**Security Technology Tools II**

**ITM437 Information Security and Technology**

**Professor: Dr. Abbas Yousefi**

**By Odiscious Dozier**

**Trident University**

**Case 03**

INTRODUCTION

Because cybercrime is on the rise, information security is a growing concern. To enhance security measures and help fight cybercrime, employing an intrusion detection system within a network or host environment is crucial. This discussion compares the, functions, features, and components, of commercial intrusion detection and prevention systems.

An intrusion detection system (IDS) specifically looks for suspicious activity, events within a network or host or both. These events may be the result of a [virus](http://www.webopedia.com/TERM/V/virus.html), [worm](http://www.webopedia.com/TERM/W/worm.html), or [hacker](http://www.webopedia.com/TERM/H/hacker.html). The IDS looks for known [intrusion or attack signatures](http://www.webopedia.com/TERM/I/intrusion_signature.html) and tracks network traffic irregularities that differ from regular system activity. The IDS is only able to provide notification of known attacks and does not perform any other actions (Beal, 2005).

PASSIVE INTRUSIOIN DETECTION SYSTEM

A passive intrusion detection system (passive IDS) is configured to monitor and analyze network traffic activity. These systems will alert operators when, potential vulnerabilities, or attacks, or both, take place, but are limited in capability; as such, they cannot perform protective or corrective measures on their own. This, along with making them easier and more rapidly deployable, makes them not impervious, but less susceptible to attacks (Beal, 2005).

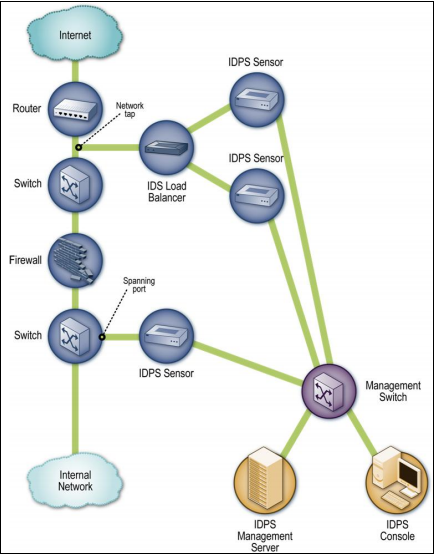
Figure 1 is an example of a Passive Network-Based intrusion detection and prevention system (IDPS) Sensor Architecture.

Figure 1: Passive Network-Based Intrusion Detection System. Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)”. Computer Security Resource Center (National Institute of Standards and Technology) (800–94). Retrieved 3 December 2015.

ACTIVE INTRUSION DETECTION SYSTEM

An active intrusion detection system (active IDS) is configured to monitor and analyze network traffic activity. These systems will alert operators when, potential vulnerabilities, or attacks, or both, take place, and they attempt to perform protective or corrective measures on their own. They are also known as, intrusion detection and prevention systems (IDPS) (Beal, 2005).

IDPS technologies differ in the way they monitor various events and the way that they are deployed. The following are four types of IDPS: Network-based, Wireless, Network Behavior Analysis, and Host-Based.

NETWORK INTRUSION DETECTION AND PREVENTION SYSTEM

Network-based IDS systems (NIDS) are often standalone hardware devices. These devices, typically, include network intrusion detection capabilities consisting of hardware, software sensors. Hardware sensors are located at various different places along the network. Software sensors are installed to system computers connected to the network. These sensors analyze network and application protocol activity via their data packets which enter and leave the network (Beal, 2005).

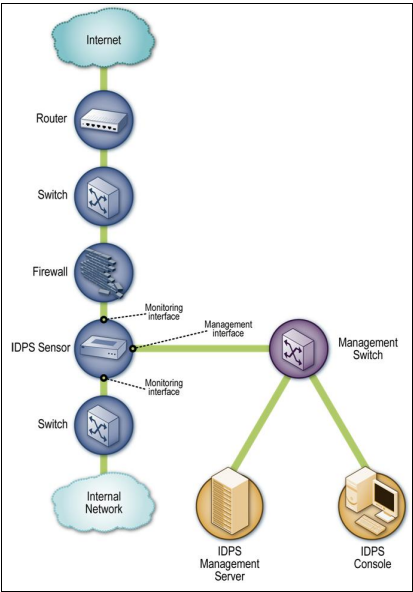
Figure 2 is an example of an Inline Network-Based Sensor Architecture.

Figure 2: Inline Network-Based Intrusion Detection System. Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)”. Computer Security Resource Center (National Institute of Standards and Technology) (800–94). Retrieved 3 December 2015.

