Intrusion Detection and Prevention Systems

Intrusion Terminology

- ***Intrusion:***
  - attack on information where malicious perpetrator tries to break into or disrupt system.
- ***Intrusion detection:***
  - includes procedures and systems created and operated to detect system intrusions
- ***Intrusion reaction:***
  - covers actions organization takes upon detecting intrusion
- ***Intrusion correction activities:***
  - restore normal operations
- ***Intrusion prevention:***
  - actions that try to deter intrusions proactively

What is Intrusion

- Anybody or anything trying to gain unauthorized access to or modification of the network or system, or affect the network's or system's availability to legitimate clients

- Virus, Trojans, Worms

- Hackers – sending specifically crafted packets to exploit any specific vulnerability

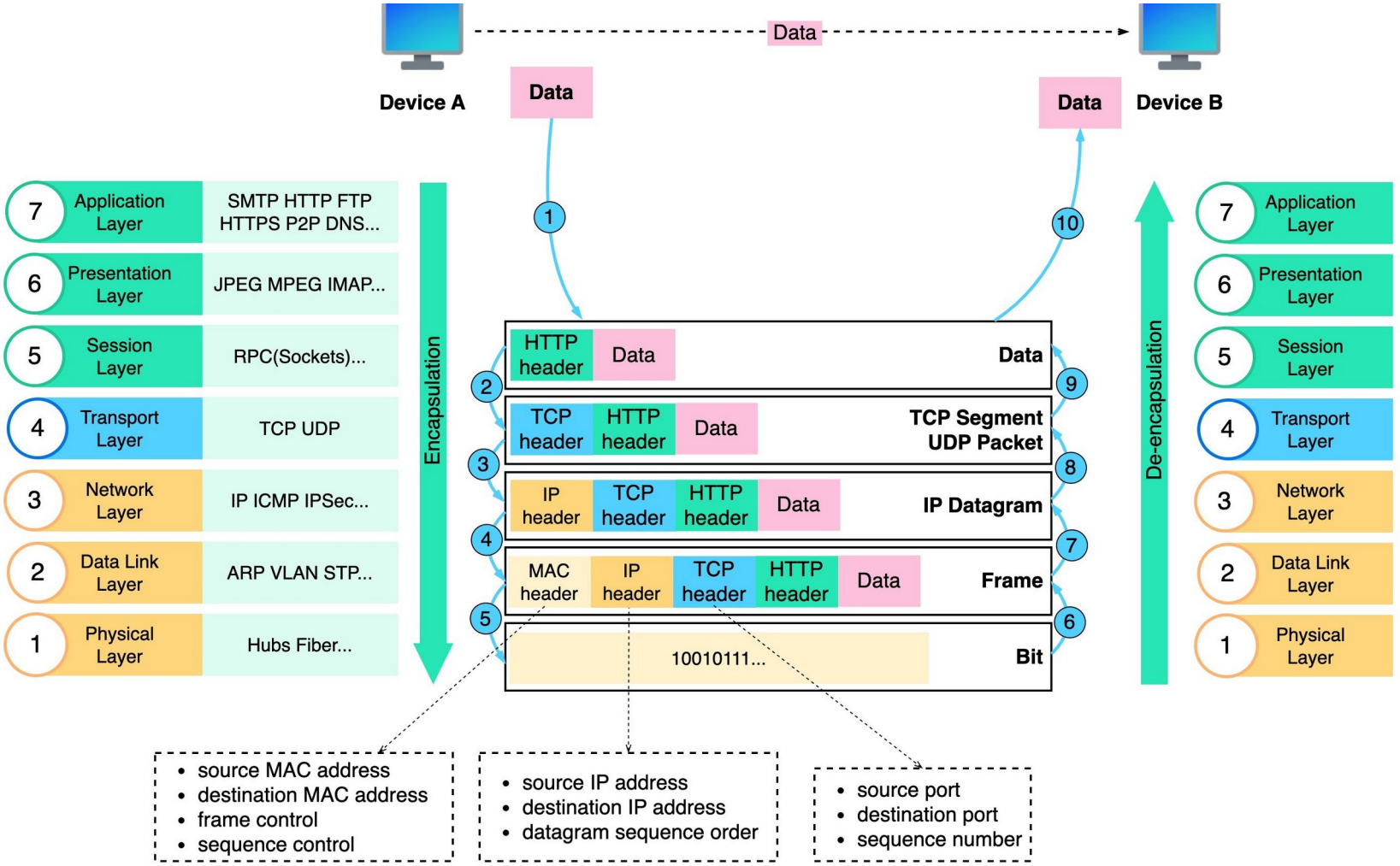
Intrusion Management Systems

- **Intrusion Management Systems (IMS)** refer to the broader category of technologies and processes that are designed to detect, prevent, and respond to unauthorized intrusions or malicious activities in a network.

