F5 White Paper

Application Security in the Cloud with BIG-IP ASM

Whether critical applications live in the cloud, in the data center, or in both, organizations need a strategic point of control for application security. F5 BIG-IP Application Security Manager (ASM) provides the security, intelligence, and performance that today's dynamic infrastructure demands.

by Peter Silva
Technical Marketing Manager

Contents

Introduction

Application threats are constantly evolving. Recent high-profile Internet attacks on organizations like HBGary, RSA, WikiLeaks, Google, Comodo, and others prove that no one is immune. Anyone could be a target, and perpetrators are extremely organized, skilled, and well-funded. Culprits are often better trained than the IT staff deployed to thwart the attacks, which are targeted, elaborate, and aggressive—not to mention creative. The attacks are multi-layered and constant, and seek not only to deface a website, but to steal valuable data. Customer data, intellectual property, state secrets, SSL certificates, and other proprietary, highly sensitive information are the top targets.

The malware and other penetration techniques are custom-made, can adapt, and can cover the tracks of those seeking the information. An assault may start at the network level with DNS, ICMP, or SYN flood attacks, then move to the application with layer 7 DoS, SQL injection, or cross-site scripts (XSS); once the system is compromised, the attacker goes after the data. Attackers also often leave "back doors" so they can easily come and go before being detected.

Many organizations do a decent job of securing their infrastructure components, but are challenged when it comes to securing their web applications, whether they are hosted in house, in a cloud environment, or both. Forrester Research reported that in 2009, 79 percent of breached records were the result of web application attacks.[1] An application breach can cost companies significant amounts of money and seriously damage brand reputation. The 2010 annual study on data breaches by Symantec and the Ponemon Institute calculated that the average cost of a breach to a company was $214 per compromised record, and $7.2 million over the entire organization.[2] In addition to financial losses, an organization may also have to address compliance and legal issues, public scrutiny, and loss of trust among shareholders and customers.

It's clear that protecting applications while still making them highly available to valid users is critical to the lifeblood of an organization. F5® BIG-IP® Application Security Manager™ (ASM) version 11 provides the application protection organizations require to block evolving threats, no matter where the applications are deployed in today's dynamic environments. BIG-IP ASM is a high-performance, ICSA-certified web application firewall (WAF) that provides a strategic point of control within the infrastructure from which enterprises can dynamically adapt to changing conditions to securely deliver crucial applications.

[1] "Security threats evolving at breakneck pace." Infosecurity-us.com. August 17, 2010.

[2] "2010 Annual Study: U.S. Cost of a Data Breach." Symantec Corporation and Ponemon Institute. March 2011.

Protecting the Application Infrastructure and Delivering Secure Applications

There are really two constituents that need protection when an organization is securing its applications: the infrastructure and the users. The infrastructure needs a layered barrier that protects against attacks, and users need protection against potential infection from the application, if it were to be compromised. Both can be a challenge, and each can directly affect the other.

BIG-IP ASM: In the Cloud or the Data Center

In version 11 of the BIG-IP system, BIG-IP ASM is available in a Virtual Edition (BIG-IP ASM VE), either as a stand-alone appliance or an add-on module for BIG-IP® Local Traffic Manager™ Virtual Edition (LTM VE). Companies often grapple with how to secure their applications in the cloud, especially when they are unable to deploy their own security appliances and must rely on the provider's solutions, which may leave organizations vulnerable and potentially liable for failing to meet regulatory requirements.

BIG-IP ASM VE delivers the same functionality as the physical edition and helps companies maintain compliance, including PCI DSS, when they deploy applications in the cloud. If an organization discovers an application vulnerability, BIG-IP ASM VE can quickly be deployed in a cloud environment, enabling organizations to immediately virtually patch vulnerabilities until the development team can permanently fix the application. Additionally, organizations are often unable to fix applications developed by third parties, and this lack of control prevents many of them from considering cloud deployments. But with BIG-IP ASM VE, organizations have full control over securing their cloud infrastructure.

