6.8.3 IDS Facts

An *intrusion detection system* (IDS) is a special network device or system of network devices that can detect attacks and suspicious activity. An active IDS system is sometimes called an *intrusion prevention system* (IPS).

Here are a few terms used in describing and configuring an IDS.

IDS Term	Description
IPS Sensor	An IPS sensor is connected inline between the external network and the edge router or firewall. This allows the IPS to drop packets and defend an attack before it enters the internal network.
IDS Sensor	An IDS sensor is connected inline between the edge router or firewall and the uplink port of an aggregation switch. Alternately it can be connected to a spanning port of the aggregation switch. Since it only analyzes packets, its detection capabilities can be set more aggressively than the IPS sensor.
Traffic Collector	The traffic collector gathers activity and event data for analysis such as inbound and outbound traffic metrics. On a host-based IDS, this also involves activity recorded by the operating system that is stored in log and audit files.
Analysis or Correlation Engine	The analysis engine analyzes the data collected by the traffic collector. A knowledge-based IDS compares the data against a signature database. A behavior-based IDS compares the data against baseline behavior information gathered over time.
Filter	For easier analysis, a filter can be used to keep more important IDS data. The filter is a query that removes or ignores less important IDS data.
VPN Concentrator	If an IDS is placed external to a VPN concentrator, it will not be capable of analyzing encrypted network traffic.
SSL Accelerator	As with a VPN concentrator, an IDS should be placed internal to a SSL accelerator so that it can analyze decrypted network traffic.
Load Balancer	An IPS is typically placed external to any load balancing systems. An IDS should be placed so that it can analyze all traffic. This means it should either be placed before load balancing or it should be connected to a spanning port on the aggregation switch that carries traffic to the load balancer.
DDos Mitigation	Since IPSs and firewalls protect the edge of the network, they are the first line of defense against DDoS attacks. While newer IPSs and firewalls have DDoS configuration settings, they should not be relied upon as the only defense against DDoS attacks.
Aggregation Switches	An IDS should be placed inline between the edge router or firewall and the uplink port of an aggregation switch. Alternately it can be connected to a spanning port of the aggregation switch.
Taps and Port Mirrors	If an IDS or IPS can't be placed inline, a tap (test access port) device can be used. The tap is placed inline and provides an additional port that echoes all traffic passing through the tap. A switch's spanning port is also known as a port mirror. A copy of all network packets seen on the switch is sent to the spanning port or port mirror. A spanning port is an ideal location for connecting an IDS.

IDS features:

- IDS administration is usually accomplished through a console by an *operator* (IDS user or administrator) that monitors events, alerts, and control sensors.
- IDS systems can use multiple data sources to find attacks. They can analyze audit files, systems logs, and real-time traffic.
- A sensor passes data from the data source to the analyzer.
- The engine, or analyzer, analyzes sensor data and events, generates alerts, and logs activity.
- An *alert* is a message indicating an event of interest (such as a possible attack).
- The IDS labels traffic based on its interpretation of whether or not the traffic poses a threat, as described in the following table:

State	Description
Positive	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	False positive traffic assessment means that the system identified harmless traffic as offensive and generated an alarm or stopped the traffic.
Negative	Negative traffic assessment means that the system deemed the traffic harmless and let it pass.
False Negative	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 action by an IDS.

There are several ways to describe typical detection systems:

Method	Variations

Response Capability	An intrusion detection system can be classified by how it responds when a threat is detected:
	▪ A passive IDS monitors, logs, and detects security breaches, but takes no action to stop or prevent the attack. A passive IDS:
	  ▪ Can send an alert, but it is the network administrator's job to interpret the degree of the threat and respond accordingly.
	  ▪ Might also perform shunning, which is simply dropping offending traffic without additional actions.
	  ▪ Cannot be detected on the network because it takes no detectible action.
	▪ An active IDS, also called an intrusion protection system (IPS), performs the functions of an IDS but can also *react* when security breaches occur. An IPS:
	  ▪ Can automate responses that may include dynamic policy adjustment and reconfiguration of supporting network devices to block the offending traffic.
	  ▪ Can terminate sessions (e.g., using the **TCP-RST** command) or terminate 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.
	
	Intrusion detection and protection systems are not mutually exclusive. When implementing a layered defense, use both to best protect your system. An active IDS can be used to prevent unauthorized access and attacks. A passive IDS will alert the network administrator when prevention has failed and then document breaches to the system.