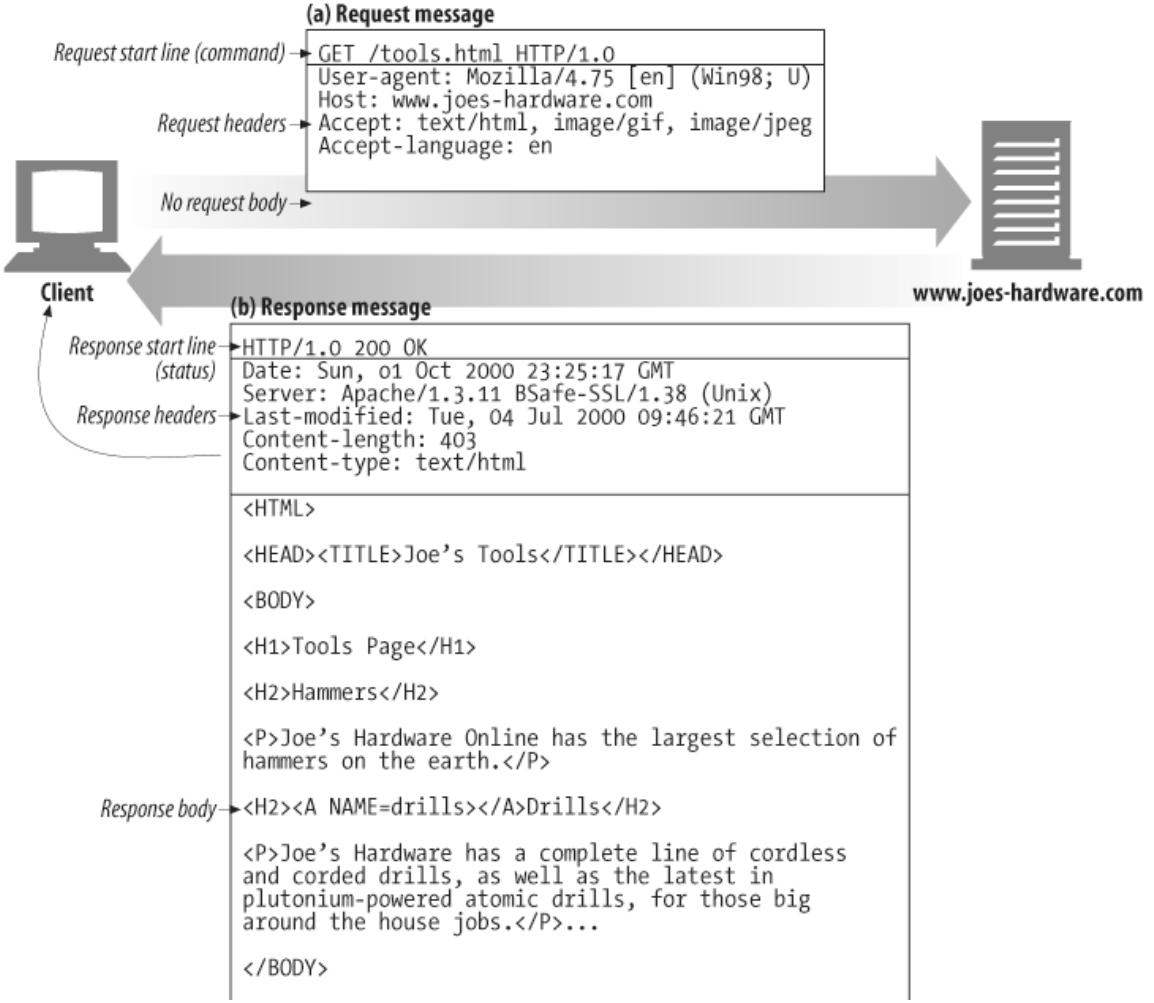
- Two categories of IMS
  - Intrusion Detection System (IDS)
  - Intrusion Prevention System (IPS)

