**Intrusion Detection/Prevention system**

1. IDS/IPS - almost interchangeable
2. Actions: Allow, Deny, Alert
3. Network based Vs Host based
4. Deeper Packet inspection
5. Detections

* Signatures
* Anomalies

An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and **issues alerts** when such activity is discovered.

It is a software application that scans a network or a system for the harmful activity or policy breaching.

Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system.

1. **Network Intrusion Detection System (NIDS):**Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks.
2. **Host Intrusion Detection System (HIDS):**Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot.
3. .**Protocol-based Intrusion Detection System (PIDS):**Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol.

What is an Intrusion Prevention System (IPS)?

An intrusion prevention system (IPS) or intrusion detection and prevention systems (IDPS) are network security applications that focus on identifying possible malicious activity, logging information, reporting attempts, and attempting to prevent them. IPS systems often sit directly behind the firewall.

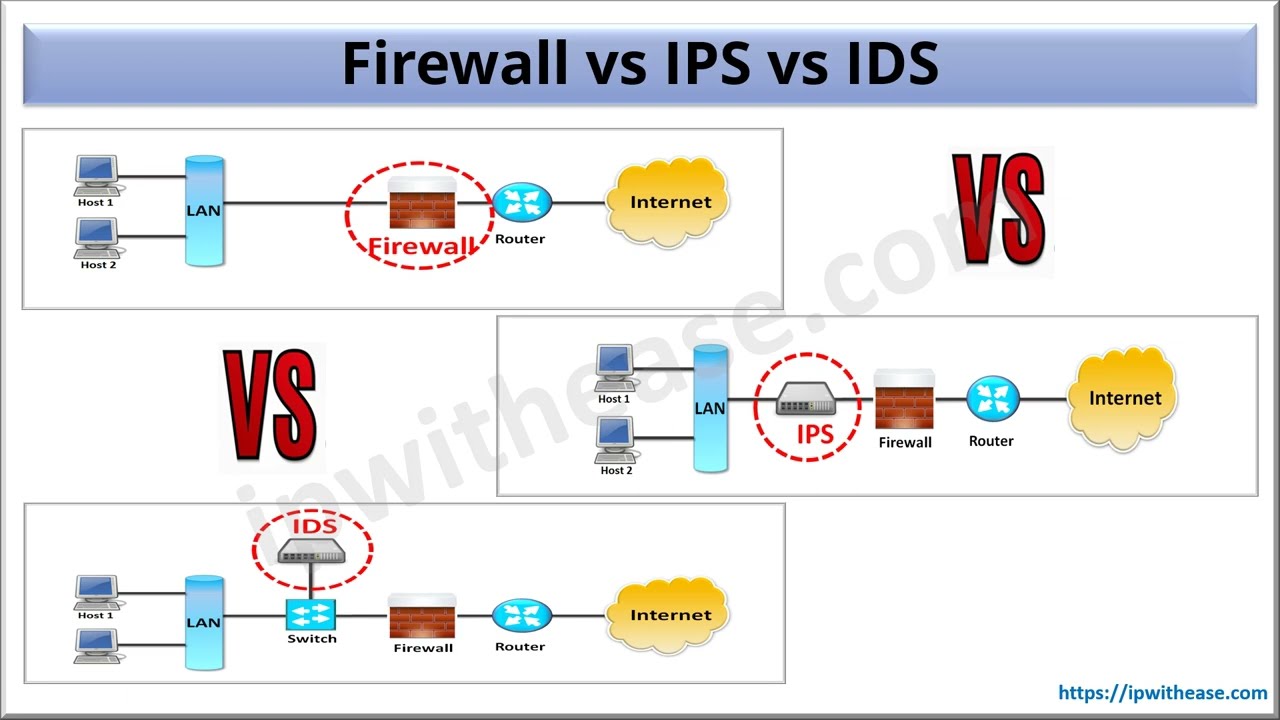
Once detected, an IPS performs real-time packet inspection on every packet that travels across the network and if deemed suspicious, the IPS will perform one of the following actions:

* Terminate the TCP session that has been exploited
* Block the offending IP address or user account from accessing any application, host, or network resource
* Reprogram or reconfigure the firewall to prevent a similar attack from occurring at a later date
* Remove or replace malicious content that remains after an attack by repackaging the payload, removing header information, or destroying infected files

**1.Network-based intrusion prevention system (NIPS):** NIPS detect and prevent malicious activity or suspicious activity by analyzing packets throughout the network. Once installed, NIPS gather information from the host and network to identify permitted hosts, applications, and operating systems on the network.

