Access Control Monitoring

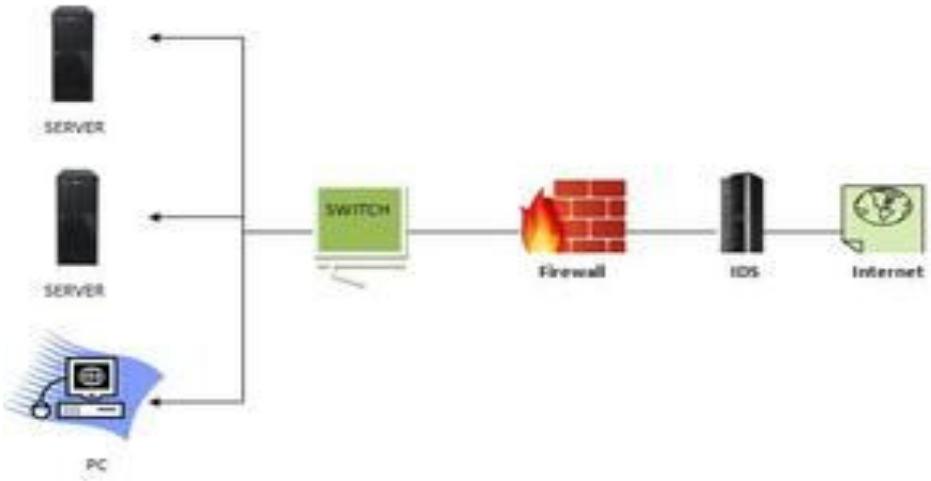
Module 4 : Identity and Access Management

IDS and IPS and anomaly detection.

- A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed.
- It is software that checks a network or system for malicious activities or policy violations.
- Each illegal activity or violation is often recorded either centrally using a SIEM system or notified to an administration.

IDS

IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders. The intrusion detector learning task is to build a predictive model (i.e. a classifier) capable of distinguishing between ‘bad connections’ (intrusion/attacks) and ‘good (normal) connections’.

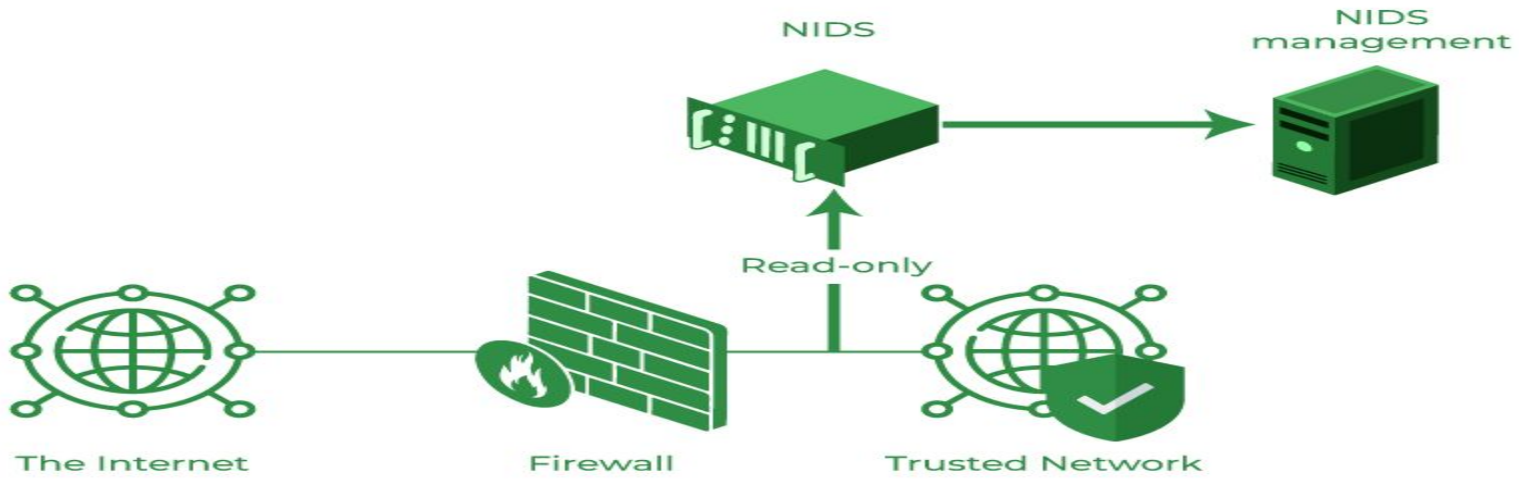


How does an IDS work?

