Volume 8, No. 4, May – June 2017

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Firewalls: A Study and Its Classification

Richa Sharma
M.Tech, Raksha Shakti University
Gujarat, India

Chandresh Parekh
Assistant Professor,Raksha Shakti University
Gujarat, India

Abstract: In today's modern life the people are blessed with the best gift of the internet. Internet helps the netizens to do their work anywhere at any time, according to their comfortability. Bye the use of the internet the people are able to do various task like online net banking, e-business, online shopping, e-tendering, getting connected to different friends & family, online courses and many more. But with the increasing use of the internet, people started to spend more and more time using the internet and wasting their precious time by performing the unwanted activities like chatting, playing games, gambling and so on. And some person tries to learn new things which is harmful to the society like hacking and tries to execute those things in the network during their working hours. Moreover these days the hackers enters into the company's network and steal the important document or damages the network, thus that company suffers the heavy lose in terms of monetary as well as its market value. Due to this reasons there is a loss to the company and to the entrepreneurs. So to keep the watch on the employee and on their firm's network the company places the firewall. Firewall is one of the important network security perimeter know to everyone. It is one of the most essential section to provide security to both the world as well as the user a firewall is defined as the software and hardware or the combination of the both. It takes care of the incoming as well as the outgoing packets. The main aim of the firewall is to protect the users and keep watch on the activities of the users

Keywords: Firewall, PFSense, Logs, Security

1. INTRODUCTION

In the present world, the number of internet users are increasing per minute. According to the survey, the number of the internet users in the world in 2000 were 414794957 and in 2016 this number is increased to 3424971237. And this number is increasing at a very fast rate [9]. So as the number of the internet users is increasing the probability of the attacks caused by using internet is increasing by 30% every year. So the researchers had find a solution to prevent this kind of attacks to some extend by detecting the attack. Some of the tools which perform the above task are IDS/IPS tools like snort, nmap, honeypot, firewalls etc. The most of the organizations uses firewall to protect the cyber-attack which occurs due the network by which they are connected.

1.1 Firewall

A firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented as both hardware and software, or a combination of both.

But the problem arises when we don't know which firewall we have to use. So to solve this problem we are making a classification so that we can select which firewall we have use according to our utilization. [10] [11]

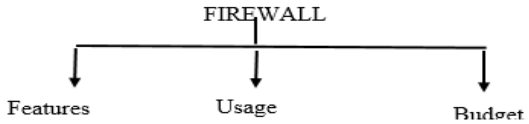

Fig 1: classification of firewall

- Based on Features
- Based on Usage
- Based on Budgets

1.1.1 Based on Features

1.1.1.1 Packet filtering firewalls

Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports. Network layer firewalls define packet filtering rule sets, which provide highly efficient security mechanisms. Packet filtering is also known as static filtering.

1.1.1.2 Circuit-level gateway

A circuit-level gateway is a type of firewall. Circuit-level gateways work at the sessionlayer of the OSImodel, or as a "shim-layer" between the applicationlayer and the transportlayer of the TCP/IP stack. They monitor TCP handshaking between packets to determine whether a requested session is legitimate. Information passed to a remote computer through a circuit-level gateway appears to have originated from the gateway. Circuit-level firewall applications represent the technology of next to first generation. Firewall technology supervises TCP handshaking among packets to confirm a session is genuine. Firewall traffic is clean based on particular session rules and may be controlled to acknowledged computers only. Circuit-level firewalls conceal the network itself from the external, which is helpful for interdicting access to impostors. But circuit-level firewalls do not clean entity packets. This is useful for hiding information about protected networks. Circuit-level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect. On the other hand, they do not filter individual packets.

