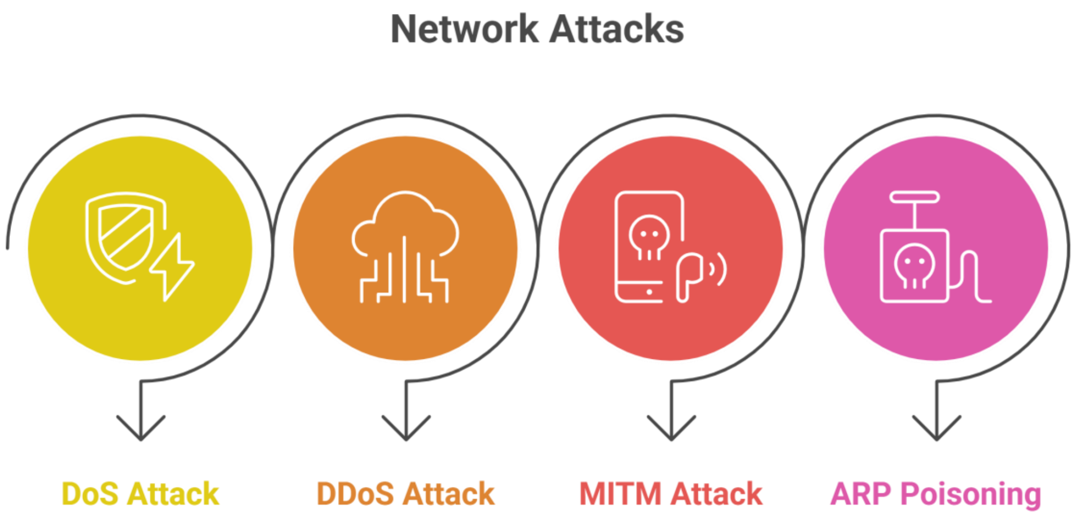
SECURITY CONCERNS AT THE NETWORK LAYER: ATTACKS (DOS, DDOS, MITM AND ARP POISONING).

Network layer security concerns involve attacks like **DoS/DDoS**, overwhelming services with traffic (e.g., flooding with requests) to cause outages, and **Man-in-the-Middle (MitM)**, where attackers intercept and alter communication between two parties, often by spoofing addresses (like ARP poisoning) to eavesdrop, steal data, or hijack sessions, disrupting confidentiality and integrity. These attacks target network protocols and infrastructure, making data unavailable or untrustworthy.



1. DoS (Denial of Service) Attack

A DoS attack is one of the simplest yet most dangerous types of network attacks. In a DoS attack, the attacker tries to make a server, website, or network unavailable to users. This is done by overwhelming the system with too many requests, causing it to slow down or crash.

Example: Imagine a shop that can only serve 50 customers at a time. A group of people intentionally blocks the entrance, so real customers cannot enter. In the digital world, the “shop” is a website, and the “people blocking the entrance” are the fake requests from the attacker.

Signs of a DoS attack:

- Websites or services become slow or unreachable.
- Servers may crash or restart frequently.
- Network traffic spikes abnormally.

How to prevent it:

- Use firewalls and intrusion detection systems.
- Limit requests from a single IP.
- Employ content delivery networks (CDNs) to absorb traffic.

2. DDoS (Distributed Denial of Service) Attack

A DDoS attack is similar to a DoS attack but more powerful. Instead of one computer, the attacker uses multiple computers or devices (often part of a botnet) to send overwhelming traffic to the target.

Example: Think of the previous shop scenario. This time, not just one group, but thousands of people from different cities block the shop. Naturally, real customers cannot enter, and the shop loses business.

Types of DDoS attacks:

- **Volume-based attacks:** Flood the network with traffic.
- **Protocol attacks:** Exploit weaknesses in network protocols like TCP or HTTP.
- **Application layer attacks:** Target specific applications, like web servers or login pages.

How to prevent it:

- Use DDoS protection services like Cloudflare or AWS Shield.
- Monitor traffic patterns for unusual spikes.
- Scale resources to handle temporary traffic surges.

3. MITM (Man-in-the-Middle) Attack

A MITM attack happens when an attacker secretly intercepts communication between two parties. The attacker can eavesdrop, modify, or steal data without the users knowing.

