Rock-solid protection for Web application delivery

By Fred Johnson, Allen Vance, and Andrew Walker

Comprehensive Web application security is vital for organizations today. Flexible, cost-effective application delivery networks built using F5® BIG-IP® platforms and Dell™ hardware and services help keep Web applications secure and available.

Ongoing, rapid growth of Web applications puts increasing amounts of sensitive enterprise data at risk of potential theft, security vulnerabilities, and multilayer attacks. Protecting an organization and its reputation by maintaining the confidentiality, availability, and performance of its applications is critical to successful business outcomes.

Today's threats are far more sophisticated than those of just a few years ago. Gone are the days of simply exhausting networking bandwidth or crashing the hard drive in a victim's desktop computer. Some of the most serious security threats now come from multilayer cyberattacks by Internet bot programs, such as distributed denial-of-service (DDoS) and SQL injection attacks that target vulnerabilities in Internet and enterprise applications. Business-critical applications and data are primary targets. Recently there have been many widely publicized incidents involving advanced attacks against both public and private organizations.

Modern attacks can be highly coordinated, distributed, and diverse in nature, sometimes rolling many different types of attacks into one. Applications and network services may be simultaneously attacked across many layers of the technology stack, from many different sources. Attackers often focus on more sinister goals, such as exposing sensitive data, cleverly redirecting users to malicious sites seeking access to financial information, or exhausting connection resources to cause a denial-of-service (DoS) attack. Stealth methods and increased complexity make these threats significantly more difficult to detect and block compared to their predecessors. Additionally, interactive Web 2.0 applications have paved the way for new threats that render traditional security solutions ineffective and blind to the attacks.

Security breaches and site outages can lead to major losses in revenue and brand reputation damage. At the same

F5 DevCentral community

The F5 DevCentral portal provides comprehensive technical documentation, discussion forums, blogs, media, and more for information on application delivery networking. Visit this community site to get tips, learn best practices, and discuss topics with peers.

bit.ly/Ods5Qr

time, today's economic challenges have many organizations facing tight budget constraints and diminishing resources—they are being asked to do more with less even as their overall security risks are increasing. The stakes are high for Web application security, and eliminating threats is impossible. Organizations must therefore seek out cost-effective solutions to improve responsiveness to vulnerabilities.

Security designed for essential Web applications

The F5 BIG-IP Application Security Manager™ (ASM™) application delivery controller is a high-performance, flexible Web application firewall (WAF) that helps secure Web applications in traditional, virtual, and cloud computing environments. BIG-IP ASM provides powerful Web application and Web site protection and helps secure deployed applications against unknown vulnerabilities. It also enables compliance for key regulatory mandates such as the Payment Card Industry Data Security Standard (PCI DSS) and an array of security standards (see the sidebar, "Integrated platform protection").

Employing specific technologies, BIG-IP ASM detects when applications are being attacked and protects them from vulnerabilities such as Layer 7 DoS and DDoS, SQL injection, command injection, cross-site scripting, Web-scraping, cookie poisoning, worms, and JavaScript Object Notation (JSON) payload attacks in Asynchronous JavaScript and XML (AJAX) widgets. Blocking attacks on the network before they reach the Web servers is often referred to as virtual patching. Integration with vulnerability scanners provides advanced application assessment and threat protections, helping secure deployed applications from unknown vulnerabilities (see the sidebar, "Security highlights for enterprise Web infrastructure").

Multilayer defense strategies can yield enhanced results. Leveraging combined solutions, BIG-IP ASM integrates application attack protection along with the Layer 2 through Layer 4 network security features provided in the F5 Traffic Management Operating System® (TMOS®) platform and the BIG-IP Local Traffic Manager™ (LTM®) application delivery controller. This approach helps dramatically reduce the risk of application and network vulnerabilities in deployments, and it can deliver cost-savings on vulnerability repairs.

Comprehensive Web application firewall management

Meeting security and compliance requirements can be daunting even for the most technically savvy IT organizations. The critical nature of protecting applications against attacks means these activities receive extremely high levels of visibility and scrutiny, especially if something goes wrong that negatively impacts the business. Managing and monitoring security devices can be complex. In an ideal world, using devices such as next-generation firewalls, intrusion prevention systems, DoS protection systems, and WAFs would be an easy matter of taking a set-it-and-forget-it approach. Unfortunately, utilizing such an ideal approach is not the case today.

