

SECURE, UNIFIED WEB APPLICATION DELIVERY WITH F5 BIG-IP AND DELL BLADE SERVERS



By Scott Siragusa

Dan Kim

The Dell™ PowerEdge™ M1000e modular blade enclosure offers the power and flexibility to meet the most demanding workloads. Dell and F5 Networks provide a comprehensive delivery system for Web applications designed for high performance and scalability as well as tight security to help safeguard critical data.

As enterprises continue to Web enable their core applications, the need for high availability, scalability, security, performance optimization, and simplified management has intensified. Blade servers—modular, ultra-dense servers using a single chassis with high redundancy—enable economies of scale in data centers while helping drastically reduce requirements for power, space, and dedicated hardware management.

However, using the advantages of blade servers for Web application delivery also requires an approach that can unify independent application and server resources and present them as one. Combining Dell PowerEdge M1000e modular blade enclosures with F5® BIG-IP® Local Traffic Manager™ (LTM) and BIG-IP Application Security Manager™ (ASM) systems offers a secure, unified way to deliver Web applications—helping simplify IT by allowing comprehensive control with flexible scalability for enhanced enterprise agility.¹

DEPLOYING SCALABLE, HIGHLY AVAILABLE WEB APPLICATIONS

Maintaining consistent availability is generally a key concern for enterprises deploying Web servers, from

e-commerce companies relying on Web applications for revenue to services organizations relying on information delivery over the Internet. Traditionally, these enterprises have implemented simple load-balancing clusters to help ensure the availability of Web servers. However, as usage increased and large deployments became common, increased network traffic, limited health-checking capabilities, and increased security concerns left organizations searching for a more comprehensive solution than these clusters could provide.

F5 BIG-IP LTM systems can detect a variety of device failures to help ensure mission-critical resources respond appropriately to maintain availability, while simultaneously accelerating performance through features like compression, RAM caching, Secure Sockets Layer (SSL) offload, and TCP optimizations. Advanced content and application checks such as Extended Content Verification (ECV) and Extended Application Verification (EAV) simulate an end-user request and monitor the true availability of application content. These advanced health-checking capabilities can help organizations achieve high levels of availability for their critical applications while helping reduce operational complexity and costs. If one

Related Categories:

Blade servers

Security

Visit DELL.COM/PowerSolutions for the complete category index.

¹For more information on the PowerEdge M1000e, see "The Next-Generation Dell PowerEdge M1000e Modular Blade Enclosure," by Chad Fenner, in *Dell Power Solutions*, February 2008, DELL.COM/Downloads/Global/Power/ps1q08-20080206-Fenner.pdf.

service is nearing the limits of its capacity, scaling it can be as simple as adding another instance of the service to the network and then to the BIG-IP load-balancing pool. By combining LTM with Dell PowerEdge M1000e blade servers, organizations can create a highly scalable, highly available environment to help them meet growing organizational demands on Web and application resources.

DEFENDING AGAINST SECURITY THREATS

Web site security is becoming increasingly complex, and increasingly crucial to Web server deployments. Some of the most serious—and most common—network security threats come from attacks targeting vulnerabilities in Web traffic or enterprise applications (see Figure 1). These attacks typically ignore conventional firewalls, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs), and are often difficult and costly to prevent.

BIG-IP LTM systems enable organizations to encrypt Web traffic by integrating SSL encryption and decryption capabilities. Offloading processor-intensive SSL transactions from front-end servers can help significantly increase the performance of Web server clusters, freeing Web sites to handle additional user requests. This solution helps maximize application availability, simplify maintenance, and reduce administration

