Global Information Assurance Certification Paper

NIDS – should you do without it?

Swee Keat Tan
Version 1.0
Security Essentials Version 1.4 (Option 1)
January 13, 2003

Abstract

One of the misconceptions about network security is that a firewall equals protection. Firewall is no 'silver bullet' and security is definitely more than a firewall. Security misconception often creates opportunity for attacks and to protect against many intrusions/attacks is to remove this opportunity. So immediately after a Firewall implementation, the next security implementation should be a Network-based Intrusion Detection System (NIDS). NIDS provides the monitoring mechanisms to detect misconfiguration of Firewall, violation of security policy, Network Service attacks and an attack in progress.

Having been a security consultant myself for many years, I am of the opinion that any organization that is not protected by NIDS should be considered as operating in a vulnerable environment. Having said that, one should not be misconstrued that Host-based IDS (HIDS, the other type of Intrusion Detection) is no better than NIDS as each has its own respective usage and benefits under different environments. Nowadays, it is a common misconception by most organizations that NIDS is an 'optional' or 'nice-to-have' piece of device within their environments. As a result, I would like to bring to their attention that NIDS offers a lot more benefits which organizations may not be aware of; hence making it a must-have device in order to better secure their environments after the Firewalls.

This paper focuses on the 'what', 'why', consideration factors and issues of Network-based Intrusion Detection System (NIDS) and that NIDS should be considered as an important security device to have in most organizations.

Introduction – IDS in a nutshell

Intrusion Detection System (IDS) is the real-time monitoring of network/system activities and the analyzing of data for potential vulnerabilities and attacks in progress; basically picking up where Firewall leaves off. Firewall, usually the first component of any perimeter defense, does a good job of keeping the 'bad guys' out and IDS's task is to ensure only the 'good guys' are assessing the network [**23**].

IDS is a handy tool for detective analysis of intrusion attempts. It does not block any traffic nor take any active measures to stop an attack. One of the major benefits about having an IDS is that it can correlate events over time and alert the security administrator on the following: - *an attack in progress, which area of the network is under attack, source of an attack and identify the*

nature of the attack. Apart from being used as an intrusion tool, IDS can also be used to create sampling of traffic patterns for network review.

Types of IDS

IDS comes in two flavors:

- Host-based Intrusion Detection System (HIDS)
- Network-based Intrusion Detection System (NIDS - also known as 'Packer Sniffer').

It is not really a question of which one is better as both of them serve different purposes.

I have had experiences in the past with organizations claiming that they do not require a NIDS since a Firewall is already in place. NIDS and Firewall serve different purposes so it is not seen as a choice between the other. Of course, if you are allowed to choose only ONE, then it will definitely be a Firewall as it has a chance of actually stopping an attack whereas an IDS functions only to DETECT and to ALERT whenever there is suspected intrusion. One must remember that a Firewall alone is not enough and a NIDS on its own is also not enough but having these two products together will be the best option.

Detection Methods

On the method of detection, IDS uses two approaches, namely signature-based and anomaly-based (also known as 'behaviour-based' or statistical intrusion).

- Signature-based commonly used in most IDS, it compares packets to a list of "signatures" known to represent an intrusion/attack. With new attacks ever increasing, organizations MUST ensure having the latest signature downloaded. This is similar to anti-virus implementation where users must ensure that they have the latest signature to protect from the latest viruses.

- Anomaly-based approach compares the behavior of the packets to a list of accepted (or suspicious) activities and alert if it looks suspicious. By analyzing activities occurring outside the normal clipping levels, evidence of events such as an in-band signaling, an intrusion or other system abuses could be detected.

In general, signature-based approach is best at identifying and repelling known intrusions/attacks while anomaly-based is best at looking at intrusions/attacks not listed in the signatures. So, which approach to use? My recommendation is to use a combination of signature-based and anomaly-based to be effective. If the signature-based misses an attack, it might be detected by the anomaly-based and vice-versa.

Various brands of NIDS

There are various brands of NIDS to choose from either commercial products or freeware products.