Example: Imagine sending a letter to your friend, but someone secretly opens it, reads it, and even changes its content before it reaches your friend. In digital terms, the “letter” can be emails, chat messages, or website data.

How attackers perform MITM attacks:

- **Wi-Fi eavesdropping:** Setting up fake Wi-Fi networks to capture data.
- **Packet sniffing:** Intercepting data packets in transit.
- **SSL stripping:** Replacing secure HTTPS connections with HTTP to capture data.

How to prevent it:

- Always use HTTPS websites.
- Avoid public Wi-Fi or use a VPN.
- Enable two-factor authentication (2FA) on accounts.
- Keep software and devices updated.

4. ARP Poisoning (Address Resolution Protocol Poisoning)

ARP poisoning is a network attack where the attacker spoofs the MAC address of a device to intercept data on a local network. It allows attackers to redirect traffic, steal sensitive information, or launch other attacks like MITM.

How it works:

- Every device on a local network has an IP and a MAC address.
- Devices use ARP (Address Resolution Protocol) to match IPs to MAC addresses.
- Attackers send fake ARP messages, tricking devices into sending data to the attacker instead of the correct destination.

Example: Imagine sending a parcel to your friend, but the delivery man is tricked into giving it to a stranger. That stranger can open it, read the contents, and even send it to your friend afterward.

How to prevent ARP poisoning:

- Use static ARP entries for critical devices.
- Deploy network security tools that detect ARP anomalies.
- Enable packet filtering and encryption to protect sensitive data.

Signs That Your Network Might Be Under Attack

Recognizing the signs of network attacks can help you respond faster:

- Slow network or unresponsive websites.
- Frequent system crashes or application failures.
- Unusual network traffic spikes.
- Unknown devices connected to your network.
- Unexpected login attempts or alerts from security systems.

General guidelines to Protect Your Network

- **Keep systems updated** – Security patches fix known vulnerabilities.
- **Use strong passwords** and change them regularly.
- **Enable firewalls and antivirus software** on all devices.
- **Segment your network** – Separate critical systems from public-facing networks.
- **Monitor logs and network traffic** for unusual activity.
- **Educate users** about phishing and safe browsing practices.

INTRODUCTION TO FIREWALLS: TYPES (PACKET FILTERING, STATEFUL INSPECTION, PROXY FIREWALLS

A firewall is a network security system, available as hardware or software, that monitors and controls incoming and outgoing traffic based on predefined rules. It acts like a security guard, filtering data packets to either:

- **Accept:** Allow the traffic.
- **Reject:** Block with an error response.
- **Drop:** Block silently without response.

Importance of Firewalls

A firewall is the first line of defense in cybersecurity, acting as a security barrier between internal systems and external networks. It forces all traffic through a single checkpoint, where data packets are monitored, filtered, and either allowed or blocked based on predefined rules. Firewalls are essential because they:

- **Prevent Unauthorized Access:** Like a locked door with a guard, only trusted users and traffic are allowed through.
- **Block Malicious Traffic:** Harmful data such as viruses, phishing attempts, or denial-of-service (DoS) attacks are stopped before reaching the system.
- **Protect Sensitive Information:** Safeguards personal and business data from theft or accidental leaks.
- **Control Network Usage:** Enforces policies such as parental controls, workplace restrictions, or government filtering.
- **Mitigate Insider Risks:** Detects suspicious applications or data exfiltration attempts from within the network.

By combining prevention, monitoring, and control, firewalls provide customizable and comprehensive protection against both external and internal threats.

Working of Firewall

A firewall inspects all incoming and outgoing traffic and decide whether to allow or block it.

1. All data packets entering or leaving the network must first pass through the firewall.
2. The firewall examines each packet against predefined security rules set by the organization.
3. If the packet matches safe rules, it is allowed; if it is suspicious, blacklisted, or contains malicious content, it is blocked.
4. Blocked or unusual traffic is recorded in logs, and real-time alerts may be generated for serious threats.
5. Since it is not possible to define every rule, the firewall applies a default policy (accept, reject, or drop). Setting the default policy to drop or reject is considered best practice to prevent unauthorized access.

