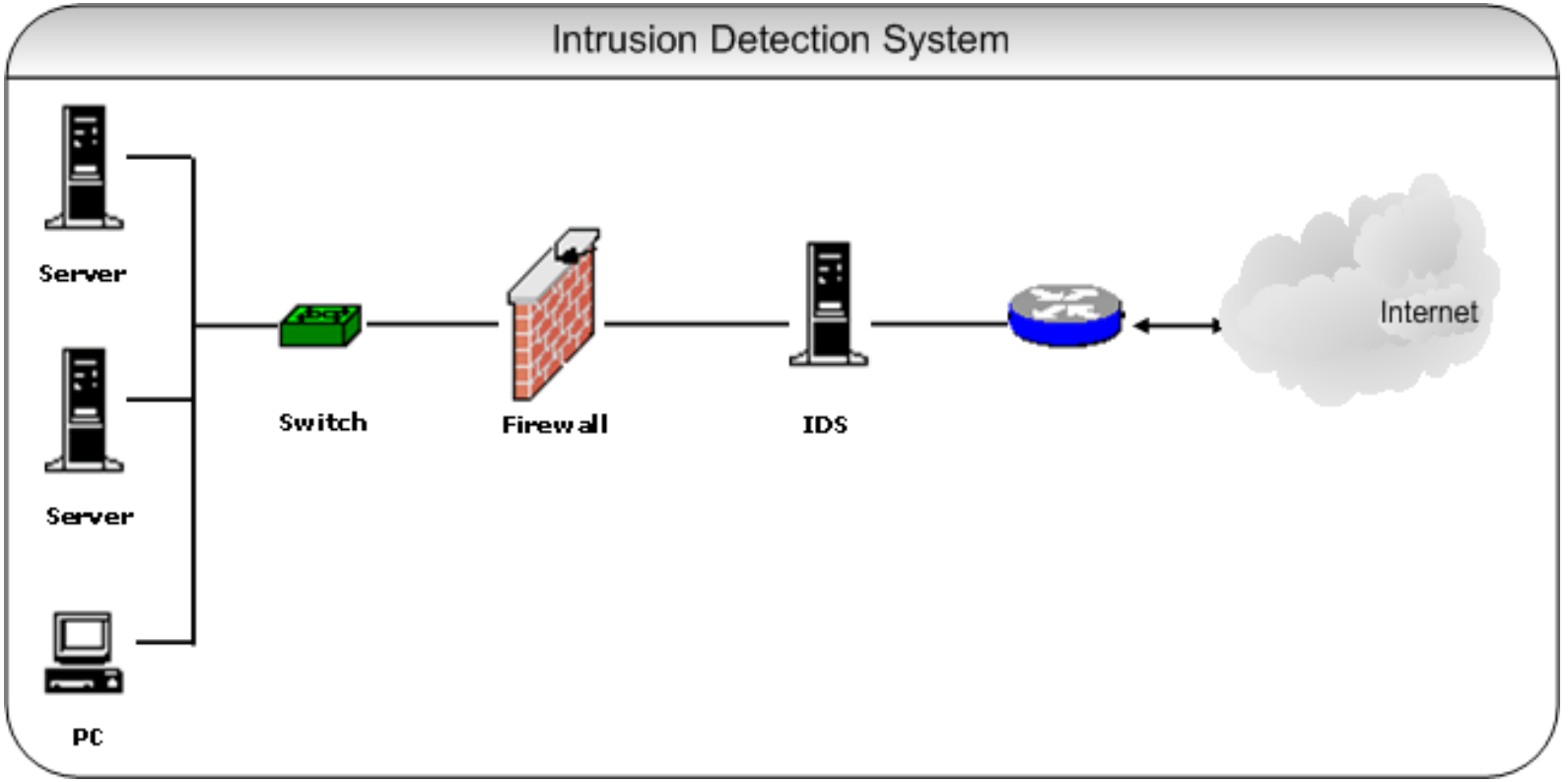
Module 5

Network Security and Applications

Intrusion Detection System(IDS)

- **Intrusion Detection** is the process of monitoring the events occurring in a computer system or network
- **Intrusion Detection System(IDS)** is a device that monitors activity to identify malicious or suspicious events
- **Intrusion Prevention** is the process of detecting the signs of intrusion and attempting to stop the intrusive effort
- **Intrusion Detection and Prevention System(IDPS)** does the job of both detecting and preventing from intrusions

