

## WHAT IS AN INTRUSION PREVENTION SYSTEM?

BY ANDREW PLATO, CISSP

ANITIAN ENTERPRISE SECURITY

COPYRIGHT © 2004 – ANDREW M. PLATO

In the race to secure information systems, one of the most popular and fastest growing segments of the security market is intrusion prevention systems or IPS. These technologies offer the promise of protecting networks and systems from the myriad of attacks, exploits, and viruses.

As the popularity of IPS has increased, so have the number of products claim to be an IPS. Since there is no strict definition of what an IPS is or is not, companies are using IPS as a marketing and sales ploy to encourage customers to purchase their products. This has a diluting affect on the concept of IPS. IPS was originally limited to a small group of technologies. Thanks to marketing efforts to re-brand IPS, practically everything is called an IPS. Exacerbating the problem is the fact that every vendor, consultant, and pundit redefines IPS to meet his/her needs.

The debate surrounding the meaning of IPS is complex. Superficially, its merely a semantic argument about a term. Underneath are deeper issues of branding, technology, and even information security. This complexity coupled with the bandwagon effect of IPS has created a confusing landscape for customers and users. When nobody can agree on what IPS means, it leads to uninformed decisions, unrealistic expectations, and misguided IT implementations.

Therefore, somebody needs to step forward and define a practical set of criteria to define intrusion detection systems. Who better than the person who helped found the entire market segment?

### Origins of IPS

In some respects, I am partially responsible for creating the term *intrusion prevention system*. From 1997-2000, I was responsible for the technical documentation at Network ICE, a Silicon Valley start-up that helped fuel the early days of the security boom. During my tenure at Network ICE, I wrote virtually all the technical manuals and marketing materials for Network ICE.

Network ICE was very concerned about differentiating their products in the market. Network ICE's main product, BlackICE, was not only able to detect intrusions, it could also respond to intrusion attempts and block the attacking machine. It was part intrusion detection system (IDS) and part firewall/reactive defense.

Working with the executives and engineers at Network ICE, I coined the term *Intrusion Prevention System* or IPS. We put it in all the technical manuals, marketing material, and mentioned it in every article written.

In 1998, Network ICE introduced their technology at Interop in Las Vegas. By 2000, we had articles in every magazine about Network ICE's IPS technology and I was meeting with a dozen companies a month in the Pacific Northwest about IPS. At first, IPS was a strange concept for traditional networking engineers. It took a lot of education and explanation to get people to see the benefits.

Since then, IPS has evolved. Network ICE was not alone in their quest to build a more perfect security technology. Other companies like IntruVert, Symantec, and Netscreen were rapidly building (or acquiring firms that built) IPS technologies.

Therefore, I think my experience with IPS gives me some credibility to define the term. As such, this paper attempts to define what an IPS is and what criteria it must meet to be considered an IPS technology.

## **IPS Criteria**

This section defines the criteria for IPS technology. The criteria were formulated out of a general survey of the technologies on the market. Moreover, these criteria are intended to reinforce the concept that IPS's are "reactive" systems that can detect and react to threats.

### **Requirement 1 – Sophisticated Analysis**

The first and most critical requirement of an IPS is that it must possess some kind of internal intelligence that can differentiate malicious activity from safe activity using some type of anomaly detection component. This component should systematically analyze system behavior or communications against a sophisticated and dynamic set of criteria, tolerances, and static signatures.

The key word in this criterion is *sophisticated*. The analysis engine must be more than just a big set of rules. It must be adaptable and dynamic.

Additionally, this analysis must be sophisticated enough to categorize and identify activity. Merely blocking malicious code or communication is not sufficient for a true IPS. It must identify the nature of the activity and provide administrators with some kind of insight into the activity. Since this is something intrusion detection systems do, its natural for the analysis component of an IPS to be an IDS engine that analyzes, ranks, identifies, and describes system or network activity.

Furthermore, this intelligence must be an integral component to the system. It cannot be a static rule-set or control list. The analysis must be exhaustive and sophisticated enough to detect subtle differences in attack vectors.

Perhaps one way to look at this concept is in terms of airport security. Consider two different security checkpoints. Guard 1 merely checks to see if you have a valid ticket. If you have the correct ticket, he lets you pass. Guard 2 checks your ticket, but he also looks through your belongings, asks you questions about where you are going, and runs your belongings through bomb and metal detectors.

Guard 1 is performing access control. He is enforcing a static set of rules. If you have a ticket, you pass. If you do not have a ticket, you cannot pass. This offers extremely limited security.

Guard 2 is performing intrusion prevention. He is not only enforcing a static rule set, he is also analyzing you and your “payload.” If you appear to be safe, he lets you pass. But if you are carrying a bomb or a gun, he blocks your passage (and probably arrests you.)

Moreover, Guard 2 is doing more than just looking at your belongings. He is asking you questions, like “where are you going today?” or “where did you come from?” He is using his intelligence to determine if you have sinister intentions. Furthermore, he is probably also paying attention to current events and adapting his sensitivity to odd behavior based on environmental factors. If there is an a warning from the government that terrorists are likely to be boarding planes, his sensitivity to strange behavior is increased.

### **Requirement 2 – Statefulness**

The Guard 1 & 2 example leads to the next criteria of IPS – statefulness. An IPS must implement some type awareness to its environment. It cannot just blindly accept or reject activity. It must have some understanding of the environment where it operates.

