International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 12 | Dec 2019 www.irjet.net p-ISSN: 2395-0072

Firewall- Prevent unauthorized users

Miss. Suchitra Shantaram Poskar

Student of M.Sc.I.T., D.B.J. College Chiplun, Ratnagiri, Maharashtra, 415605.

Abstract:- Several kinds of network devices like Firewalls are used to protect an institutional network against malicious attacks from the public Internet. This Research paper presents a detailed study of firewall technologies which are commonly used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. A firewall cannot handle all the destructive threats which are coming from unauthorized networks. Therefore, to develop a secured network different types of firewall technologies are used. The main purpose of this paper is to apply firewall capacity along with other firewall technologies such as packet filtering, network address translation, Virtual private network and proxy services in order to prevent unauthorized accesses.

A Firewall consists of software which controls the network traffic and also of hardware components like the arrangement of router, public servers, and work stations and so on. Firewall Software is a basic requirement for anyone using broadband to prevent hacking, virus and other security risks. A firewall is a software that establishes a security perimeter whose main task is to block or restrict both incoming and outgoing information over a network.. Typically firewall software works by hiding your computer from unknown persons. The firewall best solution for very critical and dangerous network threats.

Keywords: Firewalls, types of firewall, Working of firewall, Limitations of firewall, Is need of firewall? Advantages of firewall.

Introduction:-

Security is the most important aspect in a network. There are a lot of concepts for the security. **Firewall** is one of the most important concepts related to the security. The term "**firewall**" was came to use in 1764, to describe walls which distinct the parts of a building most likely to have a fire from the rest of a structure. Firewall can be software or hardware. There is much installation software for network security. A firewall is designed in order to prevent the spread of harmful events using firewall technologies to secure the network. Packet filtering, the firewall technologies that are currently existing can be named as Network addressing translation, Circuit-Level gateways, virtual private network, Proxy service, Application proxies and Application-Level gateway. The firewall has a mechanism to allow some traffic to pass while blocking the other traffic.

Computer networks are designed to connect two or more computers located at same or different incoming in world. They are free to exchange information with any other computers. This kind of sharing is a great advantage for both individuals as well as for corporate world but as we know in today's world, most important and confidential information is also exchanged on internet so attacker can do easily attack and can find out the important information and can harm the company in any manner. That's why Firewall is important to secure the information.

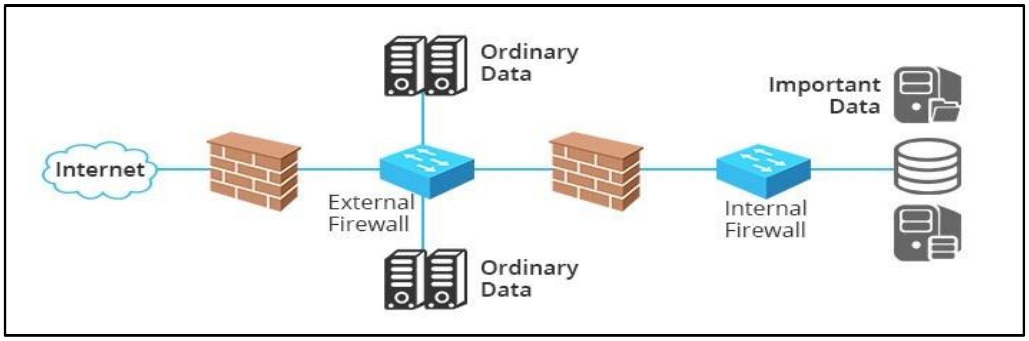


Fig:-Firewall

1) Types of Firewall:-

Hardware firewall: provides protection to a local network, Hardware firewall is usually part of TCP/IP router.

Software firewall: it is a computer with firewall software which provides protection from intruders, which may also provide internet connectivity between Private LAN and Public Network/ Internet. Maximum penetration of intruders happens and is seen on the public network only.

There are different kinds of technique which may be implemented by a firewall. Some of them are as follows :

