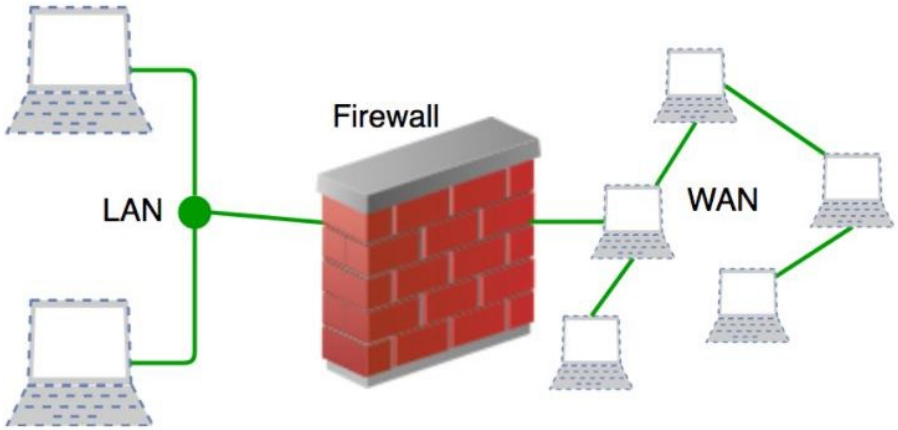
FIREWALLS

- A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.
- **Accept :** allow the traffic
  Reject : block the traffic but reply with an "unreachable error"
  Drop : block the traffic with no reply
- A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



- **Firewall design principles**
- The firewall is inserted between the premise network and internet to establish a controlled link and to erect an outer security wall or perimeter.
- The aim of this perimeter is to protect the premises network from internet based attacks and to provide a single choke point where security and audit can be imposed.
- The firewall can be a single computer system or a set of two or more systems that cooperate to perform the firewall function.
- **Firewall characteristics:**
- All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass.
- Various types of firewalls are used, which implement various types of security policies.
- The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.
- This implies that use of a trusted system with a secure operating system.
- Four techniques that firewall use to control access and enforce the site‟s security policy is as follows:
- 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 the server software itself, such as web or mail service.
- 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 attempting to access it.

Behavior control – controls how particular services are used.

- **Capabilities of firewall**
- A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.
- A firewall provides a location for monitoring security related events. Audits and alarms can be implemented on the firewall system.
- A firewall is a convenient platform for several internet functions that are not security related.
- A firewall can serve as the platform for IPsec.
- **Types of firewalls**

- There are 3 common types of firewalls.

• Packet filters

• Application-level gateways

• 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 a network packet:

· Source IP address – IP address of the system that originated the IP packet.

· Destination IP address – IP address of the system, the IP is trying to reach.

· Source and destination transport level address – transport level port number.

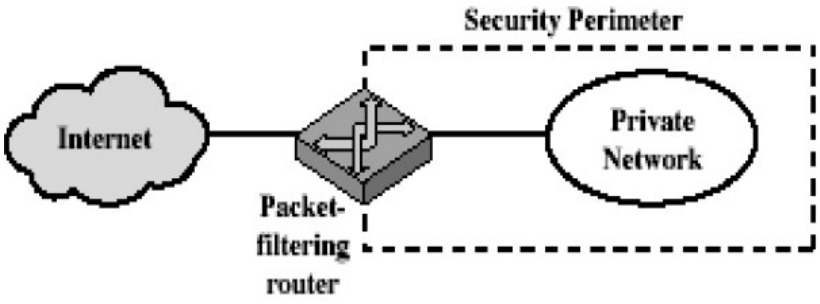
· IP protocol field – defines the transport protocol.

· Interface – for a router with three or more ports, which interface of the router the packet come 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 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.



(a) Packet-filtering router

- **Advantages of packet filter router**

· Simple

· Transparent to users

· Very fast

- **Weakness of packet filter firewalls**

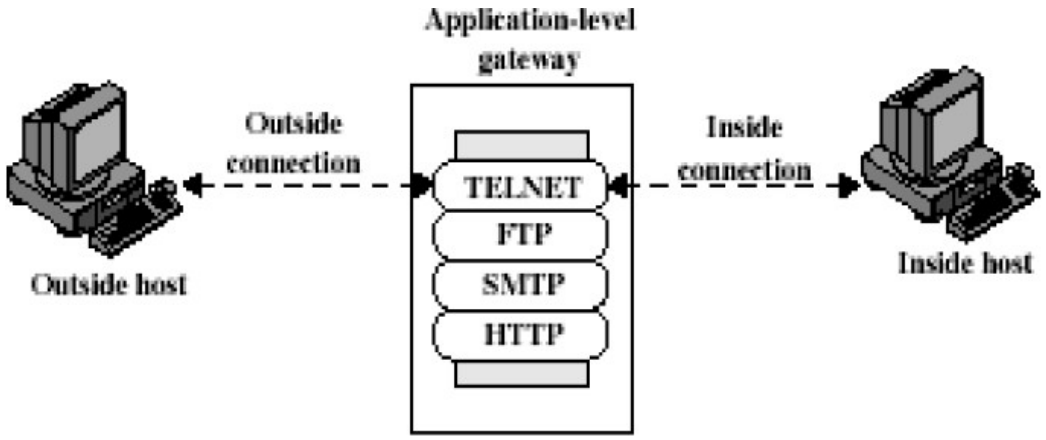
· Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application specific vulnerabilities or functions.

