Mirox
Reinforce Your Security

Intrusion Detection System

&

Intrusion Prevention System

Topics To Cover :-

❑ Types of IDS

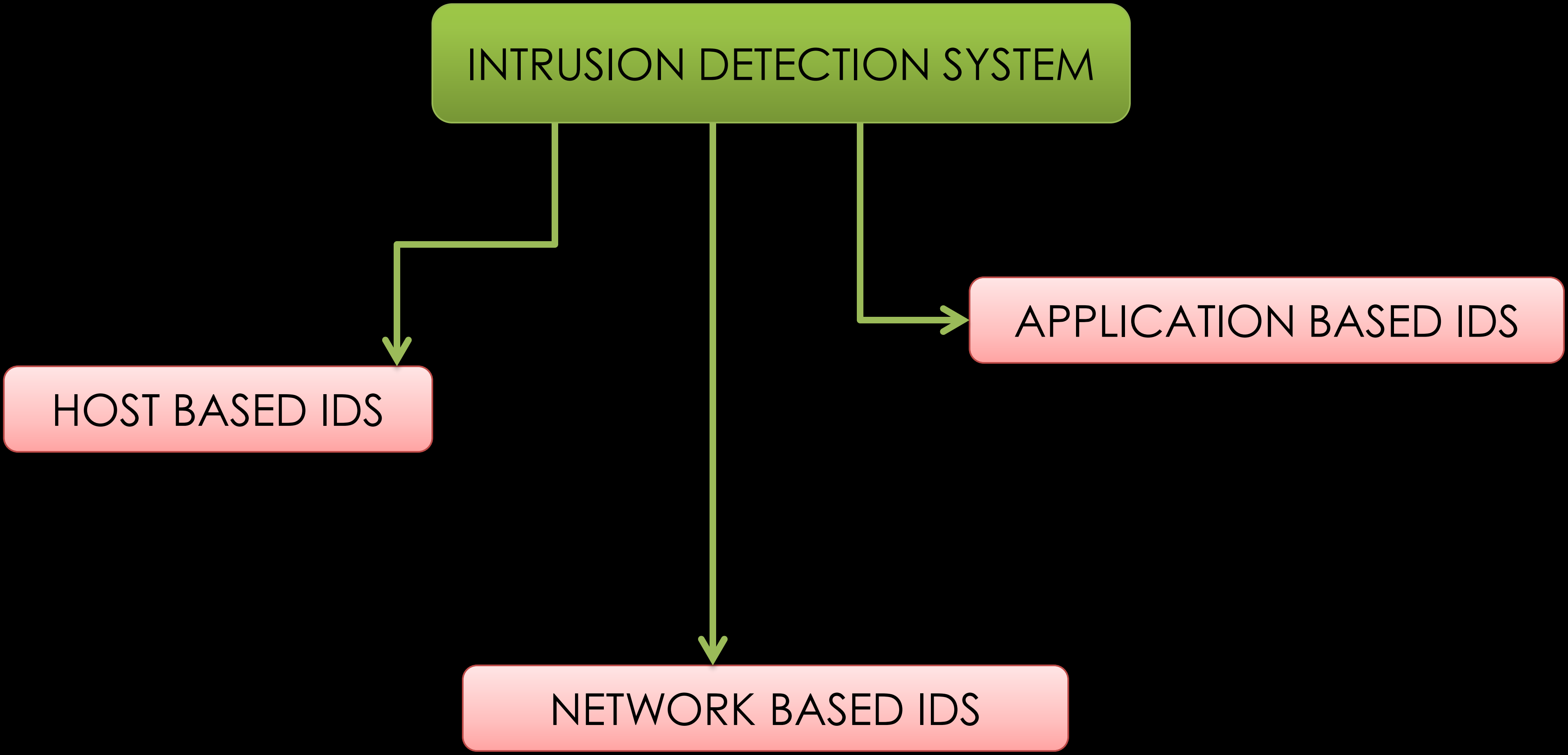
❑ Deployment of IDS

❑ Types of Signatures

❑ True/True-Negative/False-Positive/Negative

❑ Major methods of operation

❑ Types Of IDS:-



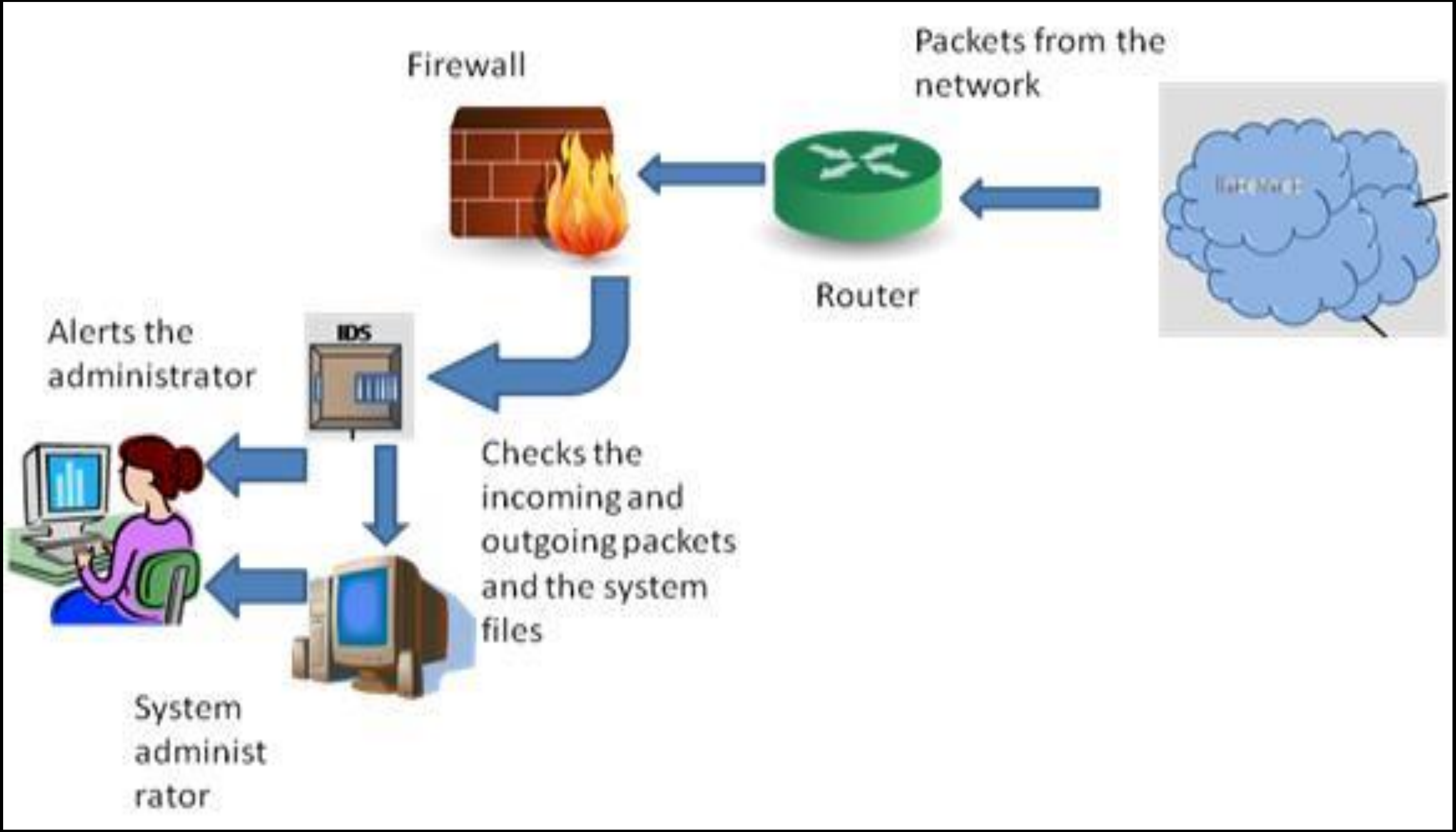
INTRUSION DETECTION SYSTEM

HOST BASED IDS

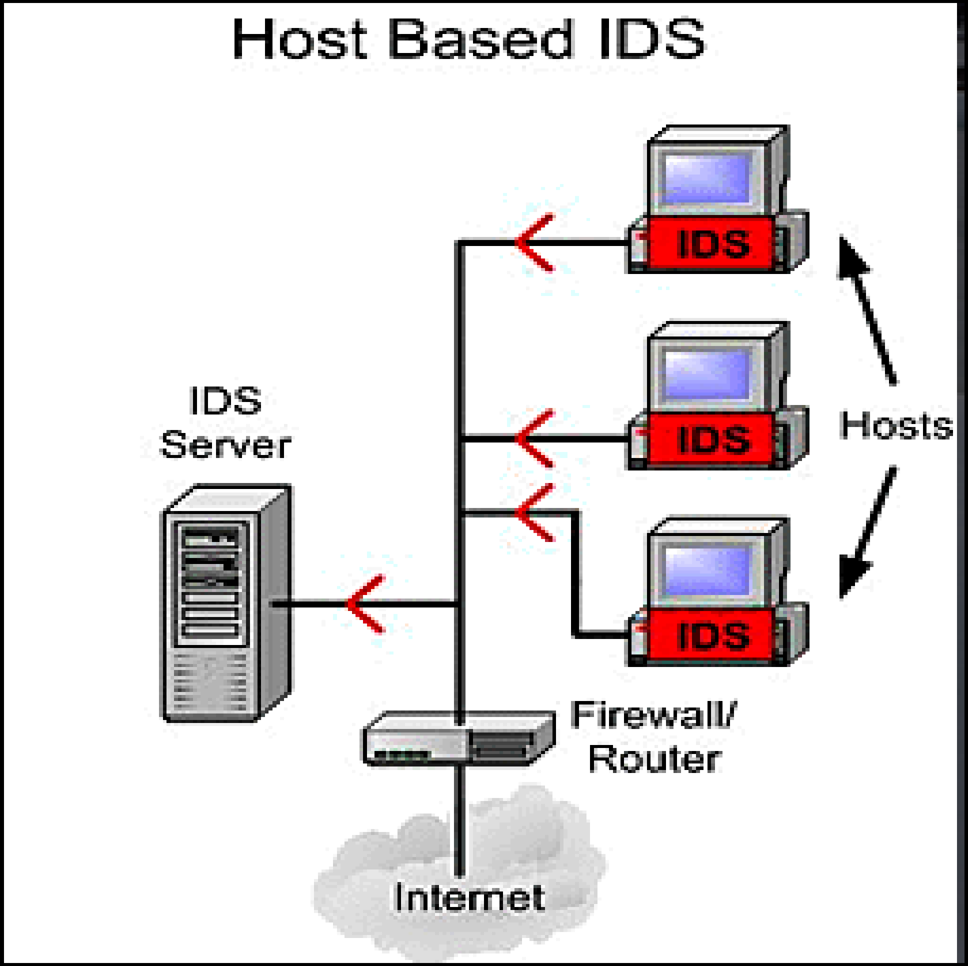
NETWORK BASED IDS

APPLICATION BASED IDS

❑ Deployment of IDS :-



❑ Host Based IDS (HIDS)



The first type of IDS to be developed and implemented.

HIDS run on individual hosts or devices on the network.

HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected.

Collect and analyze data that originate on a computer that hosts a service, such as a Web Server.

The result of the scan performed by the HIDS are logged into a secure database and compared with the knowledge base to detect any malicious activity.

Operating System Level

Determine unauthorized activities based on the following :-

- ❑ Application initiated on a system.
- ❑ Logon and Logoff credentials like date and time, login locations etc.
- ❑ Access to system resources like files/folders/memory location/registry.

Application Level

- ❑ Concentrate more on the application level log files rather than the system level log files.
- ❑ An ideal solution for detecting intrusion attempts to a database application.

