Penta SECURITY

WAPPLES V-Series

Cloud Solution Optimized for Cloud Environments

May 2014

Penta Security Systems Inc.

SL5 PUBLIC

Table of Contents

Introduction

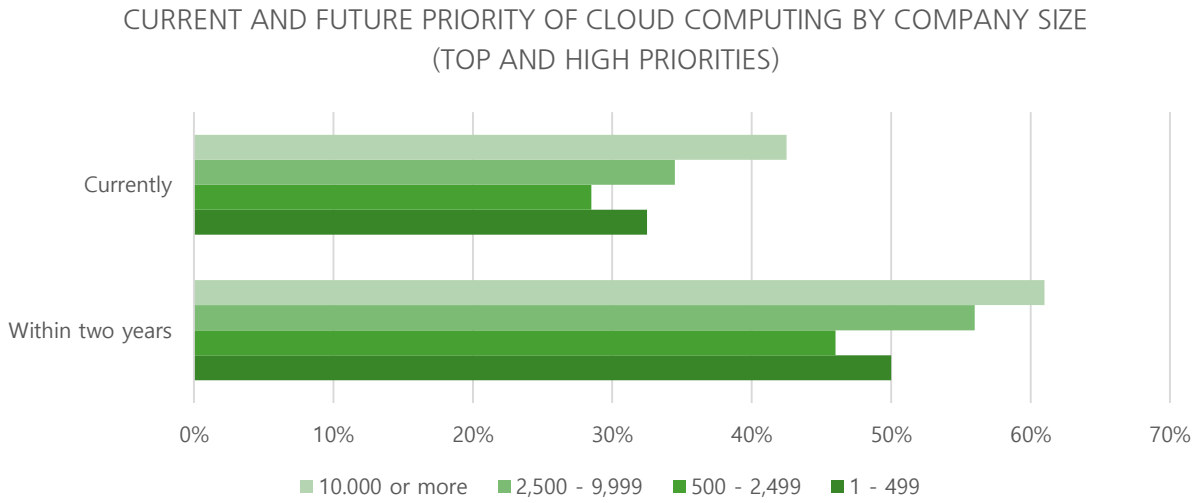
The overall cloud computing environment is evolving at an in increasing rate. The effective and cost-efficient nature of cloud environments has been drawing attention of numerous governments, corporations and individuals. This has led to the development of relevant technologies to meet the increased needs. Also, the issue of maintaining the integrity and security of data has been brought to the table, as the paradigm of computing shifts from a physical network to a cloud-based environment.

Although many cloud users are working to strengthen security, several reports indicate that cloud security has not been able to keep up with the rapidly increasing usage rate in the cloud. Considering the popularity of cloud services, providers need to establish appropriate protective measures.

Increasing Popularity

To be successful in the privates sector, any IT product must be functional and use-friendly. By meetings these standards, cloud computing has been growing at a rapid pace. According to the results of the Global State of Information Security Survey 2014 (ISC), 47 percent of the 9,600 surveyed management board members replied that they were using cloud computing. This is 24 percent higher than the previous year's result. A Gartner report predicted that the cloud service market will have an average growth of 18. 9 percent in the future.

The ISC report revealed that the priority on cloud computing is expected to rise continuously for next two years, based on information gathered from 12,000 security experts. As such, the usage rate of cloud computing will grow along with the increased prioritization. Moreover, 47 percent of security experts in information-related industries deemed cloud computing as the top priority, and this number is expected to reach 69 percent within two years.



The 2013 ISC 2 Global Information Security Workface Study

With the growth of cloud computing, cloud security solution usage is on the rise. As a result, the confidence in cloud security is at all-time high. In fact, 74 percent of executives who participated in the Global State of Information Security Survey replied that they have confidence in their cloud security solutions.

Accelerating Threat

The increasing popularity of cloud computing has bred much more than the increase in related security measures. Results from the Global State of Information Survey 2014 (GSIC 2014) indicate that detected threats against cloud environments have also increase by 25 percent since last year. Not surprisingly, new threats targeting cloud data have been rising rapidly.

