# KAPITEL 7 / *CHAPTER 7* [7]
# MODERN INTRUSION DETECTION AND PREVENTION SYSTEMS: ARCHITECTURE, TOOLS, AND ANALYTICAL METHODS

**DOI: 10.30890/2709-2313.2025-40-02-026**

## Introduction

In the evolving landscape of cybersecurity threats, the role of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) has become increasingly critical. As digital infrastructures grow more complex, traditional protective mechanisms are no longer sufficient to guard against sophisticated attacks. IDS and IPS technologies provide enhanced visibility into network activities and offer real-time mechanisms for detecting and mitigating threats. This monograph section provides an in-depth analysis of modern IDS/IPS systems, architecture, operating principles, and deployment models. It clarifies the conceptual and functional distinctions between IDS and IPS, emphasizing their complementary roles in network defense. The text then explores widely implemented tools such as Snort, Suricata, McAfee Network Security Platform, and Zeek, highlighting their features, performance characteristics, and practical limitations [1–5]. A comparative evaluation of these systems reveals shared shortcomings, including system complexity and performance trade-offs. Furthermore, the section examines essential tasks IDS/IPS systems perform and outlines criteria for choosing an optimal solution. Special attention is given to attack detection methods – including anomaly, signature, and policy-based approaches – and the advantages of combining these techniques. Finally, structured models for data analysis are proposed to enhance the adaptability and precision of intrusion detection and prevention mechanisms [6–9].

## 7.1. The Concept of IDS/IPS and Their Role in Modern Communication Systems

IDS stands for Intrusion Detection System, and IPS refers to the Intrusion

[7]***Authors:*** *Korobeinikova Tetiana Ivanivna*
***Number of characters:*** *29386*
***Author's sheets:*** *0,73*

Prevention System. Compared to traditional security tools such as antivirus software, spam filters, and firewalls, IDS/IPS provides a significantly higher level of network protection. Today, firewalls operating with IPS and IDS systems are key to detecting and defending against malicious activities. IPS and IDS systems are relatively easy to configure, simple to manage, and capable of delivering high accuracy in network monitoring. These systems offer a range of valuable features.

1. Signature Detection – network traffic is analyzed for matches against known attack profiles (patterns). This enables the identification of attacks, malicious code, false traffic, and other threats. It is suitable for detecting and blocking known threats.

2. Anomaly-Based Detection – these systems can detect known patterns and novel (non-signature-based) attack variants. This typically involves the use of artificial intelligence and machine learning models.

3. Real-Time User Activity Monitoring – the algorithms collect data about traffic and conduct a comprehensive analysis. This allows not only for identifying issues but also for precisely determining their source, timing, and method of attack.

IDS monitors traffic by comparing it to its internal database of known network attacks and baseline network behavior. This operational mechanism allows for the detection of: network attacks; unauthorized access to data; malicious scripts and programs; port scanning tools; violations of security policies; connections to botnet command and control centers and mining pools; and anomalous activity. Security policy violations can be detected by implementing custom detection patterns, which help track specific network behavior. It is important to note that an IDS system does not block attacks but merely detects and reports them to the administrator, aiding in identifying and eliminating the root cause [10]. IDS tools can be used independently or integrated into firewall systems.

IPS compares traffic against known network attack patterns to detect: changes in network traffic trends; attempts at unauthorized access; and attempts to access hazardous resources from within the organization's network. IPS can detect risks across various layers and automatically respond to them by blocking malicious traffic and generating security events for the administrator. Therefore, IPS is considered an active

protection tool. IPS functions as a second line of defense positioned behind or integrated within the firewall [11].

