SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with ‘A’ Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

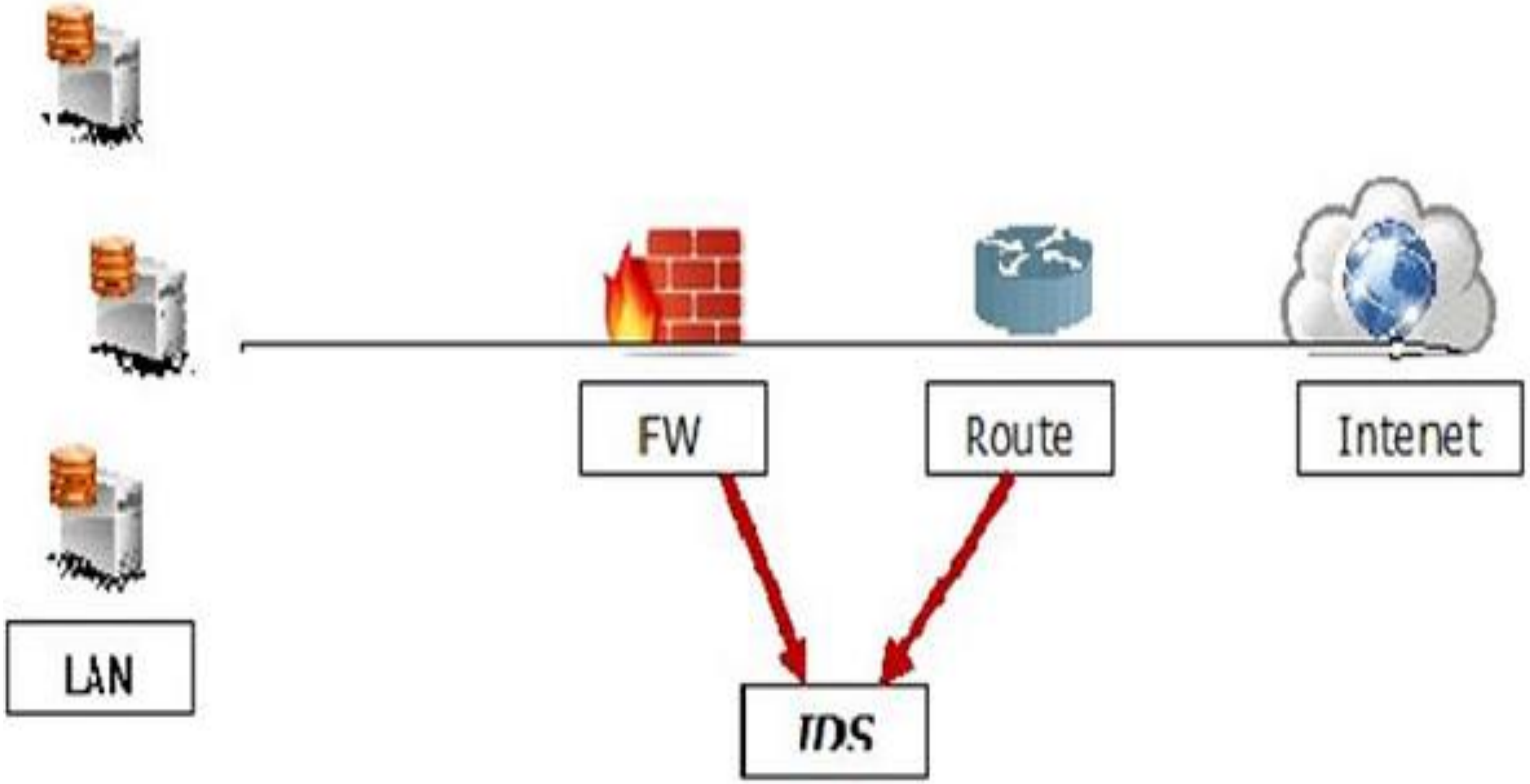
COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

Unit IV- Security Elements
Topic :IDS (Intrusion Detection System)

Intrusion detection system(IDS)

- 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**
- Intrusion Detection Systems are also as important as **the firewall because** they help us to **detect the type of attack** that is being done to our system and then to make a **solution to block them**.
- The monitoring **part like tracing logs, looking for doubtful signatures** and **keeping history of the events triggered.**
- They help also the **network administrators to check the connection integrity and authenticity** that occur.


FW
Route
Intenet
LAN
IDS

How does an IDS work?

