Networking Project 2

290396
Akash Nadigepu

Date : 15/01/2025

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

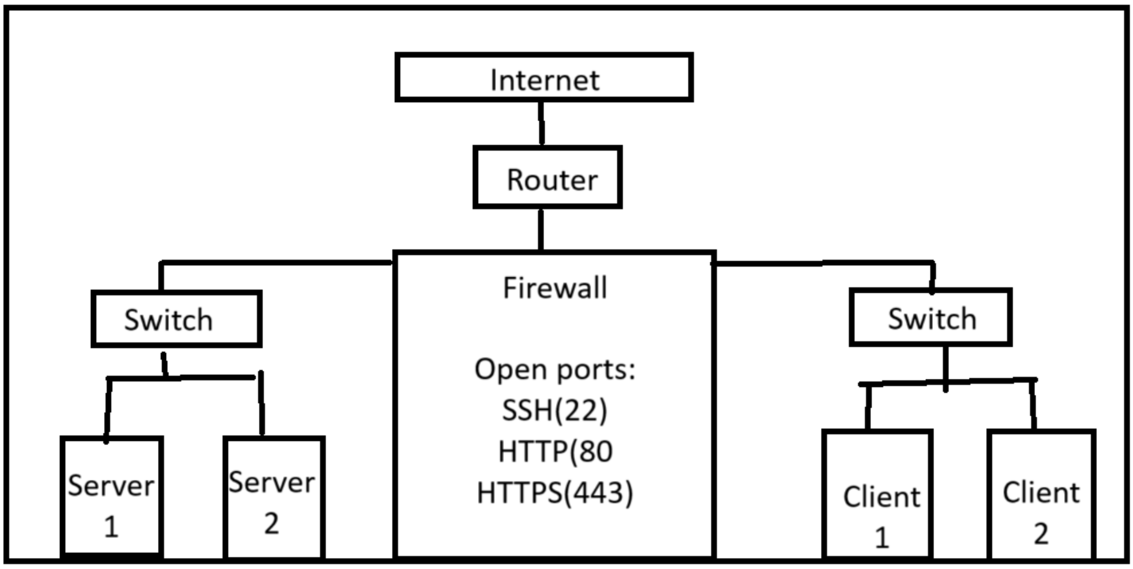
Objective

Design and implement a secure network architecture with a firewall and ensure that specific ports (SSH, HTTP, and HTTPS) are open for external access while maintaining robust security.

Network Requirements

1. **Firewall Configuration**:
   - Implement a firewall to filter and manage traffic.
   - Allow access to the following ports:
     - **Port 22** (SSH): For secure shell access.
     - **Port 80** (HTTP): For standard web traffic.
     - **Port 443** (HTTPS): For secure web traffic.
2. **Network Devices**:
   - Use a router for internet connectivity.
   - Add a switch to connect internal devices.
3. **Servers**:
   - Deploy a web server for HTTP/HTTPS traffic.
   - Configure an SSH server for remote management.
4. **Client Systems**:
   - Devices accessing the network services.
5. **Security Measures**:
   - Restrict all other ports to prevent unauthorized access.
   - Enable logging on the firewall for auditing.

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.

Conclusion

This network design ensures secure communication with minimal exposure to potential threats. By configuring the firewall to allow only essential ports (SSH, HTTP, HTTPS) and blocking all others, the network is both functional and secure.