1.1.1.3. Stateful inspection firewall

Stateful inspection has largely replaced an older technology, static packet filtering. In static packet filtering, only the headers of packets are checked -- which means that an attacker can sometimes get information through the firewall simply by indicating "reply" in the header. Stateful inspection, on the other hand, analyses packets down to the applicationlayer. By recording session information such as IP addresses and port numbers, a dynamic packet filter can implement a much tighter security posture than a static packet filter can. Stateful inspection monitors communications packets over a period of time and examines both incoming and outgoing packets. Outgoing packets that request specific types of incoming packets are tracked and only those incoming packets constituting a proper response are allowed through the firewall. In a firewall that uses stateful inspection, the network administrator can set the parameters to meet specific needs. In a typical network, ports are closed unless an incoming packet requests connection to a specific port and then only that port is opened. This practice prevents port scanning, a well-known hacking technique.

1.1.1.4. Application-level gateways (proxies)

An application gateway or application level gateway (ALG) is a firewall proxy which provides network security. It filters incoming node traffic to certain specifications which mean that only transmitted network application data is filtered. Such network applications include File Transfer Protocol (FTP), Telnet, Real Time Streaming Protocol (RTSP) and Bit Torrent. Application gateways provide high-level secure network system communication. For example, when a client requests access to server resources such as files, Web pages and databases, the client first connects with the proxy server, which then establishes a connection with the main server. The application gateway resides on the client and server firewall. The proxy server hides Internet Protocol (IP) addresses and other secure information on the client’s behalf. A computer’s internal system may communicate with an external computer using firewall protection. The application gateway and external computer function without client information or knowledge of the proxy server IP address.

1.1.1.5 Multilayer inspection firewall

The stateful multi-layer inspection (SMLI) firewall uses a sophisticated form of packet-filtering that examines all seven layers of the Open System Interconnection (OSI) model. Each packet is examined and compared against known states of friendly packets. While screening router firewalls only examine the packet header, SMLI firewalls examine the entire packet including the data.

1.1.1.6. Dynamic firewall

A dynamic packet filter is a firewall facility that can monitor the state of active connections and use this information to determine which network packets to allow through the firewall. By recording session information such as IPaddresses and port numbers, a dynamic packet filter can implement a much tighter security posture than a static packet filter.

1.1.2. Based on Usage

1.1.2.2. Software firewall

A Software Firewall is a piece of software that is installed on your computer in order to protect it from unauthorized access.

1.1.2.2. Hardware firewall

A Hardware Firewall is a device to which you connect your computers or network in order to protect them from unauthorized access.

1.1.3. Based on budgets

1.1.3.1. Commercial or paid firewall

A firewall which possess a fully fledge properties and any users can use it but they have to pay to use those services
Examples: cyberoam, SonicWALL-Dell

1.1.3.2. Free or open source firewall

The firewall which is available freely and can be used by anyone and anyone can modify the source code and even find bugs and report them
Example: IPFire, IPCop, PFSense, etc.
First and most important thing before starting my topic of dissertation, we have made a deep study on the different variety of firewall which are used most frequently. After studying about the different firewall we have gone through the different papers we have come to the problem which persist in the existing systems and tried to solve the problem found in the present system, which is explained in upcoming chapters.

2. LITERATURE REVIEW

The comparison between the commercial and the open source firewall. He had also discussed and focused on the different matters by which he could make out the difference between these two types of firewall. By this he have concluded that the proprietary firewall are better but he also said that the open source firewall can be made same as paid firewall by modifying the source code. [1]
In this paper, the authors have compressively studied the features of the open source firewall which could prevent the cyber-attacks which occurs on the open source firewall in which they have made some of the rules that would prevent the entry of the outsiders in the network. So that the malicious activities inside the network could be prevented [2]
In this paper the authors have concluded that for the specific instance a Linux firewall has superior transaction rate performance and application-level filtering capabilities. The Cisco 10s firewall is functionally superior for network level filtering, VPN capabilities due to IPSEC, integration with a heterogeneous multi-protocol environment, and scalable with support for PKI. We have also studied several Linux projects in experimental stages. Ultimately, the most effective firewall solution may be a combination of both application level and network level packet filtering. This experiment provides a basis for future experiments building toward general conclusions between open source implementations versus general commercial implementations. [3]
Successful promotion of a standard must balance the demands of adoption and appropriability. Achieving the widest

adoption of a standard attracts suppliers of complementary assets such as software and services, which in turn fuels further adoption (Shapiro and Varian 1999). This can be achieved by widespread technology licensing on favorable terms, but by doing so, the sponsor runs the risk of losing the ability to appropriate economic rents from the standard. [4]

