Intrusion Detection System (IDS):-

An **Intrusion Detection System (IDS)** is a cybersecurity solution designed to monitor network or system activities for **malicious actions or policy violations**. It detects unauthorized access, misuse, or anomalies in a computer system or network and alerts administrators to potential threats.

An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer.

The IDS is also a listen-only device. The IDS monitors traffic and reports results to an administrator. It cannot automatically take action to prevent a detected exploit from taking over the system.

Attackers are capable of exploiting vulnerabilities quickly once they enter the network. Therefore, the IDS is not adequate for prevention. Intrusion detection and intrusion prevention systems are both essential to security information and event management.

What Does an IDS Do?

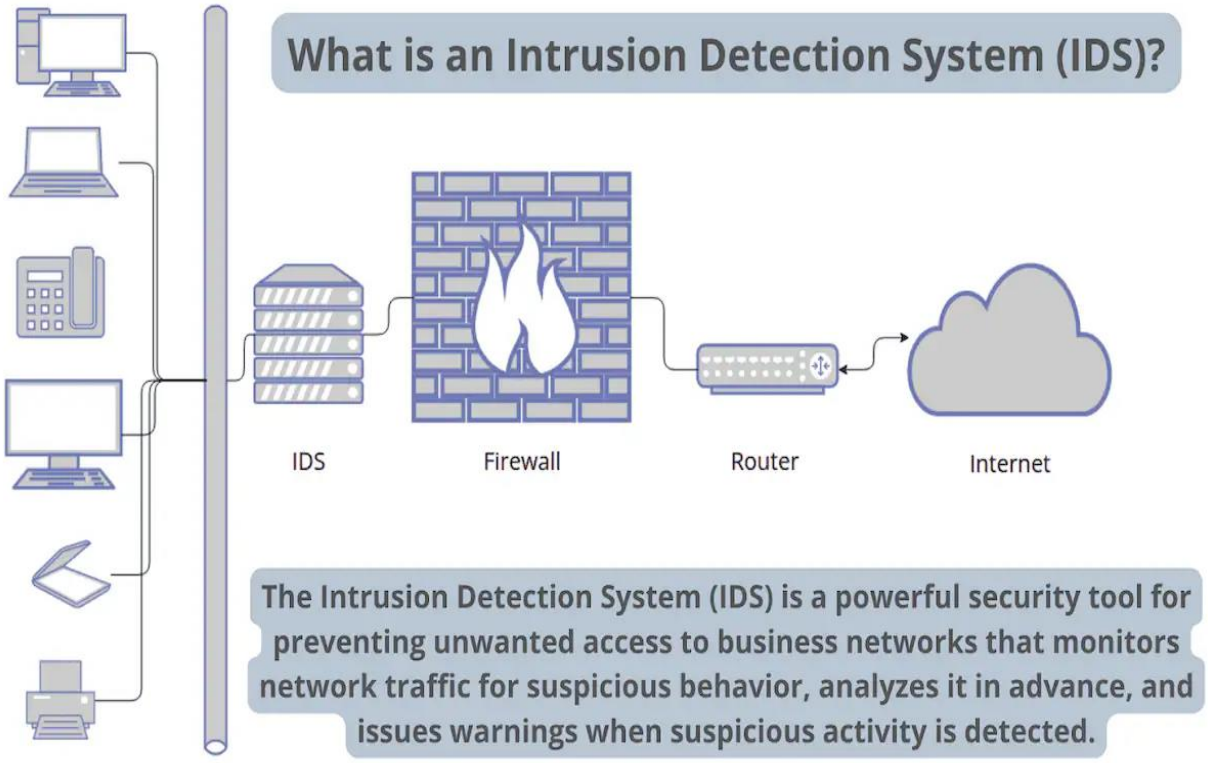
- **Monitors** network traffic or system behavior.
- **Detects** suspicious or malicious activity.
- **Alerts** system or network administrators.
- May **log events** or take limited automatic actions (like blocking IPs).

