Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 3159-0040
Vol. 2 Issue 3, March - 2015

Firewalls Implementation in Computer Networks and Their Role in Network Security

Sahithi Dandamudi
University of Bridgeport
Department of Electrical Engineering
email:sdandamu@my.bridgeport.edu

Prof. Tarik Eltaeib
Department of Computer Science
University of Bridgeport
Email:teltaeib@my.bridgeport.edu

***Abstract*—With the increased demand in Network Security there is a need for devices and software's which can provide reliable security in the Network. This paper gives a detailed explanation of implementing a Firewall in various environments and their role in network security. Firewall is a network security system that grants or rejects network access to traffic flow between an un-trusted zone and a trusted zone. The main idea of this paper is to define the role of firewall in network security and Implementation of firewall in hardware and software or combination of both.**

Keywords: Firewall, Implementation, Computer Networks, Security

I. INTRODUCTION

What is a Firewall?

A ***Firewall*** **[1]** is a networking system that helps us in preventing unauthorized access of one's computer over the internet (ie, It acts as a protection barrier between the system and the network). Firewall can enact both software and hardware appliances.

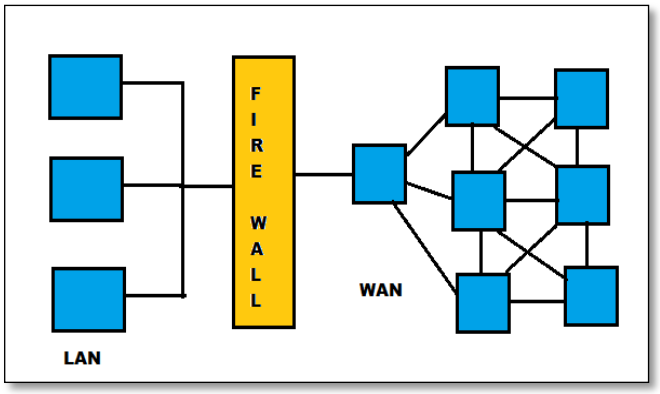

Fig.1

II. EXPLANATION

Functionality [2] and Flow control of a Firewall

Access the internet such that the internal networking system LAN is secured such that no hacker can access or they cannot harm the internet. For this purpose we use software or hardware or a combination of both in between the LAN and Internet. Based on the pre-defined set of rules, the function of the firewall is to check the data-packets coming from the Internet or any external networking system and send it to the LAN if there no vulnerabilities are found and vice-versa. Firewall drops the packet and an error is detected if there is any harmful vulnerability in the data-packets coming from the PC.

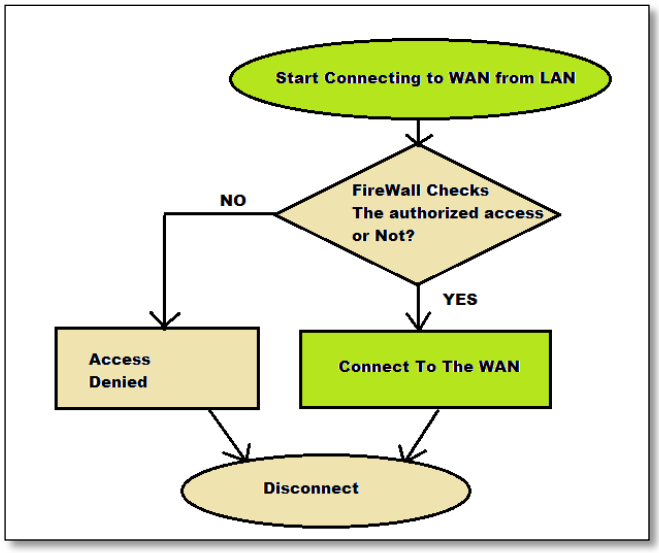

Fig.2: Network access flow using firewall

Firewall Environments and Implementation of a Firewall and Their Role in Network security

There are different types of environments where a firewall can be implemented ranging from a simple packet filter to combination of several firewalls. The choice of firewalls [3] is very attractive. They come in every size, shape and capacity that is designed according to the customer satisfaction. The type of firewall used to install depends up on the size, protection and management of the network. We discuss Implementation of firewall DMZ environment, VPN, Intranet, Extranet.