We described that, all main security elements of the project that were effective for its success. As we see, almost all of them were well known open source software that can be applied instead of too many proprietary and commercial tools. No software cost, free available updates, source code availability, comprehensive documents and so many other features can be highly persuasive for entering open source world and utilizing its practical and helpful software. [5]

In this paper authors have implemented UTM on PFSense open source firewall and then they have worked on it as trial in organizations. [6]

In this paper author had defined Network's security tool was the beginning with the something that can protect the internal network from the external accessing. So, firewall is a best perimeter defense which it develops to provide the protection on the network's traffic. Firewall system had involved in network's environment over the years from the simple method with only packets filtering to the sophisticated packet inspectors which can decide to allow or block the traffic depending on the its purpose, sources and destinations . A dynamic inspection packet method is the best technology among the others firewall's technologies. It is a good or complete firewall system for network's traffic protection. [7]

In this paper the author have explained the various shortcomings of the firewall like [8]

- It is unable to destroy the attack source
- It can't resist virus attack
- It can't resist internal attacks
- Own vulnerability
- The response of useful services
- And the future development trends of firewall
- Development trend of packet filtering technology
- Multistage filtering technology
- Antivirus function of firewall

From the literature review we have seen that the various companies are using open source firewall. The list of open source firewall are as follows [12] [13] [14].

- Untangle
- PFSense
- IPFire
- IPCop
- VyOS
- Smoothwall
- Endian
- ClearOS
- Zentyal
- IPtables
- UFW
- Vuurmuur
- ConfigServer Security firewall

3. PFSense

After the detailed study we have found that the PFSense firewall is most widely used due to its following advantages and features

PFSense is another Open Source and a very reliable firewall for FreeBSD servers. It is based on the concept of Stateful Packet filtering. It offers wide ranges of feature which is normally available on expensive commercial firewalls only.

Features [15]:

- Highly configurable and upgraded from its Web – based interface.
- Can be deployed as a perimeter firewall, router, and DHCP & DNS server.
- Configured as wireless access point and a VPN endpoint.
- Traffic shaping and Real Time information about the server.
- Inbound and Outbound load balancing.

Advantages:

- 64 bit version available.
- Most features-rich free firewall.
- Solid performance and stability.
- Lime and nimble—much faster boot-up/shutdown than Untangle.
- Has a vast following, so the documentation and forums helped me get my heard.

Limitations of PFSense from Security Perspectives

- PPTP / GRE Limitation - The state tracking code in pf for the GRE protocol can only track a single session per public IP per external server. This means if you use PPTP
- VPN connections, only one internal machine can connect simultaneously to a PPTP server on the Internet. A thousand machines can connect simultaneously to a thousand different PPTP servers, but only one simultaneously to a single server. The only available work around is to use multiple public IPs on your firewall, one per client, or to use multiple public IPs on the external PPTP server. This is not a problem with other types of VPN connections. PPTP is insecure and should no longer be used.
- Only works with static public IPs, does not work with stateful failover using DHCP, PPPoE, or PPTP type WANs.
- "Reverse" portal, i.e. capturing traffic originating from the Internet and entering your network, is not possible. Only entire IP and MAC addresses can be excluded from the portal, not individual protocols and ports.
- limited free support, no update schedule and limited safety net
- URL logging: full logs of web URL visited by the user is not obtained & the obtained URL is ip based not user based.

