Secureworks

FUNDAMENTALS

The Evolution of Intrusion Detection/Prevention: Then, Now and the Future

Learn how intrusion detection and prevention systems have changed over time and what to expect looking ahead

THURSDAY, JULY 6, 2017
BY: JOHN PIRC

Intrusion Detection vs Intrusion Prevention vs Next Generation IPS vs Next Generation Firewall

Having worked for the past 20 years for nearly every IDS/IPS vendor in product management and research, I've seen a lot of improvements to IDS/IPS products. They all are still quite similar to their original incarnation, which started with an academic paper written in 1986. The IDS/IPS basic fundamentals are still used today in traditional IDS/IPSs, in next generation intrusion prevention systems (NGIPSs) and in Next-Generation Firewalls (NGFWs). This is a look at the beginning stages of intrusion detection and intrusion prevention, its challenges over the years and expectations for the future.

The Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) started with an academic paper written by Dorothy E. Denning titled "An Intrusion-Detection Model," which led Stanford Research Institute (SRI) to develop the Intrusion Detection Expert System (IDES). That system used statistical anomaly detection, signatures and profiles of users and host systems to detect nefarious network behaviors. IDES had a dual approach. It used a rule-based Expert

System[1] to detect known types of intrusions plus a statistical anomaly detection component based on profiles of users, host systems, and target systems. For example, it could detect that a protocol like HTTP or FTP was being misused, and could detect Denial of Service (DoS) attacks when an IP address was flooding a network.

2000 - 2005: Intrusion Detection Preferred Over Prevention

In the early 2000s, IDS started becoming a security best practice. Prior to then, firewalls had been very effective for countering the threat landscape of the 1990s. Firewalls process traffic quickly as they have no "deep packet inspection," meaning they have no visibility into the content and context of network traffic. Firewalls only have the ability to react based on port, protocol and/or IP addresses. In the early 2000s new threats like SQL injections and cross site scripting (XSS) attacks were becoming popular and these attacks would pass right by the firewall. Hence the real beginning of putting the IDS into use. The popularity of IPS would come later.

During the early 2000s, few organizations had an IPS because they were concerned that the IPS could possibly block harmless anomalous traffic from prospects. The IPS works by sitting "in-line" in between an organization's network and the internet. When an event of interest (EOI) enters the network, the IPS would immediately block the EOI, which terminates the sender's connection to the organization's network. However, an EOI isn't always an attack. It simply could be some activity out of the ordinary occurring from the connection with the sender. Rather than take the chance of dropping EOI traffic coming from a prospect that is actually harmless, most companies were using an IDS rather than an IPS. Instead of sitting in between an organization's network and the internet, an IDS sits off to the side and mirrors all the traffic that comes into the network. When it discovers traffic that it perceives may be malicious, the IDS sends an alert to the organization's administrator so that an analyst can review the log activity and decide whether or not it is malicious.

In the early 2000s, the market for Intrusion Prevention Systems was so low that there were only a couple of IPS vendors. Rather than taking the chance of an IPS dropping a harmless network connection from a prospect, which may have appeared to have been anomalous activity, organizations preferred to let anomalous activity into their networks. The idea was that the IDS would alert the organization, which would review the activity logs, and when it found malicious activity, the organization would take appropriate measures to get the threat out of the network.

During this time signatures were written to detect exploits, not vulnerabilities. For any given vulnerability there could be 100 different ways to exploit it. Once criminals discovered a vulnerability, they could create more than a hundred different ways to exploit it, causing IDS

vendors to write 100 or more different exploit signatures. When one of these known exploit signatures got through the network, the IDS would send an alert to an administrator. Back then, IDS vendors would brag about how many signatures it had in its database thinking the more signatures, the better they compared to their competitors. However, having the most signatures was not really an accurate gauge for judging the best IDS as IDS vendors also used other methods to detect threats, including pattern matching, string matching, anomaly detection and heuristic-based detection.

The Adoption of IPS, 2005

When the adoption of IPS began to grow in the latter part of 2005, more vendors began supporting IPS. As vendors began competing for IPS business, they stopped bragging about the amount of signatures they had in their database. Since the IPS is inline, clients worried that all those signatures would slow down the network as each connection would have to be checked for one of those exploit-based signatures. IPS vendors began creating only one signature to satisfy each vulnerability no matter how many exploits were affiliated with it. Vendors had discovered that an IPS or an IDS that has more than 3,500 signatures is apt to hinder its performance. Today, vendors still pick the most relevant signatures that address the current threats as well as older threats that hackers still use.

To this day, intrusion detection and prevention systems (IDS/IPS) are changing and will likely continue to change as threat actors change the tactics and techniques they use to break into networks. Thus far, we looked at how an academic paper birthed the IDS/IPS concept and changed over the years until 2005. Here, I start with 2006 and share the history of IDS/IPS and my thoughts about the ways organizations will be securing their networks in the future.