WIRELESS INTRUSION DETECTIONAND PREVENTION SYSTEM

“A wireless IDPS monitors wireless network traffic and analyzes its wireless networking protocols to identify suspicious activity involving the protocols themselves” (Scarfone et al., 2007). The network and application protocol activities are the primary focus of this type of IDPS.

Figure 3 is an example of a Wireless IDPS Architecture.

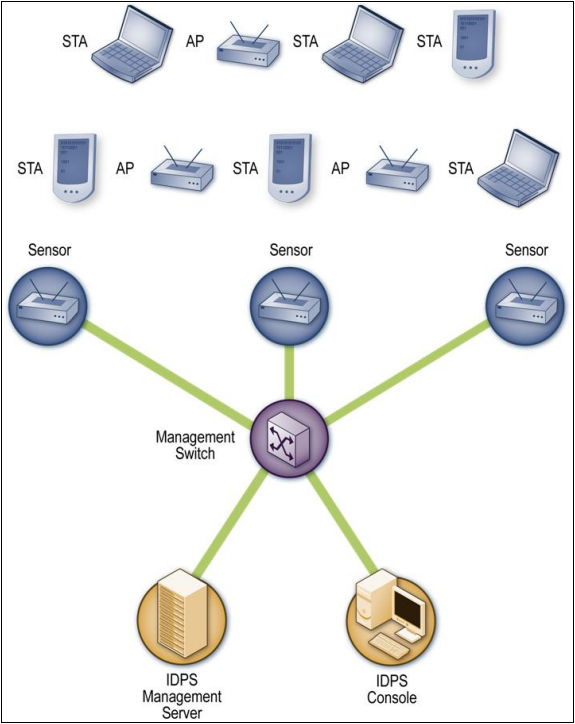


Figure 3: Wireless IDPS Architecture. Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)”. Computer Security Resource Center (National Institute of Standards and Technology) (800–94). Retrieved 3 December 2015.

NETWORK BEHAVIOR ANALYSIS (NBA)

Network Behavior Analysis (NBA) is a measure taken to enhance security that monitors network traffic for threats that generate unusual traffic flows. This can be done online or offline. Some of these malicious activities are seen in threats like, distributed denial of service (DDoS) attacks, malware, and policy violations (Scarfone et al., 2007).

HOST INTRUSION DETECTION AND PREVENTION SYSTEM

Host-based IDS systems (HIDS) are comprised of software agents that are installed on the individual computers within the system. Traffic to and from the specific machine within the system is analyzed and there are three specific intrusion events that HIDS can monitor and stop that NIDS cannot (Scarfone et al., 2007).

HIDS, above and beyond NIDS, is capable of monitoring changes to key system files and any attempt to overwrite them. HIDS are also able to monitor such activities that only an administrator would have the authority to implement. Any attempt to, install Trojan software, use methods that bypass normal authentication or secure unauthorized access, remotely, obtain access to plaintext while trying to avoid detection, or any combination of these malicious activities, can be monitored and stopped by HIDS (Beal, 2005).

Figure 3 is an example of a Host-Based IDPS Agent Deployment Architecture.

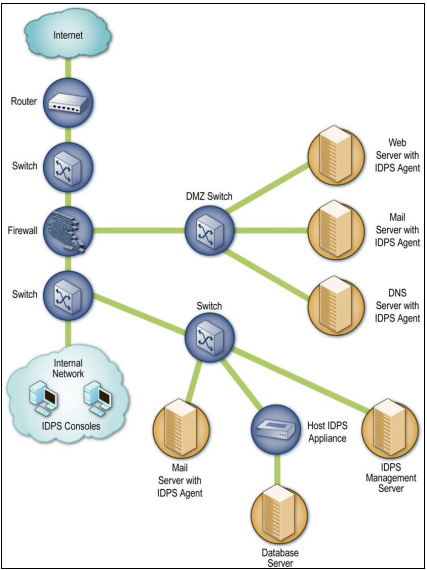


Figure 4: Host-Based IDPS Agent Deployment Architecture. Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)”. Computer Security Resource Center (National Institute of Standards and Technology) (800–94). Retrieved 3 December 2015.

MAIN FUCTIONS OF EACH SYSTEM

Recording information related to observed events is the first of three main functions of each IDPS. “Information is usually recorded locally, and might also be sent to separate systems such as centralized logging servers, security information and event management (SIEM) solutions, and enterprise management systems” (Scarfone el al., 2007).

As a system grows to multiple hosts, managing the logs and searching them for particular errors becomes quite challenging. The use of good tools to access hundreds of log files on hundreds of servers is required. Tracking or audit or analysis or any combination of these with regard to server, user behavior is useful in helping detecting problems in time (Sorce, 2015).

