WAPPLES White Paper

No. 1 Market Share in Asia-Pacific
The Intelligent Web Application Firewall

WAPPLES Inquiries:
globalbiz@pentasecurity.com

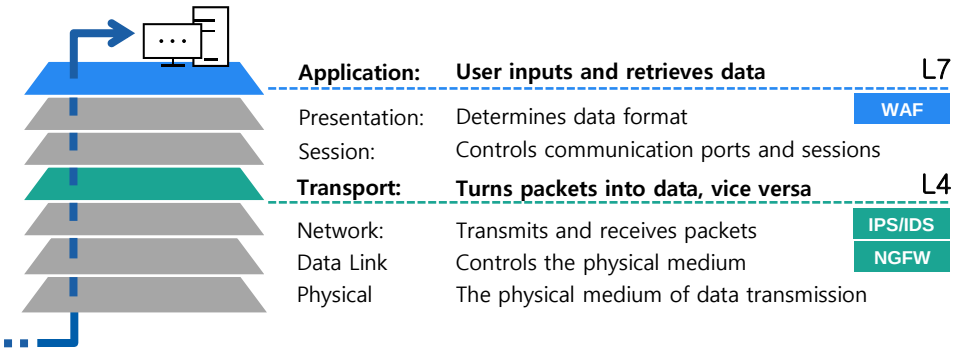
Penta SECURITY

Contents

Introduction

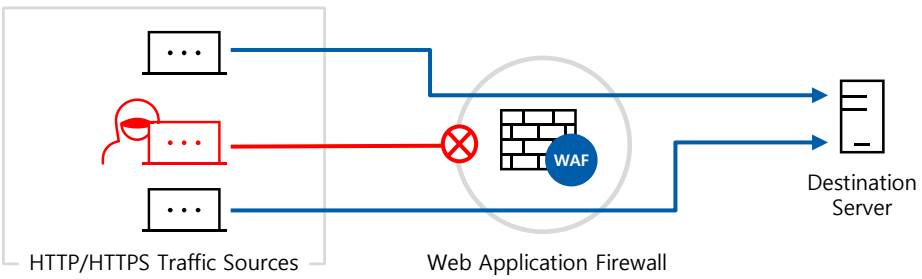
Overview

Unlike network firewalls, a **web application firewall (WAF)** is a cybersecurity solution specifically developed for securing web applications. The main role of a WAF is to protect the web server from external attacks by analyzing HTTP/HTTPS traffic flowing in and out of the application layer, the 7th layer of the OSI model (see figure below). By doing so, it ultimately prevents the leakage of server information and sensitive data.



Being the most effective defensive tool against web attacks, most cybersecurity regulations specify the WAF as a mandatory security measure for protecting personal data. This means that adopting a WAF is an obligation rather than a recommendation. Failure to do so may result in fines and penalties.

To prevent data leakage, a WAF scans web forms, discussion boards, as well as file uploads and downloads to detect any matches of sensitive data. It then responds accordingly by either flagging or blocking the data transmission. Other than safeguarding data, a WAF is also effective against fraudulent logins and website forgery. To prevent fraudulent logins, a WAF monitors the web forms to detect signs of brute-force attacks and credential stuffing. A WAF can also detect attempts of website forgery and control access as needed.



Introduction

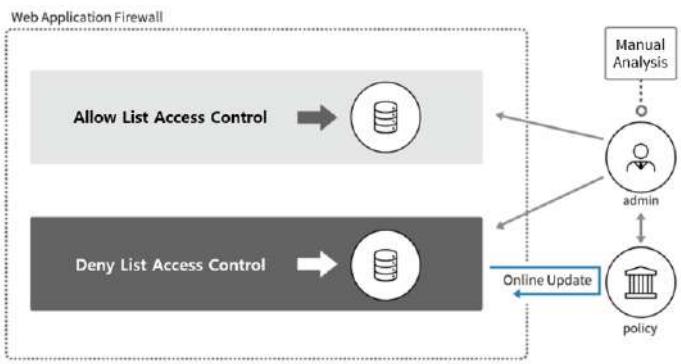
The Evolution Process of the WAF

Based on their underlying mechanisms, WAFs can be classified into 1st generation, 2nd generation, and 3rd generation and above.

