White Paper

# F5 iApps: Moving Application Delivery Beyond the Network

Traditional application delivery has focused on how to manage the network for applications. F5 iApps are a revolutionary new way of focusing on how to manage application delivery *through* the network, thereby changing how applications are delivered across the data center.

**by Alan Murphy**
Sr. Technical Marketing Manager

# Contents

# Introduction

There is a fundamental lack of application awareness and management in the network today. Data centers are built to deliver applications and services; however they are still managed as large networks. Individual networking components are managed as isolated, single-point devices. A networking router, for example, is managed as though it does nothing more than route IP traffic in a void, yet applications are 100 percent dependent on that router working as expected. Organizational and data center networks are currently viewed as a series of individual objects to be managed by individual groups, but there is no overarching view of how those components relate to each other and the rest of the infrastructure, or how those components all function together to deliver applications to users.

Managing the entire infrastructure as individual components hampers IT, in that it requires too many moving parts within different groups to adequately manage and control application delivery to users and to other services in the data center. As a result, IT departments often have complicated spreadsheets detailing which components are doing what at the network level, but no information about how those components are tied to the applications. This convoluted and isolated view of the infrastructure becomes a challenge for data center management, troubleshooting, and agile models such as self-service provisioning because there is no understanding of how the infrastructure components come together to deliver an application.

## Application Focus Shift

Despite this antiquated method IT often uses to manage the data center, applications are evolving and beginning to take center stage. This shift is forcing enterprise IT departments to start managing everything with an application-centric view rather than starting with devices and objects and piecing components together to deliver the application. This shift is largely driven by the push to adopt cloud computing and software as a service (SaaS), where the application becomes the most important component and the infrastructure becomes commoditized.

Sixty-eight percent of organizations cite application reliability and performance as the most important factor for cloud computing.

Source: IDG Report, "Global Cloud Computing Adoption: Transformation is in the Air," 2011

Managing applications is much more complex today than it was just five years ago. On the back end, applications can now reside anywhere, whether within or outside of the enterprise data center. Administrators can deploy applications between different cloud providers, run them as SaaS applications, and even spread them geographically between data centers on different continents. And with virtualization, data centers are moving away from a one-to-one, server-to-application model; resources are

shrinking while services are continuing to grow. On the front end, users are demanding new access models from mobile devices such as smartphones and tablets. The applications themselves are also moving to a much more data-rich model and relying on inter-application communication with APIs, which increase system and network resource requirements while also introducing new security threats. Yet despite this rapid consumerization of enterprise IT where the app is king, the fundamental infrastructure hasn't adapted. Managing application delivery isn't just about network components—it's also about context and understanding how users are interacting with applications in real time.

# iApps: The Era of the Application

F5® iApps™ are a powerful new set of features in the BIG-IP® system that provide 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. iApps provide a framework that application, security, network, systems, and operations personnel can use to unify, simplify, and control the entire Application Delivery Network (ADN) with a contextual view and advanced statistics about the application services supporting the business.

iApps are designed to abstract the many individual components required to deliver an application by grouping these resources together in templates associated with applications; this alleviates the need for administrators to manage discrete components on the network. Most enterprise IT departments delegate management responsibilities for various parts of the network to different groups: IP addresses, routing, and DNS are managed by the network team; physical and virtual servers, OS builds, and virus management is owned by the server team; API interaction, application standards, and access rights are owned by the application and security teams. There is typically no single group within IT that can answer the question "What components are required to deliver email in your organization and how are each of those components configured?" There are simply too many uncoordinated moving parts. iApps change this by managing everything from the application point of view. Nodes, application monitors, pools—with iApps, all of these ADN components can be clustered together and managed as part of an application workflow. This allows application and network administrators to easily define the infrastructure components required to deliver applications successfully by automating management tasks across the entire ADN.

In addition to configuring and managing various ADN and application infrastructure components, iApp policies can also define automation tasks, such as provisioning new ADN resources and managing the threshold data for a cloudbursting event. iApp policies rely on many different pieces of the BIG-IP system to manage all parts of application delivery, from applying load balancing rules for the AAA security infrastructure via F5's iRules® engine, to exposing application diagnostic and visibility data to iHealth™, F5's customer-facing support portal.

