1. Learn firewall concepts

A firewall is a security system that controls network traffic. It decides which data is allowed to enter or leave a computer or network. Firewalls work based on rules like IP address, port number, and protocol. The main purpose of a firewall is to protect systems from unauthorized access, hackers, and malware.

2. Configure rules

Firewall rules are instructions that tell the firewall what to allow and what to block. While configuring rules, we define conditions such as source IP, destination IP, port number, and protocol (TCP/UDP). These rules help control network traffic and ensure only trusted connections are permitted.

3. Allow / deny ports

Ports are communication endpoints used by services (for example, HTTP uses port 80 and HTTPS uses port 443). Allowing a port means permitting traffic through that port, while denying a port blocks all traffic using it. For example, allowing port 22 enables SSH access, while blocking unused ports improves security.

4. Test connectivity

After configuring firewall rules, connectivity testing is done to check whether the rules are working correctly. Tools like **ping**, **telnet**, or **netcat** are used to verify allowed connections. If a blocked service cannot be accessed, it confirms the firewall rule is effective.

5. Observe logs

Firewall logs record details of allowed and blocked traffic. By observing logs, we can see which IP addresses tried to connect, which ports were used, and whether the connection was permitted or denied. Logs are useful for monitoring network activity and detecting suspicious behavior.

6. Block malicious IP

If an IP address is found performing suspicious or harmful activities (such as repeated login attempts), it can be blocked using a firewall rule. Blocking malicious IPs helps prevent attacks like brute force attempts and unauthorized access, increasing overall system security.

---

7. Document rules

Documenting firewall rules means writing down all configured rules with their purpose. This includes allowed ports, blocked IPs, and special permissions. Proper documentation helps in troubleshooting, audits, and future updates, especially when multiple administrators manage the system.

---

8. Explain impact

Firewall configuration directly impacts system security and performance. Proper rules protect the system from attacks and reduce unwanted traffic. However, incorrect rules may block legitimate services or users. Therefore, firewall rules must be carefully planned, tested, and reviewed regularly.
