*International Journal of Engineering & Technology*, 7 (2.7) (2018) 58-61

International Journal of Engineering & Technology

*Website: www.sciencepubco.com/index.php/IJET*

***Research Paper***



# IoT security through web application firewall

**B. Prema Sindhuri[1]*, M. Kameswara Rao[2]**

*[1]Department of CSE, K L E F*
*[2]Department of ECSE, K L E F*
**Email: premasindhuri24@gmail.com*

**Abstract**

The current trend in home electronics needs to be Internet Connectivity. Internet of Things is a collection of many interconnected objects, services and devices that can communicate and share the data to achieve a common goal in different areas and applications using internet. Attacks on IoT devices are physical attacks, side channel attacks, cryptanalysis attacks, software attacks, network attacks. The network attacks does not require physical access to create a major disruption like DDos in the network. The attackers can insert themselves between us and our devices like Man in Middle Attack. A firewall acts as a barrier between a trusted network and an untrusted network. This is a proposed work to focus on the security challenges of IoT using web application firewall.

***Keywords***: *IPS; OWASP; Web Application Firewall(WAF).*

## 1. Introduction

IoT is a network of physical objects (things) which contain embedded technology to sense or communicate with the internal state or external environment. Massive objects are connected to internet. The security will become a big challenge for IoT. Generally, the successful attacks will occur on the application layer (OSI Model – Layer 7) as this is still the most vulnerable area.

Almost web applications have many different attacks which may easily attack to the application. According to the research by web security consortium above 49% of web applications contain vulnerabilities of high risk level detected during automatic scanning [2]. In the early days of the web, the attacks were made by trying to access vulnerable services of the web servers or in case of users, by infecting with malware.

The first generation of firewalls were hardware appliances that isolated corporate networks from the internet by filtering packets. This type of firewalls prevent upto OSI Layer 3(Network Layer). These firewalls inspect the address and port of packets based on set of filtering rules and either discards them or passes them. These are stateless firewalls because they don't have memory of previous packets so a decision is made on a straight forward packet – by – packet basis. The second generation of firewalls are connection aware and operate upto OSI Layer 4(Transport Layer). This type of firewalls inspect incoming and outgoing packets over time, they can more intelligently make filtering decisions thus providing more usability and security.

As firewalls were intended to secure internal networks from larger networks they were mainly used industrially in the 90's. In the beginning of the 90's, the rise of many still recognizable antivirus software like panda, Norton, F-Secure. They are software based firewalls installed on a personal computer(PC), so essentially a hardware appliance that is not trivial to install and configure is now accessible to consumer and sometimes this feature is even included in an antivirus software.

Web Application Firewall(WAF) as a term started appearing in 2005. These are first firewalls that prevent attacks upto OSI Layer 7 (Application Layer). Numerous high profile data breaches in recent years have driven companies to adopt WAFs and in 2013, the market earned revenues of global WAF market was $431 million[1].

## 2. Common Attacks

There are some categories of attacks which are occurred on web application [3]:

- **Script Injections**, especially SQL injections are attacks that inject another code to read or modify the data on database for the original query. This will give us an insufficient validation of input, or erroneous data.
- **Parameter Tampering**, is an attack which modifies the parameter which is given as request, and values are assigned which may not expected by the server. The Best example for the parameter tampering is script injections, but this type of attack will be denied the application or server
- **Forceful Browsing** is a one of the attack which have guide access to the accessible server assets by asking for particular URL's as opposed to utilizing connections and structures gave in the application. Using this approach an attacker can get access to application
- **Cross-site Scripting** it is also a code injection technique like script injection, where the aim of the attacker is to attack the users who are connected to that server. The attacker can send a code which can be provided by the server to different clients and it will be effected on their

**Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.**

PCs. So, The attacker can get the access of confidential information including the identity

- **Man in Middle** is an attack, the attacker which listens the data between a client and server. The attacker may get the access of privileged information or he may change the information before it reaches to the server. To prevent from the attack, the encryption mechanism with verification of digital certificates are used.
- **Distributed Denial of Service(DDoS)**, are attacks that it will stop the function of web service or it may get the access for the resources which are provided by the server. So the system will become unresponsive
- **Session Hijacking and Cookies Tampering**, these are attacks which can target the other data instead of getting the access for resources
- **Buffer Overflows**, it is a type of attack which overwrite the programs data with their own code because of limited memory allocation pools. Ofcourse, it is not a serious threat it may not affect the web application.

Web application firewalls have become the solution for protecting the applications against above few attacks also including business logic attacks and online fraud.

