Task 4 : Setup and Use a Firewall on Windows/Linux

**Firewall:-**

A **firewall** is a **network security system** that monitors and controls **incoming and outgoing network traffic** based on predetermined security rules. Its primary purpose is to **create a barrier** between a trusted internal network (like your home or office network) and untrusted external networks (like the internet).

**What a Firewall Does:-**

A firewall can:

* **Block unauthorized access** to your computer or network.
* **Allow legitimate communication** to pass through.
* **Prevent malicious traffic**, like hackers or malware, from entering your network.

**Types of Firewalls:-**

1. **Hardware Firewalls**:
   * Physical devices placed between your network and gateway.
   * Common in businesses for protecting large networks.
2. **Software Firewalls**:
   * Installed on individual devices (e.g., Windows Firewall).
   * Monitors traffic for that specific device.
3. **Cloud-based Firewalls**:
   * Provided as a service by vendors (Firewall as a Service - FWaaS).
   * Good for distributed networks and remote users.

**Key Functions:-**

* **Packet Filtering** – Blocks or allows data based on IP address, port, or protocol.
* **Proxy Service** – Acts as an intermediary between users and the services they access.
* **Stateful Inspection** – Monitors the state of active connections and makes decisions accordingly.
* **Deep Packet Inspection (DPI)** – Examines the actual content of packets to detect threats.

**Firewall Configuration:-**

Configuring a firewall involves setting rules that control how traffic is allowed or blocked on a computer or network. The exact steps depend on the type of firewall you're using—Windows, Linux (like iptables or UFW), or hardware firewalls (like Cisco, FortiGate, etc.).

**Type of firewall configuration:-**

**1. Windows Firewall Configuration**

**Applies to most home or office PCs**

**🔧 Steps:**

1. **Open Firewall Settings:**
   * **Go to Control Panel → System and Security → Windows Defender Firewall.**
2. **Allow or Block a Program:**
   * **Click "Allow an app or feature through Windows Defender Firewall".**
   * **Check/uncheck boxes for Private and Public networks.**
3. **Create Advanced Rules:**
   * **Click "Advanced Settings" (opens Windows Defender Firewall with Advanced Security).**
   * **You can add Inbound or Outbound Rules.**
   * **Choose rule type (Port, Program, etc.).**
   * **Specify protocol (TCP/UDP), port number, and action (Allow or Block).**

**2. Linux Firewall Configuration (UFW - Uncomplicated Firewall)**

UFW is a simple firewall interface for Ubuntu/Debian systems.

Basic Command:-

# Enable UFW

sudo ufw enable

# Deny all incoming connections by default

sudo ufw default deny incoming

# Allow all outgoing connections by default

sudo ufw default allow outgoing

# Allow SSH (port 22)

sudo ufw allow 22

# Allow HTTP (port 80)

sudo ufw allow 80

# Deny a specific IP

sudo ufw deny from 192.168.1.100

# View current rules

sudo ufw status

**3. Hardware Firewall Configuration (e.g., Cisco, FortiGate, SonicWall)**

Generally used in businesses or large networks.

**Common Steps:**

1. **Log in to Web Interface**:
   * Access firewall via browser (e.g., 192.168.1.1).
2. **Create Firewall Rules**:
   * Define **source/destination IP or zone**, **port**, **protocol**, and **action** (allow/deny).
   * Use NAT rules if mapping internal IPs to external.
3. **Set up Zones & Policies**:
   * Group devices into zones (e.g., LAN, WAN, DMZ).
   * Create policies to control traffic between zones.
4. **Enable Logging**:
   * Turn on logging for alerts and blocked attempts.

**Tips for Good Firewall Configuration:-**

* Block all **incoming traffic by default** and **allow only required services**.
* Regularly **review and update rules**.
* Enable **logging** and **monitor traffic**.
* Use **VPN** to access internal services securely.
* Close **unused ports** to minimize attack surface.

**Network Traffic Filtering:-**

Network traffic filtering is the process of controlling which **data packets** are allowed to enter or leave your device or network based on rules. These rules may consider:

* **IP address** (source or destination)
* **Port numbers**
* **Protocols (TCP/UDP/ICMP)**
* **Application-level services**

Example:

Allow only web traffic (HTTP and HTTPS) to a server and block all others.

**UFW (Uncomplicated Firewall) – Ubuntu/Debian**

UFW is a command-line tool that simplifies managing iptables.

# Enable UFW

sudo ufw enable

# Default deny all incoming, allow outgoing

sudo ufw default deny incoming

sudo ufw default allow outgoing