ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2017

SAFEGUARD OF SECURITY: FIREWALLS

*Ramandeep Kaur[1] AmritpalKaur[2]

MCA, Global Institutes Amritsar[1], India

Assistant Professor, GNDU, Regional Campus, Gurdaspur[2], India.

ripswarraich@yahoo.com[1]

Abstract: This article is based on network security and security issues. Day to day hackers and intruders are attacking on packets data with occurring disturbing traffic flood in source to destination way. Many techniques and types are helping us to secure our data from attackers. IP address, port number using in network security firewall for passing information on original server to clients. This paper will introduce various methods of network security using firewalls. The security that firewalls supply is only as superior as the strategy they are configured to realize.

KEYWORDS: Intruders, Proxy, Spam, Firewalls, Spoofing.

1. INTRODUCTION

A firewall is a network security wall that protects our data, information from unauthorized persons or an organisation. It is also control the network traffic where incoming and outgoing policies are passed out. The protection that firewalls provide is only as good as the policy they are configured to implement [1].The host operating system should be as secure as possible prior to installing the firewall software. This not only means knowing how the operating system was installed but also making sure that all of the security patches are applied and that unnecessary services and features are disabled or removed[2]. We called it a security wall because no unauthorized person can closed the wall without any request so; it can be hardware, software or both as shown in Figure 1.

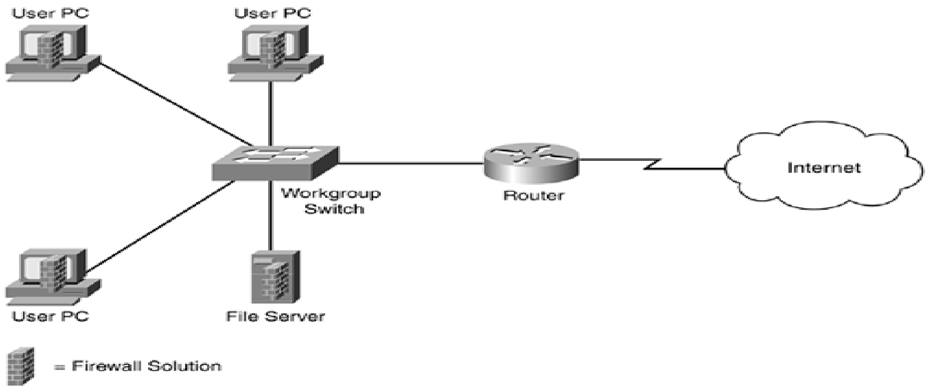


Figure 1: A Firewall securing all network devices.

1.1 Packet filtering firewall

The Packet Filtering Firewall is one of the most basic firewalls. The packet filtering firewall is sending information from source to destination with destination's IP address, source and destination post numbers, time range, protocol, type of service and various other parameters within the IP header. It works at the network level of the OSI model and the IP layer of IP/TCP model. It has set of rules to each incoming or outgoing packets. According to these set of rules the firewall can forwarded or drop the packet. It is also make use of current network routers. In the context of a TCP/IP network, a packet filter watches each individual IP datagram, decodes the header information of inbound and outbound traffic and then either blocks the datagram from passing or allows the datagram to pass based upon the contents of the source address, destination address, source port, destination port and/or connection status[3].

1.2 Circuit Level Gateway Firewall

This firewall is used to filter the conjunction of traffic between internal authorized host and external unauthorized host. A circuit-level gateway does not permit an end-to-end TCP connection [4]. It is also ensures the packets which are involved in establishing and maintaining the circuit or session between the two host is in proper manner. This type of firewall also works at network layer or session layer of OSI model. The connection is hence been established after that no further monitoring of packets are required. It is also provide more security than packet filtering firewall.

1.3 Stateful Inspection Firewall

In this type of firewall we can recognize a packet’s connection state or we also keep track of whether or not that packet is part of an established TCP session. A dynamic or "stateful" packet inspection firewall maintains a table of active TCP sessions and UDP "pseudo" sessions [5].It is also inspection the traffic of packets on the bases of state, port number and protocol. The stateful firewall is offers more security than packet filtering and circuit level gateway firewall. Permit of connections in this firewall also associated or satisfies with security policies so, the entries are only created on these connections as shown in Figure [2].

