Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth

Over the past few years many papers and books have included articles explaining and supporting either Intrusion Detection Systems (IDS) or the newer technology on the security block, Intrusion Prevention Systems (IPS). Few have reviewed the value of implementing both IDS and IPS technologies. Most papers pit the technologies against each other in a comparison or they show the evolution of IDS and the roadmap to IPS. This paper takes a different approach and places value in both technologies and how they may be deployed...

Copyright SANS Institute
Author Retains Full Rights

AD

Understanding IPS and IDS:

Using IPS and IDS together for Defense in Depth

© SANS Institute 2004, Author retains full rights.

Ted Holland
GSEC Practical v1.4b, Option 1
February 23, 2004

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Table of Contents

Table of Contents 2
Abstract 3
Introduction 3
Terms 4
  Intrusion Detection System (IDS) 4
  Host-based Intrusion Detection System (HIDS) 5
  Intrusion Prevention System (IPS) 5
Architecture Suggestions and Concerns 5
  Intrusion Detection System (IDS) 5
  Intrusion Prevention System (IPS) 7
  Staffing and training 9
Conclusion 10
References 11

© SANS Institute 2004, Author retains full rights.

Abstract

Over the past few years many papers and books have included articles explaining and supporting either Intrusion Detection Systems (IDS) or the newer technology on the security block, Intrusion Prevention Systems (IPS). Very few papers have reviewed the value add of having both IDS and IPS technologies working together. Most papers pit the technologies against each other in a comparison or they show the evolution of IDS and the roadmap to IPS. This paper takes a different approach and places value in both technologies and how they may be deployed together to provide a stronger security posture.
The purpose here is not to give the reader a single architecture for deploying IPS or IDS but the background and perspective to knowledgeably choose the technology that will help to enhance their corporate security environment. The use of both IPS and IDS technologies will greatly enhance the corporate security environment when properly configured and managed. These two tools provide critical pieces to the corporate defense in depth strategy. It is not the intention of this paper to go into the technical details associated with IPS or IDS technologies but rather cover the high level aspects of the technologies, implementation suggestions, and the concerns of IPS and IDS as they relate to staff, training, and performance.

Introduction

Networks were discovered and have been built for many years. Depending on the depth of investigation, the idea of data networks could be traced back hundreds of years. In this paper we will focus on the more recent use of networks stemming from the 1960s and 1970s. Once networks had been discovered and built, the potential for intrusion of those networks also became a reality. In response to intrusion came the idea of intrusion detection. The term IDS has been defined many ways since those early discoveries because the inevitable requirement that stems from discovering a new technology is the need and interest in monitoring that technology. Complementary to monitoring is the ability to report on new technologies and show the value of it to one's peers and business associates. Additionally there is always someone who will test the new technology to ensure that it is stable and consistent. Testing usually leads to the identification of vulnerabilities which in turn leads to the possibility of intrusion.

The next logical step after discovering a technology and the inevitable vulnerabilities associated is to identify the security parameters. One way to help determine these security parameters is to build a formula to represent the idea of security. Intrusion.com provides the following formula:

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Security = visibility + control[1]

This formula is the basis for the underlying purpose of this paper. IDS technology provides the visibility and offers many other benefits directly related to monitoring our networks. These include the active visibility of what is happening on our networks as it takes place as well as the ability to store this information for analysis and reporting at a later date. Visibility is paramount to decision making. Visibility makes it possible to create a security policy based on quantifiable, real-world data.[1] The other piece of the formula is control and will be covered in more detail in this paper through the research of IPS technology. It is IPS technology that provides an active ability to control our networks. Control is paramount to enforcement. Control makes it possible to enforce compliance with security policy.[1]

The term IPS has been thrown around for the past few years and is still being more precisely defined as the technology matures. The definition of IPS being used for the purposes of this paper is the ability to detect and prevent activity on or being introduced to a corporate network. There are multiple ways of providing this IPS capability and we will cover a few within this paper. In particular, we will look at the strengths and weaknesses of combining IPS and IDS technologies together. Unfortunately, most organizations that operate large internal networks are bound by the financial and man-power limitations of reality, and lack the resources, one way or another, to deploy the dozens or even hundreds of individual appliances necessary to operate an effective defense in depth strategy.[2] As we breakdown the various resource issues surrounding a good defense in depth strategy related to IPS/IDS technology we will discover why the use of both technologies in harmony is a fitting solution for most mid to large sized corporations.

