Internet Security & Firewalls

***Names: Syed Mahad Arshad Hussaini & Mahum Shaikh***

***ID’s: 19163 & 16419***

***Course: OS (Lab)***

***Submitted To: Miss Hira Farman***

***Department of Computer Science, Iqra University, Karachi, Pakistan***

# Abstract

Internet security is a specific aspect of broader concepts such as cybersecurity and computer security, being focused on the specific threats and vulnerabilities of online access and use of the internet. It has become a major issue in the current trend of things. And it's like an evil which if left to spread will in no time have effects on us all. This study thus examined how firewall can be applied to internet security with a look at the various techniques and types of firewall and how it can help to secure the internet. The configuration procedure for firewall and how they could be turned ON or OFF were also discussed. It was observed that the application of firewall has played a significant role in curbing security threats that have increased on the internet and the need to proffer solutions to the situation and make the internet a safer place.

However, through this study, we advocate that internet security be improved upon in order to assure the users of the Internet of security and unauthorized access denied or set to self-destroy any potential or anticipated threat.

**Keywords:** Internet Security, System Security, Firewalls, Threats, OS Security

# Introduction

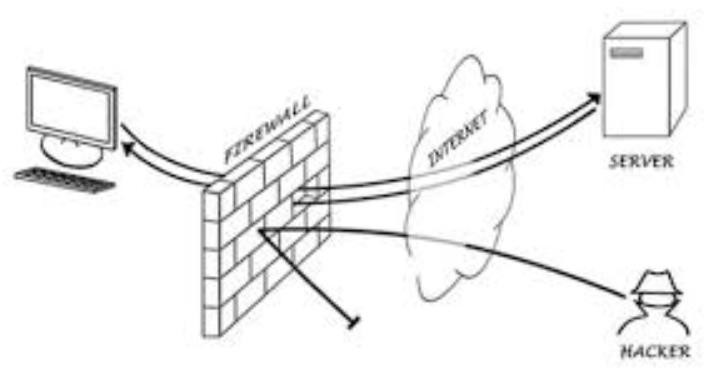
In today's digital landscape, many of our daily activities rely on the internet. Various forms of communication, entertainment, and financial and work-related tasks are accomplished online. This means that tons of data and sensitive information are constantly being shared over the internet. The internet is mostly private and secure, but it can also be an insecure channel for exchanging information. With a high risk of intrusion by hackers and cybercriminals, internet security is a top priority for individuals and businesses alike.

Internet security consists of a range of security tactics for protecting activities and transactions conducted online over the internet. These tactics are meant to safeguard users from threats such as hacking into computer systems, email addresses, or websites; malicious software that can infect and inherently damage systems; and identity theft by hackers who steal personal data such as bank account information and credit card numbers.

Nowadays, every businesses and organizations have a risk of internet security. With software being developed in a distributed environment, it is important for a company to have data security, and to have the data accessible to all members of a team. But not all data should be accessible by all users. There should be some privilege that what data should be accessible by which user. To solve this problem is to produce a secure environment and to achieve this, a firewall is the first line of defense

# Firewall

A Firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. It’s just like a fence between your computer or your internal network and the Internet. Firewalls can either be software or hardware, though it’s best to have both. A software firewall is a program installed on each computer and regulates traffic through port numbers and applications, while a physical firewall is a piece of equipment installed between your network and gateway.



# Types of Firewall

There are various types of firewalls, some common types are given below:

## Packet filtering firewall.

* + Examines the current packets and filters it
  + Susceptible to floods and DoS attacks

## Stateful packet inspection (SPI)

* + Improved version of packet filtering, also check and compares with previous packets
  + Context Aware thus less susceptible to ping floods and SYN floods (DoS), as well as being less susceptible to spoofing.

## Application-level gateway (proxy firewall)

* + Works as a proxy on application layer to filter traffic.
  + More secure but susceptible to flood or DoS attacks

## Circuit-level gateway

* + Similar to application gateways but more secure
  + Monitor TCP handshaking between packets to determine whether a requested session is legitimate.
  + Works at session layer of OSI model

## Which Firewall Architecture is Right for Your Business?

When it comes to selecting the best firewall architecture, there is no need to be explicit. It is always better to use a combination of different firewalls to add multiple layers of protection.

# Operating System Security

Security refers to providing a protection system to computer system resources such as CPU, memory, disk, software programs and most importantly data/information stored in the computer system. If a computer program is run by an unauthorized user, then he/she may cause severe damage to computer or data stored in it. So a computer system must be protected against unauthorized access, malicious access to system memory, viruses, worms etc.

# Risk and Threats to Operating System

There are some threats to Operating System which are given below.

# System Threats

System threats refers to misuse of system services and network connections to put user in trouble. System threats can be used to launch program threats on a complete network called as program attack. System threats creates such an environment that operating system resources/ user files are misused.

Following is the list of some well-known system threats.