The key word in this criterion is *awareness*. An IPS must understand its environment.

This could be in the form of maintaining network or operating system state information. For example, an in-line IPS gateway should maintain data tables on which systems are communicating and with whom.

Furthermore, state information must feedback to the analysis engines. When the detection and identification engine is analyzing information, it must take into account the state of that information. This could be in the form of tolerances or heuristics that can adapt to the network or system environment.

### **Requirement 3 – Automated Response**

In addition to detecting and identifying suspect behavior, an IPS must be able to respond to that detection. This mechanism must have the ability to automatically prevent hostile code from entering a secured area and/or executing. This prevention can be configurable and have different levels of enforcement, yet it must function (or have the option to function) automatically.

The key word in this criterion is *automated*. The response must be automatic and not require human intervention. This ensures that the product can actively protect systems and/or data and does not require constant monitoring from people.

Ideally, this automated response should be contained within the IPS technology itself. Some products have attempted to sell themselves as IPS technologies because they have an option to interface with other security technologies. For example, some products can automatically write rules in a perimeter firewall. This type of external dependency creates a weakness in the IPS technology as a whole. It makes the IPS dependent upon an external system which may or may not respond as desired. This would not disqualify a product as an IPS, but it certainly make it weaker.

### Requirement 4 – Rapid Response

Automation therefore begets immediacy. An IPS must not only respond to malicious behavior, it must do so with expedience. An IPS must actively practice and enforce protection in real or near-real-time. In other words, it must actively deliver critical protection and detection while malicious events are happening. This requirement may seem obvious, but when you look at the range of products calling themselves IPS, it would instantly invalidate many of those products.

The key word in this criterion is *active*. An IPS is not a passive system that just leisurely reports problems to some big database. It must actively protect information systems and or data from unauthorized or malicious use.

Moreover, it must implement this security in real-time. When malicious activity is detected, it must immediately respond to that activity and prevent it. It cannot wait until somebody pushes a button to enable the protection.

### Not IPS

Now that the criteria are established, its important to separate a few technologies that are not IPS. They fail to meet the criteria or are just being overly spun by the marketing people at their respective companies.

**Pre-Hardened Operating Systems:** This is a new line of products that has emerged recently. Basically, they are operating systems (usually Linux variants) that have been pre-hardened against attack. Some of them even include novel components to control access and prevent unauthorized applications from executing. These technologies offer very good security and will prevent intrusions. But they lack the internal intelligence to analyze behavior or traffic for malicious activity. They typically deal with a static set of rules that merely allow or do not allow something to execute.

**Personal Firewalls:** Sorry, but ZoneAlarm, Tiny, and all the other personal firewalls are not intrusion prevention systems. Specifically, these products all lack internal intelligence to make distinctions between normal and abnormal activity. Naturally, I would disassociate ISS's BlackICE firewall from this group, since it does contain an internal analysis engine that can perform deep inspection of network traffic for intrusions.

**Integrity Monitors:** Software that merely monitors the integrity of system files or data may be very useful in tracking changes, but it does not qualify as a IPS. This is mainly because these systems typically lack automated response mechanisms or real-time protection.

**Encryption Technologies:** Encrypting data is important. But its not an IPS. Merely encrypting data does not mean its safe. The whole concept of an IPS is to detect attempts to carry out malicious or unwanted activities. Encrypting data may increase its security, but it does not have the ability to detect and respond to attacks in real-time.

**Firewalls:** This is perhaps the most contentious issue in IPS world. Firewall vendors are desperately trying to re-brand their products as intrusion prevention systems. Firewalls are a tough to exclude, because they exhibit many of the qualities of a good IPS. Most firewall vendors have jumped on the IPS bandwagon and are rapidly trying to implement deeper levels of inspection and protection into their products. Some vendor are doing a very good job at this, others seem to be taking a piecemeal approach and just dropping in analysis on just a few high-value protocols, like HTTP. This space also includes the proxy-based firewalls, which in many ways were the predecessors of IPS. Therefore, its clear that some firewalls are IPS or have IPS qualities. While some, namely the purely stateful packet inspection type firewalls, are not IPSs.

### Conclusion

IPS is here to stay. It is a compelling and valuable addition to the information security of any organization. Understanding what IPS means and how it works is the first step toward using and benefiting from its capabilities.

It is time for the information security community to adopt some standards for IPS. Without a standard set of criteria, it becomes too easy for marketing people to mislead or mis-inform customers. This can result in poor decision making and decreased security.

Hopefully, this paper will serve as a reference to organizations on what they can expect from an IPS. This market is growing rapidly, and it is easy to become lost in the myriad of products and pitches from vendors. When you objectively analyze products, based on the criteria in this paper, it will become clear which technologies offer the most advanced capabilities for the price.

If you have any comments or suggestions for this article, please contact me at [aplato@anitian.com](mailto:aplato@anitian.com).

*NOTE: None of the companies mentioned in this document sanctioned, prompted, or compensated Andrew Plato or Anitian Enterprise Security in any way for this document, this includes Internet Security Systems.*

*This document is the property of Andrew M. Plato and the Anitian Corporation. Redistribution is permitted, provided the contents is not altered in any way and Andrew M. Plato and Anitian Enterprise Security are clearly noted as the authors.*