- Common brands of commercial products include products from vendors such as ISS RealSecure, Computer Associates eTrust IDS, NFR Network Intrusion Detection Systems, Symantec Corp.'s NetProwler, Sourcefire, etc.

  whereas,

- Common freeware products are SNORT, Tcpdump, Ethereal, etc.

We often heard of the phrase '*If it is free/open source then it will not be better*'. There will always be a question of whether freeware is any better than the commercial ones. Both categories have their pros and cons but what I feel as important is to have a skillful person to administrate the NIDS **FULL-TIME** doing the day-to-day tasks making sure the IDS is updated and tuned.

What to look for in an IDS

In the article by Mikhail Gordeev [**25**], it gives a very good description of what an IDS should accomplish: -

- *Dynamically prevent a damage that detected intrusions could cause*
- *Dynamically mitigate a damage that detected intrusions could cause*
- *Identify an activity that could lead to a more serious attack*
- *Identify an attack perpetrator*
- *Discover new attack patterns*

Apart from fulfilling the above tasks, an 'ideal' IDS should have the following requirements: -

- *Accuracy* – legitimate action in a system environment should not be treated as an anomaly or a misuse
- *Performance* – high performance in carrying out a real-time intrusion-detection
- *Completeness* – never fail to detect an intrusion
- *Fault tolerance* – resistant to attacks and their consequences
- *Timeliness* –analysis tracking as quickly as possible

Specifications for a NIDS

NIDS is extremely resource hungry in terms of processing power, memory and disk space. Due to this, it is strongly recommended to run the NIDS on a

dedicated highly stable machine. The following are the recommended specifications for a NIDS implementation: -

- Operating System (OS)

  One of the benefits of NIDS is that it is OS-independent and can run on Windows 2000, Linux, etc. The important thing is to ensure that latest patches are applied with strong security settings enabled. Furthermore, OS must be configured in accordance with the recommended best practices for stability. Network Interface Card (NIC) preferably must be configured in the promiscuous mode so attackers are not aware of the presence of this NIDS.

- Processor

  As processing power required is very high for NIDS, hence the higher the processor power the better is the processing. Anything above Pentium III with 500 MHz is recommended. Dual processors is highly recommended.

- Memory

  Memory utilization is extremely high, hence the more memory the better it would be. Minimum memory requirement should be one Gigabytes for better performance purposes.

- Disk Space

  For a NIDS to function to its best, it should be able to log all traffics. Hence, as the logging activities become heavier, the more disk space is required. It is recommend that a minimum of 40 GB of disk space is required. Note that logging is important and necessary for forensics use as well.

Due to the nature of NIDS is to operate in a 24 x 7 environment, a very stable and robust machine should be used. I would recommend 'Industrial PCs' be used for this purpose. 'Industrial PCs' come with quality and redundancy items such as power supply and usually have gone through strenuous quality assurance test making them as the most reliable machine to run a 24 x 7 environment.

Common issues with NIDS

The following are some brief description of the common issues that apply to both HIDS and NIDS: -

- False positive (or false alarm) is when an IDS classifies as a possible intrusion when it is actually a legitimate action. False positive is a nuisance similar to a smoke detector that sounds an alarm even when there is no fire and tendency for users to ignore it totally. One should try to eliminate this, if not to minimize as many of these errors as possible.

- False negative occurs when an intrusive action has taken place, but the IDS allows it to pass through as non-intrusive/behavior. False negative can be considered even more serious than false positive as it gives the users a false sense of security – in which an intrusion might had happened but the IDS does not generate any alerts.

Based on my observation, many organizations installed their NIDS using only the 'signature-based' approach and expect the NIDS to report real intrusions, without any fine tuning being carried out. Within a short time frame, they are faced with many false positives and started to ignore them. The NIDS is then left idle for a long period of time with no one to administrate it and later even forget about the existence of the NIDS. Best of all, when they are attacked, the NIDS is blamed for missing out on generating alerts.

Limitations of NIDS

NIDS does have its shortcomings that limit its effectiveness: -

- False Positives (or false alarms)

  IDS (HIDS & NIDS) known for their frequent false positives create two problems: 1) 'Crying Wolf' syndrome where real attacks may be ignored, and 2) valuable time of security staff wasted to filter out these false positives without potentially missing an attack/intrusion.

