Cybersecurity Tools

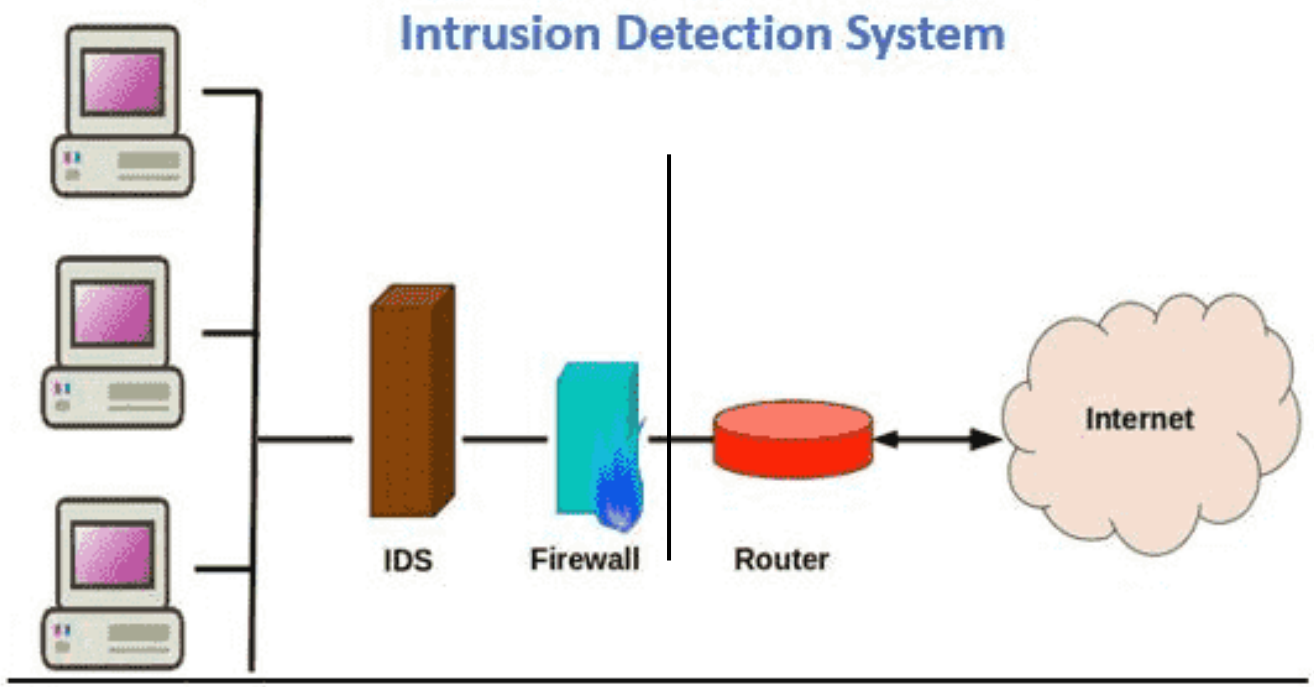
م.د.ابراهيم محمد الحليمه

2025

Network intrusion detection

The 3 Intrusion Detection System Methods
Signature-Based Intrusion Detection. Signature-Based Intrusion Detection Systems (SIDS) aim to identify patterns and match them with known signs of intrusions. ...
Anomaly-Based Intrusion Detection. ...
Hybrid Intrusion Detection.

A Network-Based Intrusion Detection System (NIDS) monitors network traffic patterns to detect suspicious activity. Sensors are placed at strategic check points, such as the DMZ or behind a firewall analysing each individual packet (inbound and outbound) for malicious activity.



What Is An Intrusion Detection System (IDS)?

An intrusion detection system (IDS) is an application that monitors network traffic and searches for known threats and suspicious or malicious activity. The IDS sends alerts to IT and security teams when it detects any security risks and threats.

Most IDS solutions simply monitor and report suspicious activity and traffic when they detect an anomaly. However, some can go a step further by taking action when it detects anomalous activity, such as blocking malicious or suspicious traffic.