The key difference between the systems lies in their response to information security violations. IDS is a monitoring tool that only recognizes suspicious activity and alerts the administrator. IPS, on the other hand, is a more comprehensive mechanism. It detects threats and immediately initiates countermeasures, such as terminating a connection or blocking the sender's IP address. In addition to the differences in response mechanisms to malicious or suspicious traffic, IDS and IPS differ in their deployment within the network infrastructure and their relation to network traffic. Typically, IDS systems are installed off-path from the network flow, processing a copy of the traffic passing through the network. In contrast, IPS systems are usually deployed in-line, directly in the traffic path as it passes through active network devices [12] (Figure 1).

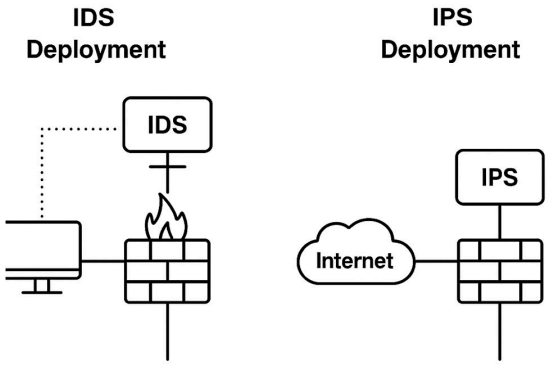


**Figure 1 – Difference Between IDS and IPS Deployments**

In this case, the advantages of IDS lie in the following: When the resources available to security tools for traffic processing are exhausted, an IDS will not affect network traffic throughput. On the other hand, an IPS installed in line with traffic flow becomes a potential bottleneck in the security system. When integrated as a module within a firewall, an IPS imposes an additional load on the firewall hardware and is often part of a Next Generation Firewall (NGFW).

## 7.2. Overview of Well-Known Intrusion Detection and Prevention Systems and Their Operational Algorithms

Snort is a classic Network Intrusion Detection System (NIDS). It is open-source software capable of operating on various operating systems and was initially developed in 1998. Originally designed as standalone software, Snort was acquired by Cisco in 2008, which is now its active partner and developer. Snort is better suited for small and medium-sized enterprises. The utility includes a packet sniffer, supports rule configuration, and offers extensive functionality. Snort is a tool for those seeking a clear and functional intrusion prevention system. Snort supports logging, content analysis, and content-based searches. It is applied for active blocking and passive detection of various attacks and probes. Snort can detect noise attacks –when an attacker sends suspicious packets to a target system and launches the attack amidst the resulting noise.

Of course, Snort does not guarantee the detection of all suspicious events, but in reality, no system currently does. Snort can be bypassed in multiple ways. For example, when using exploits, Snort may detect suspicious code by analyzing NOPs, but the code can be modified to render the malicious packets undetectable by IDS. Snort operates as follows: when a packet enters the system, it sequentially passes through decoders and preprocessors, and only then reaches the detection engine, where rules are applied. The decoders' task is to extract the network and transport layer data (e.g., IP, TCP, UDP) from the data link layer protocols (e.g., Ethernet, 802.11, Token Ring). The task of the preprocessors is to prepare data from the transport and network layers for rule application. For instance, a TCP preprocessor may handle tasks such as: State monitoring (ensuring protocol compliance), Session reassembly (reconstructing data from multiple session packets), and Protocol normalization.

Proper configuration of preprocessors can significantly improve the system's performance and reduce the amount of irrelevant data reaching the detection engine. Due to the architecture's flexibility, custom preprocessors can be easily integrated with Snort. As a result, before entering the detection engine, "super packets" are formed, to

which the rules are applied. The rule application process involves matching predefined signatures against the super packet. The rules include traffic, signatures, threat descriptions, and corresponding detection responses [12].

Suricata is a high-performance, open-source network threat detection and analysis engine widely used by private and public organizations and implemented by major vendors to protect their assets. Suricata can function both as an IDS and an IPS. It was developed by the Open Information Security Foundation (OISF) and is a free tool suitable for both small and large enterprises. The system uses a rule set and a signature language to detect and prevent threats. Suricata is compatible with Windows, Mac, Unix, and Linux. Suricata contains very little legacy code and incorporates newer developments than its competitors, allowing for faster performance.