With iApps, all ADN components are bundled together and treated as extensions of the application. For example, a new SharePoint application will need specific health monitors that check the status of the web front end, search, and database components of SharePoint. Traditionally those components would need to be individually assigned and managed, leaving room for error and drastically increasing the deployment time. With an iApp policy for SharePoint, all of those pieces become components of the application itself that can be deployed and managed in one centralized location.

# Unified iApp Components

Under the hood, iApps are made up of several discrete components, each responsible for managing a portion of the application delivery infrastructure. Tied together, these components are part of the unified BIG-IP Application Delivery Controller (ADC).

## iApp Application Services

iApps bundle application components together for delivery by creating iApp Application Services that encompass two key functions: binding applications across all ADN services, and complete management control over all application delivery resources. iApp Application Services can be applied to any part of the application during delivery. For example, an iApp Application Service for SharePoint may initially be associated with a BIG-IP® Local Traffic Manager™ (LTM) policy and a suite of SSL-related iRules. Later, administrators can associate a BIG-IP® Access Policy Manager™ (APM) access policy with that same iApp Application Service for SharePoint by checking a single iApp box, and then redistribute it throughout the entire ADN. iApp Application Services reduce operational costs by providing insight to the entire application delivery infrastructure, binding application and network dependencies together in one unified ADN system.

Similar to how object-oriented programming changed the way applications were written, iApp Application Services change the paradigm of how typical ADN functions are placed "in front" of the application. iApp Application Services can be applied to any part of the application delivery chain at any point during delivery, which allows the organization to choose what parts of the application are affected by which ADN components and at what time, all based on context. iApp policies are not confined to just building load balancing configurations. As part of the entire BIG-IP unified ADC platform, iApp policies can also include configuration settings for advanced BIG-IP modules and features, such as assigning a user access policy to the application using BIG-IP APM, or configuring cached components in BIG-IP® WebAccelerator™.

## iApp Templates

One of the most compelling benefits of iApps is templates. Although application templates have been available in BIG-IP LTM since version 10, they were limited to the initial deployment phase of new applications and weren't available to modify the running configuration down the road. iApp Templates are flexible and easy to use for deploying and managing application services—they act as the single-point interface for building, managing, and monitoring applications across all BIG-IP modules. When an administrator builds a new iApp configuration using an existing template, the resulting configuration is used across all BIG-IP devices in a device service cluster and provides the necessary information for iApp Analytics.

Beyond BIG-IP configuration and management, iApp Templates also allow multiple groups within IT to define all of the settings required to deliver and manage an application. A cross-functional team of architects can define the application parameters—from the network team providing IP address information, to the application team configuring a caching and compression policy and the security team defining access polices for users and regions—and roll out procedures in an iApp Template, then deliver the template to IT operations for deployment in test or production BIG-IP devices. Once established, iApp Templates can be modified by the applicable group and reused throughout the organization as business and IT needs evolve.

Another key benefit of iApps is removing the subject matter expert barrier to deploying a new app on the ADC and throughout the infrastructure. Application owners no longer have to think about deploying individual BIG-IP LTM devices for availability, BIG-IP® WAN Optimization Manager™ (WOM) devices for optimization, and BIG-IP ASM devices for security. With iApps, application owners will simply

add those services as part of the iApp application configuration bundle, and the unified BIG-IP platform will deploy the appropriate service and all of the moving parts associated with that service.

Application owners typically spend a great deal of time configuring applications to be delivered through BIG-IP appliances. With iApp Templates, that up-front work can be reused throughout the organization as the ADN scales up and out to additional BIG-IP devices. With completely customizable iApp Templates, organizations can save operating expenses by fine-tuning application policies once, testing them once, and then reusing that work by exporting the configurations and sharing them with additional BIG-IP devices and other IT organizations.

## iApp Ecosystem

iApp configuration policies are designed to be portable between BIG-IP systems and between users. iApp Templates can be exported on a per-application basis and reused throughout the application network. In addition, they can be exported and shared through the iApp Ecosystem on DevCentral, F5's community site, where BIG-IP administrators and developers can create, modify, and share their own iApp Templates for other applications or adjust existing iApp Templates.

