LEMUEL OKECHUKWU

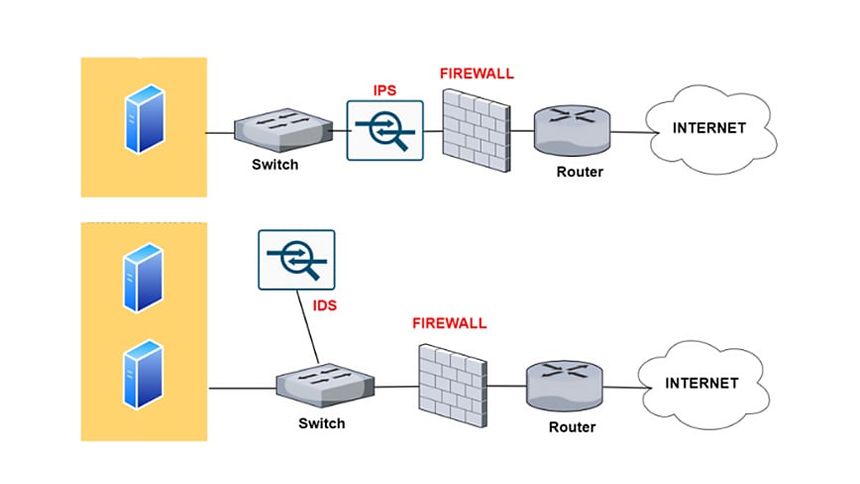
VEPH/20B/CY082

TASK 28B

**IDS and IPS : Intrusion Detection and Prevention Systems**

**TASK 28B :**

* **Provide detailed definitions and operational distinctions between Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), and elucidate the concepts of false positive, false negative, true positive, and true negative within the context of cybersecurity threat detection and response**

[](https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids)

The importance of robustly safeguarding network and host systems against unauthorized access or attacks cannot be overstated. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) stand as critical components in the security infrastructure, each playing a unique role in detecting and preventing cyber threats.

At their core, IDS and IPS serve to monitor network and system activities for malicious actions or policy violations. While both share the common goal of enhancing security, their approaches differ significantly.

* **Intrusion Detection Systems (IDS)** are designed to passively monitor and analyze traffic, identifying potential threats and alerting administrators. They do not take direct action to block or prevent the detected threat.
* **Intrusion Prevention Systems (IPS)**, on the other hand, actively monitor network traffic to detect and prevent identified threats in real-time by blocking or rerouting malicious traffic.

With the proliferation of wireless networks, WiFi Intrusion Prevention Systems (WIPS) have emerged as a crucial technology for protecting wireless networks from unauthorized access and attacks. WIPS monitor the wireless spectrum for rogue access points and malicious activities, employing automatic countermeasures to safeguard the network integrity.



**IDS and IPS Terminology**

it is important to understand the terminology that is used when talking about Intrusion Detection Systems and Intrusion Prevention Systems. They are as follows:

* Alert or Alarm
* True attack stimulus
* False attack stimulus
* False positive
* False negative
* Noise
* Site policy
* Site policy awareness
* Confidence value
* Alarm filtering

|  |  |
| --- | --- |
| Term | Description |
| Alert or Alarm | A signal suggesting a system has been or is being attacked |
| True attack stimulus | An event that triggers a system to produce an alarm and react as though a real attack were in progress |
| False attack stimulus | The event signaling the system to produce an alarm when no attack has taken place |
| False Positive | An alert or alarm that is triggered when no actual attack has taken place; i.e. an incorrect positive alert or alarm |
| False negative | A failure of the system to detect an actual attack |
| Noise | Data or interference that can trigger a false positive |
| Site policy | Guidelines within an organization that control the rules and configurations of the system |
| Site policy awareness | The ability the system has to dynamically change its rules and configurations in response to changing environmental activity |
| Confidence value | A value an organization places based on past performance and analysis to help determine its ability to effectively identify an attack |
| Alarm filtering | The process of categorizing attack alerts produced by the system in order to distinguish false positives from actual attacks |

The four methods used by IDS and IPS devices to detect attacks are:

1. Policy-based Detection
2. Anomaly-based Detection
3. Honey Pot Detection
4. Signature-based Detection

The intricate landscape of Intrusion Detection and Prevention Systems underscores the complexity and necessity of comprehensive cybersecurity measures. By understanding the distinctions and synergies between network-based and host-based systems, as well as the nuances of signature and anomaly-based detection, organizations can tailor their security infrastructure to effectively combat the ever-evolving spectrum of cyber threats. As the digital frontier expands, the strategic deployment of IDS and IPS remains a cornerstone in the quest for a secure, resilient cyber environment.