Implementation of firewall in DMZ Environment

In Computer networks, a DMZ [4] is a demilitarized zone or a neutral zone that is in between a company's private network and the outside public network.

In the below figure the Main Firewall provide the access control and protection to the server from being hacked from the public network. A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.

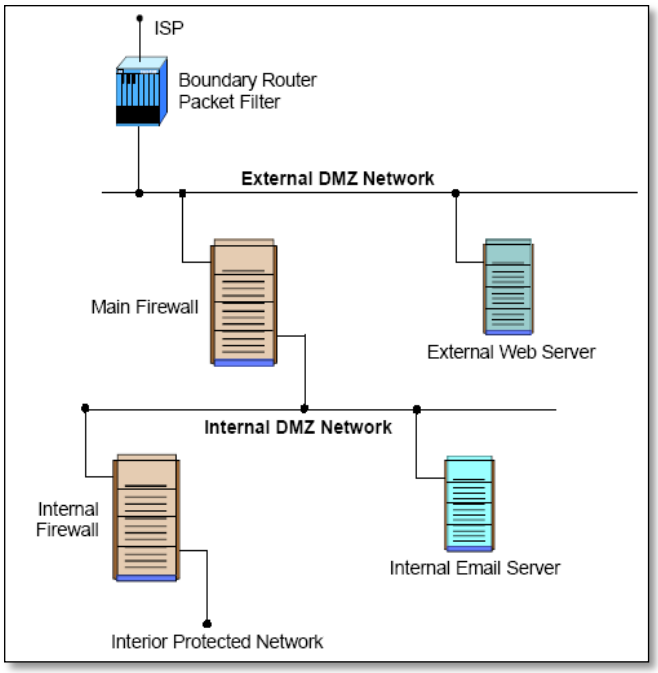

Fig.3 DMZ Implementation

Implementation of firewall in VPN

A Virtual Private Network (VPN) [5] is a private network that uses public network to connect remote sites or users together. The VPN is created by establishing a virtual point-to-point through the use of dedicated connections, virtual tunneling protocols, or traffic encryption.

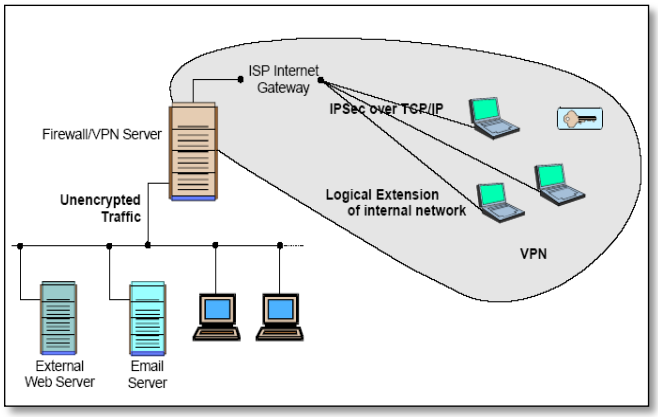

Fig.4 VPN Implementation

The VPN firewall ensures that the systems are encrypted and also ensures that only authorized users can use the network and data cannot be intercepted.

Implementation of firewall in Intranet

An Intranet is a network that employs the same types of applications, services, and protocols that are present in an internet, without external connectivity. The Firewall protects the intranet by checking the traffic flow from the interconnected intranets.

