STAMUS NETWORKS

IDS Detection Types

Visibility is the first step in effective security monitoring. That's why it is no surprise that intrusion detection systems (IDS) have become an incredibly popular first line of defense for many organizations around the world.

This guide provides an introduction to IDS types, detection methods, and alerts while also highlighting alternative means of network security that might benefit organizations looking for IDS detection without IDS challenges.

IDS Detection Types

What is IDS/IPS?

An intrusion detection/prevention system in cyber security is a security mechanism employed to safeguard computer networks and systems from unauthorized access and malicious activity. Both IDS and IPS are commonly used as a first line of defense for many organizations. Intrusion detection techniques often include monitoring traffic, comparing traffic to a set of predefined rules or signatures, and then issuing alerts when traffic matches a malicious pattern.

Intrusion detection usually concentrates on identifying and reporting potential security breaches, while intrusion prevention seeks to actively block threats. Early detection of intrusions allows security teams to take action and minimize damage. This can involve isolating infected devices, blocking attackers, or launching incident response procedures.

What is the difference between IPS and IDS?

and come with their own benefits and challenges.

- **Intrusion Detection System (IDS):** Intrusion detection system software continuously analyzes network traffic or system activity for suspicious patterns that might indicate an ongoing attack. These patterns can be identified through signature-based detection, which matches traffic against known attack signatures, or anomaly-based detection, which looks for deviations from regular behavior. Upon detecting suspicious activity, an IDS can raise alerts, log events, and provide valuable insights for security personnel to investigate and respond to potential threats.
- **Intrusion Prevention System (IPS):** An IPS extends the functionality of IDS by actively taking steps to prevent intrusions. Based on predefined security policies and identified threats, an IPS can block malicious traffic, terminate suspicious connections, or otherwise disrupt the attacker's progress. This can involve techniques like packet filtering, which blocks unwanted traffic based on pre-defined rules, or deep packet inspection, which examines the content of packets for malicious payloads. It is important to note that one of the challenges with IPS is the possibility of non-malicious traffic being blocked based on a "false positive."

What are the two main types of intrusion detection systems?

There are two main types of Intrusion Detection Systems (IDS) based on their deployment and data source:

1. Network Intrusion Detection System (NIDS): NIDS act as network monitoring devices deployed at strategic points within a computer network. Their primary function is to continuously capture and analyze network traffic data traversing a specific network segment. NIDS can be implemented in two primary ways:

- **Dedicated hardware appliances:** These are specialized devices solely designed to perform NIDS functions.
- **Software applications on network servers:** Existing network servers can be leveraged to host NIDS software, enabling them to perform network traffic analysis alongside other server functionalities.

its intended recipient. NIDS employs two main techniques for analyzing captured network traffic data: signature-based detection and anomaly-based detection.

2. Host-Based Intrusion Detection System (HIDS): In contrast to NIDS which focuses on network traffic analysis, HIDS provides security for individual devices (hosts) within the network. HIDS function as software agents deployed directly on the operating system of the host device itself. Their primary function is to monitor and analyze activity occurring on the host device. HIDS are deployed as software agents on individual servers, desktops, or laptops within the network. A single HIDS agent is typically installed on each host device for dedicated monitoring.

HIDS collects data from various sources on the host device, including:

- System logs: These logs record events and activities within the operating system of the host device.
- File access attempts: HIDS monitors attempts to access files on the host device, including successful and failed attempts.
- Running Processes: HIDS maintains a record of processes currently running on the host device.

HIDS primarily utilizes anomaly-based detection techniques. By analyzing the collected data, HIDS establishes baselines for typical host activity. Significant deviations from these baselines, such as unusual file access attempts or unexpected processes running, can indicate potential intrusions or suspicious behavior.

What are the methods of IDS/IPS detection?

There are three primary methods of IDS/IPS detection: anomaly-based, signature-based, and hybrid. These methods define how the IDS analyzes data to identify potential intrusions.