Terms

Intrusion Detection System (IDS)

Intrusion Detection is the art of detecting inappropriate, incorrect, or anomalous activity. Among other tools, an Intrusion Detection System can be used to

[1] Corporate White Paper. "Deploying and Tuning Network Intrusion Detection Systems." Intrusion.com White Paper. 2001 (2004): 3

[2] Eagle, Liam. "Enabling the Defense in Depth Security Strategy." The Web Host Industry Review. 16 April 2003. URL: http://thewhir.com/features/depth-security.cfm (6 Jan. 2004).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

determine if a computer network or server has experienced an unauthorized intrusion. [3]

Host-based Intrusion Detection System (HIDS)

A host IDS needs to be deployed on each protected machine (server or workstation). It analyzes data local to that machine such as system log files, audit trails and file system changes, and sometimes processes and system calls. HIDS alerts the administrator in case a violation of the preset rules occurs. Host IDS might use pattern matching in the observed audit trails or generate a normal behavior profile and then compare current events with this profile.[4]

Intrusion Prevention System (IPS)

An Intrusion-prevention system is used to actively drop packets of data or disconnect connections that contain unauthorised data. Intrusion-prevention technology is also commonly an extension of intrusion detection technology (IDS). [5]

Architecture Suggestions and Concerns

This architecture is being presented as a solution that will provide a high return on investment based on visibility, control, and uptime. The architecture also keeps in mind that many corporations have either implemented a partial solution or no solution for intrusion detection or prevention at this time. Using a hybrid deployment, the average mid to large size company will be able to leverage the cutting edge technology provided by the IPS while also taking advantage of the proven and mature capabilities of the IDS.

Intrusion Detection System (IDS)

First we look at the traditional IDS deployment. Most companies that have IDS installed have placed these devices in the perimeter either between the border router and the firewall or they have placed the IDS outside of the border router. The companies that have gone the extra mile to install an IDS outside of the firewall and border router have done this so that they might see the full breadth of attempted attacks against their organization. When deploying an IDS both outside perimeter devices and inside of perimeter devices a company can confirm weather or not a potential attack seen outside of the perimeter has

---

[3] Tünnissen, Jacco. "Intrusion Detection, Honeypots and Incident Handling Resources." Honeypots.com. 13 January 2004. URL: http://www.honeypots.net/ (17 Jan. 2004).

[4] Chuvakin, Anton. “Network IDS Shortcomings:
Has NIDS Reached the End of the Road?” SC Infosec Opinionwire. 6 February 2002. URL: http://www.infosecnews.com/opinion/2002/02/06_02.htm (12 Jan 2004).

[5] "Intrusion-prevention system." Wikipedia. 15 December 2003. URL: http://en.wikipedia.org/wiki/Intrusion-prevention_system (7 Jan. 2004).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

successfully made it past border routers and firewalls inside. The later approach requires more resources but provides a clearer picture on a corporate ingress/egress point and security posture. Having an IDS in either of these locations also provides a tool that captures data for analysis and possibly forensics as needed.

Most companies have deployed IDS devices on the perimeter in what is called an out of band architecture. This means that the IDS sits on a shared media and captures as many packets as it can handle in a promiscuous mode and reports this data back to a management console. Another way to deploy an IDS on the perimeter is what is called an in-line deployment. This means that all data coming into or leaving a corporation passes through this device. Another example of a device that uses an in-line architecture is a router or a firewall. Having an IDS in-line means that all data will be captured prior to it continuing into the corporate network. The downside to this type of architecture is that if the in-line device fails, depending on the configuration, all data will either continue without IDS visibility or it will stop until the IDS is fixed or removed. Either one of these deployments of in-line IDS places the company at risk if the device fails either by stopping traffic flow or blinding the company by allowing all traffic to flow without being monitored.

The most important concept in the deployment of an IDS is that an IDS is a tool used to capture and provide visibility into a corporate network. For larger companies and companies that have an added need for full visibility into network traffic, a common deployment method is to install IDS devices at all primary network points to provide visibility internally as well as externally. This type of deployment provides data needed to track down potential internal threats as well as those being posed against the company from outside. Still today the greatest risk comes from insider threats. Disgruntled employees, curious employees, outsourced services, and the trends of greater volumes of contracted services provide a higher level of vulnerability from within the network. As a result, the importance of deploying a mechanism to monitor internal traffic is paramount. The key being stressed at this point is visibility.

