IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10504

A Brief Study on The Evolution of Next Generation Firewall and Web Application Firewall

Dr. A. Shaji George[1], A. S. Hovan George[2]

Masters IT Solutions, Chennai, Chennai, Tamil Nadu, India[1,2]

Abstract: The rapid development of Information Technology (IT) has altered the appearance of the network perimeter. Data is all around, with users who access it from around the world and from all types of devices. At the same moment, Information Technology (IT) teams are implementing analytics, cloud, as well as automation to quicken the delivery of innovative applications and drive business development. These essential changes have created a threat environment that reveals weaknesses in legacy security technologies, for example, the port-based network security, as well as the different tools and technologies which are not natively incorporated. This concern has driven many enterprises to look for more sophisticated capabilities to improve their cybersecurity. Traditionally, a normal firewall follows preset Web protocols. It does not have the capability to differentiate between different types of Web traffic. This restriction forces the system in order to only permit or prohibit traffic, depending upon a specific set of built-in standards. Therefore, the protection it offers for particular protocols, ports, and IP addresses is no longer sufficient. Businesses need tougher security that is not tied down to preset settings. Modern-day firewalls need more advanced rules to control website access as well as app usage inside the enterprise networks thus the advancement of next-generation firewalls (NGFWs) and Web Application Firewall (WAFW). The main objective of this research paper is to analyze the evolution of next-generation firewalls (NGFWs) and Web Application Firewall (WAFW) and their characteristics. Also, what it is going to take to safeguard the enterprise's environment for the foreseeable future.

Keywords: Next-Generation Firewalls (NGFWs), Web Application Firewall (WAFW), SQL Injection, Cross-site Scripting (XSS), Web Scraping, OWASP Top Ten threats.

I. INTRODUCTION

The technology landscape is continually evolving. Cloud computing, virtualization as well as mobility get radically altered the manner in which companies perform business. At exactly the same time, innovative threats are going to come from a different perspective, introducing security experts with a continuing challenge of safeguarding their organization's assets [7]. Efficiently safeguarding the web properties which are prevalent all through the present organizations is conditional upon a comprehensive understanding of the functionality, as well as the restrictions, of accessible security technologies. For instance, although traditional firewalls, as well as intrusion prevention systems (IPS), are helpful for inspection out large quantities of lower-layer threats, they are significantly less adept at protecting against becoming more and more targeted, application-specific threats usually that are used against organizations now. In spite of providing significantly improved granularity for managing access to network resources, even next-generation firewalls fall short in the crucial area of web property protection [7]. In order to safeguard your organization's internet sites, applications as well as web properties against the present ever-changing cybersecurity threats, to help prevent data breaches as well as unauthorized access. Understanding the differences among the kinds of firewalls, involving how they work, and their functionality and shortcomings will make up the difference as regards whether your company will be fully protected against all types of threats on the web today. Throughout this article, we will study two different types of firewalls: next-generation firewalls and web application firewalls. We shall also demonstrate that the two kinds of firewalls that are essential to protect against many web application layer attacks. Therefore, to safeguard vital websites or web applications, it will require a web application firewall in order to complement the next-generation firewall.

II. OBJECTIVES OF THE STUDY

The objective of the active research paper is, to sum up, the evolution of Next-generation firewall and Web Application Firewall, which comes to the conclusion that the traditional firewall has some limitations. This paper discusses the features and advantages of the next-generation firewalls and Web Application Firewall.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

