Interview Questions & Answers On Firewall

1. What is a firewall?

A firewall is a network security system—either hardware, software, or a combination—that monitors and controls network traffic based on pre-defined security rules. It acts as a barrier between a trusted internal network and untrusted external networks (like the internet).
Its main job is to **allow legitimate traffic** and **block suspicious or unauthorized access**, thereby reducing the risk of attacks like malware infections, hacking attempts, or data leaks.

2. Difference between stateful and stateless firewall?

- **Stateful Firewall:**
  - Keeps track of active connections and the state of each connection (e.g., established, related).
  - Makes decisions based on both the packet and its connection history.
  - Example: If you initiate an HTTP request, it will allow the returning packets without needing separate rules.
  - More secure but slightly resource-intensive.
- **Stateless Firewall:**
  - Treats each packet in isolation without considering prior communication.
  - Makes decisions only on packet header information (IP, port, protocol).
  - Faster but less secure because it can’t detect abnormal connection patterns.

3. What are inbound and outbound rules?

- **Inbound Rules:**
  - Control traffic coming **into** your device or network from external sources.
  - Example: Blocking incoming connections on port 23 to prevent Telnet access.
- **Outbound Rules:**
  - Control traffic going **out** from your device or network to external destinations.
  - Example: Restricting outbound traffic to certain IP ranges to prevent data exfiltration.

4. How does UFW simplify firewall management?

UFW (Uncomplicated Firewall) is a command-line tool in Linux that provides a simplified interface to manage `iptables` rules.

- Instead of writing long, complex `iptables` commands, you can use short commands like `ufw allow 80` or `ufw deny 23`.
- It automatically manages IPv4/IPv6 rules.

- Provides numbered lists of rules, making it easy to add, view, and delete them.
- Ideal for beginners while still being powerful enough for advanced users.

5. Why block port 23 (Telnet)?

- Telnet transmits all data, including usernames and passwords, in **plain text**—making it vulnerable to sniffing attacks.
- It has no encryption, so attackers can easily intercept sensitive information.
- Modern systems use SSH (port 22) as a secure alternative, which encrypts all communication.

6. What are common firewall mistakes?

- Leaving unnecessary ports open, increasing the attack surface.
- Misconfigured rules that block legitimate services or fail to block dangerous traffic.
- Not enabling firewall logging, making it hard to detect suspicious activity.
- Relying solely on the firewall without updating software or using other security measures.
- Allowing “Allow All” rules for convenience, which defeats the purpose of having a firewall.

7. How does a firewall improve network security?

- Acts as a first line of defense by filtering traffic before it reaches vulnerable systems.
- Prevents unauthorized access to internal resources.
- Blocks known malicious IP addresses and ports.
- Enforces security policies for inbound and outbound traffic.
- Helps detect unusual patterns that may indicate intrusion attempts.

8. What is NAT in firewalls?

NAT (Network Address Translation) is a process in which a firewall or router changes the source or destination IP addresses in packet headers.

- **Purpose:**
  - Hides internal private IP addresses from external networks.
  - Allows multiple internal devices to share a single public IP.
- **Security Advantage:**
  - External systems cannot directly see or access internal devices, reducing the risk of direct attacks.
- Often combined with firewall rules to control which internal devices can access the internet and which external connections are allowed in.