How IDS Works: -

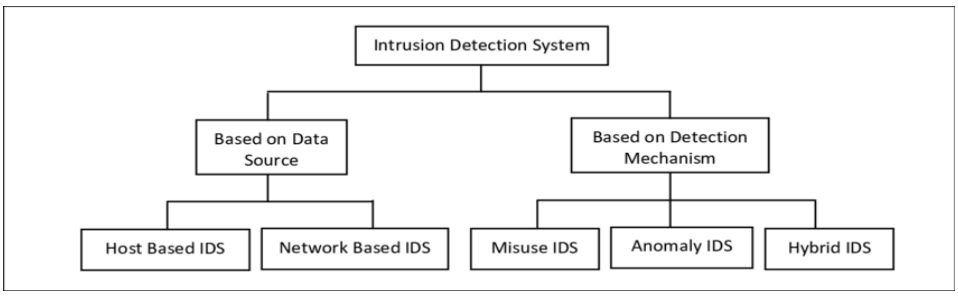
An IDS only needs to detect potential threats. It is placed out of band on the network infrastructure. Consequently, it is not in the real-time communication path between the sender and receiver of information. IDS solutions often take advantage of a TAP or SPAN port to analyze a copy of the inline traffic stream. This ensures that the IDS do not impact inline network performance.

When IDS was developed, the depth of analysis required to detect intrusion could not be performed quickly enough. The speed would not keep pace with components on the direct communications path of the network infrastructure. Network intrusion detection systems are used to detect suspicious activity to catch hackers before damage is done to the network. There are network-based and host-based intrusion detection systems. Host-based IDSes are installed on client computers; network-based IDSes are on the network itself.

An IDS works by looking for deviations from normal activity and known attack signatures. Anomalous patterns are sent up the stack and examined at protocol and application layers. It can detect events like DNS poisonings, malformed information packets and Christmas tree scans. An IDS can be implemented as a network security device or a software application. To protect data and systems in cloud environments, cloud-based IDSes are also available.



Types of Intrusion Detection Systems



IDS can be categorized based on:

1. Based on Monitoring Location:

a. Network-based IDS (NIDS):

- Monitors traffic across an entire network.
- Placed at strategic points (e.g., firewalls or routers).
- Useful for detecting external threats like DDoS or port scanning.

📌 *Example:* Snort, Suricata

b. Host-based IDS (HIDS):

- Monitors individual systems or devices.
- Analyzes OS-level activities (e.g., file integrity, logins).
- Good for detecting insider threats or malware infections.

📌 *Example:* OSSEC, Tripwire

---

2. Based on Detection Method:

a. Signature-based IDS:

- Detects known threats using predefined patterns (signatures).
- Fast and accurate for known attacks.
- Weak against new or unknown threats (zero-day attacks).

📌 *Analogy:* Like antivirus scanning for known malware signatures.

b. Anomaly-based IDS:

- Uses machine learning or statistical models to detect unusual behavior.
- Can identify novel or zero-day attacks.
- May produce more false positives due to deviations from "normal" behavior.

📌 *Analogy:* Like noticing strange behavior in a familiar friend.

c. Hybrid IDS:

- Combines signature and anomaly-based methods.

- Provides more comprehensive detection with better accuracy.

⚙️ **Related Terms:**

- **IPS (Intrusion Prevention System):** Like IDS, but can take active measures to block threats.
- **SIEM (Security Information and Event Management):** Often integrates with IDS for centralized monitoring and response.

📌 **Summary Table**

Type	Focus Area	Detection Method	Examples
NIDS	Network traffic	Signature/Anomaly	Snort, Suricata
HIDS	Host system	Signature/Anomaly	OSSEC, Tripwire
Signature-based	Known attacks	Pattern matching	Many IDS types
Anomaly-based	Unknown attacks	Behavioral analysis	AI/ML-based IDS
Hybrid	Both	Combined methods	Advanced IDS