University of Mumbai

M.Sc in Information Technology

Revised Syllabus 2019-2010

PSIT302 & PSIT3P2 – Information Security Management (ISM)

Dr. (Mrs.) R. Srivaramangai

Head, Department of Information Technology

rsrimangai@udit.mu.ac.in

Unit II – Security Management of IT Systems

- Network Security Management
- Firewalls, IDS and IPS Configuration Management
- Web and Wireless Security Management
- General Server Configuration guidelines and maintenance
- ISM Classification
- Access control Models
- Linux and Windows Case Study
- Technical Controls
- Password Management and Key Management for USers

IDS

- Intrusion detection is the process of monitoring the events occurring in a computer system or network.
- It analyzes for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.
- Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents.
- Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.
- In addition, organizations use IDPSs for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies.
- IDPSs have become a necessary addition to the security infrastructure of nearly every organization.

Definitions

- ***Intrusions:*** attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer system or network(illegal access).

- Intrusions have many causes, such as malware (worms, spyware, etc…), attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized.
- Although many intrusions are malicious in nature, many others are not; for example: a person might mistype the address of a computer and accidentally attempt to connect to a different system without authorization.

Definitions

- ***Intrusion detection:*** is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible *intrusions (incidents)*.
- ***Intrusion detection system (IDS):*** is software that automates the intrusion detection process. The primary responsibility of an IDS is to detect unwanted and malicious activities.
- ***Intrusion prevention system (IPS):*** is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

Why Intrusion Detection Prevention Systems should be used?

- It's a dire fact that while every enterprise has a firewall, most still suffer from network security problems.

- IT professionals are acutely aware of the need for additional protective technologies, and network equipment vendors are anxious to fill in the gap.
- Intrusion Prevention Systems have been promoted as cost-effective ways to block malicious traffic, to detect and contain worm and virus threats, to serve as a network monitoring point, to assist in compliance requirements, and to act as a network sanitizing agent.

Why Intrusion Detection Prevention Systems should be used?

IDPSs are primarily focused on:

- Identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.
- Identifying problems with security policies
- Documenting existing threats
- Deterring individuals from violating security policies.

- IDPSs perform the following:
  - **Recording information related to observed events.** Information is usually recorded locally, and might also be sent to separate systems such as centralized logging servers, security information and event management (SIEM) solutions, and enterprise management systems.
  - **Notifying security administrators of important observed events.** This notification, known as an *alert*, may take the form of audible signals, e-mails, pager notifications, or log entries. A notification message typically includes only basic information regarding an event; administrators need to access the IDPS for additional information.
  - **Producing reports.** Reports summarize the monitored events or provide details on particular events of interest.

- An IDPS might also alter the settings for when certain alerts are triggered or what priority should be assigned to subsequent alerts after a particular threat is detected.
- IPSs respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques:
- **The IPS stops the attack itself.** Examples:

  Terminate the network connection or user session that is being used for the attack. Block access to the target (or possibly other likely targets) from the offending user account, IP address, or other attacker attribute. Block all access to the targeted host, service, application, or other resource.

- **The IPS changes the security environment.** The IPS could change the configuration of other security controls to disrupt an attack. Such as reconfiguring a network device (e.g., firewall, router, switch) to block access from the attacker or to the target, and altering a host-based firewall on a target to block incoming attacks. Some IPSs can even cause patches to be applied to a host if the IPS detects that the host has vulnerabilities.
- **The IPS changes the attack's content.** Some IPS technologies can remove or replace malicious portions of an attack to make it benign. An example is an IPS removing an infected file attachment from an e-mail and then permitting the cleaned email to reach its recipient.

- **Most IDPSs also offer features that compensate for the use of common evasion techniques.** *Evasion* is modifying the format or timing of malicious activity so that its appearance changes but its effect is the same. Attackers use evasion techniques to try to prevent IDPSs from detecting their attacks.
- **For example:** an attacker could encode text characters in a particular way, knowing that the target understands the encoding and hoping that any monitoring IDPSs do not. Most IDPSs can overcome common evasion techniques by duplicating special processing performed by the targets. If the IDPS can "see" the activity in the same way that the target would, then evasion techniques will generally be unsuccessful at hiding attacks.