Intrusion Detection System(IDS)



IDS Functions

- Monitoring users and system activity
- Auditing system configuration for vulnerabilities and misconfiguration
- Assessing the integrity of critical system and data files
- Recognizing known attack patterns in system activity
- Identifying abnormal activity through statistical analysis
- Managing audit trails and highlighting user violation of policy or normal activity
- Correcting system configuration errors
- Installing and operating traps to record information about intruders

IDS Techniques

- Signature Based
- Anomaly Based or Heuristic IDS
- Stateful protocol analysis

Signature Based

- It is the process of comparing the signature which signifies a known threat against the events that are observed
- It uses string matching as the underlying technique
- The current packet or log entry is matched to a list of signatures
- Example:- An email with a subject “Free xyz” or an attachment “picture.jpg”

Signature Based

- It uses statistical analysis.
- Statistical tools are used for sample measurements like amount of external activity, number of active processes, number of transactions
- Statistical tools are also used to determine whether the collected measurements fit the predetermined attack signatures or not
- Ideally signatures should match every instance of an attack and also match subtle variations of the attack

Signature Based -Disadvantages

- They are ineffective against unknown threats. Example- Modifying the subject name to “Free xyzw” will change the signature and go undetected
- They cannot pair a request with the corresponding response like knowing that a request to a web server for a particular page generated a response status code of 403
- They cannot detect attacks that compromise multiple events if none of the events alone contains an indication of an attack

Anomaly Based

- It is the process of comparing definitions of activities which are supposed to be normal against observed events to identify derivations
- In the anomaly based IDS technique, profiles are created that represent the normal behaviours of users, hosts, network connections or applications.
- An initial profile is created over period of time which is known as training period
- Profile can be of the following type:
  - Static:- Not changed over a long period of time
  - Dynamic:- Constantly gets updated with additional events

Stateful Protocol Analysis

- It is the process of comparing predefined profiles of generally accepted definitions of benign(harmless) protocol activity for each protocol state against observed events to identify deviations
- “Stateful” means the Intrusion Detection System is capable of checking networks, applications and application protocols which has the concept of “state” in them
- Example: FTP consists of two states: authenticated and unauthenticated. Benign operations in unauthenticated states are providing user name, passwords

Stateful Protocol Analysis

- It can identify unexpected sequence of commands
- Suspicious sequences could be either issuing the same command repeatedly or issuing a command without first issuing the dependent command

False positive and false Negatives

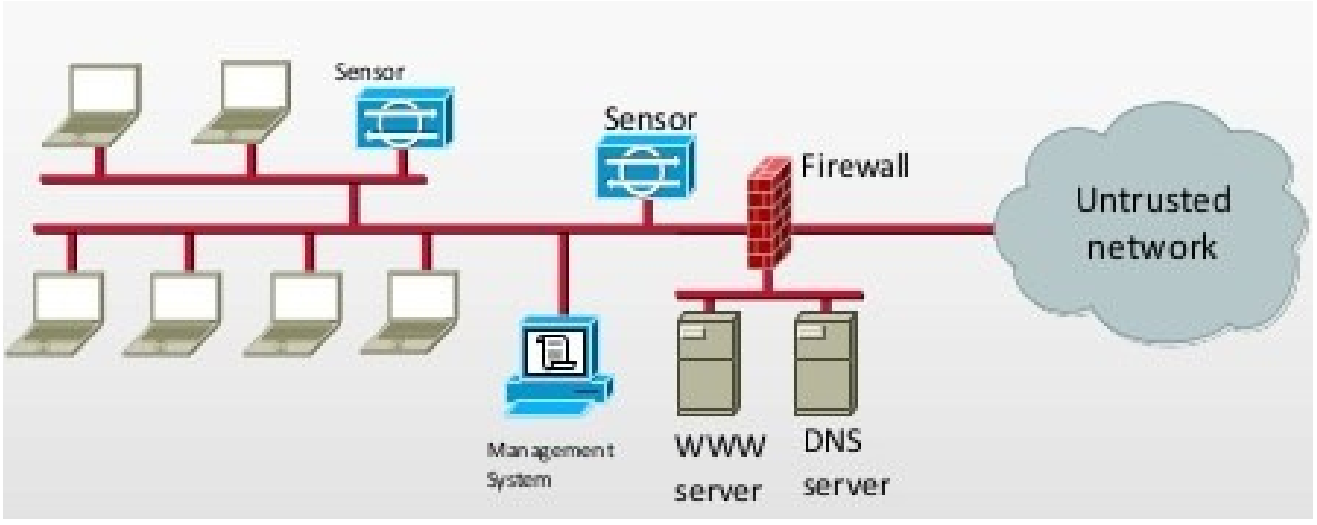
- False Positive: when IDS incorrectly identifies a benign (harmless) activity as malicious
- False Negative: When IDS fails to identify a malicious activity