4. LIMITATION OF SYSTEM

From the limitations of the firewall we have seen the limitations of the URL logging. We have seen how any user can login through firewall to access the internet for its work. Consider a scenario where the employee has just login its credentials and he/she is enjoying the internet services but due to some reasons like power loss, accidental removal of LAN cable/Ethernet cable from the system, or he/she has just log out from the services of using internet accidentally. In such cases, the complication arises. The complications or the problem that we found in any of the open source firewall is that if any such situation arises, as the user login using its credentials the ip address of the user is stored in the firewall and the logs are generated with reference to their ip address. If the above situation arises the ip allocated to the user will return back to the pool of ip. Then the user will try to login again by providing their credentials. In such cases, the same or different ip will be allocated to the existing user. If the same ip is allocated to the user then the situation is fine. But if the different ip is allocated then the previous ip will be allocated to different user in the LAN network. As we all know that all the open source firewall provides the ip based logs. So the firewall won't be able to differentiate the actual user by taking ip into consideration. So to solve this complication/problem the logs obtained by the firewall should also have the ip address. So that if any illegal issue comes into the picture then the legal person would be able to find the culprit.

As we know that the all the open source firewall gives ip based logs. But our aim is to get the logs based on ip address allotted to the user as well with its username name that time slot. So to achieve our aim we have develop a module which would give us the username and its ip address which is allotted to the user at login time. Let us understand this briefly.

5. PROPOSED SYSTEM

From figure 2, it is clear that when any user provides its authenticated credentials to the firewall to access the internet, in case 1 when module is not present the logs would be generated ip based but in case 2 when module is present the logs generated would have both ip address and user name simultaneously.

Now the question arises what is in this module which would give this username and ip address of the user simultaneously?
The answer to this question is that his module comprises of 2-3 logical scripts written in different programming languages. The programming language used to prepare this module are xml, php and .cfg. Now let understand how this module works. As shown in figure 2, its gives use a brief idea that how this module is going work. At very first instance we have fetch the credentials and ip address of the user. Now the username from the credentials and the ip address would be fetched and written in xml program. Now at this stage our module main programming will start which is written in php language which would be continuously fetching the username and ip address dynamically from the xml file and this data would be written in .cfg file of PFSense. The reason we have chosen the .cfg file in the firewall is that it is the main base for getting URL based logs in the firewall it is designed by the developers if any changes are made in the .cfg file the firewall would stop even generating ip based logs.

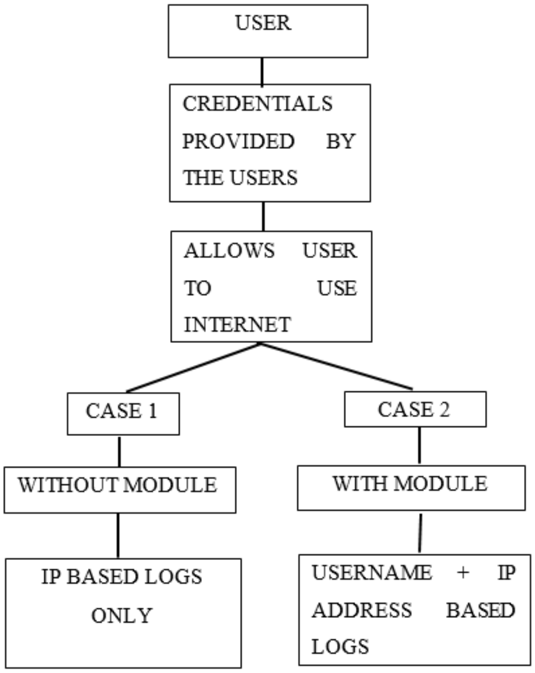
USER
CREDENTIALS PROVIDED BY THE USERS
ALLOWS USER TO USE INTERNET
CASE 1
CASE 2
WITHOUT MODULE
WITH MODULE
IP BASED LOGS ONLY
USERNAME + IP ADDRESS BASED LOGS

