Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.841 – 846

RESEARCH ARTICLE

ANALYSIS OF FIREWALL TECHNOLOGY IN COMPUTER NETWORK SECURITY

Miss. Shwetambari G. Pundkar[1], Prof. Dr. G. R. Bamnote[2]

[1]Department of Computer Science and Engineering, Sant Gadge Baba Amravati University, India
[2]Department of Computer Science and Engineering, Sant Gadge Baba Amravati University, India

[1] shwetapundkar@gmail.com; [2] grbamnote@rediffmail.com

Abstract— In computer security, a firewall is a device that blocks illegal access to an organization's network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls frequently used to prevent illegal internet users from accessing private networks connected to the Internet, especially intranets. In computer networking the term firewall is not only expressive of a general idea. It has come to mean some very accurate things. The firewall keeps track of every file entering or leaving the network in order to detect the source of viruses and other problems that might enter the network. This paper explores analysis of Firewall technology.

Keywords— Firewall Testing, Security Consideration, Firewall Terminology, Firewall Technology Overview

I. INTRODUCTION

Over the last few years, security threats to company have grown and changed significantly and so have the defences. Usual firewalls installed before 2005 are often not the best matched for existing threats and cannot defend against a number of newer threats. Computer security is a unbreakable problem. Security on networked computers is much also unbreakable. But if the machine is connected to a network, the situation is much hard. The network security is in the network information security [1]. The network security is one involves the computer science, the networking, the communication, the code word technology, the information security technology, the theory of numbers, the information theory of numbers, the information theory and so on many kinds of information. For example, an administrator may open a hole in a firewall to complete some task, but in doing so enable attackers to enter through the firewall. Do to this computer security can be in very bad condition. A firewall is a hardware or software system that prevents unauthorized access to or from a network [2] [3]. They can be implemented in hardware and software, or a arrangement of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet. Firewalls are computer security systems that protect your office/home PCs or your network from intruders, hackers & malicious code. Firewalls provide you with the necessary safety and protection. Firewalls are software programs

or hardware devices that filter the traffic that flows into PC or your network through a internet connection. They sift through the data flow & block that which they deem harmful to your network or computer system. When connected to the internet, even a separate PC or networks of interconnected computers make simple targets for malicious software & hackers. A firewall can offer the security that makes you less vulnerable and also protect your data from being compromised or your computers being taken hostage. Firewalls make it possible to filter the incoming and outgoing traffic that flows through a system [1] [4]. A firewall can use one or more sets of "rules" to inspect network packets as they come in or go out of network connections and either allows the traffic through or blocks it. The rules of a firewall can inspect one or more characteristics of the packets such as the protocol type, source or destination host address, and source or destination port. It can improve the security of a network. They can be used to do one or more of the following. Guard and padding is the applications, services, and machines of an interior network from unwanted traffic of data from the public Internet. Limit or disable access from hosts of the internal network to services of the public Internet. Support network address translation, which allows an internal network to use private IP addresses and share a single connection to the public Internet using either a single IP address or a shared pool of automatically assigned public addresses [1]. The paper is organised as above in Section 1 Introduction about Firewall Technology, Section 2 describe Working of Firewall, Section 3describe Firewall Technology Overview, section 4 describe Firewall Testing, Section 5 describe Firewall Terminology, Section 6 describe Security Consideration, Section 7 describe Firewall Characteristics and finally we conclude with section 8.

II. WORKING OF FIREWALL IN OUR PC

There are various different methods firewalls use to filter out data, and some are used in combination. These methods work at dissimilar layers of a network, which determines how specific the filtering options can be used. Firewalls can be used in a number of ways to add protection to your home or business. Large organization or corporations often have very complex firewalls in place to secure their networks. On the other side, firewalls can be configured to avoid employees from sending certain types of mails or transmitting confidence data outside of the network. On the inbound side, firewalls can be programmed to stop access to certain websites like social networking sites. Moreover, firewalls can prevent outside computers from accessing computers inside the network. A company might choose to select a single computer on the network for file sharing and all other computers could be controlled. There is no limit to the variety of configurations that are possible when using firewalls.

