

PREVENTION!!! – Network Intrusion Prevention Systems

By Jalaynea A. Cooper

Oh no! Jack's End of the Month files are gone! What! Jane's business contacts file is gone. Everyone on the network is missing something important.

This could have been PREVENTED, if they had been prepared by using a NETWORK INTRUSION PREVENTION SYSTEM!

While there are many types of Intrusion Prevention, this paper is about Network Intrusion Prevention Systems. What is Network Security?, Network Attacks and Detection, Network Intrusion Prevention, and the Future of Network Intrusion Prevention Systems. By reading this information, hopefully what happened to Jack or Jane will not happen to you!

To be completely clear about network security, it can never totally be defined. Security is in the eye of the beholder. In order to build a secure network, the key is to define what security means for to you, your company, and your organization. Follow the steps below to help build a secure network:

1. Of course, define a policy by what security means
2. Evaluate everything that goes on the network according to that policy.
3. An important note is to not make network security non-user friendly. Don't give them a reason to find ways to go around the network security. ²

What is Network Security?

Security that consists of provisions made in a computer network infrastructure, policies adopted by the network administrator to protect the network, and network-accessible resources from unauthorized access combined can be defined as Network Security. ⁴

Network security is also made up of the following:

- Starts with authenticating users
- A firewall accesses allowable policies and services to users, however does not check for harmful contents over the network.
- An NIPS detects these harmful contents over the network and monitors for suspicious traffic. ⁴

Network Attacks and Detection

To begin with, let's start with network threats and then how to detect them.

There are different types and sources of network threats. Two of the main attacks are Denial-of-Service (DoS) and Unauthorized Access.

▪ DoS

DoS is the type of attack that is labeled as the nastiest and most difficult to address. DoS attacks are easy to be launched by the attackers, hard to track, and the attackers make them hard to be refused without refusing authorized requests for service. ²

▪ Unauthorized Access

The object of unauthorized access attacks is that access of some resources is given to the attacker when they should not be given.

Executing commands illicitly, confidentiality breaches, and destructive

behavior are all examples of unauthorized access.²

Intrusion detection systems are older than intrusion prevention systems. IDS are usually further broken down into signature-based and anomaly-based which has been around since late 80s and early 90s. Signature-based intrusion detection systems work by looking for patterns that match known malicious events. Anomaly-based intrusion detection systems work by looking for anomalies that are in the network protocol, behavior patterns, or system calls.¹⁴

Sensors...Console...and an Engine. All of these things are components of an intrusion detection system. Sensors are used to generate security events. A console is used to monitor events and alerts, and to control the sensors. An engine is used to record events that are logged by the sensors.⁴

IDS monitor the traffic for unwanted and suspect activity. These systems are dependent on external response mechanisms.¹¹

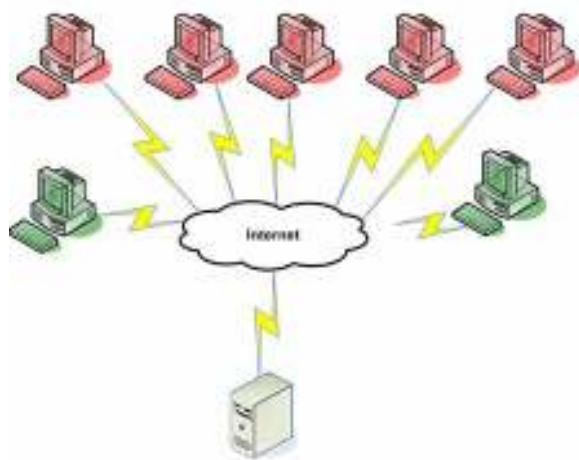


Figure 1: In a DoS attack, multiple devices (red) flood a server with requests, overwhelming the server and blocking legitimate users (green).¹²

NIPS	vs.	NIDS
Acts as network gateway		Only observes network traffic
Stops suspect packets		Logs suspect packets and generates alerts
Prevents successful intrusions		Cannot stop an intruder
False positives are VERY bad		False positives are not as big of an issue