Types of IDS technologies

- Network based
- Host Based
- Wireless
- Network Behaviour analysis

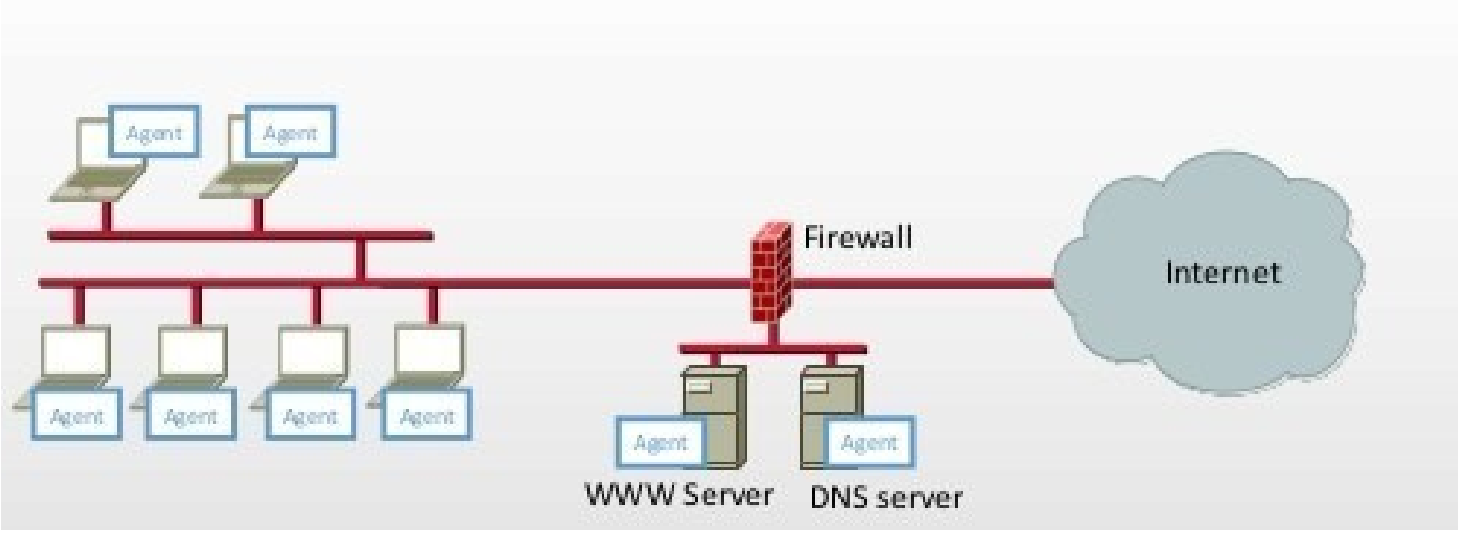
Network Based IDS

- It monitors the network traffic for a segment of network.
- It also analyses the network and application protocol activity to identify suspicious activities



