iRules you want to attach to the virtual server the iApp creates for your web servers, from the **Options** box, click the name of the applicable iRule(s) and then click the Add (**<<**) button to move them to the **Selected** box.

Finished

Review the answers to your questions. When you are satisfied, click the **Finished** button. The BIG-IP system creates the relevant objects for the FTP implementation.

Next steps

After completing the iApp Template, the BIG-IP Application Services page opens for the FTP service you just created. To see the list of all the configuration objects created to support the FTP implementation, on the Menu bar, click **Components**. The complete list of all related objects opens. You can click individual objects to see the settings.

Once the objects have been created, you are ready to use the new deployment.

Modifying DNS settings to use the BIG-IP virtual server address

Before sending traffic to the BIG-IP system, your DNS administrator may need to modify any DNS entries for the FTP implementation to point to the BIG-IP system's virtual server address.

Modifying the iApp configuration

The iApp application service you just created can be quickly and easily modified if you find it necessary to make changes to the configuration. The Strict Updates feature of the iApp prevents users from manually modifying the iApp configuration (Strict Updates can be turned off, but use extreme caution). iApp allows you to re-enter the template, make changes, and then update the template. The modifications are automatically made to any of the associated objects.

To modify the configuration

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your FTP Application Service from the list.
3. On the Menu bar, click **Reconfigure**.
4. Make the necessary modifications to the template.
5. Click the **Finished** button.

Viewing statistics

You can easily view a number of different statistics on the BIG-IP system related to the configuration objects created by the iApp template.

To view object-level statics

1. On the Main tab, expand **Overview**, and then click **Statistics**.
2. From the **Statistics Type** menu, you can select **Virtual Servers** to see statistics related to the virtual servers.
3. You can also choose **Pools** or **Nodes** to get a closer look at the traffic.
4. To see Networking statistics in a graphical format, click **Dashboard**.

For more information on viewing statistics on the BIG-IP system, see the online help or product documentation.

Appendix: Manual configuration table

We strongly recommend using the iApp template to configure the BIG-IP system for FTP traffic across the WAN. Advanced users familiar with the BIG-IP system can use the following table to manually configure the system. The following table contains a list of BIG-IP configuration objects along with any non-default settings you should configure as a part of this deployment. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

BIG-IP LTM Object	Non-default settings/Notes		
BIG-IP AAM *(Acceleration)*	*You must you must have already performed the initial symmetric optimization configuration on both systems. This can be accomplished using **Acceleration > Quick Start > Symmetric Properties** as long as you are using "Discovery". See the BIG-IP AAM documentation for more information.*		
Profiles *(Local Traffic > Profiles)*	***TCP WAN*** *(Profiles > Protocol)*	Name	Type a unique name
		Parent Profile	**tcp-wan-optimized**
	TCP LAN *(Profiles > Protocol)*	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
	iSession [2] *(Profiles > Services)*	Name	Type a unique name
		Parent Profile	**isession**
	FTP *(Profiles > Services)*	Name	Type a unique name
		Parent Profile	**ftp**
Virtual Servers (*Local Traffic > Virtual Servers*)	**iSession virtual server**		
	Name	Type a unique name	
	Type	**Standard**	
	Address	Type the IP Address for the virtual server	
	Service Port	**21**	
	Protocol Profile (client)[1]	Select the WAN optimized TCP profile you created	
	Protocol Profile (server)[1]	Select the LAN optimized TCP profile you created	
	FTP Profile	Select the FTP profile you created	
	iSession Profile [2]	Select the iSession profile you created	

[1] *You must select* **Advanced** *from the* **Configuration** *list for these options to appear*
[2] *Do not create or use this profile if you are deploying the BIG-IP system on the server side of the WAN*

Glossary

application service
iApps application services use an *iApp Template* to guide users through configuring new BIG-IP® system configurations. An application service lets an authorized user easily and consistently deploy complex BIG-IP® system configurations just by completing the information required by the associated template. Every application service is attached to a specific configuration and cannot be copied the way that iApps templates can.

iApp Template
iApps templates create configuration-specific forms used by application services to guide authorized users through complex system configurations. The templates provide programmatic, visual layout and help information. Each new application service uses one of the templates to create a screen with fields and help that guide the user through the configuration process and creates the configuration when finished.

iApps templates allow users to customize by either modifying an existing template or creating one from scratch. Users can create scratch-built templates using either the iApps Templates screen or any text-editing software.

configuration utility
The Configuration utility is the browser-based application that you use to configure the BIG-IP system.

custom profile
A custom *profile* is a profile that you create. A custom profile can inherit its default settings from a parent profile that you specify. See also parent profile.

deduplication
The BIG-IP system uses symmetric data deduplication to reduce the amount of bandwidth consumed across a WAN link for repeated data transfers. With data deduplication, the system performs pattern matching on the transmitted WAN data, rather than caching. If any part of the transmitted data has already been sent, the system replaces the previously transmitted data with references. As data flows through the pair, each device records the byte patterns and builds a synchronized dictionary. If an identical pattern of bytes traverses the WAN more than once, the system closest to the sender replaces the byte pattern with a reference to it, compressing the data. When the reference reaches the other side of the WAN, the remote system replaces the reference with the data, restoring the data to its original format.

iRule
An iRule is a user-written script that controls the behavior of a connection passing through the BIG-IP system. iRules™ are an F5 Networks feature and are frequently used to direct certain connections to a non-default load balancing pool. However, iRules can perform other tasks, such as implementing secure network address translation and enabling session persistence. You can attach iRules you created to your HTTP application service in the advanced configuration mode.

iSession
An iSession is an optimized connection between two BIG-IP systems.

iSession profile
An iSession profile defines the optimization parameters. WAN optimization requires an iSession profile, which specifies the optimization settings, such as compression and data deduplication. The iApp template uses the default isession profile.

local endpoint
The local endpoint is the BIG-IP system on which you are currently working. The systems must be set up symmetrically, so that a local endpoint connects to one or more remote endpoints.

network virtual server
A network virtual server is a virtual server whose IP address has no bits set in the host portion of the IP address (that is, the host portion of its IP address is 0, such as 192.168.1.0). This allows you to direct client traffic based on a range of destination IP addresses.

profile
Profiles are a configuration tool that you can use to affect the behavior of certain types of network traffic. More specifically, a profile is an object that contains settings with values, for controlling the behavior of a particular type of network traffic, such as HTTP connections. Profiles also provide a way for you to enable connection and session persistence, and to manage client application authentication.

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.

SNAT
A SNAT (Secure Network Address Translation) is a feature that 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 pool
A SNAT pool is a pool of translation addresses that you can map to one or more original IP addresses. Translation addresses in a SNAT pool are not self IP addresses.

virtual server
A virtual server is a traffic-management object on the BIG-IP system that is represented by an IP address and a service port. This is the address clients use to connect to the web servers (or a FQDN resolves to this address). The BIG-IP intercepts the client request, and then directs the traffic according to your configuration instructions.

VLAN
A VLAN is a logical grouping of interfaces connected to network devices. You can use a VLAN to logically group devices that are on different network segments. Devices within a VLAN use Layer 2 networking to communicate and define a broadcast domain.

Document Revision History

Version	Description	Date
1.0	New Deployment Guide for BIG-IP version 11.4	06-11-2013
1.1	- Added support for version 11.4.1 and 11.5 - Added a note on page 10 stating the "Which iSession features do you want to use?" question does not appear in version 11.5 and later if you select a WAN connects the clients to the BIG-IP system.	01-31-2014
1.2	- Added support for version 11.5.1 and 11.6.	08-25-2014

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com