## 3. Overview of Web Application Firewalls:

Web Application Firewall (WAF) is an appliance, server plugin or filter that applies a set of rules to an HTTP Conversation [7]. In General, a WAF is located on the web server it protects or on an intermediate reverse proxy between an external network and one or more web servers. This WAF monitors the Application layer and protects the web application from malicious or erroneous behavior. Therefore, it also prevents the attacks which are not prevented by Intrusion Detection Systems (IDS) and Network Firewalls.
A web application firewall is a powerful tool because it changes the behavior of a web application without requiring any changes to the web application itself. By checking the data portion of packets, more detailed information is revealed which is referred as the granularity of packet [5]. For example, inside the HTTP header there would be request which may contain user agents, cookies `and more. Web applications are rarely safe from attackers and fixing known security holes can take a significant amount of time, it is crucial to implement a WAF to systems that have consequences when they are exposed to the attacks.
All WAFs function in a similar way. They act as an intermediary service between the website application and the visitor. The implementation of WAF technologies are not to be replaced the other controls but it will complement those controls
The below diagram represents the representation of a WAF with other firewalls [10]:

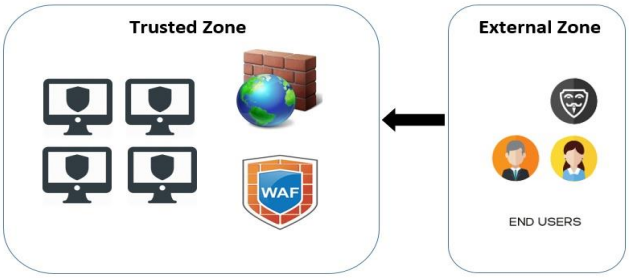



**Fig. 1:** Web Application Firewall (WAF)

To prevent the web application, the WAF can implement the security policies or rules for an application, WAF can use the positive or negative security model [4].
The positive security model means it can make the decision that which requests are accepted and rejects everything else. This is also called as whitelisting. It can be more efficient and more secure. But it is difficult to maintain if we frequently changing the application. The negative security model means it can rejects the requests and allows everything else. This is also called as blacklisting. It can be achieved by blocking the matched information of attack signatures which is compared with the traffic [4] . These policies do not consider the working of application.

WAF can be deployed in three different ways. Those are:

Reverse Proxy: In this mode, The WAF is set inline and it additionally has an IP address. Every one of the solicitations are sent to this sort of WAF which may a different demand to the web server. The security can be given upto seventh layer(Application Layer - OSI Model) by scrambling the Connection. The below diagram represents the WAF architecture which was deployed by means of reverse proxy.

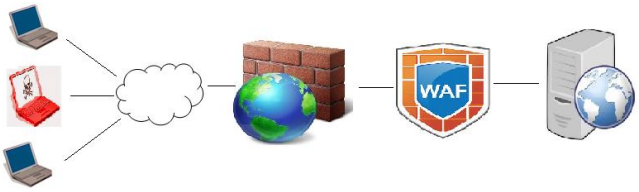



**Fig. 2:** Reverse Proxy or Bridge WAF

Bridge: In this mode likewise, the WAF is set inline and goes about as a switch. It additionally executes an inactive SSL decryption and it also able to block the traffic by removing the offending packets. It gives the high performance than reverse proxy with network changes. This mode architecture also similar to the architecture of reverse proxy WAF.

Out-of-band: In this mode, it gets the duplicate copy of a traffic through monitoring port on a network device. It also performs the passive SSL decryption but it has some limitations like the Diffie-Hellman that bridge may suffer. This WAF is placed with the help of switch to get the copy of the traffic. The below diagram represents the WAF architecture with the out-of-band deployment option

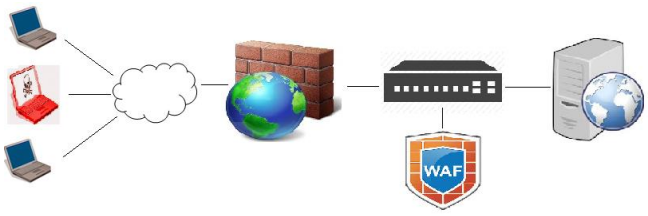



**Fig. 3:** Out-of-band WAF

Server Resident: A server occupant or implanted WAF is a product which is introduced on the host which is running the web server. This can be accomplished utilizing the free application or a web server module. The below diagram represents the Server resident WAF.

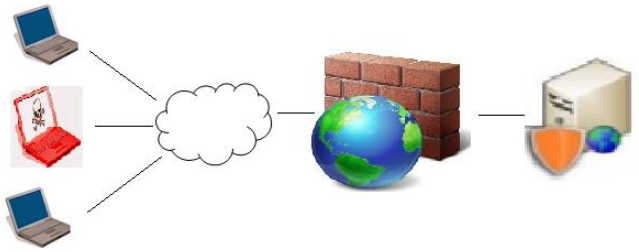


**Fig. 4:** Server Resident WAF

Cloud based: It is a newer mode but it uses a cloud provider to implement the WAF solution. It works like a reverse proxy option, the public Domain Name System(DNS) is configured to point the cloud provider which may creates the another connection to the web property. The below diagram represents the WAF shielded by the external environment which acts as the SAAS.

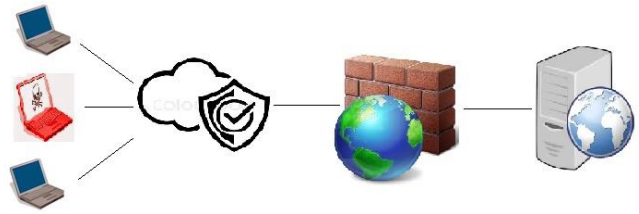


**Fig. 4:** Cloud WAF

## 4. WAF Features & Benefits

By observed most common features that WAFs have we can gain a good understanding of what WAFs generally look like. The below table was collection of a features which are essential and some extended features which are advanced than core WAFs.