During application development, organizations sometimes struggle to understand how the application will perform when secured with a WAF. Now, they can deploy BIG-IP ASM VE both in production cloud environments and in lab/test environments. Organizations can take advantage of a virtual edition WAF that is identical to their production environment by creating, testing, and tuning their web application security policies during the development phase to ensure their applications are locked down at launch. Issues like false positives and false negatives that require policy adjustments can be addressed before deployment; and blocking pages,

custom settings, and other configurations can be ready to go live. This allows organizations to verify their virtual application security, reduce testing costs, and increase testing speed, and it offers a highly flexible infrastructure for quick implementation in virtualized environments. In short, BIG-IP ASM VE is cloud-ready.

When an organization has a hybrid cloud model for cloudbursting, disaster recovery, or business continuity, it can run BIG-IP ASM VE in any combination of physical and virtual ADCs to achieve application security anywhere. In addition, in high throughput environments where multiple BIG-IP ASM stand-alone devices are deployed behind BIG-IP Local Traffic Manager (LTM) and sharing a pool, organizations can automatically synchronize their BIG-IP ASM policy among those devices.

With Automatic Policy Synchronization, BIG-IP ASM can synchronize policies automatically between pool members whenever there's a policy update. It allows organizations to cost-effectively scale on demand. This new feature significantly reduces the maintenance time associated with deployments. It also allows customers to run Policy Builder on a single BIG-IP ASM device, with the new policy updates automatically pushed to all pool members, significantly cutting complexity and deployment time. For example, change in the lab, push to production; change in data center and push to the cloud. Dynamically make policy changes in the cloud based on a bursting or a cloud-based attack, and push the policy back to the data center or lab. In addition, organizations can export the signature set when transitioning from QA to production. This improves the staging process and ensures the application is properly protected when it goes live.

In the Hardware

BIG-IP ASM v11 also includes support for F5's Virtual Clustered Multiprocessing (vCMP), the industry's first purpose-built hypervisor. With vCMP, organizations can create multiple virtual BIG-IP instances on a single piece of F5 hardware to simultaneously achieve complete logical separation and physical consolidation. This allows administrators to consolidate multiple customers, groups, or applications on a single device, while maintaining separation and control of each individually. For instance, with vCMP, organizations can provision a single instance of BIG-IP LTM and a separate instance of BIG-IP ASM. This logical separation allows BIG-IP ASM to take advantage of dedicated hardware for compute-intensive processes like compression and cryptography. The security group can manage the BIG-IP ASM instances as their own device and the network group can manage the BIG-IP LTM instances without any conflicts. You can also run different versions of BIG-IP products according to the needs of certain groups. This efficient management can help lower overall data center costs.

In the World "Wild" Web

Whether organizations choose the Virtual Edition or the physical appliance, BIG-IP ASM is designed to block all known web application vulnerabilities including the OWASP Top 10, which includes attacks like XSS, SQL injection, and cross-site request forgery (CSRF)—this is a negative security model. BIG-IP ASM can also be tuned to only allow certain user actions (a positive security model). AJAX, which is a mix of technologies (Asynchronous JavaScript and XML), is becoming more pervasive since it allows developers to deliver content without having to load the entire HTML page in which the AJAX objects are embedded. Unfortunately, poor AJAX code can allow an attacker to modify the application and prevent a user from seeing their customized content, or even initiate an XSS attack. Additionally, some developers are also using JSON (JavaScript Object Notation) payloads, a lightweight data-interchange format that is understandable by most modern programming languages and used to exchange information between browser and server. If JSON is insecure and carrying sensitive information, there is the potential for data leakage.

BIG-IP ASM v11 can parse JSON payloads and protect AJAX applications that use JSON for data transfer between the client and server. BIG-IP ASM can enforce the proper security policy and can even display an embedded blocking alert message. Very few WAF vendors are capable of enforcing JSON (other than the XML Gateways), and no other vendor can display an embedded blocking alert message. F5 is the only WAF vendor that fully supports AJAX, which is becoming more and more common even within enterprises. An organization should only buy a WAF that can handle AJAX, because even if it isn't currently using AJAX, it certainly will be in the near future.