- IDS (HIDS & NIDS) as a reactive device

  As IDS does not block an attack, hence a substantial amount of time may pass between the alert and the remediation. This potentially would allow the attacker to do irreversible damage during this time.

- Data Overload

  Tremendous amount of data generated by the IDS is expected and will be impossible for an analyst to efficiently analyze the data. Though not a must but organization should consider employing data mining method which play an important role in the area of data reduction. Data mining can help improve intrusion detection by adding a level of focus to anomaly detection. By identifying bounds for valid network activity, data mining can assist an analyst to distinguish attack activity from common everyday traffic on the network.

- Unable to read encrypted traffic

  Encrypted traffic would not be 'seen' by the NIDS. However, having a HIDS installed at the server will help on this as the traffic would be decrypted once it reaches the server.

- Weakness of the signature-based approach

- Failure to characterize slow attacks that are extended over a long time period.
- Dependency on 'attack' signature file which most vendors are not able to develop in time to counter new attacks.

- Weakness of the anomaly-based approach

  Failure to detect an attack that does not significantly change the system operating characteristics (false negative) or may falsely detect a non-attack event that had caused a momentary anomaly in the system (false positive).

- Not functioning at its best on high-speed bandwidth

  With the upcoming of high-speed network (e.g. 1 Gigabit), NIDS might not be able to process all the packets and could miss out some attacks. Solution to this would be to invest on a device such as TopLayer ('flow-mirror') [**10**] that could filter the required traffic to one or a few NIDS for processing. This help in the balancing of the NIDS's load hence enable the NIDS to function at its best even on a high-speed traffic.

- NIDS not at its best in a switched environment

  NIDS will not work in a switched environment without further configuration of the switch compared to a hub. This is due to the intelligence built into the switch that further configuration is needed so that all traffics in the switch to go through a particular port termed as span or mirrored port. However, with this configuration, network performance will be compromised.

- Subtle and stealthily attacks

  It is very difficult for NIDS to detect subtle and stealthily attacks as these attacks typically fall below the 'noise' threshold on a network. It requires a skillful person who knows the network very well, always on the job of fine-tuning the NIDS to detect such an attack.

Other usage of NIDS

NIDS is also heavily deployed in the following environment:

- HoneyPot

  HoneyPot is used to attract attacks into their environment with the intent of learning on the attacker's approach. NIDS setup in a promiscuous mode is used to monitor the attacker's activities.

- Managed Security Monitoring (MSM)

  A very niche service focussing on a 24 x 7 outsourced intrusion detection which relies heavily on IDS (HIDS and NIDS) in their job. Have been gaining popularity recently and company such as Counterpane Internet Security is best known for its MSM services.

Why NIDS

> *"For many organizations, NIDS is the logical starting point. Compared to other IDS technologies, NIDS provides the broadest impact on network security, the shortest time to deployment and the most network management information for the security dollar spent* [**18**]".

I would like to emphasize that the NIDS be placed outside the Firewall (or at the DMZ) in order to benefit from its deployment tremendously. A NIDS in this zone provides the monitoring of all traffics from the organization's connection to the Internet with immediate feedback regarding the efficiency of a network's security in real time. NIDS at the internal network is also of high value but my recommendation would be to monitor at the Internet gateway as the first priority due to the many benefits as listed below: -

- By examining all packet headers for signs of malicious and suspicious activities, NIDS is able to detect attacks that HIDS misses such as Denial-of-Service (DoS) and port-scan.

- Increased value at the DMZ

  Internet Web servers normally hosted at the DMZ zone are extremely popular targets for computer attacks. The value of the DMZ (Demilitarized Zone) can be increased though placing a NIDS. Possible intrusion could be detected and alerted by the NIDS, hence minimizing damage early in the attack progress.

