2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)

Critical Analysis on Web Application Firewall Solutions

Abdul Razzaq, Ali Hur, Sidra Shahbaz, Muddassar Masood, H Farooq Ahmad

School of Electrical Engineering and Computer Science (SEECS)
National University of Sciences and Technology, Islamabad, Pakistan
{abdul.razzaq, ali.hur, sidra.shahbaz, muddassar.masood, farooq.ahmad}@seecs.edu.pk

***Abstract*—Web Applications security has become progressively more important these days. Enormous numbers of attacks are being deployed on the web application layer. Due to dramatic increase in Web applications, security gets vulnerable to variety of threats. Most of these attacks are targeted towards the web application layer and network firewall alone cannot prevent these kinds of attacks. The basic reason behind success of these attacks is the ignorance of application developers while writing the web applications and the vulnerabilities in the existing technologies. Web application attacks are the latest trend and hackers are trying to exploit the web application using different techniques. Various solutions are available as open source and in commercial market. But the selection of suitable solution for the security of the organizational systems is a major issue. This survey paper compared the Web Application Firewall (WAF) solutions with important features necessary for the security at application layer. Critical analysis on WAF solutions is helpful for the users to select the most suitable solution to their environments.**

Keywords—Web application firewalls, web application solutions, comparison of application solutions

I. INTRODUCTION

The Web application security has become increasingly important in the last decade due to massive increase in development and use of web application technologies (such as e-business, e-sciences and e-health). A security assessment by the Application Defense Center, which included more than 250 Web applications from e-commerce, online banking, enterprise collaboration, and supply chain management sites, concluded that at least 92% of Web applications are vulnerable to some form of attack.

According to Verizon Business' 2010 Data Breach Investigations Report (DBIR)[2], a study conducted in cooperation with the United States Secret Service, provides insight. The report analyzes over 141 confirmed data breaches from 2009 which resulted in the compromise of 143 million records. The majority of breaches and data stolen in 2009 (95%) was through hacking "servers and applications."

According the survey[1] “Web applications continue to be a prime vector of attack for criminals, and the trend shows no sign of abating; attackers increasingly shun network attacks for cross-site scripting, SQL injection, and many other infiltration techniques aimed at the application layer.” Web application vulnerabilities can be attributed to many things including poor input validation, insecure session management, improperly configured system settings and flaws in operating systems and web server software.

Various methodologies and techniques have been used for the security of the application in term of safe coding, resolving configuration and establishing web application firewalls.

Safe coding is one of the one of most important technique, for this developer have to know that different security loop holes exist in web application and how to prevent them. Most of the security problems occur when there are problem in the logics of programs. To avoid these problem developer have to be aware of security issues. Web application layer unfortunately have no protocols and standards which will ensure security issues. So it solely depends on the developer and unfortunately developers are not so much trained that they can understand the security risks. So they leave loop holes in the web applications and hackers can exploit it easily.

The 2nd biggest problem with the web application is the use of third party tools like different web server to host web applications. Some time a configuration error e.g. use default setting of the web server or configuration problems between two servers leads hacker to get into the system and hack whatever it wants. For example HTTP request smuggling attack specifically happens because of the configuration

978-1-4673-5070-9/13/$31.00 ©2013 IEEE

issue of IIS server. So use of third party tools also leads us to the web application attacks.

To prevent both web application problem often web administrator relay on the web application firewalls. Web application firewalls works on the web application layer, it deeply inspect the HTTP packet and each individual part of the HTTP packet and look for the web application attacks. It looks for the malicious strings and configuration error problems using different techniques e.g. white list, blacklist, gray list etc.

Various solutions are provided by different vendors. These solutions are briefly discussed in the succeeding paragraphs:

II. WEB APPLICATION SOLUTIONS

A. Mod Security

Mod Security [3] is an open source, free web application firewall that works on Apache system. Main features are simple filtering; regular expression based filtering, URL encoding validation, Unicode encoding validation, auditing, null byte attack prevention, upload memory limits and server identity masking.

B. Imperva's Secure Sphere

Imperva's Secure Sphere [5], providing solutions that secure enterprise data centers. Secure Sphere protects proprietary information, custom business applications, and critical servers. It addresses phishing, identity theft, data theft, malicious robots, worms, denial of service, and SQL injection. It reduces web attacks, database breach, and worm infection. According to survey of Information security [8], Secure Sphere has high availability, preloading polices & signature and regularity compliance features.

C. *Barracuda network application gateway*

The Barracuda [9] is a commercial firewall that presents application ware traffic administration. Typical Barracuda Firewall functions include: a state full packet inspection firewall, IPsec VPN and intelligent traffic flow control. According to research information [8], Barracuda having higher capability of high availability, SLL acceleration & offloading, connections pooling, coach & compression, preloading polices & signature and regularity compliance features.