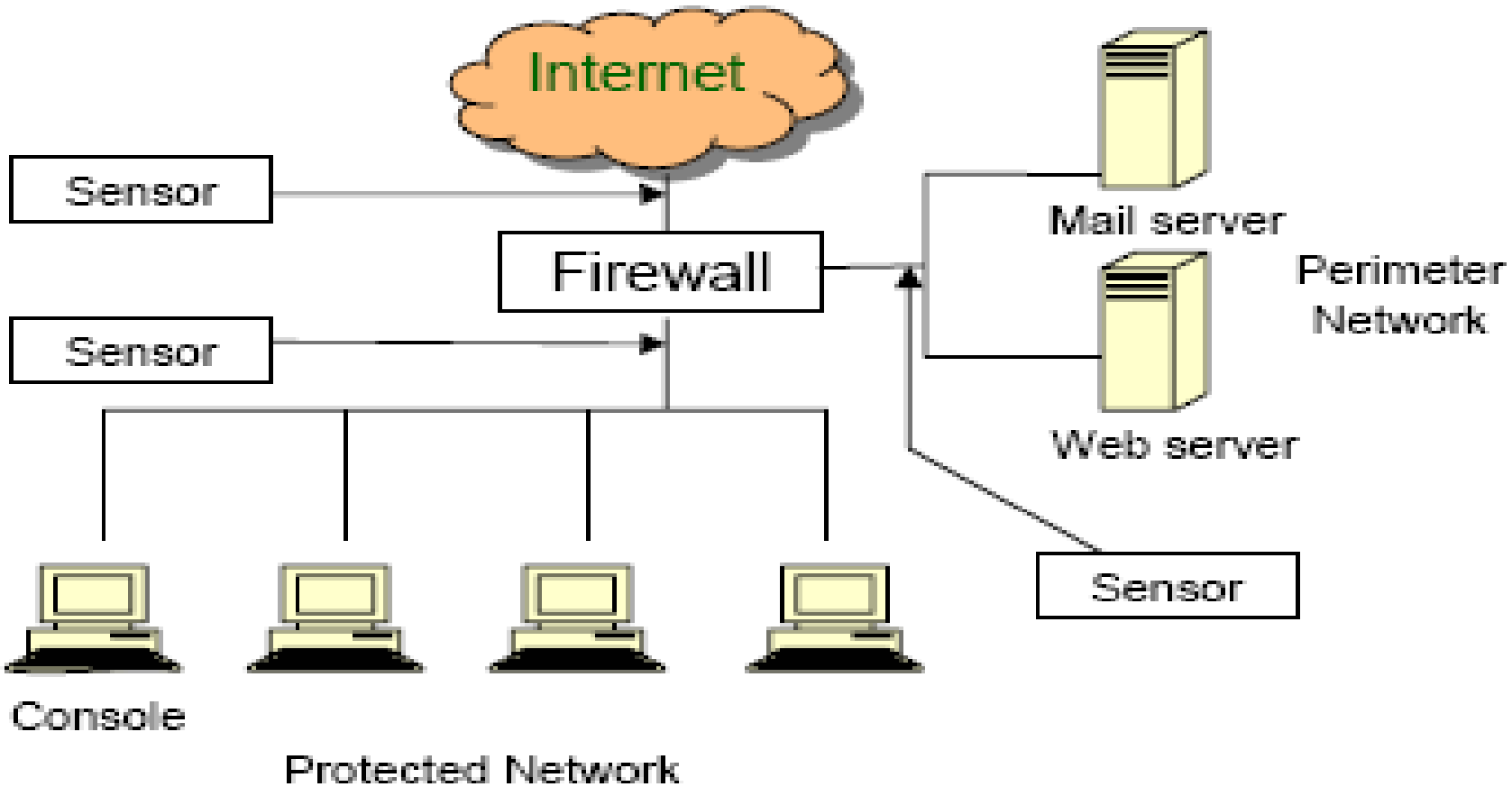
Types of IDPS Technologies

- Network-Based, which monitors network traffic for particular network segments or devices and analyzes the network and application protocolactivity to identify suspicious activity
- Wireless, which monitors wireless network traffic and analyzes it to identify suspicious activity involving the wireless networking protocols themselves
- Network Behavior Analysis (NBA), which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations (e.g., a client systemproviding network services to other systems)
- Host-Based,which monitors the characteristics of a single host and the events occurring within that host for suspicious activity.

