4. FIREWALL

❖ **Explain in detail about Firewall design principles explain types of firewalls in detail. (April/May 2011, May/June 2011, Nov/Dec 2011)**

Firewall Design Principles

- Centralized data processing system, with a central mainframe supporting a number of directly connected terminals
- Local area networks (LANs) interconnecting PCs and terminals to each other and the mainframe
- Premises network, consisting of a number of LANs, interconnecting PCs, servers, and perhaps a mainframe or two
- Enterprise-wide network, consisting of multiple, geographically distributed premises networks interconnected by a private wide area network (WAN)
- Internet connectivity, in which the various premises networks all hook into the Internet and may or may not also be connected by a private WAN

Firewall Characteristics

1. 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, as explained later in this section.
2. 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, as explained later in this section.
3. The firewall itself is immune to penetration. This implies that use of a trusted system with a secure operating system.

Firewalls focused primarily on service control, but they have since evolved to provide all four:

- **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. For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only a portion of the information on a local Web server.

Capabilities are within the scope of a firewall:

1. 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.
2. A firewall provides a location for monitoring security-related events.
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.

Firewalls have their limitations, including the following:

1. The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out capability to connect to an ISP.
2. The firewall does not protect against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.
3. The firewall cannot protect against the transfer of virus-infected programs or files.

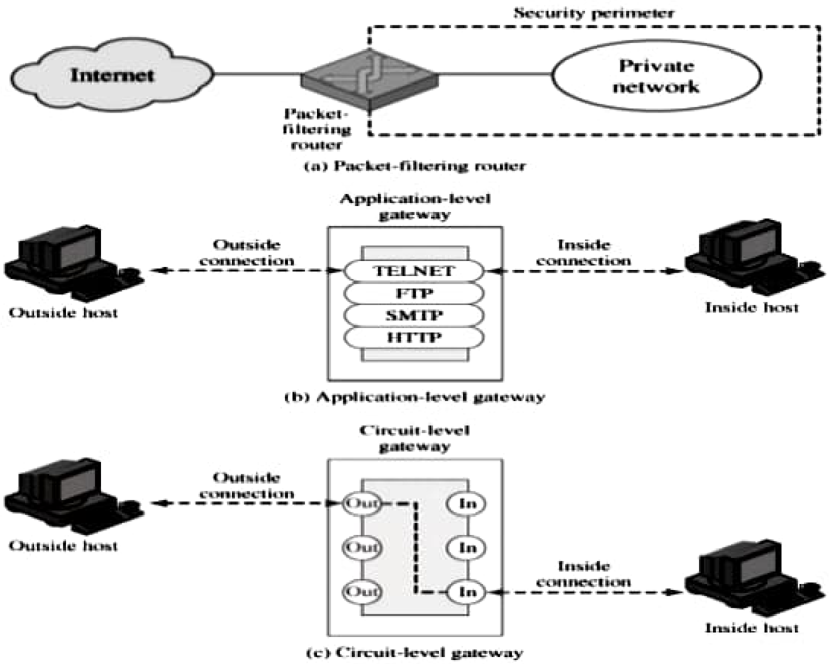
Types of Firewalls

Packet-Filtering Router

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

✔ Filtering rules are based on information contained in a network packet:

- **Source IP address:** The IP address of the system that originated the IP packet (e.g., 192.178.1.1)
- **Destination IP address:** The IP address of the system the IP packet is trying to reach (e.g., 192.168.1.2)
- **Source and destination transport-level address:** The transport level (e.g., TCP or UDP) port number, which defines applications such as SNMP or TELNET
- **IP protocol field:** Defines the transport protocol
- **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.



(a) Packet-filtering router

(b) Application-level gateway

(c) Circuit-level gateway

Figure: Firewall Types

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 and the appropriate countermeasures are thefollowing:

- **IP address spoofing**: The intruder transmits packets from the outside with a source IP address field containing an address of an internal host.
- **Source routing attacks**: The source station specifies the route that a packet should take as it crosses the Internet, in the hopes that this will bypass security measures that do not analyze the source routing information. The countermeasure is to discard all packets that use this option.
- **Tiny fragment attacks**: The intruder uses the IP fragmentation option to create extremely small fragments and force the TCP header information into a separate packet fragment.

Stateful Inspection Firewalls

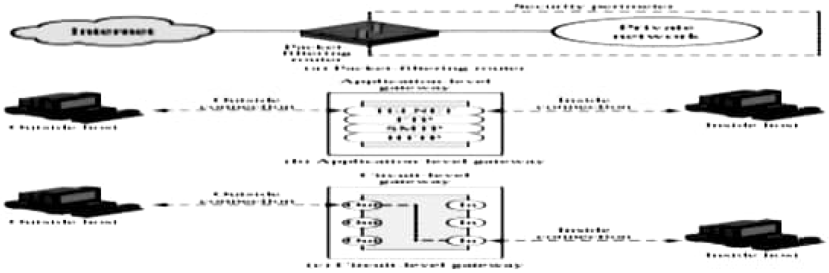
Circuit-Level Gateway

✔ 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 a TCP user on an inner host and one between itself and a TCP user on an outside host.

Bastion Host

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

Firewall Configurations



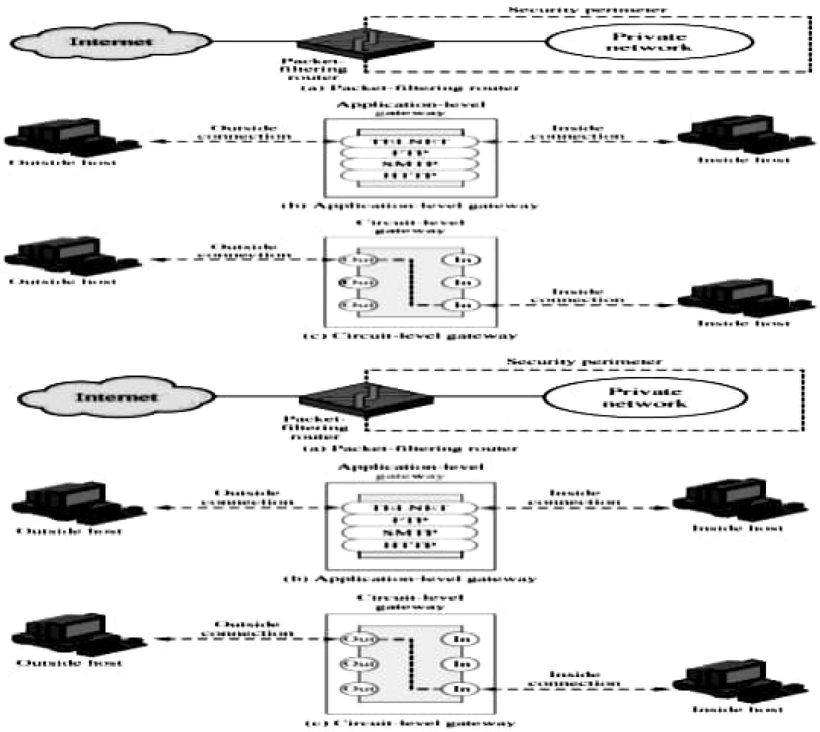


Figure: Firewall Configurations

Typically, the router is configured so that

1. For traffic from the Internet, only IP packets destined for the bastion host are allowed in.
2. For traffic from the internal network, only IP packets from the bastion host are allowed out.