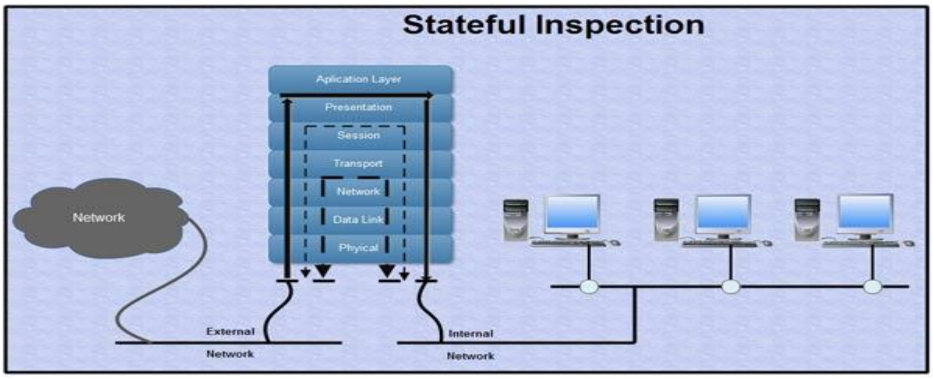


Figure 2: Process of stateful inspection firewall.

1.4 Proxy Firewall

Proxy firewall also called “application level gateways” because proxy firewall is a network security system that protects network resources by filtering messages at the application layer. In order to control risks when internal server allows connections from internet we use a technique called proxy [6]. Each layer performs a specific task on the information and passes it to the next layer. It is also help to describe the where function take place. It is also certain such HTTP our system against spam mail proxying on behalf of the internal mail server.

1.5 Hybrid Firewall

In the 21st century the development of telecommunications networks has taken giant leaps from circuit and packet switched networks towards all-IP based networks[7].It is a combination of packet filtering, proxy firewall and stateful inspection firewall and this type firewall is mostly used in modern firewall appliances for more better security.

2. EXTERNAL ATTACKS OF FIREWALL

Malicious intruders use literally hundreds of methods and tools when they attempt to compromise PCs. The following are some the most common attacks:

2.1 Network Traffic Flood

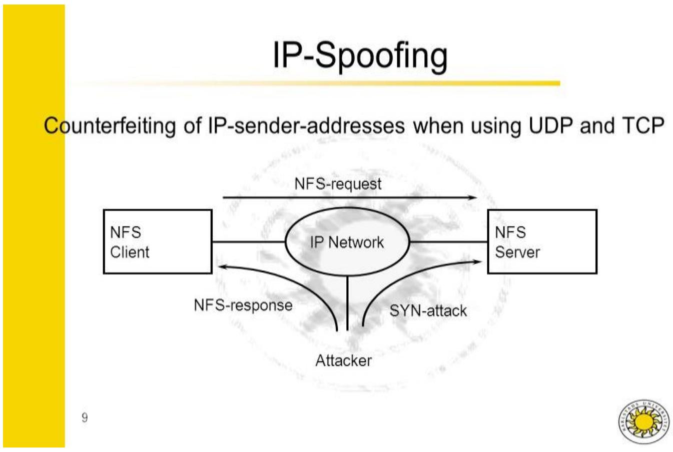
In this attack not only disturbs the normal operations of the network but also results in poor performance and system breakdown due to overwhelming requests. This is also called denial-of-service (DOS) attack. Use DoS attack identification and detection techniques to help differentiate between legitimate and malicious traffic [8]. In this attack where the perpetrator seeks to make a machine or network resource unavailable to its users by temporarily disrupting services of a host connected to the internet.

2.2 Port Scan

Every packet passes from source to destination with two different protocols that use ports TCP and UDP and both these protocols have 65,536 different ports. Intruders often scan victim computers to see which ports are active. After attackers or intruders identify the open ports, intruders narrow down future attacks to a particular port type. In other words a port san attack occurs when an attacker sends packets to our machine, varying the destination port and attacker can find out what services we are running and to get a pretty good idea if the operating system we have. In these days most internet sites get a dozen or more port scans per day or hours. Firewalls should notice this activity because it's unusual for a remote computer to connect to more than a few ports at one time. With so many different protocols and countless implementations of each for different platforms, the launch of an effective attack often begins with a separate process of identifying potential victims [9].

