Intrusion Detection and Prevention

Segurança em Redes de Comunicações

Mestrado em Cibersegurança

Mestrado em Engenharia de Computadores e Telemática

DETI-UA

universidade de aveiro

deti.ua.pt

Intrusion Detection and Prevention

- Intrusion Detection Systems (IDS)
  - Monitoring and identifying unauthorized system access or manipulation.
  - Analyzes information from multiple sources (computers, servers, services, and network traffic).
  - Identifies:
    - Intrusions, attacker outside of the organization;
    - Misuse, wrong behavior from a licit user/service.
  - Does not block/prevent intrusion.
  - Signals an alarm for:
    - Human analysis and intervention;
    - Automatic threat responses by firewalls or centralized management systems.
- Intrusion Prevention Systems (IPS)
  - At network level blocks traffic;
  - At host level kills processes, quarantines a file, blocks device access, etc...

Host-Based vs. Network-Based

- To protect specific servers or user devices the IDS/IPS is deployed at the host level.
  - Monitors traffic, processes, files’ access, devices’ access and data flows, memory allocations, physical device characteristics (temperature, power consumption, movement, etc...).
  - Nowdays called Endpoint Detection and Response (EDR).
- To protect an organization (all devices and services) the IDS/IPS is deploy at the network level.
  - Monitors traffic at the packet and flow levels. May monitor network at the physical level (radio, electric and optical signals).
  - Deployed at multiple network points:
    - Internet and WAN accesses;
    - Inter-zone communication links;
    - Wireless.

Signature vs. Anomaly Based

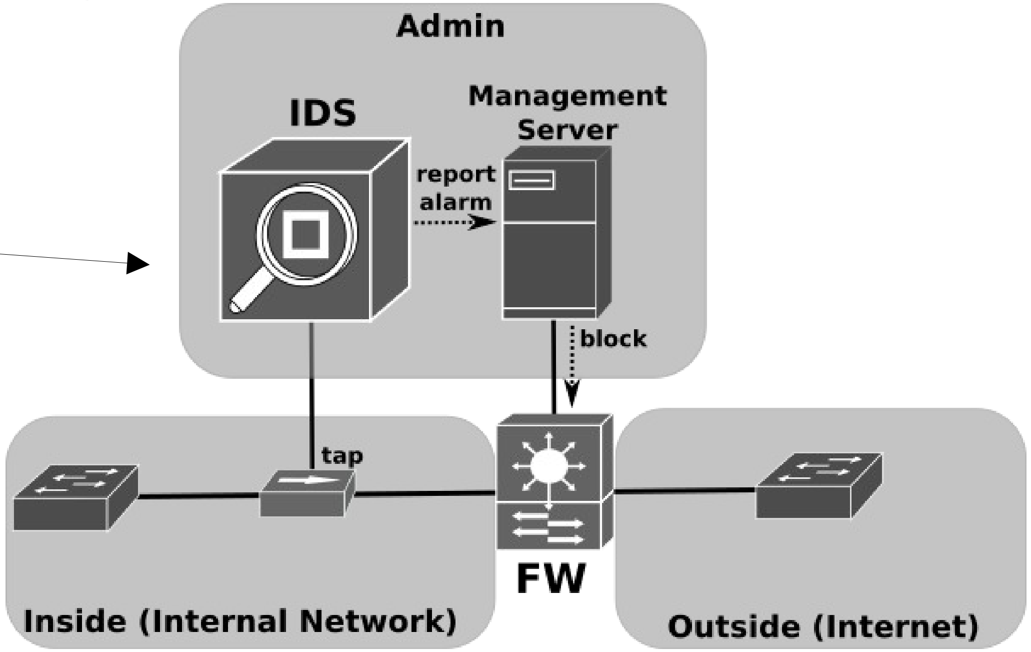
- Intrusions are detected based on two different approaches:
  - Signature based:
    - Monitored data compared to preconfigured and predetermined attack patterns known as signatures;
    - Attacks have distinct known signatures;
    - Signatures must be constantly updated to mitigate emerging threats.
    - Signatures may contain:
      - Individual packet header values or binary data patterns,
      - Sequence of packets with specific characteristics within the same flow, or
      - Set of data flows (data stream) with specific characteristics (of flows or transmitted packets/data).
  - Anomaly based:
    - Establishes a behavior baseline (profile) and detected deviation from that profile;
    - May rely only of high-level systems or network statistics, or include multiple data sources;
    - May be based on predefined rules or on AI models.

