Intrusion Prevention System (IPS)

As businesses increasingly rely on mission-critical data, confidential financial information and intellectual property in the everyday running of their operations, organisations of all sizes have become a valuable target for cybercriminals.

With a distinct rise in cyber attacks in relation to accessing critical company information, knowing who has access to your systems and when they have been accessed should be a vital part of any security process. So what can you do?

What is an IPS and how do they work?

An IPS is a piece of network security technology that works to detect and prevent identified threats in a system. Traditionally working on an individual solution, intrusion prevention systems look to learn your system inside out and continuously monitor your network, looking for anything that appears to be malicious that is immediately reported and blocked. Unlike intrusion detection systems, which are naturally passive and only report threats back, IPS are placed in the direct communication path between source and destination, actively acting on traffic that enters a network or system.

Why do you need an IPS?

As mission-critical data becomes increasingly vital for everyday operations, cybercriminals are ramping up their efforts to steal, access or hold your information for ransom in return for payment.

With an increased scale in the number, complexity and reach of cyber attacks, more clearly needs to be added to protect businesses from falling short in instances of malicious activity. While intrusion prevention systems sound more complex than they need to be, they should be a vital element of your security suite. Due to the nature of IPS, the technology provides your cybersecurity suite with two levels of security; detection and prevention of network security attacks and vulnerability exploits.

A fundamental feature of an intrusion prevention system is its ability to detect and patch vulnerabilities before they are exploited. A vulnerability is simply a weakness in a system or network that can be exploited to gain access or control. When an exploit or vulnerability is released, there is often a window of opportunity for attacks to exploit before a patch can be applied. An intrusion prevention system can be used in such instances to block attacks whilst a fix is put in place.

Why should you use Hyve for IPS?

Here at Hyve, security is at the heart of every service we provide. With this in mind, we have developed an industry-leading IPS solution, that can be seamlessly integrated into your enterprise security information management processes, with no effect on traffic speeds or business operations.

Features and benefits of our IPS

Our IPS is an in-line security appliance that inspects network traffic, identifying malicious, harmful, and/or unwanted network activity and blocking it. We ensure that the continuous inspection is performed in real-time to ensure that good network traffic is able to pass through the IPS without noticeable delay. Features include:

- Daily updates SANS_Dshield blacklisted and dirty IP database
- Spyware sites and blocks spyware calling home
- CVS database
- Stops remote exploits of critical vulnerabilities
- Keeps spyware, viruses, botnet programs and other malware out of the network
- Thwarts advanced hybrid and application-level attacks
- Provides P2P security
- Protects VoIP infrastructure
- Prevents undesired access
- Proactively protects against threats while patches are being tested and deployed
- Improves security posture through acceptable application usage enforcement
- Enables regulatory compliance through the protection of confidential data
- Protects against theft of intellectual property because of undesired access
- Reduces IT hours devoted to fixing/remediating systems infected by viruses, botnets and malware