Why IDS/IPS and Firewalls

Why IDS/IPS and Firewalls



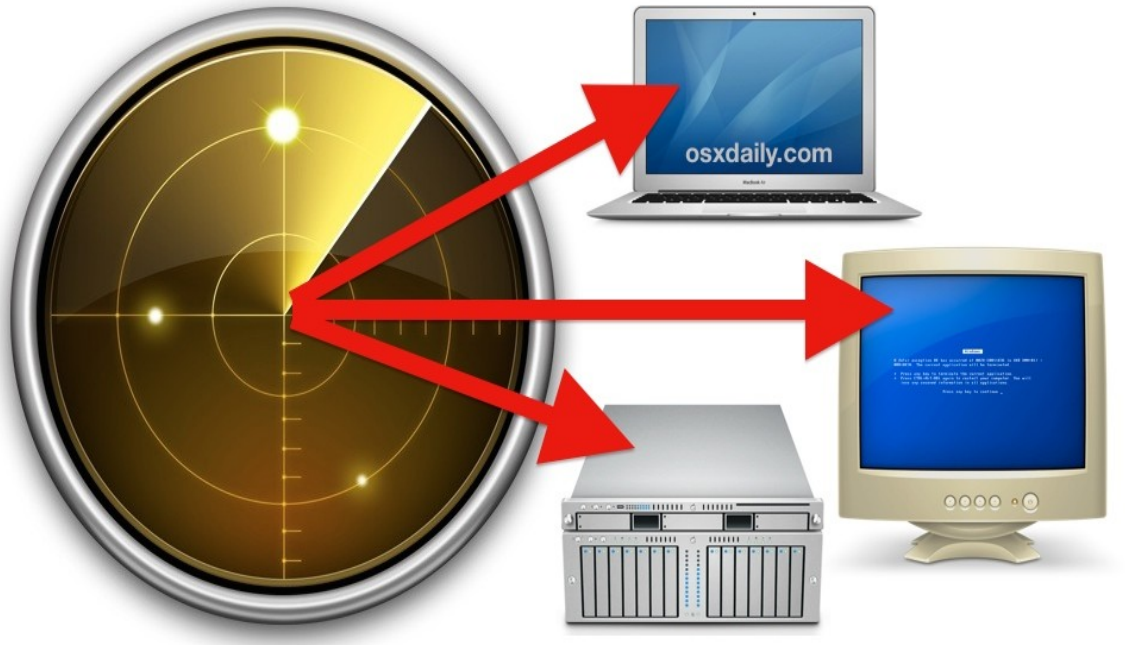
Why IDS/IPS and Firewalls



Why IDS/IPS and Firewalls

- Perimeter security devices cannot prevent all attacks
- IDS and IPS act on traffic after the firewall filters (allows) the traffic, according to configured policy.
- Firewalls filter traffic based on IP addresses and ports whereas IPS/IDS analyze the actual content (payload) of the packet.
  - Imagine an envelop which has a From Address, To Address and The Letter itself.
- Perimeter security devices like firewalls can only prevent attacks by/from outsiders, while IDS /IPS can respond to both inside and outside attacks
- Perimeter security do not detect when an attack is underway or has taken place
- Perimeter security devices do not respond/react to attacks

Why IDS/IPS and Firewalls



Port Scanning

Intrusion Detection System (IDS)

Intrusion Detection System

- IDS is software or hardware designed to monitor and analyze events occurring in a computer system or network to detect signs of security policy violation.

- Two actions taken by IDS
  - IDS is a passive system because it does not take direct action to block or stop the offending traffic or event; instead:
    - it ***logs*** the activity; or
    - It sends ***alerts*** to administrators or other systems to respond.

- Two types of IDS
  - Network-based IDS
  - Host-based IDS

- Three detection methods used by IDS
  - Signature-based
  - Anomaly-based
  - Policy-based

IDS Alert Types

- IDS generate various types of alerts when they detect suspicious or malicious activities on a network.

- Four common types of alerts
  - **True Positive** – occurs when the IDS correctly identifies a real attack or intrusion attempt.
  - **True Negative** – occurs when no alert is generated, and there is no attack or malicious activity in the network.
  - **False Positive** – occurs when the IDS generates an alert for activity that is benign or legitimate, incorrectly identifying it as malicious.
  - **False Negative** – occurs when the IDS fails to detect a real attack or malicious activity, meaning an attack goes undetected.

