Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2024, 11(4):358-365**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Developing Comprehensive Web Application Firewall (WAF) Policies for Multiple Environments, Enhancing Web Application Security

Mohammed Mustafa Khan

Abstract: Web servers are the engines that drive web applications. Web applications are the critical elements in an organization that need maximum security protection to secure workloads. Therefore, a web application firewall (WAF) is deployed to guard the web server from a plethora of attack vectors, including all the OWASP's top 10 common attacks. WAF focuses on the application layer, which is the seventh layer of the OSI (Open System Interconnection) model, due to the application layer's inherent features, which give the WAF a conducive environment in which to operate. The superiority of WAF in inspecting and blocking HTTP traffic depends on the configuration of comprehensive policy rules. Access controls are employed via Access Control Lists (ACLs) that contain rules or a group of rules that allow or deny the traffic from percolating into or out of the web server. The iptables userspace application is utilized; it queues the packets at the kernel layer and provides packet direction to pass through the WAF first before entering the webserver. At the kernel level, packets are inspected, and the decision-making process is performed; packets devoid of malicious intent are sent to the user level, whereby the webserver is operating, whereas the suspicious packets are blocked. The WAF can compare the ACL against the incoming HTTP packets from the traffic prior to reaching the webserver. The system administrator writes the policy rules and configures them via the test editor or text area space provided. The inbuilt algorithms from the WAF contain regular expressions that compare the packet payload by simply checking the pattern. The test results demonstrate the precision and accuracy of the Web Application Firewall in identifying and blocking various attacks, aligning with the OWASP top 10 web application attacks. The paper proposes the development of comprehensive web application firewall policies tailored for multiple environments, such as on-premise, cloud, and hybrid environments, ensuring powerful security across different deployment scenarios. This study aims to enhance the overall security landscape of web servers that host web applications.

Keywords: Web applications, Web application firewall policies, access control list

1. Introduction

Background

Businesses and the internet utilize web servers as their assets to generate and store information. They store diverse types of data such as images, files, web pages, videos, and any type of information the client requests on demand. A web application Firewall (WAF) is a software, appliance, or service that acts as the gatekeeper to monitor, filter, and block the HTTP traffic to and from the web service. WAF protects the web application from common web-based attacks such as SQL injection, cross-site scripting, DDoS, cookie manipulation, file inclusion, bot attacks, and all the attacks included in the OWASP top ten. It helps to reduce or protect the attack surface in the application security ecosystem [1]. WAFs have the capability of protecting web applications because they apply a set of security policy rules on HTTP traffic generated and received by web applications.

The policy rules are the core principle that aids the WAF in offering superior protection when the policies are appropriately defined and properly written. With the complex nature of web applications and the evolving sophistication of application layer attacks, configuring the rules and management of WAF can be a tedious task, and errors can occur during the process.

Problem Statement

The creation of effective WAF policies that cover different environments is challenging since there is a disparity in security requirements and operational context for various web applications. The underlying WAF solutions are not flexible and dynamic enough to address the aforementioned challenges appropriately. This study aims to develop a framework that creates effective WAF policies that optimize security across different environments.

Research Objectives

The objectives of this paper include:

• To provide a review of the current state of WAF technology and policy development in different environments.

• To analyze and present strategies for developing, implementing, and managing WAF policies that are effective across diverse IT environments.

• To explore emerging trends and future directions in WAF technology that promise to enhance web application security in increasingly complex infrastructures.

The format of this paper is structured to include a comprehensive literature review that expounds on the evolution of web application security, WAF technology, and challenges of deployment in different environments. Additionally, the paper trickles down into an overview of WAFs and their constituents. The core of the paper aims to develop WAF policies for different environments, key features, process of implementation, and policy management best practices. It is imperative to provide a holistic view of developing and managing WAF policy in different environments.

2. Literature Review

The related work focuses on the evolution of web application firewalls, the importance of WAF in web application security, and the development of web application firewall policy. The emergence of Web application firewalls as a promising technology was documented in the early 2000s. George et al. 2021 were curious and wanted to get the overall overview of the evolution of WAF technology. The authors proposed a study to identify the major components and functionalities of WAF technology. Their work not only revealed the key components and functionalities of the new hero, which is WAF technology but also revealed the significance of WAF technology in combating application-layer attacks. There was a fundamental need to establish WAF as a core asset in strategizing web application security.