1. Anomaly-Based IDS: Anomaly-based IDS focuses on identifying deviations from normal behavior within a network or system. It works by establishing a baseline for normal activity by statistically analyzing network traffic or system activity over time. This baseline becomes a reference for identifying anomalies. The IDS then continuously monitors network traffic or system activity and

2. **Signature-Based IDS:** A signature-based intrusion detection system relies on a predefined database of attack signatures to identify malicious activity. These signatures represent known patterns or fingerprints of network attacks or suspicious system behavior. The IDS continuously monitors network traffic or system activity and compares this data against the database of attack signatures. Any matches trigger an alert, indicating a potential intrusion attempt.
3. **Hybrid IDS:** A hybrid intrusion detection system combines both anomaly-based and signature-based detection methods to address the limitations of each approach. A hybrid system leverages signature-based detection for known threats and anomaly-based detection for novel attacks. This enhances the overall effectiveness of intrusion detection.

Each of these three detection methods (Anomaly-based, Signature-based, Hybrid) offers different strengths and weaknesses. Choosing the most suitable approach depends on factors like the specific security requirements of the network, the resource availability for managing the IDS, and the acceptable level of false positives.

It is also important to consider switching to a more advanced modern network security solution, such as network detection and response (NDR). The Stamus Security Platform (SSP) is a modern NDR solution that leverages the best from IDS technology without the same challenges faced by IDS users. Learn more at https://www.stamus-networks.com/stamus-security-platform

What is the most common detection method used by an IDS?

The most common detection method used by an IDS is signature-based detection.

Here's why:

- **Effectiveness against known threats:** A signature-based intrusion detection system excels at identifying well-established attack patterns with known signatures in its database. This allows for fast and accurate detection of common threats.
- **Lower processing overhead:** Matching traffic against predefined signatures is computationally less intensive compared to the analysis required for anomaly-

However, it's important to note that signature-based detection has limitations:

- **Blindness to zero-day attacks:** New and unknown attacks lack established signatures, making them invisible to this method.
- **Maintenance needs:** Signature databases require constant updates with new threat signatures to maintain effectiveness.

What are the different types of IDS alerts?

IDS alerts can be categorized based on their accuracy in reflecting actual threats. There are four main types of IDS alerts regardless of the type of intrusion detection system:

- **True Positive:** This is the ideal scenario where the IDS correctly identifies malicious traffic and raises an alert. This allows security personnel to investigate and respond to a genuine threat.
- **False Positive:** This occurs when the IDS mistakenly flags normal traffic as suspicious. This can be caused by outdated signatures, misconfigured rules, or unusual but legitimate network activity. False positives waste time and resources for security teams.
- **False Negative:** This is a critical situation where the IDS fails to detect actual malicious activity. This can happen if the attack uses a novel method without a known signature or if the IDS configuration is inadequate.
- **True Negative:** This represents the most desirable outcome where the IDS correctly identifies normal traffic and doesn't raise unnecessary alerts. This contributes to a smooth workflow for security personnel.

What are the types of computer attacks detected by IDS?

An IDS can detect a wide range of computer attacks by analyzing network traffic or system activity for suspicious patterns. Here are some common types of intrusions in cybersecurity that IDS systems are designed to identify:

mapping attempts.

- **Denial-of-Service (DoS) attacks:** These attacks aim to overwhelm your system with traffic, making it unavailable to legitimate users. IDS can detect flooding attacks like SYN floods and UDP floods.
- **Social Engineering Attacks:** While not directly detectable through network traffic analysis, IDS can flag anomalies associated with social engineering attempts. This may include unusual access attempts, phishing emails triggering downloads, or suspicious data transfers.
- **Malware:** IDS can identify attempts to download or install malware by looking for known malware signatures or suspicious file transfers.
- **Exploits:** These attacks leverage software vulnerabilities to gain unauthorized access. IDS can detect exploit attempts by monitoring network traffic for patterns associated with known vulnerabilities.
- **Privilege Escalation:** These attacks involve attackers trying to gain higher privileges within a system. IDS can flag suspicious user activity or access attempts to critical resources.
- **Insider Threats:** While more challenging to detect definitively, IDS can identify unusual activity patterns that might indicate insider threats, such as unauthorized access attempts from trusted accounts or data exfiltration attempts.

It's important to remember that IDS effectiveness depends on its configuration and the type of attack. While some attacks leave clear signatures, other more subtle attack signals such as homoglyphs and C2 beaconing are likely to be missed. That is why it is important to consider switching from IDS to a modern network detection and response (NDR) platform to make sure critical attack signals don't fly under the radar.

What are the three main methods used when evaluating IDS for effectiveness?