The operating mechanism of the **1st-gen WAF** was based on the pattern-matching method used in intrusion prevention systems (IPS). A deny list made of known attacks and an allow list made of authorized users would be registered by the administrators in advance, after which the WAF would analyze application-layer traffic and compare it with the registered lists. Everything listed on the deny list would be denied access (known as the *negative security model*), where everything on the allow list would be granted access (known as the *positive security model*). The reason two lists were needed was because it was impossible at the time to record all known attacks to the deny list. This was a crucial flaw for all 1st-gen WAFs.

A more serious flaw is that the pattern-matching method was not capable of detecting new or modified attacks. To make up for this weakness, administrators had to register a high number of attacks into the deny list. However, this significantly increased the false positive rates and undermined application performance. Moreover, developers and administrators had to manually analyze all new attacks and add them to the deny list, making these WAFs extremely expensive to operate.

1st-Gen WAF Operating Mechanism



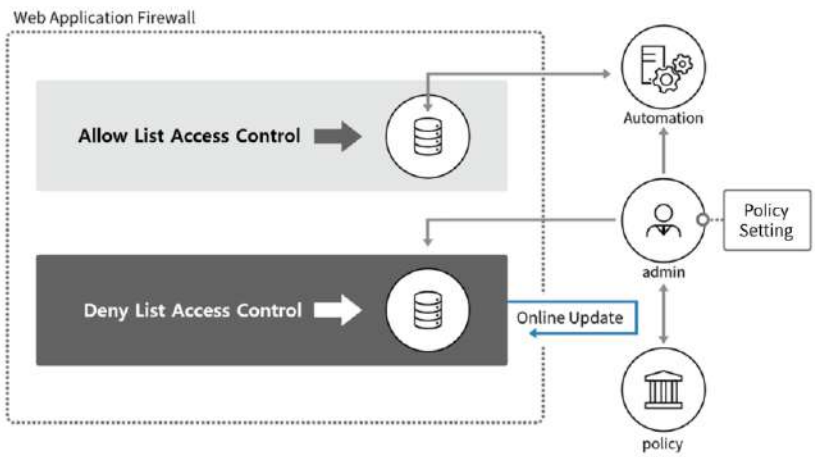
Clearly, 1st-gen WAFs were not very effective because they were slow and inefficient at adapting to the fast-changing web attack patterns. Instead of being applied in such a dynamic environment, the pattern-matching method used by 1st-gen WAFs was more suitable for static environments such as database access control.

Introduction

The **2nd-gen WAF** was born out of the efforts to overcome the operational difficulties of the 1st-gen WAF. Its major improvement was that it could automatically generate an allow list by analyzing the web application. Yet, this automated security policy generation process had some fundamental flaws. Moreover, the 2nd-gen WAF still relied on the pattern-matching method, leaving some inherent issues unsolved.

The automated allow list generation function created information to be registered in the security policy by saving the web application as a profile. However, this automated security policy generation process was criticized to be highly impractical in that it could undermine the overall function of the WAF. Along with the inherent limitations of the pattern-matching method, it was hard to say that 2nd-gen WAFs were truly any better than the previous generation.

2nd-Gen WAF Operating Mechanism



- **Low Practicality**

  It required over two weeks for the 2nd-gen WAF to automatically generate the allow list. During this process, manual intervention was required by the security administrators, resulting in an overall increase of burden in management.

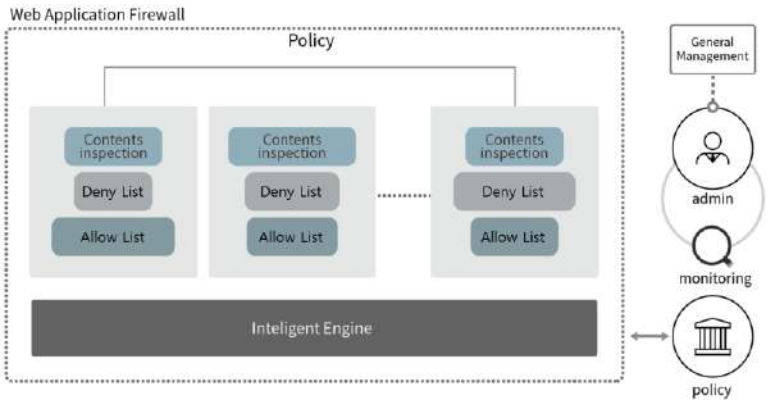
- **Inherent Limitations**

  The automated policy generation function was indeed not an effort to solve the inherent limitations of 1st-gen WAFs. Other than making the signature list management process a little more convenient, the 2nd-gen WAF had no other improvements. With the same essential structures and the same pattern-matching methods, the 2nd-gen WAF had the same limitations as the previous generation.