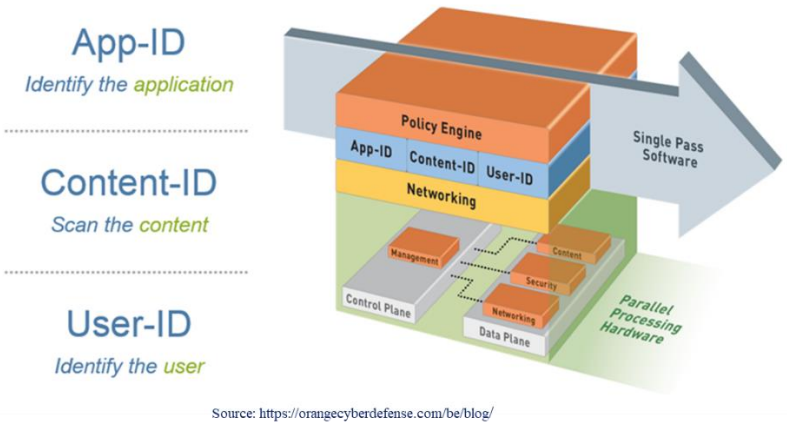
DOI 10.17148/IJARCCE.2021.10504

III.METHODOLOGY OF THE STUDY

This research mainly uses secondary data. Information that will be used for the study was exclusively based on secondary sources from various publications. The proper sources of information collected are published as well as unpublished sources like books, magazines, journals, reports, publications, and the website of numerous online journals, etc. Most editorials analyzed for this research have been collected utilizing Online Newspapers, Articles, and IT Blog database. The key terms used to look up appropriate articles contained "NGWFs" "WAFs" in the headline as well as "Next-generation firewall" "Web Application Firewall" in every text. The data has been analyzed from the period of 2010- April 2021.

IV. ABOUT NEXT-GENERATION FIREWALL

The Next-Generation Firewall (NGFW) is a portion of the 3rd generation of firewall technology, which combines a traditional firewall along with other network appliance filtering functions (NAFF) for example, inline intrusion prevention system (IPS) as well as in a deep packet inspection (DPI) [2]. The idea of the NGFW had been introduced a decade earlier by Gartner. A next-generation firewall is deep-packet inspection (DPI) firewalls that are moving beyond port and protocol inspection (PI) as well as blocking to add application-level inspection (ALI), intrusion prevention, as well as bringing intelligence from outside the firewall[2].The Traditional firewalls functioned at Layer 3 and Layer 4, and permitted or blocked traffic based upon port and protocol, with a leverage stateful inspection, and were making decisions that are based on defined policies[2].These Days it is no longer practical or trusted to carry out the security policies in such an inflexible as well as non-transparent way[1].



Source: https://orangecyberdefense.com/be/blog/

Fig. 1 Next Generation Firewall (NGFW)

Fig. 1 Next-generation Firewall (NGFW)

As incidents evolved and went on to become more sophisticated, attackers have managed to circumvent the stateful inspection firewalls, making enhanced security much more critical. Next-generation firewall began to deliver all the capabilities of the traditional firewall, as well as the additional capabilities of application control as well as integrated intrusion prevention [1]. They have also provided more granular functionality to identity location, user, as well as application. Rather than using multiple different point solutions, a next-generation firewall significantly simplifies and enhances the effectiveness of applying security rules in an increasingly sophisticated computing world [1].

V. BACKGROUND AND RELATED PROPERTIES OF FIREWALL

The firewall is a network security device that monitors inbound and outbound network traffic and allows or denies data packets based upon a set of security policies. Its objective is to create a barrier between the internal network and inbound traffic from outside sources (like the internet) in an effort to block malicious traffic such as viruses and hackers [13,14]. Firewalls thoroughly investigate the inbound traffic based upon pre-formed rules as well as filter traffic originating from unsafe or suspect sources to help prevent attacks. A Firewall guards' traffic on a computer's entrance point, known as ports, that is where information can be exchanged along with external devices [14,15].

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10504

Types of firewalls techniques

Firewalls could be either hardware or software, although it is best to have both together. The software firewall is a program that is installed on every computer and controls traffic via port numbers as well as applications, whilst the physical firewall is a piece of Hardware installed between the network and gateway.

i)The Packet filtering firewalls: the most normal form of firewall, assess packets and prohibit them from passing by if they do not match a formed security rule established. This kind of firewall monitors the packet's source and target IP addresses. Unless the packets correspond with those of a "permitted" rule in the firewall, then it is reliable for entry into the network.