2006 – 2010: Adoption of Faster Combined Intrusion Detection and Prevention Systems

Security companies that offered IDS/IPS solutions stepped up the competition by taking IPS from 1 or 2 Gbps to 5 Gbps, providing the ability to monitor more segmented networks, as well as the DMZ, web farms (the use of multiple servers to host an application so that one server does not become overloaded with traffic), and the area just inside an organization's perimeter before the attack has an opportunity to enter the main network. An IPS operating at 5 Gbps allowed greater capacity to handle the throughput on the device, allowing the device to monitor more network segments. Today, the majority of IPS platforms can provide up to 40 to 60 Gbps of protected throughput. Clients began switching from IDS to IPS, and its adoption was seeing double digit revenue growth year over year. When the Payment Card Industry Data Security Standard (PCI DSS) began requiring organizations that accept payment cards (credit cards) to install either an

IDS or a web app firewall, many of those organizations purchased an IDS/IPS. By then, the IPS technology had been more finely tuned and was much better at not blocking harmless traffic, so people began using it in the IPS mode. Meanwhile, botnets were proliferating. One way attackers were gaining control of user's computers and adding them to botnets was by planting malware on popular websites. If a user's browser plugin like Java or Adobe's Flash or PDF reader contained a vulnerability, when the user clicked on a document or link that used one of those plugins, malware would secretly be downloaded. Additionally, in 2008 hackers were using iFrame redirects on popular websites like news sites to redirect a user to the hacker's site. If end users had vulnerabilities in their applications or web browser when they landed on one of those popular sites the Iframe code would redirect them to a malicious website. This required IDS/IPS vendors to provide additional countermeasures. In addition to pattern matching, string matching, anomaly detection and heuristic based detection, vendors added information to block malicious command & control IP addresses as well as websites that were known to host malware, reducing the time it takes to detect threats.

2011 – 2015: Next Generation Intrusion Prevention Systems

The years between 2011 and 2015 were a massive turning point for IDS/IPS vendors as they began creating Next Generation Intrusion Prevention Systems (NGIPS), which included features such as application and user control. A traditional IPS inspects network traffic looking for known attack signatures and either alerts on the traffic or stops it from proceeding into your network, depending on how it has been deployed. AN NGIPS does that and provides extensive coverage of network protocols to detect a wider range of attacks. It also provides Application Control to limit the portions of an application that users can and cannot use (e.g., users may be able to post on Facebook but unable to upload any photos), and provides User Control, which would allow only certain people access to the application.

Another addition to IDS/IPS came about after the 2011 breach on RSA, the security company widely known for its two-factor authentication product. The media referred to the attack as an Advanced Persistent Threat (APT) and later reported that the breach occurred due to a phishing attack that contained a document tainted with malware. Organizations began asking security vendors if they could protect them from a document or executable that has malware embedded in it if the vendor has no signature for that malware. Most security vendors with an IDS/IPS offering could not. Clients were clamoring for an APT remedy, so vendors decided the best fix would be to add sandboxing and/or emulation capabilities on the IDS/IPS, but redesigning the hardware would take anywhere from 12 to 18 months. Meanwhile, companies like FireEye and Fidelis were growing. They were delivering a device with sandboxing or emulation capability that no other network security vendor had at the time. The sandbox was a whole new technology

category addressing the ability to find zero-day malware. Traffic that contained documents or executables via web or email were sent to that Breach Detection System.

Documents and executables would automatically be opened in the sandbox. When anything was discovered to have been malicious, the sandbox would send an alert to an administrator. Although IDS/IPS vendors would not be able to create that type of feature for at least a year, they began using MD5/SHA checksums of known bad files. Each file has a unique checksum. Checksums (also known as hashes or signatures) are strings of characters made from numbers and letters, which can be used to verify the integrity of files and text messages. If the checksum that entered the network matched the checksum the vendor had on file, the sandbox would alert the victim's organization that malware had just entered the network. Back then, this was a milestone for protecting network. Today, this type of technology is being used in NGFWs.

Although Gartner coined the term "next-generation firewall" in 2003 and predicted they would include IPS features and would be offered in 2006, NGFWs were not widely adopted until 2013. At that time they began including IDS/IPS functionality, such as using signatures to identify known attacks and looking for anomalies and protocol deviations in the packet flow.

2016 – Onward: Next Generation Firewalls

Today, most enterprises have adopted NGFWs, and the features they offer continue to grow. Since NGFWs differ by their features, organizations need to decide which are most important to them. NGFWs have pros and cons. The pros are clear: no longer will organizations need to purchase and manage as many devices as they did in the past. The cons include the fact that all those different devices that are lumped together in one device will be using the security and threat intelligence from only one vendor. Each vendor has seen different threats, so when you rely on two separate security teams to provide you with recommended policies, countermeasures and signatures, if one team has not yet seen a new threat that the other team has, you have a good chance of getting the countermeasure from at least one of those teams. So if you use an NGFW, you should augment your threat intelligence from another vendor that has a different purview of the threat landscape.

The threat landscape is constantly changing, and now security vendors are focusing on high-fidelity machine learning, which uses algorithms to analyze files, and uses noise cancellation techniques like census and whitelist checking. As machine-learning grows, attackers will discover ways to get by them too, and IPS vendors will be off to create the next security antidote. As we look toward the future, it's likely that more organizations will be looking at ways to future-proof their environments so they will have access to the latest technology and security professionals to discover, analyze and thwart the latest threats.

[1] *https://en.wikipedia.org/wiki/Expert_system*

Tags: INTRUSION DETECTION SYSTEM INTRUSION PREVENTION SYSTEM FIREWALLS

Enjoyed what you read? Share it!

RELATED CONTENT