TYPES OF NETWORK FIREWALLS

Here are the main types of network firewalls, organized by how they function and where they're deployed:

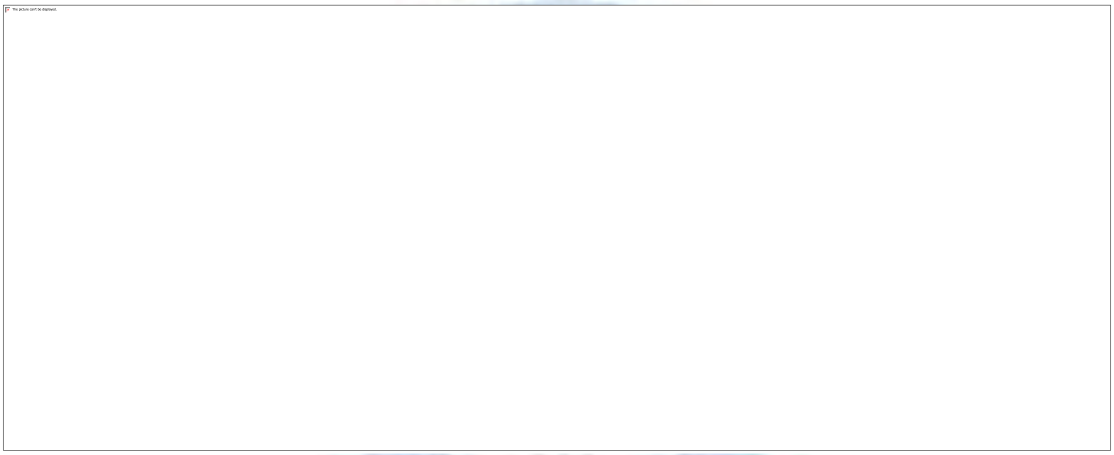
1) Based on Function (How They Filter Traffic)

Network Security is the process of protecting networks, systems, and data from unauthorized access, attacks, and damage.

a. Packet Filtering Firewall

A basic firewall that checks packet headers like IP, port, and protocol.

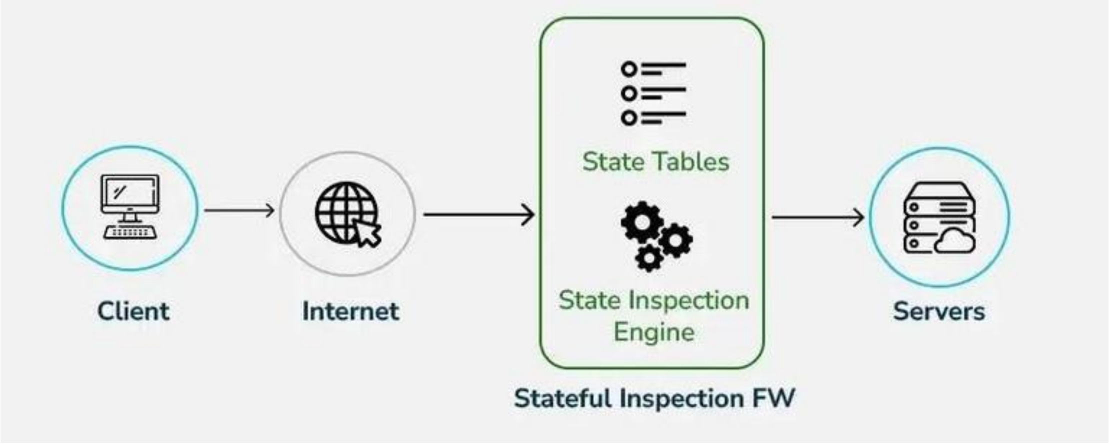
- Very fast and lightweight
- Does not inspect data inside packets
- Provides basic security only



b. Stateful Inspection Firewall

Tracks active connections and makes decisions based on traffic context.

- More secure than packet filtering
- Remembers past traffic (state table)
- Blocks suspicious or unexpected packets



c. Proxy (Application-Level) Firewall

Acts as a middleman between user and destination server.

- Filters data at the application layer
- Hides internal network details
- Can block malicious content before it reaches the user