Network-based IDS

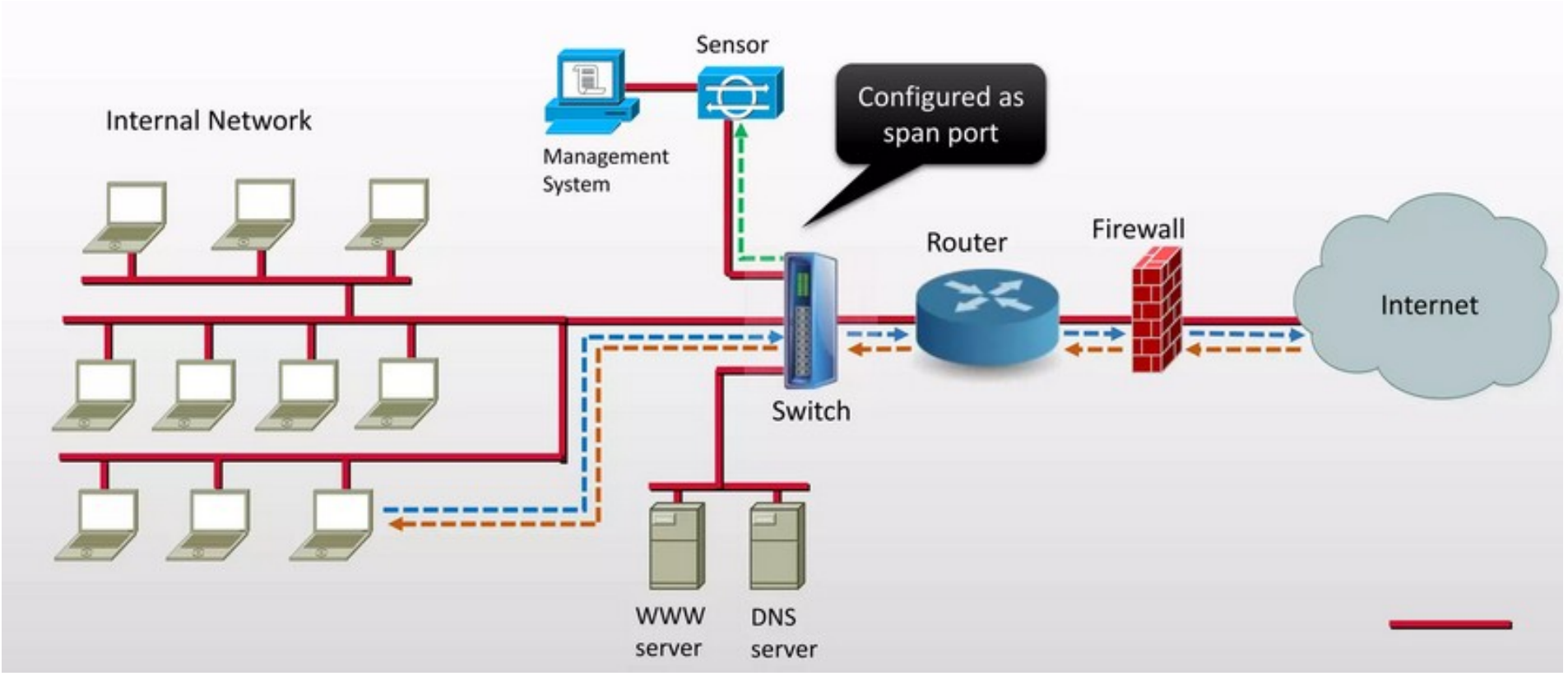
- NIDS are connected ***out-of-band*** on a network segment to monitor and analyze ***copies*** of network traffic.

- A single IDS sensor can monitor traffic for many hosts.

- They are platform independent – the OS being run by host machines does not matter.

