

QSR Issue 3 – Expert Strategies

Most people in the Information technology field have heard of **Intrusion Detection Systems (IDS)**. In some cases people have installed and currently manage IDS systems. Recently there has been a lot of discussion about **Intrusion Protection Systems (IPS)**. Vendors that have IPS systems are quick to use the line “we are not an IDS but an IPS” as a sales opening in attempt to differentiate themselves from other detection solutions available in the marketplace. In this article, we will explore the basic differences between IDS and IPS systems and identify what is important to look for when evaluating an IDS or IPS solution.

IDS systems typically come in two flavours. They are 1) Host Based Intrusion Detection System (HIDS); and 2) Network Intrusion Detection System (NIDS). The distinction is exactly what the name indicates. HIDS run on your server and are designed to detect intrusion attempts on the host server that it is installed on. NIDS sits on the network where it analyzes traffic and identifies intrusions on the network. IDS solutions identify “intrusions” in two basic ways. The first and most common detection method is **Signature** based. The second method is **Heuristics or Anomaly** based detection.

A **Signature** based detection is a “known” or “static” match. A packet or series of packets have certain characteristics that can be identified as a known threat based on the information contained in the Signature. As an example, the famous Loveletter virus has the following characteristics:

- A length of: 10,307 bytes
- Subject of e-mail will contain: ILOVEYOU
- Attachment: LOVE-LETTER-FOR-YOU.TXT.vbs

These type of characteristics can uniquely identify this virus. And these are simple, there are more complex mathematical ways to do this. Network attacks where a signature is present work on the same principle, although they tend to look for specific bit patterns in packets, specific port connections and other common network parameters.

Heuristics or Anomaly based detection engines analyze data and make decisions on the data based on predefined behavioral characteristics. Like known attacks, it is not uncommon to see a series of calls to an operating system that are unauthorized or even hostile. However, a signature is not available to identify the attack because the characteristics of the attack are unknown and it cannot be recognized. The heuristic detection process involves the assessment of unusual or uncommon behavior that is not typical to the normal processing behavior of the particular environment. In order to manage this type of unwanted traffic the administrator can adjust settings on the IDS to trigger an alert if unusual traffic is identified. One example would be where typical packet sizes on a network suddenly change to very small sizes indicating a possible attack.

IDS systems are now adding additional features to make them even more accurate. The capability of gathering historical data on the device or network is being added so that this history can be used to determine what is considered “normal” or “baseline” behavior. This “normal” or “baseline” information can then be used to assess the probability that a detected attack is hostile. This intelligence allows the IDS to respond differently to the traffic on different environments. By learning what is considered normal traffic, sudden differences can be detected and dealt with as appropriate.

Given that the complexity of systems has increased dramatically and continues to do so, the frequency of unknown attacks is also increasing. Complexity increases vulnerabilities which in turn creates more weaknesses in infrastructures that can be attacked. IPS solutions are the new breed of IDS. Although there are some fundamental differences, the concepts are exactly the same as those discussed above. The two main differences are:

1. Most IPS systems can go inline, like a firewall. Traffic must pass through them in order to get to its destination.

2. Because IPS systems can go inline, like a firewall, they not only have an ability to 'alert' about possible hostile action, they have the ability to block it, just like a firewall.

When evaluating an IPS vs IDS technology the key functions to understand and therefore the key questions to answer, regardless of the product are:

- Does this IPS solution allow me to go inline or outline?
- What is the maximum throughput it can handle if inline?
- If the IPS fails and because it is inline, does network traffic stop or does it continue?

Most IDS solutions today are becoming IPS solutions as vendors are quickly responding to the new market trends and demands. I suspect that within a year IPS solutions will be the standard in detection, offering deployment flexibility to alert and/or block.