White Paper

Strategic Solutions for Government IT

The U.S. government wants to transform its IT organization to streamline operations and smooth the transition to the data center of the future. To this end, it is moving an increasing number of applications to the cloud; minimizing duplicated IT efforts; and improving the dialogue between federal providers and contracting personnel—all with the goal of making government IT resources more flexible, reliable, and secure. This will be a project of tremendous scale that requires strategic decisions and smart, flexible technology. F5 Networks is the optimum partner to help achieve the levels of security, performance, and availability that are vital to the government IT organization of the future.

by Don MacVittie
Technical Marketing Manager

Contents

Introduction

The U.S. government is aiming to reinvent its IT organization so that it more closely resembles enterprise IT. A change of this magnitude would be significant for anyone; but for one of the largest IT environments in the world, it can seem almost insurmountable. Government IT has security requirements ranging from "no one can ever see this but the recipient" to "nearly everyone in the world must be able to access this," so the discomfiture can be acute.

All of this change must occur while budgets are flat, shrinking, or even disappearing altogether. From the government's new Cloud First policy to FIPS compliance; from IPv6 to Open Government; and from FISMA to DNSSEC, the IT workload is always increasing—but there are seldom budget increases to match.

It has been said that the future is bright, but the path to get there is long and dark. However, the government can light this path by working more closely with vendors and enterprise IT to bring about meaningful change in its own IT. Vendors are adroit in their specific domains, and enterprise IT has expertise that may not exist within the public sphere. By collaborating with both, government IT can create a clearer, more simplified path to its vision of the future—all while containing costs. Like those in the private sector, government IT must figure out how to do more with less: fewer contractors, more automation, and overall cost reduction. To achieve its goals, government IT can rely on both enterprise IT and vendors with strong knowledge of a given subject.

F5 Networks® is one of those vendors. F5 can ease impending directives, such as IPv6 implementation, making other resources available to execute changes that are more sweeping and less utilitarian.

Virtualization, Cloud, and the BIG-IP System

"F5 BIG-IP WebAccelerator enables us to handle peaks in our web activity. SSL acceleration allows us to manage all SSL certs in one place, greatly reducing management overhead. The openness of the platform through our vast collection of iRules allows complete control and customization of our environment to fulfill our mission."

Source: TechValidate Survey of a Federal Government Agency

TVID: CA7-97D-D09

Data Center and Cloud Interoperability

Moving a large number of systems to the cloud is a quick way to cut capital expenditures. The government's Cloud First policy is designed to "accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new

investments."[1] Moving to the cloud, however, presents its own set of challenges. Whenever data has to move from data center to data center, or between a data center and the cloud, Internet connection performance can become a bottleneck and affect the performance of the overall IT architecture. When addressing these challenges, administrators should consider:

- Most software is written to communicate at LAN speeds, not WAN speeds.
- Large datasets such as results from backup or replication operations can flood the bandwidth available, even if the WAN is high-speed.
- Security of data as it passes out of a WAN connection and over the Internet becomes paramount, particularly when personally identifiable information (PII) or top-secret information is being transmitted.

An Application Delivery Controller (ADC), together with a WAN optimization solution, can help organizations manage these problems without requiring extensive changes to existing application infrastructure.

BIG-IP® WAN Optimization Manager™ (WOM), which runs on the BIG-IP® Local Traffic Manager™ (LTM) ADC, offloads encryption from servers or special-use devices to F5's industry-leading hardware. BIG-IP WOM compresses and deduplicates data as it flows across the wire. The net result is less data passing through the data center WAN connection. State-of-the-art, 128-bit-key technology and a highly optimized encryption engine ensure data security.

Meanwhile, government IT needs to extend the policies and profiles it has implemented for the core data center to remote locations—whether they're secondary data centers or in the cloud—by utilizing BIG-IP LTM in the core data center as a master controller of web application traffic. BIG-IP® Application Policy Manager™ (APM) can run on BIG-IP LTM in the primary data center to extend protection to remote applications.

With F5 ARX® intelligent file virtualization and ARX Cloud Extender,™ the government can seamlessly extend its file storage infrastructure from the data center to the cloud. Customizable tiering policies automate the process of identifying and moving data to the cloud, and data stored in the cloud is presented as if it resides locally in the data center, so users and applications can access information as they always have. ARX encrypts data on the way to the cloud provider and decrypts it on the way back in to the data center, so IT data is secured while off of the LAN and the cloud is available for storage at a massive scale.

