International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 5 Issue: 9
ISSN: 2454-4248
01 – 03

Analysis of WAF and Its Contribution to Improve Security of Various Web Applications: Benefits, Challenges

Satish Kumar Alaria
Assistant Professor, Department of Computer Science & Engineering,
Arya Institute of Engineering & Technology,
Jaipur, Rajasthan (India)

Abstract: - WAF stands for web application firewall which is used to protect the web-based applications available online and also helps to filter and monitor the HTTP traffic between the web applications and the internet. It is used to provide security and maintain privacy of the websites and protect them from any kind of cyber-attack. It acts like a firewall which is kind of wall between the application and the internet and whenever any data packet comes in and goes out, it will check for its authentication and if it feels that it is safe enough then it will let it through the firewall but in case if it detects any kind of suspicion, it will not allow it to enter and use the website. The WAF can be of various types like host based, network based, cloud based depending upon the platform where the web-based application is located. It can also run as server plugins, cloud services, network appliances. The paper will discuss the importance of WAF and understand its contribution in improving the security of the web-based applications. It will also discuss the working mechanism of WAF along with its various categories and advantages and challenges of the same.

Keywords: - Introduction to web application firewall, Types of WAF, Working mechanism of WAF, Benefits of WAF, Disadvantages of WAF, Characteristics of WAF.

*****

Introduction: -

We all know that a large volume of data and information is available online which is sensitive and critical. It includes user's personnel information. Almost all the daily routine activities of the user are conducted online with the help of many applications available. For example, many applications are available for shopping, buying groceries, banking, booking flight tickets, railway reservation system etc. This saves a lot of time and efforts as all these can be carried out from the comfort of home. Since, it carries personnel information, it is at the risk of cyber-attack. It is mandatory that the application developers should pay attention to make them as secure as possible. They are using various efficient protocols and algorithms which are used for enhancing the security of these applications. One such security measure is Web application firewall whose goal is to filter all the data and information coming towards the application and allow only those data packets which are not harmful for the application. Its goal is to monitor every single data packet and filter the bad traffic from good http traffic. It also prevents and blocks malicious data packets, automated botnets attack. There are few attacks which exploits the weak key entry points of the application which are cookie poisoning, improper system configuration, SQL injection etc. All these are prevented by using latest technology of web application firewall. The simple proxy system protects the clients while WAF helps to prevent server from being attacked by the cyber-attacks. WAF acts like a wall between the web application and the internet and protects the web application from being exploited by intruders. WAF can be used to protect single web-based application as well as set or group of web-based applications. It performs like reverse proxy by verifying each client request and then letting it go to the application.

For all the online services and interactions, it is becoming critical to maintain the privacy and security of the applications. WAF is fastest growing and demanding technology which is able to protect these web-based applications from malicious attack. The critical data is stored in server. The moto of attackers is to get this information and to attack the servers, they try to attack these web-based applications and then take access to the server to fetch the important and sensitive information and exploit it to work in their favour.

Types of Web application firewalls: - [1]

There are following three main categories of WAF: -

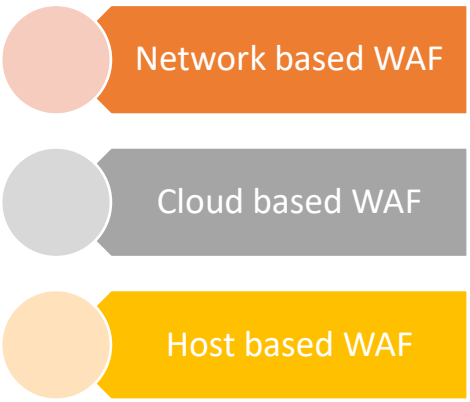

Figure 1 Web application firewalls categories.

 ISSN: 2454-4248
01 – 03

1. Network based WAF: -
   - It is one of the most-costly type of WAF as it requires maintaining physical equipment.
   - It is usually in the form of hardware which is used to reduce the latency by installing them locally.
   - It acts like a wall between the internet and the web-based application.

2. Cloud based WAF: -
   - It is one of the cheapest and available at low cost as compared to other kind of WAF available.
   - It is available in the cloud form where the WAF required for the applications of the

Company.
   - It will be available to the clients as security as a service where the clients will pay only for the services required which could be paid monthly or annually.
   - Regular updates are also done by the vendor provided by the cloud services which does not require extra amount to be paid and also does not require any work to be done by the end user.
   - The only thing which the user should look for the third-party vendors for the security as a service is that, it is customizable as per their business needs.

3. Host-based WAF: -
   - This type of WAF has capability to be integrated in the software of the web application itself.
   - It is cheaper than the network based WAF and can also be modified and customised as per the business requirements of the organisation.
   - The implementation process is complex and requires experienced professionals and also it requires local server resources.
   - The only expense is the cost required to maintain them.
   - It is also necessary that the machine which is used for the host based WAF to be updated and customised which is an expensive process.

Working mechanism of WAF: - [2]
   - As already discussed, WAF can be implemented in three ways which is network-based WAF, host-based WAF and Cloud-based WAF. They also follow certain set of rules and policies which are important for their successful implementation and protect against the attacks. These policies or rules are the protocols or security measures that are taken to protect the application form being attacked and make it secure and safe.
   - When a HTTP request is made then these algorithms and policies will verify the requests made and filter them to decide about the good requests and the malicious requests.
   - The main focus of WAF will be on the GET and POST requests generated by HTTP requests.
   - GET request is the request which is used to obtain data from the server whereas POST is the request which is used to send data to the server in order to change the state of the server.