- Report of successful and unsuccessful attacks

  The key to improving network security is to better understand attacks regardless they have been successful or unsuccessful. In fact to launch a successful attacks, attackers need much information regarding the victims such as network topology, software versions, etc. NIDS at the DMZ is able to detect such information gathering by the attackers and generate alerts. Normally we do not see many organizations being informed of such 'unsuccessful' attacks and malicious intent as most of them treat these information as irrelevant or of less important. Knowledge on this is critical to better prepared themselves for future similar attacks.

- Fast detection, notification and response

  Since NIDS detects in real-time malicious and suspicious attacks as they occur, fast action on the alerts could possible neutralize attacks.

- NIDS provides an organization a better understand of their network environment. Knowledge about their environment is of paramount advantage in keeping their site well protected from intruders/attackers.

- Without NIDS in place, it is difficult to determine if the network has been hacked or not.

- Forensics usage - Difficult for an attacker to remove evidence. Unless attackers can compromise the IDS, they cannot remove the evidence.

As stated in Counterpane Internet Security's white paper [**15**] that "*Real-world security includes prevention, detection and response. If the prevention mechanisms were perfect, you would not need detection and response"*. However, this is not so as no prevention mechanism is that perfect. Good detection and response via NIDS is necessary to make up for imperfect prevention.

Things to consider when implementing a NIDS

NIDS implementation requires quite a lot of considerations such as the placement, logging, tuning and event correlation. It seems as though many companies believe NIDS once installed will provide alert when there is a real attack. Unfortunately there are many things that can have "attack-like" qualities but turn out to be things as simple as a malfunctioning router.

- False Positives and False Negatives problems

  The biggest problem of IDS management is separating true threats from all those false positives (false alarms). These false positives are so troublesome that eventually you will either turn it off or ignore it altogether.

  Hence, the challenging task is to reduce the occurrence of both the false positive and false negative problems. This is what we termed as 'fine-tuning' your IDS, which is often neglected in many organizations due to lack of dedicated, trained, skillful personnel manning the IDS. Fine-tuning is to investigate and delve deeper into the suspicious events reported by the NIDS and to determine whether it is a real or false alert, hence separating false alarms from real attacks.

  In the book '*Intrusion Detection'* [**2**], it explains the needs to understand what is 'normal' for that environment and investigate the deviations from this baseline, hence eliminating as much as possible all of the false positives and false negatives. Unless you continuous fine-tune your NIDS, which is a very time-consuming process - *most attacks will go completely unnoticed*.

- Full-time dedicated skillful Intrusion Detection Analyst

  IDS is unlike firewalls and anti-virus software, in that it requires constant monitoring to be effective. Firewalls need occasional tweaks and anti-virus needs updating, but IDS needs 24/7 monitoring and fine-tuning if the dreaded false-positives are to be avoided [**22**].

  NIDS is a great tool but it requires skilled personnel to interpret the information (logs), to identify the real intrusions and to act fast enough to prevent further damages. The key to ensuring the efficiency and

effectiveness of a NIDS is largely dependent on the availability of a skillful Intrusion Analyst within the organization to operate and maintain it continuously. The following highlight some of the minimum basic requirements that the Intrusion Detection Analyst should have: -

- ❖ Having the necessary knowledge of the networks being monitored so that the determination of misuse versus anomalous is clear
- ❖ Differentiate between fake attacks and real attacks
- ❖ Awareness of the latest security breaches affecting the network
- ❖ Frequent check and download for latest signature from vendors
- ❖ Knowledge in writing customized signatures rather than dependent on the NIDS vendor.

In an environment where the skillful Intrusion Detection analyst is not available, organizations may consider engaging Managed Security Service Providers (MSSPs) as the cost-effective solution [**1, 22**].

- Pro-active approach

  As NIDS merely DETECTs and ALERTs so it will be important to respond immediately upon a real intrusion to make it more difficult for an attacker to attack. I strongly believe this approach if being practiced (albeit difficult but not impossible) as the key strength a NIDS could deliver confidently in preventing attacks.

- Data mining for deeper analysis is expected for the IDS to be effective

  Data mining can actually reduce the amount of data stored and sorted by culling unnecessary data from the analysis. *It is the ability to take data and pull from its patterns or deviations, which may not be seen easily to the naked eye, also term as knowledge discovery* [**24**].

