ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

A Review Paper on Computer Firewall

[1]Damodharan, [2]Prabhat Kumar Srivastava
[1][2]Department of Electronics and Communication Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh
[1]damodharan@Galgotiasuniversity.edu.in

Abstract: Computer networks and internet networks face an increasing number of security threats. For new types of attacks constantly emerging, a serious challenge is the development of versatile and innovative security-oriented approaches. This paper addresses the protection of computer systems and how computer-related assets and resources can be secured. A firewall is software that creates a security perimeter with the primary task of blocking or restricting all incoming and outgoing information over a network. These firewalls are basically ineffective and suitable for enterprise environments to maintain information security while supporting the free exchange of views. In this paper we are discussing a network firewall that protects both the corporate environment and the other networks that want to exchange information over the network. A firewall prevents the flow of internet traffic and is less restrictive of outward and inward information and also offers the illusion of anonymous internet File Transfer Protocol and site access.

Keywords: Firewalls, Firewall configuration, FTP, Gateways, Packet filter and Threats.

INTRODUCTION

Computer networks are designed to connect two or more computers around the world, located at the same or different corners. They exchange information openly with any other device. This type of sharing is a great advantage for both individuals and the corporate world but as we know in today's era, most important and confidential information is also exchanged on the internet so attackers can easily attack and find out the important information and can harm the business in any way.

The root of firewalls[1] was in the early 1990's. These provide a fireproof barrier between sections of buildings, making it harder for a fire to spread to other areas of one part of the building. Similarly, a network firewall is built for defending it from the outside in the region of a network or sub network. This defines firewall as a collection of components placed between an internal network and an external network to achieve the following goals; all interchanges must go beyond the firewall, only traffic approved by the security strategy of the internal network can pass, the firewall cannot be deflated. A firewall is a hardware device or software system or group of systems (router, proxy or gateway) designed to authorize or deny network transmission based upon set of security rules and regulations to implement handle between two networks to protect insidenetwork from outsidenetwork.

Today, computers are commonly used to equally transfer data and information than to process, for instance, a vast quantity of intimate transaction crops up every second. This networking offers a trouble-free way for outdoor unfrozen parties to reach the private network of an organization and access or interfere with internal information and resources, but in order to have a vulnerable transmission of the information being shared over the internet, one desires the principle of Network Security which needs to take corrective action to protect Ease of Use from unusual types of attackers like-hackers, interested computer neophytes, untrustworthy vendors or disgruntled employees of an organization. Network Security[2] helps to maintain certified compliance.

CHARACTERISTICS OF GOOD FIREWALL

(a) Transfer of information either from inside to outside or from outside to inside must pass through the firewall.
(b) The authorized traffic should be allowed to pass.
(c) The firewall must be strong enough to prevent from attacks.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

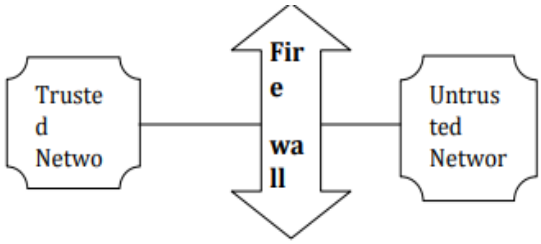

Figure 1: Firewall Network

In order to prevent our data from these threats, we need to ensure that security mechanisms, such that information inside and outside stays outside and prevents outside criminals from accessing the corporate network. The firewall[3] is one solution to that problem. Firewall's principal role is to regulate the flow of information within computer networks. By standing between the network and the outside world it protects network. The movement of data in any direction has to go through the firewall.

TYPES OF FIREWALLS

Hardware firewall: It provides security to a local network, Hardware firewall is typically part of TCP/IP router.

Software firewall: It is a computer with firewall software which provides security from intruders, which may also provide internet connectivity involving between Private LAN and Public Network. Maximum saturation of intruders happens and is seen on the public network only.

Figure 2: Hardware firewall

TYPES OF ATTACK

A. Denial-of-Service attack

DOS[4] attack is abreak in authorized user's right to use a computer or networks. It includes all types of attacks such that the authentic end user of a computer or a network cannot use it.

