To study the Risk or Issues of Firewall: Solution with different approach

Hiral B.Patel[1], Ravi S.Patel[2], Amit V.Patel[3]

Acharya Motibhai Patel Institute of Computer Studies
Ganpat University,Kherava

***Abstract*— Firewalls is very useful things for internet security problems for data transmission or other purpose but some times firewalls have some problems which are discussed in this research paper. Software firewalls that only block inwards traffic such as the Windows XP default firewall are useless at detecting programs on your system that are trying to communicate without your knowledge. Configuring a firewall can be difficult if you want maximum security and functionality. Software firewalls need to be enabled during the bootup process just after network connections enabled and disabled just before the network connection is closed. Vanilla Windows XP failed to do this, by not switched on its default firewall by default, and then only switched it on late in the bootup process. Some of us watched the ensuring virus infection disaster from safer sidelines. Some say you only need a hardware firewall. The problem is that few hardware firewalls will stop outward traffic from an unwanted program. Also they do not protect you if you bypass them via say a dial up modem when your broadband connection goes down. This is potentially particularly problematical if you have Windows file or printing sharing enabled as computers out there are testing all the time for this wonderful exploitable back door into a computer system.**

Key words: Firewall Technologies, Network Security, Access Control, Security Policy, Protective Mechanisms.

I. INTRODUCTION

A firewall is simply a group of components that collectively form a barrier between two networks.[1]. Firewall is a device that controls network traffic for security reasons. Firewall is nothing but a fire wall that protects building block from blocking entrance. In this paper we introduce technologies of firewall with its different types. Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Firewall protects the network against threat attacks and increases business productivity by managing network traffic that efficiently meets security needs and reduces your total cost of ownership. Firewall installation is the first step to secure business critical resources. Firewall Installation secures important resources of the businesses.

II. USES OF FIREWALLS

- Firewalls can be used to block access to particular sites on the Internet, or to prevent certain users or machines from accessing certain servers or services.
- A firewall can be used to monitor communications between your internal network and an external network. For example, you could use the firewall to log the endpoints and amount of data sent over every TCP/IP connection between your organization and the outside world.
- A firewall can even be used to eavesdrop and record all communications between your internal network and the outside world. A 56KB leased line at 100% utilization passes only 605 MB/day, meaning that a week's worth of Internet traffic can easily fit on a single 8mm digital tape. Such records can be invaluable for tracking down network penetrations or detecting internal subversion.

Such records also pose profound privacy questions, and possibly legal ones as well. Investigate these questions carefully before engaging in such monitoring.

- If your organization has more than one physical location and you have a firewall for each location, you can program the firewalls to automatically encrypt packets that are sent over the network between them. In this way, you can use the Internet as your own private wide area network (WAN) without compromising the data; this process is often referred to as creating a virtual private network , or VPN . (You will still be vulnerable to traffic analysis and denial of service attacks, however.)[2]

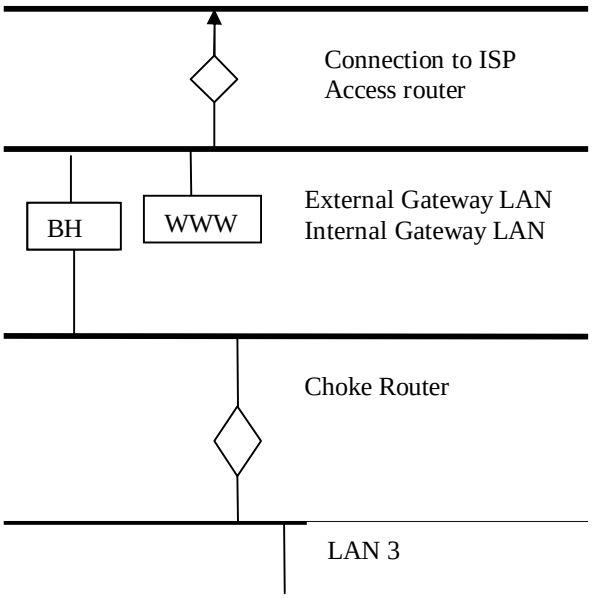
III. FIREWALL: BASIC APPROACHES

There are three basic approaches of firewalls, and we'll consider each of them

A. Application Gateways:-

The first firewalls were application gateways, and are sometimes known as proxy gateways. These are made up of bastion hosts that run special software to act as a proxy server.

