Intrusion Detection Systems (IDS)

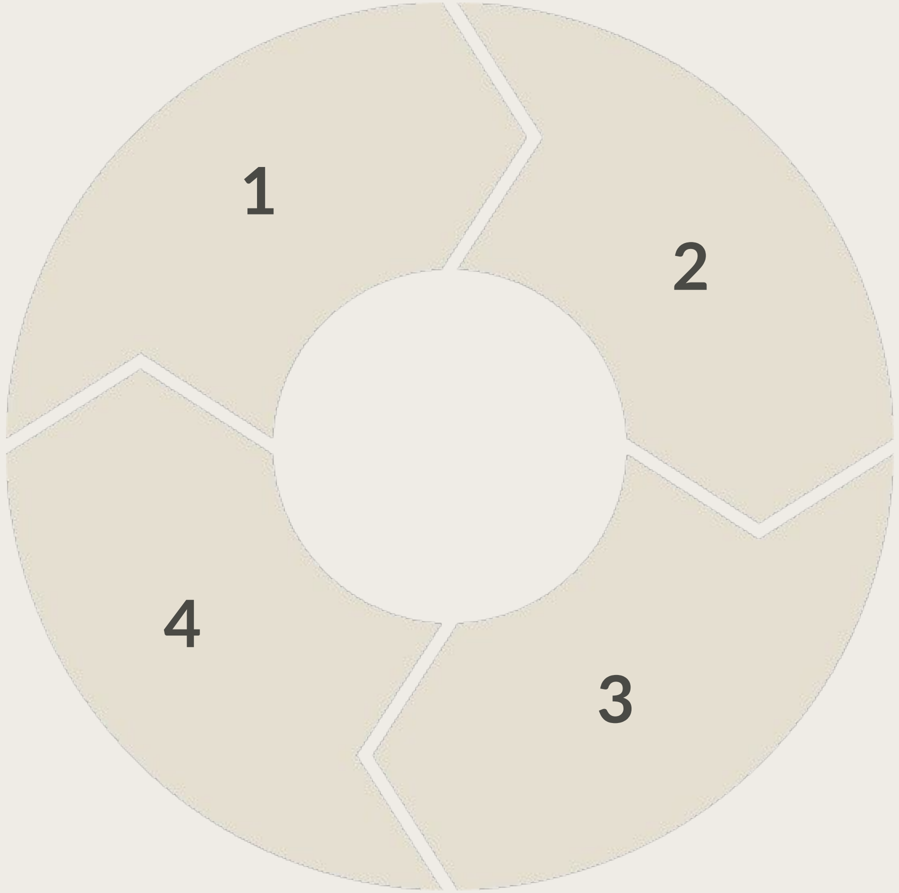
CS4062D: Introduction to Information Security

RACHEL PAUL
B221138CS

What is IDS ?

An Intrusion Detection System (IDS) is used to monitor network traffic for suspicious activity and generate alerts when such activity is discovered

Working of an IDS



Network Monitoring

IDS monitors network traffic for threats.

Data Collection

Collects and logs network traffic data.