Additionally, it offers compatibility with standard log analysis utilities, supporting the same modules as Snort. Suricata supports two IPS modes: NFQ and AF_PACKET. The NFQ IPS mode operates as follows:

1) The packet reaches the iptables.
2) An iptables rule directs it to the NFQUEUE (e.g., `iptables -I INPUT -p tcp -j NFQUEUE`);
3) From the NFQUEUE, packets are passed to user space, where Suricata processes them;
4) Suricata evaluates packets based on configured rules and returns one of three verdicts: `NF_ACCEPT`, `NF_DROP`, or `NF_REPEAT`;
5) Packets marked as `NF_REPEAT` can be flagged in the system and redirected to the beginning of the iptables chain, allowing further rule-based actions.

Starting from version 1.4, Suricata supports IPS functionality using the zero-copy mode with the AF_PACKET system, though with some limitations. The system must operate as a gateway with two network interfaces. A packet subject to a DROP rule will not be forwarded to the second interface. The advantage of zero-copy lies in its packet processing speed [11].

McAfee Network Security Platform. McAfee Network Security Platform is most

suitable for large organizations capable of allocating a substantial budget for network protection, with pricing starting at \$10,000. This cost is justified by its extensive capabilities, such as blocking many threats, restricting access to malicious websites, and preventing DDoS attacks. Due to its robust functionality, McAfee's platform may slow down network performance, requiring a trade-off between integration with other services and maximum security. The solution allows blocking new and unknown attacks by analyzing traffic with and without signatures. Signature-less intrusion detection technology enables the identification and blocking of previously unknown threats. The McAfee Threat Intelligence Exchange integration enables real-time threat awareness across physical and virtual networks. Additional integration with McAfee Advanced Threat Defense and McAfee MOVE AntiVirus (a component of McAfee Cloud Workload Security) allows organizations to automate complex security processes within a software-defined data center. Key features include: SSL decryption for inspection of inbound and outbound network traffic; Centralized management to optimize information gathering and control; Integration with McAfee's broader ecosystem for end-to-end protection from devices to the cloud.

Zeek (formerly known as Bro) is an open-source network traffic analyzer. The tool monitors network traffic and supports both standard intrusion detection mode and signature-based detection. Zeek can also detect events and allows for the creation of custom policy scripts. Free software is designed to extract hundreds of network data fields in real time. Zeek comes with built-in analyzers for many protocols (e.g., HTTP, SSL, DNS, FTP) and supports the development of custom analyzers for protocols not yet natively supported. While Zeek can detect anomalies, it does so differently from traditional IDS tools such as Suricata. Zeek duplicates the router in the network to capture a copy of the traffic. It then processes, analyzes, and structures the data according to protocols. The processed data is saved in various log files (e.g., `dns.log`, `http.log`, `conn.log`). A SIEM platform typically ingests these log files. Zeek is an excellent network data source for threat hunting, monitoring, and analysis. When properly configured, it does not interfere with the network or overwhelm security teams with irrelevant data. It extracts key fields from traffic and provides structured and

meaningful information that can be used to generate actionable detections for enhanced network protection.

## 7.3. Comparative Analysis of IPS/IDS Systems and Identification of Their Drawbacks

Snort remained the leader among intrusion detection and prevention systems for a long time. However, with the advancement of technologies, the emergence of multi-core processors, the transition to IPv6, the proliferation of user applications, and increased traffic volumes, Snort has not fully adapted to the new conditions. Although it has added support for IPv6 and application layer inspection, Snort remains single-threaded, significantly limiting its performance.