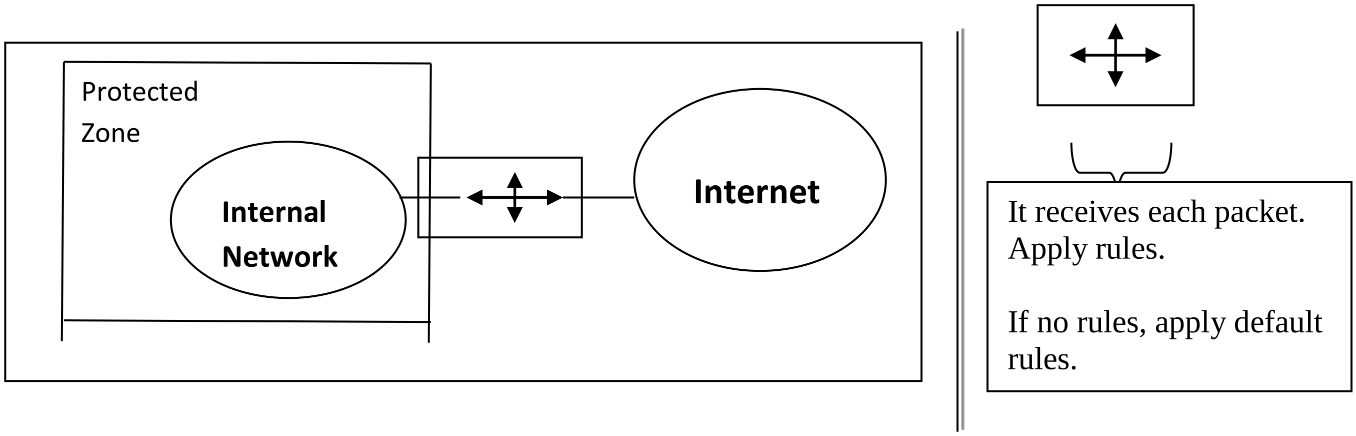
i. Packet filter
ii. Application gateway
iii. Circuit level gateway
iv. Proxy server

2. Working of Firewall:-

1. Packet Filter :

It looks at one packet at a time and then apply some set of rules to each packet and then decides to either forward the packet or discard the packet.

The rules are based on a number of fields in the IP and TCP/UDP headers i.e. Source and destination address, IP protocol field, TCP/UDP port number.



It receives each packet.
Apply rules.

If no rules, apply default rules.

Fig:- Packet Filter

Attackers can break the security with the help of following techniques:

(a) **IP ADDRESS SPOOFING:** In this type of attack, attacker send a packet to internal network, by setting source

(b)IP address equal to IP address of inside user.

Solution: we can defeat the attacker by discarding all packets which has the same source address equal to internal address.

(c) **SOURCE ROUTING ATTACKS:** Here attacker specify the route that is followed by the packet to move along the internet so that packet filter can be fooled to bypass its normal checks.

Solution: the solution of this attack is discard all packets that use this option.

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

Application gateways provide high-level secure network system communication. For example, when a client requests access to server resources such as files, Web pages and databases, the client first connects with the proxy server, which then establishes a connection with the main server.

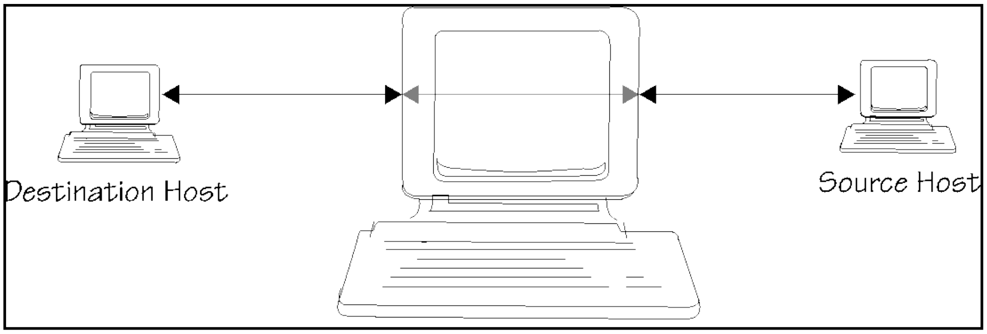


Fig:-Application Gateway

3. Circuit level gateway

A circuit-level gateway is a firewall that provides User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) connection security, and works between an Open Systems Interconnection (OSI) network model’s transport and application layers such as the session layer. Unlike application gateways, circuit-level gateways monitor TCP data packet handshaking and session fulfillment of firewall rules and policies. A proxy server is a security barrier between internal and external computers, while a circuit-level gateway is a virtual circuit between the proxy server and internal client.

