Distributed DoS

Attacks and Defenses

Técnicas de Perceção de Redes
Network Awareness

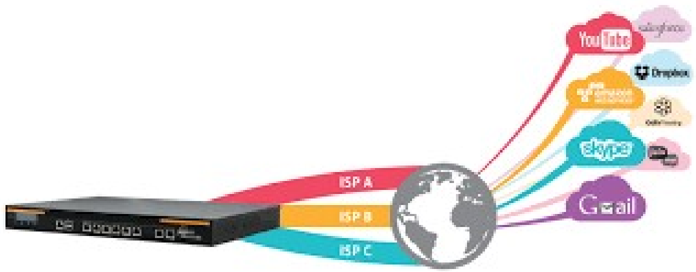
Mestrado Integrado em
Engenharia de Computadores e Telemática
DETI-UA

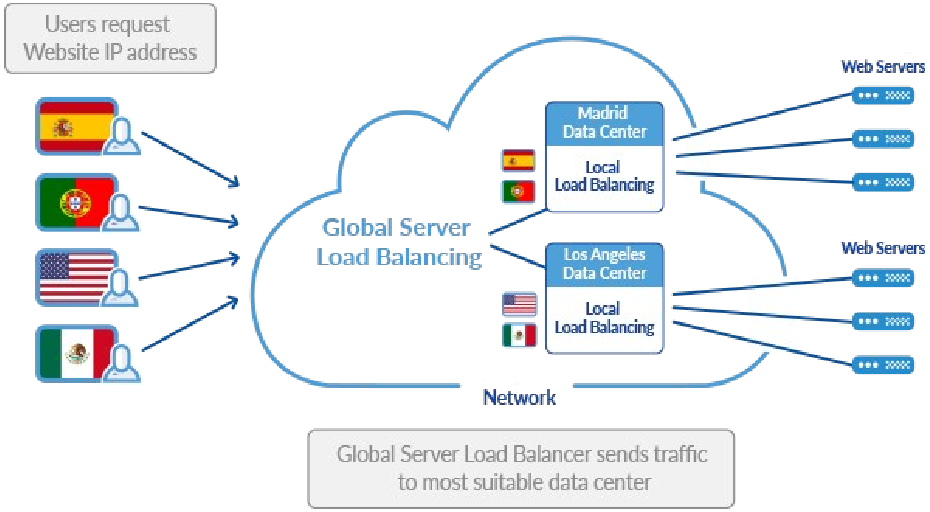
universidade de aveiro

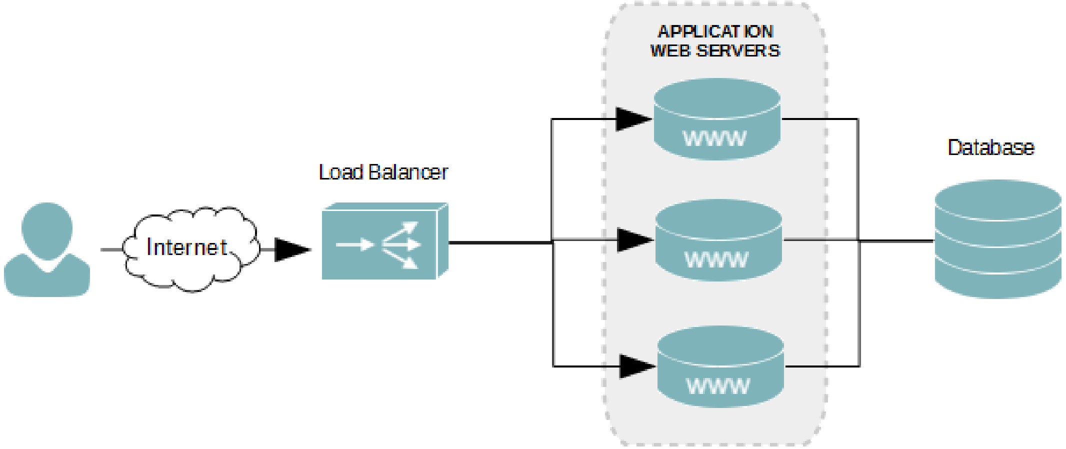
deti.ua.pt

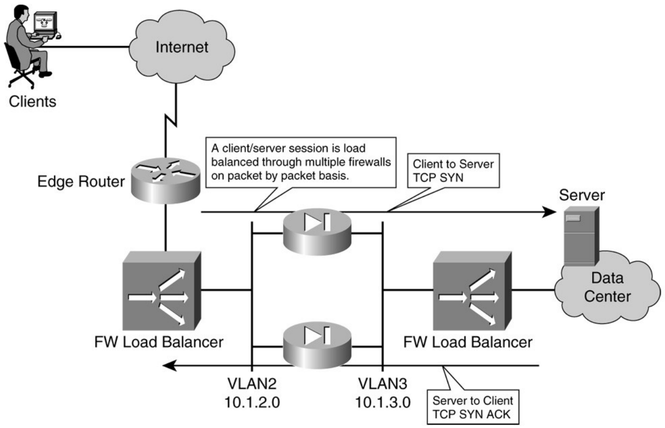
Load Balancing

- For Scalability, Redundancy, and Manageability.
- At Routing, DNS resolution, Servers, Firewalls, etc...




Users request Website IP address
Global Server Load Balancing
Madrid Data Center
Local Load Balancing
Los Angeles Data Center
Local Load Balancing
