What is an intrusion prevention system?

An[intrusion prevention system (IPS)](https://www.vmware.com/in/products/nsx-distributed-ids-ips.html" \t "_self) is a [network security](https://www.vmware.com/in/topics/glossary/content/network-security.html) 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.

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](https://www.vmware.com/in/topics/glossary/content/next-generation-firewall.html) (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.

[WATCH NOW](javascript:void(0);)

How does an intrusion prevention system work?

An intrusion prevention system is placed inline, in the flow of network traffic between the source and destination, and usually sits just behind the firewall.

When an IPS detects threats, it may take the following actions:

Drop suspicious network packets.

Block suspicious traffic.

Send alerts to security administrators.

Reconfigure firewalls.

Reset network connections.

IPS tools can help fend off denial-of-service (DoS) attacks; distributed denial-of-service (DDoS) attacks; worms; viruses; and exploits, including zero-day exploits.

There are several techniques that intrusion prevention systems use to identify threats:

* **Signature-based:** This method matches the activity to signatures of well-known threats. One drawback to this method is that it can only stop previously identified attacks and won’t be able to recognize new ones.
* **Anomaly-based:** This method monitors for abnormal behavior by comparing random samples of network activity against a baseline standard. It is more robust than signature-based monitoring, but it can sometimes produce false positives. Some newer and more advanced intrusion prevention systems use artificial intelligence and machine learning technology to support anomaly-based monitoring.
* **Policy-based:** This method is somewhat less common than signature-based or anomaly-based monitoring. It employs security policies defined by the enterprise and blocks activity that violates those policies. This requires an administrator to set up and configure security policies.

Once the IPS detects malicious activity, it can take many automated actions, including alerting administrators, dropping the packets, blocking traffic from the source address, or resetting the connection. Some intrusion prevention systems also use a “honeypot,” or decoy high-value data, to attract attackers and stop them from reaching their targets.

Types of intrusion prevention systems

There are several types of IPS, each with a slightly different purpose:

* **Network intrusion prevention system (NIPS):** This type of IPS is installed only at strategic points to monitor all network traffic and proactively scan for threats.
* **Host intrusion prevention system (HIPS):** In contrast to a NIPS, a HIPS is installed on an endpoint (such as a PC) and looks at inbound and outbound traffic from that machine only. It works best in combination with a NIPS, as it serves as a last line of defense for threats that have made it past the NIPS.
* **Network behavior analysis (NBA):** This analyzes network traffic to detect unusual traffic flows, such as DDoS (Distributed Denial of Service) attacks.
* **Wireless intrusion prevention system (WIPS):** This type of IPS simply scans a Wi-Fi network for unauthorized access and kicks unauthorized devices off the network.

Where are the benefits of an intrusion prevention system?

An intrusion prevention system offers many benefits:

* **Additional security:** An IPS works in tandem with other security solutions, and it can identify threats that those other solutions can’t. This is particularly true of systems that use anomaly-based detection. It also provides superior [application security](https://www.vmware.com/in/topics/glossary/content/application-security.html) thanks to a high level of application awareness.
* **Increased efficiency for other security controls:** Because an IPS filters out malicious traffic before it reaches other security devices and controls, it reduces the workload for those controls and allows them to perform more efficiently.
* **Time savings:** Since an IPS is largely automated, it requires less of a time investment from IT teams.
* **Compliance:** An IPS fulfills many of the compliance requirements set forth by PCI DSS, HIPAA, and others. It also provides valuable auditing data.
* **Customization:** An IPS can be set up with customized security policies to provide security controls specific to the enterprise that uses it.