ii)Packet-filtering firewalls are split into two groups, stateful and stateless. The stateless firewall investigates packets separately from each other as well as lacks perspective, which makes them easy objectives for hackers. In comparison, stateful firewalls recall information regarding formerly passed packets and are deemed far more secure.
Whilst packet-filtering firewalls may be effective, they eventually provide extremely essential protection and can be extremely limited for instance, they cannot determine whether the contents of the request that's being dispatched will have a negative impact on the application it is getting. If the malicious request which was allowed from a reliable source address would lead to, the removal of a database, a firewall would have absolutely no way of understanding that. Next-generation firewalls, as well as proxy firewalls, are more outfitted to identify those threats.

iii)Proxy firewalls filter traffic on the network on an application level. In Contrast to the fundamental firewalls, a proxy acts as a mediator between the two end systems. The client should submit a request to the firewall, where it is later assessed against a collection of security rules and subsequently allowed or denied. Most particularly, proxy firewalls examine traffic for layer 7 protocols like the HTTP as well as FTP and make use of equally stateful and deep packet inspection to identify malicious traffic.

iv)Network address translation (NAT) firewalls enable several devices with autonomous network addresses to connect to the internet through a single IP address, protecting individual IP addresses concealed. As a consequence, attackers searching a network for IP addresses will not be able to capture particular details, offering more security against the attacks. NAT firewalls are like proxy firewalls because they serve as a mediator between a group of computers as well as outside traffic.

v)Stateful multilayer inspection (SMLI) firewalls filter packets at a network, transport, and application layers and compares them against known trusted packets. Similar to NGFW firewalls, SMLI likewise inspects the whole packet and then only enables them to pass as long as they pass every layer separately. The Above-Mentioned firewalls assess packets to determine the status of the communication in order to ensure that all commenced communication is the only one taking place along with trusted sources.

vi)Unified threat management (UTM) firewall-A UTM apparatus that typically mixes, in a loosely connected way, the functions of a stateful inspection firewall together with intrusion prevention as well as antivirus. It can also include extra services and often cloud management. UTMs concentrate on being simple and easy to use [16].

vii)Next-generation firewalls (NGFW) merge traditional firewall technology with extra features, like anti-virus (AV), intrusion prevention systems (IPS), encrypted traffic inspection (ETI), and more. Most particularly, it contains deep packet inspection (DPI). Whilst basic firewalls only take a look at packet headers, deep packet inspection analyzes the data inside the packet itself, which allows users to more efficiently detect, classify, or halt packets with malicious data [16].

viii)Threat-focused NGFW-Such firewalls contain all the functionality of a traditional NGFW as well as provide enhanced threat detection as well as remediation. Together With a threat focused NGFW, you will be able to [16]:

- Figure out which assets are at highest risk with full context perception.
- Respond quickly to attacks with an intelligent security automated system that establishes policies and strengthens your defenses in a dynamic.
- Better identify evasive or suspicious activities with the network and endpoint incident connection.
- Significantly reduce the time from discovery to clean up with retrospective security that constantly monitors for suspicious activities and conduct even following an initial inspection.
- Reduce administration and lessen difficulty with unified policies which protect across the whole attack scale.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10504

VI. ABOUT WEB APPLICATION FIREWALLS (WAFs)

The web application firewall is a dedicated firewall intended for filtering and controlling HTTP traffic through internet traffic between the web clients as well as application servers. Web application firewalls (WAFs) are an important component for strong application security. Traditional network firewalls (TNF) operate at a network and transport layer together with the supervision of packet and data transfers. WAF in comparison provides Layer 7 security, typically seated between a perimeter firewall as well as a web server or application server. In contrast to its predecessor, the enduring port-connected network firewall web application firewalls go a step further in providing security for the applications served through the internet [4].