Notifying security administrators of important observed events is the second of three main functions of each IDPS. “This notification, known as an alert, occurs through any of several methods, including the following: e-mails, pages, messages on the IDPS user interface, Simple Network Management Protocol (SNMP) traps, syslog messages, and user-defined programs and scripts. A notification message typically includes only basic information regarding an event; administrators need to access the IDPS for additional information” (Scarfone et al., 2007).

Administrators have several tools to help them manage various threats and potential threats. Alarm clustering and compaction is a process of grouping similar or identical alarms into a single higher-level alarm. Alarm filtering is the process of classifying alarms so they can be organized. To measure the ability of an IDPS to correctly detect and identify attacks is defined as a confidence value and helps with the discernment of an actual attack (Whitman et al., 2014).

Producing reports is the third of three main functions of each IDPS. “Reports summarize the monitored events or provide details on particular events of interest” (Scarfone et al., 2007). These reports can be useful in business decision making and in developing future security strategies.

METHODOLOGIES OF EACH SYSTEM

Signature-Based Detection, much like antivirus software that detects malware, monitors packets that travel across the network and looks to identify those that match in signature or attributes against a database of known threats. This process opens a security threat where the IDS is unable to detect a new threat. The potential breach is because, there is a lag between a new threat being discovered on the network and the signature for detecting that particular threat being applied to the intrusion detection system (Bradley, 2015).

Anomaly-Based Detection is an IDS that monitors network traffic and compares the statistical analysis of that data against an established baseline. That baseline is defines what is normal for the given network. Considerations for the baseline include, the type of bandwidth that is normally used and the various ports, devices that generally connect to each other. An alert to the administrator or user is thrown when traffic is detected which is anomalous or significantly different than the baseline (Bradley, 2015).

Anomaly-Based Detection produce less false positives than signature-based devices, but its precision can be reduced due to network traffic issues; such as, massive updates upon a deployment and where events like a new application being deployed and everyone starts using the application at the same time occur. Devices that run anomaly-based detection also require greater computing power and may not detect attacks that run silently, slowly on the network (Casals, 2012).

Stateful Protocol Analysis (SPA) is, a resource intensive approach to intrusion detection and is also known as “deep packet inspection” when it’s applied to networks (Zaugg, 2010). Devices that employ stateful protocol analysis detection seek to understand protocols by looking at the application level to discern normal network traffic versus irregular or suspicious network traffic (Casals, 2012).

CONCLUSION

This discussion compared the, functions, features, and components, of commercial intrusion detection and prevention systems. If your network is not connected to the internet and has multiple users you might want to employ a passive intrusion detection system. If your network is connected to the internet with many users then you might want to employ a passive intrusion and detection system. The size of the organization will determine the depth and breadth of the security measures.

REFERENCES

Beal, V. (2005, July 15). Intrusion Detection (IDS) and Prevention (IPS) Systems. Retrieved December 3, 2015, from [http://www.webopedia.com/DidYouKnow/Computer\_Science/intrusion\_detection\_preve ntion.asp](http://www.webopedia.com/DidYouKnow/Computer_Science/intrusion_detection_preve%09ntion.asp)

Bradley, T. (2015). Everything You Need to Know about Intrusion Detection Systems (IDS). Retrieved December 7, 2015, from <http://netsecurity.about.com/cs/hackertools/a/aa030504.htm>

Casals, J. (2012, September 3). Why are IPS (Intrusion Prevention Systems) so difficult to tune? Retrieved December 7, 2015, from [http://www.opttic.com/ips-difficult-tune-reduce-false- positives](http://www.opttic.com/ips-difficult-tune-reduce-false-%09positives)

Examining Different Types of Intrusion Detection Systems. (2015). Retrieved November 30, 2015, from <http://www.dummies.com/how-to/content/examining-different-types-of-> intrusion-detection-s.html

Key Functions of IDPS Technologies - IDPS\_Info498. (n.d.). Retrieved December 7, 2015, from <https://sites.google.com/site/idpsinfo498/home/key-functions-of-idps-technologies>

Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)”. Computer Security Resource Center (National Institute of Standards and Technology) (800–94). Retrieved 3 December 2015.

Sorce, S. (2015). Centralized Logging. Retrieved December 7, 2015, from <https://www.freeipa.org/page/Centralized_Logging>

Whitman, M., & Mattord, H. (2014). Intrusion Detection and Prevention Systems. In Principles of information security (Fifth ed., p. 359).

Zaugg, B. (2010, June 19). An Overview of Intrusion Detection Systems Technology and Research. Retrieved December 7, 2015, from [http://www.bzaugg.com/2010/06/an- overview-of-intrusion-detection-systems-technology-and-research/](http://www.bzaugg.com/2010/06/an-%09overview-of-intrusion-detection-systems-technology-and-research/)