A Study on Firewall

Rohan Dhadge[1], Himabindu Kasireddi[2], Sakshee Thakare[3], Ananya Choudhary[4], Deepti Dave[5]
[1234]*U.G. Student, SOE, ADYPU, Lohegaon, Pune, Maharashtra, India*
[5]*Senior Faculty-IT, iNurture, Bangalore, India*

Abstract- Firewall in today's day have become integrated part of network line. It is also known as defense mechanism of any institute or organization. There are different types of firewall like Packet-Filtering firewall, Stateful Inspection firewall and many more. In this paper the authors have given their understanding of the various kinds of firewalls and a survey research in this field.

Keywords- Firewall, integrated, mechanism, packet-filtering, stateful, inspection.

I. INTRODUCTION

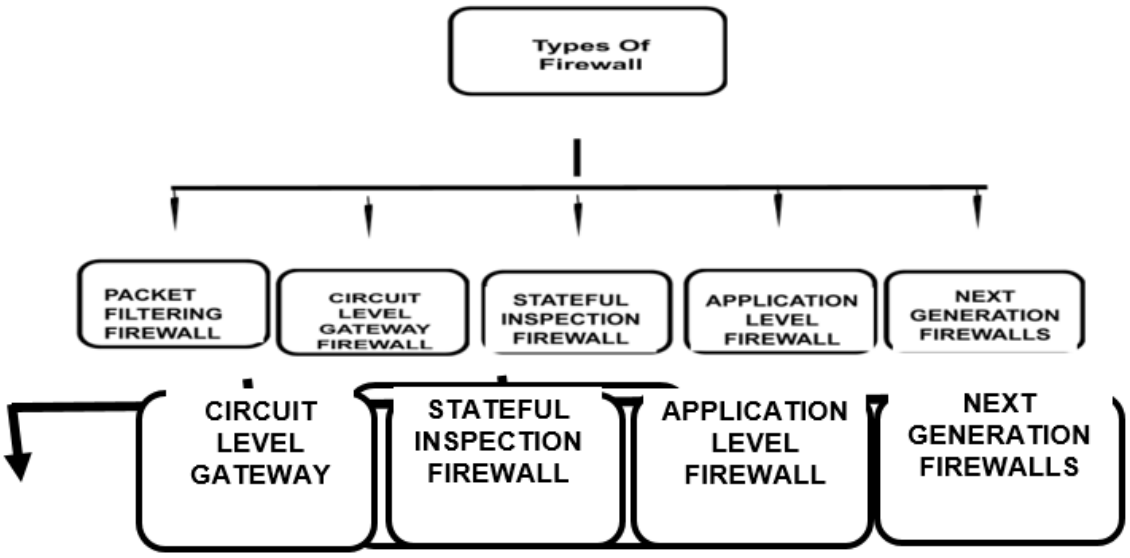
Firewalls safeguard a trusted network from an unsecured network (Figure 1 denotes firewall). They are classified in two types software or hardware based. Back in the day there were different firewall filtering policies designed to effectively keep away untrusted packets out of a network.

Even after a lot of developments have been put into designing efficient filters, vulnerabilities still exist and have been tampered by the malicious users in every possible way. Stateful firewalls are traditional and are used from long time. In fact, they are considered as the base of network security. But these firewalls are becoming less helpful in present days application as changing behavior of traffic in the network and increasing application layer attack.

Filtering a right package is becoming a challenge as almost all kinds of traffic can be tunneled through http. SQL injection tops the list of web-based vulnerabilities. Attacker with good knowledge about SQL can manipulate the query in a way that the web applications go undetected by the firewalls. As a solution on this issue, researchers have tried to apply different soft computing techniques.

In most of the existing firewalls today, with growth in the complexity of networks the list of firewalls policies are getting longer.

II. TYPES OF FIREWALL



A. PACKET FILTERING FIREWALL

This technique in firewall is used to monitor outgoing and incoming packages and control their transfer based on source and destination address, protocols and ports.

B. CIRCUIT LEVEL GATEWAY FIREWALL

This firewall quickly and easily approve or deny traffic without consuming significant computing resources, circuit-level gateways function by justifying the Transmission Control Protocol (TCP) handshake. This TCP handshake check is designed to make sure that the session the packet is from is legitimate. While extremely resource-efficient, these firewalls do not check the packet itself.

So, if a packet held malware, but had the right TCP handshake, it would pass right through. This is why circuit-level gateways are not enough to protect your business by

themselves.

C. STATEFUL INSPECTION FIREWALL

These type of firewalls successfully achieve both stages; Session filtering (TCP handshake) and data packet filtering.
That means they do the work of circuit-level as well as packet filtering firewalls. They observe all active connections and sessions and decide whether the given network packets should be allowed or not.

D. APPLICATION LEVEL FIREWALL

This type of firewall works on application level only.
That is, they only filter the packets or traffic related to the application or service for which they are sent. For example, A type of firewall for keeping an eye on the traffic to all web application a given network uses.

E. NEXT-GENERATION FIREWALLS

Some common features of next-generation firewall architectures include deep-packet inspection (checking the actual contents of the data packet), TCP handshake checks, and inspection of packet at surface-level. Next-generation firewalls may include other technologies as well, such as intrusion prevention systems (IPSs) that work to automatically stop attacks against your network.