AJAX and JSON aren't the only things to worry about. Threats can come from a variety of sources, including malicious hackers, unscrupulous users, and valid users. File upload forms and users uploading their own files can pose a significant risk to applications. Often, the first step in attacking a system is to insert code into the system and have it execute. File uploads can actually help an intruder accomplish this, enabling attackers to deface a website, introduce other vulnerabilities like XSS, add a phishing page to the website, or even upload a file in hopes that the IT administrator launches it.

In BIG-IP v10.2, F5 introduced antivirus inspection using a remote device via the Internet Content Adaptation Protocol (ICAP). This was only applied to files uploaded using HTTP multipart transactions, like when a user fills out a browser

form or includes file attachments and sends the entire message to a server. With BIG-IP v11, BIG-IP ASM will now extract every file upload and send it to an antivirus scanner for inspection. BIG-IP ASM can inspect file uploads via HTTP, as well as files that are attached to SOAP or transactions that are embedded in XML documents and every file upload within a multi-part request. For SMTP, BIG-IP ASM will inspect email content and attachments for spam. If a file is found to be infected, BIG-IP ASM will quarantine that file, effectively slamming the door on those taking the first step in trying to gain unauthorized access and protecting systems from users who might be unaware that they are sharing malware.

In the BIG-IP ASM GUI

Managing compliance is yet another daily consideration for IT. Organizations need an at-a-glance, up-to-the-minute view of their regulation requirements—the BIG-IP ASM GUI provides this. While IT departments might have a grasp on it within their own environments, compliance in the cloud can still be a significant hurdle. BIG-IP ASM is the first product to offer integration between a vulnerability assessment tool, WhiteHat's Sentinel, and a web application firewall. To comply with PCI DSS Requirement 6.6, organizations must have either a WAF or a vulnerability assessment tool. But today, many organizations realize that this is no longer an "either/or" choice. The WAF provides the web application protection while scanners provide insight into application vulnerabilities. The BIG-IP ASM and WhiteHat Sentinel combination enables organizations to quickly scan their applications for vulnerabilities and virtually patch them with the press of a button, closing the gap between vulnerability checking and detection, and remediation and protection. BIG-IP ASM now leverages WhiteHat's open API and covers more vulnerabilities than ever, and organizations can now manage the entire F5 and WhiteHat solution directly from the BIG-IP ASM GUI. This updated solution provides discovery and remediation capabilities within minutes of a central location; easy implementation for fast assessment and policy creation; the ability to dynamically configure policies in real time during assessment; and the ability mitigate unknown application vulnerabilities to reduce information and data loss. With BIG-IP ASM v11, the F5 and WhiteHat solution provides the best vulnerability coverage.

