This content is part of the Essential Guide:

Unified threat management devices: Understanding UTM and its vendors

DEFINITION

intrusion detection system (IDS)

Posted by: Margaret Rouse WhatIs.com

Contributor(s): Linda Rosencrance

An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. While anomaly detection and reporting is the primary function, some intrusion detection systems are capable of taking actions when malicious acitivity or anomalous traffic is detected, including blocking traffic sent from suspicious IP addresses.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also prone to false alarms (false positives). Consequently, organizations need to fine-tune their IDS products when they first install them. That means properly configuring their intrusion detection systems to recognize what normal traffic on their network looks like compared to potentially malicious activity.

An intrusion prevention system (IPS) also monitors network packets for potentially damaging network traffic. But where an intrusion detection system responds to potentially malicious traffic by logging the traffic and issuing warning notifications, intrusion prevention systems respond to such traffic by rejecting the potentially malicious packets.

Different types of intrusion detection systems

Intrusion detection systems come in different flavors and detect suspicious activities using different methods, including the following:

- A network intrusion detection system (NIDS) is deployed at a strategic point or points within the network, where it can monitor inbound and outbound traffic to and from all the devices on the network.
- Host intrusion detection systems (HIDS) run on all computers or devices in the network with direct access to both the internet and the enterprise internal network. HIDS have an advantage over NIDS in that they may be able to detect anomalous network packets that originate from inside the organization or malicious traffic that a NIDS has failed to detect. HIDS may also be able to identify malicious traffic that originates from the host itself, as when the host has been infected with malware and is attempting to spread to other systems.
- Signature-based intrusion detection systems monitor all the packets traversing the network and compares them against a database of signatures or attributes of known malicious threats, much like antivirus software.
- Anomaly-based intrusion detection systems monitor network traffic and compare it against an established baseline, to determine what is considered normal for the network with respect to bandwidth, protocols, ports and other devices. This type of IDS alerts administrators to potentially malicious activity.

Historically, intrusion detection systems were categorized as passive or active; a passive IDS that detected malicious activity would generate alert or log entries, but would take no actions. An active IDS, sometimes called an intrusion detection and prevention system, would generate alerts and log entries, but could also be configured to take actions, like blocking IP addresses or shutting down access to restricted resources.

Snort, one of the most widely used intrusion detection systems is an open source, freely available and lightweight NIDS that is used to detect emerging threats. Snort can be compiled on most Unix or Linux operating systems, and a version is available for Windows as well.

providing some or all of these functions to security professionals:

- monitoring the operation of routers, firewalls, key management servers and files that are needed by other security controls aimed at detecting, preventing or recovering from cyberattacks;
- providing administrators a way to tune, organize and understand relevant operating system audit trails and other logs that are often otherwise difficult to track or parse;
- providing a user-friendly interface so non-expert staff members can assist with managing system security;
- including an extensive attack signature database against which information from the system can be matched;
- recognizing and reporting when the IDS detects that data files have been altered;
- generating an alarm and notifying that security has been breached; and
- reacting to intruders by blocking them or blocking the server.

An intrusion detection system may be implemented as a software application running on customer hardware, or as a network security appliance; cloud-based intrusion detection systems are also available to protect data and systems in cloud deployments.

Benefits of intrusion detection systems

Intrusion detection systems offer organizations a number of benefits, starting with the ability to identify security incidents. An IDS can be used to help analyze the quantity and types of attacks, and organizations can use this information to change their security systems or implement more effective controls. An intrusion detection system can also help companies identify bugs or problems with their network device configurations. These metrics can then be used to assess future risks.

Intrusion detection systems can also help the enterprise attain regulatory compliance. An IDS gives companies greater visibility across their networks, making it easier to meet security regulations. Additionally, businesses can use their IDS logs as part of the documentation to show they are meeting certain compliance requirements.

Intrusion detection systems can also improve security response. Since IDS sensors can detect network hosts and devices, they can also be used to inspect data within the network packets, as well as identify the operating systems of services being used. Using an IDS to collect this information can be much more efficient that manual censuses of connected systems.

IDS versus IPS

An intrusion prevention system (IPS) is similar to an intrusion detection system, but differs in that an IPS can be configured to block potential threats. Like intrusion detection systems, an IPS can be used to monitor, log and report activities, but it can also be configured to stop threats without the involvement of a system administrator. However, organizations should be careful with IPSes because they can also deny legitimate traffic if not tuned accurately.

Margaret Rouse asks:

What benefits does your enterprise get from using intrusion detection systems?

Join the Discussion

An IDS is aimed at analyzing whole packets -- header and payload -- looking for known events. When it detects a known event, the system generates a log message detailing that event. The IDS compares the inbound traffic against the database of known attack signatures and reports any attacks it detects. An IDS warns of suspicious activity taking place, but it doesn't prevent them as does an IPS. The major flaw of an IDS is that it can produce false positives.

An intrusion prevention system is typically located between a company's firewall and the rest of its network and may have the ability to stop any suspected traffic from getting to the rest of the network.

Intrusion prevention systems execute responses to active attacks in real time. Because system administrators structure rules within the IPS that address the needs of the business, the system can monitor and evaluate threats, as well as take action in real time to stop immediate threats. An IPS actively catches intruders that firewalls or antivirus software may miss.

Continue Reading About intrusion detection system (IDS)

- Learn the basics of how network intrusion prevention systems work
- Find out how to use intrusion detection systems to prevent incidents, improve ROI
- Learn about how intrusion preventions systems can benefit the enterprise
- Read how to build intrustion detection and prevention systems in the cloud
- The National Institute of Standards and Technology's "Guide to Intrusion Detection and Prevention Systems (IDPS)"

Related Terms

cryptographic nonce

A nonce is a random or semi-random number that is generated for a specific use, typically related to cryptographic communication ... See complete definition

Diffie-Hellman key exchange (exponential key exchange)

Diffie-Hellman key exchange, also called exponential key exchange, is a method of digital encryption that uses a number raised to... See complete definition

Great Firewall of China

The Great Firewall of China is a country wide firewall that restricts content that is censored by the Chinese Government, ... See complete definition

Join the conversation

2 comments

Share your comment

Add My Comment

Oldest ▼

[-] **Margaret Rouse**

- 29 May 2007 2:48 PM

What benefits does your enterprise get from using intrusion detection systems?

Reply

[-] **ceekaygee**

- 17 May 2018 11:50 PM

Good work here! Please, I need a report on design and implementation of an IDS that secures a school's result database for my final year project. Thanks.

Reply

CLOUD SECURITY NETWORKING CIO ENTERPRISE DESKTOP CLOUD COMPUTING COMPUTER WEEKLY

SearchCloudSecurity

Top 4 strategies for cloud security automation

Automating security in the cloud can be invaluable for threat detection and mitigation. These are the key focal areas where ...

UpGuard security researchers found publicly exposed Amazon S3 buckets from data management firm Attunity, which included company ...

BACKGROUND IMAGE: iSTOCK/GETTY IMAGES

About Us Meet The Editors Contact Us Privacy Policy Videos Photo Stories Definitions

Guides Advertisers Business Partners Media Kit Corporate Site Contributors

CPE and CISSP Training Reprints Archive Site Map Events E-Products