Recognition Method	The recognition method defines how the system distinguishes attacks and threats from normal activity.
	▪ Signature recognition, 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*.
	  ▪ IDS signatures are written and updated by the IDS vendor in response to identified vulnerabilities.
	  ▪ Signature-based recognition 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 recognition usually causes more false negatives than anomaly-based IDS.
	
	Signature recognition is the most common IDS recognition type.
	
	▪ Anomaly recognition, also referred to as behavior, heuristic, or statistical recognition, monitors traffic to define a standard activity pattern as normal.
	  ▪ Clipping levels or thresholds are defined and are used to identify deviations from the norm.
	  ▪ When the threshold is reached, an alert is generated or action is taken.
	  ▪ Anomaly-based systems can recognize and respond to some unknown attacks (attacks that do not have a corresponding signature file).
	  ▪ Anomaly recognition usually causes more false positives than signature-based IDS.
	  ▪ Anomaly-based recognition systems can be fooled by incremental changes within the clipping level that cause the changed state to become the normal level of activity, thus allowing a higher level of irregularity to go unnoticed.

Detection Scope	Systems can be classified based on where the system runs and the scope of threats it looks for.
	▪ A host-based IDS (HIDS) is installed on a single host and monitors all traffic coming in to the host. A host-based IDS:
	  ▪ Is used to detect attacks that are unique to the services on the 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).
	
	Anti-virus software is the most common form of a host-based IDS.
	
	▪ A *network-based* IDS (NIDS) is a dedicated device installed on the network. It analyzes all traffic on the network.
	  ▪ An NIDS is typically implemented as part of a firewall device acting as a router. When implemented as a stand-alone device, you must direct all traffic to the IDS device using one of the following strategies:
	  ▪ Connect the IDS and other devices using a hub. The IDS will then see all traffic sent to all devices on the subnet.
	  ▪ Connect the IDS to a switch and enable spanning or diagnostic capabilities on the switch port to forward all traffic to that switch port.
	  ▪ Use a tap to connect the IDS directly to the network medium.
	  ▪ 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.
	  ▪ Be aware that an NIDS cannot 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
  - Behind the internal firewall in the corporate LAN
  - Near your critical information assets

  If you are using a switch on your network, your IDS must be placed on a special port called a spanning or diagnostic port that directly connects to the backbone of the switch so that the IDS 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 IDS communications.

- An application-aware IDS or IPS can analyze network packets to detect malicious payloads targeted at application-layer services (such as a web server).

One way to protect your real servers and networks is to create fake resources that appear to contain valuable information, such as the following:

- A *honeypot* is a device or virtual machine that entices intruders by displaying a vulnerable trait or flaw or by appearing to contain valuable data.
- A *honeynet* is a network of honeypots.
- A *tarpit* (also called a sticky honeypot) is a honeypot that answers connection requests in such a way that the attacking computer is "stuck" for a period of time. A tarpit can also transfer an attacker to a *padded cell*, a safe environment where no critical data is stored. In the padded cell, the attacker can be monitored where harm cannot be caused. Honeypots are often placed inside the padded cell.
- The two main goals of using these solutions are to:
  - Offer the attackers targets that will occupy their time and attention, distracting them from valid resources.
  - Observe the attackers to gather information about the methods of attack or to gather evidence to assist in identification or prosecution.
- When implementing these solutions, be careful that your design does not inadvertently entice otherwise-honest users from taking dishonest actions.
  - *Enticement* is the process of using a honeypot or honeynet to lure an attacker in. With enticement, the vulnerable system exists, but is unlikely to be detected by a user without malicious intent.
  - *Entrapment* is the process of encouraging a person to take dishonest or criminal actions when the person would have otherwise been unlikely to have taken that action. With entrapment, you actively solicit users to visit the system where they might be encouraged or tricked into attempting illegal access.

Be aware of the following security facts about intruder detection:

- IDS can miss frames when the network is too busy.
- IDS log reports become unreliable if the system is compromised because the attacker may have modified the log files.
- When an intruder is detected, stopping the intrusion is often more important than continuing with the hopes of gathering additional information about the attacker to catch the attacker. Allowing an intruder to spend any additional time inside of your network can lead to further breaches of confidentiality.
- After you have taken measures to stop an attack, be sure to document the incident. Make backups of the logs and audit files to retain information about the attack for future investigations.
- After audit trails are secured, repairing damage, deploying new countermeasures, and even updating the security policy are reasonable activities to perform.
- If you were unable to discover the identity of the perpetrator or means of attack, future review of the evidence and comparison to other incidents,may reveal important details or patterns.