· 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.

- **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

- **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 gatewaysets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outer host.
- Once the two connections are established, the gateway typically relays TCP segments fromone connection to the other without examining the contents.
- The security function consists of determining which connections will be allowed.

- **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.
- Common characteristics of a Bastion host are as follows:

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

- Only the services that the network administrator considers essential are installed on theBastion host.
- It may require additional authentication before a user is allowed access to the proxyservices.

· Each proxy is configured to support only a subset of standard application‟s 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 Bastionhost

Firewall configurations

There are 3 common firewall configurations.

1. Screened host firewall, single-homed basiton configuration

In this configuration, the firewall consists of two systems: a packet filtering router and a bastionhost. Typically, the router is configured so that

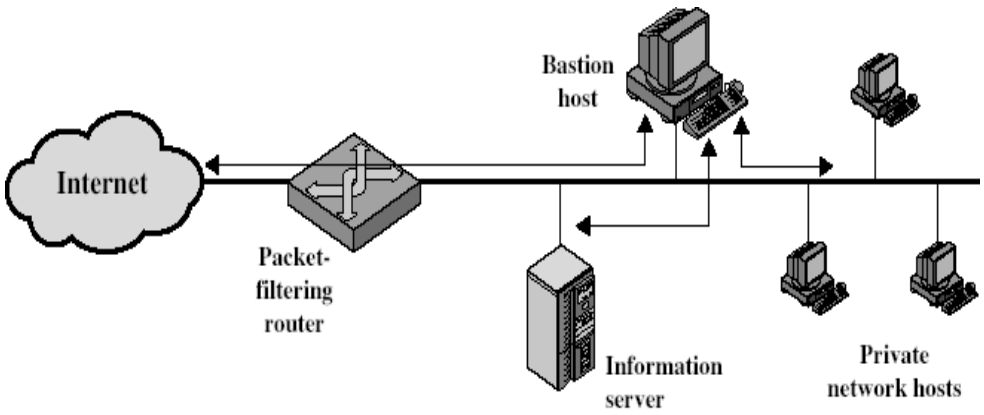
For traffic from the internet, only IP packets destined for the basiton host are allowed in.

For traffic from the internal network, only IP packets from the basiton host are allowed out.

The basiton host performs authentication and proxy functions. This configuration has greater security than simply a packet filtering router or an application level gateway alone, for two reasons:

This configuration implements both packet level and application level filtering, allowingfor considerable flexibility in defining security policy.

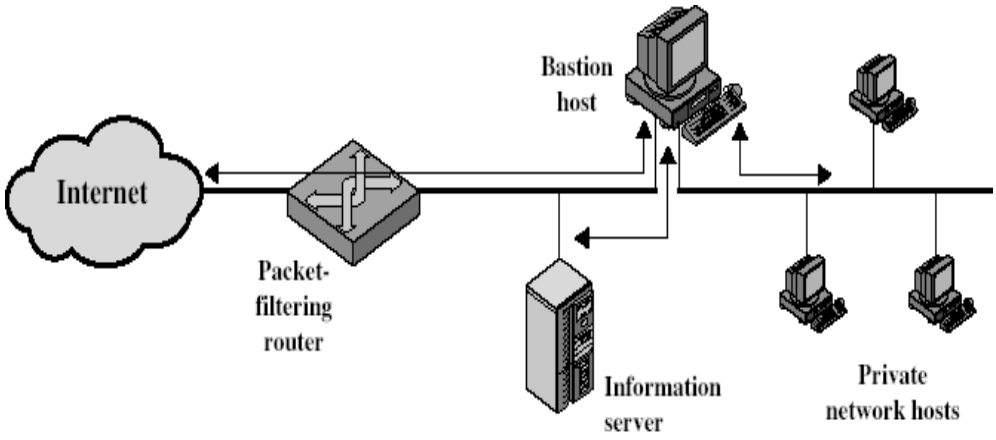
An intruder must generally penetrate two separate systems before the security of theinternal network is compromised.



(a) Screened host firewall system (single-homed bastion host)

2. Screened host firewall, dual homed basiton configuration

In the previous configuration, if the packet filtering router is compromised, traffic could flow directly through the router between the internet and the other hosts on the private network. This configuration physically prevents such a security break.