Some studies have mirrored the importance of WAFs in enhancing web application security. According to Aliero et al. (2020), WAFs act as the first line of defense against common web-based attacks. The authors put a lot of emphasis on the need to design WAF policies that are dynamic and can adapt to various environments. Research by Shaheed et al. (2022) proposed that incorporating machine learning techniques can optimize WAF efficacy via adaptive learning and real-time threat monitoring and detection.

Studies on WAF policy development geared towards the establishment of superior defined rules that can be customized and refined to suit business requirements. Applebaum et al. (2021) performed a study on signature-based and machine-learning-based WAF. The study demonstrated how a set of rules can be maximized to improve the security of WAF and similarly reduce false positives. Their findings indicated the need for adaptable policy management mechanisms to support different deployment environments.

3. Understanding WAF

Definition and Purpose

WAF can be a software or appliance that is designed to guard web applications from different types of common attacks, as listed in the OWASP top ten. It is accepted truth that traditional network firewalls operate on the network and transport layers. The application layer was left unprotected; thus, WAF was established to protect the application layer. The ultimate function of WAF is to inspect HTTP/HTTPS traffic that percolates in and out of the web applications and identify and block malicious requests prior to reaching the web server [1]. WAFs act

as a line of defense in protecting the web server from common web-based attacks such as SQL injection, local file inclusion, and cross-site scripting, to mention a few.

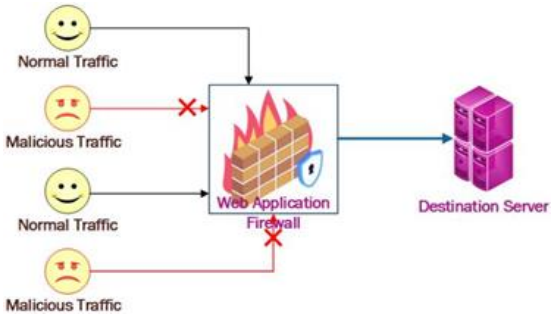


Figure Showing Positioning and working of WAF.

Key Features of WAFs

• **Protocol Validation:** Ensures that incoming traffic conforms to HTTP/HTTPS specifications [1].

• **Data loss prevention:** Provides protection against data leakage and generates alerts that help to shield data from unauthorized access, use, or modifications.

• **Automated attack prevention.** The built-in automated tools block malicious traffic from accessing the web applications.

• **Input protection:** the filtering capabilities of the WAF scrutinize all the user inputs and allow only valid user inputs to access the network.

• **Customizable set of rules**: WAFs provide a custom set of rules that allow businesses to align their security policies to meet their specific needs and risk profile [1].

Deployment Models of WAF

• **Network-based WAF:** A hardware appliance installed on-premises, typically in front of web servers [2].

• **Host-based WAF:** Software installed directly on the web server, offering protection at the application level.

• **Cloud-based WAF**: A service provided by cloud security vendors, often delivered as a reverse proxy.

Web Service Architecture

Crafting the idea of how the web service architecture works and understanding its interactions with the web applications is crucial when developing web application firewall policies. The web service architecture consists of the server side and the client side. The client requests services from the server. The server stores some images, files, and videos and also hosts web applications [6]. Knowledge of web service architecture is essential when developing web application firewall policies because it helps develop effective, efficient, and comprehensive WAF policies that enhance security without hindering the functionality and performance of web applications. Additionally, it will help position the load balancer to balance performance efficiently.

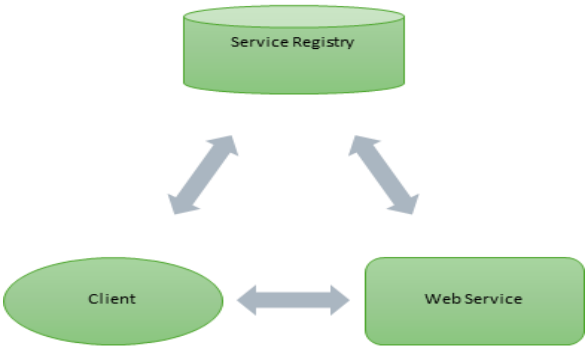


Diagram Showing Web Service Architecture

4. Understanding The Threat Landscape

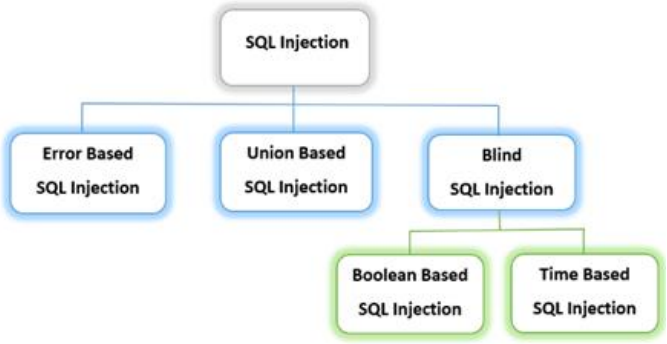
There are different types of web attacks that institutions face today [1]. It is a combination of all known and unknown cyber threats that can influence the web application. Cybercriminals have launched their attacks