- NIDS are available in two formats:
  - Appliance – consists of specialized hardware sensor and its dedicated software
  - Software – sensor software is installed on a server i.e. Snort

Network-based IDS

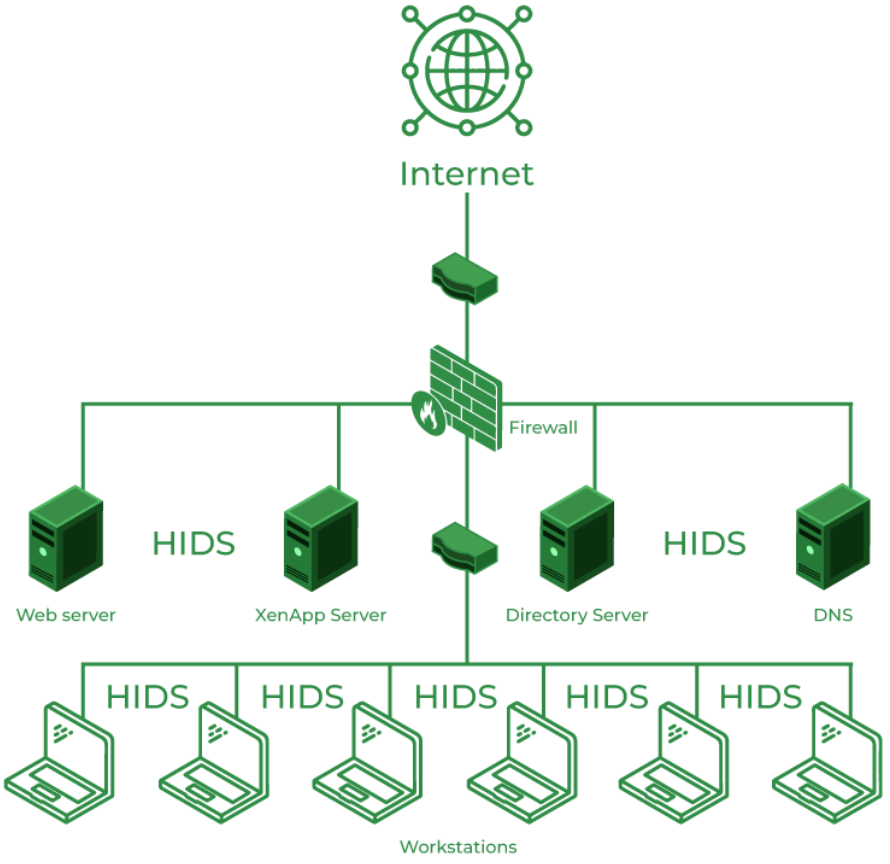


Host-based IDS

- Software agents installed on computers to monitor input and out put packets on the device

