What is a Firewall?

A **firewall** is a **security system** — either a **hardware device** or **software program** — that **monitors and controls** the data traffic going **in and out** of a computer network.

It acts as a **barrier between a trusted network (like your computer or office LAN)** and an **untrusted network (like the Internet)**.

You can think of it like a **security guard** standing at the entrance of your network — checking every piece of data that tries to enter or leave, and deciding whether to **allow it** or **block it** based on security rules. 🚧

Main Purpose of a Firewall

- Protect your computer or network from **hackers and malware**.
- Prevent **unauthorized access** to private data.
- Allow **safe network traffic** and block harmful connections.
- Monitor all **incoming and outgoing** data packets.

How a Firewall Works

Data on a network travels in small units called **packets**.
Each packet has:

- Source IP address (where it comes from)
- Destination IP address (where it's going)
- Port number (which service it's using, like web or email)

The **firewall checks each packet** against its **rules**:
✅ If it matches a "safe" rule → it's allowed.
❌ If it looks suspicious or unauthorized → it's blocked.

Example:

- Allow port 80 (HTTP) → Web browsing works.

- Block port 23 (Telnet) → Old insecure protocol is blocked.

Types of Firewalls

1. Packet Filtering Firewall

- Basic type of firewall.
- Checks source/destination IPs and ports.
- Works at the **Network Layer (Layer 3)** of the OSI model.
- Fast but not very smart (can't inspect data inside packets).

2. Stateful Firewall

- Keeps track of active connections.
- Allows only valid packets related to an established session.
- More secure than simple packet filtering.

3. Proxy Firewall (Application Layer)

- Works at the **Application Layer (Layer 7)**.
- Acts as a middleman between the user and the Internet.
- Can filter content — for example, blocking malicious websites.

4. Next-Generation Firewall (NGFW)

- Advanced firewall with **deep packet inspection**, **intrusion prevention**, and **application control**.
- Detects modern cyber threats like malware, ransomware, etc.

Why Firewalls Are Important

- Protect systems from **hackers and viruses**.
- Block **unauthorized users** from accessing private data.
- Prevent **data leaks** by monitoring outbound traffic.
- Ensure a **safe and secure network environment**.

Types by Installation

Type	Description	Example
Hardware Firewall	Physical device installed between your network and the Internet.	Cisco ASA, FortiGate
Software Firewall	Installed on computers or servers.	Windows Firewall, iptables (Linux)

Most networks use **both** — for layered protection.

In Simple Words:

A **firewall** is a **network security guard** that allows safe data and blocks harmful or suspicious data from entering or leaving your system.