Firewall

A firewall is **an essential device or software for maintaining network security by controlling and monitoring traffic between external and internal networks**. Essentially, **a firewall sits between a trusted network (e.g., a company or home network) and an untrusted network (e.g., the internet), blocking abnormal or malicious traffic**. The main functions of firewalls are as follows:

1. Traffic Filtering

Firewalls **inspect data packets and allow or block traffic based on certain rules (policies)**. For example, they can block traffic based on specific IP addresses or ports.

2. Packet Filtering

This **filters data packets based on their source and destination IPs, ports, and protocols**. Only traffic that matches predefined rules is allowed through.

3. Stateful Inspection

The firewall **tracks the state of the traffic to ensure that the connection is valid**. It tracks allowed connections and only permits data related to those connections.

4. Network Address Translation (NAT)

Firewalls **provide NAT functionality**, which **hides the internal network's IP addresses and translates them into public IP addresses for external communication**.

5. Application Layer Filtering

This **provides more granular control by analyzing traffic related to specific applications or services**. For example, it inspects and controls traffic at the application layer, like HTTP or FTP.

Firewalls can be **implemented as software or hardware**, and they are widely used for network security in both enterprise and home environments. **As the first line of defense in network security, firewalls play a crucial role in protecting systems from cyberattacks**.