IDS tools typically are software applications that run on organizations' hardware or as a network security solution. There are also cloud-based IDS solutions that protect organizations' data, resources, and systems in their cloud deployments and environments.

What Is An Intrusion In Cybersecurity?

The answer to "what is intrusion" is typically an attacker gaining unauthorized access to a device, network, or system. Cyber criminals use increasingly sophisticated techniques and tactics to infiltrate organizations without being discovered. This includes common techniques like:

Address spoofing: The source of an attack is hidden using spoofed, misconfigured, and poorly secured proxy servers, which makes it difficult for organizations to discover attackers.
Fragmentation: Fragmented packets enable attackers to bypass organizations' detection systems.
Pattern evasion: Hackers adjust their attack architectures to avoid the patterns that IDS solutions use to spot a threat.
Coordinated attack: A network scan threat allocates numerous hosts or ports to different attackers, making it difficult for the IDS to work out what is happening.

Types Of Intrusion Detection Systems (IDS)

IDS solutions come in a range of different types and varying capabilities. Common types of intrusion detection systems (IDS) include:

Network intrusion detection system (NIDS): A NIDS solution is deployed at strategic points within an organization's network to monitor incoming and **.1** outgoing traffic. This IDS approach monitors and detects malicious and suspicious traffic coming to and going from all devices connected to the network.

Host intrusion detection system (HIDS): A HIDS system is installed on individual devices that are connected to the internet and an organization's internal **.2** network. This solution can detect packets that come from inside the business and additional malicious traffic that a NIDS solution cannot. It can also discover malicious threats coming from the host, such as a host being infected with malware attempting to spread it across the organization's system.

Signature-based intrusion detection system (SIDS): A SIDS solution monitors all packets on an organization's network and compares them with attack **.3** signatures on a database of known threats.

Anomaly-based intrusion detection system (AIDS): This solution monitors traffic on a network and compares it with a predefined baseline that is **.4** considered "normal." It detects anomalous activity and behavior across the network, including bandwidth, devices, ports, and protocols. An AIDS solution uses machine-learning techniques to build a baseline of normal behavior and establish a corresponding security policy. This ensures businesses can discover new, evolving threats that solutions like SIDS cannot.

Perimeter intrusion detection system (PIDS): A PIDS solution is placed on a network to detect intrusion attempts taking place on the perimeter of **.5** organizations' critical infrastructures.

Virtual machine-based intrusion detection system (VMIDS): A VMIDS solution detects intrusions by monitoring virtual machines. It enables organizations **.6** to monitor traffic across all the devices and systems that their devices are connected to.

Stack-based intrusion detection system (SBIDS): SBIDS is integrated into an organization's **Transmission Control Protocol/Internet Protocol (TCP/IP)**, which **.7** is used as a communications protocol on private networks. This approach enables the IDS to watch packets as they move through the organization's network and pulls malicious packets before applications or the operating system can process them.

Types Of Intrusion Detection Systems (IDS)

IDS solutions come in a range of different types and varying capabilities. Common types of intrusion detection systems (IDS) include:

Network intrusion detection system (NIDS): A NIDS solution is deployed at strategic points within an organization's network to monitor incoming and **.1** outgoing traffic. This IDS approach monitors and detects malicious and suspicious traffic coming to and going from all devices connected to the network.

Host intrusion detection system (HIDS): A HIDS system is installed on individual devices that are connected to the internet and an organization's internal **.2** network. This solution can detect packets that come from inside the business and additional malicious traffic that a NIDS solution cannot. It can also discover malicious threats coming from the host, such as a host being infected with malware attempting to spread it across the organization's system.

Signature-based intrusion detection system (SIDS): A SIDS solution monitors all packets on an organization's network and compares them with attack **.3** signatures on a database of known threats.

Anomaly-based intrusion detection system (AIDS): This solution monitors traffic on a network and compares it with a predefined baseline that is **.4** considered "normal." It detects anomalous activity and behavior across the network, including bandwidth, devices, ports, and protocols. An AIDS solution uses machine-learning techniques to build a baseline of normal behavior and establish a corresponding security policy. This ensures businesses can discover new, evolving threats that solutions like SIDS cannot.