To help organizations manage Web application security, BIG-IP ASM offers features that make WAF configurations easy to perform through an intuitive, Web browser–based graphical user interface (GUI). Organizations can choose between automated learning or manual methods of policy configuration for enhanced deployment flexibility and control. Monitoring, reporting, and further tuning or tightening of the policies is also possible through the BIG-IP ASM Web management interface. The configuration wizard for BIG-IP LTM settings streamlines the tasks of creating HTTP classes and assigning them to existing load-balancing virtual servers. An easy-to-use attack signature update process helps keep BIG-IP ASM current and servers protected from new attacks and threats.

For organizations that need security expertise and wish to avoid staff augmentation, a managed security service provider (MSSP) with certified security experts may be a

Integrated platform protection

The BIG-IP platform has earned ICSA Labs network firewall and Web application firewall (WAF) certifications* and supports the following among numerous security standards and mandates:

Hardware security modules

- Federal Information Processing Standards (FIPS) 140-2 Level 2 Certified F Series, including BIG-IP models 6900F, 8900F, 11000F, and 11050F
- Key third-party management solutions for many certificates
- Third-party Public-Key Cryptography Standards (PKCS) #11 certificate format and network-based hardware security modules
- Secure Vault key protection on local storage

Vertical mandates for hardware security modules

- Financial and insurance: Payment Card Industry (PCI)
- Government: FIPS 140-2
- Health care: Health Insurance Portability and Accountability Act (HIPAA)

* For more information on ICSA Labs, visit icsalabs.com.

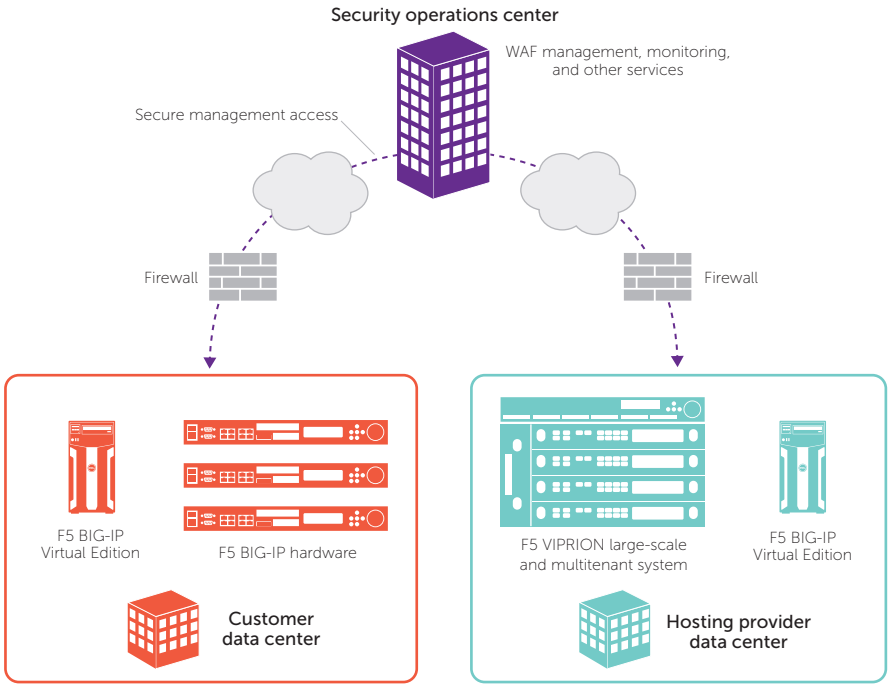

Figure 1. MSSP management and monitoring services for BIG-IP ASM deployments across different types of data centers

well-suited, cost-effective alternative (see Figure 1). An MSSP can be a single point of contact for security services such as device management and monitoring, unified threat management, application penetration testing, compliance and reporting, security consulting, and application security tuning, among other services. In addition to daily WAF management and monitoring activities, an MSSP helps organizations achieve PCI compliance for specific applications and provides an application security posture, trending, statistics, and other information through a secure self-service Web portal. (For more information on WAF management, see the sidebar, "End-to-end Web presence defense.")