F5 will routinely release official iApp Templates for new applications through the iApp Ecosystem on DevCentral; this leverages the engineering work for new applications from F5 partners such as Microsoft, IBM, and Oracle, as well as application templates specific to vertical markets such as financial, government, and health care.

## iApp Analytics

The majority of an iApp policy is geared toward configuring the traffic management components required to deliver applications. However, iApp also includes tools for monitoring applications across the entire ADN and provides real-time application performance statistics, and diagnostic and troubleshooting information such as application response time, network latency, and connection statistics for the entire application, virtual servers, pools, and nodes. Unlike traditional monitoring tools, iApp Analytics collects performance data at the application level, binding the information to the application itself rather than to individual infrastructure components. iApp Analytics also collects other information at the application level, such as a single URL, and details are shared down to individual ADN components such as virtual servers, pools, and nodes. Application owners can monitor

performance from the application through the application servers and all the way down to the network. This allows organizations to monitor exactly how the application is performing in real time based on application response, network conditions, and user context.

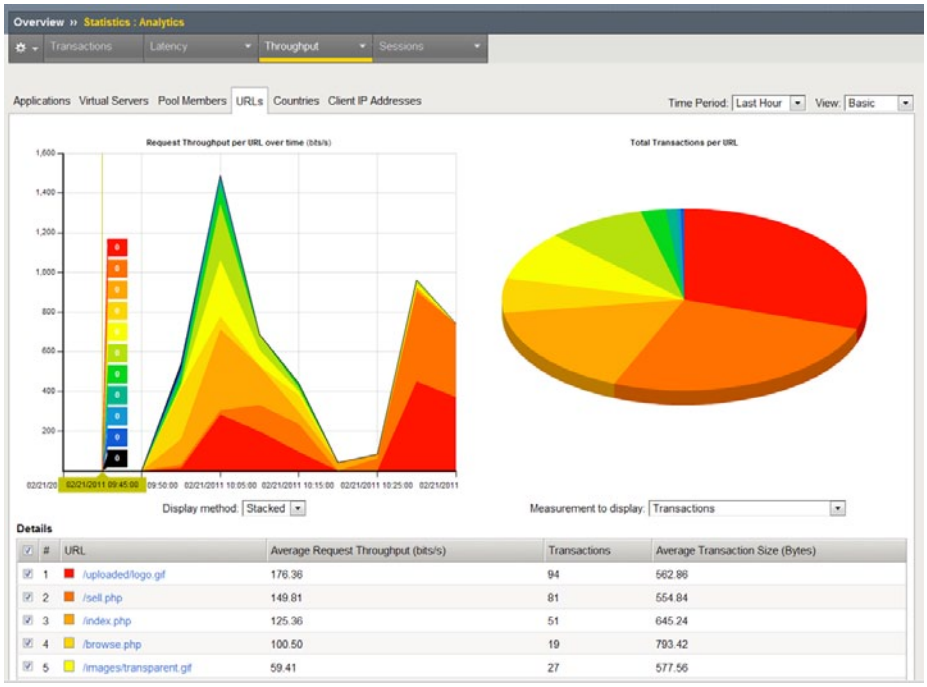


**Figure 1: Per-application visibility and reporting with iApp**

iApp Analytics provides aggregated application visibility and reporting tools at the application level. Rather than providing a long list of statistics for individual components, which doesn't easily equate to application performance, iApp Analytics ties infrastructure performance and availability data to the performance of the entire application. If one node is slow to respond, how does that affect the application for mobile users? iApp Analytics allows the enterprise to measure infrastructure performance as it relates to application delivery, and to factor that application performance data into business intelligence tools such as troubleshooting, ROI calculations, and capacity planning. iApp Analytics goes beyond simply providing a more robust dashboard or more detailed reports and brings real-time performance information back into the ADN, so administrators and automated provisioning systems can make delivery decisions and changes to infrastructure components on the fly on a service-by-service level.

# Device Service Clusters

Data center hardware devices are typically run in redundant pairs, either in Active/Standby (one system manages 100 percent of the duties while another system waits for the first system to go offline before picking up those duties) or Active/Active (both systems distribute the workload between devices). Both redundant configurations are a best practice for any mission-critical hardware deployment, yet they contain one major design flaw: this redundant architecture is based on the entire device failing.