1 http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf

With ARX's advanced file virtualization technology, Tier 3 storage, archival storage, replication, and backup can now all occur in the cloud. One of the quickest and easiest ways to start utilizing the cloud is to migrate old and seldom-accessed files to encrypted cloud storage. These files can still be retrieved at any time, but they are not cluttering up local NAS, so government IT can minimize its investment in NAS.

Security in the Wider World

While most ADC functionality is readily understandable when extended to the cloud, security can be tricky for access to any remote application, because information about who has access is generally stored in the data center. Virtual editions of BIG-IP® Application Security Manager™ (ASM), F5's web application firewall, and BIG-IP APM (for VPN access) extend functionality to the cloud, similarly to other F5 products, except that a return call may be required to access ADS or other AAA tools to complete authentication.

While it is not 100 percent intuitive to offer up security from a primary data center to cloud-based applications, the only effective alternative is to replicate an AAA product into the cloud and authenticate "locally" to the cloud. This introduces synchronization issues and can fracture reporting about attempted attacks between internal and external resources.

Extending Data Center Control to the Cloud

The data center already has a wealth of information about valid users, application access rights, load balancing, and file tiering. F5's physical and virtual products provide a platform for using this information to make important decisions about routing users to the correct location, moving files automatically to the appropriate tier, and extending application security to include remote data centers and the cloud. Because infrastructure is adapting to the needs of the applications, existing applications written with load balancing in mind do not need to change; rather all of the work on adaptability is done at the F5 device or VM layer.

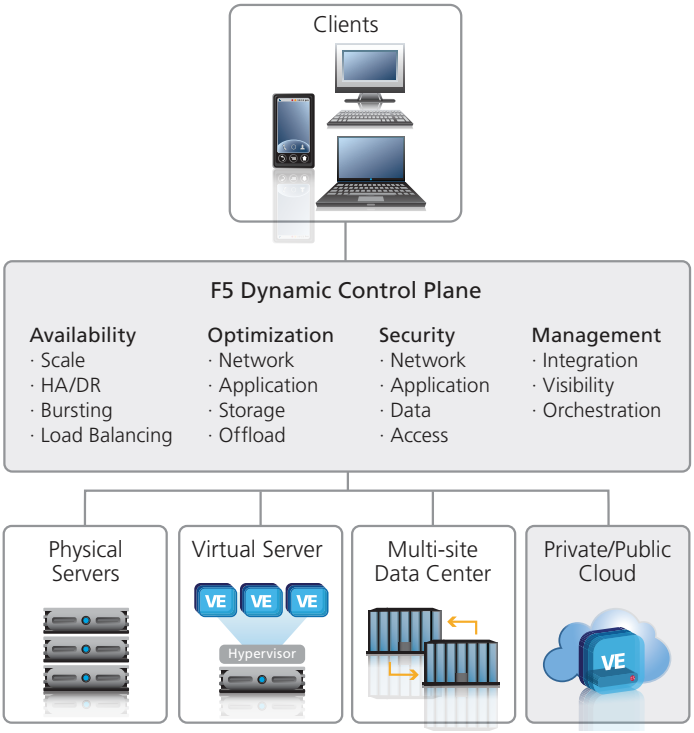

Figure 1: F5 is in physical and virtual servers, multiple data centers, and the cloud

Physical devices that can coordinate the heaviest loads provide a level of adaptability that, when combined with virtual devices that can be deployed anywhere a VM can be deployed, enables government IT to keep the network unified as it spreads across a variety of platforms.

Virtualization

Virtualization will be a key factor in the government's bid to transform its IT, whether it's increasing virtualization efforts to gain efficiency or moving applications to the cloud. F5 BIG-IP® products enable organizations to increase virtualization by offloading critical functionality and intelligently routing connections; and ARX offers streamlined access to NAS and cloud storage with improved performance and resource leveling. BIG-IP products support all three major virtualization vendors quickly and intuitively, allowing government IT staff to support multiple vendors or switch between them. Be it VDI or data center virtualization, the BIG-IP system is designed with IT needs in mind.

Mobile Device Access

Mobile devices are continuing to transform the way many industries operate, and the federal government is no exception. In fact, the U.S. General Services Administration has established the Making Mobile Gov Project to help government agencies meet the needs of constituents. "The federal government must deliver services and information always, anytime, anywhere. Many agencies are already pushing the government's adoption of consumer mobile services."[2]

Mobile devices present a new set of challenges for federal IT organizations. More and more, employees are working remotely. They're also using their own laptops, tablets, and smartphones to work. Even employees who work remotely and are issued laptops and smartphones often want access from their preferred tablet.