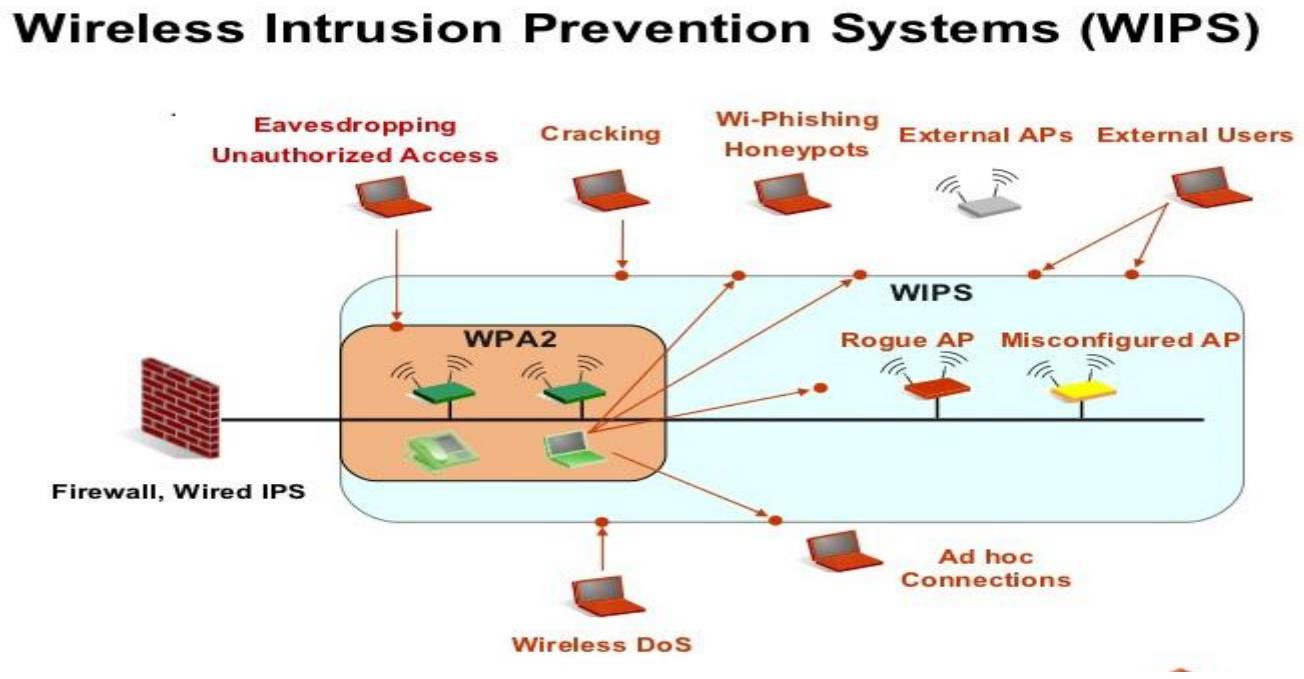
Host Based IDS

- It monitors the host and the events that occur within the host



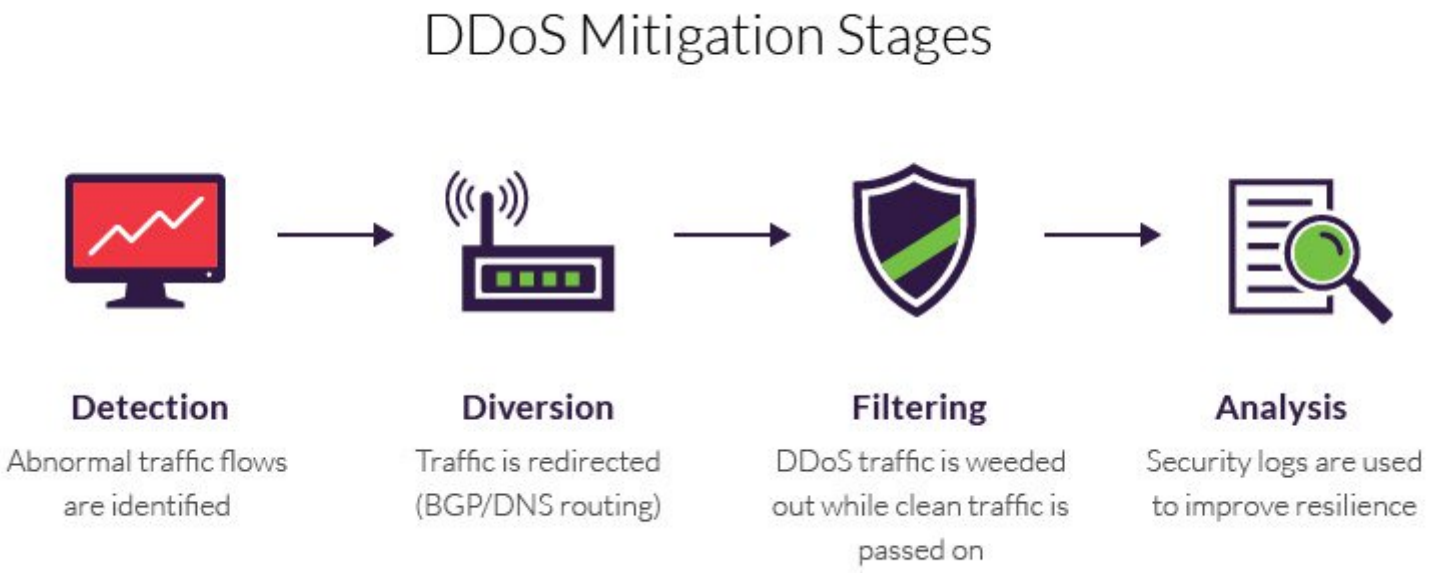
Wireless IDS

- It monitors the wireless network traffic.
- It identifies suspicious activities involving wireless protocols