mostly on web infrastructures since most businesses use web applications to support their workflow operations. The threat landscape is ever-evolving, and advanced attacks are constantly being launched. The OWASP foundation ranked the top 10 attacks that intend to attack web applications, APIs, and websites. The OWASP top 10 that are relevant to this discussion are discussed below. It is crucial to comprehend the threat landscape for the proper development of web application firewall policies for different environments, including on-premise, cloud-based, and hybrid. WAF provides a solution for each of the attacks discussed below.

Figure Showing Different Types of Web Attacks

SQL injection

A type of common web attack that involves inserting malicious SQL statements into a web application's input fields. The malicious SQL statement grants the attacker access to the web application, and the attacker begins to manipulate the application's database [5]. This can lead to unauthorized access to sensitive data, data modification, or even complete control over the database. Most of the legacy applications succumb to this kind of attack. The WAF can be used to protect legacy applications since it can inspect the HTTP/S request, detect the patterns used, deny the request, and eventually ban the IP address of the sender by whitelisting or blacklisting. Overall, WAF has SQL injection defenses that detect any SQL injection attempts into web applications.



Flowchart Showing Types of SQL Injection Attacks

Cross-Site Scripting (XSS)

This is a web security vulnerability that enables an attacker to inject malicious scripts into web pages viewed by users. XSS attacks happen when an attacker utilizes a web application to deliver malicious code through a browser-side script to another web user. An attacker utilizes XSS to send a script with malicious intent to another user without the user even noticing it is from an untrusted source since the browser itself can not even fathom if the script is from a legitimate source with no bad intention [5]. Browsers have a tendency to store user data. The script will inspect all the cookies, sensitive information, and session tokens and send them back to the attacker. Some scripts are superior and can rewrite the HTML page content. The two major categories of XSS attacks are reflected XSS attacks and stored XSS attacks. Additionally, blind XSS is one of the known site-site scripting attacks. WAF prevents this attack by analyzing the malicious script and blocks any requests before the script is executed.

Broken Access Control

Legitimate users have permissions on the scope of what they are supposed to access. Access control implements a policy that restricts authenticated users on the actions they can perform. When access control fails to enforce a policy that restricts unauthorized users from accessing sensitive data or performing actions such as modification data deletion, which is beyond their scope, it can be fatal since it will deny other authenticated users from accessing the data [5]. WAF can prevent this type of attack by just enforcing the rate limit throttling and employing the principle of least privilege, among others.

Cross-Site Request Forgery (CSRF)

Type of XSS vulnerability that allows an attacker to assume the identity trust underlying between the web application and user by coercing a user to access the page containing malice intent, whereas the CSFR performs exploitation of trust between the web application and user by obliging the browser of the victims to produce requests the vulnerable application thinks are authentic requests from the victim. Once the attacker is granted access to a web application, they capitalize on the vulnerability by carrying out data breach actions and unauthorized money transfers [10]. The WAF features, such as input validation, can be used to prevent these attacks since it sanitizes and validates all the input data from the client slide and decides to allow or deny depending on the nature of the inspection.

Vulnerabilities in third-party Components

Refer to security flaws in software libraries used by Apache web servers, frameworks such as WordPress plugins, modules, or other components developed by external entities that are incorporated into a web application [5]. These third-party components are widely used to save development time, add functionality, and improve efficiency. Despite having various benefits, the third-party components are hobbled by security challenges if not well managed. This system needs to be regularly updated. It is a common phenomenon when updating any system that can allow malicious patches to execute. WAF inspects all the downloaded updates and ensures they are secure before executing them.