Table 1: NIPS vs. NIDS¹⁰

Network Intrusion Prevention Systems

What is a network intrusion prevention system? This has become more and more of an inquiry. Intrusion prevention systems were invented in the late 1990s. The first IPS was the BlackICE product from NetworkIce Corporation.⁷ “Network intrusion prevention systems are usually hardware devices that are situated in the network.”¹

Intrusion detection systems were detecting attacks, but were not preventing them so enters intrusion prevention systems. Intrusion prevention systems are used to monitor networks for unwanted behavior and to prevent this behavior.⁴

An intrusion prevention system’s key components consist of the global and local host access controls, IDS, global and local security policy, risk management software, and globally accessible consoles for managing IPS.¹⁵

With the use of intrusion prevention systems, the inconvenience of examining the alerts and correcting the damage done by successful attackers is considerably reduced.⁶

Another question posed is “What will NIPS Provide?” A network intrusion prevention system is used to protect the confidentiality, integrity, and availability of

the network. Electronic information on the network will be protected from attackers, therefore maintaining the network's confidentiality. The integrity will also be maintained due to the fact that information was not compromised, that Company A is worth my business versus Company B that has a security breach every month. Finally, availability. Network intrusion prevention systems help to protect the availability of a network by preventing such threats as unauthorized use and DoS.⁹

Future of Network Intrusion Prevention Systems

Not only Network Intrusion Prevention, but Intrusion prevention is anticipated to grow rapidly in the future. IPS is not expected to replace IDS. Instead, both will be used together in order to provide maximum network protection. Advancement in data correlation and alert fusion methods also play a part in the advancement of NIP systems. It is also predicted that due to the improvements in the future that forensics functionality in NIPS will be improved.³

Basically, as technology and network intrusions continue to advance and grow; the same goes for the Network Intrusion Prevention Systems that protect them. Look forward to seeing more and more NIP systems as time moves on!

Examples

One of the top Intrusion Prevention Systems is the *TippingPoint IPS*.



Figure 2: TippingPoint Intrusion Prevention System⁵

The price on this NIP system will range around \$4,995-\$169,995. At gigabit speeds, this system provides application, performance, and infrastructure protection.⁵

Another top NIP system is the *Symantec Network Security 7100 Series*. This system will cost around \$11,300. Protocol anomaly, signature, along with statistical and vulnerability attack interception techniques are used to keep attacks - (known and unknown) from spreading throughout the networks.⁵

McAfee is said to have the industry's most advanced and proven intrusion prevention solution. One of the key advantages is that this system improves time-to-protection and time-to-confidence with real-time security that is automated and actionable. Performance ranges from 100 Mbps to multi-Gbps. Models range from I-1200 to I-4010. To compare these models see:http://www.mcafee.com/us/enterprise/products/tools/network_intrusion_prevention/intrushield_app_chart.html.⁸



Figure 3: McAfee IntruShield Network IPS⁸

Questions to ask your NIPS vendor
<ul style="list-style-type: none"> ▪ Where is this product designed to sit on the network?
<ul style="list-style-type: none"> ▪ How does this product discover machines and services running on the network that need IPS protection?
<ul style="list-style-type: none"> ▪ Does your product have a learning mode, how long does it take, and how do you recommend running it in learning mode?
<ul style="list-style-type: none"> ▪ How easily can you run this product in an alert-only mode?
<ul style="list-style-type: none"> ▪ What kinds of traffic can this product block?
<ul style="list-style-type: none"> ▪ What are the action options offered by this product once malicious traffic is discovered? Ex. Drop-only, pass and track, pass and alert, pass but limit.
<ul style="list-style-type: none"> ▪ What kind of communication happens between the IPS device and either an installed firewall or a built-in one?
<ul style="list-style-type: none"> ▪ Does the product provided centralize configuration and/or management capabilities?
<ul style="list-style-type: none"> ▪ What are your configuration options (rules per port, per system)?
<ul style="list-style-type: none"> ▪ What is the overall strategy to alert you of both malicious activity and of blocked traffic?
<ul style="list-style-type: none"> ▪ What is the product's reporting capabilities?
<ul style="list-style-type: none"> ▪ Does this product have the ability to connect to a Security Event Management system via some event reporting mechanism?
<ul style="list-style-type: none"> ▪ If this device's log fills, will it continue to operate without logging?
<ul style="list-style-type: none"> ▪ Does the vendor offer log analysis tools for forensics and capacity planning?

