Achieving A Higher Level Of Business and Network Adaptability With F5's Unified Application Infrastructure Services

Overview

While it is important to understand the numerous features and benefits that F5's BIG-IP traffic management solutions bring to an organization, such as high availability, improving application performance, optimizing infrastructure, and providing unique application security, the goal of this paper is to explore a more fundamental business and technical problem plaguing today's organizations - and how BIG-IP solves it.

Challenges

The Core Challenge: Today's networks are still not intelligent and flexible enough

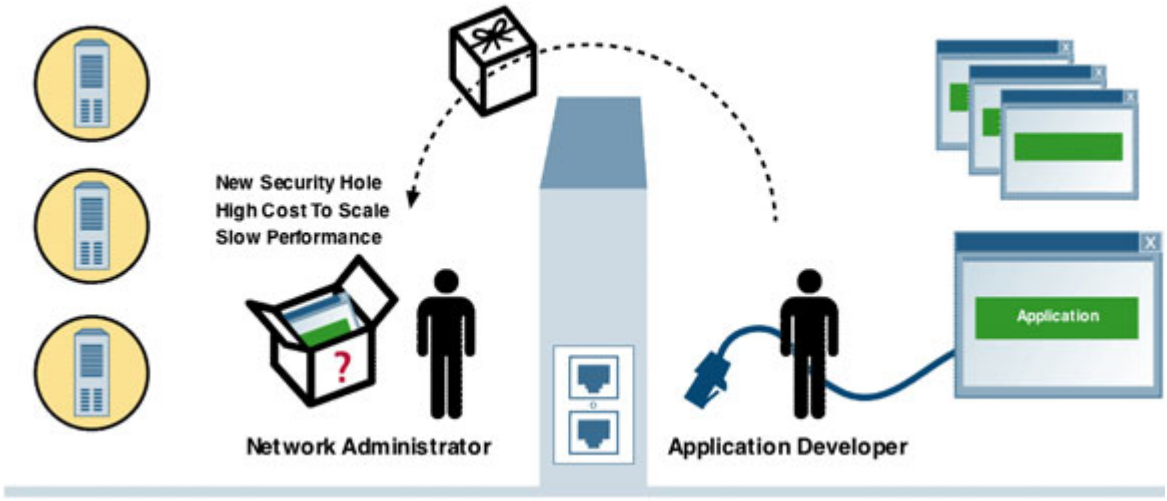
Application delivery challenges are costing organizations millions of dollars -- Clearly, applications have become the lifeblood of modern businesses by connecting the workforce, partners, and customers to information and services. Enterprises that F5 deals with report downtime costs them up to 3.6 million dollars an hour ($1,000 every second). But it is not only about uptime, it is also about how quickly applications can be rolled out, the performance of those applications for the end user, the cost of supporting the infrastructure, and the level of security achieved.

The increasing number of diverse applications is difficult to manage -- With evolving technologies, rapidly changing applications, and unique network requirements, it is often impossible for applications to be optimized right out of the box. Whether the application is developed internally or by a third party, software developers are unable to know or predict myriad issues that will arise. This is partly because of the various conditions that can occur in IP networks (such as Internet latency) and the fact that so many disparate users and systems are trying to communicate and utilize an application efficiently.

There are a number of obstacles and exceptions that arise and usually they are not discovered until it is too late - after the application is deployed. For most organizations, managing the integration and supporting infrastructure around all of their applications is a difficult challenge. Integrating new and old systems, combined with the continuous pressure to roll-out new applications, places more management stress on IT organizations.

The application fire drill -- Organizations often invest millions of dollars in an application, only to discover a driving need for more functionality, or that the application will not scale efficiently, cannot be easily integrated or secured, or is prohibitively slow for remote users across the WAN. The options for fixing these problems usually revolve around coding application changes or installing a point network device. Over time, organizations have typically solved their application problems in the network, which provided a quicker resolution to the problem because the network provides a centralized point of control that can be applied across other applications.

In many cases, the problems of application delivery are compounded further because of the organizational boundaries between application, network and security teams.