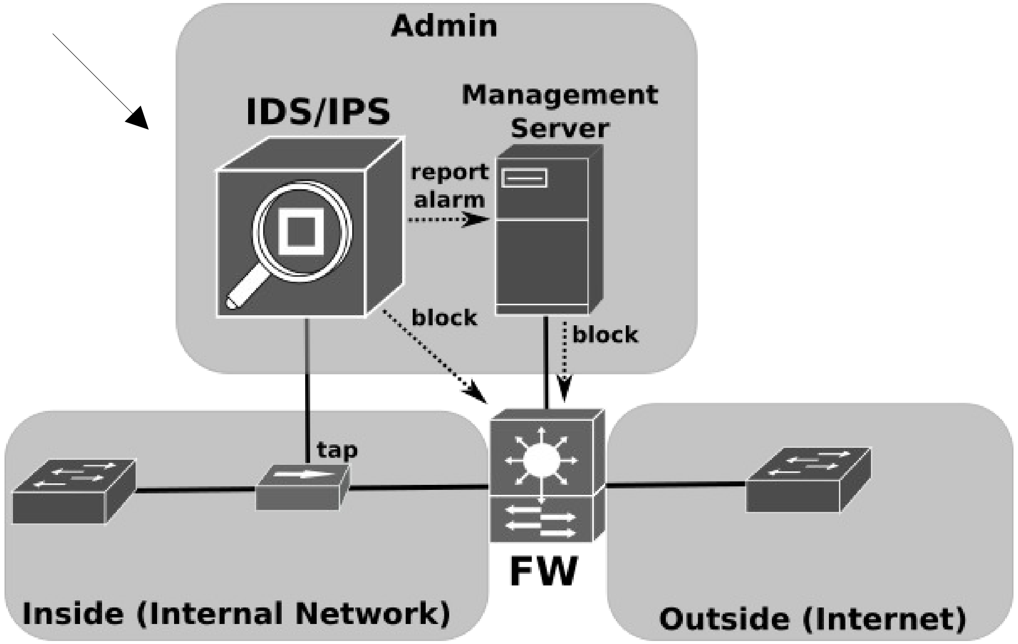
Endpoint Detection and Response (EDR)

- Referred also to as endpoint detection and threat response (EDTR).
- Monitor, record and analyze the activities and events on devices.
- Provide continuous and comprehensive visibility of the devices processes and user activities.
- Enables a direct response to incidents in devices/servers.
- May be fully deployed only on the device, or with an agent on device and external data analyze/storage.

Network Deployment (1)

