Firewalls

- Firewall **isolates organization's internal network from larger outside network/Internet**.
- It can be a **hardware, software or combined system** that **prevents unauthorized access to or from internal network.**
- All data packets **entering or leaving the internal network pass through the firewall**, which **examines each packet and blocks those that do not meet the specified security criteria.**
- Deploying firewall at **network boundary** is like **aggregating the security at a single point**

Firewall is considered as an essential element for the following reasons −

- Internal network and hosts are unlikely to be properly secured.
- Internet is a dangerous place with criminals, users from competing companies, disgruntled ex-employees, spies from unfriendly countries, vandals, etc.
- To prevent an attacker from launching denial of service attacks on network resource.
- To prevent illegal modification/access to internal data by an outsider attacker.

Firewall is categorized into **three basic types** −

1. Packet filter (Stateless & Stateful)
2. Application-level gateway
3. Circuit-level gateway

Stateless & Stateful Packet Filtering Firewall

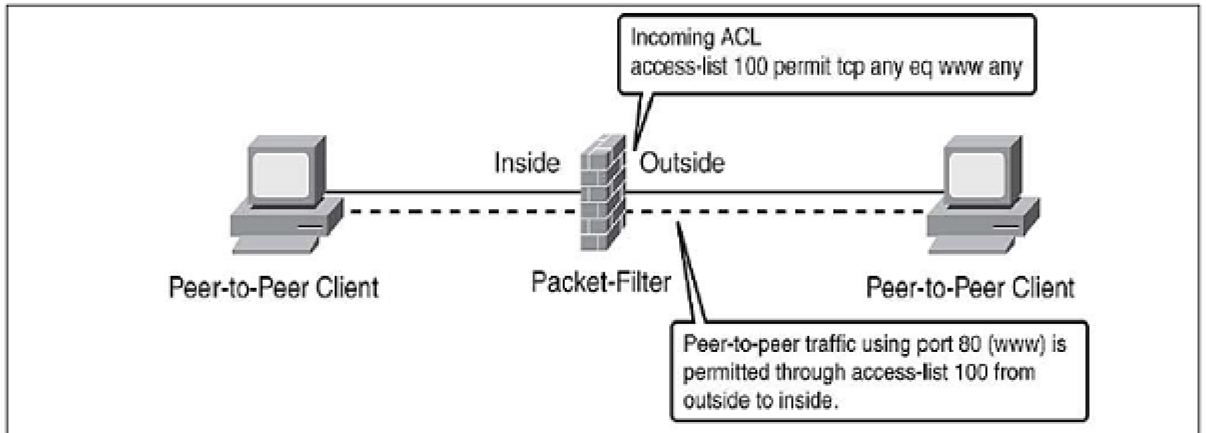
- In this type of firewall deployment, **the internal network is connected to the external network/Internet via a router firewall**. The firewall **inspects and filters data packet-by-packet**.
- **Packet-filtering firewalls** allow or block the packets mostly based on criteria such as source and/or destination IP addresses, protocol, source and/or destination port numbers, and various other parameters within the IP header and IP header fields such as ICMP message type, TCP SYN and ACK bits, etc.

Packet filter rule has two parts −

- **Selection criteria** − It is a used as a **condition and pattern matching** for **decision making**.

- **Action field** – This part specifies **action to be taken** if an IP packet meets the selection criteria. **The action could be either block (deny) or permit (allow) the packet across the firewall**.

- Packet filtering is generally accomplished **by configuring Access Control Lists (ACL) on routers or switches**. **ACL is a table of packet filter rules**.
- As traffic enters or exits an interface, **firewall applies ACLs from top to bottom to each incoming packet, finds matching criteria and either permits or denies the individual packets**.



Incoming ACL
access-list 100 permit tcp any eq www any

Peer-to-peer traffic using port 80 (www) is permitted through access-list 100 from outside to inside.