Signal

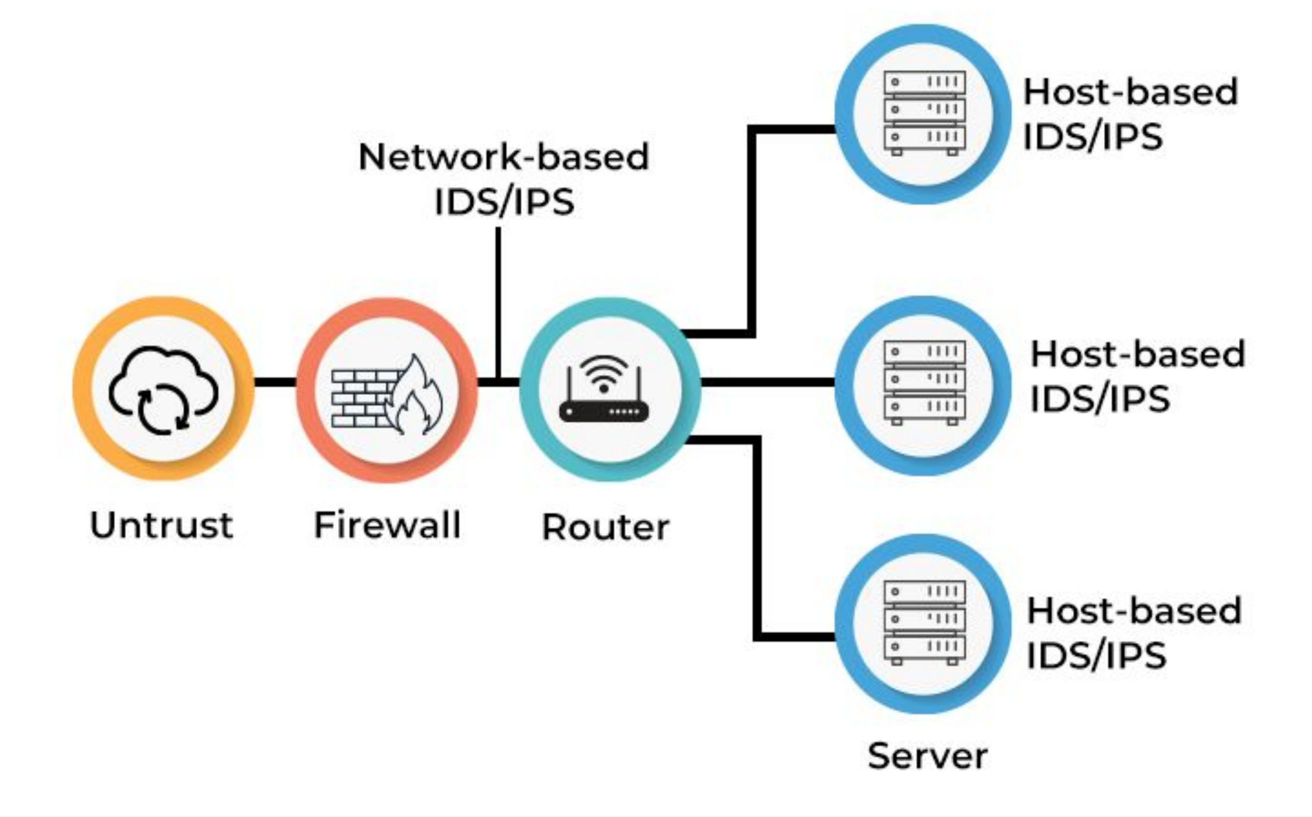
Alerts sent to the Network Security Administrator.

Data Analysis

Analyzes data to find suspicious behavior.

