1. FIREWALL DESIGN PRINCIPLES:

* A Firewall forms a barrier through which the traffic going in each direction must pass. A firewall security policy dictates which traffic is authorized to pass in each direction.

* A firewall may be designed to operate as a filter at the level of IP packets, or may operate at higher protocol layer.

* Information Systems in Corporation, government agencies, other organizations have undergone a steady evolution.

  - Centralized data processing system, with a central mainframe supporting a number of directly connected terminals.
  - Local Areal Networks interconnecting PCs and terminals to each other and the mainframe.
  - Permises network, Consisting of a number of LANs interconnecting PCs, Servers, perhaps mainframe / two.
  - Enterprise-wide network, Consisting of multiple, geographically distributed permises networks interconnected by a private Wide Area Network (WAN)
  - Internet Connectivity, in which the various permises networks all hook into the internet and may or may not also be connected by private WAN.

* Internet connectivity is no longer an option for most organizations. However while internet access provides benefits to the organization, it enables the outside world to reach and interact with local network assert.

* This Creates the threat to the organization While it is possible to equip each workstation and server on the premises network with strong security features,
  - Intrusion protection
  - Firewall.

* The firewall is inserted between the permise network and internet to establish a controlled link and to erect an outer security wall or perimeter.

* The aim of the perimeter is to protect the permises network from internet based attacks and to provide a single choke point where security, audit can be imposed.

* The firewall can be a single computer system or a set of two or more systems that cooperates to perform the firewall function.

* Firewalls can be an effective means of protecting a local system / network of systems from network based Security threats while at the same time affording access to the outside world via wide area network and Internet.

FIREWALL CHARECTERISTICS:

(1) All traffic from inside to outside and outside to inside, must pass through the firewall. This achieved by physically blocking all success to the local network except via the firewall. Various configurations are possible

(2) Various types of firewalls are used, which implement various types of security policies.

(3) The firewall itself is immune to penetration. This implies that use of a trusted system with a secure OS.
This implies that use of trusted system with secure OS.

(4) Only authorized traffic, as defined by the local security policy, will be allowed to pass.

Site's Security policy :-

* Four techniques that firewall use to control access and enforce the site's security policy is as follows,

    1. Service Control
    2. Direction control
    3. User control
    4. Behaviour control.

* Originally firewalls focused primarily on Service Control, but they have since evolved to provide all four.

Service Control:-

* Determines the type of internet services that can be accessed, inbound or outbound.
* The firewall may filter traffic on this basis of IP address, and TCP port number, May provide proxy software that receives and interprets each service request before passing it on or may host Server software itself.

Direction Control:-

* Determines the direction in which particular service request may be initiated and allowed to flow through the firewall.

User Control:-

* Controls access to a service according to which user is acheiving / attempting to access it. This feature is typically applied to users inside the firewall perimeter.

Behaviour Control:-

* Controls how particular Services are used.

  For example, the firewall may filter email to eliminate spam, or it may enable external access to only a portion of the information on a local web Server.

CAPABILITIES OF FIREWALL:-

(1) A Firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnarables services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.

(2) A Firewall provides a location for monitoring Security related events. Audits and alarms can be implemented on the firewall system.

(3) A Firewall is a convenient platform for several internet functions that are not security related.

(4) A Firewall can serve as the platform for IPsec. Using tunnel mode capability, the firewall can be used to implement Virtual private network (VPN).

FIREWALL LIMITATIONS:-

* The firewall cannot protect against attacks that bypass the firewall.
* Internal systems may have dial-out capability to connect to ISP.
* An internal LAN may support a modem pool that provides dial-in capability for travelling employees and telecommuters.

* Firewall does not protect against internal threats.
The firewall does not protect against transfer.
Threats such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.

* The firewall cannot protect against transfer of virus infected programs / files. Because variety of OS and applications supported inside the perimeter

* It would be impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, messages for viruses.

2. TYPES OF FIREWALL:

* There are three types of firewalls, are available

(1) Packet Filters

(2) Application level gateways

(3) Circuit level gateways.

Packet Filtering Router :-

* A packet filtering router applies a set of rules to each incoming IP packet and then forwards or discards the packet.

* The router is typically configured to filter packets going in both directions. Filtering rules are based on the information contained in network packet.