Allowing sensitive application access for individuals who need it to do their job while blocking access for the rest of the public Internet will be a long-term goal for government IT. The primary obstacle is of course security; but IT must also address how critical applications are downloaded to devices with limited bandwidth and limited storage. There is no value in granting file or application access to individuals if they cannot actually use the file or application.

For government IT, the perceived performance of its public-facing websites is as important as its ability to accommodate employees, since all U.S. citizens and most citizens of other countries are valid guests. As with employees, many people use their phones to find the one bit of information they need right now—for example, the hours of Yellowstone National Park or how much beer they can bring back from Canada.

BIG-IP APM can authenticate users and provide access to applications, while stopping those without access rights before they ever get to the server the application is running on. This is important, because it lessens the threat vector from vulnerabilities in operating systems or port listening services. By working with the existing AAA solution, BIG-IP APM complements rather than replaces an existing infrastructure. BIG-IP APM leverages the infrastructure to provide not only authorization, authentication, and access control, but to prevent the user from seeing the target machine unless they have the rights to get there. If they do not have rights, BIG-IP APM directs them to an error page not on the application server, and away from sensitive information.

2 http://www.gsa.gov/portal/category/101571

CAC PKI authentication can be configured in BIG-IP LTM to manage constrained delegation across a federated infrastructure. This means that once CAC is supported, a trust relationship between authentication domains is all that users from another agency need to access applications. BIG-IP LTM will handle CAC PKI authentication across domains, or to Kerberos in general.

BIG-IP® WebAccelerator™ can optimize content for various devices, providing maximum flexibility in how a page is delivered to slower connections and smaller storage environments, and optimizing the experience for small devices without requiring a large amount of recoding. Better performance without a rewrite is the ideal solution to small device issues.

Living Documentation and Open Collaboration

Former Federal CIO Vivek Kundra was a strong proponent of improving relationships between government and industries via more open collaboration, and using living documentation to transfer knowledge. In late 2010, he issued an implementation plan addressing those issues.

F5 strongly believes that both open collaboration and living documentation can offer many benefits to government IT without requiring significant funding. To explore the potential of open collaboration among peers and living documentation, F5 created DevCentral. It intended to achieve just what Kundra suggested—but the benefit to customers exceeded expectations.

DevCentral (devcentral.f5.com) is an online community that offers practical, real-world solutions and discussions to bridge the gap between application developers and network professionals. DevCentral offers tools, techniques, and collaboration to help the F5 user community create and build upon solutions. Users can discuss F5 products, best practices, and even some partner products. They can also find living documentation for several special features of F5 technology, including the iRules® scripting language, the iControl® programming API, the TMSH (TMOS® Shell) command-line interface and GUI, and F5 Management Packs. This documentation originated with F5 employees, but has grown with user participation to include working samples, explanations of settings on F5 devices, and how-to articles that help users get the most out of their F5 products.

This type of interaction within government IT—both staff joining internal and vendor sites like F5's DevCentral, and living documentation in the form of internal Wikis of "tribal knowledge" and systems implementation histories—would help government IT manage its rapidly changing environment. It would allow those with key knowledge to document existing systems in a public area, while allowing those planning the future of government IT to access this information so they can chart a way forward.

Perhaps the most significant hurdle when developing a community is time. A community won't spring up overnight, and if unattended, it will likely become obsolete. The first six months in particular are key—a dedicated staff must encourage participation and be the last resort for content. Long-term, with both user retention and attracting new users in mind, this staff must manage information flow and direct users to the resources they need via both indices and articles. Information about various initiatives and projects must be constantly refreshed. DevCentral had 14,000 users in 2007; today it has over 80,000 and thousands of pages of conversation and documentation, proving that if properly nurtured, such a platform can reap great benefits to the IT user community.

Changes Are Coming

The IT sphere is constantly evolving, and infrastructures must keep pace. Government IT in particular can expect more change than most IT organizations, simply because of its size and the amount of sensitive content it must manage and share.

IPv6

The government uses a large number of public IP addresses, and as the progenitor of the IP standard, it will be one of the first large organizations to take the plunge and implement IPv6.

But even after World IPv6 Day in January 2011, questions linger about whether a large organization can move to IPv6 before the bulk of its clients have begun accepting IPv6 packets.

