DOI: 10.2507/35th.daaam.proceedings.xxx

WEB APPLICATION FIREWALLS (WAFS) IN PROTECTING SOFTWARE

Ivana Bilić, Karlo Josic*, Drazen Pranic & Sanja Ribaric

This Publication has to be referred as: Bilic, I[vana]; Josic, K[arlo], Pranic [D]razen & Ribaric, S[anja] (2024). Web Application Firewalls (WAFs) in Protecting Software, Proceedings of the 35th DAAAM International Symposium, pp.xxxx-xxxx, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-xx-x, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/35th.daaam.proceedings.xxx

Abstract

Web Application Firewalls (WAFs) are vital in safeguarding web applications by inspecting and managing HTTP traffic between the application and the Internet, adhering to the principles of the CIA (Confidentiality, Integrity, Availability) triangle. This paper explores the function of WAFs in enhancing security through strict traffic filtering based on pre-defined rules. It also highlights the importance of balancing application security and performance to prevent potential slowdowns due to extensive security checks. The paper's topic extends to the likely consequences of imprecise rules, which could block legitimate requests, reducing user satisfaction and possible loss of clientele.

Keywords: Web Application Firewall (WAF); security policies; OWASP; traffic filtering; cybersecurity.

1. Introduction

The globalisation of the market and technological advancements have encouraged the adaptation of software development to enable web applications to scale a large volume of requests. The transition from monolithic applications to microservices, which communicate through diverse networks, has significantly evolved. To safeguard data and users, these microservices must adhere to the principles of confidentiality, integrity, and availability (CIA). Achieving this requires transforming and scaling up security measures and application development. Given the alarming rate of nearly 4000 cyberattacks daily worldwide, the frequency of such incidents serves as a crucial metric, offering insights into the extent and prevalence of cyber threats organisations face [1]. Continuous awareness among software developers and security experts is essential, as they must remain on track with emerging vulnerabilities and consistently assess their assets to integrate the most effective tools for protection.

The Open Web Application Security Project (OWASP), the organisation that annually publishes the "OWASP Top 10," recommends [2] the adoption of web security firewalls as one of the best practices to mitigate security risks. Integration of Web Application Firewalls involves configuring them as reverse proxies, where they intercept each incoming request and assess it against a predefined set of rules to determine the presence of malicious content. While this enhances the system's security, it does come at the expense of potentially slowing down the application response. Also, admins of Web Application Firewall's rules need to be careful. If the rules aren't precise, the system might classify false negatives, leading to losing customers.

2. Security challenges in software protection

Applications and APIs have become increasingly critical to business success [3]. Employees, partners, providers, customers, and other users rely on various applications to communicate, collaborate, and transact business. APIs have exploded recently as organisations power mobile applications, the Internet of Things (IoT), internal applications, partner applications, and cloud-based customer services.

The more organisations rely on applications and APIs, the more attractive these digital assets are to attackers. Hackers today use automated bots to crawl websites at random, looking for vulnerabilities in applications they can use to access a database, load malicious files onto a web server, or take down a server with an overwhelming amount of traffic [4].

To effectively mitigate risks, it is essential to begin by identifying the assets that require safeguarding. This entails a comprehensive recognition and classification of the organisation's critical components. Following asset identification, the next crucial step involves pinpointing potential risks that could compromise the security and functionality of these assets. The MATA model then comes into play, providing a structured approach to risk management. This model involves Mitigating risks by implementing preventative measures, accepting certain risks, transferring risk responsibility through mechanisms like insurance or outsourcing, and avoiding risks by eliminating or redesigning processes. In tandem with this risk management model, the Open Web Application Security Project (OWASP) is a valuable resource, particularly in web applications.

