Intrusion Detection System (IDS) &Intrusion Prevention System (IPS): Case Study

Asmaa Shaker Ashoor, Prof. Sharad Gore

Abstract: IPS and IDS both examine traffic looking for attacks but they are critically different. The differences between deployment of these system in networks in which IDS are out of band in system, means it cannot sit within the network path but IPS are in-line in the system, means it can pass through in between the devices.IDS generates only alerts if anomaly traffic passes in network traffic, it would be false positive or false negative, means IDS detects only malicious activities but no action taken on those activities but IPS has feature of detection and prevention with auto or manual action taken on those detected malicious activities like drop or block or terminate the connections. This paper discusses difference between Intrusion Detection system and intrusion Prevention System (IDS/IPS) technology in computer networks Here IDS and IPS systems stability, performance and accuracy wise result are comparing in this paper.

Keywords: IDS, IPS, threats, malicious activities, alerts

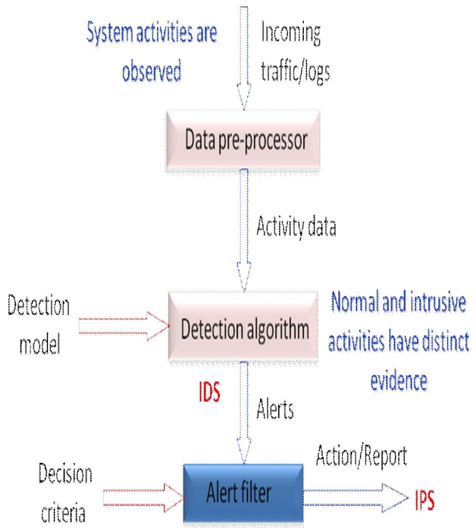
INTRODUCTION

Intrusion is a set of actions aimed at compromising the basic network security goals like confidentiality, integrity, availability of a computing/networking resource. Intrusion detection systems (IDS) are basically identifying intrusion threats, attacks and malicious activities in a network and generate alerts. The limitation of IDS is they cannot resolve network attacks; it passes in network for only watches network traffic like packet sniffing. The IDS are basically analyses the copied packets on the network segment for detecting attacks or attack has already taken place, this to alert network admin for what is happening in network Intrusion prevention system (IPS) is the process of both detecting intrusion activities or threats and managing responsive actions on those detected intrusions and threats throughout the network. IPS are monitoring real time packet traffic with malicious activities or which match specific profiles and will trigger the generation of alerts and it can drop, block that traffic in real time pass through in network. The mainly IPS counter measures is to stop an attack in progress.

“In simple terms, IDS may be perfectly suited for network attack monitoring and for alerting administrators of emerging threats. But its speed, performance and passive limitations have opened the door for IPS to challenge it as the proactive defense weapon of choice.” [http://www.infoworld.com/article/03/04/04/14ips-sb_1.html, April 04, 2003].

IDS and IPS terms under network security

In network security the firewall serves main purpose of security but it allows network traffic on specified ports to either in or out of the network. The firewalls cannot do to detect this network traffic sent on a particular port or legitimate port or part of an intrusion attempts or attacks. If, for example, allow remote access to an internal web server through allowing inbound access on TCP port 80, then an attacker could use this port to attack the Web server. In this case the IDS can distinguish traffic between the allowed connections to Web server or attempted attack to Web server by comparing the signature of the traffic to a database of known attack signatures. The IDS will notify such an attack enabling and generate alert for take appropriate action and IPS, on the other hand, take action on that detected attacked connections or drop / close this connection. Intrusion Detection and Intrusion Prevention Systems, IDS and IPS respectively, are network level defences deployed in thousands of computer networks worldwide. The basic difference between these two technologies are lies in how they provide protection for network environments with respect to detection and prevention terms. IDS generate only alerts or logs after threats or malicious activities are occurred. Intrusion Detection Systems simply detect possible intrusions and report this to network administrators.



Role of IDS and IPS technology in network security

The actual role of IDS and IPS in network security shows in above diagram with details. How this detection algorithm and alert filter works with predefined rule sets for generating activity data or alerts for take an appropriate action on intrusive activities. Intrusion Prevention Systems, IPS, perform the same analysis as Intrusion Detection Systems are detected because they are deployed in-line in the network, between other network components, they can take action on that malicious activity. Intrusion Prevention Systems will not only detect the intrusions but will take actions to like terminating the connection.

Difference between IDS and IPS systems

IDS and IPS are originally developed for addressing requirements of lacking in most firewalls. IDS are basically used to detecting the threats or intrusions in network segment. But IPS is focused on identifying those threats or intrusions for blocking or dropping their activities. The IDS and IPS are list of similar functions like packet inspection, stateful analysis, TCP segment reassembly, deep packet inspection, protocol validation, and signature matching.