2.3 IP Spoofing

In this attack intruders gains unauthorized access to computer with the help of IP address of every system or that system. Attack can also modify the packet in this attack. In this IP spoofing attack intruders can also find out the workstation's place with IP address. Spoofing can be done when an attacker searches to be someone else in order gain access to restricted resources or steal information [10] as shown in Figure [3].



IP-Spoofing

Counterfeiting of IP-sender-addresses when using UDP and TCP

Figure 3: Working of IP spoofing.

Man-in-middle attack is also including in this IP spoofing attack because in MIMA modification of packet data is also possible.

2.4 Fragmentation Attacks

In this attack intruders breaking up the packet data into several small size so, this is a major problem because the important messages or data cannot pass out from source to destination in proper way. Fragmentation attack occurs when two fragments contained within the same IP datagram have offsets that overlap each other in the datagram [11].Sometime packets travel long distance from source to destination so different transmission media may have different constraints on the flow of information and in attacking time some size may be lost or modify and data will not arrival to the particular destination.

3. RECENT ADVACEMENTS IN FIREWALLS

With the fast progress of Internet, the backbone of Internet needs more powerful router with Gbps and even Tbps links. Thus, packet processing becomes the bottleneck of Internet backbone routers [12]. Wire speed packet input processing is not only meaningful for Internet backbone router, but also useful in layer 4/7 switch, high speed firewall and intrusion detection system. In this paper, the recent advance in the research of wire speed packet input processing is surveyed, and the key problems and solutions of wire speed packet input processing are analyzed in detail. Finally, some open problems are identified.

It seems every day another security vendor releases their version of the NextGen firewall. While Palo Alto Networks staked their claim to the NextGen firewall some time ago, everyone from Check Point to Fortinet has recently announced NextGen firewalls. [13]

FireMon recognized the value and power of these firewall advancements and has been a partner of Palo Alto for some time, focused on providing management for this new technology. While NextGen firewalls offer significant and important new capabilities to the firewall technology, the management problem remains. No matter how great the technology, if it is ineffectively managed, it will fail to solve the problem.

There are a couple key advancements in NextGen firewalls worth noting: user-based access policies and application intelligence. While most firewalls have provided user access control by requiring secondary authentication at the gateway, this was completely disjointed from the existing directory infrastructure and complicated to manage. As a result, it was not often implemented. NextGen firewalls, through directory integration, have the potential to change access management from IP-based to user or user group based access. This is a huge advancement, changing the paradigm of IP access control to user control. And in a world of mobile and wireless devices, this makes access control much more dynamic and effective security.

Application intelligence and the incorporation of that intelligence into the firewall policy helps address the reality of web applications and dynamic protocol / port use in malware and applications. Access policies can now be managed by application or application category. Not only does this address the desired control application use in the enterprise, it can help address malware that makes its way into the enterprise in any form (on USB drive, laptop, phone, etc). If the policy is effectively managed, malware that used to freely tunnel across open ports out of the network and potentially enable backdoor command and control capabilities will be denied, blocking a critical security issue.

But NextGen firewalls can’t solve the problem of poor management. Even these new capabilities don’t magically solve the management problem. In fact, in many ways, they create new problems in need of solutions. I am a big proponent of this advancement in firewall technology and we are excited to offer solutions to help address these new issues. Be on the lookout for a few posts addressing these issues and FireMon’s innovative solutions to help organizations manage the NextGen firewalls.

4. ADVANTAGES AND APPLICATIONS

- The software of firewall is free and easy to install.
- The hardware of firewall is fast and secure.
- The operating system of firewall is less prone for attacks so, this in turn reduces the security risk.
- The firewall controls the network access to one or more computers.
- The firewall is a wall to keep the intruders from attacking.
- The router is connected to the internal and our network; the routers are separate devices that protect our entire network.
- Firewall uses a variety of techniques to protect against the attacks such as proxy servers.
- The firewall protects your computer by acting as a gate through which both all the data must pass, It blocks certain kinds of traffic [14].
- Firewall mask our IP address, port number and limit traffic types and limit the connections to the trusted networks only.
- Firewall also helpful in OSI and IP/TCP model layers.
- Packets-data can securely and protected send from source to destination.