- An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.
- It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.
- The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.
- If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.
- The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

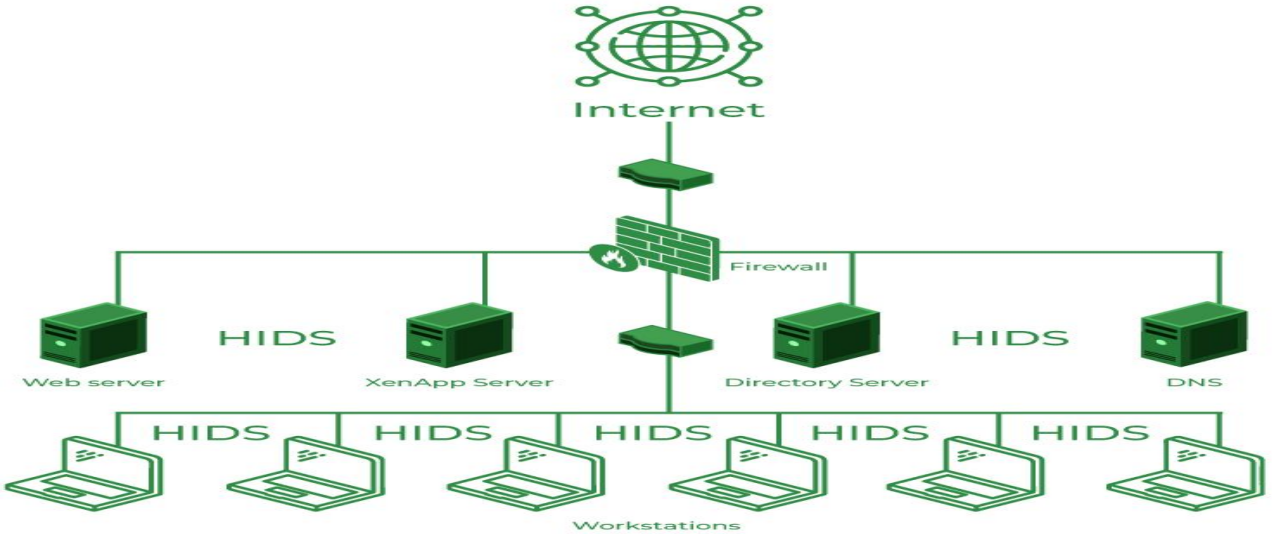
Classification of Intrusion Detection System

Network Intrusion Detection System (NIDS): Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network.



Host Intrusion Detection System (HIDS):

- Host Intrusion Detection System (HIDS): Host intrusion detection systems (HIDS) run on independent hosts or devices on the network.
- A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected.
- It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate.
-



Protocol-based Intrusion Detection System (PIDS):

Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accepting the related HTTP protocol.

Application Protocol-based Intrusion Detection System (APIDS): An application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols.

For example, this would monitor the SQL protocol explicitly to the middleware as it transacts with the database in the web server

Hybrid Intrusion Detection System:

- Hybrid Intrusion Detection System: Hybrid intrusion detection system is made by the combination of two or more approaches to the intrusion detection system.
- The hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS

Benefits of IDS

Detects malicious activity: IDS can detect any suspicious activities and alert the system administrator before any significant damage is done.