Placement of Network IDPSs

- **Deployment options:**
- Outside firewall
- Just inside firewall

  -Combination of both will detect attacks getting through firewall and may help to refine firewall rule set.
- Behind remote access server
- Between business units
- Between corporate network and partner networks
- Sensors may need to be placed in all switched network segments

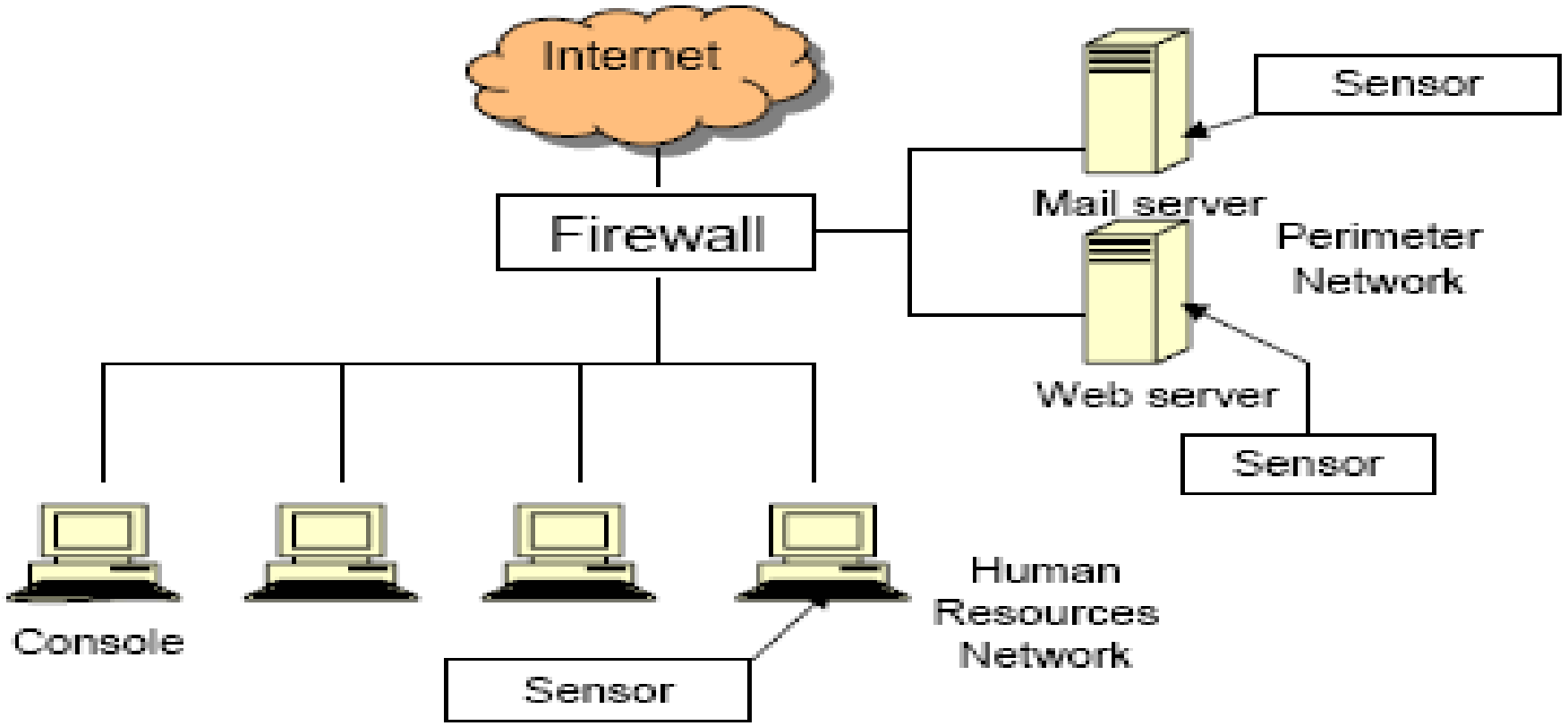

Internet
Sensor
Firewall
Sensor
Mail server
Perimeter
Network
Web server
Sensor
Console
Protected Network

