Firewalls: A study on Techniques, Security and Threats

Pooja Kaplesh[1] and Anjuli Goel[2]

[1]*Chandigarh University, Mohali*

[2] *Chandigarh University, Mohali*

Abstract

Information and excitement for computer system security is developing day by day along with its requirement. The interest is no uncertainty, due to the advancements with the extension of web services and due to the extension in the quantity of organizations that usually placing their deals and data channels on the internet or web. Web security has turned into a noteworthy issue in the present pattern of things. And it's like an evil which whenever left to spread will in a matter of seconds have consequences for every one of us. This paper hence analyzes web security with a glance at firewall and how it can help secure the system and web. A firewall is a piece of a computer or network system that is configured to prevent communication from unauthorized sources whereas allowing access from authorized sources. The techniques and kinds of firewalls are additionally talked about. The paper further examines firewall and how it can help in web security, business security and individual system security. It further discussed important considerations how a firewall can be selected, designed or configured. Finally threats to a firewall are also listed.

Keywords: *Web, Firewall, Security, Computer traffic, Network, Packet filters, Access control list, Threats*

1. Introduction

Security is the most essential perspective in a system. There are a ton of ideas for system security. Firewall is a standout amongst the most imperative ideas identified with the system security. A Firewall can be implemented as software or it can be a hardware that basically blocks unauthorized communication going out or coming to a network. Lots of softwares are available to provide security at system or network level. In same manner, firewall devices are also used for providing system security.

Firewalls are much of the time used to prevent unapproved internet users to get access to private systems connected with the Internet. All information that is coming and going outside the networks need to pass through the firewall, which analyze each and every packet and block those that don't meet the certain security policies. Generally, firewalls are configured to secure against unauthenticated intuitive logins from third party. This helps prevent hackers to log into computer system on your network. Additionally firewalls that are complex may block traffic from the outside to within, yet allow users within to communicate a little more freely with the outside.[2] Because of absence of absolute security schemes a network should be presently designed with multilayers so that it create a barrier against violating operations. Basic purpose of information security emphasis on protecting data or information that is saved

in computer systems, particularly on servers. Servers usually have number of security layers so as to ensure the security of information and data. The inner layer of network security is Access Right layer. The purpose of designing this layer is to control organizes assets (data) and rights (rights to client for assets access). This layer deals with allotments, organizers and records. The next to this layer(second) limits account makes it to count usernames and passwords (Password/Login) information. This is a normally employed technique of assurance because of its simplicity, directness, efficient and very strong. The administrator has obligation to control and deal with the operations of different users. The third outer layer used an information encryption technique called Data Encryption. Information is scrambled by using a specific algorithm such that even if someone tries to access information, won't be able to examine it without an encryption key. The outer or peripheral layer called Firewall avoids intrusions and filters unwanted outgoing or incoming information packets.

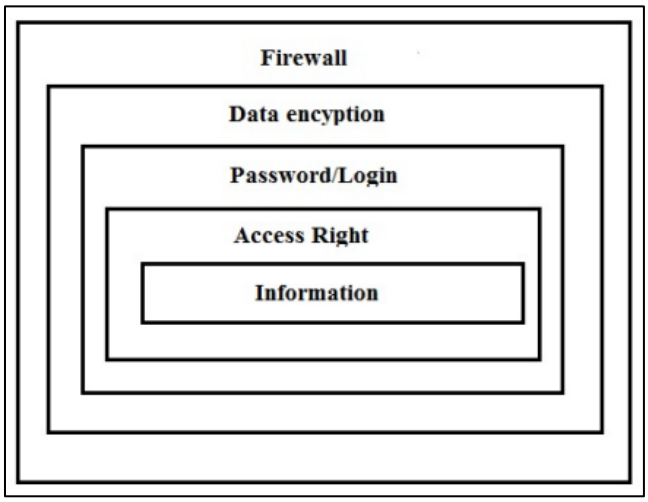

Figure 1: Network Security Levels[3]

2. Key Features of a firewall

Before learn about how a firewall functions, we have to comprehend what a firewall can and can't do. A wide range of a firewalls share some broad highlights and capacities to distinguish what a firewall can do. In fact a firewall must have these essential capacities:

- Control and arrange traffic
- Authentication access
- Protect organization assets
- Maintain and provide details regarding events
- Work as a mediator
- Protect network resources from the harmful actions while accessing internet.
- Assure protected and secure access to your internal assets to outside users
- May increase performance of network system.