- It also performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting

Host-based IDS



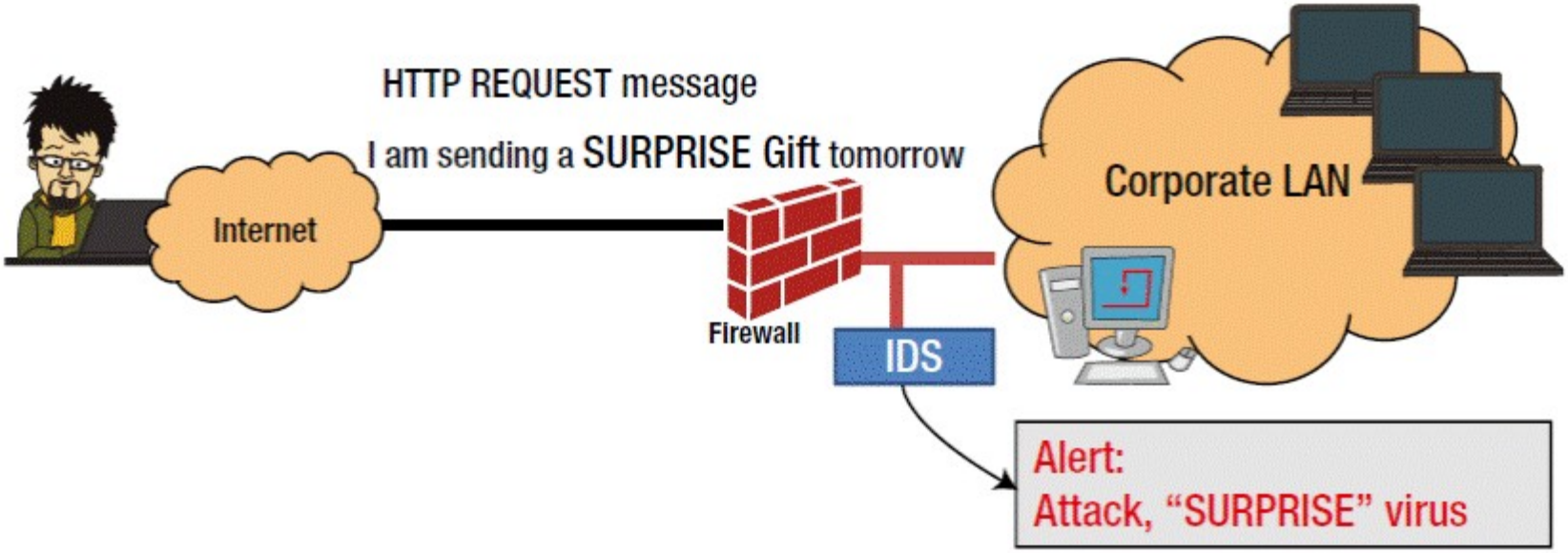
NIDS vs HIDS

Feature	NIDS	HIDS
Scope	Monitors network traffic across multiple devices	Monitors individual host activities and logs
Placement	Network	Installed on individual hosts
Traffic type	Analyzes network traffic before an attack reaches its target	Analyzes system logs, processes, and file integrity on target system
Focus	Network-wide detection	Host-specific detection
Real-time detection	Detects attacks in near real-time as traffic flows	Often analyzes logs after events occur
Encrypted traffic	Cannot inspect encrypted traffic	Can inspect traffic once decrypted
Resource impact	No impact on host performance	Consumes host system resources
Example threats detected	Network-based attacks (DDoS, port scanning, malware spread)	Host-based attacks (file tampering, privilege escalation, malware attack)
Best for	Monitoring large-scale network traffic	Monitoring specific endpoints or critical servers

Signature-based Detection

- Signature-based IDS analyzes content of each packet (payload) and compares it with a set of predefined signature rules.
- Works similar to an anti-virus
  - IDS's signature database must be updated to keep pace with new attacks
- Low false positive rates
- Highly effective towards well known attacks
- Fails to identify Zero Day Attacks and Advanced Malware Attacks
- Can be bypassed by changing the signature of attack

Signature-based Detection



Signature to Fire:

Header : IPv4	Protocol: HTTP	Destination Port: 80	Signature String: SURPRISE

Anomaly-based Detection

- It first establishes a baseline of normal behavior
- Monitors network traffic and compares it against the established baseline.
- Sounds alarm when monitored activity is outside baseline parameters.
- Prone to high false positive rates
- Effective against Zero Day Attacks and Advanced Malware Attacks

Policy-based Detection

- **Predefined Rules**
  - Administrators establish rules or policies that define what constitutes suspicious activity. For example, the policy may define access controls, allowed protocols, or file access permissions.

- **Real-time Monitoring**
  - The IDS continuously monitors network or system traffic and activities, comparing them against the defined policies. If any activity violates these rules, it triggers an alert.

- **For example**
  - Unauthorized access attempts (e.g., users trying to access restricted files).
  - Violations of internal policies (e.g., using non-allowed applications or services).
  - Access to sensitive resources during non-business hours.
  - Use of prohibited network protocols i.e. http or Telnet instead of HTTPS or SSH or port scans.

Intrusion Prevention System (IPS)

