cloudbric
THE EASIEST WEBSITE PROTECTION

Cloudbric | Website security you can depend on

With the advancement of technology such as mobile, cloud computing, and IoT the world has become increasingly interconnected through the seemingly endless expansion of new web applications. This has resulted in the internet becoming a dynamic global environment of commerce and communication, with subjects ranging from enterprise to small business and individual users. However, as social interaction through web applications increases due to the extension of the web application player, the greater the risks they have become exposed to. This is because security for web application users has not evolved as quickly as web applications themselves, becoming the number-one target of hackers these days.

Once web applications became the number one target of hackers, a new form of security was needed. Web application firewalls (WAFs) were introduced by a variety of information technology security firms to defend web applications against the rapidly growing arsenal of threats. However the shortcomings of the early generations of WAFs such as labor intensiveness, high rates of false positives and the their cost, and the technology entry barrier of security discouraged many web application users from utilizing WAFs to protect their systems.

In response to the need for a reliable, affordable, and easy-to-use web application security solution, Cloudbric-the easiest website protection service from Penta Security Systems, Inc. - was created. Cloudbric offers advanced, all-inclusive, and accessible security service powered by WAPPLES, - the latest generation WAF from Penta Security Systems, Inc. - which utilizes an intelligent, logic-based engine, capable of keeping pace with the rapidly evolving threats which target web applications.

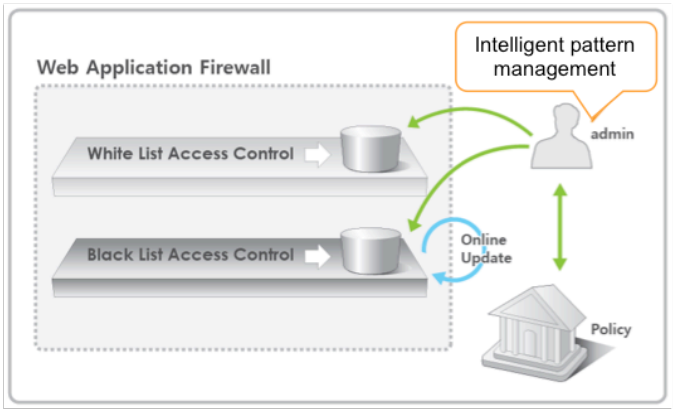
Drawbacks of Previous WAFs

The major operating principle of first generation WAFs was pattern matching, a process that involved extensive administrative manpower. After an administrator added a known attack pattern (black list), the first generation WAF compared web traffic to the updated patterns by analyzing them at the application level. Unfortunately, the first generation WAF was absent of a detection system for new or modified attacks. Additionally, attempts to add patterns for all conceivable attacks led to both a deterioration in web application performance, an increase in false positives, and a heavy workload for the WAF administrative team. The high costs of manpower and high level of knowledge of security required to operate a first generation WAF, combined with its inability to protect against new or modified attacks, its tendency to produce false positives, and its poor system performance limited its success in the IT security market.

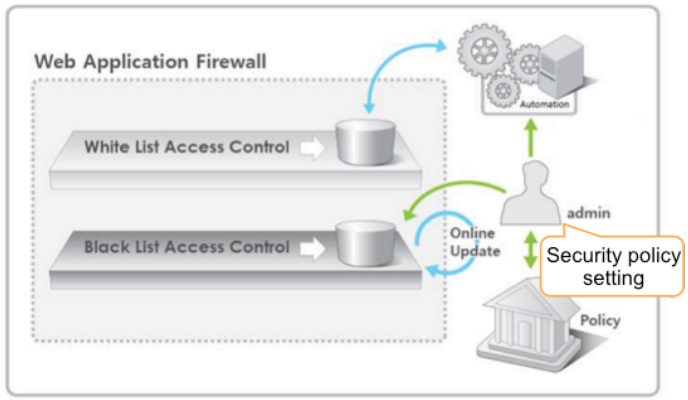
The second generation WAF attempted to remedy the flaws and limitations of the first generation. By analyzing the web application(s) protected by the WAF, the second generation WAF was able to automatically establish a security policy (white list). Unfortunately, such automatically established policies could take up to two weeks to implement, rendering this solution impractical for the rapidly changing environment of the web. Additionally, while the policies were established automatically, they still required manual configuration by an administrator, thus increasing – not reducing – the administrative burden and the knowledge of web application security. Lastly, as pattern matching

remained the basis for the second generation WAF, it still suffered from many of the limitations which afflicted the first generation WAF, namely an inability to protect against unknown attacks, a tendency to produce false positives, and slow system performance.