Placement of the NIDS

This has been answered in my previous section that the best place for a NIDS is at the edge of the network. As mentioned, the DMZ area is the most vulnerable environment and must be monitored at all times for possible intrusions or threats and speedy action upon detection of intrusions is required.

Having an NIDS outside the firewall is like the analogy of knowing who is knocking on the door (*connecting to your system*), whereas for NIDS after the firewall is to see those that are allowed access (*using the system*).

Of course, the better solution is to have NIDS both inside the network and at the edge of the network.

To shun or Not to shun

Shunning is the term used to configure the NIDS to set rules in the Firewall/router automatically. First thought for most security administrators would be to jump to this shunning process. However if you think further, it may cause more problems due to the many false positives that will be detected (which NIDS is known for). One must remember that attacks such as Port and ping scans, DoS and DDoS are not good candidates for shunning as the source IP addresses can be spoofed, hence can trigger potential denial-of-service for the organization. However, we could still identify attacks that are distinct enough such as 'remote buffer overflow'. Also, note that it takes a certain amount of time for the NIDS and the Firewall/router to complete the rule filter change.

There is suggestion that for shunning to work best, it should be on a 'timed event'. That is when the Firewall/router does block traffic, it would only be from a specific IP address and only for a few seconds or minutes, depending on the severity of the attack. So when an attacker is using a legitimate user's IP address, traffic is only disrupted for a short period of time.

Next Generation NIDS

The next generation of NIDS is to concentrate on a more proactive approach, which will allow the system to thwart attacks. This technology is called Intrusion Prevention System (IPS) [**9, 11, 12**]. Already, we see vendors such as Top Layer, Okena, Intruvert selling this technology. This system works in the INLINE mode, hence the possibility of a single line of failure. I am not in favor (uncomfortable) of such approach as I feel that if an event is important enough to be automatically blocked, then I think it is equally important for further investigation to avoid the possible denial-of-service for the organization due to the automatic block. As highlighted by Bruce Schneier, CTO of Counterpane Internet Security that *you NEED PEOPLE to assess the threat*.

I would say IPS is good when compared to HIDS but not NIDS. A very valid reason for IPS as in addition to offering strong security is that administrators *do not need to rush to deploy any new patches for fear of a security threat by not deploying the latest patches*.

Conclusion

Having NIDS will definitely necessitate hiring new IT (Security) professionals and will require loads of administrative attentions as NIDS requires continuous administration and fine-tuning to be effective.

However, I believe that the benefits of having NIDS far outweigh its disadvantages, as the best way to identify and often prevent a network attack is through a NIDS.

Hence, having a NIDS is very important but if organizations do not have the expertise to handle it, they should consider outsource to MSSPs as they have the aggregate of expertise which is difficult to have and costly to acquire and maintain in-house within organizations. The real skills and security comes from maintaining the solutions and not from installing it. In fact, surveys have shown that it costs much lower to outsource security tasks than to maintain the security personnel in-house.

Based on the findings of the "2002 Computer Crime and Security Survey" [**16**] confirms "*that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting*". We have also seen substantial growth in sales for security products yet we still see attacks continue to happen at an increasing pace. This is to prove my point that *security is not about buying security products*. It should be the monitoring for any abnormal traffic and known attack pattern via NIDS and triggering an alert for further investigation should be the way to go in preventing an attack. Regardless, NIDS (at the DMZ) is the best solution available in the real world that allows any measure of proactive protection and attack response. Sure it is not foolproof and automatic as it still requires human interaction, but NIDS is able to provide unobtainable level of network protection and it will only get better with continuous fine-tuning. Consider the state of the network security today, without using NIDS, how else can you know if you have been attacked?

It is certain that NIDS has become an important role in providing for a secure network architecture. It is essential for organizations to realize that it is less expensive to be prepared than to recover from complex business interruption after the fact, hence the saying '*Prevention is better than cure*'. So, should an organization do without NIDS?

