WAF Implementation to Provide Security Against DDoS Attacks

Sanica Kamble[1]

[1]PG Student, Vivekanand Education Society's Institute of Technology, Dept. of MCA, Mumbai, India

---***---

Abstract - *In today's tech savvy world, every business wants its presence online, be it a small business or a big business. This is an important business move as it becomes easy to target all kinds of audience at any time of the day. Hence, it becomes very important to secure web applications to provide round-the-clock and reliable service to the consumers. Almost all the Web Applications use Network firewalls, however, they only provide security on the 3rd and 4th layer of OSI Layer architecture. Moreover, there is a possibility that there are a lot of loopholes in the web application itself which makes the web application layer (7th layer of OSI) vulnerable of attacks. Here's when Web Application Firewall (WAF) plays an important role to secure the web applications. This paper focuses on how WAF is used to provide security or how it deals with the DDoS botnet attacks.*

***Key Words*: WAF (Web Application Firewall), DDoS (Distributed Denial of Service), OSI (Open Systems Interconnection), ML (Machine Learning)**

1. INTRODUCTION

Our lives revolve around the internet. Even in times of Corona pandemic, the internet has become our saviour. There is nothing that it can't provide. We seek for various services on the web. In order to keep receiving these services it's important to secure the web applications of the services providers. There are a lot of web applications that provide real time critical information or run 24/7, these can't afford to be down at any point of time. For these very reasons, it becomes necessary to secure the application layer security as this is the most vulnerable layer.

The motives behind the DDos attacks can be to deprive the information to be passed on to the public to create panic and chaos, to tarnish the brand image, politics, revenge or a hacker(attacker) having a fun time [1]. Sometimes there is not an attacker/hacker behind the DDoS attacks but some genuine increase in traffic can also cause the same consequences as that of the DDos. Hence it is really important to differentiate between the real ones and the genuine ones and the security layer must provide that service.

The most recent DDos attack attempt happened in mid-March 2020 and was made on the website of the US department of health & human services. This was an attempt to disable the website and to deprive citizens of access to official data about the pandemic and measures taken against it and in the meantime spread hoax news on the social media but the attempt was failed. Similar attack happened on the large Paris-based group of hospitals Assistance Publique-Hôpitaux de Paris; their systems were down for several hours but the entire organization wasn't paralyzed due to this [2].

The year 2020 has seen a greater number of DDos attacks than previous years as the entire world is now relying upon the internet more than ever! [3]

On the plus side people are becoming more aware about DDoS attacks [3]. More emphasis is put on the architecture of the application to make it more secure against 7th layer attacks.

The main reason for application layer attacks is mostly poor coding. Poor coding includes missing validations on input fields. Another reason is, no thought process was made while creating an architecture diagram. Other reasons being poor session management, using 3rd party applications which cannot guarantee the safeguard of our applications. All of these can happen if unskilled people or developers are used while developing a web application leaving various loopholes for attackers. The basic level of protection against application layer attacks can be provided by using safe coding methods, proper validations, putting a lot of thought process while creating an architecture diagram. While all of these are important at providing a basic level of security there has to be a much powerful level of security between the application and its endpoint. Here is when WAF comes in picture.

2. INTRODUCTION TO WAF

WAF is an acronym for Web Application firewall which specifically focuses on providing security at the application layer (7th layer) that is the top layer of OSI model. It provides security against the following:

i) Cross-site-scripting

ii) Sql injection

iii) DDoS

All of the above-mentioned attacks are application layer based.

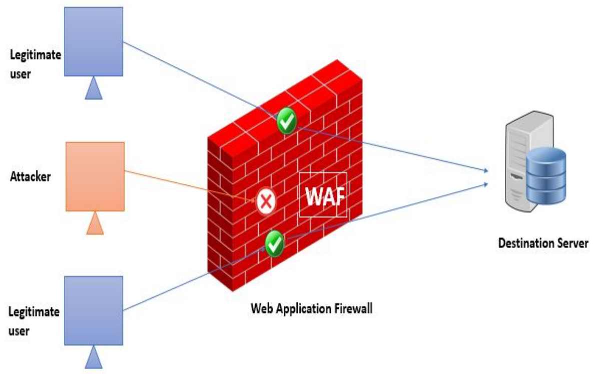

Fig -1: Showing how a WAF just accepts requests from legitimate sources [4].

There are various types of vendors that provide WAF:

1. AWS WAF
2. Fortinate
3. Symantec
4. Akamai
5. Securi

The above-mentioned vendors provide security against WAF. Every WAF provided by a vendor is designed for a specific purpose. It's most likely that it won't have all the features.

3. DDoS PROTECTION WITH WAF

Layer 7 DDos (Distributed Denial of Service) attack or application layer attacks are designed to target the top layer of OSI model. This is because this is where API calls take place. Their job is to consume the server resources more than the application can handle in turn make the application slow or stop completely, this is how users are denied services hence the name Denial of Service. Distributed word in DDos states that the requests don't come from a single source but from multiple sources (botnets).

It's pretty much easy to attack the application layer and bring the system down with just low bandwidth [5]. All the attacker has to do is send multiple requests to the target. In this condition the amount or resources an attacker is using to make requests are much less than the resources a server/target might use to fulfil the request. But flooding of requests isn't always done by the attacker, the traffic might be a cause of legitimate user requests too. Hence, it is also important to understand the difference between an attack and legitimate user requests. The requests coming from an attack may seem like real attacks which make it very difficult to analyse it and curb at the earliest possible.