Introduction

By logically combining techniques such as deny list detection, allow list detection, and web traffic content analysis to defend against each type of web attack, the **3rd-gen WAF** significantly reduces false positives compared to the previous two generations. In addition, the 3rd-gen WAF can detect new attack variants by utilizing logic, reducing the total amount of signatures needed on the list. This solves the issue of having to constantly update the signature list, as required by the previous two generations of WAF. Administrators can now focus on customized policy setting rather than having to worry about list generation itself, making WAF management much more efficient.

3rd-Gen WAF Operating Mechanism



Today, cyberattacks are evolving at faster rates partially due to rapid technological and environmental changes such as the need to work from home. To cope with these new challenges, many 3rd-gen WAFs utilize rule-based logical detection enabled by AI and machine learning technology, further enhancing their performance.

Machine learning allows computers to learn by analyzing data without direct instructions, then use the results of the analyses to solve problems and improve performance all by themselves. In an environment exposed to an increasing number of rapidly evolving web attacks, it is no longer difficult to offer robust security by simply comparing existing patterns. WAFs that run on rules created by machine learning can detect diverse types of web attacks with near-perfect accuracy.

Introduction

Case Study: Web Application Security Threats

According to Verizon's 2020 Data Breach Investigations Report[1], about half of all data breaches today are caused by attacks targeting web application vulnerabilities. As attacks on web applications continue to grow, it becomes difficult to cope with the ever-increasing new attack variants with existing WAFs. Based on Symantec's Internet Security Threat Report released in 2019[2], there had been 357,019,453 new variants of malicious codes/malware discovered in 2016 and another 669,947,865 discovered in 2017. In order to defend against these new web attack variants, it is essential to adopt an intelligent WAF like WAPPLES, equipped with a logic-based detection engine based on rules generated by AI and machine learning technology.

- **South Korean hotel booking platform suffers web attack**

  The IT network of a popular hotel booking platform in South Korea was hacked, leaking a total of 3,410,000 records, including the personally identifiable information (PII) and hotel reservation information of over 990,000 users. The company's website was vulnerable to SQL injection and its admin homepage lacked security tools that would detect and block session hijacking. As one of the most common web attacks, SQL injection can be easily prevented with a WAF. This case shows that all organizations in both the public and private sectors must adopt a WAF.

- **French IT giant hit by ransomware attack**

  One of the largest IT firms in France was hit by a new strain of the Ryuk ransomware family. Since its cybersecurity provider was not aware of the new ransomware strain, the company was unprotected. Even though the IT giant claimed that the ransomware only affected a small part of its network, it was not able to provide any estimates of leaked data. To protect against new strains of ransomware, a WAF run on rules based on AI and machine learning is necessary.

- **US public school attacked by new malware variant**

  A public school in the US suspended remote learning due to an unexpected cyberattack. The attack was caused by a new malware variant that was undetectable by its cybersecurity provider. As the FBI investigated the case, the school had to shut down its IT systems for three weeks to prevent the malware from any further spread. Some servers remained unrecoverable. Again, a rule-based WAF built on machine learning would have prevented this incident.

1. 2020 Data Breach Investigations Report by Verizon
2. 2019 Internet Security Threat Report by Symantec

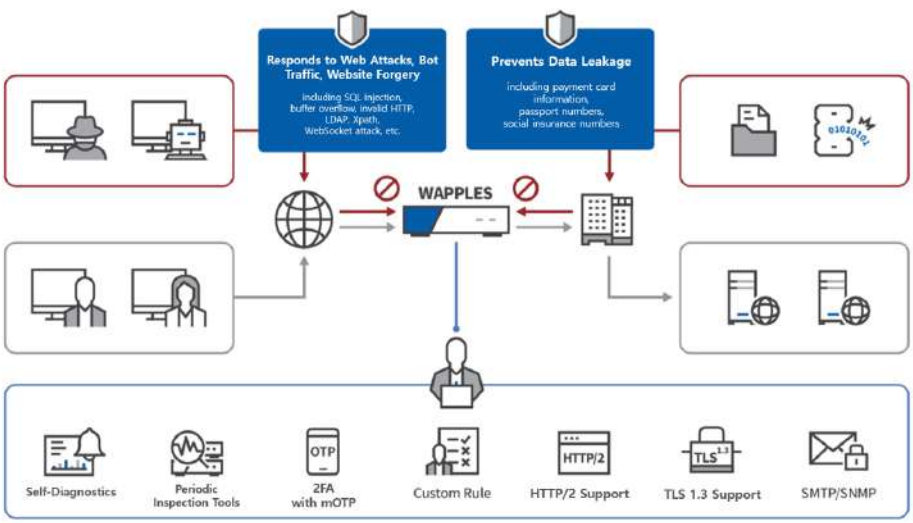
Why WAPPLES?