Often, an application team concentrates on business functionality and views the network as a socket that is open to them. They believe plugging their application in is all that is required of them. Fundamentally, these teams often have limited understanding of the networking issues that their application will face when being delivered over a diverse network to a varied set of users. These types of challenges are simply not in their domain of expertise.

Conversely, the IT department typically waits for the application to "fly over the wall" - knowing that it is often a problem waiting to happen. When the application is deployed and issues are uncovered, the alarm sounds and the organization must figure out how to solve the problem to protect their very expensive investment.

It is this continuous barrage of application surprises that force many IT and security teams to scurry for quick point solutions. After all, changing the application is difficult, often takes months to accomplish, and in many cases simply is not an option because it is a 3rd party application. For IT, these fire drills have become a common part of life. Administrators often say, "I know we have three critical application projects rolling out in 6 months from different teams, I just have no idea what the applications will look like and how they will behave when deployed."

Existing solutions cannot adapt -- The evidence is clear: walk into any major data center today and you'll find a proliferation of devices that have accumulated over time to solve a particular set of application pains. These sites include myriad point appliances and partially consolidated boxes which aim to improve, at some level, the reliability, cost, performance, or security of delivering the applications. This trend began with devices like load balancers, and has been extended to a number of different technologies and devices that have evolved over time to solve application delivery challenges including rate shapers, SSL accelerators, caches, application proxies, compression devices, DoS and other application security boxes.

What Is Required To Solve the Problem?

IT organizations need a better way to optimize application delivery, bring together needed functions, and address the frequent "application fire drills" without costly application coding, incurring major infrastructure cost, and adding significant management overhead through point and partially consolidated systems. To do this requires a fundamentally new approach which delivers:

- **Complete application intelligence:**
  The solution must be a full participant in the applications in order to completely inspect application flows. With significant investments in legacy applications and a strong need to

migrate them over IP, the solution must handle all IP applications, not just HTTP. Just as voice and data are converging on IP, so are new and legacy applications.

- **Total control over traffic:**
  The solution must be located at a centralized point to carefully target functions and adjust to unforeseen needs. To do this, organizations need total control in exercising the functions required and bridging possible integration issues between application hosts and network consumers.

- **Unified and flexible:**
  The solution must bring together a rich set of functions in a cohesive system that can be easily extended, as networks and application demands are constantly changing. Further, it must quickly and cost effectively adapt to various needs that each application throws at the network.

- **High performance:**
  The solution must combine all of the above functionality, without sacrificing performance. The network device needs to be reliable and scalable to handle core processing needs.

- **Manageable:**
  The solution must be designed to support multiple functions rather than rudimentary consolidation and fit into organizational work flows. Ultimately, the services offered by the solution should be easily repeatable and reusable so that standard services can be created and offered across all business units and application teams.

Solution The Solution: BIG-IP and TM/OS

The BIG-IP® version 9 is a next generation traffic management product from F5. Version 9 was designed to solve the key challenges faced by businesses today: the secure and optimized delivery of their applications.

The fundamental difference between F5's approach and every other product on the market today is F5's design focus. F5's focus was to design a solution that not only offered powerful application traffic management functionality, but a solution that could effectively broker and address the changing demands of networks and applications and the users accessing them.