One concern of IDS deployments is the performance factor. The IDS solutions offered today have come a long way in design and the use of high-performance components that help to ensure the greatest amount data capture. Even with the higher performance components and updated software, a known fact is that current IDS implementations have a tendency to drop packets due to the high throughput of today's high bandwidth network devices. Performance is a key issue in both IDS and IPS deployments. Another concern with IDS deployments is encryption. Currently, most IDS solutions do not have the ability to decrypt packets inbound or outbound and this blinds security administrators as to what is coming into and going out of corporate networks. With the explosive growth of VPN and other encrypted data streams the need to have a solution like IPS at the perimeter is becoming more and more necessary. Laura Tyler provides

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

insight to both problems, switched networks and encryption, in her support of implementing both IDS and IPS technologies in an article she wrote for TechRepublic. Here is Laura's comment, "There are a few fundamental problems with how some IDSs work today. First, as more and more network traffic becomes encrypted, IDSs become useless because they can't parse encrypted traffic. Second, as networks become more heavily switched, they typically see only a small amount of the traffic on your network. On a switched network, you need to greatly increase the number of intrusion detection sensors to monitor traffic on all the network segments. On large networks, this means that the total cost of ownership of IDSs can be very high. Third, IDSs generate a huge number of false positives, telling you that your network is being attacked when it's not. These three problems are leading many companies to switch to IPSs."[6]

Some companies have added what are called Host-based IDS (HIDS) deployments to their organization to provide a more granular level of visibility. Using a HIDS provides the visibility needed to identify and track intrusion attempts on a specific host or application. We will cover the defense in depth strategy later in this paper when we emphasize the importance of using multiple levels of intrusion detection and prevention in order to provide a more secure computing environment. The use of HIDS technology has become popular also as a result of the explosive growth of switched networks. The trend away from a shared network medium has caused a need to rethink IDS deployments due to their passive nature in capturing data from a shared medium. HIDS are a result of this paradigm change and as a result provide a high level of visibility into each network node. A challenge to security administrators in some cases is the volume of data generated from these deployments and those companies with small security staffs are especially concerned. Staffing, training and resource issues will be covered in more detail later in this paper.

Intrusion Prevention System (IPS)

Next we look at the Intrusion Prevention System (IPS) and the deployment strategies associated with this technology. IPS technologies in either software or hardware are relatively new. One could say that the idea has been around for a long time and might suggest that router access control lists or firewall rules might be considered a basic IPS. Neil Desai opened an article posted on the SecurityFocus web site with this statement, "You blended your IDS with my firewall! No, you blended your firewall with my IDS! Either way, when you combine the blocking capabilities of a firewall with the deep packet inspection of

---

[6] Taylor, Laura. "Intrusion detection in not intrusion prevention." ZDNet Australia. 9 February 2004. URL: http://www.zdnet.com.au/insight/0,39023731,20267597,00.htm (11 Feb. 2004).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

an IDS, you get the new kid on the block: intrusion prevention systems or IPS."[7] The truth is that the IPS market place is just starting to mature enough to actually identify what an IPS really is. Still today there are many definitions for IPS and many views as to the requirement for IPS implementations. Some groups even suggest that IPS is an evolution of IDS and that eventually the IDS will disappear and all intrusion related products will focus around prevention. A company by the name of Sourcefire is working on a term and product line that combines multiple technologies in what is called "Real-time Network Awareness (RNA)". RNA enables organizations to more confidently protect their networks through a unique patent pending combination of passive network discovery, behavioral profiling, and integrated vulnerability analysis to deliver the benefits of real-time network profiling and change management without the drawbacks of traditional approaches to identifying network assets and vulnerabilities.[8] The reality is that weather or not the IDS is placed in a museum or not, the need to capture and track data traversing our networks will be of paramount importance. In addition to Sourcefire's RNA technologies that are trying to bridge the gap between IPS and IDS functionality, other companies are building IPS technologies around the premise of identifying and stopping intrusions vice tracking the intrusions and capturing data for analysis or forensics.