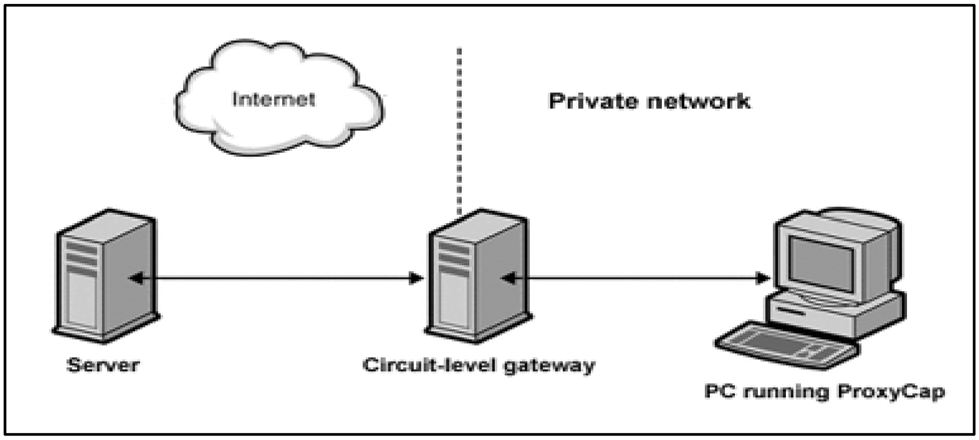


Fig:-Circuit level gateway

4. Proxy Service :

- A proxy server is a type of gateway that hides the true network address of the computer connecting through it.
- A proxy server connects to the internet, makes the requests for pages, connections to servers etc and receives the data on behalf of computer behind it.

— A firewall capabilities lie in the fact that a proxy can be configured to allow only certain types traffic to pass.
— Proxy firewalls are considered to be the most secure type of firewall because they prevent direct network contact with other systems.

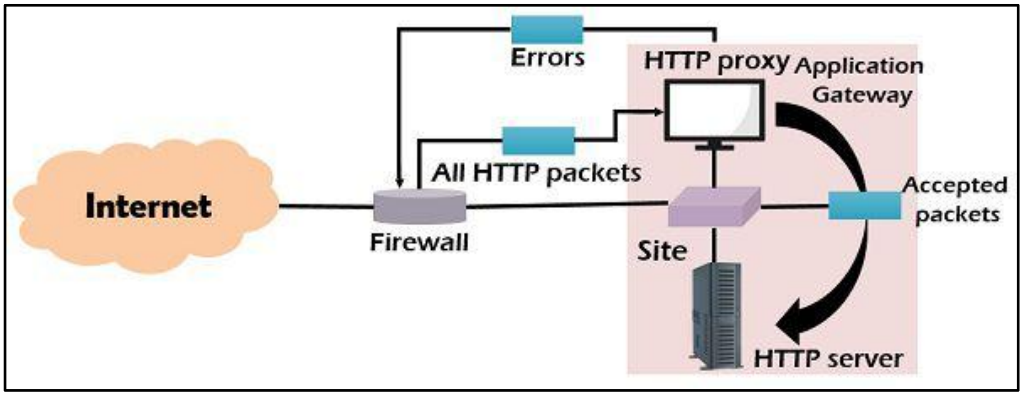


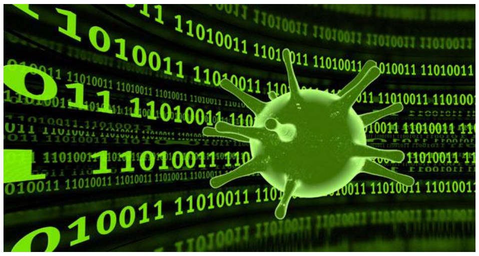
Fig:- Proxy server

3. Limitations of firewall:

Till now as we discussed about all the security it provides to us and also a firewall is an extremely useful security measure for any organization but at the same time it does not solve all the practical security problems. Its main limitations are as follows:

(i) **Virus attacks:**

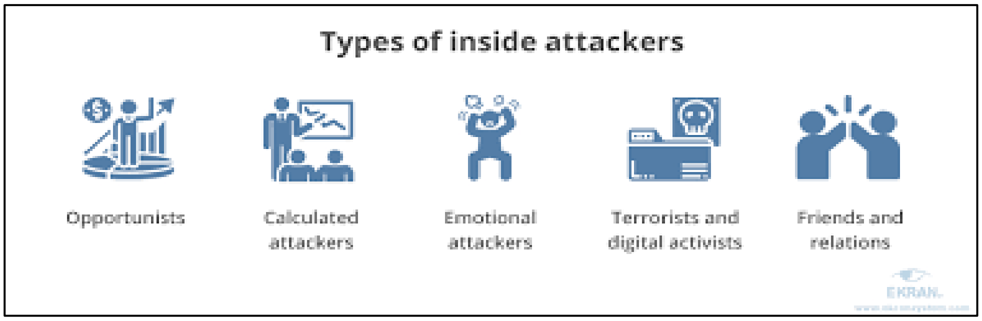
A firewall can not completely protect the internal network from virus threats because it can not scan every incoming packet for virus contents.