Meanwhile, the threats against web applications has endured and evolved. The web application layer remained vulnerable and a frequent target of hackers. A solution was needed, one which could overcome the drawbacks of the early generations of WAFs to offer secure, reliable, cost-effective, and easy-to-use security. A new breed of WAF – an intelligent WAF – one based on an entirely new concept, was needed. Such an intelligent WAF would need to be capable of analyzing web traffic, detecting attacks, analyzing and classifying them, and finally, applying appropriate countermeasures to block detected attacks. An intelligent WAF would need to be able to perform these functions without the continual involvement of administrative staff, in order to protect web applications in a stable manner while easing the administrative workload and management costs.



〈 1st Generation WAF 〉



〈 2nd Generation WAF 〉

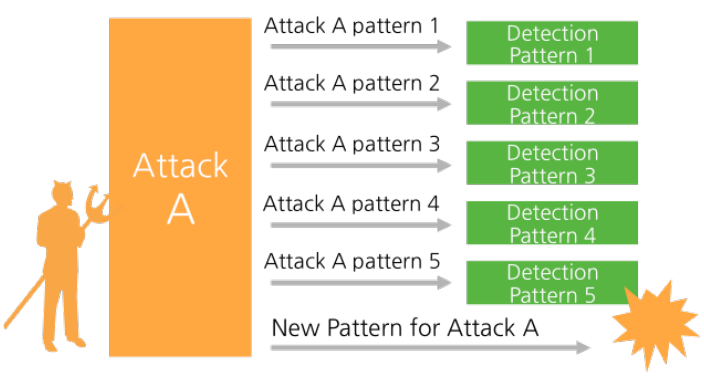
WAPPLES: The Third Generation WAF

In response to the need for an intelligent WAF that could meet the security, Penta Security Systems, Inc. created WAPPLES: the third generation WAF. Unlike previous generations of WAFs, WAPPLES is equipped with an intelligent logic analysis engine, designed to identify attacks against the web application (whether previously known or unknown) and defend against them.

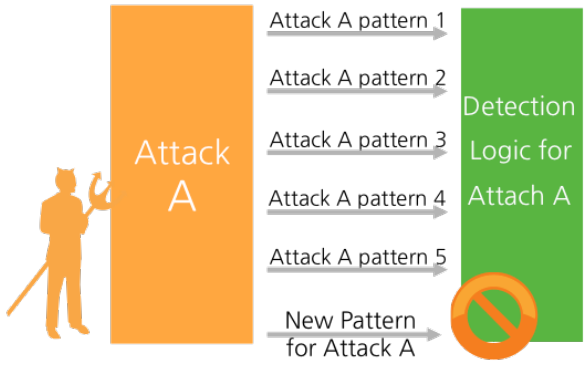
The COCEP Engine and its 26 Rules

WAPPLES runs on an intelligent logic analysis engine called Contents Classification and Evaluation Processing, or COCEP. This logic analysis engine utilizes a system of 26 'rules' (see Appendix A for detailed explanations of each rule) to execute a logical analysis of all types of traffic. This analysis enables WAPPLES to determine whether or not the traffic constitutes a threat to the web application, and to take appropriate countermeasures when threats are detected. If traffic can successfully pass through all 26 rules, WAPPLES determines that the traffic is not an attack, and transports the data to the web application. The split-second performance of the COCEP enables WAPPLES to determine if traffic is safe in just 1/1000 of a second, leaving system performance unaffected.

Unlike previous generations of WAFs, WAPPLES does not require the administrator to add patterns manually, as the COCEP logically recognizes attacks (whether previously known or unknown) on its own. Likewise, the automated functionality of WAPPLES allows it to automatically respond to attacks detected by the COCEP, without involving administrative personnel. Additionally, as the COCEP engine operates on logic, rather than pattern matching, this allows WAPPLES to boast a much lower rate of false positives compared to its earlier counterparts, which do not consider the characteristics of each attack. WAPPLES offers intelligent and accurate protection against threats that target web applications, enabling PCI-DSS certified security and the ability to detect and block the threats enumerated in the OWASP Top Ten – 2013 report. Web attack detection and response through the logic analysis of the COCEP have made WAPPLES the new paradigm of web application security.