Although most executives have confidence in their cloud security measures, there are many glaring shortcomings. In 2013, there was an incident where the cloud-based memo service Evernote was hacked, with millions of users being forced to change their passwords. This was an important event that sparked awareness of the vulnerabilities in the cloud, even for a cloud service with 50 million users. Furthermore, although investment into security has increased since last year according to the GSIC 2014, security expenditures comprises a meager 3.8 percent of the total IT-related budget, and only 18 percent of those surveyed had security policies for cloud service management. The current status of cloud security can be illustrated by the quote below.

> *Overall, the costs and complexity of responding to incidents are increasing, and security controls have not kept pace with the ever-change threat landscape.*
>
> **Shane Sims**
> **PwC Principal**

In order to respond to the ever-increasing threats targeting cloud data, cloud service users must work to check their cloud security and find appropriate security measures.

Limitations of Pre-existing WAFs

In the past, implementing WAFs was a challenge, in both physical networks or cloud environments. This was due to the well-known limitations of previous generation WAFs. These limitations were the main reason why cloud service providers were unwilling to use WAFs.

The 1st generation WAF were quite cumbersome, because the security administrator had to manage them with their pattern matching-based design. Although the blacklist can be generated automatically, the whitelist requires manual management through updates executed by the security administrator. These WAFs were designed to detect and block attacks, by filtering web traffic through these lists. Hence, the 1st generation WAFs required regular manual operations, causing too much work for the administrator. These WAFs could not respond to new threats immediately, and would often hinder web application performance when the lists had too many signatures.

2nd generation WAFs is list-based, much like their 1st generation counterparts. The key difference is that whitelists, in addition to blacklists, are generated automatically . In order to generate these lists, however, it takes a significant amount of time and effort to analyze traffic prior to starting the security service, and to modify security policies according to different web environments. Moreover, even automatically generated lists require manual management by the administrators, increasing the management burden. Moreover, the inability of the pattern-matching method to catch previously unknown attacks poses a glaring limitation.

Finally, 1st and 2nd generation WAFs use single black/white lists to respond to all threats, instead of using different ones for different attack categories. This has led to a high rate of false positives, which not only lowers detection accuracy but also hinders system performance.

WAPPLES, a 3rd Generation WAF

To overcome the limitations of the previous generations of WAFs, Penta Security Systems developed a revolutionary 3rd generation WAF, called WAPPLES.

Unlike other WAFs, WAPPLES utilizes the COCEP (Contents Classification and Evaluation Processing) engine, a logical analysis engine developed independently by Penta Security Systems. Performing an extensive analysis of web traffic with its 26 detection rules that are categorized by primary attack types, COCEP allows for a much lower rate of false positives, compared to its earlier counterparts that do not consider the characteristics of each attack. Also, by utilizing a logical analysis of web traffic, instead of relying on black/white lists that need constant updates, WAPPLES eliminates the management burden that other WAFs place on security administrators.

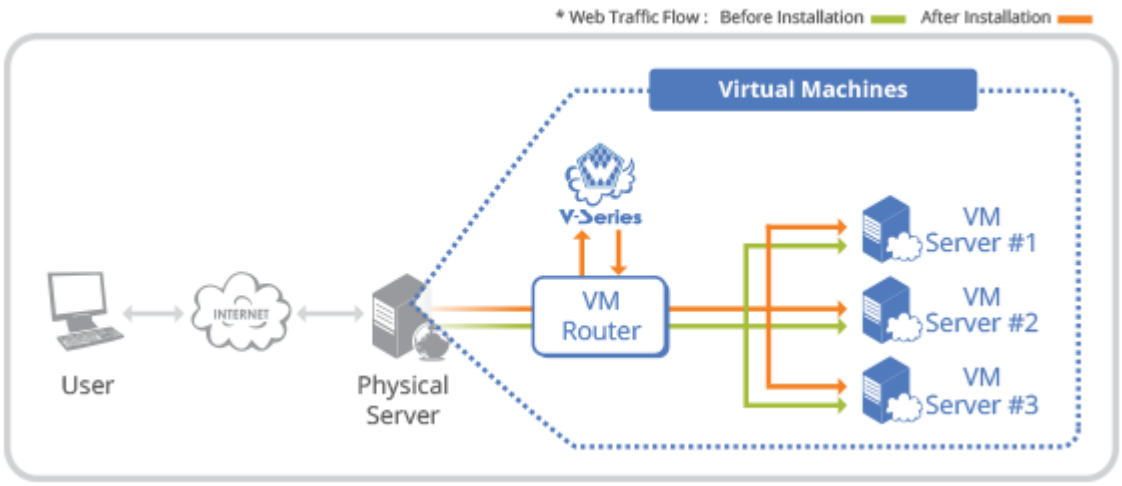
WAPPLES was initially released in 2004, and has over 2,500 units deployed all over the world.