(ii) **Insider's intrusion:**

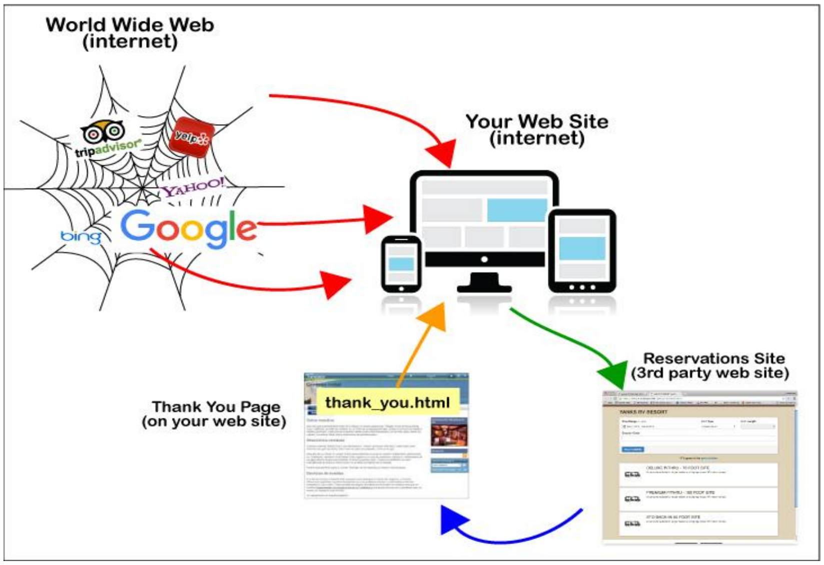
A firewall is designed to protect insider from outside attacks but if an inside user attacks the internal network, the firewall cannot prevent from such type of attack.

An insider attack is a malicious attack perpetrated on a network or computer system by a person with authorized system access.



(iii) **Direct internet traffic:**

Direct traffic is defined as visits with no referring website. When a visitor follows a link from one website to another, the site of origin is considered the referrer. These sites can be search engines, social media, blogs, or other websites that have links to other websites. Direct traffic categorizes visits that do not come from a referring URL.


World Wide Web (internet)
tripadvisor
yelp
YAHOO!
bing
Google
Your Web Site (internet)
Reservations Site (3rd party web site)
Thank You Page (on your web site)
thank_you.html

4. Is need of Firewall?

Yes, we need a firewall because the main goal of firewall to protect the system.

If your PC is connected to the Internet, you are a potential target to an array of cyber threats, such as hackers, key loggers, and Trojans that attack through un patched security holes. This means that if you, like most people shop and bank online, are vulnerable to identity theft and other malicious attacks.

Firewalls work like a filter between your computer/network and the Internet. You can program what you want to get out and what you want to get in. Everything else is not allowed. There are several different methods firewalls use to filter out information, and some are used in combination. These methods work at different layers of a network, which determines how specific the filtering options can be.

A firewall works as a barrier, or a shield, between your PC and cyber space. When you are connected to the Internet, you are constantly sending and receiving information in small units called packets. The firewall filters these packets to see if they meet certain criteria set by a series of rules, and thereafter blocks or allows the data. This way, hackers cannot get inside and steal information such as bank account numbers and passwords from us.

For the personal use:-

- Firewall use to protect our personal computer and private network from malicious mischief.
- Viruses are often the first type of malware hat can be transmitted to computer through email or over the internet and can quickly cause a lot of damage to your files.
- It can allow all traffic to pass through except data that meets a predetermined set of criteria, or it can prohibit all traffic unless it meets a predetermined set of criteria.

5. Advantages of firewall:

- Low Cost
- Packet filters make use of current network routers

- Makes Security Transparent to End Users.
- Easy to install. High speed.
- Packet filters make use of current network routers. Therefore implementing a packet filter security system is typically less complicated than other network security solutions.
- Packet Filter generally faster than other firewall technologies because they perform fewer evaluations.

References:-

- Types of firewall,:- http://books.google.co.in/books
- Working of Firewall:- https://www.slideshare.net/ firewalls-70374684

  https://www.techopedia.com/definition/24780/circuit-level-gateway
- Limitation of firewall:- https://www.smartbugmedia.com/blog

  https://www.techopedia.com/definition/26217/insider-attack
- Is need of firewall?:- https://computertutorflorida.com/2011/09/is-a-firewall-necessary/

  https://www.slideshare.net/vaishiika/firewalls-70374684

  https://www.comodo.com/resources/home/how-firewalls-work.php
- Advantages of firewall:- https://www.slideshare.net/vaishiika/firewalls-70374684