〈Detection Engine of 1st and 2nd Generation WAF〉

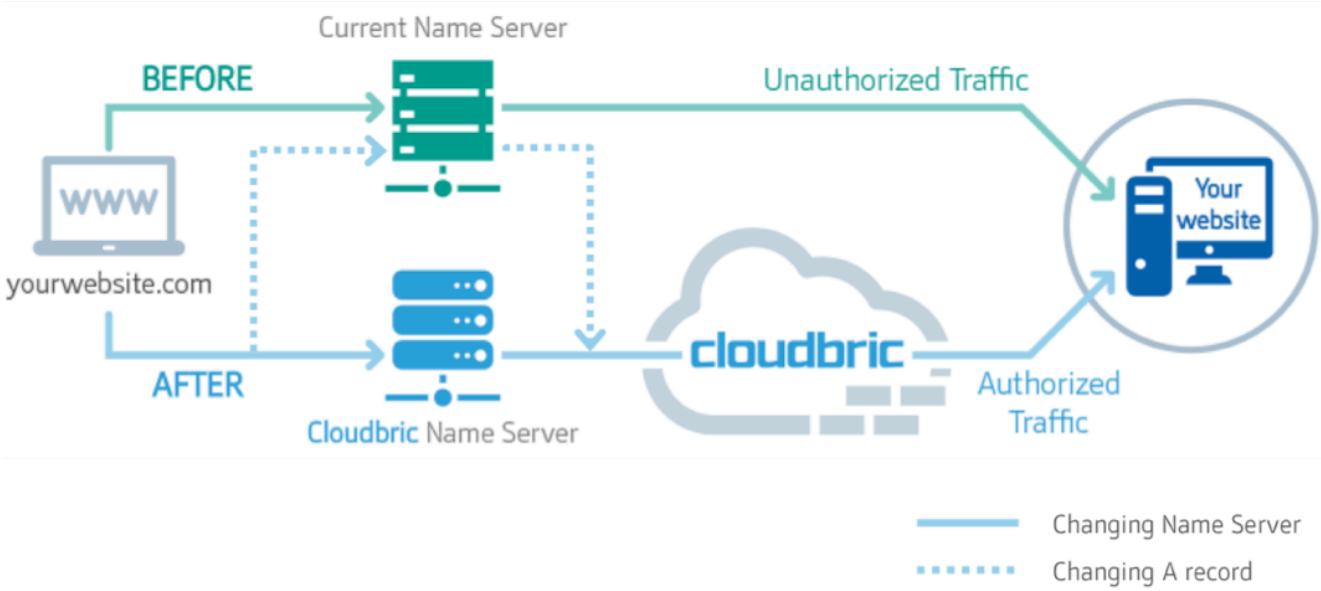


〈 WAPPLES COCEP Engine 〉

Though WAPPLES resolved the drawbacks of 1st and 2nd WAF solutions, it remains unaffordable for SMBs and individual users in terms of both cost and knowledge required for WAF security. Therefore, in response to this need, Penta Security System, Inc. created Cloudbric which offers Security as a Service.

What is Cloudbric?

Cloudbric offers WAPPLES security as a service without requiring installation of a WAF solution in front of the web server which was previously needed as either hardware or software form. Cloudbric just requires a DNS (Domain Name Server) setting change of the website to make itself a proxy server. A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers.



< Traffic flow before and after DNS setting change >

Every website has a domain name and web server IP. Prior to setting the proxy server, the domain is mapped to the web server IP so that when a client enters the domain, the website DNS setting lets the request go directly to its web server. DNS setting change lets the Cloudbric server reside between the client and web server, so that all requests pass through the Cloudbric server, in which WAPPLES is installed. Of course WAPPLES is already set up by security specialists, which reduces the WAF user's burden of knowing technical security details.

Distinguishing Factors

Advanced

Cloudbric is based on WAPPLES, which resolves the fundamental problems of previous generations of WAFs. While the first and second generation WAFs employed a pattern matching method, WAPPLES can intelligently detect and block known, new and modified attacks by logically analyzing web traffic with the COCEP engine. Based on WAPPLES, Cloudbric provides reliable and accurate protection against the OWASP TOP 10 vulnerabilities with guaranteed low false positives and high performance.

Accessible

Cloudbric boasts an easy-to-use and user-friendly console.
With a simple DNS setting change of website, not only the security staff, but those who do not have security knowledge can utilize WAF easily. Cloudbric, which is already setup by security specialist, provides WAF automatically after a DNS setting change. It analyzes and blocks malicious attacks while traffic passes through it.

