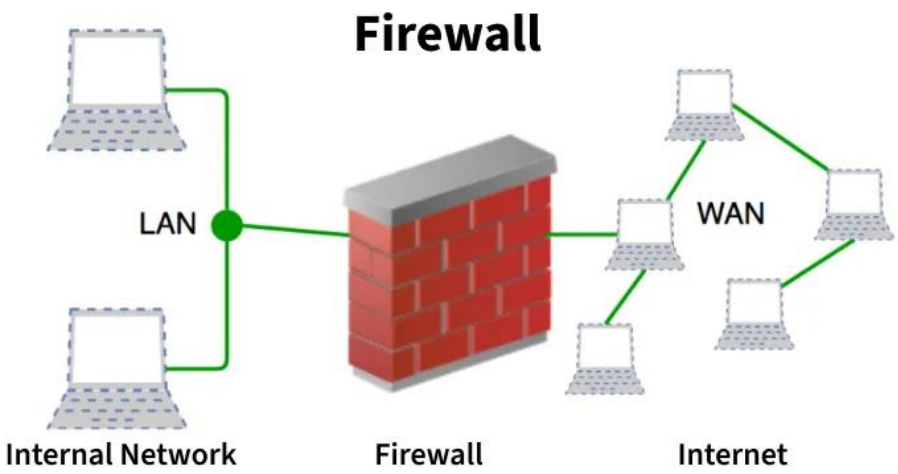
Firewall And Routing

Firewall – Summary and Key Points

- **Definition**

A **firewall** is a network security device (hardware or software) that monitors and controls **incoming and outgoing traffic** based on **predefined security rules**.
It acts as a **security guard** between your internal network and the outside world.



Firewall Actions

- **Accept:** Allow the traffic.
- **Reject:** Block the traffic but send an "unreachable" message.
- **Drop:** Block the traffic silently (no reply).

Need for a Firewall

1. **Prevent Unauthorized Access** – Keeps intruders out, like locking a door.
2. **Block Malicious Traffic** – Stops harmful or spam data.
3. **Protect Sensitive Data** – Keeps personal/business info safe.
4. **Prevent Cyber Attacks** – Defends against hackers and malware.
5. **Control Network Usage** – Limits what websites or services can be accessed.

Working of a Firewall

1. All data entering/leaving passes through the firewall.
2. Firewall checks packets against **security rules**.
3. **Allow or block** decisions are made.
4. **Logs and alerts** are generated for unusual activity.
5. **Default policy:** If no rule matches, follow *default action* (best practice: set to **drop**).

🔹 Types of Firewalls

1. Based on Network Placement

- Packet Filtering Firewall
- Stateful Inspection Firewall
- Proxy (Application-Level) Firewall
- Circuit-Level Gateway
- Web Application Firewall (WAF)
- Next-Generation Firewall (NGFW)

2. Based on System Protected

- Network Firewall
- Host-Based Firewall

3. Based on Data Filtering

- Perimeter Firewall
- Internal Firewall
- Distributed Firewall

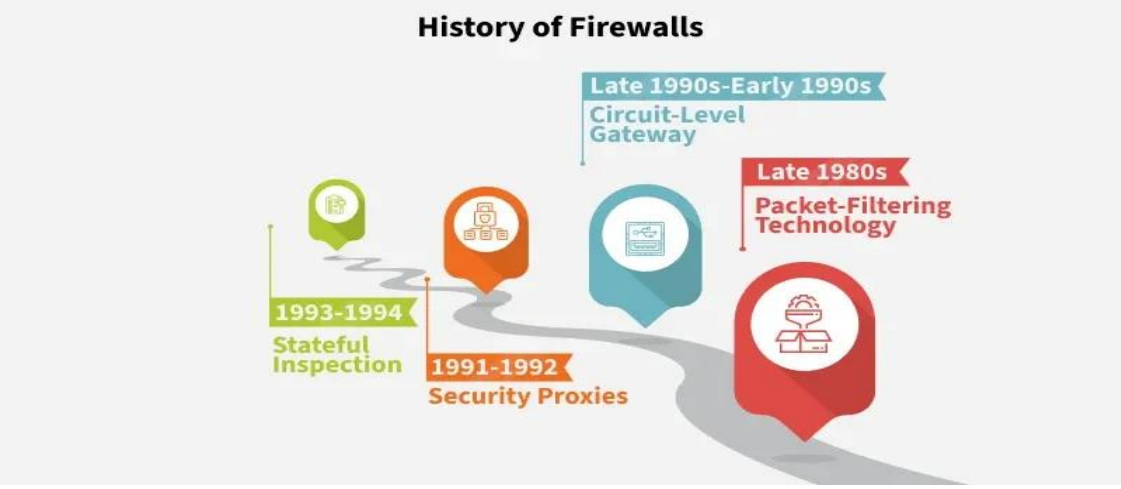
4. Based on Form Factor

- Hardware Firewall
- Software Firewall

🔹 Importance

- Acts as **first line of defense** against cyber threats.
- Filters traffic to prevent **unauthorized access**, **malware**, and **data leaks**.
- Essential for **secure communication** and **network control**.