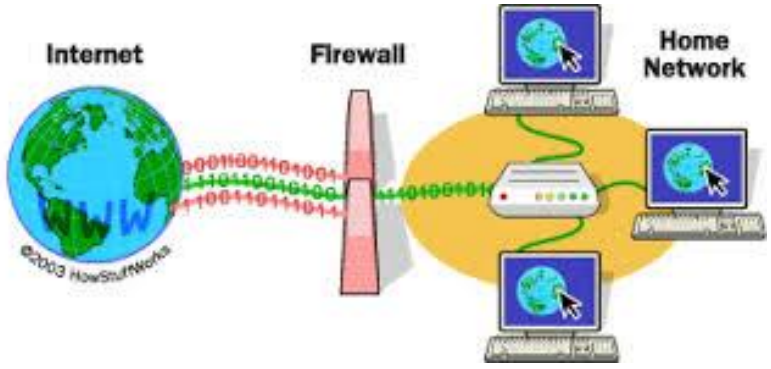

Fig 1. Working of Firewall

For residence use, firewalls work much more basically .The main goal of a standalone firewall is to protect your personal computer and private network from various threads. Malware, malicious software, is the main threat to your home computer. Viruses are the first type of malware that comes to mind. A virus can be transmitted to your system through email or over the Internet and can quickly cause a lot of injure to your files. There are two ways a Firewall can prevent this from occurrence. It can allow all interchange to pass through except data that meets a preset set of criteria.

Firewall uses the later way to prevent malware from installing on your computer. This free software firewall, from a global security solutions provider and certification power, uses the patent pending "Clean PC Mode" to disallow any applications from being installed on your computer unless it meets one of two criteria. Those criteria are as follow a) the user gives authorization for the installation and b) the application is on a widespread list of standard applications provided by this firewall. With this feature, you don't have to worry about unauthorized programs installing on your computer without your awareness.

This firewall is rated as a top firewall suggested for both basic and complex users. It has a number of exclusive features including "Defense +," a complex Host interruption Prevention System which is also known as HIPS, which prevents changes to critical system resources. This software is greatly customizable, so that you can

regulate it to suit your exact needs. This Internet Security Suite combines the award-winning firewall with a controlling antivirus to secure millions of computers around the world free.

A. Firewall technology overview

A firewall does the selection that is less suitable for a router to do. A router's primary function is addressing, whereas a firewall's primary role is filtering. Firewalls can also do auditing. Even more important, firewalls can look at an entire packet's contents, including the data area, whereas a router is worried only with source and destination MAC and IP addresses [6]. Three main types of firewalls are in common use today: packet filters, application gateways, and stateful inspection firewalls. They are described in the following sections.

1) Packet Filters:

A packet filter is the simplest form of firewall. A packet filter firewall will evaluate any IP packet that attempts to traverse the firewall against its access control list. If the packet is certified, it is sent from first to last. If not, the packet filter can either without a sound drop the packet or sends back an ICMP error response. Packet filters only look at five things: the source and destination IP addresses, the source and destination ports, and the protocol such as UDP, TCP/IP, and so on. These tests are very fast because each packet contains all the data in the packet headers which is necessary to make its willpower. Due to its simplicity and speed, a packet filter can be enabling on your routers, eliminating the need for a dedicated firewall. One problem with packet filters is that they generally do not look extremely enough into the packet to have any idea what is essentially being sent in the packet [2]. Though you might have configured a packet filter to allow accessing the port 25, the Simple Mail Transfer Protocol (SMTP) port, a packet filter would never know if some other protocol was used on that port. For example, a user on one system might run his Secure Shell daemon on that port, knowing that the traffic would be allowed by the packet filter, and be able to SSH through the firewall against plan. Another problem with packet filters is that they are not successfully able to handle protocols that rely on various dynamic connections [3]. The FTP protocol, for example, opens a command channel on which the multiple commands are sent. Whenever data is transferred between the hosts, such as files or the LIST output, a separate connection is established. You would need to have an ACL that would allow these data associations through for FTP to work. However, packet filters do not read the FTP command channel to know when such an ACL should be allowed [2].

