Interview Questions

1️⃣ What is a firewall?

A **firewall** is a network security device or software that monitors and controls incoming and outgoing network traffic based on predefined security rules.
It acts as a **barrier between trusted and untrusted networks**, inspecting packets and allowing or blocking them according to policies designed to protect systems from unauthorized access, malware, or data exfiltration.

2️⃣ Difference between Stateful and Stateless Firewalls

Feature	Stateful Firewall	Stateless Firewall
Connection Awareness	Tracks the **state** of active connections (e.g., established, new, related).	Evaluates each packet **individually**, without tracking connection states.
Decision Basis	Uses context from previous packets to make decisions.	Relies solely on static rules (IP, port, protocol).
Performance	Slightly slower due to session tracking.	Faster, simpler packet filtering.
Example	Windows Defender Firewall, UFW (via iptables/nftables).	Basic access control lists (ACLs) on routers.

✅ **Summary:** Stateful firewalls provide **smarter and more secure filtering**, while stateless firewalls are **faster but less adaptive**.

3️⃣ What are Inbound and Outbound Rules?

- **Inbound Rules:** Control traffic **entering** the system or network. Example: Blocking all inbound TCP connections on port 23.
- **Outbound Rules:** Control traffic **leaving** the system. Example: Restricting outbound access to specific IPs or applications.

These rules define how the firewall manages data flow and help enforce the **principle of least privilege**.

4️⃣ How does UFW simplify firewall management?

UFW (Uncomplicated Firewall) is a user-friendly command-line front end for managing **iptables/nftables** on Linux.
It simplifies firewall configuration through easy commands like

```
sudo ufw allow 22/tcp
sudo ufw deny 23/tcp
```

Instead of writing complex rule chains, UFW provides **readable syntax, automatic rule ordering, and status summaries**, making it ideal for administrators and beginners alike.

5️⃣ Why block port 23 (Telnet)?

Port **23** is used by the **Telnet** protocol, which transmits data—including usernames and passwords—in **plain text**.
Because it lacks encryption, it is **highly vulnerable** to eavesdropping and credential theft.
Modern secure alternatives like **SSH (port 22)** have replaced Telnet. Blocking port 23 prevents exploitation and unauthorized access attempts.

6️⃣ What are common firewall mistakes?

Common misconfigurations that reduce firewall effectiveness include:

- Allowing overly broad rules (e.g., “allow all” or “any-any” policies).
- Forgetting to restrict **outbound traffic** or unnecessary services.
- Not reviewing or updating rules regularly.
- Placing firewalls incorrectly within the network topology.
- Failing to log or monitor blocked connection attempts.

✅ Proper rule management, logging, and periodic audits are key to maintaining firewall integrity.

7️⃣ How does a firewall improve network security?

A firewall improves network security by:

- **Filtering malicious traffic** and blocking unauthorized connections.
- **Segregating network zones** (e.g., separating the internal LAN from the Internet).
- **Preventing port scans and brute-force attacks.**
- **Limiting the exposure** of vulnerable services.
- Providing **logging and visibility** into attempted intrusions.

In essence, it enforces **access control** and reduces the attack surface of systems and networks.

8️⃣ What is NAT in firewalls?

NAT (Network Address Translation) is a technique that allows multiple devices on a private network to share a single public IP address.
In the context of firewalls, NAT:

- **Hides internal IP addresses** from external users (adds a layer of security).
- Enables **port forwarding** for controlled access to internal services.
- Helps **conserve public IPv4 addresses**.

Firewalls with NAT functionality combine packet filtering with address translation, effectively securing and managing network traffic flow.