5. Developing Waf Policies for Multiple Environments

The different environments include:

6. On-Premise Waf Policies

On-premise web application policies are applied on hardware or virtual machines that are deployed on the corporate site or in an organization [7]. The organization has complete control of the infrastructure and is responsible for creating superior configuration policies. The policies developed must be able to cover internal and external threats. The policies can be customized to fit the specific needs of the organization. Most organizations have web servers that run web applications deployed on their premises, or they host them at the data centers. The system administrator is responsible for creating some policies and configuring the policies that appropriately help to protect the vital IT assets of the organization.

Types of Policies

Access Control: Access to the WAF management interface and web application can be restricted by the use of IP whitelisting, role-based access control, and multifactor authentication. The system administrator can create a whitelisting policy that rejects all the requests and only allows the requests that are known and devoid of malicious intent. Whitelisting contains an inventory of familiar IP addresses that are secure and match the new incoming IP addresses. When no match is found in the inventory, it blocks the new IP address and generates an alert. Whitelisting is commonly used policy than blacklisting because it utilizes few computing resources. Role-

based access control grants only specific IP requests to a particular web application. The system administrator needs to manually configure this feature in the WAF. Multifactor authentication policy must be configured to prompt the user to provide additional verification factors to access the web applications.

Intrusion detection and prevention: It is a tremendous aspect to create rules that detect and block common web attacks, such as SQL injection file inclusion, to mention a few. Anomaly detection can be utilized to find out unusual traffic patterns. Inspecting the behavior analysis of network traffic helps to detect strange patterns. Isolation of these anomalies takes place, followed by immediate destruction of these traffic.

API rate limiting and throttling: Rate limiting and throttling provide a system administrator with capabilities to set certain permissions to determine if certain API calls are valid or invalid. Rate limiting allows the request to pass through until a certain threshold is reached at a given period of time. The threshold factors to be used entail the size of the payload, the number of requests, and the type of content accessed. The throttle demonstrates a temporary state and is used to control the amount of data accessed by clients via an API. When the limit is exceeded, the policy implemented automatically blocks the process.

7. Cloud Waf Policies

As companies begin to move their applications and data to the cloud, the traditional approaches to building and protecting applications are becoming obsolete. The cloud web application firewall is managed by a third-party provider of the organizational preference [7]. Some of the cloud providers in the market include Amazon Web Services, Azure, IBM Clouds, Nutanix Clouds, Oracle Cloud, and Google Cloud Platform, to mention a few. The cloud providers implement policies using the evolved cloud-native security features. The company does not need to worry about the security policy configuration since the cloud providers have security engineers who will manage all the security aspects on their behalf. Security engineers coordinate with the system administrators to learn the specific business rules of the organization and develop WAF policies that align with the business requirements. As long as the security license is valid, the WAF policy will always protect the web applications.

Types Of Policies

Application layer DDoS protection: The type of attack that targets the whole Web Application Firewall aiming at particular vulnerabilities. This attack renders the application useless to legitimate users and, thus, makes it impossible to access the requested content. The specific applications from the web server will be unavailable, triggering error 404, which simply means the file is not found. This is detrimental since it slows the productivity level of the clients. Nonetheless, this kind of attack can be prevented by implementing permissions that support the flow telemetry analysis that utilizes the behavioral analysis to detect abnormalities and attacks.

Compliance and data protection: The use, sharing, and storage of personal data must be protected against malicious intentions. Data regulation permissions must be properly implemented. The adoption of technology to support various in-service deliveries, such as an online business that accepts online payments and electronic medical devices that support patient intervention, is rapidly growing. Standards such as the Health Insurance Portability and Accountability Act (HIPAA) that protects patient data, the Payment Card Industry Data Security Standard (PCI-DSS) that ensures online payment safety, and the General Data Protection Regulatory) GDPR sets rules for the collection and processing of personal information, specifically among the European member states, and WAF policies must be compliant. Encryption techniques must be implemented to protect stored data, as well as data in use and transit.

API security: When the company wants to access the web applications hosted in the cloud, you might be wondering how the company now accesses its web applications and workloads. API is the mechanism that enables the interaction to occur. Cybercriminals have targets to spoof the API and try to gain access to the web applications. It is essential to create superior rules that REST API security will use to countermeasure common web-based attacks.

8. Hybrid WAF Policies

Hybrid environments have become a fundamental aspect of institutions. It combines on-premise and cloud resources. The hybrid environment requires policies that ensure seamless security across the on-premise and cloud platforms. This involves maintaining consistency in WAF rules, addressing data transfer security between

on-premise and cloud components, and using hybrid security tools that can manage the two environments cohesively [7].