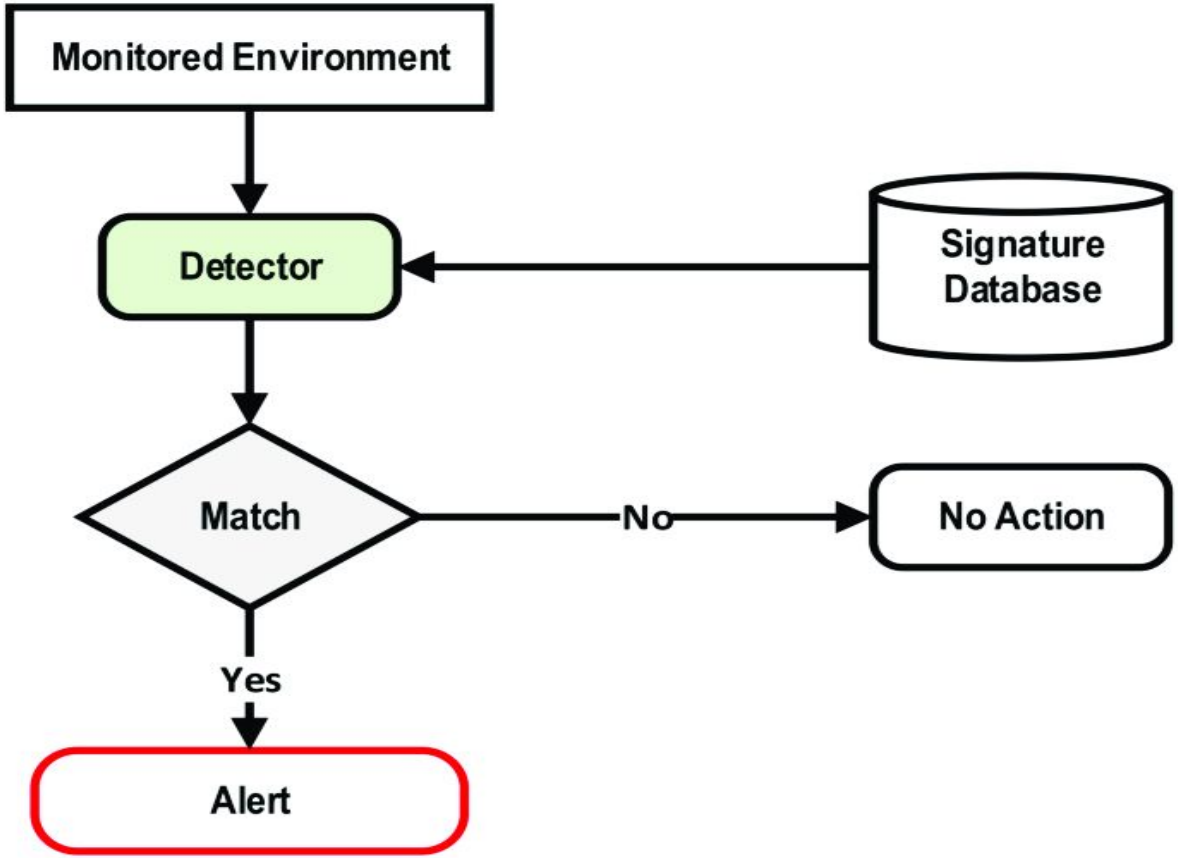
Improves network performance: IDS can identify any performance issues on the network, which can be addressed to improve network performance.

Compliance requirements: IDS can help in meeting compliance requirements by monitoring network activity and generating reports.

Provides insights: IDS generates valuable insights into network traffic, which can be used to identify any weaknesses and improve network security.

Detection Method of IDS

Signature-based Method: Signature-based IDS detects the attacks on the basis of the specific patterns such as the number of bytes or a number of 1s or the number of 0s in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in the system but it is quite difficult to detect new malware attacks as their pattern (signature) is not known.

