



**FOR IMMEDIATE RELEASE**

**CONTACTS:** Alane Moran  
F5 Networks, Inc.  
206/272-6850  
a.moran@f5.com

Holly Hagerman  
Connect Public Relations  
801/373-7888  
hollyh@connectpr.com

## **F5 Provides Essential Capabilities for Federal Government Agencies to Improve Security and Efficiency while Driving Costs Down**

*New **BIG-IP® v11** helps agencies and organizations achieve a stronger security posture and improve attack protection for network, applications, and data*

**SEATTLE, JULY 26, 2011** – [F5 Networks, Inc.](#) (NASDAQ: FFIV), the global leader in Application Delivery Networking, today announced that its [BIG-IP® version 11 software](#) delivers end-to-end application access control to help [federal government organizations](#) improve their security posture and minimize the risk of network- and application-based attacks. Enhancements in BIG-IP v11 are especially applicable to federal government agencies and contractors, as well as any public sector organization working to secure its environment against cyber threats while keeping service levels high and costs low.

Today, IT departments are migrating more information and data to virtual and cloud environments to reduce costs and boost service levels, but the decentralized nature of cloud environments makes it increasingly difficult to ensure application and data security. For instance, attacks related to [DNS](#) services and interactive Web 2.0 applications are on the rise. Government agencies saw a 39 percent growth in cyber incidents in 2010<sup>1</sup>, marking a 445 percent increase in cyber attacks since 2006<sup>2</sup>. And in recent years, government agencies and public sector organizations also have experienced their share of WikiLeaks-style breaches of confidential information.

While battling a proliferation of increasingly complex attacks, government agencies and public sector organizations are also tasked with meeting progressively stringent mandates and standards. These include data center consolidation efforts, the “[Cloud First](#)” initiative, and federal requirements like the [Federal Information Security Management Act of 2002](#) (FISMA), [Federal](#)

[Information Processing Standards](#) (FIPS), and [Domain Name System Security Extensions](#) (DNSSEC).

In addition, agencies must do all of this while operating within the constraints of today's budget deficits. Traditional static data center solutions further restrict the IT organization. For instance, to prevent DNS [denial of service \(DoS\) attacks](#), many IT departments scale their DNS infrastructure by adding more DNS servers. This drives up hardware costs, adds to administrative complexity, and increases IT management overhead—without achieving the linear performance scalability that's required.

### **BIG-IP v11: Flexible and Dynamic Attack Protection and Access Control**

Fourteen of the 15 executive branch departments of the U.S. government, as well as numerous Department of Defense and civilian agencies rely on [BIG-IP solutions](#) to boost application performance and security. With BIG-IP v11, these organizations and others can take advantage of an application-centric model for application delivery—in both physical and virtual environments. Building on the extensive capabilities of previous versions, BIG-IP v11 provides additional services to support the dynamic data center while enhancing security and improving IT efficiency.

For instance, through its unique and layered network and application security infrastructure, BIG-IP v10 delivered scalable, flexible, and controlled global and local DNS solutions; FIPS compliancy; and the ability to preconfigure applications to prevent security vulnerabilities. As a strategic point of control for Application Delivery Networking, BIG-IP v11 helps organizations secure the latest interactive web applications, deliver high-performance and scalable DNS responses, and improve authentication, authorization, and single sign-on services to control how users are allowed to access applications.

“BIG-IP v11 delivers a centralized point of control for security, enabling government agencies and other organizations to respond dynamically to constantly changing web threats,” said Erik Giesa, VP of Product Management and Product Marketing at F5. “We’ve made significant advancements in this release, for example, with [iApps™](#) templates that provide appropriate configuration settings for [NIST 800-53](#) compliance, making it quick and easy to deploy new devices and check configurations of existing ones. With BIG-IP v11, we look forward to helping

our federal government customers improve their security posture and scale to support global environments—all while dramatically reducing IT infrastructure and administrative costs.”

## **Details**

BIG-IP v11 provides many enhancements to application delivery, control, and security. A few of the most notable advancements include:

- **Dynamic Services for Unified Access and Security Control**

BIG-IP v11 introduces iApps, a template-driven system that automates application deployment. iApps technology helps reduce human error by enabling an organization’s IT department to apply preconfigured, approved security policies and repeat and reuse them with each application deployment.

