

CounterSnipe Technologies

IPS Next Generation Perimeter Protection

Introduction

Intrusion prevention technology is the next step in intelligent perimeter control that promises even larger reductions in risk at a lower total cost of ownership. This paper outlines the potential benefit that Intrusion Prevention Systems (IPS) can bring to your organisation.

What is IPS?

As processing power increases and security devices gain the ability to do more complex analysis on data, so does the remit that these devices attempt to reach increase. Traditionally, firewalls only dealt with the analysis of Layer 3 (TCP/IP) information to determine the legitimacy of traffic. Some firewall technology (Application proxies) was focused on management of traffic on higher levels but that is normally limited to the management of either a single or only a few well-known protocols. However, it was found that even though traditional analysis was very effective at providing access control to specific services, there were problems in that it had no ability to scrutinise the specific behaviour of users to determine the legitimacy of their interaction with a large number of network based services. This is where IPS enters the scene and it has some major benefits over traditional firewall technology:

1. It is built on top of firewall technology and extends the functionality thereof rather than attempting to replace it.
2. It explicitly evaluates application traffic for known signatures of unauthorised traffic and prevents this traffic from entering the protected environment.
3. It interacts on either Layer 2 or Layer 3 with the network and is therefore easy to integrate into your existing network security architecture.
4. IPS is built on IDS technology, which aspires to identify unauthorised traffic based on traffic signatures.
5. The signature-based system is focused on known malicious behaviour and therefore reduces the probability of false positives.
6. The signature-based system is also not limited to specific types of network services, but covers most known and wide implement services.

How does this all work?

Different IPS devices obviously have different internal workings, but the bulk of devices are placed in-line with your data stream and all data has to pass through the device. The device then matches traffic patterns with the signatures of known unauthorised behaviour. If a signature matches, the device normally alerts the system administration and drops the packet. It might do a soft drop and terminate the TCP/IP connection or it might do a hard drop by just dropping the specific packet that matched the signature.

What are the potential benefits to your organisation?

The principle benefits to your organisation is a reduction in vulnerability and risk for the following reasons:

1. The bulk of unauthorised traffic now never proceeds beyond your security perimeter therefore current and future unknown vulnerabilities are not exposed.
2. Your incident management process is automated to a certain degree.

Secondary benefits include:

1. A reduction in Incident Management cost because it results in a reduction in the amount of false positives generated by your IDS and therefore and consequent reduction in the load on your incident response team.
2. An improvement in your defence-in-depth because you can now use different overlapping technologies to protect your environment.
3. A general reduction in exposure as the improvements in your Incident Response capability will reduce the amount of pain that you will feel when an incident takes place.
4. A general improvement in your security posture as you now have improved vision and control of your network security posture.
5. Cost improvements through centralised planning, implementation and management.

So, what makes the APD different?

The Active Protection Device from Countersnipe is a market leader in the IPS field for the following reasons:

1. It makes use of the Snort rule syntax and is based on currently available Open Source Snort rules; therefore the product scans for a large number of vulnerabilities and has a high ratio of traffic throughput to false positives.
2. Is based on the world renowned scalable Snort architecture and it is a high performance device (up to Gigabit speeds)
3. The secure web based management interface allows easy remote management of the devices as well as flexible alert management.
4. The APD software engineering framework is based on the Debian APT package management system which means that rule updates, product updates and security updates are of a high quality, and consequently there is little risk in the update process. All you have to do is point your device back to the secure Countersnipe repositories for automated upgrades.
5. The APD software interface is focused not only on alert management, but also on device management. That means that you have the ability to make backups of your own configuration data, view in-depth system performance graphs and manage your rule configuration remotely.
6. You have the opportunity to take ownership of as much of the intellectual property as required by your organisation because the product is based on Open Source Software.

Conclusion

IPS is an exciting new technology that will form an integrated part of the worldwide network security infrastructure and it can bring real world cost and risk savings to your organisation.

About CounterSnipe Technologies

CounterSnipe Technologies is dedicated to the provision of IT security products with a focus on maximum Active Protection of the corporate Infrastructures. The team at CounterSnipe have been working together since early 2002 to develop the flagship product - the Active Protection Device for in line protection of corporate assets. The emphasis is on ensuring a precision delivery of engineering elements in all of the products we build, ensures World class solutions for customers. CounterSnipe is a privately held company, headquartered in Atlanta, Georgia with an ever-increasing presence in the International market.

CounterSnipe Technologies
1230 Peachtree Tower
Suite 1800
Atlanta
Georgia 30309
USA