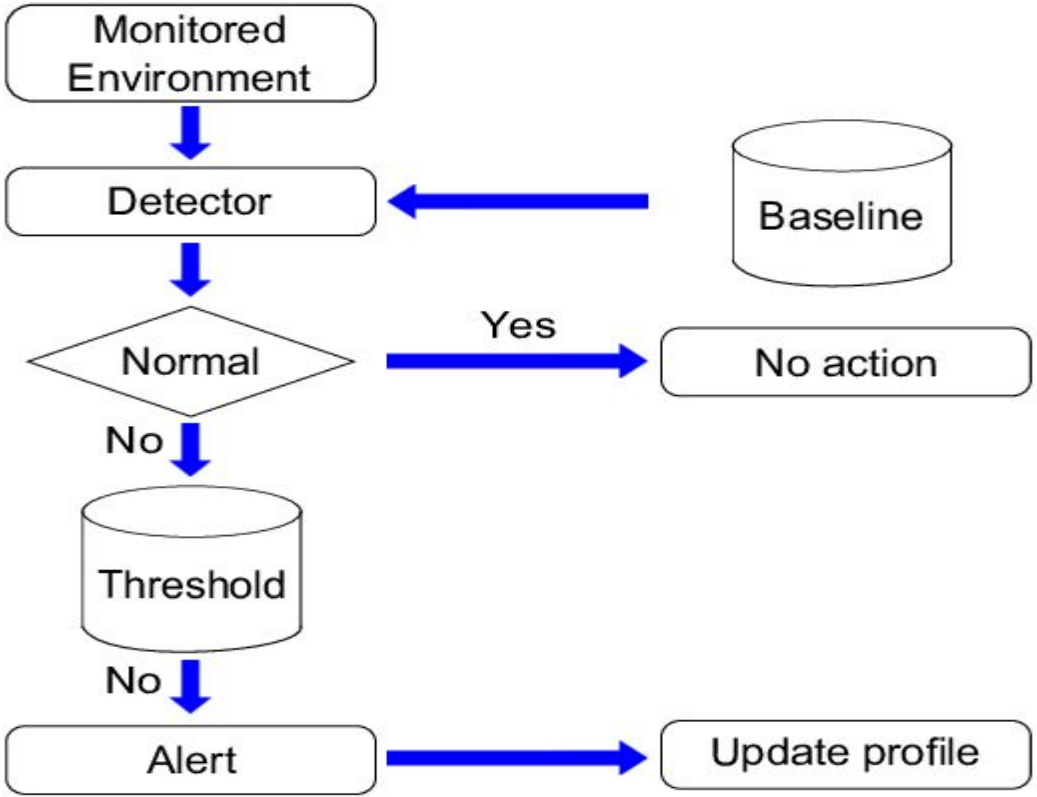


Signature-based Method

Anomaly-based Method:

Anomaly-based IDS was introduced to detect unknown malware attacks as new malware is developed rapidly. In anomaly-based IDS there is the use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in the model.

The machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

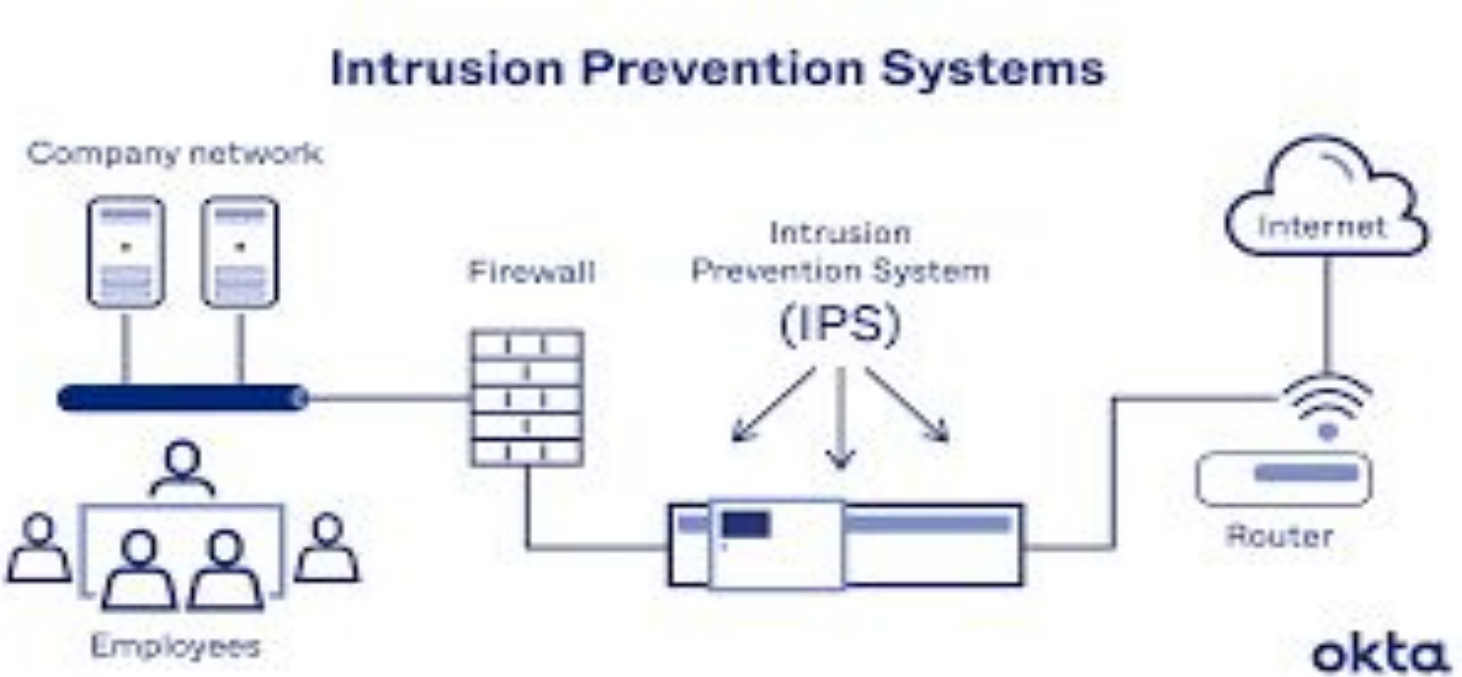


Anomaly-based Method

Table1. Comparison between Misuse and Anomaly Detection

Misuse Detection/Signature Based Detection	**Anomaly Detection/Profile Based Detection**
Advantages	**Advantages**
1. High detection rate and accuracy for known behaviors or patterns 2. Simplest and useful method 3. Low false alarm rate	1. Accuracy for unknown behaviors 2. Missing pattern rate is low 3. Detect novel and unexpected vulnerabilities
Disadvantages	**Disadvantages**
1. It can detects only known attacks 2. Needs usual updates of rules 3. No segregation between attack endeavor and successful attack 4. Missing pattern rate is high	1. Needs to be more trained or else increases false alarm rate. 2. Low detection rate and high false alarm rate 3. It can detect new attacks because intrusion detection is based on latest updates.

IPS(intrusion prevention systems)



Why Do You Need an IPS?

Protection Against Known and Unknown Threats: An IPS can block known threats and also detect and block unknown threats that haven't been seen before.

Real-Time Protection: An IPS can detect and block malicious traffic in real-time, preventing attacks from doing any damage.

Compliance Requirements: Many industries have regulations that require the use of an IPS to protect sensitive information and prevent data breaches.

Cost-Effective: An IPS is a cost-effective way to protect your network compared to the cost of dealing with the aftermath of a security breach.

Increased Network Visibility: An IPS provides increased network visibility, allowing you to see what's happening on your network and identify potential security risks.

Classification of Intrusion Prevention System (IPS):

Network-based intrusion prevention system (NIPS):

It monitors the entire network for suspicious traffic by analyzing protocol activity.

Wireless intrusion prevention system (WIPS):

It monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.

Network behavior analysis (NBA):

It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy violations.

Host-based intrusion prevention system (HIPS):

It is an inbuilt software package which operates a single host for doubtful activity by scanning events that occur within that host.

Detection Method of Intrusion Prevention System (IPS):

Signature-based detection:

Signature-based IDS operates packets in the network and compares with pre-built and preordained attack patterns known as signatures.

Statistical anomaly-based detection:

Anomaly based IDS monitors network traffic and compares it against an established baseline. The baseline will identify what is normal for that network and what protocols are used. However, It may raise a false alarm if the baselines are not intelligently configured.

Stateful protocol analysis detection:

This IDS method recognizes divergence of protocols stated by comparing observed events with pre-built profiles of generally accepted definitions of not harmful activity.