**Firewall**

* A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predefined security rules.
* It acts as a barrier between a trusted internal network and untrusted external networks, helping to block malicious traffic and unauthorized access.
* Firewalls help protect against cyber threats like malware, viruses, intrusions, and DoS (Denial-of-Service) attacks.

**Types Of Firewalls**

* **Packet-Filtering Firewall** – It Analyze individual packets and filters them based on rules (IP address, port, protocol).
* **Stateful Inspection Firewall** - Tracks active connections and makes decisions based on the context of traffic.
* **Proxy Firewall** - Acts as an intermediary between users and the internet. Inspects the data at the application layer (e.g., HTTP, FTP).
* **Next-Generation Firewall (NGFW)** - Combines traditional firewall with advanced features like intrusion prevention, deep packet inspection, and application control.
* **Software vs. Hardware Firewalls** - Software firewalls run on devices like PCs or servers whereas Hardware firewalls are dedicated devices placed at the network’s edge.

**VPN**

* A Virtual Private Network (VPN) is a secure technology that creates an encrypted connection (tunnel) over the internet between your device and a remote server.
* It helps you browse securely, protect your data from prying eyes, and access restricted or region-locked content.
* VPNs add an extra layer of security when using unsecured public networks (e.g., at cafes or airports).

**Types of VPNs**

* **Remote Access VPN** - Used by individuals to connect to a private network securely via the internet.
* **Site-to-Site VPN** - Connects entire networks (e.g., branch offices) over the internet.
* **Client-Based vs. Network-Based VPNs** – In Client-based VPNs Software installed on the device. In Network-based VPNs It Configured on a router or firewall device.