What is WAPPLES V-Series?

Developed in its entirety by Penta Security Systems Inc., WAPPLES V-Series is a virtual WAF solution for cloud computing providers and users of cloud computing.

Provided as a virtual image rather than an appliance, it is optimized for virtual environments and protects enterprise systems using cloud environments, while supporting various virtual solutions such as VMware vSphere, Citrix XenServer, Microsoft Hyper-V, and Red Hat KVM.

V-Series operates on the same principle as its appliance counterpart, and thus provides the same high level of security in virtualized environments.



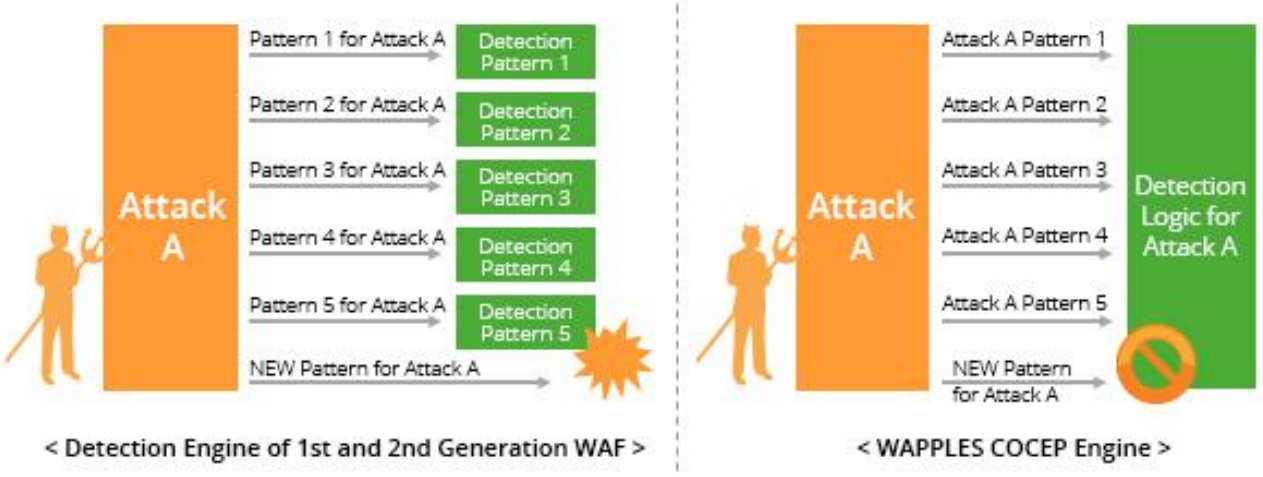
Web Traffic Flow

- *All web traffic passes through V-series before heading to the VM servers. Hence V-Series can detect attacks targeting VM servers within the physical server.*

Distinguishing Factors

With its revolutionary design based on an intelligent attack analysis engine, WAPPLES was introduced as a remedy to the limitations of other WAFs. With WAPPLES V-Series, this technological approach has been extended to cloud environments.

