Subject: Information and Communication Technology (ICT)
Topic: Intrusion Prevention systems(IPS)
Lesson: Two
Teacher: Chinyere **.**E. Ikpah
Class: Senior Secondary Class 2
Duration: 80 Minutes

Objectives:

At the end of this lesson, students should be able to:

- define intrusion prevention system
- explain two main types of intrusion prevention system,
- explain IPS classifications,
- describe prevention methods of IPS,
- explain IDPS terminologies,

What is an intrusion prevention system?

An intrusion prevention system (IPS) is a network security tool (which can be a hardware device or software) that continuously monitors a network for malicious activity and takes action to prevent it, including reporting, blocking, or dropping it, when it does occur.

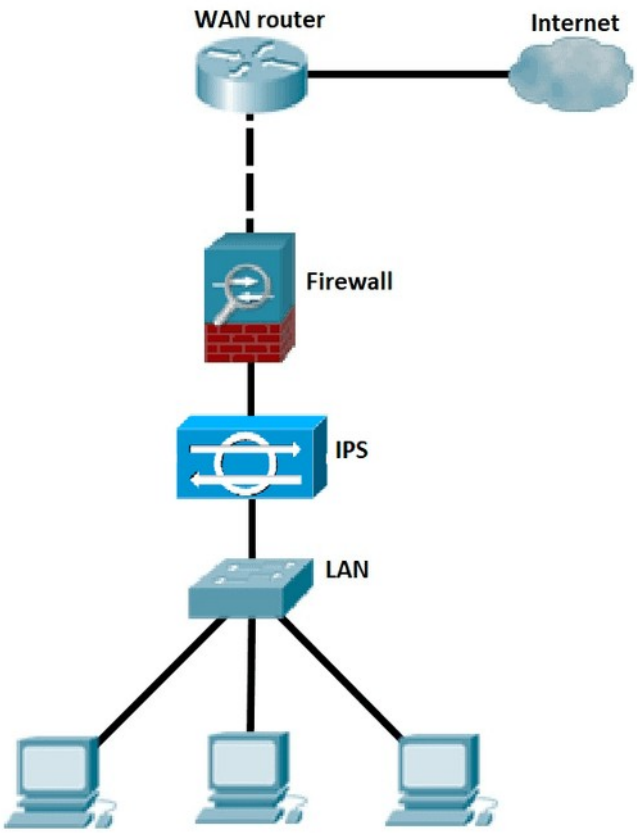

Fig 4: Overview of Intrusion Prevention System

IPS monitors network traffic for potential threat and automatically takes action to block them by alerting the security team, terminating dangerous connections, removing malicious content, or triggering other security devices.

IPS solutions evolved from Intrusion Detection Systems (IDSs), which detects and report threat to the security system. IPS has the same threat detection and reporting functions as an IDS plus automated threat prevention abilities, which is why IPSs are sometimes called “Intrusion Detection and Prevention Systems” (IDPSs).

It is more advanced than an intrusion detection system (IDS), which simply detects malicious activity but cannot take action against it beyond alerting an administrator. Intrusion prevention systems are sometimes included as part of a next-generation firewall (NGFW) or unified threat management (UTM) solution. Like many network security technologies, they must be powerful enough to scan a high volume of traffic without slowing down network performance.

Types of IPS

There are two main types of IPS:

1. **Network-Based IPS:** A Network-Based IPS is installed at the network perimeter and monitors all traffic that enters and exits the network.
2. **Host-Based IPS:** A Host-Based IPS is installed on individual hosts and monitors the traffic that goes in and out of that host.

Classification of Intrusion Prevention System (IPS):

Intrusion Prevention System (IPS) is classified into 4 types:

Network-based intrusion prevention systems (NIPS)

A network-based intrusion prevention system (NIPS) monitors inbound and outbound traffic to devices across the network, inspecting individual packets for suspicious activity. NIPS are placed at strategic points in the network. They often sit immediately behind firewalls at the network perimeter so they can stop malicious traffic that breaks through. NIPS may also be placed inside the network to monitor traffic to and from key assets, like critical data centers or devices.

Host-based intrusion prevention systems (HIPS)

A host-based intrusion prevention system (HIPS) is installed on a specific endpoint, like a laptop or server, and monitors only traffic to and from that device. HIPS are usually used in conjunction with NIPS to add extra security to vital assets. HIPS can also block malicious activity from a compromised network node, like ransom ware spreading from an infected device.

Network behavior analysis (NBA)

Network behavior analysis (NBA) solutions monitor network traffic flows. While NBAs may inspect packets like other IPSs, many NBAs focus on higher-level details of communication sessions, such as source and destination IP addresses, ports used, and the number of packets transmitted.

NBAs use anomaly-based detection methods, flagging and blocking any flows that deviate from the norm, like DDoS attack traffic or a malware-infected device communicating with an unknown command and control server.

Wireless intrusion prevention systems (WIPS)

A wireless intrusion prevention system (WIPS) monitors wireless network protocols for suspicious activity, like unauthorized users and devices accessing the company's wifi. If a WIPS detects an unknown entity on a wireless network, it can terminate the connection. A WIPS can also help detect misconfigured or unsecured devices on a wifi network and intercept man-in-the-middle attacks, where a hacker secretly spies on users' communications.

Prevention Methods OF IPS

Blocking malicious traffic

An IPS may end a user's session, block a specific IP address, or even block all traffic to a target. Some IPSs can redirect traffic to a honeypot, a decoy asset that makes the hackers think they've succeeded when, really, the SOC is watching them.

Removing malicious content

An IPS may allow traffic to continue but scrub the dangerous parts, such as by dropping malicious packets from a stream or removing a malicious attachment from an email.

Triggering other security devices

An IPS may prompt other security devices to act, such as by updating firewall rules to block a threat or changing router settings to prevent hackers from reaching their targets.

Enforcing security policies

Some IPSs can prevent attackers and unauthorized users from doing anything that violates company security policies. For example, if a user tries to transfer sensitive information out of a database it's not supposed to leave, the IPS would block them.

Intrusion Detection and Prevention Systems Terminologies

1. True Positive ⟶ Malicious, Alarm

2. True Negative ⟶ No Malicious, No Alarm

3. False Positive ⟶ No Malicious, Alarm

4. False Negative ⟶ Malicious, No Alarm

Actions 1 and 2 are good actions while actions 3 and 4 are bad actions. The worst action is action 4.

Summary:

In this lesson, we were able to:

- define intrusion prevention system
- explain two main types of intrusion prevention system,
- explain IPS classifications,
- describe prevention methods of IPS,
- explain IDPS terminologies,

Evaluations:

1. Which of these are two main types of IPS?

   A. Network-Based IPS and Hybrid-Based IPS
   B. Newton-Based IPS and Host-Based IPS
   C. Network-Based IPS and Host-Based IPS
   D. Newton -Based IPS and Hybrid -Based IPS

2. Which type of IPS is installed at the network perimeter and monitors all traffic that enters and exits the network?

   A. Network-Based IPS
   B. Host-Based IPS
   C. Newton -Based IPS
   D. Hybrid -Based IPS

3. Which type of IPS is installed on individual hosts and monitors the traffic that goes in and out of that host?

   A. Network-Based IPS
   B. Hybrid-Based IPS
   C. Newton -Based IPS
   D. Host -Based IPS

4. IPS is classified into how many?

   A. Three
   B. Four
   C. Five
   D. Six

5. When malicious packets/traffic pass through a network and an alarm was generated is known as

   A. FALSE POSITIVE

B. FALSE NEGETIVE

C. TRUE POSITIVE

D. TRUE NEGETIVE