🔹 History (Evolution)



- **1980s:** Packet Filtering – DEC Corporation.
- **Early 1990s:** Circuit-Level Gateways – AT&T Bell Labs.
- **1991–1992:** Application Firewalls (SEAL) – Marcus Ranum.
- **1993–1994:** Stateful Inspection – Check Point (Gil Shwed).

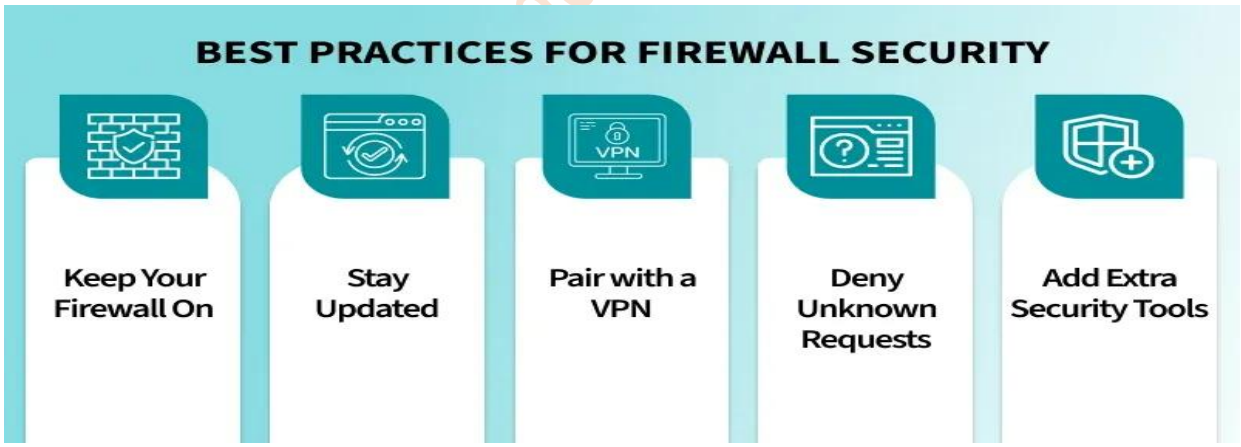
🔹 Firewall Functions

- **Monitors** and **filters** traffic.
- **Logs** and reports blocked activities.
- **Reduces attack surface** by being the only entry/exit point.
- **Prevents** both **external** (hackers, malware) and **internal** threats (unauthorized apps).

🔹 Firewall Protects Against

- Hackers, malware, and phishing attacks.
- Unauthorized network access.
- Data leaks or exfiltration.
- Inappropriate web content (via filters).
- Misuse of company networks or resources.