A firewall is only an exterior layer of protection so it cannot do everything. It is just an artificial machine so it cannot categorize information as best or worst. It can just square traffic with simply characterized attributes. Additionally, a firewall cannot prevent an attack if that does not cross through it. Essentially it

does not prevent an information breach when data is duplicated. To wrap things up, a firewall cannot play a role of virus scanner because of its processing speed, the regular occurrences of viruses and data encryption to mask a virus. Despite that it is considered to be one of the most commonly used protection techniques todays. [3]

3. What Firewall Software Does

Firewalls act as a filter between a home network and the Internet. User can configure in its own way what information he wants to get away and what he wants to get inside. All the other stuff is not permitted. There are various different approaches or techniques firewalls use to filter traffic, and some of them are used together. These techniques function at various levels of a network, which decides how proper the filtering options can be at each level. Firewalls can be utilized in various techniques to provide security to your home network or business. [9]

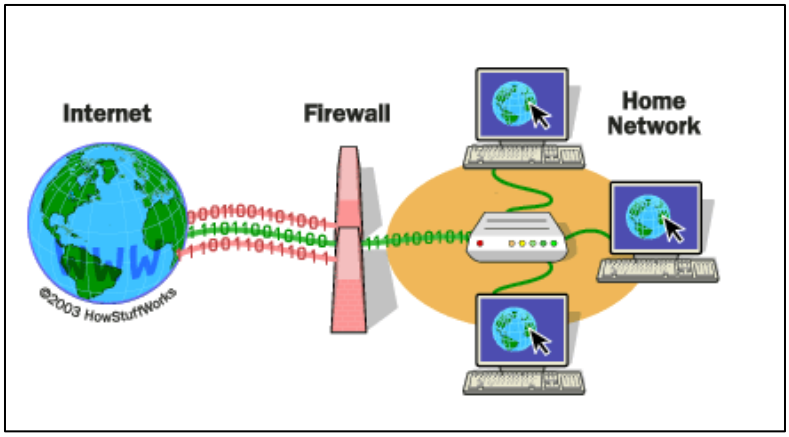

Figure 2. How Firewall works [9]

3.1 How do Firewalls secure Businesses?

- Huge organizations often use very complex firewalls set up to secure their network systems.
- Firewalls can be designed to prevent workers from sending particular kinds of messages or transmitting delicate information outside of the system.
- Firewalls can be configured to prevent access to specific websites (such as social networking websites).
- Firewalls can prevent access of outside PCs to get access to PCs inside the system.
- An organization can allot a single PC on the network for file/document transferring and rest of other PCs could be restricted.

3.2 Firewall for home or personal use

- The primary objective of a home firewall is to secure your own computer and private network(intranet) from malicious activities.
- Virus, a malware or malicious software, is the main threat to your home computer. It can be transmitted to your computer through email or other Internet services and can make a great deal

of harm to your files in no time. For example, Trojan horse programs and spyware are other malicious programs normally intended to gain your private information

- There are two different ways a Firewall can keep this from occurring. It can enable all traffic to go through except the information that meets a predefined set of rules, or it may also restrict all traffic unless it meets a predefined set of rules.[9]
- Example: *Comodo Firewall* meant to prevent malware from locating on your computer system.