D. Breach Security's Web Defend

According to research information [8], Web Defend having higher availability, preloading polices & signature and regularity compliance features. But it lackcapability of load balancing, SLL acceleration & offloading, connections pooling, coach & compression, and week in zero day detection.

E. F5 –Big IP

BIG-IP ASM (Application Security Manager) [11] includes comprehensive, built-in authenticated application security policies for frequent applications as well as aregular policy-building engine that can become accustomed to application updates. This Firewall works as an appliance and provides main facilities like traffic monitoring and blocking. This firewall is among the top ten in the web application firewalls solutions.

F. Web Sniper

WebSniper [12] protects the web servers from disclosure to behavioral attack patterns e.g. buffer overflow exploits, path traversals, SQL injections and cross-site scripting, by implementing signature based detection / prevention. WebSniper supervise the requests sent via Internet, and differentiate between justifiable requests and illegitimate requests. WebSniper can also stop zero day attack, and utter their management as distinct in the configuration. WebSniper also ensure and adapts responses returned from the Web server, to protect customers and prevent data thefts and leaks. It is implemented as ISAPI (Internet Server Application Programming Interface) file to correspond proficiently with Web server. It is a desktop based reverse proxy firewall.

G. I-Sentry

I-Suite [13] is an amalgamated threat management gateway appliance that is equipped with Web application and Web service security administration functionality. Other i-Suite modules security functionalities are access control, vulnerability assessment, single sign-on, Web application discovery, content acceleration, monitoring, user authentication, identity/access management, and data leakage prevention. I-Sentry uses ICX™ technology to monitor and detect all known and unknown attacks, including all OWASP Top Ten attacks.

H. Secure IIS

eEye Secure IIS [14] endow with application layer fortification against zero day attacks, known exploits, and unconstitutional Web access. Secure IIS scrutinize requests at every level of processing either on network layer or at kernel level. Secure IIS supervises data as it is routed by IIS and can block a request at any point if it is similar to any class of attack, including SQL injection and XSS etc.

I. Web Defend

WebDefend [15] is a WAF appliance that present applications layer solution with real-time detection of attacks. It is PCI DSS compliance and provides detection and protection against known vulnerabilities and up-coming threats such as Google hacking, malicious bots, site scraping and zero-day attacks.

J. Anchiva

Anchiva [20] endow with URL filtering, along with a wide variety of other functions such as botnet protection, bandwidth management, antimalware protection, keyword filtering on outbound traffic, and Web content auditing. Anchiva firewall identifies and detects different types of Web form inputs, URL parameters, and block exposure of sensitive information.

K. Profense

Armorlogic's Profense [16] is built on the positive and white listing security model. It allows the authentic requests and disallows everything else. This approach provides protection against zero day attacks (unknown threats). A negative security model having signatures of known attacks can be used in mixture with the firewall's positive policy rules.

L. Citrix

Citrix web Application Firewall [17] is an inclusive Web application security solution that blocks known vulnerabilities and zero day (unknown) attacks against Web applications. This Web Application Firewall implementsa positive security model that allows only accurate behavior of application, without checking attack signatures.

M. WebApp secure

The WebAppsecure Web application firewall [18] inspects HTTP traffic that floods freely through conformist perimeter defenses. Traffic that does not severely adhere to the planned strategy is involuntarily blocked and reported. By implement a white listing approach it is also capable to block known and unknown viruses, worms, and attacks including URL parameter tampering, cookie-tampering and SQL injection.

N. Server defender AI

Server Defender [19] is an effective firewall against the web application attacks and created with the idea of a WASLC (Web Application Security Life Cycle).

III. Evaluation Criteria for Web Application Firewall Comparison

Fifteen web application solutions have been selected for comparison that includes F5, Barracuda, Web Sniper, i-Sentry, Secure IIS, Easy Guard, Web Defend, Secure Sphere, Anchiva, Profanes, Citrix, WebApp secure, eServer Secure, Server defender AI and Mod Security. Detailed comparison has been carried out by selecting the criteria of 'defense mechanism' that includes security policy control, monitoring, blocking, response filtering, attack prevention, authentication, web site cloaking, deep inspection, session protection and overall security performance as shown in table 1. Criteria also include management interface as shown in table 2.
Value of specifications are reflected in the tables with the help of symbols that having specific meaning. Cell of table having tick symbol indicates that the specified feature is available in the firewall. Blank cell indicates the specified feature is not available, question marks symbol indicates that there is no information about the specific feature and HA indicates that feature is only available with the hardware appliance.

