CyberSecurity Research Report

Intrusion Prevention Systems/Intrusion Detection Systems

Submitted By – Siya Arora

Student ID –

Submitted to –

Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) are two very crucial components of network security. They provide network administrators with the ability to detect and prevent potential security breaches that could otherwise compromise the integrity and confidentiality of the data. They’re are designed to monitor and analyze network traffic for malicious activity and unauthorized access.

Intrusion Detection Systems (IDS) emerged in the late 1990s to detect traffic patterns indicative of incoming attacks. In the 2000s, IDS morphed into Intrusion Prevention Systems (IPS) as it acquired additional security capabilities. Over the years, IDS/IPS has become a standard capability of the network security stack.

An Intrusion Prevention System (IPS) is a network security system that works to prevent malicious activity by detecting and blocking it in real-time. An IPS typically sits inline on the network, monitoring traffic as it flows through the network. When the system detects a potential threat, it takes action to block the threat before it can reach its target. Other features of IPS include Real-time traffic analysis, Automatic Blocking, Signature-based detection and Anomaly-based detection.

There is Four types of IPS –

* Network – It Analyzes protocol packets throughout the entire packet. It gathers information from the host about permissions, applications and Operating systems. It does not analyze encrypted network traffic and handle high traffic loads.
* Wireless – Operate at the Data-Link layer of the OSI model. It detects the presence of malicious devices and prevents them from using the enterprise network by scanning for Denial of Service attacks
* Network behaviour - Spot attacks that involve unusual and anomalous traffic on your network. Universal vendor-created profiles usually act as baseline of normal behavior.
* Host-based - Scan events that occur within a host you specify. Also prevents the host machine from processing malicious activity on the network and prevents access to sensitive information located on the host.

Intrusion Detection Systems (IDS), on the other hand, are network security systems that detect and alert security personnel about potential security incidents. IDS systems do not block malicious activity, but rather they notify security personnel about suspicious activity that needs to be investigated. Traffic analysis, event-correlation, Signature-based detection and Anomaly-based detection make IDS an effective security technology.

There is mainly Five different types of IDS –

* Network – strategically placed on a chosen point on your network and examine all traffic on all devices from that point; traffic flow is not altered or impeded
* Host - Examine traffic to and from independent devices within your network, and leave all other devices alone; mainly operates by scanning data in system files on the device
* Protocol-based - Place protection between a device and the server, and monitor all traffic that goes between them
* Application protocol-based - Place protection within a group of servers and watch how they communicate with one another
* Hybrid - Combine some of the approaches listed above into a system that best suits the company’s network and demands

While IPS and IDS seem to be performing the similar tasks, they do have some key differences. One of the major differences is that IDS is mainly useful in detecting threats as compared to an IPS being useful in detecting and taking preventative measures. IPS systems take immediate action to prevent threats and IDS systems simply alert security personnel. Another difference is that an IDS is typically deployed as a passive device, while an IPS is deployed as an active device that sits in the path of network traffic.

An IPS can do the job of an IDS, but vice-versa is not possible. IPS solutions are mostly autonomous and use machine learning-powered models to do the job. Contrastingly, IDS relies on human resource to implement measures after scanning networks for threats.

IDS/IPS serve multiple important functions. They detect any and all intrusion attempts by monitoring the network traffic and host systems. Such early detection prevents potential damage and loss. Once any suspicious activity is detected, it generates an alert and takes proactive measures. They are also helpful in identifying and resolving performance issues in the network.

Another important feature of IPS/IDS is that they analyse security breaches to identify patterns and trends in security breaches to help prevent future attacks. They also help organizations comply with regulatory requirements related to network security. They are combined to give best functionality since when the two technologies are combined into a single appliance, the administrator has the option to deploy as an inline IPS or detection only with sensors strategically placed to passively monitor traffic.

There are certain challenges associated with the implementation of IPS/IDS systems like false alerts, positive or negative, which can lead to either legitimate activity being classified as malicious or fails to detect a threat when it is designed to evade the system. These systems also have a performance impact on the network if it is not properly optimized becoming the cause of slower speeds and decreased productivity. Last, but not the least, these systems are also expensive to implement and maintain especially if an organization chooses to use multiple types of systems for comprehensive prevention.

The market for IDS/IPS is growing at a steady rate due to the adoption of advanced technologies post-covid. The top key-players in the market are Checkpoint, Cisco, HP, McAfee, IBM and Juniper Networks. Its major applications are in a variety of industries like aerospace, defence and intelligence, healthcare.

Most companies deploy both IDS and IPS to protect their networks and assets. They are the most crucial component of any organization’s security strategy as internet security threats are becoming more silent and dangerous. These systems merge signature and behaviour-based technologies that secure corporate network infrastructures as well as personal computers.

# References

N. (2021, May 5). *Intrusion Detection System (IDS): Signature vs. Anomaly-Based*. N-able. https://www.n-able.com/blog/intrusion-detection-system

Check Point Software. (2022, July 15). *What is an Intrusion Detection System (IDS)?* <https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/>

*IDS vs. IPS: Definitions, Comparisons & Why You Need Both | Okta*. (n.d.). Okta, Inc. https://www.okta.com/identity-101/ids-vs-ips/

Gillis, T. (n.d.). *You searched for ids/ips - Network and Security Virtualization - VMware*. Network and Security Virtualization. https://blogs.vmware.com/networkvirtualization/?s=ids%2Fips

Michael Swanagan, C. I. S. S. P. (2021, October 21). *Intrusion detection vs prevention systems: What's the difference?* PurpleSec. Retrieved February 20, 2023, from https://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems/

*TechLibrary*. Learn About Series - Technical Documentation - Support - Juniper Networks. (n.d.). Retrieved February 20, 2023, from https://www.juniper.net/documentation/en\_US/learn-about/

Ashtari, H. (2022, March 21). *IDS vs. IPS: Key Difference and Similarities - Spiceworks*. Spiceworks. https://www.spiceworks.com/it-security/network-security/articles/ids-vs-ips/