WAPPLES, the Intelligent WAF

WAPPLES is a web application firewall (WAF) equipped with an intelligent logic-based detection engine built on machine learning technology. Designed and built with the fundamentals of web application security in mind, WAPPLES is not only effective against all the common web attacks, but also plays a key role in preventing data leakage, unauthorized access, and website forgery, all of which are growing threats to organizations today. Using the intelligent detection engine, it is also able to respond to new attacks launched by advanced persistent threats (APT).

WAF users often complain about having false positives because the security administrator in charge would have to manually go through the false positives and add them as exceptions to the security policies. On the other hand, WAPPLES' low false positive rate saves a lot of time and resources in management.

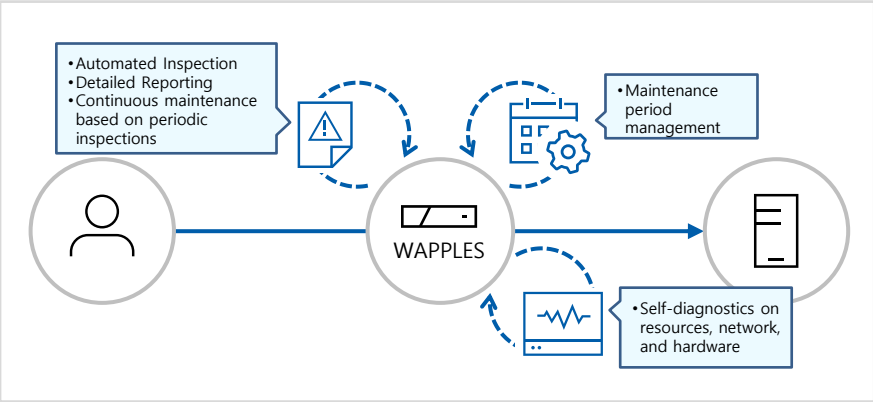
WAPPLES' COCEP™ detection engine is developed in-house by Penta Security. Machine learning technology is applied not only to enhance its detection capability, but also to provide additional benefits like self-diagnostics and threat reports. WAPPLES blocks unknown and zero-day attacks, guarantees a low false positive rate through accurate detection, and allows for easy and convenient management. With defined rules and custom rules, WAPPLES protects the server from web attacks by analyzing and detecting by attack type. Since WAPPLES' detection mechanism is based on grasping the characteristics of the attack itself, false positives rarely occur.



Why WAPPLES?

• Real-Time Self-Diagnostics and Periodic Inspection

Maintenance is crucial for WAFs. In terms of application-type WAFs, most vendors perform periodic inspections by having site visits monthly, quarterly, or semi-annually, looking for system abnormalities such as CPU overload. However, even the most outstanding engineers make errors, and the inspection results would be influenced by the engineers' judgments. There had been incidents where the admin passwords were shared via P2P by mistake. Even a small mistake can pose tremendous threats to security, hence it would be better to reduce the need for human management while maintaining performance levels.



WAPPLES is capable of **real-time self-diagnostics** based on machine learning. By doing so, it checks for issues like traffic overload, CPU/memory overload, and insufficient DB capacity. Administrators can set desired thresholds and receive warnings when thresholds are exceeded. In addition, WAPPLES conducts machine learning analysis on its operation log data to determine the presence of abnormalities and prevent problems in advance.

WAPPLES is also capable of **automated maintenance** through periodic inspection tools. Every time an engineer performs inspection, a report is generated by analyzing the detection and audit logs as well as data from real-time self-diagnostics. Inspection results that were verbally explained by engineers in the past are now summed up in detailed automated reports, allowing administrators to gain an objective overview on the status of the WAF.