Flexible and adaptable configurations

The BIG-IP platform is rooted in advanced traffic management with deep feature sets to support many specific application,

Security highlights for enterprise Web infrastructure

BIG-IP Application Security Manager (ASM) is designed to support secure, mission-critical enterprise Web infrastructure with a wide range of features.

- Network traffic security through an ICSA Labs–certified network firewall
- Protection against threats listed on the Open Web Application Security Project (OWASP) Top 10 Web Application Security Risks
- Integration with WhiteHat Sentinel, Cenzic Hailstorm technology, Qualys QualysGuard Web Application Scanning, IBM® Security AppScan, Splunk, and other security solutions
- Easy-to-update attack signatures that protect against generalized and known application attacks
- IP version 6 (IPv6) support, IP geolocation enforcement, and analytics
- File upload detection to block end users from uploading binary executables
- Support for session tracking, event correlation, and response checking and logging
- System-generated learning suggestions from the BIG-IP ASM Learning Manager resource for tuning policies
- Help simplifying and standardizing setup of BIG-IP using the F5 iApps™ configuration wizard
- Self-service configuration analysis and support using the F5 BIG-IP iHealth® Web portal tool
- Management access provided by the Web browser–based graphical user interface (GUI), Traffic Management Shell, and Linux® OS–style command-line interfaces
- Secure, out-of-band Ethernet management and serial console interfaces
- Lights-out management of the system over Secure Shell (SSH) or the serial console provided by Always-On Management whenever power has been applied—that is, when the device is plugged in—even if the host subsystem is turned off

networking, and security configurations. BIG-IP is often referred to as the Swiss Army knife of application delivery and security. This flexibility can help to significantly reduce costs to deploy and manage WAF technology. Integrated and consolidated, resilient scale-out, and pooled fail-open deployment models (see Figures 2, 3, and 4, respectively) supporting Web applications running on Dell PowerEdge™ servers, for example, demonstrate easy adaptation to supporting networks. These deployment models also provide a range of capabilities that help organizations realize enormous benefits from BIG-IP ASM.

An important benefit of BIG-IP is the capability to consolidate multiple functions into a single appliance. Software add-on modules can be layered together through licensing. All BIG-IP units, regardless of provisioned licensed software modules, contain a core set of platform features and functionality. BIG-IP ASM is a modular component of the TMOS architecture and leverages the dynamic features that are part of that architecture. These common features include a comprehensive reverse proxy, the F5 BIG-IP SSL Acceleration™ module, digital certificates management, Federal Information Processing Standards (FIPS) compliance, virtual LAN (VLAN) segmentation, remote authentication and authorization, enhanced logging, and TCP/IP optimization. In addition, they include connection pooling, IP and port filtering, rate shaping, and F5 iRules® scripts.

BIG-IP ASM is available as a stand-alone appliance, as a virtual edition (BIG-IP ASM VE), and as a product module in the BIG-IP system—for example, BIG-IP ASM and BIG-IP LTM. The stand-alone appliance includes comprehensive BIG-IP ASM functionality with SSL acceleration, Web caching, essential Layer 4 load balancing, and other beneficial features to optimize WAF deployments. BIG-IP ASM VE and the F5 VIPRION® system with the F5 virtual

