The goal of a firewall is to be a barrier on the network to prohibit bad behavior.

- All traffic must go through the firewall
- Physically Firewalls are Routers/System

Types
- Packet Filtering
  - Stateful, packet filtering with heuristics, keeps track of connection to stop session hijacking
  - No end to end connections, proxy between you and the destination. (performance)
  - Proxy let you pretend to be someone else on the network, VPNs tunnel to different networks and create secure SSL connections
  - Network Availability is Key, but creates threats, attack vectors
  - Firewalls are inserted between the local network and the Internet
  - Firewalls must handle all traffic or it’s pointless
  - Firewalls should have policies to deal with different types of traffic

Access Policies
- Based on ports because they expect certain types of traffic.
- Application level, Gateways
- Identity Based
- Network Activity

Firewall shouldn’t be by-passable
Internal traffic is assumed safe

Default Policies
- Forward, permit unless prohibited
- Discard, Prohibit unless permitted

Advantages, simplicity fast
Limited, tiny fragment,

Stateful
- Looks at packets and makes decision’s

Gateways
Must have proxy code for each application
Secure but costly and performance