**Assignment – 5**

**Write a short summary on Firewall and VPN.**

**What Is a Firewall:**

A firewall acts as a barrier between your internal network and external threats. It monitors and controls incoming and outgoing network traffic based on predefined security rules. Firewalls protect your devices from unauthorized access and block harmful data packets.

Types of Firewall

* Packet-Filtering Firewall: Filters data packets based on rules like IP address, port, and protocol.
* Stateful Inspection Firewall: Tracks active connections and matches incoming packets with existing ones.
* Proxy Firewall: Acts as a middleman, inspecting and filtering requests for added security.
* Next-Generation Firewall (NGFW): Offers advanced features like intrusion prevention and application control.

**Key Features of Firewalls**

* Monitors network traffic.
* Blocks unauthorized access.
* Filters harmful content and data packets.
* Prevents malware and hacking attempts.

**VPN or Virtual Private Network:**

VPN creates a secure, encrypted connection between your device and a remote server. This connection allows you to browse the internet privately and securely, hiding your IP address and encrypting your data. VPNs are commonly used to access websites or content that might be blocked in your location or to protect your online privacy on public Wi-Fi networks.

Here's a more detailed explanation:

* Encryption:

VPNs encrypt your internet traffic, making it unreadable to anyone who might intercept it, like hackers or your ISP.

* IP Masking:

Your real IP address is hidden, and your data is routed through the VPN server, making it appear as though you're connecting from the server's location, not your actual one.

* Privacy:

By masking your IP and encrypting your data, VPNs help protect your browsing history, location, and online activities from being tracked by websites and other parties.