1. **Differentiate between IDS/IPS with Firewalls**

An Intrusion Detection System (IDS) senses any authorized access to your host or network and sends you an alert. The sensing is usually done using certain rules about unusual behaviour. For example, Snort.

An Intrusion Prevention System (IPS) detects unauthorized access and then prevents it. Therefore, you would not need to manually block the attack yourself. For example, Cisco IPS.

A firewall acts as a secretary to your host system. It's job is to filter the incoming traffic from the internet. It decides which packets are safe enough to be sent to your system, and which packets are eligible to be sent out of your system to the internet. For example, Windows Firewall.

2. **Which is better IDS or IPS? What would you buy as a Network admin?**

IPS. As IDS only analyze and monitor network traffic for signs that indicate attackers are using a known cyberthreat to infiltrate or steal data from your network. IDS systems compare the current network activity to a known threat database to detect several kinds of behaviors like security policy violations, malware, and port scanners.

Where as IPS live in the same area of the network as a firewall, between the outside world and the internal network. IPS proactively deny network traffic based on a security profile if that packet represents a known security threat.