Security Methodologies used in WAF: -
There are following three main types of approaches used in the configuration of the WAF: -

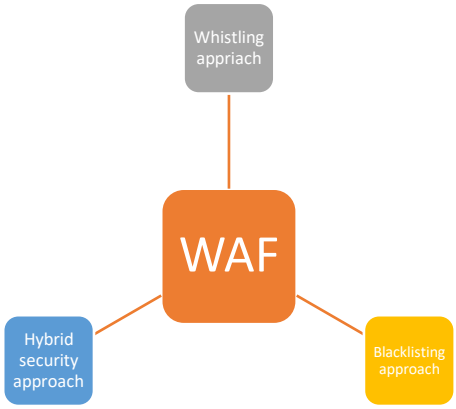

Figure 2 Methodologies of configuration of WAF.

1. Whitelisting approach: -
   - This approach will allow only pre-approved data packets to enter and use the web application. It will verify whether the generated request fulfils special criteria or not.
   - By default, this approach will deny access to all the data packets which cannot be trusted and will allow only trusted data packets to enter and use the application.
   - This method is useful only when the audience using the application is less in number for example limited numbe4r of employees in the company.
   - It cannot be useful for websites and applications which are public as it will block the genuine requests also.

2. Blacklisting approach: -
   - This method will block and not give access to the known malicious attacks and the vulnerabilities like attack signatures, malicious attacks, unauthorised web traffic etc.
   - If there are a number of requests from same IP address then this approach will block DDoS attacks and save the applications.

 ISSN: 2454-4248
01 – 03

- This approach is useful to be used in the public websites and application since requests can be received from unfamiliar clients.

3. Hybrid Security Approach: -
   - This approach is the combination of the first two approaches that is it integrates the positives of whitelisting approach and blacklisting approach. It can be used on internal as well as external networks.

Benefits of WAF: - [3]

Having a WAF between the web application and internet protects it from being attacked and provides security and privacy of the website is maintained. Following are the advantages of WAF: -

- It helps to protect the website and application from cookies poisoning, SQL injection prevention, prevent cross-site scripting etc.
- WAFs safeguard web applications and APIs against various sorts of interior and outside assaults, for example, infusion assaults, application-layer refusal of administration (DoS), cross-webpage prearranging (XSS), computerized assaults (bots), among others. WAFs give signature-based insurance and furthermore assist with positive security models and peculiarity openness.
- WAF follows set of rules which are known as policies and also uses various security protocols and algorithms, all these acts like a layer between the online application and the internet and thus prevents the application from attack by separating the good traffic from bad traffic.
- By conveying Web Application Firewalls before a web application, a protection is made between the web application and the Internet. A WAF, which is a converse intermediary, safeguards the server from being uncovered by making clients go through the Web Application Firewall prior to arriving at the server.

Limitations of WAF: - [4]

Following are some of the challenges of the WAF: -

1. Lack of user-friendly interfaces: -
   In open sources WAF's, there is lack of clear and user-friendly interfaces which makes it difficult to understand the data in the traffic and it is not able to identify the vulnerabilities it consists of.

2. False positives and negatives: -
   WAF's uses predefined patterns and decides the legitimacy of the data packets based on these patterns. It tends to give false result for positives and negatives if there is some variation in these patterns. False negative takes place when a bad request is not identified properly and a false positive takes place when there is a good data packet but it is marked as malicious data packet.

3. Replay attacks: - This is a challenging task for a WAF to protect the website and application from replay attacks which takes place when a valid data packet is delayed and also is repeatedly sent by the intruder.
4. Cost and maintenance issues: - The cost of implementation of WAF is higher and small business cannot afford it. It also requires regular update of the systems on which WAF installed failing which will not give desired results which it is supposed to give.

Conclusion: - WAF represents web application firewall which is utilized to safeguard the electronic applications accessible on the web and furthermore assists with separating and screen the HTTP traffic between the web applications and the web. It is utilized to give security and keep up with security of the sites and shield them from any sort of digital assault. It behaves like a firewall which is somewhat wall between the application and the web and at whatever point any information bundle comes in and goes out, it will check for its validation and on the off chance that it feels that it is sufficiently protected, it will let it through the firewall however in the event that assuming it distinguishes any sort of doubt, it won't permit it to enter and utilize the site. The WAF can be of different sorts like host based, network based, cloud put together depending with respect to the stage where the electronic application is found. It can likewise run as server modules, cloud administrations, network apparatuses. With the increase in number of online applications for daily routine activities, the need for having efficient Waf is also growing and discoveries and innovations are being made to enhance the features.

References: -

[1]. https://www.imperva.com/learn/application-security/what-is-web-application-firewall-waf/
[2]. https://www.ascentinfosec.com/blog/web-application-firewall-an-introduction/#
[3]. https://www.strongboxit.com/web-application-firewalls-waf-and-its-advantages/
[4]. https://en.cloudbric.com/blog/2020/12/open-source-web-application-firewall-downsides/