How a IDS/IPS can help improve your corporation's network security

By Patrick Mitchell

12/13/2023

To start off some basic definitions should be covered. Intrusion detection system(IDS) is a server that analyzes network traffic to look for malicious events and report them back to you. Intrusion detection systems cannot prevent any attacks and that is where intrusion prevention systems come into play. Intrusion prevention systems(IPS) are similar to Intrusion detection systems but they can prevent attacks unlike IDS's. The next thing to understand is how these devices monitor or know how to find attacks that may be occurring within your network. IDS/IPS's use something called signatures which are known attack patterns and the second thing IDS/IPS's use is something called anomaly(behavior based) detection. The difference between these two methods is that signatures are good for finding attack patterns that have been recycled. A good example of this is a disgruntled employee plugging in a flash drive with malware he downloaded off of tor and put it into a coworkers computer and the IDS catching a signature of the known malware. Quartining that computer from the network and using data sanitization would be the best chain of action. But what about new types of malware? Malware that doesn't have a signature. Well that is where anomaly based detection comes in. Anomaly based IDS/IPS have a normal baseline of what is considered normal within your network and if something out of the ordinary occurs it will flag what is considered suspicious/malicious. Anomaly based detection can help prevent zero day threats within your network. A down side to anomaly based detection versus signature is that it is much more common to receive false positives while using this type of IPS/IDS so that is something to be considered while picking out the right IPS/IDS solution for your network.

The next thing to cover is Host based IDS/IPS's vs network based IDS/IPS. A host based IDS/IPS scans the inbound and outbound traffic of a single computer/endpoint. This very much depends on the use case and how big your corporation is. If you are a one man IT guy working at a small company with 5 users or less you could look into host based intrusion detection/prevention systems. If you are a system administrator at a company with hundreds of end users you could set up a network based IPS/IDS that monitors all the traffic on the network versus all the inbound/outbound traffic on singular endpoints. The more users you have the harder it is to manage host based IDS/IPS especially if you have a large group of end users(1000 plus people) So when it comes to choosing the right IDS/IPS looking at the amount of end users and the size of business is an important aspect to consider when making a decision. Overall these both have their use cases, it just depends on the budget, and size of your company.

The next thing to consider is what types of attacks IPS/IDS can detect, prevent and what types of attack they might encounter in general. Some of the most common attack types are DOS/DDOS (Denial of service and Distributed denial of service), brute forcing, ransomware, spyware, insider threats, supply chain attacks etc. There are many different types of attacks your intrusion detection/prevention system could encounter. A common type of attack that even amateurs can perform is a DDOS attack. A DDOS attack relies on using what is known as a botnet which you can either rent out for a fee or collect your own by infecting computers through malicious domains. After the threat actor has collected his “bots” which are just infected endpoints they are used to launch an attack against your network. One of the most common DDOS attacks is also known as Syn flood attack which works by abusing a TCP connection. A syn flood attack works by rapidly opening a connection with a server. The best way to visualize this is an attacker using his botnet(large group of infected computers) most likely using a script within his c2(Command and control) server that would allow him to use all infected computers to rapidly open up connections to a server which would then cause the server to be overwhelmed and then crash. Another example of an attack that IPS/IDS can run into is known malware. Signature based IDS/IPS are good at detecting malware with known signatures. A good example of malware is a keylogger. A IDS with signature based detection would detect it within a computer or network as long as the keylogger has a signature and isn't a zero day attack. If the keylogger is a zero day attack then having an IDS/IPS that is anomaly based would be more efficient in stopping them as anomaly based is behavioral versus a signature for an already known threat.

The next thing to think about is cost and budget; alongside how many IPS/IDS are needed as well as what type of hardware you will be using. Now a simple snort based IDS can be set up on something as small as a raspberry pi (average MSRP $50) to specialized servers that can run it which can get quite expensive. You can also invest in a next generation firewall which can be expensive but they usually have IDS/IPS services packaged within which helps centralize more services and have less hardware to worry about managing within your organization.There are many different types of software for IDS/IPS. Some of the most well known Intrusion detection systems/prevention systems include snort (which is free and open source), palo alto network which isn't free but they offer a lot outside of IDS/IPS as it is a next generation firewall with IDS/IPS services built into it. Snort and Palo alto networks provide a lot of good information and can help your organization safeguard its network and its information. A lot of what type of IPS/IDS you use also depends on budget. Some organizations may not even have the budget for IPS/IDS or may only have the budget for something small like a Dell OptiPlex or raspberry pi. If you have a bigger budget I would recommend getting a PaloAlto next generation firewall due to the fact that it is very customizable, easy to configure, good user interface, and acts as a firewall alongside a IPS/IDS.
Overall it is best to research multiple possibilities before choosing an IDS/IPS for your business.

