DoS/DDoS

DoS/DDoS

- Interruption causes in service (availability) to legitimate users
  - Using up all of the targets resources to accept network connections
    - Resulting in additional connections being denied
  - Sending a message that resets target host’s subnet mask
    - Causing a disruption of the target’s subnet routing
  - Filling up a target’s hard drive storage space

DoS/DDoS

- Cloud Provider network should offer protection against traditional network security issues such as:
  - Distributed denial of service (DDoS) attacks, man-in-the-middle attacks, IP spoofing, and port scanning.
- Network protection devices, including firewalls, needed:
  - To monitor and control network communications at the external boundary
  - and at internal boundaries within the network.
- These network boundary devices employ traffic flow policies, or access control lists (ACLs), that enforce the flow of traffic.
- Firewalls should be deployed in a layered approach to perform packet inspection with security policies configured to filter the packets based on:
  - Protocol, port, source, and destination IP address to identify authorized sources, destinations, and traffic types.

DoS/DDoS

- Vulnerability notification systems needed to monitor security incidents, advisories, and other related information.
- Scaled to support large amount of traffic
    - Wirespeed
- 3-7 layer attack prevention
- Load balancers can inspect traffic
- SYN encryption, support high capacity connection tables
- Pattern matching, flow validation, ICMP flood limitation, strict TCP forwarding
- NIDS — Monitors and block suspicious network traffic
    - NIDS sensors can be in Intrusion Prevention System (IPS) or Intrusion Detection System (IDS)