Perimeter intrusion detection system (PIDS): A PIDS solution is placed on a network to detect intrusion attempts taking place on the perimeter of **.5** organizations' critical infrastructures.

Virtual machine-based intrusion detection system (VMIDS): A VMIDS solution detects intrusions by monitoring virtual machines. It enables organizations **.6** to monitor traffic across all the devices and systems that their devices are connected to.

Stack-based intrusion detection system (SBIDS): SBIDS is integrated into an organization's **Transmission Control Protocol/Internet Protocol (TCP/IP)**, which **.7** is used as a communications protocol on private networks. This approach enables the IDS to watch packets as they move through the organization's network and pulls malicious packets before applications or the operating system can process them.

4 Benefits of Intrusion Detection Systems (IDS):

01

Understanding risk

02

Shaping security strategy

03

Regulatory compliance

04

Faster response times

Intrusion detection system (IDS) challenges

While IDS solutions are important tools in monitoring and detecting potential threats, they are not without their challenges. These include:

.1 **False alarms**: Also known as false positives, these leave IDS solutions vulnerable to identifying potential threats that are not a true risk to the organization. To avoid this, organizations must configure their IDS to understand what normal looks like, and as a result, what should be considered as malicious activity.

.2 **False negatives**: This is a bigger concern, as the IDS solution mistakes an actual security threat for legitimate traffic. An attacker is allowed to pass into the organization's network, with IT and security teams oblivious to the fact that their systems have been infiltrated.

As the threat landscape evolves and attackers become more sophisticated, it is preferable for IDS solutions to provide false positives than false negatives. In other words, it is better to discover a potential threat and prove it to be wrong than for the IDS to mistake attackers for legitimate users. Furthermore, IDS solutions increasingly need to be capable of quickly detecting new threats and signs of malicious behavior.

What Is The Difference Between A Firewall And IDS?

Firewalls and intrusion detection systems (IDS) are cybersecurity tools that can both safeguard a network or endpoint. Their objectives, however, are very different from one another.

IDS: Intrusion detection systems are passive monitoring tools that identify possible threats and send **.1** out notifications to analysts in **security operations centers (SOCs).** In this way, incident responders can promptly look into and address the potential event.

Firewall: A firewall, on the other hand, analyzes the metadata contained in network packets and **.2** decides whether to allow or prohibit traffic into or out of the network based on pre-established rules. A firewall essentially creates a barrier that stops certain traffic from crossing through it.

An IDS is focused on detecting and generating alerts about threats, while a firewall inspects inbound and outbound traffic, keeping all unauthorized traffic at bay.

Services / Snort / Alerts

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

Clear all interface log files

Alert Log View Settings

Interface to Inspect WAN — Choose interface..

Auto-refresh view

1000 — Alert lines to display.

Save

Alert Log Actions Download | Clear

Alert Log View Filter

Last 1000 Alert Log Entries

Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description
2017-07-23 20:49:52	1	UDP	A Network Trojan was Detected	66.240.205.34	1066		16464	1:31136	MALWARE-CNC Win.Trojan.ZeroAccess inbound connection
2017-07-22 06:15:49	2	UDP	Potentially Bad Traffic	163.172.17.76	54465		5060	140:26	(spp_sip) Method is unknown
2017-07-21 09:26:30	2	UDP	Potentially Bad Traffic	163.172.22.169	52428		5060	140:26	(spp_sip) Method is unknown
2017-07-21 01:03:28	2	UDP	Potentially Bad Traffic	163.172.17.76	46834		5060	140:26	(spp_sip) Method is unknown
2017-07-20 20:36:37	2	UDP	Potentially Bad Traffic	163.172.22.169	54788		5060	140:26	(spp_sip) Method is unknown
2017-07-20 08:31:30	2	UDP	Potentially Bad Traffic	163.172.17.76	59571		5060	140:26	(spp_sip) Method is unknown