3.3 What does a firewall NOT do?

Although a firewall manages traffic efficiently but still it does not provide full security and can make you fully safe on the internet. It is considered to be one of the first lines of defense, but all alone it will not secure you totally. This is the reason an internet security software packages includes several other parts of software also. A portion of the things a firewall does not secure you against are mentioned as follow:

- Viruses, worms and spam messages
- Wireless Network that is not configured well.
- Installation of malware software (secures you from spyware activities, but these activities may still be available in your PC)

4. Types of firewall techniques

Firewalls are regularly used to stay away from unlawful Internet clients from getting to individual systems that are connected to the Internet. There are a few firewall procedures and every firewall may utilize at least two than two methods in show. One of the significant problems that any organization encounters while tries to verify their sensitive information is finding the correct apparatuses for the activity. Even for a typical instrument, for example, a firewall, numerous organizations probably won't have an unmistakable thought of how to locate the correct firewall for their requirements, how to design those firewalls, or why such firewalls may be vital. The initial phase in finding the correct firewalls to ensure your organization's information is to comprehend what sort of firewalls there are. At this moment, there are five distinct sorts of firewall models, comprehensively:

1.) Packet-filtering firewall
2.) Stateful inspection firewalls
3.) Circuit-level gateways
4.) Proxy or Application-level gateways firewalls
5.) Next-generation firewalls

1.) Packet-filtering firewall

This technique is based on most fundamental and oldest type of firewall model. Packet-filtering firewalls essentially make a checkpoint at a traffic switch or router. The firewall directly check the information packets passing through router or switch for example, the source and destination IP address, packet number, port number, and other data without opening up the packet to investigate its information. It works on network layer of network model. This technique applies a lot of principles (in view of content of IP and transport header fields) on every packet and dependent on the result, chooses to either transfer or dispose of the packet. For instance, a rule could determine to hinder all

approaching traffic from a specific IP address or deny all traffic that utilizes UDP protocol. In the event that there is no match with any predefined rules, it will make default move. The default activity can be to 'dispose everything' or to 'acknowledge all packets'.

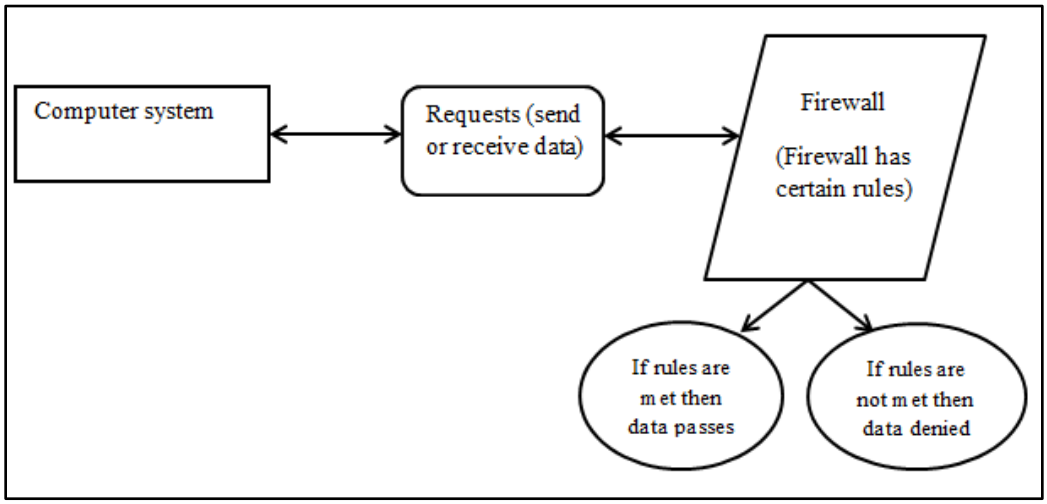

Figure 3. Packet-filtering firewall

Static versus Dynamic Filtering

In a static channel, every packet is freely assessed, with no reference to any first packet that may have gone in either route. A static channel may likewise be alluded to as a static NAT or detached screening firewall. The methods depicted here can give full straightforward redundancy and load sharing through firewalls that utilization static filtering or sifting.

In a dynamic channel, the choice on whether to pass a packet or parcel relies upon what packets have just experienced the firewall. Instances of dynamic channels incorporate stateful investigation and proxies. These channels screen the monitor of parcels, viably opening gaps in the firewall for every correspondence session on an as-required premise, (for example, when an inside client puts a demand for administration), and afterward close the gaps when they're never again required for approved traffic.