The three main methods used when evaluating IDS for effectiveness are the detection/false positive rate, false negative/time to detect rate, and scenario-based testing. Let's take a look at each:

1. Detection Rate and False Positive Rate:

involves analyzing two key metrics:

- **Detection Rate (DR):** This measures the percentage of actual attacks successfully detected by the IDS. A high DR indicates good sensitivity in catching threats.
- **False Positive Rate (FPR):** This measures the percentage of normal activities mistakenly flagged as suspicious by the IDS. A low FPR is crucial to avoid overwhelming security personnel with unnecessary alerts.

Evaluating these metrics together helps assess the trade-off between catching threats and generating false alarms. A good IDS should have a high DR and a low FPR.

2. False Negative Rate and Time to Detection:

This method focuses on the speed and accuracy of the IDS in identifying threats. It involves analyzing two additional metrics:

- **False Negative Rate (FNR):** This measures the percentage of actual attacks that the IDS misses entirely. A low FNR is essential to avoid leaving your system vulnerable.
- **Time to Detect (TTD):** This measures the time taken by the IDS to detect and raise an alert for an attack. A low TTD allows for faster response and minimizes potential damage.

Evaluating these metrics helps assess the IDS's responsiveness and ability to minimize the window of opportunity for attackers.

3. Scenario-Based Testing:

This method involves simulating real-world attack scenarios against the IDS. This can be done using pre-recorded attack data or specialized testing tools. Scenario-based testing helps assess the IDS's effectiveness against various attack types and its ability to adapt to evolving threats.

comprehensive understanding of an IDS's strengths and weaknesses, allowing them to choose the most suitable solution for their specific needs.

Explore a modern alternative

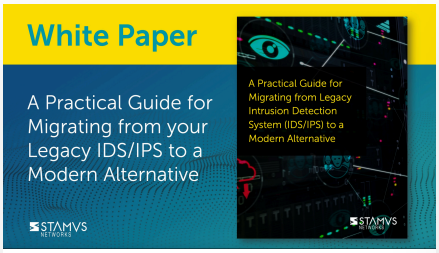
IDS is undoubtedly a powerful and effective means to detect known threats on your organization's network. Unfortunately, most IDS deployments are riddled with false positives, provide limited threat detection, and lack sufficient visibility into anomalous activity and subtle attack signals. Traditional IDS vendors have failed to innovate in ways that solve these challenges, leading to inefficient or downright ineffective threat detection.

You need a network security platform that doesn't generate an endless stream of useless alerts across part of your network, and instead automatically identifies alerts of interest and notifies you of only serious and imminent threats. Your organization deserves response-ready detection with visibility into your entire network regardless of the environment with easy access to all the contextual evidence you need to stop an attack before it can cause damage. Replace your legacy IDS with a modern network detection and response platform that gives you these features and more.

The Stamus Security Platform™ is a network-based threat detection and response solution that eliminates the challenges of legacy IDS while lowering your response time. Stamus Security Platform harnesses the full potential of your network, bringing state-of-the-art threat detection, automated event triage, and unparalleled visibility to the security team.

Book a demo to see if Stamus Security Platform is right for your organization.

Learn more about upgrading your IDS

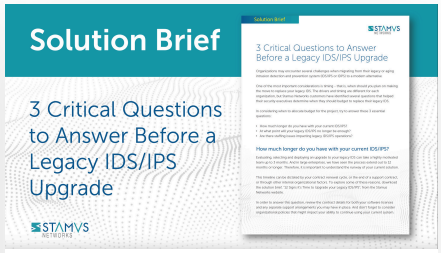


A Practical Guide for Migrating from y IDS/IPS

Download

12 Signs it's Time to Upgrade your /IPS

Download



3 Questions to Answer Before Upgrade

Download

Experience Stamus Security Platform Live

REQUEST A DEMO

platform, company, or technology. That's why we leverage the power of community to deliver the next generation of open and transparent network defense. Trusted by security teams at the world's most targeted organizations, our flagship offering – Clear NDR™ – empowers cyber defenders to uncover and stop serious threats and unauthorized network activity before they harm their organizations. Clear NDR helps defenders see more clearly and act more confidently through detection they can trust with results they can explain.

Indianapolis, USA

Paris, France

contact@stamus-networks.com

Privacy