Network Level

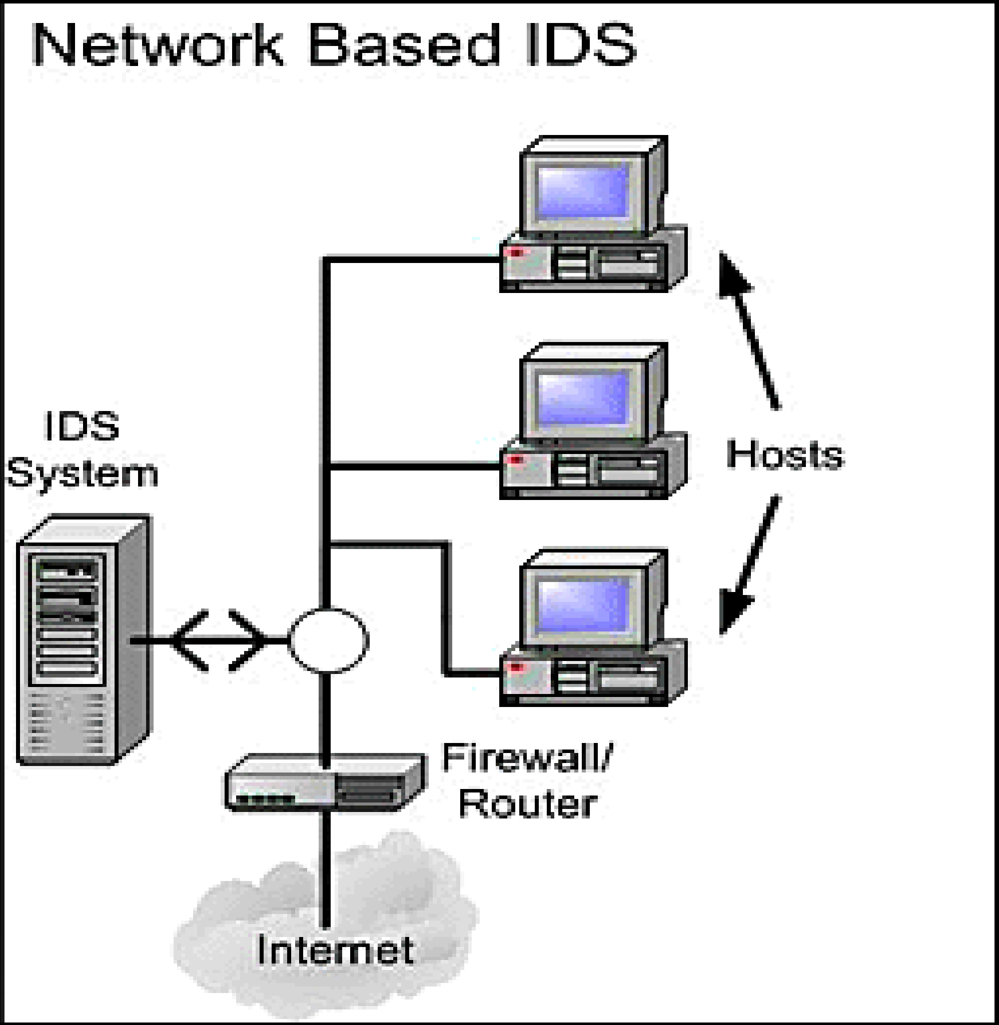
- A network-level HIDS works on the network packets that are addressed to particular host.
- If a packet is not addressed to host, the network-level HIDS will not collect and work on the network packet.

Advantages of HIDS

- Cost effective when compared to NIDS for a small to medium sized network.
- HIDS can provide another layer of security by detecting attacks missed by other security tools in the architecture.
- More control and command over the system entities like memory, registry, system files etc.

- Verifies success or failure of an attack
- Monitors System Activities
- Detects attacks that a network based IDS fail to detect
- Near real time detection and response
- Does not require additional hardware
- Lower entry cost

❑ Network Based IDS (NIDS)



Placed at a strategic point or points within the network to monitor traffic to and from all devices on the network.

Abnormal behavior is sensed, the alert can be sent to the administrator.