Figure: 1 Application Gateway



These are also typically the slowest, because more processes need to be started in order to have a request serviced. Figure 1 shows a application gateway.

B. Packet Filtering:-

Packet filtering is a technique whereby routers have ACLs (Access Control Lists) turned on. By default, a router will pass all traffic sent it, and will do so without any sort of restrictions. Employing ACLs is a method for enforcing your security policy with regard to what sorts of access you allow the outside world to have to your internal network, and vice versa.

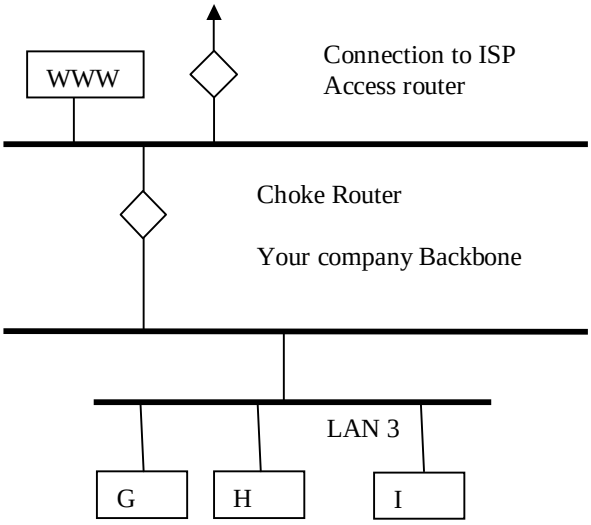
There is less overhead in packet filtering than with an application gateway, because the feature of access control is performed at a lower ISO/OSI layer (typically, the transport or session layer). Due to the lower overhead and the fact that packet filtering is done with routers, which are specialized computers optimized for tasks related to networking, a packet filtering gateway is often much faster than its application layer cousins. Figure 2 shows a packet filtering gateway.

Because we're working at a lower level, supporting new applications either comes automatically, or is a simple matter of allowing a specific packet type to pass through the gateway. (Not that the possibility of something automatically makes it a good idea; opening things up this way might very well compromise your level of security below what your policy allows.)

C. Hybrid Systems:-

In an attempt to marry the security of the application layer gateways with the flexibility and speed of packet filtering, some vendors have created systems that use the principles of both.

Figure: 2 A Sample packets filtering gateway



Other possibilities include using both packet filtering and application layer proxies. The benefits here include providing a measure of protection against your machines that provide services to the Internet (such as a public web server), as well as provide the security of an application layer gateway to the internal network. Additionally, using this method, an attacker, in order to get to services on the internal network, will have to break through the access router, the bastion host, and the choke router. [1]

IV. FIREWALL TECHNOLOGIES

The way firewalls offer protection and the level of protection vary widely. Broadly speaking, most of the available firewall technologies fall into one of the categories described below.

A. Packet Filtering:-

Packet filters, implemented on routers, filter on user defined content, such as IP address. They examine a packet at the network layer and are application independent. This allows them to deliver good performance and scalability. They are the least secure type of firewall. The reason is that they cannot understand the context of a given communication, making them easier for hackers to break [2, 5]. Packet filters have two choices with regard to outbound FTP connections. They can either leave the entire upper range of ports open (greater than 1023) [3] to allow the file transfer session to take place over the dynamically allocated port, but

exposes the internal network or they can shut down the entire upper range of ports to secure the internal network which blocks other services.