Table 1: DEFENSE MECHANISM OF VARIOUS WEB APPLICATION FIREWALLS

Feature: Defense Mechanisms	F5	Barracuda	Web Sniper	i-Sentry	Secure IIS	Easy Guard	Web Defend	Secure Sphere	Anchiva	Profense	Citrix	WebApp secure	eServer Secure	Server defender AI	Mod Security
Security Policy Control															
1. Time Efficient	✓	✓	✓		✓	?	✓	✓	✓	✓	✓		✓	✓	✓
2. Well Organized	✓	✓	✓		✓	?	✓	✓	✓	✓	✓	✓	✓	✓	✓
3. Effective			✓		✓	?				✓					
Monitoring	HA	HA	✓			✓		✓	✓	✓	HA	✓	✓	✓	✓
Blocking	HA	HA	✓	✓	✓	✓	✓	✓	✓	✓	HA	✓	✓	✓	✓
Response filtering	✓	✓	✓	?					✓	✓					✓
Attack prevention	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web site cloaking	✓	✓	✓	✓	✓	✓		✓		✓	?				?
Authentication and Web SSO	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	?	✓	✓	✓	✓
Deep Inspection	HA	✓	✓	✓	✓	✓	✓	✓	✓	✓	?			✓	✓
Session protection	✓	✓	✓	?	?	?	?	✓		✓	✓				✓
Overall Security Performance	✓	✓					✓	✓							

Table 2: MANAGEMENT INTERFACE OF WEB APPLICATION FIREWALLS

Features	F5	Barracuda	Web Sniper	i-Sentry	Secure IIS	Easy Guard	Web Defend	Secure Sphere	Anchiva	Profanes	Citrix	WebApp secure	eServer Secure	Server defender AI	Mod Security
Management Interface															
Web based	✓	✓		✓	?	?		✓	✓	✓	✓	✓	✓		✓
Command line	✓	✓			?	?			✓						✓
Desktop based	✓	✓	✓		?	?	✓				✓	?		✓	
Ease-to-use		✓						✓		✓	✓				
Comprehensiveness	✓	✓					✓	✓		✓					
Flexibility	✓			✓						✓					✓

IV. CRITICAL ANALYSIS

Through the analysis of various Web application firewalls following limitations of various firewall has been highlighted:

- Mod Security unable to detect [7], session id brute forcing attack, forced browsing attack, authentication brute-forcing, HTML hidden field manipulation attack and also lack semantics to understand the contextual nature of attack vector.
- Security group, f5 Web Application Security Manager has mentioned the four reasons [6] to not use Mod Security.
    - Mod Security runs on every web server which is an additional load on the servers that negatively impact the performance and decreases capacity to serve users as well as applications.
    - Expertise are needed to write rules after understanding the attacks which is time consuming task otherwise you have to trust third-party which is an unnecessary security risk.
    - Expertise is needed in the HTTP protocol for sanitizing the HTTP response. Moreover you have to be an expert in Apache configuration directives, and the specific directives used to configure Mod Security.
    - The configuration and writing complex rules & regular expression have to be done manually unless you purchase a commercial version of Mod Security.
- Secure Sphere lacks semantics to understand the context of input vector. It sequentially searches for pattern matching with attack signature. It also less effective for zero days attacks. Secure Sphere required more manual intervention in configuration [8].
- Snort IDS [7] has 868+ signatures out of 1940+ for web layer attacks. Most are for known vulnerabilities in web servers, such as: IIS directory traversal attack and chunked transfer-encoding attacks. Out of these signatures only a few are generic signatures for web application attacks, such as cross-site scripting attack and /usr/bin/perl or other Unix command attempts. Snort posses complicated setup of signatures and only as good as its rule set i.e. Depend upon the effectiveness of rules applied. For management problem a security expert is required. It lacks semantics because it does not take context into account. In Snort rules have to be manually updated.
- Barracuda has disappointing reporting mechanism, limited to alerts, diagnostics and errors. It also lacks traffic shaping mechanism. It is a commercial firewall which comes as an appliance and cannot be used as a plug-in. It is not a freeware firewall. According to Cisco comparison of firewalls its load balancing is not so much efficient [10]. It is a signature based firewall so performance can be improvised.
- Breach Security's Web Defend lacks capability of load balancing, SLL acceleration & offloading, connections pooling, coach & compression, and week in zero day detection.
- Web Sniper has no load balancing module so not performance problem is there. It is a signature based firewall so not so much efficient web application attacks detection.
- F5 –Big IP Firewall work as an appliance and it is too much costly. It cannot be used as a plug-in and all it main facilities like traffic monitoring and blocking can be used while using its device. It's not open source firewall. It is a signature based firewall so performance can be improvised.
- Monitoring and blocking mechanism of I-Sentry is not so much efficient. This is application layer firewall again it is using signature based system and when an http packet is checked for the web attack it will be checked against thousands of signatures which is not good for the performance.
- Monitoring and blocking of Secure IIS is not so much efficient and also response filtering is also not present over here.SSL support is also very week it did not support JKS for SSL. User monitoring is also an issue for this firewall. User tracking function is not available.
- Web Defend firewall is not so much efficient for the web application monitoring and blocking these facilities are not provided in this firewall, and it did not support all the encryption schemes.
- Anchiva firewall does not contain web clocking facilities and session attacks are gaining more attentions these days and it is very much important for WAF's but this firewall doesn't contain the protection again the session attacks. Deep Logging features are not available too. Encryption scheme is also partially supported so encrypted attacks can be done on this firewall.
- Profense provides limited support for SSL because there is no support of JKS provided in this firewall and also Encryption schemes are partially supported, that will leads to the encrypted attacks over web application.

