- Filename: eccouncil-ceh31250-v11-12-2-1-firewalls.md
- Show Name: CEHv11 (312-50)
- Topic Name: Network and Perimeter Hacking: Evading Firewalls, IDS, and Honeypots
- Episode Name: Firewalls
  ==========

Firewalls

Objectives:

- Define what an IDS/IPS is and explain its function and basic process
- List and define the different types of IDS/IPS

- What is a firewall?
  - Could be Hardware or Software
    - Why not both?
  - Doorman (are you on the list?)
    - Demo simple ACL with `iptables`
- How are firewalls typically deployed?
  - A couple of different ways
    - Gateway/Bastion Host
    - DMZ or 'Screened Subnet'
    - Multi-homed
- Firewall Technology Types
  - Packet Filtering
  - Circuit-Level Gateway
  - Application-Level
  - Stateful (combo of Packet+Circuit+Application)
  - Proxy
  - NAT
  - VPN
- Firewall Evasions
  - Firewalking for detection
  - IP Spoofing
  - Fragmentation
  - Proxy
  - Tunneling Traffic
    - SSH
    - HTTP
    - ICMP
    - DNS
  - MITM
  - Social Engineering/Phishing
- Defense against evasions?
  - Implicit Deny
  - Rules for both Ingress AND Egress
  - Regular updates
  - Regular rule testing and review

- Logging and monitoring