Server Client

B. Multi Layer Firewall:-

Traditional firewalls normally protect a network against external attack. An extension of this idea places firewall functionality within a network to protect it against internal attack. This strategy is presently limited, since systems used to implement firewalls are generally slow. The multi layer firewall (MLF) uses filtering functionality at layer 3 and layer2 to implement the security policy [5]. The MLF concept is implemented by using a network traffic analyzer and monitoring tool called Traffics allong with Tartan, the MLF policy management tool. Tartan consists ts of a graphical user interface to create and edit policy and a policy engine that compiles the high level MLF policy. The MLF prototype was designed by Dan Nessett, 3com Technology Develoment Center, CA and Pola Humenn, Blackwatch Technologies, Inc. NY. It is more or less like packet filtering technology, the major difference being that it does filtering at layer 2 and layer 3.

C. Stateful Inspection Firewalls:-

Stateful Inspection overcomes the limitations of the packet filters and application firewalls by providing full application - layer awareness without breaking the client/server model. With stateful inspection, the packet is intercepted at the network layer and the INSPECT Engine takes control of it. The engine extracts state related information required for the security decision from all application layers and maintains the information in dynamic state tables for evaluating subsequent connection attempts. This provides a highly secure solution and offers maximum performance, scalability, and extensibility. An example of a stateful inspection firewall is the Check Point Firewall - 1 [3].

D. Application Layer Firewalls:-

As the name implies, application gateways operate in user space at the application layer of the open system interconnection (OSI) model, controlling the traffic between directly connected networks. A separate gateway listens on the appropriate TCP/UDP port on the firewall for each protocol that the firewall relays. This approach provides a high level of control over all major TCP/IP services and allows extensive logging, neither of which packet-filtering techniques can provide. In the past, application-level firewalls performed poorly, because a new process was forked to handle each connection. See the figure below [3]: The overhead involved in forking a new process for each connection is not acceptable. The application gateways used in the AltaVista Firewall have been designed to address this limitation, without sacrificing security. Each application gateway is implemented using a single process to handle all connections

E Alarm System:-

Application Firewalls use a dedicated alarm system to monitor the security of the firewall and to respond to attempts to circumvent the security of the firewall.It can also respond to less serious anomalies such as incorrect passwords. The alarm system is implemented by the alarm daemon alarmd, which monitors events generated by application gateways or other servers on the firewall. These are communicated to alarmd by means of log messages. The alarm system associates one or more alarms with each event. Each alarm includes one or more actions to take when the event occurs. The alarm that is triggered when an event occurs depends on the state of the firewall, that is, the current level of security awareness of the firewall. The state of the firewall is represented using the colors green, yellow, orange, and red. Each color represents a different security awareness level, ranging from under no threat to under serious threat.The following list describes each state and the level of awareness associated with the state. _Green: The firewall has not detected any events, and all appears normal. _Yellow: The firewall has detected one or more events that may indicate a malicious attempt to compromise the firewall or the private network. If no further event occurs in the next two hours, the firewall returns to the green state. _Orange:

F. Authentication Service:-

When users log on to most computer systems, they specify a password to prove their identity to the system. User authentication is the process by which a computer system verifies the identity of a user or entity through a unique password. The authentication service on the firewall provides a mechanism by which the identity of a user can be verified. This allows organizations to implement security policies that specify that only certain users are allowed to use particular services to access resources through the firewall. When users wish to establish a connection, they must first identify themselves so that the firewall can associate them (via their identifiers) with the connection. This identifier is then presented by the application gateway to the ACL system, which then decides if the connection request will be allowed or denied. When an application gateway on the firewall requires a user to supply an identifier, a sequence of actions occurs as follows: _The gateway connects to authd and specifies the identifier for the user. Authd accesses the user database and, after checking that the user is registered and that the user record has not expired, determines what mechanism to use to authenticate the user.

G. The Name Service:-

The Firewall name service is implemented using a name service daemon (dnsd). Dnsd acts as a gateway accepting

DNS queries from both the private and external networks. It also accepts DNS queries directly from application gateways and supports daemons running on the firewall.