**Table 1:** WAF Features

| Feature | Core WAF | Extended WAF | Not a WAF |
|---|---|---|---|
| Understands application Layer protocols: HTTP | ✓ | | |
| - HTTPS | ✓ | | |
| - XML | | ✓ | |
| IP Blocking by IP Range | ✓ | | |
| - By geolocation | | ✓ | |
| - By reputation | | ✓ | |
| Request Blocking | ✓ | | |
| Response Blocking | | ✓ | |
| Negative Security Model | ✓ | | |
| Positive security Model | | ✓ | |
| Virtual Patching | ✓ | | |
| Character Decoding | ✓ | | |
| Brute force Mitigation | ✓ | | |
| Cookie protection | | ✓ | |
| Logging | ✓ | | |
| Reporting | | ✓ | |
| Vulnerability Scanning | | | ✓ |
| Software Debugging | | | ✓ |

### 4.1. Benefits

These firewalls work to prevent the web application from unauthorized data. It also beneficial for any online business, especially e-commerce and online retailers because it stores the private user data securely. The WAF can automatically filter out malicious web traffic and it allow our business to manually decide who they want to block from their site.

These WAFs protect against [9]:
- SQL injection, comment spams
- XSS
- DDoS attacks
- Application Specific attacks
- Automatic protection from diverse threats
- Real time reporting and robust logging

## 5. Comparison of WAF & IPS

When WAF features are compared with Intrusion Protection System(IPS) features it have some similarities between those two systems but it also some differences. IPS is an inline packet inspector that it has ability to reject the packet or it may terminate the connection. Thus it also relies mainly on identifying signatures but not understanding the web application like WAFs can do. The below table that compares the features of IPS with WAF [8].

**Table 2:** Comparison of WAF & IPS Features

| Security Feature | IPS | WAF |
|---|---|---|
| SQL Injection and XSS | Limited | Yes |
| CSRF Prevention | No | Yes |
| Inspect HTTPS traffic | No | Yes |
| Encoded traffic | No | Yes |
| Virus Protection | Yes | Yes |
| Request, Response rewrite | No | Yes |
| Rate control Protection | No | Yes |
| Session Tampering/ Hijacking | No | Yes |
| Application layer DOS protection | No | Yes |
| Data Theft Protection, Cloaking | No | Yes |
| Forceful Browsing Prevention | No | Yes |
| Brute force approach | No | Yes |
| Application access logging and user audit trails | No | Yes |
| Web Services Projection | No | Yes |

## 6. Conclusion

The most important aspects of IoT with particular focus on security challenges, the vision of IoT allow people to be connected anytime, anywhere with anyone and anything using network and any services. IoT devices played a big part in DDoS attacks and we are only in the beginning of the IoT trend. To provide the Security from the attacks which occurred from the application, the WAF is used to filter the malicious traffic from the web traffic. During the implementation of WAF the XML Parser will help from the complications. That plugin will take the support of XML and XMPP. But if the IoT devices use mobile connections, like many things what we are working today they are not behind a firewall, which makes them more vulnerable.

## References

[1] Frost & Sullivan, "High-Profile Data Breaches Demand Web Application Firewall Adoption," [online]. Available: http://ww2.frost.com/news/press-releases/highprofile-data-

breaches-demand-web-application-firewall-adoption/ [Accessed 14th July 2016].
[2] Darisuz palka, Marak Zachara, “Learning Web Application Firewall – Benefits and Caveats”, August 2011.
[3] Hope P., Walther B.: Web Security Testing Cookbook. O’Reilly Media, ISBN: 9780-596-51483-9 (2008)
[4] Jason Pubal, “Web Application Firewall”, Gold Certification, Sans Institute, March 13, 2015.
[5] SANS Institute. (2012). The OSI Model: An Overview. [Online].Available:http://www.sans.org/reading_room/whitepapers/standards/osi-model - overview_543
[6] Alexander Endraca, Bryan King, George Nodalo, Maricone Sta. Maria, and Isaac Sabas, “ Web Application Firewall”, International Journal of e-Education, e-Business, e-Management and e-Learning, Vol. 3, No. 6, December 2013.
[7] Web Application Security Consortium, “Web Application Firewall Evaluation Criteria," [online]. Available: http://projects.webappsec.org/w/page/13246983/WAFEC%201%20HTML%20Version [Accessed 29th June 2016].
[8] Joonas Bloomberg, “ Securing Internet of Things with a Web Application Firewall”, Master Thesis, 2017.
[9] Richardh, “Benefits of using a Web Application Firewall” [online]. Available https://www.veber.co.uk/web-application-firewall-benefits/ [September 7, 2016].
[10] Tony Perez, “Website Application Firewalls(WAF)- Practical Approach to Website Security”, [online]. Avaliable: https://blog.sucuri.net/2017/02/website-application-firewalls-waf-practical-approach-to-website-security.html [February 3, 2017].