(b) Screened host firewall system (dual-homed bastion host)

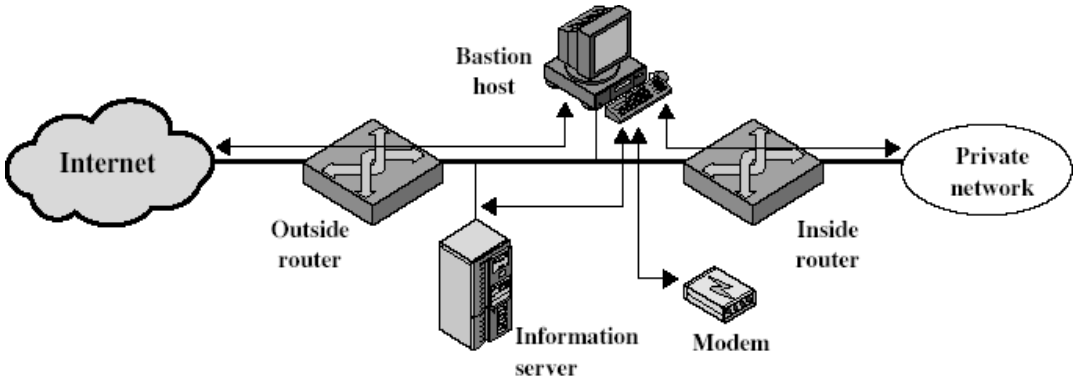
3. Screened subnet firewall configuration

In this configuration, two packet filtering routers are used, one between the basiton host and internet and one between the basiton host and the internal network. This configurationcreates an isolated subnetwork, which may consist of simply the basiton host but may also include one or more information servers and modems for dial-in capability. Typically both the internet and the internal network have access to hosts on the screened subnet, but traffic acrossthe screened subnet is blocked. This configuration offers several advantages:

There are now three levels of defense to thwart intruders.

The outside router advertises only the existence of the screened subnet to the internet; therefore the internal network is invisible to the internet.

Similarly, the inside router advertises only the existence of the screened subnet to the internal network; therefore the systems on the internal network cannot construct direct routes to the internet.



(c) Screened-subnet firewall system

Trusted systems

One way to enhance the ability of a system to defend against intruders and malicious programs is to implement trusted system technology.

Data access control

Following successful logon, the user has been granted access to one or set of hosts and applications.This is generally not sufficient for a system that includes sensitive data in its database. Throughthe user access control procedure, a user can be identified to the system. Associated with each user, there can be a profile that specifies permissible operations and file accesses. The operating system can then enforce rules based on the user profile. The database management system, however, must control access to specific records or even portions of records. The operating system may grant a user permission to access a file or use an application, following which there are no further security checks, the database management system must make a decision on each individual access attempt. That decision will depend not only on the user's identity but also on the specific parts of the data being accessed and even on the information already divulged to the user.

A general model of access control as exercised by an file or database management system is that of an access matrix. The basic elements of the model are as follows:

Subject: An entity capable of accessing objects. Generally, the concept of subject equateswith that of process.

Object: Anything to which access is controlled. Examples include files, portion of files,programs, and segments of memory.

Access right: The way in which the object is accessed by a subject. Examples are read,write and execute.

One axis of the matrix consists of identified subjects that may attempt data access. Typically, this list will consist of individual users or user groups. The other axis lists the objects that may be accessed. Objects may be individual data fields. Each entry in the matrix indicates the access rights of that subject for that object. The matrix may be decomposed by columns, yielding **access control lists.** Thus, for each object, an access control list lists users and their permitted access rights. The access control list may contain a default, or public, entry.

a. Access matrix

Access control list for Program1:

Process1 (Read, Execute)

Access control list for Segment A:

Process1 (Read, Write)

Access control list for Segment B:

Process2 (Read)

b. Access control list

Capability list for Process1: Program1 (Read, Execute) Segment A (Read)

Capability list for Process2:

Segment B (Read)

c. Capability list

Decomposition by rows yields **capability tickets**. A capability ticket specifies authorized objects and operations for a user. Each user has a number of tickets and may be authorized to loan or give them to others. Because tickets may be dispersed around the system, they present a greater security problem than access control lists. In particular, the ticket must be unforgeable. One way to accomplish this is to have the operating system hold all tickets on behalf of users. These tickets would have to be held in a region of memory inaccessible to users.

The concept of Trusted Systems

When multiple categories or levels of data are defined, the requirement is referred to as multilevel security. The general statement of the requirement for multilevel security is that a subject at a high level may not convey information to a subject at a lower or noncomparable level unless that flow accurately reflects the will of an authorized user. For implementation purposes, this requirement is in two parts and is simply stated. A multilevel secure system must enforce:

No read up: A subject can only read an object of less or equal security level. This is

referred to as **simple security property.**

No write down: A subject can only write into an object of greater or equal security level. This is referred to as ***-property (star property).**

These two rules, if properly enforced, provide multilevel security.

Reference Monitor concept

The reference monitor is a controlling element in the hardware and operating system of a computer that regulates the access of subjects to objects on the basis of

security parameters of the subject and object. The reference monitor has access to a file, known as the security kernel database that lists the access privileges (security clearance) of each subject and the protection attributes (classification level) of each object. The reference monitor enforces the security rules and has the following properties:

Complete mediation: The security rules are enforced on every access, not just, fr example, when a file is opened.

Isolation: The reference monitor and database are protected from unauthorised modification.

Verifiability: The reference monitor's correctness must be provable. That is, it must be possible to demonstrate mathematically that the reference monitor enforces the security rules and provides complete mediation and isolation. Important security events, such as detected security violations and authorized changes to the security kernel database, are stored in the audit file.