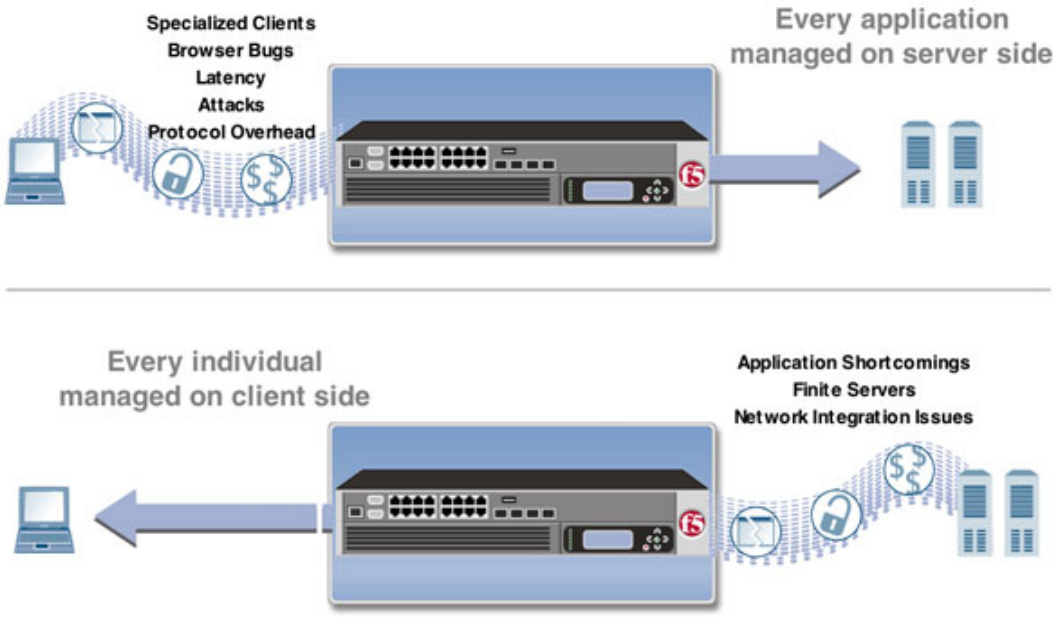
To accomplish this, F5 invested over 450,000 man hours to design a powerful new architecture called the TM/OS (Traffic Management / Operating System). The TM/OS provides a unified architecture which brings new levels of application intelligence and network flexibility that effectively eliminates the "application fire drill."

Total Vision - Complete Application Flows - True Application Fluency

The TM/OS Fast Application Proxy is the cornerstone of this architecture, providing a revolutionary approach which goes beyond any application traffic management solution on the market today. Compared with packet-based solutions, TM/OS enables BIG-IP to deliver market leading solutions that support entire application flows which can facilitate better end-to-end application deployments. The TM/OS Fast Application Proxy delivers:

- **The understanding of two way conversations** - Powered by independent client-side and server-side TCP stacks, the TM/OS Fast Application Proxy can see, inspect and control bi-directional TCP/IP traffic flows from server and client to provide unprecedented adaptability for corporate applications. This enables superior control across all functions of the box by providing a system that can react based on server conditions, error messages, and content being passed back to the clients. For example, leveraging the TM/OS, BIG-IP can spot error codes and take customized action based on 404 or 900 errors to prevent users from seeing content failures.

- **Independent client and server control** - Because the TM/OS engine is by nature a full proxy, the BIG-IP device can now segregate and independently control every application device and user connected to the system. As a full broker of communications, this allows the BIG-IP system to optimize communication for every single end device communicating through it. This optimization can take place up and down the entire stack, from the transport layer to the protocol and application layers. For example, certain browser types like Netscape often have incompatibilities with various applications. The TM/OS can accept input from the application in native form and dynamically translate/transform aspects of the communication or content for successful delivery to that particular client type. In this way, the BIG-IP system acts as an intermediary between disparate systems for superior interoperability. The BIG-IP system provides organizations with superior performance for clients, and a reduced cost of integrating networked applications.



- **Support for legacy applications over IP with session-aware traffic management**
  The BIG-IP system is the only solution able to understand the breadth of IP applications and still provide session based inspection and control. Leveraging the TM/OS, the BIG-IP system allows organizations to forgo proprietary solutions to manage legacy applications, while improving the scale and performance of those resources. For example, legacy applications which pipeline many sessions over single, long lived connections can still be load balanced to scale requests across multiple backend systems.

- **The ability to see and modify all content**
  Building on F5's past innovations, BIG-IP's Universal Inspection Engine has been integrated and expanded to deliver full content payload inspection capabilities -- delivering the ability to see any piece of L7 information including header and payload as it passes through the system. This inspection can be leveraged to better deliver and secure applications.