Web Servers
Web Servers
Network
Global Server Load Balancer sends traffic to most suitable data center



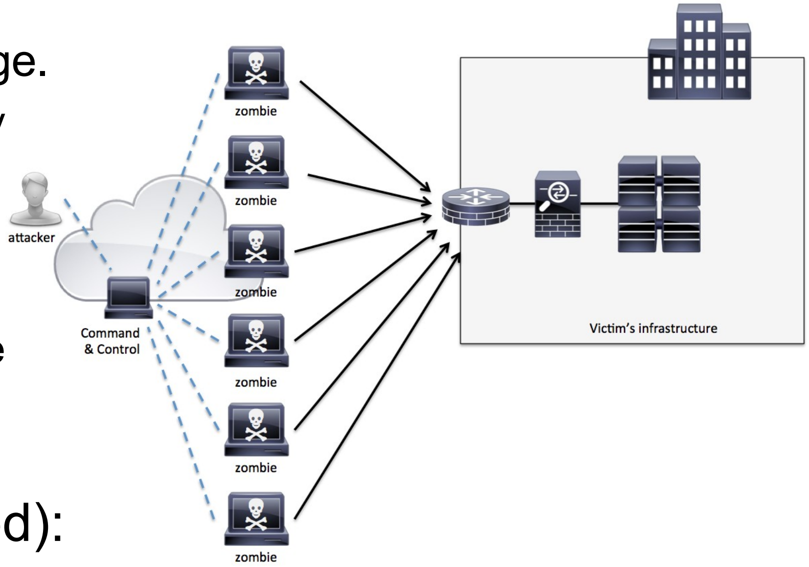


Load Balancing Algorithms

- Round Robin
  - Requests are distributed across the group of servers sequentially.
- Least Connections
  - A new request is sent to the server with the fewest current connections to clients.
  - The relative computing capacity of each server is factored into determining which one has the least connections.
- IP Hash
  - The IP address of the client is used to determine which server receives the request.
- “Smart”
  - Based on an external source of information.