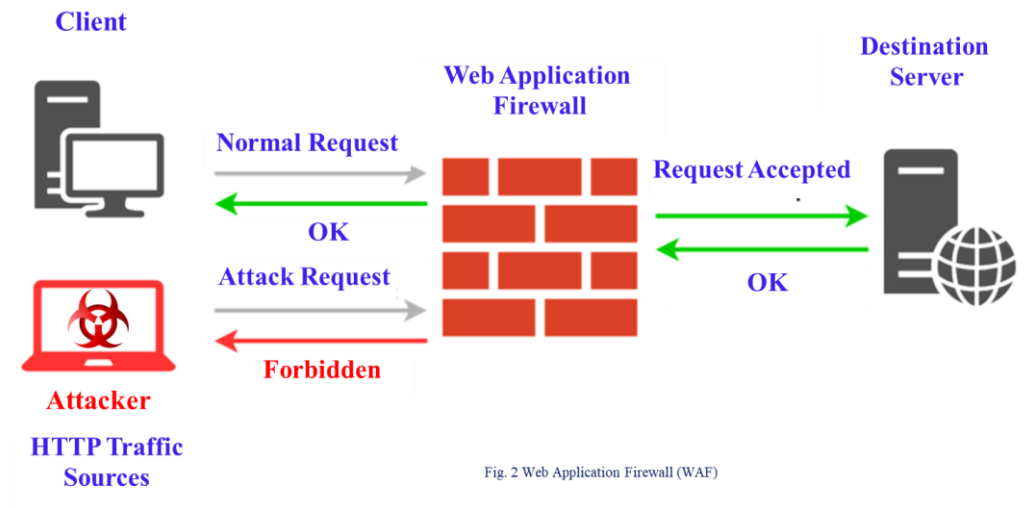


Fig. 2 Web Application Firewall (WAF)

While the proxy server protects the customer machine's identity through using the intermediary, a WAF is a kind of reverse-proxy, shielding the server from being exposed by requiring clients to go through the WAF before they reach the server. A WAF operates through a series of rules often referred to as policies. Such policies aim to safeguard against vulnerabilities in the application by way of filtering off malicious traffic [5]. The main task for WAFs is to safeguard particular applications from web-based attacks on the application level. Though, WAFs continue to insert advanced features such as threat intelligence, load balancing, intrusion prevention, and much more, so their function is expanding. At the same moment, WAF technology is becoming increasingly a part of more detailed security solutions such as next-generation firewalls (NGFW), unified threat management (UTM), and much more [4]. All these possible threats explain the need for committed Web Application Firewall technology [1]. In summary, WAFs close the protection gap left by conventional firewalls when tackling application security [4].

VII. THE FUNCTIONS OF WEB APPLICATION FIREWALL

A Web application Firewall (WAF) provides protection for your web apps by means of filtering, monitoring, as well as blocking every malicious HTTP/HTTPS traffic traveling to web-based applications and helps prevent unauthorized data from exiting the app [9]. This is done by complying with a set of policies that assist you in determining what traffic remains malicious and what traffic is secure [7,8]. Simply as a proxy server functions as an intermediary to safeguard the identity of a client, a Web application Firewall (WAF) operates in a similar manner but in the reverse is referred to as a reverse proxy which acts as an intermediary which protects the web app server from the potentially malicious client [8].

Web application firewalls (WAFs) may come in the form of software, an appliance, or provided as-a-service. Policies may be customized to meet the unique requirements of the web application or else a set of web applications. Though many WAF requires that you update the policies frequently to address new vulnerabilities, innovations in machine-learning enable several Web applications firewalls (WAF) to be automatically updated [7,8]. This automated system is becoming increasingly critical as the threat landscape continues to increase in complexity and uncertainty. (Fig, 3)

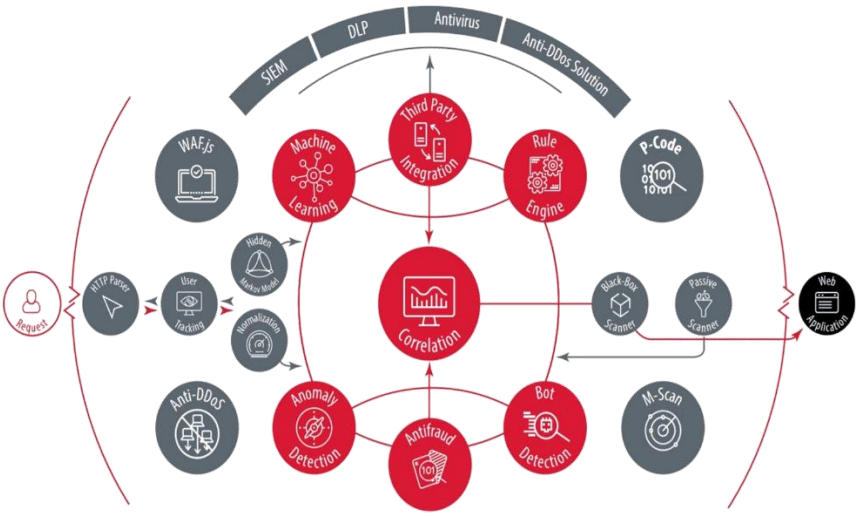
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10504