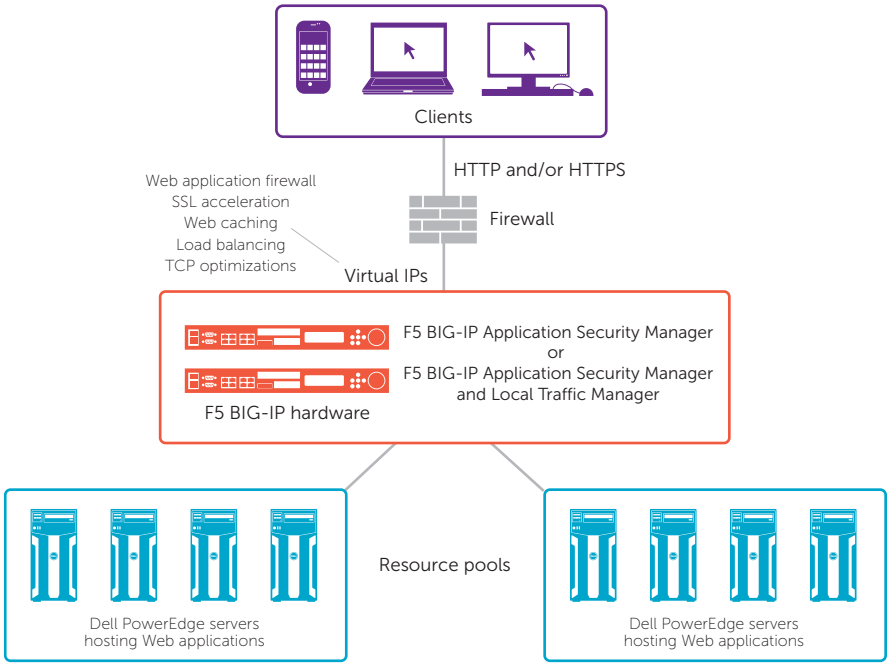

Figure 2. High-availability deployment utilizing BIG-IP ASM or integrated BIG-IP ASM and BIG-IP LTM for protecting Web application infrastructure

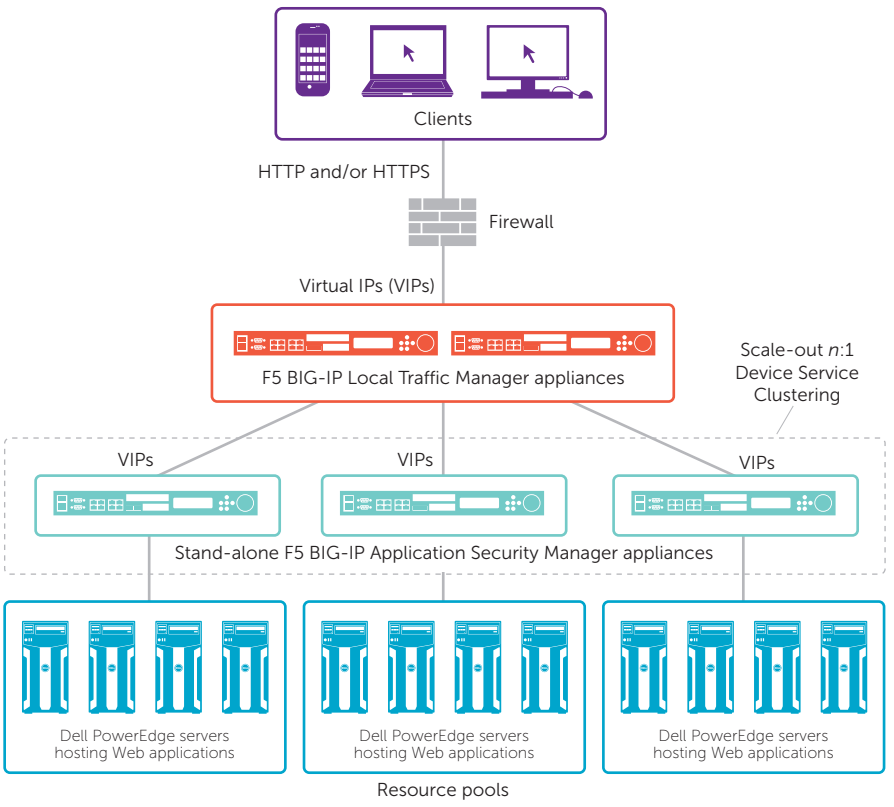

Figure 3. Scale-out deployment for resilient failure protection using *n*:1 Device Service Clustering