- **Advanced Analytics and Reporting Capabilities**

Through iApps™ analytics, BIG-IP v11 provides real-time visibility into application performance, which helps IT staff identify the root cause of security and performance issues quickly and efficiently.

- **Sophisticated Protection Against DNS Attacks**

DNS Express™, a new feature of [BIG-IP Global Traffic Manager](#)™ (GTM™), is a high speed, in-memory DNS engine. When BIG-IP GTM is positioned in front of an organization’s main DNS servers, DNS Express handles DNS requests up to ten times faster—a speed that makes DoS attacks easier to withstand. Combined with DNSSEC, DNS Express helps federal government agencies successfully respond to complex attacks and consolidate DNS infrastructure by up to 70 percent to reduce CapEx and OpEx.

- **Protection for Interactive Web 2.0 Applications**

Using a new [JavaScript Object Notation](#) (JSON) parser, F5’s [BIG-IP Application Security Manager](#)™ (ASM™) web application firewall protects JSON payloads and [Asynchronous](#)

[JavaScript and XML](#) (AJAX) widgets from application attacks. In the event of a policy violation, BIG-IP ASM displays a unique blocking page that includes a support ID so users can contact the network administrator for resolution.

- **Support for Internet Protocol version 6 and version 4 (IPv6 and IPv4)**

BIG-IP v11 provides advanced support for IPv6 with built-in DNS 6-to-4 translation services and the ability to direct traffic to any server in mixed IPv4 and IPv6 environments. This gives organizations the flexibility to support IPv6 devices today while transitioning their backend servers to IPv6 over time.

- **Enhancements to Application Access and Accelerated Remote Access**

BIG-IP v11 with [BIG-IP Access Policy Manager](#)<sup>™</sup> (APM<sup>™</sup>) provides a central point from which to manage authentication, single sign-on, and access control lists for web applications. BIG-IP APM supports site-to-site IPsec tunnels, application tunnels, Kerberos ticketing, enhanced virtual desktops, Android and iOS clients, and multi-domain single sign-on. Additionally, APM functionality can be deployed as part of the [BIG-IP Edge Gateway](#)<sup>™</sup> solution—a package that combines the capabilities of BIG-IP Access Policy Manager, [BIG-IP WebAccelerator](#)<sup>™</sup>, and [BIG-IP WAN Optimization Manager](#)<sup>™</sup>—to support up to 60,000 concurrent users.

### **Supporting Quotes**

“The migration to the cloud offers significant potential for reducing infrastructure and administration costs while improving services, but it also creates serious security challenges,” said Jeff Wilson, Principal Analyst, Security, [Infonetics Research](#). “F5’s BIG-IP v11 addresses these challenges and equips government agencies with the proper tools to execute on the federal [25-point IT reform action plan](#), so that government can take full advantage of IT to better serve its constituents.”

“Government agencies are under increasing pressure to meet the White House’s cybersecurity legislative agenda, achieve data center efficiency, and take action on the 25-point action plan for solving federal IT challenges,” said Craig P. Abod, President of [Carahsoft](#), an IT solutions provider for federal, state, and local government agencies. “F5’s BIG-IP v11 addresses these

challenges by helping agencies build highly secure and adaptable cloud-ready infrastructures, while providing capabilities to easily control user access to resources. As F5 Networks' government contract aggregator and distributor, we are excited to make this solution available to our extensive network of reseller partners and our government customers.”

### **TechValidate Stats**

TechValidate, an independent research organization, recently analyzed data collected from F5 federal government agency customers and contractors that have experience with BIG-IP solutions. In response to the survey, customers reported the following:

- **Federal Agencies Improve Application Security with F5** – Over half of federal IT organizations have enhanced application security by deploying F5 BIG-IP solutions. (Source: TechValidate. [TVID: A52-6DD-0BC](#))
- **F5 Supports Government Compliance and Certification Requirements** – Nearly half of federal IT organizations purchased F5 BIG-IP solutions over alternatives to support government compliance and certification requirements including DNSSEC, Common Criteria, FIPS, and IPv6. (Source: TechValidate. [TVID: 429-105-ACF](#))
- **F5 Improves Application Performance for Federal Agencies** – 70 percent of federal IT organizations have improved application performance with their F5 BIG-IP solutions. (Source: TechValidate. [TVID: E90-432-06E](#))