Fig 2: work of the module

Figure 3 shows can we implement the module

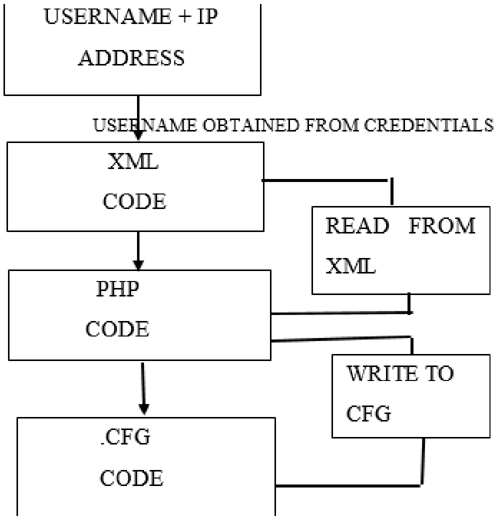

Fig 3: Implementation of the module

6. REFERENCES

1. Lamastra, Cristina Rossi. "Software innovativeness. A comparison between proprietary and Free/Open Source solutions offered by Italian SMEs." R&D Management 39.2 (2009): 153-69. Web.
2. Fuertes, Walter; Zambrano, Patricio; Sánchez, Marco; Santillán, Mónica; Villacís, César, Repowering an Open Source Firewall Based on a Quantitative Evaluation; et al. International Journal of Computer Science and Network Security (IJCSNS); Seoul 14.11 (Nov 2014): 118-125.
3. Patton, S., D. Doss, and W. Yurcik. "Open source versus commercial firewalls: functional comparison." Proceedings 25th

Annual IEEE Conference on Local Computer Networks. LCN 2000 (n.d.): n. page Web.

4. Joel West and Jason Dedrick, “Open Source Standardization: The Rise of Linux in the Network Era,” Knowledge, Technology & Policy, 14, 2 (Summer 2001): 88-112
5. S. D. Sajjadi Torshizi, S. Rostampour and M. Tanha, "New secure and low-cost design for defense in depth implementation using open source software," *2011 IEEE Student Conference on Research and Development*, Cyberjaya, 2011, pp.448-453.
6. V. Asghari, S. Amiri and S. Amiri, "Implementing UTM based on PFSense platform," *2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI)*, Tehran, 2015, pp. 1150-1152. doi: 10.1109/KBEI.2015.7436210.
7. Firkhan Ali Bin Hamid Ali, "A study of technology in firewall system," *2011 IEEE Symposium on Business, Engineering and Industrial Applications (ISBEIA)*, Langkawi, 2011, pp. 232-236. doi: 10.1109/ISBEIA.2011.6088813
8. H. Mao, L. Zhu and M. Li, "Current State and Future Development Trend of Firewall Technology," *2012 8th International Conference on Wireless Communications, Networking and Mobile Computing*, Shanghai, China, 2012, pp. 1-4.
9. "Internet Users." Number of Internet Users (2016) - Internet Live Stats. N.p., n.d. Web. 06 May 2017.
10. “Firewall Classification” N.p., 2017. Web. 6 May 2017.
11. Subramanian, Karun. "Firewall Classifications And Architectures". *Karunsubramanian.com*. N.p., 2017. Web. 6 May 2017.
12. Shah, Palak. "Top 10 Effective And Efficient Open Source Firewalls - Open Source For You". Open Source For You. N.p., 2017. Web. 6 May 2017.
13. "The Hunt For The Ultimate Free Open Source Firewall Distro". Mondaiji Dot Com. N.p., 2017. Web. 6 May 2017.
14. Shrivastava, Tarunika, and View Posts. "10 Useful Open Source Security Firewalls For Linux Systems". Tecmint.com. N.p., 2017. Web. 6 May 2017.
15. "Features List - Pfsensedocs". Doc.pfsense.org. N.p., 2017. Web. 6 May 2017.