**ABSTRACT**

The Firewalls and internet Security defines three basic types of firewall: packet filters, circuit hybrid firewalls, level gateways, and application gateways. Of course, there are also hybrid firewalls, which can be combination of all three.

Packet filter gateways are usually comprised of a series of simple checks based on the source and destination IP address and ports. They are very simply to the user since it will probably not even realize that the checks are taking place. However, that simplicity is also their biggest problem: there is no way for the filter to securely distinguish one user from another. These are frequently located on routers.

Circuit-level gateways are much like packet filters except that they operate at a different level of the OSI protocol stack. Unlike most packet filters, connections passing through a circuit-level gateway appear to the remote machine as if they originated from the firewall. This is very useful to hide information about protected networks.

Application gateways represent a totally different concept for firewalls. Instead of a list of simple rules which control which packets or sessions should be allowed through, a program accepts the connection, typically performs strong authentication on the user which often requires one-time passwords, and then often prompts the user for information on what host to connect to.

Hybrid gateways are ones where the above types are combined. Quite frequently one finds an application gateway combined with a circuit-level gateways or packet filters, since it can allow internal hosts unencumbered access to unsecured networks while forcing strong security on connects from unsecured networks into the secured internal networks.

INDEX

**Contents Page No.**

1. INTRODUCTION

2. NEED FOR FIREWALL

3. HISTORY OF FIREWALL

4. DESIGN GOALS FOR A FIREWALL

5. BASIC CONCEPTS OF A FIREWALL

6. ROLE OF FIREWALLS

7. CONCLUSION

8. REFERENCES

**1. INTRODUCTION**

The Internet has made large amount of information available to the average computer user at home, in business and education. For many people, having access to this information is no longer just an advantage; it is essential.

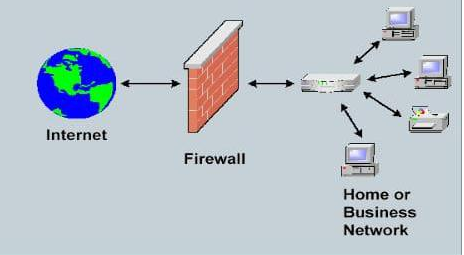
By connecting a private network to the internet can expose or confidential data to malicious attack from anywhere in the world. The intruders could gain access to your sites private information or interfere with use of your own systems.

Users who connect their computers to the internet must be aware of these dangers, their implications and how to protect their data and their critical systems. Therefore, security of network is the main criteria here and firewalls provides this security.

The internet firewalls keep the flames of internet hell out of your network or, to keep the members of your LAN pure by denying them access the all the evil internet temptations.

**Firewall Definition**

1. A Firewall is simply a program or hardware device that filters the information coming to the internet connection into your private network or computer system.



**Application Firewall**

An application firewall is a special firewall that is specifically coded for the type of traffic it is inspecting. The most widely developed application firewall is the web application firewall. A web application firewall is less concerned with source and destination addresses, and focuses on the actual data in the packet to see if the requests being sent to a web server, and the replies issued from the web server, meet its rules.

For example, a web application firewall may have a rule that says a requested URL may not be more than 256 characters long. When a packet is found that has a longer URL in the request field it can be dropped without to the web server.

**What Is The Difference Between A Host-based Firewall And A Networkbased Firewall?**

A host-based firewall is installed on an individual computer to protect it from activity occurring on its network. The policy may affect what traffic the computer accepts from the Internet, from the local network, or even from itself.

A network-based firewall is implemented at a specified point in the network path and protects all computers on the “internal” side of the firewall from all computers on the “external” side of the firewall.

Network-based firewalls may be installed at the perimeter, or edge, of a network to protect a corporation from hosts on the Internet, or internally to protect one segment of the community from another, such as separating corporate and residential systems, or research systems from marketing systems. A network-based firewall cannot protect one computer from another on the same network, or any computer from itself.

**Hardware Firewall Vs Software Firewall**

**Hardware firewall**

Hardware firewalls are integrated into the router that sits between a computer and the Internet. They typically use packet filtering, which means they scan packet headers to determine their source, origin, destination addresses and check with the existing user defined rules to make an allow/deny decision.