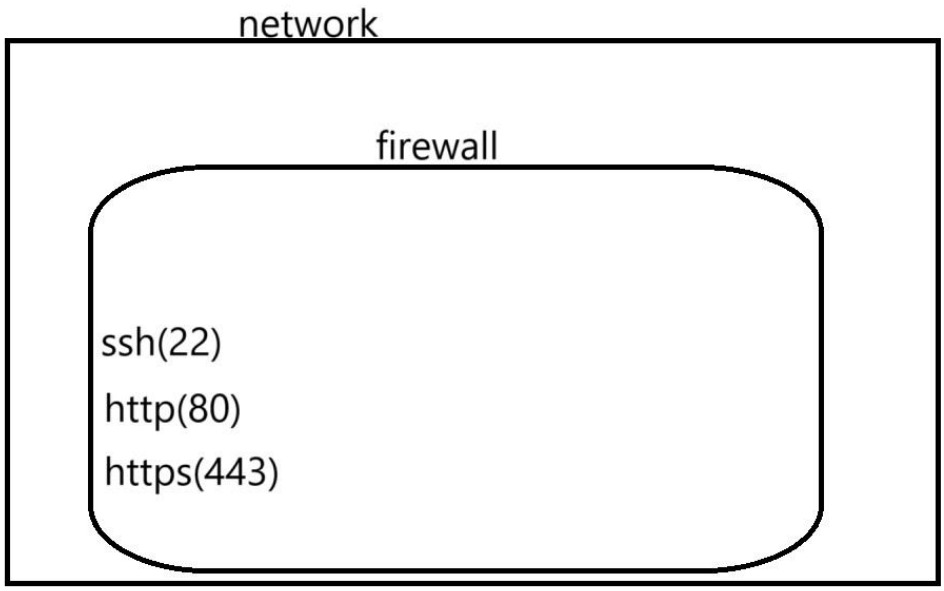
Networking Project 2

Project 2: Network Design with Firewall and Open Ports (SSH, HTTP, HTTPS)



Network Diagram

Implementation Steps

1. Firewall Configuration

- **Set up the firewall**:
  - Use a hardware firewall or software-based firewall (e.g., iptables, pfSense).
  - Configure the following rules: ○ Allow incoming traffic on port 22 (SSH). ○ Allow incoming traffic on port 80 (HTTP).
  - Allow incoming traffic on port 443 (HTTPS). Block all other incoming traffic.

Example iptables commands:

- iptables -A INPUT -p tcp --dport 22 -j ACCEPT
- iptables -A INPUT -p tcp --dport 80 -j ACCEPT
- iptables -A INPUT -p tcp --dport 443 -j ACCEPT iptables -A INPUT -j DROP

2. Network Device Setup

- **Router**: ○ Connect the router to the ISP for internet access.
  - Configure the router's WAN and LAN settings. • **Switch**:
  - Connect the switch to the router for distributing the network to internal devices.

3. Server Configuration

- **Web Server**: ○ Install a web server (e.g., Apache or Nginx).
  - Configure the server to listen on ports 80 and 443.
- **SSH Server**:
  - Install and configure an SSH server (e.g., OpenSSH). ○ Ensure the server is listening on port 22.

4. Security Enhancements

- **Firewall Logging**: ○ Enable logging to monitor traffic and detect unauthorized attempts.
- **SSH Configuration**:
  - Use key-based authentication for SSH access.
  - Disable root login via SSH.
- **Web Server Security**:
  - Use SSL/TLS certificates for HTTPS. ○ Regularly update the web server software.