IDS & IPS

Most organisations have either an IDS or an IPS, and may have both as part of their security information and event management framework.

Intrusion Detection Systems (IDS)

A system that monitors network traffic for suspicious activity and alerts users when such activity is discovered.

Warns of suspicious activity taking place, but it doesn't prevent it.

There are two main types of Intrusion Detection System:

1. Network Intrusion Detection System (NIDS)
2. Host Intrusion Detection System (HIDS)

A host-based intrusion detection system (**HIDS**) is installed on the client computer. A network-based intrusion detection system (**NIDS**) resides on the network.

A system with direct access to both the enterprise internal network and the internet, the **HIDS** captures a 'picture' of the file set of an entire system and then compares it to a previous picture. If the system finds major discrepancies, such as files that are missing, etc, then it immediately alerts the administrator about it.

In addition to the two main types of **IDS**, there are also two main subsets of these **IDS** types.

The IDS subsets include:

1. Signature-based Intrusion Detection System (**SBIDS**)
2. Anomaly-based Intrusion Detection System (**ABIDS**)

An **IDS** that works like Antivirus software, **SBIDS** tracks all the packets passing over the network and then compares them to a database containing attributes or signatures of familiar malicious threats.

Lastly, **ABIDS** tracks the traffic of a network and then compares it to an established measure and this allows the system to find what's normal for the network in terms of Ports, Protocols, Bandwidth, and other devices. ABIDS can quickly alert administrators about any unusual or potentially malicious activity in the network.

What are the capabilities of Intrusion Detection Systems?

The basic function of IDS is monitoring the traffic of a network to detect any intrusion attempts being made by unauthorised people. However, there are some other functions/capabilities of IDS as well.

They include:

- Monitoring the operation of files, routers, key management servers, and firewalls that are required by other security control and these are the controls that help to identify, prevent, and recover from cyber attacks.
- Allowing non-technical staff to manage system security by providing a user-friendly interface.

- Allowing administrators to adjust, arrange, and understand the key audit trails and other logs of operating systems that are generally hard to dissect and keep track of.
- Blocking the intruders or the server to respond to an attempted intrusion.
- Notifying the administrator that the network security has been breached.
- Detecting altered data files and reporting them.
- Providing an extensive database of attack signature with which the information from the system can be matched.

What are the benefits of IDS?

There are several benefits of Intrusion Detection software. Firstly, **IDS** software provides you with the ability to detect unusual or potentially malicious activity in the network.

Another reason for having an **IDS** at your organisation is equipping the relevant people with the ability to analyse not only the number of attempted cyber-attacks occurring in your network but also their types. This will provide your organisation with the required information to implement better controls or change existing security systems.

IDS false positives are usually just a minor inconvenience. Although the **IDS** incorrectly labels legitimate traffic as malicious, it does not prevent the traffic from entering the network.

Some other benefits of IDS software are:

- Detecting problems or bugs within your network device configurations. This will help in better assessing future risks.
- Attaining regulatory compliance. It is easier to meet security regulations with **IDS** as it provides your organization with greater visibility across networks.
- Improving security response. **IDS** sensors allow you to assess data within the network packets as they are designed to identify network hosts and devices. Additionally, they can detect the operating systems of the services being used.

What is the difference between IDS, IPS, and Firewall?

This is another frequently asked question about **IDS**. Three essential network components i.e. **IDS**, **IPS**, and **Firewall** help to ensure a network’s security. However, there are differences in how these components function and secure the network.

The biggest difference between Firewall and **IPS**/**IDS** is their basic function; while Firewall blocks and filters network traffic, **IDS**/**IPS** looks to identify malicious activity and alert an administrator to prevent cyberattacks.

A rules-based engine, Firewall analyses the source of the traffic, destination address, destination port, source address, and protocol type to determine whether to allow or block the traffic coming in.

An active device, **IPS** are situated between the Firewall and the rest of the network and the system keeps track of inbound packets and what they are used for before deciding to block or allow the packets into the network.

A passive device, **IDS** monitors data packets passing over the network and then compares it to patterns in the signature database to decide whether or not to alert the administrator. If the intrusion detection software detects an unusual pattern or a pattern that deviates from what is normal and then reports the activity to the administrator.

List of the Best Intrusion Detection Software:

1. **Solarwinds** - Windows
2. **Zeek (Bro)** - Unix, Linux, Mac-OS
3. **OSSEC** - Unix, Linux, Windows, Mac-OS
4. **Snort** - Unix, Linux, Windows
5. **Suricata** - Unix, Linux, Windows, Mac-OS
6. **Security Onion** - Linux, Mac-OS

Intrusion Prevention Systems (IPS)

Intrusion prevention systems work to the maxim “**better late than never**.” Ideally, you wouldn’t want any outsiders getting unauthorised access to your system. However, this is not a perfect world and there are many cons that hackers can pull to trick authorised users into giving away their credentials.

Specifically, intrusion prevention systems are **extensions to intrusion detection systems**. **IPS**s act once suspicious activity has been identified. So, there may already have been some damage done to the integrity of your system by the time the intrusion has been spotted.

The IPS is able to perform actions to shut down the threat. These actions include:

- Restoring log files from storage
- Suspending user accounts
- Blocking IP addresses
- Killing processes
- Shutting down systems
- Starting up processes
- Updating firewall settings
- Alerting, recording, and reporting suspicious activities

The responsibility of admin tasks that make many of these actions possible is not always clear. For example, the protection of log files with encryption and the backing up of log files so that they can be restored after tampering are two threat protection activities that are usually defined as intrusion detection system tasks.

Intrusion Prevention Systems are usually:

- Located between a company's firewall and the rest of its network.
- Warns of suspicious activity talking place and prevents it.

Limitations of intrusion prevention systems

IPS false positives can be more serious. When an **IPS** mistakes legitimate traffic for a threat, it stops the legitimate traffic from entering the network, which could impact any part of the organisation, not just the IT team.

> Protecting the boundary of your network will prevent a large number of hacker attacks. The installation of firewalls and antivirus is still important. These protection measures have become very effective at preventing malicious code from getting onto a network. However, they have been so successful that **hackers have found other ways to get access to a company’s computing infrastructure**.

The best Intrusion Prevention Systems

There is a remarkably large number of IPS tools available at the moment. **Many of these are free**. However, it would take you a long time to study and try every single **IPS** on the market. This is why we have put together this guide to intrusion prevention systems.

Our methodology for selecting an IPS tool

We reviewed the IPS market and analysed tools based on the following criteria:

- **Procedures to detect email-bound cons, such as phishing**
- **Automated attack mitigation steps**
- **The ability to interface with other IT security systems**
- **Settings to let the user allow automated response**
- **Data storage for historical analysis plus analytical tools in the dashboard**
- **Attack protection for the IPS’s own processes and logs**
- **A free, demo, trial, or money-back guarantee**
- **Value for money**

Tools:

1. **Datadog Real-time Threat Monitoring**
2. **Solarwinds**
3. **CrowdStrike Falcon XDR**
4. **Splunk**
5. **Sagan**
6. **OSSEC**
7. **Fail2Ban**
8. **Zeek**