B. Eavesdropping

It factually means secretly listening to a discussion and basically all kinds of attacks like theft such as the e-mail passwords, message, records, data, and information over the network connection by listening on the connection.

C. Host Attacks

It mostly attacks the vulnerabilities of operating systems or how the system is prearranged and administered.

D. Password Guessing

It involves guessing of the password for nasty activities.

E. Protocol-based attacks

It involves taking benefits of known or unknown network services.

F. Social Engineering

This is a kind of harass by the social means. Basically attacker acts as an unadulterated user or administrator and extracts all the mysterious information from the user socially.

G. War Dialing

This type of attack is a distinctive in its own way that basically means accessing the personal desktop of somebody via modems. Firewall plays[5] a very important role in protecting networked computers from intractable violent intrusions that might require judgment or result in data theft or denial of service or any of the above-mentioned network attacks.

FIREWALL CONFIGURATION:

A firewall is a combination of packet filters and application gateways. Depending on this, following are the configurations of firewall.

Screened Host Firewall, Single Homed Bastion:

In this type of configuration a firewall consists of following parts:

(i) A packet filtering router
(ii) An application gateway

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 2, February 2018

The main purpose of this type is as follows:

- The packet filter is used to check the destination addr ess field of the incoming IP packet only if it is intend ed for the application gateway[6]. It also performs the same role on output data by inspecting the outgoing I P source address field.
- Application gateway is used to performauthentication and proxy functions.

Disadvantage:

- Real connection

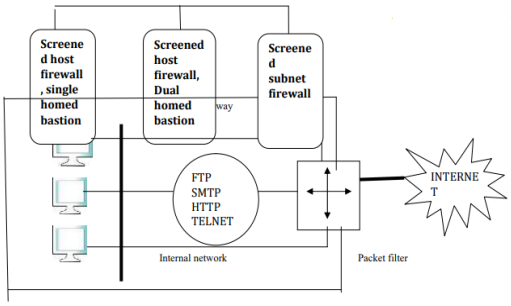

Figure 3: Screened host firewall, single- homed bastion

Screened Host Firewall, Dual Homed Bastion:

To overcome the disadvantage of a screened host firewall, single homed bastion configuration, another configuration is available known as screened host firewall, Dual homed bastion.

In this, it avoids direct connections between internal hosts and the packet filter because it connects the packet filter to the application gateway, which has a separate connection to the internal hosts. Now if it effectively hits the packet filter[7]. Attacker is only available to program gateway. It willprovide internal hosts with security.

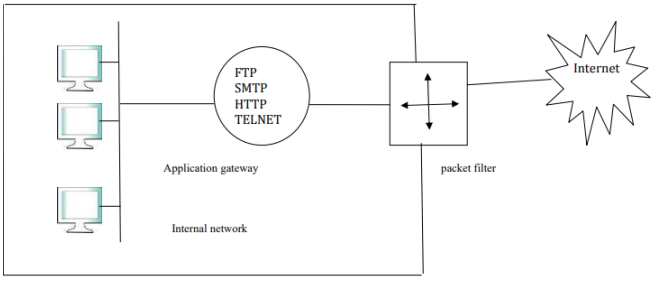

Figure 4: Screened host Firewall, dual homed bastion

Screened Subnet Firewall:

It offers the highest level of security among all firewall configurations. It is improved version over all firewall configuration schemes available. This uses two packet filters, one between internet gateway and application gateway[8], the other between application gateway and internal network.

LIMITATIONS OF FIREWALL

So far as we have discussed all the security it provides us with and a firewall is an extremely useful security measure for any organization but at the same time it does not solve all the practical security issues. The key drawbacks are:

- Virus attack: A firewall cannot fully protect the internal network from virus attacks, as it cannot search every incoming packet for virus content.
- Insider's intrusion[9]: A firewall is designed to protect insider from outside attacks but if an inside user attacks the internal network, the firewall cannot prevent from such type of attack.
- Direct internet traffic:A firewall is only successful if it is the only exit point for the network, but if there is more than one exit point from which the attacker can exchange information, the firewall cannot carefully manage these situations.