<ul style="list-style-type: none"> ▪ What secure management access methods does this device support? Are these the only methods enabled by default?
--

Table 2: Questions to ask your NIPS vendor¹³

Conclusion

Network intrusion prevention systems (NIPS) are usually classified as a combination of intrusion detection systems and firewalls. NIPS are used as a great way to prevent attacks from happening on the network.

Since network intrusion prevention systems are fairly new, the enhancements and features of a NIPS are still growing and will continue to grow.

As everyone knows; networks enhance more and more everyday. Along with these enhancements, attackers find new ways to threaten networks. To follow the attackers, more ways are invented to prevent this intrusion of the network. So from network intrusion prevention systems to network attackers, "Bring It On!"

Resources

1. Crystal, G. (2007). *What are the Different Types of Intrusion Prevention?* Retrieved October 26, 2007, from Wise Geek: www.wisegeek.com/what-are-the-different-types-of-intrusion-prevention.htm
2. Curtin, M. (1997, March). *Introduction to Network Security*. Retrieved October 02, 2007, from <http://www.interhack.net/pubs/network-security.html>
3. Future of Intrusion Detection & Prevention. In C. Endorf, p. E. Schultz, & J. Mellander, *Intrusion Detection & Prevention* (pp. 345-359). McGraw-Hill.
4. *Intrusion detection system*. (n.d.). Retrieved October 02, 2007, from <http://en.wikipedia.org>
5. *Intrusion Detection/Prevention*. (2007, April). Retrieved November 26, 2007, from Search Security: http://searchsecurity.techtarget.com/magazinePrintFriendly/0,296905,sid14_gci1257119,00.html
6. *Intrusion Prevention Systems (IPS)*. (2004, January). Retrieved October 26, 2007, from <http://nsslabs.com/WhitePapers/intrusion-prevention-systems.htm>
7. *Intrusion-prevention system*. (n.d.). Retrieved December 01, 2007, from Safe 'n' Sec: <http://www.safensoft.com/security.phtml?c=587>
8. *Network Intrusion Prevention*. (n.d.). Retrieved November 26, 2007, from McAfee: http://www.mcafee.com/us/enterprise/products/network_intrusion_prevention/index.html
9. *Network Intrusion Prevention*. (n.d.). Retrieved November 26, 2007, from McAfee: http://www.mcafee.com/us/local_content/white_papers/wp_nps_justification_roi.pdf
10. *Network Intrusion Prevention Systems*. (n.d.). Retrieved November 26, 2007, from <http://www.mycert.org.my/mycert-sig/mycert-sig-05/slides/mycert-sig5-nips.pdf>
11. Roesch, M. (2005, September 12). *Search Security*. Retrieved November 26, 2007, from Next-generation intrusion prevention: Time zero (during the attack): http://searchsecurity.techtarget.com/ti/0,289483,sid_gci1121310,00.html
12. Sullivan, D. (2007, January 26). *Network-based attacks*. Retrieved November 26, 2007, from Search Security: http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1238059,00.html
13. *Top 20 (or there about) Questions for your IPS vendor*. (2004, February 16). Retrieved December 01, 2007, from Network World: <http://www.networkworld.com/reviews/2004/0216ips20qs.html>
14. Vossen, J. (2004, January 21). *The ABC's of intrusion detection*. Retrieved November 26, 2007, from Search Security: http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci945521,00.html
15. Yakabovicz, E. P.-C. (2003, November 10). *IDS and IPS: Information security technology working together*. Retrieved November 26, 2007, from Search Security: http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1049326,00.html