An alternative to Snort is Suricata. The key difference lies in Suricata's multi-threaded architecture, which enables it to utilize multiple CPU cores simultaneously, providing better load distribution. This allows for processing a greater volume of data without being constrained by the number of rules applied, giving Suricata a slight performance advantage over Snort. One of Suricata's strengths is that it also leverages most of the rule sets developed for Snort in addition to its unique features. Suricata outputs event data in JSON format, greatly simplifying its integration with third-party tools, including log visualization and monitoring platforms like Kibana. Another significant advantage of Suricata is its ability to operate at Layer 7 of the OSI model, enhancing its capacity to detect application-level threats. In its rules, it is not necessary to strictly specify port numbers, as required in Snort; it is sufficient to define the protocol and action. Suricata's modules automatically analyze the traffic and identify the protocol, even if non-standard ports are used. A downside of Suricata is the large number of configuration options and somewhat lacking documentation in specific areas.

Zeek is an excellent tool for threat hunting. While many IDS tools (e.g., Suricata) focus on signature- and rule-based detection, Zeek can also be used this way; its strength lies in protocol-specific deep analysis. The more data available during threat

hunting, the better the outcome. Zeek's disadvantage is its lack of a graphical user interface and its emphasis on functionality, which can make it less accessible for general users.

McAfee Network Security Platform is a relatively expensive solution compared to open-source alternatives. However, it is significantly more effective in scenarios requiring maximum network protection. McAfee's key strength is its ability to operate with and without signatures, enabling it to detect previously unknown attacks. Its downside is the potential slowdown in network performance due to its extensive feature set.

The common shortcomings of modern IDS/IPS solutions include system or network performance degradation, extensive and complex configuration requirements, complexity of interface interaction, and system configuration being complex for inexperienced users.

## 7.4. Analysis of Tasks and Challenges in Modern Intrusion Detection and Prevention Systems

Identifying the specific tasks IPS/IDS systems perform makes it possible to formulate the key requirements for selecting a particular solution. Intrusion detection systems perform two primary functions. First, they collect evidential data for incident investigation (e.g., in cases where an attacker maintains prolonged access to an organization's resources). Second, they monitor for malicious activity. Therefore, the main requirements for IDS are comprehensive coverage of known exploits and vulnerabilities (i.e., up-to-date signature databases) and system persistence, meaning the ability to collect relevant information continuously. Ideally, the system should also be capable of detecting previously unknown vulnerabilities and attacks – i.e., operate in a signature-less mode.

Intrusion prevention systems, in turn, focus on traffic normalization, attack blocking, and damage mitigation. The requirements for IPS differ somewhat. First, reliability is crucial – system operation must not be interrupted. Malfunctions may lead

to serious consequences such as connection loss or denial-of-service (DoS). Second, the system must maintain a low rate of false positives. Beyond reliability, one of the primary requirements for intrusion detection and prevention systems is to ensure high network throughput performance. In other words, such systems must not interfere with the regular operation of the network.

Additionally, the system should offer flexible configuration options and generate clear output for users and third-party visualization tools. However, the availability of extensive configuration options should not result in excessive complexity, and the user interface must remain accessible and understandable. Thus, the requirements for an ideal or near-ideal intrusion detection and prevention system may be summarized as follows: the current signature database is for detecting all known threats and vulnerabilities; capability to detect previously unknown attacks and vulnerabilities (signature-less detection); system reliability and continuity, ensuring uninterrupted data collection; low false positive and error rate; high network throughput; flexible configuration and functionality, including support for multiple operational modes; ease of use for both users and third-party tools; user-friendly interface.

### 7.5. Attack Detection Methods in IDS/IPS Systems

In general, attack detection methods can be categorized into three main groups: anomaly-based detection methods, signature-based detection methods, and policy-based detection methods. The anomaly-based method helps to detect suspicious activity in the network and on individual hosts. To apply this method, data on regular system operation is first collected and stored in profiles. Detection modules then use these profiles to analyze current activity and compare it against the established norm. This method does not require an extensive signature database, which is a clear advantage. However, it also tends to generate a high number of false positives. The signature-based method analyzes all traffic by comparing it to existing signature patterns that indicate specific attacks. Compared to the anomaly-based method, this approach generally produces fewer false positives. However, an extensive and

frequently updated signature database must ensure comprehensive coverage of known threats. The policy-based method requires predefined and explicitly configured network security rules, according to which traffic is analyzed. These rules may specify host interaction policies, allowed ports and protocols, access timeframes, etc. This method is highly flexible, as policies can be tailored to the specific needs of each organization. However, such customization requires prior experience and a thorough analysis of the organization's operational characteristics [9].