Security dangers to Packet Filters:

- **IP address Spoofing:** In this sort of assault, an interloper from the outside attempts to send a bundle towards the interior corporate system with the source IP address set equivalent to one of the IP address of inner clients.
  Aversion: Firewall can defeat this assault in the event that it disposes of the considerable number of packets that land at the approaching side of the firewall, with source IP equivalent to one of the inside IPs.
- **Source Routing Attacks:** In this sort of assault, the attacker or aggressor indicates the route to be taken by the packet with a want to trick the firewall.

Aversion: Firewall can crush this assault on the off chance that it disposes of the considerable number of packets that utilization the choice of source directing otherwise known as way tending to**.**

- **Minor Fragment Attacks:** Commonly, the measure of the IP packet is more prominent than the most extreme size permitted by the fundamental system, for example, Ethernet, Token Ring and so forth. In such cases, the packet should be divided, so it very well may be conveyed further. The assailant utilizes this normal for TCP/IP convention. In this sort of assault, the aggressor purposefully makes sections of the first packet and sends it to trick the firewall.

  Aversion: Firewall can defeat this assault in the event that it disposes of the considerable number of packets which utilize the TCP protocol and is divided. Dynamic Packet Filters permit incoming TCP packets only if they are responses to the outgoing TCP packets. [5]

Advantages of packet firewall:

- The beneficial thing about these firewalls is that they don't consume much resource. This implies they don't have large effect on system performance and are moderately simple.
- Low cost as few resources are utilized.
- These firewalls are also additionally easy to bypass than other firewalls with more powerful examination features.

Disadvantages of packet firewall:

- Subject to IP spoofing
- Does not have any knowledge about packet information hence provides low security.
- Examines IP and TCP headers as it operates only on network layer [4]

2.) **Stateful inspection firewalls:** This technique is also called 'Dynamic Packet Filtering'. Stateful firewall basically keeps track of the status of active links and uses this information to decide which packet should be allowed through it. In this approach, firewall keeps a record of dynamic TCP and UDP sessions information in tabular form including session's sender and recipient IP, port numbers, and also TCP sequence number. Records are made for only those UDP or TCP connections that fulfill characterized security criteria's; packets related with these sessions are allowed to go through the firewall. Sessions that don't coordinate with any policy are denied, similar to any packets got that don't coordinate a current table section.

Stateful inspection is more secure than packet filtering because it just permits information having a place with current session. For example, instead of allowing any host to send any kind of TCP traffic, it can verify the client when the session is built up, it can decide if the packets truly carry HTTP.

Advantages to Stateful Firewalls

- These can provide much more granularity in securing a system or network. Just by issuing a few straightforward checks to verify everything is ok, we can offload a lot of unnecessary work that our flow or stream based firewall would have needed to do.
- Stateful firewall is secured than packet filtering firewall.
- It has Logging and Tracking facilities.

Disadvantages to Stateful Firewalls

- Stateful Firewalls needs robust hardware system to perform high speed filtering which require more cost to implement.
- These firewalls do not use any client-server architecture.
- Packet screening is tricky and hard to manage in this technique.
- Due to costly hardware these firewalls have limited resources to filter traffic, so there could be a situation where it cannot advance traffic as it has exceeded the limit of the firewall's session table. [7]

3.) **Circuit-level gateway firewalls:** Circuit level firewalls are operated at the Session layer of the network model and they monitor TCP (three way handshake) connection to verify that a requested connection is authenticated or not. It goes about as a virtual association between the remote host and the inner clients by making another association among itself and the remote host. It additionally changes the source IP address in the parcel and puts its very own location at the spot of source IP address of the bundle from end clients. Thusly, the IP locations of the inner clients are concealed and verified from the outside world.

Advantage of Circuit-level gateway firewalls:

- Circuit level gateways are not much costly.
- These firewalls are resource-efficient.
- They are faster than application or proxy firewalls
- They can block the connections between users and secure the internal IP addresses

Disadvantage of Circuit-level gateway firewalls:

- These firewalls are not able to block TCP protocol and do not have mechanism to maintain good log record.
- They do not identify the protocols like HTTP and URL
- These firewalls do not filter the packet itself. So, a malicious packet, however, had the correct TCP handshake, will pass directly through. After making a Connection, an intruder may take benefit of accessing packet. This is the reason circuit-level gateway is not that much useful to protect your business from anyone else. [8]

