dms

The Capabilities of an IPS Behind a Next-Gen Firewall

www.dmstechnology.com

A next-gen firewall incorporates elements of an IPS, network traffic monitoring, and other security measures to best protect your network.

But hey, let's be completely honest.

You probably haven't heard of an intrusion prevention system (IPS) before. You probably don't know how it works, nor do you know how it differs from a traditional firewall. You'll be relieved to know that we're going to break down what they do, and how they differ from one another. And we're going to do it right now.

The **firewall** is the stoic guardian of your network. It sits on the edge of your network data, facing the massive amount of digital traffic that wants to get in. While it's a tough guy on the outside, the firewall actually wants to let traffic in. It checks, counter-checks, and counter-counter-checks to see if there are any explicit rules that say that the traffic can pass. If so, it gets the green light and allows traffic to pass safely into your network.

While the firewall is the "nice guy" that looks for reasons to let traffic in, an **IPS** can be likened to a vengeful bouncer at a club. It deeply dislikes network traffic. It will search for reasons (even miniscule ones) to deny entry access to incoming traffic. It checks, counter-checks, and counter-counter-checks to see if there are any explicit reasons to prevent traffic from entering. Since it typically sits behind the firewall in the network, it acts as a double-checking system.

But that's not all.

> "Cybercrime damage costs will hit $6 trillion annually by 2021."
>
> - CSO

An IPS won't just wait for something bad to come its way. It actively searches out threats in your network and works to block them from ever deploying anything damaging. Since it's a fact that cybercrime damage costs will hit $6 trillion annually by 2021, it's more important than ever to have a more secured network. Though they provide similar functions, an IPS can offer your network some serious benefits above and beyond your firewall.

Let's take a look at some of them.

Attack and defend

An IPS has the ability to detect and halt malicious attacks that slip past firewalls and antivirus measures. The technology behind the IPS utilizes several different processes for detecting attacks, and each process has its own operational scope. Because of its wide array variable processes, an IPS can catch a significant number of attacks that would be undetectable to a lone firewall.

Sometimes, the attacks that strike your network are new and unknown. These attacks can't be detected by the use of signature-detecting measures (which is the basis for most network security scanners). However, an IPS can automatically regulate itself and understand the typical data flow of the network. When something highly out-of-the-ordinary occurs, the IPS begins to check for an attack and raises the security level in the process. This is mostly helpful for detecting an incoming distributed denial-of-service (DDoS) attack.

Customize and manage

An IPS doesn't have to be a default and static system. Often, it is configured to run customized scans within the organization's network. Not only can it detect malicious traffic, but it can also prevent the usage of disallowed applications and negate the effects of specific cyberattacks on the organization itself (this can include spear phishing attacks or specifically targeted email spoofing).

Managing an IPS is as pain-free as possible. Due to its wide array of coverage, an IPS consolidates network management by providing a single point of security. This makes it extremely easy to control the traffic throughout a company's network. In turn, that simplifies the scanning for incoming threats and keeps the network infrastructure safer than ever before.

Here's a practical example of the IPS at work: A network administrator knows that the company has been under siege by multiple spear phishing emails. With each spear phishing attack averaging $1.6 million, it's a priority to keep them away from end users. Using their technical knowledge, the network admin creates a rule to block out shared characteristics between each phishing email. With some trial and error, the phishing emails are phased out due to the IPS catching them before delivery.

Keep in mind that not every IPS is created equal. Some may offer more customization than others, but the ability to specify rules and seek out individual traits is common among all systems.

Protect and assist

It's important to note that IPS are good for more than just the management of network traffic threats. They are also fully capable of managing the protection of other elements in your organization's security. If an IPS were set to protect a specific security measure in your network, it would do take two important actions. First, it would prevent the incoming attack from reaching into your network and causing disarray. Second, the IPS would protect the security device itself from an attack. It may seem surprising, but attacks often target your security measures or devices instead of your actual network.

> "... each spear phishing attack averages $1.6 million..."
>
> - Cloudmark

Many times, cyberattackers will try to exploit the security devices within your network to gain further access into your network. Taking down a device gives them more room to avoid being found within your system, giving them free reign. In short, an IPS will ease the workload of the security devices by assisting with network protection for them, as well as device-specific

protection. Using an IPS will prevent overloads of malicious traffic from reaching the security devices while simultaneously driving down usage of processing resources.

Bolster your network security

While remarkably advanced, a next-gen firewall can't do everything on its own. In the modern world of advanced cyberattacks, your business needs something to give you the edge in security.

Leveraging the super-vigilant capabilities of an IPS will keep your network safe and secure from any assault on your infrastructure. However, It's important to note that an IPS is only as good as the people setting it up. It takes people with great technical knowledge and network know-how. Do you want to leave it's effectiveness up to chance? Of course not.

That's where we come in. At DMS Technology, we've skillfully implemented IPS setups throughout many networks. We want to partner with you to take your network security to the next level.

Contact us for more information, or to schedule a consultation to see how an IPS can work for you.

New York Office

780 Third Ave, 15th Fl
New York, NY 10017
United States

P: 212-561-5222
www.dmstechnology.com

London Office

Berkeley Square House, 2nd Floor
Berkeley Square, London W1J 6BD
United Kingdom

P: 0207-084-7155
www.dmstechnology.com