### 7.6. Data Processing and Analysis Using a Combined Signature-Policy Method

IDS/IPS systems are highly flexible tools that allow for the use of combined attack detection methods. One practical approach is the combination of signature-based and policy-based methods. In this setup, the system can identify and block suspicious traffic using signatures while verifying the result against predefined policies. Let us examine this method in more detail. Figure 2 illustrates the combined detection method using both signature and policy analysis.

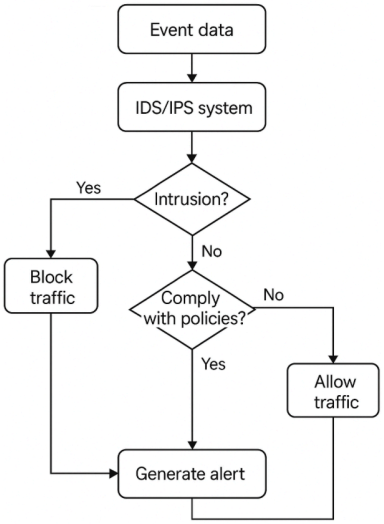


**Figure 2 – Diagram of the Combined Signature and Policy Detection Method**

In the first stage, the IDS/IPS system collects data about each event. This data includes the sender and receiver IP addresses, their ports, the protocol used, and the

timestamp of the event. Next, the system analyzes the data using predefined signatures to determine whether an intrusion occurs. The traffic is blocked if an intrusion is detected, and a corresponding alert is generated. If not, the traffic is permitted, and the event is passed to the following policy compliance analysis stage. At the policy analysis stage, the event is checked against predefined rules. For example, specific IP address ranges may be allowed or denied; particular hosts or networks may be permitted to connect only via specific ports, protocols, or certain times. This dual-layer analysis not only enables effective detection through signatures but also allows system customization through organizational policies. However, detailed work is required to define and maintain these policies based on the organization's needs.

## 7.7. Method for Analyzing Data from IDS/IPS Systems

Data analysis from IDS/IPS systems refers to examining and processing all data operated on and produced jointly by IDS/IPS components functioning as a unified system. The relevant dataset (D) includes: d1 – whether a connection was established, d2 – sender IP address, d3 – receiver IP address, d4 – sender port, d5 – receiver port, d6 – protocol used, d7 – internal (home) network IP addresses, d8 – trusted IP addresses and their allowed ports and protocols, d9 – blocked IP addresses.

The data can be divided into two groups: d1–d6 – acquired directly from the IDS/IPS system; d7–d9 – derived from configured security settings.

These data points are used in specific tasks (T) that generate recommendations (R). The tasks include: t1 – if no connection was established, determine whether both sender and receiver belong to the internal network (uses d1, d2, d3, d7); t2 – if a connection was established and the receiver belongs to the internal network, determine whether the sender is on the blocked list (uses d1, d2, d3, d7, d9); t3 – if a connection was established, the receiver is internal, and the sender is trusted, verify whether the sender used an allowed port (uses d1, d2, d3, d5, d7, d8); t4 – if a connection was established, the receiver is internal, and the sender is trusted, verify whether the sender used an allowed protocol (uses d1, d2, d3, d6, d7, d8); t5 – if no threat is detected,

verify whether all security settings have been fully configured (uses d7, d8, d9).