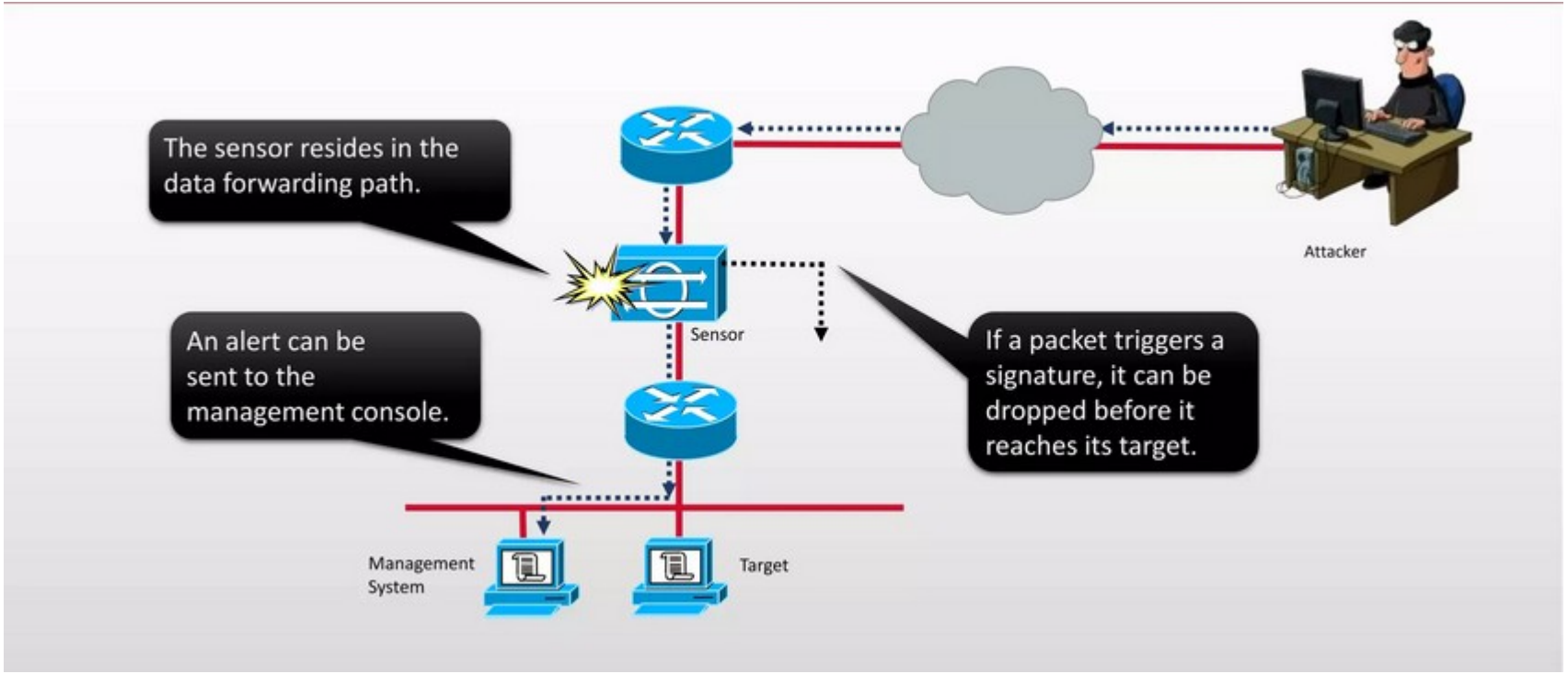
Intrusion Prevention System (IPS)

- IPS is software or hardware designed to:
  - monitor and analyze events occurring in a computer system or network to detect signs of security policy violation;
  - take appropriate action against the offending traffic

- IPS is an ***active*** system:
  - It ***logs*** the offending event or traffic;
  - It takes direct ***action*** to block or stop the offending event;
  - It sends ***alerts*** to administrators.

- An IPS is similar to an IDS apart from the fact that an IPS can take action and is placed inline of data.

Placement of IPS



IPS Placement and Actions

- Placement
  - An IPS is placed inline of traffic

- An IPS takes immediate action to stop the detected threat. This can include:
  - Blocking malicious IP addresses or connections.
  - Terminating suspicious sessions or traffic flows.
  - Modifying firewall rules to prevent further access.
  - Sending alerts to administrators.

Types of IPS and Detection Methods

- Types of IPS:
  - Network-based IPS (NIPS)
  - Host-based IPS (HIPS)