Source: Positive Technologies

Fig 3 Function of Web Application Firewall (WAF)

Fig. 3 Function of Web Application Firewall (WAF)

VIII. THE PREVENTION OF ATTACKS USING WAFS

Notably, Web Application Firewalls (WAFs) are designed to operate in combination with a comprehensive suite of security products such as traditional firewalls as well as intrusion prevention systems (IPS). At the same time, they are very effective at blocking certain kinds of attacks, they are not intended to protect against every threat. With this in mind, the most widespread cyber-attacks in applications that WAFs help to prevent [17].

SQL injection	Is a kind of attack that inserts an SQL query that enables the hackers to read confidential data, spoof identity, change the data, perform administrative tasks, and occasionally issue orders to the operating system.
Cross-site Scripting (XSS)	Is a kind of injection, wherein malicious scripts are injected into the trusted websites. The hackers send out malicious code, frequently browser-side script, to the end-user, if exposed, the user will have no method of understanding that the script should not be reliable and executes it. A malicious script can gain access to sensitive information or alter the content.
Application layer attacks or layer 7 (L7) DDoS attacks	layer 7 (L7) DDoS attacks related to a kind of malicious behavior intended to target the "highest" layer (7) in the OSI model in which common internet requests like HTTP GET as well as HTTP POST occur. Such layer 7 attacks, in contrast with network layer attacks like DNS Amplification, are especially effective owing to their use of server resources in addition to the network resources.
Web Scraping	Web scraping is a technique of obtaining certain information from the website, frequently using it for their own websites. A web application firewall(WAF) may prevent scripting or machines from obtaining data from a website.
Cookie Poisoning	Is a kind of cyberattack where the hackers manipulate a cookie that will be returned to a server. The modified cookie can be manipulated to bypass security or to steal confidential information.
Unvalidated input	Attackers alter HTTP requests (plus the URL, headers, and form fields) so that they can bypass the website's security methods.
Utilizing Buffer Overflow Vulnerabilities	A buffer overflow or a buffer overrun is a software coding error that happens when there is more data into a buffer than it can handle, which is causing the data to spill over into nearby storage. Buffer-overflow could create the entry point for cyber threats allowing a hacker to overwrite a portion of an application's memory.

Fig 4 The Prevention of Attacks using (WAFs)

Fig 4 The Prevention of Attacks using (WAFs)

IX. THE BENEFITS OF WEB APPLICATION FIREWALLS (WAFS)

The Web application firewalls offer a smart response based upon web security settings to prospective threats that might affect a network [9]. Web application firewalls are specifically designed. to help safeguard the network from potential threats that have not yet been discovered, which implies that executing this solution may save an organization from

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10504

zero-day threats, SQL injections, cross-site scripting attacks, security vulnerabilities, and other kinds of threats[10]. Properly formed wireless application firewalls also participate in mitigation actions in situations where the bot attacks or else unnecessary traffic incidents occur. WAF will maintain a clean application traffic flow while at the same time defending all any malicious data flows.

The following table gives a detailed overview of the functionality of each kind of firewall.

	Next-Generation Firewall (NGFW)	Web Application Firwall (WAF)
OSI Model Coverage	Layers 3-7	Layer 7
Typical Deployment	Gateway	Reverse proxy
Network Threat Protection	Yes	Yes HTTP(s) only
Restrict Traffic with Security Policies	Yes	Yes HTTP(s) only
Malware Prevention	with Integrate IDS/IPS	with Integrate IDS/IPS
DDos Protection	Layer 3 and 4 only	Layer 3 - 7 with CDN
Web Application Protection	Basic	Fully Supported
OWASP Top 10 Coverage	Basic	Fully Supported
Customisable web application rules	No	Yes Supported
Heuristics-based matching against web exploits	No	Yes Supported
Web application modelling for additional protection	No	Yes Supported