Each task generates a corresponding recommendation: r1 (from t1): No threat – connection between internal hosts blocked; recommended to review rules and security settings; r2 (from t2): High threat level – a blocked host accessed the internal network; recommended to define access-restricting rules immediately; r3 (from t3): Medium threat level – a trusted host accessed the internal network via a prohibited port; recommended to restrict access via rule configuration; r4 (from t4): Medium threat level – a trusted host accessed the internal network via a prohibited protocol; recommended to restrict access via rule configuration; r5 (from t5): Low threat level – incomplete security settings; recommended to complete configuration to enable accurate future recommendations.

A diagram of the method of analyzing data from intrusion detection and prevention systems is shown in Figure 3.

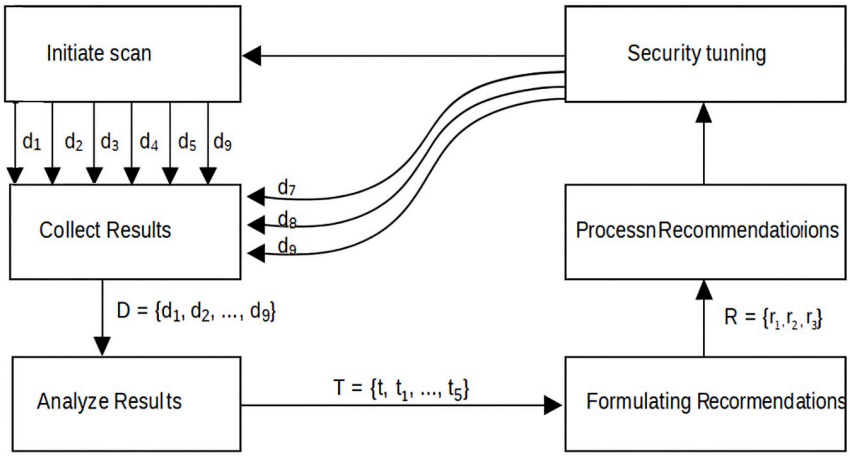


**Figure 3 – Diagram of the Data Analysis Method from IDS/IPS Systems**

Intrusion detection and prevention systems rely on three core attack detection methods: anomaly-based, signature-based, and policy-based. These allow the systems to identify threats and suspicious activities within a network environment. For improved reliability and security, signature-based and policy-based methods are recommended. With this approach, the IDS/IPS system analyzes traffic using signature matching, while subsequent policy-based analysis interprets the results in the context of predefined organizational rules. This layered detection strategy enhances accuracy

and allows system customization based on the network's specific needs.

## Summary and conclusions

The comprehensive analysis presented in this section confirms the indispensable role of IDS and IPS technologies in modern cybersecurity frameworks. Network defense mechanisms must evolve accordingly as attack vectors become more diverse and sophisticated. IDS and IPS systems detect malicious behaviors and can prevent data breaches and service disruptions when configured effectively.

Each reviewed technology – Snort, Suricata, McAfee, and Zeek – demonstrates distinct strengths. Snort offers clarity and community-driven rule development; Suricata excels in multi-threaded performance and deep packet inspection; McAfee provides enterprise-grade protection with advanced threat intelligence; and Zeek offers highly customizable protocol-level analysis. Despite these advantages, all systems exhibit limitations: resource intensity, configuration complexity, and usability barriers for non-expert users. To address these challenges, future IDS/IPS implementations should focus on the following priorities: Integration of multiple detection methods to improve coverage and reduce false positives; Real-time adaptability to detect zero-day exploits; Modular architectures that support automation and scalability; User-centric design with intuitive interfaces and standardized outputs for SIEM systems.

Ultimately, the ideal IDS/IPS solution must combine high detection accuracy with operational efficiency, policy flexibility, and user-friendly configuration. Leveraging combined signature- and policy-based methods, along with structured data analysis, enhances the resilience of network defense systems and ensures a more proactive and intelligent cybersecurity posture for organizations of all sizes.