Like its appliance counterpart, WAPPLES V-Series provides detection with COCEP. Since it analyzes attacks using a logic-based method instead of the old pattern-matching method, it can detect previously unknown attacks and boasts a low rate of false positives compared to other WAFs.



Difference from 1st and 2nd Generation WAFs

WAPPLES V-Series provides the same level of high security as appliance type WAPPLES, while supporting various hypervisors such as VMware vSphere, Citrix XenServer, RHEV KVM and Microsoft Hyper-V. Also, it is optimized for cloud environments with its virtual form, allowing high scalability without the need for additional hardware.

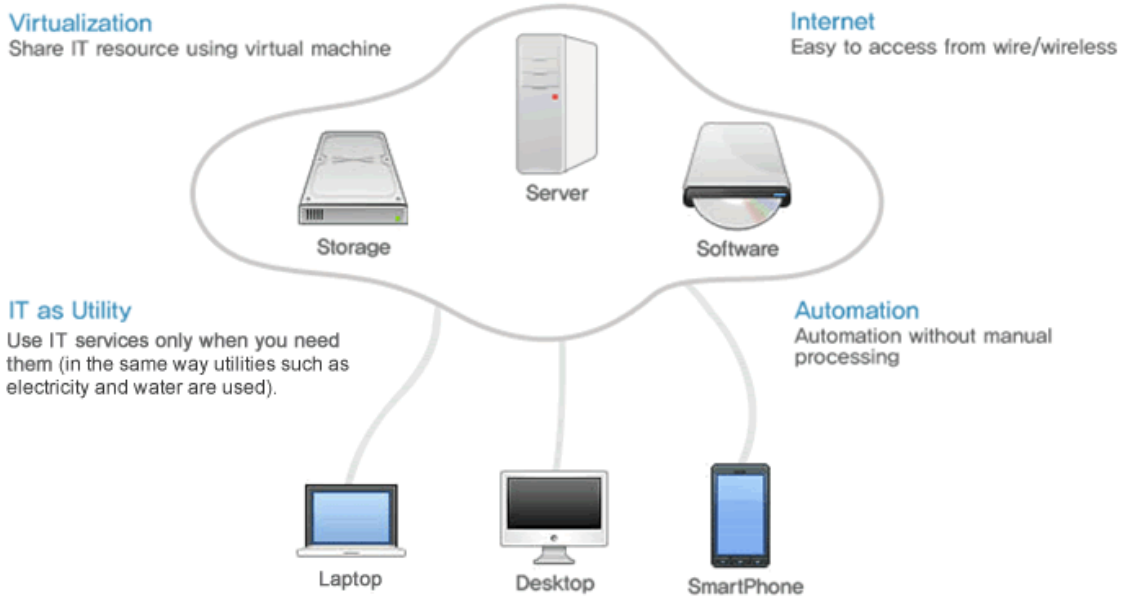
Through the WAPPLES V-Series GUI Console, security policies can be established and managed easily by administrators, even those who are not experts in managing web applications. After installation, modifications in the application do not necessitate any modification to WAPPLES V-Series, further lightening the management burden.

In terms of cost, it requires less Total Cost of Ownership (TCO) compared to its hardware counterpart, thus reducing management costs.

WAPPLES V-Series distinguishes itself from earlier WAFs in various aspects such as security, scalability, convenience and cost, with nine years of industry experience behind it.

Services for Cloud Service Providers

Potential cloud service customers continue to show concerns about storing their data in a cloud environment. Cloud service providers can solve these concerns by providing the WAPPLES V-Series solution.



Cloud Services

Customers can provide high-level security and management through WAPPLES V-Series, a WAF optimized for cloud environments.

As the WAF exists on a cloud as a virtual product, customers can gain access through a simple transaction process. Hence, cloud service providers can offer their cloud services with adequate security.