A better approach is to build a fault-tolerant architecture based on what the device is doing at any point during application delivery, rather than whether the entire device is online or down. BIG-IP devices enable a scalable, fault-tolerant architecture at the application level, creating failover protection for application configurations between devices. BIG-IP device service clusters run in two different configuration options: Sync-Only and Sync-Failover modes.

### Sync-Only

BIG-IP device service clusters Sync-Only mode allows multiple BIG-IP hardware and software appliances to dynamically share application-specific delivery configurations and templates between devices, removing the need for an administrator to manually update full device configurations when there are changes. Since BIG-IP application policies are separated from the hardware configurations, administrators can sync application and networking information between devices rather than duplicating an entire BIG-IP configuration file. This enables IT to run different BIG-IP devices with different configurations, but still sync unique application configurations and policies between those devices. For example, BIG-IP® Application Security Manager™ (ASM) policies can be synced between BIG-IP devices without affecting other application policies on each device or requiring the security team to manually install individual BIG-IP ASM policies on each device.

### Sync-Failover

In addition to syncing between devices, application configurations can failover active and live application traffic between devices, taking the Active/Active concept to the application layer. BIG-IP device service clusters Sync-Failover mode extends the 1:1 notion of Active/Active to N:1, where as many Active devices as needed can share the application load depending on resource constraints and availability. This

is very similar to the idea of RAID 5 striping where the number of disks can be determined based on need and redundancy. As more application delivery resources are needed, administrators can add active BIG-IP devices to a device service cluster, which takes on some of the overall application delivery load without adding a second dedicated standby device just in case the new device goes offline. With BIG-IP device service clusters, every new device in the group takes on some amount of redundancy by being available for the extra application load should one of the devices go offline. The more BIG-IP devices that become part of a device service cluster, the more efficiently the application load can be spread between all available devices.

# Strategic Point of Control

Two key tenets of iApps are visibility and control. iApps provide unprecedented levels of availability and control across the entire infrastructure; but this is dependent upon their placement at a strategic point of control, where all application delivery logic can be applied dynamically to all bi-directional application traffic with a coordinated mediation layer between the users, the applications, and the data. This layer presents a consistent interface and set of services that can be used for all applications and data regardless of their current location. This layer uses an intelligent understanding of context—*who* is accessing *what* from *where* and *why*—to determine the optimal connection among users, applications, and data. Finally, it provides a deep understanding of context to inform the underlying application and data elements about the current resource requirements and to instruct the infrastructure to adapt in real time to ensure optimized application and data access.

This strategic flow of application information becomes part of an iApp configuration. Initial configuration with an iApp Template is based on *how* the application should be delivered in an ideal architecture; the application is managed throughout the delivery lifecycle through iApp Templates and BIG-IP device service clusters, providing the *what* and *where*; and finally iApp Analytics brings the *why* portion, enabling dynamic reconfiguration as the application delivery environment changes and reporting that information back to IT for analysis. iApps are in strategic points of control—the only place that allows such granular and broad application delivery management.

# Conclusion

As organizations begin moving to more modular cloud and SaaS models, managing applications becomes more important than building infrastructure. Many of the benefits that come from moving to a more agile model are not associated with managing the infrastructure; yet managing application deployments, performance, and availability in cloud and SaaS environments is often difficult because the application is still tied to infrastructure. iApps bind application control, visibility, and management to the infrastructure required to deliver those applications and services beyond the data center.

iApps support the architecture that transforms a network from a static resource comprising isolated components to a unified, flexible, and resilient pool of resources directly associated with an application or service. This enables rapid network deployment, integration, management, and visibility at the application layer. iApps provide complete control over the entire application delivery infrastructure by adapting the network to the application. The resulting quick deployment and single-point capabilities save operational costs. For the first time, organizations can create a common and highly reusable catalogue for security, acceleration, and availability services at a strategic point of control to dramatically increase the organizational agility and efficiency of F5 BIG-IP devices.

With iApps, F5 has created a paradigm shift in how administrators view and manage the network by moving management responsibility from the network components to the application. iApps increase IT agility and efficiency by enabling organizations to manage the security, optimization, availability, health, and performance of not only the ADN devices in the network, but of the mission-critical applications running the business. In this way, iApps create a truly unified Application Delivery Network.

**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