### **Background Data: Security Statistics for Federal Agencies**

Of 107,439 incidents reported to the [US-CERT](#) in FY2010<sup>1</sup>:

**Phishing:** 56,579 incidents, 52.7 percent of incidents.

**Virus/Trojan/worm/logic bomb:** 11,001; 10.2 percent

**Malicious website:** 7,971; 7.4 percent

**Non-cyber:** 7,741; 7.2 percent

**Policy violation:** 6,888; 6.4 percent

**Equipment theft/loss:** 5,395; 5 percent

**Suspicious network activity:** 3,121; 2.9 percent

**Attempted access:** 2,712; 2.5 percent

**Social engineering:** 1,571; 1.5 percent

### **Additional Resources**

- [BIG-IP v11 Information Page](#)
- [BIG-IP v11 DevCentral Page](#)
- [iApps Page on DevCentral](#)
- [F5 iApps: Moving Application Delivery Beyond the Network – White Paper](#)
- [High-Performance DNS Services in BIG-IP Version 11 – White Paper](#)
- [Secure, Optimized Global Access to Corporate Resources – White Paper](#)
- [Securing JSON and AJAX Messages with F5 BIG-IP ASM – Solution Profile](#)

### **Availability**

BIG-IP version 11 software and virtual editions of F5's [BIG-IP Global Traffic Manager](#), [Application Security Manager](#), and [WAN Optimization Manager](#) products will be available in the third quarter of calendar year 2011.

### **About TechValidate**

TechValidate is a trusted third-party service that verifies the usage, configuration, and benefits of technology products and services. The company directly interfaces with business and technology end users to collect and validate information about their deployments. TechValidate's promise to the end-user community is to provide unbiased, verified information about the usage and benefits of technology products and services. More information is available at [www.techvalidate.com](http://www.techvalidate.com).

### **About F5 Networks**

F5 Networks, Inc., the global leader in Application Delivery Networking (ADN), helps the world's largest enterprises and service providers realize the full value of virtualization, cloud

computing, and on-demand IT. F5<sup>®</sup> solutions help integrate disparate technologies to provide greater control of the infrastructure, improve application delivery and data management, and give users seamless, secure, and accelerated access to applications from their corporate desktops and smart devices. An open architectural framework enables F5 customers to apply business policies at “strategic points of control” across the IT infrastructure and into the public cloud. F5 products give customers the agility they need to align IT with changing business conditions, deploy scalable solutions on demand, and manage mobile access to data and services. Enterprises, service and cloud providers, and leading online companies worldwide rely on F5 to optimize their IT investments and drive business forward. For more information, go to [www.f5.com](http://www.f5.com).

You can also follow [@f5networks](https://twitter.com/f5networks) on Twitter or visit us on [Facebook](https://www.facebook.com/f5networks) for more information about F5, its partners, and technology. For a complete listing of F5 community sites, please visit [www.f5.com/news-press-events/web-media/community.html](http://www.f5.com/news-press-events/web-media/community.html).

F5, BIG-IP, iApps, DNS Express, Global Traffic Manager, GTM, Application Security Manager, ASM, Access Policy Manager, APM, Edge Gateway, WebAccelerator, and WAN Optimization Manager are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries. All other product and company names herein may be trademarks of their respective owners.

<sup>1</sup>“Federal Cyber Incidents Rose 39% in 2010,” Government Information Security News, [http://www.govinfosecurity.com/articles.php?art\\_id=3463&rf=2011-03-24-eg](http://www.govinfosecurity.com/articles.php?art_id=3463&rf=2011-03-24-eg), March 24, 2011.

<sup>2</sup>“Government IT contractors remain optimistic about future,” Homeland Security Newswire, <http://www.homelandsecuritynewswire.com/government-it-contractors-remain-optimistic-about-future>, January 12, 2011.

This press release may contain forward looking statements relating to future events or future financial performance that involve risks and uncertainties. Such statements can be identified by terminology such as "may," "will," "should," "expects," "plans," "anticipates," "believes," "estimates," "predicts," "potential," or "continue," or the negative of such terms or comparable terms. These statements are only predictions and actual results could differ materially from those anticipated in these statements based upon a number of factors including those identified in the company's filings with the SEC.

###