Placement of host IDPSs

Deployment options:

- Key servers that contain mission-critical and sensitive information.
- Web servers.
- FTP and DNS servers.
- E-commerce database servers, etc.
- Other high value assets.

May also emplace these randomly to obtain probabilistic measure of hosts becoming compromised.


Internet
Firewall
Sensor
Mail server
Perimeter
Network
Web server
Sensor
Console
Human
Resources
Network
Sensor

Evaluation of IDPS Products

- Security capabilities, including information gathering, logging, detection, and prevention
- Performance, including maximum capacity and performance features
- Management, including design and implementation (e.g., reliability, interoperability, scalability, product security), operation and maintenance (including software updates), and training, documentation, and technical support
- Life cycle costs, both initial and maintenance costs.

Other Uses of IDPS

- Identifying security policy problems. An IDPS can provide some degree of quality control for security policy implementation, such as duplicating firewall rule sets and alerting when it sees network traffic that should have been blocked by the firewall but was not because of a firewall configuration error.
- Documenting the existing threat to an organization. IDPSs log information about the threats that they detect.
- Understanding the frequency and characteristics of attacks against an organization's computing resources is helpful in identifying the appropriate security measures for protecting the resources. The information can also be used to educate management about the threats that the organization faces.
- Deterring individuals from violating security policies. If individuals are aware that their actions are being monitored by IDPS technologies for security policy violations, they may be less likely to commit such violations because of the risk of detection.

Key Functions of IDPS Technologies

- Recording information related to observed events. Information is usually recorded locally, and might also be sent to separate systems such as centralized logging servers, security information and event management (SIEM) solutions, and enterprise management systems.
- Notifying security administrators of important observed events. This notification, known as an alert, occurs through any of several methods, including the following:
  - e-mails, pages, messages on the IDPS user interface, Simple Network Management Protocol (SNMP) traps, syslog messages, and user-defined programs and scripts.
- A notification message typically includes only basic information regarding an event; administrators need to access the IDPS for additional information. Producing reports.
- Reports summarize the monitored events or provide details on particular events of interest.

IDS vs IPS

- The IPS stops the attack itself
  - Terminate the network connection or user session that is being used for the attack
  - Block access to the target (or possibly other likely targets) from the offending user account, IP address, or other attacker attribute
  - Block all access to the targeted host, service, application, or other resource.
- The IPS changes the security environment.
  - The IPS could change the configuration of other security controls to disrupt an attack.
  - Common examples are reconfiguring a network device (e.g., firewall, router, switch) to block access from the attacker or to the target, and altering a host-based firewall on a target to block incoming attacks.
  - Some IPSs can even cause patches to be applied to a host if the IPS detects that the host has vulnerabilities.
- The IPS changes the attack's content.
  - Some IPS technologies can remove or replace malicious portions of an attack to make it benign.
  - A simple example is an IPS removing an infected file attachment from an e-mail and then permitting the cleaned email to reach its recipient.
  - A more complex example is an IPS that acts as a proxy and normalizes incoming requests, which means that the proxy repackages the payloads of the requests, discarding header information.

Common Detection Methodologies
Signature-Based Detection

- A signature is a pattern that corresponds to a known threat.
- Signature-based detection is the process of comparing signatures against observed events to identify possible incidents.

➢A telnet attempt with a username of "root", which is a violation of an organization's security policy

➢An e-mail with a subject of "Free pictures!" and an attachment filename of "freepics.exe", which are characteristics of a known form of malware

➢An operating system log entry with a status code value of 645, which indicates that the host's auditing has been disabled.