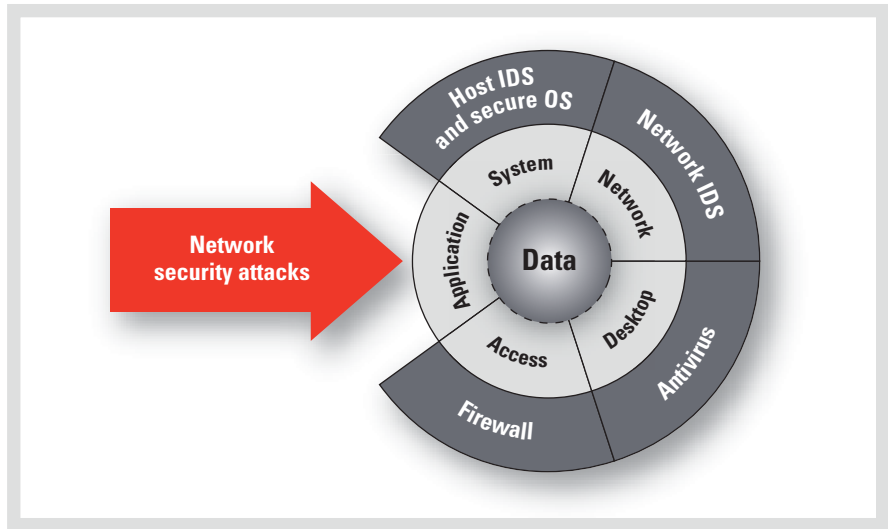


Figure 1. Enterprise applications are a key vector for network security attacks

overhead. By offloading SSL and persistence functions, administrators can create a comprehensive proxy environment with increased application performance. Figure 2 illustrates a typical deployment of BIG-IP LTM systems and Dell PowerEdge M1000e blade servers in a secure, highly scalable, highly available environment.

LTM systems are also available with a Federal Information Processing Standard (FIPS) 140-2 Level 3 certified cryptographic/SSL accelerator. FIPS products from F5 Networks meet the high levels of security standards required by government agencies, financial services, and health care organizations by integrating a tamper-resistant key protection module and sophisticated key

management capabilities. Centralizing this feature on an LTM system rather than deploying it on each Web server individually can provide significant savings on management costs.

MEETING SECURITY STANDARDS

The Payment Card Industry (PCI) Security Standards Council—founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International—created the PCI Data Security Standard (DSS) to manage the ongoing evolution of security in this industry. This standard applies to organizations that process, store, and transmit cardholder and transaction data, and includes 12 basic requirements organized into six core areas.²

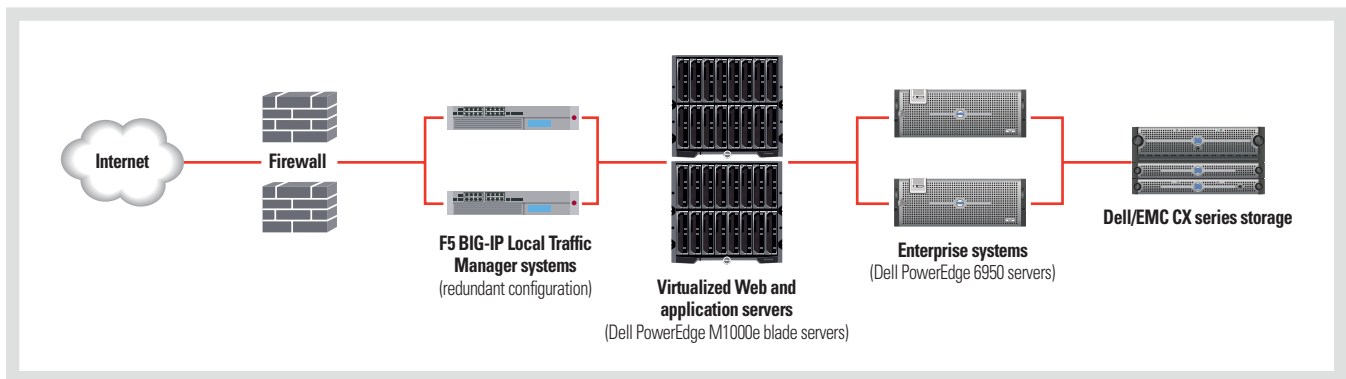


Figure 2. F5 BIG-IP Local Traffic Manager systems with Dell PowerEdge M1000e blade servers help provide a secure, highly scalable, highly available environment

²For more information, visit www.pcisecuritystandards.org/tech.