NIDS are also capable of comparing signatures for similar packets to link and drop harmful detected packets which have a signature matching the records in the NIDS.

Network-based intrusion detection analyzes data packets that travel over the actual network.

Network based IDS uses techniques like “packet-sniffing” to pull data from TCP/IP or other protocol packets traveling along the network.

Two types :-

On-Line and Off-Line NIDS

❑ On-Line NIDS deals with the network in real time.

❑ It analyses the Ethernet packets and applies some rules, to decide if it is an attack or not.

❑ Off-line NIDS deals with stored data and passes it through some processes to decide if it is an attack or not.

❑ Application Based IDS (APIDS)

An Application based IDS is like a host-based IDS designed to monitor a specific application.

e.g. Antivirus software designed specifically to monitor mail server.

An APIDS is extremely accurate in detecting malicious activity for the applications it protects.

APIDS will check the effective behavior and event of the protocol.

The system or agent is placed between a process and group of servers that monitors and analyzes the application protocol between devices.

❑ Types of Signatures :-

- ❑ Signature Based
- ❑ Anomaly Based
- ❑ Rule Based
- ❑ Stateful Protocol Analysis

❑ Signature Based

Compares signatures against observed events to identify possible incidents.

This is the simplest detection method because it compares only the current unit of activity.

Signature based IDS refers to the detection of attacks by looking for specific patterns.

Byte sequences in network traffic, or known malicious instruction sequences used by malware.

❑ Anomaly Based

To detect unknown attacks.

Basic approach is to use machine learning to create a model of trustworthy activity, and then compare new behaviour against this model.

This approach enables the detection of previously unknown attacks.

Compares definitions of what is considered normal activity with observed events in order to identify significant deviations.

❑ Rule Based

A knowledge base programmed as rules will decide the output alongside an inference engine.

If the defined rules for example all match, a certain assumption can be determined in which an action may take place.

❑ Stateful Protocol Analysis

Stateful protocol analysis identifies deviations of protocol state similarly to the anomaly-based method.

Monitoring requests with its corresponding response.

Every request should have a predictable response.

Those responses that fall outside of expected results will be flagged and analysed further.

❑ True/True-Negative/False-Positive/Negative :-

- ➢ True Positive
- ➢ True Negative
- ➢ False Positive
- ➢ False Negative

- True Positive = Correctly Identified

True positive (TP) : If the analysed event is correctly classified as intrusion/malicious.

- True Negative = Correctly Rejected

True negative (TN) : If the analysed event is correctly classified as normal/innocuous.

- False Positive = Incorrectly Identified

False positive (FP) : If the analysed event is innocuous (or ‘‘clean’’) from the perspective of security, but it is classified as malicious.

- False Negative = Incorrectly Rejected

False negative (FN) : If the analysed event is malicious but it is classified as normal/innocuous.

True Positive : It is an event when an intrusion did happen and the IPS did react on it. This is a normal thing.

True Negative : No intrusion happened and no action is taken by an IPS. This represents a normal traffic flow. This is also normal.

False Positive : It is not an intrusion but rather a situation when normal user traffic triggers an alarm. This can cause a lot of log entries or even drop normal user traffic. This is NOT normal.

False Negative : This is a situation in which an intrusion did happen and IPS totally missed it! This is also NOT normal.

❑ Major methods of operation

Monitor incoming connection attempts .

Examine host based incoming and outgoing network connections.

Particularly related to the unauthorized connection attempts to TCP or UDP ports and can also detect incoming Portscans.

Protect the network/host by intercepting suspicious packets and looking for aberrant payloads (packet inspection).

Monitor login activity onto the networking layer of their protected host.

looking for unusual activity on a system occurring at unexpected times, particular network locations or detecting multiple login attempts.

Identification of successful intruders.

Identification of own system weaknesses.

Repelling potential intruders by simply making them aware of the existence of the auditing means.

Allowing of parameterization for easy recording of system event logs and user activities.

Providing an option of self-disengagement of logging mechanisms in the event of insufficient space or DoS attacks.

Reasonable minimum system resource consumption for auditing purposes.

THANK YOU !