The second to last thing to cover is why Intrusion detection systems/ Intrusion prevention systems are important to a business's network security. IDS/IPS are important to network security because not only do they provide monitoring features within your network they also can prevent live cyber attacks from intruding your network. IDS/IPS provide an extra layer of security within your organization alongside your other security appliances such as a SIEM, Firewall, etc. A single cyberattack alone can stop your business from being as productive and can lose your corporation millions of dollars. According to cisa.gov “As one example, thousands of small and medium businesses (SMBs) have been harmed by ransomware attacks, with small businesses three times more likely to be targeted by cybercriminals than larger companies and total cost of cybercrimes to small businesses reached $2.4 billion in 2021.” This example alone speaks volume considering that cyberattacks and information breaches are costing companies billions every year. There are many aspects that go into safeguarding your network such as hiring an IT team and having a group of network security specialists within the IT department, installing and managing software, monitoring network activity, creating security policies, risk factors etc. Having an intrusion detection/prevention system is important due to the fact that it helps you not just have visibility over your network but protection as well. Having network security can help prevent your company from losing money, or important information from being leaked out to the public or business competitors. Overall network security(Physical security as well) is very important to help keep assets, information, documentation, and PII secure.

Overall to summarize, getting an Intrusion detection/prevention system for your business can help prevent threat actors from attacking your network alongside being able to properly identify attacks or data breaches in your network. Depending on the size of your business, your business needs, and budget your option may vary on what type of Intrusion detection/prevention system you may need. If your company has a higher budget you can look into getting a next generation firewall which usually has intrusion detection/prevention systems built into the firewall. A good example of a next generation firewall with intrusion detection/prevention systems built into it is the PaloAlto next generation firewall which can help you efficiently manage SaaS applications such as office 365 and or google suite, it can help monitor and prevent cyber attacks as well as tell you the source of where they came from. Overall intrusion detection/prevention systems are a good layer of network security to include inside your organization. There are many different types of Intrusion detection/prevention systems such as signature, anomaly based, and whether the IDS/IPS is network or host based. It all depends on what you need for your buisiness.

Work cited (MLA):

“What Is IDS and IPS?” *Juniper.Net*, juniper, www.juniper.net/us/en/research-topics/what-is-ids-ips.html. Accessed 12 Dec. 2023.

“Signatures” *Juniper.Net*, juniper, https://threatlabs.juniper.net/home/search/#/list/ips?page_number=1&page_size=20 Accessed 12 Dec. 2023.

“Intrusion Detection System(IDS): Signature vs. Anomaly-Based.” *N-Able.Com*, 15 Mar. 2021, www.n-able.com/blog/intrusion-detection-system. Accessed 12 Dec. 2023.

Ashtari, Hossein. “Intrusion Detection System vs. Intrusion Prevention System: Key Differences and Similarities.” *Spiceworks.Com*, spiceworks, 21 Mar. 2022, www.spiceworks.com/it-security/network-security/articles/ids-vs-ips/. Accessed 12 Dec. 2023.

Baker, Kurt. “Types of Cyber Attacks.” *Crowdstrike.Com*, crowdstrike, 9 Nov. 2023, www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/. Accessed 12 Dec. 2023.

“What Is an Intrusion Prevention System?” *Paloaltonetworks*, www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips. Accessed 13 Dec. 2023.

“Syn Flood Attack.” *Cloudflare*, cloudflare, www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/#:~:text=A%20SYN%20flood%20(half%2Dopen,consuming%20all%20available%20server%20resources. Accessed 13 Dec. 2023.

“Intrusion Detection System(IDS).” *Checkpoint*, Check Point Software Technologies Ltd., www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/. Accessed 13 Dec. 2023.