Implementation Procedure and Effect

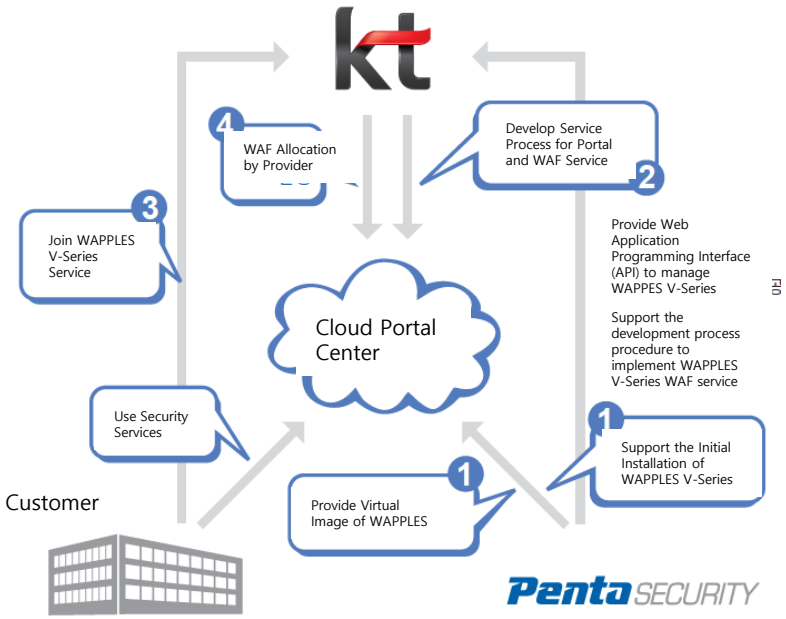
For the implementation of WAPPLES V-Series, collaboration between the cloud service provider and Penta Security Systems is necessary.

The cloud service provider creates the website to use the WAF service, and establishes user procedures. Penta Security Systems supports the initial installation of the WAPPLES V-series model, chosen by the cloud service provider for their cloud environment. The cloud service provider then configures the WAF so that it is available to customers after purchase.

Upon selecting WAPPLES V-Series, users are protected with a web application firewall that is easy to use. As a result, cloud service providers can gain more trust from their customers, with a comparative advantage over their competitors.

Success Story: KT ucloud biz

In 2011, the telecommunications company KT started ucloud, the first cloud service in Korea. Much like Amazon's EC2, all KT services (web server hosting, data storage, software application) are provided through the cloud.



KT ucloud biz Deployment Model

To meet the increasing demand from customers, KT has provided WAFs through their cloud environment. In addition, KT elected to provide this service by using WAPPLES V-Series exclusively. By providing this WAF solution from the very beginning of their cloud services, KT was able to raise both security and consumer trust.

Summary

As more enterprises and individuals are implementing cloud computing for its effectiveness and cost efficiency, cloud security is becoming increasingly important,. Although many cloud security solutions have surfaced, the adoption of WAFs has been relatively low. This is because of high installation and maintenance costs, not to mention the difficulties related to operating WAFs. Also, most WAFs were not designed with cloud environments in mind. Therefore, in the eyes of many experts, WAFs have not seemed suitable for cloud security.

However, provided in a virtual image form, WAPPLES V-Series has changed this perception. With its ease of installation and operation, the V-Series is a solution that can be implemented with manageable initial costs. It also raised the standards of cloud WAFs by boasting the same high level of security as its appliance counterpart.

Optimized for cloud environments, WAPPLES V-Series can help grow the cloud environment achieve security by providing intelligent, accurate and convenient cloud security services.

APPENDIX A: WAPPLES V-Series 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

t h a n k **y o u**

Penta Security Systems Inc. (Headquarter)
Hanjin Shipping Bldg. 20th fl. 25-11
Yoido-dong, Youngdeungpo-ku, Seoul, Korea 150-949
Tel. 82-2-780-7728 Fax. 82-2-786-5281 / www.pentasecurity.com

Penta Security Systems K.K. (Branch)
Ascend Akasaka Bldg. 3F, 3-2-8 Akasaka,
Minato-Ku, Tokyo 107-0052 Japan
Tel. 81-3-5573-8191 Fax. 81-3-5573-8193 /
www.pentasecurity.co.jp