In the ever-evolving field of cybersecurity, it’s very important to have clarity of industry terms and associated technologies. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are two such technologies that people often confuse with each other. In order to ensure network security, it’s important for IT professionals to the difference between them and understand how they operate.

**What are IDS and IPS?**

Both systems are parts of network that detect and prevent hackers from intrusion into your system. Both these systems ensure network security. They help compare network packets and traffic against a cyber threat database and flag and packets that are causing offense.

The main difference between the two is that IDS monitors while IPS controls. Intrusion Detection Systems only scan and check the packets while Intrusion Prevention Systems prevent hackers from delivering the packet to the network.

**Differences between IDS and IPS**

By definition, an Intrusion Detection System monitors and analyzes network security by detecting signs of intrusion. It then flags any hacking methods and known threats. Intrusion Detection Systems ensure network security by detecting malware, backdoors, port scanners, phishing and other system security violations.

Intrusion Prevention Systems are located between the outside internet and internal network. If IDS flags a threat, IPS takes it as malicious traffic and denies access. If the traffic corresponds to a known database threat, IPS shuts down the delivery of the packets.

While both systems strengthen network security, the steps taken after detection sets the two apart. An IDS requires human interaction to read the results and create an action plan for resolving the identified threats. IPS is automated and blocks threatening traffic before it can cause damage to your network security. It prevents known threats from entering your network.

An Intrusion Detection System is not inline. Hence, traffic does not need to pass through it. In IPS however, traffic has to flow through. Furthermore, false positive by IDS only causes alarms. But an IDS showing false positive can cause you to lose important data or function.

Though both systems provide network security, it is only against known threats. You need to update both tools regularly for them to perform effectively. It cannot check for security threats that it has no knowledge of.

To sum it up, IDS and IPS are often overlapped now, and IPS mostly dominates the scene. Many vendors also provide hybrid detection and prevention systems tools for providing both features of detection and prevention.