Integrated and extensible functions - Unified Application Infrastructure Services
Layered on top of the TM/OS is a modular and extensible set of functions called Application Infrastructure Services (AIS). AIS are unified within the TM/OS so that every function running on the BIG-IP leverages the power and control of the core platform.

Unlike simple consolidated functions, Application Infrastructure Services provide superior control to invoke and tune these services based on measured environmental variables (such as TCP RTT of

connecting clients), rich traffic inspection (such as user, application, or payload variables) and even system information (such as CPU load). In this way, organizations gain rich and unprecedented flexibility to target functionality like compression, SSL, rate shaping, cloaking and authentication for each and every application type. These services can now be offered as a unified and repeatable set for any organization's application portfolio.

For example, the TM/OS and compression services combine to provide a more intelligent solution that is unmatched within the industry, including the ability to:

- *Achieve 50% higher compression results by intelligently tuning settings per application type.*
- *Determine the type of connection the request is coming from and target compression to dial-up clients where it is needed most.*
- *Adapt compression effort based on CPU load.*

The power to customize - the only programmable network language

In BIG-IP v9, new iRules language and capabilities provide a paradigm shift for application networking, delivering sophisticated application logic that results in unprecedented intelligence and flexibility for any network. The new iRules language is a powerful, event-based programming language which can leverage any feature delivered on the BIG-IP system. iRules are based on TCL (Tool Command Language) and have been extended to include extensive network/application and traffic events, and rich control capabilities across packets and data flows. This provides organizations with the ability to adapt to the challenges of evolving application networking needs in a cost effective and timely manner.

NOTE: It is important to note that iRules are not required for configuration. The BIG-IP system has a comprehensive user interface which allows users to easily enable functions with a click of a button or by configuring application services profiles through a simple user interface. However, as mentioned previously, we know from first hand experience that it is impossible to predict myriad application challenges that organizations experience daily and to pre-define them in a template. The iRules feature was designed to overcome these application challenges. iRules provide an unprecedented level of control by which organizations can apply more intelligence and more quickly adapt than any other solution.

In order to demonstrate the power and flexibility of iRules, here are a few simple security examples:

Rule 1 - Cloaking: This is used to clean the Web server signatures so that unwanted information is not transmitted to hackers who are attempting to fingerprint the application and servers which run on your Web site. The alternative to cloaking is to attempt to police and clean information being sent out by various applications - creating significant management overhead. This rule removes all of the non-essential headers that are not in the inclusion list.

```
rule when HTTP_RESPONSE {
  #
  # Remove all but the given headers.
  #
  HTTP::header sanitize "ETag" "Content-Type" "Connection"
}
```

Rule 2 - Selective encryption: By encrypting cookies, organizations eliminate security risks such as session hijacking and cookie tampering, which allow hackers to falsify identity to access

systems. This rule demonstrates the ability to encrypt and decrypt arbitrary HTTP cookies:

```
rule when HTTP_REQUEST {
  #
  # Decrypt the cookie on its way to the server.
  #
  HTTP::cookie decrypt "cookie_name" "password-key"
}
rule when HTTP_RESPONSE {
  #
  # Encrypt the cookie on its way to the client.
  #
  HTTP::cookie encrypt "cookie_name" "password-key"
}
```

Rule 3 - Content protection: This is a simple rule that selectively collects, inspects and replaces any instance of social security numbers from server responses. Organizations can use a rule like this to protect and cleanse any sensitive data from leaving their site:

```
rule ssn_rule {
when HTTP_REQUEST {
  Set secure_dir "/cgi-bin/"

  # Check for sensitive documents.
  if {[HTTP::uri] contains $secure_dir } {
    set check_content 1

    # Don't allow data to be chunked.
    if {[HTTP::version] == "1.1"} {
    if {[HTTP::header is_keepalive]} {

      # Adjust the Connection header.
      HTTP::header replace "Connection" "Keep-Alive"
    }
    HTTP::version "1.0"
   }
  } else {
   set check_content 0
  }
  }

when HTTP_RESPONSE {
  if {$check_content == 1} {
  # Calculate the amount to collect
  set content_length 0
  if {[HTTP::header exists "Content-Length"]} {
   set content_length [HTTP::header "Content-Length"]
  }

  # If the header is missing, use a sufficiently large number
  if {$content_length == 0} {
    set content_length 4294967295
  }
  HTTP::collect $content_length
```

```
  }
 }
when HTTP_RESPONSE_DATA {
  set payload [HTTP::payload [HTTP::payload length]]
  set ssnx "xxx-xxx-xxxx"

  # Find the SSN numbers
  regsub -all {\d{3}-\d{2}-\d{4}} $payload $ssnx new_response

  # Replace the content if there was a match
```