A Security Information and Event Management (SIEM) system is instrumental in addressing security challenges within software protection. SIEM enables real-time detection of suspicious behaviour and unauthorised access attempts by continuously monitoring events and activities across the software infrastructure, mitigating potential security threats. SIEM provides insights into vulnerabilities, unauthorised changes, and other security issues by aggregating and correlating log data from various sources within the software environment. Leveraging advanced analytics and threat intelligence, SIEM identifies patterns indicative of malware infections, insider attacks, and other threats, triggering automated responses or alerting security personnel for further investigation and remediation. Additionally, SIEM facilitates compliance monitoring by ensuring adherence to security policies, standards, and regulations and supports incident investigation and forensic analysis in case of a security breach involving software assets. Through integration with other security controls and technologies, such as intrusion detection/prevention systems and antivirus solutions, SIEM offers a centralised approach to security management, enhancing overall protection against emerging threats and bolstering software security measures [5].

One of the most famous projects is OWASP Top 10, a list of the top 10 security risks web applications face, which uses the SIEM tools approach. The OWASP Top 10 Security Risks for 2023 are:

- Injection Attacks
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfigurations
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring logging and monitoring [6].

Creating a secure environment for web applications is paramount, whether the application is hosted on-premises or in the cloud. Various tools play a crucial role in adding an extra layer of protection to mitigate potential threats and vulnerabilities.

3. Concept of Web Application Firewall (WAF)

A Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between them and the Internet. It operates at layer 7 (the OSI model) and protects web applications from attacks such as forgery, cross-site scripting (XSS), file inclusion, and SQL injection [7].

Deploying a Web Application Firewall before a Web application creates a shield between it and the Internet. A web application firewall is a reverse proxy that acts as a single entry point for external systems to access resources on private subnets. Web Application Firewalls can run as a network appliance, server plugin, or cloud service. Advanced Web Application Firewalls allow analysts, security experts, and other users to define advanced rules with granular customisation options [8].

WAF is equipped with robust security features such as access control, content filtering, and virtual patching, helping to minimise security vulnerabilities and ensure compliance with industry standards and best practices. Organisations can customise security policies and rule sets within WAF configurations to meet specific security requirements, effectively combating emerging threats and adapting to evolving attack strategies. Additionally, WAFs often include logging and reporting functions, empowering security teams to monitor and analyse web traffic, identify security breaches, and conduct thorough investigations as needed. WAF plays a crucial role in proactively preventing threats, managing access control with precision, and providing comprehensive visibility into web application traffic, thereby significantly enhancing the security posture of web applications and protecting sensitive data and critical assets from cyber threats.

3.1. Web Application Firewall Rules

Web application firewall rules define how to inspect HTTP/HTTPS web traffic (requests) to an application, where and what parameters and conditions to look for in the request, and what action the WAF should take when a request matches those definitions.

WAF comes with predefined rules. Vendors often include a database with known signatures of malicious software and IP addresses. Advanced Web Application Firewalls allow analysts, security experts, and other users to define advanced rules with granular customisation options to improve their applications' security and performance and reduce network load on application servers.

Some examples of custom rules in WAF:

- Block access to specific sections of a website based on IP address or Headers,
- Prevent search engine bots from accessing a website,
- Redirect traffic to a maintenance page,
- Add header to specific requests,
- Change the value of a header to another value.

Conditions, actions, priorities, and descriptions can be defined for each rule. The conditions describe the request; they define desired or unwanted requests. The action is triggered when the request meets the condition. Priorities exist to initiate the correct action if a request meets multiple conditions.

3.2. WAFs deployment types

Software-based WAFs run as any other service in the system. They can run in a Docker container, which will intercept user requests. Software-based WAFs are easy to maintain, upgrade, and scale, especially in Kubernetes/OpenShift platforms. Containers/pods can be configured to scale based on traffic, which can prevent latency. The load balancer in OpenShift will automatically create another pod based on the amount of memory used or processing time.