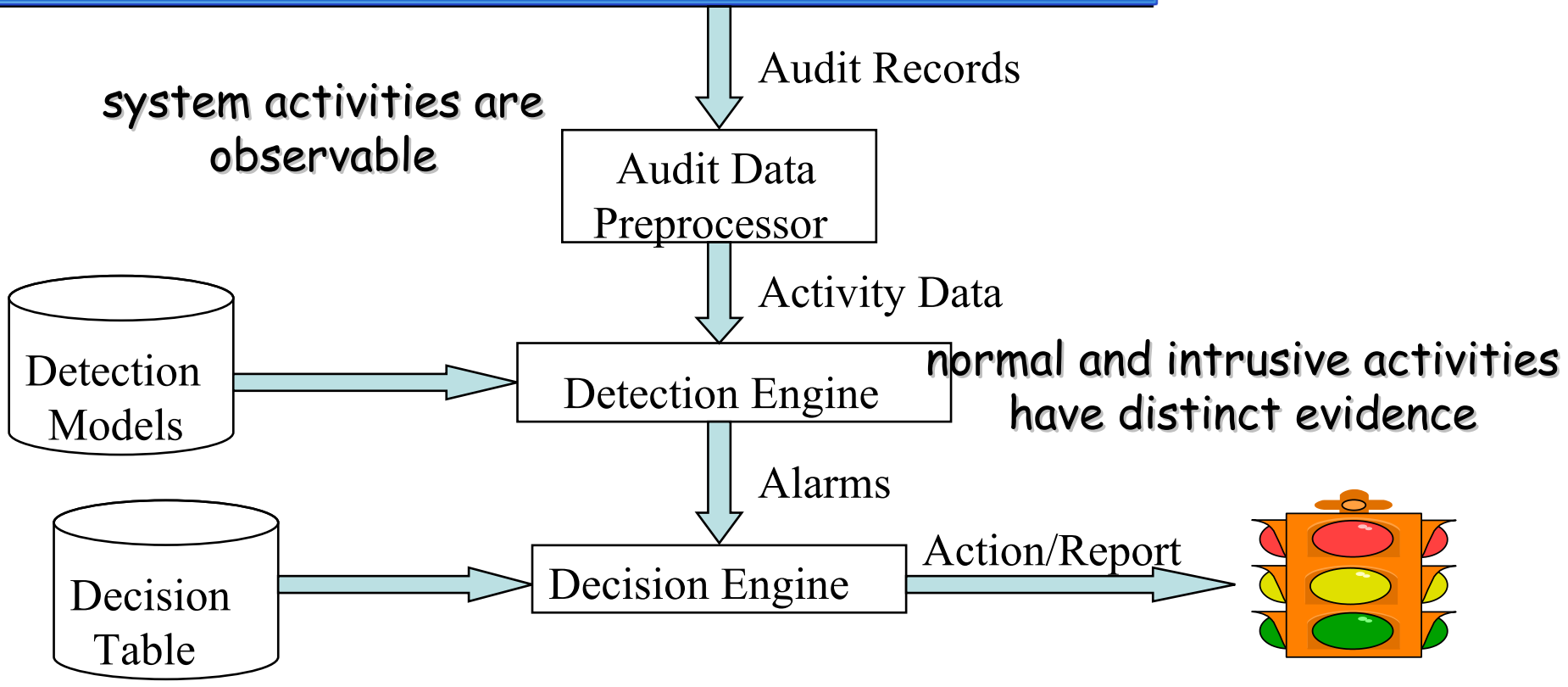


Network Behaviour Analysis

- The network traffic is analyzed to identify threats that create unusual traffic flows, DoS attacks, malwares and policy violations.



