I am looking to build out a small section of technical overviews on the topic of: Intrusion Prevention Systems. Sub-sections should include: What are Intrusion Prevention Systems? Host Intrusion Prevention Network Intrusion Prevention Types of IPS Software Prevention versus Detection Shortcoming of Intrusion Prevention Solutions The content should be written without voice, be agnostic and informative providing useful links and references to any factual claims. We have provided a bulleted list of sub-topics that we would like covered with flexibility to add additional relevant areas or combine existing. 1,200 words per topic.

WHAT ARE INTRUSION PREVENTION SYSTEMS?

An intrusion prevention system is a type of network security technology that continuously evaluates inbound and outbound network flows to identify and prevent suspicious attacks. When threats have been identified, the IPS notifies the network administrator and takes certain automated, preventative actions based on predefined rules established by the administrator. These actions include:

- Stopping the attack. This may entail resetting TCP connections and blocking traffic from the source address.
- Changing the security environment. For example, other security controls, such as firewalls, may be reconfigured to interrupt an attack.
- Altering the contents of the attack. The system may replace or eliminate the malicious portions of an attack to make it harmless.

The components of an IPS typically include a sensor or agent for monitoring and examining activity, a management server, a database server and a console program. The IPS is deployed directly in the communication path between the source and destination to conduct comprehensive inspections of packets in real-time.

There are three different types of methodologies that an IPS can be configured to use to detect suspicious activity. The majority of IPS solutions utilize multiple methodologies in order to enhance the scope and accuracy of the detection. One of the determining factors that help determine which methodologies to employ is the network security policies for the organization. The different methodologies include:

- Signature-Based. The signature-based methodology uses predefined signatures or patterns of known network threats. If an attack corresponds to any of the signatures, the ISP will initiate the appropriate preventative actions. In order for a signature-based IPS to remain effective, its signature library has to be updated regularly.
- Anomaly-Based. This methodology entails monitoring network flows for unexpected or abnormal behaviors. Profiles are used to represent the normal behaviors of hosts, uses, applications or network connections. When an anomaly is detected, the IPS will immediately block access to the host.
- Policy-Based. The network security policies, which are based on the enterprise's security policies and the network infrastructure, are configured by network administrators and are used as references to gauge network activity. The network administrator is notified if an activity on the network violates a security policy.

Intrusion prevention systems are key aspects of network security for enterprises of all sizes. They are most effective when implemented as part of a comprehensive network protection strategy.

TYPES OF IPS SOFTWARE

The various types of IPS solutions, and each one has their own weaknesses and strength. A practical application may require the use of multiple solutions in order to an optimal level of network security from attacks. This IPS software can be divided in four different categories based on the manner in which they are deployed and the types of incidents they monitor:

- Network-Based. A network-based IPS is usually stationed at the division points between networks where it monitors network traffic and evaluates network and application protocol activity to detect malicious activity.
- Host-Based. An host-based IPS is used to provide protection for a single host. It monitors the characteristics of that host and the events taking place in that host for suspicious activity. Host-based intrusion prevention systems are typically used on the most critical hosts within a network.
- Wireless. Wireless-based IPS solutions oversee wireless network flows and analyzes wireless networking protocols. In addition to being deployed within the vicinity of an enterprise's wireless network for monitoring, wireless-based IPS solutions may also be deployed to sites where there is unauthorized wireless networking.
- Network Behavior Analysis. NBA IPS solutions assess network traffic to root out threats that result in unusual traffic flows. These threats may include policy violations, distributed denial of service attacks and certain types of malware. While NBA IPS solutions are typically set up to monitor traffic flows on the internal networks of an enterprise, they may also be stationed where they are able to monitor the flows between an enterprise's networks and its business partners' networks, the Internet or other types of external networks.

HOST INTRUSION PREVENTION

The characteristics of the single host that are monitored by a host-based intrusion prevention system can include system logs, files access, wireless and wired network flows, file modifications, running processes and modifications to applicant and system configuration. A host-based IPS can be implemented on different types of machines, including workstations, servers and computers. It provides protection for a unique host by establishing a barrier through which all system calls and application calls must filter, permitting only those that are legitimate.

NETWORK INTRUSION PREVENTION

A network-based intrusion prevention system establishes a protection system by creating physical security zones that are able to trap hostile traffic. However, it is only when its sensor is deployed in an inline mode, or stationed so that the network data it monitors and analyzes in real-time passes through it, is it able to halt attacks by obstructing traffic; network-based IPS sensors that are deployed in passive mode can only monitor a copy of the traffic. The prevention capabilities of network-based IPS inline sensors include restricting bandwidth, inline firewalling and modifying malicious content.

PREVENTION VERSUS DETECTION

Both detection and prevention are necessary aspects of effective network security. Detection is a reactive security practice that typically uses an intrusion detection system to detect and report ongoing attacks. In contrast, prevention is a proactive measure that is implemented by an intrusion prevention system, which can not only detect and report attacks, but also prevent identified threats. An IDS is deployed on the outside of the network, able to scan only copies of the network packets and conduct an offline analysis of the data, while an IPS is an inline security component, placed in the direct communication path between two networks so that it can perform inspections of the traffic in real-time and execute immediate preventative tasks to prevent the suspicious traffic from exiting or entering the network.

SHORTCOMINGS OF INTRUSION PREVENTION SOLUTIONS

One of the most common disadvantages of an IPS is the regular detection of false positives and false negatives. Cases of false positives tend to occur when activity on the network is automatically blocked because it does not fall in the range of normal behaviors and is deemed by the system as being suspicious. This represents an error and generally is caused by excessively tight proactive controls or excessively relaxed reactive controls. The occurrence of an excessive number of false positive can degrade the intrinsic value of the data received from the system and can pose an issue as network attacks increase over time. While an IPS can be configured to limit the occurrences of false positives, doing so does not eliminate the necessity of responding to them. Not monitoring the false positives can result in real attacks being ignored of slipping through.

False negatives tend to occur when malicious traffic is not detected by the system, even though a signature for the particular threat exists in the signature library. The failure of the security control to properly respond is an error and results from overly strict reactive controls or overly relaxed proactive controls.

Another issue with the IPS is that in order to remain effective against new threats, the signature library has to be continuously updated. Without frequent updates, an IPS will not be able to detect the most recent threats or notify administrators of their occurrences. Until a new signature is added to the signature library, the system will be vulnerable.