Packet travels through cloud and reaches firewall which may allow or deny the packet reaching its destination. Firewalls look at the Source IP, Destination IP and the port. The firewall will block by default. Firewalls cannot look at the contents of the packet which may or may not be malicious. IPSs help with this by acting as another layer the packet has to go through after the firewall that inspects the payload of the packet.

Network Based Detection Systems
- Tools available to you:
  - Sensors -> searching packet by packet
    - Looking at packets as they come in
      - Problem: overload
      - Actively vs Passively looking at them
    - Passively: as they go through
  - Where can you live when searching for packets?
    - Inside the firewall
      - Have pre-filtered packets when they go through the firewall then to you
    - Past the external firewall
    - Sensor locations matter -> problems cannot be solved with one system because location of sensor like cause some issues to be missed.
  - Purpose of external firewall
    - Looks at meta-data, what’s inside the packets

Today, there are distributed systems. Attacks on distributed systems is harder to detect on a single computer apart of the system.
- To help with this problem computers gossip with each other, sharing info of what is coming to each computer and letting other computers know what is going on

Network-Based IDS (NIDS)
- Monitors traffic at selected points on a network -> this system is placed on a specific port which listens to incoming traffic.