The idea of an IPS denying traffic is the most important aspect regarding this paper. Many corporations have not deployed IDS technology or entertained IPS technology for one primary reason. This reason is that time is money and network availability is paramount to all organizations. The argument can be made that an IPS or IDS deployment is actually a technology that helps ensure network uptime and availability by identifying and possibly preventing network intrusions and attacks that would normally be the cause of network downtime. The costs associated with an IPS or IDS deployment are not typically associated as a revenue generating expense. In many cases the argument can be made that the decision to deploy IPS or IDS technology is like the chicken and the egg analogy. Because IPS and IDS deployments do not directly generate revenue it is hard to justify the expense. However, the opposite of this argument is that without visibility into the network and the ability to prevent intrusions and attacks there is a potential increase of costs associated in dealing with such activities. One could argue that with a properly configured IPS deployment, a company could save money through identifying and preventing a worm or virus attack. As companies develop matrices to quantify the amount of money and/or time lost due to virus or worm attacks they will have the supporting information to justify the costs associated with IPS and/or IDS deployments.

---

[7] Desai, Neil. "Intrusion Prevention Systems: the Next Step in the evolution of IDS." Security Focus. 27 February 2003. URL: http://www.securityfocus.com/infocus/1670 (14 Jan 2004).

[8] "Real-time Network Awareness." Sourcefire. February 2004. URL: http://www.sourcefire.com/products/rna.html (14 Jan 2004).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

As companies begin to realize the potential savings associated with preventing the downtime associated with one of the almost weekly worm or virus attacks they will be more inclined to leverage preventative measures like IPS technologies. Likewise the use of IDS technologies can be used to confirm the time savings and provide the data needed to address insider threats. Over the past few years we have seen an increase in the level of responsibility associated with using technology. The multiple compliance requirements levied on companies by federal organizations also places the IT departments on alert from the standpoint of having to provide policies, procedures and capabilities to ensure good technology deployments and practices. Using a combination of IPS and IDS technologies will clearly raise the level of visibility and control for corporate networks.

This is where the suggestion of IPS and IDS technologies existing in harmony comes to bear. The recommendation of this paper is to strategically place IPS technology at the perimeter of the corporate network to help in preventing zero day attacks such as worms or viruses through anomaly based rules as well as signature based inspection of packets. The use of a properly tuned and managed IPS solution at all corporate ingress/egress points will help ensure that the newest and previously identified threats are dropped at the perimeter. As new technologies and applications are developed it is critical that the IPS team is involved through development to ensure that legitimate traffic is allowed to pass. There is typically greater latitude for traffic being dropped or stopped at the perimeter of the network than within the network. This internal network uptime is where the deployment of IDS technology is still critical. Most IDS architectures provide a passive means of collecting and identifying malicious or unknown activity and alerting a team to begin investigation of such activity. The traffic continues to pass and business continues normally but in this case any suspicious activity is flagged for investigation. Using this type of architecture promotes uptime while also emphasizing the need for monitoring the insider threat.

Having an IPS deployment in the outer portions of the network will provide the preventative measures and control needed to combat new and existing threats while including an IDS inside of the firewall and at critical internal network nodes will provide visibility and confirmation as to inside activity. The costs associated with this type of deployment are far less than those needed to deploy both technologies in parallel. A key aspect that we need to cover is staffing and training because people are a key resource needed in either of these deployments to be successful.

Staffing and training

One of the biggest challenges today is finding and retaining qualified and skilled security staff. Deploying either IPS or IDS technology requires specialized skills that typical network and systems administrators do not have. Usually a security expert comes from a background that includes work experience in either

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

networking or systems administration and sometimes both. However, the additional and specialized skills associated with security analysis and reporting are not typically skills that an employee develops unless they receive this specialized training through courses or being part of a security team. Because of the relatively new IPS technology there are few generic courses available other than vendor specific training. It is granted that many of the skills associated with IDS support are directly mapped to supporting IPS technologies; however, there are a few aspects that are unknown and will only be developed over time.

Companies on shoe string budgets or that do not currently have a security architecture in place will find staffing and training most challenging. These companies will probably cannibalize their systems and network teams to build the group needed to support IPS and IDS technologies. Depending on the group initiative and support of management for this type of organization will determine the success of an IPS and/or IDS deployment. Companies with fully staffed security groups will also find the challenge of finding, training, and retaining highly skilled engineers to be daunting when adding IPS to an existing IDS architecture.