Source IP Address:-

The IP address of the system that originated the IP packet
Eg:- 192.178.1.1

Destination IP Address:- The IP address of the system the IP packet is trying to reach (192.168.1.2)

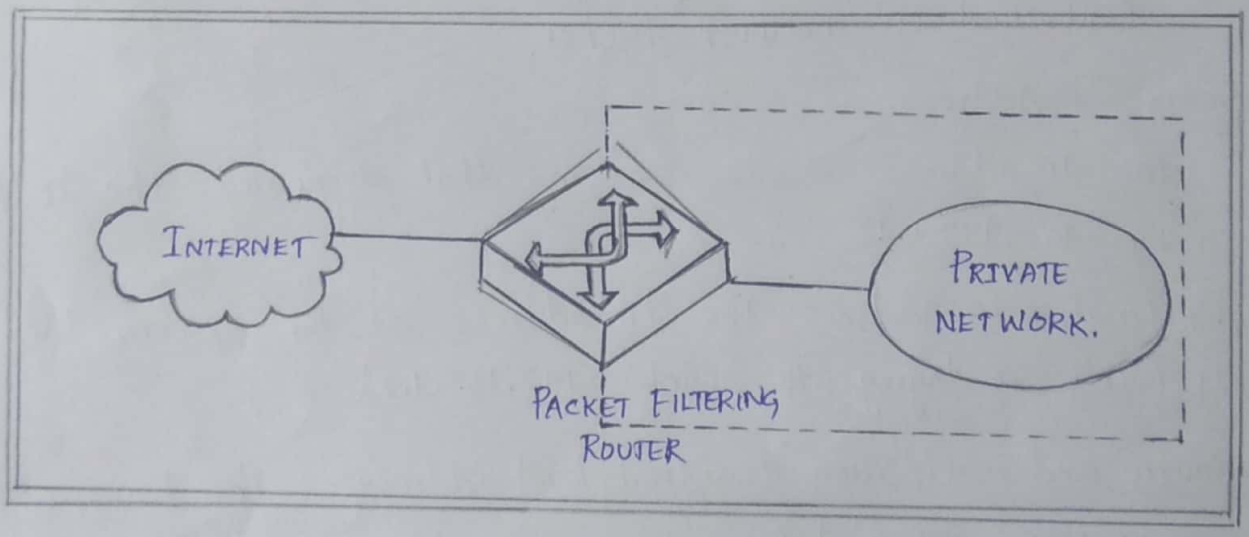
Source and Destination transport level address:- The transport level port number, which defines applications like SNMP / TELNET.

IP Protocol Field:- Defines the Transport layer

Interface :- For a router with three or more ports, which interface of the router the packet came from or which interface of the router the packet is destined for.

* The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header.
* If there is a match to one of the rules, that rule is invoked to determine whether to forward / discard the packet.
* If there is no match to any rule, then a default action is taken.
* Two default policies are possible :-
    1. Default = discard :- That is which is not expressly permitted is prohibited.
    2. Default = forward :- That which is not expressly prohibited is permitted.

Architecture:-



* The default discard policy is the more Conservative. Initially everything is blocked, and services must be added on a case-by-case basis.
* This policy is more visible to users, who are most likely to see the firewall as a hindrance.
* The default forward policy increases ease of use for end users but provides reduced security.

Advantages:-

- Packet filtering routers are Simple.
- It is transparent to the users.
- It is very fast in nature.

Weakness:-

- Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application specific vulnerabilities or functions.
- Because of the limited information available to the firewall, the logging functionality present in packet filter firewall is limited.
- It does not support advanced user authentication schemes.
- They are generally vulnerable to attacks such as layer address spoofing.
- Some of the attacks that can be made on packet filtering routers and the appropriate counter measures are the following,
    - IP address spoofing
    - Source routing attacks
    - Tiny fragment attacks.

IP address Spoofing:-

* The intruders transmit packets from the outside with a source IP address field containing an address of an Internal host.

Countermeasure:-

* To discard packet with an inside source address if the packet arrives on an external interface.

Source Routing attacks:-

* The source station specifies the route that a packet should take as it crosses the internet. ie it will bypass the firewall.

Counter measure:-

* To discard all packets that will use this option.

