- Filename: eccouncil-ceh31250-v12-12-2-1-firewalls.md
- Show Name: CEHv12 (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`
            - Implicit **DENY**
                - `sudo iptables --policy INPUT DROP`
            - Deny List
        - ```
          sudo iptables --policy INPUT ACCEPT
          sudo iptables -A INPUT -p tcp --source 192.168.202.132 -j DROP
          sudo iptables -A INPUT -p tcp --source 192.168.202.200 -j REJECT
          ```
            - Allow List
        - ```
          sudo iptables --policy INPUT DROP
          sudo iptables -A INPUT -p tcp --source 192.168.202.132 -j ACCEPT
          ```
- How are firewalls typically deployed?
    - A couple of different ways
        - Gateway/Bastion Host
        - DMZ or 'Screened Subnet'
        - Multi-homed
- Firewall Technology Types
    - Packet Filtering
        - Filters packets based on rules(ACL)
    - Circuit-Level Gateway
        - Filters based on session-layer
            - Uses rules to determine whether session is legit
    - Application-Level
        - Filters based on application specific rules
            - WAF
    - Stateful
        - Filters by traffic state
            - LISTEN
            - ESTABLISHED
            - RELATED
            - CLOSING
        - `sudo iptables -A INPUT -m conntrack --cstate RELATED,ESTABLISHED -j ACCEPT`

    - Proxy
    - NAT
    - VPN

- Firewall Evasions
    - Firewalking for detection
    - IP Spoofing
    - Fragmentation
    - DoS/DDoS
        - Crash the Firewall
        - Firewall fails open (sometimes)
            - Allows malicious traffic to reach target
    - 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