Common Detection Methodologies
Anomaly-Based Detection

- Anomaly-based detection is the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations.
- An IDPS using anomaly-based detection has profiles that present the normal behavior of such things as users, hosts, network connections, or applications.
- The major benefit of anomaly-based detection methods is that they can be very effective at detecting previously unknown threats.
- An initial profile is generated over a period of time (typically days, sometimes weeks) sometimes called a training period. Profiles for anomaly-based detection can either be static or dynamic.

A profile for a network might show that Web activity comprises an average of 13% of network bandwidth at the Internet border during typical workday hours. The IDPS then uses statistical methods to compare the characteristics of current activity to thresholds related to the profile, such as detecting when Web activity comprises significantly more bandwidth than expected and alerting an administrator of the anomaly..

Common Detection Methodologies
Stateful Protocol based Analysis

- Stateful protocol analysis is the process of comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations.
- relies on vendor-developed universal profiles that specify how particular protocols should and should not be used.
- is capable of understanding and tracking the state of network, transport, and application protocols that have a notion of state.
- use protocol models, which are typically based primarily on protocol
- standards from software vendors and standards bodies(e.g., Internet Engineering Task Force [IETF] , Request for Comments [RFC]

The existence of a large binary file in the User-Agent field of an HTTP request would be very unusual and likely an intrusion. A protocol analyzer could detect this anomalous behavior and instruct the IPS engine to drop the offending packets

Typical Components

- Sensor or Agent.
  - Sensors and agents monitor and analyze activity.
  - The term sensor is typically used for IDPSs that monitor networks, including network-based, wireless, and network behavior analysis technologies. The term agent is typically used for host-based IDPS technologies.
- Management Server.
  - Is a centralized device that receives information from the sensors or agents and manages them.
  - Matching event information from multiple sensors or agents, such as finding events triggered by the same IP address, is known as correlation.
  - In larger IDPS deployments, there are often multiple management servers, and in some cases there are two tiers of management servers.
- Database Server.
  - Is a repository for event information recorded by sensors, agents, and/or management servers. Many IDPSs provide support for database servers.
- Console.
  - Is a program that provides an interface for the IDPS's users and administrators. Console software is typically installed onto standard desktop or laptop computers.
  - Some consoles are used for IDPS administration only, such as configuring sensors or agents and applying software updates, while other consoles are used strictly for monitoring and analysis.
  - Some IDPS consoles provide both administration and monitoring capabilities.

Security Capabilities

- Information Gathering Capabilities
  - Identifying Hosts
  - Identifying Operating Systems
  - Identifying Applications
  - Identifying Network Characteristics
- Logging Capabilities
- Detection Capabilities
- Prevention Capabilities

Logging Capabilities

- Timestamp (usually date and time)
- Connection or session ID (typically a consecutive or unique number assigned to each TCP connection or to like groups of packets for connectionless protocols)
- Event or alert type
- Rating (e.g., priority, severity, impact, confidence)
- Network, transport, and application layer protocols
- Source and destination IP addresses
- Source and destination TCP or UDP ports, or ICMP types and codes
- Number of bytes transmitted over the connection
- Decoded payload data, such as application requests and responses
- State-related information (e.g., authenticated username)
- Prevention action performed