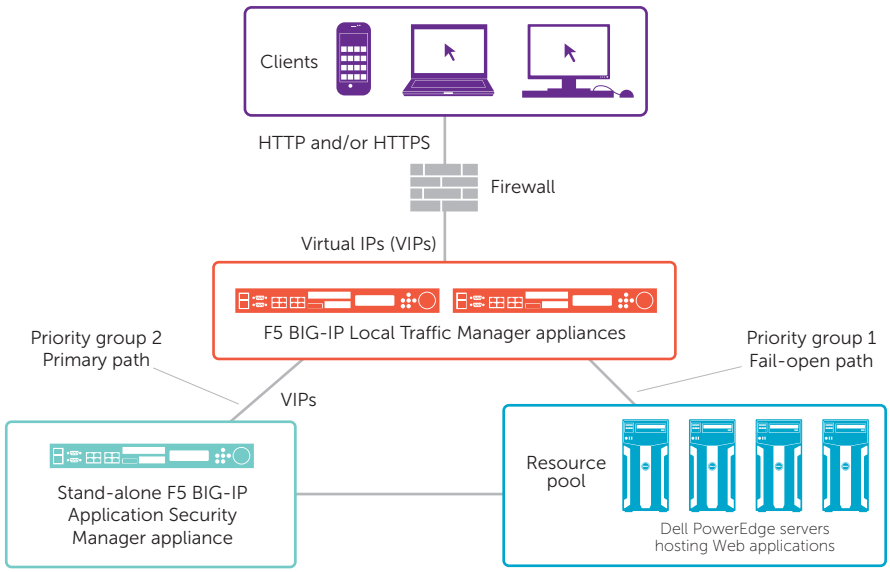

Figure 4. Pooled deployment for fail-open capability using Priority Group Activation

clustered multiprocessing (vCMP®) feature support multitenancy as separate BIG-IP instances, while all systems support internal security boundaries through administrative partitions, route domains, and rate shaping.

Fast, increasingly efficient processing of application traffic helps reduce latency because data flows through the BIG-IP stack only once; yet all the features—such as WAF, SSL acceleration, Web caching, TCP optimizations, and load balancing—are applied to the traffic. As a result, performance and end-user experience may actually improve when BIG-IP ASM is added in front of applications. Enhanced performance and reduced cost are major advantages, particularly when compared to the additional latency and management complexity that can be created by stringing together many single-purpose appliances from different vendors.

Taking advantage of the platform flexibility, some organizations can add BIG-IP ASM to their existing BIG-IP LTM units by simply purchasing add-on software module licenses. This approach helps avoid the need to purchase additional hardware. These products and their functionality require minimum platform specifications and F5 TMOS version 11.1 Hotfix 2 or higher.

Advanced approaches for protecting Web applications

With the rising number and sophistication of attacks on Web applications, implementing strong cyberdefense strategies is more important than ever before. Configuration flexibility, advanced multilayer security protections, and straightforward management options are key factors to successfully managing costs and maintaining maximum security throughout application life cycles. Together, Dell and F5 provide a high-quality and cost-effective array of solutions to help solve today's Web application security challenges. PS

Authors

Fred Johnson is a partner engineer at F5 Networks dedicated to Dell Labs, sales, and Dell technology services.

Allen Vance is a product manager for data and application security services at Dell SecureWorks and is a Certified Information Systems Security Professional (CISSP) with a Certificate of Cloud Security Knowledge (CCSK).

Andrew Walker is a solutions design engineer at F5 Networks focused on Dell technology services worldwide.

End-to-end Web presence defense

To help organizations defend their Web presence, the Dell SecureWorks Web application firewall (WAF) management service provides 24/7 management and real-time monitoring for WAF devices. By supporting the entire WAF life cycle, this service helps ensure that security appliances provide a high degree of protection without interrupting legitimate business traffic to and from applications, such as Web applications running on Dell PowerEdge servers. Certified security experts help build comprehensive, end-to-end systems from solution design, deployment, continuous tuning, configuration management, and monitoring and analysis to ongoing maintenance, backup and recovery, performance and availability management, and security and compliance reporting. Dell SecureWorks can collaborate with organizations as an extension to their security staff, working closely together to enable fast, accurate detection and response to security incidents.

Learn more

Dell SecureWorks managed security services:
bit.ly/MZvWf8

F5 BIG-IP ASM:
bit.ly/KrMSLK

Dell SecureWorks:
bit.ly/LRxxbn

OWASP Top 10 project:
bit.ly/ioBuA3