CONCLUSION

As we have addressed so far, firewall is a very important part of computer security against viruses, spyware, Trojans and other malware, as well as between direct malicious attacks from outside the network and outside. A

good firewall[10] is one which provides complete network security without affecting the speed of our device and access to our network. To provide protection, one should keep an eye on following things.

- We should never install any software fromsuspicious sources. Always download from the respected sites available on internet.
- Use a firewall to monitor all data or informationover the internet.
- On every computer a firewall software must beinstalled else it will only take one PC to become infected and very fast it will affect the all computers available on that network.

REFERENCES

[1] E. W. Fulp, "Firewalls," in *Managing Information Security: Second Edition*, 2013.

[2] R. Marty and B. Rexroad, "Network security," in *Building the Network of the Future: Getting Smarter, Faster, and More Flexible with a Software Centric Approach*, 2017.

[3] B. Yang, "Firewall," in *Information Assurance and Security Technologies for Risk Assessment and Threat Management: Advances*, 2011.

[4] P. Rengaraju, V. R. Ramanan, and C. H. Lung, "Detection and prevention of DoS attacks in Software-Defined Cloud networks," in *2017 IEEE Conference on Dependable and Secure Computing*, 2017, doi: 10.1109/DESEC.2017.8073810.

[5] Cisco, "What Is a Firewall?," *Cisco*. 2017.

[6] A. Wool, "Trends in firewall configuration errors: Measuring the holes in Swiss cheese," *IEEE Internet Computing*. 2010, doi: 10.1109/MIC.2010.29.

[7] X. Xu, Z. M. Mao, and J. A. Halderman, "Internet censorship in China: Where does the filtering occur?," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2011, doi: 10.1007/978-3-642-19260-9_14.

[8] T. Zia, A. Zomaya, V. Varadharajan, and M. Mao, *Security and Privacy in Communication Networks*. 2013.

[9] M. V. Pawar and J. Anuradha, "Network security and types of attacks in network," in *Procedia Computer Science*, 2015, doi: 10.1016/j.procs.2015.04.126.

[10] Symantec, "Internet security threat report," 2016.

[11] Ishleen Kaur, Gagandeep Singh Narula, Ritika Wason, Vishal Jain and Anupam Baliyan, "Neuro Fuzzy—COCOMO II Model for Software Cost Estimation", International Journal of Information Technology (BJIT), Volume 10, Issue 2, June 2018, page no. 181 to 187 having ISSN No. 2511-2104.

[12] Ishleen Kaur, Gagandeep Singh Narula, Vishal Jain, "Differential Analysis of Token Metric and Object Oriented Metrics for Fault Prediction", International Journal of Information Technology (BJIT), Vol. 9, No. 1, Issue 17, March, 2017, page no. 93-100 having ISSN No. 2511-2104.

[13] Basant Ali Sayed Alia, Abeer Badr El Din Ahmedb, Alaa El Din Muhammad,El Ghazalic and Vishal Jain, "Incremental Learning Approach for Enhancing the Performance of Multi-Layer Perceptron for Determining the Stock Trend", International Journal of Sciences: Basic and Applied Research (IJSBAR), Jordan, page no. 15 to 23, having ISSN 2307-4531.

[14] RS Venkatesh, PK Reejeesh, S Balamurugan, S Charanyaa, "Further More Investigations on Evolution of Approaches for Cloud Security", International Journal of Innovative Research in Computer and Communication Engineering , Vol. 3, Issue 1, January 2015

[15] K Deepika, N Naveen Prasad, S Balamurugan, S Charanyaa, "Survey on Security on Cloud Computing by Trusted Computer Strategy", International Journal of Innovative Research in Computer and Communication Engineering, 2015

[16] P Durga, S Jeevitha, A Poomalai, M Sowmiya, S Balamurugan, "Aspect Oriented Strategy to model the Examination Management Systems", International Journal of Innovative Research in Science, Engineering and Technology , Vol. 4, Issue 2, February 2015