NETWORK SECURITY:ROLL OF FIREWALL

Yogesh Bhatia, Sanjeev Verma
Student, Department of Information Technology,
Dronacharya College of Engineering, Gurgaon, Hr, India

Abstract- **Internet security has become an important issue nowadays. And it's like an evil which if left to spread will in no time have effects on us all. This paper examines internet security with the use of firewall and how it can be used for internet security. A firewall is a part of a computer system or network which is designed to block unauthorised access to our system. This paper takes the descriptive method of writing. The techniques and types of firewalls are also discussed. This paper also discusses firewall and how it canbe used to help in internet security.**

I. INTRODUCTION

Network security is an important issue that must be seriously taken into consideration when designing a network. Network security is the policies and procedures followed by a network administrator to protect the network devices from threats and at a same time, the unauthorized users must be prevented from accessing the network.

Firewall is a network security system that controls the incoming and outgoing network traffic . A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is assumed not to be secure and trusted. Firewalls exist both as a software solution and as a hardware appliance. Many hardware-based firewalls also offer other functionality to the internal network they protect, such as acting as a DHCP server for that network.

Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions.

Firewalls can be implemented in either hardware or software, or a combinationof both. Firewalls are frequently used to prevent unauthorized Internet usersfrom accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

II. TYPES OF FIREWALL TECHNIQUES

1.Packet Filters: It is the process of passing or blocking packets at a network interface based on source and destination addresses, ports, or protocols. The packet filter examines the header of each packet based on a specific set of rules, and on that basis, decides to prevent it from passing (called DROP) or allow it to pass (called ACCEPT).

2.Application Gateway: An application gateway or application level gateway (ALG) is a firewall proxy which provides network security. It filters incoming node traffic to certain specifications which mean that only transmitted network application data is filtered. Such network applications include File Transfer Protocol (FTP), Telnet, Real Time Streaming Protocol (RTSP) and BitTorrent.

3.Circuit level gateway: A type of firewall that provides session-level control over network traffic. Similar in operation to packet filtering routers, circuit-level gateways operate at a higher layer of the Open Systems Interconnection (OSI) reference model protocol stack.

4.Proxy server: In an enterprise that uses the Internet, a proxy server is a server that acts as an intermediary between a endpoint device and the Internet so that the enterprise can ensure security, administrative control, and caching service.

III. MECHANISM OF PASSWORD

Passwords is a word or string of characters to identify and authenticate when users try to access the system. Computer user uses passwords for different purposes:

logging into accounts, retrieving e-mail, accessing applications, databases, networks, web sites. There are number of ways in which a password can be used. For Instance, if somebody wants to gain access can listen for a username password as an authorized user gains access over a network. In addition, unwanted users which can mount an attack on the access gateway, entering an entire dictionary of words (or license plates or any other list) against a password field. Users may loan their password to a co-worker or inadvertently leave out a list of system passwords. But there are certain technologies and tools which helps us to make our network more secure. In remote access situations, one-time password generation assumes that a password will be compromised. Before leaving the internal network, a list of passwords that will work only one time against a given username is generated. When logging into system remotely, a password can be used only once and then will no longer be valid. Password aging is a feature that requires users to create new passwords every so often. Many organization computer networks are designed to require users to have different passwords to access different parts of the system. Single system is essentially a centralized access control list which finds who is authorized to access different areas of the computer network and a mechanism to provide the expected password.

IV. CONCLUSION

The Firewall which is used as the gateway for the network should be used in such a way that it should not allow unwanted users entering into the network . Network audit information such as log messages and network monitoring tool's record will also help in securing the network by providing information about the network access In this research paper basics of the IP address of the computer sending the packets, the IP address of the computer receiving the packets, the type of packet (TCP, UDP, etc.), The port number, and URL's which allow us to protect our system from a wide variety of hazards, including service attacks and hack attempts. Firewall has played vital role in internet security and its uses should be enhanced and the software should be improved upon.

Distributed firewalls allows the network security policy to remain the control of the system administrators. As long as more research is needed in this area to determine robustness, efficiency, and scalability

REFERENCES

[1] http://searchnetworking.techtarget.com/definition/packetfiltering?q=application+gateway

[2] http://www.techopedia.com/definition/4189/application-gateway

[3] http://searchnetworking.techtarget.com/tutorial/Introduction-to-firewalls-Types-offirewalls

[4] http://en.wikipedia.org/wiki/Firewall_(computing)

[5] http://www.thenetworkencyclopedia.com/entry/circuit-level-gateway/

[6] http://whatis.techtarget.com/definition/proxy-server

[7] http://www.academia.edu/334946/INTERNET_SECURITY_THE_ROLE_OF_FIREWALL_SYSTEM