References

[1] Andress, Mandy. Surviving Security: How to Integrate People, Process, and Technology. Sams Publishing. 2002. 166 - 183

[2] Rebecca Gurley Bace, Intrusion Detection. Macmillan Technical Publishing. 2000. 79 – 133, 165, 217 - 232

[3] Chris Brenton, Mastering Network Security. Sybex inc. 1999. 254 – 271

[4] Ronald L. Krutz and Russell Dean Vines, The CISSP Prep Guide, John Wiley & Sons Inc, 62 – 63, 233

[5] Intrusion Detection FAQ, SANS Institue Resources, URL: http://www.sans.org/resources/idfaq/what_is_id.php

[6] Mike Bobbit, “Inhospitable Hosts – Attackers may try the door, but Intrusion Prevention tools won’t let them in”, October 2002 URL: http://www.infosecuritymag.com/2002/oct/cover.shtml

[7] Anne Saita, “Paying For Protection – Customers see immediate results, buy time to patch at their leisure”, October 2002 URL: http://www.infosecuritymag.com/2002/oct/casestudy.shtml

[8] David Newman, Joel Snyder and Rodney Thayer, “Crying wolf: False alarms hide attacks”, 24 June 2002, URL: http://www.nwfusion.com/techinsider/2002/0624security1.html

[9] Next Generation Intrusion Detection Systems (IDS), Intruvert Networks Inc, March 2002 URL: http://www.intruvert.com/technology/white_papers.htm

[10] Network Intrusion Detection Systems: Important IDS Network Security Vulnerabilities, Top Layer Networks Inc, September 2002 URL: http://www.toplayer.com/pdf/WhitePapers/wp_network_intrusion_system.pdf

[11] Top Layer Advances Network Intrusion Prevention With Attack Mitigator IPS Suite, Top Layer Networks Inc, 11 November 2002 URL: http://www.toplayer.com/content/news/pr/2002/111102.jsp

[12] 'Intrusion prevention' raises hopes, concerns, Network World Fusion, 04 November 2002 URL: http://www.nwfusion.com/news/2002/1104prevention.html

[13] Strategies to Reduce False Positives and False Negatives, SecurityFocus, 11 September 2001 URL: http://online.securityfocus.com/cgi-bin/sfonline/infocus.pl?id=1463

[14] Strategies to Reduce False Positives and False Negatives in NIDS, Part Two, SecurityFocus, 27 September 2001 URL: http://online.securityfocus.com/infocus/1477

[15] Managed Security Monitoring, Counterpane Internet Security, URL: http://www.counterpane.com/msm.html

[16] Computer Security Issues & Trends Vol. Viii, No.1, Spring 2002, URL: http://www.gocsi.com/press/20020407.html

[17] 'Intrusion Prevention Will Replace Intrusion Detection', Gartner, 30 August 2002 URL: http://www.gartner.com/reprints/intruvert/109596.html

[18] ‘Network Intrusion Detection, part 1: Laying the groundwork’, SearchNetworking.com, 22 Jun 2001 URL: http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci803169,00.html

[19] 'Network Intrusion Detection, part 2: Maximizing the value of your IDS', SearchNetworking.com, 29 Jun 2001 URL: http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci803173,00.html

[20] 'Recommendations for deploying an intrusion-detection system', SearchNetworking.com, 01 Nov 2001 URL: http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci799689,00.html

[21] 'Intrusion Detection, the next generation: Making it practical', SearchNetworking.com, 16 Jul 2001 URL: http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci803055,00.html

[22] 'It makes sense to outsource IDS, expert say', SearchSecurity.com, 12 Nov 2002 URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci862918,00.html

[23] 'Intrusion-detection systems sniff out security breaches', SearchSecurity.com, 14 Feb 2002 URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci802278,00.html

[24] 'Data Mining in Intrusion Detection', SANS Institute Resources, 24 Oct 2000 URL: http://www.sans.org/resources/idfaq/data_mining.php

[25] Mikhail Gordeev, 'Intrusion Detection: Techniques and Approaches', URL: http://www.infosys.tuwien.ac.at/Teaching/Courses/AK2/vor99/t13/