2) Application Gateways:

An application gateway goes one step beyond a packet filter. Instead of simply checking the IP parameters, it actually looks at the application layer data. Single application gateways are often called proxies, such as an SMTP proxy that understand the SMTP protocol. These check the data that is being sent and authenticate that the particular protocol is being used perfectly. Let's say we were create an SMTP application gateway. It would need to keep track of the state of the link: Has the client sent a HELO/ELHO request? Has it sent a MAIL FROM before attempting to send a DATA request? As long as the protocol is obeyed, the proxy will shuttle the commands from the client to the server. The application gateway must understand the protocol and process both sides of the conversation [7]. As such, it is a much more CPU exhaustive process than a simple packet filter. However, this also lends it a larger element of security. You will not be able to run the earlier described SSH-over-port-25 trick when an application gateway is in the way because it will realize that SMTP is not in use. Furthermore, because an application gateway understands the protocols in use, it is able to support difficult protocols such as FTP that create casual data channels for each file transfer [8]. As it reads the FTP command channel, it will make out the data channel declaration and allow the specified port to traverse the firewall only until the data transfer is complete. Often there is a protocol that is not directly understood by your application gateway but that must be allowed to traverse the firewall. SSH and HTTPS are two effortless examples. Because they are encrypted end to end, an application gateway cannot read the traffic actually being sent [9]. In these cases, there is usually a way to configure your firewall to allow the appropriate packets to be sent without invasion by the firewall. It can be difficult to put together application gateways into your standard routing hardware due to the processing overhead [10]. Some newer high-end routers are able to function as application gateways, but you'll need plenty of CPU power for satisfactory presentation.

3) Stateful Inspection:

In computing, a this firewall is a firewall that keeps track of the state of network associations (such as TCP streams, UDP communication) travelling across it. The firewall is programmed to differentiate legal packets for different types of connections. Only packets matching is an active connection will be allowed by the firewall; others will be rejected it inspection, also referred to as Dynamic Packet Filtering, is a security feature. Check Point Software introduced this inspection in the use of its Firewall 1 in 1994. this firewall assessment

takes the basic ethics of packet filtering and adds the concept, so that the Firewall considers the packets in the context of before packets. So for example, it records when it sees a packet in an internal table and in many execution will only allow TCP packets that match an existing conversation to be forwarded to the network [3]. This has a number of advantages over simpler packet filtering: It is possible to build up firewall rules for protocols which cannot be correctly controlled by packet filtering. There is a risk that vulnerabilities in individual protocol decoders could permit an attacker to gain control over the firewall. This worry highlights the need to keep firewall software updated. Some of these firewalls also increase the possibility that personally hosts can be trick into solicit outside connections. This option can only be totally eliminated by auditing the host software. Some firewalls can be conquered in this way by simply screening a web page. More complete control of traffic is possible [6]. Equally, there are some disadvantages to this assessment solution, in that the execution is automatically more complex and therefore more likely to be errors [8]. It also requires a device with more memory and a more influential CPU for a given traffic weight, as data has to be stored about each and every load flow seen over a period of time.

B) Firewall Testing

Firewalls plays important role in network protection and in many cases build the only line of security against the unidentified rival, systematic Firewall testing has been ignored over years [1]. The reason for this lies in the missing of undependable, helpful and received testing methodologies. Efficiency testing is hard to do without particular tools, and even if you have particular tools, you may not get good results. Efficiency testing should focus on three areas: (1) intrusion prevention (2) antimalware (3) application identification. If you want to block peer-to-peer file sharing, open a few different Torrent clients and see what happens. Performance testing has to be completed by "pass/fail" indicators. For example, when the firewall starts to reject to open new sessions, the test should end as you have gone away from the limits. You should also set other limits, such as greatest latency time, to define when the firewall is not behaving sufficiently well. Do the same for applications such as webmail or face book, which both are the most important candidates for application identification and control. Don't try an automatic test tool, as the results are never as exact as the real application talking to real servers. This is especially correct of applications that are ambiguous, such as Bit Torrent and Skype, which can never be perfectly virtual in a test tool. Performance testing also usually requires particular tools, but has become so well-liked that there are open source alternative. When testing presentation remember to check your bad test against a null device a router or patch cable would work. This will tell you the maximum speed of your analysis bed. From there, keep in mind noted network tester David Newman's Laws of Testing: It must be repeatable, it must be worrying, and it must be significant. Take the device you're testing to its confines, even if you don't predict going that far. This will tell you where you will hit a wall in the upcoming and where you have sufficient headroom to grow. There are three general approaches to firewall testing:

- Penetration testing
- Testing of the firewall implementation
- Testing of the firewall rules

The goal of penetration testing is to expose security flaw of a goal network by running attacks against it. Penetration testing includes information get-together, searching the network and attacking the target. The attacks are performed by running vulnerability testing tools, Saint that check the firewall for likely breaches of security to be exploited. If vulnerabilities are detected, they have to be permanent. Penetration testing is usually performed by the system administrators themselves or by a third party (e.g. hackers, security experts) that try to break into the computer system. The problem is that we have to be sure that we can trust the external experts. Penetration testing is a way to perform firewall testing but it is not the only one and it is not the way we precede.

Testing of the firewall working focuses on the firewall software. The examiner checks the firewall working for bugs. Different firewall commodities support different firewall languages. Thus, firewall rules are vendor-exact. Consider a hardware firewall deploying vendor- exact firewall rules. The firewall execution testing approach evaluates if the firewall rules communicate to the action of the firewall. Firewall execution testing is primarily performed by the firewall vendors to increase the consistency of their products.

Testing of the firewall rules confirmed whether the security policy is correctly executed by a set of firewall rules. A security plan is a document that sets the basic mandatory rules and morality on information security.

Such a document should be plan in every company. The firewall rules are future to implement the directives in the security plan.
Considering the test packet driven advance, firewall testing includes two phases:
The identification of appropriate test cases that examine the behaviour of the firewall and the practical performance of these tests.

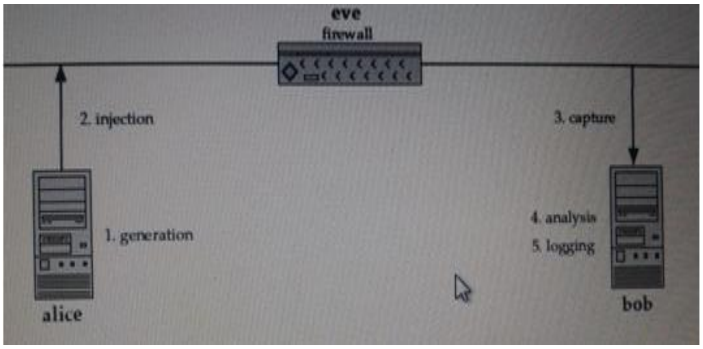

Fig 2. Single firewall test scenario

In this paper, we focus on the second part of the testing procedure. Our goal is to design and execute a tool that takes test packets as an input and automatically performs firewall testing by executing the following steps:
1. Generate packets according to the test packet specifications.
2. Inject the packets before the firewall.
3. Capture those packets behind the firewall that are forwarded by the firewall.
4. Analyze the results with respect to the expected outcome.
5. Log the packets leading to irregularities.
Above Figure illustrates the operations of the testing tool has to provide and at the same time, it represents the test atmosphere we are working with: Two hosts are connected via a firewall. The hosts build, inject, capture, analyze and log the packets. That is, the packets are crafted and injected by the sending host and the receiving host captures, analyzes and logs the packets if they make it through the firewall. Both hosts act as sender and receiver and the communication is therefore bidirectional. Companies infrequently have a single firewall but an entire firewall system. Thus, firewall Testing has to be performed for various firewalls [9] [10].

C) *Terminology*

Firewall terminology varies from one computer to compute. so it is very important to need to define the terms likes Gateways, Interfaces, Zones, and Hosts.

1) Gateway:

A gateway is simply a device that joins together two dissimilar networks. In the most common circumstances, is an internal network is with the internet. These are the packet filtering devices. A router is an example of a gateway device. A router is a device that does *routing*, deciding where packets are sent to base on its IP address. Gateways can be either firewalls or routers. A firewall is a filter that tests packets against a set of defined rules in order to decide whether to allow the packets through this network. In many devices, the working principle of both a gateway and a firewall is present. Of course, there are dedicated versions of each for use in large enterprise networks.