Architected for the future
The TM/OS provides a modular design by which new AIS's can be rapidly developed and incorporated. This allows organizations to quickly add new functions, resulting in better network adaptability. As other needs develop, such as XML parsing, organizations have a centralized location in the network for intelligent processing. In addition, the BIG-IP system and its TM/OS were designed from the ground up to handle emerging network requirements like IPv6. The TM/OS architecture provides complete IPv6 gateway support for organizations that need to translate between addresses. This provides a powerful solution to gracefully transition new IPv6 services and avoid expensive application rewrites.

Real world performance at network speeds
Unlike many solutions which are architected to perform well for benchmarks with isolated functions, the TM/OS architecture delivers leading performance in real world deployments. Through an optimized traffic processing architecture, the TM/OS delivers lower latency processing and superior scalability for running multiple services on a given traffic flow. F5 combines this revolutionary new software architecture with an industry leading line of new application switches which integrate a variety of ASICs and hardware offload solutions with high performance processing to handle core traffic requirements.

Becoming more application aware
The TM/OS architecture allows F5 to extend the capabilities of iControl®, our industry-exclusive open API and SDK, by offering tighter and more granular integration. With accelerated performance and optimized capabilities for complex applications, this SOAP/XML API and TM/OS enable superior application intelligence and integration.

- iControl API - iControl extends the control plane so that applications can influence the network. By integrating iControl into the core TM/OS, applications can realize faster performance and more options in terms of requests to the API. Whether a simple application is making basic requests or advanced applications are performing bulk requests, iControl v9 offers increased performance and control.

- Event API - iControl has been extended into a full event service that allows applications to subscribe to a vast list of events that occur on a BIG-IP system. This enables better real-time tracking of events that occur on the network while reducing the network traffic and chatter required for constant requests being placed by pull-based applications. Event messages can be delivered flexibly in either verbose or even compact formats ideal for pagers or PDAs.

Summary BIG-IP version 9 is a revolutionary departure from traditional traffic management devices. The new BIG-IP system, with its Traffic Management Operating System and Application Infrastructure Services, as well as iRules, allows organizations to easily adapt to evolving application requirements and diverse networks. This provides a more intelligent and adaptable way to secure,

optimize, and deliver applications, enabling organizations to efficiently and competitively run their business.

Unlike the competition, F5 offers the only unified application traffic management architecture designed specifically to understand and act upon entire application flows and all IP application types, which results in greater business agility and successful outcomes for an organization's applications. BIG-IP version 9 eliminates the need for numerous point solutions, consolidating the functionality on a unified platform that can be easily leveraged and extended. The BIG-IP system transforms the network into a competitive advantage for any business.

About F5 F5 enables organizations to successfully deliver business-critical applications and gives them the greatest level of agility to stay ahead of growing business demands. As the pioneer and global leader in Application Traffic Management, F5 continues to lead the industry by driving more intelligence into the network to deliver advanced application agility. F5 products ensure the secure and optimized delivery of applications to any user - anywhere. Through its flexible and cohesive architecture, F5 delivers unmatched value by dramatically improving the way organizations serve their employees, customers and constituents, while lowering operational costs. Over 6,000 organizations and service providers worldwide trust F5 to keep their businesses running. The company is headquartered in Seattle, Washington with offices worldwide. For more information go to www.f5.com.