1. What is a firewall?
   Ans: A firewall is a network security device designed to monitor, filter, and control incoming and outgoing network traffic based on predetermined security rules. The primary purpose of a firewall is to establish a barrier between a trusted internal network and untrusted external networks.

2. Difference between stateful and stateless firewall?
   Ans: Stateful uses the concept of a state table where it stores the state of legitimate connections.
   Stateless firewall filters are only information in a packet but stateful firewall filter inspects firewall filter inspects everything inside data packet.

3. What are inbound and outbound rules?
   Ans: Inbound and outbound security rules serve to regulate incoming and outgoing network traffic, respectively.

4. How does UFW simplify firewall management?
   Ans: UFW(Uncomplicated Firewall) simplifies firewall management by providing a user-friendly interface on the top of the more complex IP table.

5. Why block port 23 (Telnet)?
   Ans: Telnet is an insecure protocol that transmits login credentials in plaintext, making it vulnerable to eavesdropping attacks. Therefore, it is recommended to restrict the inbound access to TCP port 23 to prevent unauthorized access to Telnet services.

6. What are common firewall mistakes?
   Ans: 1. Access from external devices to protected resources is not functioning properly.
   2. Access from the protected resources to unprotected is not functioning
   3. Access to the firewall is not functioning properly.

7. How does a firewall improve network security?

Ans: Firewalls protect inspect and authenticate all data packets in network traffic before they are allowed to move to a more sure environment.

8. What is NAT in firewalls?
   Ans: a service that operates on a router or edge platform to connect private networks to public networks like the internet.