Components of Intrusion Detection System



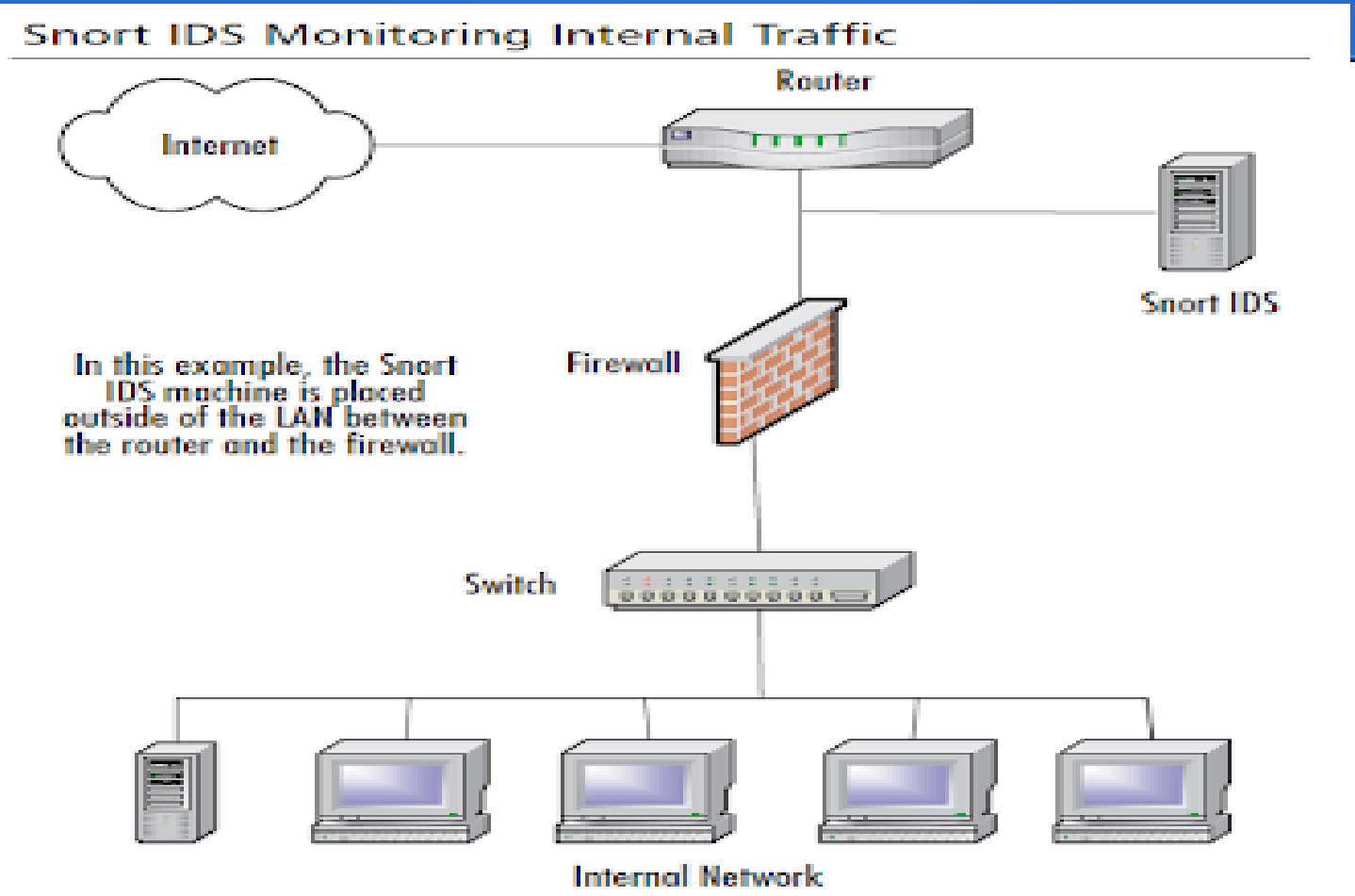
SNORT-IDPS

- It is a light weight open source network intrusion prevention and network intrusion detection system
- It is signature based
- It captures and analyses packets coming across a network connection for content that matches known attacks
- Snort uses flexible rules language that describe traffic that it should collect or pass
- It has real time alerting capability and generates log

SNORT

- When an attack takes place, the alert gives us the following information:
  - Date and time of attack
  - Source and destination IP address with port numbers
  - Type of attack
  - Priority (low, medium, high)