- Detection Methods:
  - Signature-based detection
  - Anomaly-based detection

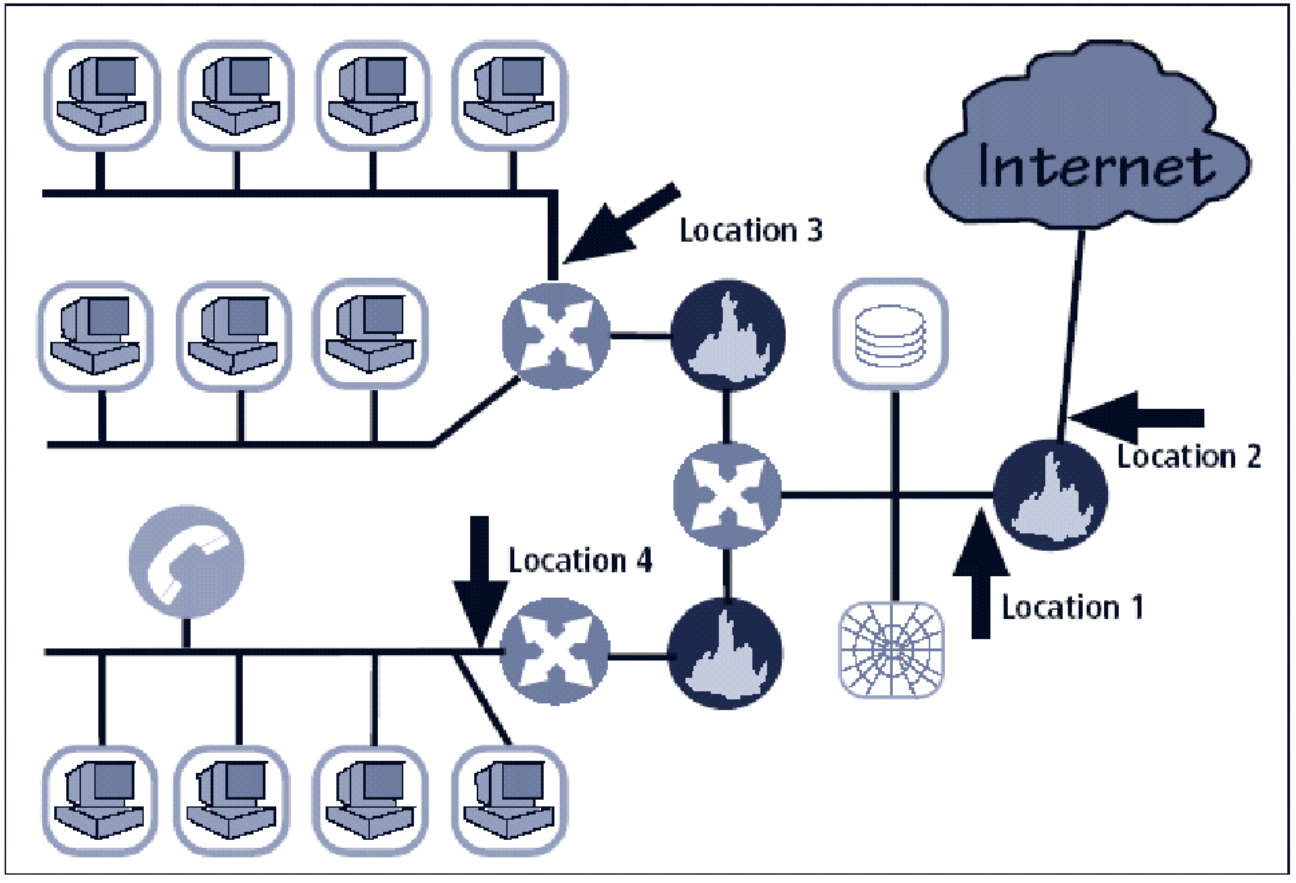
IDS/IPS Comparison Table

Feature	IDS	IPS
Primary function	Monitors and detects	Monitors, detects, prevents
Response action	Logs and generates alerts	Logs and blocks threats
Network position	Out-of-band	Inline
Traffic impact	No impact on network traffic	Adds latency to traffic
Use case	Ideal for threat detection	Ideal for threat prevention
Management	Requires manual response	Works autonomously
Complexity	Easier to implement	More complex set up
Effectiveness	Offending traffic may reach intended target	Reacts in real-time

Deploying NIDS/NIPS

- NIST recommends four locations for NIDS:
  - Location 1 – behind each external firewall
  - Location 2 – in front of each external firewall
  - Location 3 – on major network backbones
  - Location 4 – on critical subnets

Deploying NIDS/NIPS



Honeypots

Honeypots

- **Honeypots -** decoy systems designed to lure potential attackers away from critical systems

- Design goals:
  - Divert attacker from accessing critical systems
  - Gather intelligence about attacker's activity and patterns
  - Encourage attacker to linger so admins can document event, respond

- **Honeynets -** collection of honeypots connected in a subnet

- Honeypots should be used carefully to avoid accidentally providing attackers with additional resources to launch further attacks.

- Summary

  IDS/IPS systems are an essential part of layered security architecture, complementing other defenses like firewalls, antivirus software, and threat intelligence platforms, to provide a more comprehensive network protection solution

End