Types of IDS

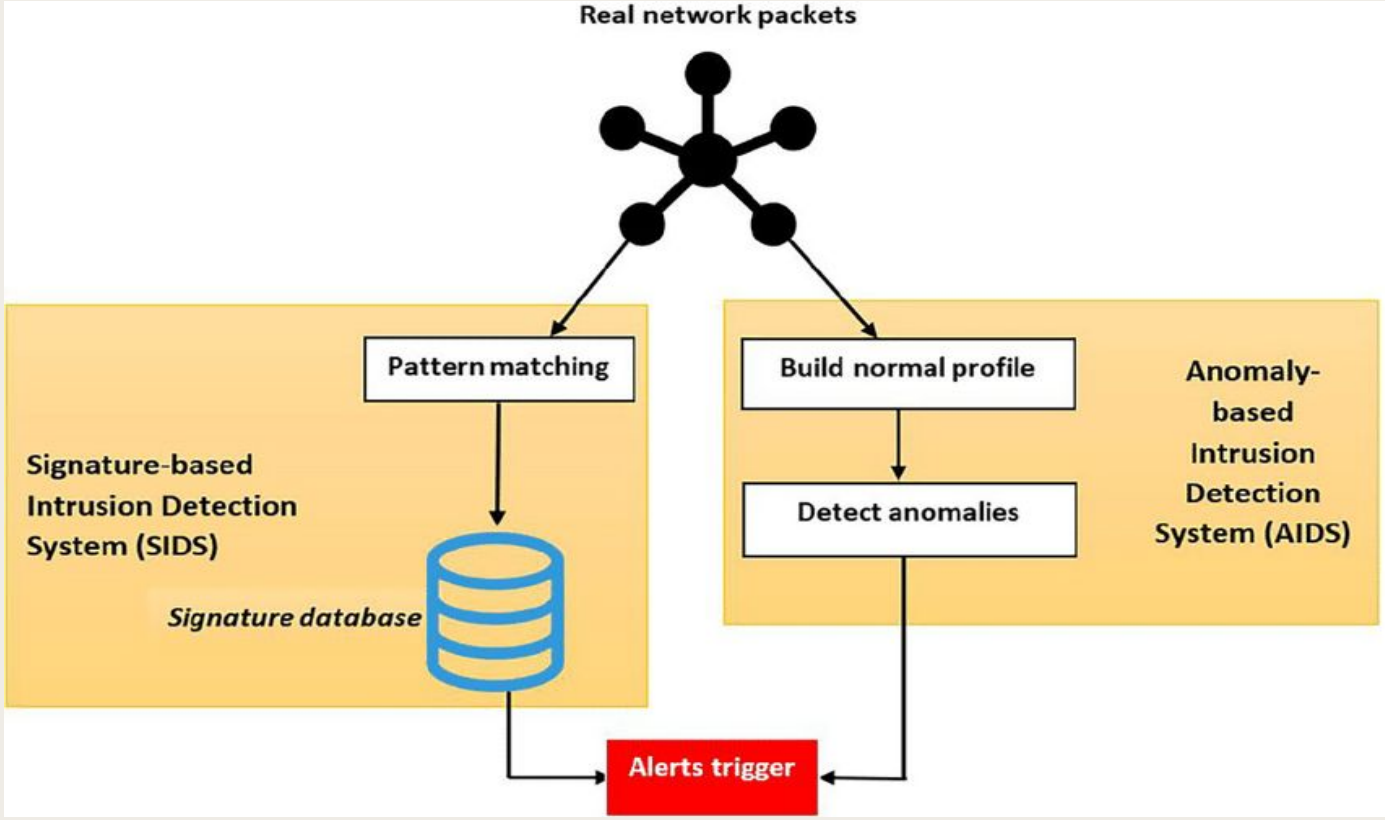
Based on how the IDS is deployed.



- **Network- based IDS**
  monitors the entire network
- **Host-based IDS**
  monitors only the host system on which it resides.

Types of IDS

Based on how the IDS detects threats.



- **Anomaly-based IDS**
  Detects unusual behavior with predefined baseline
- **Signature-based IDS**
  Alerts if it finds known suspicious signatures

Emerging Technology in IDS

The global IDS market is projected to reach USD 9.3 billion by 2032 (USD 5.8 billion in 2023), with a Compound Annual Growth Rate (CAGR) of 5.30% during the forecast period.

1 **AI & ML**

AI and ML enhance threat detection through advanced pattern recognition.

2 **Behavioral Analysis**

Behavioral Analysis helps detect deviations to uncover zero-day exploits.

3 **SIEM Integration**

SIEM Integration consolidates security events for improved response capabilities.

4 **Cloud-based Solutions**

Cloud-based Solutions offer scalable IDS tailored for dynamic cloud environments.

5 **IoT Security Integration**

IoT-driven IDS monitors network traffic from IoT devices, identifying vulnerabilities and preventing botnet attacks like Mirai.

6 **Edge Computing Integration**

Provides real-time threat detection closer to the source, reducing latency and improving response time.

7 **Deception Technology**

Deception Technology deploys decoys and traps to mislead attackers, helping organizations detect and study malicious behavior.

References

[1] S. A. Aljawarneh, "SIDSs vs. AIDSs detection main phases," ResearchGate, 2021.

[2] H. Badgujar, "What is IDS (Intrusion Detection System)? How it works?," Medium, 2023.

[3] "DS/IPS on an Enterprise Network", ZD Brightspot, 2022.

[4] E. Kavas, "Strengthening Network Security: Evolution and Future of IDS & IPS," LinkedIn.

[5] N. Sharma, A. Gupta, A. Jain, and R. C. Jain, "Artificial Intelligence Based Intrusion Detection Techniques - A Review," ResearchGate, 2014.

[6] Market Research Future, "Intrusion detection system market research report – Forecast 2030." MarketResearchFuture.