4.) **Application gateways:** Application firewalls review network packets to check whether data is valid (at the application layer) before allow making a connection. It investigates the data encapsulated in all packets going through network and after that it provides complete connection state. These firewalls also validate other security information like user passwords and service requests. Application or proxy services are used for specific reason in order to control traffic such as FTP or HTTP. These services can provide increased access control , detailed checks needed for data validity, and they can generate summary report about the traffic to identify and track traffic
It is otherwise called Proxy server. It works as:
Step-1: User contacts the application door utilizing a TCP/IP application, for example, HTTP.
Step-2: The application door or gateway gets some information about the remote host with which the client needs to set up an connection or association. It likewise requests the client id and secret key that is required to get to the administrations of the application door.
Step-3: After confirming the genuineness of the client, the application door gets to the remote host for the benefit of the client to convey the packets.

Application level firewalls can also be implemented as Caching Servers which in way increase the network performance and makes it easier to track traffic.

Advantage of application-level gateway firewalls:

- It provides high level of security
- It has event and logging mechanism and can identify the protocols like HTTP and URL
- These firewall can do processing and manipulation on data packet.
- They have power to shield internal IP addresses
- They do not allow making a direct connection between endpoints.
- It has more control over traffic going through the firewall

Disadvantage of application -level gateway firewalls:

- This firewall is slower than packet filter firewall and stateful firewall.
- Some protocols for example SMTP or HTTP need own gateway proxy
- It may require extra client configuration information.
- It is expensive.

5.) **Next-generation firewalls:** A next-generation firewall is a network security device that provides capabilities beyond a traditional, stateful firewall. Some regular highlights of next-generation firewall architectures contains application awareness and control, deep-packet inspection (checking the genuine contents of the data packet), TCP handshake checks, and integrated intrusion prevention that automatically stop attacks against your network.

Anyway, which firewall design is the correct one for your business?

- The packet filter firewall or circuit-level firewall, which gives basic security that, has minimum performance impact.
- The stateful firewall structure that combines the abilities of both of the past two choices, but has a better performance impact.
- A proxy application firewall or next-generation firewall that provides better security in exchange for extra cost and considerably higher performance impact?

To give better insurance, your systems should have numerous layers of firewalls, both at the perimeter and separating different resources on your system. Having extra firewalls makes your system harder to break by making extra resistance top to bottom that secludes distinctive resources—influencing it so attackers to need to perform additional work to achieve the majority of your most delicate data. The specific firewalls that you will need to utilize will rely upon the abilities of your system, important consistence necessities for your industry, and the assets you have set up to deal with these firewalls.

5. Choosing and Configuring a Firewall

The Internet is a risky spot loaded up with a consistent blast of automated outputs that scrub the Internet for vulnerable targets. When distinguished, these vulnerable targets get diversity of attacks. A large number of the attackers have no clue that possesses the targets, and a definitive objective relies upon both the attacker and the kind of target. Choosing a suitable firewall shields your network system from the Internet and vice versa.[10]

5.1 Important points to consider while Selecting a Firewall

- **Network firewalls vs. desktop firewalls:** There are numerous desktop firewalls exist to secure your individual PCs for example, Zone Alarm. Although, to secure overall network system, you have to choose a network firewall device.
- **Software and hardware firewall:** With the use of software firewalls, you introduce the program over a current Windows or Linux server, which at that point turns into your devoted firewall. Some of the examples of software firewall are Microsoft ISA Server or Smoothwall. Hardware firewalls are devices with their own operating systems and dedicated hardware. These are designed by Linksys, Cisco, Netgear, Watchguard, and SonicWall. To secure your individual system, software firewall is enough but at network level, hardware firewall is required. For high security, You need to use both hardware as well as software firewall since hardware firewall protects your system only in a LAN or private network within an organization whereas software firewall protects the system outside the organization also.
- **Network size:** A firewall device should have sufficient processing power to deal with various connections with respect to size of your network.
- **Network topology:** The numbers of networks you have installed on your system need a level of protection. Suppose you have four networks, for example, one for the employees, one for the public access, and one for wireless access point and another for your servers. In this situation you require a firewall with four Ethernet ports and a port for your web connection. But the firewall you have selected has three ports then you could manage a second firewall or a managed switch to provide separation between these different kinds of subnetworks.
- **DMZ(demilitarized zone):** A DMZ is basically a small screened subnetwork for hosted Internet services(like Web servers, proxy servers and e-mail servers) that separates an internal organization network from other untrusted public networks, basically the internet. The firewall basically secures the servers in demilitarized zone and checks traffic going out and coming to the servers. There are many methods to configure a DMZ and even installing a DMZ may affect the type of firewall you have configured.
- **Content separating:** Check whether your security technique you are using, require some type of content filtering? A couple of few firewall organizations do offer such kind of service. Firewall may download a boycott of prohibited sites regularly. But, this service may cost additional.