F5 IPv6 Gateway™ and BIG-IP® Global Traffic Manager™ (GTM) can help ease the transition to IPv6 in several ways. First and foremost, both products support IPv6 translation, which allows an organization to keep IPv4 internally while supporting IPv6 externally. This is not a viable option for the long term, but in the short term it allows an organization to support up-and-coming IPv6 clients without excluding

the bulk of the world's clients. They also allow routing by version, so IPv4 connections can be routed to one destination while IPv6 connections are routed to another, enabling IT to move applications and servers to IPv6 in a managed way, rather than with the all-or-nothing approach of "flicking the switch."

By keeping IPv4 support, government doesn't have to leave the bulk of citizens behind, because it can move applications to IPv6 at its leisure as the client base supports it. This approach neatly solves the looming IPv6 problem.

Furthermore, the BIG-IP system handles application translation between IPv4 and IPv6—so applications whose function includes looking at packet-layer information will be insulated from the changes required to support IPv6. Government IT will never have to rewrite an application to support both types of communication.

DNSSEC

From DNS poisoning to DoS, the hazards DNSSEC can guard against are broad. Because it's imperative to address these threats to sensitive information in a timely manner, government IT will implement DNSSEC much more quickly than other organizations with similar challenges.

BIG-IP GTM includes DNS Express, a high-speed DNS system that sits in front of core DNS servers to mitigate DoS attacks while serving up the information in the core DNS servers. From this location, DNS Express can reduce DNS infrastructure by improving performance per DNS server.

Conclusion

Government IT is facing many challenges in the next five to ten years, and all indications are that funding will be tight. F5 can provide solutions for its most critical problems. Those solutions are proven to save money in the long term, and the modular nature of the BIG-IP system means that government IT can deploy one set of hardware to meet a variety of needs.

F5 not only has the tools to help government IT tackle some of the largest issues looming on the horizon, but hosts an example of a thriving community that includes community maintained documentation, peer relationships, and a hefty dose of peer-to-peer assistance that is readily accessible to government IT staff.

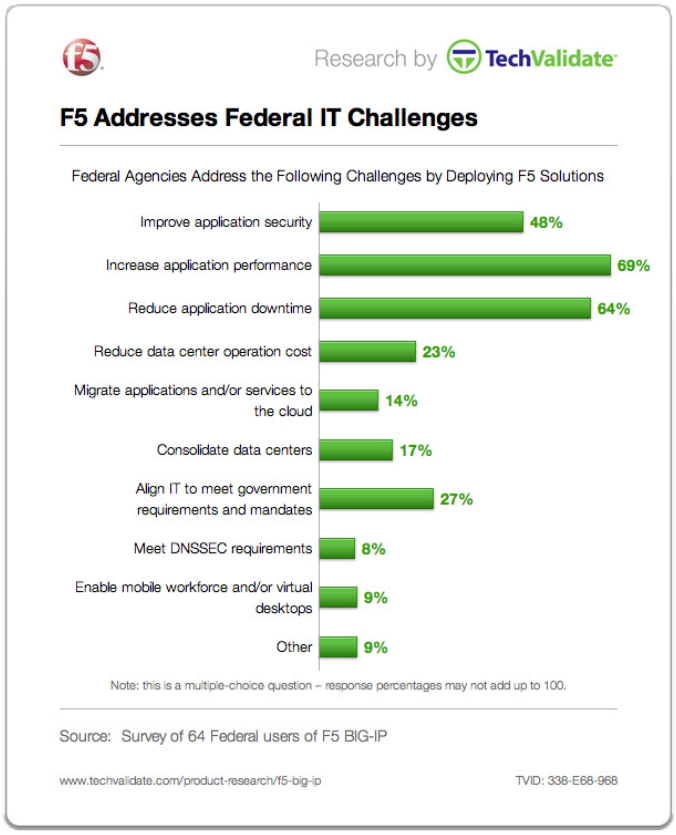

Figure 2: F5 products can address the spectrum of challenges government IT is facing

On DevCentral some of the toughest questions about utilizing F5 products in a production environment are asked and answered, and at a minimum it is a good place to start research about whether F5 products are suitable to an upcoming project. At the maximum, this multi-platform social networking site is a good example of how collaboration within government could be improved with minimum overhead.

Combine the Application Delivery Controller functionality of the award-winning BIG-IP platform with ARX file virtualization and tiering, and government IT can do more with less, while achieving various goals and mandates.

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