Th best example of security gate in term of difference of IDS and IPS is, An IDS works like a patrol car within the border, monitoring activities and looking for abnormal situations. But an IPS operates like a security guard at the gate of allowing and denying access based on credentials and some predefined rule set, or policy. No matter how strong the security at the gate is, the patrols continue to operate in a system that provides its own checks.

Intrusion detection system (IDS)

The IDS is software or an appliance that detects a threat, unauthorized or malicious network traffic. IDS has their own predefined rule sets, through that it can inspect the configuration of endpoints to determine whether they may be susceptible to attack (this is known as host-based IDS), and also it can record activities across a network and compare it to known attacks or attack patterns (this is called network-based IDS). The purpose of intrusion detection is to provide monitoring, auditing, forensics, and reporting of network malicious activities.

- Preventing network attacks
- Identifying the intruders
- Preserving logs in case the incident leads to criminal prosecution

Intrusion prevention system (IPS)

The IPS are not only detect the bad packets caused by malicious codes, botnets, viruses and targeted attacks, but also it can take action to prevent those network activity from causing damage on network. The attacker's main motive is to take sensitive data or intellectual property, through that they interested in whatever they can get from customer data like employee information, financial records etc. The IPS is specified to provide protection for assets, resources, data, and networks.

- IPS stops the attack itself
- IPS changes the security environment

The differences of IDS & IPS are categorized in four objectives as Network Stability & Performance

The IDS are deployed out of band in network means it passes all network traffic to this system but not through in between devices, the processing capability is matching with average network load. The latency between capture and reporting can range from a few seconds to minutes, but also it also depends on human response time. The IDS are a logging device, the large memory buffers to absorb traffic bursts & average network loads. The IPS are deployed in-line in network means, it passes through in between the devices and which works in peak network load with large memory buffers to absorb traffic bursts is unacceptable. The latency is in microseconds which give the faster application response time with higher processing capacity.

Accuracy- False Positives

There are three basic rules to find accuracy with false positives in IDS and IPS:

- The IDS has minimizes false positives but an IPS have no false positives. This changes dramatically the writing and testing of the alert filters.
- The IDS false positive alerts on an intrusion that it can be or cannot be – succeed, but IPS false positive blocks legitimate traffic.
- The anomaly filters cannot be used for blocking.

Accuracy- False Negatives

The accuracy of false negatives is simply a missed attack. The goal of this type of system is based on coverage of high priority attacks. The IDS may become overwhelmed with traffic beyond its capacity, dropping packets needed to detect the attack and an IPS is overwhelming the device causes traffic to be blocked or dropped preventing the attack from succeeding to detect anomalies.

Data log analysis

The IDS and IPS devices are gives a comprehensive logs and data collection, its without actionable alerts, the data gathered from these devices and sensors throughout the network can be used for event correlation and network forensics in a post-attack scenario. This type of data is critical for analysis during and after attacks and can help for organization with both incident response and compliance audits.

Conclusion

Intrusion types of systems are put in place to serve a business needs for meeting an objective of network security. The IDS and IPS are to provide a foundation of technology meets to tracking, identifying network attacks to which detect through logs of IDS systems and prevent an action through IPS systems. If the host with critical systems, confidential data and strict compliance regulations, then it's a great to use of IDS, IPS or both in network environments. The basic benefits of IDS and IPS systems are as:

- Normal and intrusive malicious activities detected
- Proactive protection of network security infrastructure
- Operational efficiencies to reduced need to react to event logs for protection
- Increased coverage against packet attacks and zero-day attacks

The deterministic intrusion detection or prevention is the next generation firewall with deep packet inspection and sniffing in network. But it is not a silver bullet, to become a basic at the border and deeper in the network for "Defense in Depth."[1]

References

[1] Jennifer Jabbusch , "IDS vs. IPS: How to know when you need the technology", 22 November 2010

[2] Brian Smith, "IPS vs. IDS".

[3] Robert Drum," IDS & IPS Placement for network protection" , CISSP 26 March 2006.

[4] Pete Lindstrom, "Intrusion prevention systems (IPS): Next generation firewalls" , A Spire Research Report – March 2004 by, Spire Security.

[5] IPS vs. IDS: Similar on the Surface, Polar Opposites Underneath white paper by Tipping point.

[6] Jan Vykopal, "Security Analysis of a Computer Network", Masaryk University
Brno, master thesis,2008.

[7] Ahmad Almulhem, Intrusion Detection System", Computer Engineering Department, Kfupm,2008.

[8] Karen Scarfone ,Peter Mell, " Guide to Intrusion Detection and Prevention Systems (IDPS)", National Institute of Standards and Technology,2007.

[9] Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth, SANS Institute, 2004.

- [1] Asmaa Shaker Ashoor, Department Computer Science, Pune University, asmaa_zaid218@yahoo.com,
- prof sharad Gore, Department Statistic, Pune University, sdgore@stats.unipune.ernet.in