- Filename: eccouncil-ceh31250-v11-10-6-1-dos-and-ddos-countermeasures.md
- Show Name: CEHv11 (312-50)
- Topic Name: Network and Perimeter Hacking: Denial of Service
- Episode Name: DoS and DDoS Countermeasures
  ==========

DoS and DDoS Countermeasures

Objectives:

- List and explain the common DoS/DDoS detection and mitigation techniques and strategies
- List and explain common DoS/DDoS protection mechanisms and appliances

---

- Countermeasures
    - Detection
        - Activity Profiling
            - Network activity baselines
            - Traffic increases are indicators of attack
        - Sequential Change-Point Detection
            - Algorithmic detection of DoS
                - Cumulative Sum Algorithm
        - Wavelet-Based Signal Analysis
            - Spectral analysis of an input signal
                - Spectral Window energy is analyzed for anomalies
    - Strategies
        - Absorb
            - Scale up resources
        - Degrade
            - Shut off non-critical resources
        - Shut Down
            - Turn off service
        - Deflect
            - Use decoys(honeypots/honeynets) to attract the attacks
        - Prevent / Mitigate
            - Ingress/Egress filtering
            - TCP Intercept
                - Routers can validate connection requests
                    - Stops SYN floods
            - Rate limiting or QoS
            - Blackholing
            - Sinkholing

- What about botnet protection?
  - Blackholing
  - ISP protection
  - Cisco IPS Source IP Reputation Filtering
  - RFC 3704
    - Checks for spoofed IPs and blocks them
- Any other protections?
  - Hardware appliances
    - https://www.checkpoint.com/quantum/ddos-protector/
  - Software
  - Services
    - https://www.fortinet.com/products/ddos/fortiddos
  - ISP or 3rd-party service
  - Updates/Patches
  - Encryption
  - No unused/unnecessary ports/services