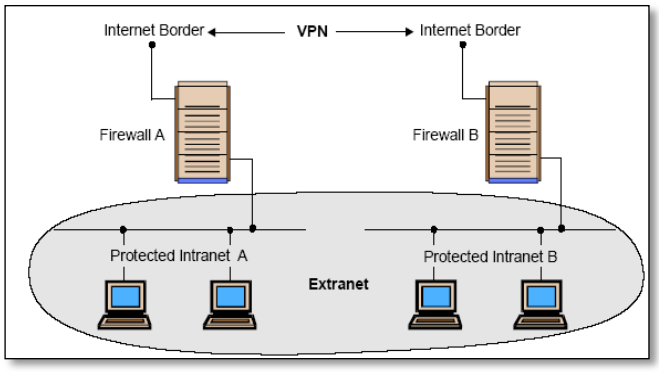

Fig.5 Firewall Implementation in Intranet

Implementation of Firewall in Extranet.

Extranet is usually a business to business intranet. The Control access is provided to the remote user based on the authentication and authorization as provided by a VPN.

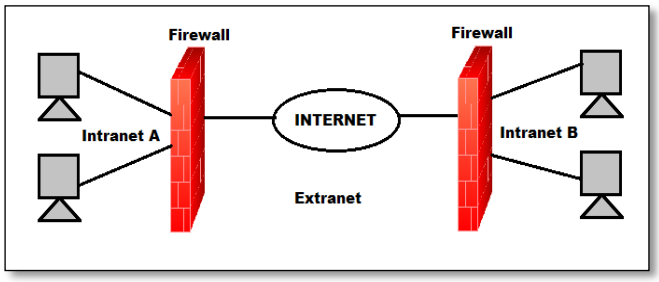

Fig.6 Implementation in Extranet

Who needs a *Firewall*? [5]

Whenever the user plans to connect to the internet from home or company, he needs a ***firewall***. To protect our network from the viruses, hacking etc, we have to install a *firewall.*

Kinds of Firewalls

Firewall is of two kinds. They are

- ✓ Software Based Firewall
- ✓ Hardware *Based* Firewall

Software based firewall is used for personal computers (e.g., home used).

Hardware firewalls are used for the bigger networks (e.g., office use). These firewalls has software component where traffic cannot come or go in our system.

Types of Firewalls

Firewalls are broadly classified into four categories. They are discussed below.

Packet Filters

The Packet Filters [6] firewalls work at the network level of the OSI model. Each packet is compared to a set of criteria before it is forwarded. Packet filtering firewalls is low cost and has low impact on network performance.

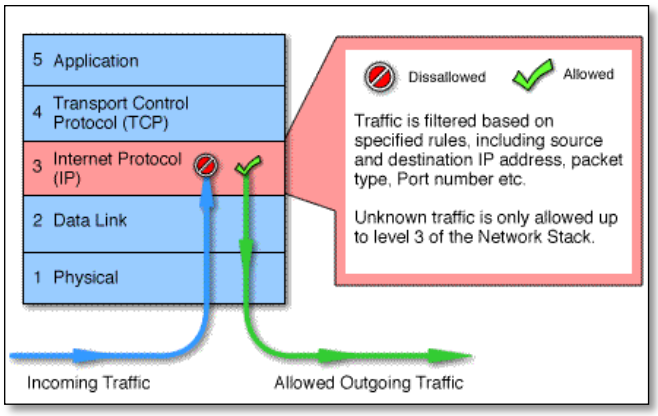

Fig.7 Packet Filtering

Circuit Level Firewalls

Circuit level firewalls work at the sessions layer of the OSI model, or the TCP layer of TCP/IP.

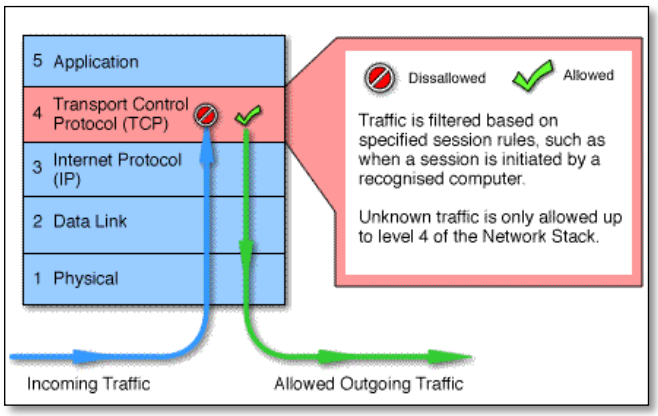

Fig.8 Circuit Level

Application Level Firewalls

Application level Firewalls [7], also called proxies are similar to circuit-level gateways except that they are application specific that is the gateway that is configured to be a web proxy will not allow any FTP, telnet or other traffic through.