V. FIREWALL LIMITATIONS

As pointed out in [10], "Information security professionals often find themselves working against misconception and popular opinions formed from incomplete data. Some of these opinions spring more from hope than fact, such as the idea that internal network security can be solved simply by deploying a firewall".

- A firewall is by its nature perimeter defense, and not geared to combating the enemy within, and consequently no useful counter measure against a user who abuses authorized access to the domain.

A firewall is no real defense against malicious code problems like viruses and Trojan horses, although some are capable of scanning the code for telltale signs.

- Configuring packet-filtering rules tends to be complicated process in the course of which errors can easily occur, leading to holes in the defence. In addition, testing the configured rules tends to be a lengthy and difficult process due to the shortcomings of current testing tools. Normal packet-filtering routers cannot enforce some security policies simply because the necessary information is not available to them. [7]

VI. FIREWALL ISSUES

1) Software firewalls that only block inwards traffic such as the Windows XP default firewall are useless at detecting programs on your system that are trying to communicate without your knowledge. This has become a big problem, particularly if you have the bad luck to install malware by mistake, because with this type of Firewall you will miss easily generated warnings that you have a problem.

2) Two software firewalls are dysfunctional. They usually fight each other and your system grinds to a halt (Honourable exception Unix where an Itables firewall like configuration might well coexist with a higher level firewall but this is detail for Nerds)

3) Configuring a firewall can be difficult if you want maximum security and functionality. Luckily most decent firewalls now come with reasonable defaults with good interfaces.

4) Software firewalls need to be enabled during the bootup process just after network connections enabled and disabled just before the network connection is closed. Vanilla Windows XP failed to do this, by not switched on its default firewall by default, and then only switched it on late in the bootup process. Some of us watched the ensuring virus infection disaster from safer sidelines.

5) Software firewalls can be disabled by user action or during updates. Hardware firewalls are safer.

6) Some say you only need a hardware firewall. The problem is that few hardware firewalls will stop outward traffic from an unwanted program. Also they do not protect you if you bypass them via say a dial up modem when your broadband connection goes down. This is potentially particularly problematical if you have Windows file or printing sharing enabled as computers out there are testing all the time for this wonderful exploitable back door into a computer system. It is also probably part of the explaination Microsoft did not switch on the original XP firewall by default...all software development and most beta testing would have been done behind hardware firewalls.

VII. BENEFITS OF A FIREWALLS

Firewalls protect private local area networks from hostile intrusion from the Internet. Consequently, many LANs are now connected to the Internet where Internet connectivity would otherwise have been too great a risk.

Firewalls allow network administrators to offer access to specific types of Internet services to selected LAN users. This selectivity is an essential part of any information management program, and involves not only protecting private information assets, but also knowing who has access to what. Privileges can be granted according to job description and need rather than on an all-or-nothing basis.[9]

VIII. CONCLUSION

Firewall is useful for internet services provided by hardware and software. It is useful for protecting the data or information during the data or information transmission .firewall provides both facilities hardware as well as software with the help of firewall user can protect the internet work and here we discussed about issues and problems solving by firewall. It's our solo research paper for awareness of issues and problem and solving difficulties during the internet service.

References

[1]. Matt Curtin Introduction to Network Security March 1997
[2]. Book of Practical Unix & Internet Security, Chapter 21
[3].http://www.checkpoint.com/products/technology Check Point Software Technologies Ltd. Stateful Firewall Technology - Products and Solutions. 2000.
[4]. Oliver J Leahy Dermot M. Tynan J. Mark Smith, Sean G. Doherty. Firewall technology. Digital Technical Journal, (2), 1997.
[5]. Dan Nessett and Pola Humenn. Multilayer Firewall. 1999.
[6]. Yakomba Yavwa ,The Firewall Technology May 2, 2000
[7]. Habtamu Abie An Overview of Firewall Technologies1 January 2000
[8.]http://www.ganfyd.org/index.php?title=Issues_with_Firewalls
[9].http://www.networking\Firewall, Firewalls, Interent Security, Corporate Firewall - Vicomsoft.htm