

Intrusion Detection vs. Intrusion Prevention: The difference and what you need to know

By Brad Doctor, Principal security architect

Originally published in CyberDefense Magazine, March 2004

The topic of IDS (intrusion detection systems) versus IPS (intrusion prevention/protection systems) is turning into a war within the technical security community. There are three schools of thought: pro-IDS, pro-IPS, and those who espouse a combination of both technologies. No matter which side of this debate you are on, both IDS and IPS provide added value that can be an integral part of a best-practices, layered network security approach. This approach centers on maintaining appropriate security measures and procedures at five different levels within an IT environment - perimeter, network, host, application, and data.



In this article, we will examine both technologies - their history and their future - with an eye towards helping you choose the right solution for your needs.

The Precursor to IDS solutions

Although the IDS versus IPS debate is a hot debate within the IT industry, NIDS or network-based IDS (as opposed to HIDS or host-based IDS) is a relatively mature technology. Technical readers may be familiar with a tool released quite a few years ago called TCPdump. TCPdump and a number of similar tools that passively monitored network traffic were the precursors of today's intrusion detection systems. Because these tools relied primarily on the user's skill set to be effective, they had limited functionality and automation compared to modern-day IDS products.

The core technology utilized in tools such as TCPdump is still the basis for most IDS (and IPS) products today. Of course, today's IDS tools contain a much more sophisticated technology than their primitive predecessors. State tracking, anomaly detection, and ever-increasing bandwidth monitoring capacity are key elements in a modern IDS system.

Current IDS functionality

Today's IDS is a combination of signature analysis, network traffic monitoring, and network behavior analysis (also referred to as anomaly detection) technologies. The heart of most solutions today is signature analysis (i.e. monitoring traffic for known attack patterns - everything from minor attacks through the latest, high-profile worms). Typically, a signature-based IDS is configured with thousands of rules that detect potentially malicious attacks and codes. Positive proof of the effectiveness of IDS solutions and why they are an important component to a layered network security strategy is the sheer volume of attacks they are able to detect.

Two drawbacks to signature-based IDS solutions are false-positives and the time lapse to create signatures for new exploits. False-positives are pattern matches inaccurately identified as attacks. Historically false-positives have inundated administrators thus causing an even greater problem - desensitization. Today's solutions are actively and aggressively trying to solve the issue of false-positives,

including providing elaborate "tuning" mechanisms which effectively disable signatures that cause false-positives.

Similar to anti-virus software, an attack must be analyzed before a signature is developed to recognize it. This time lapse can be critical. Recently, the time between a new vulnerability and its associated exploit has been decreasing, placing more pressure on IDS manufacturers to rush signatures to the market. The recent MyDoom attack benefited from this time interval, allowing it to become the fastest spreading worm in history. Timely delivery of signatures is integral to overall IDS effectiveness.

An alternative to signature-based IDS is called behavioral or anomaly-based IDS. The basic premise of this sub-category of IDS is that normal network traffic generally behaves within certain patterns. For example, opening network ports in rapid succession is typically not seen in normal traffic, so a behavioral or anomaly-based IDS may flag that traffic as abnormal and identify it as a port scan (generally a precursor to an attack). Large, sustained amounts of fragmented packets are also abnormal patterns and will also be flagged. These systems have not broken into the mainstream, but seek to provide an alternative to the drawbacks of signature-based systems.

Monitoring for intrusions is a critical component of any network security policy. The greatest challenge when working with IDS systems has been sifting through and utilizing the large volume of data generated. Due to the nature of its design, the role of IDS systems have largely been one of postmortem or historical reporting. The critical question facing IDS solutions is this: Is detecting attacks enough?

Early IPS Systems

Early intrusion prevention systems were spawned from intrusion detection systems. IPS vendors took the next step and began to block detected attacks. The earliest generation of the IPS blocked attacks by integrating with firewalls (and sometimes with routers or switches). The IPS would instruct the firewall to insert a rule to block traffic from or to a particular IP address or port. These systems took action on attacks and were particularly effective in blocking systematic attacks from particular networks or hosts.