**2.Host-based intrusion prevention system (HIPS):** A system or program employed to protect critical computer systems. HIPS analyze activity on a single host to detect and prevent malicious activity, primarily through analyzing code behavior. They are often praised for being able to prevent attacks that use [encryption](https://www.upguard.com/blog/encryption). HIPS can also be used to prevent sensitive information like [personally identifiable information (PII)](https://www.upguard.com/blog/personally-identifiable-information-pii) or [protected health information (PHI)](https://www.upguard.com/blog/protected-health-information-phi) from being extracted from the host

**3.Wireless intrusion prevention system (WIPS):** WIPS monitor the radio spectrum for the presence of unauthorized access points and automatically take countermeasures to remove them.



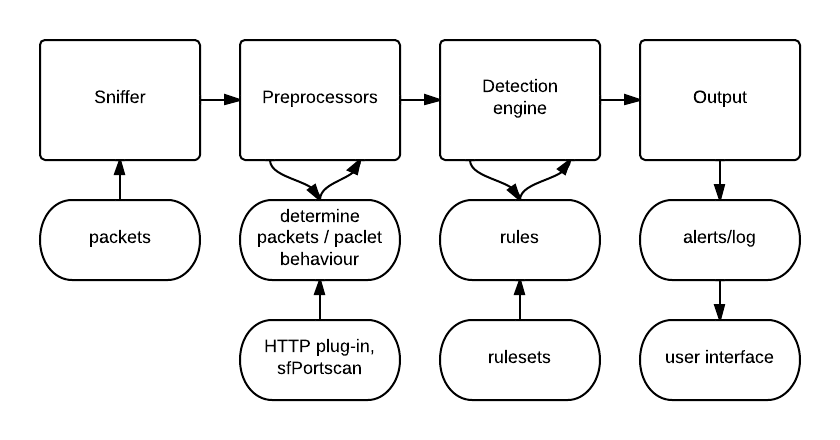
**SNORT**

Long a leader among enterprise intrusion prevention and detection tools.

Snort is referred to as a **packet sniffer** that

* **monitors network traffic,**
* scrutinizing each packet closely to **detect a dangerous payload or suspicious anomalies.**

Snort first started as a packet sniffer. Another common example of a packet sniffer is tcpdump, or its graphical big brother Wireshark. In order to evolve into the IDS software that it is today, Snort added a few things in its architecture. It currently functions as a core with plug-ins system, where its primal component (the sniffer) is the core and the other elements act as plug-ins.

****

The other elements are the preprocesors, the detection engine and the output.

1. **The sniffer** – as the name says, it “sniffs” (collects) network traffic and identifies each packet structure (layer information). After collecting, the raw data (packets) are being sent to the preprocessors.

2. **The preprocessors** – perform certain actions to determine what kind of packets or what kind of behaviour is Snort dealing with. There are muliple preprocessor plugins. As we can see in the picture above, one of the is the HTTP plug-in which will identify HTTP packets. The sfPortscan preprocessor is a good example of how Snort determines packet “behaviour”. Having defined protocols, scan types and sensitivity levels it can identify multiple packets as a port scan. After doing its job, the processors will send the information to the detection engine.

3. **The detection engine** – compares each packet with each rule from a predefined ruleset. If packets match the rule contents (or the other way around), they are being forwarded to the output.

4. **The output** – will log and/or trigger alerts based on the rule action. Logs can be saved in different formats (syslog format, unified2) and to different locations (directly to db). As they are, logs and alerts are a bit difficult to read from the command line (especially when we are talking about orders of 10000 or more) – this being the main reason why user interfaces are required. Snort user interfaces ([Snorby](https://truica-victor.com/how-to-install-snorby-for-snort/), ACID) act as extensions to the Output component of Snort.

**What is the primary advantage of using a network-based intrusion detection system (NIDS)?**

The primary advantage of an NIDS is the ***low maintenance involved in analyzing traffic in the network*.**

An NIDS is ***easy and economical to manage*** because the signatures are not configured on all the hosts in a network segment.

***Configuration usually occurs at a single system***, rather than on multiple systems.

By contrast, host-based intrusion detection systems (HIDSs) are difficult to configure and monitor because the intrusion detection agent should be installed on each individual workstation of a given network segment.

HIDSs are configured to use the operating system audit logs and system logs, while NIDSs actually examine the network packets.

Individual hosts do not need real-time monitoring because intrusion is monitored on the network segment on which the NIDS is placed, and not on individual workstations.

**SNORT**

Platform: Unix, Linux, Windows

Type: NIDS

Features:

1. Packet sniffer,
2. Packet logger,
3. Threat intelligence,
4. Signature blocking,
5. Real-time updates for security signatures,
6. In-depth reporting,
7. Ability to detect a variety of events including OS fingerprinting, SMB probes, CGI attacks, buffer overflow attacks, and stealth port scans.