Types of Policies

Disaster recovery and business continuity: Fatal incidents occur and disrupt business functions. When catastrophes occur, failover operations and redundancy between the on-premise and cloud environments must be performed. The normal functions of business are made available, and continuity proceeds. It is crucial to implement failure over security policy prior to the occurrence since cybercriminals have learned during such transition the security aspects of businesses can be easily jeopardized.

Unified policy management: These are consistent WAF policies that are developed across on-premise and cloud environments to maintain a unified security landscape. It is vital to standardize these policies to ensure organizations remain protected against common web attacks irrespective of the locations. The central management console for the deployment and management of these policies boosts the security aspects since critical incidents that require immediate attention are displayed in a single point of control that is easy to view and simplifies the administration. Centralizing the administration activities enables faster monitoring of the application of updates on demand and ensures compliance with existing regulatory bodies such as HIPAA, GDPR, and PCC-DSS. This also positions the institution in front of cyber threats before they manifest, thus enhancing the overall security of web applications.

9. Future Trends In WAF

Web application firewalls are holding a promising future for institutions pertaining to security enhancement and optimization. We have seen WAF's capabilities in the protection of web applications. Going forward, it is important to integrate WAF with other security tools and infrastructure, such as Security Information and Event Management (SIEM), to develop a comprehensive security strategy that is proactive to cyber defense [8]. The integration of SIEM will foster real-time threat detection and response. WAF policies should be aligned with SIEM to streamline incident management, minimize the risk of data breaches, and enhance visibility. Additionally, integration enables automated workflows and enforces security policies across different environments, including on-premise, cloud, and hybrid.

10. Conclusion

Developing comprehensive WAF policies tailored to cloud, on-premises, and hybrid environments is critical for enhancing web application security. By understanding the unique needs of each environment, crafting targeted security policies, and continuously testing and improving these policies, you can effectively protect your web applications from a wide range of cyber threats. Regular updates and a proactive security stance will ensure that your web application remains secure as the threat landscape becomes more superior and more severe.

References

[1]. Dawadi, B. R., Adhikari, B., & Srivastava, D. K. (2023). Deep Learning Technique-Enabled Web Application Firewall for the Detection of Web Attacks. Sensors, 23(4), 2073. https://doi.org/10.3390/s23042073.

[2]. Siramdasu, M. K. (2023, July 25). Web Application Firewall (WAF) - Explained. Teamwin Global Technologica Pvt Ltd. https://teamwin.in/index.php/2023/07/25/web-application-firewall-waf-explained/

[3]. Applebaum, S., Gaber, T., & Ahmed, A. (2021). Signature-based and machine-learning-based web application firewalls: a short survey. Procedia Computer Science, 189, 359-367.

[4]. GEORGE, D. A. S., & GEORGE, A. H. (2021). A Brief Study on The Evolution of Next Generation Firewall and Web Application Firewall. Ijarcce: international Journal of Advanced Research in Computer and Communication Engineering, 10 (5), 31–37.

[5]. OWASP. (2021). A06 Vulnerable and Outdated Components - OWASP Top 10:2021. Owasp.org. https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

[6]. Dang, D., Chen, C., Li, H., Yan, R., Guo, Z., & Wang, X. (2021). Deep knowledge-aware framework for web service recommendation. The Journal of Supercomputing, 77(12), 14280-14304.

[7]. Gorantla, V. A. K., Gude, V., Sriramulugari, S. K., Yuvaraj, N., & Yadav, P. (2024, March). Utilizing hybrid cloud strategies to enhance data storage and security in e-commerce applications. In 2024 2nd International Conference on Disruptive Technologies (ICDT) (pp. 494-499). IEEE.

[8]. Rahmawati, T., Shiddiq, R. W., Sumpena, M. R., Setiawan, S., Karna, N., & Hertiana, S. N. (2023, November). Web Application Firewall Using Proxy and Security Information and Event Management (SIEM) for OWASP Cyber Attack Detection. In 2023 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS) (pp. 280-285). IEEE.

[9]. Shaheed, A., & Kurdy, M. B. (2022). Web application firewall using machine learning and features engineering. Security and Communication Networks, 2022(1), 5280158.

[10]. Aliero, M. S., Shamaki, B. I., KALGO, B. S., & Bello, A. A. M. (2020). WEB APPLICATION FIREWALL. International Journal Of All Research Writings, 3(4), 26-43.