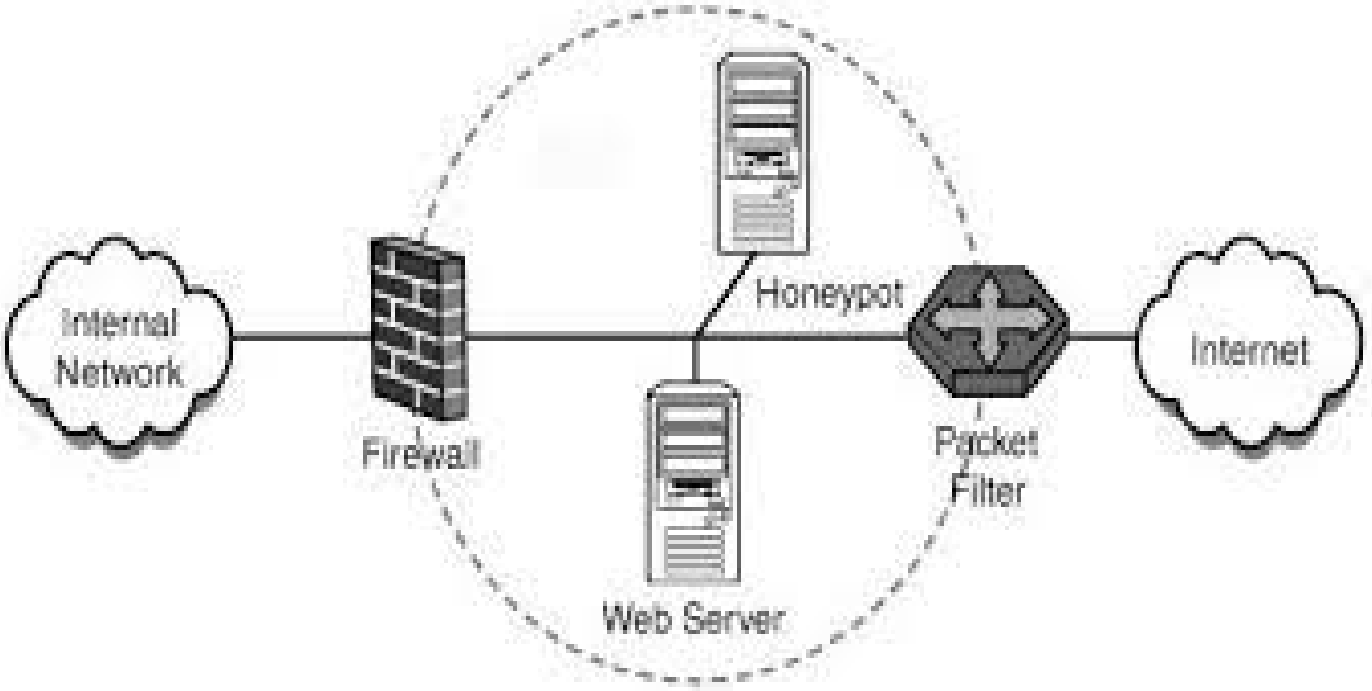
SNORT


Snort IDS Monitoring Internal Traffic
Router
Internet
Snort IDS
In this example, the Snort IDS machine is placed outside of the LAN between the router and the firewall.
Firewall
Switch
Internal Network

Honeypots

- Honeypots are closely monitored network decoys for the sole purpose of being exploited.
- They can distract the attackers from valuable machines on a network
- They can provide a warning about new attack and exploitation trends
- They allow in-depth examination of the attacker’s activity through its extensive logging capability
- Deployment of honeypots in a network should not affect critical network services and applications

Honeypots


Internal Network
Firewall
Honeypot
Web Server
Packet Filter
Internet

Honeypots-Types

- **Low interaction or Production Honeypots:**
  - Easy to use and install
  - Captures only limited amount of information.
  - Used by corporate firms
- **High interaction or Research Honeypots:**
  - Complex to deploy and maintain.
  - Captures extensive information.
  - Used by research, military or government organizations

Layer wise vulnerabilities and defense

Layer	Attacks	Defense
Application Layer	SQL injection	Network based IDS
Transport Layer	Port scanning	Network based IDS
Network Layer	SYN flooding	Firewall
Data Link Layer	MAC spoofing	Intelligent WLAN system