# Intrusion Detection and Prevention

Segurança em Redes de Comunicações Mestrado em Cibersegurança Mestrado em Engenharia de Computadores e Telemática DETI-UA



### 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.

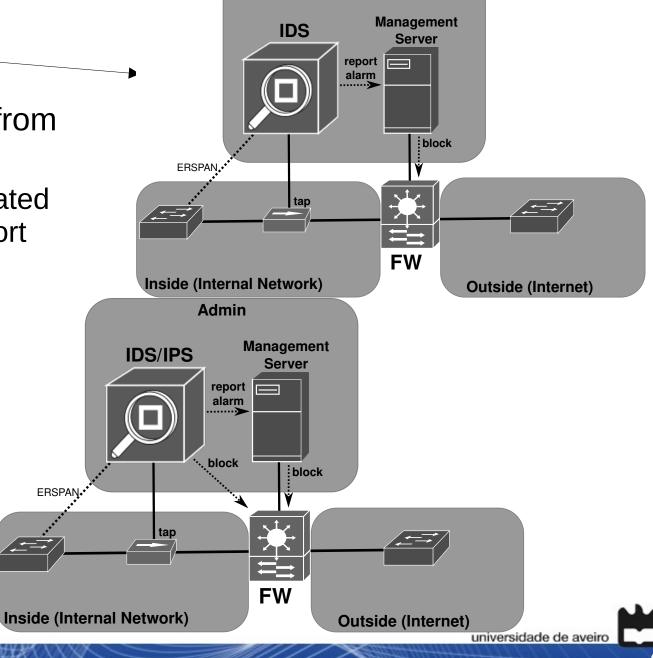
 ERSPAN GRE tunnel from switch.

> ERSPAN: Encapsulated Remote Switched Port **ANalyzer**

Reports to network management system.

IPS

IDS with firewall integration.

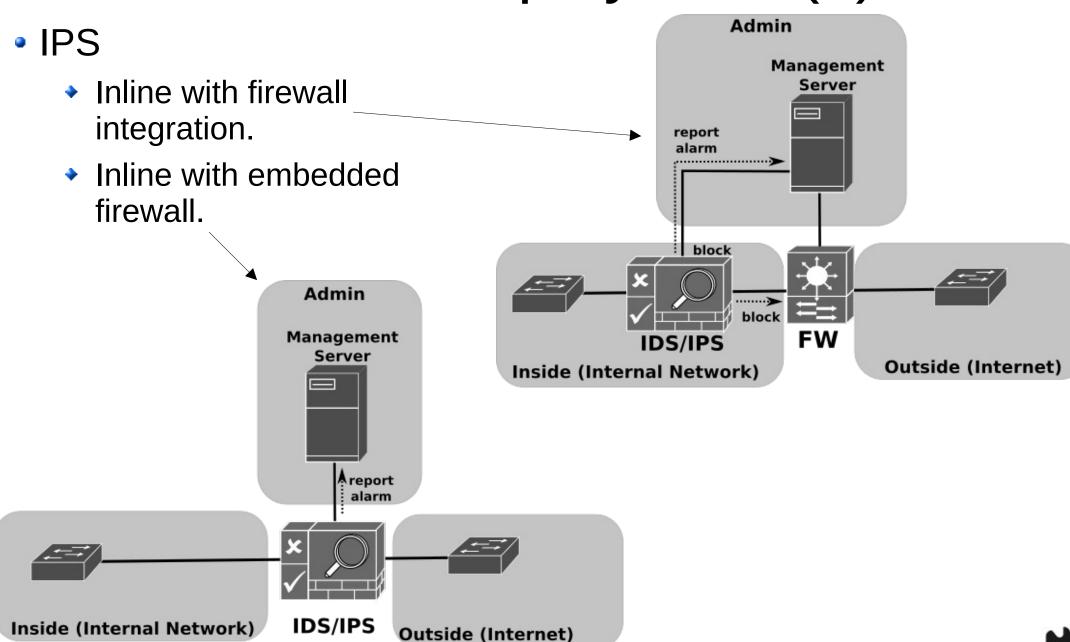


#### **ERSPAN**

- Stands for "Encapsulated Remote Switched Port Analyzer".
- Mirrors traffic from one or more switch ports.
- Sends the mirrored traffic to one or more destinations.
- The traffic is encapsulated in Generic Routing Encapsulation (GRE).

```
ERSPAN_example.pcapng [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
         <u>V</u>iew <u>G</u>o <u>C</u>apture <u>A</u>nalyze <u>S</u>tatistics Telephony <u>T</u>ools <u>I</u>nternals <u>H</u>elp
                                                                 1 0.000000000
                          110 10.2.1.10 10.2.1.11 TCP
                                                                             0 40032 > http [SYN] Seq=0 win=2048 Len=0 MSS=1460
 Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
  Ethernet II, Src: Cisco_aa:bb:cc (40:55:39:aa:bb:cc), Dst: HonHaiPr_dd:ee:ff (44:37:e6:dd:ee:ff)
 Internet Protocol Version 4, Src: 10.1.2.1 (10.1.2.1), Dst: 10.1.2.3 (10.1.2.3)
  Generic Routing Encapsulation (ERSPAN)
  Encapsulated Remote Switch Packet ANalysis
     0001 .... .... = Version: Type II (1)
     .... 1111 0011 1100 Vlan: 3900
     ...0 .... = Unknown2: 0
          0... = Direction: Incoming (0)
          .0.. .... = Truncated: Not truncated (0)
     .... ..00 0010 0000 = SpanID: 32
     Unknown7: 00000a22
  Ethernet II, Src: Cisco_aa:bb:cc (40:55:39:aa:bb:cc), Dst: HewlettP_11:22:33 (b4:b5:2f:11:22:33)
  Internet Protocol Version 4, Src: 10.2.1.10 (10.2.1.10), Dst: 10.2.1.11 (10.2.1.11)
  Transmission Control Protocol, Src Port: 40032 (40032), Dst Port: http (80), Seq: 0, Len: 0
      44 37 e6 dd ee ff 40 55 39 aa bb cc 08 00 45 00 00 60 03 2e 40 00 fe 2f 12 a6 0a 01 02 01 0a 01 02 03 10 00 88 be 00 00 03 2e 1f 3c 00 20 00 00
                                                               .`..@../ ......
                                                               0a 22 b4 b5 2f 11 22 33
                                 40 55 39 aa bb cc 08 00
      45 00 00 2c 65 2d 00 00
                                 27 06 b5 68 0a 02 01 0a
f9 80 ff b5 00 00 00 00
      0a 02 01 0b 9c 60 00 50
      60 02 08 00 81 08 00 00 02 04 05 b4 00 00
File: "C:\temp\ERSPAN\ERSPAN_example.pcapng" 0 Bytes 00:00:01
                                                                 Packets: 2 Displayed: 2 Marked: 0 Load time: 0:00.000
```

# Network Deployment (2)



FW

## **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.