Cloud-hosted WAFs are WAFs that are hosted and managed by a third-party provider. They inspect incoming traffic to a web application and block any traffic that does not meet the configured security rules. Cloud-hosted WAFs are typically deployed as a service, with the WAF provider managing the hardware and software infrastructure required to run the WAF.

A hardware-based WAF (commonly referred to as network-based WAF) is installed locally on a network. These are often the most expensive WAFs, requiring maintenance and storage space. Their primary purpose is to minimise latency. Hardware-based WAFs are commonly leveraged by large organisations with the budget and headcount to manage on-premises appliance and IT infrastructure [9].

3.3. Pros and cons

A Web Application Firewall (WAF) acts as a security layer for your application by scanning and filtering all incoming traffic. It effectively manages requests by applying rules to allow or block specific content. Additionally, a WAF is a preventive measure against various threats, including DDoS attacks, injection attacks, and cross-site scripting (XSS).

Using a WAF also has some disadvantages. First, a WAF can introduce latency and overhead to the HTTP traffic, as it must process and analyse each request and response. It can also affect the functionality and usability of the web application, as it may block some legitimate traffic or trigger some false positives. Second, a WAF can be bypassed or evaded by sophisticated attacks, such as obfuscation, encryption, fragmentation, and zero-day attacks. It can also be vulnerable to attacks like brute force, flooding, or poisoning. Third, a WAF can be costly and complex to deploy and maintain, requiring specialised hardware, software, or services. It also requires constant monitoring, tuning, and updating to keep up with the web application changes and security requirements.

4. Web Application Firewalls Case study

Table 1 examines the top 10 implementations of WAFs for case study research. This was based on the diverse array of solutions tailored to meet the varied security needs of organisations across different industries and sizes.

Solution	Company size	Options	Integration with
Akamai	all (with limitations)	Bot mitigation API security Layer 7 DDoS protection DevOps integration	Existing systems
AWS	medium to large	Protection from common threats like web exploits and bots Monitoring, filtering, and rate-limiting capabilities	AWS services and infrastructure
Barracuda networks	medium to large	Reliable traffic inspection Filtering of network traffic Outbound network scanning	Existing security infrastructure
Cloudflare	all (with limitations)	Integration with CDN and global network Instant access to Cloudflare's global network	Cloudflare's CDN and global network
F5	small	Spam protection Implementation of SMTP and FTP protocol checks	Existing systems and protocols
Fastly	medium	Next-gen WAF with adaptive protection against advanced threats DDoS protection and TLS encryption	Existing infrastructure and applications
Fortinet	medium to large	Machine learning for accurate protection against DDoS attacks and common threats Comprehensive visibility and support for intelligent threat identification	Machine learning
Imperva	all (with limitations)	Application security across all cloud environments (SaaS, PaaS, IaaS) Fast setup and automated protection	Existing security stacks and workflows
NetScaler	medium to large	Bot mitigation API protection Advanced security features Integration with existing security stacks	Existing security infrastructure and protocols
Sucuri	small to medium	Robust protection against threats SSL certificate creation High-performance caching Access to the Sucuri WAF network	Various environments and platforms

Table 1. Case study of WAF implementations

From industry giants like Akamai and AWS to specialised providers such as Barracuda Networks and Sucuri, each WAF solution brings unique features and strengths. Businesses have many options, whether robust protection against common threats, seamless integration with existing systems, or specialised functionalities like bot mitigation and API security. As cybersecurity threats continue to evolve, the importance of implementing effective WAF solutions cannot be overstated. By carefully evaluating their requirements and selecting the most suitable WAF provider, organisations can bolster their defences, safeguard their web applications, and protect sensitive data from cyber threats in an increasingly digital world.

5. Future Security challenges and research

If "Zero Day Charlie" were to exploit vulnerabilities in an application that traditional Web Application Firewalls (WAFs) were unaware of, it could lead to a zero-day attack. In this scenario, Zero Day Charlie would capitalise on security flaws or weaknesses within the application that developers or the security community have not yet identified or patched. Since traditional WAFs rely on established patterns and signatures for threat detection, they likely prove ineffective against zero-day exploits.

