1. **What is a firewall?**
   A firewall is a security device—either hardware or software—that acts as a guard for a network. It monitors incoming and outgoing traffic and decides whether to allow or block it based on a set of security rules.
2. **Difference between stateful and stateless firewall?**
   - **Stateless:** A simple firewall. It checks every data packet individually and doesn't know what happened before. It's fast but not very smart.
   - **Stateful:** A smarter firewall. It remembers the connections. If you start a conversation with a website, it knows that the website's reply is part of that same conversation and automatically lets it back in. It's much more secure.
3. **What are inbound and outbound rules?**
   - **Inbound:** Rules for traffic *coming into* your computer. This is for protecting you from outside attacks. (Example: Blocking a hacker trying to connect to your PC).
   - **Outbound:** Rules for traffic *going out of* your computer. This can prevent a virus on your PC from connecting to an attacker's server.
4. **How does UFW simplify firewall management?**
   UFW (Uncomplicated Firewall) simplifies things by using very simple commands. Instead of writing complex, multi-line rules needed for the underlying Linux firewall (iptables), you can just write sudo ufw allow ssh or sudo ufw deny 80. It makes firewall management much faster and less error-prone.
5. **Why block port 23 (Telnet)?**
   Telnet is an extremely old and **insecure** protocol. When you use Telnet, your username and password are sent over the network in **plain text**, with no encryption. Anyone "listening" on the network can easily steal your credentials. It should always be blocked and replaced with a secure alternative like SSH (port 22).
6. **What are common firewall mistakes?**
   - **"Allow Any, Any" Rule:** Creating a rule that allows all traffic from any source to any destination. This essentially turns the firewall off.
   - **Incorrect Rule Order:** In some firewalls, the order of rules matters. A broad "allow" rule placed before a specific "deny" rule can render the deny rule useless.

- **Not Deleting Old Rules:** Leaving old, temporary rules in place can create security holes later on.

7. **How does a firewall improve network security?**
   A firewall is the first line of defense. It improves security by creating a barrier between your trusted internal network (your PC) and an untrusted external network (the internet). It drastically reduces your "attack surface" by blocking access to ports and services that don't need to be exposed.

8. **What is NAT in firewalls?**
   NAT stands for **Network Address Translation**. It's a feature used by almost every home router. It allows multiple devices on your private network (with private IPs like 192.168.1.X) to share a single, public IP address on the internet. This also adds a layer of security because it hides your individual devices' IP addresses from the outside world.