* **Worm** − Worm is a process which can choked down a system performance by using system resources to extreme levels. A Worm process generates its multiple copies where each copy uses system resources, prevents all other processes to get required resources. Worms processes can even shut down an entire network.
* **Port Scanning** − Port scanning is a mechanism or means by which a hacker can detects system vulnerabilities to make an attack on the system.
* **Denial of Service** − Denial of service attacks normally prevents user to make legitimate use of the system. For example, a user may not be able to use internet if denial of service attacks browser's content settings.

Operating system's processes and kernel do the designated task as instructed. If a user program made these process do malicious tasks, then it is known as

# Program Threats

One of the common example of program threat is a program installed in a computer which can store and send user credentials via network to some hacker. Following is the list of some well-known program threats.

* **Trojan Horse** − Such program traps user login credentials and stores them to send to malicious user who can later on login to computer and can access system resources.
* **Trap Door** − If a program which is designed to work as required, have a security hole in its code and perform illegal action without knowledge of user then it is called to have a trap door.
* **Logic Bomb** − Logic bomb is a situation when a program misbehaves only when certain conditions met otherwise it works as a genuine program. It is harder to detect.
* **Virus** − Virus as name suggest can replicate themselves on computer system. They are highly dangerous and can modify/delete user files, crash systems. A virus is generally a small code embedded in a program. As user accesses the program, the virus starts getting embedded in other files/ programs and can make system unusable for user

Software are the backbone of a computer environment - providing users with a simple and easy-to-use interface for hardware and software installed on a computer. Exploitation of operating system code causes damage to computers, giving hackers the ability to steal data and damage both hardware and software. Operating system security is important because it protects the central computer control system.

# Operating System Firewalls:

Both Operating Systems i.e. Windows and Linux has its own simple built-in firewall.

## Windows Firewall

Windows first started shipping a primitive firewall, called Internet Connection Firewall (ICF), with Windows 2000. It was very simple. Each version of Windows since then has expanded upon this idea. Windows 10 ships with a fully functioning firewall. This firewall can block inbound and outbound packets.

More importantly, you can apply rules differently depending on where the traffic comes from. You can set up rules for three areas or profiles:

* Domain: For those computers authenticated on your domain.
* Public: For computers from outside your network. You would treat outside traffic more carefully than traffic coming from another machine in your domain.
* Private: Private refers to traffic from your own computer, thus the term private.
* Administrators should always follow these rules with all packet filtering firewalls:

The Windows Firewall also has a logging feature, but it is disabled by default. Turn this feature on

## Linux Firewall

Linux has firewall capabilities built into the operating system

The first widely used Linux firewall was called ipchains. It was essentially a chain of rules for filtering traffic.

## IPTables

The more modern iptables replaced ipchains and is the primary firewall for Linux. On most Linux systems, iptables is installed as **/usr/sbin/iptables.**

An iptables firewall is made up of three different kinds of objects: tables, chains, and rules. Basically, the tables contain chains of rules

Each chain has a series of rules that define how to filter packets. There are actually three tables and each has some standard rule chains in it.

The three tables and their standard chains are as follow:

Packet Filtering: This table is the essential part of the firewall. It is a packet filtering firewall and it contains three standard chains: INPUT, OUTPUT, and Forward. The INPUT chain processes incoming packets, and the OUTPUT chain processes traffic sent out from the machine. If the firewall system is also acting as a router, only the FORWARD chain applies to routed packets.

Network Address Translation: This table is used for performing network address translation on outbound traffic that initiates a new connection. This is used only if your machine is serving as a gateway or proxy server.

Packet Alteration: This table is used only for specialized packet alteration. It is often called the mangle table because it alters, or mangles, packets. It contains two standard chains. This table might not even be needed for many standard firewalls.

iptables requires some configuration. You can do it through the GUI (KDE, GNOME, etc.) but the shell commands are common to most distributions. Let’s take a look at some common basic configuration.

To list the current iptables rules use:

## iptables –L

To allow communication on a specific port, SSH port 22 and HTTP port 80 for example use:

## iptables –A INPUT –p tcp –dport ssh –j ACCEPT iptables –A INPUT –p tcp –dport 80 –j ACCEPT

If you do not explicitly need a port, then block it. For example, if you are not running a web server on that machine, then block all inbound port 80 traffic. With home machines, you can usually block all ports. With individual workstations on a network, you may need to keep some ports open in order to allow various network utilities to access the machine.

Unless you have a compelling reason not to, always block ICMP traffic because many utilities such as ping, tracert, and many port scanners use ICMP packets. If you block ICMP traffic, you will prevent many port scanners from scanning your system for vulnerabilities.

# Conclusion

Internet security has become a major concern as many businesses now make their transactions online. It’s therefore means that the internet must be secured for business to be done. The use of firewalls in our systems as a result cannot be over emphasized upon. Corporate bodies and companies can now prevent hackers and unrestricted access to their database or some vital information by the use firewalls. Firewall has played a major in internet security and its use should be encouraged and the software should be improved upon, such that a time will come when people can rest assured that the internet is now safe from potential treat as a result of unauthorized access.