However, first generation IPS solutions had a number of drawbacks:

- They were incapable of stopping the first attack because the time to insert a firewall rule was longer than the time it took for the attack to pass through the network gateway.
- The firewall blocking was generally based on the IP address. The result was often that legitimate traffic would be blocked with malicious traffic. Because network proxies and NAT (Network Address Translation, which is often used in conjunction with proxies and firewalls) are so widely used in today's LAN / WAN environments, many administrators believed that this negated the positive effects of blocking attacks.
- Hackers could evade these systems with relative ease. For example, even if the original host was blocked, other hosts were still allowed to launch the same attack before being blocked. This created a weakness in dealing with distributed attacks.

Despite these drawbacks, IPS solutions still provided significant value by blocking attacks that would have otherwise entered an organization's network and caused damage.

IPS: The Holy Grail?

Fortunately, first-generation IPS systems didn't last long. The modern IPS system is much more sophisticated. Systems now stop traffic before an attack ever enters a network, and they only stop the traffic that should be stopped - or in certain cases, only the packets that should be blocked. Similar to the evolution of firewalls, IPS systems today are extremely effective and scalable because they "scrub" or deeply inspect the traffic to ensure that only legitimate traffic makes it into the network. This method of attack blocking alleviates the issue of blocking entire networks as well as stopping distributed attacks.

IPS solutions have evolved into proactive devices that sit in-line on a network, just as a firewall or router does. As a consequence of sitting in-line, IPS solutions are required to match high-traffic, gigabit-level requirements.

As traffic has increased, the number of attacks has grown as well. Clever algorithms have been created to correlate attacks with other network data to filter or qualify the real attacks on which administrators need to focus their attention. All other attacks - which the correlation algorithms determine to be irrelevant - are either immediately blocked or ignored by the IPS.

While today's IPS technology is a significant step forward, the debate continues. Inline IPS solutions now introduce latency as every packet needs to be inspected. With impatient customers and employees, delay can translate into lost revenue. Thus the next phase of the debate begins...

The Future of IDS

Today's IDS systems are generally standalone point solutions. The market trend, however, is for IDS to be integrated into gateway security solutions containing firewalls, VPN, and other security applications. Integrated gateway solutions often have limited IDS functionality compared to standalone IDS systems. In the future, however, integrated solutions will become full-featured and their integration will be seamless and transparent to network administrators. The device, including routers and switches in the future, will simply have a much higher level of knowledge about the traffic it is passing.

The Future of IPS

Unlike IDS technology, IPS will likely continue to evolve as a standalone solution. Both from an algorithm point of view and from a computer power perspective, IPS systems still have much room for improvement and we expect that they will remain single-point solutions for a long time to come.

The need for increased accuracy in IPS systems is rapidly raising the performance bar for IPS products in the marketplace today. In the near future, vendors will fully automate the intrusion prevention process by virtually eliminating false-positives and ensuring that an IPS, independent of the firewall, can block almost all attacks that try to enter the network.

The Technology Investment

When choosing the solution that best meets your needs, it is safe to say that both IDS and IPS technologies have merits and drawbacks. An investment in standalone IDS technology may not be a wise long term solution due to its current integration with gateway security devices. IDS systems are moving to be a more monitoring solution, and many organizations are deploying both IDS and IPS solutions.

The majority of the industry would agree that properly configured IPS systems bring a great amount of added value to proactively blocking attacks. The risks currently associated with IPS systems, including letting some attacks through and detecting false-positives, can be mitigated with careful configuration and monitoring of the system.

Ultimately, an IPS's ability to automatically block the latest worm that attacks a network in the middle of the night is where its true value is revealed. This type of 24x7x365 protection is why the promise of an effective IPS is so alluring and why the quest for the perfect IPS is ongoing.

Skeptics and critics abound for both IDS and IPS solutions. Ultimately, the truth may be somewhere in the middle. Careful analysis of an organization's needs and criteria will lead it to make the most appropriate decision when it comes to either intrusion detection or intrusion prevention.

About the author:

Brad Doctor, CISSP, is StillSecure's principal security architect. He has been involved in IT security for more than 10 years. Prior to StillSecure, Mr. Doctor consulted for such companies as Apple Computer, Phoenix Technologies, and the Monster Board, fulfilling network and host-based security needs. In addition to traditional IT security, Mr. Doctor also worked with Quova, Inc. as the Director of Research where he led the development of Quova's proprietary IP Geolocation technology, presently used by Visa International to detect credit card fraud. Brad is an active member in ISSA and is the Recording Secretary for the ISSA Denver Chapter.