- Logging and real time monitoring of Citrix is a weak point of this firewall. Also the encryption scheme is partially supported.
- WebApp secure firewall is lacking with the session protection and web clocking. It is also lacking with the response filtering and deep inspection functionalities of the http packet. Monitoring and logging facilities are not so much satisfactory. It is a white list based firewall which did not contain the black list technique so it cannot take the advantage of hybrid techniques.
- Server Defender system is lacked with web site clocking and response filtering. Session protection is also not available as a feature and also it did not inspect the web services traffic. It also partially supports the encryption techniques.

V. FINDINGS/RECOMMENDATIONS

Following are the key finding derived from caparison and critical analysis of web application firewalls

1. Web application has become the prime target for hackers; WAF is essential solution for each organization operating on Internet. Moreover a WAF is also essential for e-business due to PCI DSS 6.6 compliance.
2. WAF is highly customized for each environment
3. There is no perfect solution for protection of application, however feature wise various WAFs have advantages over others.
4. SecurSphere can be deployed in various deployment modes like reverse proxy, transparent proxy and in bridge mode.
5. In overall security performance, F5, Barracuda, SecurSphere and WebDefend are effective firewalls. In open source community ModSecurity also providing the satisfactory performance.

VI. CONCLUSION

The nature of cyber-attacks has been shifted from the "spray & pray" approach of general viruses and worms to highly sophisticated targeted attacks against specific organizations, applications and sensitive data. Financially motivated attackers now have a soft target. Instead of wasting their efforts on non-specific network intrusion attempts, they're now targeting the sensitive data accessible through Web applications, and traditional methods of network security are powerless to stop them.

The available security solutions are ineffective due to their focus on network layer and limitations in their core technological design. Organizations have to deploy another layer of defense called Web application firewall. Various solutions available as open source and in commercial market are creating problem for selecting the suitable solution for the security of the organizational systems. This survey paper compared the WAF solutions with important features necessary for the security at application layer. Critical analysis on WAF solutions is helpful for the users to select the most suitable solution to their environments.

VII. REFERENCES

1. Jim Beechey, "Web Application Firewalls:Defense in Depth for Your Web Infrastructure" March 2009
2. Website Security Statistics Report (2010) , Fall 2010, 10th addition- Industry Benchmarks
3. Mod Security, http://www.modsecurity.org/
4. Greg DeArment, Chad Ozust, "The Evolution of IDS"
5. SecureSphere – The First Dynamic Profiling Firewall, http:// www.imperva.com
6. Four reasons not to use ModSecurity, http://devcentral.f5.com/weblogs/macvittie/archive/2008/07/ 23/3477.aspx July 23, 2008.
7. K. K. Mookhey, Network Intelligence "Detection and Evasion of Web Application Attacks," http://www.nii.co.in.
8. Sandra kay miller, Information security, product review 2008
9. http://www.barracudanetworks.com/ns/products/ng_firewall_ overview.php
10. PCI-DSS -Information Supplement: Application Reviews and Web Application Firewalls Clarified
11. http://www.f5.com/products/big-ip/ application-security-manager.html.html
12. http://www.bugsec.com/index.php?q=WebSniper
13. http://www.bee-ware.net/en/solutions/ web-application-firewall
14. http://www.eeye.com/Products/SecureIISWeb- Server-Security.aspx
15. https://www.trustwave.com/webapplication- firewall.php
16. http://www.armorlogic.com/profense_overview.html
17. http://www.citrix.com/English/ps2/products/subfeature. asp?contentID=2300448
18. http://www.webscurity.com/products.htm
19. http://www.port80software.com/ products/serverdefendervp
20. www.anchiva.com/