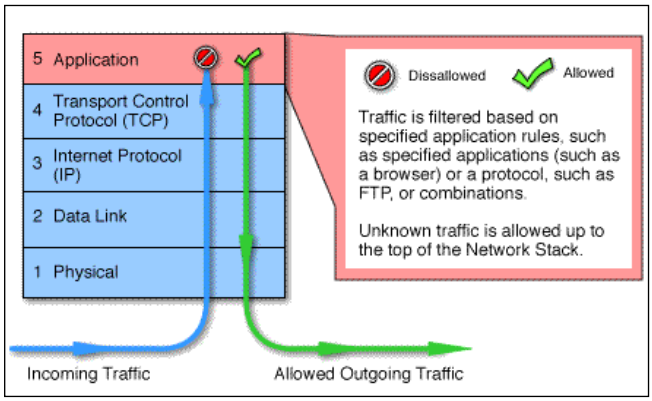

Fig.9 Application Level Firewalls

Stateful Multilayer Firewalls

Stateful multilayer firewalls [8] combine the aspects of the other three types of firewalls. They filter packets at the network layer, determine whether session packets are legitimate and evaluate contents of packets at the application layer.

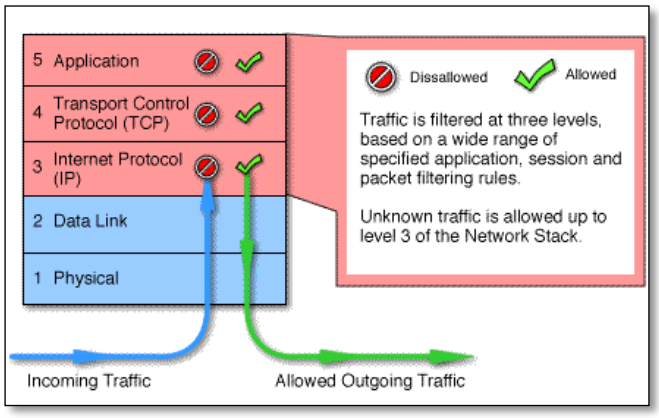

Fig.10 Stateful Multilayer Firewalls

Real Time Example of a Firewall in Windows Operating System

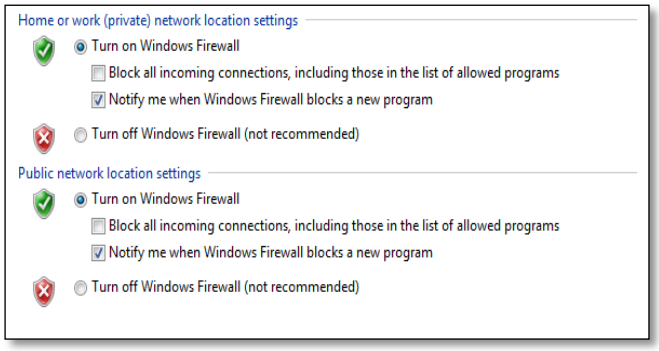

Fig.11

By considering Windows Operating System, The above figure shows that the ***firewall*** is turned ON.

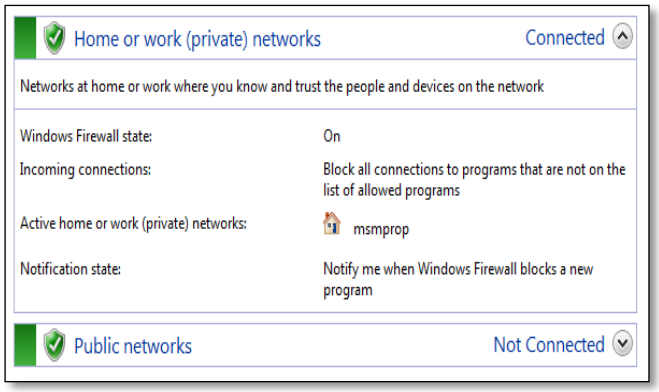

Fig.12

As the firewall is turned on, the Home network is protected from the malicious software and other networking attacks.