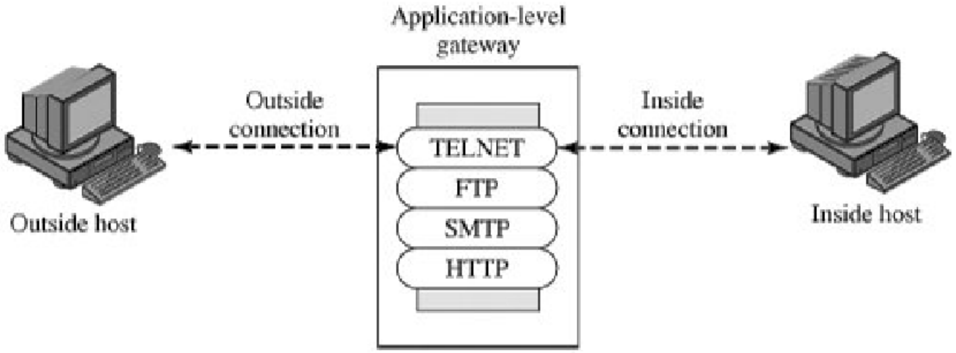
Stateless Packet Firewall

- **Stateless firewall** looks at packet and **allows it if its meets the criteria even if it is not part of any established ongoing communication**.
- Hence, such firewalls are replaced by **stateful firewalls** in modern networks. This type of firewalls offer a **more in-depth inspection method** over the only ACL based packet inspection methods of stateless firewalls.
- Stateful firewall monitors the **connection setup and teardown process to keep a check on connections at the TCP/IP level.**
- This allows them to keep track of connections state and determine which hosts have open, authorized connections at any given point in time.
- They reference the rule base only when a new connection is requested.
- Packets belonging to existing connections are compared to the firewall's state table of open connections, and decision to allow or block is taken.
- This process saves time and provides added security as well. No packet is allowed to pass the firewall unless it belongs to already established connection.

- It can timeout inactive connections at firewall after which it no longer admit packets for that connection.

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 **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.**



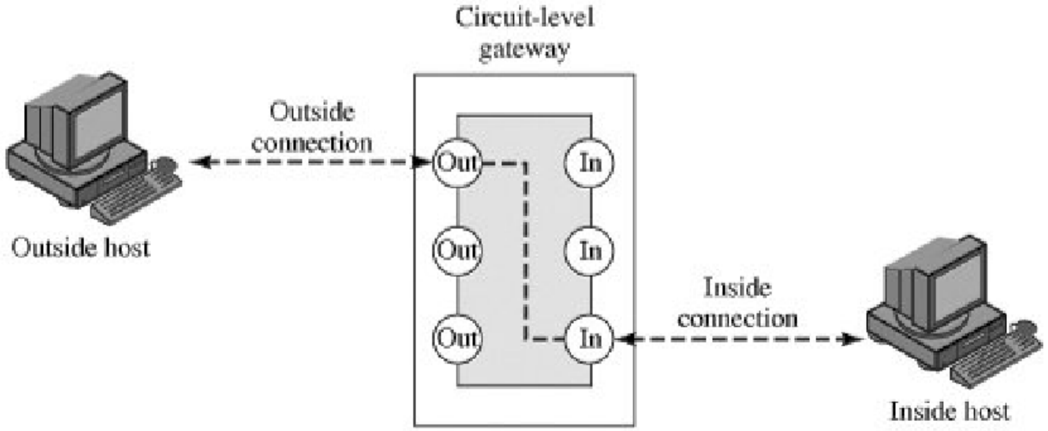
- Application-level gateways tend to be **more secure than packet filters**.

- Rather than trying to deal with the numerous possible combinations that are to be allowed and forbidden at the TCP and IP level, the application-level gateway need only scrutinize a few allowable applications.
- In addition, **it is easy to log and audit all incoming traffic at the application level**.
- A prime disadvantage of this type of gateway is **the additional processing overhead on each connection**. In effect, there are two spliced connections between the end users, with the gateway at the splice point, and the gateway must examine and forward all traffic in both directions.

3. Circuit-Level Gateway

- A third type of firewall is the circuit-level gateway.
- This can be a **stand-alone system or it can be a specialized 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 a TCP user on an inner host and one between itself and a TCP user on an outside 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.
- In this configuration, the gateway can incur the processing overhead of examining incoming application data for forbidden functions but does not incur that overhead on outgoing data.

An example of a circuit-level gateway implementation is the SOCKS package.

SOCKS consists of the following components:

- The **SOCKS server**, which runs on a UNIX-based firewall.
- The **SOCKS client library**, which runs on internal hosts protected by the firewall.
- **SOCKS-ified** versions of several standard client programs such as FTP and TELNET.

1. When a TCP-based client wishes to establish a connection to an object that is reachable only via a firewall, it must open a TCP connection to the appropriate SOCKS port on the SOCKS server system.
2. The SOCKS service is located on TCP port 1080.
3. If the connection request succeeds, the client enters a negotiation for the authentication method to be used, authenticates with the chosen method, and then sends a relay request.
4. The SOCKS server evaluates the request and either establishes the appropriate connection or denies it. UDP exchanges are handled in a similar fashion.
5. In essence, a TCP connection is opened to authenticate a user to send and receive UDP segments, and the UDP segments are forwarded as long as the TCP connection is open.