Tiny Fragment attacks:-

* The intruder create extremely small fragments and force the TCP header information into a separate packet fragment.
* The attacker hopes that only the first fragment is examined and the remaining fragments are passed through.

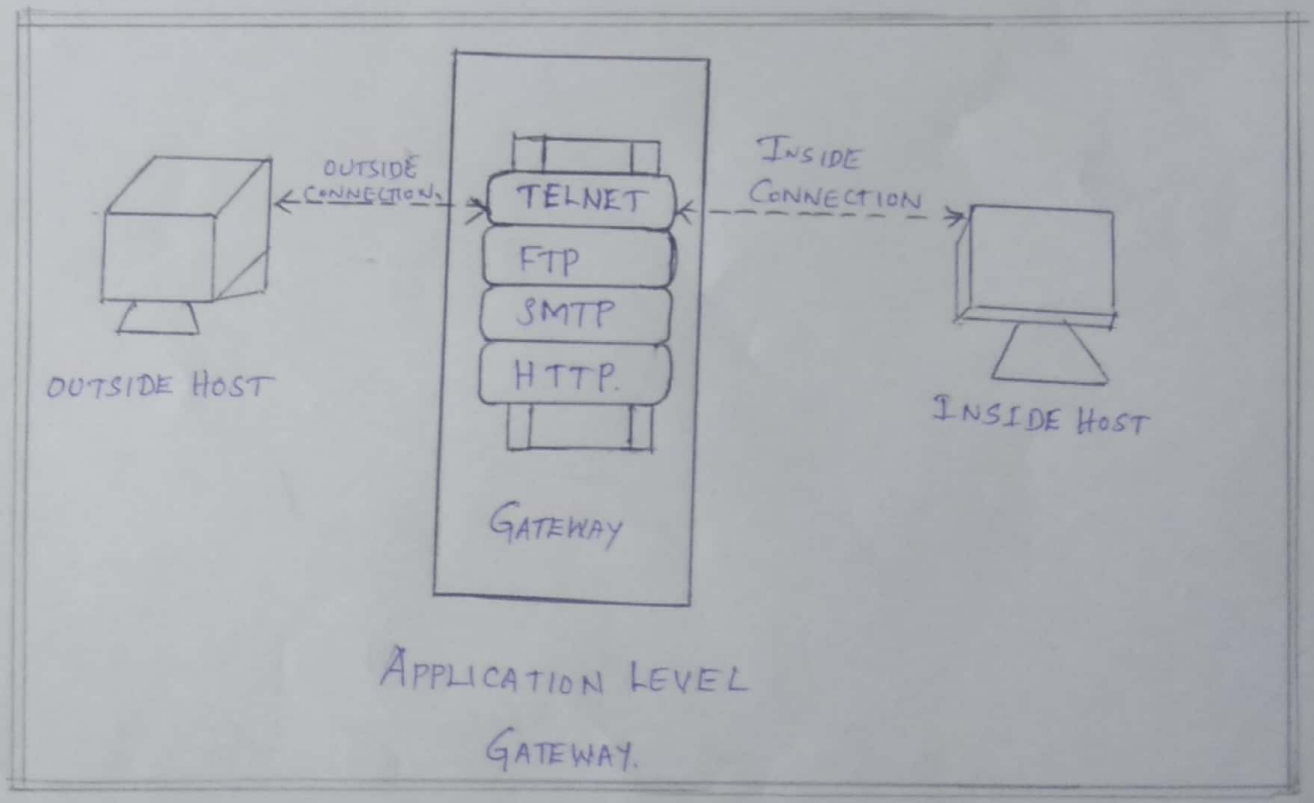
Counter measure:-

* To discard all packets where the protocol type is TCP and IP fragment offset is equal to 1.

Application level gateway:-

* An application level gateway is also called Proxy Server. acts as a relay of application level traffic.
* The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.
* When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints.

Architecture:-



APPLICATION LEVEL GATEWAY.