F5 solutions can help organizations in all six DSS core areas and 10 out of 12 requirements. Most notably, requirement 6.6 in the DSS specification explicitly states the need for either an annual code review of applications or a Web application firewall to address security vulnerabilities in Web applications—a key feature available as a stand-alone appliance or product module for F5 BIG-IP.

BIG-IP ASM systems are designed to provide comprehensive protection for Web applications and operational infrastructure. These systems use an auto-adaptive approach to application delivery security in which the security policy is automatically updated based on observed traffic patterns. This simplified approach to configuration helps simplify implementation and maintenance and reduce overall total cost of ownership.

ASM also includes features beyond Web application security. As an underlying base, it provides Web application firewall functionality such as protection against cross-site scripting, buffer overflow, SQL or OS injection, cookie poisoning, forceful browsing, and manipulation of invalidated input, as well as content scrubbing and resource cloaking. By providing comprehensive security for International Organization for Standardization (ISO) Open System Interconnection (OSI) model Layer 2 (data link) through Layer 7 (application), ASM offers a holistic approach to application delivery security. From robust distributed denial-of-service (DDoS) attack protection, Layer 4 (transport) filtering, and Layer 7 DoS attack protection to Layer 7 application security, ASM offers a comprehensive approach to application delivery security.

The latest ASM version introduces a host of advanced security features such as XML firewall, FTP security, evasion attack protection, and active code protection. The new Real Traffic Policy Builder™ engine provides security heuristics to not only inspect bidirectional traffic in real time, but also parse JavaScript,


“Together, F5 Networks and Dell can provide comprehensive solutions to help make Web applications secure, fast, and highly available for organizations of all sizes to help them maximize return on investment.”

Flash, and active code. In addition, this adaptive learning and tuning engine can help significantly reduce the administrative overhead for managing policy definitions. Organizations can deploy ASM as a stand-alone device or as a module on an LTM system.

In addition to providing a highly secure application firewall, ASM is also designed for high performance. By taking advantage of the F5 Traffic Management OS (TMOS™) unified architecture, ASM can use compression, RAM caching, SSL offload, TCP optimizations, and other performance optimizations to help accelerate firewall and application performance. Basing a Web application delivery infrastructure on ASM and Dell PowerEdge M1000e blade servers can help organizations create a highly scalable, high-performance environment while simultaneously helping ensure security.

CREATING A UNIFIED WEB APPLICATION DELIVERY FRAMEWORK

F5 Networks is the global leader in application delivery networking, and the Dell PowerEdge M1000e modular blade enclosure provides a highly redundant, highly energy-efficient server chassis while enabling maximum flexibility and modularity. By adding intelligence and manageability into the network to offload applications, F5 BIG-IP systems help optimize applications and allow them to work faster and consume fewer resources than they would otherwise. The F5 extensible architecture helps intelligently integrate

application optimization, protect the application and the network, and deliver application reliability—all on one universal platform. Together, F5 Networks and Dell can provide comprehensive solutions to help make Web applications secure, fast, and highly available for organizations of all sizes to help them maximize return on investment. 

Scott Siragusa is the senior strategic partner manager on the Dell/F5 Partner Team specializing in application delivery and security solutions. He has more than 9 years of experience in marketing, solution architecture, and business development with Dell and F5 Networks.

Dan Kim is a product marketing manager for F5 Networks specializing in application delivery and security solutions. He has been with F5 Networks for over 7 years and in the network and IT industry for almost 10 years.

MORE ONLINE
DELL.COM/PowerSolutions

QUICK LINKS

F5 Networks:
www.f5.com

Dell PowerEdge M1000e:
DELL.COM/Blades