11.3.2 IDS Facts

The first step in defending a network against unauthorized access is knowing that someone is gaining access. An intrusion detection system (IDS) is a special network device that can detect attacks and suspicious activity. An active IDS is known as an intrusion prevention system (IPS).

This lesson covers the following topics:

- Differences between IDSs and IPSs
- Detection methods
- Device implementation

Differences between IDSs and IPSs

The below table shows the differences between an IDS and an IPS:

IDS	IPS
A passive IDS monitors, logs, and detects security breaches, but it takes no action to stop or prevent the attack. A passive IDS: ▪ Can send an alert, but this requires the security administrator to interpret the degree of the threat and respond accordingly ▪ Cannot be detected on the network because it takes no detectable actions	An active IDS, also called an IPS, performs the functions of an IDS but can also react when security breaches occur. An IPS: ▪ Can automate responses to malicious or suspicious traffic ▪ Can terminate sessions (using the **TCP-RST** command) or restart other processes on the system. ▪ Performs behaviors that can be seen by anyone watching the network. Usually these actions are necessary to block malicious activities or discover the identity of an intruder. Updating filters and performing reverse lookups are common behaviors of an active IDS.

Using both of these devices in a network provides the best network detection and protection. If a malicious packet makes it past the IPS, the IDS serves as a backup and alerts the security operations team.

The IDS also records and logs everything (this can be viewed in the follow-up).

The steps a IDS/IPS takes when monitoring traffic are:

- A sensor passes data from the source to the analyzer.
- The engine, or analyzer, analyzes the sensor data and events, generates alerts, and logs all activity. An *alert* is a message indicating an event of interest (such as a possible attack)
- The IDS/IPS labels traffic based on its interpretation of whether or not the traffic poses a threat, as described in the following table.

State	Description
Positive	A positive traffic assessment means that the system detected an attack and the appropriate alarms and notifications were generated or the correct actions were performed to prevent or

	stop the attack.
False positive	A false positive traffic assessment means that the system identified harmless traffic as offensive and generated an alarm or stopped the traffic.
Negative	A negative traffic assessment means that the system deemed the traffic harmless and let it pass.
False negative	A false negative traffic assessment means that harmful traffic was allowed to pass without any alerts being generated or any actions being taken to prevent or stop it. This is the worst possible scenario.

Detection Methods

Both systems monitor data packets for malicious or unauthorized traffic. The below table shows the different methods they can use to distinguish attacks and threats from normal traffic:

Detection Method	Description
Signature-based	Signature-based detection, also referred to as pattern matching, dictionary recognition, or misuse-detection (MD-IDS), looks for patterns in network traffic and compares them to known attack patterns called signatures. Similar to how viruses have a unique fingerprint that antivirus programs use to detect their presence, malicious packets have a unique fingerprint that the IDS can use to do the same. These fingerprints are referred to as signatures. ▪ Signatures are written and updated by the IDS vendors. ▪ Signature-based detection cannot detect unknown attacks; they can only detect attacks identified by published signature files. For this reason, it is important to update signature files on a regular basis. ▪ Signature-based detection usually causes more false negatives than heuristic-based detection.
Heuristic-based	Heuristic-based detection, also referred to as behavior, anomaly, or statistical-based detection, first defines a baseline of normal network traffic and then monitors it. It looks for anything that falls outside that baseline. ▪ Clipping levels, or thresholds, are defined and used to identify deviations from the baseline. ▪ When the threshold is reached, an alert is generated or action is taken. ▪ Heuristic-based systems can recognize and respond to some unknown attacks (attacks that do not have a corresponding signature file). ▪ This detection method usually causes more false positives than signature-based detection.

Device Implementation

An IDS/IPS can be implemented as a host-based or network-based device. The below table describes each implementation:

Implementation Method	Description
Host-based	

	A *host-based* IDS (HIDS) is a program installed on the host system itself that monitors all traffic coming into the host. A host-based IDS: ▪ Is used to detect attacks that are unique to the services and applications on that system. It can monitor application activity and modifications as well as local system files, logon audit files, and kernel audit files. ▪ Is typically unaware of other devices on the network but can be detected and could be the target of an attack itself. ▪ May rely on auditing and logging capabilities of the operating system. ▪ Can analyze encrypted traffic (because services running on the host decrypt the traffic) Antivirus software is the most common form of a host-based IDS One issue with host-based IDSs is that the software must be installed and configured on each system being protected. This can lead to excessive administrative effort. Also, if the host-system is compromised, the log reports on that system become unreliable because the attacker may have modified the log files.
Network-based	A *network-based IDS* (NIDS) is a dedicated device installed on the network. It analyzes all traffic on the network in real time. There are two options when installing an NIDS: ▪ The first option is to install the NIDS out of band. This means it is installed outside the flow of traffic. ▪ The IDS is usually connected with a network tap, such as a switch. This allows it to monitor network traffic without being in the way. ▪ The other option is to install the NIDS as an *inline* device. This means it is installed in the flow of traffic and all traffic goes through the NIDS. It is then analyzed and either allowed to continue on or is stopped. Some other things to be aware of when implementing a NIDS are: ▪ An NIDS is typically unaware of individual hosts on the network. It cannot be detected by attacking systems. ▪ An NIDS is particularly well suited for detecting and blocking port scanning and DoS attacks. ▪ An NIDS is unable to analyze encrypted traffic ▪ An NIDS should be placed at all critical junctions within a network, including backbones and critical choke points, such as: ▪ Inside the DMZ ▪ Between the firewall and the internal LAN ▪ Near any critical information assets ▪ If using a switch on the network, the NIDS must be placed on a special port called a *spanning* or *diagnostic* port that directly connects to the backbone of the switch. This way, the NIDS can see all traffic on that segment. ▪ A control center should be set up to receive all IDS data. This is where all decision-making should take place in regards to NIDS communications. ▪ A application-aware NIDS can analyze network packets to detect malicious payloads targeted at Application layer services (such as a web server).