FIREWALLS

Firewall Characteristics

- Firewalls can be an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet.
- A firewall is inserted between the premises network and the Internet to establish a controlled link and to create an outer security wall or perimeter, forming a single choke point where security and audit can be imposed.

A firewall:

1.Defines a single choke point that keeps unauthorized users out of the protected network,

2. provides a location for monitoring security-related events

3. is a convenient platform for several Internet functions that are not security related, such as NAT and Internet usage audits or logs

4. A firewall can serve as the platform for IPSec to implement virtual private networks.

5. The firewall itself must be immune to penetration, since it will be a target of attack.

Firewall Limitations

- cannot protect from attacks bypassing it
    - eg sneaker net, trusted organisations, trusted services (eg SSL/SSH)
- cannot protect against internal threats
    - eg disgruntled employees
- cannot protect against transfer of all virus infected programs or files
    - because of huge range of O/S & file types

Design goals for a firewall:

- All traffic from inside to outside, and vice versa, must pass through the firewall

- Only authorized traffic, as defined by the local security policy, will be allowed to pass
- The firewall itself is immune to penetration

Techniques that firewalls use to control access and enforce the site's security policy:

Service control

- Determines the types of Internet services that can be accessed, inbound or outbound

Direction control

- Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall

User control

- Controls access to a service according to which user is attempting to access it

Behavior control

- Controls how particular services are used

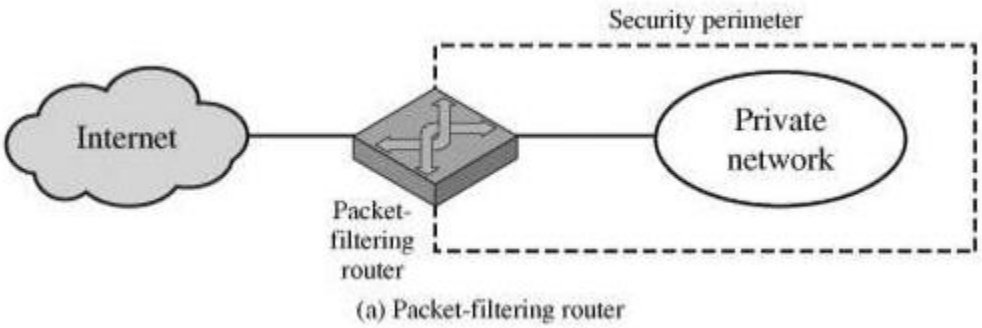
5.4 TYPES OF FIREWALLS

- Packet Filters
- Application-Level Gateways
- Circuit-Level Gateways

1. 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 a network packet:
    - Source IP address
    - Destination IP address
    - Source and destination transport level address Interface

- Interface



(a) Packet-filtering router

- 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 or discard the packet. If there is no match to any rule, then a default action is taken.
- Two default policies are possible:
  - Default = discard: That which is not expressly permitted is prohibited.
  - Default = forward: That which is not expressly prohibited is permitted.

Some of the attacks that can be made on packet-filtering routers

• IP address spoofing: where intruder transmits packets from the outside with internal host source IP address

• Source routing attacks: where source specifies the route that a packet should take to bypass security measures

• Tiny fragment attacks: intruder uses the IP fragmentation option to create extremely small fragments and force the TCP header information into a separate fragment to avoid filtering rules needing full header info

Example

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

Advantages of packet filter router

- Simple
- Transparent to users
- Very fast

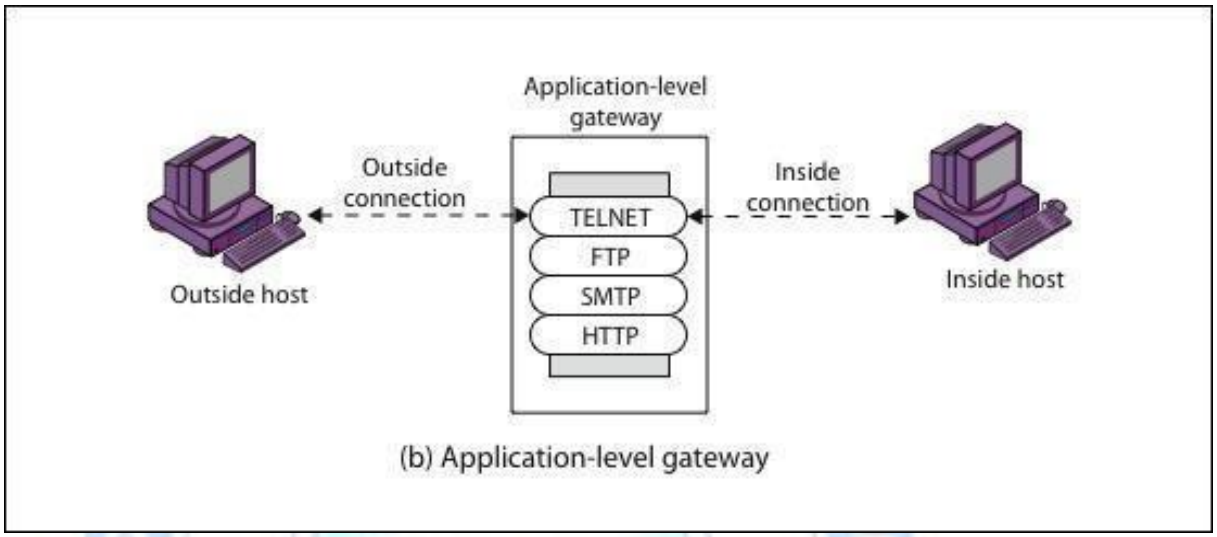
Weakness of packet filter firewalls

- Because packet filter firewalls do not examine upper-layer data, they can not prevent attacks that employ application specific vulnerabilities or functions.
- 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.

2. Application level gateway

- An Application level gateway, also called a 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.

- 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.



(b) Application-level gateway

3. Circuit-Level Gateway

- Circuit level gateway can be a stand-alone system or it can be a 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,
    - between itself and a TCP user on an inner host
    - between itself and a TCP user on an outer host.
- Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents.
- The security function consists of determining which connections will be allowed.
- A typical use of circuit-level gateways is a situation in which the system administrator trusts 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.
- Example of implementation is the SOCKS package