The ramifications of a zero-day attack are severe, granting attackers the ability to infiltrate systems and exfiltrate sensitive data without detection. Organisations may need robust defences to detect and respond to zero-day attacks, such as sophisticated threat detection mechanisms and real-time monitoring. Furthermore, zero-day attacks present a significant challenge for security teams, necessitating rapid response and mitigation strategies to mitigate the impact on affected systems and prevent further exploitation. Well-known examples are NotPetya and Stuxnet, which have multiple zero-day vulnerabilities in their code [10].

To mitigate the risk of zero-day attacks, organisations must adopt a multi-layered security approach that includes proactive threat intelligence, comprehensive vulnerability management, and advanced security solutions capable of detecting abnormal behaviour and unidentified threats. Additionally, staying informed about emerging security threats and promptly updating systems and software are crucial to reducing vulnerability to zero-day exploits. By implementing these measures, organisations can bolster their defences and minimise the potential impact of zero-day attacks on their systems and data.

A next-generation firewall is designed to address advanced security threats at the application level through intelligent, context-aware security features. Next-generation firewall specifications vary by provider, but they generally include some combination of the following features:

- Deep-packet inspection, which inspects the data contained in packets on layer 7 of the OSI model.
- Intrusion Prevention System (IPS) monitors the network for malicious activity and blocks it where it occurs. Monitoring can be conducted based on malware signatures, or the request can be processed in sandboxes. Sandbox environments are isolated environments that exist to test potential malicious programs.
- External threat intelligence, or communication with a threat intelligence network to ensure that threat information is current and help identify bad actors.
- High performance, which can handle and scale large amounts of network traffic.

Firewall as a Service (FWaaS) represents a cloud-based approach to firewall implementation, offering enhanced scalability and streamlined maintenance procedures. In this model, the firewall software's responsibility rests with the service provider, alleviating enterprises from the burden of routine tasks such as patch management, upgrades, and resource allocation [11]. With FWaaS, organisations benefit from the inherent scalability of cloud services, as resources dynamically scale up or down based on processing demands. This ensures optimal performance and availability without manual intervention from internal IT teams.

Moreover, FWaaS provides flexibility and agility that traditional on-premises firewall solutions may struggle to match. By offloading firewall management to a specialised provider, organisations can redirect their internal resources toward strategic initiatives rather than routine maintenance tasks. Additionally, FWaaS offers the advantage of centralised management and monitoring, allowing for comprehensive oversight of firewall policies and security posture across distributed environments. This centralised approach streamlines security operations, enhances visibility, and facilitates rapid response to emerging threats, ultimately bolstering the overall resilience of the organisation's network infrastructure.

6. Conclusion

The dynamic nature of the internet and the continuous evolution of technology underscore the critical importance of robust security measures for web applications. The globalisation of markets and the shift from monolithic applications to microservices have compelled organisations to embrace agile software development practices and adopt proactive risk mitigation strategies. OWASP's annual Top 10 highlights the pivotal role of Web Application Firewalls (WAFs) in defending against prevalent cyber threats. While WAFs serve as effective reverse proxies, offering an additional layer of security by scrutinising incoming requests, striking a delicate balance between security and application response speed is imperative. Administrators tasked with defining WAF rules must navigate this balance cautiously, mindful of the potential for false negatives that could inadvertently impact legitimate users.

As cyberattacks become increasingly frequent and sophisticated, organisations must adopt proactive measures to safeguard their data and users effectively. This entails regularly assessing vulnerabilities, implementing robust security tools, and fostering ongoing collaboration between security experts and software developers [12]. By promoting a culture of cooperation and vigilance, organisations can develop resilient systems capable of adapting to the ever-changing cybersecurity landscape, bolstering their defences against emerging threats, and ensuring the integrity and security of their web applications.