A key area that will surely receive additional coverage in the near future will be the reshaping of IT staffs to meet emerging security requirements. There are companies that are realizing the need to develop staff to address the various compliance issues being levied on their organizations by federal agencies. There is also an area that hasn't been discussed that will require the attention of IT managers and that is how staff requirements will change as technologies change. Currently the defense against viruses and worms usually falls on the shoulders of systems administrators to patch and maintain virus definitions on all server and desktop systems. Most companies also employ analysts and trainers that provide communicate and training to users on awareness to help avoid the spread of viruses and worms.

Some analysts could argue that with the implementation of a properly configured and maintained IPS architecture, a company will reap the benefits of needing fewer desktop administrators and system administrators currently required to keep up with patches and anti-virus definitions in response to worm and virus releases. This change could easily result in retooling these network and systems administrators as well as other key IT staff to acquire the skills needed to manage and support a new security environment.

Conclusion

There are many technologies in the market today to help companies fight the inevitable network and system attack. Having IPS and IDS technologies are only two of many resources that can be deployed to increase visibility and control within a corporate computing environment. The most important aspect of security is defense in depth. The term has been used in almost all security papers in one form or another with the underlying concept of providing multiple levels of

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

security. There are verify few companies that employ every security solution and there is a reason. The concept of defense in depth is the emphasis on using the best defensive technologies and mechanisms within your organization to obtain the appropriate security environment. Most companies fall within a few similar security architects but those architectures usually differ based on business requirements and potential risks.

Choosing the appropriate security architecture is the most important goal for any company. This paper suggests an architecture that employs both IPS and IDS technologies used together to positively influence an organizational security posture. The goal of this paper was to show how IPS technology could safely and efficiently be positioned at the perimeter to help manage the visibility and control of intrusions and attacks. The second goal was to show the huge benefit of leveraging IDS technology to monitor internal networks while providing the least intrusive method for identifying possible internal threats. Using both technologies in harmony will provide the needed perimeter and core defenses to combat zero day and existing threats while also having the visibility into internal networks with the ability to provide forensic data and trend analysis.

References

Corporate White Paper. "Deploying and Tuning Network Intrusion Detection Systems." Intrusion.com White Paper. 2001 (2004): 2 – 16.

Eagle, Liam. "Enabling the Defense in Depth Security Strategy." The Web Host Industry Review. 16 April 2003. URL: http://thewhir.com/features/depth-security.cfm (6 Jan. 2004).

Tünnissen, Jacco. "Intrusion Detection, Honeypots and Incident Handling Resources." Honeypots.com. 13 January 2004. URL: http://www.honeypots.net/ (17 Jan. 2004).

Chuvakin, Anton. "Network IDS Shortcomings:
Has NIDS Reached the End of the Road?" SC Infosec Opinionwire. 6 February 2002. URL: http://www.infosecnews.com/opinion/2002/02/06_02.htm (12 Jan. 2004).

"Intrusion-prevention system." Wikipedia. 15 December 2003. URL: http://en.wikipedia.org/wiki/Intrusion-prevention_system (7 Jan. 2004).

Taylor, Laura. "Intrusion detection in not intrusion prevention." ZDNet Australia. 9 February 2004. URL:

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

http://www.zdnet.com.au/insight/0,39023731,20267597,00.htm (11 Feb. 2004).

Desai, Neil. “Intrusion Prevention Systems: the Next Step in the evolution of IDS.” Security Focus. 27 February 2003. URL: http://www.securityfocus.com/infocus/1670 (14 Jan. 2004).

“Real-time Network Awareness.” Sourcefire. February 2004. URL: http://www.sourcefire.com/products/rna.html (14 Jan. 2004).

Briere, Daniel and Bacco, Claudia. “Intrusion Prevention Systems complete security”. Network World Fusion. 15 October 2002 URL: http://www.nwfusion.com/edge/columnists/2002/1015bleed.html (18 Jan. 2004).

Lindstrom, Pete. "Guide to Intrusion Prevention.” Information Security Magazine October 2002 (2004): 38-45.

Information Assurance Solutions Group. "Defense in Depth.” National Security Agency White Paper. January 2004 (2004): 1-5.

Snyder, Joel. "Turning the Network Inside Out." Information Security Magazine June 2003 (2004): 28-42.

Fratto, Mike. "Inside the NIP Hype War." Network Computing Magazine September 2003 (2004): 38 - 58.

Snyder, Joel. “Taking Aim.” Information Security. January 2004. URL: http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss306_art540,00.html (6 Feb. 2004).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced