

# **Intrusion Prevention Systems**

by Nick Ierace, Cesar Urrutia, and Richard Bassett

*Intrusion Prevention Systems are an important component of IT systems defense, and without this technology our data and our networks are much more susceptible to malicious activities.*

*[Richard A. Bassett is an Assistant Professor of Management Information Systems at Western Connecticut State University, where Nick Ierace and Cesar Urrutia are studying MIS security.]*

## **I. Introduction**

Intrusion Prevention Systems, a more advanced version of Intrusion Detection Systems, are now making their mark on the IT industry reaching a new level of network security. An IPS (Intrusion Prevention System) is any device (hardware or software) that has the ability to detect attacks, both known and unknown, and prevent the attack from being successful. Basically an IPS is a firewall which can detect an anomaly in the regular routine of network traffic and then stop the possibly malicious activity.

There are many reasons why someone would want to use an IPS, among these are extra protection from denial of service attacks and protection from many critical exposures found in software such as Microsoft Windows. The capabilities of IPSs are already in use by large organizations and in the near future we will more than likely see private home users utilizing a variation of IPS.

## **II. IPS in Depth**

The necessity to stop attacks and intrusions in real time and to protect valuable assets is why Intrusion Prevention Systems were created. IPS has become an essential next-level of defense for corporate environments that want operational transparency to users while protecting data and network resources. The existence of an IPS appliance should not affect the day-to-day function of the network. The design and configuration of an IPS is a major part in the effective use of the hardware and software available in the market today we will address some key issues for an efficient IPS.

IPSs are active, in-line devices that can drop attack packets or disconnect connections before reaching the host. IPS focuses on what an attack does -- its behavior, which does not change.

In addition to using signatures, IPSs use a set of rules to represent either permissible or harmful behavior. Traffic in real time is then compared to the set of rules and either permitted or blocked. IPSs detect intrusions based on stateful analysis of the traffic passing through them.

An IPS device must utilize Stateful Inspection to perform advanced protection against new types of attacks as well as defend against the growing frequency and scale of DDoS attacks. They perform TCP segment reassembly, traffic analysis, application protocol validation, and signature matching to identify the attack. Each

of these features will affect your network throughput in some manor, depending on the size and capability of the network so it is very important to know the current needs and expected need for future growth.

Large enterprise environments can almost expect to have a bottleneck and system failures if the IPS or the network bandwidth/backbone cannot process expected throughput. If the IPS fails the flow of packets stops and the network becomes unavailable, this is something which should not be allowed to occur. So as you can see there are a number of factors which must be considered when designing IPS. Will the IPS features be built into a switch, router, and/or firewall, or will the device be a standalone IPS? Will it work together with an application based IPS? Where will the device be placed within the network or on the outside? What is the expected throughput and required level of availability, what is the desired user experience? These are the questions that network managers need to ask when installing or using Intrusion Preventions Systems. Internet Security Systems, Fortinet, Lucid Security, 3Com's Tripping Point Technologies, Top Layer Networks are just a few of the major players in the growing field of IPS competitors. Intrusion Preventions Systems is going to become the dominate choice for intrusion systems in the next couple of years and seems to be replacing the IDS which still is in use in combination with current IPSs. The only effective way to know how an IPS appliance will affect your network is to put it in line and see what happens.

Some of the features that have been most common in ISS, Fortinet and TrippingPoint were the use of signature patterns to determine if an attack is taking place. This tends to be an issue with blocking or monitoring, when you have very large signatures sets that your IPS appliance must keep up with; making it difficult to keep latency at bay. The solution is to make sure that the product selected is able to maintain signatures and also give a well built interface which is easy to understand and navigate. Juniper's NetScreen IDP 1000 was rated as having one of the best interfaces with full configuration and management along excellent summary data.

While dealing with the management console software you must also take into account the load these types of applications will put on your servers and how it will affect the performance. Internet Security Systems Proventia G1000-400: recommends that their Site Protector and Site Protector Management Console software components run on separate systems in order to run reports with out bringing the system down. While there are products like Proventia G1000-400, there also is the choice of out-of-the-box solutions like Tipping Point,s UnityOne-1200 Intrusion Prevention System for "set it and forget it" type solutions. If the user doesn't want or need to know all the details involved in IPS this would be an Ideal solution, however one should also be aware of the lacking Interface involved with out-of-the-box products.

### **III. Pros and Cons**

Intrusion Prevention Systems do have weaknesses; however, the downsides can be balanced against the benefits of the systems overall performance. IPSs are a relatively new development, so there hasn't been a tremendous amount of time for IPSs to evolve into what one day they potentially could be. One of the most common problems with an IPS is the detection of false positives or false negatives, this occurs when the system blocks a activity on the network because it is out of the normal and so it assumes it is malicious, causing denial of service to a valid user, trying to do a

valid procedure; or in the case of a false negative, allowing a malicious activity to go by. The main problem with IDS has been that they have produced a tremendous number of alerts one IDS user reported having 1.8 million alerts monthly. This issue has been addressed, but it is very difficult to completely eliminate it. There will almost always be false positives; however it should be one of the main goals of the network administrators and the manufacturers of IPSs to minimize this as much as they can. False positives are typically generated by systems that rely on a single detection method, and by ones that cannot be configured at different levels to fit into the operational environment. If an IPS uses multiple techniques to detect malicious activities and inspect the incoming packets there is lesser chance of having false positives/negatives. Network administrators should be able to minimize false positives and false negatives by thoroughly training the IPS, by training in the initial installation phase and also continuing to train the system as it is online. The network administrator must tell the IPS that certain jobs are non-malicious and should not be red flagged as well as continue to update the IPS for new malicious activities that it may not be aware of, such as new viruses.

Unfortunately the detection of false positives are not the only downside to Intrusion Prevention Systems, for the best results you would want to have IPSs deployed in multiple spots on the network. If you are concerned with DDoS/Syn Flood type attacks, you'd probably put us close to the edge of the network, between the router and the firewall. If you are more concerned with attacks on your critical resources (server farms, e-mail, databases, etc.) you'd deploy us directly in front of those resources. The problem is that the IPS starts to be quite expensive, as each of these IPSs tend to run anywhere in between \$25,000 and \$80,000 depending on the amount of users that are being supported. If there are multiple IPSs on the network then every packet of data must make multiple stops from its original destination to get to the end user, this will cause loss of network performance, and this also causes another problem.

In a typical location, the aggregated traffic on a switch's span port can nearly be a gigabit. Systems that cannot handle such traffic volumes start to lose packets. This in turn may result in false negatives. On top of the possibility of the network being slowed down by the IPS, if the IPS is over worked, and too many packets are coming in, it will drop packets, exposing a false negative if malicious traffic gets through this way. As time goes on faster IPSs will be created and in fact most IPSs available today can handle up to a gigabit of traffic, network administrators should be aware of the bandwidth capabilities of a IPS and be sure to find one suitable for their network traffic.

All though today's IPSs have come a long way from where they originally started there are still issues that must be worked out; however, even with these downsides the benefits that we receive from IPSs lead us to a protection that any one other security method can not provide. It has the ability to act like antivirus software by detecting malicious signatures, stopping them and then auditing (showing capabilities of a honeypot) where they are coming from and where they are trying to go. IPSs can prevent exposures in many software programs that would allow hackers to damage data on a users system or cause an overflow of network traffic. This is one of the biggest advantages of the IPS, as it should give software manufacturers a significantly greater amount of time to look for any backdoors in their programs before hackers/malicious users have the opportunity to expose them. This is also beneficial to corporations or very large networks where not every computer has the most recent critical updates.

The usefulness of an IPS becomes evident for many school university network administrators, where the most common issue that they would face are personal computers on their network with out antivirus software and outdated security patches. Something that we may begin to see more of is application level IPSs. These would be programs built into an operating system that are very similar to the hardware type IPS, however would only monitor flow on that client work station, or at a server. Disadvantages of this software would be similar to that of the hardware version, false positives, but this would be to a greater degree in the sense that the user may not be computer savvy and if a procedure they are trying to perform comes up as a malicious activity in the IPS and they are cut off, it becomes time consuming for the IT department to have to check on every computer that has a false positive scenario. If an application level IPS is installed on a client workstation it can be designed specifically for that person, which makes it an even more secure IPS than that of the hardware level IPS that would be placed to block all of the client computers. This means that there can be a more specific set of rules for that workstations IPS to follow, making it even harder for malicious activity to work its way around the IPS and lowering the amount of false positives.

#### **IV. Real World Applications**

The actual effects of an IPS in a real world environment become visible when we look into the case of Widener University. The main goal that Widener University had was to protect their databases as well as their users on their main network; the major difficulty in doing this was their large amount of foreign computers with access onto their network. This meant that they had many students, computers connecting onto their network with already infected and un-patched software. This is a challenge many institutions and corporations also have as they open their networks to mobile workers, students, and other authorized guests. The way which Widener University used a IPS to address this issue was by placing a IPS in front of the firewall for incoming traffic from external sources, and then placing another IPS behind the firewall for outgoing traffic from internal users, accessing their databases. This proved to be very helpful on the Universities network and was able to stop attacks from malicious code such as MS Blaster and Welchia worm.

The Widener University case shows that IPSs can play a very valuable role in network security. With out the use of this IPS the University would have faced a tremendous amount of work for its IT department in efforts to clean up any damages done from the infiltration of malicious codes. The IPS prevents a large amount of downtime that would occur if it were not there, this is done by it stopping any damage that may have made its way to the databases from internal or even external attacks. The IPS also makes it easier for the administrators to see where attacks are coming from so that they can address them and prevent any further attacks from that location.

#### **V. Ethics**

Ethical issues that should be addressed with Intrusion Prevention Systems are among most standard ethics that any network administrator would have to follow. There should be a standard set of ethic guidelines specifically for that company,s network administrator, as this administrator has access to all data on any server databases where much confidential data is stored. Administrators have the ability to look through anyone's files; however in most generic codes of ethic it is listed, even

though they do have permissions and access to other user files, they should only be going into those files with the knowledge and permission of the files owner.

The IPS will require similar ethic codes to be followed as every packet of information that flows through that network will go through the IPS and be thoroughly inspected. If an anomaly or a signature is found within a packet and it is then looked through by the network administrator, that data could be confidential and should remain inaccessible to any public users. This means that all audit logs containing any anomalies or signatures that were red flagged, must be considered confidential data. If the audit logs are accessible to unauthorized users then the results of this could be very significant and damaging to that company depending on what data was being stored in the audit logs.

Ethics must be displayed at all times by network administrators; they must show good judgment and should contact a user before looking through their data. If a job process is stopped by an IPS, the administrator should notify the user if they are not yet aware, and then gain their permission to analyze that data to see what the anomaly was within the data. The administrator should not share any information that he may find within the inspection of that data and must be able to ensure the confidentiality of that data. Ethics are important and guidelines should be set when using an IPS to ensure the security of any data that may be passing through an IPS. Ethical and moral issues such as privacy when embracing new applications are common ethical dilemmas network professionals have to face, but its more then just your ethical prospective. You might be confident in your personal ethics, but what about those of your department or company, it's important to maintain your company,s code of ethics and make sure your end users and IT staff are aware and understand the code of ethics.

## **VI. Conclusions**

IPS is a powerful security system and it's proving to make a significant impact in information systems. As time goes on we will see IPSs expand out into more organizations as another defense in keeping data secure. IPSs capabilities range from being able to stop DDoS attacks, to protecting un-patched security exposures on workstations or zero day attacks. There are different forms of IPSs and we can anticipate more variations as more companies enter the IPS market. There are limitations of IPSs however these limitations for the most part can be worked around, the amount of users going through a IPS must be delegated and monitored, if too many users or too much network traffic is attempting to be processed by a IPS, packets can be lost allowing malicious activity to bypass the system.

IPSs have only been out in real world applications for a short time and in approximately five years they have already grown rapidly. The amount of network bandwidth that can be handled through IPS units has grown substantially from the initial IPSs as there are now units capable of supporting up to a gigabit per second; however a unit like this becomes quite costly. The biggest issue that network administrators and manufacturers of IPSs face is the matter of false positives and false negatives. These prove to be a significant problem as a false positive can end up causing a denial of service, something which the system is designed to prevent. We see in false negatives a need for a more strict set of rules for the IPS to follow, or we will see malicious activity working its way through our IPS. The major dilemma is how strict the IPS rules can be to the point that there are n amount of false positives to prevent n amount of false negatives.

In the end we see that IPSs are useful and have proven to make significant differences on large networks where many attacks are evident. We can expect to see different forms of IPSs evolving to match the needs of our business world, such as IPSs built into system applications. IPSs are another line of defense that we can count on to keep our data even more secure, however at this point in time, in order for a IPS to be necessary on a network, it would have to be protecting very valuable data, or ensuring the uptime of a very large and busy network, due to the high costs of a IPS.

### **Principal Works Consulted:**

1. *Desai, Neil. Intrusion Prevention Systems: the Next Step in the Evolution of IDS.* Accessed on February 5, 2005. Available at <http://www.securityfocus.com/infocus/1670>
2. *Stonesoft. Winning the Battle Against False Positives.* Accessed on February 13, 2005. Available at [http://www.stonesoft.com/files/products/StoneGate/SGWP\\_winningTheBattleAgainstFalsePositives\\_print.pdf](http://www.stonesoft.com/files/products/StoneGate/SGWP_winningTheBattleAgainstFalsePositives_print.pdf)
3. *Shepard, David. Regional Sales Manager Top Layer Networks.* Accessed on February 7, 2005. Available at [dsheperd@toplayer.com](mailto:dsheperd@toplayer.com)
4. *Mathis, M. Fragmentation Considered Very Harmful.* Accessed on February 20, 2005. Available at <http://www.psc.edu/~jheffner/drafts/draft-mathis-frag-harmful.XX.html>
5. *Top Layer Networks, Inc. Case Study Attack Mitigator IPS.* Accessed on February 7, 2005. Available at <http://www.toplayer.com/pdf/widenercase.pdf>
6. *Sequeria, Dinesh. Intrusion Prevention Systems: Security's Silver Bullet?* Accessed February 20, 2005. Available at <http://cnscenter.future.co.kr/resource/security/ids/03-03sequeira.pdf>.
7. *Raja, Sanjay. Network Intrusion Prevention.* Accessed on February 7, 2005. Available at [http://www.toplayer.com/generic/TLN\\_Stateful\\_WP.pdf](http://www.toplayer.com/generic/TLN_Stateful_WP.pdf)
8. *Ethan Allen.* Accessed on February 28, 2005. Available at <http://www.fortinet.com/doc/FGT400ADS.pdf>
9. *Joanne Cummings. Six Ways to Stay Ethical*  
07/21/03<http://www.nwfusion.com/you/2003/0721ethicsside.html>

Source: *Ubiquity*, Volume 6, Issue 19 (June 1-8 2005)  
<http://www.acm.org/ubiquity>