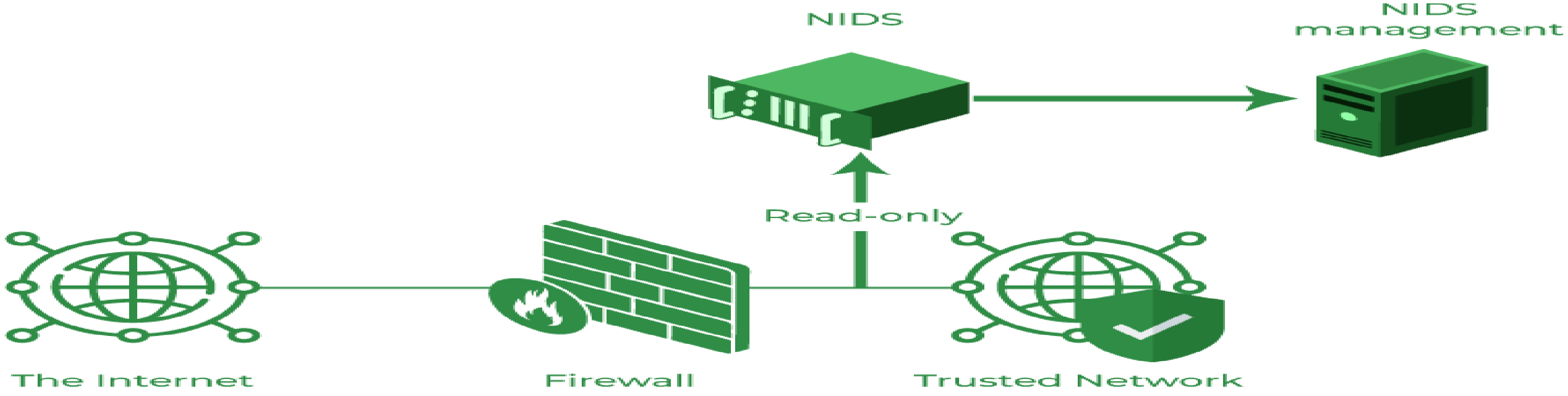
- An IDS (Intrusion Detection System) **monitors the traffic** on a computer network to **detect any malicious activity**.
- It **analyzes the data flowing** through the network to look for patterns and signs of abnormal behavior.
- The IDS **compares the network activity** to a set of predefined rules 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

IDS are classified into 5 types:

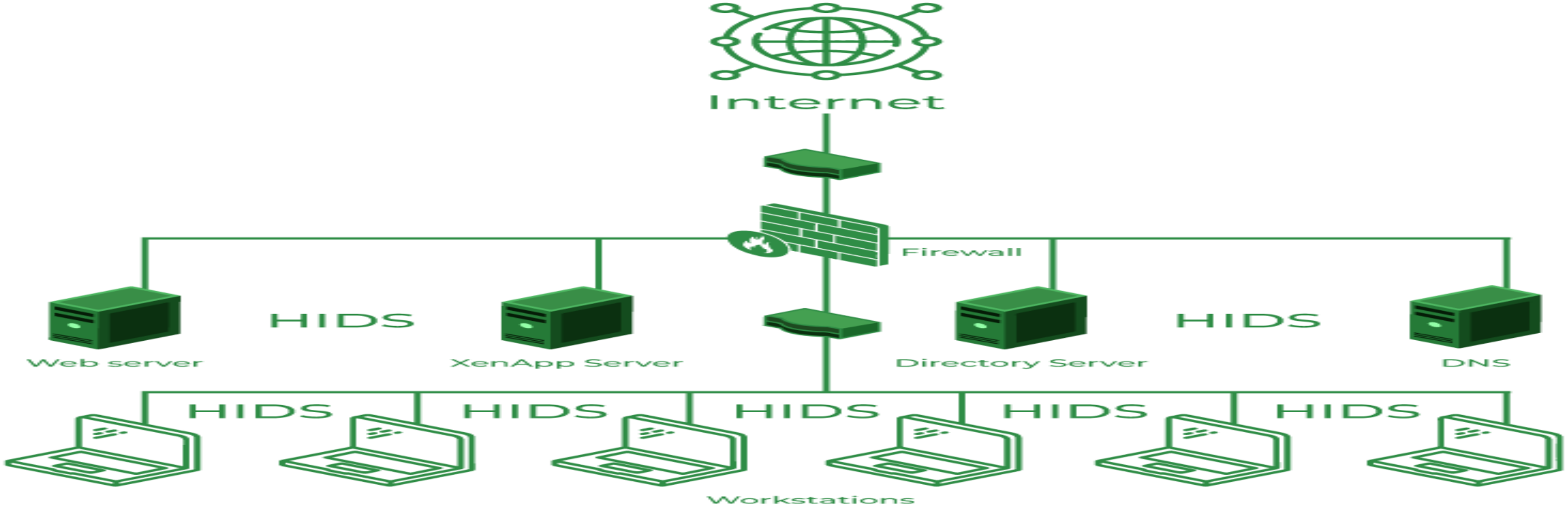
Network Intrusion Detection System (NIDS):

- Network intrusion detection systems (NIDS) are **set up at a planned point within the network** to **examine traffic** from all devices on the network.
- An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.



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.**
- An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.



Protocol-based Intrusion Detection System (PIDS): (server)

- 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**.
- As HTTPS is unencrypted and before instantly entering **its web presentation layer** then this system would need to reside in this interface, between to use the HTTPS.

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 (direct execution) 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 is **made by the combination of two or more approaches** to the intrusion detection system.

- In the hybrid intrusion detection system, **the host agent or system data is combined with network information** to **develop a complete view of the network system.**

- The hybrid intrusion detection system is **more effective in comparison to the other intrusion detection system**.

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.

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.

Comparison of IDS with Firewalls

Firewalls

- Firewalls **restrict access between networks to prevent intrusion** and if an **attack** is from **inside the network it doesn’t signal**.

IDS

- An **IDS describes a suspected intrusion** once it has happened and then signals an alarm.

Any Query????

Thank you……