5.2 Firewall Configuration: The following steps help to get the process involved in firewall implementation. This basically provides an overview to get you know the steps of firewall setup.

Step 1: Secure your firewall

In case the attackers gain access to your configured firewall itself then the overall network system will be insecure. Thus, it is a mandatory step to firstly secure your firewall device. The following points need to be considered:

- Always upgrade firewall devices to the most recent firmware version.
- Turn off, delete and rename default user accounts and modify all default passwords. Always try to use tricky or secure passwords only. Make a practice to change your passwords frequently and don't access shared user accounts.
- Deactivate simple network management protocol (SNMP) or design it to use a safe network.

Step 2: Create your firewall zones

So as to secure the valuable resources on any network, you must initially identify kind of assets or resources(like transaction card data and patient information). At that point, make a plan of your system structure with the goal that these benefits can be assembled together and put into systems or zones. For example, all servers that provide some of the services over the internet (like web services and email services etc.) should be placed into a dedicated zone(DMZ) that will allow limited incoming traffic from the internet .In the same way, servers that are accessed indirectly from the internet, for example database servers, could be placed in internal server zones. The more zones you create, the more secure your network. However, managing more zones needs extra time and resources, so be careful while selecting number of network zones you want to create.

Step 3: Set up access control lists

Since you have built up your system zones and appointed to interfaces, afterward you need to decide precisely which traffic should probably stream into and out of each zone. This incoming and outgoing traffic will be allowed utilizing firewall rules known as access control lists (ACLs) that are implemented on each and every interface on firewall. You need to ensure that ACLs implemented are specific to the definite source or destination IP addresses and also port numbers. Don't forget to set both inbound and outbound ACLs to each interface on firewall in order to ensure that only authorized traffic is passed into and out of each zone. Ensure that there is a "deny all" rule should be implemented to filter out all unauthorized traffic, at the end of each access control list.

Step 4: Set up your firewall services and logging

On the off chance that your firewall is likewise equipped for going about as a dynamic host setup convention (DHCP) server, organize time convention (NTP) server, interruption counteractive action framework (IPS), and so forth, at that point feel free to arrange the administrations that you want to utilize. Disable all the additional administrations that you never mean to utilize.

Step 5: Test your firewall setup

While testing, check that your firewall functions as expected. Remember to check that traffic will be blocking that should be blocked by access lists. When you ended with testing firewall, it should be prepared for production. Don't forget to maintain a backup of firewall setup so that information is not lost in case of any failure.

6. Threats to Firewall

- Even when a firewall is installed, and updated with latest vulnerability patches, still it can create problems if the firewall's configuration settings create conflicts. This may degrade performance and may fail to provide security on your company's network
- Less advanced firewalls may just check the packet's source of origin and destination before approving or denying a request therefore, it is easy for an attacker to get access on network's firewall.
- Default password creates every security problem imaginable, including accountability issues when network events occur.
- Firewalls can mitigate some types of DDoS attacks, they can still be overloaded by protocol attacks.
- Attackers can get access to the firewall though unencrypted HTTP connections, as this may be exploited by an outsider connecting to the same network, in case of an open wireless network.
- The host of software firewall should be updated on timely basis.