Cloudbric also offers the information of visits and attack detections with an intuitive console. This intuitive console allows users to view the status of the website such as attack purpose, attacker information, and detection events, and to customize an additional blacklist or whitelist.

< Cloudbric Intuitive Console >

All-Inclusive

In response to the problem, a small business or individual cannot afford the high cost of a WAF solution either in hardware or software, however, Cloudbric provides comprehensive security solutions for all web application users because no matter how small they are, they are still under threat from web attacks.

It is an innovative model compared to current WAF solutions, but it is quite reasonable considering it charges WAF based on the size of the website. Additionally, since it is based on WAPPLES image, businesses can switch their WAF solution from the Cloudbric service to WAPPLES appliance or software much smoothly when it expands.

Summary

As the number of web applications is increasing and more individuals and businesses are implementing these applications, security for its users is becoming increasingly important. However, the adoption of WAFs has been relatively low as a result of the shortcomings of early generation WAFs and a high technology entry barrier for non-security specialists.

WAPPLES was introduced as a remedy to the limitations that earlier WAFs suffered from, with its revolutionary design based on intelligent attack analysis. However, it still requires understanding of security technology and is not affordable for SMBs and individuals. In order to allow all web application users to utilize WAF protection themselves from web attacks, Cloudbric brings about WAPPLES as a service. With Cloudbric, users are only required to simply change the DNS setting of website to utilize the most advanced, comprehensive security service all at a manageable cost.

The threats facing web applications are ever-present and continuously evolving. The best method for securing web applications is an intelligent and ever vigilant sentinel, standing guard over the web application layer. The Wapples based Cloudbric, provides such a defense for all web application users.

APPENDIX A: WAPPLES Rules

Buffer Overflow	Block invalid requests causing buffer overflow attacks (Compare subject length and maximum value)
Cookie Poisoning	Blocks the falsification of cookies containing authentication information
Cross Site Scripting	Blocks malicious script code having the possibility to be executed by the client
Directory Listing	Block the leakage of web sites' directory and files
Error Handling	Controls error messages so as to avoid exposure of information about web server, WAS, DBMS server, etc
Extension Filtering	Blocks access of files which do not have permitted file extensions
File Upload	Blocks the upload of files which can be executed on the web server
Include Injection	Blocks the injection of untrustworthy files and external URIs
Input Content Filtering	Blocks or substitutes words that are not permitted on a website
Invalid HTTP	Blocks access not in compliance with HTTP standards
Invalid URI	Blocks access not in compliance with standard URI syntax
IP Black List	Blocks when more than the set value of access attempts from the same source IP are detected during a specific time (value set by user)
IP Filtering	Blocks access to a specific IP range or countries (set by user)
Parameter Tampering	Blocks attacks which send maliciously manipulated parameters to websites
Privacy File Filtering	Blocks leakage of private information from files transmitted from the web server
Privacy Input Filtering	Blocks leakage of private information via HTTP request
Privacy Output Filtering	Blocks leakage of private information via HTTP response
Request Header Filtering	Blocks HTTP requests having headers that have been abnormally modified
Request Method Filtering	Blocks risky HTTP request methods
Response Header Filtering	Blocks leakage of web server information via HTTP response
SQL Injection	Blocks requests to inject SQL Query statements
Stealth Commanding	Blocks requests to execute specific commands in the web server through HTTP Request

Suspicious Access	Blocks access which does not fit the standard web browser request
Unicode Directory Traversal	Blocks request of access to directory and files using vulnerabilities related to Unicode manipulation of the web server
URI Access Control	Controls requests of access to specific URIs and files
Website Defacement	Detects defacement of websites and recovers the web page

* *Rule:* Categorized by characteristic features of different attack types

APPENDIX B: International Patents and Certifications

- Payment Card Industry Data Security Standard (PCI-DSS) Certification
- Korea National Intelligence Service CC Evaluation (EAL4) Registration
  No. NISS-2049-2010
- China Patent: Method of Detecting a Web Application Attack Chinese Application
  No. 201010287262.2
- Japan Patent: Method of Detecting a Web Application Attack Application
  No. 2010-178803
- Korea Patent: Method for Detecting a Web Application Attack
  No. 10-2010-0064363
- Korea Patent: Method for Detecting a Web Attack Based on a Security Rule
  No. 10-2009-0077410
- Korea Patent: Linking with Web Source Vulnerability Analysis Tool
  No. 10-2011-0127909