**ABSTRACT**

An Intrusion Detection System (IDS) is a Security system as like device or [software application](https://en.wikipedia.org/wiki/Software_application) or monitoring server or hardware instrument that monitors a [network](https://en.wikipedia.org/wiki/Computer_network) or systems for un-authorized or malicious activity or policy violations. Detected activity or Un-authorized Access is typically reported either to an administrator or collected centrally using a [security information and event management](https://en.wikipedia.org/wiki/Security_information_and_event_management) system.

An Intrusion Detection System (IDS) is a network security technology originally built for detecting vulnerability exploits against a target application or computer. [Intrusion Prevention Systems](https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips) (IPS) extended IDS solutions by adding the ability to block threats in addition to detecting them and has become the dominant deployment option for IDS/IPS technologies. This article will elaborate on the configuration and functions that define the IDS deployment.

An IDS needs only to detect threats and as such is placed out-of-band on the network infrastructure, meaning that it is not in the true real-time communication path between the sender and receiver of information. We ensuring that IDS does not impact on inline network performance.

IDS was originally developed this way because at the time the depth of analysis required for intrusion detection could not be performed at a speed that could keep pace with components on the direct communications path of the network infrastructure.

As explained, the IDS is also a listen-only device. The IDS monitors traffic and reports its results to an administrator, but cannot automatically take action to prevent a detected exploit from taking over the system. Attackers are capable of exploiting vulnerabilities very quickly once they enter the network, rendering the IDS an inadequate deployment for prevention device.

IDS consist of three different components: a host monitor per host, a single LAN monitor for each broadcast LAN segment, and server system director. The IDS director is responsible for evaluation of security state of the entire system of computers. It receives report and information from each host and LAN monitor and aggregate the information to make its decision. The Host monitor is primarily responsible for simple detection and reporting notable events. This paper provides in-depth discussion of the IDS architecture and capabilities of the system.