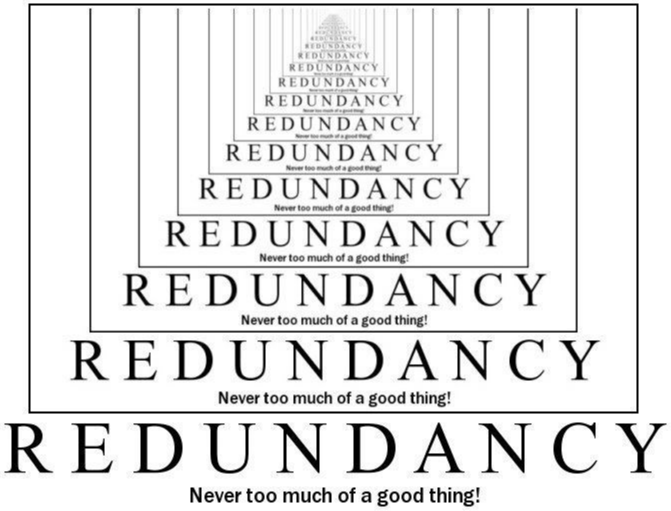
DDoS Detection

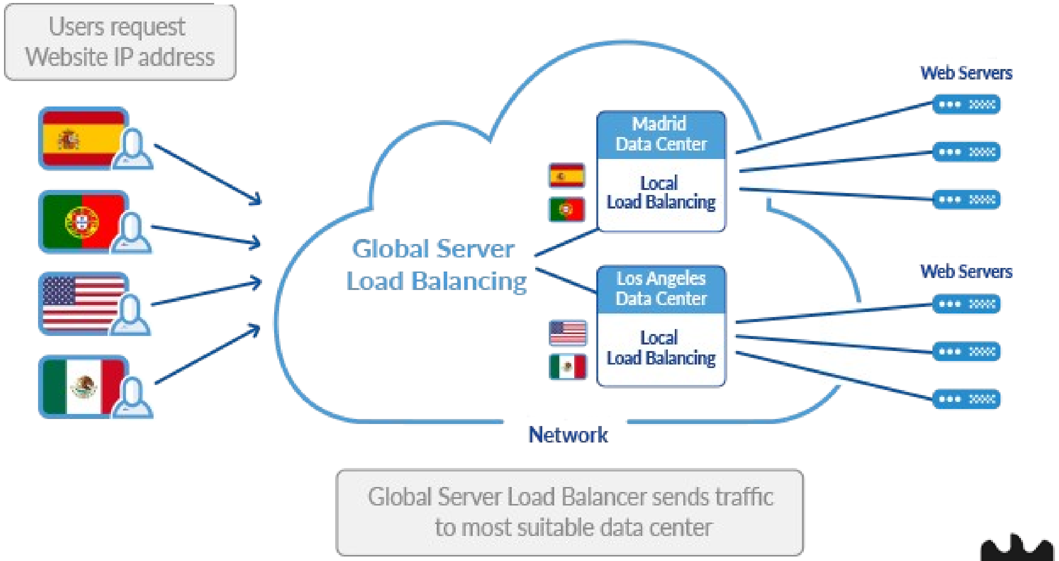
- At target:
  - Resource utilization much higher than average.
    - Traffic, service requests, CPU load, memory occupation, etc...
    - Easy to detect.
  - With slow start → Detect at early stage!
    - Detect small/medium variation from average usage.
    - More difficult, but still easy.
- At source (even when externally controlled):
  - Very difficult detection.
  - Requires the detection of small variations from normal behavior.
    - Amount of resources consumed and contacted destinations.
    - Constant monitoring and historic.
  - In near future, entities with sources of attacks could me liable.



Counter-Measures (1)

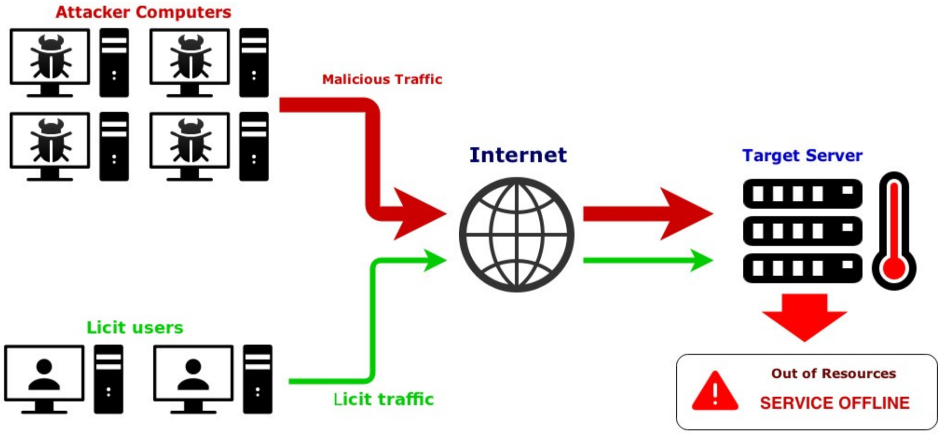
- Brute-force defense.
  - Add more servers.
  - Add more access points.
    - Via DNS.
  - Add more BW/Accesses.
  - Add more Firewalls.
  - …
- Control service distribution with load balancers.
  - At multiple levels:
    - DNS
    - Routing
    - Firewall
    - Servers
    - ...





Counter-Measures (2)

- Important to maintain service active!
  - At least at minimum levels.
- Identify licit requests / licit users
  - Based on bad behavior
    - Pending TCP session requests (incomplete 3-handshake)
    - Complete TCP sessions, with unreasonable content accesses
      - In number, in sequence, without authentication, etc...
  - Based on good behavior
    - Low level of requests is not enough
    - Analyze requests to validate users
    - Analyze source IP
    - Correlate information with service authentication.



- Protect licit users
  - Block illicit users
    - In TCP with RST to clean allocation in path.
  - Redirect licit users to a protect environment
    - Server, VLAN, equipments, etc…
    - Usage of “smart” load balancing!