III. ADVANTAGE OF FIREWALL

- Concentration of security; all software logging and functions is stored on firewall system to avoid unauthorized access
- Filtering the Protocol; The process where the protocols and services that are unnecessary or less secure are filtered by firewall.
- Hiding Information, A feature where the firewall hides important information like names of internal systems or e-mail addresses and hence revels less information to other hosts.
- Application Gateway; Here the firewalls requires any (inside or outside) user to login or connect to the firewall first before further connection and thus filters the protocol.
- Extended logging; Firewalls focuses on extended logging on a particular system.
- Centralized and a simple network service management. E-mail, ftp, gopher and other services are situated on firewall systems and cannot be maintained on too many systems at once.

IV. LIMITATIONS OF FIREWALL

- Firewall cannot secure itself by attacks that by-pass it.
- It also cannot guard itself against internal threats when an insider gives away confidential information to an outsider
- It could be incapable to protect itself from infected files and viruses since it is difficult to scan all traffic that is incoming.
- Difficult to integrate into a mesh network.

V. MANUFACTURERS OF FIREWALL HARDWARE/SOFTWARE

Software:

- Palo Alto
- Fortinet
- CISCO
- Juniper Technologies

Hardware:

- Checkpoint
- Sophos UTM
- pfSense
- Watch Guard XTM

VI. LITERATURE REVIEW

- Security is a very essential aspect in a network. There are a lot of concepts for network security. Firewall is one of the most crucial concepts related to the network security. The concept of “firewall” first came in use in 1764 which represents walls which separate the parts of the building that are likely to catch fire easily than the rest of the structure. Firewall can be both; software and hardware. Various software installation tools are available for security of network, similarly, there are different devices of firewall for network security.[1]
- Firewall represents a wall used to protect from fire. In the technical world, firewall refers to protection of network and blocks network traffic. It creates an obstruction between a secure and untrusted network and also secures confidential data. Protects the company from unethical use.[2]
- Computer networks are designed to connect a group of computers located at same or different corners in world. They are free to exchange information with any other computer. This kind of sharing is a great advantage for both individuals as well as for corporate world but as we know in today’s era, most important and confidential information is also exchanged on internet so attacker can do easily attack and can find out the important information and can harm the company in any manner.[3]
- The proposed research focuses on various technologies. packet filtering, Virtual Private Networks, Network Address Translation and firewall capacity. Firewall performance directly effects to network security and firewall performance depends on capacity of firewall. If firewall capacity high, it will give high performance. Therefore, research team selected firewall capacity for more secured network.[4]
- Computer networks are liable to attacks and it has wide range of attacks associated with it. There are chromatic types of internet attackers- un-ethical hackers, deceitful vendors or employees of an organization. It is not necessary that attacks always originated from extrinsic (external) parties but can also be caused by lack of intrinsic (internal) information security, and due to bad policies and procedures. To avoid the impact of internet attacks and the later consequences Distributed Firewall is

used.

- It protects by securing crucial network endpoints, exactly where unauthorized users want to get through. Filters traffic from internal as well as internet network. They overcome failure problem presented by firewall.[1]
- Firewall is an essential part of the computer against malwares, viruses, Trojan and spyware and malicious attacks from inside or outside of network. A good firewall protects network without affecting speed of the system[3]

VII. ANALYSIS

	Packet filtering firewall	**Stateful inspection firewalls**	**Circuit-level gateways**	**Application-level gateways**	**Next-gen firewalls**
Layer on which it operates	It uses network layer.	It uses network layer.	It is uses session layer.	It uses application layer	Depends on the basis of security. Mostly, application layer can be selected
How it works or methodology	It is used to monitor packets on the basis of Internet protocol addresses(IP), ports and other protocols.	It monitors TCP/IP handshaking between packets	It is advanced type of filtering of packet firewall. It keeps a record of all connections through a firewall.	It first establishes a connection to the source of the traffic and then inspects the incoming data packet	It includes deep-packet inspection, TCP handshake checks, inspection of packets at surface-level and intrusion prevention systems.
Content based filtering	Cannot be used for content-based filtering	Can be used for content-based filtering	Can be used for content-based filtering and also monitors "state" of a communication	Can be used for content-based filtering	Might Use content-based filtering to provide better security
Weakness	It cannot prevent application layer attacks and TCP/IP protocol attacks. It doesn't check the payloads.	The connection is vulnerable after it us established	It cannot inspect application layer traffic such as HTTP traffic	It is not compatible with all the network protocols	It cannot enforce policy of passwords or avoid wrong use of passwords.

VIII. CONCLUSION

As we have discussed so far that firewall is very important part of computer defense against viruses, spyware, Trojans and other malwares and also between direct malicious attacks from outside and outside. Such existing studies will be undertaken in near future. The paper gives an idea of the content based filtering of each and every type of firewalls.

IX. REFERENCE

[1]. International Journal of Scientific and Research Publications, Volume 6, Issue 4, April 2016 504 ISSN 2250-3153

[2]. International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 – 8616, Volume 4, Issue 12, December 2015

[3]. International journal for Research in applied science and engineering technology Vol. 1 Issue II, September 2013, ISSN: 2321-9653

[4]. International Journal of P2P Network Trends and Technology (IJPTT) – Volume 6 Issue 1 January to February 2016

[5]. Firewall Policy Modeling, Analysis and Simulation: a Survey, Vadim Zaliva, lord@crocodile.org, May 9, 2008

[6]. Critical Analysis on Web Application Firewall Solutions Abdul Razzaq, Ali Hur, Sidra Shahbaz, Muddassar Masood, H Farooq Ahmad
School of Electrical Engineering and Computer Science (SEECS) National University of Sciences and Technology, Islamabad, Pakistan @seecs.edu.pk