2) Interface:

In computer system, an interface is the point of interaction with software, or computer hardware, or with peripheral devices such as a computer monitor or a keyboard. Each connection is done from this interface. Some computer interfaces such as a touch screen can send and receive data, while others such as a mouse, microphone or joystick can only send data. On this, gateway each interface has its own IP address

3) Zones:

Zone policy firewall is also known as "Zone-base-Policy Firewall" or "ZPF" change the firewall from the interface-based model to a more elastic, more simply understood zone-based configuration model. ZPF General Rules describe the rules leading interface behavior and the flow of traffic between zone-member interfaces. It is assigned to zones, and check policy is applied to traffic moving between the zones. Inter-zone policies offer significant elasticity and granularity, so different inspection policy can be functional to several host groups associated to the same router edge

4) Hosts:

A network host is a computer linked to a computer network. A network host may offer information assets, services, and applications to users or other nodes on the network. A network host is a network node that is assign to a network layer host address [5].

III. CHARACTERISTICS

The characteristics of the firewall protection consist of the following:

1) Dissimilar safety levels based on the place of the computer:

When your PC links to a network, the firewall applies a safety level in agreement with the type of network. If you want to change the safety level assigned originally.

2) Safety of Wi-Fi:

These blocks interruption attempts launched through Wi-Fi network. When an impostor attempts to entrance, a pop-up counsel is displayed that allows you to instantly block the hit.

3) Access to the network and the Internet:

It specifies which programs installed on your computer can enter the network or the Internet.

4) Blocks:

The firewall can chunk the access of the programs that you indicate not be able to enter the local network or the Internet. It also blocks access from other computers that try to bond to programs installed on your system.

5) Meaning of rules:

It defines rules that you can use to identify which links you want to permit and the ports and zones through which the links can be recognized [7].

IV. CONCLUSIONS

Now a day, the firewall also has its own limitation, which does not undergo firewall's process; the firewall is helpless, if it is protected in the network through SLIP and the PPP way directly and is with the connection of internal user, will then creates the safe hidden danger. The protection that firewalls provide is as good as the rule they are configured to execute. The study of real organization data shows that corporate firewalls are often enforce rule sets that violate well established security plan. Finally, by analysing the paper we can say that firewall strategies are user-friendly to the network security.

REFERENCES

[1] Canghong Zhang, Based on nework security firewall technology,Information technology,Chinese new technology new product, 2009.
[2] Rui Wang. Haibo Lin, Network security and firewall technology, Tsinghua university publishing house, in 2000
[3] Kuang Chu,network security and firewall technology, Chongqing university publishing house,2005
[4] S. Smith, E. Palmer, and S. Weingart, "Using a high-performance, programmable secure coprocessor," in Proc. International Conference on Financial Cryptography, Anguilla, British West Indies, 1998.
[5] P. Liu and S. Jajodia ,"Multi-phase damage confinement in database systems for intrusion tolerance," in Proc. 14th IEEE Computer Security Foundations Workshop,Nova Scotia, Canada, June 2001.
[6] S. W. Lodin and C. L.Schuba, "Firewalls fend off invasions from the net," *IEEE Spectrum*, vol. 35, no. 2, 1998.
[7] A. Wool, "A quantitative study of firewall configuration errors," *Computer*, vol. no. 6,2004.
[8] M. R. Lyu and L. K. Y. Lau, "Firewall security: policies, testing and performance evaluation," in *Proc. 2000 International Conference on* Computer Systems and Applications.
[9] J. J¨urjens and G. Wimmel, "Specification-based testing of firewalls," in Proc. 2001 International Andrei Ershov Memorial Conference on Perspectives of System Informatics.
[10] Check Point's Press Release "Check Point Introduces Revolutionary Internet Firewall Product Providing Full Internet Connectivity with Security; Wins 'BEST OF SHOW' Award at Net world Interpol '94". 1994
[11] Yu Qiu,Internet network security and firewall technology discussion,Mianyang Normal school journal ,2004.

