# Basic Firewall Concepts – Bullet Points

## What is a Firewall?

* A security system that controls incoming and outgoing network traffic.
* Acts as a barrier between trusted and untrusted networks.
* Filters traffic based on pre-set security rules.

## Types of Firewalls

* Packet-Filtering Firewall  
   - Filters packets based on IP address, port, and protocol.
* Stateful Inspection Firewall  
   - Tracks connection states and filters traffic accordingly.
* Application-Layer Firewall  
   - Filters traffic at the application level (e.g., HTTP, FTP).
* Next-Generation Firewall (NGFW)  
   - Includes intrusion detection, deep packet inspection, and app control.

## Firewall Rules

* Direction: Inbound (to the system) or Outbound (from the system).
* Port/Service: Specifies which ports (e.g., 22, 80) are allowed/blocked.
* Protocol: TCP, UDP, ICMP, etc.
* Action: Allow or Deny.

## Default Policies

* Default Deny Inbound: Blocks all incoming traffic unless allowed.
* Default Allow Outbound: Allows internal devices to connect out by default.

## Common Uses

* Block unused or dangerous ports (e.g., port 23 - Telnet).
* Allow secure services (e.g., SSH on port 22, HTTPS on port 443).
* Prevent unauthorized access to a system or network.
* Monitor and log network traffic for suspicious activity.

## Firewall Benefits

* Protects against unauthorized access.
* Reduces exposure to attacks and malware.
* Enforces company or personal network policies.
* Enhances system and network security.