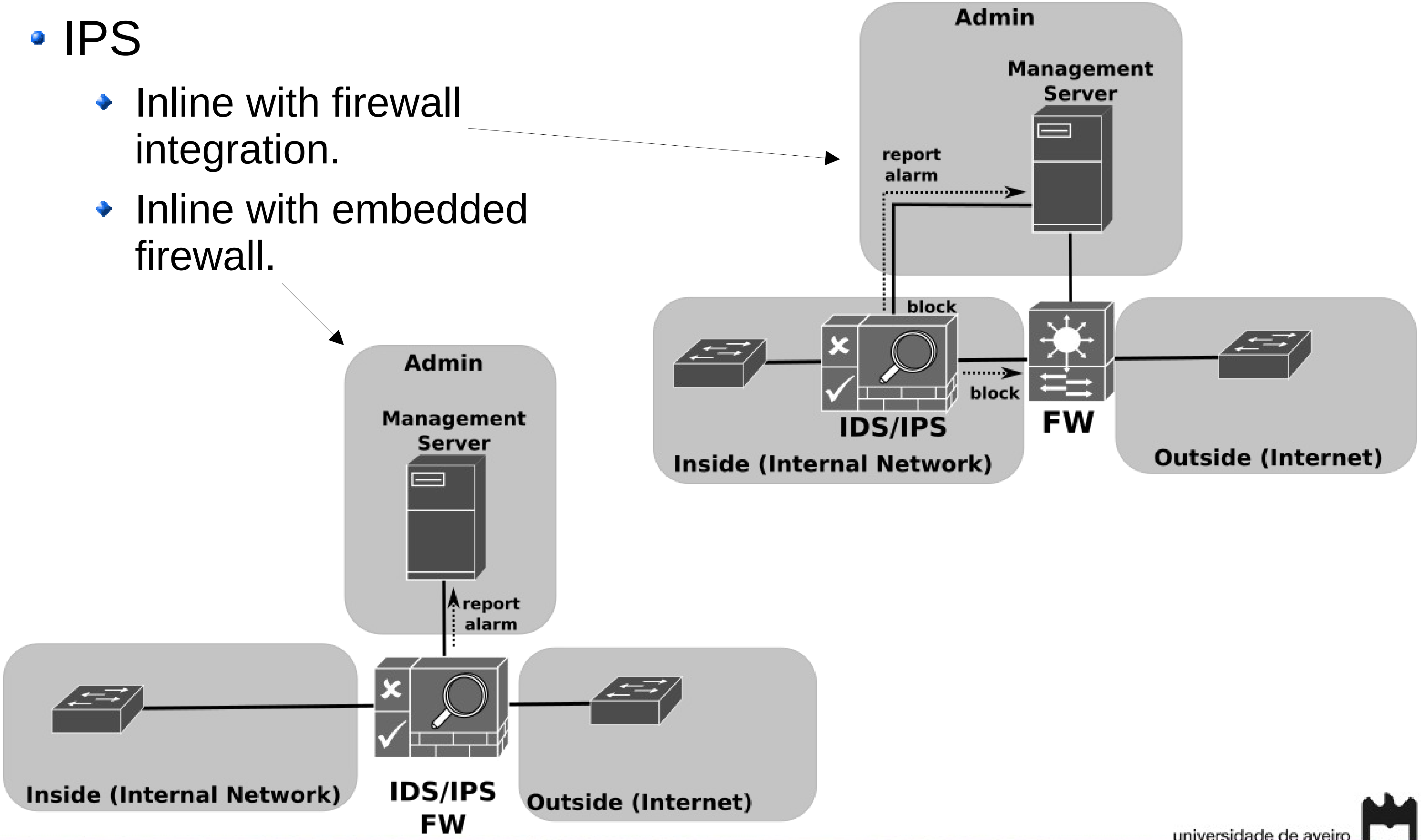
- IDS
  - Network tap.
  - Reports to network management system.
- IPS
  - Network tap with firewall integration.





Network Deployment (2)

- IPS
    - Inline with firewall integration.
    - Inline with embedded firewall.



IDS/IPS Actions

- Suricata
  - alert - generate an alert.
  - pass - stop further inspection of the packet.
  - drop - drop packet and generate alert.
  - reject - send RST/ICMP unreach error to the sender of the matching packet.
  - rejectsrc - same as just reject.
  - rejectdst - send RST/ICMP error packet to receiver of the matching packet.
  - rejectboth - send RST/ICMP error packets to both sides of the conversation.
- Snort
  - alert - generate an alert using the selected alert method, and then log the packet.
  - log - log the packet.
  - pass - ignore the packet.
  - drop - block and log the packet.
  - reject - block the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.
  - sdrop - block the packet but do not log it.