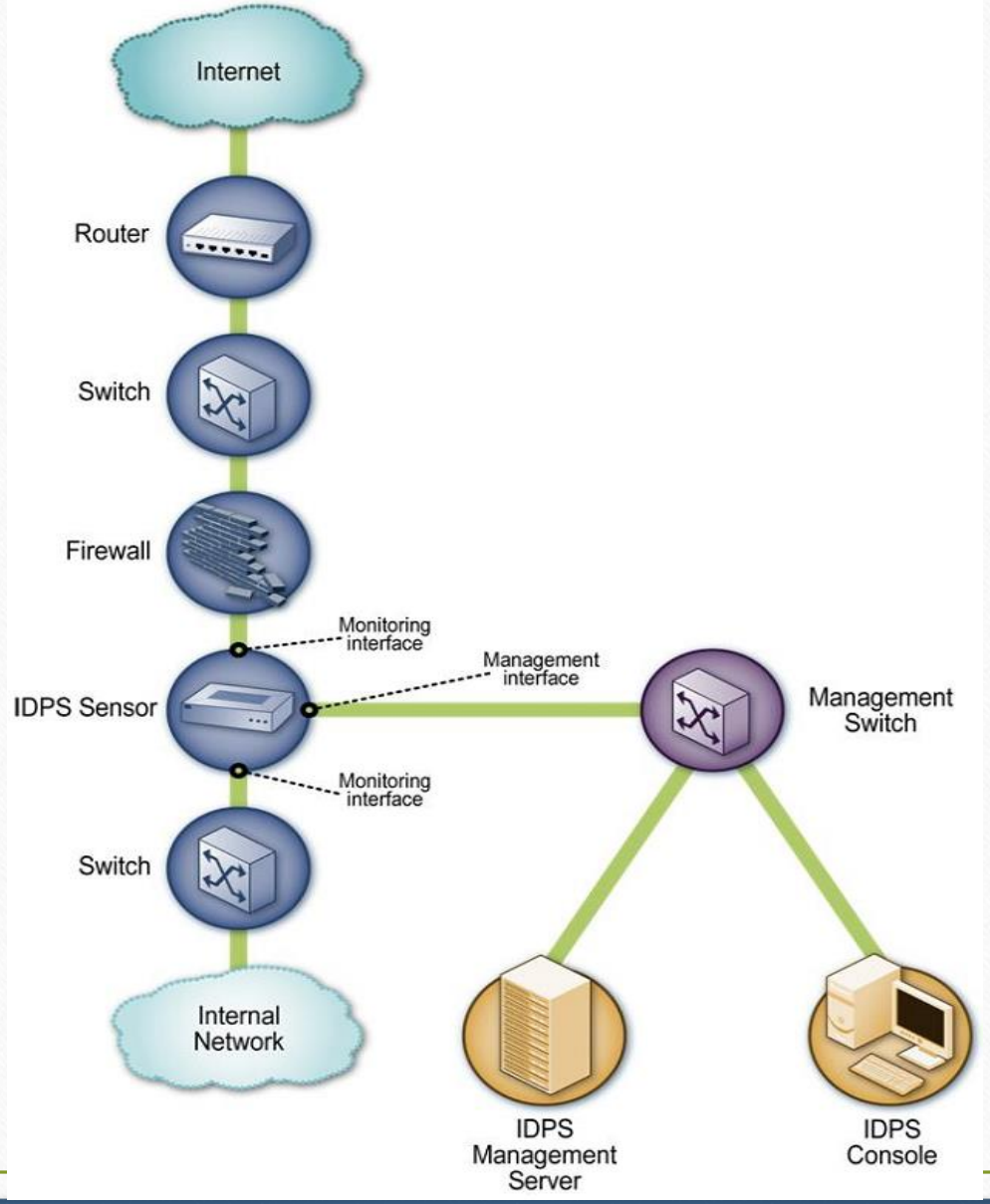
Detection Capabilities

- Types of events detected
  - Application layer reconnaissance and attacks
  - Transport layer reconnaissance and attacks
  - Network layer reconnaissance and attacks
  - Unexpected application services
  - Policy violations
- Detection accuracy
- Tuning and customization
- Technology limitations.

Implementation – Architectural Design

- Where the sensors or agents should be placed
- ~~How reliable the solution should be and what measures should be used to achieve that reliability~~, such as having multiple sensors monitor the same activity in case a sensor fails, or using multiple management servers so that a backup server can be used in case the primary server fails
- Where the other components of the IDPS will be located (e.g., management servers, database servers, consoles), and how many of each component are needed to achieve the necessary usability, redundancy, and load balancing goals
- With which other systems the IDPS needs to interface, including the following:
  - Systems to which it provides data, such as security information and event management software, centralized log servers, e-mail servers, and paging systems
  - Systems on which it initiates prevention responses (e.g., firewalls, routers, switches)
  - Systems that manage IDPS components, suchas network management software (for a management network) or patch management software (for keeping consoles' operating systems and applications fully up-to-date)

Inline Network-Based IDPS Sensor Architecture



Passive Network-Based IDPS Sensor Architecture