- Hardware firewalls are costly and hard to upgrade. [17]

7. Conclusion

As the Internet becomes more a part of business, firewalls are becoming an important element of an overall network security policy. It plays an important role in computer system security against viruses, spyware, Trojans and other malwares attacks from outside of network. A good firewall provides full security to our network and system without making any influence on the speed of computer system and network access. In order to provide security, one should always keep some points in mind: One should never install any software from suspected sources. Always download from the respected sites available on internet. Secure your firewall firstly and then use it to monitor all information that we want to transfer over the internet. On each PC a firewall software must be installed else it will to become infected and very fast it will impact all PCs connected to that network.

References

8.1 Journal Article

[1] Dr. Ajit singh, Madhu Pahal, Neeraj Goyat," A Review Paper On Firewall", School Of Engineering And Sciences, Bhagat Phool Singh Mahila Vishwavidyalaya Sonipat (Haryana),September **(2013).**
[2] S.C. Tharaka, R.L.C. Silva, S. Sharmila, S.U.I. Silva, K.L.D.N. Liyanage, A.A.T.K.K. Amarasinghe, D. Dhammearatchi," High Security Firewall: Prevent Unauthorized Access Using Firewall Technologies" International Journal of Scientific and Research Publications, Volume 6, Issue 4, April **(2016)**
[3] Binh Nguyen," Network Security and Firewall" Helsinki Metropolia University of Applied Sciences,April**(2016)**.
[4] Imran, Mohammad, Abdulrahman Algamdi, and Bilal Ahmad. "Role Of Firewall Technology In Network Security". International Journal of Innovations & Advancement in Computer Science **(2016)**
[5] FIREWALLS, available at: http://mercury.webster.edu/aleshunas/COSC%205130/Chapter-22.pdf
[6] Types of firewall and possible attacks,available at: https://www.geeksforgeeks.org/types-of-firewall-and-possible-attacks/
[7]Chris Roeckl Director, Corporate Marketing," Stateful Inspection Firewalls", available at: http://www.eircomictdirect.ie/docs/juniper/wp_firewall.pdf
[8] Firewalls and types, Cisco community, available at: https://community.cisco.com/t5/security-documents/firewall-and-types/ta-p/3112038
[9] How Firewall Works, Comodo Security Solutions, available at: https://www.comodo.com/resources/home/how-firewalls-work.php
[10] Selecting and Configuring a Firewall, techsoup for libraries, available at: http://www.techsoupforlibraries.org/planning-for-success/networking-and-security/selecting-and-configuring-a-firewall

[11] Saba Khan1 and Rakesh Gupta2," Future Aspect of Firewall in Internet Security" Department of Computer Science Engineering, Department of Electrical and Electronics Engineering Roorkee Engineering and Management Technology Institute Shamli, UP, India**(2013)**
[12] MacVittie, Lori. "The Application Delivery Firewall Paradigm". international journal of emerging trends & technology in computer science 6.4 (2013): 8. Print. February **(2016)**
[13]Configure firewall, Symantec, available at: https://support.symantec.com/en_US/article.HOWTO98492.html
[14] Aakanksha Chopra," Security Issues of Firewall", Assistant Professor (IT), Jagan Institute of Management Studies (JIMS), Rohini, New Delhi, February**(2016)**
[15] Richa Sharma and Chandresh Parekh," Firewalls: A Study and Its Classification", International Journal of Advanced Research in Computer Science, Volume 8, No. 4, May – **(June 2017)**
[16] Firewalls, Version 2 CSE IIT , Kharagpur, nptel available at: https://nptel.ac.in/courses/106105080/pdf/M8L3.pdf
[17] Ramandeep Kaur and AmritpalKaur, "SAFEGUARD OF SECURITY: FIREWALLS", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 3, March(**2017)**

[18] William Hugh Murray, "An Introduction to Internet Security and Firewall Policies" available at: http://www.ittoday.info/AIMS/DSM/82-10-16.pdf,

8.2 Book

[19] Brian Komar, Ronald Beekelaar, and Joern Wettern, PhD," Firewalls for Dummies 2nd edition", Wiley Publishing, Inc**(2003)**

8.3 Chapter in a Book

[20] Firewalls and Virtual Private Networks, available at: https://www.wiley.com/legacy/compbooks/press/0471348201_09.pdf