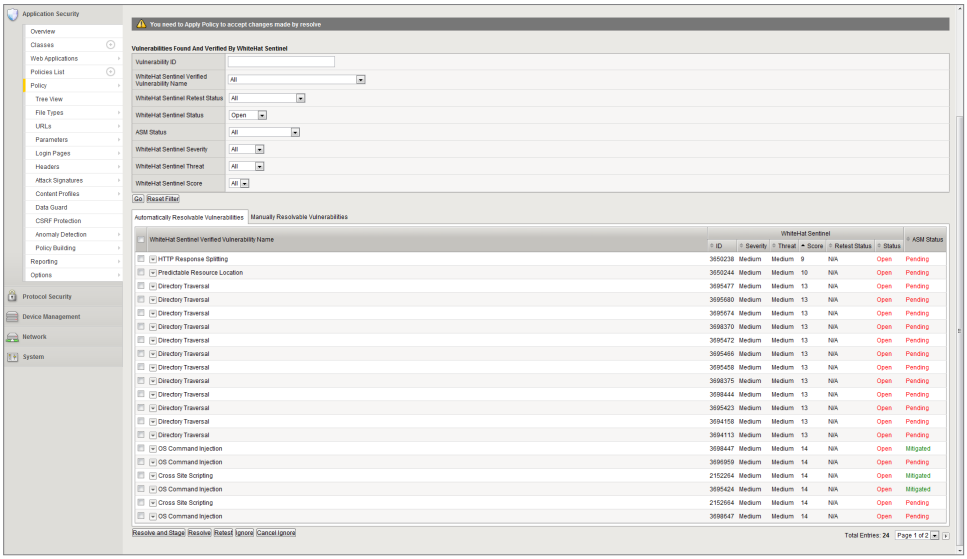

Figure 1: Integrated vulnerability assessment with WhiteHat Sentinel

Also included in BIG-IP ASM v11 is the BIG-IP Dashboard, which gives administrators a high-level overview of BIG-IP ASM status from security, health, and capacity perspectives with no configuration required. Simply run traffic through BIG-IP ASM, open the BIG-IP Dashboard, and select the BIG-IP ASM view from the drop-down menu. Security administrators can review Traffic Summary (throughput, TPS, requests), Attack Types, and any Anomaly Statistics. They can see the entire infrastructure or one particular application in real time or historically. Managing the security of applications and infrastructure has never been easier.

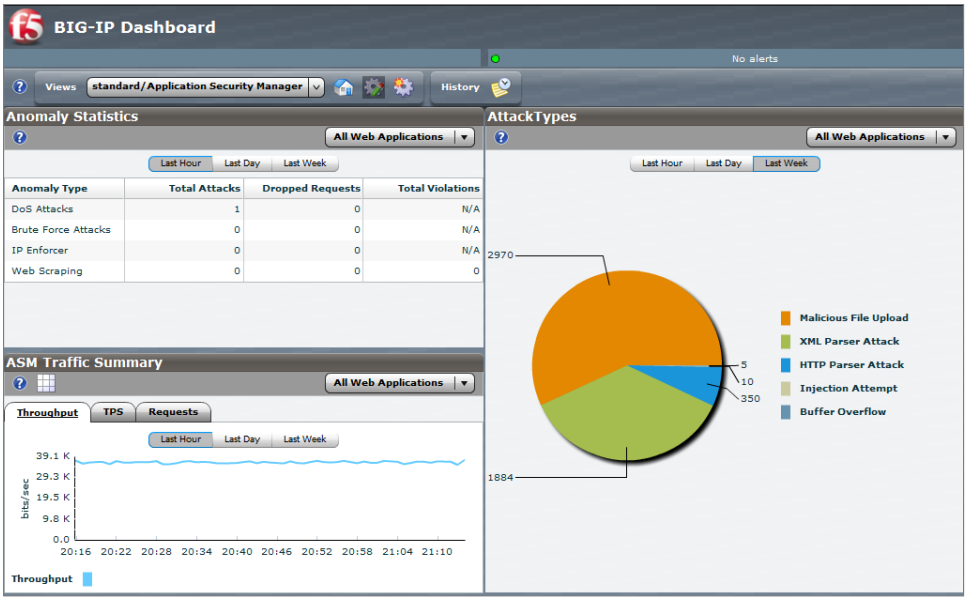

Figure 2: BIG-IP ASM Dashboard

Conclusion

F5 BIG-IP ASM v11 is the most comprehensive WAF on the market. BIG-IP ASM VE is cloud-ready, offering flexible deployment and cloud security for virtualized applications, including the ability to sync policies among BIG-IP ASM cluster members. Organizations can easily consolidate multiple customers, groups, and applications on a single BIG-IP device. BIG-IP ASM can secure the latest interactive web applications, including those utilizing AJAX/JSON, and enhances ICAP support.

BIG-IP ASM also has the deepest vulnerability assessment integration, which gives organizations the most comprehensive vulnerability coverage for evolving threats and helps organizations exceed the recommendations of PCI DSS Requirement 6.6.

BIG-IP Application Security Manager v11 provides the application protection organizations require to block evolving threats, no matter where applications are deployed in today's dynamic environments.

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

CS01-00052 0711