WAPPLES also automatically handles maintenance period management by providing a maintenance service alarm function, reducing the burden of administrators.

Why WAPPLES?

Case Study of WAPPLES

- **Japanese online shopping platform A Mall**

  Founded in the early 1990s, A Mall is a retail giant that operates shopping centers across Japan. At the time, A Mall's security infrastructure for its online shopping platform was outdated and ineffective, forcing the company to pay heavy maintenance costs.

  Web attacks targeting A Mall's website were increasing. Eventually, the website was paralyzed due to a DDoS attack, halting all services. After a security vulnerability scan, it found that its web server structure was altered due to a cross site scripting (XSS) attack on its website. The hackers stole sensitive personal data after gaining unauthorized access to the server.

  After adopting WAPPLES, A Mall was able to cut their security maintenance costs by half, and it had since then never fell victim to any web attacks such as DDoS or XXS. By safeguarding sensitive personal data, WAPPLES also helped A Mall comply with PCI-DSS.

As an industry-first, Penta Security's WAPPLES provides remote technical maintenance services and tools such as self-diagnostics, periodic inspection tools, and Tech 365 remote tech support. Through self-diagnostics, WAPPLES recognizes problems that occur during operation and solve them on their own while transmitting the information to the administrator in real-time, minimizing the need for any direct site visits. In addition, Tech 365, which operates 24 hours a day, 365 days a year, ensures stable service even in situations where face-to-face technical support is difficult.

As COVID-19 brings traditional offices into remote environments, remote tech support for security appliances becomes crucial. This makes WAPPLES a perfect solution for organizations with remote office settings. Indeed, WAPPLES received twice the number of orders from the public and educational sectors in 2020 as compared to 2019.

Conclusion

To prepare for the growing threats on web applications, adopting an intelligent WAF based on machine learning technology is required.

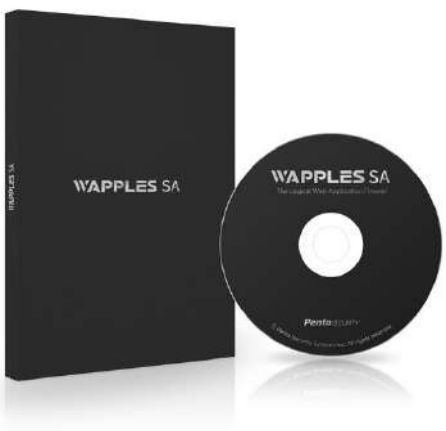
1. WAPPLES is an intelligent WAF run on a logic-based detection engine built on machine learning technology.

2. WAPPLES is a 4-in-1 web application solution that not only detects and blocks web attacks, but also prevents data leakage, unauthorized access, and website forgery.

3. WAPPLES has received CC certification and GS certification.

4. WAPPLES offers robust security with outstanding detection accuracy.

5. WAPPLES keeps itself at a constant state of perfection through real-time self-diagnostics and automated periodic inspection, all enabled by machine learning.



About Penta Security Systems Inc.

Penta Security is a leader in web, IoT, and data security solutions and services.

Since its establishment in 1997, Penta Security's cybersecurity mission was based on the ideology of openness built by trust. Instead of blocking and restricting sharing, Penta Security develops security technologies to enhance openness by securing the sharing process. To this end, it has been conducting R&D for more than 20 years based on encryption technology, which lies at the core of cybersecurity today.

Penta Security's three core product lines – data security, web security, and authentication – have become essential security elements to protect the valuable information of millions of people around the world. Today, Penta Security is considered a global leader on the cybersecurity stage.

For inquiries on WAPPLES – the No. 1 WAF in Asia-Pacific, visit pentasecurity.com/wapples or email globalbiz@pentasecurity.com

Keywords

#Web Application Firewalls #WAPPLES #WAF #OWASP #Machine Learning #URL #Encryption #CC Certification #Load Balancing #Sticky Session #SQL Injection #Self-diagnostics #Periodic Inspection

Penta SECURITY
TRUST FOR AN OPEN SOCIETY

Penta Security Systems Inc.

20th Floor, Eusu Holdings Building
25 Gukjegeumyoung-ro 2-gil
Yeongdeungpo-gu, Seoul, Korea
Tel. 82-2-780-7728 Fax. 82-2-786-5281