Future research in web application security could encompass several areas to address emerging challenges and technological advancements. One avenue for exploration lies in integrating machine learning and artificial intelligence techniques into Web Application Firewalls (WAFs), aiming to enhance threat detection and mitigation capabilities. Additionally, research could focus on developing innovative approaches for early detection and mitigation of zero-day threats, leveraging anomaly detection and threat intelligence to bolster security measures.

Another promising area for investigation is the security implications of serverless architectures, particularly in securing serverless functions and microservices. Research in this domain could explore new strategies and technologies to mitigate potential vulnerabilities and ensure robust protection against attacks in serverless environments. Furthermore, exploring privacy-preserving techniques for web applications, considering the increasing concerns around data privacy and evolving privacy regulations, could lead to the development of more secure and privacy-centric web applications. By delving into these research directions, the field of web application security can advance towards more effective and resilient solutions to safeguard against evolving cyber threats and ensure the integrity and security of web applications and their data.

7. References

[1] https://www.getastra.com/blog/security-audit/how-many-cyber-attacks-per-day, (2024). How Many Cyber Attacks Per Day: The Latest Stats and Impacts in 2024, Accessed on: 2024-1-16

[2] https://owasp.org/, (2024). Open Worldwide Application Security Project (OWASP), Accessed on: 2024-1-18

[3] Dakic, V., Jakobovic, K., & Zgrablic, L. (2022). Linux Security in Physical, Virtual, and Cloud Environments. In DAAAM Proceedings (pp. 0151–0160). DAAAM International Vienna, DOI: 10.2507/33rd.daaam.proceedings.021

[4] Islam, S. A., MohanKumar, M., & Jannat, U. K. (2023). Exploring the Effectiveness of Web Application Firewalls Against Diverse Attack Vectors. In 2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA). 2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA), DOI: 10.1109/iceca58529.2023.10395379

[5] Suskalo, D., Moric, Z., Redzepagic, J., & Regvart, D. (2023). Comparative Analysis of IBM Qradar and Wazuh for Security Information and Event Management. In DAAAM Proceedings (pp. 0096–0102). DAAAM International Vienna, DOI: 10.2507/34th.daaam.proceedings.014

[6] https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/ (2024), Cloudflare WAF Accessed on: 2024-1-16

[7] Chen, H.-C., Nshimiyimana, A., Damarjati, C., & Chang, P.-H. (2021). Detection and Prevention of Cross-site Scripting Attack with Combined Approaches, 2021 International Conference on Electronics, Information, and Communication (ICEIC), DOI:10.1109/iceic51217.2021.9369796

[8] https://expertinsights.com/insights/the-top-web-application-firewalls/ (2024). Expert InSights, Accessed on: 2024-1-18

[9] Ghanbari, Z., Rahmani, Y., Ghaffarian, H., & Ahmadzadegan, M. H. (2015). Comparative approach to web application firewalls. In Proceedings of 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), pp. 808-812, ISBN:978-1-4673-6506-2, DOI: 10.1109/kbei.2015.7436148

[10] Kaminska, M., Broeders, D., & Cristiano, F. (2021). Limiting Viral Spread: Automated Cyber Operations and the Principles of Distinction and Discrimination in the Grey Zone, In Proceedings of 13th International Conference on Cyber Conflict (CyCon 2021), pp. 59-72, ISBN:978-9916-9565-5-7, ISSN: 2325-5374, DOI: 10.23919/cycon51939.2021.9468290

[11] https://www.cloudflare.com/learning/security/what-is-next-generation-firewall-ngfw/ (2024), Cloudflare NGFW, Accessed on: 2024-1-26

[12] Liang, J., & Kim, Y. (2022). Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall, Proceedings of 12th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0752-0759, ISBN:978-1-6654-8303-2, DOI: 10.1109/ccwc54503.2022.9720435