



F5 White Paper

Security and Acceleration— the Sweet Spot of Application Delivery

Few vendors want to admit that adding a web application security solution can also add latency, which can be kryptonite for websites. No website, especially an e-commerce site, wants to add any delay to users' interaction. Web application security that also delivers blazing fast websites might sound like an oxymoron, but it is not with F5.

By Peter Silva

Technical Marketing Manager



Contents

Introduction	3
The Security Half	3
The Acceleration Half	4
<hr/>	
What's the big deal?	5
<hr/>	
The Sweet Spot	6
<hr/>	
How It All Works Together	6
<hr/>	
Conclusion	7



Introduction

It's like the old Reese's peanut butter cups commercial, but now we are talking about security acceleration instead of candy bars. "You've stuck your security in our acceleration." "Yeah, well your acceleration has broken our security." Securing applications and preventing attacks while simultaneously ensuring consistent, rapid user response, is a basic web application requirement. Yet web application security traditionally comes at the expense of speed.

This is an especially important issue for online retailers, where slow performance can mean millions of dollars in lost revenue and a security breach can be just as devastating. More than 70 percent of consumers say they would no longer do business with a company that exposed their sensitive information.

Web application performance is also critical for corporate operations, particularly for remote workers, where slow access to enterprise applications can destroy productivity. As more applications are being delivered through a standard browser over the Internet, the challenge of accelerating web applications without compromising security grows.

Ensuring both web application security and performance has usually required multiple point solutions and plenty of computing and staff resources to properly configure and manage them. Because each of these "extra" devices has its own way of proxying transactions, packets can slow to a crawl due to the extra overhead of TCP and application processing. Fast and secure in a single, individually wrapped unit does seem like two contrary goals, but if you're looking for that magical mix, F5 can satisfy your sweet tooth.

The Security Half

As of March 2009, 63 percent of websites had high, critical, or urgent security vulnerabilities. ScanSafe reported that data theft Trojan attacks increased 1,559 percent in 2008.¹ From an IT perspective, a security breach or a poorly performing web application can have devastating consequences. Ponemon Institute reported that the average cost of a data breach is \$6.6 million,² but the January 2007 compromise of credit card data at TJX has already cost the company more than \$150 million.³ With regulations such as PCI and SOX, there are hefty fines and potential jail time if companies fail to secure data. Security is almost always at the top of CIOs' worry lists.



As the Internet has evolved, so have security issues. Attacks that used to compromise layer 3 and 4 are now focusing on layer 7. Thieves are smarter and more daring, breaching large information warehouses rather than single individuals. Things like web application firewalls are now a requirement, particularly for PCI compliance. In addition, as the workforce becomes more mobile, applications need to be available in more places and on more devices, adding to the complexity of enforcing security without impacting productivity.

Security concerns just keep getting bigger. Consider that a few years back, the browser's main purpose was to surf the net. Today, browser usage is a daily tool for both personal and professional needs. In addition to the usual web application activities like ordering supplies, checking traffic, and booking travel, we also submit more private data like health details and payroll information.

The browser acts as a secret confidant in many areas of our lives since it helps transmit highly sensitive data in both our work and social spheres. It goes both ways—while other people, providers, sites, and systems have our sensitive data, we may also be carrying their sensitive data on our own devices. The Internet today is more than a function of paying bills or getting our jobs done—it holds our digital identity for both work and play. And once a digital identity is out there, there's no retracting it. We just hope there are proper controls in place to keep it secret and safe.

The Acceleration Half

For retail web applications and search engines, downtime or poor performance means lost revenue. According to Continuity Central, Warwick Business School published research in 2008 that showed significant, tangible costs to business for search engine downtime. It can be more than \$500,000 in lost revenue for an unplanned outage lasting just an hour.⁴ For financial institutions, the loss can be in the several million dollar range. And downtime costs more than just lost revenue. Not adhering to a service level agreement can incur remediation costs or penalties. Non-compliance with certain regulatory laws can result in fines. Additionally, the damage to a company's brand reputation—whether it's from an outage, poor performance, or breach—can have long-lasting, detrimental effects to the company.



These days, many people now have high-speed connections to the home. But applications have matured and now offer users pipe-clogging rich data like video, Flash and other multi-media, or Web 2.0-delivered content. If the website is slow, users will probably go somewhere else. It happens all the time. You type in a URL only to watch the browser icon spin and spin. You might try to reload or retype, but more often, you simply type a different URL to a similar site. If you are doing research, buying something, or visiting a friend's photo page, for example, you want the browser to load the application fast. With an e-commerce site, poor performance usually means a lost sale because you probably won't wait around if your cart doesn't load quickly or stalls during the secure check-out process.

If it's a business application in a SaaS deployment and you're stuck with a sluggish site, then that's lost productivity and a frustrated user. It can also mean a time-consuming trouble ticket for IT. Corporate users want and expect LAN-like performance, even when they are mobile. When application performance suffers, the business suffers.

What's the big deal?

Typically, securing an application can come at the cost of end-user productivity because of deployment complexity. Implementing website security—like a web application firewall—adds yet another mediation point where the traffic between the client and the application is examined and processed. This naturally increases the latency of the application, which can become painfully apparent with globally disbursed or highly mobile users who must deal with existing high round-trip time or limited bandwidth.

Having another touch-point or process between the client and server also increases the cost of the deployment. The cost is not just in the devices; ongoing management and maintenance take their toll as well. Using multiple devices can mean using multiple management interfaces, increasing the learning curve for administrators, and making troubleshooting more difficult if a problem occurs. Many companies face this dilemma, and the solution is not always simple. There is fear of negatively impacting application performance and fear of owning the problem. Web application performance and security administration can cross organizational structures within companies, making ownership splintered and ambiguous.



The Sweet Spot

Fortunately, you can now integrate security and acceleration into a single device with the arrival of BIG-IP® version 10 on BIG-IP® Local Traffic Manager™ (LTM). By adding the BIG-IP® Application Security Manager™ (ASM) module and the BIG-IP® WebAccelerator™ module to BIG-IP LTM, not only are you able to deliver web application security and acceleration, but the combination provides faster deployment and simplifies the process of managing and deploying web applications. These integrated components provide the means to both secure and accelerate your web applications with ease. A single platform addressing all your application delivery needs and gives significant benefits for both the application users and system administrators.

F5's unified security and web application acceleration takes a single platform approach that receives, examines, and acts upon application traffic as a single operation, in the shortest possible time and with the least complexity. Additionally, F5's management GUI allows varying levels of access to system administrators according to their roles (security administrators, network administrators, and so on). This ensures that administrators have appropriate management access without granting them access to restricted, role-specific management functions. F5's BIG-IP ASM and BIG-IP WebAccelerator combination isn't your typical "integrated" function device. This is a true, internal system integration and not just co-deployment of multiple proxies on the same device.

How It All Works Together

F5 TMOS® architecture is at the heart of all BIG-IP products. TMOS uses a proxy-based architecture specifically designed to control and modify the requests and responses that flow between users and applications. TMOS is the foundation for the BIG-IP v10 platform, providing underlying networking functions and calling BIG-IP modules for execution as needed.

BIG-IP LTM often serves as the base for other BIG-IP product modules. BIG-IP LTM defines and performs health checks to determine whether application servers are operational and how quickly they are responding to current user requests, ensuring that traffic is directed to the server best able to handle the request at that moment.



BIG-IP ASM offers validated application templates to quickly secure popular applications and uses policies to actively monitor user traffic, determine appropriate behavior, and recommend new security policies as needed. Application security policies help ensure an application vulnerability threat is eliminated even if still present within the application code. BIG-IP ASM helps security administrators implement web application security that protects the application infrastructure without unnecessarily restricting valid actions, and it helps commerce sites fulfill PCI DSS requirements.

BIG-IP WebAccelerator speeds web application delivery, especially for remote and mobile users. BIG-IP WebAccelerator ensures that any file cacheable by a web browser, even if seemingly dynamic, is marked to guarantee the web browser caches the file. It loads the file directly from browser cache on subsequent visits. BIG-IP WebAccelerator also caches objects, delivering them directly to users and reducing demand on the web application infrastructure. Whether users are in a remote office, at home, or on the road, they receive the fastest possible access to web-enabled content for the best possible user experience. BIG-IP WebAccelerator improves page load time, reduces demand on web servers, and reduces WAN bandwidth usage.

The single-platform integration of these functions means that BIG-IP v10 can share context between security and acceleration—something you don't get with multiple devices. Sharing context, such as users' network, device, location, and integrity state, enables both the security side and the acceleration side to make intelligent, real-time decisions on delivering fast, available, and secure applications.

With BIG-IP v10, you can now deploy and manage a highly available, very secure, and incredibly fast web application infrastructure all from the same unified GUI on BIG-IP v10. With built-in application ready templates, rolling out a new service is easy. Simply follow an intuitive wizard and enter your unique values to create your optimized and secure Application Delivery Networking infrastructure.

White Paper

Security and Acceleration—the Sweet Spot of Application Delivery

Conclusion

F5's unified web application security and acceleration in BIG-IPv10 offers an unmatched solution for directing, securing, and accelerating web applications. Retail and remote users receive faster web pages. For IT, it minimizes WAN bandwidth utilization, safeguards web applications, and prevents data leakage, all while directing traffic to the application server best able to service a request.

Best of all, unlike other concoctions requiring multiple devices, this solution is available on a single device that delivers superior features and the highest levels of performance. Using the unified web application security and acceleration solution, a single proxy secures, accelerates, optimizes, and ensures application availability for all your critical web applications.

¹ ScanSafe: "[Credit Crunch Fuels Surge in Web Attacks](#)"

² Information Week: "[Data Loss Costing Companies \\$6.6 Million Per Breach](#)"

³ Computerworld: "[TJX Says Breach Costs May Exceed \\$150M](#)"

⁴ Continuity Central: "[Zero-Downtime System Migrations](#)"

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
info.asia@f5.com

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

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