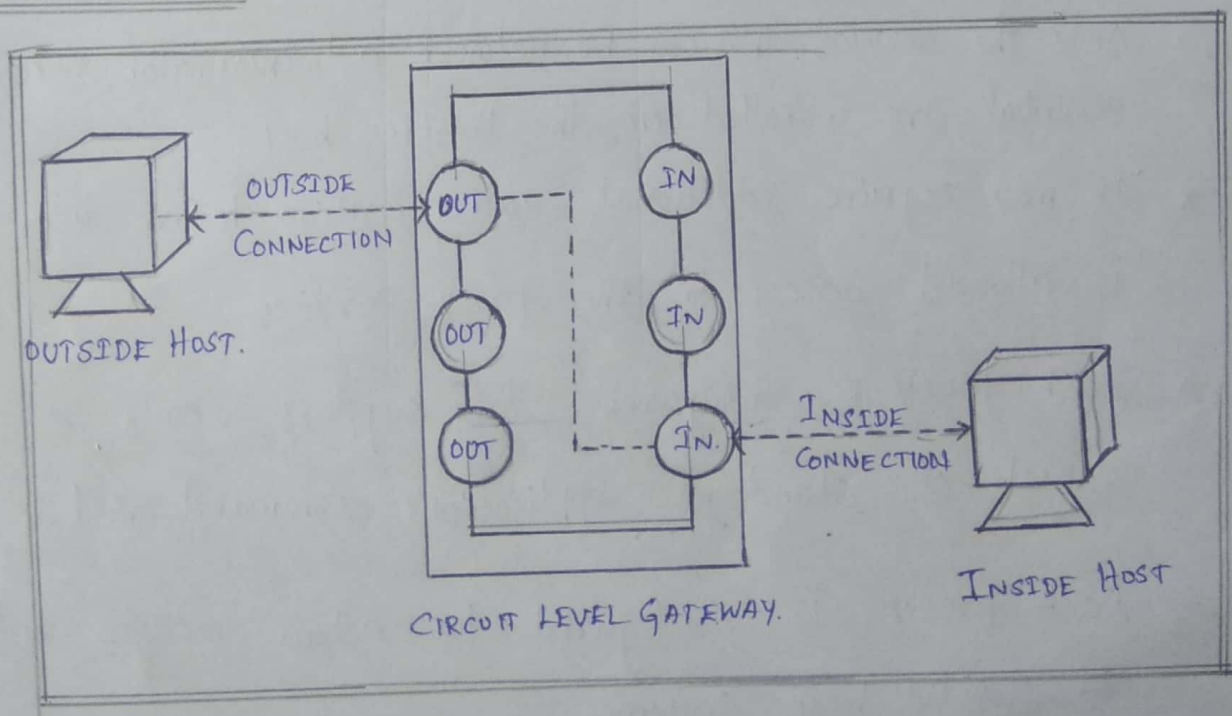
* Application level gateways tend to be more Secure than packet filters. It is easy to log and audit all incoming traffic at the application level.

* A prime disadvantage is the additional processing overhead on each connection.

Circuit level Gateway:-

* Circuit level gateway can be a stand-alone system or it can be specified function performed by an application level gateway for certain applications.
* A Circuit level gateway does not permit an end-to-end TCP connection rather the gateway sets up two TCP connections,
  - One between itself and TCP user on an inner host.
  - One between itself and TCP user on an outer host.
* Once the two connections are established, the gateway typically relays TCP segment from one connection to the other without examining the contents.
* The security function consist of determining which connections will be allowed.

Architecture:-



* A typical circuit level gateway is used in a situation in which the system administrator trust the internal users.

* The gateway can be configured to support application level or proxy service on inbound connections and circuit level functions for outbound connections.

Bastion Host:

* It is a system identified by the firewall administrator as a critical strong point in the network's security.

* The bastion host serves as a platform for an application level and circuit level gateway.

Charecteristics:-

* The Bastion host hardware platform executes a secure version of its operating system, making it a trusted system.

* Only the services that can be network administrator consider essential are installed on the Bastion host.

* It may require additional authentication before user is allowed access to the proxy services.

* Each proxy is configured to support only a subset of standard applications command set.

* Each proxy is configured to allow access only to specific host systems.

* Each proxy maintains detailed audit information by logging all traffic, each connection and the duration of each connection.
* Each proxy is independent of other proxies on the Bastion host.
* A proxy generally performs no disk access other than to read its initial Configuration file.
* Each proxy runs on a non privileged user in a private and secured directory on the Bastion host.