5. THREATS OF FIREWALL

- IN software of firewall has no centralized management.
- Software of firewall may be slow down applications as well as work also.
- The host of software firewall needs to be updated regularly and software is difficult to remove.
- Not suitable where response times are critical.
- The purchases of hardware firewall will be expensive and very hard to upgrade.
- Difficult to install and very completive involves wiring.

- The firewall may be difficult to use correctly especially for the new users.
- The maintaining of security at the machine level can be difficult.
- Difficult to find out packets and original data.
- When a firewall rule is modified, the service request number in the comment field of the rule is to be replaced, but within the service request itself, a comment that links back to the original service request is to be added. By following this process, all changes to the firewall, will be auditable back to their origin [15].
- There are no magic bullets and firewall is not an excuse to not implement software controls on internal networks or ignore host security on servers.

6. CONCLUSION

After all the illustrations of firewall network security, the security is very important and difficult topic.we have examined several Internet-centric firewall designs in an attempt to meet security and performance requirements of multitier applications [16]. The key, routers, threats for building a secure network is to define what security means to our organization. By deploying firewalls in series, we were able to significantly increase the difficulty of obtaining unauthorized access to sensitive resources from the network. The security tools, techniques and applications need to be woven in such a way that they produce positive sense of security amongst the security community. As a report of this research works the new approaches of network security is best suited integrated solution which ought to be deployed in research organization to learn more and more about further new attacks and will be sort every problem soon. In the types of network security firewall hybrid type is one of the best as compared to other types.

7. FUTURE SCOPE

In future this research will upgraded by new technology, each and every tool, hardware, software, routers, threads, address will become more secure from attacks will become more secure from attacks. Automated signature of intruders will be increased and deployed in an every organisation for external attacks. The firewall network security will become immune system this is fights off attacks. The security developments that are taking place within the same set of security technology that is being used today and tomorrow also with minor adjustments. This level of examination, often referred to as deep packet inspection, examines the actual payload of a packet and provides far better content-filtering capabilities than traditional packet-filtering firewalls [17].

8. REFRRENCES

1. A Wool, A quantitative study of firewall configuration errors. IEEE Computer Society 2004; 37:62-67.
2. D Daemon, W Abernathy, Essential Check Point FireWall-1 NG: An Installation, Configuration, and Troubleshooting Guide. Addison-Wesley Professional 2004.
3. S Dan, The Packet Filter: A Basic Network Security Tool. SANS Institute 2000 – 2002.
4. V Selvi, R Sankar et al. The Design and Implementation of On-Line Examination Using Firewall security. IOSR Journal of Computer Engineering 2014; 16:20-24.
5. R Chris, Stateful Inspection Firewalls. Juniper Networks 2004.
6. S Ajit, International Journal For Research In Applie Science And Engineering Technology 2013; 1.
7. K Amit, MC Maurya, Hybrid Intrusion Detection System. International Journal of Engineering and Advanced Technology (IJEAT).2013; 2:294-297.
8. C Mike how to prevent DoS attacks in the enterprise. University of Notre Dame.
9. BL Cynthia, R Chris, et al. Detection and Characterization of Port Scan Attacks. Department of Computer Science &Engineering University of California, San Diego.
10. SK Sanjay, S Rahul, et al. Security on Voice over Internet Protocol from Spoofing attacks. International Journal of Advanced Research in Computer and Communication Engineering 2012; 1:153-160.
11. MR Deepthi, Various Fragmentation attacks due to Manipulating IPv6 Extension Headers. International Journal of Research in Science & Engineering; 1:291-295.

12. LD Feng, Y Zhang, et al. Wire-Speed Packet Input Processing. Journal of Computer Research and Development 2002.
13. D Matt, Advancements of Next Generation Firewalls. Firewall Management FireMon Risk Analyser News.
14. S Heba, Software firewalls and hardware firewalls advantages and disadvantages. 2015.
15. C Maree, Improving Firewall Security post Acquisition. SANS Institute 2004 InfoSec Reading Room.
16. Z Lenny, Firewall Deployment for Multi-Tier Applications. 2002.
17. K Rohan, Application Firewall System. International Journal on Computer Science and Engineering 2016; 8:8-15.