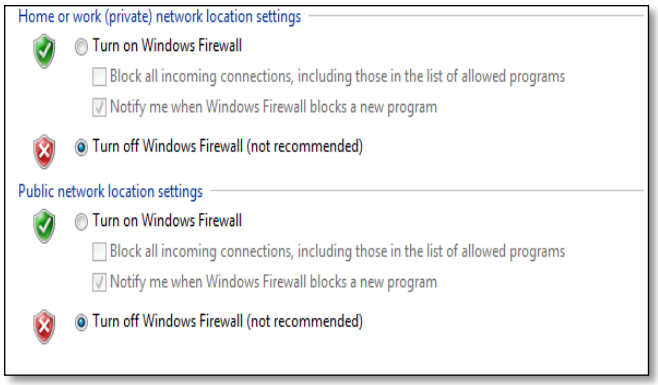

Fig.13

By considering Windows Operating System, The above figure shows that the ***firewall*** is turned OFF.

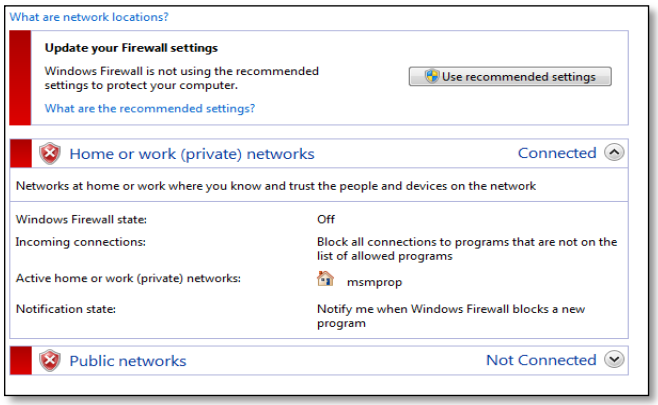

Fig.14

As the firewall is turned OFF, the home network is prone to hacking and Data theft.

A ***Firewall*** is not the same thing as an antivirus program. To protect one's own computer, we need both firewall and an antivirus and anti-malware program.

Technical Feasibility and Limitations of Firewall

The Technical Feasibility of Firewalls is limited due to the following limitations [9]

A firewall plays a vital role in network security and is designed to address the issues of data integrity and confidentiality of internal network. The importance of including a firewall in security strategy is consequent; however, firewalls do have following limitations:

- A firewall can't prevent the users or attackers with modems from dialing in to or out of the internal network.
- Firewalls cannot enforce the password policy or prevent misuse of the password.
- Firewalls cannot stop internal users from accessing websites with malicious program code and software's that might install viruses.
- Firewalls can't protect from poor decisions.

Future of Firewalls

Firewalls will continue to advance as the attacks on IT industry and infrastructure become more and more sophisticated. Firewalls that scan for viruses as they enter the network and several firms are currently exploring this idea, but it is not yet in wide use.

Conclusion

It is clear that some form of security for private networks connected to the internet is essential. A firewall is an important and necessary part of that security, but cannot be expected to perform all the required security functions.

References

[1] Firewalls by Dr.Talal Alkharobi.

[2] Basic Firewall Functionality – Joel Snyder

[3] Implementing a Distributed Firewall-Sotiris Loannidis, Angelos D.Keromytis, Steve M. Bellovin, Jonathan M. Smith.

[4] DMZ (demilitarized zone)-Margaret Rouse

[5][6][7][8] Firewalls By Hareesh Pattipati.

[9] Network Security First-Step: Firewalls - Donald Stoddard, Thomas M. Thomas.