To handle all the problems of DDoS attacks it is very important to configure the WAF properly [5]. WAF will figure out the difference between legitimate requests and bogus requests and save the system from going offline.

WAF works on policies or sets of protocols, some of them are default security protocols that the WAF will provide and others can be customized [4]. It is possible to customize WAF with the required set of protocols. The customization would depend upon the type of application it will be implemented in. It is really very important to analyse the need of the website before configuring WAF for it so that it serves its purpose. The study can be done as early as in the requirement gathering phase, here you can have a rougher estimation of the request load the web application will be facing in its real environment and then accordingly the suggestions of the policies the WAF would have for the web application can be made or even after the web application has been deployed.

The WAF limits the rate of the requests which can prevent DDoS attacks and it allows quick changing of policies during such a situation.

Configuring the WAF policies suited for the web application can be done as follows: -

1. Analyse the web application in its real environment. This can be done manually. The traffic the web application receives is monitored passively for weeks. This will give the average figure of the number of requests received.
2. Study the types of requests received. This will be important to know what kinds of requests should be allowed and what kinds of requests to block.
3. Analyse the vulnerabilities of web applications and set policies for the WAF accordingly.

Importance of analysing web application for WAF implementation: -

1. Once the average number of requests are known it will help in recognizing the botnet attacks.
2. Analysing the type of request will help in differentiating between the spoofed requests and the legitimate once.
3. The vulnerabilities of the web application can help to set some extra level of protocols in the WAF for better experience and protection from DDoS attacks.

WAF configuration models: -

1. *Negative Security model*: -

   It provides protection against the attacks that were already known. The WAF will be configured such that the known type of attacks / requests that might harm the web application will be blocked beforehand. Hence, it is also called the blocklist model [4].

2. *Positive Security model*: -

   It allows only the known requests. The WAF will be configured such that it will allow only the types of requests that are to be received by the web application. Hence, it is also called as the allow list model [4].

3. Hybrid Security model:

   The hybrid security model was created to overcome the flaws of the negative and positive security model. Hence, the name hybrid [6].

Depending on the need of the web application/ organization the WAF can be configured like the above-mentioned models for web application security.

WAF Implementation: -

It can be implemented in 3 ways:

1. Network based WAF: -

Network based WAF(NWAF) is a hardware device. It will be installed closer to the server, which makes it easier to access it. It provides reduction in the latency of the web application. It also provides rule replicating hence deploying it on a large scale will be easier.

Drawbacks: -

- Takes storage space.
- Expensive
- Suitable for small scale web applications

2. *Host based WAF: -*

Host based WAF (HWAF) are integrated directly into the application software. These are much cheaper than the HWAF ones and more customizable.

Drawbacks: -

- Consumes a lot of local server resources and might harm the speed of the web application.
- Since it is implemented inside the application there might be implementation complexity.
- It can be very costly.

3. Cloud based WAF: -

Cloud based WAF (CWAF) are the most affordable options. The organization just has to pay for the services as long as CWAF is used for their web application. Here the configuration, implementation and maintenance overheads are comparatively reduced. It will also provide regular updates.

Drawbacks: -

- CWAFs are provided by third parties hence they are not as much customizable and also some of the features might not be known beforehand.
- Here you might also end up paying extra for the features you might not need.

The implementation of WAF will depend upon the size of web applications and also the budget of the organization. The key here is to keep in mind the drawbacks of three before implementing it for the web application.

Basic Characteristics of WAF:

- It does the entire scanning of the application on a daily basis.
- It monitors the web application at regular intervals for malicious activity.
- Some WAFs (vendor specific) use ML to train the WAF with the changing nature of DDoS attacks, identifying the DDoS bots (pretender bots) or for identifying malicious activity and to stop/block it [7].

4. FINDINGS

1. It's easy to target/ attack web applications due to the vulnerabilities in the code. Hence, security at 7th layer is important
2. WAF works on a set of policies that are customizable.

3. Every vendor provides WAF with different policies.
4. It works on two models and can be implemented according to the needs and budget of the organization.
5. WAFs can be trained using Machine Learning (ML)

5. CONCLUSIONS

A web application cannot be made perfect. There will always be some loopholes. Hence, web applications have been a prime target. Using WAF it is possible to cover up those loopholes and save the web application from going offline. The service that the web application provides is very important to build up its brand value and customer base. WAF provides great customizable features and is easy to implement. Helps the web application to always be Online.

ACKNOWLEDGEMENT

First & foremost, I would like to thank our guide Prof. Indira Bhattachariya, for her guidance and support. Through our many discussions, she helped us to form and solidify ideas, that led to the completion of this paper.

REFERENCES

[1] https://www.pentasecurity.com/blog/ddos-top-6-hackers-attack/#:~:text=Seeking%20Their%20Revenge,seek%20revenge%20on%20your%20enemy.

[2] https://securelist.com/ddos-attacks-in-q1-2020/96837/

[3] https://www.comparitech.com/blog/information-security/ddos-statistics-facts/

[4] https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

[5] https://www.cloudflare.com/learning/ddos/application-layer-ddos-attack/

[6] https://www.ptsecurity.com/ww-en/analytics/knowledge-base/waf-web-application-firewall/#:~:text=Web%20application%20firewalls%20are%20designed,whenever%20it%20detects%20malicious%20traffic.

[7] https://avinetworks.com/what-is-a-web-application-firewall/