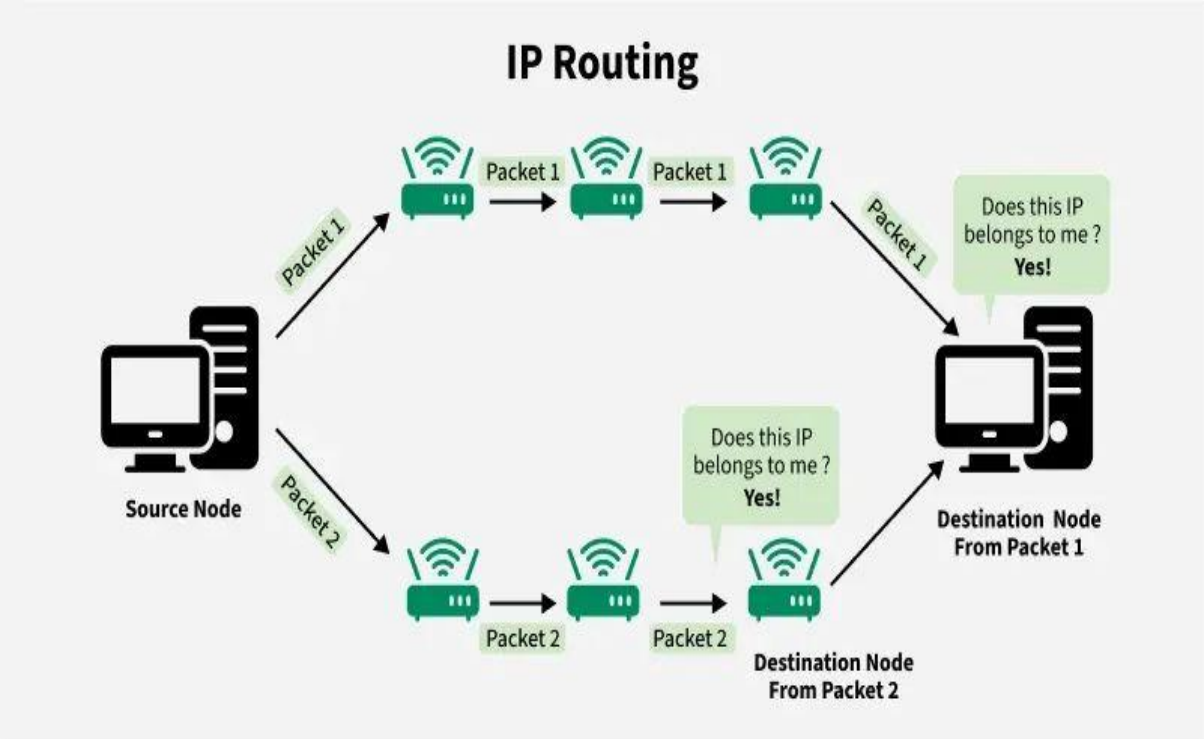
🔹 Firewall Security Best Practices



1. Always **keep the firewall enabled**.
2. **Regularly update** firewall software and firmware.
3. Use **strong security rules** and review them often.
4. Combine with **VPN** for added encryption.
5. **Monitor logs** for unusual activity.

What is Routing :

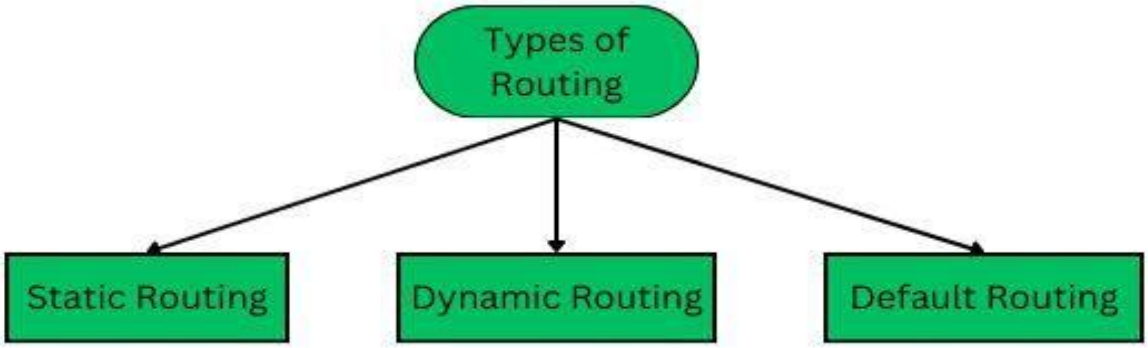
- Routing is the process of **selecting the best path** for data packets to travel across one or more networks — from **source to destination**.
  It ensures efficient and reliable communication in **packet-switched networks (like the Internet)**.
- A **router** is a **network device** that forwards data packets between networks.
- Works on **Layer 3 (Network Layer)** of the OSI model.
- Uses **IP addresses** to determine the best route.
- Connects multiple networks (e.g., LAN to WAN).



🔹 How Routing Works

1. **Source node** sends packets with destination IP in the header.
2. **Router** reads the IP, checks its **routing table**, and decides the next hop.
3. Packets move **hop by hop** until reaching the **destination node**.
4. **Hop count** limits how many routers a packet can cross; if exceeded, packet is dropped.

Types of Routing



1. **Static Routing** –
    - Routes set **manually** by admin.
    - Best for **small networks**.
    - Full control but not scalable.
2. **Dynamic Routing** –
    - Routes **automatically updated** using algorithms.
    - Adapts to network changes.
    - Best for **large networks**.
3. **Default Routing** –
    - Used when no specific route is found.
    - Packets sent to a **default gateway (0.0.0.0/0)**.
    - Common in small or single-exit networks.

Routing Process (Step-by-Step)

1. **Communication starts** between source and destination.
2. Data is **split into packets** with IP headers.
3. Routers consult **routing tables** to find the best path.
4. Packets move through **multiple hops**.
5. At the destination, packets are **reassembled** and checked for errors.

Main Routing Protocols

Protocol	Type	Description
RIP	Distance Vector	Uses hop count as metric.
OSPF	Link State	Uses Dijkstra's algorithm.
EIGRP	Hybrid	Combines distance-vector and link-state.
BGP	Path Vector	Used for routing between ISPs.
IS-IS	Link State	Common in large enterprise networks.

🔹 Routing Metrics

Metrics help determine the **best path** for data:

1. **Hop Count** – Fewer hops = better route.
2. **Bandwidth** – Higher bandwidth = faster transmission.
3. **Delay** – Lower delay = faster delivery.
4. **Load** – Less traffic = more efficient route.
5. **Reliability** – Stable links preferred.

🔹 Types of Routing Protocols

1. **Distance Vector Routing** – Shares routing tables with neighbors.
    - Uses **Bellman-Ford Algorithm**.
    - Example: RIP.
2. **Link State Routing** – Shares updates only when network changes.
    - Uses **Dijkstra's Algorithm**.
    - Example: OSPF, IS-IS.

🔹 Advantages of Routing

- Highly **scalable** for large networks.
- Enables **load balancing** and **efficient data delivery**.
- Supports **automated route management** (in dynamic routing).

🔹 Disadvantages of Routing

- **Static routing:** Not scalable, hard to manage.
- **Dynamic routing:** Uses more CPU, memory, and bandwidth.
- **Default routing:** Can be risky if not configured properly.