Fig 5 Functionality of each kind of firewall

X. THE MOST SUITABLE FIREWALL FOR AN ORGANIZATION

There is absolutely no universal solution that can satisfy the exceptional requirements for the security of each organization. Moreover, every one of the various types of firewalls has its own advantages and limitations. Packet filtering firewalls are basic but provide limited security, whilst stateful inspection, as well as proxy firewalls, may compromise network efficiency. Next-generation firewalls appear to be a full package, though not all organizations possess the budget or resources to set up and manage them successfully. As attacks are becoming more sophisticated, the organization's security defenses should catch up. One single firewall safeguarding the perimeter of the internal network from external threats will not be sufficient. Every asset in a private network requires its own individual protection as well. The best thing to do is to implement a layered approach to security rather than relying upon the capabilities of a particular firewall. There is no need to even agree on one when how to leverage the advantages of multiple firewalls with regard to an architecture enhanced particularly for an organization’s security needs [6].

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10504

XI. CONCLUSION

Bearing in mind the threats which corporate networks are facing today, it is quite clear that organizations want to reconsider their security methods. In summary, the next-generation firewalls remain capable of preventing many kinds of network threats to protect against unauthorized access and modification of the characteristics inside an organization's network. Earlier, regular network firewalls, as well as intrusion prevention systems, might have provided sufficient protection for the small number of web-based applications that the typical organization is considered to be significant. With the present significantly greater reliance on web attributes and the dramatic change by hackers toward aimed, application-specific attacks, though, this is no longer the case. Nevertheless, a Web application firewall offers a lot more comprehensive rules designed to block out web application layers and is an extremely suggested prerequisite if an organization wants to guarantee the security as well as reliability of their public-facing websites or web applications. This research paper provides a brief study about next-generation firewalls and web application firewalls. We are able to conclude by reviewing that Web Application Firewalls (WAFs) safeguard web applications, as well as Next-generation firewalls (NGFWs), protect networks. Organizations that depend on web-facing applications may benefit greatly from a WAF. For these clients, it is in most instances suggested to execute both solutions. Altogether, both kinds of firewalls will deliver an all-round defense against many of the most common threats on the internet today.

REFERENCES

[1]. Orange Cyberfefense- 07 Dec. 2017-https://orangecyberdefense.com/be/blog/infrastructure/waf-vs-ngfw/
[2]. https://www.zscaler.com/resources/security-terms-glossary/what-is-next-generation-firewall.
[3]. BANFFCYBER TECHNOLOGIES-Network-Firewalls-are-NOT-good-enough-to-secure-your-website.
[4]. Top Web Application Firewall (WAF) Vendors-Drew Robb-May 7, 2021.
[5]. CLOUDFLARE-https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/
[6]. Parallels-What Are the Basic Types of Firewalls- Giorgio Bonuccelli – November 4, 2020.
[7]. https://www.f5.com/services/resources/glossary/web-application-firewall
[8]. https://azure.microsoft.com/en-us/services/web-application-firewall/
[9]. POSITIVE TECHNOLOGIES- What is a web application firewall- May 28, 2019.
[10]. https://avinetworks.com/what-is-a-web-application-firewall/
[11]. XAAS JOURNAL-8 Types of Cyberattacks a Web Application Firewall (WAF) is Designed to Stop-Mike Monocello - March 5, 2019.
[12]. HP-NETWORKWORLD Custom Solution Group- White paper / Why you need a Next-Generation Firewall.
[13]. https://www.forcepoint.com/cyber-edu/firewall
[14]. TechTarget- SearchSecurity-Inbound vs. outbound firewall rules: What are the differences- by Kevin Beaver, Principle Logic, LLC.
[15]. netwrix blog-Network Security Devices You Need to Know About- Jeff Melnick – January 22, 2019.
[16]. https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html#~types-of-firewalls
[17]. https://www.researchgate.net/publication/350580133_Serverless_Computing_the_Next_Stage_in_Cloud_Computing's_Evolution_and_an_Empowerment_of_a_New_Generation_of_Developers